8-60 Machines virtuelles limitées en ressources réseau

Les applications utilisant beaucoup le réseau rencontrent souvent des goulots d'étranglement dans les segments de chemin d'accès extérieurs à l'hôte VMware ESXi :

- Exemple : les liaisons WAN entre un serveur et un client

Si vous pensez qu'une machine virtuelle est limitée en ressources réseau, procédez comme suit :

- Vérifiez que VMware Tools est installé. Les pilotes réseau améliorés ne sont disponibles que si VMware Tools est installé.
- Mesurez l'efficacité de la bande passante entre la machine virtuelle et le système homologue.
- Recherchez d'éventuels paquets ignorés, en réception comme en transmission.

Tout comme les problèmes de performances des ressources disque, les problèmes de performances réseau sont généralement causés par la saturation d'une liaison réseau entre client et serveur. Exécutez un outil comme Iometer ou effectuez un transfert de fichiers volumineux pour tester la bande passante réelle.

Les performances réseau dépendent de la charge de travail applicative et de la configuration du réseau. La présence de paquets réseau abandonnés est le signe d'un goulot d'étranglement sur le réseau. Pour savoir si certains paquets sont ignorés, accédez aux diagrammes de performances avancés et examinez les valeurs des compteurs réseau « droppedTx » et « droppedRx » associés à une machine virtuelle.

En règle générale, plus les paquets réseau sont volumineux et plus le réseau est rapide. En effet, comme les paquets sont importants, le nombre de paquets transférés est moins élevé, ce qui réduit d'autant la capacité CPU requise pour traiter les données. Cependant, une taille importante des paquets peut entraîner dans certains cas une latence de réseau élevée. Lorsque les paquets réseau sont de petite taille, le nombre de paquets transférés est plus élevé, mais le réseau ralentit, car le traitement des données requiert plus de capacité CPU.

8-61 Laboratoire 14 : Surveillance des performances des machines virtuelles

Utiliser les outils de surveillance du système pour refléter la charge de travail CPU

1. Créer la charge de travail CPU
2. Utiliser des diagrammes de performances pour surveiller l'utilisation des ressources CPU
3. Annuler les modifications apportées aux machines virtuelles

8-62 Rappel des objectifs de la formation

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

8-63 Leçon 4 : Utilisation des alarmes

8-64 Objectifs de la formation

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

- Créer des alarmes associées à des déclencheurs basés sur des conditions
- Créer des alarmes associées à des déclencheurs basés sur des événements
- Afficher les alarmes déclenchées et en accuser réception

8-65 À propos des alarmes

Une alarme est une notification émise en réponse à certains événements ou conditions relatifs à un objet de l'inventaire.

Il existe des alarmes par défaut pour les différents objets d'inventaire. De nombreuses alarmes par défaut sont définies pour les hôtes et les machines virtuelles.

Vous pouvez créer des alarmes personnalisées pour un vaste éventail d'objets d'inventaire :

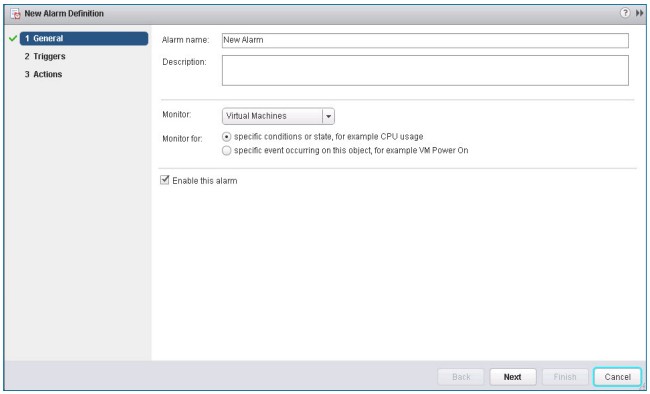
- Les machines virtuelles
- Les hôtes, les clusters et les Data Centers
- Les banques de données et les clusters de banques de données
- Les réseaux, les commutateurs distribués et les groupes de ports distribués

Les alarmes sont des notifications émises en réponse à certains événements ou conditions relatifs à un objet de l'inventaire. VMware propose un ensemble d'alarmes prédéfinies pour la plupart des objets de l'inventaire vCenter Server. Par exemple, il existe des alarmes portant sur l'utilisation des ressources CPU et mémoire pour les hôtes, les machines virtuelles et les pools de ressources. Vous pouvez également définir des alarmes personnalisées pour les machines virtuelles, les hôtes, les clusters, les Data Centers, les banques de données, les clusters de banques de données, les réseaux, les commutateurs distribués et les groupes de ports distribués.

Les alarmes prédéfinies peuvent être configurées. Cependant, si une alarme prédéfinie n'est pas à même de gérer les conditions, états ou événements que vous souhaitez surveiller, nous vous recommandons de définir des alarmes personnalisées plutôt que de modifier des alarmes prédéfinies.

8-66 Paramètres des alarmes

Pour surveiller votre environnement, vous pouvez créer et modifier des définitions d'alarme dans vSphere Web Client.



Sur la page « General », donnez un nom à l'alarme et associez-lui une description et un type.

Vous pouvez également sélectionner l'élément à surveiller :

- « Specific conditions or state » : l'alarme basée sur des conditions. Il est possible de créer des alarmes basées sur des conditions pour les machines virtuelles, les hôtes et les banques de données.
- « Specific events occurring on this object » : l'alarme basée sur des événements. Il est possible de créer des alarmes basées sur les événements pour les machines virtuelles, les hôtes, les clusters, les Data Centers, les banques de données, les clusters de banques de données, les réseaux, les commutateurs virtuels distribués et les groupes de ports virtuels distribués.

Vous pouvez également utiliser la page « General » pour activer ou désactiver l'alarme, en sélectionnant ou désélectionnant la case à cocher **Enable this alarm**.

8-67 Déclencheurs d’alarmes

Pour fonctionner, une alarme requiert un déclencheur :

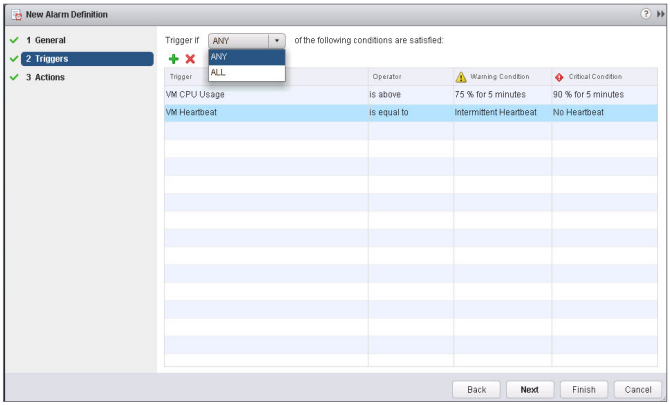
- Un déclencheur de condition ou d’état surveille l’état ou la condition en cours :
  - Exemples :
    - La taille du snapshot actuel d’une machine virtuelle dépasse 2 Go.
    - Un hôte utilise 90 % de sa mémoire totale.
    - Une banque de données est déconnectée de l’ensemble des hôtes.
- Un déclencheur d’événement surveille les événements :
  - Exemples :
    - L’intégrité du matériel d’un hôte a été affectée.
    - Une licence a expiré dans le Data Center.
    - Un hôte n’est plus associé au commutateur distribué.

Les déclencheurs d’alarmes sont configurés pour générer des avertissements et des alertes lorsque les critères indiqués sont remplis. Les alarmes sont associées à des déclencheurs d’état/de condition ou à des déclencheurs d’événement.

- Le déclencheur d’état ou de condition : surveille la condition ou l’état actuels d’une machine virtuelle, d’un hôte ou d’une banque de données. Les conditions ou états portent sur le fonctionnement, les connexions et les mesures de performances (comme l’utilisation des ressources disque ou CPU).
- Le déclencheur d’événement : surveille les événements qui se produisent suite à des opérations concernant un objet géré dans l’inventaire ou dans le système vCenter Server. Exemple : un événement est enregistré chaque fois qu’une machine virtuelle (c’est-à-dire un objet géré) est clonée, créée, supprimée, déployée ou migrée.

8-68 Configuration de déclencheurs de condition ou d'état

Les déclencheurs de condition ou d'état surveillent les mesures d'un hôte, d'une machine virtuelle ou d'une banque de données.



Comme le montre la diapositive, vous pouvez configurer un déclencheur de condition pour obtenir une alarme lorsque les cas suivants sont vérifiés :

- Le taux d'utilisation des ressources CPU par une machine virtuelle doit être supérieur à 75 % pendant plus de 5 minutes pour qu'un avertissement soit généré.
- Le taux d'utilisation des ressources CPU par une machine virtuelle doit être supérieur à 90 % pendant plus de 5 minutes pour qu'une alerte soit générée.

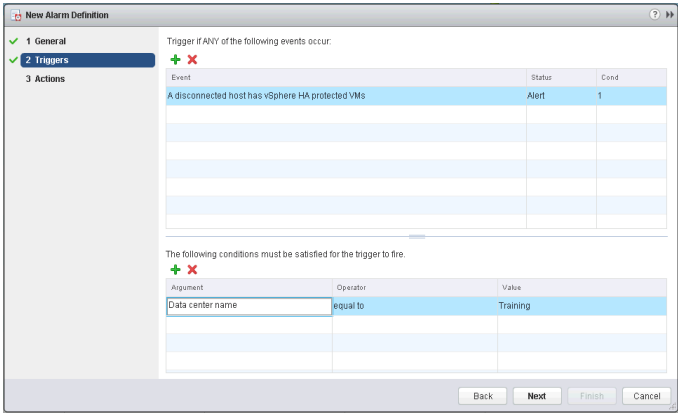
Les périodes définies permettent de garantir qu'une condition mesurée est valable et n'est pas le fruit d'un pic accidentel.

La diapositive indique également que vous pouvez configurer un déclencheur d'état afin de générer une alerte lorsqu'une machine virtuelle ne présente aucun signal de pulsation. Lorsque les conditions entraînant son déclenchement ne sont plus avérées, une alarme déclenchée se réinitialise et cesse de s'exécuter.

Si vous ajoutez plusieurs déclencheurs, vous pouvez décider de déclencher une alarme si l'une des conditions est satisfaite, ou si elles le sont toutes.

8-69 Configuration des déclencheurs d'événement

Les déclencheurs d'événement surveillent l'état actuel d'un hôte, d'une machine virtuelle ou d'une banque de données.

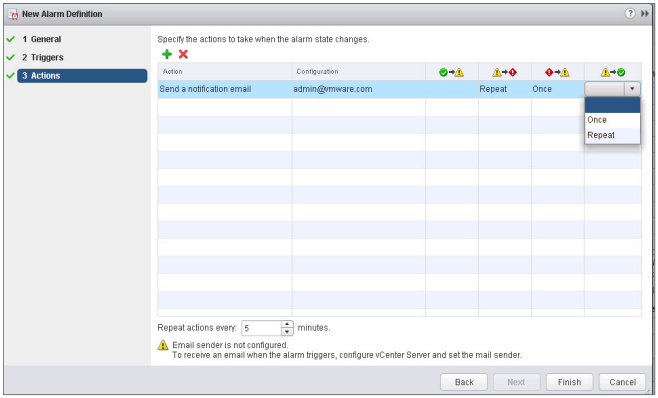


Les déclencheurs d'événement ne reposent pas sur des seuils ou des durées. Ils utilisent des arguments, des opérateurs et des valeurs pour identifier la condition de déclenchement d'une alarme. Dans l'exemple représenté, le déclencheur d'événement surveille l'événement suivant : « A disconnected host has vSphere HA protected VMs ».

Chaque fois qu'un hôte hébergeant des machines virtuelles devant être protégées par vSphere HA est déconnecté, l'alerte est déclenchée. Une condition a également été configurée pour déclencher cette alerte uniquement lorsque le client se trouve dans un Data Center nommé « Training ».

8-70 Configuration des actions

Vous pouvez définir les actions effectuées par le système lorsque l'alarme est déclenchée ou change d'état.



Une alarme est constituée d'un déclencheur et d'une action. Cette action correspond à l'opération effectuée suite à l'exécution du déclencheur (par exemple, envoi d'une notification par e-mail à un ou plusieurs administrateurs).

Dans la boîte de dialogue « New Alarm Definition », accédez à l'onglet **Actions** et spécifiez les actions que le système doit exécuter lorsque l'alarme se déclenche. Les couleurs et formes proposées permettent d'indiquer le degré de gravité de l'alarme : le cercle vert indique un niveau normal, le triangle jaune correspond à un avertissement et le losange rouge signale une alerte.

Vous pouvez définir le déclenchement d'alarmes pour signaler les changements d'état :

- La transition d'un cercle vert à un triangle jaune
- La transition d'un triangle jaune à un losange rouge
- La transition d'un losange rouge à un triangle jaune
- La transition d'un triangle jaune à un cercle vert

Pour chaque action, vous pouvez indiquer une option à associer à chaque transition de couleur :

- La valeur **Empty** indique que la transition ne suscite aucun intérêt particulier.
- La valeur **Once** indique que vCenter Server ne doit exécuter l'action qu'une seule fois.
- La valeur **Repeat** indique que vCenter Server doit répéter l'action jusqu'au prochain changement de couleur. La valeur par défaut est de 5 minutes. La valeur maximale est de 2 jours. La valeur temporelle par défaut indiquée est associée au menu déroulant **Repeat actions every**, qui figure sur la partie inférieure de la boîte de dialogue.

Chaque type d’alarme est associé aux actions suivantes :

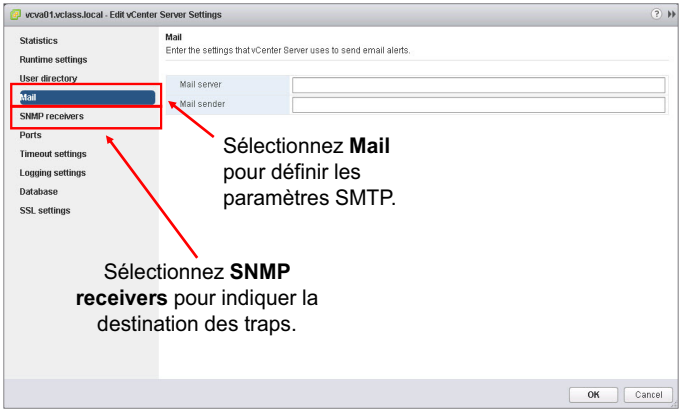
- L’envoi d’un e-mail de notification
- L’envoi d’un trap de notification
- L’exécution d’une commande

Les alarmes des machines virtuelles et des hôtes sont liées à des actions supplémentaires, par exemple :

- La migration d’une machine virtuelle
- La mise sous tension d’une machine virtuelle
- La mise hors tension d’une machine virtuelle
- Le redémarrage d’un client sur une machine virtuelle
- La suspension de l’exécution d’une machine virtuelle
- Le redémarrage d’un hôte
- L’arrêt d’un hôte

8-71 Configuration des notifications de vCenter Server

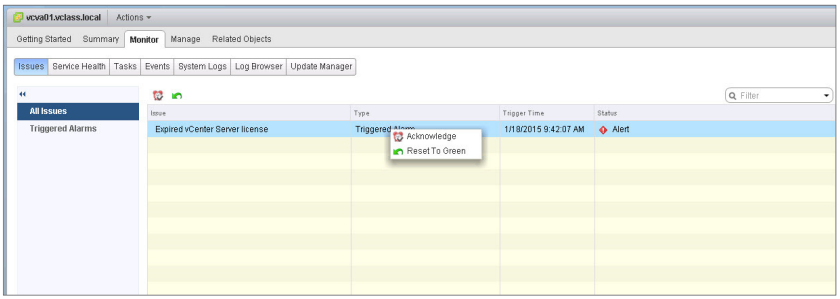
Vous devez configurer l'adresse e-mail du compte expéditeur pour activer des opérations de vCenter Server, telles que l'envoi de notifications par e-mail, en tant qu'actions associées aux alarmes.



Vous pouvez configurer jusqu'à quatre récepteurs pour les traps SNMP. Ces récepteurs doivent être configurés selon un ordre numérique. Chaque trap SNMP nécessite une communauté, un nom d'hôte et un port correspondants.

8-72 Affichage et accusé de réception des alarmes déclenchées

La fonction d'accusé de réception d'une alarme permet d'effectuer un suivi du traitement des alarmes traitées.



Lorsque vous accusez réception d'une alarme dans vSphere Web Client ou dans vSphere Client, les actions associées à cette alarme cessent de s'exécuter. Les alarmes ainsi validées ne sont ni supprimées, ni réinitialisées.

Lorsque vous accusez réception d'une alarme, vous informez les autres utilisateurs que vous prenez le problème en charge. Exemple : sur un hôte, une alarme définie porte sur la surveillance de l'utilisation des ressources CPU. Lorsqu'elle est déclenchée, elle envoie un e-mail à un administrateur. Une forte augmentation du taux d'utilisation des ressources CPU déclenche l'alarme, qui envoie un e-mail à l'administrateur de l'hôte. L'administrateur accuse réception de l'alarme déclenchée afin d'avertir les autres administrateurs qu'il prend le problème en charge, évitant ainsi l'envoi d'autres e-mails relatifs à cette alarme. Cette alarme reste cependant visible au sein du système.

8-73 Laboratoire 15 : Utilisation des alarmes

Utiliser la fonction d'alarme de vCenter Server Appliance

1. Créer une alarme de machine virtuelle pour surveiller une condition donnée
2. Créer une alarme de machine virtuelle pour surveiller un événement
3. Déclencher des alarmes de machine virtuelle et les acquitter
4. Désactiver les alarmes de machine virtuelle

8-74 Rappel des objectifs de la formation

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

- Créer des alarmes associées à des déclencheurs basés sur des conditions
- Créer des alarmes associées à des déclencheurs basés sur des événements
- Afficher les alarmes déclenchées et en accuser réception

8-75 Points clés

- Pour assurer une gestion adéquate des ressources, vSphere propose des mécanismes permettant de réduire, d'augmenter ou de maintenir l'accès à une ressource déterminée.
- vSphere veille à ce qu'une machine virtuelle ne puisse pas consommer de trop grandes quantités d'une ressource. Il octroie une quantité garantie de ressources à une machine virtuelle dont les performances sont insuffisantes, ou dont le fonctionnement nécessite une certaine quantité de ressources.
- Vous pouvez faire appel à un pool de ressources pour répartir et allouer des ressources à des machines virtuelles ou à d'autres pools de ressources.
- Une vApp est un conteneur renfermant une ou plusieurs machines virtuelles. Une vApp permet de packager et de gérer des applications corrélées.
- L'onglet **Performance** vous permet de surveiller les performances d'un hôte ou d'une machine virtuelle, en temps réel ou sur une période donnée.
- Grâce aux alarmes, vous pouvez surveiller l'inventaire vCenter Server et envoyer des notifications lorsqu'une condition ou un événement spécifiques surviennent.

Des questions ?

MODULE 9

vSphere HA, vSphere Fault Tolerance et protection des données

9-2 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

9-3 Importance

La plupart des entreprises dépendent de services informatiques tels que messagerie électronique, bases de données et applications Web. Toute défaillance de l'un de ces services peut signifier une perte de productivité et de revenus.

La configuration de services informatiques à haute disponibilité est donc un élément crucial pour assurer la compétitivité des entreprises dans les environnements économiques actuels.

9-4 Leçons du module

Leçon 1 :	Présentation de vSphere HA
Leçon 2 :	Architecture de vSphere HA
Leçon 3 :	Configuration de vSphere HA
Leçon 4 :	Présentation de vSphere Fault Tolerance
Leçon 5 :	vSphere Replication

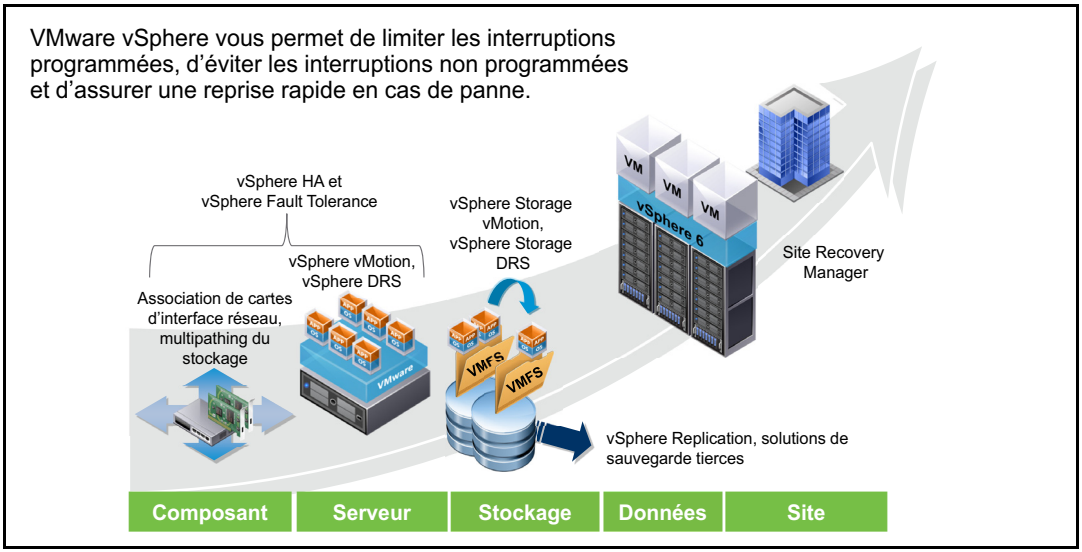
9-5 Leçon 1 : Présentation de vSphere HA

9-6 Objectifs de la formation

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

- Décrire les options à configurer pour assurer la haute disponibilité de votre environnement vSphere
- Décider des réactions de vSphere HA en cas de panne d'un hôte VMware ESXi, d'une machine virtuelle ou d'une application

9-7 Protection à tous les niveaux



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. vSphere vous offre les avantages suivants :

- Haute disponibilité indépendamment du matériel, du système d'exploitation et des applications
- Réduction des interruptions de service planifiées pour cause de maintenance courante
- Reprise automatique en cas de panne

De nombreuses méthodes permettent de garantir une haute disponibilité dans les environnements virtualisés. vSphere fait appel aux technologies suivantes pour maintenir la disponibilité des machines virtuelles exécutées dans un environnement de ce type :

- Migration des machines virtuelles
- Chemins d'accès multiples pour les adaptateurs d'E/S
- Équilibrage de la charge des machines virtuelles
- Tolérance aux pannes
- Outils de reprise d'activité

vSphere HA assure une protection de base de vos machines virtuelles en redémarrant celles-ci en cas de panne de l'hôte. vSphere Fault Tolerance offre un niveau de disponibilité supérieur dans la mesure où il permet aux utilisateurs de protéger leurs machines virtuelles contre toute perte de données, de transaction ou de connexion consécutive à une défaillance d'un hôte. Enfin, vSphere Fault Tolerance garantit une disponibilité en continu en veillant à ce que les VMs principale et secondaire se trouvent dans un état identique en tout point du cycle d'exécution des instructions de la machine virtuelle.

vSphere vMotion et vSphere Storage vMotion maintiennent la disponibilité des machines virtuelles durant les arrêts planifiés, notamment lorsque des hôtes ou des ressources de stockage doivent être déconnectés à des fins de maintenance. Grâce à la propriété d'encapsulation des machines virtuelles, la récupération du système en cas de panne du stockage s'effectue de façon simple, rapide et fiable. vSphere Storage vMotion permet notamment la prise en charge des interruptions de service de stockage planifiées qui résultent de la mise à niveau des baies de stockage vers les dernières versions du microprogramme, de la technologie ou de VMFS.

VMware vSphere® Replication™ permet à une plate-forme vSphere de protéger les machines virtuelles en mode natif, en copiant leurs fichiers de disque virtuel vers un autre emplacement dès qu'elles sont prêtes à être récupérées.

L'encapsulation des machines virtuelles est exploitée par des applications de sauvegarde tierces qui prennent en charge les sauvegardes de niveau fichier ou de l'image via vSphere Data Protection pour assurer la protection des données. Les solutions de sauvegarde jouent un rôle primordial dans les opérations de récupération exécutées en cas de suppression de fichiers ou de disques et en cas de corruption ou d'infection de systèmes d'exploitation clients ou de systèmes de fichiers.

Site Recovery Manager vous donne la possibilité de restaurer rapidement l'infrastructure informatique de votre entreprise, minimisant ainsi le temps d'interruption de l'activité.
Site Recovery Manager automatise les processus de configuration et de basculement, ainsi que le test des plans de reprise d'activité. Site Recovery Manager nécessite l'installation de vCenter Server sur le site protégé et sur le site de reprise. Site Recovery Manager requiert également, au choix, une capacité de réplication basée sur un hôte via vSphere Replication, ou une capacité de réplication basée sur la baie préconfigurée entre le site protégé et le site de reprise.

9-8 Disponibilité de vCenter Server : Recommandations

Assurez une haute disponibilité de vCenter Server et des composants sous-jacents.

vCenter Server repose sur les principaux composants suivants :

- Base de données vCenter Server :
  - Créer un cluster pour la base de données
  - Configurer la sauvegarde et la restauration en natif
- Source d'identité et d'authentification :
  - Par exemple, vCenter Single Sign-On (service inclus dans Platform Services Controller) et Active Directory
  - Effectuer la configuration avec plusieurs serveurs redondants

Méthodes permettant d'assurer la disponibilité de vCenter Server :

- Utilisez vSphere HA et vCenter Server High Availability pour protéger la machine virtuelle vCenter Server.

Pour garantir la haute disponibilité de vCenter Server, il convient d'assurer celle des composants qu'il met en œuvre :

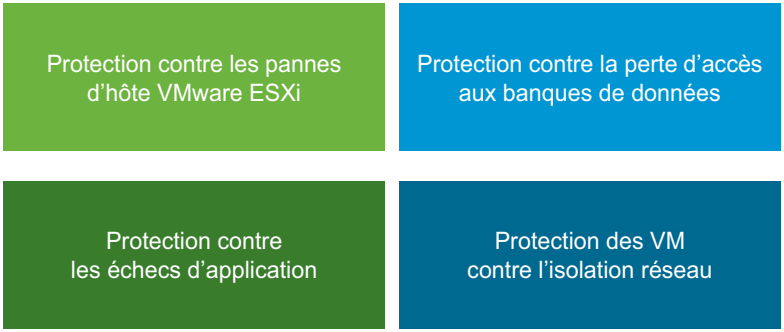
- Base de données vCenter Server
- Source d'identité et d'authentification, telle que vCenter Single Sign-On ou Active Directory (AD). vCenter Single Sign-On est l'un des services d'infrastructure communs intégrés dans Platform Services Controller. Si votre environnement exploite AD, veillez à ce que ce composant soit configuré avec plusieurs serveurs redondants.

La haute disponibilité peut être implémentée dans vCenter Server via vSphere HA, qui offre la protection requise en cas de panne matérielle ou de défaillance d'un système d'exploitation.

Pour la protection de vCenter Server Appliance, vous pouvez utiliser vCenter Server High Availability.

9-9 À propos de vSphere HA

vSphere HA utilise plusieurs hôtes VMware ESXi configurés au sein d'un cluster afin d'assurer une reprise rapide en cas de panne et une haute disponibilité à faible coût pour les applications exécutées sur les machines virtuelles.



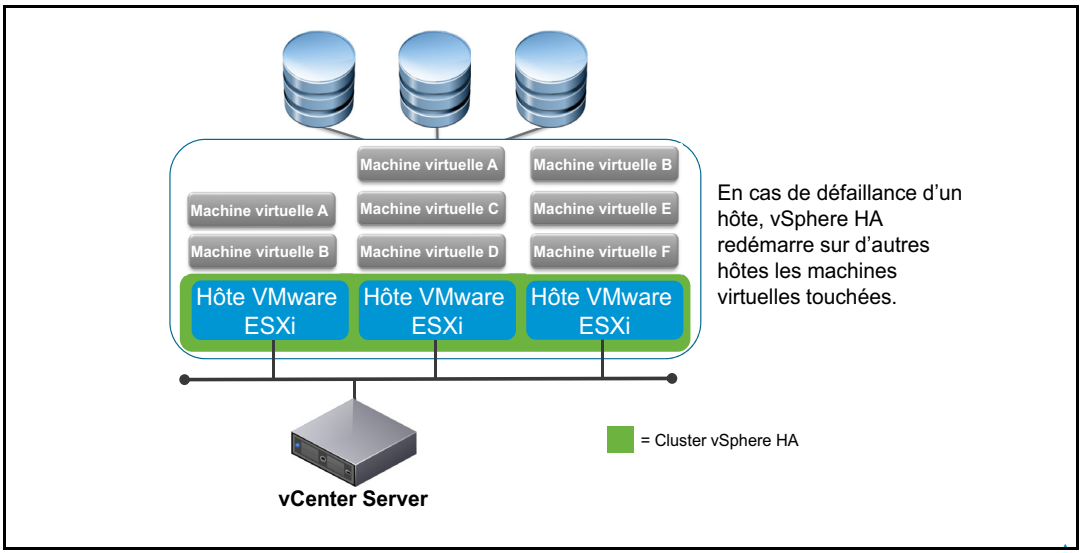
vSphere HA conjugue plusieurs types de protection de la disponibilité des applications :

- Protection contre les pannes du serveur via le redémarrage des machines virtuelles sur d'autres hôtes du cluster
- Protection contre les pannes de l'application à travers une surveillance permanente de la machine virtuelle et sa réinitialisation lorsqu'une panne est détectée
- Protection contre les problèmes d'accessibilité à la banque de données et récupération automatique des machines virtuelles concernées Si la fonction VMCP (Virtual Machine Component Protection) est activée, les machines virtuelles touchées sont redémarrées sur d'autres hôtes accédant encore aux banques de données
- Protection des machines virtuelles contre l'isolation du réseau : les machines virtuelles dont l'hôte se trouve isolé sont redémarrées sur le réseau de gestion ou le réseau vSAN. Cette protection est assurée même si le réseau a été partitionné.

À la différence d'autres solutions de clustering, vSphere HA protège l'ensemble des charges de travail en s'appuyant sur l'infrastructure elle-même :

- Vous n'avez aucun logiciel spécifique à installer au sein de l'application ou sur la machine virtuelle. Toutes les charges de travail sont protégées par vSphere HA. Une fois vSphere HA configuré, aucune mesure supplémentaire n'est nécessaire pour protéger les nouvelles machines virtuelles : celles-ci sont automatiquement protégées.
- Vous pouvez associer vSphere HA avec vSphere DRS en vue de déployer une protection contre les pannes et d'assurer un équilibrage de la charge à l'échelle de tous les hôtes d'un cluster.

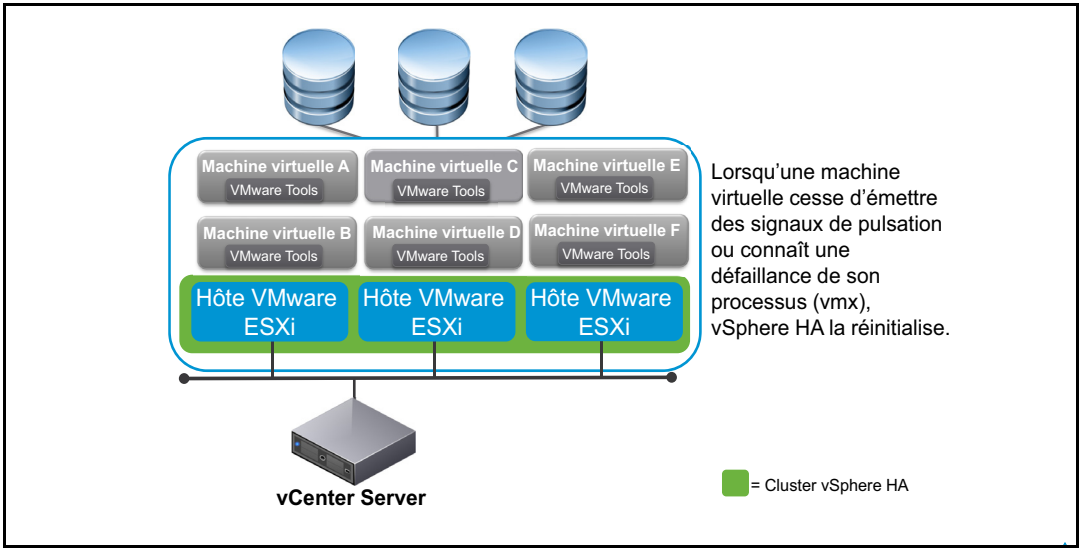
9-10 Scénario d'utilisation de vSphere HA : Panne d'un hôte VMware ESXi



vSphere HA est également capable de déterminer si un hôte VMware ESXi connaît un problème d'isolation ou une panne. En cas de panne d'un hôte VMware ESXi, vSphere HA se charge de redémarrer les machines virtuelles précédemment exécutées par cet hôte sur les hôtes restants du cluster.

