Guide de disponibilité vSphere

ESX 4.1
ESXi 4.1
vCenter Serveur 4.1

Ce document prend en charge la version de chacun des produits répertoriés, ainsi que toutes les versions publiées par la suite jusqu'au remplacement dudit document par une nouvelle édition. Pour rechercher des éditions plus récentes de ce document, rendez-vous sur : http://www.vmware.com/fr/support/pubs.

FR-000316-00

vmware®

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

http://www.vmware.com/fr/support/pubs/

Le site Web de VMware propose également les dernières mises à jour des produits.

N'hésitez pas à nous transmettre tous vos commentaires concernant cette documentation à l'adresse suivante :

docfeedback@vmware.com

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

VMware, Inc.
100-101 Quartier Boieldieu
92042 Paris La Défense
France
www.vmware.com/fr

Table des matières

À propos de ce guide

Le *Guide de disponibilité vSphere* présente des solutions assurant la continuité d'activité, ainsi que la mise en place de VMware® Haute disponibilité (HA) et de VMware Fault Tolerance.

Public cible

Ce livre est destiné à tous ceux qui veulent assurer la continuité d'activité à l'aide des solutions VMware HA et Tolérance aux pannes. Les informations fournies dans ce livre sont destinées aux administrateurs du système Windows ou Linux expérimentés qui connaissent le fonctionnement de la technologie des machines virtuelles et des centres de données.

Glossaire VMware Technical Publications

VMware Technical Publications fournit un glossaire des termes qui peuvent éventuellement ne pas vous être familiers. Pour consulter la définition des termes utilisés dans la documentation technique VMware, visitez le site Web http://www.vmware.com/support/pubs.

Commentaires sur les documents

VMware prend en considérations vos suggestions pour améliorer sa documentation. Si vous avez des commentaires, envoyez-les à docfeedback@vmware.com

documentation de vSphere

La documentation vSphere® se compose de la combinaison de l'ensemble des documentations de VMware vCenter Server et ESX/ESXi. Le *Guide de disponibilité vSphere* traite d'ESX®, d'ESXi et de vCenter® Server.

Ressources de support technique et de formation

Les ressources de support technique suivantes sont à votre disposition. Pour accéder à la version actuelle de ce guide et à d'autres guides, allez sur http://www.vmware.com/support/pubs.

Support en ligne et téléphonique

Pour soumettre des demandes d'ordre technique à l'assistance en ligne, consulter les informations concernant vos produits et contrats et inscrire vos produits, rendez-vous sur http://www.vmware.com/support.

Les clients ayant souscrit des contrats de support appropriés peuvent utiliser le support téléphonique pour obtenir une réponse rapide à leurs problèmes prioritaires. Allez sur http://www.vmware.com/support/phone_support.html.

Offres de support

Pour en savoir plus sur la façon dont les offres d'assistance VMware peuvent satisfaire les besoins de votre entreprise, rendez-vous sur http://www.vmware.com/support/services.

VMware Professional Services

Les cours VMware Education Services proposent de nombreux exercices pratiques, des exemples d'étude de cas, ainsi que de la documentation destinée à servir de référence sur site. Les cours sont disponibles sur site, en salle de cours et en ligne et en direct. Pour les programmes pilotes sur site et les meilleures pratiques de mise en œuvre, VMware Consulting Services propose des offres destinées à vous aider à évaluer, planifier, élaborer et gérer votre environnement virtuel. Pour accéder aux informations sur les classes de formation, les programmes de certification et les services-conseil, rendez-vous sur http://www.vmware.com/services.

Continuité d'activité et minimisation des interruptions de service 1

Qu'elles soient prévues ou imprévues, les interruptions de service engendrent des coûts considérables. Mais les solutions assurant des niveaux élevés de disponibilité ont toujours été chères et difficiles à implémenter et à gérer.

Les logiciels de VMware assurent facilement et à moindre coût un niveau élevé de disponibilité pour les applications importantes. Avec vSphere, les entreprises peuvent augmenter facilement le niveau de disponibilité de base assuré pour toutes les applications et fournir des niveaux élevés de disponibilité plus facilement et à moindre frais. Avec vSphere, vous pouvez :

- Assurer une disponibilité élevée indépendamment du matériel, du système d'exploitation et des applications.
- Éliminer les interruptions de service prévues pour les opérations de maintenance ordinaires.
- Assurer la restauration automatique en cas de dysfonctionnement.

vSphere permet de réduire les interruptions de service prévues, d'éviter des interruptions de service imprévues et de récupérer rapidement suite à des interruptions.

Ce chapitre aborde les rubriques suivantes :

Réduction des interruptions de service prévues

Les interruptions de service prévues représentent généralement plus de 80 % des interruptions de service d'un centre de données. La maintenance matérielle, la migration des serveurs et les mises à niveau des microprogramme imposent une interruption du service des serveurs physiques. Pour réduire les répercussions de ces interruptions de service, les entreprises doivent reporter la maintenance à des plages horaires peu pratiques et difficiles à planifier.

vSphere permet aux entreprises de réduire considérablement les interruptions de service prévues. Comme les charges de travail d'un environnement vSphere peuvent être déplacées dynamiquement sur différents serveurs physiques sans interruptions de service, la maintenance des serveurs peut être effectuée sans exiger une interruption des applications et du service. Avec vSphere, les entreprises :

- éliminent les interruptions de service pour les opérations de maintenance ordinaires.
- éliminent les plages de maintenance prévues.
- exécutent la maintenance à tout moment sans perturber les utilisateurs et les services.

VMware vMotion® et la fonctionnalité Storage vMotion de vSphere permet aux entreprises de réduire les interruptions de service prévues car les charges de travail d'un environnement VMware peuvent être déplacées dynamiquement sur d'autres serveurs physiques ou sur d'autres stockages sous-jacents sans interruption de service. Les administrateurs peuvent effectuer plus rapidement des opérations de maintenance entièrement transparentes, sans devoir planifier des plages de maintenance peu pratiques.

Prévention les interruptions de service imprévues

Alors qu'un hôte ESX/ESXi constitue une plate-forme stable pour l'exécution d'applications, les entreprises doivent aussi se protéger contre les interruptions de service imprévues provoquées par des défaillances matérielles ou logicielles. vSphere renforce considérablement les capacités des infrastructures des centres de données, ce qui contribue à éviter des interruptions de service imprévues.

Ces capacités vSphere font partie d'une infrastructure virtuelle et sont transparentes pour le système d'exploitation et les applications exécutées sur les machines virtuelles. Ces fonctions peuvent être configurées et utilisées par toutes les machines virtuelles sur un système physique, ce qui réduit le coût et la complexité de la prévision d'une disponibilité supérieure. Les fonctions clés de la tolérance aux pannes sont intégrées à vSphere :

- Stockage partagé. Élimine des points de panne isolés en stockant les fichiers des machines virtuelles dans des espaces de stockage partagés, comme Fibre Channel ou iSCSI SAN, ou encore NAS. Il est possible de faire appel aux fonctions de réplication et de mise en miroir SAN pour conserver les copies mises à niveau des disques virtuels dans des sites de reprise.
- Association d'interfaces réseau. Assure la tolérance aux défaillances des cartes réseau individuelles.
- chemins multiples du stockage. Assure la tolérance aux défaillances des emplacements de stockage.

En outre, les fonctions de VMware HA et Tolérance aux pannes peuvent réduire ou éliminer les interruptions de service imprévues en assurant respectivement la reprise d'activité rapide suite à une interruption et la continuité de la disponibilité.

VMware HA assure une reprise d'activité rapide suite à une interruption

VMware HA a recours à plusieurs hôtes ESX/ESXi configurés en cluster pour assurer une reprise d'activité rapide suite à une interruption et une haute disponibilité à moindres coûts pour les applications exécutées sur des machines virtuelles.

VMware HA protège la disponibilité des applications de manière suivante :

- Il protège contre une défaillance du serveur en redémarrant les machines virtuelles sur d'autres hôtes au sein du cluster.
- Il protège contre les défaillances des applications en surveillant en permanence une machine virtuelle et en la réinitialisant en cas de détection d'une défaillance.

Contrairement aux autres solutions de mise en clusters, VMware HA fournit l'infrastructure nécessaire à la protection de toutes les charges de travail :

- Il n'est pas nécessaire d'installer des logiciels spéciaux dans l'application ou sur la machine virtuelle. Toutes les charges de travail sont protégées par VMware HA. Après la configuration de VMware, aucune action n'est requise pour protéger de nouvelles machines virtuelles. Elles sont protégées automatiquement.
- Vous pouvez associer VMware HA à VMware Distributed Resource Scheduler (DRS) pour assurer la protection contre les pannes, et pour répartir la charge entre tous les hôtes d'un cluster.

VMware HA présente plusieurs avantages face aux solutions de basculement habituelles :

Configuration minimale	Quand un cluster VMware HA a été configuré, toutes les machines virtuelles du cluster sont incluses dans le basculement sans configuration supplémentaire.
Coûts et configuration matérielle réduits	La machine virtuelle fait office de conteneur portable pour les applications et elle peut être déplacée parmi les hôtes. Les administrateurs évitent ainsi de reproduire les configurations sur plusieurs machines. Lorsque vous utilisez VMware HA, vous devez disposer de suffisamment de ressources pour le basculement de tous les hôtes protégés par VMware HA. Toutefois, le système vCenter Server gère automatiquement les ressources et configure les clusters.
Disponibilité accrue des applications	Une application exécutée au sein d'une machine virtuelle a accès à une disponibilité accrue. Comme la machine virtuelle peut récupérer d'une défaillance matérielle, toutes les applications qui démarrent au moment de l'initialisation ont une disponibilité accrue sans accroître la charge de calcul, même si l'application n'est pas en cluster. En surveillant et en répondant aux signaux de pulsation des VMware Tools et en réinitialisant les machines virtuelles qui ne répondent plus, elle assure également une protection contre les défaillances du système d'exploitation client.
Intégration DRS et vMotion	En cas de défaillance d'un hôte et du redémarrage des machines virtuelles sur d'autres hôtes, DRS peut fournir des recommandations de migration ou faire migrer les machines virtuelle en équilibrant les ressources allouées. Si l'hôte source et/ou l'hôte de destination d'une migration sont défaillants, VMware HA peut faciliter la récupération suite à la défaillance.

VMware Fault Tolerance assure la continuité de la disponibilité

VMware HA assure un niveau de protection de base pour vos machines virtuelles en les redémarrant en cas de panne de l'hôte. VMware Fault Tolerance assure un niveau de disponibilité supérieur en permettant aux utilisateurs de protéger les machines virtuelles contre une défaillance de l'hôte sans perte de données, de transactions ou de connexions.

Tolérance aux pannes applique la technologie de VMware vLockstep sur la plate-forme de l'hôte ESX/ESXi pour assurer la continuité de la disponibilité. La continuité de la disponibilité s'effectue en vérifiant que les états des machines virtuelles principales et secondaires demeurent identiques tout au long de l'exécution des instructions de la machine virtuelle. vLockstep s'en assure en faisant exécuter des séquences d'instructions x86 identiques aux machines virtuelles principales et secondaires. La machine virtuelle principale capture les entrées et événements (en provenance du processeur et à destination des périphériques d'E/S virtuels) et les relit sur la machine virtuelle secondaire. La machine virtuelle secondaire exécute les mêmes instructions que la machine virtuelle principale, alors qu'une seule image de machine virtuelle (la machine virtuelle principale) exécute toute la charge de travail.

Si l'hôte exécutant la machine virtuelle principale ou l'hôte exécutant la machine virtuelle secondaire est défaillant, un basculement transparent se produit. L'hôte ESX/ESXi en état de marche devient la machine virtuelle principale sans perte de connexions réseau ou de transactions en cours. Le basculement transparent évite toute perte de données et assure le maintien des connexions réseau. En cas de basculement transparent, une nouvelle machine virtuelle est réaffectée et la redondance est rétablie. Le processus est entièrement transparent et automatisé et se produit même en cas d'indisponibilité du vCenter Server.

Création et utilisation des clusters VMware HA 2

Les clusters VMware HA permettent de réunir plusieurs hôtes ESX/ESXi de façon à ce qu'ils fournissent, en tant que groupes, un niveau de disponibilité supérieur pour les machines virtuelles à celle d'un seul hôte ESX/ESXi. Quand vous prévoyez la création et l'utilisation d'un nouveau VMware HA, les options choisies affectent la manière dont le cluster correspondant réagit aux pannes des hôtes ou des machines virtuelles.

Avant de créer un cluster VMware HA, vous devez savoir comment VMware HA identifie les défaillances et l'isolement de l'hôte et comment il réagit dans ces situations. Vous devez aussi connaître le mode de fonctionnement du contrôle d'admission de façon à être capable de choisir les règles qui répondent le mieux à vos besoins de basculement. Lorsqu'un cluster a été créé, vous pouvez en personnaliser le comportement avec des attributs avancés et en optimiser les performances en suivant les meilleures pratiques recommandées.

Ce chapitre aborde les rubriques suivantes :

Fonctionnement de VMware HA

VMware HA assure la disponibilité élevée des machines virtuelles en les plaçant avec leurs hôtes respectifs dans un cluster. Les hôtes du cluster sont surveillés et, en cas de défaillance, les machines virtuelles d'un hôte défectueux sont redémarrés sur d'autres hôtes.

Hôtes principaux et secondaires d'un cluster VMware HA

Lorsque vous ajoutez un hôte dans un cluster VMware HA, un agent est transféré vers l'hôte et configuré afin de communiquer avec d'autres agents du cluster. Les cinq premiers hôtes ajoutés dans le cluster sont nommés des hôtes principaux et tous les hôtes suivants sont nommés des hôtes secondaires. Les hôtes principaux conservent et copient tous les états du cluster et servent à initier des actions de basculement. Si un hôte principal est supprimé du cluster, VMware HA promeut un autre hôte (secondaire) au rang d'hôte principal. Si un hôte principal va être déconnecté pendant une durée prolongée, supprimez-le du cluster, de façon à pouvoir le remplacer par un hôte secondaire.

Tout hôte rejoignant le cluster doit communiquer avec un hôte principal existant pour achever sa configuration (sauf au moment de l'ajout du premier hôte au cluster). Un hôte principal au moins doit être opérationnel pour le bon fonctionnement de VMware HA. Si tous les hôtes principaux ne sont pas disponibles (sans réaction), aucun hôte ne peut être configuré correctement avec VMware HA. Tenez compte de la limite fixée à cinq hôtes

principaux par cluster lors de la planification de l'étendue du cluster. De plus, si le cluster est implémenté dans un environnement de serveur lame, ne placez pas plus de quatre hôtes principaux sur un seul châssis de lame. Si les cinq hôtes principaux sont dans le même châssis et que celui-ci échoue, votre cluster perd la protection VMware HA.

L'un des hôtes principaux est aussi nommé hôte principal actif. Ses responsabilités sont les suivantes :

- Décision du point de départ du redémarrage des machines virtuelles.
- Suivi des tentatives de redémarrage échouées.
- Choix du moment approprié pour continuer à essayer de redémarrer une machine virtuelle.

Si l'hôte principal actif est défectueux, un autre hôte principal le remplace.

Détection des pannes et isolation du réseau de l'hôte

Les agents communiquent les uns avec les autres et surveillent la réactivité des hôtes du cluster. Cette communication s'effectue par l'échange de signaux de pulsation à un intervalle d'une seconde par défaut. Si 15 secondes passent sans réception de signaux de pulsation de la part d'un hôte et que l'hôte ne peut pas exécuter de ping, il est déclaré défaillant. En cas de défaillance de l'hôte, les machines virtuelles exécutées sur cet hôte sont basculées, c'est-à-dire qu'elles sont redémarrées sur des hôtes de remplacement.

Remarque En cas de défaillance de l'hôte, VMware HA ne bascule pas de machines virtuelles vers un hôte qui est en mode de maintenance.

L'isolation du réseau de l'hôte se produit lorsque l'hôte fonctionne toujours, mais qu'il ne peut plus communiquer avec d'autres hôtes du cluster. D'après les paramètres par défaut, si un hôte cesse de recevoir les signaux de pulsation de tous les autres hôtes du cluster pendant plus de 12 secondes, il tente d'envoyer un ping à ses adresses d'isolation. Si cela échoue aussi, l'hôte se déclare isolé du réseau. Le ping est uniquement envoyé à une adresse d'isolation lorsque les pulsations ne sont plus reçues d'aucun autre hôte du cluster.

Si la connexion réseau de l'hôte isolé n'est pas restaurée au bout de 15 secondes ou davantage, les autres hôtes du cluster considèrent l'hôte isolé comme défectueux et tentent de basculer ses machines virtuelles. Mais lorsqu'un hôte isolé conserve l'accès au stockage partagé, il conserve aussi le verrouillage disque sur les fichiers des machines virtuelles. Pour éviter une corruption potentielle des données, le verrouillage disque VMFS empêche les opérations d'écriture simultanée dans les fichiers disque des machines virtuelles et les tentatives de basculement des machines virtuelles des hôtes isolés échouent. Par défaut, l'hôte isolé arrête ses machines virtuelles, mais il est possible de modifier la réaction d'isolation de l'hôte en optant pour **[Laisser sous tension]** ou **[Mise hors tension]** . Reportez-vous à « Options de machine virtuelle », page 23.

Remarque Si vous vous assurez que l'infrastructure réseau est suffisamment redondante et qu'un chemin d'accès au réseau est disponible en permanence, l'isolation du réseau de l'hôte devrait se produire très rarement.

Utilisation conjointe de VMware HA et DRS

L'utilisation de VMware HA avec Distributed Resource Scheduler (DRS) allie le basculement automatique avec l'équilibrage de charge. Cette combinaison peut aboutir à un rééquilibrage plus rapide des machines virtuelles après leur déplacement sur d'autres hôtes par VMware HA.

Quand VMware HA exécute le basculement et redémarre les machines virtuelles sur des hôtes différents, la première priorité est la disponibilité immédiate de toutes les machines virtuelles. Après le redémarrage des machines virtuelles, les hôtes sur lesquels elles sont exécutées peuvent se retrouver surchargés, tandis que la charge d'autres hôtes est plus légère, en comparaison. VMware HA utilise le CPU et la réservation de mémoire de la machine virtuelle pour déterminer si un hôte dispose de suffisamment de capacité disponible pour prendre en charge la machine virtuelle.

Dans un cluster utilisant DRS et VMware HA avec le contrôle d'admission activé, les machines virtuelles ne sont pas nécessairement évacuées des hôtes passant en mode de maintenance. Ce comportement intervient par suite des ressources réservées pour le redémarrage des machines virtuelles en cas de panne. Il faut migrer manuellement les machines virtuelles en dehors des hôtes avec vMotion.

Dans certains scénarios, VMware HA ne parvient pas à basculer des machines virtuelles par suite de contraintes de ressources. Ceci peut se produire pour plusieurs raisons.

- Le contrôle d'admission HA est désactivé et Gestion de l'alimentation distribuée (DPM) est activé. Cela peut aboutir à la consolidation par DPM des machines virtuelles sur un nombre inférieur d'hôtes et à la mise en veille des hôtes vides, ce qui ne laisse pas suffisamment de réserve de capacité active pour effectuer un basculement.
- Les règles (requises) d'affinité de machine virtuelle/hôte peuvent limiter les hôtes sur lesquels certaines machines virtuelles peuvent être placées.
- Il peut y avoir suffisamment de ressources cumulées mais celles-ci sont fragmentées sur plusieurs hôtes de sorte qu'elles ne peuvent pas être utilisées par les machines virtuelles pour le basculement.

Dans ce cas, VMware HA utilise DRS pour essayer d'ajuster le cluster (par exemple, en sortant les hôtes du mode de veille ou en migrant les machines virtuelles pour défragmenter les ressources du cluster) de sorte que HA puisse exécuter les basculements.

