Disponibilité vSphere

VMware vSphere 5.5
VMware ESXi 5.5
vCenter Server 5.5

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-001254-00

vmware®

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

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

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 Disponibilité de vSphere

Disponibilité vSphere présente les solutions permettant d'assurer la continuité d'activité, et explique notamment comment mettre en place vSphere® High Availability (HA) et vSphere Fault Tolerance.

Public ciblé

Ces informations sont destinées à tous ceux qui veulent assurer la continuité d'activité à l'aide des solutions vSphere HA et Fault Tolerance. Les informations fournies dans ce manuel sont destinées aux administrateurs système Windows ou Linux expérimentés qui connaissent le fonctionnement de la technologie des machines virtuelles et des centres de données.

Continuité d'activité et minimisation des interruptions de service 1

Qu'elles soient prévues ou imprévues, les interruptions de service engendrent des coûts considérables. Cependant les solutions assurant des niveaux élevés de disponibilité sont généralement 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 quels que soient les matériels, le système d'exploitation et les applications.
- Réduire 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 :

Réduire les 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 peuvent :

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

vSphere vMotion® et la fonctionnalité Storage vMotion de vSphere permettent 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.

Prévenir les interruptions de service imprévues

Alors qu'un hôte ESXi offre une plate-forme stable pour exécuter des 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 les 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. Des fonctions clés de disponibilité 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 adaptateurs réseau individuelles.
- chemins multiples du stockage. Assure la tolérance aux défaillances des emplacements de stockage.

En outre, les fonctions vSphere HA et Fault Tolerance peuvent réduire ou éliminer les interruptions de service imprévues en assurant respectivement la reprise rapide de l'activité suite à une interruption et la continuité de la disponibilité.

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

vSphere HA a recours à plusieurs hôtes 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.

vSphere HA protège la disponibilité des applications de la 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 cluster, vSphere 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 vSphere HA. Une fois que vSphere HA est configuré, aucune action n'est requise pour protéger de nouvelles machines virtuelles. Elles sont protégées automatiquement.
- Vous pouvez associer vSphere HA à vSphere Distributed Resource Scheduler (DRS) pour assurer la protection contre les pannes, et pour répartir la charge entre tous les hôtes d'un cluster.

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

Configuration minimale	Quand un cluster vSphere 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 vSphere HA, vous devez disposer de suffisamment de ressources pour le basculement des hôtes que vous souhaitez protéger avec vSphere 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 de VMware Tools et en redémarrant 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, vSphere HA peut faciliter la récupération suite à la défaillance.

vSphere Fault Tolerance assure la continuité de la disponibilité

vSphere HA assure un niveau de protection de base pour vos machines virtuelles en les redémarrant en cas de défaillance de l'hôte. vSphere 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.

Fault Tolerance assure la continuité de la disponibilité 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. Ceci s'effectue à l'aide de la technologie VMware vLockstep sur la plate-forme de l'hôte ESXi. 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 faisant fonctionner la machine virtuelle principale ou l'hôte faisant fonctionner la machine virtuelle secondaire est défaillant, un basculement immédiat et transparent se produit. L'hôte ESXi en état de marche devient la machine virtuelle principale sans qu'il y ait perte des connexions réseau ou des 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.

Créer et utiliser des clusters vSphere HA

2

Les clusters vSphere HA permettent à un ensemble d'hôtes ESXi de travailler conjointement, de façon à fournir aux machines virtuelles, en tant que groupe, un niveau de disponibilité supérieur à celui d'un seul hôte ESXi. Si vous envisagez de créer et d'utiliser un nouveau cluster vSphere HA, les options choisies affectent la manière dont ce cluster réagit aux pannes des hôtes ou des machines virtuelles.

Avant de créer un cluster vSphere HA, vous devez savoir comment vSphere HA identifie les pannes et l'isolation de l'hôte et comment il réagit à 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 à vos besoins de basculement. Après avoir créé un cluster, vous pouvez en personnaliser le comportement avec des attributs avancés et en optimiser les performances en suivant les recommandations.

Remarque Un message d'erreur peut apparaître lorsque vous essayez d'utiliser vSphere HA. Pour plus d'informations sur les messages d'erreur relatifs à vSphere HA, consultez l'article de la base de connaissances VMware sur http://kb.vmware.com/kb/1033634.

Ce chapitre aborde les rubriques suivantes :

Fonctionnement de vSphere HA

vSphere HA assure la disponibilité élevée des machines virtuelles en les rassemblant 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 redémarrées sur d'autres hôtes.

Lorsque vous créez un cluster vSphere HA , un seul hôte est automatiquement sélectionné en tant qu'hôte maître. L'hôte maître communique avec vCenter Server et surveille l' état de protection de toutes les machines virtuelles et des hôtes esclaves. Différents types de défaillances d'hôtes sont possibles, et l'hôte principal doit les détecter et les traiter de façon adaptée. L'hôte principal doit faire la différence entre un hôte défaillant et un hôte se trouvant dans une partition de réseau ou réseau isolé. L'hôte principal utilise le signal de pulsation de banques de données pour déterminer le type de panne.

Hôte maître et hôtes esclaves

Lorsque vous ajoutez un hôte à un cluster vSphere HA, un agent est transféré vers l'hôte et configuré pour communiquer avec les autres agents du cluster. Chaque hôte du cluster fonctionne en tant qu'hôte principal (maître) ou hôte secondaire (esclave).

Lorsque vSphere HA est activé pour un cluster, tous les hôtes actifs (ceux qui ne sont pas en mode standby ou maintenance, ou qui ne sont pas déconnectés) participent au choix de l'hôte principal du cluster. L'hôte contenant le plus grand nombre de banques de données a l'avantage pour être choisi. Habituellement, il n'existe qu'un hôte principal par cluster, tous les autres sont des hôtes secondaires. Si l'hôte principal est défaillant, fermé, mis en mode standby ou éliminé du cluster, un nouvel hôte principal doit être choisi.

L'hôte principal d'un cluster a un certain nombre de responsabilités :

- Surveiller l'état des hôtes secondaires. Si un hôte secondaire est défaillant ou devient inaccessible, l'hôte principal identifie les machines virtuelles qui doivent être redémarrées.
- Surveiller l'état d'alimentation de toutes les machines virtuelles protégées. Si une machine virtuelle est défaillante, l'hôte principal s'assure qu'elle est redémarrée. Grâce à un moteur de placement local, l'hôte principal détermine également où le redémarrage doit avoir lieu.
- Gérer les listes d'hôtes et de machines virtuelles protégées du cluster.
- Servir d'interface de gestion vCenter Server du cluster et rendre compte de l'état de santé du cluster.

Les hôtes secondaires apportent une contribution essentielle au cluster en exécutant des machines virtuelles localement, en surveillant leur état d'exécution et en communiquant les mises à jour d'état à l'hôte principal. Un hôte principal peut également exécuter et surveiller des machines virtuelles. Les hôtes principaux et les hôtes secondaires mettent en œuvre les fonctions de surveillance de VM et d'application.

Une des fonctions exercées par l'hôte maître est la coordination des redémarrages de machines virtuelles protégées. Une VM est protégée par un hôte maître après que vCenter Server observe que l'état d'alimentation de la VM est passé de hors tension à sous tension en réponse à une action de l'utilisateur. L'hôte maître conserve la liste des machines virtuelles protégées dans les banques de données du cluster. Un hôte maître nouvellement élu utilise ces informations pour déterminer quelles machines virtuelles doivent être protégées.

Remarque Si vous déconnectez un hôte d'un cluster, aucune des machines virtuelles enregistrées sur cet hôte n'est protégée par vSphere HA.

Types de pannes des hôtes et détection

L'hôte principal d'un cluster vSphere HA est responsable de la détection des pannes des hôtes secondaires. Selon le type de panne détecté, les machines virtuelles exécutées sur les hôtes peuvent nécessiter un basculement.

Dans un cluster vSphere HA, trois types de pannes d'hôtes sont détectés :

- Un hôte cesse de fonctionner (autrement dit, il est défaillant).
- Un hôte est réseau isolé.
- Un hôte perd sa connexion réseau avec l'hôte principal.

L'hôte principal surveille la réactivité des hôtes secondaires du cluster. Cette communication s'effectue par l'échange, toutes les secondes, de signaux de pulsation réseau. Lorsqu'un hôte principal cesse de recevoir des signaux de pulsation d'un hôte secondaire ou esclave, il vérifie la réactivité de l'hôte avant de le déclarer défaillant. Le contrôle de réactivité effectué par l'hôte principal permet de déterminer si l'hôte secondaire échange des signaux de pulsation avec une des banques de données. Reportez-vous à la section « Signal de pulsation de banque de données », page 16. Par ailleurs, l'hôte principal vérifie si l'hôte répond aux pings ICMP envoyés à ses adresses IP de gestion.

Si un hôte principal est incapable de communiquer directement avec l'agent présent sur un hôte secondaire, si l'hôte secondaire ne répond pas aux pings ICMP, et si l'agent n'émet pas de signaux de pulsation, il est considéré comme défaillant. Les machines virtuelles des hôtes sont redémarrées sur d'autres hôtes. Si un tel hôte secondaire échange des signaux de pulsation avec une banque de données, l'hôte principal considère qu'il se trouve dans une partition de réseau ou qu'il est réseau isolé, et continue donc de surveiller l'hôte et ses machines virtuelles. Reportez-vous à la section « Partitions de réseau », page 16.

L'isolation du réseau de l'hôte survient lorsqu'un hôte, toujours en cours d'exécution, ne parvient plus à observer le trafic provenant des agents vSphere HA sur le réseau de gestion. Si un hôte cesse d'observer ce trafic, il tente d'envoyer un ping aux adresses d'isolation du cluster. Si cela échoue aussi, l'hôte se déclare isolé du réseau.

L'hôte principal surveille les machines virtuelles exécutées sur un hôte isolé. S'il constate qu'elles s'arrêtent, et s'il est responsable de ces machines virtuelles, il les redémarre.

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.

Déterminer les réponses aux problèmes de l'hôte

Si un hôte tombe en panne et que ses machines virtuelles doivent être redémarrées, vous pouvez contrôler l'ordre dans lequel cela se fait la priorité de redémarrage de la VM. De même, vous pouvez configurer la réponse de vSphere HA lorsque des hôtes perdent la connectivité au réseau de gestion à d'autres hôtes en utilisant les paramètres de réponse d'isolation.

Ces paramètres s'appliquent à toutes les machines virtuelles du cluster en cas de défaillance ou d'isolement d'un hôte. Vous pouvez configurer des exceptions pour des machines virtuelles spécifiques. Reportez-vous à la section « Personnaliser une VM individuelle dans vSphere Web Client », page 35.

Priorité de redémarrage des VM

La priorité de redémarrage VM détermine l'ordre relatif dans lequel les machines virtuelles sont placées sur un nouvel hôte après une panne d'hôte. Les machines virtuelles sont redémarrées séquentiellement sur leurs nouveaux hôtes, en commençant par les machines virtuelles ayant la priorité la plus élevée, puis 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. Notez que si vSphere HA ne parvient pas à mettre sous tension une machine virtuelle à haute priorité, il tentera le processus avec les machines virtuelles de priorité inférieure. Pour cette raison, la priorité de redémarrage des VM ne peut être utilisée pour appliquer une priorité de redémarrage pour une application avec plusieurs machines virtuelles. De même, 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 des ressources supplémentaires ne seront pas disponibles. Les machines virtuelles sont redémarrées sur les hôtes de basculement, s'ils ont été préalablement définis.

Les valeurs de ce paramètre sont les suivantes : Désactivé, Basse, Moyen (par défaut) et Haut. Si l'option Désactivé est sélectionnée, vSphere HA est désactivé pour la machine virtuelle, ce qui signifie qu'elle n'est pas redémarrée sur d'autres hôtes ESXi en cas de dysfonctionnement de son hôte. Le paramètre Désactivé est ignoré par la fonction Surveillance de VM et d'application de vSphere HA car cette fonction protège les machines virtuelles contre les pannes de niveau système d'exploitation et non contre les pannes de machine virtuelle. Lorsqu'une panne se produit au niveau du système d'exploitation, vSphere HA redémarre le système d'exploitation et la machine virtuelle est laissée en fonctionnement sur le même hôte. Vous pouvez modifier ce paramètre pour des machines virtuelles individuelles.

Remarque La réinitialisation d'une machine virtuelle provoque un redémarrage du système d'exploitation client mais ne place pas la machine virtuelle en cycle d'alimentation.

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

Par exemple, dans le cas d'une application multitâche, vous pouvez classer les attributions en fonction 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.

Réponse d'isolation de l'hôte

La réponse à l'isolement d'un hôte détermine les événements survenant lorsqu'un hôte d'un cluster vSphere HA perd ses connexions au réseau de gestion mais continue à fonctionner. Vous pouvez utiliser la réponse d'isolation pour que vSphere HA atteigne les machines virtuelles en cours d'exécution sur un hôte isolé et les redémarrer sur un hôte non isolé hôte. Les réponses à l'isolement d'un hôte exigent que l'État de surveillance de l'hôte soit activé. Si l'état de surveillance de l'hôte est désactivé, les réponses à l'isolement d'un hôte sont également suspendues. Un hôte détermine qu'il est isolé lorsqu'il est incapable de communiquer avec les agents en cours d'exécution sur les autres hôtes et d'envoyer un ping à ses adresses d'isolement. Lorsque cela se produit, l'hôte exécute sa réponse d'isolement. Les réponses sont les suivantes : Laisser sous tension (la valeur par défaut), Mettre hors tension, puis basculer et Arrêter, puis basculer. Vous pouvez personnaliser cette propriété pour des machines virtuelles individuelles.

Remarque Si le paramètre de priorité de redémarrage d'une machine virtuelle est défini sur Désactiver, aucune réponse d'isolation de l'hôte n'est effectuée.