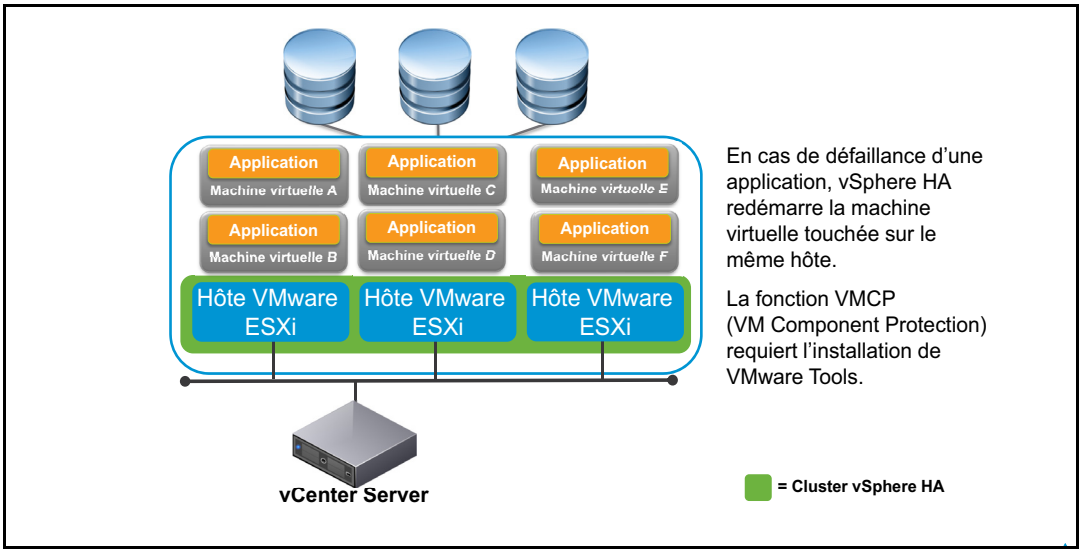
La durée de l'interruption de service enregistrée dans un cluster donné dépend du temps nécessaire au système d'exploitation client et aux applications pour redémarrer suite au basculement de la machine virtuelle.

9-11 Scénario d'utilisation de vSphere HA : Panne du système d'exploitation client



Si la surveillance des machines virtuelles est activée, l'agent vSphere HA présent sur chacun des hôtes supervise VMware Tools pour chaque machine virtuelle exécutée sur l'hôte. Lorsqu'une machine virtuelle cesse d'envoyer des signaux de pulsation, le système d'exploitation client est réinitialisé. La machine virtuelle reste implantée sur le même hôte.

9-12 Scénario d'utilisation de vSphere HA : Échec d'application



L'agent présent sur chaque hôte peut éventuellement surveiller les signaux de pulsation des applications exécutées sur chacune des machines virtuelles. En cas de panne d'une application, la machine virtuelle sur laquelle cette application est exécutée est redémarrée sur le même hôte. La surveillance des applications requiert un agent de surveillance tiers compatible avec la surveillance d'applications sur machine virtuelle.

9-13 Scénario d’utilisation de vSphere HA : Perte d’accès aux banques de données

Si la fonction VMCP (VM Component Protection) est activée, vSphere HA peut détecter les problèmes d’accessibilité à la banque de données et assurer une récupération automatique des machines virtuelles concernées.

Vous pouvez définir la réaction de vSphere HA à ce type de panne, qu’il s’agisse de créer des alarmes liées aux événements ou de redémarrer des machines virtuelles sur d’autres hôtes :

- Erreur PDL (Permanent Device Loss) :
  - Perte d’accès irrécupérable
  - Survient lorsqu’un périphérique de stockage signale que la banque de données n’est plus accessible à l’hôte
  - Réactions possibles : **Issue events** ou **Power off and restart VMs**
- Erreur APD (All Paths Down) :
  - Récupérable
  - Représente une perte d’accès temporaire ou de type inconnu
  - Réactions possibles : **Issue events**, **Power off and restart VMs--conservative restart policy** ou **Power off and restart VMs--aggressive restart policy**.

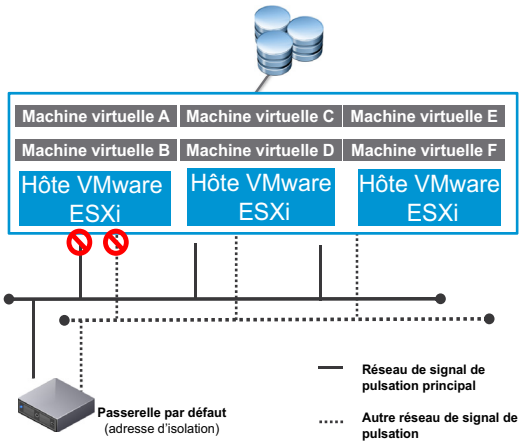
9-14 Scénario d'utilisation de vSphere HA : Protection des machines virtuelles contre l'isolation réseau

vSphere HA redémarre les machines virtuelles dont l'hôte se trouve isolé sur le réseau de gestion ou le réseau vSAN.

Un hôte en cours d'exécution est isolé du réseau lorsqu'il n'est plus en mesure d'observer le trafic émanant des agents vSphere HA sur le réseau de gestion :

- vSphere HA lance des requêtes ping vers les adresses d'isolation réseau du cluster. Une adresse d'isolation réseau est une adresse IP vers laquelle le système envoie des requêtes ping pour déterminer si un hôte est isolé du réseau.
- Si l'envoi de requête ping échoue, l'hôte se déclare isolé du réseau.

Cette protection est assurée même si le réseau a été partitionné.



Si vous faites en sorte que l'infrastructure réseau soit suffisamment redondante et qu'un chemin réseau au moins soit disponible en permanence, les problèmes d'isolation réseau des hôtes ont moins de chances de se produire.

9-15 Importance des réseaux de signal de pulsation redondants

Dans un cluster vSphere HA, les signaux de pulsation présentent les caractéristiques suivantes :

- Ils circulent entre l'hôte maître et les hôtes esclaves.
- Ils permettent de déterminer si un hôte maître ou esclave connaît une défaillance.
- Ils sont acheminés via un réseau de signal de pulsation.

Les réseaux de signal de pulsation redondants assurent une détection des pannes fiable et minimisent les risques de scénarios d'isolation d'un hôte.

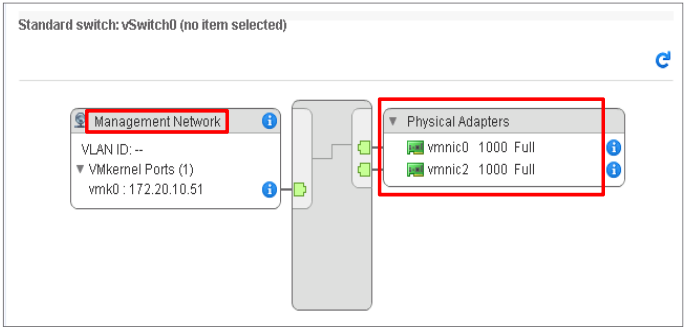
Mise en œuvre d'un réseau de signal de pulsation :

- Réseau implémenté via un port VMkernel réservé pour la gestion
- Réseau implémenté via un port VMkernel réservé pour le trafic vSAN (en cas d'utilisation de vSAN)

VMware recommande une mise en réseau de signal de pulsation redondant pour votre cluster vSphere HA. Si cette redondance n'est pas assurée, votre configuration de basculement présente un point unitaire de panne. En cas de panne de la connexion d'un hôte maître, une seconde connexion reste disponible pour envoyer des signaux de pulsation aux autres hôtes.

9-16 Redondance via l’association de cartes d’interface réseau

Vous pouvez utiliser l’association de cartes d’interface réseau pour créer un réseau de signal de pulsation redondant sur les hôtes VMware ESXi.



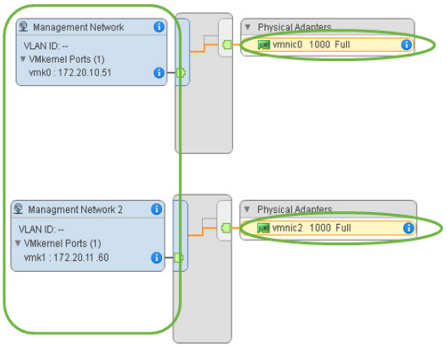
Association de cartes d’interface réseau sur un hôte VMware ESXi

9-17 Redondance via des réseaux supplémentaires

Vous pouvez également créer la redondance en configurant d'autres réseaux de signal de pulsation.

Sur chaque hôte VMware ESXi, créez un deuxième port VMkernel sur un commutateur virtuel distinct, en le dotant de son propre adaptateur physique.

Les réseaux de gestion redondants permettent la détection fiable des défaillances et évitent les situations d'isolation ou de placement sur une autre partition, car les signaux de pulsation peuvent être envoyés sur plusieurs réseaux.



Dans la plupart des implémentations, l'association de cartes d'interface réseau assure une redondance suffisante des signaux de pulsation, mais vous avez également la possibilité de créer une seconde connexion au réseau de gestion reliée à un commutateur virtuel distinct.

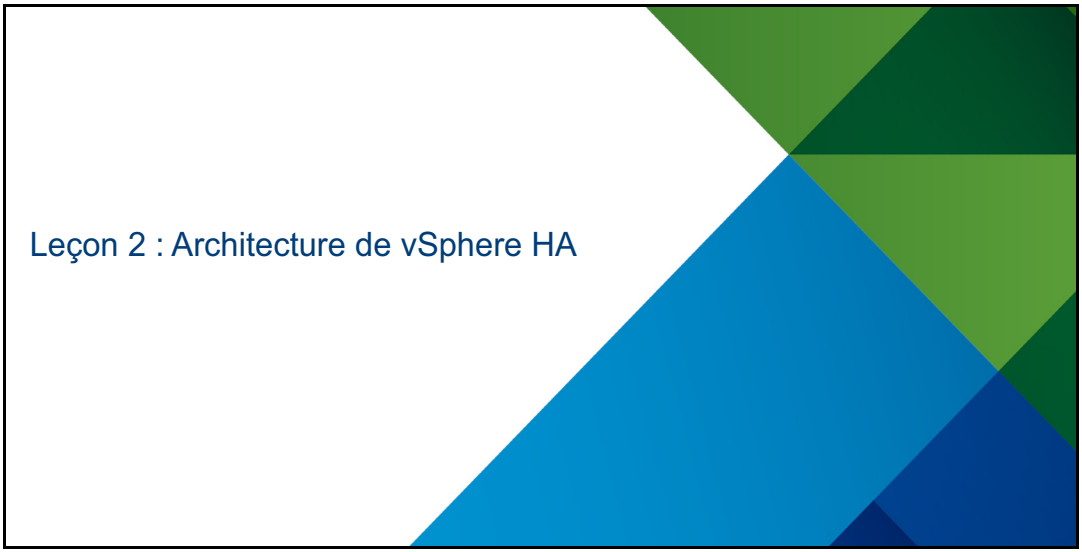
La connexion au réseau de gestion originale est utilisée à des fins de transport réseau et de gestion. Une fois cette seconde connexion au réseau de gestion créée, vSphere HA envoie des signaux de pulsation via les deux connexions au réseau de gestion. En cas de panne de l'un de ces chemins, vSphere HA continue à envoyer et à recevoir des signaux de pulsation via l'autre chemin.

9-18 Rappel des objectifs de la formation

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

- Décrire les options à configurer pour assurer la haute disponibilité de votre environnement vSphere
- Décider des réactions de vSphere HA en cas de panne d'un hôte VMware ESXi, d'une machine virtuelle ou d'une application

9-19 Leçon 2 : Architecture de vSphere HA

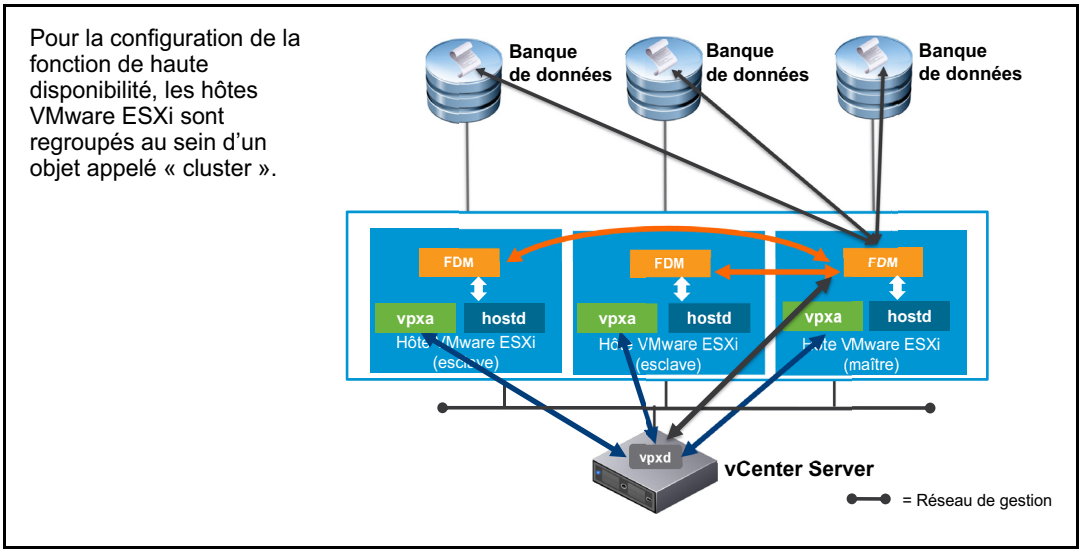


9-20 Objectifs de la formation

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

- Décrire les mécanismes de pulsation utilisés par vSphere HA
- Identifier et évoquer d'autres scénarios de panne
- Connaître les considérations relatives à la conception de vSphere HA

9-21 Architecture vSphere HA : Communication avec les agents



Lorsque vSphere HA est activé, le service Fault Domain Manager (FDM) démarre sur les hôtes membres du cluster. Une fois les agents FDM démarrés, les hôtes du cluster sont considérés comme appartenant à un domaine de pannes. Les hôtes ne peuvent pas participer à un domaine de pannes lorsqu'ils sont en mode maintenance, en mode veille ou déconnectés de vCenter Server. Un hôte ne peut se trouver que dans un seul domaine de pannes à la fois.

Le domaine de pannes est géré par un hôte maître. Tous les autres hôtes sont appelés « hôtes esclaves ». Les agents FDM présents sur les hôtes esclaves communiquent tous avec le service FDM présent sur l'hôte maître.

La détermination de l'hôte maître donne lieu à un processus de désignation. Le système désigné comme maître est celui qui peut accéder au plus grand nombre de banques de données. Lorsque plusieurs hôtes du cluster ont accès au même nombre de banques de données, le processus de désignation détermine l'hôte maître en se fondant sur l'ID d'objet géré (MOID) qui lui a été attribué par vCenter Server.

Le processus de désignation d'un nouveau maître prend environ 15 secondes et survient dans les circonstances suivantes :

- vSphere HA est activé.
- Le maître connaît une panne système résultant de l'un des facteurs suivants :
  - L'hôte maître est placé en mode maintenance.
  - L'hôte maître est placé en mode veille.
  - vSphere HA est reconfiguré.

- Les hôtes esclaves ne peuvent pas communiquer avec l'hôte maître en raison d'un problème réseau.

Durant le processus de désignation, les agents vSphere HA candidats communiquent entre eux à travers le réseau de gestion ou le réseau vSAN d'un cluster vSAN en utilisant le protocole UDP (User Datagram Protocol). Toutes les connexions réseau sont en mode point à point. Une fois l'agent maître désigné, l'hôte maître et les hôtes esclaves utilisent le protocole TCP sécurisé pour communiquer entre eux. Après le démarrage de vSphere HA, vCenter Server contacte l'agent hôte maître et lui envoie la liste des hôtes membres du cluster ainsi que la configuration de ce dernier. Ces informations sont stockées en local sur l'hôte maître, puis distribuées aux hôtes esclaves appartenant au même cluster. Si des hôtes sont ajoutés au cluster dans le cadre du fonctionnement normal, l'agent maître envoie une mise à jour à tous les hôtes existants du cluster.

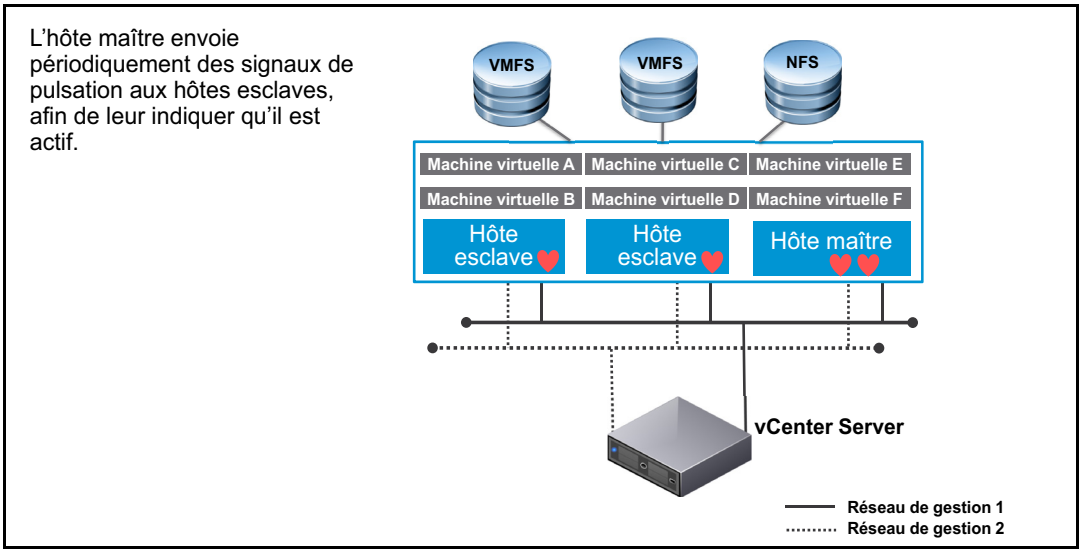
L'hôte maître fournit une interface permettant à vCenter Server de demander l'état du domaine de pannes et de générer un rapport sur son intégrité, ainsi que sur la disponibilité des machines virtuelles. vCenter Server indique à l'agent vSphere HA les machines virtuelles à protéger et lui transmet leur liste de compatibilité de machine virtuelle à hôte. Les changements d'état sont signalés à l'agent, via hostd, ainsi qu'à vCenter Server, via vpxa. L'hôte maître surveille l'intégrité des hôtes esclaves et, lorsque l'un d'eux connaît une panne, il se charge des machines virtuelles exécutées sur celui-ci.

Chaque hôte esclave surveille l'intégrité des machines virtuelles exécutées en local et transmet les changements d'état à l'hôte maître. Un hôte esclave surveille également l'intégrité de l'hôte maître.

La configuration, la gestion et la supervision de vSphere HA sont assurées via vCenter Server. La maintenance des données de configuration du cluster est assurée par le processus vpxd exécuté sur le système vCenter Server. Les modifications apportées à la configuration du cluster sont signalées à l'agent maître par le processus vpxd. L'agent maître publie alors une copie mise à jour des informations de configuration du cluster, qui est récupérée par chacun des esclaves. Chaque esclave enregistre les informations de configuration mises à jour sur un stockage local. La liste des machines virtuelles protégées est stockée sur chaque banque de données. La liste des machines virtuelles est mise à jour après toute opération de mise sous tension (passage à l'état protégé) ou de mise hors tension (passage à l'état non protégé) déclenchée par l'utilisateur. La mise à jour intervient une fois que vCenter Server a constaté ces opérations.

Une machine virtuelle passe à l'état protégé après toute opération entraînant une mise sous tension. Le fait de restaurer un snapshot avec état de mémoire sur une machine virtuelle entraîne la mise sous tension de cette dernière et son passage à l'état protégé. Inversement, toute action utilisateur entraînant la mise hors tension de la machine virtuelle, telle que la restauration d'un snapshot sans état de mémoire ou l'exécution d'une opération de veille au sein du client, entraîne le passage de la machine virtuelle à l'état non protégé.

9-22 Architecture vSphere HA : Signaux de pulsation réseau

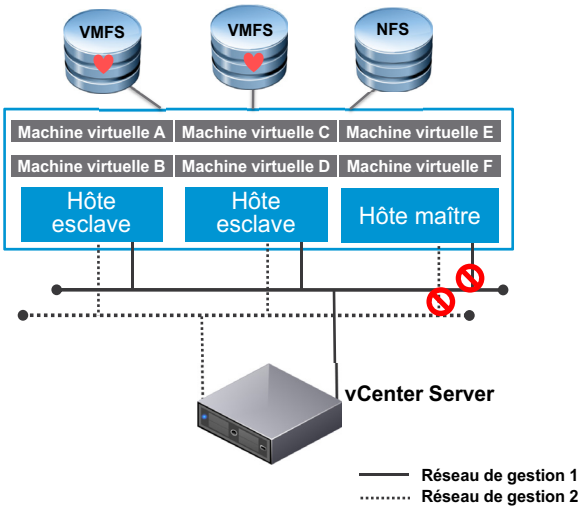


L'hôte maître envoie des signaux de pulsation à chacun des hôtes esclaves présents sur l'ensemble des réseaux de gestion configurés. Chaque hôte esclave n'utilise cependant qu'un seul réseau de gestion pour communiquer avec le maître. En cas de panne du réseau de gestion utilisé pour la communication avec le maître, l'esclave bascule sur une autre interface de gestion pour communiquer avec l'hôte maître.

Si un hôte esclave ne répond pas dans le délai d'expiration prédéfini, l'hôte maître le déclare en tant qu'agent non accessible. En cas d'absence de réponse d'un hôte esclave, l'hôte maître cherche à déterminer la cause du problème. L'hôte maître doit établir si l'hôte esclave s'est bloqué, ou si son absence de réponse est due à une panne du réseau ou à un état d'inaccessibilité de l'agent vSphere HA.

9-23 Architecture vSphere HA : Signaux de pulsation de banque de données

Les banques de données servent de canal de communication de secours pour la détection des signaux de pulsation des machines virtuelles et des hôtes.



Les signaux de pulsation de la banque de données permettent de faire la distinction entre un hôte défaillant et isolé ou un hôte placé sur une autre partition. vSphere HA ne tente de redémarrer les machines virtuelles que dans les situations suivantes :

- Un hôte est tombé en panne (absence de signaux de pulsation réseau, de requêtes ping et de signaux de pulsation de banque de données).
- Un hôte est isolé et le paramètre « Host isolation response » du cluster est configuré sur « Power off » ou « Shut down ».

9-24 Scénarios de panne vSphere HA

vSphere HA est capable d'identifier et de traiter divers types de pannes :

- Panne d'un hôte esclave
- Hôte maître défaillant
- Panne réseau (isolation d'un hôte)

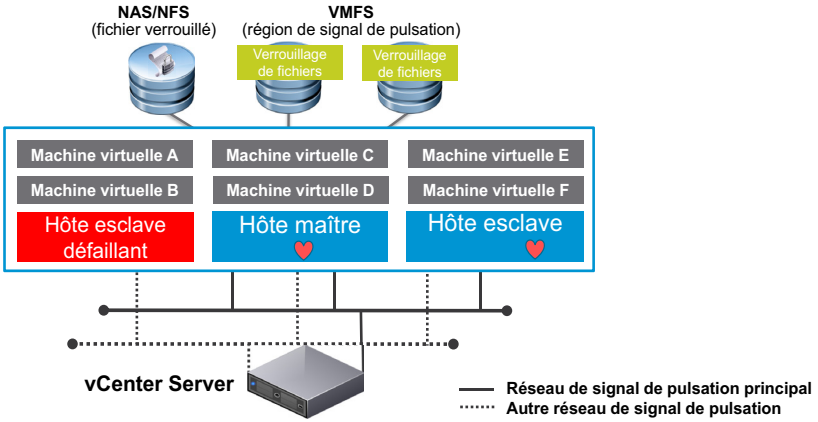
VMCP permet à vSphere HA de détecter et de traiter les pannes liées au stockage :

- Défaillance de l'accès à la banque de données
  - APD
  - PDL

vSphere HA est également capable de déterminer si un hôte VMware ESXi connaît un problème d'isolation ou une panne. Un hôte VMware ESXi « isolé » ne peut pas détecter le trafic en provenance d'autres hôtes du cluster et ne peut pas émettre de commande ping vers la passerelle par défaut. Si un hôte VMware ESXi est défaillant, vSphere HA doit redémarrer les machines virtuelles qui s'exécutaient sur cet hôte et sur les hôtes restants du cluster. Si l'hôte VMware ESXi est isolé (il ne peut pas émettre de commande ping vers la passerelle par défaut ou l'adresse d'isolation et ne détecte pas le trafic du réseau de gestion), l'hôte exécute la réponse des hôtes isolés.

9-25 Hôtes esclaves défaillants

Lorsqu'un hôte esclave ne répond pas aux signaux de pulsation réseau émis par l'hôte maître, l'agent vSphere HA maître tente de déterminer la cause de ce problème.



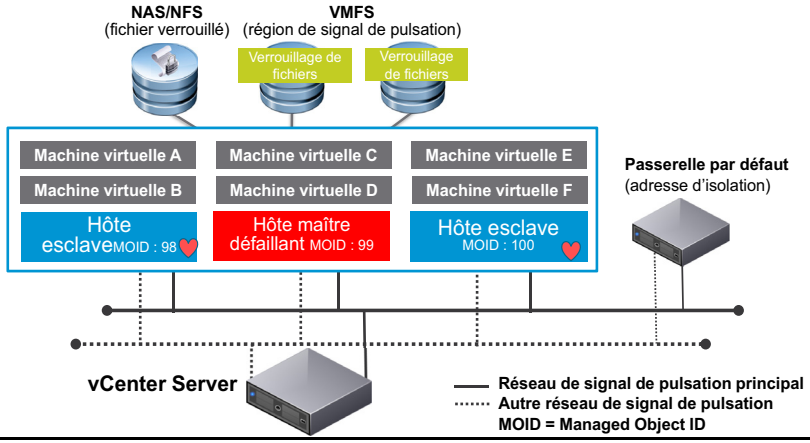
L'hôte maître doit établir si l'hôte esclave s'est bloqué, ou si son absence de réponse est due à un problème réseau tel qu'une règle de pare-feu mal configurée ou une défaillance d'un composant. La réaction de vSphere HA dépend du type de panne.

S'il ne peut pas obtenir de signaux de pulsation via le réseau, l'hôte maître doit déterminer si l'hôte esclave a rencontré une panne réseau ou s'il s'agit d'une défaillance du système. L'hôte maître recherche à la fois des réponses aux requêtes ping et des pulsations de banque de données. En l'absence de réponse aux requêtes ping et de signaux de pulsation de banque de données, l'hôte est déclaré défaillant. L'absence conjuguée de signaux de pulsation réseau et de signaux de pulsation de banque de données indique une panne complète de l'hôte.

Pour VMFS, la lecture d'une région de pulsation de la banque de données permet de déterminer si l'hôte envoie toujours des signaux de pulsation vers celle-ci. Pour les banques de données NFS, vSphere HA crée un fichier nommé `host-<X>-hb`, qui est verrouillé par l'hôte VMware ESXi accédant à la banque de données. Ce fichier permet de garantir que le VMkernel envoie des signaux de pulsation à la banque de données et met périodiquement à jour le fichier verrouillé. L'hôte maître se fonde sur l'horodatage du fichier verrouillé pour déterminer si l'esclave est affecté par une panne réseau ou par une défaillance de l'hôte. Pour les deux exemples de stockage ci-dessus, l'instance de vCenter Server sélectionne un ensemble réduit de banques de données destinataires des signaux de pulsation envoyés par les hôtes. Les banques de données accessibles au plus grand nombre d'hôtes sont sélectionnées comme candidats, mais deux banques de données seulement sont choisies (par défaut), de façon à minimiser la surcharge de traitement associée.

9-26 Hôtes maîtres défaillants

Lorsque l'hôte maître est basculé en mode maintenance ou tombe en panne, les hôtes esclaves détectent que cet hôte n'émet plus de signaux de pulsation.



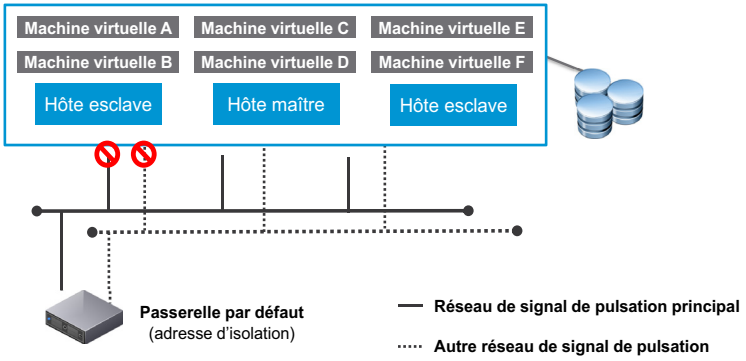
Dans ce cas, un processus de désignation est déclenché afin de sélectionner un nouvel hôte maître. L'hôte désigné comme maître est celui qui peut accéder au plus grand nombre de banques de données. Si tous les hôtes esclaves disposent de droits d'accès identiques sur les banques de données, le processus de désignation choisit comme nouvel hôte maître le système hôte auquel vCenter Server a attribué l'ID d'objet géré (MOID) le plus haut placé dans l'ordre alphabétique lors de son ajout à l'inventaire vCenter Server.

En cas de panne de l'hôte maître, les esclaves participent à la désignation d'un nouveau maître. Une fois sélectionné, le nouvel hôte lit les adresses MAC et IP des hôtes et des machines virtuelles indiquées dans une liste d'hôtes stockée sur une banque de données. Cette liste d'hôtes permet au maître de déterminer s'il doit ou non accepter la connexion d'un esclave.

Le nouveau maître lit un fichier présent sur chacune des banques de données et contenant l'état de toutes les machines virtuelles, puis détermine quelles sont les machines virtuelles qui sont protégées par vSphere HA et qui pourraient nécessiter un redémarrage. Le nouveau maître identifie tout d'abord les machines virtuelles qui sont exécutées sur les hôtes esclaves. Il établit ensuite, par élimination, la liste des machines virtuelles nécessitant un redémarrage. Ce même processus est utilisé pour redémarrer les machines virtuelles en cas de panne complète d'un cluster.

9-27 Hôtes isolés

Si l'hôte ne reçoit pas de signaux de pulsation, ou s'il n'a pas accès au trafic de désignation empruntant le réseau de gestion et n'est pas en mesure d'envoyer des requêtes ping à la passerelle par défaut, il est isolé.



Un hôte est déclaré isolé lorsque les deux conditions suivantes sont réunies :

- L'hôte ne reçoit pas de signaux de pulsation réseau.
- L'hôte ne peut pas envoyer de requêtes ping à ses adresses d'isolation.

La diapositive illustre plusieurs scénarios susceptibles d'entraîner une isolation réseau. Lorsqu'un hôte perd simultanément sa connectivité avec les réseaux de signal de pulsation principal et alternatif, il ne peut plus recevoir les signaux de pulsation réseau émanant des autres hôtes du cluster vSphere HA. La diapositive montre par ailleurs que ce même hôte n'est plus capable d'envoyer des requêtes ping à son adresse d'isolation.

Lorsqu'un hôte est isolé, l'agent vSphere HA maître doit s'assurer qu'il reste néanmoins actif, en vérifiant l'existence de signaux de pulsation de banque de données. vSphere HA n'utilise les signaux de pulsation de banque de données qu'en cas d'isolation ou de placement d'un hôte sur une autre partition.

9-28 Considérations de conception

Certains choix de conception permettent de minimiser les problèmes d'isolation d'hôtes :

- Mettre en œuvre des réseaux de signal de pulsation redondants
- Mettre en œuvre des adresses d'isolation redondantes

Si des événements d'isolation d'hôte surviennent, des choix de conception adéquats permettent à vSphere HA de déterminer si un hôte isolé est toujours actif.

Le réseau des machines virtuelles doit être physiquement séparé du réseau de signal de pulsation.

Mettre en œuvre les banques de données de façon à les séparer du réseau de gestion en recourant à l'une de ces approches ou en combinant les deux :

- Fibre Channel sur fibre optique.
- Séparation physique du réseau de stockage IP par rapport au réseau de gestion.

Lorsqu'une banque de données est basée sur Fibre Channel, l'accès à cette banque de données n'est pas interrompu par une panne réseau. En cas d'utilisation de banques de données exploitant le stockage IP (par exemple, NFS, iSCSI ou FCoE), vous devez instaurer une séparation physique (ou, en cas d'impossibilité, une séparation logique) entre le réseau de stockage IP et le réseau de gestion (c'est-à-dire le réseau de signal de pulsation).

9-29 Pannes du stockage des machines virtuelles

Un nombre grandissant de machines virtuelles et de banques de données étant installées sur chaque hôte, des problèmes de connectivité du stockage peuvent survenir. Ils s'avèrent coûteux, mais rares.

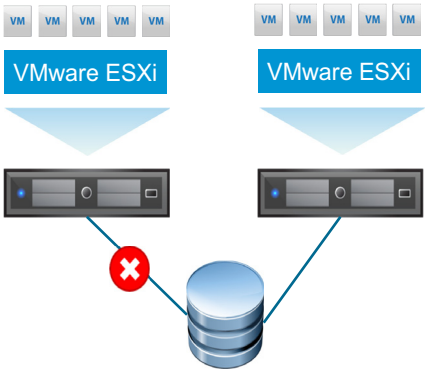
Les problèmes de connectivité sont dus aux facteurs suivants :

- Défaillance du réseau ou d'un commutateur
- Mauvaise configuration de la baie
- Coupures de courant

Les problèmes de connectivité du stockage affectent la disponibilité des machines virtuelles :

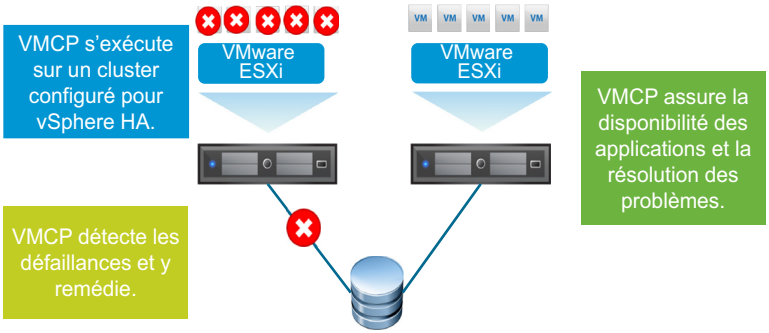
- Les machines virtuelles placées sur les hôtes affectés sont difficiles à gérer.
- Les applications situées sur les disques connectés se bloquent.