Si DPM est en mode manuel, vous devrez éventuellement confirmer les recommandations de mise sous tension des hôtes. De même, si DPM est en mode manuel, vous devrez éventuellement confirmer les recommandations de migration.

Si vous utilisez les règles d'affinité entre machine virtuelle et hôte requises, sachez que ces règles doivent obligatoirement être respectées. VMware HA n'effectue pas de basculement si cela risque d'enfreindre une règle.

Pour plus d'informations sur DRS, reportez-vous au *Guide de gestion des ressources*.

Contrôle d'admission VMware HA

vCenter Server utilise le contrôle d'admission pour assurer que suffisamment de ressources sont disponibles dans un cluster pour permettre la protection par basculement et pour assurer que les réservations de ressources pour les machines virtuelles sont respectées.

Trois types de contrôle d'admission sont disponibles.

Hôte	Garantit qu'un hôte dispose de suffisamment de ressources pour satisfaire les réservations de toutes les machines virtuelles qui y sont exécutées.
Pool de ressources	Garantit qu'un pool de ressources dispose de suffisamment de ressources pour satisfaire les réservations, les partages et les limites de toutes les machines virtuelles qui y sont associées.
VMware HA	Garantit qu'une part suffisante des ressources du cluster sont réservées à la restauration des machines virtuelles en cas de défaillance de l'hôte.

Le contrôle d'admission impose des contraintes d'utilisation des ressources et toute action contrevenant à ces contraintes n'est pas autorisée. Parmi les exemples d'actions pouvant être interdites, on peut citer :

- Mise sous tension d'une machine virtuelle.
- Migration d'une machine virtuelle sur un hôte ou dans un cluster ou un pool de ressources.
- Augmentation de la réservation de CPU ou de mémoire d'une machine virtuelle.

Parmi les trois types de contrôle d'admission, seul le contrôle d'admission VMware HA peut être désactivé. Mais sans ce contrôle, il n'est pas possible d'assurer que toutes les machines virtuelles du cluster peuvent être redémarrées après une défaillance d'hôte. VMware déconseille de mettre hors tension le contrôle d'admission, mais vous pouvez avoir besoin de le faire temporairement pour les raisons suivantes :

- Si vous devez enfreindre les contraintes de basculement lorsqu'il n'y a pas suffisamment de ressources pour les prendre en charge (par exemple, si vous mettez les hôtes en veille pour en tester le fonctionnement avec DPM).
- Si un processus automatisé doit effectuer des actions qui risquent d'enfreindre temporairement les contraintes de basculement (par exemple, dans le cadre d'une mise à niveau dirigée par VMware Update Manager).
- Si vous devez exécuter des tests ou des opérations de maintenance.

Règles de contrôle d'admission Défaillances d'hôte tolérées par le cluster

Vous pouvez configurer VMware HA pour tolérer un nombre spécifié de défaillances d'hôtes. Avec les règles de contrôle d'admission Défaillances d'hôte tolérées par le cluster, VMware HA s'assure que même si un nombre d'hôtes spécifié est défectueux, les ressources demeurent en quantité suffisante sur le cluster pour le basculement de toutes les machines virtuelles de ces hôtes.

Avec les règles Défaillances d'hôte tolérées par le cluster, VMware HA effectue le contrôle d'admission de la manière suivante :

1 Calcule la taille du slot.

   Un slot est une représentation logique de la mémoire et des ressources CPU. Par défaut, il est dimensionné pour satisfaire aux exigences de chaque machine virtuelle sous tension dans le cluster.

2 Détermine le nombre de slots pouvant se trouver sur chaque hôte du cluster.

3 Détermine la Capacité de basculement actuelle du cluster.

   Il s'agit du nombre d'hôtes défectueux permettant de conserver un nombre suffisant de slots pour satisfaire toutes les machines virtuelles sous tension.

4 Détermine si la Capacité de basculement actuelle est inférieure ou non à la Capacité de basculement configurée (précisée par l'utilisateur).

   Si c'est le cas, le contrôle d'admission n'autorise pas l'opération.

Remarque La Capacité maximale de basculement configurée pouvant être définie est limitée à quatre. Chaque cluster contient jusqu'à cinq hôtes principaux et s'ils tombent tous en panne simultanément, le basculement de toutes les machines virtuelles risque d'échouer.

Calcul de la taille du slot

La taille d'un slot est déterminée par deux composants, la CPU et la mémoire.

- VMware HA calcule la taille de CPU à partir de la CPU réservée par chaque machine virtuelle sous tension, en sélectionnant la valeur la plus élevée. Si aucune CPU n'a été réservée pour une machine virtuelle, une valeur de 256 MHz est définie par défaut. Cette valeur peut être modifiée par l'attribut avancé das.vmcpuminmhz.)
- VMware HA calcule la taille du composant de mémoire à partir de la mémoire réservée (plus la capacité supplémentaire de mémoire) de chaque machine virtuelle sous tension, en sélectionnant la valeur la plus élevée. Il n'y a pas de valeur par défaut pour la mémoire réservée.

Si le cluster contient des machines virtuelles ayant des valeurs de réservation bien plus élevées que d'autres, celles-ci influeront sur le calcul de la taille du slot. Pour l'éviter, vous pouvez préciser une limite supérieure pour la CPU ou le composant de mémoire de la taille du slot en utilisant respectivement les attributs avancés das.slotcpuinmhz ou das.slotmeminmb.

Utilisation des slots pour déterminer la capacité de basculement actuelle

Une fois la taille du slot calculée, VMware HA détermine les ressources de CPU et de mémoire disponibles sur chaque hôte pour les machines virtuelles. Ces valeurs sont contenues dans le pool de ressources racine de l'hôte, et non dans les ressources physiques totales de l'hôte. Les ressources utilisées à des fins de virtualisation ne sont pas incluses. Seuls les hôtes qui sont connectés, qui ne sont pas en mode de maintenance et qui ne présentent pas d'erreurs VMware HA sont pris en compte.

Le nombre maximum de slots pouvant être pris en charge par chaque hôte est alors déterminé. À cette fin, la quantité de ressources CPU de l'hôte est divisée par le composant de CPU de la taille de slot et le résultat est arrondi. Le même calcul est fait pour la quantité de ressources de mémoire de l'hôte. Ces deux valeurs sont comparées et la plus basse équivaut au nombre de slots pouvant être pris en charge par l'hôte.

La Capacité de basculement actuelle est calculée en déterminant le nombre d'hôtes (en commençant par le plus gros) pouvant être défectueux tout en conservant un nombre suffisant de slots pour satisfaire toutes les machines virtuelles sous tension.

Informations d'exécution avancées

Lorsque vous sélectionnez les règles de contrôle d'admission Défaillances d'hôte tolérées par le cluster, le lien **[Informations d'exécution avancées]** apparaît dans la rubrique VMware HA de l'onglet **[Résumé]** du cluster dans vSphere Client. Cliquez sur ce lien pour afficher les informations suivantes à propos du cluster :

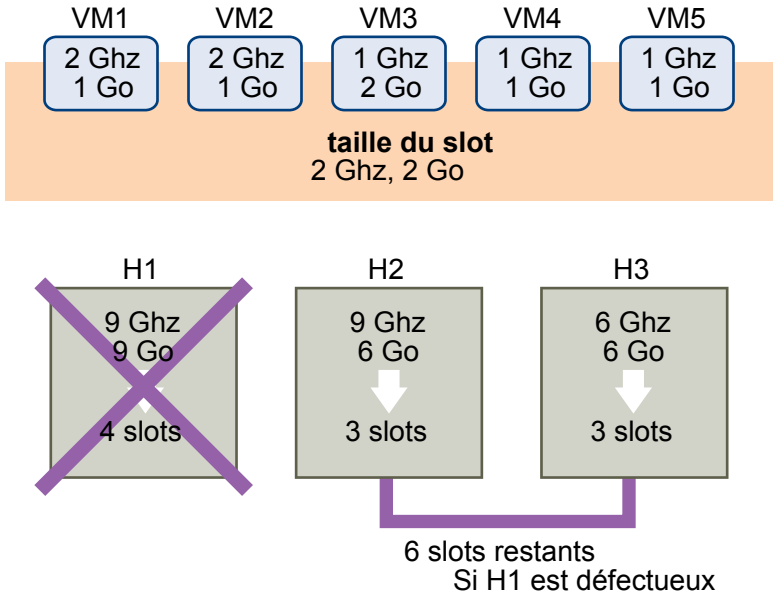
- Taille du slot.
- Nombre total de slots dans le cluster. Somme des slots pris en charge par les hôtes en état de marche dans le cluster.
- Slots utilisés. Nombre de slots associés aux machines virtuelles sous tension. Ce nombre peut être supérieur au nombre de machines virtuelles sous tension si vous avez défini une limite supérieure pour la taille du slot au moyen des options avancées. Ceci parce que quelques machines virtuelles peuvent occuper plusieurs slots.
- Slots disponibles Nombre de slots disponibles pour mettre sous tension des machines virtuelles supplémentaires dans le cluster. VMware HA réservation le nombre de slots requis par le basculement. Les slots restants sont disponibles pour mettre sous tension de nouvelles machines virtuelles.
- Nombre total de machines virtuelles sous tension dans le cluster.
- Nombre total d'hôtes dans le cluster.
- Nombre total d'hôtes en marche dans le cluster. Nombre d'hôtes qui sont connectés, qui ne sont pas en mode de maintenance et qui ne présentent pas d'erreurs VMware HA.

Exemple 2-1. Règles de contrôle d'admission Défaillances d'hôte tolérées par le cluster

Nous allons illustrer par un exemple le mode de calcul de la taille de slot et son utilisation avec cette règle de contrôle d'admission. Effectuons les suppositions suivantes à propos d'un cluster :

- Le cluster est composé de trois hôtes, ayant chacun des quantités différentes de CPU et de ressources mémoire disponibles. Le premier hôte (H1) a 9 Ghz de ressources CPU et 9 Go de mémoire disponibles. Le second (H2) a 9 Ghz de CPU et 6 Go de mémoire disponibles et le troisième (H3) a 6 Ghz de CPU et 6 Go de mémoire disponibles.
- Il y a cinq machines virtuelles sous tension dans le cluster avec des besoins en CPU et en mémoire différents. VM1 a besoin de 2 Ghz de ressources CPU et 1 Go de mémoire, tandis que VM2 utilise 2 Ghz et 1 Go VM3 a besoin de 1 Ghz et de 2 Go, VM4 exige 1 Ghz et 1 Go, VM5 nécessite 1 Ghz et 1 Go.
- Défaillances d'hôte tolérées par le cluster sont définies sur la valeur 1.

Figure 2-1. Exemple de contrôle d'admission avec des règles de Défaillances d'hôte tolérées par le cluster



1 La taille du slot est calculée en comparant à la fois les exigences de CPU et de mémoire des machines virtuelles et en sélectionnant la plus élevée.

   Le besoin en CPU le plus élevé (partagé par VM1 et VM2) est de 2 Ghz, tandis que le besoin en mémoire le plus élevé (VM3) est de 2 Go. Partant de là, la taille du slot se compose d'une CPU de 2 Ghz et d'une mémoire de 2 Go.

2 Le nombre maximum de slots pouvant être pris en charge par chaque hôte est déterminé.

   H1 peut prendre en charge quatre slots. H2 peut prendre en charge trois slots (le plus bas de 9 Ghz/2 Ghz et 6 Go/2 Go) et H3 peut aussi en prendre en charge trois.

3 La Capacité de basculement actuelle est calculée.

   Le plus gros hôte est H1 et s'il est défectueux, le cluster contient toujours six slots, ce qui est suffisant pour les cinq machines virtuelles sous tension. Si H1 et H2 sont défectueux, il ne reste que trois slots, ce qui est insuffisant. Par conséquent, la Capacité de basculement actuelle est de 1.

Le cluster a un slot disponible (les six slots de H2 et H3 moins les cinq slots utilisés).

Règles de contrôle d'admission Pourcentage de ressources de cluster réservées

Il est possible de configurer VMware HA pour effectuer le contrôle d'admission en réservant un pourcentage spécifique de ressources de cluster à la récupération en cas de pannes d'hôte.

Avec les règles de contrôle d'admission Pourcentage de ressources de cluster réservées, VMware HA assure qu'un pourcentage spécifié de ressources de cluster cumulées est réservé au basculement.

VMware HA effectue le contrôle d'admission conformément aux règles de Ressources de cluster réservées.

1 Calcul des besoins totaux en ressources pour toutes les machines virtuelles sous tension dans le cluster.

2 Calcul les ressources totales de l'hôte disponibles pour les machines virtuelles.

3 Calcul la Capacité CPU de basculement actuelle et la Capacité mémoire de basculement actuelle du cluster.

4 Détermine si la Capacité CPU de basculement actuelle est inférieure ou non à la Capacité de basculement configurée (spécifiqueée par l'utilisateur).

   Si c'est le cas, le contrôle d'admission n'autorise pas l'opération.

VMware HA utilise les réservations effectives des machines virtuelles. Si une machine virtuelle n'a pas de réservations, c'est-à-dire que la valeur de réservation est nulle, alors 0 Mo de mémoire par défaut et 256 MHz de CPU sont appliqués.

Calcul de la Capacité de basculement actuelle

Les besoins totaux en ressources des machines virtuelles sous tension sont composés de deux composants, CPU et mémoire. VMware HA calcule ces valeurs.

- Le besoin en composant CPU est obtenu en additionnant la CPU réservée par les machines virtuelles sous tension. Si aucune CPU n'a été réservée pour une machine virtuelle, une valeur de 256 MHz est définie par défaut (cette valeur peut être modifiée par l'attribut avancé das.vmcpuminmhz).
- La taille du composant de mémoire est obtenue en additionnant la mémoire réservée (plus la capacité supplémentaire de mémoire) de chaque machine virtuelle sous tension.

Les ressources totales des hôtes disponibles pour les machines virtuelles sont calculées en additionnant les ressources de CPU et de mémoire des hôtes. Ces valeurs sont contenues dans le pool de ressources racine de l'hôte, et non dans les ressources physiques totales de l'hôte. Les ressources utilisées à des fins de virtualisation ne sont pas incluses. Seuls les hôtes qui sont connectés, qui ne sont pas en mode de maintenance et qui ne présentent pas d'erreurs VMware HA sont pris en compte.

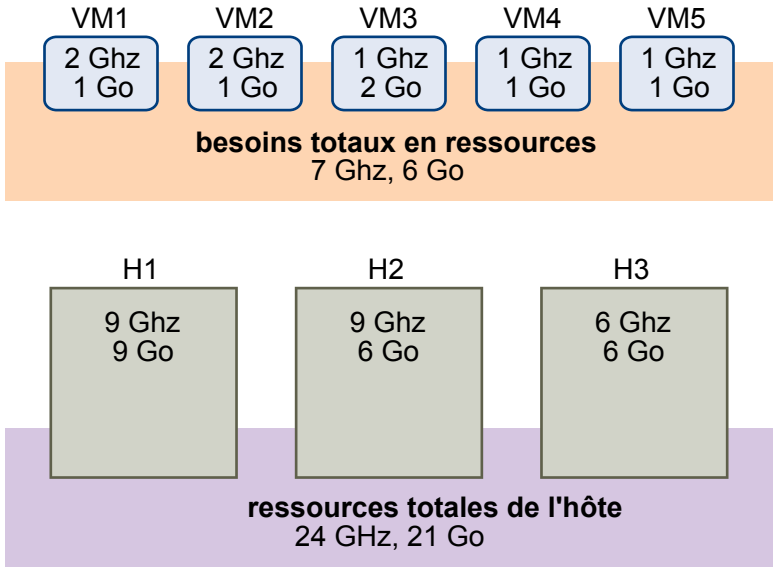
La Capacité CPU de basculement actuelle est calculée en soustrayant les besoins totaux en ressources CPU des ressources CPU totales des hôtes et en divisant le résultat par les ressources CPU totales des hôtes. La Capacité mémoire de basculement actuelle est calculée de la même manière.

Exemple 2-2. Règles de contrôle d'admission Pourcentage de ressources de cluster réservées

Nous allons illustrer par un exemple le mode de calcul de la Capacité de basculement actuelle et son utilisation avec cette règle de contrôle d'admission. Effectuons les suppositions suivantes à propos d'un cluster :

- Le cluster est composé de trois hôtes, ayant chacun des quantités différentes de CPU et de ressources mémoire disponibles. Le premier hôte (H1) a 9 Ghz de ressources CPU et 9 Go de mémoire disponibles. Le second (H2) a 9 GHz de CPU et 6 Go de mémoire disponibles et le troisième (H3) a 6 GHz de CPU et 6 Go de mémoire disponibles.
- Il y a cinq machines virtuelles sous tension dans le cluster avec des besoins en CPU et en mémoire différents. VM1 a besoin de 2 Ghz de ressources CPU et 1 Go de mémoire, tandis que VM2 utilise 2 Ghz et 1 Go, VM3 a besoin de 1 Ghz et de 2 Go, VM4 exige 1 Ghz et 1 Go, VM5 nécessite 1 GHz et 1 Go.
- La Capacité de basculement configurée est de 25 %.

Figure 2-2. Exemple de contrôle d'admission utilisant les règles de Pourcentage de ressources de cluster réservées



Les besoins totaux en ressources des machines virtuelles sous tension sont de 7 Ghz et 6 Go. Les ressources totales de l'hôte disponibles pour les machines virtuelles sont de 24 Ghz et 21 Go. Partant de là, la Capacité CPU de basculement actuelle s'élève à 70% ((24 Ghz - 7 Ghz)/24 Ghz). De même, la Capacité mémoire de basculement actuelle s'élève à 71% ((21 Go - -6 Go)/21 Go).

Comme la Capacité de basculement configurée pour le cluster est de 25 %, 45 % des ressources CPU totales du cluster et 46 % des ressources mémoire totales du cluster sont toujours disponibles pour les machines virtuelles supplémentaires.

Règles de contrôle d'admission Spécifier un hôte de basculement

Il est possible de configurer VMware HA afin de désigner un hôte spécifique comme hôte du basculement.

En cas de défaillance d'un hôte, les règles de contrôle d'admission Spécifier un hôte de basculement prévoient que VMware HA tente de redémarrer ses machines virtuelles sur un hôte de basculement prédéfini. Si ce n'est pas possible car l'hôte de basculement est lui-même en panne ou ses ressources sont insuffisantes, par exemple, VMware HA tente de redémarrer ces machines virtuelles sur d'autres hôtes du cluster.

Pour s'assurer que des capacités restent disponibles sur l'hôte de basculement, il n'est pas possible de mettre sous tension des machines virtuelles ou d'utiliser vMotion pour faire migrer des machines virtuelles vers l'hôte de basculement. De plus, DRS n'utilise pas l'hôte de basculement pour la répartition de la charge.

L'hôte de basculement actuel apparaît dans la section VMware HA de l'onglet **[Résumé]** du cluster dans vSphere Client. L'icône de statut qui se trouve à côté de l'hôte peut être verte, jaune ou rouge.

- Vert. L'hôte est connecté, il n'est pas en mode de maintenance et ne présente pas d'erreurs VMware HA. Aucune machine virtuelle sous tension ne réside sur l'hôte.
- Jaune. L'hôte est connecté, il n'est pas en mode de maintenance et ne présente pas d'erreurs VMware HA. Mais des machines virtuelles sous tension résident sur l'hôte.
- Rouge. L'hôte est déconnecté, il est en mode de maintenance ou présente des erreurs VMware HA.

Choix d'une règle de contrôle d'admission

Les règles de contrôle d'admission VMware HA doivent être choisies en fonction des besoins de disponibilité et des caractéristiques du cluster. Différents critères doivent être pris en compte lors du choix de règles de contrôle d'admission.