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 préserver son état. L'arrêt est préférable à la mise hors tension de la machine virtuelle qui ne prend pas en compte pas les dernières modifications apportées aux disques ni ne valide les transactions. Le basculement des machines virtuelles qui sont en train de se fermer est plus long car la fermeture doit aussi être effectuée. 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 vSphere HA, vous pouvez changer les paramètres par défaut du cluster relatifs à la Priorité de redémarrage et à la Réponse à l'isolement de machines virtuelles spécifiques. Ces remplacements sont utiles pour les machines virtuelles qui sont utilisées pour des 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.

Si la réponse à l'isolement d'un hôte est désactivée (autrement dit, s'il laisse les machines virtuelles sous tension lorsqu'il est isolé) et si l'hôte n'a plus accès au réseau de gestion et au réseau de stockage, une situation de division peut survenir. Dans ce cas, l'hôte isolé perd le verrouillage des disques et les machines virtuelles sont basculées vers un autre hôte, même si les instances d'origine des machines virtuelles continuent de s'exécuter sur l'hôte isolé. Lorsque l'hôte retrouve l'accès à la banque de données de la VM, il y aura deux copies des VM, bien que la copie sur l'hôte initialement isolé n'ait pas accès aux fichiers vmdk et que la corruption des données soit empêchée.

Pour résoudre ce problème, ESXi génère une question sur la machine virtuelle qui a perdu les verrouillages disque pour le moment où l'hôte quittera son état d'isolation et réalise qu'il ne peut pas obtenir de nouveau les verrouillages disque. vSphere HA répond automatiquement à cette question ce qui permet à l'instance de la machine virtuelle qui a perdu les verrouillages disque de s'arrêter, laissant uniquement l'instance qui dispose des verrouillages disque.

Surveillance des VM et applications

Surveillance de VM redémarre les machines virtuelles si leurs signaux de pulsation de VMware Tools n'ont pas été reçus pendant un certain temps. De même, la Surveillance d'application peut redémarrer une machine virtuelle si les signaux de pulsation 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 vSphere HA.

Lorsque vous activez la Surveillance de VM, le service Surveillance de VM (à l'aide de VMware Tools) vérifie si chaque machine virtuelle du cluster fonctionne en vérifiant la régularité des signaux de pulsations et l'activité des E/S à partir du processus VMware Tools exécuté sur le client. Si aucun signal de pulsation ou activité des E/S n'est reçu, cela est probablement dû à une défaillance du système d'exploitation client ou au fait que les VMware Tools n'ont pas eu le temps de terminer certaines tâches. Dans ce cas, le service Surveillance de VM détermine que la machine virtuelle est défectueuse et la machine virtuelle redémarre pour restaurer le service.

Il arrive qu'occasionnellement, les machines virtuelles ou les applications qui continuent à fonctionner correctement, cessent d'émettre des signaux de pulsation. Pour éviter les réinitialisations inutiles, le service Surveillance de VM surveille aussi l'activité des E/S d'une machine virtuelle. Si aucun signal de pulsation n'est reçu pendant la période de défaillance, la fréquence des statistiques des E/S (attribut défini au niveau du cluster) est vérifiée. La fréquence des statistiques des E/S détermine si un disque ou une activité réseau s'est produite sur la machine virtuelle au cours des deux minutes (120 secondes) précédentes. 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 signaux de pulsation personnalisés pour les applications à surveiller. Après avoir fait cela, la surveillance d'application fonctionne de la même manière que la Surveillance de VM. Si les signaux de pulsation d'une application ne sont pas reçus 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 cela est peu probable, une sensibilité de surveillance élevée peut entraîner l'identification erronée de dysfonctionnements alors que la machine virtuelle ou l'application en question fonctionne toujours mais les signaux de pulsation ne sont pas reçus du fait de certains facteurs tels que des contraintes de ressources. Une sensibilité de surveillance basse se traduit par des interruptions de service prolongées entre les défaillances avérées et le redémarrage des machines virtuelles. Sélectionnez l'option qui offre un compromis intéressant par rapport 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 de statistiques d'E/S en cochant la case **Personnalisé**.

Tableau 2-1. Paramètres de surveillance des machines virtuelles

Paramètre	Intervalle de défaillance (en secondes)	Période de réinitialisation
Haut	30	1 heure
Moyen	60	24 heures
Faible	120	7 jours

Lorsque des dysfonctionnements sont détectés, vSphere HA réinitialise les machines virtuelles. La réinitialisation contribue à garantir que les services restent disponibles. Pour éviter de réinitialiser constamment des machines virtuelles en cas d'erreurs non transitoires, les machines virtuelles sont réinitialisées par défaut trois fois seulement au cours d'une période configurable. Après trois réinitialisations

des machines virtuelles, vSphere HA n'effectue aucune tentative supplémentaire pour redémarrer les machines virtuelles en cas de nouvel échec et ce jusqu'à ce que la période définie ne soit écoulée. Vous pouvez configurer le nombre de réinitialisations à l'aide du paramètre personnalisé **Nbre maximum de réinitialisations par machine virtuelle**.

Remarque Les statistiques de réinitialisation sont effacées lorsque la machine virtuelle est mise hors tension puis sous tension, ou quand elle est migrée à un autre hôte en utilisant vMotion. Cela provoque le redémarrage du système d'exploitation d'hôte, mais de façon différente à un «redémarrage» dans lequel l'état d'alimentation de la VM est changé.

Partitions de réseau

En cas de défaillance du réseau de gestion d'un cluster vSphere HA, un sous-ensemble d'hôtes du cluster risque d'être incapable de communiquer avec les autres hôtes sur le réseau de gestion. De multiples partitions peuvent se produire dans un cluster.

Un cluster partitionné entraîne une diminution de la protection des machines virtuelles et une altération des fonctions de gestion du cluster. Réparez le cluster partitionné dès que possible.

- Protection de VM. vCenter Server permet de mettre sous tension une VM, mais celle-ci n'est protégée que si elle s'exécute sur la même partition que l'hôte principal qui en est responsable. L'hôte principal doit communiquer avec vCenter Server. Un hôte principal est responsable d'une machine virtuelle s'il a bloqué exclusivement un fichier défini par le système sur la banque de données contenant le fichier de configuration de la machine virtuelle.
- Gestion de cluster. vCenter Server ne peut communiquer qu'avec certains hôtes du cluster, et ne peut se connecter qu'à un hôte principal. Par conséquent, il se peut que les modifications de configuration relatives à vSphere HA ne prennent pas effet tant que le problème de partition n'est pas résolu. Suite à cette défaillance, une des partitions pourrait s'exécuter selon l'ancienne configuration, tandis qu'une autre utiliserait les nouveaux paramètres.

En cas de partition d'un cluster vSphere HA contenant des hôtes antérieurs à ESXi 5.0, il se peut que vSphere HA mette sous tension, à tort, une VM qui avait été mise hors tension par l'utilisateur ou n'arrive pas à redémarrer une VM défaillante.

Signal de pulsation de banque de données

Lorsque l'hôte principal d'un cluster vSphere HA ne peut pas communiquer avec un hôte secondaire sur le réseau de gestion, l'hôte principal utilise le signal de pulsation de banque de données pour déterminer si l'hôte secondaire est défaillant, s'il se trouve dans une partition de réseau ou s'il est réseau isolé. Si l'hôte secondaire a arrêté le signal de pulsation de banque de données, il est considéré comme défaillant et ses machines virtuelles sont redémarrées ailleurs.

vCenter Server sélectionne un ensemble de banques de données préférées pour le signal de pulsation. Cette sélection a pour but d'optimiser le nombre d'hôtes ayant accès à une banque de données de signaux de pulsation et de minimiser le risque que les banques de données soient sauvegardées par le même LUN ou le même serveur NFS.

Vous pouvez utiliser l'attribut avancé das.heartbeatdsperhost pour modifier le nombre de banques de données de signaux de pulsation sélectionné par vCenter Server pour chaque hôte. La valeur par défaut est deux et la valeur maximale est cinq.

vSphere HA crée un répertoire à la racine de chaque banque de données qui sert à la fois au signal de pulsation de banques de données et à maintenir l'ensemble des machines virtuelles protégées. Le nom de ce répertoire est `.vSphere-HA`. Vous ne devez ni supprimer ni modifier les fichiers stockés dans ce répertoire car cela peut avoir des répercussions sur les opérations. Plusieurs clusters peuvent utiliser une banque de données. Des sous-répertoires sont donc créés dans ce répertoire pour chaque cluster. Ces répertoires et fichiers font partie de la racine, et seule celle-ci peut les lire et les modifier. L'espace disque utilisé par vSphere HA dépend de plusieurs facteurs, notamment la version de VMFS et le nombre d'hôtes qui utilisent

la banque de données pour le signal de pulsation. Avec vmfs3, l'utilisation maximale est d'environ 2 Go et l'utilisation type est d'environ 3 Mo. Avec vmfs5, l'utilisation normale maximale est d'environ 3 Mo. L'utilisation vSphere HA de la banque de données ajoute une charge additionnelle négligeable et n'a pas d'impact sur la performance des autres opérations de la banque de données.

vSphere HA limite le nombre de machines virtuelles qui peuvent avoir des fichiers de configuration sur une banque de données unique. Consultez *Configurations Maximales* pour connaître les limites mises à jour. Si vous placez plus que ce nombre de machines virtuelles sur une banque de données et que vous les mettez sous tension, vSphere HA ne protège un certain nombre de machines virtuelles que jusqu'à cette limite.

Remarque Une banque de données de Virtual SAN ne peut pas être utilisée pour le signal de pulsation de banque de données. Par conséquent, si aucun autre stockage partagé n'est accessible à tous les hôtes du cluster, il se peut qu'aucune banque de données de signaux de pulsation ne soit utilisée. Toutefois, si vous disposez d'un stockage qui peut être atteint par un chemin réseau alternatif indépendant de Virtual SAN, vous pouvez l'utiliser pour configurer une banque de données de signaux de pulsation.

Sécurité vSphere HA

Plusieurs fonctions de sécurité permettent d'améliorer vSphere HA.

Sélectionner les ports de pare-feu ouverts

vSphere HA utilise les ports 8182 TCP et UDP pour la communication d'agent à agent. Les ports de pare-feu s'ouvrent et se ferment automatiquement pour assurer qu'ils sont ouverts uniquement lorsque cela est nécessaire.

Fichiers de configuration protégés par les autorisations du système de fichiers

vSphere HA stocke les informations de configuration sur le système de stockage local ou sur le ramdisk s'il n'existe aucune banque de données locale. Ces fichiers sont protégés par les autorisations du système de fichiers et sont accessibles uniquement par l'utilisateur racine. Les hôtes sans stockage local sont pris en charge uniquement si ils sont gérés par Auto Deploy.

Journalisation détaillée

L'emplacement des fichiers journaux choisi par vSphere HA dépend de la version de l'hôte.

- Pour les hôtes ESXi 5.x, vSphere HA écrit sur syslog uniquement par défaut. Les journaux sont donc placés à l'endroit indiqué dans la configuration de syslog. Les noms des fichiers journaux de vSphere HA sont précédés de `fdm`, fault domain manager (gestionnaire de domaine de pannes), qui est un service de vSphere HA.
- Pour les hôtes existants 4.x ESXi, vSphere HA écrit dans `/var/log/vmware/fdm` sur le disque local, ainsi que syslog si il est configuré.
- Pour les hôtes hérités ESX 4.x, vSphere HA écrit sur `/var/log/vmware/fdm`.

Connexions vSphere HA sécurisées

vSphere HA se connecte aux agents vSphere HA à l'aide d'un compte d'utilisateur, `vpxuser`, créé par vCenter Server. Ce compte est le même que celui utilisé par vCenter Server pour la gestion de l'hôte. vCenter Server crée un mot de passe aléatoire pour ce compte et le change régulièrement. La fréquence de renouvellement du mot de passe est définie par le paramètre `VirtualCenter.VimPasswordExpirationInDays` de vCenter Server. Les utilisateurs ayant des privilèges d'administration sur le dossier racine de l'hôte peut se connecter à l'agent.

Communication sécurisée	Toutes les communications entre vCenter Server et l'agent vSphere HA sont sécurisées par SSL. La communication d'agent à agent utilise également le protocole SSL sauf pour les messages d'élection, qui utilisent UDP. Les messages d'élection sont vérifiés via SSL de sorte qu'un agent non autorisé puisse empêcher uniquement l'hôte sur lequel l'agent s'exécute d'être choisi comme hôte principal. Dans ce cas, un problème de configuration du cluster est émis afin que l'utilisateur soit informé du problème.
Vérification du certificat SSL de l'hôte requise	vSphere HA exige que chaque hôte dispose d'un certificat SSL vérifié. Chaque hôte génère un certificat auto-signé lors de son premier démarrage. Ce certificat peut être généré une nouvelle fois ou remplacé par un certificat émis par une autorité. Si le certificat est remplacé, vSphere HA doit être reconfiguré sur l'hôte. Si un hôte se déconnecte de vCenter Server après la mise à jour de son certificat et si l'agent de l'hôte ESXi ou ESX est redémarré, vSphere HA est automatiquement reconfiguré au moment où l'hôte est reconnecté à vCenter Server. Si la déconnexion n'est pas due au fait que la vérification du certificat SSL de l'hôte de vCenter Server est désactivée à ce moment-là, vérifiez le nouveau certificat et reconfigurez vSphere HA sur l'hôte.

Utilisation de vSphere HA avec Virtual SAN

Vous pouvez utiliser Virtual SAN comme stockage partagé pour un cluster vSphere HA. Lorsqu'il est activé, Virtual SAN cumule les disques de stockage locaux spécifiés qui sont disponibles sur les hôtes afin de créer une banque de données unique partagée par tous les hôtes.