La fonction VMCP n'est pas prise en charge avec vSAN.



9-30 À propos de VMCP

VMCP offre une protection contre les pannes de stockage affectant les machines virtuelles.



Seuls les clusters vSphere HA qui contiennent des hôtes VMware ESXi 6.x peuvent être utilisés pour activer la fonction VMCP.

Si la fonction VMCP est activée, vSphere HA peut détecter les problèmes d'accessibilité de la banque de données et assurer une récupération automatique des machines virtuelles concernées.

VMCP protège le système contre les problèmes d'accessibilité à la banque de données qui peuvent affecter une machine virtuelle exécutée sur un hôte au sein d'un cluster vSphere HA. Si un problème de ce type survient, l'hôte affecté ne peut plus accéder au chemin d'accès au stockage d'une banque de données spécifique. Vous pouvez définir la réaction de vSphere HA à ce type de panne, qu'il s'agisse de créer des alarmes liées aux événements ou de redémarrer des machines virtuelles sur d'autres hôtes.

Seuls les clusters vSphere HA qui contiennent des hôtes VMware ESXi 6.x peuvent être utilisés pour activer la fonction VMCP. Les clusters contenant des hôtes d'une version précédente ne peuvent pas activer VMCP. Quant à ces hôtes, ils ne peuvent pas être ajoutés à un cluster pour lequel la fonction VMCP est activée.

9-31 Rappel des objectifs de la formation

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

- Décrire les mécanismes de pulsation utilisés par vSphere HA
- Identifier et évoquer d'autres scénarios de panne
- Connaître les considérations relatives à la conception de vSphere HA

9-32 Leçon 3 : Configuration de vSphere HA

9-33 Objectifs de la formation

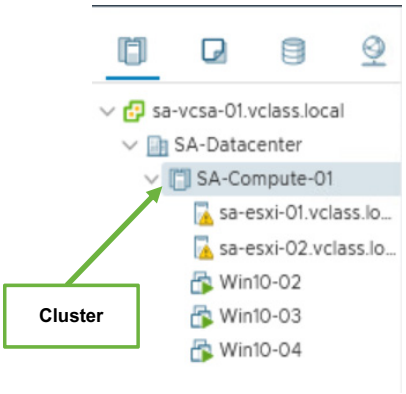
À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Connaître les exigences relatives à la création et à l'utilisation d'un cluster vSphere HA
- Configurer un cluster vSphere HA

9-34 À propos des clusters

vSphere utilise des clusters pour autoriser le partage de ressources physiques au sein d'un groupe d'hôtes VMware ESXi. vCenter Server gère les ressources d'un cluster comme un pool de ressources unique.

Vous avez la possibilité d'activer des fonctionnalités telles que vSphere HA, vSphere DRS ou vSAN au sein d'un cluster.



vSphere HA exploite plusieurs hôtes VMware ESXi configurés au sein d'un cluster pour assurer une récupération rapide en cas de panne et une haute disponibilité des applications exécutées sur les machines virtuelles. Les ressources sont gérées par vCenter Server. Vous avez la possibilité d'activer des fonctionnalités telles que vSphere HA, vSphere DRS ou vSAN au sein d'un cluster.

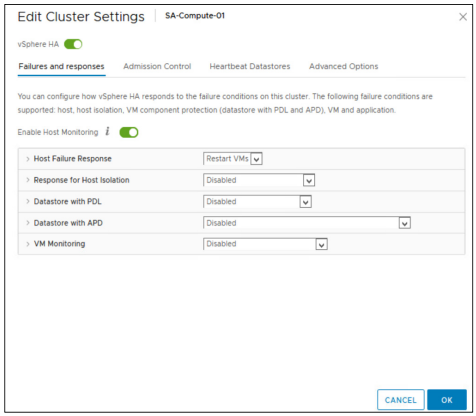
9-35 Conditions requises pour vSphere HA

Vous devez respecter les contraintes relatives à la création d'un cluster vSphere HA :

- Utilisez soit VMware vSphere® Essentials Plus Kit, soit VMware vSphere® Standard Edition™.
- Un cluster peut accueillir de 2 à 64 hôtes VMware ESXi.
- Chacun des hôtes doit être configuré avec une adresse IP statique. En cas d'utilisation du protocole DHCP, assurez-vous que chaque hôte conservera la même adresse après chaque redémarrage.
- Les hôtes doivent avoir au moins un réseau de gestion en commun.
- Pour assurer le fonctionnement de la fonction de surveillance des machines virtuelles, vous devez installer VMware Tools sur chaque machine virtuelle.
- Seuls les clusters vSphere HA qui contiennent des hôtes VMware ESXi 6.x peuvent être utilisés pour activer la fonction VMCP.

9-36 Configuration des paramètres de vSphere HA

Lorsque vous créez ou configurez un cluster vSphere HA, vous devez spécifier les paramètres régissant le mode opératoire de cette fonctionnalité.

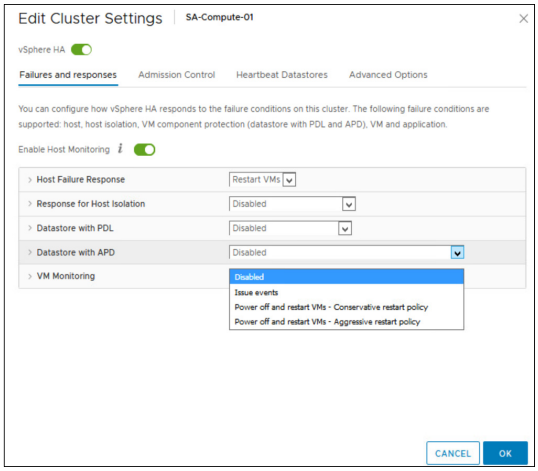


vSphere Web Client et vSphere Client offrent tous deux la possibilité de configurer les paramètres vSphere HA suivants :

- Conditions d'échec et réponses en matière de disponibilité : définissez les paramètres déterminant les réponses requises en cas de panne ou d'isolation de l'hôte, ainsi que la surveillance des machines virtuelles et la fonctionnalité VMCP.
- « Admission Control » : activez ou désactivez le contrôle d'admission pour le cluster vSphere HA et sélectionnez une règle pour sa mise en application.
- « Heartbeat datastores » : spécifiez les préférences relatives aux banques de données utilisées par vSphere HA pour les signaux de pulsation de banque de données.
- « Advanced options » : définissez les options avancées permettant de personnaliser le comportement de vSphere HA.

9-37 Paramètres de vSphere HA : « Failures and Responses »

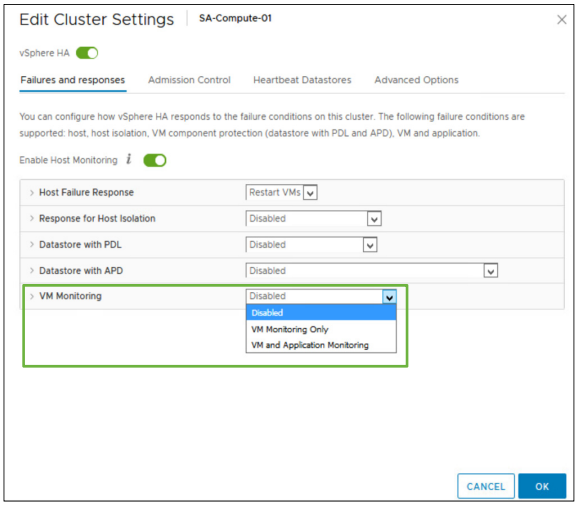
Le volet « Failures and Responses » vous permet de configurer la réaction de votre cluster en cas de panne.



Le volet « Failures and Responses » vous permet de configurer les réactions de votre cluster face à différents types de problèmes. Vous pouvez notamment spécifier la réponse du cluster vSphere HA en cas de panne ou d'isolation de l'hôte. Vous avez également la possibilité de configurer les actions de la fonction VMCP (VM Component Protection) en réponse aux erreurs PDL (Permanent Device Loss) et APD (All Paths Down), ainsi que d'activer la surveillance des machines virtuelles.

9-38 Paramètres de vSphere HA : « VM Monitoring »

Les paramètres de la section « Virtual Machine Monitoring » vous permettent de contrôler la surveillance des machines virtuelles.



Par défaut, le paramètre **VM Monitoring** est défini sur **Disabled**.

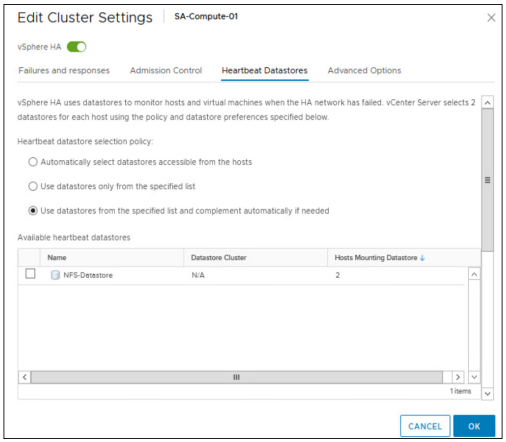
Le service de surveillance des machines virtuelles redémarre individuellement les VMs dont le système ne reçoit pas les signaux de pulsation VMware Tools ou dont le système d'exploitation client n'a pas émis d'E/S depuis 2 minutes (par défaut). Lorsqu'aucun de ces critères n'est rempli, l'explication la plus probable réside dans une panne du système d'exploitation client. Dans ce cas, le service de surveillance des machines virtuelles conclut à une panne de la machine virtuelle et redémarre celle-ci de manière à restaurer le service.

Vous pouvez configurer le degré de sensibilité de la surveillance. Une sensibilité élevée permet de déterminer une panne plus rapidement. Même si cela est improbable, une surveillance très sensible peut entraîner la détection abusive de pannes dans les cas où la machine virtuelle ou l'application fonctionne toujours et où l'absence de réception de signaux de pulsation résulte de facteurs tels que des contraintes liées aux ressources. Une surveillance de faible sensibilité se traduit quant à elle par des interruptions de service plus longues entre la panne réelle et la réinitialisation de la machine virtuelle. Sélectionnez une option assurant un compromis optimal en fonction de vos besoins.

Sélectionnez **VM Monitoring Only** pour activer le redémarrage individuel des machines virtuelles en cas de non-réception des signaux de pulsation dans un délai prédéfini. Vous pouvez également sélectionner **VM and Application Monitoring** afin d'activer la surveillance des applications.

9-39 Paramètres de vSphere HA : « Heartbeat Datastores »

Un fichier de signal de pulsation est créé sur les banques de données sélectionnées. Il est utilisé en cas de panne du réseau de gestion.

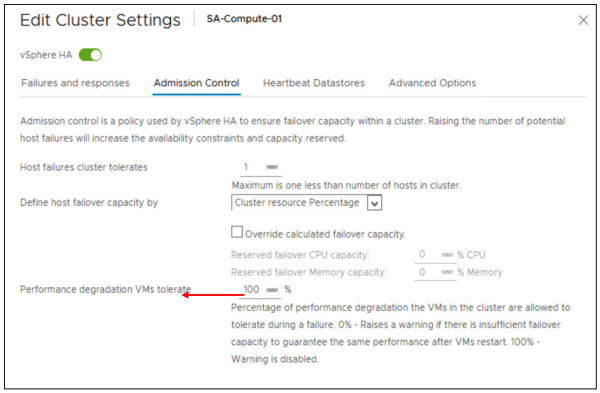


L'utilisation des signaux de pulsation de banque de données permet à l'hôte maître de déterminer si un hôte est tombé en panne ou si un problème d'isolation réseau s'est produit. En cas d'interruption des signaux de pulsation de banque de données émanant de l'hôte esclave, ce dernier est considéré comme défaillant. Dans ce cas, les machines virtuelles de l'hôte en panne sont redémarrées sur un autre hôte du cluster vSphere HA.

L'exploitation des signaux de pulsation de banque de données permet de renforcer le contrôle d'intégrité d'un hôte en mobilisant d'autres ressources que le seul réseau de gestion. Vous avez la possibilité de configurer la liste des banques de données à surveiller pour un hôte déterminé. Vous pouvez également laisser vSphere HA prendre cette décision, ou combiner les deux méthodes.

9-40 Paramètres de vSphere HA : « Admission Control »

vCenter Server utilise la fonction de contrôle d'admission afin de garantir qu'un cluster dispose de ressources suffisantes pour assurer la protection par basculement, mais aussi le respect des réservations de ressources des machines virtuelles.



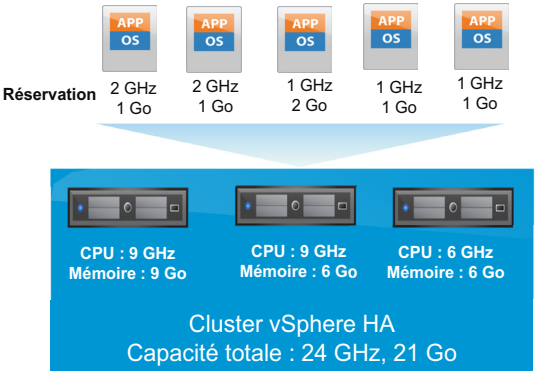
Une fois que vous avez créé un cluster, le contrôle d'admission vous permet de spécifier si les machines virtuelles doivent ou non être redémarrées lorsqu'elles enfreignent les contraintes de disponibilité. Le cluster réserve les ressources nécessaires pour assurer le basculement de l'ensemble des machines virtuelles sur le nombre d'hôtes spécifié.

Les paramètres de contrôle d'admission sont les suivants :

- **Disabled** : cette option (non recommandée) désactive le contrôle d'admission et autorise ainsi la mise sous tension de machines virtuelles enfreignant les contraintes de disponibilité.
- **Slot Policy** : un slot est une représentation logique d'un ensemble de ressources mémoire et CPU. Avec l'option « Slot Policy », vSphere HA calcule la taille de slot, puis détermine le nombre de slots pouvant être accueillis par chaque hôte du cluster et en déduit la capacité de basculement actuelle du cluster.
- **Cluster resource Percentage** : cette option (sélectionnée par défaut) permet de spécifier le pourcentage des ressources CPU et mémoire du cluster qui doit être réservé en tant que capacité de basculement.
- **Dedicated failover hosts** : cette option sélectionne les hôtes à utiliser pour les actions de basculement. Si un hôte de basculement par défaut ne présente pas les ressources nécessaires, les basculements pourront néanmoins s'effectuer sur d'autres hôtes du cluster.

9-41 Exemple : Contrôle d'admission basé sur un pourcentage des ressources du cluster

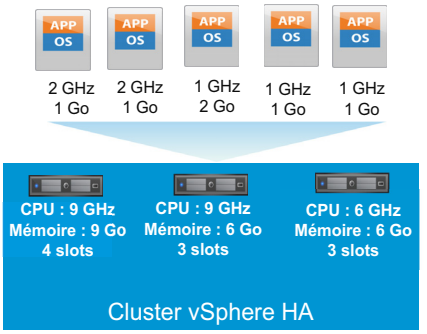
- Réservations totales des machines virtuelles : 7 GHz et 6 Go.
- La capacité de basculement actuelle pour les ressources CPU est égale à 70 % :
  - ((24 GHz - 7 GHz)/24 GHz) = 70,8 %
- La capacité de basculement actuelle pour les ressources mémoire s'établit à 71 % :
  - ((21 Go - 6 Go)/21 Go) = 71,4 %



9-42 Exemple : Contrôle d’admission basé sur des slots

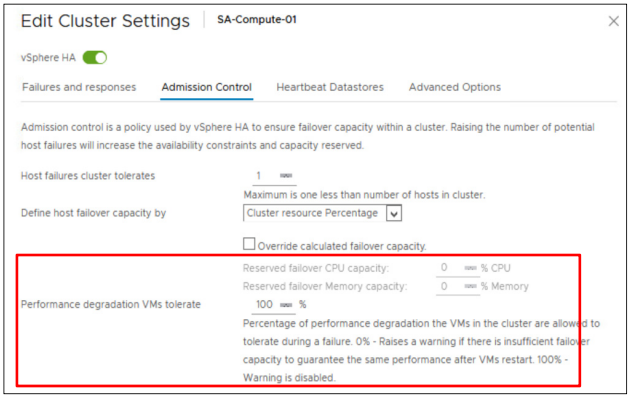
Le slot correspond à la réservation de capacité CPU et mémoire requise par chaque VM sous tension au sein du cluster :

- Calculer la taille de slot : 2 GHz de CPU et 2 Go de mémoire.
- Calculer le nombre de slots par hôte. Dans notre exemple, le cluster offre 10 slots.
- La capacité de basculement actuelle correspond à un hôte. Dans notre exemple, la capacité de basculement est égale à quatre (l’hôte du cluster qui offre les plus grandes capacités comporte quatre slots) :
  - En cas de panne de l’hôte 1, il restera six slots dans le cluster, ce qui est suffisant pour mettre les cinq machines virtuelles sous tension.
  - En cas de panne des hôtes 1 et 2, il ne reste que trois slots, ce qui s’avère insuffisant.
- Si la capacité de basculement actuelle est inférieure à la capacité de basculement configurée, interdire toute nouvelle mise sous tension de VM.



9-43 Paramètres de vSphere HA : « Performance Degradation VMs Tolerate »

Le seuil de dégradation des performances tolérée par les machines virtuelles définit le pourcentage de dégradation des performances que les machines virtuelles du cluster sont autorisées à tolérer en cas de panne.



Le contrôle d'admission peut également être configuré de manière à émettre des avertissements lorsque le taux d'utilisation actuel dépasse le pourcentage de capacité de basculement. Le calcul de la réduction des ressources prend en compte la mémoire réservée et la mémoire supplémentaire d'une machine virtuelle avant d'autoriser la mise sous tension ou la migration de cette VM, ou la modification de ses réservations.

La définition du seuil « Performance degradation VMs tolerate » vous permet de spécifier les conditions de signalement d'un problème de configuration. Par exemple :

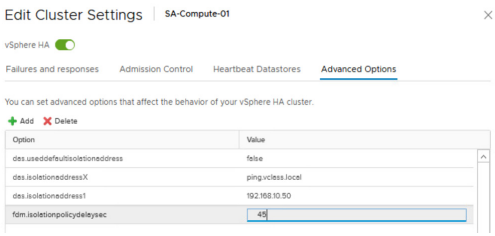
- Le seuil par défaut, fixé à 100 %, ne génère aucun avertissement.
- Si vous réduisez ce seuil à 0 %, un avertissement est généré dès que le taux d'utilisation du cluster dépasse la capacité disponible.
- Si vous fixez le seuil à 20 %, la réduction de performances tolérée est calculée selon la formule : la réduction de performances = le taux d'utilisation actuel x 20 %. Lorsque le taux d'utilisation actuel minoré de la réduction de performances dépasse la capacité disponible, un problème de configuration est signalé.

Le seuil « Performance degradation VMs tolerate » n'est disponible que si vSphere DRS est désactivé.

9-44 Paramètres de vSphere HA : « Advanced Options »

Vous pouvez personnaliser le comportement de vSphere HA en configurant ses options avancées :

- Pour empêcher un cluster d'utiliser l'adresse d'isolation par défaut (passerelle par défaut) :
  - das.usedefaultisolationaddress = false
- Pour obliger un cluster à émettre une commande ping vers d'autres adresses d'isolation :
  - das.isolationaddressX = adresse_accessible_par_ping
- Pour obliger un cluster à attendre au-delà de la fenêtre d'action par défaut de 30 secondes en cas d'isolation :
  - fdm.isolationpolicydelaysec = > 30 s
- Pour imposer une taille de slot maximale (mémoire et CPU) :
  - das.slotmeminmb = 100
  - das.slotcpuinmhz = 32



Vous pouvez définir des options avancées affectant le comportement de votre cluster vSphere HA. Pour en savoir plus, consultez le document *Guide de disponibilité vSphere*, à l'adresse http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

9-45 À propos du redémarrage orchestré de vSphere HA

Le redémarrage orchestré par vSphere HA permet d'organiser le redémarrage des VMs et les dépendances entre VM selon cinq niveaux de priorité.

Sélectionnez ci-dessous les conditions à satisfaire pour qu'une machine virtuelle soit considérée comme prête :

- Les ressources de la machine virtuelle sont allouées.
- La machine virtuelle est sous tension.
- La pulsation de VMware Tools est détectée.
- La pulsation de l'application VMware Tools est détectée.

Vous avez la possibilité de configurer un délai à appliquer après la réalisation d'une condition donnée.

Niveau de priorité :

- Les machines virtuelles peuvent être regroupées en niveaux selon leur priorité de démarrage. Les machines virtuelles dotées du niveau de priorité 1 sont les premières à obtenir leurs ressources et à être mises sous tension.
- vSphere HA attend que toutes les machines virtuelles de niveau 1 aient rempli leurs conditions de redémarrage pour passer aux machines virtuelles de niveau 2, et ainsi de suite.

En cas de panne sur un hôte, les machines virtuelles sont affectées à d'autres hôtes présentant de la capacité non réservée, à commencer par les VMs les plus prioritaires. Le processus se poursuit avec les machines virtuelles de moindre priorité, jusqu'à ce que toutes les machines soient placées ou que le cluster n'offre plus suffisamment de capacité disponible pour répondre aux exigences de réservation ou de capacité supplémentaire de mémoire des machines virtuelles. Chaque hôte redémarre les machines virtuelles qui lui sont affectées en procédant par ordre de priorité.

En cas d'insuffisance de ressources, vSphere HA attend que des capacités non réservées supplémentaires deviennent disponibles (par exemple, suite à la remise en ligne d'un hôte) pour effectuer une nouvelle tentative de placement des machines virtuelles. Pour éviter des situations de ce type, il convient de configurer le contrôle d'admission vSphere HA de façon à réserver une plus grande quantité de ressources exploitables en cas de panne. Le contrôle d'admission vous permet de limiter la part de la capacité du cluster qui est réservée par les machines virtuelles, sachant que cette capacité ne sera plus disponible pour répondre aux besoins de réservation et de capacité supplémentaire de mémoire d'autres machines virtuelles en cas de panne.

9-46 Configuration du redémarrage orchestré par vSphere HA

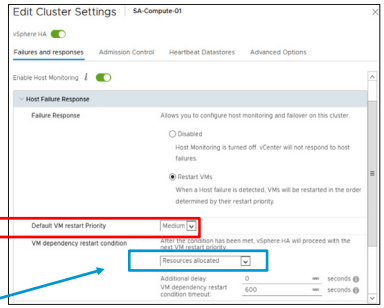
Les machines virtuelles normales reçoivent par défaut la priorité de redémarrage « Medium », à l'exception des VMs dont le niveau de priorité est explicitement défini par des paramètres de remplacement.

Exceptions :

- Les VMs agents sont toujours démarrées en premier et leur priorité de redémarrage n'est pas configurable.
- Les VMs secondaires vSphere Fault Tolerance sont basculées avant les VMs normales. Les VMs principales respectent la priorité de redémarrage normale.

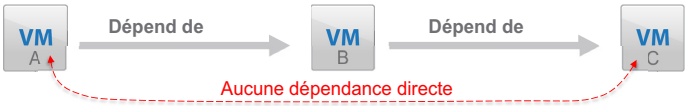
Priorités :
« Lowest » (5), « Low », « Medium » (priorité par défaut), « High », « Highest » (1)

Conditions :
- Ressources allouées
- Sous tension
- Signaux de pulsation du client détectés
- Signaux de pulsation de l'application détectés



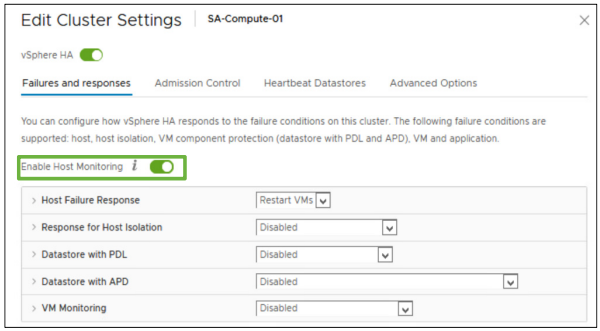
9-47 Dépendances des machines virtuelles lors du redémarrage orchestré

Une machine virtuelle ne peut dépendre que d'autres VMs de priorité égale ou supérieure. Seules les dépendances directes sont prises en charge. Une dépendance entre VMs constitue une règle immuable. La création de dépendances cycliques provoque l'échec du redémarrage des machines virtuelles.



Dans vSphere versions 6.5 et ultérieures, vSphere HA redémarre uniquement les machines virtuelles issues d'un hôte défaillant. Si nécessaire, configurez des règles d'affinité visant à conserver les machines virtuelles sur un même hôte.

Désactivez la surveillance des hôtes avant de modifier les composants de réseau virtuel impliquant les ports VMkernel configurés pour le trafic de gestion ou le trafic vSAN. Cette action empêche toute tentative de basculement indésirable sur les machines virtuelles.

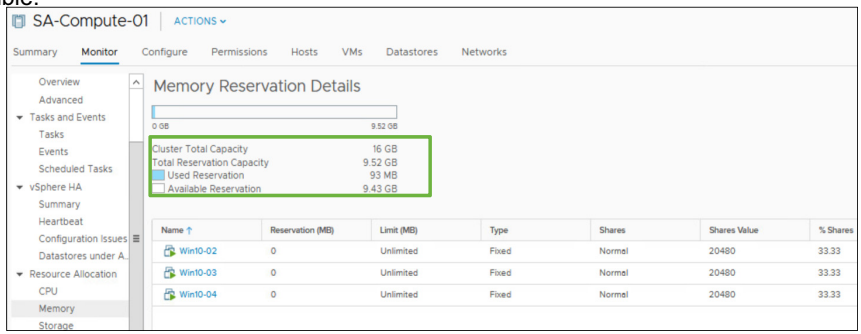


Voici quelques suggestions pour éviter la détection erronée de pannes d'hôte ou de problèmes d'isolation réseau suite à l'interruption des signaux de pulsation vSphere HA durant la maintenance du réseau :

- La modification des paramètres de matériel réseau ou de mise en réseau est susceptible d'interrompre les signaux de pulsation sur lesquels vSphere HA se fonde pour la détection des pannes d'hôte, ce qui peut entraîner une tentative de basculement intempestive des machines virtuelles. Si vous apportez des modifications aux réseaux auxquels appartiennent vos hôtes VMware ESXi en cluster, interrompez la fonction de surveillance des hôtes et placez l'hôte en mode maintenance.
- La surveillance des hôtes n'est requise qu'en cas de modification de composants ou de propriétés de réseau virtuel impliquant les ports VMkernel configurés pour le trafic de gestion ou le trafic vSAN, qui sont utilisés par le service de pulsation réseau de vSphere HA.
- Une fois les changements de configuration réseau effectués sur les hôtes VMware ESXi (par exemple, ajout de groupes de ports, retrait de commutateurs virtuels ou interruption de la surveillance des hôtes), vous devez reconfigurer vSphere HA sur tous les hôtes du cluster, de façon à déclencher une nouvelle inspection des informations réseau. Réactivez ensuite la surveillance des hôtes.

9-49 Réservation de ressources de cluster

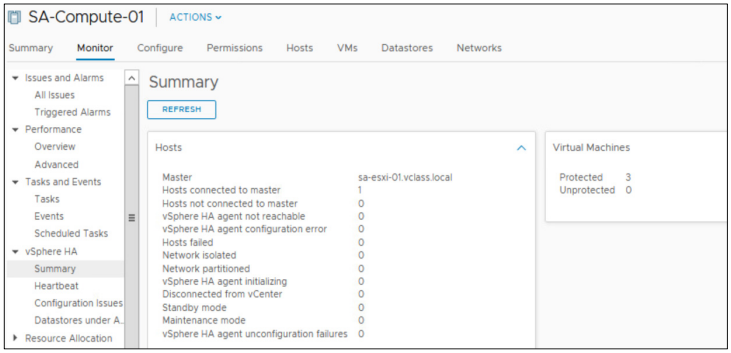
La page « Resource Allocation » de l'onglet **Monitor** indique la quantité totale de ressources disponibles sur le cluster (CPU, mémoire, capacité supplémentaire de mémoire, capacité de stockage), ainsi que la capacité réservée par les machines virtuelles et la capacité restant disponible.



vCenter Server utilise la fonction de contrôle d'admission de vSphere HA afin de garantir qu'un cluster dispose de ressources suffisantes pour assurer la protection par basculement, ainsi que le respect des réservations de ressources des machines virtuelles.

9-50 Surveillance de l’état du cluster

Pour surveiller l’état d’un cluster vSphere HA, il suffit de consulter la page « Summary » de l’onglet Monitor.



Pour surveiller l’état d’un cluster vSphere HA, il suffit de consulter la page « Summary » du volet vSphere HA, sous l’onglet **Monitor**.

Votre cluster et les hôtes qu’il contient sont exposés à des problèmes de configuration ou à d’autres erreurs susceptibles d’entraver le bon fonctionnement de vSphere HA. Vous pouvez surveiller ces erreurs sur la page « Configuration Issues », accessible depuis cette même zone.

9-51 Laboratoire 16 : Utilisation de vSphere HA

Utiliser la fonctionnalité vSphere HA

1. Créer un cluster configuré pour vSphere HA
2. Ajouter vos hôtes VMware ESXi au cluster
3. Tester les fonctionnalités de vSphere HA
4. Afficher l'utilisation des ressources du cluster vSphere HA
5. Gérer la taille de slot de vSphere HA
6. Configurer un cluster vSphere HA avec contrôle d'admission strict

9-52 Rappel des objectifs de la formation

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

- Connaître les exigences relatives à la création et à l'utilisation d'un cluster vSphere HA
- Configurer un cluster vSphere HA

9-53 Leçon 4 : Présentation de vSphere Fault Tolerance

9-54 Objectifs de la formation

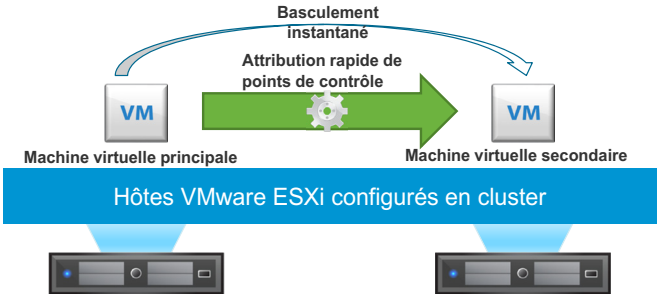
À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Décrire les avantages liés à l'utilisation de vSphere Fault Tolerance
- Expliquer le fonctionnement de vSphere Fault Tolerance
- Décrire les principales fonctionnalités de vSphere Fault Tolerance
- Décrire le fonctionnement de vSphere Fault Tolerance avec vSphere HA et vSphere DRS
- Activer vSphere Fault Tolerance depuis vSphere Web Client

9-55 À propos de vSphere Fault Tolerance

vSphere Fault Tolerance fournit des capacités de basculement instantané et de disponibilité continue :

- Sans interruption de service
- Aucune perte de données
- Aucune perte de connexion TCP



L'activation de vSphere Fault Tolerance sur vos machines virtuelles vous permet d'assurer la continuité d'activité en maintenant des niveaux de disponibilité et de protection des données plus élevés que ceux qu'offre vSphere HA.

vSphere Fault Tolerance, qui repose sur la plate-forme hôte VMware ESXi, assure une disponibilité en continu du système, grâce à l'exécution de machines virtuelles identiques sur des hôtes distincts.

Vous pouvez utiliser ce logiciel avec la plupart des machines virtuelles stratégiques. Il assure la disponibilité en continu pour une machine de ce type, en créant et en gérant une autre machine virtuelle (identique et également disponible en continu) destinée à la remplacer en cas de basculement.

La machine virtuelle ainsi protégée est appelée « machine virtuelle principale ». La machine virtuelle dupliquée est appelée « machine virtuelle secondaire ». La machine virtuelle est créée et exécutée sur un hôte distinct de celui de la machine virtuelle principale. Le type d'exécution de la machine secondaire est identique à celui de la machine principale. La machine virtuelle secondaire peut prendre le relais à tout moment sans générer d'interruption, ce qui permet de garantir une protection tolérante aux pannes.

La machine virtuelle principale et la machine virtuelle secondaire se surveillent mutuellement en permanence, de façon à garantir la continuité de la fonction de tolérance aux pannes. En cas de panne de l'hôte exécutant la VM principale, le basculement s'effectue de manière transparente ; la VM secondaire est immédiatement activée en remplacement de la VM principale. Une nouvelle VM secondaire est alors démarrée, et la redondance requise pour assurer la tolérance aux pannes est rétablie automatiquement. De même, si l'hôte exécutant la VM secondaire rencontre une panne, il est immédiatement remplacé. Dans l'un et l'autre cas, les utilisateurs ne subissent aucune interruption de service ni perte de données.