Éviter la fragmentation des ressources

La fragmentation des ressources se produit lorsqu'il y a suffisamment de ressources cumulées pour le basculement d'une machine virtuelle. Toutefois, ces ressources sont réparties sur plusieurs hôtes et sont inutilisables car une machine virtuelle peut uniquement être exécutée sur un seul hôte ESX/ESXi à la fois. Les règles de Défaillances d'hôte tolérées par le cluster évitent la fragmentation des ressources en définissant un slot comme réservation maximale des machines virtuelles. Les règles de Pourcentage de ressources de clusters ne traitent pas du problème de la fragmentation des ressources. Les règles Spécifier un hôte de basculement n'entraînent pas la fragmentation des ressources car un seul hôte est réservé au basculement.

Flexibilité de la réservation des ressources de basculement

Les règles de contrôle d'admission diffèrent de part la granularité qu'elles accordent au moment de la réservation des ressources du cluster pour la protection du basculement. Les règles de Défaillances d'hôte tolérées par le cluster permettent de définir le niveau de basculement d'un à quatre hôtes. Les règles de Pourcentage de ressources de cluster permettent de définir jusqu'à 50 % de ressources du cluster pour le basculement. Les règles Spécifier un hôte de basculement autorisent uniquement la spécification d'un seul hôte de basculement.

Hétérogénéité des clusters

Les clusters peuvent être hétérogènes en termes de réservations des ressources des machines virtuelles et de capacités des ressources totales des hôtes. Dans un cluster hétérogène, les règles de Défaillances d'hôte tolérées par le cluster peuvent être insuffisantes puis qu'elles tiennent uniquement compte des plus grosses réservations de machines virtuelles lors de la définition de la taille du slot et qu'elles envisagent uniquement la défaillance du plus gros hôte lors de l'estimation de la Capacité de basculement actuelle. Les deux autres règles de contrôle d'admission ne sont pas affectées par l'hétérogénéité des clusters.

Remarque VMware HA tient compte de l'utilisation des ressources des machines virtuelles pour la tolérance aux pannes dans les calculs de contrôle d'admission. Les règles de Défaillances d'hôte tolérées par le cluster veulent qu'un slot soit affecté à une machine virtuelle secondaire, tandis que les règles de Pourcentage de ressources de clusters prévoient que l'utilisation des ressources des machines virtuelles secondaires soit prise en compte lors de l'évaluation de l'utilisation des ressources du cluster.

Liste de vérification VMware HA

La liste de vérification VMware HA contient les exigences que vous devez connaître avant de créer et d'utiliser un cluster VMware HA.

Exigences applicables à un cluster VMware HA

Consultez cette liste avant de configurer un cluster VMware HA. Pour plus d'informations, suivez les références croisées appropriées ou consultez « Création d'un cluster VMware HA », page 20.

- Tous les hôtes doivent disposer d'une licence pour VMware HA.
- Le cluster doit contenir deux hôtes au minimum.
- Tous les hôtes doivent avoir un nom d'hôte unique.
- Tous les hôtes doivent être configurés avec des adresses IP statiques. Si vous utilisez DHCP, vérifiez que l'adresse de chaque hôte est conservée après les redémarrages.
- Tous les hôtes doivent avoir accès aux mêmes réseaux de gestion. Il doit au moins y avoir un réseau de gestion commun parmi tous les hôtes et il est recommandé d'avoir au moins deux réseaux de gestion communs. Les réseaux de gestion diffèrent selon la version de l'hôte que vous utilisez.
  - Hôtes ESX - réseau de la console du service.
  - Hôtes ESXi antérieurs à la version 4.0 - Réseau VMkernel.
  - Hôtes ESXi version 4.0 et ultérieure - Réseau VMkernel et case à cocher activée **[Réseau de gestion]** .

  Reportez-vous à « Meilleures pratiques de mise en réseau », page 29.
- Pour vous assurer que toutes les machines virtuelles peuvent être exécutées sur n'importe quel hôte du cluster, tous les hôtes doivent avoir accès aux même réseaux et banques de sonnées de machines virtuelles. De même, les machines virtuelles doivent se trouver sur des stockages partagés, et non locaux, sinon il ne peut pas y avoir de basculement en cas de défaillance de l'hôte.
- Le fonctionnement de surveillance des machines virtuelles nécessite l'installation des outils VMware. Reportez-vous à « Surveillance MV et application », page 25.
- DNS doit être configuré pour tous les hôtes d'un cluster VMware HA de façon à ce que des noms d'hôte courts (sans suffixe de domaine) de tous les hôtes du cluster puissent être résolus avec l'adresse IP appropriées à partir de n'importe quel hôte du cluster. Sinon, la tâche de Configuration de HA risque d'échouer. Si vous ajoutez l'hôte à l'aide de l'adresse IP, activez aussi la recherche DNS inversée (l'adresse IP doit pouvoir être résolue en nom d'hôte court).

Remarque VMware HA ne prend pas en charge IPv6

Création d'un cluster VMware HA

VMware HA fonctionne dans le cadre d'un cluster d'hôtes ESX/ESXi. Vous devez créer un cluster, le remplir d'hôtes et configurer les paramètres VMware HA avant de pouvoir établir la protection du basculement.

Lorsque vous créez un cluster VMware HA, vous devez configurer divers paramètres qui déterminent la mise en œuvre de la fonction. Avant de commencer, identifiez les nœuds du cluster. Ces noeuds sont les hôtes ESX/ESXi qui fourniront les ressources pour la prise en charge des machines virtuelles et qui seront utilisés par VMware HA pour la protection du basculement. Déterminez ensuite la manière dont ces nœuds doivent être reliés les uns aux autres et au stockage partagé où résident les données de la machine virtuelle. Lorsque l'architecture de la mise en réseau est en place, vous pouvez ajouter les hôtes au cluster et terminer de configurer VMware HA.

Vous pouvez activer et configurer VMware HA avant d'ajouter des nœuds d'hôtes au cluster. Toutefois, tant que les hôtes n'ont pas été ajoutés, le cluster n'est pas entièrement opérationnel et quelques paramètres du cluster ne sont pas disponibles. Par exemple, les règles de contrôle d'admission Spécifier un hôte de basculement ne sont pas disponibles tant qu'un hôte n'a pas été défini comme hôte de basculement.

Remarque La fonction de démarrage et d'arrêt de machine virtuelle (démarrage automatique) est désactivée pour toutes les machines virtuelles résidant sur des hôtes qui se trouvent dans un cluster VMware HA (ou qui y ont été placées). VMware recommande de ne pas réactiver manuellement ce paramètre pour l'une des machines virtuelles. Cela risque d'interférer avec les actions des fonctions du cluster, comme VMware HA ou Tolérance aux pannes.

Créer un cluster VMware HA

Votre cluster peut être activé pour VMware HA. Un cluster avec VMware HA est une condition préalable pour la tolérance aux pannes. VMware recommande de commencer par créer un cluster vide. Après avoir planifié les ressources et l'architecture réseau du cluster, vous pouvez utiliser vSphere Client pour ajouter des hôtes au cluster et définir les paramètres VMware HA du cluster.

Connectez vSphere Client à vCenter Server en utilisant un compte ayant des droits d'accès administrateur au cluster.

Prérequis

Vérifiez que toutes les machines virtuelles et leurs fichiers de configuration résident sur des stockages partagés. Vérifiez que les hôtes sont configurés pour accéder à ce stockage partagé, afin de pouvoir mettre sous tension les machines virtuelles à l'aide de différents hôtes dans le cluster.

Vérifiez que chaque hôte d'un cluster VMware HA possède un nom d'hôte (de 26 caractères au maximum) attribué attribué et une adresse IP statique associée à chacune des cartes réseau virtuelles.

Vérifiez que les hôtes sont configurés pour avoir accès au réseau de machines virtuelles.

Remarque VMware recommande des connexions réseau de gestion redondantes pour VMware HA. Pour plus d'informations sur la configuration d'un réseau redondant, consultez la rubrique« Redondance des chemins d'accès de réseau », page 30.

Procédure

1 Sélectionnez les vues {[Hôtes & Clusters]}.

2 Cliquez avec le bouton droit sur le centre de données dans l'arborescence d'inventaire d'inventaire d'inventaire et sélectionnez **[Nouveau cluster]** .

3 Complétez le paramètre de l'assistant Nouveau cluster.

N'activez pas VMware HA (ou DRS) à ce moment.

4 Cliquez sur **[Terminer]** pour fermer l'assistant et créer le cluster.

Vous avez créé un cluster vide.

5 Utilisez vSphere Client pour ajouter des hôtes au cluster en vous référant à la planification des ressources et de l'architecture réseau du cluster.

6 Cliquez avec le bouton droit sur le cluster et sélectionnez **[Modifier les paramètres]** .

La boîte de dialogue Paramètres du cluster permet de modifier les paramètres de VMware HA (et autres) pour le cluster.

7 Sélectionnez **[Allumer VMware HA]** sur la page des fonctions de cluster.

8 Configurez les paramètres VMware HA comme il convient pour le cluster.

- État de surveillance d'hôte
- Contrôle d'admission
- Options de machine virtuelle
- Surveillance de VM

9 Cliquez sur **[OK]** pour fermer la boîte de dialogue Paramètres du cluster.

Vous avez maintenant un cluster VMware HA disponible, rempli avec des hôtes.

Fonctions de cluster

Le premier panneau de l'assistant Nouveau cluster permet de définir les options de base du cluster.

Ce panneau permet de nommer le cluster et de choisir une ou deux fonctions de cluster.

Nom	Nommez le cluster. Ce nom figure dans le panneau d'inventaire de vSphere Client. Vous devez saisir un nom pour continuer à créer le cluster.
Allumer VMware HA	Lorsque cette case à cocher est sélectionnée, les machines virtuelles redémarrent sur un autre hôte du cluster en cas de dysfonctionnement d'un hôte. Vous devez allumer VMware HA pour activer VMware Fault Tolerance sur n'importe quelle machine virtuelle du cluster.
Allumer VMware DRS	Si cette case à cocher est sélectionnée, DRS répartit la charge des machines virtuelle à travers le cluster. DRS place et migre également les machines virtuelles lorsqu'elles sont protégées par HA.

Vous pouvez modifier ces fonctions de cluster ultérieurement.

État de surveillance d'hôte

Après avoir créé un cluster, activez la surveillance d'hôte de façon à ce que VMware HA puisse surveiller les pulsations émises par l'agent VMware HA sur chaque hôte dans le cluster.

Quand **[Activer la surveillance de l'hôte]** est sélectionné, chaque hôte ESX/ESXi du cluster est surveillé pour s'assurer de son bon fonctionnement. En cas de défaillance d'un hôte, les machines virtuelles sont redémarrées sur un autre hôte. La surveillance d'hôte est aussi requise pour le bon fonctionnement du processus de récupération VMware Fault Tolerance.

Remarque Si vous devez effectuer des opérations de maintenance réseau risquant de déclencher des réactions d'isolation des hôtes, VMware vous recommande de suspendre préalablement VMware HA en désactivant la surveillance d'hôte. Lorsque la maintenance est terminée, activez à nouveau la surveillance d'hôte.

Activation ou désactivation du contrôle d'admission

L'assistant Nouveau cluster permet d'activer ou de mettre hors tension le contrôle d'admission pour le cluster VMware HA et de choisir les règles d'application.

Il est possible d'activer ou de mettre hors tension le contrôle d'admission pour le cluster HA.

Activer : Ne mettez pas sous tension les machines virtuelles qui violent les contraintes de disponibilité	Active le contrôle d'admission, applique des contraintes de disponibilité et conserve la capacité de basculement. Il est interdit d'effectuer sur une machine virtuelle toute opération qui réduit les ressources non réservées dans le cluster et qui enfreint les contraintes de disponibilité.
Désactiver : Mettez sous tension les machines virtuelles qui violent les contraintes de disponibilité	Désactive le contrôle d'admission Les machines virtuelles peuvent, par exemple, être mises sous tension même si cela aboutit à une capacité de basculement insuffisante. Lorsque vous faites cela, aucun avertissement n'est présenté et le cluster ne devient pas rouge. Si un cluster a une capacité de basculement insuffisante, VMware HA peut continuer à effectuer des basculements et il utilise le paramètre de priorité de redémarrage de la machine virtuelle pour préciser quelles machines virtuelles doivent être mise sous tension les premières.

VMware HA prévoit trois règles d'application du contrôle d'admission en cas d'activation.

- Défaillances d'hôte que le cluster tolère
- Pourcentage des ressources de cluster réservées en tant que capacité de basculement de secours
- Spécifier un hôte de basculement

Remarque Voir « Choix d'une règle de contrôle d'admission », page 19 pour plus d'informations sur le fonctionnement du contrôle d'admission VMware HA.

Options de machine virtuelle

Les paramètres par défaut des machines virtuelles contrôlent l'ordre dans lequel les machines virtuelles sont redémarrées (priorité de redémarrage VM), ainsi que la réponse de VMware HA lorsque des hôtes ne sont plus reliés par réseau à d'autres hôtes (réponse d'isolation de l'hôte).

Ces paramètres s'appliquent à toutes les machines virtuelles du cluster en cas de défaillance des hôtes ou d'isolation. Vous pouvez configurer des exceptions pour des machines virtuelles spécifiques. Reportez-vous à « Personnaliser le comportement de VMware HA pour une machine virtuelle », page 28.

Paramètre de priorité de redémarrage des machines virtuelles

La priorité de redémarrage des machines virtuelles détermine l'ordre relatif de redémarrage des machines virtuelles en cas d'échec de l'hôte. Les machines virtuelles sont redémarrées successivement sur leurs nouveaux hôtes, les machines virtuelles ayant la priorité la plus élevée commencent, et vient le tour de celles ayant une priorité inférieure, jusqu'à ce que toutes les machines virtuelles aient redémarré ou qu'il n'y ait plus de ressources de cluster disponibles. Si le nombre de défaillances d'hôtes dépasse le seuil autorisé par le contrôle d'admission, les machines virtuelles ayant une priorité inférieure risquent de ne pas redémarrer tant que davantage de ressources ne sont pas disponibles. Les machines virtuelles sont redémarrées sur l'hôte de basculement, s'il a été préalablement défini.

Les valeurs de ce paramètre sont les suivantes : Désactivé, Basse, Moyen (par défaut) et Haut. Si Désactivé est sélectionné, VMware HA est désactivé pour la machine virtuelle, ce qui signifie qu'elle n'est pas redémarrée sur d'autres hôtes ESX/ESXi en cas de dysfonctionnement de son hôte ESX/ESXi. La sélection de Désactivé n'affecte pas la surveillance des machines virtuelles. Par conséquent, si une machine virtuelle est défaillante sur un hôte qui fonctionne correctement, cette machine virtuelle est réinitialisée sur le même hôte. Vous pouvez modifier ce paramètre pour des machines virtuelles individuelles.

Les paramètres de priorité du redémarrage des machines virtuelles varient en fonction des besoins de l'utilisateur. VMware vous recommande d'associer une priorité de redémarrage élevée aux machines virtuelles qui fournissent les services les plus importants.

Par exemple, dans le cas d'une application multitâche, vous pouvez classer les attributions d'après des fonctions hébergées sur les machines virtuelles.

- Haute. Serveurs de base de données qui fournissent des données aux applications.
- Moyenne. Serveurs d'application qui exploitent les données de la base de données et fournissent des résultats sur des pages web.
- Basse. Serveurs Web qui reçoivent des demandes d'utilisateurs, transmettent des requêtes à des serveurs d'application et transmettent les résultats aux utilisateurs.

Paramètre de réponse d'isolation de l'hôte

La réponse d'isolation de l'hôte détermine les événements survenant lorsqu'un hôte dans un cluster VMware HA perd ses connexions réseau de gestion mais poursuit son exécution. Les réponses d'isolation des hôtes exigent que l'État de surveillance d'hôte soit activé. Si l'état de surveillance d'hôte est désactivé, les réponses d'isolation des hôtes sont également suspendues. Un hôte détermine qu'il est isolé lorsqu'il cesse de recevoir des heartbeats de tous les autres hôtes et qu'il est incapable d'envoyer un ping à des adresses d'isolation. Lorsque cela se produit, l'hôte exécute sa réponse d'isolation. Les réponses sont les suivantes : Laisser sous tension, Mettre hors tension et Arrêter (par défaut). Vous pouvez personnaliser cette propriété pour des machines virtuelles individuelles.

Pour utiliser le paramètre Arrêter la machine virtuelle, vous devez installer VMware Tools dans le système d'exploitation client de la machine virtuelle. L'arrêt de la machine virtuelle offre l'avantage de conserver son état. L'arrêt est préférable à la mise hors tension de mise hors tension de machine virtuelle qui ne purge pas les dernières modifications apportées aux disques ni ne valide les transactions. Le basculement des machines virtuelles qui sont éteintes est plus long car l'arrêt doit aussi être effectué. Les machines virtuelles qui n'ont pas été arrêtées au bout de 300 secondes ou du délai défini par l'attribut avancé das.isolationshutdowntimeout seconds, sont mises hors tension.

Remarque Lorsque vous avez créé un cluster VMware HA, vous pouvez remplacer les paramètres par défaut du cluster relatifs à la Priorité de redémarrage et à la Réponse d'isolation pour les machines virtuelles spécifiques. Ces remplacements sont utiles pour les machines virtuelles qui sont utilisées pour les tâches spéciales. Par exemple, les machines virtuelles qui fournissent des services d'infrastructure, comme DNS ou DHCP, doivent éventuellement être mises sous tension avant d'autres machines virtuelles du cluster.

Surveillance MV et application

Surveillance de VM redémarre les machines virtuelles si leurs heartbeats VMware Tools n'ont pas été reçus pendant une certaine période. De même, la Surveillance d'application peut redémarrer une machine virtuelle si les heartbeats d'une application exécutée ne sont pas reçus. Il est possible d'activer ces fonctions et de configurer la sensibilité de la surveillance de l'absence de réaction par VMware HA.

Lorsque vous activez Surveillance de VM, le service Surveillance de VM (utilisant VMware Tools) vérifie si chaque machine virtuelle du cluster fonctionne en contrôlant les pulsations régulières et l'activité d'E/S du processus VMware Tools exécuté sur le client. Si aucune pulsation ou activité d'E/S n'est reçue, c'est probablement parce que le système d'exploitation client est défectueux ou que les VMware Tools n'ont pas eu le temps de terminer les tâches. Dans ce cas, le service Surveillance de VM détermine que la machine virtuelle est défectueuse et la machine virtuelle redémarre pour être remise en service.

Occasionnellement, les machines virtuelles ou les applications qui continuent à fonctionner correctement cessent d'émettre des heartbeats. Pour éviter les réinitialisations superflues, le service Surveillance de VM surveille aussi l'activité d'E/S d'une machine virtuelle. Si aucun heartbeat n'est reçu pendant la période de défaillance, l'intervalles statistique d'E/S (un attribut défini au niveau du cluster) est vérifié. L'intervalle statistique d'E/S détermine si un disque ou une activité réseau s'est produite pour la machine virtuelle au cours des deux minutes (120 secondes) passées. Si ce n'est pas le cas, la machine virtuelle est réinitialisée. Cette valeur par défaut (120 secondes) peut être modifiée à l'aide de l'attribut avancé das.iostatsinterval.

Pour activer la surveillance d'application, il faut d'abord obtenir le SDK approprié (ou utiliser une application qui prend en charge la surveillance de l'application VMware) et l'utiliser pour configurer des pulsations personnalisées pour les applications devant être surveillées. Une fois fait, la surveillance d'application fonctionne de la même manière que Surveillance de VM. Si les pulsations d'une application ne sont pas reçues pendant un certain temps, sa machine virtuelle est redémarrée.

