Disponibilité vSphere

Update 1
Modifié le 13 août 2020
VMware vSphere 6.0
VMware ESXi 6.0
vCenter Server 6.0

vmware®

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

https://docs.vmware.com/fr/

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

VMware France SAS.
Tour Franklin
100-101 Terrasse Boieldieu
92042 Paris La Défense 8 Cedex
France
www.vmware.com/fr

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 cible

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 livre sont destinées aux administrateurs du système Windows ou Linux expérimentés qui connaissent le fonctionnement de la technologie des machines virtuelles et des centres de données.

Informations mises à jour

Ce document *Disponibilité vSphere* est mis à jour à chaque nouvelle version du produit ou lorsque cela s'avère nécessaire.

Ce tableau indique l'historique des mises à jour du document *Disponibilité vSphere*.

Révision	Description
10 août 2020	VMware prend l'intégration au sérieux. Pour encourager ce principe avec notre client, notre partenaire et notre communauté interne, nous remplaçons en partie la terminologie de notre contenu. Nous avons mis à jour ce guide pour supprimer des instances de langage non inclusif.
7 octobre 2016	Version initiale.

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 contient 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 pannes 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.
- Il protège contre les erreurs d'accessibilité de la banque de données en redémarrant les machines virtuelles affectées sur d'autres hôtes ayant toujours accès à leurs banques de données.
- Il protège les machines virtuelles contre l'isolation réseau en les redémarrant si leurs hôtes se retrouvent isolés sur le réseau de gestion ou Virtual SAN. Cette protection est assurée même si le réseau s'est retrouvé partitionné.

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.

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 options avancées et en optimiser les performances en suivant les recommandations.

Note Vous pouvez obtenir un message d'erreur lorsque vous essayez d'utiliser vSphere HA. Pour plus d'informations sur les messages d'erreur relatifs à vSphere HA, reportez-vous à l'article de la base de connaissances VMware sur http://kb.vmware.com/kb/1033634.

Ce chapitre contient 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 principal. L'hôte principal communique avec vCenter Server et surveille l'état de protection de toutes les machines virtuelles et des hôtes secondaires. 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 du réseau et de la banque de données pour déterminer le type de panne.

Clusters vSphere HA (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_ynopbsu2/uiConfId/49694343/)

Hôtes principal et secondaire

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 comme un hôte principal ou un hôte secondaire.

Lorsque vSphere HA est activé pour un cluster, tous les hôtes actifs (ceux qui ne sont pas en mode de veille ou de 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, arrêté, mis en mode de veille ou supprimé 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 en échec 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 assure son redémarrage. 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 machines virtuelles et d'applications.

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

Note 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 de la panne 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 :

- Panne : un hôte cesse de fonctionner.
- Isolation : un hôte se retrouve isolé sur le réseau.
- Modion : un hôte perd la connectivité 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, il vérifie la réactivité de l'hôte avant de le déclarer en échec. 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 . 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 en échec. 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 isolé du réseau, et continue donc de surveiller l'hôte et ses machines virtuelles. Reportez-vous à la section Partitions de réseau .

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.

Note 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 échoue et que ses machines virtuelles doivent être redémarrées, vous pouvez contrôler l'ordre dans lequel cela se fait avec le paramètre de priorité de redémarrage des machines virtuelles. 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. D'autres facteurs sont également pris en compte lorsque vSphere HA redémarre une machine virtuelle après un échec.

Les paramètres suivants s'appliquent à toutes les machines virtuelles du cluster en cas d'échec ou d'isolation d'un hôte. Vous pouvez configurer des exceptions pour des machines virtuelles spécifiques. Reportez-vous à la section Personnaliser une machine virtuelle secondaire .

Priorité de redémarrage des VM

La priorité de redémarrage des machines virtuelles détermine l'ordre relatif dans lequel des ressources sont attribuées aux machines virtuelles en cas d'échec d'un hôte. Les machines virtuelles de ce type sont attribuées aux hôtes avec une capacité non réservée. Celles ayant la priorité la plus élevée sont attribuées en premier, puis les machines virtuelles ayant une priorité inférieure, et ainsi de suite jusqu'à ce que toutes les machines virtuelles aient été placées ou qu'aucune capacité de cluster ne soit disponible pour satisfaire aux réservations ou à la mémoire de temps système des machines virtuelles. Ensuite, un hôte redémarre les machines virtuelles qui lui sont attribuées par ordre de priorité. En cas de ressources insuffisantes, vSphere HA attend de disposer de capacité non réservée supplémentaire, par exemple, grâce au retour en ligne d'un hôte, puis tente à nouveau de placer ces machines virtuelles. Pour empêcher que cette situation se présente, configurez le contrôle d'admission de vSphere HA afin qu'il réserve davantage de ressources en cas d'échec. Le contrôle d'admission vous permet de contrôler la capacité de cluster réservée par les machines virtuelles qui est indisponible afin de satisfaire aux réservations et à la mémoire de temps système des machines virtuelles.