9-56 Fonctionnalités de vSphere Fault Tolerance

vSphere Fault Tolerance protège les applications stratégiques hautes performances et ce, quel que soit le système d'exploitation utilisé.

vSphere Fault Tolerance :

- Prend en charge des machines virtuelles dont la configuration comprend jusqu'à 8 VCPU et 128 Go de mémoire
- Prend en charge jusqu'à 4 VMs tolérantes aux pannes par hôte, avec un nombre maximal de 8 VCPU pour l'ensemble de ces VMs
- Prend en charge la migration via vSphere vMotion pour les machines virtuelles principale et secondaire
- Crée une copie secondaire de tous les fichiers et les disques d'une machine virtuelle
- Effectue une copie rapide des points de contrôle, afin d'assurer la synchronisation entre les CPU principaux et secondaires
- Prend en charge plusieurs formats de disque de machine virtuelle : provisionnement fin, provisionnement définitif avec mise à zéro en différé et provisionnement définitif avec mise à zéro immédiate
- Utilisable avec vSphere DRS si la compatibilité EVC (Enhanced vMotion Compatibility) est activée
- Assure l'interopérabilité avec vSAN

Vous pouvez utiliser vSphere Fault Tolerance avec vSphere DRS uniquement lorsque la fonction de compatibilité améliorée de vMotion (EVC, Enhanced vMotion Compatibility) est activée. Ce processus permet aux machines virtuelles tolérantes aux pannes de bénéficier d'un positionnement initial optimisé.

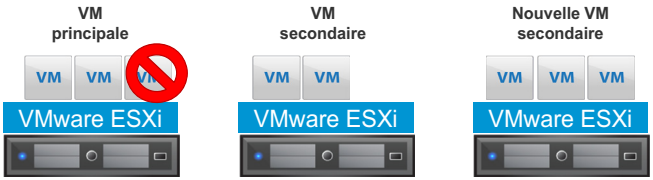
Lorsqu'un cluster est configuré pour EVC, vSphere DRS émet les recommandations de placement initial relatives aux machines virtuelles tolérantes aux pannes et vous permet d'associer un niveau d'automatisation vSphere DRS aux VM principales. Chaque VM secondaire adopte systématiquement les mêmes paramètres que la VM principale à laquelle elle est associée.

Lorsque la fonctionnalité vSphere Fault Tolerance est utilisée pour les machines virtuelles d'un cluster avec fonctionnalité EVC désactivée, le niveau d'automatisation vSphere DRS des machines virtuelles tolérantes aux pannes est défini sur « Disabled ». Dans un tel cluster, une VM principale ne peut être mise sous tension que sur l'hôte sur lequel elle est enregistrée, et le placement de sa VM secondaire est automatisé.

9-57 vSphere Fault Tolerance avec vSphere HA et vSphere DRS

vSphere Fault Tolerance fonctionne avec vSphere HA et vSphere DRS :

- vSphere HA :
  - Est requis pour l'utilisation de vSphere Fault Tolerance
  - Redémarre les machines virtuelles défaillantes
  - Est compatible avec vSphere Fault Tolerance
- vSphere DRS :
  - Sélectionne les hôtes affectés à l'exécution des machines virtuelles principale et secondaire lors de la mise sous tension d'une machine virtuelle
  - Ne migre pas automatiquement les machines virtuelles tolérantes aux pannes

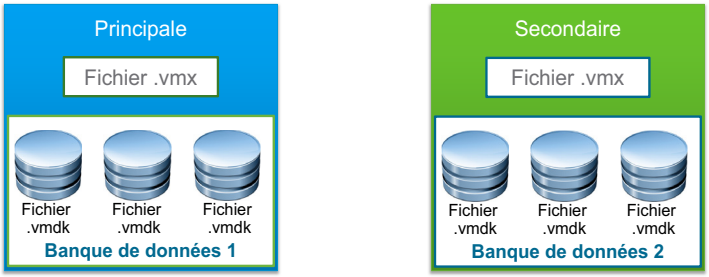


Une machine virtuelle tolérante aux pannes et sa copie secondaire ne peuvent pas s'exécuter sur un même hôte. Grâce à cette restriction, la panne d'un hôte ne peut pas entraîner celle des deux machines virtuelles.

9-58 Fichiers VMDK redondants

vSphere Fault Tolerance crée deux machines virtuelles complètes.

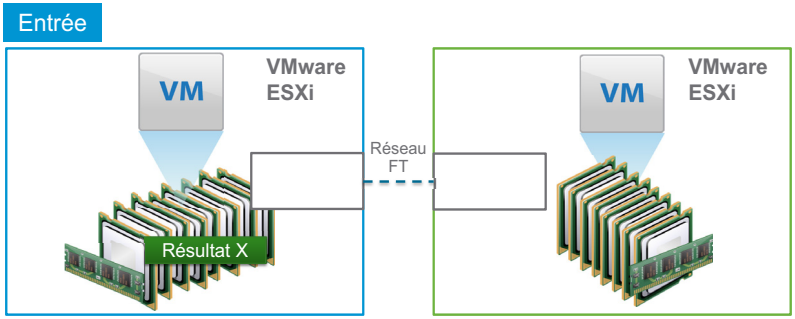
Chaque machine virtuelle possède son propre fichier de configuration `.vmx` et ses propres fichiers `.vmdk`. Chaque machine virtuelle peut se trouver sur une banque de données distincte.



vSphere Fault Tolerance assure une redondance à des fins de basculement en créant deux copies complètes de la machine virtuelle protégée. Les fichiers de machine virtuelle peuvent être placés sur la même banque de données. VMware recommande cependant de les placer sur des banques de données distinctes, de façon à permettre leur récupération en cas de panne de la banque de données.

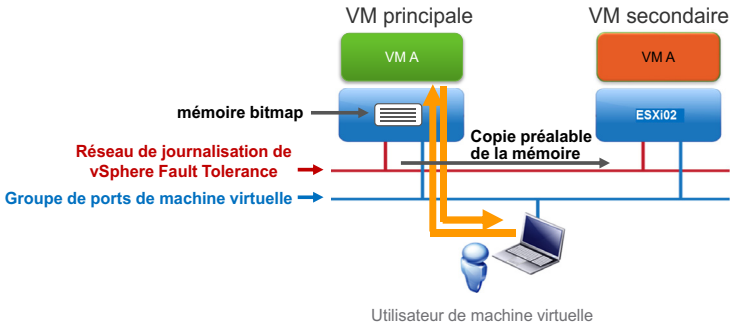
9-59 Point de contrôle de vSphere Fault Tolerance

Les modifications apportées sur la machine principale ne sont pas traitées sur la machine secondaire. La mémoire est mise à jour sur la machine secondaire.



9-60 vSphere Fault Tolerance : Copie préalable

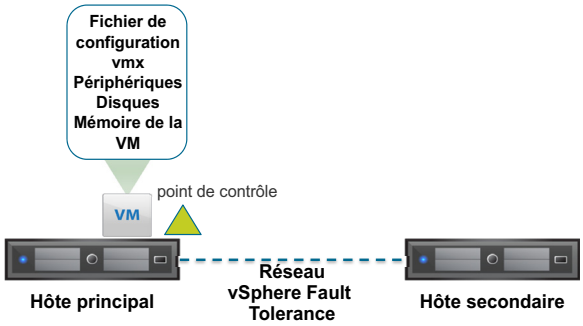
À l'aide de vSphere Fault Tolerance, une seconde VM est créée sur l'hôte secondaire. La mémoire de la machine virtuelle source est ensuite copiée vers l'hôte secondaire.



9-61 Point de contrôle rapide de vSphere Fault Tolerance

Dans le cadre de vSphere Fault Tolerance, l'intervalle entre les points de contrôle SMP (Symmetric Multi-Processing) est dynamique.

Cet intervalle s'adapte pour optimiser les performances des charges de travail.



Pour appliquer vSphere Fault Tolerance aux machines virtuelles SMP (Symmetric Multi-Processing), vous devez effectuer en continu des copies (points de contrôle) ultrarapides de la machine virtuelle de l'hôte principal. Cette méthode a pour effet de générer périodiquement des copies (points de contrôle) de la machine virtuelle de l'hôte principal qui sont envoyées vers l'hôte secondaire. En cas de blocage de l'hôte principal, la machine virtuelle reprend son exécution sur l'hôte secondaire au point correspondant au dernier envoi réseau.

L'objectif est de relever des points de contrôle des machines virtuelles au moins toutes les 10 millisecondes, tout en minimisant la surcharge CPU sur le chemin critique. Les traitements relevant d'un chemin non critique peuvent être transférés sur un autre cœur de processeur. La machine virtuelle principale est copiée en continu (prise de point de contrôle), et ces copies (points de contrôle) sont envoyées à un hôte secondaire.

La copie complète initiale (point de contrôle) est créée à l'aide d'une forme modifiée de migration via vSphere vMotion sur l'hôte secondaire. La machine virtuelle principale retient chaque paquet réseau sortant jusqu'à ce que la copie suivante (point de contrôle) ait été envoyée à l'hôte secondaire.

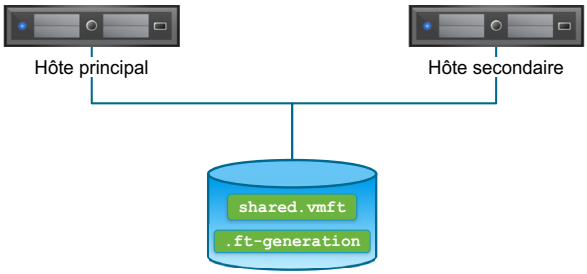
En cas de blocage de l'hôte principal, l'exécution de la machine virtuelle peut reprendre sur l'hôte de sauvegarde à partir de la dernière copie complète (point de contrôle).

Dans le cadre de vSphere Fault Tolerance, les données de point de contrôle constituent les dernières pages mémoire modifiées. La machine virtuelle source s'interrompt pour l'accès à cette mémoire. La durée de cette interruption est généralement inférieure à 1 seconde.

9-62 Fichiers partagés vSphere Fault Tolerance

vSphere Fault Tolerance comprend des fichiers partagés :

- `shared.vmft` évite la modification des UUID.
- `.ftgeneration` est associé à l'état de dédoublement.

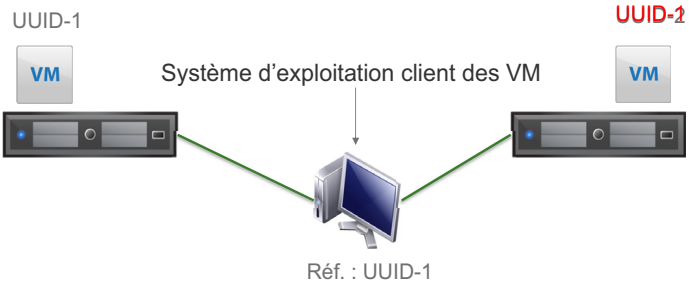


Un dédoublement de machines virtuelles peut se produire lorsqu'un hôte esclave se trouve isolé du réseau ou placé sur une autre partition que l'hôte maître et que ce dernier ne peut pas communiquer avec lui via les banques de données de signal de pulsation. Dans un tel cas, l'hôte maître ne peut pas établir l'état d'activité de l'hôte esclave et déclare donc celui-ci inactif.

L'hôte maître tente de redémarrer les machines virtuelles exécutées sur l'hôte isolé ou placé sur une autre partition. Ce redémarrage aboutit même si les machines virtuelles ont poursuivi leur exécution sur l'hôte isolé ou placé dans une autre partition, et que ce dernier a perdu l'accès aux banques de données des machines virtuelles lorsque le problème d'isolation ou de partitionnement s'est produit. Il y a alors dédoublement, dans la mesure où deux instances d'une même machine virtuelle coexistent. Le fichier `.ftgeneration` garantit qu'une seule instance de la machine virtuelle sera autorisée à effectuer des opérations de lecture ou d'écriture sur les disques virtuels de cette machine virtuelle.

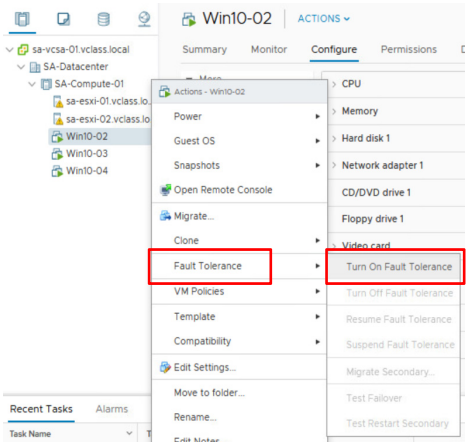
9-63 À propos du fichier shared.vmft

Le fichier `shared.vmft`, qui se trouve sur une banque de données partagée, est le fichier de métadonnées de vSphere Fault Tolerance. Ce fichier contient les UUID des instances principale et secondaire, ainsi que les chemins des fichiers vmx principal et secondaire.



9-64 Activation de vSphere Fault Tolerance sur une machine virtuelle

Vous pouvez activer vSphere Fault Tolerance pour une machine virtuelle via vSphere Web Client.



Une fois le déploiement de vSphere Fault Tolerance mené à bien à l'échelle de votre cluster, vous pouvez mettre cette fonctionnalité en œuvre en l'activant individuellement sur certaines machines virtuelles.

Avant l'activation de vSphere Fault Tolerance, des vérifications de validation sont effectuées sur la machine virtuelle concernée.

Une fois ces vérifications effectuées avec succès et vSphere Fault Tolerance activé sur une machine virtuelle, de nouvelles options viennent s'ajouter dans la section « Fault Tolerance » du menu contextuel. Ces options permettent de désactiver vSphere Fault Tolerance, de migrer la VM secondaire et de tester le basculement, ainsi que le redémarrage de la VM secondaire.

Lorsque la fonctionnalité vSphere Fault Tolerance est activée, vCenter Server réinitialise la limite de mémoire de la machine virtuelle et aligne la réservation de mémoire sur la taille de mémoire de la machine virtuelle. Tant que la fonctionnalité vSphere Fault Tolerance reste activée, vous ne pouvez pas modifier la réservation, la taille et la limite de mémoire, ni le nombre de VCPU ou de parts. Vous n'avez pas non plus la possibilité d'ajouter ni de supprimer des disques pour la machine virtuelle. Lorsque vSphere Fault Tolerance est désactivé, les paramètres modifiés ne retrouvent pas leur valeur d'origine.

9-65 Rappel des objectifs de la formation

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

- Décrire les avantages liés à l'utilisation de vSphere Fault Tolerance
- Expliquer le fonctionnement de vSphere Fault Tolerance
- Décrire les principales fonctionnalités de vSphere Fault Tolerance
- Décrire le fonctionnement de vSphere Fault Tolerance avec vSphere HA et vSphere DRS
- Activer vSphere Fault Tolerance depuis vSphere Web Client

9-66 Leçon 5 : vSphere Replication

9-67 Objectifs de la formation

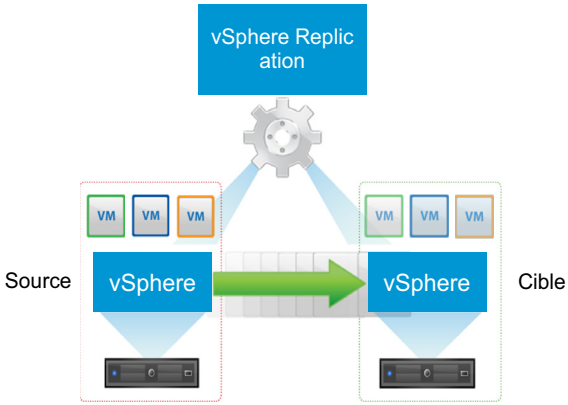
À la fin de cette leçon, vous devriez être en mesure d'atteindre les objectifs suivants :

- Décrire vSphere Replication
- Configurer vSphere Replication
- Récupérer des machines virtuelles répliquées
- Identifier les avantages liés au délestage du traitement des sauvegardes et au suivi des blocs modifiés

9-68 À propos de vSphere Replication

Le logiciel vSphere Replication est une extension de vCenter Server.

Il assure la réplication et la récupération par hyperviseur des machines virtuelles.



vSphere Replication constitue une alternative à la réplication basée sur la baie de stockage. Cette fonctionnalité protège les machines virtuelles contre les pannes de site partielles ou complètes en les répliquant selon l'un des schémas suivants :

D'un site source vers un site cible :

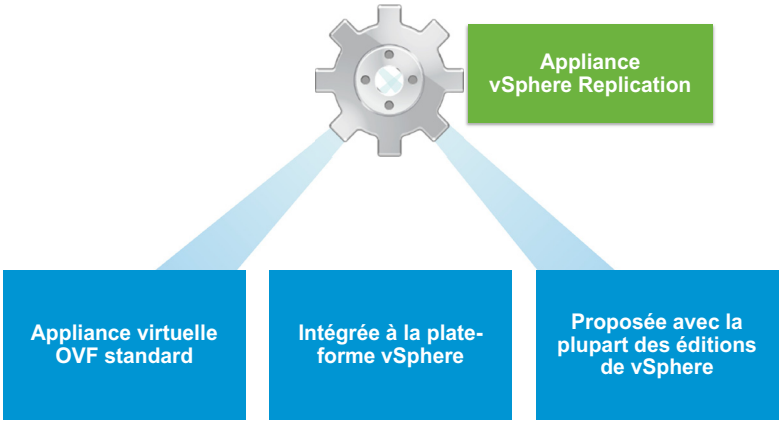
- d'un cluster vers un autre à l'intérieur d'un même site ;
- d'un ensemble de sites sources vers un site cible distant partagé.

vSphere Replication offre plusieurs avantages par rapport à la réplication basée sur le stockage :

- Protection des données pour un coût par machine virtuelle réduit par rapport à la réplication basée sur la baie de stockage
- Solution de réplication offrant une grande flexibilité quant au choix des fournisseurs de stockage pour les sites sources et cibles
- Coût par réplication globalement réduit par rapport à la réplication basée sur la baie de stockage

9-69 À propos de l'appliance vSphere Replication

L'appliance vSphere Replication fournit tous les composants requis pour assurer la réplication dans vSphere.



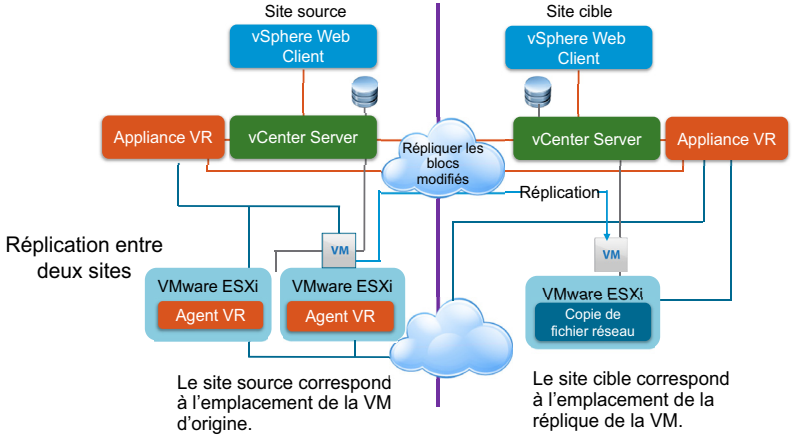
L'appliance vSphere Replication comprend les composants suivants :

- Serveur vSphere Replication fournissant le cœur d'infrastructure de vSphere Replication
- Base de données intégrée contenant les informations de configuration et de gestion des réplications
- Serveur de gestion vSphere Replication assurant les fonctionnalités suivantes :
  - Configuration du serveur vSphere Replication
  - Activation, gestion et surveillance des réplications
  - Authentification des utilisateurs et vérification de leurs autorisations en matière d'exécution des opérations vSphere Replication
- Plug-in pour vSphere Web Client offrant une interface utilisateur pour vSphere Replication

Vous pouvez commencer à utiliser vSphere Replication aussitôt après le déploiement de l'appliance. L'appliance vSphere Replication fournit l'interface de gestion d'appliance virtuelle (VAMI) qui permet de reconfigurer l'appliance après son déploiement. Vous pouvez notamment utiliser cette interface pour modifier les paramètres de sécurité ou les paramètres réseau de l'appliance, ou encore pour configurer une base de données externe. Vous avez également la possibilité de déployer des serveurs vSphere Replication supplémentaires à l'aide d'un package OVF distinct.

9-70 Fonctions de réplication

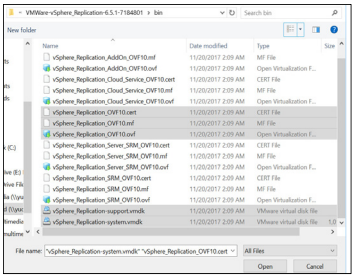
vSphere Replication vous permet de répliquer une machine virtuelle d'un site source sur un site cible, de surveiller et gérer l'état de la réplication, et de restaurer la machine virtuelle sur le site cible.

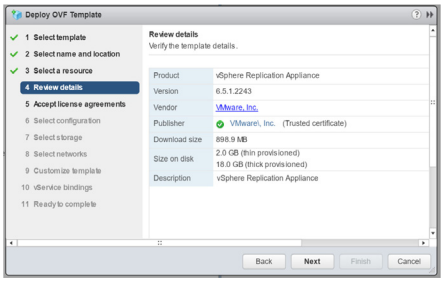


9-71 Déploiement de l’appliance virtuelle vSphere Replication

Pour pouvoir utiliser vSphere Replication, vous devez accéder à vSphere Web Client afin de déployer l’appliance vSphere Replication sur un hôte VMware ESXi :

- Téléchargez le package d’installation dans un répertoire local, ou récupérez son URL.
- Recourez à l’assistant de déploiement vSphere OVF standard pour déployer l’appliance :
  - Sélectionnez **vCenter > Hosts and Clusters**.
  - Cliquez avec le bouton droit sur un hôte et sélectionnez **Deploy OVF Template**.





L’appliance vSphere Replication s’enregistre en tant qu’extension auprès de l’instance de vCenter Server concernée.

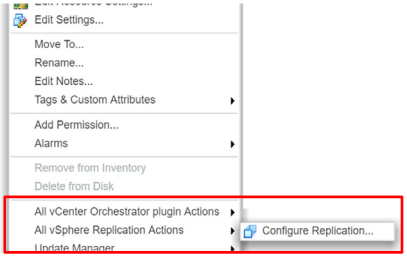
L’appliance vSphere Replication contient un serveur vSphere Replication intégré qui assure la gestion du processus de réplication. Afin de couvrir les besoins d’équilibrage de charge à l’échelle de votre environnement, il peut s’avérer nécessaire de déployer des serveurs vSphere Replication supplémentaires sur chacun des sites. Les serveurs vSphere Replication supplémentaires que vous déployez sont eux-mêmes des appliances virtuelles. Tout serveur vSphere Replication supplémentaire doit être enregistré auprès de l’instance de l’appliance vSphere Replication du site concerné.

L’appliance vSphere Replication fournit l’interface VAMI. Cette interface vous permet de reconfigurer la base de données vSphere Replication, les paramètres réseau, les certificats de clé publique et les mots de passe associés aux appliances. vSphere Replication peut être déployé avec une adresse IPv4 ou IPv6. Le mélange d’adresses IP, tel que l’utilisation d’une adresse IPv4 et d’une adresse IPv6 pour une même appliance, n’est pas pris en charge. Pour s’enregistrer en tant qu’extension, vSphere Replication s’appuie sur la propriété VirtualCenter.FQDN de l’instance de vCenter Server. En cas d’utilisation d’une adresse IPv6 pour vSphere Replication, la propriété VirtualCenter.FQDN doit être définie sur un nom de domaine complet pouvant être résolu sous la forme d’une adresse IPv6 ou d’une adresse littérale. Lorsque vSphere Replication fonctionne avec une adresse IPv6, tous les composants de l’environnement, dont l’instance vCenter Server et les hôtes VMware ESXi, doivent être accessibles via l’adresse IPv6.

9-72 Configuration de vSphere Replication pour une seule machine virtuelle

Si vous souhaitez configurer vSphere Replication pour une machine virtuelle déterminée, effectuez l'une des actions suivantes dans vSphere Web Client :

- Sélectionnez la machine virtuelle dans l'inventaire, puis sélectionnez **Actions > All vSphere Replication Actions > Configure**.
- Cliquez avec le bouton droit sur la machine virtuelle dans l'inventaire, puis sélectionnez **All vSphere Replication Actions > Configure**.



vSphere Replication est capable de protéger des machines virtuelles individuelles et leurs disques virtuels en les répliquant à un autre emplacement.

Lors de la configuration de la réplication, vous définissez un objectif de point de reprise afin de déterminer l'intervalle de temps entre les réplications. Par exemple, un objectif de point de reprise fixé à 1 heure garantit que la machine virtuelle ne perdra pas plus d'une heure de données pendant la récupération. Des objectifs de point de reprise plus serrés réduisent la quantité de données perdue lors d'une récupération, mais accroissent la consommation de bande passante réseau nécessaire pour synchroniser la réplique.

Chaque fois qu'une machine virtuelle atteint son objectif de point de reprise, vSphere Replication enregistre environ 3 800 octets de données dans la base de données d'événements de vCenter Server. Si vous spécifiez une période courte pour l'objectif de point de reprise, le volume des données stockées dans la base de données peut devenir très conséquent. Pour éviter d'ajouter de trop grands volumes de données à la base de données d'événements de vCenter Server, réduisez le nombre de jours pendant lequel vCenter Server conserve les données d'événement. Voir la section relative à la configuration de la règle de conservation de la base de données dans le guide *Gestion de vCenter Server et des hôtes*, disponible à l'adresse suivante : https://docs.vmware.com/en/VMware-vSphere/6.7/vsphere-esxi-vcenter-server-67-host-management-guide.pdf. Une autre solution consiste à définir une période plus longue pour l'objectif de point de reprise.

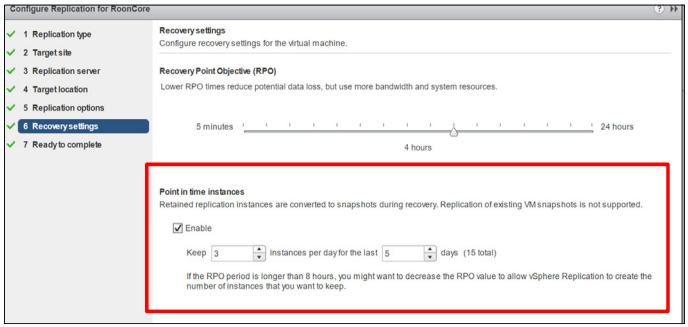
vSphere Replication garantit des répliques « crash-consistent » pour tous les disques appartenant à une même machine virtuelle. L'utilisation de la fonction de mise au repos Microsoft Volume Shadow Copy Service (VSS) est susceptible d'assurer un niveau plus élevé de cohérence. Les types de mise au repos disponibles sont déterminés par le système d'exploitation de la machine virtuelle. Pour plus d'information sur la prise en charge de la mise au repos VSS pour les machines virtuelles Windows, voir les matrices de compatibilité relatives à vSphere Replication 5.8, disponibles à l'adresse suivante : https://www.vmware.com/support/vsphere-replication/doc/vsphere-replication-compat-matrix-5-8.html.

Vous avez la possibilité d'utiliser vSphere Replication avec une banque de données vSAN sur les sites source et cible. Pour plus d'informations sur les contraintes liées à l'utilisation de vSphere Replication avec le stockage vSAN, voir le document *Utilisation de vSphere Replication avec le stockage vSAN*, disponible sur http://docs.vmware.com.

9-73 Configuration de plusieurs instantanés et de l'objectif de point de reprise

vSphere Web Client vous permet de configurer plusieurs instantanés au cours de la configuration de vSphere Replication.

La valeur que vous spécifiez à l'aide du curseur **Recovery Point Objective (RPO)** détermine la planification de la réplication.



Lorsque vous configurez une machine virtuelle pour la réplication, l'agent vSphere Replication transfère les blocs modifiés sur les disques de cette machine virtuelle du site source vers le site cible, où ces blocs sont appliqués à la copie de la machine virtuelle. Ce processus est indépendant de la couche de stockage. vSphere Replication procède initialement à une synchronisation complète de la machine virtuelle source avec sa réplique. Vous pouvez utiliser des copies primaires de réplication pour réduire le temps et la bande passante nécessaires à la réplication initiale.

Lors de la configuration de la réplication, vous avez la possibilité de définir un objectif de point de reprise et d'autoriser la conservation d'instances correspondant à plusieurs instantanés.

En tant qu'administrateur, vous pouvez surveiller et gérer l'état de la réplication. Vous disposez à cet effet des informations relatives aux réplications entrantes et sortantes, à l'état des sites source et cible, ainsi qu'aux problèmes, avertissements ou erreurs liés à la réplication.

Lorsque vous récupérez manuellement une machine virtuelle, vSphere Replication crée une copie de la machine virtuelle connectée au disque de réplique, mais ne connecte aucune des cartes d'interface réseau virtuelles à des groupes de ports. Vous pouvez alors examiner le processus de récupération et l'état de la réplique de machine virtuelle, puis connecter celle-ci aux réseaux. Vous avez la possibilité de ramener une machine virtuelle à l'état qui était le sien à un point donné dans le temps (par exemple, son dernier état cohérent connu). vSphere Replication présente les instances conservées comme de simples snapshots de machine virtuelle que vous pouvez restaurer.

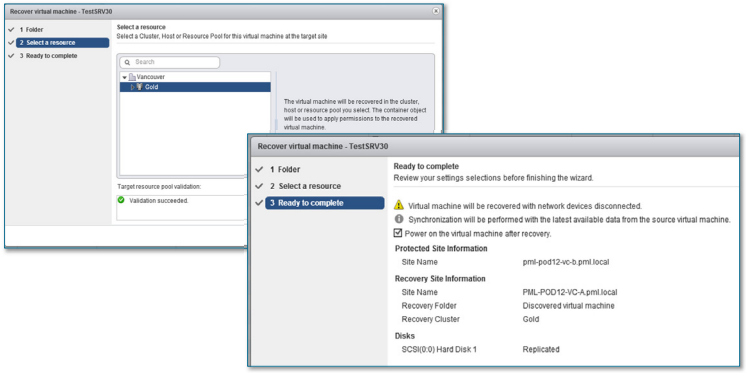
vSphere Replication stocke les données de configuration de la réplication dans une base de données intégrée. Vous pouvez aussi configurer vSphere Replication pour l'utilisation d'une base de données externe.

Vous avez la possibilité de répliquer une machine virtuelle entre deux sites, dans la mesure où vSphere Replication est installé sur les sites source et cible. Une seule appliance vSphere Replication peut être déployée sur chaque système vCenter Server. Vous avez toutefois la possibilité de déployer des serveurs vSphere Replication supplémentaires.

9-74 Récupération de machines virtuelles

vSphere Replication vous permet de récupérer les machines virtuelles qui ont été correctement répliquées sur le site cible.

Pour récupérer des machines virtuelles une à une, accédez à l'onglet **Incoming Replications**.



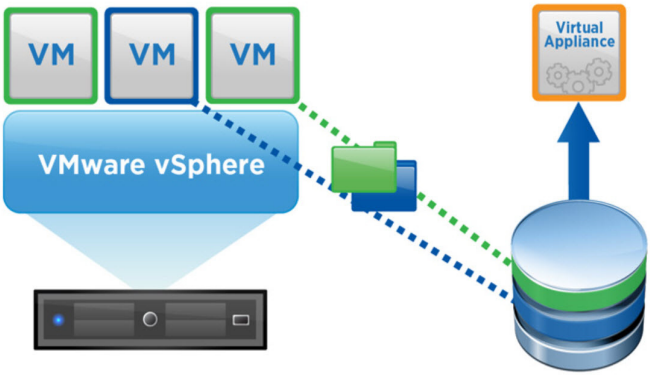
Vous utilisez l'assistant « Recover virtual machine » de vSphere Web Client sur le site cible pour effectuer la récupération.

Vous êtes invité à préciser si vous souhaitez restaurer la machine virtuelle avec l'intégralité de ses données les plus récentes, ou uniquement avec les données les plus récentes disponibles sur le site cible. Si vous sélectionnez **Recover with recent changes** en vue d'éviter toute perte de données, vSphere Replication effectue une synchronisation complète de la machine virtuelle du site source vers le site cible avant de procéder à sa récupération. Cette option implique que les données de la machine virtuelle source soient accessibles. Vous ne pouvez la sélectionner que si la machine virtuelle est hors tension. Si vous sélectionnez **Recover with latest available data**, vSphere Replication récupère la machine virtuelle à l'aide des données issues de la réplication la plus récente sur le site cible, sans synchronisation préalable. Cette option entraîne la perte des éventuelles données modifiées depuis la dernière réplication. Sélectionnez cette option si la machine virtuelle source est inaccessible ou si ses disques sont corrompus.

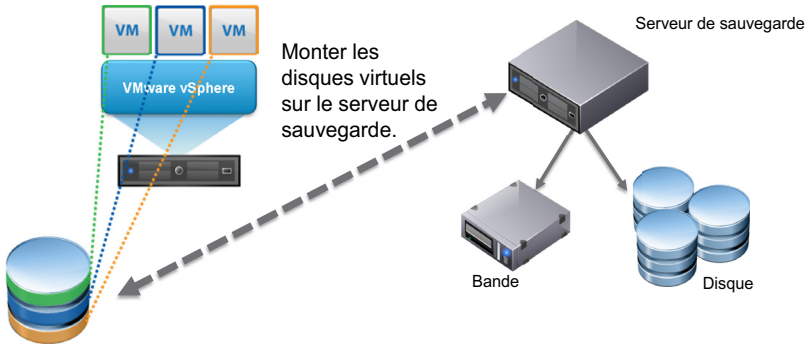
vSphere Replication valide vos entrées et récupère la machine virtuelle. Si la récupération aboutit, l'état de la machine virtuelle passe à « Recovered ». La machine virtuelle apparaît dans l'inventaire du site cible.