Vous pouvez configurer le niveau de sensibilité de la surveillance. Une sensibilité de surveillance élevée permet de conclure plus rapidement à un dysfonctionnement. Même si c'est peu probable, une sensibilité de surveillance élevée peut aboutir à l'identification erronée de dysfonctionnements alors que la machine virtuelle ou l'application en question fonctionne toujours mais que les heartbeats ne sont pas reçus à cause de contraintes de ressources notamment. Une sensibilité de surveillance basse résulte en des interruptions de service prolongées entre les défaillances avérées et le redémarrage des machines virtuelles. Sélectionnez l'option qui offre un compromis efficace à vos besoins.

Les paramètres par défaut de la sensibilité de surveillance sont décrits dans Tableau 2-1. Vous pouvez aussi indiquer des valeurs personnalisées à la fois pour la sensibilité de la surveillance et les intervalles statistiques d'E/S en sélectionnant la case à cocher **[Personnalisé]** .

Tableau 2-1. Paramètres de surveillance des machines virtuelles

Paramètre	Intervalle d'échec	Période de réinitialisation
Haut	30	1 heure
Moyen	60	24 heures
Faible	120	7 jours

Lorsque des dysfonctionnements ont été détectés, VMware HA réinitialise les machines virtuelles. La réinitialisation contribue à garantir que les services demeurent disponibles. Pour éviter de réinitialiser constamment des machines virtuelles en cas d'erreurs non provisoires, les machines virtuelles sont réinitialisées par défaut trois fois seulement au cours d'une période configurable. Après trois reinitialisations des machines virtuelles, VMware HA n'effectue aucune autre tentative pour redémarrer les machines virtuelles après des échecs ultérieurs jusqu'à ce que la période définie ne soit écoulée. Vous pouvez configurer le nombre de réinitialisations à l'aide du paramètre personnalisé **[Réinitialisations maximales par machine virtuelle]** .

Personnalisation du comportement de VMware HA

Après avoir créé un cluster, vous pouvez modifier les attributs spécifiques qui affectent le comportement de VMware HA. Vous pouvez également modifier les paramètres par défaut du cluster hérités par des machines virtuelles individuelles.

Examinons les paramètres avancés que vous pouvez utiliser pour optimiser les clusters VMware HA dans votre environnement. Comme ces attributs affectent le fonctionnement de HA, modifiez-les avec prudence.

Définir les options avancées de VMware HA

Pour personnaliser le comportement de VMware HA, définissez les options avancées VMware HA.

Prérequis

Cluster VMware HA dont il faut modifier les paramètres.

Privilèges de l'administrateur du cluster.

Procédure

1 Sélectionnez **[VMware HA]** dans la boîte de dialogue Paramètres du cluster.

2 Cliquez sur le bouton **[Options avancées]** pour ouvrir la boîte de dialogue Options avancées (HA).

3 Saisissez chaque attribut avancé devant être modifié dans une zone de texte de la colonne **[Option]** et saisissez une valeur dans la colonne **[Valeur]** .

4 Cliquez sur **[OK]** .

Le cluster utilise des options que vous avez ajoutées ou modifiées.

Attributs avancés de VMware HA

Vous pouvez définir des attributs avancés qui affectent le comportement du cluster VMware HA.

Tableau 2-2. Attributs avancés de VMware HA

Attribut	Description
das.isolationaddress[...]	Règle l'adresse pour exécuter un ping pour déterminer si un hôte est isolé du réseau. Le ping est uniquement envoyé à cette adresse lorsque les heartbeats ne sont plus reçus d'aucun autre hôte du cluster. En l'absence de précision, la passerelle par défaut du réseau de gestion est utilisé. Cette passerelle par défaut doit être une adresse fiable et disponible, de sorte que l'hôte puisse déterminer s'il est isolé du réseau. Vous pouvez indiquer plusieurs adresses d'isolation (jusqu'à 10) pour le cluster : das.isolationaddressX, où X = 1-10. Vous devez généralement en indiquer une par réseau de gestion. L'indication d'un nombre excessif d'adresses ralentit la détection de l'isolation.
das.usedefaultisolationaddress	Par défaut, VMware HA utilise la passerelle par défaut du réseau de console comme adresse d'isolation. Cet attribut indique l'utilisation ou non de ce réglage par défaut (vrai | faux).
das.failuredetectiontime	Modifie la durée par défaut de détection de panne pour la surveillance d'hôte. La valeur par défaut est de 15 000 millisecondes (15 secondes). Cela correspond à la durée pendant laquelle un hôte n'a pas reçu de heartbeats de la part d'un autre hôte et à l'écoulement de laquelle il déclare que l'hôte est défectueux.

Tableau 2-2. Attributs avancés de VMware HA (suite)

Attribut	Description
das.failuredetectioninterval	Modifie l'intervalle des heartbeats parmi les hôtes VMware HA. Cela se produit par défaut toutes les 1 000 millisecondes (1 seconde).
das.isolationshutdowntimeout	Période pendant laquelle le système attend que la machine virtuelle s'arrête avant de la mettre hors tension. Cela s'applique uniquement si la réponse d'isolation de l'hôte est Arrêter la machine virtuelle. La valeur par défaut est de 300 secondes.
das.slotmeminmb	Définit la limite maximale de la taille d'un slot de mémoire. Si cette option est utilisée, la taille du slot est inférieure à cette valeur ou à la réservation de mémoire maximale plus la capacité supplémentaire de toute machine virtuelle sous tension dans le cluster.
das.slotcpuinmhz	Définit la limite maximale de la taille d'un slot de CPU. Si cette option est utilisée, la taille du slot est inférieure à cette valeur ou à la réservation de CPU maximale de toute machine virtuelle sous tension dans le cluster.
das.vmmemoryminmb	Définit la valeur de ressources de mémoire par défaut associée à une machine virtuelle si sa réservation de mémoire n'est pas précisée ou nulle. C'est utilisé pour les règles de contrôle d'admission Défaillances d'hôte tolérées par le cluster. Si aucune valeur n'est spécifiée, la valeur par défaut est de 0 Mo.
das.vmcpuminmhz	Définit la valeur des ressources CPU par défaut associée à une machine virtuelle si sa réservation de CPU n'est pas précisée ou nulle. C'est utilisé pour les règles de contrôle d'admission Défaillances d'hôte tolérées par le cluster. Si aucune valeur n'est spécifiée, la valeur par défaut est de 256 MHz.
das.iostatsinterval	Modifie l'intervalle statistique d'E/S par default de sensibilité de surveillance des machines virtuelles. La valeur par défaut est de 120 (secondes). Peut être définie sur une valeur supérieure ou égale à 0. Une valeur nulle désactive la vérification.

Remarque Si vous modifiez la valeur de l'un des attributs avancés suivants, vous devez mettre hors tension, puis réactiver VMware HA avant que les modifications ne s'appliquent.

- das.isolationaddress[...]
- das.usedefaultisolationaddress
- das.failuredetectiontime
- das.failuredetectioninterval
- das.isolationshutdowntimeout

Personnaliser le comportement de VMware HA pour une machine virtuelle

Les paramètres par défaut du cluster relatifs à la priorité de redémarrage, à la réponse d'isolation et à la surveillance des machines virtuelles sont associés à chaque machine virtuelle d'un cluster VMware HA. Vous pouvez préciser des comportements spécifiques à chaque machine virtuelle en changeant ces valeurs par défaut. Si la machine virtuelle quitte le cluster, ces paramètres sont perdus.

Procédure

1 Sélectionnez le cluster et choisissez **[Modifier les paramètres]** dans le menu contextuel.

2 Sélectionnez **[Options de machine virtuelle]** sous VMware HA.

3 Sélectionnez une machine virtuelle dans le panneau Paramètres de la machine virtuelle et personnalisez son paramètre **[Priorité redémarrage VM]** ou **[Réponse isolation hôte]** .

4 Sélectionnez **[Surveillance de VM]** sous VMware HA.

5 Sélectionnez une machine virtuelle dans le panneau Paramètres de la machine virtuelle et personnalisez son paramètre **[Surveillance de VM]** .

6 Cliquez sur **[OK]** .

Le comportement de la machine virtuelle diffère désormais des réglages par défaut du cluster pour chaque paramètre modifié.

Meilleures pratiques aux clusters VMware HA

Pour des performances optimales des clusters VMware HA, VMware recommande de respecter quelques règles élémentaires. La configuration du réseau et la redondance sont des critères importants de la conception et de l'implémentation du cluster.

Paramètre d'alarmes pour contrôler les changements des clusters

Quand VMware HA ou Tolérance aux pannes interviennent pour préserver la disponibilité en effectuant un basculement de machine virtuelle, par exemple, vous voulez probablement être averti des changements. Il est possible de configurer des alarmes dans vCenter Server qui seront déclenchées lorsque ces actions sont effectuées et de définir des alertes, sous forme de messages électroniques, par exemple, envoyées à un groupes d'administrateurs prédéfinis.

Contrôle de la validité du cluster

Un cluster valide ne présente aucune violation des règles de contrôle d'admission.

Un cluster activé pour VMware HA devient non valide (rouge) lorsque le nombre de machines virtuelles sous tension dépasse les conditions de basculement, c'est-à-dire que la capacité de basculement actuelle est inférieure à la capacité de basculement configurée. Si le contrôle d'admission est désactivé, les clusters ne deviennent pas non valides.

La page Résumé du cluster dans vSphere Client présente la liste des problèmes de configuration des clusters. La liste détaille les causes de la non validité d'un cluster ou de son affectation excessive (jaune).

Le comportement DRS n'est pas affecté par le fait qu'un cluster soit rouge à cause d'un problème lié à VMware HA.

Vérification de l'état opérationnel du cluster

Un cluster ou ses hôtes peuvent connaître des problèmes de configuration et d'autres erreurs qui nuisent au bon fonctionnement de VMware HA. Vous pouvez vérifier ces erreurs sur l'écran État opérationnel de cluster qui est accessible dans vSphere Client, sous la rubrique VMware HA de l'onglet **[Résumé]** du cluster. Vous devez résoudre tous les problèmes répertoriés.

Meilleures pratiques de mise en réseau

VMware émet quelques recommandations relatives à la configuration des cartes d'interface réseau hôtes et de la topologie du réseau pour VMware HA. Les meilleures pratiques incluent des recommandations pour vos hôtes ESX/ESXi, et traitent aussi du câblage, des commutateurs, des routeurs et des pare-feu.

Configuration et maintenance du réseau

Les suggestions suivantes de maintenance du réseau contribuent à éviter la détection accidentelle d'hôtes défectueux et une isolation réseau à cause de la perte de signaux de pulsation VMware HA.

- En cas de modification des réseaux sur lesquels se trouvent les hôtes ESX/ESXi en clusters, VMware recommande de suspendre la fonction de surveillance d'hôte. Les changements de matériel ou de paramètres réseau peuvent interrompre les signaux de pulsation utilisés par VMware HA pour détecter les défaillances d'hôtes, ce qui risque d'entraîner des tentatives malvenues de basculement des machines virtuelles.
- Lorsque vous modifiez la configuration réseau directement sur les hôtes ESX/ESXi, par exemple, pour ajouter des groupes de port ou pour supprimer des vSwitches, VMware recommande de placer l'hôte en mode maintenance en plus de suspendre sa surveillance.

Remarque Comme la mise en réseau est un aspect essentiel de VMware HA, l'administrateur de VMware HA doit être tenu informé de toute maintenance du réseau.

Réseaux utilisés pour les communications VMware HA

Pour identifier les opérations réseau qui risquent de perturber le bon fonctionnement de VMware HA, il est nécessaire d'identifier les réseaux de gestion utilisés pour les pulsations et d'autres communications VMware HA.

- Sur les hôtes ESX du cluster, les communications VMware HA sont acheminées via tous les réseaux qui sont identifiés comme réseaux de console de service. Les réseaux VMkernel ne sont pas utilisés par ces hôtes pour les communications VMware HA.
- Sur les hôtes ESX du cluster, les communications VMware HA sont acheminées par défaut via tous réseaux VMkernel sauf ceux spécifiques à vMotion. S'il n'y a qu'un seul réseau VMkernel, VMware HA le partage avec vMotion, si nécessaire. Avec ESXi 4.0 et version ultérieure, il faut aussi cocher explicitement la case Gestion de réseau si VMware HA doit utiliser ce réseau.

Considérations liées au réseau au niveau du cluster

Pour le bon fonctionnement de VMware HA, tous les hôtes du cluster doivent avoir des réseaux compatibles. Le premier nœud ajouté au cluster impose les réseaux devant être acceptés par tous les hôtes suivants autorisés à entrer dans le cluster. Les réseaux sont considérés comme compatibles lorsque la combinaison de l'adresse IP et du masque de sous-réseau produit un réseau dont la combinaison correspond à celle d'un autre hôte. Si vous essayez d'ajouter un hôte ayant trop ou pas assez de réseaux de gestion ou si l'hôte ajouté a des réseaux incompatibles, la configuration échoue et le panneau Détails de la tâche fournit des informations sur cette incompatibilité.

Par exemple, si le premier hôte ajouté dans le cluster comporte deux réseaux utilisés pour les communications VMware HA (10.10.135.0/255.255.255.0 et 10.17.142.0/255.255.255.0), les deux même réseaux doivent être configurés sur tous les hôtes suivants et utilisés pour les communications VMware HA.

Adresses d'isolation réseau

Une adresse d'isolation réseau est une adresse IP qui reçoit une commande ping pour déterminer si un hôte est isolé du réseau. Le ping est uniquement envoyé à cette adresse lorsqu'un hôte a cessé de recevoir les signaux de pulsation de tous les autres hôtes du cluster. Si un host peut envoyer un ping à son adresse d'isolation réseau, l'hôte n'est pas isolé du réseau et les autres hôtes du cluster ont échoué. Mais si l'hôte ne peut pas envoyer de ping à son adresse d'isolation, il est probable que l'hôte ait été isolé du réseau et aucune action de basculement n'est entreprise.

L'adresse d'isolation réseau est la passerelle par défaut de l'hôte. Une seule passerelle est définie par défaut, quel que soit le nombre de réseaux de gestion définis. Par conséquent, il faut utiliser l'attribut avancé das.isolationaddress[...] pour ajouter des adresses d'isolation pour des réseaux supplémentaires. Reportez-vous à « Attributs avancés de VMware HA », page 26.

Lorsque vous définissez des adresses d'isolation supplémentaires, VMware recommande d'augmenter la valeur de l'attribut avancé das.failuredetectiontime à 20 000 millisecondes (20 secondes) ou d'avantage. Un nœud isolé du réseau a besoin d'un certain délai pour lever le verrouillage VMFS de sa machine virtuelle si la réponse d'isolation de l'hôte est de basculer les machines virtuelles (et non de les laisser allumées). Cela doit se produire avant que les autres nœuds ne déclarent que le nœud a échoué, de façon à ce qu'ils puissent allumer les machines virtuelles sans recevoir de message d'erreur indiquant que les machines virtuelles sont toujours verrouillées par le nœud isolé.

Pour plus d'informations sur les attributs avancé VMware HA, voir « Personnalisation du comportement de VMware HA », page 26.

Autres considérations sur la mise en réseau

Configuration des commutateurs. Si les commutateurs réseau physiques qui relient les serveurs prennent en charge le paramètre PortFast (ou équivalent), activez-le. Ce paramètre empêche un hôte de se tromper en déterminant qu'un réseau est isolé au cours de l'exécution de longs algorithmes STA.

Pare-feu d'hôtes Sur les hôtes ESX/ESXi, VMware HA doit ouvrir automatiquement les ports de pare-feu suivants.

- Port entrant : TCP/UDP 8042-8045
- Port sortant : TCP/UDP 2050-2250

Noms de groupes de ports et étiquettes réseau. Utilisez des noms de groupes de ports cohérents et des étiquettes réseau sur les VLAN des réseaux publics. Les noms de groupes de ports permettent de reconfigurer l'accès au réseau par les machines virtuelles. Si vous utilisez des noms incohérents entre le serveur d'origine et le serveur de basculement, les machines virtuelles sont déconnectées de leur réseau après le basculement. Les étiquettes réseau sont utilisées par les machines virtuelles pour rétablir la connectivité réseau au redémarrage.

Redondance des chemins d'accès de réseau

La redondance des chemins d'accès entre les nœuds de cluster est importante pour la fiabilité de VMware HA. Un réseau de gestion isolé finit par être un point de panne isolé, ce qui aboutit à des basculements même si le réseau uniquement est défectueux.

S'il n'y a qu'un seul réseau de gestion, toute défaillance entre l'hôte et le cluster peut provoquer une situation de basculement inutile (ou erronée). Les défaillances possibles incluent les pannes de cartes réseau, les pannes de câbles réseau, la suppression de câbles réseau et les réinitialisations de commutateurs. Examinez ces causes possibles de défaillances entre les hôtes et efforcez-vous de les minimiser en prévoyant la redondance du réseau.

Il est possible d'implémenter la redondance du réseau au niveau de l'association de cartes réseau, ou au niveau réseau de gestion. Dans la plupart des implémentations, l'association des cartes réseau offre une redondance suffisante, mais il est possible d'utiliser ou d'ajouter au besoin la redondance de réseau de gestion. La mise en réseau de gestion redondante garantit la fiabilité de la détection des pannes et évite la réalisation de conditions d'isolation car les signaux de pulsation peuvent être transmis via plusieurs réseaux.

Configurez un nombre aussi réduit que possible de segments matériels entre les serveurs d'un cluster. L'objectif est de limiter les points de panne isolés. De plus, les chemins contenant trop de bonds peuvent provoquer des retards de paquets de signaux de pulsation et augmenter les points de panne éventuels.

Redondance par association de cartes réseau

L'utilisation d'une association de deux cartes réseau connectées pour séparer les commutateurs physiques améliore la fiabilité d'un réseau de gestion. Le cluster est plus résilient car les serveurs connectés par deux cartes réseau (et par des commutateurs séparés) ont deux chemins indépendants pour la transmission et la réception de signaux de pulsation. Pour configurer une association de cartes réseau pour réseau de gestion, configurez les vNIC de la configuration vSwitch pour la configuration Active ou Standby. Les réglages recommandés pour les paramètres des vNIC sont les suivants :

- Équilibrage de charge par défaut = Router en fonction de l'ID du port d'origine
- Retour arrière = Non

Lorsque vous avez ajouté un adapteur réseau à l'hôte de votre cluster VMware HA, vous devez reconfigurer VMware HA sur cet hôte.

Redondance réseau utilisant un réseau secondaire

Au lieu d'associer des cartes réseau pour assurer la redondance des signaux de pulsation, vous pouvez créer une connexion de réseau de gestion secondaire qui est liée à un commutateur virtuel distinct. La connexion de réseau de gestion principale est utilisée pour le réseau et à des fins de gestion. Lorsque la connexion de réseau de gestion secondaire est créée, VMware HA transmet des signaux de pulsation à la fois sur les connexions de réseau de gestion principales et secondaires. Si un chemin est défaillant, VMware HA peut continuer à transmettre et à recevoir des signaux de pulsation sur l'autre chemin.

Fourniture de la tolérance aux pannes à des machines virtuelles 3

Il est possible d'activer VMware Fault Tolerance pour les machines virtuelles afin d'assurer la continuité d'activité avec des niveaux de disponibilité et de protection des données supérieurs à ceux offerts par VMware HA.

La tolérance aux pannes est intégrée à la plate-forme hôte ESX/ESXi (par la technologie VMware vLockstep) et elle assure la continuité de la disponibilité en exécutant des machines virtuelles identiques en mode rigide virtuel sur des hôtes distincts.

Pour obtenir des résultats optimums de la tolérance aux pannes, il est nécessaire d'en comprendre le fonctionnement, de savoir comment l'activer sur un cluster et sur des machines virtuelles, de connaître les recommandations d'usage et les conseils de dépannage.