Avant d'utiliser vSphere HA avec Virtual SAN, vous devez connaître les exigences et les limitations liées à l'interopérabilité de ces deux fonctions.

Pour plus d'informations sur Virtual SAN, reportez-vous à *Stockage vSphere*.

Conditions requises pour les hôtes ESXI

Pour utiliser Virtual SAN avec un cluster vSphere HA, les conditions suivantes doivent être remplies :

- Tous les hôtes ESXi du cluster doivent être de la version 5.5 ou ultérieure.
- Le cluster doit avoir au moins trois hôtes ESXi.

Différences de mise en réseau

Virtual SAN dispose de son propre réseau. Lorsque Virtual SAN et vSphere HA sont activés sur le même cluster, le trafic entre agents HA circule sur ce réseau de stockage et non pas sur le réseau de gestion. vSphere HA utilise le réseau de gestion uniquement lorsque Virtual SAN est désactivé. vCenter Server choisit le réseau approprié lorsque vSphere HA est configuré sur un hôte.

Remarque Virtual SAN ne peut être activé que si vSphere HA est désactivé.

Si vous modifiez la configuration de Virtual SAN, les agents vSphere HA ne choisissent pas automatiquement les nouveaux paramètres réseau. Pour modifier Virtual SAN, vous devez effectuer la procédure suivante dans vSphere Web Client :

1 Désactivez la surveillance de l'hôte pour le cluster vSphere HA.

2 Modifiez Virtual SAN.

3 Cliquez avec le bouton droit sur chacun des hôtes du cluster et sélectionnez **Reconfigurer HA**.

4 Réactivez la surveillance de l'hôte pour le cluster vSphere HA.

Tableau 2-2 montre les différences de mise en réseau de vSphere HA en fonction de l'utilisation ou non de Virtual SAN.

Tableau 2-2. Différences de mise en réseau de vSphere HA

	Virtual SAN activé	Virtual SAN désactivé
Réseau utilisé par vSphere HA	Réseau de stockage de Virtual SAN	Réseau de gestion
Banques de données de signaux de pulsation	Toutes les banques de données montée sur plusieurs hôtes, sauf les banques de données de Virtual SAN.	Toutes les banques de données montées sur plusieurs hôtes.
Hôte déclaré comme isolé	Adresses d'isolation ne répondant pas aux commandes ping et réseau de stockage de Virtual SAN inaccessible.	Adresses d'isolation ne répondant pas aux commandes ping et réseau de gestion inaccessible.

Paramètres de réservation de capacité

Lorsque vous réservez de la capacité pour votre cluster vSphere HA à l'aide d'une stratégie de contrôle d'admission, ce paramètre doit être cohérent avec le paramètre de Virtual SAN correspondant qui permet d'assurer l'accessibilité des données en cas de panne. Plus précisément, la valeur du paramètre définissant le nombre de pannes toléré dans l'ensemble des règles de Virtual SAN ne doit pas être inférieure à la capacité réservée par le paramètre de contrôle d'admission de vSphere HA.

Par exemple, si l'ensemble de règles de Virtual SAN n'autorise que deux pannes, la stratégie du contrôle d'admission de vSphere HA doit réserver une capacité équivalente à seulement une ou deux pannes d'hôte. Si vous utilisez la stratégie du pourcentage de ressources de cluster réservées sur un cluster disposant de huit hôtes, vous ne devez pas réserver plus de 25 % des ressources du cluster. Si vous utilisez la stratégie des pannes d'hôtes tolérées par le cluster sur ce même cluster, la valeur du paramètre ne doit pas dépasser deux hôtes. Si vSphere HA réserve une capacité inférieure, l'activité du basculement peut être imprévisible ; si, au contraire, il réserve une capacité trop élevée, la contrainte imposée à la mise sous tension des machines virtuelles et aux migrations vMotion entre clusters est excessive.

Utilisation conjointe de vSphere HA et DRS

L'utilisation de vSphere HA avec Distributed Resource Scheduler (DRS) allie le basculement automatique à l'équilibrage de la charge. Cette association peut aboutir à un cluster mieux équilibré une fois que vSphere HA a déplacé les machines virtuelles sur d'autres hôtes.

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

Dans un cluster utilisant DRS et vSphere HA avec le contrôle d'admission activé, les machines virtuelles ne sont pas nécessairement évacuées des hôtes passant en mode 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 cas, vSphere HA ne parvient pas à basculer les machines virtuelles en raison 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 ces cas-là, vSphere HA peut utiliser DRS pour essayer d'ajuster le cluster (par exemple, en sortant les hôtes du mode 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 VM et hôte requises, sachez que ces règles doivent obligatoirement être respectées. vSphere HA n'effectue pas de basculement si cela risque d'enfreindre une règle.

Pour plus d'informations sur DRS, consultez la documentation *Gestion des ressources vSphere*.

Contrôle d'admission vSphere 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.
vSphere 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 qui peuvent être interdites, on peut citer :

- la mise sous tension d'une machine virtuelle.
- la migration d'une machine virtuelle sur un hôte ou dans un cluster ou un pool de ressources.
- l'augmentation de la réserve de CPU ou de mémoire d'une machine virtuelle.

Parmi les trois types de contrôle d'admission, seul le contrôle d'admission vSphere HA peut être désactivé. Cependant, sans ce contrôle, il est impossible de garantir que le nombre de machines virtuelles attendu puisse être redémarré après une défaillance. Ne désactivez pas 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 mode 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 vSphere Update Manager).
- Si vous devez exécuter des tests ou des opérations de maintenance.

Le contrôle d'admission réserve la capacité, mais en cas de panne, vSphere HA utilise la capacité disponible restante pour les redémarrages de la machine virtuelle. Par exemple, vSphere HA place plus de machines virtuelles sur un hôte que ce que le contrôle d'admission permettrait pour des mises en tensions par des utilisateurs.

Remarque Lorsque le contrôle d'admission vSphere HA est désactivé, vSphere HA garantit qu'au moins deux hôtes du cluster sont sous tension même si DPM est activé et peut regrouper toutes les machines virtuelles sur un seul hôte. Ceci permet de garantir que le basculement est possible.

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

Vous pouvez configurer vSphere HA pour qu'il tolère un nombre défini de défaillances d'hôtes. Avec la stratégie de contrôle d'admission Défaillances d'hôte tolérées par le cluster, vSphere HA s'assure que même si un nombre d'hôtes spécifié est défaillant, les ressources demeurent en quantité suffisante sur le cluster pour permettre le basculement de toutes les machines virtuelles de ces hôtes.

Avec la stratégie Défaillances d'hôte tolérées par le cluster, vSphere HA effectue le contrôle d'admission de la manière suivante :

1 Calcule la taille d'emplacement.

   Un emplacement 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 d'emplacements 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 d'emplacements 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 Vous pouvez définir une taille d'emplacement spécifique pour les CPU et la mémoire dans la section de contrôle d'admission des paramètres vSphere HA dans vSphere Web Client

Calcul de la taille d'emplacement

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

- vSphere HA calcule la taille de CPU à partir du CPU réservé par chaque machine virtuelle sous tension, en sélectionnant la valeur la plus élevée. Si aucun CPU n'a été réservé pour une machine virtuelle, une valeur de 32 MHz est définie par défaut. Cette valeur peut être modifiée par l'attribut avancé das.vmcpuminmhz.)
- vSphere HA calcule la taille de la 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 d'emplacement. Pour éviter cela, vous pouvez préciser une limite supérieure pour le CPU ou le composant de mémoire de la taille d'emplacement en utilisant respectivement les attributs avancés das.slotcpuinmhz ou das.slotmeminmb. Reportez-vous à « Attributs avancés de vSphere HA », page 33.

Vous pouvez également déterminer le risque de fragmentation des ressources dans le cluster en regardant le nombre de machines virtuelles qui nécessitent plusieurs emplacements. Ceci peut être calculé dans la section de contrôle d'admission des paramètres vSphere HA dans vSphere Web Client. Les machines virtuelles peuvent nécessiter plusieurs emplacements si vous avez spécifié une taille fixe ou maximale d'emplacements dans les options avancées.

Utiliser les emplacements pour déterminer la capacité de basculement actuelle

Une fois la taille d'emplacement calculée, vSphere HA détermine les ressources de CPU et de mémoire disponibles sur chaque hôte pour les machines virtuelles. Ces valeurs sont celles contenues dans le pool de ressources racine de l'hôte, et non dans les ressources physiques totales de l'hôte. Vous trouverez les données sur les ressources d'un hôte utilisé par vSphere HA dans l'onglet **Résumé** de l'hôte, sur vSphere Web Client. Si tous les hôtes de votre cluster sont identiques, vous pouvez obtenir ces données en divisant les chiffres relatifs au cluster dans son ensemble par le nombre d'hôtes. Les ressources utilisées à des fins de virtualisation ne sont pas incluses. Seuls les hôtes qui sont connectés, qui ne sont pas en mode maintenance et qui ne présentent pas d'erreurs vSphere HA sont pris en compte.

Le nombre maximum d'emplacements 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 d'emplacement 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 d'emplacements 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 d'emplacements pour satisfaire toutes les machines virtuelles sous tension.

Informations d'exécution avancées

Lorsque vous sélectionnez la politique de contrôle d'admission des défaillances de l'hôte tolérées par le cluster, le volet **Infos d'exécution avancées** apparaît dans la section vSphere HA de l'onglet **Moniteur** du cluster dans vSphere Web Client. Ce volet affiche les informations suivantes concernant le cluster :

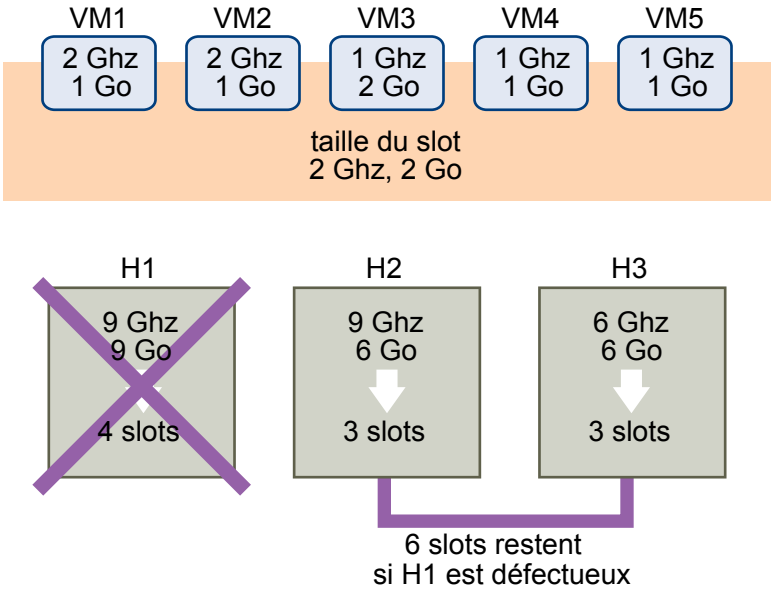
- Taille d'emplacement.
- Nombre total d'emplacements dans le cluster. Somme des emplacements pris en charge par les hôtes en état de marche dans le cluster.
- Emplacements utilisés. Nombre d'emplacements associés aux machines virtuelles sous tension. Ce nombre peut être supérieur au nombre de machines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

Exemple : Stratégie de contrôle d'admission Défaillances d'hôte tolérées par le cluster

Nous allons illustrer par un exemple le mode de calcul de la taille d'emplacement et son utilisation avec cette stratégie de contrôle d'admission. Prenons les hypothèses suivantes pour 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 a besoin de 2 GHz et 1 Go, VM3 a besoin de 1 GHz et de 2 Go, VM4 a besoin de 1 GHz et 1 Go, VM5 a besoin de 1 GHz et 1 Go.
- Les défaillances d'hôte tolérées par le cluster sont définies sur la valeur 1.

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



1 La taille d'emplacement 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 d'emplacement se compose d'un CPU de 2 GHz et d'une mémoire de 2 Go.

2 Le nombre maximum d'emplacements pouvant être pris en charge par chaque hôte est déterminé.

   H1 peut prendre en charge quatre emplacements. H2 peut prendre en charge trois emplacements (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 emplacements, ce qui est suffisant pour les cinq machines virtuelles sous tension. Si H1 et H2 sont défectueux, il ne reste que trois emplacements, ce qui est insuffisant. Par conséquent, la Capacité de basculement actuelle est de 1.

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

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

Il est possible de configurer vSphere HA pour effectuer le contrôle d'admission en réservant un pourcentage spécifique de ressources de CPU et de mémoire du cluster à la récupération en cas de pannes d'hôtes.

Les règles de contrôle d'admission Pourcentage de ressources de cluster réservées permettent à vSphere HA de réserver au basculement un pourcentage spécifié de ressources cumulées de CPU et de mémoire du cluster.

vSphere HA met en œuvre le contrôle d'admission conformément aux règles de Ressources de cluster réservées suivantes :

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

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

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

4 Détermine si la Capacité de basculement de CPU actuelle ou la Capacité de basculement mémoire actuelle sont inférieures ou non à la Capacité de basculement configurée correspondante (spécifiée par l'utilisateur).

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

vSphere HA utilise les réserves effectives des machines virtuelles. Si une machine virtuelle n'a pas de réserves, c'est-à-dire que la valeur de réserve est nulle, les valeurs utilisées par défaut sont 0 Mo de mémoire et 32 MHz de CPU.

Remarque Les règles de contrôle d'admission Pourcentage de ressources de cluster réservées vérifient également qu'il existe au moins deux hôtes compatibles vSphere HA dans le cluster (à l'exception des hôtes qui passent en mode maintenance). S'il n'y a qu'un hôte compatible vSphere HA, aucune opération n'est autorisée, même si le pourcentage de ressources disponibles est suffisant. Cette vérification supplémentaire s'explique par le fait que vSphere HA ne peut pas effectuer de basculement s'il n'y a qu'un seul hôte dans le cluster.