9-75 vSphere Storage APIs - Data Protection

vSphere Storage APIs - Data Protection permet aux produits de sauvegarde d'effectuer des sauvegardes efficaces, centralisées, hors hôte et hors LAN de machines virtuelles vSphere.



9-76 Délestage du traitement des sauvegardes



Configurez l'environnement de stockage de sorte que le serveur de sauvegarde accède aux volumes de stockage gérés par les hôtes VMware ESXi.

Le traitement des sauvegardes est transféré de l'hôte VMware ESXi au serveur de sauvegarde, ce qui permet d'éviter une surcharge des ressources VMware ESXi locales.

L'un des principaux goulets d'étranglement limitant les performances de sauvegarde provient souvent du serveur de sauvegarde, qui gère l'ensemble des tâches liées à la coordination des sauvegardes. L'une de ces tâches de sauvegarde consiste à copier les données d'un point A à un point B. D'autres tâches de sauvegarde sollicitent lourdement les ressources CPU. Par exemple, certaines tâches ont pour but de déterminer les données qui doivent être sauvegardées ou non. D'autres visent à dédupliquer les données, ou à compresser les données écrites sur la cible.

Un serveur doté de ressources CPU insuffisantes peut ralentir considérablement les performances de sauvegarde, d'où l'importance de ne pas lésiner sur les ressources du serveur de sauvegarde. Un serveur physique ou une machine virtuelle abondamment dotés en ressources mémoire et CPU sont indispensables pour garantir des performances de sauvegarde optimales.

Les sauvegardes hors LAN présentent l'intérêt de réduire la charge appliquée aux ressources physiques de l'hôte VMware ESXi lors de la sauvegarde des machines virtuelles en transférant le traitement de ces sauvegardes de l'hôte VMware ESXi à un serveur proxy de sauvegarde.

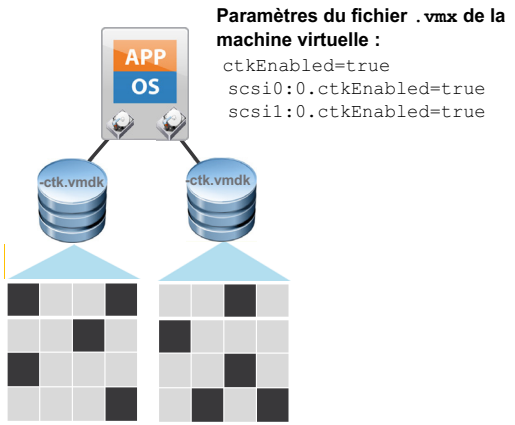
Vous pouvez configurer votre environnement de sorte qu'il effectue des sauvegardes hors LAN vers le serveur proxy de sauvegarde. Pour les besoins des sauvegardes hors LAN, le serveur de sauvegarde doit avoir accès au stockage géré par les hôtes VMware ESXi sur lesquels les machines virtuelles à sauvegarder sont exécutées.

Si vous avez recours au stockage relié au réseau (NAS) ou au stockage en attachement direct (DAS), assurez-vous que le serveur proxy de sauvegarde ait bien accès aux volumes requis via un mécanisme de transport réseau. Si vous prévoyez d'effectuer une sauvegarde SAN directe, zonez le SAN et configurez les mappages hôte des sous-systèmes de disques. Les mappages hôte doivent être configurés de telle sorte que tous les hôtes VMware ESXi ainsi que le serveur proxy de sauvegarde accèdent aux mêmes volumes de disques.

9-77 À propos du suivi des blocs modifiés

Le suivi des blocs modifiés vous permet de copier uniquement les blocs de fichier qui ont été modifiés depuis la dernière sauvegarde.

Le suivi des blocs modifiés permet d'effectuer des sauvegardes plus rapides car incrémentielles.



Le suivi des blocs modifiés (CBT) est une fonctionnalité de VMkernel qui conserve la trace des modifications apportées aux blocs de stockage des machines virtuelles. En assurant le suivi des modifications de bloc effectuées sur les machines virtuelles, VMkernel permet d'optimiser le processus de sauvegarde relatif aux applications conçues pour exploiter les API vSphere Storage APIs - Data Protection.

vSphere Data Protection améliore l'efficacité des sauvegardes d'image en exploitant la fonctionnalité de suivi des blocs modifiés (CBT), qui réduit considérablement le temps nécessaire à la sauvegarde d'une image de machine virtuelle donnée, et offre la possibilité de traiter un grand nombre de machines virtuelles au cours d'une fenêtre de sauvegarde déterminée.

Lors des opérations de récupération, vSphere Data Protection tire également parti du suivi des blocs modifiés pour récupérer les machines virtuelles à leur emplacement d'origine de manière rapide et efficace. Dans le cadre du processus de récupération, VMware vSphere Data Protection s'appuie sur le suivi des blocs modifiés pour identifier les blocs ayant subi des modifications depuis la dernière sauvegarde. Le suivi des blocs modifiés permet de limiter les transferts de données liés à la récupération au sein de l'environnement vSphere, mais aussi et surtout de réduire le délai de récupération.

De plus, Data Protection évalue la charge de travail liée aux deux méthodes de restauration possibles (restauration d'une image complète ou récupération via CBT) et utilise la méthode la plus rapide. Cette fonction est utile dans le cas où le taux de modifications depuis la dernière sauvegarde de la machine virtuelle à restaurer est très élevé, de sorte que l'opération d'analyse CBT entraînerait une charge plus importante que la récupération directe de l'image complète. Data Protection détermine quelle méthode permet de récupérer le plus rapidement les machines virtuelles de l'environnement.

9-78 Rappel des objectifs de la formation

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

- Décrire vSphere Replication
- Configurer vSphere Replication
- Récupérer des machines virtuelles répliquées
- Identifier les avantages liés au délestage du traitement des sauvegardes et au suivi des blocs modifiés

9-79 Points clés

- vSphere HA redémarre les machines virtuelles sur les hôtes restants du cluster.
- Les hôtes d'un cluster vSphere HA sont liés par une relation maître-esclave.
- La mise en œuvre de réseaux de signal de pulsation redondants s'effectue soit par association de cartes d'interface réseau, soit par création de réseaux de signal de pulsation supplémentaires.
- vSphere Fault Tolerance assure un fonctionnement sans aucune interruption de service pour les applications devant être disponibles en permanence.
- vSphere Replication peut être utilisé pour protéger les machines virtuelles dans le cadre d'une stratégie de reprise d'activité.
- vSphere Replication est la seule solution de réplication par hyperviseur qui opère au niveau de chaque disque de machine virtuelle, ce qui permet des réplications entre des banques de données hébergées sur tout type de stockage.

Des questions ?

MODULE 10

vSphere DRS

10-2 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

10-3 Importance

Pour assurer l'évolution de votre environnement vSphere, vous devez maîtriser les fonctionnalités et fonctions de vSphere permettant de gérer plus efficacement les hôtes déployés dans cet environnement.

vSphere DRS vous donne le moyen d'améliorer les niveaux de service en garantissant les ressources appropriées aux machines virtuelles. Chaque administrateur système a également la possibilité de surveiller et de gérer un plus grand volume d'infrastructure.

10-4 Objectifs de la formation

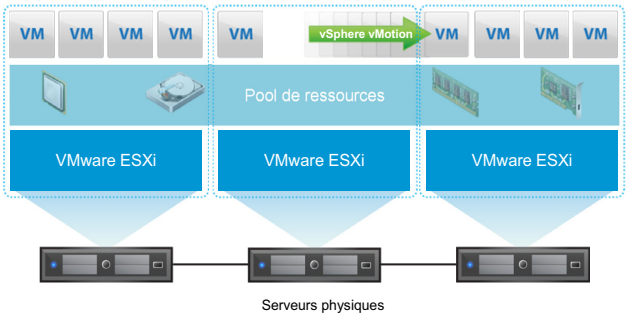
À la fin du module, vous devriez être en mesure d'atteindre les objectifs suivants :

- Décrire les fonctions d'un cluster vSphere DRS
- Créer un cluster vSphere DRS
- Examiner les informations relatives à un cluster vSphere DRS
- Supprimer un hôte d'un cluster vSphere DRS

10-5 À propos de vSphere DRS

vSphere DRS regroupe la capacité de calcul d'un ensemble de serveurs en pools de ressources logiques.

vSphere DRS alloue les ressources disponibles aux machines virtuelles en fonction de règles prédéfinies reflétant les besoins métiers et l'évolution des priorités.



vSphere DRS permet d'améliorer l'allocation des ressources sur l'ensemble des hôtes et des pools de ressources. Cette solution recueille des informations sur l'utilisation des ressources à l'échelle de tous les hôtes et de toutes les machines virtuelles du cluster, puis émet des recommandations (ou fait migrer des machines virtuelles) dans ces deux situations :

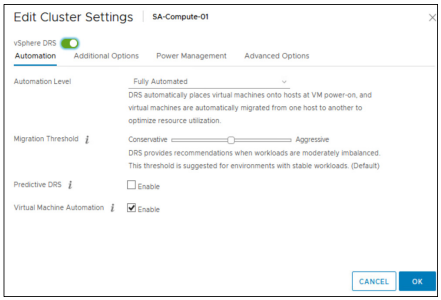
- Placement initial : lorsque vous mettez une machine virtuelle sous tension dans le cluster pour la première fois, vSphere DRS peut soit placer cette machine virtuelle, soit émettre une recommandation.
- Équilibrage de charge : vSphere DRS tente d'améliorer l'utilisation des ressources à l'échelle du cluster en migrant automatiquement des machines virtuelles (vSphere vMotion) ou en émettant des recommandations de migration pour des machines virtuelles.

10-6 Conditions requises pour le cluster vSphere DRS

vSphere DRS fonctionne de manière optimale lorsque les machines virtuelles répondent aux exigences de la migration via vSphere vMotion.

Si vous envisagez d'utiliser vSphere DRS à des fins d'équilibrage de charge, les hôtes du cluster doivent faire partie d'un réseau de migration via vSphere vMotion. Dans le cas contraire, vSphere DRS peut néanmoins émettre des recommandations quant à leur placement initial.

Pour utiliser le stockage partagé, configurez tous les hôtes du cluster comme suit. Tous les hôtes du cluster doivent avoir accès aux mêmes banques de données.



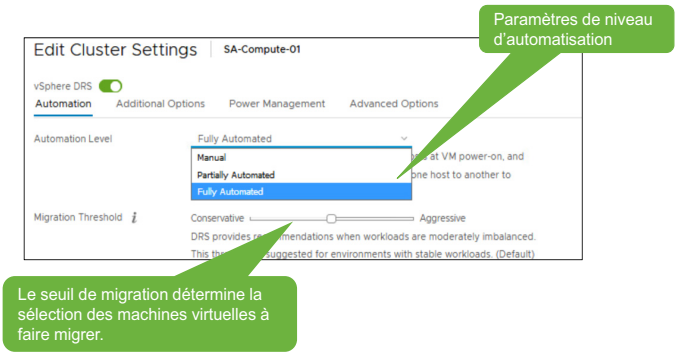
Un hôte VMware ESXi™ ajouté à un cluster vSphere DRS doit satisfaire à certaines conditions pour pouvoir utiliser les fonctionnalités de ce cluster :

- vSphere DRS fonctionne de manière optimale lorsque les machines virtuelles répondent aux exigences de vSphere vMotion.
- Si vous envisagez d'utiliser vSphere DRS à des fins d'équilibrage de charge, les hôtes de votre cluster doivent faire partie d'un réseau vSphere vMotion.
- Configurez tous les hôtes gérés pour l'utilisation de stockage partagé : les banques de données VMFS, vSAN, vSphere Virtual Volumes ou NFS.
- Placez les disques de toutes les machines virtuelles sur un stockage partagé accessible aux hôtes source et de destination.

Vous pouvez soit créer des clusters vSphere DRS, soit activer vSphere DRS sur des clusters vSphere HA ou vSAN existants.

10-7 Paramètres du cluster vSphere DRS : Niveau d'automatisation

Configurez le niveau d'automatisation pour le placement initial des machines virtuelles et l'équilibrage de charge dynamique des VMs en cours d'exécution.



Pour créer un cluster vSphere DRS, cliquez avec le bouton droit de la souris sur votre Data Center dans l'inventaire, puis sélectionnez **New Cluster**. La boîte de dialogue « New Cluster » s'affiche. Entrez un nom descriptif pour votre cluster et cochez la case **Turn On VMware DRS**.

Dans la fenêtre vSphere DRS qui vous est présentée (voir diapositive), commencez par définir le niveau d'automatisation. Selon le niveau d'automatisation spécifié, vSphere DRS vous présente des recommandations de migration ou assure automatiquement le placement des machines virtuelles sur les hôtes. vSphere DRS prend de telles décisions de placement au moment de la mise sous tension d'une machine virtuelle ou lorsque des machines virtuelles doivent être déplacées entre les hôtes du cluster à des fins de rééquilibrage. Les modèles d'automatisation suivants sont disponibles :

- **Manual** : lorsque vous mettez une machine virtuelle sous tension, vSphere DRS affiche une liste d'hôtes recommandés pour le placement de cette dernière. En cas de déséquilibre du cluster, vSphere DRS affiche des recommandations de migration de la machine virtuelle.
- **Partially automated** : lorsque vous mettez une machine virtuelle sous tension, vSphere DRS place cette dernière sur l'hôte le mieux adapté. En cas de déséquilibre du cluster, vSphere DRS affiche des recommandations de migration manuelle de machines virtuelles.
- **Fully automated** : lorsque vous mettez une machine virtuelle sous tension, vSphere DRS place cette dernière sur l'hôte le mieux adapté. En cas de déséquilibre du cluster, vSphere DRS migre automatiquement les machines virtuelles des hôtes surexploités vers les hôtes sous-exploités, afin de garantir une utilisation équilibrée des ressources du cluster.

Le seuil de migration détermine le degré de réactivité avec lequel vSphere DRS prend ses décisions de migration de machines virtuelles :

- Niveau 1 (« Conservative ») : application des seules recommandations de priorité 1. vCenter Server applique uniquement les recommandations répondant aux contraintes des clusters, telles que les règles d'affinité ou les obligations de maintenance des hôtes.
- Niveau 2 : application des recommandations de priorité 1 ou 2. vCenter Server applique les recommandations promettant d'améliorer significativement l'équilibrage de la charge du cluster.
- Niveau 3 (par défaut) : application des recommandations de priorité 1, 2 ou 3. vCenter Server applique les recommandations visant au minimum une amélioration notable de l'équilibrage de la charge du cluster.
- Niveau 4 : application des recommandations de priorité 1, 2, 3 ou 4. vCenter Server applique les recommandations visant une amélioration même modérée de l'équilibrage de la charge du cluster.
- Niveau 5 (« Aggressive ») : application de l'ensemble des recommandations. vCenter Server applique toute recommandation susceptible d'entraîner une amélioration même légère de l'équilibrage de la charge du cluster.

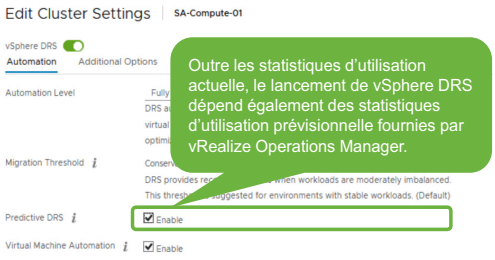
10-8 Paramètres du cluster vSphere DRS : « Predictive DRS »

vSphere DRS et VMware vRealize® Operations Manager™ combinent diverses données pour anticiper les besoins à venir et pour déterminer où et quand des points sensibles risquent d'apparaître.

Le collecteur de données de vSphere DRS récupère des statistiques auprès des sources suivantes :

- Statistiques d'utilisation des ressources émanant des hôtes
- Statistiques prévisionnelles émanant du serveur vRealize Operations Manager

Les statistiques d'utilisation prévisionnelle prévalent systématiquement sur les statistiques d'utilisation actuelle.



En cas d'évolution des besoins en ressources d'une machine virtuelle, vSphere DRS n'est pas capable de prévoir par lui-même la demande à venir. vSphere DRS peut toutefois exploiter les statistiques fournies par VMware vRealize® Operations Manager™ afin d'analyser la charge de travail que les machines virtuelles auront à traiter dans un proche avenir. vSphere DRS peut alors s'appuyer sur les niveaux de charge de travail prévisionnelle et d'utilisation actuelle pour anticiper les futurs besoins en ressources dans ses décisions de placement.

Si l'utilisation actuelle est plus importante que l'utilisation prévisionnelle, les statistiques d'utilisation actuelle prévalent et les recommandations sont générées sur la base de ces valeurs.

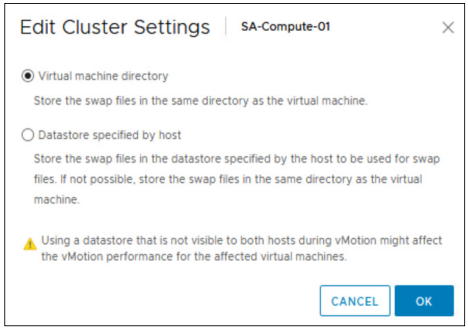
Dans le cas contraire, c'est le niveau d'utilisation prévisionnel qui est adopté pour définir les besoins actuels de la machine virtuelle. Les ressources sont ainsi disponibles avant même que la VM en ait besoin, évitant ainsi tout impact potentiel sur les performances.

Par défaut, le mode proactif de DRS table sur une marge d'anticipation d'une heure pour garantir la rapidité des migrations.

10-9 Autres paramètres de cluster : Emplacement du fichier d'échange

Par défaut, les fichiers d'échange d'une machine virtuelle se trouvent dans une banque de données, au sein du dossier contenant les autres fichiers de cette machine virtuelle.

Vous avez cependant la possibilité de les placer dans une autre banque de données.



Par défaut, le fichier d'échange est créé au même emplacement que le fichier de configuration de la machine virtuelle, qui peut se trouver dans une banque de données VMFS, NFS, vSAN ou vSphere Virtual Volumes. Dans le cas d'une banque de données vSAN ou vSphere Virtual Volumes, le fichier d'échange est créé sous la forme d'un objet vSAN ou vSphere Virtual Volumes distinct.

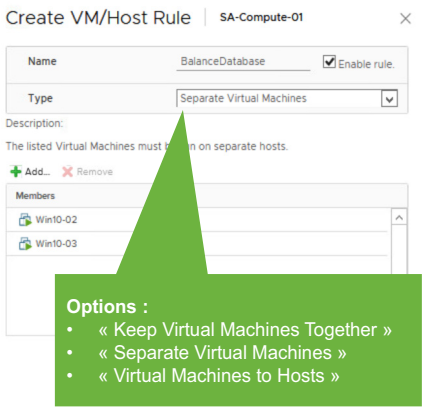
Un fichier d'échange est créé par l'hôte VMware ESXi lors de la mise sous tension de la machine virtuelle. En cas d'impossibilité de créer ce fichier, la machine virtuelle ne peut pas démarrer. Au lieu d'accepter le paramètre par défaut, vous pouvez sélectionner l'une des options suivantes :

- Recourir aux options de configuration VM par VM pour remplacer la banque de données par un autre emplacement de stockage partagé.
- Utiliser un échange local hôte, qui vous permet de spécifier une banque de données stockée localement sur l'hôte. Vous pouvez ainsi maintenir le processus d'échange au niveau d'un hôte de façon à économiser de l'espace sur le SAN. Cette option peut toutefois entraîner une légère dégradation des performances de vSphere vMotion, dans la mesure où les pages placées dans un fichier d'échange local sur l'hôte source devront être transférées sur l'hôte de destination via le réseau. Actuellement, les banques de données vSAN et vSphere Virtual Volumes ne peuvent pas être spécifiées en tant qu'échange local hôte.

10-10 Paramètres du cluster vSphere DRS : affinité entre les machines virtuelles

Les règles d'affinité de vSphere DRS indiquent que les machines virtuelles sélectionnées doivent être placées sur le même hôte (affinité) ou sur des hôtes distincts (anti-affinité).

- Règles d'affinité : à utiliser pour les systèmes multi-VMs impliquant une communication intensive entre les machines virtuelles.
- Règles d'anti-affinité : à utiliser pour les systèmes multi-VMs présentant des exigences d'équilibrage de charge ou de haute disponibilité.



Une fois que le cluster vSphere DRS est créé, vous pouvez modifier ses propriétés afin de créer des règles spécifiant les contraintes d'affinité. Les règles suivantes sont prises en charge :

- Règles d'affinité : vSphere DRS maintient certaines machines virtuelles ensemble sur un même hôte (par exemple, pour des raisons de performances).
- Règles d'anti-affinité : vSphere DRS évite que certaines machines ne se retrouvent ensemble (par exemple, pour des raisons de disponibilité).

La diapositive illustre une règle d'anti-affinité exigeant que deux machines virtuelles (Greg01 et Greg01-2) soient placées sur des hôtes distincts, sans doute pour des raisons de disponibilité ou de performances. À l'inverse, vous pouvez recourir à des règles d'affinité pour conserver certaines machines virtuelles sur un même hôte et bénéficier ainsi d'avantages accrus en termes de colocalisation ou de performances, notamment si ces machines virtuelles communiquent entre elles de manière intensive.

Si deux règles entrent en conflit, il ne vous est pas possible de les activer simultanément.

Lorsque l'ajout ou la modification d'une règle met le cluster en infraction immédiate avec cette règle, le système continue à fonctionner en tentant de corriger la violation.

Dans le cas des clusters vSphere DRS dont le niveau d'automatisation par défaut est configuré sur « Manual » ou « Partially automated », les recommandations de migration visent simultanément le respect des règles d'affinité et l'équilibrage de la charge.

10-11 Paramètres du cluster vSphere DRS : groupes DRS

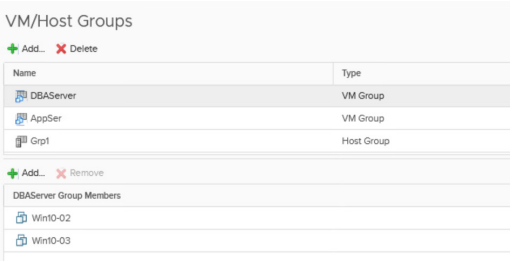
Les groupes de VMs ou d'hôtes sont utilisés pour définir des règles d'affinité VM/hôte.

Types de groupes de VMs ou d'hôtes :

- Groupes de VMs : une machine virtuelle peut appartenir à plusieurs groupes DRS de machines virtuelles.
- Groupes d'hôtes : un hôte peut appartenir à plusieurs groupes DRS d'hôtes.

Une machine virtuelle peut appartenir à plusieurs groupes de VMs.

Un hôte peut appartenir à plusieurs groupes d'hôtes.



La troisième option en matière de règles d'affinité vSphere DRS consiste à définir une règle d'affinité entre machines virtuelles et hôtes. Ce type de règle permet d'indiquer si des machines virtuelles peuvent ou non être exécutées sur un hôte déterminé. Pour simplifier l'administration, les machines virtuelles peuvent être placées dans des groupes de VMs ou d'hôtes. Pour un même cluster vSphere DRS, vous pouvez créer un ou plusieurs groupes de VMs ou d'hôtes comprenant chacun une ou plusieurs machines virtuelles. Sur la diapositive, le groupe DBAServer est un groupe DRS de machines virtuelles. Une machine virtuelle peut appartenir à plusieurs groupes DRS de machines virtuelles.

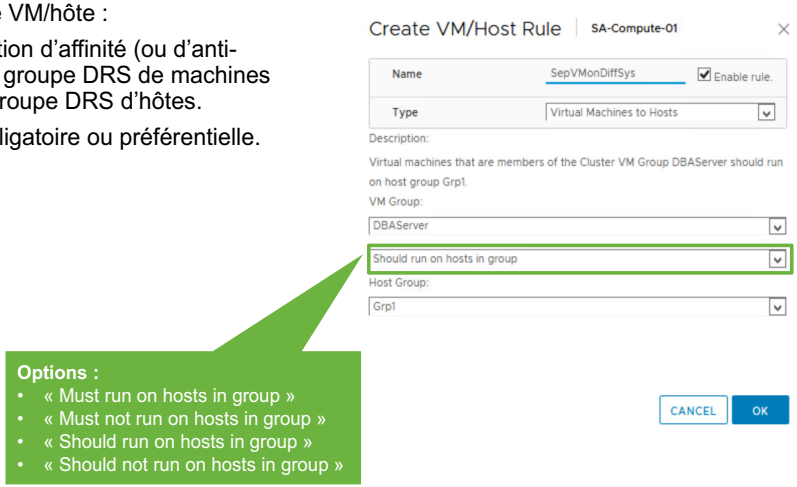
De même, un groupe DRS d'hôtes peut comprendre un ou plusieurs hôtes VMware ESXi. Un hôte peut appartenir à plusieurs groupes DRS d'hôtes. Sur la diapositive, le groupe Grp1 est un groupe DRS d'hôtes.

Les groupes DRS ont principalement pour but de vous aider lors de la définition de règles DRS appelées règles d'affinité machines virtuelles/hôtes.

10-12 Paramètres du cluster vSphere DRS : règles d'affinité VM/hôte

Une règle d'affinité VM/hôte :

- Indique une relation d'affinité (ou d'anti-affinité) entre un groupe DRS de machines virtuelles et un groupe DRS d'hôtes.
- Est une règle obligatoire ou préférentielle.



Une règle d'affinité ou d'anti-affinité machines virtuelles/hôtes indique si les membres d'un groupe DRS de machines virtuelles donné peuvent s'exécuter sur les membres d'un groupe DRS d'hôtes.

À la différence d'une règle d'affinité pour machines virtuelles, qui indique l'affinité (ou l'anti-affinité) entre des machines virtuelles, une règle d'affinité VM/hôte spécifie une relation d'affinité entre un groupe de machines virtuelles et un groupe d'hôtes. Ces règles peuvent être obligatoires ou préférentielles.

Une règle d'affinité machines virtuelles/hôte inclut les composants suivants :

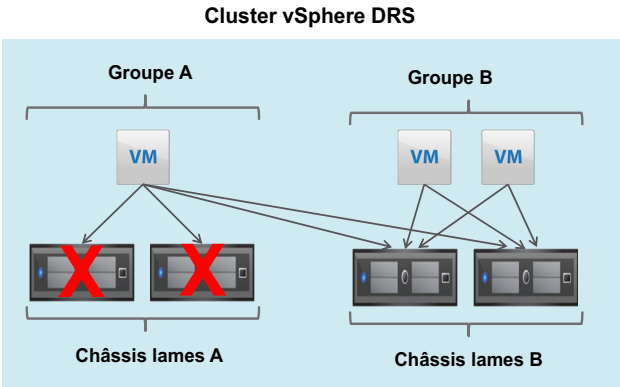
- Un groupe DRS de machines virtuelles
- Un groupe DRS d'hôtes
- L'indication du caractère obligatoire (« must ») ou préférentiel (« should ») de la règle, et de son statut de règle d'affinité (« run on ») ou d'anti-affinité (« not run on »).

Les règles d'affinité VM/hôte étant définies à l'échelle du cluster, les machines virtuelles et les hôtes qui sont inclus dans une règle doivent tous résider dans le même cluster. Une machine virtuelle supprimée du cluster perd son affiliation à tous ses groupes de machines virtuelles, y compris les groupes DRS, même si elle est ultérieurement réintroduite dans le cluster.

10-13 Règle d'affinité VM/hôte : préférentielle

Une règle préférentielle s'applique avec une certaine souplesse et peut être enfreinte si nécessaire.

Exemple : la répartition de machines virtuelles entre différents systèmes lames.



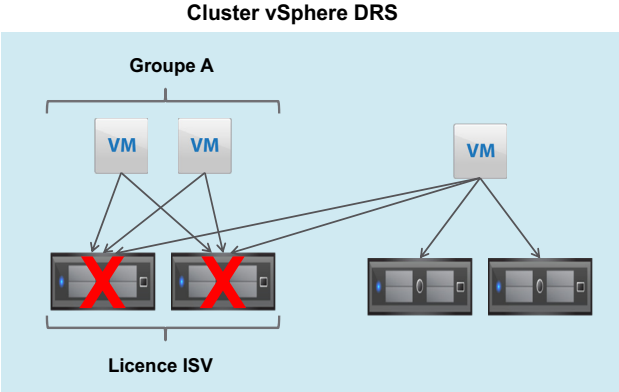
Une règle préférentielle est une règle dont l'application admet une certaine souplesse. Il est permis d'enfreindre une règle préférentielle pour assurer le bon fonctionnement de vSphere DRS, de vSphere HA ou de VMware vSphere® Distributed Power Management™.

Une règle préférentielle peut être utilisée pour maintenir des machines virtuelles sur des systèmes lames distincts afin d'optimiser les performances. Sur la diapositive, les groupes A et B sont des groupes DRS de machines virtuelles. Les châssis lames A et B sont des groupes DRS d'hôtes. L'objectif est de contraindre les machines virtuelles du groupe A à s'exécuter sur les hôtes du groupe Châssis lames A, et celles du groupe B, à s'exécuter sur les hôtes du groupe Châssis lames B. En cas de panne des hôtes, vSphere HA redémarre les machines virtuelles sur les autres hôtes du cluster. Si les hôtes sont placés en mode maintenance ou deviennent surchargés, vSphere DRS transfère les machines virtuelles vers les autres hôtes du cluster.

10-14 Règle d'affinité VM/hôte : obligatoire

Une règle obligatoire est appliquée de façon stricte et n'admet aucune exception.

Exemple : le déploiement de licences ISV sur certains hôtes.



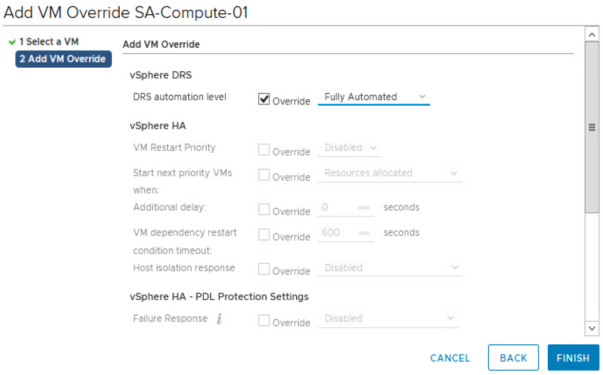
Vous pouvez opter pour une règle d'affinité VM/hôte à caractère obligatoire (plutôt que préférentiel) lorsque le logiciel exécuté sur vos machines virtuelles présente des conditions de licences restrictives. Vous pouvez appliquer cette règle lorsque le logiciel exécuté sur vos machines virtuelles présente des conditions de licences restrictives. En ce cas, placez les machines virtuelles concernées dans un groupe DRS . Créez ensuite une règle spécifiant que ces machines virtuelles doivent être exécutées dans un groupe DRS d'hôtes contenant exclusivement des hôtes munis des licences requises.

Lorsque vous créez une règle d'affinité VM/hôte répondant aux contraintes de licence ou de configuration matérielle des logiciels exécutés sur vos machines virtuelles, il vous appartient de vérifier que les groupes sont correctement configurés. La règle ne contrôle pas les logiciels exécutés sur les machines virtuelles et n'est pas informée de la présence ou de l'absence de licences tierces sur les différents hôtes VMware ESXi.

Sur la diapositive, le groupe A est un groupe DRS de machines virtuelles. Vous pouvez contraindre le groupe A à se lancer sur les hôtes du groupe Licence ISV afin de garantir que les machines virtuelles du groupe A s'exécutent exclusivement sur des hôtes munis des licences requises. Toutefois, en cas de défaillance des hôtes du groupe Licence ISV, vSphere HA ne peut pas redémarrer les machines virtuelles du groupe A sur des hôtes d'un autre groupe. De même, si les hôtes du groupe Licence ISV sont placés en mode maintenance ou deviennent surchargés, vSphere DRS ne peut pas transférer les machines virtuelles du groupe A vers des hôtes n'en faisant pas partie.

10-15 Paramètres du cluster vSphere DRS : automatisation à l'échelle d'une VM

Vous pouvez personnaliser le niveau d'automatisation de chaque machine virtuelle d'un cluster de manière à remplacer le niveau d'automatisation défini à l'échelle du cluster.



La définition du niveau d'automatisation à l'échelle de certaines machines virtuelles vous permet d'ajuster précisément l'automatisation à vos besoins. Par exemple, vous pourriez avoir besoin de mieux contrôler le placement d'une machine virtuelle particulièrement critique pour votre activité. Dans ce cas, définissez son niveau d'automatisation sur « Manual ». Si le niveau d'automatisation d'une machine virtuelle est défini sur « Disabled », vCenter Server ne migre pas cette machine virtuelle et n'émet aucune recommandation de migration à son sujet.