Ce chapitre aborde les rubriques suivantes :

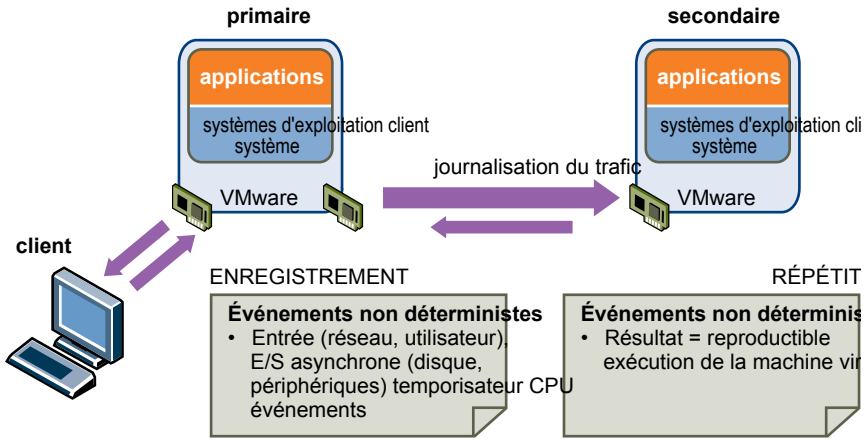
Fonctionnement de la tolérance aux pannes

VMware Fault Tolerance assure la disponibilité continue des machines virtuelles en créant et maintenant une VM secondaire identique à la VM primaire et disponible en permanence pour la remplacer en cas de situation de basculement.

Il est possible d'activer la tolérance aux pannes sur la plupart des machines virtuelles cruciales pour une mission. Une copie de la machine virtuelle, qui se nomme la machine virtuelle secondaire, est créée et exécutée en mode rigide virtuel avec la machine virtuelle principale. VMware vLockstep capture les entrées et les événements qui se produisent sur la machine virtuelle principale et les transmet à celle de la machine virtuelle

secondaire qui est exécutée sur un autre hôte. À partir de ces informations, l'exécution de la machine virtuelle secondaire est identique à celle de la machine virtuelle principale. Comme la machine virtuelle secondaire est en mode rigide virtuel avec la machine virtuelle principale, elle peut reprendre l'exécution à tout moment sans interruption, assurant ainsi une protection tolérante aux pannes.

Figure 3-1. Machine virtuelle principale et machine virtuelle secondaire dans une paire avec tolérance aux pannes



Les machines virtuelles principale et secondaire échangent des heartbeats en continu. Cet échange permet à la paire de machines virtuelles de contrôler mutuellement leur état pour assurer le maintien permanent de la tolérance aux pannes. Un basculement transparent se produit en cas de défaillance de l'hôte sur lequel la machine virtuelle principale est exécutée. Dans ce cas, la machine virtuelle secondaire est immédiatement activée pour remplacer la machine virtuelle principale. Une nouvelle machine virtuelle secondaire démarre et la redondance de la tolérance aux pannes est rétablie en quelques secondes. Si l'hôte de la machine virtuelle secondaire devient défectueux, il est aussi immédiatement remplacé. Dans l'un ou l'autre cas, les utilisateurs ne constatent aucune interruption de service ni perte de données.

Une machine virtuelle tolérante aux pannes et sa copie secondaire ne sont pas autorisées à fonctionner sur le même hôte. Cette restriction garantit qu'une défaillance de l'hôte ne peut pas entraîner la perte des deux machines virtuelles. Vous pouvez aussi utiliser les règles d'affinité entre machine virtuelle et hôte pour préciser les hôtes sur lesquels certaines machines virtuelles peuvent être exécutées. Si vous utilisez ces règles, souvenez-vous que pour chaque machine virtuelle principale affectée par une règle précise, la machine virtuelle secondaire qui y est associée est aussi affectée par la même règle. Pour plus d'informations sur les règles d'affinité, reportez-vous au *Guide de gestion des ressources*.

La tolérance aux pannes évite les situations de division qui peuvent résulter en deux copies actives d'une machine virtuelle après la reprise suite à un dysfonctionnement. Le verrouillage atomique des fichiers sur les stockages partagés est utilisé pour coordonner le basculement de façon à ce qu'un côté seulement continue à exécuter la machine virtuelle principale et une nouvelle machine virtuelle secondaire est automatiquement réaffectée.

Remarque Le contrôle anti-affinité est effectué à la mise sous tension de la machine virtuelle principale. Les machines virtuelles principales et secondaires peuvent être sur les même hôtes lorsqu'elles sont toutes deux hors tension. C'est un comportement normal. Quand la machine virtuelle principale s'allume, la machine virtuelle secondaire est démarrée sur un hôte différent.

Utilisation de la tolérance aux pannes avec DRS

Vous pouvez utiliser VMware Fault Tolerance avec VMware Distributed Resource Scheduler (DRS) quand la fonction Compatibilité améliorée de vMotion (EVC) est activée. Ce processus permet aux machines virtuelles tolérantes aux pannes de bénéficier d'un meilleur placement initial et d'être incluses dans les calculs d'équilibrage de charge du cluster.

Quand EVC est activé pour un cluster, DRS émet les recommandations de placement initiales pour les machines virtuelles tolérantes aux pannes, les déplace pendant le rééquilibrage de la charge du cluster et vous autorise à attribuer un niveau d'automatisation DRS aux machines virtuelles principales (la machine virtuelle secondaire adopte toujours le même paramètre que la machine virtuelle principale associée). Pour plus d'informations sur EVC, reportez-vous au *Guide d'administration du centre de données VMware vSphere*.

DRS ne place pas plus d'un nombre prédéfini de machines virtuelles principales ou secondaires sur un hôte au cours du placement initial ou de l'équilibrage de charge. Cette limite est contrôlée par l'option avancée das.maxftvmsperhost. La valeur par défaut de cette option est de 4. Mais si vous choisissez une valeur nulle, DRS ignore cette restriction.

Quand VMware Fault Tolerance est utilisé pour les machines virtuelles d'un cluster pour lequel EVC est désactivé, les machines virtuelles tolérantes aux pannes reçoivent des niveaux d'automatisation DRS "désactivés". Dans ce type de cluster, chaque machine virtuelle principale est uniquement mise sous tension sur son hôte enregistré, sa machine virtuelle secondaire est placée automatiquement et aucune des machines virtuelles tolérantes aux pannes n'est déplacée pour l'équilibrage de charge.

Si vous utilisez des règles d'affinité avec deux machines virtuelles tolérantes aux pannes, une règle d'affinité VM-VM s'applique uniquement à la machine virtuelle principale, tandis qu'une règle d'affinité machine virtuelle-hôte s'applique à la fois à la machine virtuelle principale et à sa machine virtuelle secondaire.

Cas d'utilisation de tolérance aux pannes

Plusieurs situations typiques peuvent bénéficier de l'utilisation de VMware Fault Tolerance.

La tolérance aux pannes assure un meilleur niveau de continuité d'activité que VMware HA. Lorsqu'une machine virtuelle secondaire doit intervenir pour remplacer son homologue, la machine virtuelle principale, la machine virtuelle secondaire joue immédiatement le rôle de machine virtuelle principale, la totalité de l'état de la machine virtuelle étant préservé. Les applications sont déjà en cours d'exécution et les données conservées en mémoire ne doivent pas être ressaisies ou rechargées. Ce n'est pas le cas du basculement assuré par VMware HA qui redémarre les machines virtuelles affectées par un dysfonctionnement.

Ce haut niveau de continuité et la meilleure protection des informations d'états et des données informe les scénarios du déploiement possible de la tolérance aux pannes.

- Les applications qui doivent être disponibles en permanence, surtout celles présentant des connections longues durées de clients que les utilisateurs veulent conserver pendant la défaillance matérielle.
- Applications personnalisées qui n'ont pas d'autres moyens de former un cluster.
- Cas où la grande disponibilité peut être assurée par des solutions de formation de cluster personnalisées qui sont très compliquées à configurer et à entretenir.

Tolérance aux pannes à la demande

Un autre cas pratique de protection d'une machine virtuelle par la tolérance aux pannes s'intitule la tolérance aux pannes à la demande. Dans ce cas, une machine virtuelle est correctement protégée par VMware HA pendant son fonctionnement normal. Pendant certaines périodes critiques, vous voudrez renforcer la protection de la machine virtuelle. Pendant la production d'un rapport trimestriel, par exemple, dont l'interruption pourrait retarder la mise à disposition d'informations cruciales pour une mission. VMware Fault

Tolerance permet de protéger la machine virtuelle avant la production du rapport, puis d'éteindre ou de mettre hors tension la tolérance aux pannes après la publication du rapport. Vous pouvez utiliser la Tolérance aux pannes à la demande pour protéger la machine virtuelle au cours d'une période critique et revenir aux ressources normales pour les opérations non critiques.

Liste de vérification de tolérance aux pannes

La liste de vérification suivante contient les exigences en matière de cluster, d'hôte et de machine virtuelle que vous devez connaître avant d'utiliser VMware Fault Tolerance.

Consultez cette liste avant de configurer la tolérance aux pannes. Vous pouvez aussi utiliser l'utilitaire VMware SiteSurvey (téléchargeable sur http://www.vmware.com/download/shared_utilities.html) pour mieux comprendre les problèmes de configuration associés au cluster, à l'hôte et aux machines virtuelles utilisées pour VMware FT.

Exigences aux clusters pour la tolérance aux pannes

Les exigences suivantes aux clusters doivent être remplies avant d'utiliser la tolérance aux pannes.

- Vérification du certificat de l'hôte activée. Reportez-vous à « Activer la vérification du certificat de l'hôte », page 39.
- Deux hôtes certifiés FT au minimum utilisant la même version de tolérance aux pannes ou le même numéro de compilation d'hôte . Le numéro de version de tolérance aux pannes apparaît sur l'onglet **[Résumé]** d'un hôte dans le vSphere Client.

  Remarque Pour les hôtes antérieurs à ESX/ESXi 4.1, cet onglet énumère les numéros de build d'hôte. Les correctifs peuvent provoquer une variation des numéros de build d'hôte entre les installations ESX et ESXi. Pour vous assurer que vos hôtes sont compatibles avec la tolérance aux pannes, ne mélangez pas les hôtes ESX et ESXi dans une paire FT.

- Les hôtes ESX/ESXi ont accès aux mêmes banques de données et réseaux des machines virtuelles. Reportez-vous à « Recommandations relatives à la tolérance aux pannes », page 46.
- Journalisation de la tolérance aux pannes et réseau vMotion configuré. Reportez-vous à « Configurer la mise en réseau des machines hôtes », page 40.
- cluster VMware HA créé et activé. Reportez-vous à « Création d'un cluster VMware HA », page 20. VMware HA doit être activé avant la mise sous tension des machines virtuelles tolérantes aux pannes ou l'ajout d'un hôte dans un cluster qui prend déjà en charge des machines virtuelles tolérantes aux pannes.

Exigences aux hôtes pour la tolérance aux pannes

Les exigences suivantes aux hôtes doivent être remplies avant d'utiliser la tolérance aux pannes.

- Les hôtes doivent avoir des processeurs appartenant au groupes de processeurs compatibles avec la tolérance aux pannes. Il est également fortement recommandé que les processeurs des hôtes soient compatibles entre eux. Voyez l'article de base de connaissance de VMware http://kb.vmware.com/kb/1008027 pour plus d'informations sur les processeurs pris en charge.
- Les hôtes doivent disposer d'une licence pour VMware Fault Tolerance.
- Les hôtes doivent être certifiés pour VMware Fault Tolerance. Consultez http://www.vmware.com/resources/compatibility/search.php et sélectionnez **[Recherche par tolérance aux pannes jeux compatibles]** pour confirmer si les hôtes sont certifiés.
- La configuration de chaque hôte implique l'activation de la virtualisation matérielle (HV) dans le BIOS.

Pour confirmer la compatibilité des hôtes dans le cluster pour la prise en charge de la tolérance aux pannes, vous pouvez aussi effectuer des vérifications de conformité de profils comme décrit dans « Créer un cluster VMware HA et vérifier la conformité », page 42.

Remarque Quand un hôte ne peut pas prendre en charge VMware Fault Tolerance, vous pouvez en consulter les raisons sur l'onglet **[Résumé]** de l'hôte dans vSphere Client. Cliquez sur l'icône de légende bleue à côté du champ **[Hôte configuré pour FT]** et une liste des conditions pour la tolérance aux pannes que l'hôte ne satisfait pas s'affiche.

Exigences aux machines virtuelles pour la tolérance aux pannes

Les exigences suivantes aux machines virtuelles doivent être remplies avant d'utiliser la tolérance aux pannes.

- Aucun périphérique non pris en charge n'est attaché à la machine virtuelle. Reportez-vous à « Interopérabilité de la tolérance aux pannes », page 37.
- Les machines virtuelles doivent être conservées dans des fichiers de RDM virtuel ou de disque de machine virtuelle (VMDK) qui sont approvisionnés en lourd. Lorsqu'une machine virtuelle est conservée dans un fichier VMDK qui est approvisionné en allégé et que vous tentez d'activer la tolérance aux pannes, un message vous avertit que le fichier VMDK doit être converti. Vous devez mettre hors tension la machine virtuelle pour exécuter la conversion.
- Les fonctions incompatibles ne doivent pas être exécutées avec les machines virtuelles tolérantes aux pannes. Reportez-vous à « Interopérabilité de la tolérance aux pannes », page 37.
- Les fichiers de machines virtuelles doivent être conservés dans un stockage partagé. Les solutions de stockage partagé approuvées comprennent Fibre Channel, iSCSI (matériel et logiciel), NFS et NAS.
- Seules les machines virtuelles avec un seul vCPU sont compatibles avec la tolérance aux pannes.
- Les machines virtuelles doivent être exécutées sur l'un des systèmes d'exploitation clients pris en charge. Consultez l'article dans la base de connaissances VMware accessible à l'adresse http://kb.vmware.com/kb/1008027 pour plus d'informations.

Interopérabilité de la tolérance aux pannes

Avant de configurer VMware Fault Tolerance, vous devez connaître les fonctions et produits incompatibles avec la tolérance aux pannes.

Fonctions vSphere non prises en charge par la tolérance aux pannes

Les fonctions vSphere suivantes suivantes ne sont pas prises en charge pour les machines virtuelles tolérantes aux pannes.

- Snapshots. Les snapshots doivent être supprimés ou soumis avant l'activation de la tolérance aux pannes sur une machine virtuelle. De plus, il n'est pas possible de prendre des snapshots des machines virtuelles sur lesquelles la tolérance aux pannes est activée.
- Stockage vMotion Il n'est pas possible d'appeler le stockage vMotion pour les machines virtuelles pour lesquelles la tolérance aux pannes est activée. Pour migrer le stockage, il faut mettre hors tension temporairement la tolérance aux pannes et exécuter l'action de stockage vMotion. Une fois fait, vous pouvez réactiver la tolérance aux pannes.

- Clones liés. Il n'est pas possible d'activer la tolérance aux pannes sur une machine virtuelle qui est liée à un clone et il n'est pas non plus possible de créer un clone lié à partir d'une machine virtuelle dont la tolérance aux pannes est activée.
- VMware Consolidated Backup (VCB) Il n'est pas possible de sauvegarder une machine virtuelle dont la tolérance aux pannes est activée avec VCB, vStorage API for Data Protection, VMware Data Recovery ou tout autre produit de sauvegarde similaire exigeant l'utilisation d'un snapshot de machine virtuelle, comme effectué par ESX/ESXi. Pour sauvegarder ainsi une machine virtuelle tolérante aux pannes, il faut préalablement mettre hors tension la tolérance aux pannes, puis la réactiver après la sauvegarde. Les snapshots de stockage basé sur une baie n'affectent pas la tolérance aux pannes.

Fonctions et périphériques incompatibles avec la tolérance aux pannes

Pour qu'une machine virtuelle soit compatible avec la tolérance aux pannes, la machine virtuelle ne doit pas utiliser les fonctions ou périphériques suivants.

Tableau 3-1. Fonctions et périphériques incompatibles avec la tolérance aux pannes et les actions correctives

Fonction ou périphérique incompatible	Action corrective
Machines virtuelles à multiprocesseur symétrique (SMP). Seules les machines virtuelles avec un seul vCPU sont compatibles avec la tolérance aux pannes.	Reconfigurez la machine virtuelle comme vCPU unique. De nombreuses charges de travail présentent de bonnes performances avec une configuration à vCPU unique.
Mappage disque brut physique (RDM).	Reconfigurez les machines virtuelles avec des périphériques virtuels pris en charge par des RDM physiques de façon à ce qu'ils utilisent des RDM virtuels à la place.
Lecteur de CD-ROM ou de disquettes virtuels pris en charge par un périphérique physique ou distant.	Retirez le lecteur de CD-ROM ou de disquettes virtuels ou reconfigurez la prise en charge avec une image ISO installée sur le stockage partagé.
Clients paravirtualisés.	Si la paravirtualisation n'est pas requise, reconfigurez la machine virtuelle sans VMI ROM.
Périphérique USB et audio.	Déconnectez ces périphériques de la machine virtuelle.
Virtualisation d'identification N-Port (NPIV).	Désactivez la configuration NPIV de la machine virtuelle
relais de cartes réseau	Cette fonction n'est pas prise en charge par la tolérance aux pannes et doit donc être désactivée.
Pilotes réseau vlance.	La tolérance aux pannes ne prend pas en charge les machines virtuelles qui sont configurées avec les cartes réseaux virtuelles vlance. Toutefois, vmxnet2, vmxnet3 et e1000 sont intégralement pris en charge.
Disques virtuels pris en charge par des disques de provisionnement lourds ou légers dont les fonctions de cluster ne sont pas activées.	Lorsque vous activez la tolérance aux pannes, la conversion au format de disque approprié est effectuée par défaut. Vous devez mettre hors tension la machine virtuelle pour déclencher cette conversion.
Connexion de périphériques à chaud	La fonction de connexion à chaud est automatiquement désactivée pour les machines virtuelles tolérantes aux pannes. Pour la connexion des périphériques à chaud (ajout ou suppression), vous devez mettre hors tension temporairement la tolérance aux pannes, effectuer la connexion à chaud, puis réactiver la tolérance aux pannes. **Remarque** En cas d'utilisation de la tolérance aux pannes, modifier les paramètres d'un adapteur réseau virtuelle au cours du fonctionnement d'une machine virtuelle est une opération de connexion à chaud car elle exige de "débrancher" la carte réseau, puis de la "rebrancher". Prenons l'exemple d'un adapteur réseau virtuelle pour une machine virtuelle en cours d'exécution. Si vous modifiez le réseau auquel la carte réseau virtuelle est connectée, la tolérance aux pannes doit préalablement être désactivée.

Tableau 3-1. Fonctions et périphériques incompatibles avec la tolérance aux pannes et les actions correctives (suite)

Fonction ou périphérique incompatible	Action corrective
Extended Page Tables/Rapid Virtualization Indexing (EPT/RVI).	EPT/RVI est automatiquement désactivé pour les machines virtuelles pour lesquelles la tolérance aux pannes est activée.
Ports série ou parallèles	Déconnectez ces périphériques de la machine virtuelle.
IPv6	Utilisez les adresses IPv4 avec la tolérance aux pannes.

Préparation du cluster et des hôtes à la tolérance aux pannes

Pour activer VMware Fault Tolerance pour votre cluster, les conditions préalables de la fonction doivent être remplies et il est nécessaire d'effectuer quelques étapes de configuration sur les hôtes. Une fois ces étapes accomplies et votre cluster créé, vous pouvez aussi vérifier que la configuration est conforme aux exigences requises pour l'activation de la tolérance aux pannes.

Les tâches devant être effectuées avant de tenter d'activer la tolérance aux pannes pour le cluster sont les suivantes :

- Activer la vérification du certificat de l'hôte (s'il s'agit d'une mise à niveau d'une ancienne version de vCenter Server)
- Configurer la mise en réseau de chaque hôte
- Créer un cluster VMware HA, ajouter des hôtes et vérifier la conformité

Lorsque le cluster et les hôtes sont prêts, vous pouvez activer la tolérance aux pannes pour vos machines virtuelles. Reportez-vous à « Mettre sous tension la tolérance aux pannes pour des machines virtuelles », page 44.