Calcul de la Capacité de basculement actuelle

Les ressources totales requises par les machines virtuelles sous tension incluent deux composants, CPU et mémoire. vSphere HA calcule ces valeurs.

- Le besoin en composant CPU est obtenu en additionnant le CPU réservé par les machines virtuelles sous tension. Si aucun CPU n'a été réservé pour une machine virtuelle, une valeur de 32 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 celles 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 maintenance et qui ne présentent pas d'erreurs vSphere HA sont pris en compte.

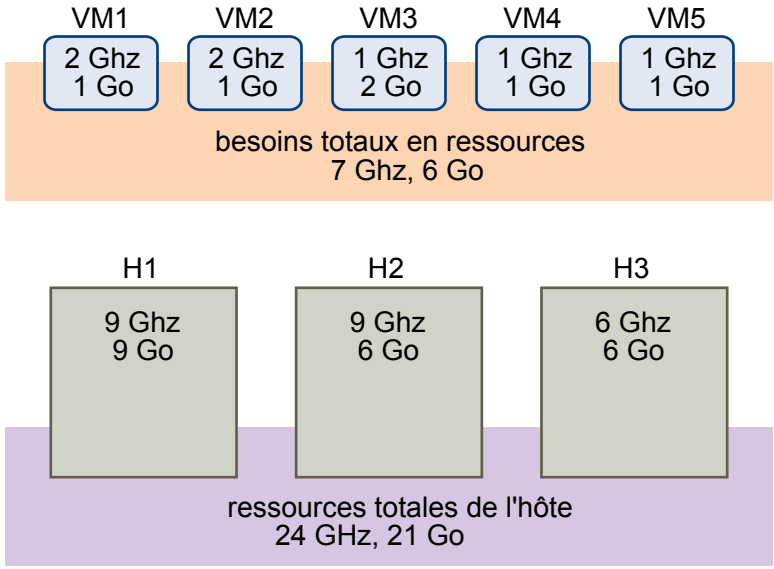
La Capacité CPU de basculement actuelle est calculée en soustrayant les besoins totaux en ressources CPU des ressources CPU totales des hôtes et en divisant le résultat par les ressources CPU totales des hôtes. La Capacité mémoire de basculement actuelle est calculée de la même manière.

Exemple : 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. Prenons les hypothèses suivantes pour 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 a besoin de 2 Ghz et 1 Go, VM3 a besoin de 1 Ghz et de 2 Go, VM4 a besoin de 1 Ghz et 1 Go, VM5 a besoin de 1 Ghz et 1 Go.
- La capacité de basculement configurée pour le processeur et la mémoire est pour tous deux 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 des hôtes de basculement

Il est possible de configurer vSphere HA afin de désigner des hôtes spécifiques comme hôtes de basculement.

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

Pour que des capacités restent disponibles sur un hôte de basculement, vous ne pouvez pas mettre sous tension des machines virtuelles ni utiliser vMotion pour faire migrer des machines virtuelles vers un hôte de basculement. De plus, DRS n'utilise pas d'hôte de basculement pour la répartition de la charge.

Remarque Si vous utilisez les règles de contrôle d'admission Définir les hôtes de basculement et désignez plusieurs hôtes de basculement, DRS ne cherche pas à faire respecter les règles d'affinité VM-VM pour les machines virtuelles qui s'exécutent sur des hôtes de basculement.

Les hôtes de basculement actuels apparaissent dans la section vSphere HA de l'onglet **Résumé** du cluster. L'icône de statut qui se trouve à côté de chaque hôte peut être verte, jaune ou rouge.

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

Choisir une règle de contrôle d'admission

Les règles de contrôle d'admission de vSphere 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 des 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 ne peut être exécutée que sur un seul hôte ESXi à la fois. La configuration par défaut de la règle de Défaillances d'hôte tolérées par le cluster évite 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 des hôtes de basculement n'entraînent pas la fragmentation des ressources car des hôtes sont réservés au basculement.

Flexibilité de la réservation des ressources de basculement

Les règles de contrôle d'admission diffèrent de par la granularité qu'elles accordent au moment de la réservation des ressources du cluster pour la protection du basculement. Les règles Défaillances d'hôte tolérées par le cluster permettent de définir le niveau de basculement d'un certain nombre d'hôtes. Les règles Pourcentage de ressources de cluster permettent d'attribuer jusqu'à 100 % des ressources de CPU ou de mémoire du cluster pour le basculement. Les règles Spécifier un hôte de basculement permettent de spécifier un ensemble d'hôtes 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 puisqu'elles tiennent uniquement compte des plus grosses réserves 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 vSphere HA tient compte de l'utilisation des ressources des machines virtuelles secondaires tolérantes 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 contrôle de vSphere HA

La liste de contrôle de vSphere HA contient les spécifications que vous devez connaître pour pouvoir créer et utiliser un cluster vSphere HA.

Spécifications applicables à un cluster vSphere HA

Consultez cette liste avant de configurer un cluster vSphere HA. Pour plus d'informations, suivez les références croisées appropriées ou consultez « Créer un cluster vSphere HA », page 28.

- Tous les hôtes doivent disposer d'une licence pour vSphere HA.
- Le cluster doit contenir deux hôtes au minimum.
- 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.
- Il doit y avoir au moins un réseau de gestion commun parmi tous les hôtes mais il est recommandé d'en avoir au moins deux. 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 ultérieures - Réseau VMkernel avec case **Traffic de gestion** cochée.

  Reportez-vous à la section « Meilleures pratiques pour la mise en réseau », page 37.
- 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.

  Remarque vSphere HA utilise le signal de pulsation de banque de données pour différencier les hôtes partitionnés, isolés ou défaillants. Par conséquent, s'il ya des banques de données plus fiables dans votre environnement, configurez vSphere HA pour leur donner la préférence.
- Le fonctionnement de surveillance des machines virtuelles nécessite l'installation des outils VMware. Reportez-vous à la section « Surveillance des VM et applications », page 15.
- vSphere HA prend en charge IPv4 et IPv6. Un cluster utilisant à la fois ces deux versions de protocole est cependant plus susceptible d'entraîner une partition de réseau.

Créer un cluster vSphere HA

vSphere HA fonctionne dans le cadre d'un cluster d'hôtes ESXi (ou ESX hérités). Vous devez créer un cluster, le remplir d'hôtes et configurer les paramètres vSphere HA pour que la protection du basculement puisse être établie.

Lorsque vous créez un cluster vSphere HA, vous devez configurer divers paramètres qui déterminent le mode de fonctionnement de la fonction. Avant de commencer, identifiez les nœuds du cluster. Ces nœuds sont les hôtes ESXi qui fourniront les ressources pour la prise en charge des machines virtuelles et qui seront utilisés par vSphere 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 mise en réseau est en place, vous pouvez ajouter les hôtes au cluster et terminer la configuration de vSphere HA.

Vous pouvez activer et configurer vSphere 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 la machine virtuelle (démarrage automatique) est désactivée pour toutes les machines virtuelles résidant sur des hôtes qui se trouvent dans un cluster vSphere HA (ou qui y ont été déplacées). Le démarrage automatique n'est pas pris en charge avec vSphere HA.

Créer un cluster vSphere HA dans vSphere Web Client

Pour activer le cluster pour vSphere HA, commencez par créer un cluster vide. Après avoir planifié les ressources et l'architecture de réseau de votre cluster, utiliser vSphere Web Client pour ajouter des hôtes au cluster et spécifier les paramètres du cluster vSphere HA.

Connecter vSphere Web Client au vCenter Server en utilisant un compte disposant des autorisations d'administrateur de 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 des différents hôtes dans le cluster.

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

Remarque Utilisez des connexions réseau de gestion redondantes pour vSphere HA. Pour plus d'informations sur la configuration d'un réseau redondant, consultez la rubrique« Redondance des chemins de réseau », page 38. Vous devez configurer aussi les hôtes avec au moins deux banques de données pour fournir de redondance à la pulsation de banques de données vSphere HA.

Procédure

1 Dans vSphere Web Client accédez au centre de données où vous voulez que le cluster réside

2 Cliquer sur **Créer un cluster**.

3 Complétez le paramètre de l'assistant Nouveau cluster.

Ne pas mettre sous tension vSphere HA (ou DRS).

4 Cliquez sur **OK** pour fermer l'assistant et créer le cluster.

Vous avez créé un cluster vide.

5 Sur la base de votre plan pour les ressources et l'architecture de réseau du cluster, utiliser vSphere Web Client pour ajouter des hôtes au cluster.

6 Accédez au cluster.

7 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.

8 Sélectionner **vSphere HA** et cliquer sur **Modifier**.

9 Sélectionnez **Activer vSphere HA**.

10 Configurez les paramètres vSphere HA comme il convient pour le cluster.

- Surveillance d'hôte
- Contrôle d'admission
- Surveillance de VM
- Signal de pulsation de banque de données
- Options avancées

11 Cliquez sur **OK**.

Vous disposez désormais d'un cluster vSphere HA configuré et rempli d'hôtes. Reportez-vous à « Configuration des paramètres de cluster vSphere HA dans vSphere Web Client », page 29.

Remarque Un cluster doit obligatoirement être compatible avec vSphere HA pour que Fault Tolerance fonctionne.

Configuration des paramètres de cluster vSphere HA dans vSphere Web Client

Lorsque vous créez un cluster vSphere HA ou que vous configurez un cluster existant, vous devez configurer les paramètres qui déterminent le mode de fonctionnement de la fonction.

Dans vSphere Web Client vous pouvez configurer les paramètres vSphere HA suivants :

Surveillance d'hôte — Activez la surveillance de l'hôte pour permettre aux hôtes du cluster d'échanger des signaux de pulsation réseau et à vSphere HA d'agir lorsqu'il détecte des pannes. Ici vous pouvez également définir la priorité de réponse de redémarrage de la VM et d'isolation de l'hôte.

Remarque La surveillance d'hôte est aussi requise pour le bon fonctionnement du processus de récupération de vSphere Fault Tolerance.

Contrôle d'admission — Activez ou désactivez le contrôle d'admission pour le cluster vSphere HA et choisissez une règle pour déterminer son application.

Surveillance de VM — Activer la surveillance des VM ou surveillance des VM et application.

Signal de pulsation de banque de données — Indiquez vos préférences pour les banques de données que vSphere HA utilise pour le signal de pulsation des banques de données.

Options avancées — Personnalisez le comportement de vSphere HA en définissant les options avancées.

Configurer la surveillance d'hôte

Après avoir créé un cluster, la surveillance d'hôte permet à l'hôte maître vSphere HA de répondre aux défaillances de l'hôte ou de la machine virtuelle et à l'isolation du réseau de gestion. La priorité de redémarrage et la réponse d'isolement de l'hôte de la VM déterminent comment vSphere HA répond défaillances d'hôtes et aux isolations.

La page Surveillance d'hôte apparaît uniquement si vous avez activé vSphere HA.

Procédure

1 Dans vSphere Web Client, accédez au cluster vSphere HA .

2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.

3 Sous Paramètres, sélectionner **vSphere HA** et cliquer sur **Modifier**.

4 Développez **Surveillance d'hôte** pour afficher les options de configuration pour la surveillance de l'hôte.

5 Sélectionnez **Surveillance d'hôte** pour activer cette fonction.

6 Sélectionnez la **Priorité redémarrage VM** pour les machines virtuelles dans le cluster.

La priorité de redémarrage détermine l'ordre de redémarrage des machines virtuelles en cas d'échec de l'hôte. Les machines virtuelles de plus haute priorité sont démarrées en premier. Cette priorité s'applique seulement par hôte. Si plusieurs hôtes échouent, toutes les machines virtuelles sont migrées du premier hôte par ordre de priorité, puis toutes les machines virtuelles du deuxième hôte par ordre de priorité, et ainsi de suite.

7 Sélectionnez la **Réponse d'isolation de l'hôte**.

La réponse d'isolation de l'hôte détermine les événements survenant lorsqu'un hôte dans un cluster vSphere HA perd la connexion réseau de sa console mais poursuit son exécution.

8 Cliquez sur **OK**.

La Surveillance d'hôte est activée et les paramètres de priorité de redémarrage et de réponse d'isolation de l'hôte prennent effet.

Configurer le contrôle d'admission

Après la création d'un cluster, le contrôle d'admission permet de spécifier si les machines virtuelles peuvent être démarrées si elles violent les contraintes de disponibilité. Le cluster réserve des ressources pour permettre le basculement de toutes les machines virtuelles en cours d'exécution sur le nombre d'hôtes spécifié.

La page Contrôle admission apparaît uniquement si vous avez activé vSphere HA.

Procédure

1 Dans vSphere Web Client, accédez au cluster vSphere HA.

2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.

3 Sous Paramètres, sélectionner **vSphere HA** et cliquer sur **Modifier**.

4 Développez **Contrôle d'admission** pour afficher les options de configuration.

5 Sélectionnez une règle de contrôle d'admission à appliquer au cluster.

Option	Description
Définir la capacité de basculement à partir du nombre statique d'hôtes	Sélectionnez le nombre maximal de pannes d'hôte dont vous pouvez récupérer ou pour lesquels vous pouvez garantir le basculement. En outre, vous devez sélectionner une règle de taille de slot.
Définir la capacité de basculement en réservant un pourcentage des ressources du cluster	Spécifiez un pourcentage des ressources CPU et de mémoire du cluster à réserver comme capacité disponible pour prendre en charge les basculements.
Utilisez des hôtes de basculement dédiés	Sélectionnez les hôtes à utiliser pour les actions de basculement. Les basculements peuvent toujours se produire sur d'autres hôtes du cluster si l'hôte de basculement par défaut ne dispose pas des ressources suffisantes.
Ne pas réserver de la capacité de basculement	Cette option permet de mettre sous tension les VM qui violent les contraintes de disponibilité.