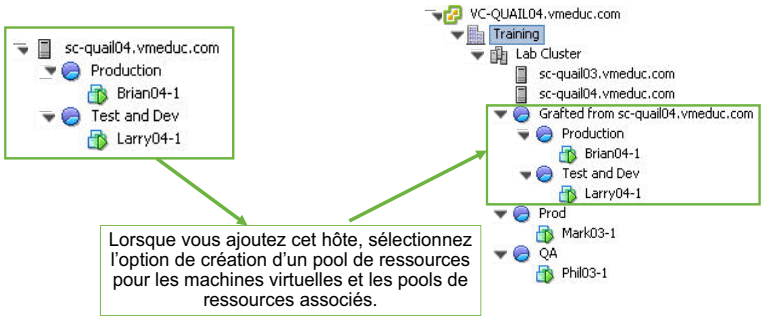
Il est donc recommandé d'activer l'automatisation. Sélectionnez le niveau d'automatisation en fonction des caractéristiques de votre environnement et du confort recherché. Par exemple, si vous n'êtes pas encore familiarisé avec les clusters vSphere DRS, l'option **Partially Automated** vous permet de conserver un certain contrôle sur le placement des machines virtuelles. Une fois que vous aurez bien maîtrisé le comportement et le fonctionnement de vSphere DRS, vous pourrez définir le niveau d'automatisation sur **Fully Automated**. Définissez le niveau d'automatisation sur **Manual** pour les machines virtuelles sur lesquelles vous souhaitez exercer un contrôle plus étendu, comme vos machines virtuelles stratégiques.

10-16 Ajout d'un hôte à un cluster

Lorsque vous ajoutez ou transférez un hôte dans un cluster vSphere DRS, vous pouvez conserver la hiérarchie des pools de ressources de l'hôte existant.

Si vSphere DRS n'est pas activé, les pools de ressources de l'hôte sont perdus.

Exemple : Ajout de l'hôte sc-quail04 au cluster Lab Cluster.



Pour ajouter un hôte à un cluster vSphere DRS, faites glisser un hôte VMware ESXi vers un objet cluster de l'inventaire. Utilisez l'assistant « Add Host » pour mener à bien le processus.

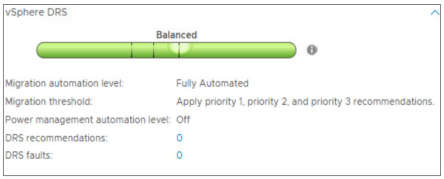
Lorsque vous ajoutez un hôte doté de pools de ressources à un cluster vSphere DRS, il vous faut décider du placement de ces pools de ressources. Par défaut, la hiérarchie des pools de ressources est supprimée et l'hôte est ajouté au même niveau que les machines virtuelles. Vous avez toutefois la possibilité de conserver la hiérarchie de pools de ressources de l'hôte existant en activant vSphere DRS. Vous pouvez également choisir de greffer les pools de ressources de l'hôte sur la hiérarchie de pools de ressources du cluster. Le greffage consiste à ajouter les branches de l'arborescence de l'hôte à l'arborescence du cluster, à l'instar de branches d'arbre fruitier transplantées sur un porte-greffe.

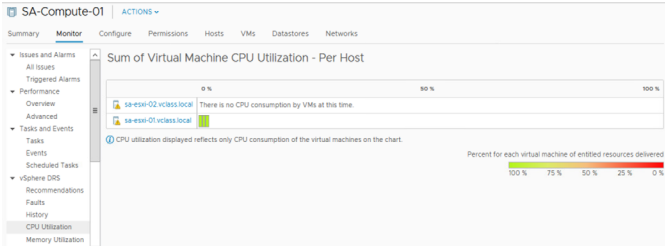
vSphere Web Client ne vous permet pas d'enregistrer le pool de ressources sous le nom « Grafted from *nom_hôte* ». Vous devez obligatoirement entrer un autre nom pour ce pool de ressources.

10-17 Affichage des informations relatives au cluster vSphere DRS

L'onglet **Summary** du cluster fournit également des informations se rapportant spécifiquement à vSphere DRS.

La page « vSphere DRS » accessible depuis l'onglet **Monitor** permet d'afficher des données sur l'utilisation des ressources CPU, mémoire et réseau pour un hôte donné.





Le volet « vSphere DRS » de l'onglet **Summary** du cluster n'apparaît que lorsque vSphere DRS est activé. Cette section fournit les informations suivantes sur vSphere DRS :

- Niveaux d'automatisation sélectionnés
- Nombre de recommandations et d'erreurs émises par vSphere DRS
- Seuil de migration configuré

Chaque recommandation de migration reçoit un niveau de priorité déterminé en fonction de la mesure de déséquilibre du cluster. Cette mesure correspond à la valeur « Current host load standard deviation » affichée sous l'onglet **Summary** du cluster dans vSphere Web Client. Plus le déséquilibre de charge sera élevé, plus la recommandation de migration sera prioritaire.

Sous l'onglet **Monitor**, cliquez sur la page « vSphere DRS ». Cliquez sur le lien **CPU Utilization**, **Network Utilization** ou **Memory Utilization** pour afficher un diagramme présentant tous les hôtes du cluster et montrant comment leurs ressources CPU et mémoire sont allouées aux différentes machines virtuelles.

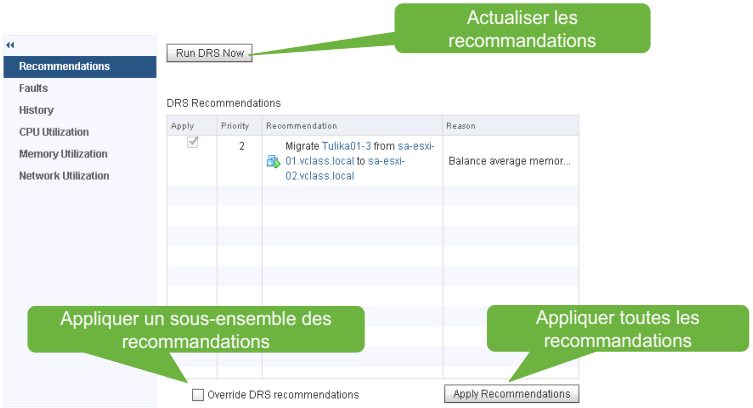
Pour l'utilisation des ressources CPU, les informations associées à la machine virtuelle sont représentées par une zone de couleur. Le fait de pointer cette zone colorée fait apparaître les données d'utilisation des ressources CPU par la machine virtuelle. Si la machine virtuelle reçoit bien les ressources auxquelles elle a droit, cette zone s'affiche en vert. La couleur verte signifie que la machine virtuelle dispose de 100 % des ressources auxquelles elle a droit. Si cette zone présente de manière prolongée une couleur autre que le vert (par exemple, le taux de ressources fournies inférieur à 80 %), il est préférable de rechercher les causes de cette anomalie (par exemple, recommandations non appliquées).

En ce qui concerne l’utilisation de la mémoire, les zones correspondant aux machines virtuelles ne sont pas affichées en couleur, car il est souvent difficile de catégoriser le rapport entre mémoire consommée et mémoire allouée.

Pour l’utilisation des ressources réseau, les données affichées correspondent à l’ensemble du trafic empruntant les interfaces réseau physiques de l’hôte.

10-18 Affichage des recommandations relatives à vSphere DRS

L'onglet **vSphere DRS** affiche des informations sur les recommandations émises par vSphere DRS pour le cluster, les erreurs qui se sont produites lors de l'application de ces recommandations et l'historique des actions vSphere DRS.



Après avoir sélectionné l'objet cluster, cliquez sur l'onglet **Monitor**, puis sur l'onglet **vSphere DRS**. Les trois premières vues sont les suivantes : « Recommendations », « Faults » et « History ».

La vue « Recommendations » présente l'ensemble actuel de recommandations générées en vue d'optimiser l'utilisation des ressources du cluster via des migrations ou la gestion de l'alimentation. Seules les recommandations manuelles qui attendent une confirmation de l'utilisateur apparaissent dans cette liste :

Pour actualiser les recommandations, cliquez sur **Run DRS Now**.

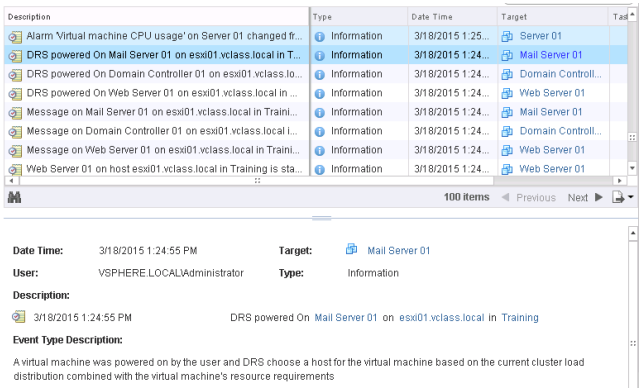
Pour appliquer toutes les recommandations, cliquez sur **Apply Recommendations**.

Pour n'appliquer qu'une partie des recommandations, activez la case à cocher **Override DRS recommendations**. Cochez la case située en regard de chaque recommandation souhaitée, puis cliquez sur **Apply Recommendations**.

10-19 Surveillance de l’état du cluster

Sélectionnez l’objet cluster dans l’inventaire afin d’afficher l’état du cluster ainsi que tous ses hôtes et machines virtuelles.

Consultez les onglets **Tasks** et **Events** du cluster pour en savoir plus.



vSphere Web Client indique si un cluster vSphere DRS est valide, surchargé (triangle jaune) ou non valide (losange rouge). La surcharge ou la non-validité d’un cluster vSphere DRS peuvent résulter de différentes causes :

- Un cluster peut se trouver surchargé par suite d’une panne d’hôte.
- Un cluster passe à l’état non valide lorsque vous mettez des machines virtuelles sous tension à l’aide de VMware Host Client alors que vCenter Server n’est pas disponible.
- Un cluster passe également à l’état non valide lorsqu’un utilisateur réduit la réservation associée à un pool de ressources parent alors qu’une machine virtuelle est en cours de basculement.
- Si des modifications sont apportées à des hôtes ou à des machines virtuelles via vSphere Web Client alors que vCenter Server n’est pas disponible, ces changements sont pris en compte. Une fois la disponibilité de vCenter Server rétablie, certains clusters peuvent alors s’afficher en rouge ou en jaune dans la mesure où leurs contraintes ne sont plus satisfaites.

Pour en savoir plus sur les états de cluster, consultez le document *Guide de gestion des ressources de vSphere*, disponible à l’adresse http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs.

10-20 Mode maintenance et mode veille

Avant toute intervention sur un hôte d'un cluster (par exemple, installation de mémoire supplémentaire ou suppression d'un hôte), vous devez basculer cet hôte en mode maintenance :

- Les machines virtuelles exécutées sur cet hôte doivent être migrées vers un autre hôte ou être éteintes.
- Vous ne pouvez pas mettre sous tension ni faire migrer des machines virtuelles sur un hôte passant en mode maintenance.
- En mode maintenance, l'hôte ne vous permet pas de déployer ou de mettre une machine virtuelle sous tension.
  - Lorsque DRS fonctionne en mode automatisé, la VM sous tension est automatiquement migrée d'un hôte passant en mode maintenance.

Le basculement d'un hôte en mode veille entraîne sa mise hors tension.

Le mode veille est utilisé par VMware vSphere® Distributed Power Management™ à des fins d'optimisation de la consommation d'énergie.

Vous basculez un hôte en mode maintenance lorsque vous avez besoin d'intervenir sur celui-ci (par exemple, pour installer de la mémoire supplémentaire). Un hôte ne peut adopter ou quitter le mode maintenance que par suite d'une demande utilisateur.

Les machines virtuelles qui sont exécutées sur un hôte passant en mode maintenance doivent être éteintes ou migrées vers un autre hôte, en mode manuel ou de façon automatique, via vSphere DRS. L'hôte poursuit l'exécution de la tâche « Enter Maintenance Mode » jusqu'à ce que toutes les machines virtuelles en cours d'exécution soient mises hors tension ou transférées. Vous ne pouvez pas mettre sous tension ni faire migrer des machines virtuelles sur un hôte passant en mode maintenance.

Lorsque l'hôte ne comporte plus aucune machine virtuelle en cours d'exécution, son icône indique qu'il est passé en mode maintenance. L'onglet **Summary** de cet hôte indique également son nouvel état. Un hôte se trouvant en mode maintenance ne permet pas le déploiement ni la mise sous tension d'une machine virtuelle.

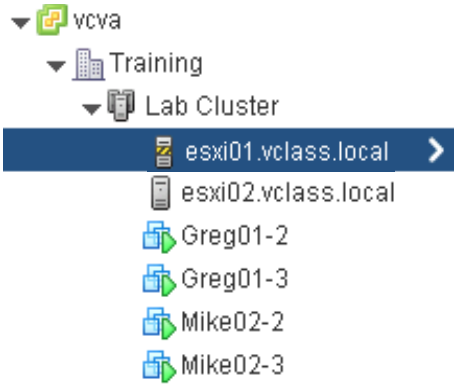
Le basculement d'une machine hôte en mode veille entraîne sa mise hors tension.

En règle générale, le basculement des machines hôtes en mode veille est assuré par vSphere DPM à des fins d'optimisation de la consommation d'énergie. Le basculement d'un hôte en mode veille entraîne sa mise hors tension. Vous avez également la possibilité de déclencher manuellement le passage d'un hôte en mode veille. Lors de sa prochaine exécution, vSphere DRS est toutefois susceptible d'annuler ou de vous recommander d'annuler votre modification. Si vous souhaitez qu'un hôte reste hors tension, placez-le en mode maintenance avant de le mettre hors tension.

10-21 Suppression d'un hôte du cluster vSphere DRS

Avant de supprimer un hôte d'un cluster vSphere DRS, prenez en compte les éléments suivants :

- La hiérarchie de pools de ressources reste associée au cluster.
- Dans la mesure où l'hôte doit être basculé en mode maintenance, toutes les machines virtuelles déployées sur celui-ci sont mises hors tension.
- Les ressources disponibles pour le cluster sont réduites.



Pour supprimer un hôte d'un cluster, cliquez avec le bouton droit de la souris sur cet hôte dans l'inventaire, puis sélectionnez **Enter Maintenance Mode**. Une fois l'hôte basculé en mode maintenance, faites-le glisser vers un autre emplacement de l'inventaire, tel que le Data Center ou un autre cluster.

Avant de supprimer un hôte d'un cluster vSphere DRS, prenez en compte les éléments suivants :

- Lorsque vous supprimez un hôte d'un cluster, il conserve uniquement le pool de ressources root, même si vous avez utilisé un cluster vSphere DRS et greffé le pool de ressources hôte lors de l'ajout de l'hôte au cluster. La hiérarchie reste associée au cluster. Vous avez la possibilité de créer une hiérarchie de pool de ressources spécifique pour l'hôte.
- Lorsqu'un hôte est placé en mode maintenance, toutes ses machines virtuelles en cours d'exécution doivent être éteintes ou suspendues, ou encore migrées vers d'autres hôtes à l'aide de vSphere vMotion. Les machines virtuelles dont les disques utilisent le stockage local doivent être mises hors tension, interrompues ou migrées vers un autre hôte et une autre banque de données via une migration vSphere vMotion « Shared-Nothing ». Lorsque vous supprimez l'hôte du cluster, les machines virtuelles qui lui sont encore associées sont également retirées du cluster.

- La suppression d’un hôte du cluster a pour effet de réduire les ressources disponibles pour ce dernier. Si le cluster dispose encore de ressources suffisantes pour couvrir les réservations de l’ensemble de ses machines virtuelles et pools de ressources, il ajuste l’allocation des ressources pour tenir compte de cette réduction. Si le cluster n’a plus assez de ressources pour couvrir les réservations de tous ses pools de ressources, mais qu’il lui en reste suffisamment pour les réservations de l’ensemble de ses machines virtuelles, une alarme est émise et vSphere DRS continue à fonctionner.

10-22 Désactivation de vSphere DRS et restauration d'une arborescence de pools de ressources

Vous avez la possibilité de désactiver vSphere DRS pour un cluster déterminé.

En ce cas, les pools de ressources sont supprimés du cluster.

La hiérarchie et les règles d'affinité des pools de ressources du cluster qui sont supprimées lors de désactivation de vSphere DRS ne sont pas rétablies lorsque vSphere DRS est réactivé.

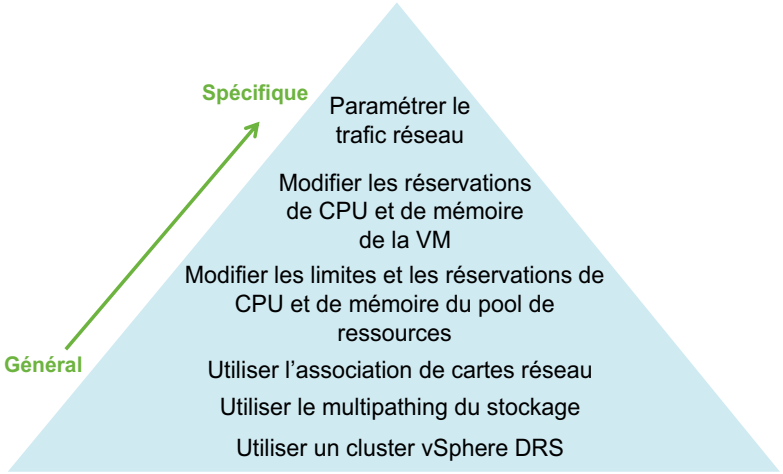
Pour éviter de perdre ces pools de ressources, enregistrez un snapshot de leur arborescence sur votre machine locale.

En réactivant vSphere DRS, vous aurez ainsi la possibilité de restaurer le snapshot préalablement enregistré contenant cette arborescence de pools de ressources.

Vous avez la possibilité de restaurer le pool de ressources à partir d'un snapshot lors de l'activation de vSphere DRS. Trois conditions doivent être réunies pour la restauration de l'arborescence d'un pool de ressources :

- vSphere DRS doit être activé.
- Un snapshot ne peut être restauré que sur le cluster où il a été pris.
- Aucun autre pool de ressources ne doit se trouver dans le cluster.

10-23 Méthodes d'amélioration des performances des machines virtuelles



Prenez connaissance des différentes méthodes à votre disposition pour améliorer les performances d'une machine virtuelle. Ces méthodes sont recensées de la plus spécifique à la plus générale. Les méthodes spécifiques portent sur une machine virtuelle donnée. Les méthodes générales s'appliquent à plusieurs entités. Vous disposez de plusieurs méthodes pour améliorer les performances d'une machine virtuelle :

- Si une machine virtuelle est limitée en ressources réseau, recourez au paramétrage du trafic réseau afin de lui attribuer plus de bande passante durant les heures de pointe.
- Si une machine virtuelle est limitée en ressources mémoire, ajoutez-lui des parts de mémoire ou augmentez sa réservation de mémoire.
- Si une machine virtuelle est limitée en ressources CPU, ajoutez-lui des parts de CPU ou augmentez sa réservation de CPU.
- Si une machine virtuelle est limitée en ressources CPU ou mémoire, augmentez les limites ou les réservations du pool de ressources auquel elle appartient.
- Si la charge réseau est déséquilibrée, vous pouvez recourir à l'association de cartes réseau pour répartir celle-ci entre plusieurs adaptateurs réseau physiques.
- Si la charge d'E/S disque est déséquilibrée, le multipathing du stockage vous permet d'équilibrer celle-ci entre les différents chemins d'accès à une banque de données.

- Si la charge des machines virtuelles est déséquilibrée, vous pouvez regrouper plusieurs hôtes dans un cluster vSphere DRS afin d'équilibrer la charge des machines virtuelles entre tous les hôtes de ce cluster.

10-24 Utilisation de VMware vSphere HA avec vSphere DRS

Plusieurs facteurs peuvent empêcher vSphere HA de basculer des machines virtuelles :

- Le contrôle d'admission vSphere HA est désactivé, et les ressources disponibles sur les hôtes restants ne sont pas suffisantes pour mettre toutes les VM défaillantes sous tension.
- Des règles d'affinité VM/hôte obligatoires interdisent à vSphere HA d'effectuer le basculement.
- Les ressources disponibles sont globalement suffisantes, mais elles sont fragmentées entre plusieurs hôtes. Dans ces différents cas, vSphere HA fait appel à vSphere DRS pour tenter d'aménager le cluster en migrant des machines virtuelles de façon à défragmenter les ressources.

Lorsque vSphere HA effectue les basculements et redémarre les machines virtuelles sur différents hôtes, sa priorité est d'assurer la disponibilité de l'ensemble des machines virtuelles. Après un redémarrage des machines virtuelles, les hôtes sur lesquels celles-ci ont été mises sous tension sont généralement très chargés, tandis que d'autres présentent une charge de travail relativement légère.

vSphere HA est étroitement intégré avec vSphere DRS. Lorsqu'un basculement se produit, vSphere HA commence par vérifier que l'hôte considéré présente les ressources nécessaires à une telle opération. Si les ressources requises ne sont pas disponibles, vSphere HA demande à vSphere DRS de lui procurer si possible ces ressources manquantes. L'utilisation inefficace de ressources peut engendrer une fragmentation des ressources sur l'ensemble du cluster. vSphere HA demande (sans pouvoir la garantir) une défragmentation des ressources visant à satisfaire les besoins en ressources de cette machine virtuelle.

De plus, vSphere DRS égalise les nombres de parts et les limites associées aux machines virtuelles avant de basculer celles-ci. Ce processus d'aplatissement garantit que les machines virtuelles obtiendront les ressources auxquelles elles auraient eu droit si elles avaient été basculées sur le pool de ressources approprié.

10-25 Laboratoire 17 : Mise en œuvre des clusters vSphere DRS

Mettre en œuvre un cluster vSphere DRS

1. Créer un déséquilibre de charge
2. Créer un cluster vSphere DRS
3. Vérifier le bon fonctionnement du cluster vSphere DRS
4. Créer, tester et désactiver une règle d'affinité entre VM
5. Créer, tester et désactiver une règle d'anti-affinité
6. Créer, tester et désactiver une règle d'affinité VM/hôte

10-26 Rappel des objectifs de la formation

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

- Décrire les fonctions d'un cluster vSphere DRS
- Créer un cluster vSphere DRS
- Examiner les informations relatives à un cluster vSphere DRS
- Supprimer un hôte d'un cluster vSphere DRS

10-27 Points clés

- Les clusters vSphere DRS permettent la gestion automatisée des ressources pour plusieurs hôtes VMware ESXi.
- vSphere DRS fonctionne de manière optimale lorsque les machines virtuelles répondent aux exigences de la migration via vSphere vMotion.

Des questions ?

MODULE 11

vSphere Update Manager

11-2 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

11-3 Importance

Au fil du temps, la configuration matérielle et logicielle de votre environnement vSphere peut subir des modifications, notamment sous la forme de mises à jour ou de correctifs logiciels.

vSphere Update Manager met en œuvre ces modifications de manière ordonnée, contrôlée et systématique, pour une gérabilité et une évolutivité optimales de votre environnement vSphere.

11-4 Objectifs de la formation

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

- Décrire les fonctionnalités de VMware vSphere Update Manager
- Utiliser vSphere Update Manager pour créer et associer une référence

11-5 À propos de vSphere Update Manager

vSphere Update Manager permet de centraliser et d'automatiser la gestion des correctifs et des versions pour les hôtes VMware ESXi, le matériel de machine virtuelle, VMware Tools et les appliances virtuelles :

- vSphere Update Manager permet de réduire les risques de sécurité :
  - Réduction du nombre de vulnérabilités
  - Élimination des nombreuses failles de sécurité exploitant d'anciennes vulnérabilités
- vSphere Update Manager limite la disparité des systèmes déployés dans un environnement :
  - Simplification de la gestion
  - Réduction des risques de sécurité
- vSphere Update Manager assure un fonctionnement plus fluide des hôtes :
  - Application de correctifs visant notamment les bogues
  - Dépannage simplifié

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

vSphere Update Manager permet de centraliser et d'automatiser la gestion des correctifs et des versions pour vSphere, et prend en charge les hôtes VMware ESXi, le matériel des machines virtuelles, les outils VMware Tools et les appliances virtuelles. Les mises à jour que vous indiquez peuvent être appliquées aux hôtes VMware ESXi, au matériel des machines virtuelles et aux appliances virtuelles que vous analysez. vSphere Update Manager vous permet d'effectuer les tâches suivantes :

- Analyser la conformité du matériel des machines virtuelles, des appliances et des hôtes, et appliquer les mises à jour requises
- Mettre directement à niveau les hôtes, le matériel des machines virtuelles, les outils VMware Tools et les appliances virtuelles
- Appliquer des logiciels tiers aux hôtes

En vous assurant que les versions des correctifs sont à jour pour le matériel des machines virtuelles comme pour les hôtes VMware ESXi, vous limitez le nombre de vulnérabilités dans un environnement, ainsi que l'éventail des problèmes à résoudre. Tous les systèmes requièrent un effort permanent d'application des correctifs, de reconfiguration ou d'application d'autres solutions. La réduction de la disparité et le maintien de la conformité des systèmes d'un environnement relèvent par conséquent des meilleures pratiques de sécurité. Enfin, dans la mesure où une partie des correctifs ont une fonction de débogage, vSphere Update Manager contribue au bon fonctionnement des environnements en évitant les interruptions de service et les erreurs.

vCenter Server Appliance propose vSphere Update Manager en tant que service facultatif. vSphere Update Manager est inclus dans l'offre vCenter Server Appliance.

VMware gère son infrastructure en utilisant un outil automatisé appelé vSphere Update Manager. Il est possible d'utiliser vSphere Update Manager pour automatiser l'application des correctifs VMware aux hôtes et des mises à jour client à VMware Tools. Pour appliquer des correctifs, vSphere Update Manager utilise une référence créée par l'utilisateur et l'applique à l'élément d'infrastructure sélectionné. Ces mises à jour de référence peuvent être appliquées à un seul et unique objet, mais aussi à un grand nombre d'objets simultanément.

11-6 Fonctionnalités de vSphere Update Manager

vSphere Update Manager offre les fonctionnalités suivantes :

- Téléchargement automatisé des correctifs :
  - Le téléchargement automatisé des correctifs commence par le téléchargement des informations seules.
  - Il est planifié selon des intervalles configurables.
- Création de références et de groupes de références.
- Possibilité d'associer des références ou des groupes de références à des objets d'inventaire.
- Analyse : les systèmes de l'inventaire bénéficient d'une analyse de conformité par rapport aux références.
- Mise en conformité : les systèmes de l'inventaire qui ne sont pas conformes peuvent recevoir automatiquement les correctifs requis.

vSphere Update Manager assure un ensemble d'opérations garantissant une gestion efficace des correctifs et des mises à niveau.

Ce processus commence par le téléchargement d'informations relatives à un ensemble de correctifs de sécurité. Ces correctifs sont regroupés sous la forme de références contenant chacune un ou plusieurs correctifs. Plusieurs références peuvent être combinées en un groupe de références. Un tel groupe vous permet d'associer des références de toutes sortes, puis de lancer l'analyse et la mise en conformité d'un objet d'inventaire par rapport à l'ensemble de ces références. Lorsqu'un groupe combine des références de mise à niveau et de correctifs, la mise à niveau est exécutée en premier.

Vous pouvez analyser un ensemble d'appliances virtuelles et d'hôtes VMware ESXi, afin de vérifier leur conformité avec une référence ou un groupe de références et d'effectuer les mises à jour ou mises à niveau requises, le cas échéant. Ces processus peuvent être démarrés manuellement ou via des tâches planifiées.

11-7 Composants de vSphere Update Manager

vSphere Update Manager requiert une connectivité réseau avec vCenter Server et comprend plusieurs composants :

- Le composant serveur de vSphere Update Manager peut être installé sur le même ordinateur que vCenter Server sous Windows ou sur une autre machine. vSphere Update Manager est intégré dans l'offre vCenter Server Appliance et proposé en tant que service facultatif.
- Le composant client : la fonctionnalité vSphere Update Manager apparaît sous l'onglet **Update Manager** lorsqu'un hôte VMware ESXi est sélectionné dans vSphere Web Client.
- Base de données :
  - Le serveur et le service de téléchargement vSphere Update Manager que vous installez sous Windows requièrent une base de données pour le stockage et l'organisation des données serveur.
  - Une base de données Oracle ou Microsoft SQL Server est requise (uniquement pour vSphere Update Manager sous Windows).

11-8 Configuration de vSphere Update Manager

Vous ne pouvez modifier la configuration de vSphere Update Manager que si vous détenez les privilèges adéquats.

Pour accéder aux paramètres d'administration, cliquez sur l'icône **Update Manager**, sur la page d'accueil de vSphere Web Client :

- Connectivité réseau : modifiez l'adresse IP ou le nom d'hôte du magasin de correctifs.
- Paramètres de téléchargement : modifiez l'emplacement de téléchargement pour les nouveaux correctifs et les nouvelles mises à niveau des appliances virtuelles.
- Calendrier de téléchargement : modifiez la planification par défaut pour la recherche de mises à niveau si votre environnement requiert des vérifications plus fréquentes ou moins fréquentes.
- Calendrier de recherche de notifications : configurez le moment et la fréquence auxquels vSphere Update Manager recherche les rappels ou les corrections de correctifs.
- Paramètres relatifs aux machines virtuelles : spécifiez si vSphere Update Manager doit prendre un snapshot de la machine virtuelle avant l'application des mises à jour.
- Paramètres relatifs aux hôtes et aux clusters : activez le démarrage rapide, configurez l'état de fonctionnement des VM, et désactivez temporairement vSphere HA, vSphere Fault Tolerance et vSphere DPM.

Vous ne pourrez modifier les paramètres de vSphere Update Manager que si vous disposez des privilèges nécessaires pour configurer les paramètres et le service vSphere Update Manager. Ces autorisations doivent être affectées sur le système vCenter Server auprès duquel vSphere Update Manager est enregistré.

Connectez VMware vSphere® Update Manager Client™ au système vCenter Server auprès duquel vSphere Update Manager est enregistré. Sur la page d'accueil de vSphere Web Client, cliquez sur l'icône **Update Manager** afin d'accéder aux paramètres d'administration :

- Connectivité réseau : les ports réseau sont configurés lors de l'installation. Les paramètres de connectivité réseau de vSphere Update Manager vous permettent de modifier l'adresse IP ou le nom d'hôte du magasin de correctifs.
- Source de téléchargement : si le système de déploiement est connecté à Internet, vous pouvez télécharger directement les extensions et correctifs VMware ESXi, ainsi que les mises à niveau relatives aux appliances virtuelles.
- Paramètres de proxy : vous pouvez configurer vSphere Update Manager pour le téléchargement de mises à jour depuis Internet via un serveur proxy.
- Recherche de mises à jour (calendrier de téléchargement) : vSphere Update Manager vérifie régulièrement les mises à niveau des appliances virtuelles, les correctifs d'hôtes et les extensions. En règle générale, les paramètres de planification par défaut sont suffisants. Cependant, vous pouvez modifier la planification si votre environnement requiert des vérifications plus ou moins fréquentes.

- Calendrier de recherche de notifications : par défaut, vSphere Update Manager recherche à intervalles prédéfinis les notifications concernant les rappels de correctifs, les corrections de correctifs et les alertes. Vous pouvez modifier cette planification. Par défaut, la tâche de recherche des notifications et d'envoi des alertes de notification est activée et s'appelle « VMware vSphere Update Manager Check Notification ». En modifiant cette tâche, vous pouvez configurer le moment et la fréquence auxquels vSphere Update Manager recherche les rappels ou les corrections de correctifs et envoie des notifications à l'adresse e-mail que vous spécifiez.
- Paramètres relatifs aux machines virtuelles : par défaut, vSphere Update Manager est configuré pour prendre un snapshot de la machine virtuelle avant l'application de la mise à jour. En cas d'échec de la mise en conformité, vous pouvez utiliser le snapshot pour rétablir la machine virtuelle à l'état précédant l'opération. vSphere Update Manager ne prend pas de snapshot des machines virtuelles à tolérance aux pannes ou exécutant la version 3 du matériel de machine virtuelle. Si vous décidez néanmoins de prendre des snapshots pour ces machines virtuelles, cela peut entraîner l'échec de la mise en conformité. Vous pouvez conserver ces snapshots indéfiniment ou pendant une durée déterminée.
- Paramètres relatifs aux hôtes et aux clusters : ces paramètres vous permettent de spécifier le comportement de vSphere Update Manager vis-à-vis des hôtes et des clusters.

Pour en savoir plus, consultez le document *Installation et administration de VMware vSphere Update Manager*, à l'adresse https://www.vmware.com/support/pubs/vum_pubs.html. Vous pouvez également consulter le *Guide de mise à niveau vSphere*, disponible à l'adresse http://www.vmware.com/fr/support/support-resources/pubs/vsphere-esxi-vcenter-server-6-pubs

11-9 Références et groupes de références

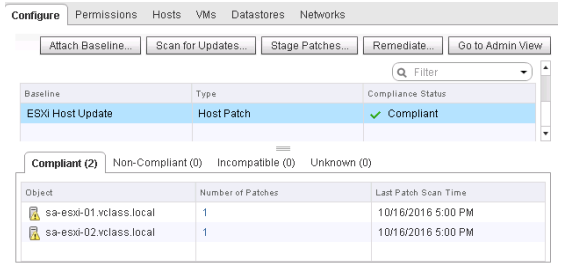
Une référence contient un ou plusieurs correctifs, extensions ou mises à niveau.

vSphere Update Manager réunit les références par défaut suivantes :

- Référence de correctif dynamique critique des hôtes
- Référence de correctif dynamique non critique des hôtes
- Référence de mise à niveau de VMware Tools
- Référence de mise à niveau du matériel VMware
- Référence de mise à niveau des appliances virtuelles

Un groupe de références rassemble plusieurs références.

Un groupe de références peut contenir une référence de mise à niveau ainsi qu'une ou plusieurs références de correctif ou d'extension.



Une référence peut être constituée de mises à niveau, d'extensions ou de correctifs. Chaque référence représente ainsi un assemblage d'un ou plusieurs correctifs, extensions ou mises à niveau.