Activer la vérification du certificat de l'hôte

La vérification du certificat de l'hôte permet de configurer les hôtes ESX/ESXi de façon à ce qu'ils vérifient leurs identités mutuelles, ce qui contribue à sécuriser l'environnement. La vérification du certificat de l'hôte est requise pour les hôtes ESX/ESXi sur lesquels résident les machines virtuelles tolérantes aux pannes.

Si vous avez installé la version 4.1 de VMware vCenter Server, la vérification du certificat de l'hôte est activée automatiquement. Si vous avez mis à niveau à partir d'une version antérieure, vous devez effectuer la procédure manuellement. Au cours de cette procédure, vous verrez la liste des hôtes et leur certificat pour vérification. Vous pouvez vérifier le certificat de l'hôte avant de valider l'activation de la vérification du certificat. Les hôtes non vérifiés au cours de cette étape doivent être vérifiés et reconnectés manuellement.

Procédure

1 Connectez vSphere Client à vCenter Server.

2 Sélectionnez **[Administration]** , puis **[Paramètres vCenter Server]** .

La fenêtre **[Paramètres vCenter Server]** apparaît.

3 Cliquez sur **[Paramètres SSL]** dans le panneau gauche.

4 Cochez la case **[vCenter exige des certificats SSL d'hôtes vérifiés]** .

5 Cliquez sur **[OK]** .

Configurer la mise en réseau des machines hôtes

Sur chaque hôte que vous voulez ajouter dans un cluster VMware HA, vous devez configurer deux commutateurs réseau différents, de façon à ce que l'hôte prenne aussi en charge VMware Fault Tolerance.

Pour activer la tolérance aux pannes d'un hôte, vous devez exécuter deux fois cette procédure, une fois par option de groupe de ports pour veiller à ce que suffisamment de bande passante soit disponible pour la journalisation de la tolérance aux pannes. Sélectionnez une option, terminez la procédure, et recommencez-la une seconde fois en sélectionnant l'autre option de groupes de port.

Prérequis

Des cartes réseau (NIC) de plusieurs gigaoctets sont nécessaires. Pour chaque hôte compatible avec la tolérance aux pannes, il faut au minimum deux adaptateurs réseau physiques de plusieurs gigaoctets : par exemple, l'une dédiée à la journalisation de la tolérance aux pannes et l'autre dédiée à vMotion. VMware recommande trois cartes réseau ou davantage pour assurer la disponibilité. Les cartes réseau de journalisation vMotion et de tolérance aux pannes doivent être sur des sous-réseaux différents.

Procédure

1 Connectez vSphere Client à vCenter Server.

2 Dans l'inventaire de vSphere Server, sélectionnez l'hôte et cliquez sur l'onglet **[Configuration]** .

3 Sélectionnez **[Mise en réseau]** sous **[Matériel]** , puis cliquez sur le lien **[Ajouter gestion réseau]** .

L'assistant Ajouter un réseau apparaît.

4 Sélectionnez **[VMkernel]** sous **[Types connexion]** et cliquez sur **[Suivant]** .

5 Sélectionnez **[Créer un commutateur virtuel]** et cliquez sur **[Suivant]** .

6 Fournir une étiquette pour le commutateur.

7 Sélectionnez **[Utiliser ce groupe de ports pour vMotion]** ou **[Utiliser ce groupe de ports pour la journalisation de la tolérance aux pannes]** puis cliquez sur **[Suivant]** .

8 Indiquez une adresse IP et un masque de sous-réseau et cliquez sur **[Suivant]** .

9 Cliquez sur **[Terminer]** .

Lorsque vous avez créé à la fois un commutateur virtuel de journalisation vMotion et de tolérance aux pannes, vous pouvez créer d'autres commutateurs virtuels en cas de besoin. Ajoutez ensuite l'hôte au cluster et suivez les étapes nécessaires à l'activation de la tolérance aux pannes.

Suivant

Pour confirmer la réussite de l'activation de vMotion et de la tolérance aux pannes sur l'hôte, consultez son onglet **[Résumé]** dans le vSphere Client. Dans le volet Général, les champs **[vMotion activé]** et **[Hôte configuré pour FT]** doivent être définis sur oui.

Remarque Si vous configurez la mise en réseau pour la prise en charge de la tolérance aux pannes mais que vous désactivez ensuite le port de journalisation de la tolérance aux pannes, les paires de machines virtuelles tolérantes aux pannes qui sont déjà sous tension le restent. Mais si une situation de basculement surgit, une nouvelle machine virtuelle secondaire n'est pas démarrée après le remplacement de la machine virtuelle principale par sa machine virtuelle secondaire. Par conséquent, la nouvelle machine virtuelle principale fonctionne en étant non protégée.

Exemple de configuration de la mise en réseau des hôtes pour la tolérance aux pannes

Cet exemple présente la configuration réseau de l'hôte pour la tolérance aux pannes dans un déploiement typique avec quatre cartes réseau de plusieurs gigaoctets. Ce déploiement garantit un service adéquat pour chaque type de trafic identifié ici et il pourrait être considéré comme une configuration exemplaire.

La tolérance aux pannes intervient pendant toute la durée de la défaillance d'un hôte physique en raison d'une interruption de l'alimentation électrique, d'une panique du système ou d'autres raisons comparables. Les défaillances des emplacements de stockage ou du réseau ou de tous composants de serveurs physiques qui n'ont pas de répercussions sur l'état opérationnel de l'hôte n'initient pas un basculement de la tolérance aux pannes sur la machine virtuelle secondaire. Par conséquent, les clients sont vivement encouragés à utiliser la redondance appropriée (par exemple, l'association de cartes réseau) pour réduire les risques de perte de la connectivité des machines virtuelles en faveur de composants d'infrastructure comme des réseaux ou des baies de stockage.

Les règles d'association des cartes réseau sont configurées sur les groupes de port vSwitch (vSS) (ou groupes de ports virtuels distribués pour vDS) et régissent la manière dont vSwitch gère et répartit le trafic sur les adaptateurs réseau physiques (vmnics) des machines virtuelles, des ports vmkernel et des ports de consoles de services. Un groupes de port unique est généralement utilisé pour chaque type de trafic, chacun étant généralement associé à un VLAN différent.

Directives de configuration de mise en réseau des hôtes

Les directives suivantes vous permettent de configurer la mise en réseau des hôtes pour la prise en charge de la tolérance aux pannes avec différentes combinaisons de types de trafic (par exemple, NFS) et plusieurs adaptateurs réseau physiques.

- Répartissez chaque association de cartes réseau sur deux commutateurs physiques assurant la continuité des domaines L2 pour chaque VLAN entre deux commutateurs physiques.
- Utilisez des règles d'association déterministe pour vous assurer que des types de trafic particulier présentent une affinité avec un adapteur réseau particulière (active/veille) ou un ensemble de cartes réseau (par exemple, ID port virtuel d'origine).
- Quand des règles active/veille sont utilisées, associez les types de trafic pour réduire les répercussions en cas de basculement où les deux types de trafic partagent un vmnic.
- Quand des règles active/veille sont utilisées, configurez tous les adaptateurs actifs pour un type de trafic particulier (par exemple, journalisation de la tolérance aux pannes) sur le même commutateur physique. Cela réduit le nombre de bonds réseau et diminue les possibilités de surexploitation du commutateur.

Exemple de configuration avec cartes réseau de 4 Go

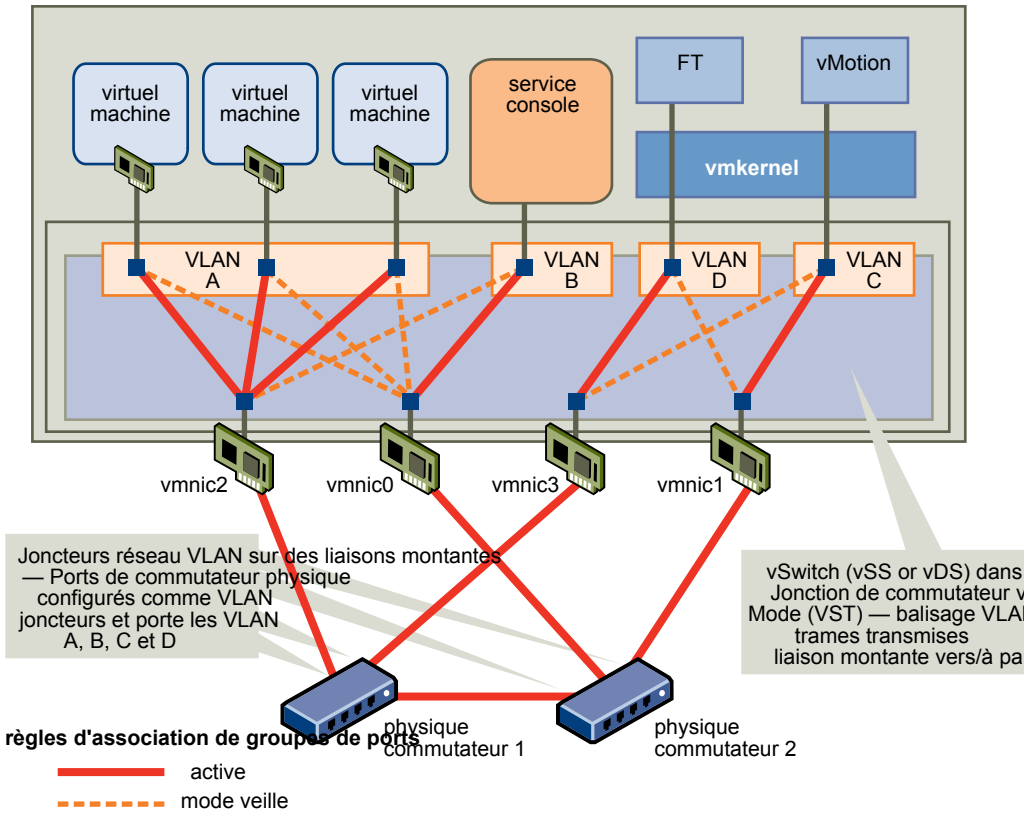
Figure 3-2 illustre la configuration réseau d'un seul l'hôte ESX/ESXi avec quatre cartes réseau de plusieurs gigaoctets compatibles avec la tolérance aux pannes. Les autres hôtes du cluster tolérant aux pannes seraient configurés de la même manière.

Cet exemple utilise quatre groupes de ports configurés comme suit :

- VLAN A : groupes de ports réseau des machines virtuelles actif sur vmnic2 (vers le commutateur physique #1) ; en veille sur vmnic0 (vers le commutateur physique #2.)
- VLAN B : groupes de ports de console de service actif sur vmnic0 (vers le commutateur physique #2) ; en veille sur vmnic2 (vers le commutateur physique #1.)
- VLAN C : groupes de ports de vMotion actif sur vmnic1 (vers le commutateur physique #2) ; en veille sur vmnic3 (vers le commutateur physique #1.)
- VLAN D : groupes de ports de journalisation de la tolérance aux pannes actif sur vmnic3 (vers le commutateur physique #1) ; en veille sur vmnic1 (vers le commutateur physique #2.)

vMotion et la journalisation de la tolérance aux pannes peuvent partager le même VLAN (configurez le même nombre de VLAN dans les deux groupes de ports), mais ils exigent leur propre adresse IP unique résidant dans différents sous-réseaux IP. Toutefois, des VLAN séparés peuvent être préférés si des restrictions de qualité de service (QoS) sont en vigueur sur le réseau physique avec des règles de QoS basées sur VLAN. QoS est particulièrement utilisée lorsque le trafic concurrent intervient, par exemple, lorsque plusieurs bonds de commutateurs physiques sont utilisés ou quand un basculement a lieu et que plusieurs types de trafic entrent en concurrence pour des ressources réseau.

Figure 3-2. Exemple de configuration de mise en réseau pour la tolérance aux pannes



Créer un cluster VMware HA et vérifier la conformité

Tolérance aux pannes VMware est utilisée dans le cadre d'un cluster VMware HA. Après avoir configuré la mise en réseau de chaque hôte, créez le cluster VMware HA et ajoutez-y les hôtes. Vous pouvez vérifier que le cluster est configuré correctement et est conforme aux exigences relatives à l'activation réussie de la tolérance aux pannes.

Procédure

1 Connectez vSphere Client à vCenter Server.

2 Dans l'inventaire de vSphere Server, sélectionnez le cluster et cliquez sur l'onglet **[Conformité de profil]** .

3 Cliquez sur **[Vérifier la conformité maintenant]** pour exécuter les tests de conformité.

Pour visionner les tests effectués, cliquez sur **[Description]** .

Les résultats du test de conformité sont affichés en bas de l'écran. Un hôte est désigné comme étant conforme ou non conforme.

Remarque Pour plus d'informations sur la création d'un cluster VMware HA, reportez-vous à Chapitre 2, « Création et utilisation des clusters VMware HA », page 11.

Fourniture de la tolérance aux pannes à des machines virtuelles

Après avoir suivi les étapes nécessaires pour activer VMware Fault Tolerance pour votre cluster, vous pouvez utiliser la fonction en l'activant pour des machines virtuelles individuelles.

L'option pour activer la tolérance aux pannes n'est pas disponible (grisée) si l'une de ces conditions s'applique :

- La machine virtuelle réside sur un hôte qui n'a pas de licence pour la fonction.
- La machine virtuelle réside sur un hôte qui est dans le mode maintenance ou le mode de veille.
- La machine virtuelle est déconnectée ou orpheline (son fichier .vmx n'est pas accessible).
- L'utilisateur n'a pas l'autorisation d'activer la fonction.

Si l'option pour activer la tolérance aux pannes est disponible, cette tâche doit encore être validée et peut échouer si certaines conditions n'est pas remplies.

Contrôles de validation pour l'activation de la tolérance aux pannes

Plusieurs contrôles de validation sont exécutés sur une machine virtuelle avant de pouvoir activer la tolérance aux pannes.

- Le contrôle de certificat SSL doit être activé dans les paramètres de vCenter Server.
- L'hôte doit être dans un cluster HA VMware ou un cluster mixte HA et DRS VMware.
- L'hôte doit avoir ESX/ESXi 4.0 ou ultérieur installé.
- La machine virtuelle ne doit pas avoir plusieurs vCPU.
- La machine virtuelle ne doit pas avoir de snapshots.
- La machine virtuelle ne doit pas être un modèle.
- La machine virtuelle ne doit pas avoir VMware HA désactivé.

Plusieurs vérifications de validation supplémentaires sont effectuées pour les machines virtuelles sous tension (ou celles qui sont en cours de mise sous tension).

- Le BIOS des hôtes où résident les machines virtuelles tolérantes aux pannes doit avoir la virtualisation matérielle (HV, Hardware Virtualization) activée.
- L'hôte qui prend en charge la machine virtuelle principale doit avoir un processeur qui prend en charge la tolérance aux pannes.
- L'hôte qui prend en charge la machine virtuelle secondaire doit avoir un processeur qui prend en charge la tolérance aux pannes et dont la famille ou le modèle de CPU est le même que l'hôte qui prend en charge la machine virtuelle principale.
- Les composants matériels doivent être certifiés compatibles avec la tolérance aux pannes. Pour le vérifier, reportez-vous au Guide de compatibilité VMware à l'adresse http://www.vmware.com/resources/compatibility/search.php et sélectionnez **[Recherche par tolérance aux pannes jeux compatibles]** .
- La combinaison du système de la machine virtuelle d'exploitation invité et le processeur doit être prise en charge par la tolérance aux pannes (par exemple, Solaris de 32 bits sur des processeurs AMD n'est pas actuellement pris en charge). Consultez l'article dans la base de connaissances VMware accessible à l'adresse http://kb.vmware.com/kb/1008027 pour plus d'informations sur la combinaison de processeurs et les systèmes d'exploitation clients pris en charge.
- La configuration de la machine virtuelle doit être valide pour être utilisée avec une tolérance aux pannes (par exemple, la configuration ne peut comporter aucun périphérique non pris en charge.).

Quand votre effort d'activation de la tolérance aux pannes pour une machine virtuelle réussit aux contrôles de validation, la machine virtuelle secondaire est créée. Le placement et le statut immédiat de la machine virtuelle secondaire dépendent de l'état sous tension ou hors tension de la machine virtuelle principale quand vous avez activé la tolérance aux pannes.

Si la machine virtuelle principale est sous tension :

- L'état complet de la machine virtuelle principale est copié et la machine virtuelle secondaire est créée, placée sur un hôte compatible distinct et mise sous tension si elle passe le contrôle d'admission.
- L'état de tolérance aux pannes affiché sur l'onglet **[Résumé]** de la machine virtuelle dans le vSphere Client est **[Protégé]** .

Si la machine virtuelle principale est hors tension :

- La machine virtuelle secondaire est créée immédiatement et enregistrée dans le cluster d'un hôte (Il doit être enregistré sur un hôte plus approprié lorsqu'il est mis sous tension.)
- La machine virtuelle secondaire est mise sous tension seulement après la mise sous tension de la machine virtuelle principale.
- L'état de tolérance aux pannes affiché sur l'onglet **[Résumé]** de la machine virtuelle dans vSphere Client est **[Non protégé, VM inactive]** .
- Quand vous essayez de mettre sous tension la machine virtuelle primaire après l'activation de la tolérance aux pannes, les contrôles supplémentaires de validation sont exécutés. Pour mettre sous tension correctement, la machine virtuelle ne doit pas employer la paravirtualisation (VMI).

  Après le passage de ces contrôles, les machines virtuelles principales et secondaires sont mises sous tension et placées sur les hôtes distincts et compatibles. L'état de tolérance aux pannes affiché sur l'onglet **[Résumé]** de la machine virtuelle dans le vSphere Client est marqué **[Protégé]** .

Mettre sous tension la tolérance aux pannes pour des machines virtuelles

Vous pouvez activer Tolérance aux pannes VMware par l'intermédiaire de vSphere Client.

Quand la tolérance aux pannes est activée, vCenter Server désactive la limite de mémoire de la machine virtuelle et définit la réservation de mémoire en fonction de la taille de la mémoire de la machine virtuelle. Si la tolérance aux pannes reste activée, il n'est pas possible de modifier la réservation de mémoire, sa taille, la limite ou les partages. Quand la tolérance aux pannes est désactivée, les valeurs d'origine de tous les paramètres qui ont été modifiés ne sont pas restaurées.

Connectez vSphere Client à vCenter Server en utilisant un compte ayant des droits d'accès administrateur au cluster.

Procédure

1 Sélectionnez les vues Hôtes & Clusters.

2 Cliquez avec le bouton droit sur une seule machine virtuelle et sélectionnez **[Tolérance aux pannes] > [Démarrer tolérance aux pannes]** .

  Si vous sélectionnez plusieurs machines virtuelles, le menu **[Tolérance aux pannes]** est désactivé. Vous devez activer Tolérance aux pannes pour une seule machine virtuelle à la fois.

La machine virtuelle spécifiée est désignée comme machine virtuelle principale et une machine virtuelle secondaire est établie sur un autre hôte. La machine virtuelle principale est désormais tolérante aux pannes.

Affichage des informations sur les machines virtuelles tolérantes aux pannes

Vous pouvez consulter les machines virtuelles tolérantes aux pannes dans l'inventaire de vCenter Server en utilisant le vSphere Client.

Remarque Vous ne pouvez pas mettre hors tension la tolérance aux pannes de la machine virtuelle secondaire.

Le volet VMware Fault Tolerance apparaît dans l'onglet **[Résumé]** pour la machine virtuelle primaire et inclut des informations sur la machine virtuelle.

état de la tolérance aux pannes

Indique l'état de tolérance aux pannes de la machine virtuelle.