6 Cliquez sur **OK**.

Le contrôle d'admission est activé et la politique que vous avez choisi prend effet.

Configurer la surveillance des VM et applications

La fonction Surveillance des machines virtuelles utilise les informations de signal de pulsation capturées par VMware Tools comme proxy pour la disponibilité des systèmes d'exploitation clients. Cette fonction permet à vSphere HA de réinitialiser ou de redémarrer automatiquement les machines virtuelles qui ont perdu leur capacité de produire un signal de pulsation.

La page Surveillance de VM apparaît uniquement si vous avez activé vSphere HA.

Procédure

1 Dans vSphere Web Client, accédez au cluster vSphere HA .

2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.

3 Sous Paramètres, sélectionner **vSphere HA** et cliquer sur le bouton **Modifier**.

4 Développez **Surveillance VM** pour afficher les options de configuration.

5 Sélectionnez **Surveillance de VM seulement** pour redémarrer des machines virtuelles individuelles si leurs signaux de pulsation ne sont pas reçus dans un délai déterminé.

Vous pouvez sélectionner **Surveillance de VM et d'application** afin d'activer également la surveillance des applications.

6 Définissez la sensibilité de la surveillance des machines virtuelles en déplaçant le curseur entre **Bas** et **Haut**.

7 (Facultatif) Sélectionnez **Personnalisé** pour fournir des paramètres personnalisés.

8 Cliquez sur OK.

Configurer le signal de pulsation d'une banque de données

vSphere HA utilise le signal de pulsation de banque de données pour identifier les hôtes défaillants et les hôtes qui résident dans une partition réseau. Le signal de pulsation d'une banque de données permet à vSphere HA de contrôler les hôtes en cas de partition du réseau de gestion et de continuer à répondre aux défaillances qui se produisent.

Vous pouvez spécifier les banques de données que vous voulez utiliser pour le signal de pulsation des banques de données.

Procédure

1 Dans vSphere Web Client, accédez au cluster vSphere HA .

2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.

3 Sous Paramètres, sélectionner **vSphere HA** et cliquer sur **Modifier**.

4 Développez **Signal de pulsation de la banque de données** pour afficher les options de configuration du signal de pulsation de la banque de données.

5 Pour indiquer à vSphere HA comment sélectionner les banques de données et comment traiter vos préférences, choisissez une des options suivantes :

Tableau 2-3.

Options de signal de pulsation de banque de données
Sélectionner automatiquement les banques de données accessibles à partir de l'hôte
Utiliser les banques de données uniquement à partir de la liste spécifiée
Utiliser la banque de données de la liste spécifiée et compléter automatiquement si nécessaire

6 Dans le volet **Banques de données des signaux de pulsation disponibles**, sélectionner les banques de données que vous souhaitez utiliser pour le signal de pulsation.

Les banques de données répertoriées sont partagées par plusieurs hôtes du cluster vSphere HA. Lorsque vous sélectionnez une banque de données, le volet inférieur affiche tous les hôtes du cluster vSphere HA qui peuvent y accéder.

7 Cliquez sur **OK**.

Personnaliser le comportement de vSphere HA

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

Vérifiez les paramètres avancés que vous pouvez utiliser pour optimiser les clusters vSphere HA dans votre environnement. Ces attributs affectent le fonctionnement de vSphere HA. Modifiez-les donc avec prudence.

Définir les options avancées dans vSphere Web Client

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

Prérequis

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

Procédure

1 Dans vSphere Web Client, accédez au cluster vSphere HA .

2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.

3 Sous Paramètres, sélectionner **vSphere HA** et cliquer sur **Modifier**.

4 Cliquez sur **Options avancées**.

5 Cliquez sur **Ajouter** et tapez le nom de l'option avancée dans la zone de texte.

Vous pouvez définir la valeur de l'option dans la zone de texte dans la colonne Valeur.

6 Répétez l'étape 5 pour chaque nouvelle option que vous souhaitez ajouter et cliquez sur **OK**.

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

Attributs avancés de vSphere HA

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

Tableau 2-4. Attributs avancés de vSphere HA

Attribut	Description
das.isolationaddress[...]	définit l'adresse pour exécuter un ping afin de déterminer si un hôte est isolé du réseau. Le ping est uniquement envoyé à cette adresse lorsqu'aucun autre hôte du cluster ne reçoit de signaux de pulsation. En l'absence de précision, la passerelle par défaut du réseau de gestion est utilisée. 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'isolement (jusqu'à 10) pour le cluster : das.isolationaddressX, où X = 0-9. Vous devez généralement en indiquer une par réseau de gestion. L'indication d'un nombre excessif d'adresses ralentit la détection de l'isolement.
das.usedefaultisolationaddress	Par défaut, vSphere HA utilise la passerelle par défaut du réseau de console comme adresse d'isolement. Cet attribut indique l'utilisation ou non de ce paramètre par défaut (vrai | faux).
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 à l'isolement de l'hôte est Arrêter la machine virtuelle. La valeur par défaut est de 300 secondes.
das.slotmeminmb	Définit la limite maximum de la taille d'un emplacement de mémoire. Si cette option est utilisée, la taille d'emplacement est la plus petite de cette valeur ou la réserve de mémoire maximale plus la capacité supplémentaire de n'importe quelle machine virtuelle sous tension dans le cluster.
das.slotcpuinmhz	Définit la limite maximale de la taille d'un emplacement de CPU. Si cette option est utilisée, la taille d'emplacement est la plus petite de cette valeur ou la réserve de CPU maximale de n'importe quelle 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 réserve de mémoire n'est pas précisée ou nulle. Celle-ci est utilisée pour la stratégie 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 réserve de CPU n'est pas précisée ou nulle. Celle-ci est utilisée pour la stratégie de contrôle d'admission Défaillances d'hôte tolérées par le cluster. Si aucune valeur n'est spécifiée, la valeur par défaut est de 32 MHz.
das.iostatsinterval	Modifie l'intervalle de statistique des E/S par défaut pour la 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.

Tableau 2-4. Attributs avancés de vSphere HA (suite)

Attribut	Description
das.ignoreinsufficienthbdatastore	Désactive les problèmes de configuration créés si l'hôte n'a pas suffisamment de banques de données de signaux de pulsation pour vSphere HA. La valeur par défaut est "faux".
das.heartbeatdsperhost	Modifie le nombre de banques de données de signaux de pulsation nécessaire. Les valeurs peuvent s'étendre de 2 à 5 et la valeur par défaut est 2.
fdm.isolationpolicydelaysec	Le nombre de secondes pendant lesquelles le système attend avant d'exécuter la politique d'isolation une fois que l'isolation de l'hôte est déterminée. La valeur minimale est 30. S'il une valeur inférieure à 30 est définie, le délai sera de 30 secondes.
das.respectvmvmantiaffinityrules	Détermine si vSphere HA applique les règles d'anti-affinité VM-VM. Avec la valeur par défaut « false », les règles ne sont pas appliquées. Si la valeur « true » est choisie, les règles sont appliquées (même si vSphere DRS n'est pas activé). Dans ce cas, vSphere HA ne bascule pas sur une machine virtuelle s'il viole une règle en le faisant, mais émet un événement signalant que les ressources sont insuffisantes pour effectuer le basculement. Pour plus d'informations sur les règles d'anti-affinité, reportez-vous à *Gestion des ressources vSphere*.

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

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

Options Plus prises en charge

Dans vCenter Server 5.x, un certain nombre d'options de configuration avancées de vSphere HA ne sont plus prises en charge. Les options suivantes ne sont plus prises en charge.

- das.consoleUser
- das.consoleNode
- das.consolePerm
- das.primaryCount
- das.checkVmStateDelay
- das.trace
- das.traceLevel
- das.traceOutput
- das.preferredPrimaries
- das.disableUWSwapRequirement
- das.sensorPollingFreq
- das.bypassNetCompatCheck
- das.defaultfailoverhost

- das.failureDetectionTime
- das.failureDetectionInterval

Si vous essayez de définir l'une des options non prises en charge, vCenter Server 5.0 signalera que l'option n'est pas valide. En outre, si vous mettez à jour vCenter Server 5.x depuis une ancienne version possédant l'une des options définies, elles seront supprimées et ne seront plus actives.

Personnaliser une VM individuelle dans vSphere Web Client

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

Procédure

1 Dans vSphere Web Client, accédez au cluster vSphere HA .

2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.

3 Sous Paramètres, sélectionnez **Remplacements VM** et cliquez sur **Ajouter**.

4 Utilisez le bouton **+** pour sélectionner les machines virtuelles sur lesquelles appliquer les remplacements.

5 Cliquez sur **OK**.

6 (Facultatif) Vous pouvez changer les paramètres de **Niveau d'automatisation**, **Priorité redémarrage VM**, **Réponse d'isolement d'hôte, Surveillance VM**, ou **Sensibilité de surveillance VM**.

Remarque Vous pouvez afficher les paramètres par défaut du cluster pour ces paramètres en commençant par développer **Paramètres**, puis en développant **vSphere HA**.

7 Cliquez sur **OK**.

Le comportement de la VM est désormais différent des réglages par défaut du cluster pour chaque paramètre que avez modifié.

Meilleures pratiques pour les clusters vSphere HA

Pour garantir des performances optimales des clusters vSphere HA, vous devez suivre certaines meilleures pratiques. Cette rubrique met en évidence quelques-unes des meilleures pratiques essentielles pour un cluster vSphere HA. Vous pouvez également consulter la publication *Meilleures pratiques du déploiement vSphere High Availability* pour poursuivre la discussion.

Définir des alarmes pour surveiller les changements des clusters

Quand vSphere HA ou Fault Tolerance interviennent pour préserver la disponibilité en effectuant un basculement de machine virtuelle, par exemple, vous avez la possibilité d'être averti de ces changements. Dans vCenter Server, configurez des alarmes qui seront déclenchées lorsque ces actions surviendront, et recevez des alertes, sous forme de messages électroniques, par exemple, envoyées à un groupe d'administrateurs prédéfini.

Plusieurs alarmes par défaut sont disponibles pour vSphere HA.

- Ressources de basculement insuffisantes (alarme de cluster)
- Impossible de trouver le cluster principal (alarme du cluster)
- Basculement en cours (alarme du cluster)

- Statut de l'hôte HA (alarme d'hôte)
- Erreur de surveillance de VM (alarme de machine virtuelle)
- Action de surveillance de VM (alarme de machine virtuelle)
- Échec du basculement (alarme de machine virtuelle)

Remarque Les alarmes par défaut contiennent le nom de la fonction, vSphere HA.

Surveillance de la validité du cluster

Un cluster valide est un cluster sur lequel il n'y eu aucune violation des stratégies de contrôle d'admission.

Un cluster sur lequel HA est activé devient invalide lorsque le nombre de machines virtuelles sous tension dépasse les exigences de basculement, ce qui signifie, 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.

Dans vSphere Web Client, sélectionnez **vSphere HA** dans l'onglet **Moniteur** du cluster, puis sélectionnez **Problèmes de configuration**. La liste de problèmes actuels de vSphere HA apparaît.

Le comportement DRS n'est pas affecté par un cluster rouge à cause d'un problème lié à vSphere HA.

Interopérabilité de vSphere HA et de Storage vMotion dans un cluster mixte

Dans les clusters où des hôtes ESXi 5.x et ESX/ESXi 4.1 ou des hôtes antérieurs sont présents et où Storage vMotion est largement utilisé ou Storage DRS est activé, ne déployez pas vSphere HA. vSphere HA pourrait répondre à une défaillance de l'hôte en redémarrant une VM sur un hôte avec une version ESXi différente de celle sur laquelle la VM a été lancée avant la défaillance. Un problème peut survenir si, au moment de la défaillance, la machine virtuelle participait à une action de Storage vMotion sur un hôte ESXi 5.x, et si vSphere HA redémarre la VM sur un hôte ayant une version antérieure à ESXi 5.0. Pendant l'allumage de la machine virtuelle, des tentatives ultérieures d'opérations de snapshot pourraient corrompre l'état du vdisk et rendre la machine virtuelle inutilisable.

Pratiques d'excellence pour le contrôle d'admission

Les recommandations suivantes constituent les pratiques d'excellence pour le contrôle d'admission vSphere HA.

- Sélectionnez la stratégie de contrôle d'admission Pourcentage de ressources de cluster réservées. Cette stratégie offre la plus grande flexibilité en termes de dimensionnement d'hôtes et de machines virtuelles. Lors de la configuration de cette stratégie, choisissez un pourcentage de CPU et de mémoire qui reflète le nombre de pannes que vous voulez que l'hôte prenne en charge. Par exemple, si vous voulez que vSphere HA réserve des ressources pour deux pannes et que vous avez dix hôtes d'une capacité égale dans le cluster, spécifiez 20 % (2/10).
- Assurez-vous d'attribuer la même taille à tous les hôtes du cluster. Pour la stratégie Défaillances d'hôte tolérées par le cluster, un cluster non équilibré entraîne un excès de capacité réservé au traitement des pannes car vSphere HA réserve la capacité pour les hôtes les plus volumineux. Pour la stratégie Pourcentage de ressources du cluster, un cluster non équilibré nécessite que vous spécifiez des pourcentages plus élevés que nécessaire pour réserver une capacité suffisante en anticipation au nombre de pannes d'hôtes.