Les valeurs de ce paramètre sont Désactivée, Basse, Moyenne (par défaut) et Haute. Le paramètre Désactivée est ignoré par la fonctionnalité Surveillance de VM et d'application de vSphere HA car celle-ci protège les machines virtuelles contre les échecs au niveau du système d'exploitation et non contre les échecs des machines virtuelles. Lorsqu'un échec 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.

Note La réinitialisation d'une machine virtuelle provoque un redémarrage du système d'exploitation invité 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 fonctionnalités 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.

Si un hôte échoue, vSphere HA tente d'inscrire sur un hôte actif les machines virtuelles concernées qui étaient sous tension et qui disposent d'un paramètre de priorité de redémarrage défini sur Désactivée ou qui étaient hors tension.

Réponse d'isolation de l'hôte

La réponse d'isolation d'hôte détermine les événements survenant lorsqu'un hôte d'un cluster vSphere HA perd ses connexions au réseau de gestion, mais continue à s'exécuter. Vous pouvez utiliser la réaction à l'isolation afin que vSphere HA mette hors tension les machines virtuelles en cours d'exécution sur un hôte isolé et les redémarre sur un hôte non isolé. Les réponses d'isolation d'hôte exigent que l'état de surveillance de l'hôte soit activé. Si l'état de surveillance de l'hôte est désactivé, les réponses d'isolation d'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'isolation. L'hôte exécute ensuite sa réponse d'isolation. Les réponses sont Mettre hors tension et redémarrer les VM ou Arrêter et redémarrer les machines virtuelles. Vous pouvez personnaliser cette propriété pour des machines virtuelles individuelles.

Note Si le paramètre de priorité de redémarrage d'une machine virtuelle est défini sur Désactivée, aucune réponse d'isolation d'hôte n'est fournie.

Pour utiliser le paramètre Arrêter et redémarrer les machines virtuelles, vous devez installer VMware Tools dans le système d'exploitation invité 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 s'arrêter 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'option avancée `das.isolationshutdowntimeout` sont mises hors tension.

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 d'isolation 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.

Une condition de split-brain peut se produire sur une machine virtuelle lorsqu'un hôte se retrouve isolé ou partitionné depuis un hôte principal qui ne peut pas communiquer avec lui à l'aide des banques de données des signaux de pulsation. Dans une telle situation, l'hôte principal n'est pas en mesure de déterminer si l'hôte est actif et le déclare inactif. L'hôte principal fait ensuite une tentative pour redémarrer les machines virtuelles qui s'exécutent sur l'hôte isolé ou partitionné. Cette tentative réussit si les machines virtuelles continuent de s'exécuter sur l'hôte isolé ou partitionné et celui-ci perd l'accès aux banques de données des machines virtuelles quand il s'est retrouvé isolé ou partitionné. Il existe alors une condition de split-brain, car la machine virtuelle se retrouve avec deux instances. Toutefois, seule une de ces instances est en mesure de lire ou d'écrire sur les disques virtuels de la machine virtuelle. VM Component Protection peut vous aider à empêcher cette condition de split-brain. Lorsque vous activez VMCP avec le paramètre intensif, il contrôle l'accessibilité de la banque de données sur les machines virtuelles sous tension et arrête celles qui perdent l'accès à leurs banques de données.

Pour résoudre ce problème, ESXi génère une question sur la machine virtuelle qui a perdu les verrouillages disque pour le moment où l'hôte quitte son état d'isolation et est dans l'impossibilité 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 se mettre hors tension, laissant uniquement l'instance qui dispose des verrouillages disque.

Facteurs pris en charge pour le redémarrage de la machine virtuelle

Après un échec, l'hôte principal du cluster fait une tentative de redémarrage des machines virtuelles concernées en identifiant un hôte susceptible de les mettre sous tension. Lors de la sélection de cet hôte, l'hôte principal tient compte d'un certain nombre de facteurs.

Accessibilité des fichiers

Avant le démarrage d'une machine virtuelle, ses fichiers doivent être accessibles depuis l'un des hôtes actif du cluster avec lequel l'hôte principal peut communiquer via le réseau.

Machine virtuelle et compatibilité de l'hôte

S'il existe des hôtes accessibles, la machine virtuelle doit être compatible avec au moins l'un d'entre eux. La compatibilité définie pour une machine virtuelle comprend l'effet de l'une des règles d'affinité machine virtuelle/hôte. Par exemple, si une règle permet à une machine virtuelle de s'exécuter sur deux hôtes, elle est prise en compte pour le placement sur ces deux hôtes.