- Protected. Indique que les machines virtuelles principale et secondaire sont sous tension et fonctionnent comme prévu.
- Non protégé. Indique que la machine virtuelle secondaire ne fonctionne pas. Les raisons possibles sont répertoriés dans le tableau.

Tableau 3-2. Raisons pour l'état non protégé de la machine virtuelle principale

Raison pour l'état non protégé	Description
Démarrage	Tolérance aux pannes est en train de démarrer la VM secondaire. Ce message n'est visible que pour une courte période de temps.
VM secondaire nécessaire	La machine virtuelle principale fonctionne sans machine virtuelle secondaire, ainsi la machine virtuelle principale n'est actuellement pas protégée. Ceci se produit généralement quand il n'y a aucun hôte compatible dans le cluster disponible pour la machine virtuelle secondaire. Corrigez cette situation en plaçant un hôte compatible en ligne. S'il existe un hôte compatible en ligne dans le cluster, il peut être nécessaire d'approfondir la question. Dans certaines circonstances, la désactivation de la tolérance aux pannes puis sa réactivation corrige ce problème.
Désactivé	La tolérance aux pannes est actuellement désactivée (aucune machine virtuelle secondaire ne fonctionne). Ceci se produit quand la tolérance aux pannes est désactivée par l'utilisateur ou quand vCenter Server désactive la tolérance aux pannes après avoir échoué dans la mise sous tension de la machine virtuelle secondaire.
Machine virtuelle hors exécution	La tolérance aux pannes est activée mais la machine virtuelle est hors tension. Mettez sous tension la machine virtuelle pour atteindre l'état Protected.

Emplacement secondaire

Affiche l'hôte ESX/ESXi sur lequel la machine virtuelle secondaire est hébergée.

CPU secondaire totale	Indique l'utilisation de la CPU de la machine virtuelle secondaire, exprimée en MHz.
Mémoire secondaire totale	Indique l'utilisation de la mémoire de la machine virtuelle secondaire, exprimée en Mo.
Intervalle vLockstep	Intervalle de temps (en secondes) requis pour que la machine virtuelle secondaire corresponde à l'état d'exécution actuel de la machine virtuelle primaire. En général, cet intervalle est inférieur à une demi-seconde. Aucun état n'est perdu pendant un basculement, quelle que soit la valeur de l'intervalle vLockstep.
Log Bandwidth	La quantité de capacité réseau utilisée pour envoyer les informations de journalisation de VMware Fault Tolerance depuis l'hôte exécutant la machine virtuelle principale jusqu'à l'hôte exécutant la machine virtuelle secondaire.

Pour chaque hôte configuré pour prendre en charge la tolérance aux pannes, vous pouvez consulter les informations sur ses machines virtuelles tolérantes aux pannes en accédant à l'onglet **[Résumé]** de l'hôte dans vSphere Client. [Trans]The **[Tolérance aux pannes]** section of this screen displays the total number of Primary and Secondary VMs residing on the host and the number of those virtual machines that are powered on. [Trans]If the host is ESX/ESXi 4.1 or greater, this section also displays the Fault Tolerance version the host is running. Autrement, elle mentionne le numéro de build de l'hôte. [Trans]For two hosts to be compatible they must have matching FT version numbers or matching host build numbers.

Recommandations relatives à la tolérance aux pannes

Pour bénéficier de résultats optimums avec la tolérance aux pannes, VMware recommande de respecter quelques meilleures pratiques.

En plus des rubriques ci-dessous, vous pouvez aussi consulter le livre blanc sur http://www.vmware.com/resources/techresources/10040 pour plus d'informations sur les recommandations relatives à la tolérance aux pannes.

Configuration d'hôte

Suivez les recommandations suivantes lors de la configuration des hôtes.

- Les hôtes exécutant les machines virtuelles principales et secondaires doivent fonctionner à des fréquences de processeur assez proches sinon la machine virtuelle secondaire risque de redémarrer plus souvent. Les fonctions de gestion de l'alimentation de la plate-forme qui ne sont pas ajustées selon la charge de travail (modes de limitation de puissance et de basse fréquence pour économiser de l'énergie, par exemple) peuvent entraîner de fortes variations des fréquences du processeur. Si des machines virtuelles secondaires sont redémarrées régulièrement, désactivez tous les modes de gestion de l'alimentation sur les hôtes exécutant des machines virtuelles tolérantes aux pannes ou veillez à ce que tous les hôtes soient exécutés avec les même modes de gestion de l'alimentation.
- Appliquez la même configuration d'extension de jeux d'instructions (activé ou désactivé) à tous les hôtes. Le processus d'activation ou de désactivation des jeux d'instructions varie en fonction du BIOS. Reportez-vous à la documentation du BIOS de vos hôtes pour plus d'informations sur la configuration des jeux d'instructions.

Clusters homogènes

VMware Fault Tolerance peut fonctionner dans des clusters avec des hôtes non uniformes, mais il est préférable que les clusters aient des nœuds compatibles. Au moment de la construction du cluster, tous les hôtes doivent intégrer les éléments suivants :

- Processeurs appartenant au même groupes de processeurs compatibles.
- Accès commun aux banques de données utilisées par les machines virtuelles.
- La même configuration réseau de machines virtuelles.
- La même version ESX/ESXi
- Le même numéro de version de tolérance aux pannes (ou de numéro de compilation d'hôte pour les hôtes antérieurs à ESX/ESXi 4.1).
- Les même paramètres BIOS (gestion de l'alimentation et hyperthreading) pour tous les hôtes.

Exécutez **[Vérifier la conformité]** pour identifier les incompatibilités et les corriger.

Performances

Pour accroître la bande passante disponible pour le trafic de journalisation entre les machines virtuelles principales et secondaires, utilisez un adapteur réseau 10 Gbit au lieu d'un modèle 1 Gbit et activez l'utilisation des Trames jumbo.

Stocker les images ISO sur des stockages partagés pour un accès permanent

Les images ISO auxquelles accèdent les machines virtuelles dont la tolérance aux pannes est activée doivent être conservées sur des stockages partagés qui sont accessibles aux deux instances de machines virtuelles tolérantes aux pannes. Si cette configuration est utilisée, le CD-ROM dans la machine virtuelle continue à fonctionner correctement, même en cas de basculement.

Pour les machines virtuelles dont la tolérance aux pannes est activée, il est possible d'utiliser les images ISO qui sont uniquement accessibles par la machine virtuelle principale. Dans ce cas, la machine virtuelle principale peut accéder à l'image ISO, mais en cas de défaillance, le CD-ROM signale les erreurs comme s'il n'y avait pas de support. Cette situation peut être tolérée si le CD-ROM est utilisé pour une opération provisoire et non critique comme une installation.

Basculements vers des machines virtuelles

Une machine virtuelle principale ou secondaire peut basculer, même si son hôte ESX/ESXi n'est pas défectueux. Dans ce cas, l'exécution de la machine virtuelle n'est pas interrompue mais la redondance est temporairement perdue. Pour éviter ce type de basculement, soyez conscient de quelques-unes des situations pouvant survenir et prenez des mesures pour les éviter.

Panne matérielle partielle liée au stockage

Ce problème peut survenir lorsque l'accès au stockage est lent ou interrompu sur l'un des hôtes. Lorsque cela se produit, de nombreuses erreurs de stockage sont présentes dans le journal VMkernel. Pour résoudre ce problème, vous devez éliminer les problèmes de stockage.

Panne matérielle partielle liée au réseau

Si la carte réseau de journalisation ne fonctionne pas ou si les connexions à d'autres hôtes via cette carte réseau sont défectueuses, cela risque de déclencher le basculement d'une machine virtuelle tolérante aux pannes de façon à rétablir la redondance. Pour éviter ce problème, dédiez un adapteur réseau séparée au trafic de journalisation vMotion et FT et exécutez uniquement les migrations vMotion quand les machines virtuelles sont moins actives.

Bande passante insuffisante sur le réseau de la carte de journalisation

Cela peut se produire lorsque trop de machines virtuelles tolérantes aux pannes se trouvent sur un hôte. Pour résoudre ce problème, répartissez davantage les paires de machines virtuelles tolérantes aux pannes entre les hôtes.

Défaillances de vMotion en raison du niveau d'activité des machines virtuelles

En cas d'échec de la migration vMotion d'une machine virtuelle tolérante aux pannes, celle-ci peut avoir besoin d'être basculée. Cela se produit généralement lorsque la machine virtuelle est trop active pour que la migration soit achevée avec seulement des perturbations minimales de l'activité. Pour éviter ce problème, effectuez uniquement les migrations vMotion quand les machines virtuelles sont moins actives.

Une activité excessive sur le volume VMFS peut entraîner le basculement des machines virtuelles

Lorsqu'un certain nombre d'opérations de verrouillage du système de fichiers, de mises hors et sous tension des machines virtuelle ou de migrations vMotion se produisent sur un seul volume VMFS, cela risque de déclencher le basculement des machines virtuelles tolérantes aux pannes. La réception de nombreux avertissements relatifs à des réservations SCSI dans le journal VMkernel peut être un symptôme. Pour résoudre ce problème, réduisez le nombre d'opérations dans le système de fichiers ou vérifiez que la machine virtuelle tolérante aux pannes se trouve sur un volume VMFS qui ne contient pas un grand nombre de machines virtuelles régulièrement mises sous tension, mises hors tension ou migrées à l'aide de vMotion.

Le manque d'espace dans le système de fichiers empêche le démarrage d'une machine virtuelle secondaire

Vérifiez que les systèmes de fichiers /(root) ou /vmfs/*datasource* ont de l'espace disponible. Ces systèmes de fichiers peuvent être pleins pour de nombreuses raisons et un manque d'espace peut empêcher le démarrage d'une nouvelle machine virtuelle secondaire.

Mise à niveau des hôtes utilisés pour la tolérance aux pannes

Lorsque vous mettez à niveau des hôtes qui contiennent des machines virtuelles tolérantes aux pannes, vérifiez que les machines virtuelles principales et secondaires continuent à être exécutées sur des hôtes ayant le même numéro de version de tolérance aux pannes ou de numéro de compilation d'hôte (pour les hôtes antérieurs à ESX/ESXi 4.1).

Prérequis

Vérifiez que vous possédez des privilèges d'administrateur sur les clusters.

Vérifiez que vous possédez des jeux de quatre hôtes ESX/ESXi ou davantage hébergeant des machines virtuelles tolérantes aux pannes sous tension. Si les machines virtuelles sont hors tension, les machines virtuelles principales et secondaires tolérantes aux pannes peuvent être déplacées sur des hôtes de versions différentes.

Remarque Cette procédure de mise à niveau est adaptée aux clusters de quatre nœuds au minimum. Les mêmes instructions peuvent être suivies avec un plus petit cluster, mais les intervalles sans protection seront légèrement plus longs.

Procédure

1 Avec vMotion, migrez les machines virtuelles tolérantes aux pannes à partir des deux hôtes.

2 Mettez à niveau les deux hôtes évacués avec la même version d'ESX/ESXi.

3 Désactivez la tolérance aux pannes sur la machine virtuelle principale.

4 Avec vMotion, déplacez la machine virtuelle principale vers l'un des hôtes mis à niveau.

5 Activez la tolérance aux pannes sur la machine virtuelle principale qui a été déplacée.

6 Répétez Étape 1 à Étape 5 pour autant de paires de machines virtuelles tolérantes aux pannes que les hôtes mis à niveau peuvent en accueillir.

7 Avec vMotion, répartissez les machines virtuelles tolérantes aux pannes.

Tous les hôtes ESX/ESXi d'un cluster sont mis à niveau.

Recommandations de configuration de la tolérance aux pannes par VMware

VMware vous recommande de respecter certaines directives lors de la configuration de la tolérance aux pannes.

- En plus des machines virtuelles non tolérantes aux pannes, vous ne devez pas avoir plus de quatre machines virtuelles (principales ou secondaires) tolérantes aux pannes par hôte unique. Le nombre de machines virtuelles tolérantes aux pannes que vous pouvez exécuter en toute sécurité sur chaque hôte est basé sur la taille et la charge de travail variables des hôtes ESX/ESXi et des machines virtuelles.
- Si vous accédez au stockage partagé par NFS, utilisez du matériel NAS dédié avec un adapteur réseau de 1 Gbit au minimum pour parvenir aux performances réseaux requises pour le bon fonctionnement de la tolérance aux pannes.
- Veillez à ce qu'un pool de ressources contenant des machines virtuelles tolérantes aux pannes dispose de réserves de mémoire dépassant la capacité de mémoire des machines virtuelles. La réservation de mémoire d'une machine virtuelle à tolérance aux pannes est définie par la taille de la mémoire de la machine virtuelle lorsque la tolérance aux pannes est activée. Sans cet excédent de pool de ressources, il risque de ne pas y avoir de mémoire disponible comme capacité supplémentaire.
- Utilisez 16 disques virtuels au maximum par machine virtuelle tolérante aux pannes.
- Pour assurer la redondance et une protection maximale de la tolérance aux pannes, il est recommandé d'avoir un nombre minimum de trois hôtes par cluster. Dans une situation de basculement, on dispose ainsi d'un hôte capable de gérer la nouvelle machine virtuelle secondaire qui est créée.

Dépannage de la tolérance aux pannes

Il est nécessaire de connaître quelques rubriques de dépannage pour conserver un haut niveau de performance et de stabilité pour les machines virtuelles tolérantes aux pannes et pour réduire les taux de basculement.

Les rubriques de dépannage traitent essentiellement de problèmes que vous risquez de rencontrer au cours de l'utilisation de la fonction Tolérance aux pannes VMware sur les machines virtuelles. Les rubriques expliquent également comment résoudre les problèmes.

Vous pouvez vous référer aux informations fournies en annexe *Messages d'erreurs de tolérance aux pannes* pour faciliter le dépannage de la tolérance aux pannes. L'annexe contient la liste des messages d'erreurs que vous pourriez rencontrer lorsque vous essayez d'utiliser la fonction, ainsi que des conseils sur la résolution de l'erreur, le cas échéant.

La virtualisation matérielle doit être activée

Vous devez activer la virtualisation matérielle (HV) avant d'utiliser VMware Fault Tolerance.

Problème

Lorsque vous essayez de mettre sous tension une machine virtuelle dont la Tolérance aux pannes est activée, un message d'erreur risque d'apparaître si vous n'avez pas activé HV.

Cause

Ceci est souvent dû au fait que la virtualisation matérielle (HV) n'est pas disponible sur le serveur ESX/ESXi sur lequel vous essayez de mettre sous tension la machine virtuelle. Il est possible que la virtualisation matérielle ne soit pas non plus disponible parce qu'elle n'est pas prise en charge par les composants matériels du serveur ESX/ESXi ou qu'elle n'a pas été activée dans le BIOS.

Solution

Si les composants matériels du serveur ESX/ESXi prennent en charge la virtualisation matérielle, mais que celle-ci n'est pas activée, activez-la dans le BIOS du serveur. Le processus d'activation de la virtualisation matérielle varie en fonction du BIOS. Reportez-vous à la documentation du BIOS de vos hôtes pour plus d'informations sur la configuration de la virtualisation matérielle.

Si les composants matériels du serveur ESX/ESXi ne prennent pas en charge la virtualisation matérielle, basculez sur des composants matériels qui utilisant des processeurs qui prennent en charge la tolérance aux pannes.

Des hôtes compatibles doivent être disponibles pour les machines virtuelles secondaires

Si vous mettez sous tension une machine virtuelle avec la Tolérance aux pannes activée et qu'aucun hôte compatible n'est disponible pour sa machine virtuelle secondaire, un message d'erreur s'affichera peut-être.

Problème

Le message d'erreur suivant est susceptible de s'afficher dans le panneau Tâches récentes :

```
La machine virtuelle secondaire ne peut être allumée car il n'existe pas d'hôte compatible.
```

Cause

Ce problème peut s'expliquer de différentes manières. Parmi les causes possibles, on peut citer le fait qu'il n'y a pas d'autres hôtes dans le cluster, qu'il n'y a pas d'autres hôtes dont la virtualisation matérielle est activée, que les banques de données sont inaccessibles, qu'il n'y a pas de capacité disponible ou que les hôtes sont en mode maintenance.

Solution

S'il n'y a pas suffisamment d'hôtes, ajoutez-en davantage dans le cluster. S'il y a des hôtes dans le cluster, vérifiez qu'ils prennent en charge la virtualisation matérielle et que celle-ci est activée. Le processus d'activation de la virtualisation matérielle varie en fonction du BIOS. Reportez-vous à la documentation du BIOS de vos hôtes pour plus d'informations sur la configuration de la virtualisation matérielle. Vérifiez que les hôtes disposent de capacité suffisante et qu'ils ne sont pas en mode de maintenance.

Une machine virtuelle secondaire sur un hôte surchargé dégrade les performances de la machine virtuelle principale

Lorsqu'une machine virtuelle principale semble ralentie, alors que la charge de travail de son hôte est légère et qu'elle conserve du temps de CPU inactif, vérifiez que l'hôte sur lequel la machine virtuelle secondaire est exécutée n'est pas surchargé.

Problème

Lorsqu'une machine virtuelle secondaire réside sur un hôte fortement chargé, ceci peut affecter la performance de la machine virtuelle principale.

Une manifestation de ce problème peut être le voyant jaune ou rouge pour l'intervalle vLockstep sur le panneau de tolérance aux pannes de la machine virtuelle principale. Cela signifie que la machine virtuelle secondaire a quelques secondes de retard par rapport à la machine virtuelle principale. Dans ce cas, la tolérance aux pannes ralentit la machine virtuelle principale. Si l'intervalle vLockstep reste jaune ou rouge de manière prolongée, cela indique que la machine virtuelle secondaire ne bénéficie pas de suffisamment de ressources CPU pour suivre la machine virtuelle principale.

Cause

Une machine virtuelle secondaire exécutée sur un hôte dont les ressources de CPU sont surchargées ne bénéficiera pas nécessairement de la même quantité de ressources CPU que la machine virtuelle principale. Si c'est le cas, la machine virtuelle principale doit ralentir pour que la machine virtuelle secondaire parvienne à la suivre. Elle réduit alors sa vitesse d'exécution pour atteindre la vitesse inférieure de la machine virtuelle secondaire.

Solution

Pour résoudre ce problème, définissez une réservation de CPU explicite pour la machine virtuelle principale en réglant une valeur en MHz suffisante pour l'exécution de la charge de travail au niveau de performances requis. Cette réservation est appliquée à la fois aux machines virtuelles principale et secondaire, ce qui garantit qu'elles pourront toutes deux fonctionner à la vitesse spécifiée. Pour vous aider à définir cette réservation, consultez les courbes de performances de la machine virtuelle (avant l'activation de la tolérance aux pannes) pour vérifier la quantité de ressources CPU utilisée dans des conditions normales.

Les machines virtuelles ayant une grosse mémoire peuvent empêcher l'utilisation de la tolérance aux pannes

Il est uniquement possible d'activer la tolérance aux pannes sur les machines virtuelles dont la mémoire ne dépasse pas 64 Go.

Problème

L'activation de la Tolérance aux pannes sur une machine virtuelle possédant plus de 64 Go peut échouer. La migration d'une machine virtuelle tolérante aux pannes, en cours d'exécution et utilisant vMotion, risque aussi d'échouer si sa mémoire dépasse 15 Go ou si celle-ci change à une vitesse supérieure à la capacité de copie de vMotion sur le réseau.

Cause

Cela se produit à cause de la capacité de mémoire de la machine virtuelle, il n'y a plus suffisamment de bande passante pour achever l'opération de basculement vMotion pendant le délai d'expiration par défaut (8 secondes).

Solution

Pour résoudre ce problème, avant d'activer la tolérance aux pannes, éteignez la machine virtuelle et augmentez son délai d'expiration en ajoutant la ligne suivante dans le fichier vmx de la machine virtuelle :

```
ft.maxSwitchoverSeconds = "30"
```

où 30 est le délai d'expiration en nombre de secondes. Activez la tolérance aux pannes et rallumez la machine virtuelle. Cette solution devrait être efficace lorsque le réseau présente une forte activité.