- Si vous prévoyez d'utiliser la stratégie Défaillances d'hôte tolérées par le cluster, faites en sorte que les spécifications de dimensionnement des machines virtuelles soient similaires sur toutes les machines virtuelles configurées. Cette stratégie utilise des tailles d'emplacement pour calculer la capacité qui doit être réservée à chaque VM. La taille d'emplacement repose sur la plus grande mémoire et CPU réservées nécessaires à une machine virtuelle. Lorsque vous mélangez des machines virtuelles ayant des spécifications de CPU et de mémoire différentes, le calcul détermine la plus grande taille d'emplacement possible, ce qui limite la consolidation.
- Si vous prévoyez d'utiliser la stratégie Définir les hôtes de basculement, indiquez le nombre de pannes d'hôtes à prendre en charge puis spécifiez ce nombre d'hôtes en tant qu'hôtes de basculement. Si le cluster n'est pas équilibré,, les hôtes de basculement désignés doivent être au moins de la même taille que les hôtes de non-basculement dans votre cluster. Cela garantit une capacité suffisante en cas de panne.

Utiliser Auto Deploy avec vSphere HA

Vous pouvez utiliser simultanément vSphere HA et Auto Deploy pour améliorer la disponibilité de vos machines virtuelles. Auto Deploy approvisionne les hôtes lorsqu'ils s'allument. Vous pouvez également le configurer pour installer l'agent vSphere HA sur ces hôtes pendant le processus de démarrage. Pour plus de détails, consultez la documentation d'Auto Deploy incluse dans le guide Installation et configuration de vSphere.

Mise à niveau d'hôtes dans un cluster à l'aide de Virtual SAN

Si vous mettez à niveau les hôtes ESXi dans votre cluster vSphere HA vers la version 5.5 ou une version ultérieure, et que vous prévoyez également d'utiliser Virtual SAN, suivez ce processus.

1 Mettez à niveau tous les hôtes.

2 Désactivez vSphere HA.

3 Activez Virtual SAN.

4 Réactivez vSphere HA.

Meilleures pratiques pour la mise en réseau

Suivez les meilleures pratiques pour la configuration des adaptateurs réseau hôtes et la topologie du réseau pour vSphere HA. Les pratiques d'excellence incluent des recommandations pour vos hôtes ESXi, et traitent aussi du câblage, des commutateurs, des routeurs et des pare-feu.

Configuration et maintenance du réseau

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

- Lors d'une modification des réseaux sur lesquels se trouvent les hôtes ESXi en clusters, suspendez la fonction de surveillance d'hôte. Les changements de matériel ou de paramètres réseau peuvent interrompre les signaux de pulsation utilisés par vSphere HA pour détecter les défaillances d'hôtes, ce qui risque d'entraîner des tentatives intempestives de basculement des machines virtuelles.
- Lorsque, par exemple, vous modifiez la configuration du réseau sur les hôtes ESXi, l'ajout de groupes de ports, ou la suppression de vSwitches, suspendez la surveillance d'hôte. Après avoir effectué les modifications de configuration de réseau, vous devez reconfigurer vSphere HA sur tous les hôtes du cluster, ce qui provoque une nouvelle inspection des informations du réseau. Réactivez ensuite la Surveillance d'hôte.

Remarque La mise en réseau étant un aspect essentiel de vSphere HA, l'administrateur de vSphere HA doit être tenu informé de toute opération de maintenance du réseau.

Réseaux utilisés pour les communications vSphere HA

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

- Sur les hôtes hérités ESX du cluster, les communications vSphere 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 vSphere HA.
- Sur les hôtes ESXi du cluster, les communications vSphere HA sont acheminées par défaut via les réseaux VMkernel, sauf ceux spécifiques à vMotion. S'il n'existe qu'un seul réseau VMkernel, vSphere HA le partage avec vMotion, si nécessaire. Avec ESXi 4.x et ESXi, vous devez aussi cocher explicitement la case **Trafic de gestion** si vSphere HA doit utiliser ce réseau.

Remarque Pour garder le trafic de l'agent vSphere HA sur les réseaux que vous avez spécifiés, configurez des hôtes de façon à ce que les cartes vmkNICs utilisées par vSphere HA ne ne partagent pas les sous-réseaux avec les cartes vmkNIC utilisées à d'autres fins. Les agents vSphere HA envoient des paquets en utilisant une carte pNIC associée à un sous-réseau donné s'il y a aussi au moins une carte vmkNIC configurée pour le trafic de gestion vSphere HA. Par conséquent, pour assurer la séparation de flux réseau, les cartes vmkNIC utilisés par vSphere HA et par les autres fonctionnalités doivent être sur des sous-réseaux différents.

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 hôte peut envoyer un ping à son adresse d'isolation réseau, l'hôte n'est pas isolé dans le réseau et soit les autres hôtes du cluster ont échoué, soit le réseau s'est partitionné. 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. Vous devez utiliser l'attribut avancé das.isolationaddress[...] pour ajouter des adresses d'isolation à des réseaux supplémentaires. Reportez-vous à la section « Attributs avancés de vSphere HA », page 33.

Redondance des chemins de réseau

La redondance des chemins de réseau entre les nœuds de cluster est importante pour la fiabilité de vSphere 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.

Si vous avez un seul réseau de gestion, toute défaillance entre l'hôte et le cluster peut provoquer une activité de basculement inutile (ou faux) si la connectivité du signal de pulsation des banques de données n'est pas conservé lors de la panne de réseau. Les défaillances possibles incluent les pannes de adaptateurs 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 assurant une redondance du réseau.

Il est possible d'implémenter la redondance du réseau au niveau de l'association de adaptateurs réseau, ou au niveau réseau de gestion. Dans la plupart des implémentations, l'association des adaptateurs 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 ou de partition 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 adaptateurs réseau

L'utilisation d'une association de deux adaptateurs 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 adaptateurs 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 adaptateurs 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 une carte réseau à un hôte de votre cluster vSphere HA, vous devez reconfigurer vSphere HA sur cet hôte.

Redondance réseau utilisant un réseau secondaire

Au lieu d'associer des adaptateurs 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 originelle est utilisée pour le réseau et à des fins de gestion. Lorsque la connexion de réseau de gestion secondaire est créée, vSphere HA transmet des signaux de pulsation sur les deux connexions de réseau de gestion à la fois. Si un chemin est défaillant, vSphere HA continue à transmettre et à recevoir des signaux de pulsation par l'autre chemin.

Assurer Fault Tolerance des machines virtuelles 3

Il est possible d'activer vSphere 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 vSphere HA.

Fault Tolerance est intégrée à la plate-forme hôte 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 optimaux de Fault Tolerance, il est nécessaire d'en comprendre le fonctionnement, de savoir comment l'activer sur un cluster et sur des machines virtuelles, et de connaître les meilleures pratiques pour son utilisation.

Remarque Vous verrez parfois apparaître des messages d'erreur quand vous tenterez d'utiliser Fault Tolerance. Pour plus d'informations sur les messages d'erreur liés à Fault Tolerance, consultez l'article de la base de connaissances VMware sur http://kb.vmware.com/kb/1033634.

Ce chapitre aborde les rubriques suivantes :

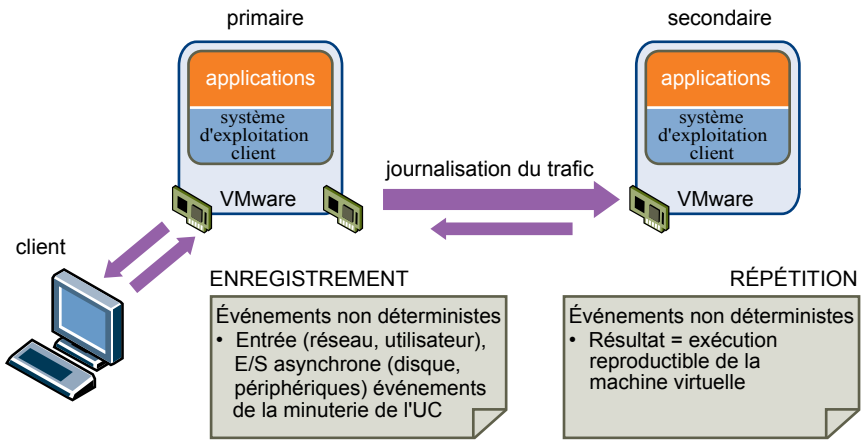
Fonctionnement de Fault Tolerance

vSphere 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 Fault Tolerance sur la plupart des machines virtuelles cruciales pour une mission. Une copie de la machine virtuelle, que l'on appelle 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 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.

Remarque Le trafic de la journalisation de la tolérance aux pannes entre les machines virtuelles primaires et secondaires est chiffré et contient un réseau client et des données E/S de stockage, ainsi que le contenu de la mémoire du système d'exploitation client. Ce trafic peut inclure des données sensibles telles que des mots de passe en texte brut. Pour éviter que ces données ne soient divulguées, assurez-vous que ce réseau est sécurisé, notamment pour éviter les « attaques de l'intercepteur ». Par exemple, vous pourriez utiliser un réseau privé pour le trafic de la journalisation de la tolérance aux pannes.

Figure 3-1. Machine virtuelle principale et machine virtuelle secondaire dans une paire avec Fault Tolerance



Les machines virtuelles principale et secondaire échangent des signaux de pulsation en continu. Cet échange permet à la paire de machines virtuelles de contrôler mutuellement leur état pour assurer le maintien permanent de Fault Tolerance. 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 Fault Tolerance 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 à la documentation *Gestion des ressources vSphere*.

Fault Tolerance évite les situations de division qui peuvent se traduire par 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.

Utiliser Fault Tolerance avec DRS

Vous pouvez utiliser vSphere Fault Tolerance avec vSphere 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).

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 la 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 vSphere 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. Si une règle d'affinité VM-VM est définie pour une machine virtuelle principale, DRS tente de corriger toutes les violations survenant après un basculement (c'est-à-dire, après le déplacement effectif de la machine virtuelle principale vers un nouvel hôte).

Cas d'utilisation de Fault Tolerance

Plusieurs situations types peuvent bénéficier de l'utilisation de vSphere Fault Tolerance.

Fault Tolerance assure un meilleur niveau de continuité d'activité que vSphere 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, l'état de la machine virtuelle restant entièrement 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 vSphere 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 Fault Tolerance.

- Les applications qui doivent être disponibles en permanence, surtout celles présentant des connexions 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.

Fault Tolerance à la demande

Un autre cas pratique de protection d'une machine virtuelle par Fault Tolerance s'intitule Fault Tolerance à la demande. Dans ce cas, une machine virtuelle est correctement protégée par vSphere 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. vSphere Fault Tolerance permet de protéger cette machine virtuelle avant la production du rapport, puis d'arrêter ou de désactiver Fault Tolerance après la publication du rapport. Vous pouvez utiliser Fault Tolerance à la demande pour protéger la machine virtuelle pendant une période critique et revenir aux ressources normales pour les opérations non critiques.

Liste de vérification de Fault Tolerance

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

Consultez cette liste avant de configurer Fault Tolerance. Vous pouvez également 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 utilisés pour vSphere FT.

Remarque Le basculement des machines virtuelles tolérantes aux pannes ne dépend pas de vCenter Server, mais vous devez utiliser vCenter Server pour configurer vos clusters de Fault Tolerance.

Spécifications des clusters pour Fault Tolerance

Les exigences suivantes aux clusters doivent être remplies avant d'utiliser Fault Tolerance.

- Deux hôtes certifiés FT au minimum utilisant la même version de Fault Tolerance ou le même numéro de version d'hôte. Le numéro de version de Fault Tolerance apparaît dans l'onglet **Résumé** d'un hôte dans vSphere Web Client.

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

- Les hôtes ESXi ont accès aux mêmes banques de données et réseaux des machines virtuelles. Reportez-vous à la section « Pratiques d'excellence pour Fault Tolerance », page 56.
- Journalisation de Fault Tolerance et réseau vMotion configuré. Reportez-vous à la section « Configurer la mise en réseau des machines hôtes dans vSphere Web Client », page 47.
- Cluster vSphere HA créé et activé. Reportez-vous à la section « Créer un cluster vSphere HA », page 28. vSphere HA doit être activé avant la mise sous tension des machines virtuelles tolérantes aux pannes ou avant l'ajout d'un hôte dans un cluster qui prend déjà en charge des machines virtuelles tolérantes aux pannes.

Conditions requises pour les hôtes pour Fault Tolerance

Les conditions suivantes concernant les hôtes doivent être remplies avant d'utiliser Fault Tolerance.

- Les hôtes doivent avoir des processeurs appartenant au groupe de processeurs compatibles avec FT. Il est également fortement recommandé que les processeurs des hôtes soient compatibles entre eux. Consultez l'article de la base de connaissances de VMware sur http://kb.vmware.com/kb/1008027 pour obtenir des informations sur les processeurs pris en charge.
- Les hôtes doivent avoir une licence pour Fault Tolerance.
- Les hôtes doivent être certifiés pour Fault Tolerance. Reportez-vous à la section http://www.vmware.com/resources/compatibility/search.php et sélectionnez **Recherche par jeux compatibles tolérants aux pannes** pour déterminer si vos 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 et vérifier la conformité dans vSphere Web Client », page 50.

Conditions des machines virtuelles pour Fault Tolerance

Les conditions des machines virtuelles suivantes doivent être remplies avant d'utiliser Fault Tolerance.

- Aucun périphérique non pris en charge n'est attaché à la machine virtuelle. Reportez-vous à la section « Interopérabilité de Fault Tolerance », page 45.
- 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 Fault Tolerance, un message vous avertit que le fichier VMDK doit être converti. Vous devez mettre hors tension la machine virtuelle pour exécuter la conversion.
- vSphere Fault Tolerance n'est pas pris en charge sur les disques de machine virtuelle de plus de 2 To.
- Les fonctions incompatibles ne doivent pas être exécutées avec les machines virtuelles tolérantes aux pannes. Reportez-vous à la section « Interopérabilité de Fault Tolerance », page 45.
- 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 Fault Tolerance.
- Les machines virtuelles doivent être exécutées sur l'un des systèmes d'exploitation clients pris en charge. Consultez l'article de la base de connaissances de VMware sur http://kb.vmware.com/kb/1008027 pour plus d'informations.