Vous avez la possibilité d'assembler des références existantes en groupes de références, dont chacun pourra contenir une référence de mise à niveau et une ou plusieurs références de correctif et d'extension, ou encore une combinaison de références de correctif et d'extension. L'analyse d'un groupe d'hôtes, de machines virtuelles et d'appliances virtuelles permet d'évaluer leur niveau de conformité par rapport à un ensemble de références ou de groupes de références.

Pour créer, modifier ou supprimer des références ou des groupes de références, vous devez disposer du privilège « Manage Baseline ». Pour joindre des références ou des groupes de références, vous devez disposer du privilège « Attach Baseline ». Ces privilèges doivent être affectés sur le système vCenter Server auprès duquel vSphere Update Manager est enregistré.

vSphere Update Manager inclut les références de correctif dynamiques et les références de mise à niveau par défaut suivantes :

- Critical Host Patches (Predefined) : vérifie la conformité des hôtes VMware ESXi avec l'ensemble des correctifs critiques.
- Non-Critical Host Patches (Predefined) : vérifie la conformité des hôtes VMware ESXi avec l'ensemble des correctifs facultatifs.
- VMware Tools Upgrade to Match Host (Predefined) : vérifie la conformité des machines virtuelles par rapport à la dernière version de VMware Tools déployée sur l'hôte. vSphere Update Manager prend en charge la mise à niveau de VMware Tools pour les machines virtuelles placées sur les hôtes exécutant VMware ESXi version 5.0 ou ultérieure.

- VM Hardware Upgrade to Match Host (Predefined) : vérifie que le matériel virtuel d'une machine virtuelle est conforme à la toute dernière version prise en charge par l'hôte. VMware vSphere Update Manager prend en charge la mise à niveau vers la version vmx-11 du matériel virtuel sur les hôtes exécutant VMware ESXi 6.x.
- VA Upgrade to Latest (Predefined) : vérifie la conformité des appliances virtuelles par rapport à la dernière version publiée de l'appliance virtuelle.

11-10 Création et modification de références d'extension ou de correctif

L'assistant « New Baseline » vous permet de créer des références de correctif, d'extension et de mise à niveau personnalisées en fonction des besoins spécifiques de votre déploiement :

- Créez une référence de correctif fixe :
  - Une référence fixe correspond à un ensemble de correctifs qui ne seront pas actualisés en fonction de la disponibilité de correctifs.
- Créez une référence de correctif dynamique :
  - Une référence dynamique se compose d'un ensemble de correctifs répondant à certains critères.
- Créez une référence d'extension hôte :
  - Les références d'extension contiennent des logiciels supplémentaires pour les hôtes VMware ESXi. Ces logiciels supplémentaires peuvent être des logiciels VMware ou tiers.
- Filtrez les correctifs ou les extensions dans l'assistant « New Baseline » :
  - Lors de la création d'une référence de correctif ou d'extension, vous avez la possibilité de filtrer les correctifs et les extensions disponibles dans le référentiel vSphere Update Manager, afin de localiser ceux que vous souhaitez inclure dans la référence ou exclure de cette dernière.

La création et la gestion des références s'effectuent sous l'onglet **Update Manager**. Vous pouvez mettre les hôtes en conformité avec des références contenant des correctifs ou des extensions. Selon les critères que vous sélectionnez, les références de correctif peuvent être de type dynamique ou fixe.

Le contenu des références de correctif dynamiques est automatiquement mis à jour en fonction de la disponibilité de correctifs répondant aux critères que vous spécifiez. Les références fixes contiennent uniquement les correctifs que vous sélectionnez, indépendamment des téléchargements de nouveaux correctifs.

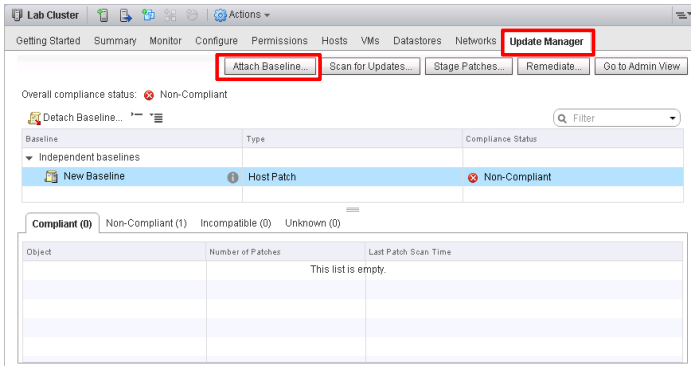
Les références d'extension contiennent des modules logiciels supplémentaires pour les hôtes VMware ESXi. Ce logiciel supplémentaire peut être un logiciel VMware ou tiers. Vous pouvez ainsi recourir à des références d'extension pour installer des modules supplémentaires, puis à des références de correctif pour les mettre à jour.

Si votre système vCenter Server appartient à un groupe connecté en mode vCenter Linked Mode et qu'il existe plusieurs instances de vSphere Update Manager, les références que vous créez ne s'appliquent pas aux objets d'inventaire gérés par les autres systèmes vCenter Server du groupe. Les références sont propres à l'instance vSphere Update Manager que vous sélectionnez.

11-11 Association de références

Pour accéder aux informations de conformité et analyser les objets de l'inventaire par rapport à un ensemble de références ou de groupes de références, vous devez tout d'abord associer les références ou groupes de références souhaités à ces objets.

Vous pouvez effectuer cette opération depuis l'onglet **Update Manager** de vSphere Web Client :



Pour afficher des informations sur la conformité et vérifier celle de certains objets de l'inventaire par rapport à des références ou des groupes de références spécifiques, vous devez d'abord relier ces références ou ces groupes de références aux objets concernés.

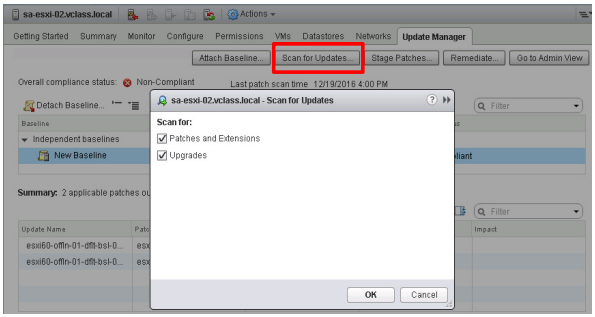
Avant de pouvoir utiliser des références et des groupes de références, vous devez les associer à des objets sélectionnés dans l'inventaire, tels que des machines virtuelles, des appliances virtuelles, des hôtes ou des objets conteneurs.

Bien qu'il soit possible de joindre des références ou des groupes de références à des objets individuels, il existe une méthode plus efficace : l'association à des objets conteneurs (dossiers, vApps, clusters et Data Centers). Les objets vSphere individuels héritent des références associées à l'objet conteneur parent. Si vous supprimez un objet d'un conteneur, vous supprimez également les références héritées de cet objet.

Si le système vCenter Server est connecté à d'autres systèmes vCenter Server via un domaine vCenter Single Sign-On commun, vous pouvez associer des références et des groupes de référence aux objets gérés par le système vCenter Server auprès duquel le logiciel vSphere Update Manager est enregistré. Les références et groupes de références que vous joignez sont spécifiques de l'instance vSphere Update Manager enregistrée auprès du système vCenter Server.

11-12 Analyse de mises à jour

L'analyse consiste à évaluer des objets d'inventaire par rapport à une référence ou à un groupe de références.



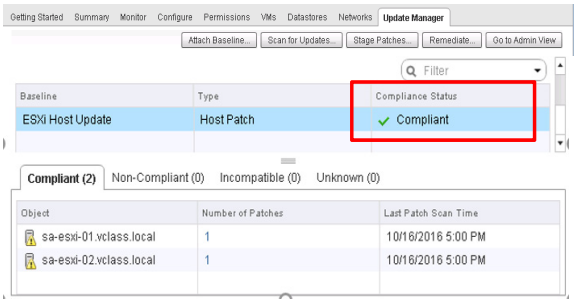
L'analyse consiste à évaluer les attributs d'un ensemble d'hôtes, de machines virtuelles ou d'appliances virtuelles par rapport aux correctifs, extensions et mises à niveau spécifiés dans la référence ou le groupe de références associés. Vous pouvez configurer vSphere Update Manager pour l'analyse de machines virtuelles, d'appliances virtuelles et d'hôtes VMware ESXi par rapport à des références ou à des groupes de références en planifiant ou en démarrant manuellement des analyses afin de générer des informations sur la conformité.

Si vous sélectionnez un objet conteneur, tous ses objets enfants sont également analysés. La durée d'une analyse dépend de la taille de l'infrastructure virtuelle et du niveau de la hiérarchie d'objets à partir duquel vous lancez cette analyse.

Une fois qu'un objet d'inventaire est associé à une référence, vous pouvez lancer une analyse en sélectionnant cet objet, puis en sélectionnant **Scan for updates**.

11-13 Vérification de la conformité des objets vSphere

Vous pouvez examiner les informations relatives à la conformité des machines virtuelles, des appliances virtuelles et des hôtes par rapport aux références ou aux groupes de références que vous leur avez associés.



Le fait de sélectionner un objet conteneur vous permet de consulter le statut de conformité global des références associées, ainsi que le statut de conformité de chacune d'entre elles. En sélectionnant l'une des références associées à cet objet conteneur, vous accédez au statut de conformité de cette seule référence.

En sélectionnant une machine virtuelle, une appliance ou un hôte donnés, vous obtenez son statut de conformité global par rapport à l'ensemble des références, ainsi que le nombre de mises à jour. Si vous poursuivez en sélectionnant l'une des références associées à cet objet, vous obtenez le nombre de mises à jour regroupées par statut de conformité pour cette référence.

L'état conforme indique qu'un objet vSphere est conforme à toutes les références rassemblées dans le groupe de références associé, ou à l'ensemble des correctifs, extensions et mises à jour spécifiés dans la référence associée. Un état conforme ne nécessite aucune autre action. Lorsqu'une référence contient des correctifs ou des mises à niveau non pertinents pour l'objet cible, ces mises à niveau individuelles, ainsi que les références ou les groupes de références qui les contiennent, sont traités comme étant non applicables et considérés comme conformes.

Un état non conforme indique qu'une ou plusieurs références d'un groupe, ou un ou plusieurs correctifs, extensions ou mises à niveau d'une référence, sont applicables à l'objet cible, mais sont manquants (non installés) sur celui-ci. Vous devez en ce cas mettre l'objet cible en conformité.

11-14 Mise en conformité des objets

Vous pouvez mettre en conformité des machines virtuelles, des modèles, des appliances virtuelles et des hôtes :

- La mise en conformité peut être effectuée immédiatement ou planifiée à une date ultérieure.
- Le mode d'exécution de la mise en conformité d'un hôte varie en fonction des types de références associées et de l'appartenance ou non de l'hôte à un cluster.
- Pour les hôtes VMware ESXi d'un cluster, le processus de mise en conformité est par défaut séquentiel.
- La mise en conformité des hôtes d'un cluster requiert la désactivation temporaire des fonctionnalités de cluster, telles que vSphere DPM et le contrôle d'admission vSphere HA.

Vous pouvez corriger la non-conformité des machines virtuelles, des appliances virtuelles et des hôtes en lançant manuellement une mise en conformité ou en la planifiant au moment qui vous convient.

Vous pouvez mettre en conformité les machines et les appliances virtuelles de façon simultanée.

Si le système vCenter Server est connecté à d'autres systèmes vCenter Server via un domaine vCenter Single Sign-On commun, vous ne pouvez mettre en conformité que les objets d'inventaire gérés par le système vCenter Server auprès duquel vSphere Update Manager est enregistré.

Le mode d'exécution de la mise en conformité d'un hôte varie en fonction des types de référence associés et selon que l'hôte appartient ou non à un cluster.

Pour les hôtes VMware ESXi d'un cluster, le processus de mise en conformité est par défaut séquentiel. Avec vSphere Update Manager version 6 ou ultérieure, vous pouvez opter pour l'exécution en parallèle du processus de mise en conformité des hôtes.

Lorsque vous mettez en conformité un cluster d'hôtes en mode séquentiel et que l'un des hôtes ne parvient pas à passer en mode maintenance, vSphere Update Manager signale une erreur, et le processus s'arrête et échoue. Les hôtes du cluster qui ont déjà été mis en conformité demeurent au niveau mis à jour. Ceux qui n'ont pas encore été traités au moment de la défaillance du processus de mise en conformité ne sont pas mis à jour. Si un hôte appartenant à un cluster configuré pour vSphere DRS exécute une machine virtuelle sur laquelle vSphere Update Manager ou vCenter Server sont installés, vSphere DRS commence par tenter de migrer cette machine virtuelle exécutant vCenter Server ou vSphere Update Manager vers un autre hôte pour assurer le succès de la mise en conformité. S'il est impossible de migrer la machine virtuelle vers un autre hôte, la mise

en conformité échoue pour l'hôte concerné, mais le processus n'est pas interrompu. vSphere Update Manager passe alors à la mise en conformité de l'hôte suivant du cluster.

Au sein d'un cluster, la mise en conformité des hôtes VMware ESXi via une mise au niveau n'est effectuée que lorsque l'ensemble des hôtes du cluster peuvent être mis à niveau.

La mise en conformité des hôtes d'un cluster requiert la désactivation temporaire des fonctionnalités de cluster, telles que vSphere DPM et le contrôle d'admission vSphere HA. Il convient également de désactiver vSphere Fault Tolerance s'il est exécuté sur certaines des machines virtuelles lancées sur les hôtes, ainsi que de déconnecter les périphériques amovibles connectés à ces machines virtuelles, de façon à permettre la migration de ces dernières via vSphere vMotion. Avant de lancer un processus de mise en conformité, vous pouvez générer un rapport indiquant sur quels clusters, hôtes ou machines virtuelles ces fonctionnalités de cluster sont activées.

Lorsque vous mettez en conformité un cluster d'hôtes en parallèle, vSphere Update Manager traite plusieurs hôtes à la fois.

Lors d'une mise en conformité en parallèle, s'il échoue pour un hôte donné, vSphere Update Manager l'ignore et passe aux autres hôtes du cluster, en évaluant continuellement le nombre maximal d'hôtes pouvant être mis en conformité de façon simultanée sans affecter les paramètres de vSphere DRS.

Vous pouvez spécifier le nombre maximal d'hôtes pouvant être mis en conformité de façon simultanée.

Dans le cas des hôtes d'un cluster vSAN, vSphere Update Manager applique le processus de mise en conformité de manière séquentielle, même si vous avez opté pour la mise en conformité en parallèle. En effet, de par sa conception, un cluster vSAN ne peut avoir qu'un seul hôte en mode maintenance à un moment donné.

11-15 Notification de rappel de correctif

vSphere Update Manager entre régulièrement en contact avec VMware afin de télécharger les notifications concernant les rappels de correctifs, les nouveaux correctifs et autres alertes :

- L'option **Notification Check Schedule** est sélectionnée par défaut.

En cas de réception d'une notification de rappel de correctif, vSphere Update Manager effectue les actions suivantes :

- Il génère une notification dans l'onglet « Notifications ».
- Il cesse d'appliquer le correctif concerné aux hôtes. Il signale le correctif comme étant rappelé dans la base de données.
- Il supprime les fichiers binaires du correctif de son référentiel de correctifs.

vSphere Update Manager ne désinstalle pas les correctifs rappelés des hôtes VMware ESXi. Il attend une nouvelle version du correctif, qu'il applique alors aux hôtes concernés afin de les mettre en conformité.

vSphere Update Manager entre régulièrement en contact avec VMware afin de télécharger les informations (notifications) concernant les rappels de correctifs, les nouveaux correctifs et autres alertes. Vous pouvez modifier la planification en cours en redéfinissant le paramètre **Notification Check Schedule** proposé sous l'onglet **Configuration** de vSphere Update Manager.

En cas de publication de correctifs comportant des problèmes avérés ou potentiels, ces correctifs sont rappelés dans les métadonnées et vSphere Update Manager les signale en conséquence. Si vous tentez d'installer un correctif rappelé, vSphere Update Manager vous informe du rappel de ce correctif et n'installe pas ce dernier sur l'hôte. Si vous avez déjà installé un tel correctif, vSphere Update Manager indique que le correctif rappelé est installé sur certains hôtes, supprimant également tous les correctifs rappelés de son référentiel de correctifs.

Lorsqu'un nouveau correctif est publié, vSphere Update Manager le télécharge et vous invite à l'installer afin de résoudre les problèmes que pourrait causer le correctif rappelé. Si vous tentez d'installer le correctif rappelé, vSphere Update Manager vous le signale et vous invite à installer la correction de ce correctif.

11-16 Intégration d'EAM avec vSphere Update Manager

ESX Agent Manager (EAM) permet à VMware NSX® de préparer les hôtes VMware ESXi en leur adjoignant l'extension de chemin de données et d'outils hôte NSX requise :

- vSphere Update Manager crée automatiquement une référence EAM gérée par le système pour chaque cluster VMware ESXi préalablement préparé par VMware NSX® Manager™.
- Lorsqu'une nouvelle version de l'extension de chemin de données et d'outils hôte NSX est publiée, les références EAM se mettent à jour et signalent la non-conformité du cluster VMware ESXi de manière automatique. Ces références émettent également une recommandation de mise en conformité concernant la mise à jour des extensions installées sur les hôtes ESXi.

vSphere ESX Agent Manager (EAM) automatise le processus de déploiement et de gestion des agents vSphere ESX, et permet d'étendre les fonctionnalités d'un hôte VMware ESXi de façon à fournir les services supplémentaires requis par une solution vSphere déterminée.

Les machines virtuelles d'agent ESX sont comparables aux services exploités sous Windows ou Linux. Elles démarrent avec le système d'exploitation et s'arrêtent avec celui-ci. Le comportement des machines virtuelles d'agent ESX est transparent pour l'utilisateur. Un hôte vSphere passe à l'état prêt lorsque le système d'exploitation VMware ESXi a démarré et que toutes les machines virtuelles d'agent ESX ont été provisionnées et mises sous tension.

EAM vous permet de surveiller l'état d'intégrité des agents ESX, et empêche les utilisateurs d'effectuer sur ces agents certaines opérations susceptibles d'affecter les VMs qui les utilisent. Par exemple, EAM peut empêcher la mise hors tension de la machine virtuelle d'un agent ESX ou son retrait d'un hôte VMware ESXi contenant d'autres machines virtuelles qui utilisent cet agent.

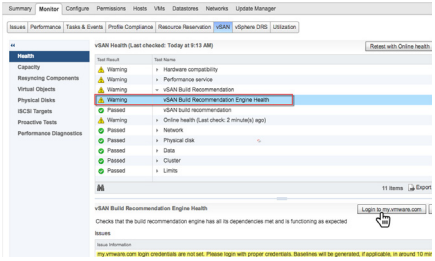
11-17 Intégration de vSAN avec vSphere Update Manager

Afin de garantir la conformité du cluster vSAN aux dernières mises à jour, vSAN 6.6.1 (et versions ultérieures) est intégré avec vSphere Update Manager.

vSAN génère les références et groupes de références système à utiliser avec vSphere Update Manager.

Le catalogue des versions de vSAN contient des informations actualisées sur les versions disponibles, sur l'ordre de préférence des versions et sur les correctifs critiques nécessaires pour chaque version. Le catalogue des versions de vSAN est hébergé sur VMware Cloud™.

vSphere Update Manager détermine la procédure de mise à niveau appropriée pour chaque cluster vSAN à partir des informations actualisées du catalogue des versions vSAN. vSAN inclut également les pilotes et les mises à jour de correctif correspondant à la version recommandée dans sa référence système.



La gestion des correctifs et des versions de la solution vSAN est pleinement intégrée dans cette dernière. Des recommandations concernant la version de vSAN sont générées de manière automatique sur la base des informations contenues dans le Guide de compatibilité VMware, du catalogue des versions de vSAN et de la détection de la configuration matérielle sous-jacente.

Pour mettre à jour vSAN :

1. Ajoutez vos informations d'authentification my.vmware.com dans le moteur de recommandations de build vSAN.

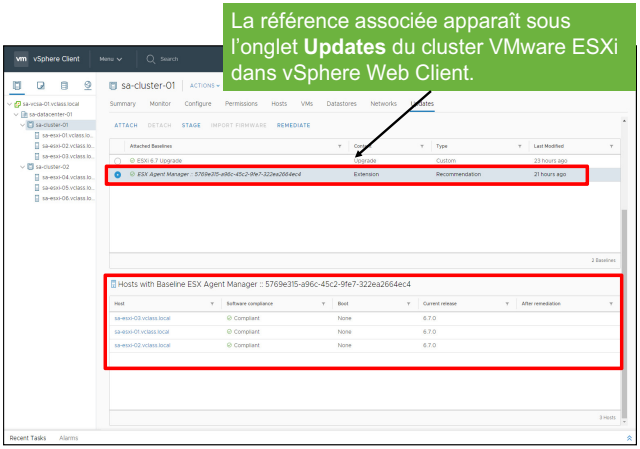
   Lorsque vous vous connectez, vSAN génère un groupe de références contenant les mises à jour recommandées pour chaque cluster vSAN. Les références système vSAN sont répertoriées dans le volet « Baselines » de l'onglet **Baselines and Groups**.

2. Pour mettre à jour le cluster vSAN, cliquez sur l'onglet **Update Manager**, puis sur **Remediate**.

11-18 À propos des références système

Une référence système permet de garantir la conformité et la compatibilité d'un cluster VMware ESXi avec les logiciels, mises à jour ou extensions recommandés dans cette référence :

- Les références système sont en lecture seule, et elles sont créées et gérées de manière automatique par vSphere Update Manager.
- Une fois qu'un cluster VMware ESXi a été préparé par NSX Manager, la référence EAM est automatiquement associée à ce cluster et soumise à une analyse de conformité.



11-19 Intégration de vSphere Update Manager avec vSphere DRS

Lorsqu'il effectue des opérations de mise en conformité sur un cluster VMware ESXi, vSphere Update Manager s'intègre automatiquement avec vSphere DRS :

- Dans un cluster vSphere DRS, vSphere Update Manager place les hôtes en mode maintenance avant l'exécution de vSphere DRS. Le placement des hôtes en mode maintenance entraîne l'évacuation des hôtes du cluster vSphere DRS en préalable à leur mise en conformité.
- Lorsqu'une opération de placement en mode maintenance est appelée, certaines vérifications préalables sont effectuées afin de vérifier que l'hôte VMware ESXi peut effectivement passer en mode maintenance.
- Le cas échéant, vSphere signale les problèmes de configuration pouvant faire obstacle au passage d'un hôte VMware ESXi en mode maintenance.

Si les vérifications suivantes ne donnent pas satisfaction, l'opération de placement en mode maintenance échoue en indiquant les raisons de son échec :

- Vérifications au niveau de l'hôte VMware ESXi :
  - « ESXi host cluster participation »
  - « Powered-on virtual machine capacity »
  - « vSphere DRS enabled status »
  - « vSphere DRS fully automated status »
- Vérifications au niveau des machines virtuelles :
  - « Virtual machine vSphere DRS manual override »
  - « Virtual machine vSphere DRS rule conflict »
  - « vSphere HA admission control violation »

11-20 Laboratoire 18 : Utilisation de vSphere Update Manager

Installer, configurer et utiliser vSphere Update Manager

1. Modifier les paramètres de cluster
2. Configurer vSphere Update Manager
3. Créer une référence de correctif
4. Associer une référence et rechercher des mises à jour
5. Préparer les correctifs sur l'hôte VMware ESXi
6. Mettre en conformité l'hôte VMware ESXi

11-21 Rappel des objectifs de la formation

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

- Décrire les fonctionnalités de VMware vSphere Update Manager
- Utiliser vSphere Update Manager pour créer et associer une référence

11-22 Points clés

- vSphere Update Manager permet de minimiser les vulnérabilités et les failles de sécurité en assurant les mises à jour et en réduisant la disparité des systèmes déployés dans un environnement.

Des questions ?

MODULE 12

Résolution des problèmes vSphere

12-2 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**

12-3 Importance

Vous pouvez rapidement identifier, diagnostiquer et résoudre un problème si vous appliquez une méthodologie de résolution des problèmes efficace de manière homogène et reproductible.

Le fait de connaître les outils adaptés à chaque type de problème vous permet de gagner du temps et d'optimiser l'efficacité du processus de résolution.

12-4 Leçons du module

Leçon 1 :	Outils de résolution des problèmes
Leçon 2 :	Présentation de la résolution des problèmes

12-5 Leçon 1 : Outils de résolution des problèmes

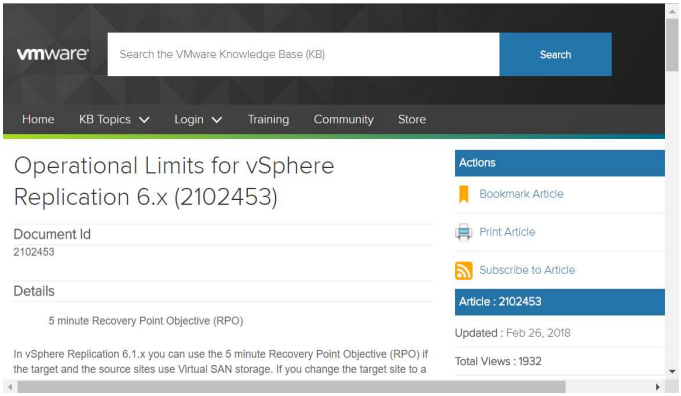
12-6 Objectifs de la formation

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

- Passer en revue les outils de résolution des problèmes
- Rechercher des fichiers journaux importants
- Utiliser vSphere Syslog Collector

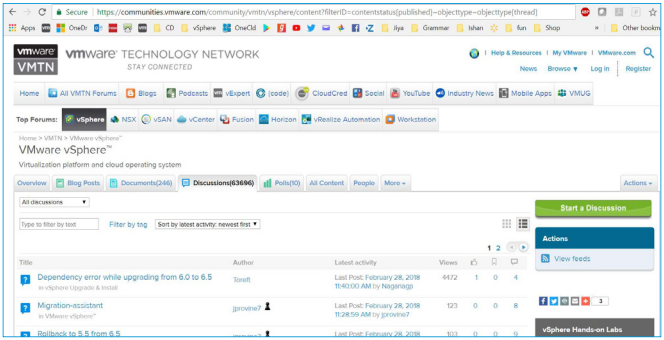
12-7 À propos de la Base de connaissances VMware

La Base de connaissances VMware fournit des solutions de support, des messages d'erreur et des guides de résolution des problèmes.



12-8 À propos de la Communauté VMware

La Communauté VMware est une famille de sites Web et de communautés en ligne comprenant des blogs, des forums de discussion, des documents et un partage d'informations concernant les produits et les services, les logiciels et technologies de virtualisation, ainsi que les services fournis par VMware et ses filiales.



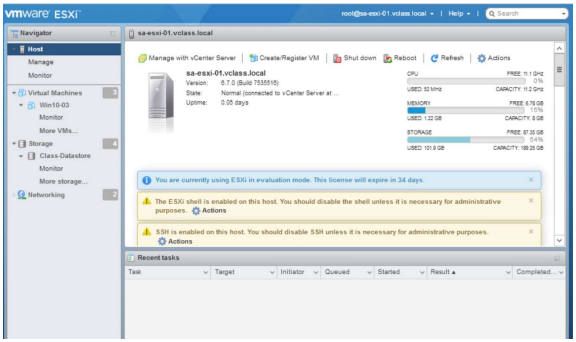
La Communauté VMware offre un forum permettant l'échange d'informations entre les utilisateurs de la virtualisation et des produits et services associés, les participants aux programmes VMware tels que les programmes bêta, les groupes d'utilisateurs et les comités consultatifs des clients.

12-9 À propos de VMware Host Client

Vous utilisez VMware Host Client pour assurer une gestion d'urgence lorsque vCenter Server est momentanément inaccessible.

Les fonctions VMware Host Client incluent les opérations suivantes :

- Les opérations de la virtualisation de base, telles que le déploiement et la configuration des machines virtuelles présentant différents niveaux de complexité
- La création et la gestion de réseaux et de banques de données
- Le réglage avancé des options au niveau de l'hôte afin d'améliorer les performances



VMware Host Client est un client HTML5 permettant de se connecter à un hôte VMware ESXi unique et de gérer ce dernier.

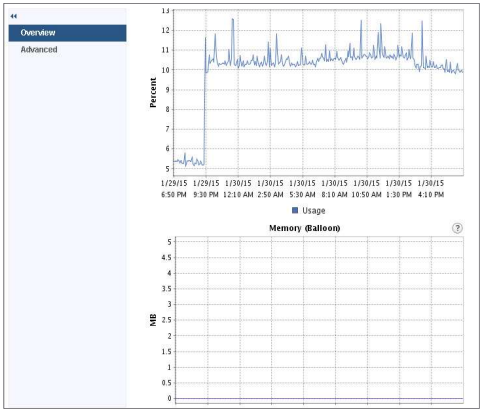
Vous pouvez utiliser VMware Host Client pour accomplir des tâches administratives et des tâches de résolution des problèmes de base, ainsi que des tâches administratives avancées sur votre hôte VMware ESXi cible. Vous pouvez également utiliser VMware Host Client pour assurer une gestion d'urgence lorsque vCenter Server est inaccessible.

Bien que leurs interfaces utilisateur soient similaires, VMware Host Client et vSphere Web Client ne remplissent pas les mêmes fonctions. vSphere Web Client vous permet de vous connecter à vCenter Server et de gérer plusieurs hôtes VMware ESXi. Vous utilisez VMware Host Client pour gérer un hôte VMware ESXi unique.

12-10 Surveillance de l’environnement virtuel à l’aide des diagrammes de performances

VMware propose des outils vous permettant de surveiller votre environnement virtuel et d’identifier l’origine des problèmes potentiels ou actuels :

- Les diagrammes généraux présentent dans un même panneau plusieurs jeux de données destinés à évaluer les statistiques relatives aux ressources, et affichent des diagrammes miniatures concernant les objets enfants. Des diagrammes portant sur un objet parent et un objet enfant sont également disponibles.
- Les diagrammes avancés fournissent davantage d’informations que les diagrammes généraux. Ils sont configurables et peuvent être imprimés ou exportés.



Partie du panneau « Overview » des diagrammes de performances de l’hôte

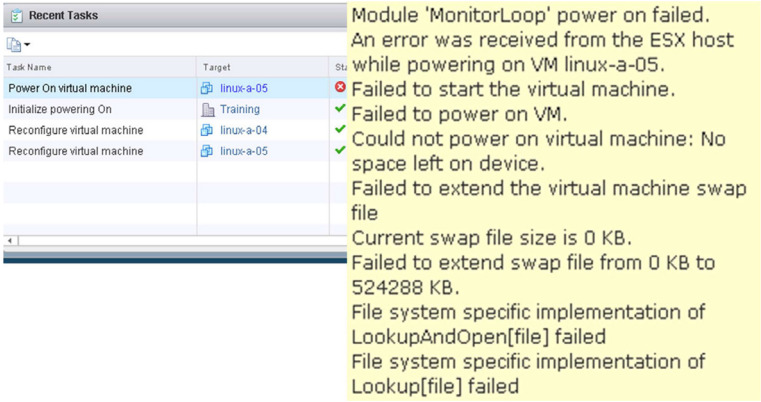
Le sous-système de statistiques vSphere collecte des données sur l’utilisation des ressources par les objets d’inventaire. Les données de nombreuses mesures sont collectées à intervalles rapprochés, puis traitées et archivées dans la base de données vCenter Server. Vous pouvez accéder aux informations statistiques par le biais d’utilitaires de ligne de commande dédiés à la surveillance, ou en visualisant les diagrammes de performances proposés dans vSphere Web Client.

Les options des diagrammes de performances accessibles par l’intermédiaire du menu **View** dépendent du type d’objet d’inventaire que vous sélectionnez.

12-11 Visualisation et interprétation des informations de diagnostic

Vous pouvez visualiser les messages de diagnostic dans l'interface utilisateur ou dans les fichiers journaux.

Vous interprétez les messages de diagnostic pour déterminer la cause profonde des problèmes.



12-12 Emplacement des journaux vCenter Server

La plupart des fichiers journaux vCenter Server se trouvent sur vCenter Server Appliance dans le répertoire `/var/log/vmware/`.

Les journaux relatifs aux composants vCenter Server sont stockés dans des sous-répertoires. Par exemple, le sous-répertoire `vpxd-svcs` contient les journaux des services vCenter Server.

Certains journaux, tels que `FirstBoot.log`, figurent dans `/var/log`.

```
root@sa-vcsa-01 [ /var/log/vmware ]# ls
applmgmt          rsyslogd        vmdird
applmgmt-audit    rsyslogd-2068   vmdnsd
cis-license       rsyslogd-2078   vmon
cloudvm           sca             vmware-imagebuilder
cm                sso             vmware-sps
content-library   syslog          vmware-updatemgr
eam               vapi            vpostgres
journal           vcha            vpxd
mbcs              vctop           vpxd-svcs
netdumper         vmafd           vsan-health
perfcharts        vmafdd          vsm
psc-client        vmcad           vsphere-client
rbd               vmcam           vsphere-ui
rhttpproxy        vmdir
```

Par défaut, vCenter Server stocke ses fichiers journaux dans un emplacement par défaut. Cet emplacement repose sur le chemin d'installation du logiciel.

Pour plus d'informations sur l'emplacement des fichiers journaux vCenter Server, consultez l'article 2110014 de la Base de connaissances VMware, disponible à l'adresse suivante : http://kb.vmware.com/kb/2110014.

12-13 Journaux communs

Les journaux communs sont communs à tous les systèmes vCenter Server.