Remarque Si vous augmentez le délai d'expiration à 30 secondes, la machine virtuelle tolérante aux pannes risque de ne plus répondre pendant une durée plus longue (jusqu'à 30 secondes) lors de l'activation de la tolérance aux pannes ou lorsqu'une nouvelle machine virtuelle secondaire est créée suite à un basculement.

L'utilisation de la CPU par la machine virtuelle secondaire semble excessive

Dans certains cas, vous constaterez que l'utilisation de la CPU pour une machine virtuelle secondaire est supérieure à celle de la machine virtuelle principale qui y est associée.

Problème

Lorsque la machine virtuelle principale est inactive, la différence relative entre les machines virtuelles principale et secondaire peut paraître importante.

Cause

Le fait de relire des événements (comme des interruptions du temporisateur) sur la machine virtuelle secondaire peut être légèrement plus coûteux en charge de calcul que leur enregistrement sur la machine virtuelle principale. Cette charge additionnelle est minime.

Solution

Aucune requise. L'examen de l'utilisation effective de la CPU révèle que très peu de ressources CPU sont utilisées par la machine virtuelle principale ou secondaire.

Annexe : Message d'erreurs de tolérance aux pannes

Vous rencontrerez parfois des messages d'erreurs dans le cas de l'utilisation de VMware Fault Tolerance (FT). Les tableaux ci-dessous énumèrent quelques messages d'erreurs. Chaque message d'erreur s'accompagne d'une description et d'informations sur la résolution de l'erreur, le cas échéant. En plus de l'onglet **[Tâches et événements]** de vSphere Client, vous pouvez aussi consulter les erreurs de tolérance aux pannes dans l'onglet **[Récapitulatif]** de la machine virtuelle.

Messages d'erreurs de configuration de tolérance aux pannes

Le tableau ci-dessous énumère quelques messages d'erreurs qui apparaissent lorsque votre hôte ou cluster n'est pas configuré correctement pour la prise en charge de la tolérance aux pannes. Reportez-vous à « Liste de vérification de tolérance aux pannes », page 36 pour plus d'informations sur les exigences de configuration des hôtes et des clusters pour la tolérance aux pannes.

Tableau A-1. Erreurs de configuration

Message d'erreur	Description et solution
La CPU de l'hôte n'est pas compatible avec les exigences requises pour la machine virtuelle. Non-concordance détectée pour les fonctions suivantes : La CPU ne correspond pas	La tolérance aux pannes exige que les hôtes des machines virtuelles principales et secondaires utilisent la même CPU. Activez la tolérance aux pannes sur une machine virtuelle enregistrée sur un hôte ayant un modèle de CPU, une famille et une version concordants dans le cluster. Si ce type d'hôtes n'existe pas, vous devez en ajouter un . Ces erreurs se produisent aussi lorsque vous tentez de migrer une machine virtuelle tolérante aux pannes sur un autre hôte.
La configuration de la tolérance aux pannes de l'entité {entityName} pose un problème : La tolérance aux pannes n'est pas prise en charge par les composants matériels de l'hôte	La tolérance aux pannes est uniquement prise en charge sur des processeurs spécifiques et des configurations de BIOS avec la virtualisation matérielle (HV) activée. Pour résoudre ce problème, utilisez des hôtes ayant des modèles de CPU et des configurations de BIOS compatibles.
La ROM de la machine virtuelle n'est pas prise en charge	La machine virtuelle utilise un noyau VMI et est paravirtualisée. VMI n'est pas pris en charge par la tolérance aux pannes et doit être désactivé pour la machine virtuelle.
L'hôte {hostName} a rencontré des problèmes de tolérance aux pannes pour la machine virtuelle {vmName}. Consultez la liste des erreurs pour plus d'informations	Pour résoudre ce problème, dans vSphere Client, sélectionnez l'opération de tolérance aux pannes défectueuse dans le volet Tâches récentes ou dans l'onglet **[Tâches et événements]** et cliquez sur le lien **[Détails de vue]** qui apparaît dans la colonne Détails.
La configuration de la tolérance aux pannes de l'entité {entityName} pose un problème : vérifiez les certificats de l'hôte non définis pour vCenter Server	La case "Vérifier les certificats de l'hôte" n'est pas cochée dans les paramètres SSL de vCenter Server. Vous devez cocher cette case. Reportez-vous à « Activer la vérification du certificat de l'hôte », page 39.
La configuration de la tolérance aux pannes de l'entité {entityName} pose un problème : HA n'est pas activé sur la machine virtuelle	Cette machine virtuelle se trouve sur un hôte qui n'est pas dans un cluster VMware HA ou VMware HA a été désactivé. La tolérance aux pannes exige VMware HA.

Tableau A-1. Erreurs de configuration (suite)

Message d'erreur	Description et solution
La configuration de la tolérance aux pannes de l'entité {entityName} pose un problème : L'hôte est inactif	Vous devez activer la tolérance aux pannes sur un hôte actif. Un hôte est dit inactif lorsqu'il est déconnecté, en mode maintenance ou en veille.
L'hôte {hostName} ne dispose pas d'une licence pour la tolérance aux pannes.	Toutes les éditions de VMware vSphere ne disposent pas d'une licence pour la tolérance aux pannes. Vérifiez la version utilisée et mettez-la à niveau vers une version qui comprend la tolérance aux pannes.
La configuration de la tolérance aux pannes de l'entité {entityName} pose un problème : aucune licence vMotion ou carte réseau virtuelle n'est configurée pour vMotion	Vérifiez que vous avez configuré correctement le réseau sur l'hôte. Reportez-vous à « Configurer la mise en réseau des machines hôtes », page 40. Si c'est le cas, vous devez éventuellement acheter une licence vMotion.
La configuration de la tolérance aux pannes de l'entité {entityName} pose un problème : aucun adapteur réseau virtuelle n'est configurée pour la journalisation de la tolérance aux pannes	Aucun adapteur réseau de journalisation de la tolérance aux pannes n'a été configurée. Consultez « Configurer la mise en réseau des machines hôtes », page 40 pour plus d'informations.
L'hôte {hostName} ne prend pas en charge les machines virtuelles dont la tolérance aux pannes est activée. Ce produit VMware ne prend pas en charge la tolérance aux pannes.	Le produit utilisé n'est pas compatible avec la tolérance aux pannes. Pour utiliser le produit, vous devez mettre hors tension la tolérance aux pannes. Ce message d'erreur apparaît principalement quand vCenter Server gère un hôte ayant une version précédente d'ESX/ESXi ou en cas d'utilisation de VMware Server.
La configuration de la tolérance aux pannes de l'entité {entityName} pose un problème : La tolérance aux pannes n'est pas prise en charge par VMware Server 2.0	Mettez à niveau vers la version VMware ESX ou ESXi 4.1 ou une version ultérieure.
La version compilation ou la version de la fonction de tolérance aux pannes de l'hôte de destination est différente de la version build actuelle ou de la version de la fonction de tolérance aux pannes : {build}.	Les versions de la fonction de tolérance aux pannes doivent être identiques sur les hôtes actuels et de destination. Choisissez un hôte compatible ou mettez à niveau des hôtes incompatibles.

Erreurs de configuration des machines virtuelles

Quelques problèmes de configuration des machines virtuelles peuvent générer des messages d'erreurs.

Deux messages d'erreurs risquent d'apparaître lorsque la configuration des machines virtuelles ne prend pas en charge la tolérance aux pannes.

- La configuration de la tolérance aux pannes de l'entité {entityName} pose un problème : la configuration actuelle de la machine virtuelle ne prend pas en charge la tolérance aux pannes
- La configuration de la tolérance aux pannes de l'entité {entityName} pose un problème : les fonctions d'enregistrement et de lecture ne sont pas prises en charge par la machine virtuelle

La tolérance aux pannes fonctionne uniquement sur une machine virtuelle ayant une seule vCPU. Les erreurs suivantes risquent de se produire lorsque vous essayez d'activer la tolérance aux pannes sur une machine virtuelle ayant plusieurs vCPU :

- La machine virtuelle a {numCpu} CPU virtuelles et n'est pas prise en charge à cause de : Tolérance aux pannes
- La configuration de la tolérance aux pannes de l'entité {entityName} pose un problème : machine virtuelle ayant plusieurs CPU virtuelles.

La tolérance aux pannes n'est pas compatible avec certaines fonctions vSphere. Si vous essayez d'activer la tolérance aux pannes sur une machine virtuelle utilisant une fonction vSphere qui ne prend pas en charge la tolérance aux pannes, l'un des messages d'erreurs suivants risque d'apparaître. Pour utiliser la tolérance aux pannes, vous devez mettre hors tension la fonction vSphere sur la machine virtuelle problématique ou activer la tolérance aux pannes sur une machine virtuelle qui n'utilise pas ces fonctions.

- La configuration de la tolérance aux pannes de l'entité {entityName} pose un problème : la machine virtuelle a un ou deux snapshots
- La configuration de la tolérance aux pannes de l'entité {entityName} pose un problème : machine virtuelle modèle

Les messages d'erreurs suivants risquent d'apparaître si la machine virtuelle comporte un périphérique non pris en charge. Pour activer la tolérance aux pannes sur cette machine virtuelle, supprimez le périphérique non pris en charge, puis activez la tolérance aux pannes.

- La sauvegarde de fichiers ({backingFilename}) pour le périphérique de disque virtuel n'est pas prise en charge par la tolérance aux pannes
- La sauvegarde de fichiers ({backingFilename}) pour le périphérique de disquette virtuelle n'est pas prise en charge par la tolérance aux pannes
- La sauvegarde de fichiers ({backingFilename}) pour le périphérique de CDROM virtuel n'est pas prise en charge par la tolérance aux pannes
- La sauvegarde de fichiers ({backingFilename}) pour le port série virtuel n'est pas prise en charge par la tolérance aux pannes
- La sauvegarde de fichiers ({backingFilename}) pour le port parallèle virtuel n'est pas prise en charge par la tolérance aux pannes

Le tableau suivant énumère d'autres erreurs de configuration des machines virtuelles. Consultez « Interopérabilité de la tolérance aux pannes », page 37 pour plus d'informations.

Tableau A-2. Autres problèmes de configuration des machines virtuelles

Message d'erreur	Description et solution
L'hôte spécifié n'est pas compatible avec la machine virtuelle secondaire tolérante aux pannes.	Reportez-vous à « Dépannage de la tolérance aux pannes », page 49 pour des causes possibles de cette erreur.
Hôte non compatible pour la machine virtuelle secondaire {vm.name}	Reportez-vous à « Dépannage de la tolérance aux pannes », page 49 pour des causes possibles de cette erreur.
Le disque {Périphérique} de la machine virtuelle utilise le mode disque {mode} qui n'est pas pris en charge.	La machine virtuelle est équipée d'un ou de plusieurs disques durs configurés pour utiliser le mode Indépendant. Modifiez les paramètres de la machine virtuelle, sélectionnez chaque disque dur et désactivez le mode Indépendant. Adressez-vous à votre administrateur système pour savoir ce qui est acceptable pour l'environnement.

Tableau A-2. Autres problèmes de configuration des machines virtuelles (suite)

Message d'erreur	Description et solution
Les blocs inutilisés des disques de la machine virtuelle n'ont pas été nettoyés sur le système de fichiers. Le nettoyage est nécessaire pour la prise en charge de fonctions comme la tolérance aux pannes.	Vous avez essayé d'activer la tolérance aux pannes sur une machine virtuelle sous tension ayant des disques à provisionnement lourd avec la propriété zéros différés. La tolérance aux pannes ne peut pas être activée sur ce type de machine virtuelle lorsqu'elle est allumée. Mettez la machine virtuelle hors tension, puis activez la tolérance aux pannes, puis rallumez la machine virtuelle. Cela modifie le format du disque de la machine virtuelle lorsqu'elle est remise sous tension. L'activation de la tolérance aux pannes peut nécessiter un certain temps pour terminer si le disque virtuel a une grosse capacité.
Les blocs des disques de la machine virtuelle n'ont pas été entièrement provisionnés sur le système de fichiers. Le nettoyage est nécessaire pour la prise en charge de fonctions comme la tolérance aux pannes.	Vous avez essayé d'activer la tolérance aux pannes sur une machine virtuelle sous tension ayant des disques à provisionnement allégé. La tolérance aux pannes ne peut pas être activée sur ce type de machine virtuelle lorsqu'elle est allumée. Mettez la machine virtuelle hors tension, puis activez la tolérance aux pannes, puis rallumez la machine virtuelle. Cela modifie le format du disque de la machine virtuelle lorsqu'elle est remise sous tension. L'activation de la tolérance aux pannes peut nécessiter un certain temps pour terminer si le disque virtuel a une grosse capacité.

Erreurs d'exploitation

Le tableau ci-dessous énumère les messages d'erreurs qui apparaissent en cours d'utilisation des machines virtuelles tolérantes aux pannes.

Tableau A-3. Erreurs d'exploitation

Message d'erreur	Description et solution
Aucun hôte adapté n'a été trouvé pour placer la machine virtuelle secondaire tolérante aux pannes pour la machine virtuelle {vmName}	La tolérance aux pannes exige que les hôtes des machines virtuelles principales et secondaires utilisent la même CPU ou famille, le même numéro de version de tolérance aux pannes ou numéro de compilation d'hôte et niveau de correctif. Activez la tolérance aux pannes sur une machine virtuelle enregistrée sur un hôte ayant un modèle de CPU ou une famille concordants dans le cluster. Si ce type d'hôtes n'existe pas, vous devez en ajouter un .
La machine virtuelle secondaire tolérante aux pannes n'a pas été activée car la machine virtuelle principale tolérante aux pannes n'a pas été activée.	vCenter Server signalera la raison de l'impossibilité d'activer la machine virtuelle principale. Corrigez les conditions, puis réessayez l'opération.
L'activation de la machine virtuelle secondaire tolérante aux pannes pour {vmName} n'a pas pu être effectuée dans un délai de {timeout} secondes.	Réessayez de mettre sous tension la machine virtuelle secondaire. Le délai d'expiration peut être imputable à des problèmes de réseau ou d'autres problèmes temporaires.
vCenter a désactivé la tolérance aux pannes sur la machine virtuelle {vm.name} car la machine virtuelle secondaire n'a pas pu être activée.	Pour diagnostiquer la raison de l'impossibilité d'activer la machine virtuelle secondaire, reportez-vous à « Dépannage de la tolérance aux pannes », page 49.
Nouvelle synchronisation des machines virtuelles principale et secondaire	La tolérance aux pannes a détecté une différence entre les machines virtuelles principale et secondaire. Elle peut être due à des événements provisoires qui ont lieu à cause de différences matérielles ou logicielles entre les deux hôtes. La tolérance aux pannes a démarré automatiquement une nouvelle machine virtuelle secondaire et aucune action n'est requise. Si ce message apparaît souvent, signalez-le au support technique qui vérifie s'il y a un problème.

Tableau A-3. Erreurs d'exploitation (suite)

Message d'erreur	Description et solution
La configuration de la tolérance aux pannes de l'entité {entityName} pose un problème : aucune information de configuration pour la machine virtuelle	vCenter Server ne dispose pas d'informations sur la configuration de la machine virtuelle. Vérifiez si la machine virtuelle est mal configurée. Vous pouvez essayer de supprimer la machine virtuelle de l'inventaire et de la réenregistrer.
Impossible de modifier le comportement DRS de la machine virtuelle secondaire tolérante aux pannes {vmName}.	Impossible de modifier le comportement DRS sur les machines virtuelles secondaires tolérantes aux pannes. Cette configuration est héritée de la machine virtuelle principale.
Les machines virtuelles de la même paire tolérante aux pannes ne peuvent se trouver sur le même hôte.	Vous avez essayé d'activer vMotion pour une machine virtuelle secondaire avec le même hôte que celui sur lequel se trouve une machine virtuelle principale. Une machine virtuelle principale et sa machine virtuelle secondaire ne peuvent pas résider sur le même hôte. Sélectionnez un hôte de destination différent pour la machine virtuelle secondaire.
Impossible d'ajouter un hôte avec des machines virtuelles dont la tolérance aux pannes est activée sur un cluster non compatible HA.	La tolérance aux pannes exige que le cluster soit activé pour VMware HA. Modifiez les paramètres du cluster et activez VMware HA.
Impossible d'ajouter un hôte avec des machines virtuelles dont la tolérance aux pannes est activée sous la forme d'un hôte autonome.	Désactivez la tolérance aux pannes avant d'ajouter l'hôte comme hôte autonome à vCenter Server. Pour désactiver la tolérance aux pannes, ajoutez l'hôte à un cluster VMware HA, cliquez avec le bouton droit de la souris sur chaque machine virtuelle sur l'hôte et sélectionnez Arrêter tolérance aux pannes. Lorsque la tolérance aux pannes est désactivée, l'hôte peut être transformé en hôte autonome.
Impossible de régler la priorité de redémarrage HA sur Désactivé pour la machine virtuelle tolérante aux pannes {vmName}.	Ce paramètre n'est pas autorisé pour une machine virtuelle tolérante aux pannes. Cette erreur se produit uniquement en cas de réglage de la priorité de redémarrage d'une machine virtuelle tolérante aux pannes sur Désactivé.
L'hôte dispose déjà du nombre recommandé de {maxNumFtVms} machines virtuelles tolérantes aux pannes	Pour mettre sous tension ou migrer d'autres machines virtuelles tolérantes aux pannes sur cet hôte, déplacez l'une des machines virtuelles tolérantes aux pannes vers un autre hôte ou désactivez cette restriction en configurant l'option avancée VMware HA das.maxftvmsperhost sur 0.

Erreurs d'exploitation SDK

Le tableau ci-dessous énumère les messages d'erreurs qui apparaissent en cours d'utilisation de SDK.

Tableau A-4. Erreurs d'exploitation SDK

Message d'erreur	Description et solution
Cette opération n'est pas prise en charge par une machine virtuelle secondaire d'une paire tolérante aux pannes.	Une opération non prise en charge a été exécutée directement sur la machine virtuelle secondaire utilisant l'API. La tolérance aux pannes n'autorise pas l'interaction directe avec la machine virtuelle secondaire (sauf pour la déplacer ou la migrer sur un hôte différent).
La configuration de la tolérance aux pannes de l'entité {entityName} pose un problème : la machine virtuelle secondaire existe déjà	La machine virtuelle principale a déjà une machine virtuelle secondaire. N'essayez pas de créer plusieurs machines virtuelles secondaires pour la même machine virtuelle principale.

Tableau A-4. Erreurs d'exploitation SDK (suite)

Message d'erreur	Description et solution
La machine virtuelle secondaire avec instanceUuid '{instanceUuid}' a déjà été activée.	Vous avez essayé d'activer la tolérance aux pannes sur une machine virtuelle sur laquelle la tolérance aux pannes était déjà activée. Cette opération provient généralement d'un API.
La machine virtuelle secondaire avec instanceUuid '{instanceUuid}' a déjà été désactivée.	Vous avez essayé de mettre hors tension la tolérance aux pannes sur une machine virtuelle secondaire sur laquelle la tolérance aux pannes était déjà désactivée. Cette opération provient généralement d'un API.

Remarque Pour les erreurs liées à la compatibilité CPU, consultez l'article dans la base de connaissances VMware accessible à l'adresse http://kb.vmware.com/kb/1008027 pour plus d'informations sur les processeurs et les systèmes d'exploitation clients pris en charge. Vous pouvez aussi utiliser l'utilitaire VMware SiteSurvey (téléchargeable sur http://www.vmware.com/download/shared_utilities.html) pour avoir une connaissance approfondie des problèmes de configuration associés au cluster, à l'hôte et aux machines virtuelles utilisées pour VMware FT.

Index

V