Interopérabilité de Fault Tolerance

Avant de configurer vSphere Fault Tolerance, vous devez connaître les fonctions et produits incompatibles avec Fault Tolerance.

Fonctions vSphere non prises en charge par Fault Tolerance

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

- Snapshots. Les snapshots doivent être supprimés ou engagés avant l'activation de Fault Tolerance sur une machine virtuelle. De plus, il n'est pas possible de prendre des snapshots de machines virtuelles sur lesquelles Fault Tolerance est activée.

- Stockage vMotion Il n'est pas possible d'appeler le stockage vMotion pour les machines virtuelles pour lesquelles Fault Tolerance est activée. Pour migrer le stockage, il faut mettre hors tension temporairement Fault Tolerance et exécuter l'action de stockage vMotion. Une fois ceci fait, vous pouvez réactiver Fault Tolerance.
- Clones liés. Il n'est pas possible d'activer Fault Tolerance 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 Fault Tolerance est activée.
- Sauvegardes des machines virtuelles. Il n'est pas possible de sauvegarder une VM ayant la FT activée et utilisant vStorage API for Data Protection, vShpere Data Protection ou tout autre produit de sauvegarde similaire exigeant l'utilisation d'un snapshot de VM, comme effectué par ESXi. Pour sauvegarder une machine virtuelle tolérante aux pannes de cette façon, il faut préalablement désactiver la tolérance aux pannes, puis la réactiver après la sauvegarde. Les snapshots de stockage basés sur une baie n'affectent pas la tolérance aux pannes.
- Virtual SAN.

Fonctions et périphériques incompatibles avec Fault Tolerance

Pour qu'une machine virtuelle soit compatible avec Fault Tolerance, celle-ci ne doit pas utiliser les fonctions ou périphériques suivants.

Tableau 3-1. Fonctions et périphériques incompatibles avec Fault Tolerance 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 Fault Tolerance.	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 sauvegarde 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 adaptateurs réseau	Cette fonction n'est pas prise en charge par Fault Tolerance et doit donc être désactivée.
Pilotes réseau vlance.	Fault Tolerance ne prend pas en charge les machines virtuelles qui sont configurées avec les adaptateurs 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 Fault Tolerance, la conversion au format de disque approprié est effectuée par défaut. Vous devez mettre hors tension la machine virtuelle pour déclencher cette conversion.

Tableau 3-1. Fonctions et périphériques incompatibles avec Fault Tolerance et les actions correctives (suite)

Fonction ou périphérique incompatible	Action corrective
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 Fault Tolerance, effectuer la connexion à chaud, puis réactiver Fault Tolerance. **Remarque** Lorsque vous utilisez Fault Tolerance, la modification des paramètres d'une carte réseau virtuelle pendant le fonctionnement d'une machine virtuelle constitue une connexion à chaud, car cela exige de « débrancher » la carte réseau, puis de la « rebrancher ». Prenons l'exemple d'une carte 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 arrêtée.
Extended Page Tables/Rapid Virtualization Indexing (EPT/RVI).	EPT/RVI est automatiquement désactivé pour les machines virtuelles pour lesquelles Fault Tolerance est activée.
Ports série ou parallèles	Déconnectez ces périphériques de la machine virtuelle.
IPv6	Utilisez les adresses IPv4 avec la carte réseau de journalisation FT.
Périphériques vidéo dont la 3D est activée.	Fault Tolerance ne prend pas en charge les périphériques vidéo dont la 3D est activée.
Microprogramme EFI virtuel	Assurez-vous que la VM est configurée pour utiliser le firmware du BIOS avant d'installer le système d'exploitation d'hôte.

Préparer votre cluster et vos hôtes à Fault Tolerance

Pour activer vSphere 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 Fault Tolerance.

Les tâches devant être effectuées avant de tenter d'activer Fault Tolerance pour le cluster sont les suivantes :

- Configurer la mise en réseau de chaque hôte
- Créer un cluster vSphere HA, ajouter des hôtes et vérifier la conformité

Lorsque le cluster et les hôtes sont prêts, vous pouvez activer Fault Tolerance pour vos machines virtuelles. Reportez-vous à la section « Activer Fault Tolerance pour les machines virtuelles dansvSphere Web Client », page 52.

Configurer la mise en réseau des machines hôtes dans vSphere Web Client

Vous devez configurer deux commutateurs réseau différents sur chacun des hôtes que vous souhaitez ajouter à un cluster vSphere HA, de façon à ce que l'hôte prenne aussi en charge vSphere Fault Tolerance.

Pour activer Fault Tolerance d'un hôte, vous devez exécuter deux fois cette procédure, une fois pour chaque option de groupe de ports afin de vous assurer qu'il y a suffisamment de bande passante disponible pour la journalisation de Fault Tolerance. Sélectionnez une option, terminez la procédure, et recommencez-la une seconde fois en sélectionnant l'autre option de groupes de port.

Prérequis

Des adaptateurs réseau (NIC) de plusieurs giga-octets sont nécessaires. Pour chaque hôte compatible avec Fault Tolerance (Fault Tolerance), il faut au minimum deux adaptateurs réseau physiques de plusieurs gigaoctets : par exemple, l'une dédiée à la journalisation de Fault Tolerance et l'autre dédiée à vMotion. Utilisation de trois adaptateurs réseau ou plus pour assurer la disponibilité.

Remarque Les cartes réseau de journalisation vMotion et de tolérance aux pannes doivent être sur des sous-réseaux différents. IPv6 n'est pas pris en charge sur la carte réseau de journalisation FT.

Procédure

1 Dans vSphere Web Client, accédez à l'hôte

2 Cliquez sur l'onglet **Gérer**, puis cliquez sur **Mise en réseau**.

3 Cliquer sur **Actions > Toutes les Actions vCenter > Ajouter réseau**.

4 Sélectionnez **Adaptateur de réseau VMkernel** sur la page Sélectionner un type de connexion et cliquez sur **Suivant.**

5 Sélectionner **Nouveau commutateur standard** et cliquer sur **Suivant**.

6 Attribuer des adaptateurs réseaux physiques gratuits à l'interrupteur, puis cliquer sur **Suivant**.

7 Fournir une étiquette réseau et activer les services que vous désirez et cliquer sur **Suivant**.

8 Fournir une adresse IP et le masque de sous-réseau et cliquer sur **Terminer** après avoir examiné vos paramètres.

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

Suivant

Remarque Si vous configurez la mise en réseau pour la prise en charge de Fault Tolerance mais que par la suite vous désactivez le port de journalisation de Fault Tolerance, les paires de machines virtuelles à Fault Tolerance qui sont déjà sous tension le restent. Mais dans le cas de situation de basculement, une nouvelle VM secondaire n'est pas démarrée après le remplacement de la VM principale par sa VM secondaire. Par conséquent, la nouvelle VM principale fonctionne en état non protégé.

Exemple de configuration de la mise en réseau des hôtes de Fault Tolerance

Cet exemple décrit la configuration du réseau hôte de Fault Tolerance dans un déploiement typique avec quatre cartes NIC de 1 Go. Ce déploiement garantit un service adéquat pour chaque type de trafic identifié dans cet exemple il pourrait être considéré comme la meilleure configuration possible.

Fault Tolerance assure une disponibilité totale pendant toute la durée de la défaillance d'un hôte physique due à une coupure de l'alimentation électrique, une panique du système ou à toute autre raison de ce type. Les défaillances au niveau du chemin de stockage ou du réseau, ou encore de tout autre composant du serveur physique qui n'ont pas de répercussions sur l'état opérationnel de l'hôte ne provoquent pas un basculement de Fault Tolerance sur la machine virtuelle secondaire. Par conséquent, les clients sont vivement encouragés à utiliser la redondance appropriée (par exemple, l'association de adaptateurs réseau) pour réduire les risques de perte de connexion des machines virtuelles en faveur de composants d'infrastructure comme des réseaux ou des baies de stockage.

Les règles d'association des adaptateurs 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) à partir des machines virtuelles et des ports vmkernel. Un groupe de ports unique est généralement utilisé pour chaque type de trafic, chacun étant généralement associé à un VLAN différent.

Instructions 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 Fault Tolerance avec différentes combinaisons de types de trafic (par exemple, NFS) et plusieurs adaptateurs réseau physiques.

- Répartissez chaque association de adaptateurs réseau sur deux commutateurs physiques assurant la continuité des domaines L2 pour chaque VLAN entre les deux commutateurs physiques.
- Utilisez des règles d'association déterministe pour vous assurer que des types de trafic particuliers présentent une affinité avec une carte réseau particulière (active/veille) ou un ensemble de adaptateurs réseau (par exemple, ID port virtuel d'origine).
- Quand des règles active/veille sont utilisées, associez les types de trafic pour réduire les répercussions dans le 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 surabonner le commutateur à des liaisons de commutateurs.

Exemple de configuration avec quatre cartes NIC de 1 Go

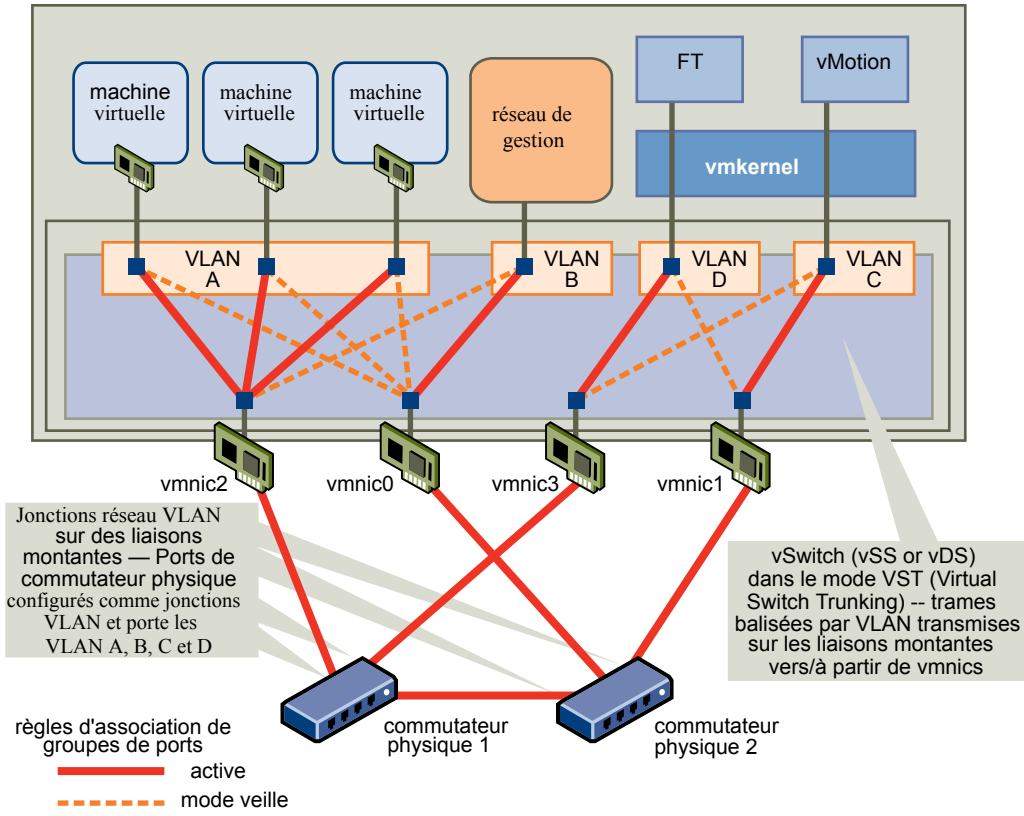
Figure 3-2 décrit la configuration du réseau pour un seul hôte ESXi avec quatre cartes NIC de 1 Go prenant en charge Fault Tolerance. Les autres hôtes du cluster FT seraient configurés de la même manière.

Cet exemple utilise quatre groupes de ports configurés comme suit :

- VLAN A : Port réseau des machines virtuelles actif au niveau du groupe sur vmnic2 (vers le commutateur physique #1) ; en veille sur vmnic0 (vers le commutateur physique #2.)
- VLAN B : Port réseau de gestion actif au niveau du groupe sur vmnic0 (vers le commutateur physique #2) ; en veille sur vmnic2 (vers le commutateur physique #1.)
- VLAN C : Port de vMotion actif au niveau du groupe sur vmnic1 (vers le commutateur physique #2) ; en veille sur vmnic3 (vers le commutateur physique #1.)
- VLAN D : Port de journalisation FT actif au niveau du groupe sur vmnic3 (vers le commutateur physique #1) ; en veille sur vmnic1 (vers le commutateur physique #2.)

La journalisation vMotion et FT peut partager le même VLAN (configurez le même nombre de VLAN dans les deux groupes de ports), mais exige que leurs propres adresses IP uniques résident 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 Fault Tolerance



Créer un cluster et vérifier la conformité dans vSphere Web Client

vSphere Fault Tolerance est utilisé dans le cadre d'un cluster vSphere HA. Après avoir configuré la mise en réseau de chaque hôte, créez le cluster vSphere HA et ajoutez-y les hôtes. Vous pouvez vérifier que le cluster est configuré correctement et qu'il est conforme aux exigences pour l'activation de Fault Tolerance.

Procédure

1 Dans vSphere Web Client, accédez au cluster.

2 Cliquez sur l'onglet **Surveiller** puis sur **Conformité de profil**.

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

Les résultats des tests de conformité apparaissent et la conformité ou non de chaque hôte s'affiche.