Répertoire de journal	Description
`applmgmt`	VMware Appliance Management Service
`CloudVM`	Journaux concernant l'attribution et la distribution des ressources parmi les services
`CM`	VMware Component Manager
`rhttpproxy`	Proxy Web inverse
`SCA`	VMware Service Control Agent
`Vapi`	VMware vAPI Endpoint
`vmaffd`	Démon VMware Authentication Framework
`vmdird`	Démon du service d'annuaire VMware
`Vmon`	VMware Service Lifecycle Manager
`vSphere-Client`	VMware vSphere Web Client

12-14 Journaux de nœud de gestion

Les journaux de nœud de gestion apparaissent sur les systèmes vCenter Server Appliance qui sont des nœuds combinés (déploiement à nœud unique) ou des nœuds tiers.

Le tableau ci-après répertorie certains des journaux de nœud de gestion les plus importants.

Journal	Description
`AutoDeploy`	VMware vSphere Auto Deploy Waiter
`content-library`	Service de bibliothèque de contenu VMware
`EAM`	VMware ESX Agent Manager
`InvSvc`	Service d'inventaire VMware
`vmcam`	VMware vSphere Authentication Proxy
`vpxd`	VMware VirtualCenter Server
`vPostgres`	Service de base de données vFabric Postgres

12-15 Journaux Platform Services Controller

Les journaux Platform Services Controller apparaissent sur les nœuds Platform Services Controller.

Journal	Description
`cis-license`	Service de gestion des licences VMware
`SSO`	Service de jetons sécurisés VMware
`Vmcad`	Démon VMware Certificate Authority

12-16 Journal vCenter Server important pour la résolution des problèmes

Le fichier `vpxd.log` est le principal fichier journal concernant vCenter Server. La plupart des actions vCenter Server sont capturées dans le fichier `vpxd.log` situé dans le répertoire `/var/log/vmware/vpxd/`.

```
2017-03-03T17:37:30.809Z info vpxd[7FD7BF66C700] [Originator@6876 sub=vpxLro opID=urn:vmomi:VirtualMachine:vm-128:596e26b2-df48-4c88-b39c-eb702
ba52e66.properties:01-3d] [VpxLRO] -- BEGIN lro-24393 -- ResourceModel -- cis.data.provider.ResourceModel.query -- 5266df8c-2f36-e3c4-1d59-c474
66b43db1(52723af4-e7c1-92c5-02c8-4108140b6ba2)
2017-03-03T17:37:30.810Z info vpxd[7FD7BF66C700] [Originator@6876 sub=vpxLro opID=urn:vmomi:VirtualMachine:vm-128:596e26b2-df48-4c88-b39c-eb702
ba52e66.properties:01-3d] [VpxLRO] -- FINISH lro-24393
2017-03-03T17:37:30.813Z info vpxd[7FD7BF66C700] [Originator@6876 sub=vpxLro opID=urn:vmomi:VirtualMachine:vm-128:596e26b2-df48-4c88-b39c-eb702
ba52e66.properties:01-ef] [VpxLRO] -- BEGIN lro-24394 -- ResourceModel -- cis.data.provider.ResourceModel.query -- 5266df8c-2f36-e3c4-1d59-c474
66b43db1(52723af4-e7c1-92c5-02c8-4108140b6ba2)
2017-03-03T17:37:30.813Z info vpxd[7FD7BF66C700] [Originator@6876 sub=vpxLro opID=urn:vmomi:VirtualMachine:vm-128:596e26b2-df48-4c88-b39c-eb702
ba52e66.properties:01-ef] [VpxLRO] -- FINISH lro-24394
2017-03-03T17:37:30.815Z info vpxd[7FD7BFE7C700] [Originator@6876 sub=vpxLro opID=urn:vmomi:VirtualMachine:vm-128:596e26b2-df48-4c88-b39c-eb702
ba52e66.properties:01-df] [VpxLRO] -- BEGIN lro-24395 -- ResourceModel -- cis.data.provider.ResourceModel.query -- 5266df8c-2f36-e3c4-1d59-c474
66b43db1(52723af4-e7c1-92c5-02c8-4108140b6ba2)
2017-03-03T17:37:30.815Z info vpxd[7FD7BFE7C700] [Originator@6876 sub=vpxLro opID=urn:vmomi:VirtualMachine:vm-128:596e26b2-df48-4c88-b39c-eb702
ba52e66.properties:01-df] [VpxLRO] -- FINISH lro-24395
2017-03-03T17:37:30.816Z info vpxd[7FD7BFE7C700] [Originator@6876 sub=vpxLro opID=urn:vmomi:VirtualMachine:vm-128:596e26b2-df48-4c88-b39c-eb702
ba52e66.properties:01-67] [VpxLRO] -- BEGIN lro-24396 -- ResourceModel -- cis.data.provider.ResourceModel.query -- 5266df8c-2f36-e3c4-1d59-c474
66b43db1(52723af4-e7c1-92c5-02c8-4108140b6ba2)
2017-03-03T17:37:30.816Z info vpxd[7FD7BFE7C700] [Originator@6876 sub=vpxLro opID=urn:vmomi:VirtualMachine:vm-128:596e26b2-df48-4c88-b39c-eb702
ba52e66.properties:01-67] [VpxLRO] -- FINISH lro-24396
```

12-17 Emplacement des journaux d'hôte VMware ESXi

La plupart des fichiers journaux d'hôte VMware ESXi figurent dans le répertoire `/var/log`.

```
[root@sa-esxi-01:/var/log] ls
Xorg.log                ipmi                    vitd.log
auth.log                jumpstart-stdout.log    vmauthd.log
boot.gz                 kickstart.log           vmkdevmgr.log
clomd.log               lacp.log                vmkernel.log
configRP.log            nfcd.log                vmkeventd.log
ddecomd.log             osfsd.log               vmksummary.log
dhclient.log            rabbitmqproxy.log       vmkwarning.log
epd.log                 rhttpproxy.log          vmware
esxcli-software.log     sdrsinjector.log        vmware-vmsvc.log
esxupdate.log           shell.log               vobd.log
fdm.log                 smbios.bin              vprobe.log
hbrca.log               storagerm.log           vpxa.log
hostd-probe.log         swapobjd.log            vsanmgmt.log
hostd.log               sysboot.log             vsansystem.log
hostdCgiServer.log      syslog.log              vsanvpd.log
hostprofiletrace.log    tallylog                vvold.log
iofilter-init.log       upitd.log
iofiltervpd.log         usb.log
```

Si un espace de travail persistant est configuré, une grande partie de ces journaux est stockée sur le volume de travail, `/scratch/log`. Le répertoire `/var/log` contient des liens symboliques (identifiés en bleu clair dans la sortie) vers les fichiers journaux figurant dans `/scratch/log`. Pour obtenir la liste des fichiers journaux vers lesquels pointent ces liens symboliques, exécutez la commande `ls -l`.

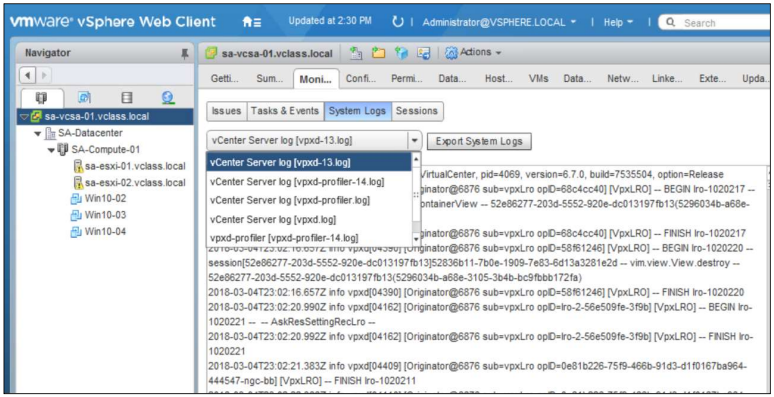
12-18 Journaux d'hôte VMware ESXi utiles pour la résolution des problèmes

Selon l'action exécutée, les hôtes VMware ESXi alimentent plusieurs fichiers journaux.

Journal	Description
`hostd.log`	Journaux de service de gestion d'hôte
`syslog.log`	Initialisation des services de gestion, surveillances, tâches planifiées et utilisation de Direct Console User Interface (ESXi Console) (DCUI)
`vmkernel.log`	Journaux VMkernel principaux, consignant les événements de détection des périphériques, de stockage, de périphérique réseau et de pilote, ainsi que les démarrages de machine virtuelle
`vmkwarning.log`	Résumé des messages d'avertissement et d'alerte extraits des journaux VMkernel
`vmksummary.log`	Résumé des démarrages et arrêts d'hôte VMware ESXi, et pulsation horaire avec la disponibilité, le nombre de machines virtuelles en cours d'exécution et la consommation des ressources de service

12-19 Visualisation des fichiers journaux vCenter Server dans vSphere Web Client

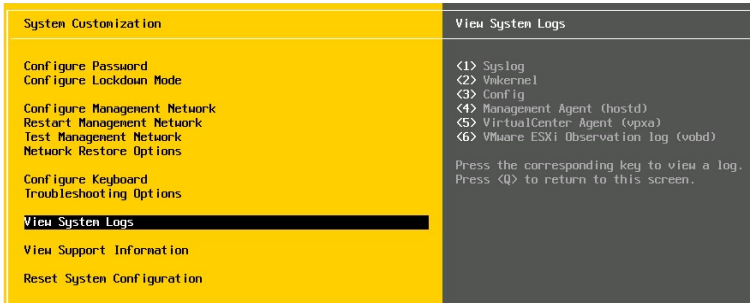
Vous pouvez utiliser vSphere Web Client pour visualiser les fichiers journaux sur les systèmes vCenter Server. Utilisez l'onglet **Monitor** correspondant aux systèmes vCenter Server.



12-20 Visualisation des fichiers journaux dans DCUI

Si vCenter Server n’est pas disponible, vous pouvez utiliser DCUI pour visualiser les fichiers journaux.

DCUI ne vous permet de visualiser les fichiers journaux que d’un seul hôte VMware ESXi.



Dans la console de l’hôte VMware ESXi, appuyez sur F2 et connectez-vous à DCUI à l’aide du nom et du mot de passe de l’utilisateur root. Appuyez sur la touche appropriée pour rechercher le fichier journal (/), afficher l’aide (H) ou fermer l’écran de visualisation du fichier journal (Q).

12-21 À propos de vSphere Syslog Collector

vSphere Syslog Collector centralise les fichiers journaux alimentés par la totalité des hôtes VMware ESXi.

vSphere Syslog Collector permet de combiner les fichiers journaux de plusieurs hôtes et offre une structure pour la journalisation réseau.

vSphere Syslog Collector est préinstallé sur vCenter Server Appliance.

Le serveur vSphere Syslog Collector utilise par défaut le port 514 pour TCP et UDP, et le port 1514 pour SSL.

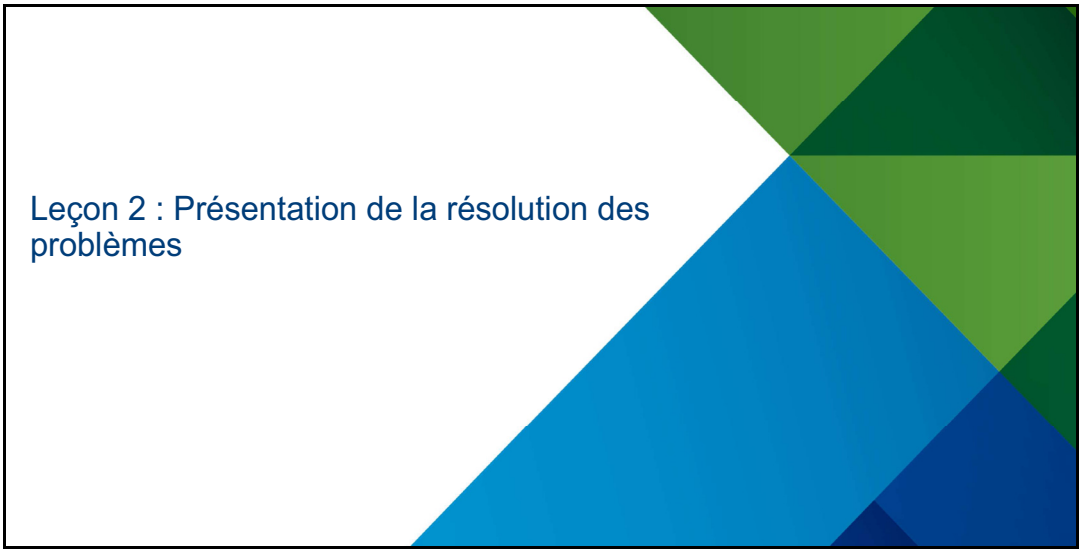
vSphere Syslog Collector offre une architecture unifiée pour la journalisation système. Grâce à vSphere Syslog Collector, vous pouvez diriger les journaux des hôtes VMware ESXi vers un serveur du réseau, au lieu d'enregistrer ces journaux sur un disque local.

12-22 Rappel des objectifs de la formation

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

- Passer en revue les outils de résolution des problèmes
- Rechercher des fichiers journaux importants
- Utiliser vSphere Syslog Collector

12-23 Leçon 2 : Présentation de la résolution des problèmes



12-24 Objectifs de la formation

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

- Définir la portée de la résolution des problèmes
- Utiliser une approche structurée pour résoudre les problèmes de configuration et d'ordre opérationnel
- Appliquer la méthodologie de résolution des problèmes pour diagnostiquer de manière logique les anomalies et améliorer l'efficacité du dépannage

12-25 Processus de résolution des problèmes

La résolution des problèmes est une approche systématique qui consiste à identifier la cause profonde d'un problème et à définir les étapes permettant de résoudre ce dernier.

Un processus de résolution des problèmes classique comprend les étapes suivantes :

1. Définition du problème.
2. Identification de la cause du problème.
3. Résolution du problème.

Le processus de résolution des problèmes est amorcé dès qu'un utilisateur signale un problème. Dans ce contexte, le terme utilisateur désigne toute personne ayant recours au système, qu'il s'agisse d'un utilisateur final ou d'un administrateur. Parfois, le problème signalé par l'utilisateur ne correspond pas au véritable problème. Il arrive qu'un utilisateur rapporte uniquement les symptômes du problème.

Bien qu'un problème observé puisse se trouver directement à l'origine des symptômes, il a généralement une cause plus fondamentale.

12-26 Définition d’un problème système

Un problème système est une défaillance dans un système ou dans l’un de ses composants qui altère les services requis pour l’environnement de production normal.

Les problèmes système émanent d’origines diverses :

- Problèmes de configuration
- Conflit entre les ressources
- Attaques du réseau
- Logiciels :
  - Bogues
  - Interopérabilité
- Matériel :
  - Défaillances
  - Compatibilité matérielle

Ne présumez pas que l’identification d’un symptôme spécifique suffit à comprendre la nature exacte d’un problème. Procédez à une analyse en profondeur et vérifiez qu’aucun autre élément n’est compromis.

Un système comporte plusieurs composants, aussi bien logiciels que matériels. Par exemple, un hôte VMware ESXi se compose d’une CPU, de mémoire, ainsi que de logiciels de stockage, de mise en réseau et d’hyperviseur. De même, une machine virtuelle comprend différents composants, tels qu’une ou plusieurs applications, un système d’exploitation client et du matériel virtuel. Un problème qui survient dans un système est susceptible de perturber et d’altérer des services de production parfaitement fonctionnels auparavant.

12-27 Collecte des symptômes d'un problème

La première étape du processus de résolution d'un problème consiste à collecter les symptômes.

Une même cause profonde prend souvent la forme de différents symptômes signalés par les utilisateurs.

Il est impératif d'établir une distinction entre les symptômes d'un problème et la cause profonde de celui-ci.

Symptôme	Cause possible	Cause profonde
Un ou plusieurs LUN d'une baie de stockage ne sont pas visibles pour un hôte VMware ESXi spécifique.	Les LUN non visibles ne sont pas présentés correctement à l'hôte VMware ESXi.	
	Défaillance de routage.	Une défaillance réseau est survenue entre l'hôte VMware ESXi et la baie de stockage. Aucun chemin redondant n'est disponible.
Vous ne parvenez pas à vous connecter à vCenter Server avec vSphere Web Client.	Le démarrage du service VirtualCenter Server a échoué.	vCenter Server Appliance comporte une base de données endommagée.
	Le chemin réseau entre votre emplacement et vCenter Server Appliance est hors service.	

Des problèmes peuvent se produire dans n'importe quel environnement informatique. Des comportements d'applications complexes, des exigences fluctuantes et des infrastructures partagées sont susceptibles d'engendrer des anomalies dans des environnements précédemment stables.

La résolution des problèmes requiert une compréhension exhaustive des interactions entre les composants logiciels et matériels d'un environnement informatique. L'évolution vers un environnement informatique virtualisé ajoute de nouvelles couches logicielles et de nouveaux types d'interactions qui doivent être pris en compte lors de la résolution des problèmes.

12-28 Collecte d’informations supplémentaires

Posez des questions afin d’obtenir des informations supplémentaires pour définir le problème :

- Le problème peut-il être reproduit ?
  - Fournissez une méthode reproductible permettant de recréer le problème, ainsi qu’un moyen de vérifier que le problème a été résolu.
- Quelle est la portée du problème ?
  - Le problème affecte-t-il un seul objet ou plusieurs objets ?
- Le système fonctionnait-il auparavant ?
  - Si tel est le cas, quelles modifications ont été apportées à l’environnement ou à la configuration ?
- Le problème est-il déjà connu ?
  - Consultez les références, telles que les notes de mise à jour, pour déterminer si le problème a déjà été documenté.

Un processus de résolution des problèmes efficace doit commencer par une vue d’ensemble de l’environnement informatique, puis réduire de manière systématique la portée de l’examen à mesure que les sources de défaillance possibles sont éliminées. Les procédures de résolution des problèmes qui démarrent par une conception étroite de l’origine d’un problème s’enlisent fréquemment dans une analyse détaillée d’un seul composant, alors que la véritable source du problème réside à un autre emplacement de l’infrastructure.

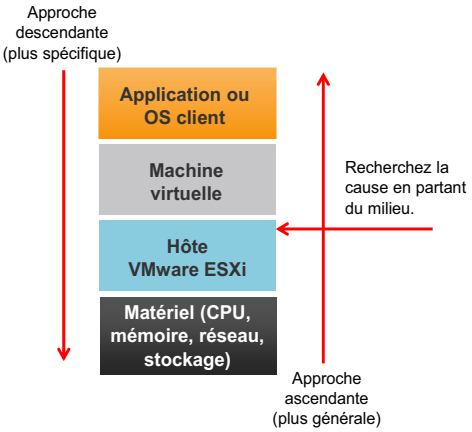
Pour localiser rapidement l’origine d’un problème, vous devez adopter une méthodologie de résolution des problèmes logique évitant les idées préconçues concernant la source de la défaillance.

12-29 Identification des causes possibles et choix de l'approche appropriée

L'adoption d'une approche structurée en matière de résolution des problèmes vous permet de déterminer la cause profonde d'un problème avec rapidité et efficacité.

En vous basant sur les caractéristiques du problème, appliquez l'une des approches de résolution suivantes :

- Recherchez la cause en adoptant une approche descendante.
- Recherchez la cause en adoptant une approche ascendante.
- Recherchez la cause en partant du milieu.



Dans un environnement virtuel VMware, la cause profonde d'un problème peut résider dans n'importe quel composant virtuel. Savoir où commencer à chercher la cause profonde n'est généralement pas chose facile. Par conséquent, la collecte d'un maximum d'informations concernant le problème peut vous aider à déterminer le composant virtuel que vous devrez commencer par examiner.

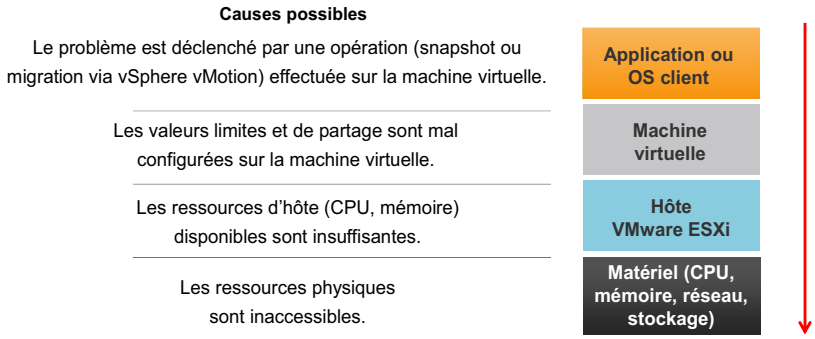
Vous pouvez appliquer l'une des approches de résolution suivantes :

- Approche descendante : démarrez la procédure de résolution des problèmes dans le système d'exploitation client, puis descendez progressivement dans la pile en examinant successivement la machine virtuelle, l'hôte VMware ESXi, et enfin le matériel.
- Approche ascendante : démarrez la procédure de résolution des problèmes au niveau du matériel, puis remontez progressivement dans la pile en examinant successivement l'hôte VMware ESXi, la machine virtuelle, et enfin le système d'exploitation client.
- Approche en partant du milieu : démarrez la procédure de résolution des problèmes au milieu de la pile. Par exemple, commencez par la machine virtuelle et testez les causes possibles. Les résultats du test déterminent si vous devez poursuivre la procédure en remontant la pile ou en la descendant.

12-30 Détermination de la cause profonde

Pour déterminer la cause profonde, testez votre environnement et éliminez les causes possibles.

Exemple : la machine virtuelle ne répond plus.



Une bonne connaissance de l'infrastructure virtuelle générale et de la configuration de votre système spécifique se révèle d'une grande utilité pour l'identification des causes possibles d'un problème. Classez les causes possibles par priorité, de la plus probable à la moins probable. Puis testez chacune d'elles afin de déterminer la cause la plus susceptible d'occasionner le problème, appelée cause profonde.

Dans l'exemple de problème ci-dessus, une machine virtuelle ne répond plus. Dans le cas d'un système non réactif, le système d'exploitation semble figé et aucun message d'erreur ne s'affiche. Toutefois, le système d'exploitation est toujours en cours d'exécution. La résolution des problèmes de ce type peut nécessiter la consultation de certains documents, tels que les articles de la Base de connaissances VMware. Par exemple, pour remédier au problème d'absence de réponse d'une machine virtuelle, reportez-vous à l'article 1007819 de la Base de connaissances VMware, accessible à l'adresse suivante : http://kb.vmware.com/kb/1007819.

La résolution de ce problème nécessite l'adoption d'une approche descendante. Commencez par les opérations effectuées sur la machine virtuelle, vérifiez la configuration de cette dernière, puis assurez-vous que l'hôte sur lequel réside la machine virtuelle dispose de ressources suffisantes.

12-31 Résolution du problème

Après avoir identifié la cause profonde, évaluez l'impact du problème sur les opérations :

- Impact élevé : résolvez immédiatement le problème.
- Impact modéré : résolvez le problème lorsque cela vous est possible.
- Impact minime : résolvez le problème au cours de la prochaine fenêtre de maintenance.

Identifiez les solutions possibles et leur impact sur l'environnement vSphere :

- Solution à court terme : solution de contournement.
- Solution à long terme : reconfiguration.
- Analyse d'impact : évaluation de l'impact de la solution sur les opérations.

Remédiez au problème en mettant en œuvre la solution la plus efficace.

Après avoir identifié la cause profonde, résolvez le problème. Pour ce faire, vous identifiez les solutions possibles du problème, puis vous mettez en œuvre l'une de ces solutions.

Lorsque vous déterminez la solution la mieux adaptée, évaluez l'impact du problème sur les opérations standard. Par exemple, si le problème entraîne l'inaccessibilité d'applications stratégiques, il a un impact élevé et doit donc être immédiatement résolu.

Vous pouvez choisir de commencer par mettre en œuvre une mesure corrective à court terme afin que les systèmes puissent être rapidement remis en ligne. Avant d'implémenter cette solution à court terme, documentez toutes les modifications que vous avez apportées au système depuis l'apparition du problème. En outre, sauvegardez les fichiers journaux alimentés depuis le début du problème. Certaines solutions à court terme peuvent avoir un effet destructeur et tronquer d'importantes informations de journal nécessaires à l'obtention d'une assistance supplémentaire.

Pour finir, vous pouvez mettre en œuvre une solution à long terme plus durable afin d'éviter toute réapparition du problème.

12-32 Exemple de scénario : définition du problème

Problème : la migration via vSphere vMotion échoue avec un message d'erreur.

Scénario : vous tentez de migrer la machine virtuelle VM01 de l'hôte ESXi01 vers l'hôte ESXi02. Après quelques minutes, la migration vSphere vMotion échoue avec un message d'erreur.

S'agit-il d'un problème lié à vSphere vMotion ou du symptôme d'un problème sous-jacent ?

Le message d'erreur vous fournit des informations supplémentaires.

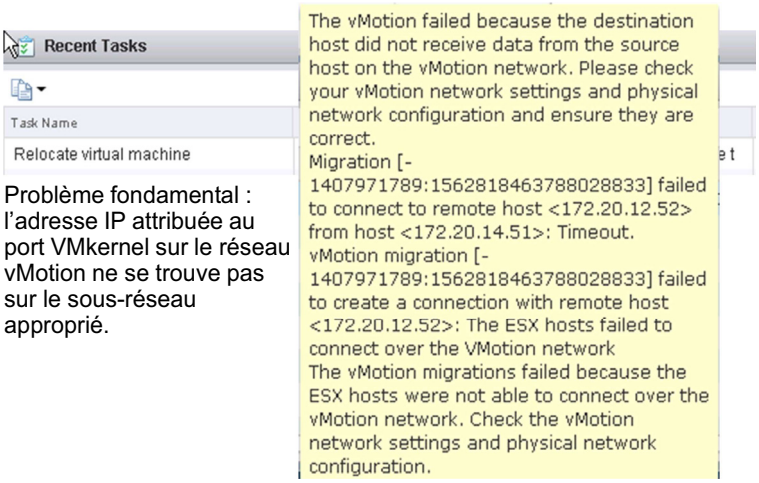
Dans l'exemple ci-dessus, vous utilisez la méthodologie de résolution des problèmes pour diagnostiquer un problème de migration via vSphere vMotion. Vous effectuez une migration vSphere vMotion par le biais de vSphere Web Client, mais cette migration échoue avec un message d'erreur.

À ce stade, vous n'êtes pas en mesure de déterminer si le problème est propre à vSphere vMotion ou s'il se situe dans l'infrastructure sous-jacente, comme le stockage ou la mise en réseau.

Pour identifier la zone posant problème, collectez des informations relatives au problème, en commençant par les éventuels messages de diagnostic qui s'affichent dans vSphere Web Client.

12-33 Exemple : collecte d’informations

Les messages d’erreur peuvent vous aider à déterminer le problème.



Problème fondamental : l’adresse IP attribuée au port VMkernel sur le réseau vMotion ne se trouve pas sur le sous-réseau approprié.

vSphere Web Client affiche des messages d’erreur concernant la tâche de migration vSphere vMotion ayant échoué, qui fournissent les informations suivantes :

- Une erreur système générale s’est produite : la migration via vSphere vMotion a échoué, car les hôtes VMware ESXi ne sont pas parvenus à se connecter par le biais du réseau vSphere vMotion. Vérifiez les paramètres réseau vSphere vMotion et la configuration du réseau physique.
- La migration vSphere vMotion n’est pas parvenue à créer une connexion avec l’hôte distant 172.20.13.52 : les hôtes VMware ESXi n’ont pas pu se connecter par le biais du réseau vSphere vMotion.
- La migration n’est pas parvenue à se connecter à l’hôte distant 172.20.13.52 à partir de l’hôte 172.20.12.51 : expiration du délai de connexion.

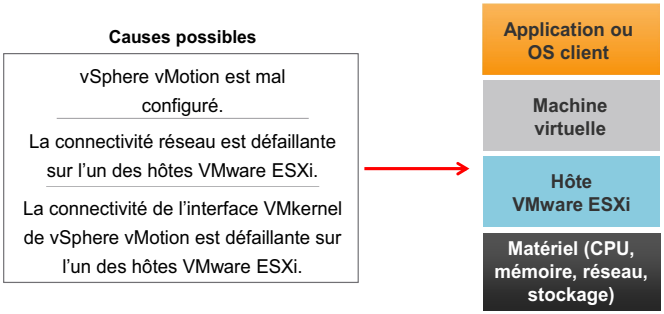
  Les adresses IP font référence aux interfaces VMkernel de vSphere vMotion sur l’hôte distant (ESXi02) et l’hôte local (ESXi01).
- La migration via vSphere vMotion a échoué, car l’hôte de destination n’a pas reçu de données de la part de l’hôte source sur le réseau vSphere vMotion. Vérifiez que les paramètres réseau vSphere vMotion et la configuration du réseau physique sont corrects.

Le premier message d’erreur de la pile est utile et vous invite à vérifier les paramètres réseau vSphere vMotion, ainsi que la configuration du réseau physique. Tous les messages d’erreur ne se révèlent pas aussi utiles.

12-34 Exemple : identification des causes possibles

Utilisez les informations que vous avez collectées pour identifier les causes possibles :

- D'après les messages d'erreur, la migration via vSphere vMotion a échoué, car les hôtes ESXi01 et ESXi02 ne sont pas parvenus à se connecter par le biais du réseau vMotion.
- Cet échec signale une éventuelle erreur de configuration sur l'hôte VMware ESXi.
- Vérifiez la connectivité de l'interface VMkernel de vSphere vMotion.



Le message d'erreur signale des problèmes de connectivité avec le réseau vMotion pouvant avoir les causes suivantes :

- vSphere vMotion est mal configuré.
- La connectivité réseau entre ESXi01 et ESXi02 est défaillante.
- La connectivité de l'interface VMkernel de vSphere vMotion entre ESXi01 et ESXi02 est défaillante.

Lorsque vous initialisez la migration via vSphere vMotion, plusieurs vérifications de compatibilité sont effectuées avant le début de la migration. Ceci vous permet d'éliminer différentes causes possibles, telles que la désactivation de vSphere vMotion ou l'incompatibilité des CPU, car ces aspects de configuration sont vérifiés avant la migration.

12-35 Exemple : résolution du problème

Dans cet exemple, supposons que la cause profonde du problème soit une adresse IP incorrecte d'une interface VMkernel pour vSphere vMotion sur l'hôte ESXi02.

Évaluez l'impact du problème sur les opérations :

- L'impact probablement élevé :
  - Le problème affecte toutes les machines virtuelles qui sont migrées vers l'hôte ESXi02.
  - Le problème a également une incidence sur le bon fonctionnement de vSphere DRS.

Identifiez les solutions possibles pour résoudre le problème :

- La solution à court terme : ne migrez pas les machines virtuelles vers l'hôte ESXi02.
- La solution à long terme : corrigez l'adresse IP de l'interface VMkernel de vSphere vMotion de l'hôte ESXi02.

La mise en œuvre de la solution ne doit impliquer aucune interruption de service.

Une fois que vous avez identifié la cause profonde, déterminez les solutions susceptibles de corriger le problème. L'impact du problème sur les opérations standard (élevé, modéré ou minime) détermine le degré d'urgence de mise en œuvre de la solution.

Pour finir, identifiez le type de solution adapté à ce problème. Vous pouvez décider de mettre en œuvre une solution à court terme afin de rétablir le fonctionnement normal du système. Documentez toutes les modifications que vous avez apportées au système depuis l'apparition du problème. En outre, sauvegardez les fichiers journaux alimentés depuis le début du problème, car les journaux sont régulièrement remplacés et risquent de ne plus être accessibles par la suite.

12-36 Définition des niveaux de gravité et des temps de réponse cibles VMware

La gravité du problème et les niveaux de service du programme de support acheté déterminent la rapidité et la méthode de réponse cibles.

Le tableau ci-après répertorie les temps de réponse cibles pour la fourniture de la réponse initiale. Pour obtenir la liste complète des temps de réponse de VMware, ainsi qu'une description des niveaux de gravité des problèmes, accédez à l'adresse suivante : https://www.vmware.com/fr/support/policies/severity.

Niveau de gravité	Définition	Temps de réponse stratégique
Critique 1	Le serveur de production ou d'autres systèmes stratégiques sont en panne, et aucune solution de contournement n'est immédiatement disponible.	30 minutes maximum, 24 h/24, 7 j/7
Majeur 2	Une fonctionnalité essentielle est sérieusement endommagée.	2 heures ouvrées, 12 h/24, 7 j/7
Mineur 3	Perte partielle et non critique des fonctionnalités du logiciel.	4 heures ouvrées, 12 h/24, 5 j/7
Superficiel 4	Questions d'utilisation générales.	8 heures ouvrables, 12 h/24, 5 j/7

12-37 Rappel des objectifs de la formation

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

- Définir la portée de la résolution des problèmes
- Utiliser une approche structurée pour résoudre les problèmes de configuration et d'ordre opérationnel
- Appliquer la méthodologie de résolution des problèmes pour diagnostiquer de manière logique les anomalies et améliorer l'efficacité du dépannage

12-38 Points clés

- L'adoption d'une approche structurée en matière de résolution des problèmes vous aide à remédier aux problèmes avec rapidité et efficacité.
- L'établissement d'une distinction entre les symptômes et les problèmes constitue une étape clé du processus de résolution des problèmes.
- Une bonne connaissance préalable du fonctionnement de l'infrastructure virtuelle VMware et de la configuration de votre système se révèle d'une grande utilité dans le cadre du processus de résolution des problèmes.

Avez-vous des questions ?