Assurer Fault Tolerance des machines virtuelles

Après avoir suivi toutes les étapes nécessaires à l'activation de vSphere Fault Tolerance pour votre cluster, vous pouvez utiliser cette fonction en l'activant sur des machines virtuelles individuelles.

L'option permettant d'activer Fault Tolerance 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 en mode maintenance ou standby.
- 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 Fault Tolerance 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 Fault Tolerance

Plusieurs contrôles de validation sont exécutés sur une machine virtuelle avant de pouvoir activer Fault Tolerance.

- Le contrôle de certificat SSL doit être activé dans les paramètres de vCenter Server.
- L'hôte doit se trouver dans un cluster vSphere HA ou un cluster mixte vSphere HA et DRS.
- L'hôte doir 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 vSphere HA désactivé.
- Aucun périphérique vidéo dont la 3D est activée ne doit être présent sur la machine virtuelle.

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 Fault Tolerance.
- L'hôte qui prend en charge la machine virtuelle secondaire doit avoir un processeur qui prend en charge Fault Tolerance 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 Fault Tolerance. Pour en avoir la confirmation, consultez le Guide de compatibilité VMware sur http://www.vmware.com/resources/compatibility/search.php et sélectionnez **Recherche par ensembles compatibles Fault Tolerance**.
- La combinaison du système de la machine virtuelle d'exploitation invité et le processeur doit être prise en charge par Fault Tolerance (par exemple, Solaris de 32 bits sur des processeurs AMD n'est pas actuellement pris en charge). Consultez l'article de la base de connaissances de VMware sur http://kb.vmware.com/kb/1008027 pour obtenir des informations sur les combinaisons 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 Fault Tolerance (par exemple, la configuration ne peut comporter aucun périphérique non pris en charge.).

Quand votre effort d'activation de Fault Tolerance 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 Fault Tolerance.

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.
- Le statut de Fault Tolerance affiché pour la machine virtuelle est **protégée**.

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.
- Le statut de Fault Tolerance affiché pour la machine virtuelle est **Non protégée, VM pas en exécution**.
- Quand vous essayez de mettre sous tension la machine virtuelle primaire après l'activation de Fault Tolerance, 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. Le statut de Fault Tolerance de la machine virtuelle est marqué comme **Protégée**.

Activer Fault Tolerance pour les machines virtuelles dans vSphere Web Client

Vous pouvez activer vSphere Fault Tolerance via vSphere Web Client.

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

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

Procédure

1 Dans vSphere Web Client, accédez à la VM pour laquelle vous souhaitez activer Fault Tolerance

2 Cliquez avec le bouton droit la machine virtuelle et sélectionner **Toutes les actions vCenter > Fault Tolerance > Démarrer Fault Tolerance**.

3 Cliquez sur **Oui**.

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

Définir les options pour les machines virtuelles Fault Tolerant dans vSphere Web Client

Après avoir activé vSphere Fault Tolerance pour une machine virtuelle, de nouvelles options sont ajoutées à la section Tolérance aux pannes de son menu contextuel.

Dans le vSphere Web Client, il existe des options pour mettre hors tension ou désactiver Fault Tolerance, faire migrer la machine virtuelle secondaire, tester le basculement et tester le redémarrage de la machine virtuelle secondaire.

Désactiver Fault Tolerance dans vSphere Web Client

La désactivation de vSphere Fault Tolerance supprime la machine virtuelle secondaire, sa configuration et l'ensemble de son historique.

Utilisez l'option **Désactiver Fault Tolerance** si vous n'avez pas prévu de réactiver la fonction. Dans le cas contraire, utilisez l'option **Désactiver Fault Tolerance**.

Remarque Si la VM secondaire réside sur un hôte en mode maintenance, déconnecté ou qui ne répond pas, vous ne pouvez pas utiliser l'option **Arrêter tFault Tolerance**. Dans ce cas, désactivez, puis activez Fault Tolerance.

Procédure

1 Dans vSphere Web Client, accédez à la VM pour laquelle vous souhaitez arrêter Fault Tolerance.

2 Cliquez avec le bouton droit sur la machine virtuelle et sélectionner **Toutes les actions vCenter > Fault Tolerance > Désactiver Fault Tolerance**.

3 Cliquez sur **Oui**.

Fault Tolerance est arrêtée pour la machine virtuelle sélectionnée. L'historique, ainsi que la VM secondaire de la VM sélectionnée sont supprimés.

Migrer une VM secondaire dans vSphere Web Client

Une fois que vSphere Fault Tolerance est activé pour une VM principale, vous pouvez migrer sa VM secondaire associée.

Procédure

1 Dans vSphere Web Client, accédez à la VM primaire pour laquelle vous souhaitez migrer sa VM secondaire.

2 Cliquez-droit sur la machine virtuelle et sélectionner **Toutes les actions vCenter > Fault Tolerance > Migration secondaire**.

3 Remplissez les options de la boîte de dialogue Migrer et validez les changements que vous faites.

4 Cliquez sur **Terminer** pour appliquer les modifications.

La VM secondaire associée à la machine virtuelle insensible aux défaillances sélectionnée est migrée vers l'hôte spécifié.

Désactiver Fault Tolerance dans vSphere Web Client

La désactivation de vSphere Fault Tolerance pour une machine virtuelle suspend sa protection de Fault Tolerance, mais conserve la machine virtuelle secondaire, sa configuration et tout l'historique. Utilisez cette option pour réactiver la protection Fault Tolerance à l'avenir.

Procédure

1 Dans vSphere Web Client, accédez à la VM pour laquelle vous souhaitez désactiver Fault Tolerance.

2 Cliquez-droit sur la machine virtuelle et sélectionner **Toutes les actions vCenter > Fault Tolerance > Désactiver Fault Tolerance**.

3 Cliquez sur **Oui**.

Fault Tolerance est désactivée pour la machine virtuelle sélectionnée. L'historique et la machine virtuelle secondaire de la machine virtuelle sélectionnée sont préservés et seront utilisés si la fonction réactivée.

Suivant

Une fois que vous avez désactivé Fault Tolerance, l'option du menu devient **Activer Fault Tolerance**. Activer cette option pour réactivez cette fonction.

Tester le basculement de Fault Tolerance dans vSphere Web Client

Vous pouvez provoquer une situation de basculement pour une VM principale sélectionnée afin de tester la protection de Fault Tolerance.

Cette option est indisponible (grisée) si la VM est mise sous tension.

Procédure

1 Dans vSphere Web Client accédez à la VM primaire pour laquelle vous souhaitez tester le basculement.

2 Cliquez avec le bouton droit sur la machine virtuelle et sélectionner **Toutes les actions vCenter > Fault Tolerance > Tester le basculement**.

3 Consultez les détails sur le basculement dans la console de travail.

Cette tâche provoque la défaillance de la VM principale afin de s'assurer que la VM secondaire la remplace. Une nouvelle VM secondaire est également démarrée, pour replacer la VM principale dans un état protégé.

Tester le redémarrage de VM secondaire dans vSphere Web Client

Vous pouvez provoquer la défaillance d'une VM secondaire afin de tester la protection Fault Tolerance fournie pour une VM principale sélectionnée.

Cette option est indisponible (grisée) si la VM est mise sous tension.

Procédure

1 Dans vSphere Web Client, accédez à la VM primaire pour laquelle vous souhaitez effectuer le test.

2 Cliquez avec le bouton droit sur la machine virtuelle et sélectionner **Toutes les actions vCenter > Fault Tolerance > Tester le redémarrage secondaire**.

3 Consultez les détails du test dans la Console des tâches

Cette tâche a pour conséquence l'arrêt de la VM secondaire qui assurait la protection Fault Tolerance pour la VM principale sélectionnée. Une nouvelle VM secondaire est alors démarrée, replaçant la la VM principale dans un état protégé.

Consulter les informations sur les machines virtuelles Fault Tolerant dans vSphere Web Client

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

Remarque Vous ne pouvez pas mettre hors tension Fault Tolerance de la machine virtuelle secondaire.

Le volet vSphere Fault Tolerance apparaît dans l'onglet **Résumé** pour la machine virtuelle principale et contient des informations sur la machine virtuelle.

état de Fault Tolerance Indique l'état de Fault Tolerance de la machine virtuelle.

- Protégée. Indique que les machines virtuelles principale et secondaire sont sous tension et fonctionnent comme prévu.

- Non protégée. La VM secondaire ne fonctionne pas. Les raisons possibles sont répertoriées dans le tableau.

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

Raison de l'état non protégé	Description
Démarrage	Fault Tolerance est en train de démarrer la VM secondaire. Ce message n'est visible que pendant une courte durée.
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 VM secondaire. Remédiez à 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 Fault Tolerance puis sa réactivation suffit pour corriger ce problème.
Désactivé	Fault Tolerance est actuellement désactivée (aucune machine virtuelle secondaire ne fonctionne). Ceci se produit quand Fault Tolerance est désactivée par l'utilisateur ou quand vCenter Server désactive Fault Tolerance après avoir échoué dans la mise sous tension de la machine virtuelle secondaire.
Machine virtuelle hors fonctionnement	Fault Tolerance est activée mais la machine virtuelle est hors tension. Mettez sous tension la machine virtuelle pour obtenir l'état Protégé.

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

CPU secondaire totale Indique l'utilisation du CPU de la machine virtuelle secondaire, exprimée en MHz.

Mémoire secondaire totale 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.

Largeur de bande de journalisation Capacité réseau utilisée pour envoyer les informations de journalisation de vSphere Fault Tolerance, de l'hôte exécutant la machine virtuelle principale à l'hôte exécutant la machine virtuelle secondaire.

Pratiques d'excellence pour Fault Tolerance

Pour garantir des résultats Fault Tolerance optimaux, vous devez respectez certaines meilleures pratiques.

En plus des informations suivantes, consultez le livre blanc *Recommandations et considérations sur VMware Fault Tolerance* sur http://www.vmware.com/resources/techresources/10040.

Configuration d'hôte

Tenez compte des meilleures pratiques 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 réglées 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

vSphere Fault Tolerance peut fonctionner dans des clusters contenant 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 être configurés comme suit :

- Processeurs appartenant au même groupe de processeurs compatibles.
- Accès commun aux banques de données utilisées par les machines virtuelles.
- La même configuration réseau de machines virtuelles.
- La même version d'ESXi.
- Le même numéro de version de Fault Tolerance (ou numéro de version d'hôte pour les hôtes antérieurs à ESX/ESXi 4.1).
- Les mêmes paramètres de 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 une carte réseau de 10 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 Fault Tolerance est activée doivent être conservées sur des stockages partagés accessibles aux deux instances de la machine virtuelle tolérante aux pannes. Si vous utilisez cette configuration, le CD-ROM présent dans la machine virtuelle continue de fonctionner correctement, même en cas de basculement.

Pour les machines virtuelles dont Fault Tolerance 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 basculement, 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.

Éviter les partitions de réseau

Une partition de réseau survient quand un cluster vSphere HA connaît une défaillance du réseau de gestion qui isole certains hôtes de vCenter Server et les isole les uns des autres. Reportez-vous à la section « Partitions de réseau », page 16. En cas de partition, la protection de Fault Tolerance peut être réduite.

Dans un cluster vSphere HA partitionné utilisant Fault Tolerance, la machine virtuelle principale (ou sa machine virtuelle secondaire) pourrait se retrouver dans une partition gérée par un hôte principal qui n'est pas responsable de cette machine virtuelle. Si un basculement est nécessaire, une machine virtuelle secondaire est redémarrée uniquement si la machine virtuelle principale se trouvait dans une partition gérée par un hôte principal qui en était responsable.

Pour réduire les risques de panne de votre réseau de gestion entraînant une partition du réseau, suivez les recommandations figurant dans « Meilleures pratiques pour la mise en réseau », page 37.

Afficher les erreurs Fault Tolerance dans vSphere Web Client

Lorsque les tâches liées à votre implémentation de Fault Tolerance provoquent des erreurs, vous pouvez afficher l'information à leur sujet dans le volet **Tâches récentes**.

Le volet **Tâches récentes** affiche un résumé de chaque erreur sous l'onglet **Échec**. Pour plus d'informations sur les tâches qui ont échoué, cliquez sur **Plus de tâches** pour ouvrir la Console des tâches.

Dans la console des tâches, chaque tâche est répertoriée avec ses informations qui comprennent son Nom, sa cible, et son État. Dans la colonne État, si la tâche a échoué, le type de faute générée est décrit. Pour plus d'informations sur une tâche, sélectionnez-la et les détails apparaîtront dans le volet sous la liste des tâches.

Mettre à niveau les hôtes utilisés pour Fault Tolerance

Lorsque vous mettez à jour 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 version 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 ensembles d'au moins quatre hôtes ESXi hébergeant des machines virtuelles tolérantes aux pannes qui sont 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 de façon à ce qu'ils aient la même version d'ESXi.

3 Désactivez Fault Tolerance sur la machine virtuelle principale.

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

5 Activez Fault Tolerance sur la machine virtuelle principale qui a été déplacée.

6 RépétezÉtape 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 ESXi d'un cluster sont mis à niveau.

Recommandations de configuration de vSphere Fault Tolerance

Vous devez respecter certaines directives lors de la configuration de Fault Tolerance.

- 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 faire tourner en toute sécurité sur chaque hôte est fonction de la taille et de la charge de travail, variables, de l'hôte ESXi et des machines virtuelles.
- Si vous accédez au stockage partagé par NFS, utilisez du matériel NAS dédié avec au moins une carte réseau 1 Gbit pour atteindre les performances réseaux requises pour le bon fonctionnement de Fault Tolerance.
- 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 réserve de mémoire d'une machine virtuelle tolérante aux pannes est définie par la taille de la mémoire de la machine virtuelle lorsque Fault Tolerance 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 Fault Tolerance, il est recommandé d'avoir au minimum 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.

Index

R

S

T

V