Réservations de ressources

Parmi les hôtes sur lesquels la machine virtuelle peut s'exécuter, au moins un doit disposer d'une capacité non réservée suffisante pour satisfaire aux besoins de la mémoire de temps système de la machine virtuelle et aux réservations de ressources. Quatre types de réservations sont prises en compte : CPU, mémoire, vNIC et lecteur Flash virtuel. De plus, un nombre de ports réseau suffisant doit être disponible pour mettre sous tension la machine virtuelle.

Limites d'hôtes

En plus des réservations de ressources, une machine virtuelle ne peut être placée sur un hôte que si cela ne lui fait pas dépasser le nombre maximal de machines virtuelles autorisées ou de vCPU utilisés.

Contraintes de la fonctionnalité

Si l'option avancée qui a été définie nécessite que vSphere HA fasse respecter les règles d'affinité machine virtuelle/machine virtuelle, vSphere HA n'enfreint pas cette règle. De plus, vSphere HA n'enfreint pas les limites configurée pour chaque hôte pour les machines virtuelles Fault Tolerance.

Si aucun hôte ne répond aux considérations précédentes, l'hôte principal émet un événement indiquant qu'il ne dispose pas des ressources suffisantes pour que vSphere HA démarre la machine virtuelle et ressaiera une fois les conditions du cluster améliorées. Par exemple, si la machine virtuelle n'est pas accessible, l'hôte principal réessaie après une modification de l'accessibilité des fichiers.

Limites des tentatives de redémarrage de la machine virtuelle

Si la tentative de l'agent principal vSphere HA de redémarrer une machine virtuelle, qui implique son enregistrement et sa mise sous tension, échoue, ce redémarrage est réessayé après un délai d'attente. vSphere HA tente ces redémarrages un nombre maximal de tentatives (6 par défaut), mais tous les échecs de redémarrage ne sont pas comptabilisés dans ce nombre maximal.

Par exemple, la raison la plus probable qu'une tentative de redémarrage échoue est que soit la machine virtuelle continue de s'exécuter sur un autre hôte, soit que vSphere HA a essayé de redémarrer la machine virtuelle trop tôt après que celle-ci ait échoué. Dans ce cas, l'agent principal retarde la nouvelle tentative de deux fois le délai d'attente imposé après la dernière tentative, avec un délai minimal de 1 minute et un délai maximal de 30 minutes. Par conséquent, si le délai est défini sur 1 minute, la tentative initiale est à T=0, les tentatives supplémentaires seront effectuées à T=1 (1 minute), T=3 (3 minutes), T=7 (7 minutes), T=15 (15 minutes) et T=30 (30 minutes). Chacune de ces tentatives est décomptée du nombre maximal et seules six tentatives sont effectuées par défaut.

Les autres échecs de tentatives entraînent des tentatives qui sont comptabilisées, mais avec un intervalle de temps différent. Par exemple, l'hôte sélectionné pour redémarrer la machine virtuelle perd l'accès à l'une des banques de données de la machine virtuelle après que l'agent principal ait fait son choix. Une tentative est alors effectuée après un délai par défaut de 2 minutes. Cette tentative est décomptée de la limite.

Enfin, certaines tentatives ne sont pas comptabilisées. Par exemple, si l'hôte sur lequel la machine virtuelle devait être redémarrée échoue avant que l'agent principal n'émette la demande de redémarrage, une nouvelle tentative est effectuée au bout de 2 minutes, mais cet échec n'est pas soustrait du nombre maximal de tentatives.

Notifications de redémarrage de la machine virtuelle

vSphere HA génère un événement de cluster lorsqu'une opération de basculement est en cours pour les machines virtuelles du cluster. L'événement affiche également un problème de configuration dans l'onglet **Résumé du cluster** qui indique le nombre de machines virtuelles en cours de redémarrage. Il existe quatre catégories distinctes de machines virtuelles de ce type.

- Les machines virtuelles en cours de placement : vSphere HA tente actuellement de redémarrer ces machines virtuelles
- Les machines virtuelles en attente d'une tentative : une tentative de redémarrage a échoué et vSphere HA attend actuellement qu'un délai arrive à expiration avant de réessayer.
- Les machines virtuelles nécessitant des ressources supplémentaires : les ressources disponibles sont insuffisantes pour redémarrer ces machines virtuelles. vSphere HA retente lorsque davantage de ressources deviennent disponibles. Par exemple un hôte revient en ligne.
- Machines virtuelles Virtual SAN inaccessibles : vSphere HA ne peut pas redémarrer ces machines virtuelles Virtual SAN, car elles ne sont pas accessibles. Il réessaiera dès qu'il y aura un changement d'accessibilité.

Ces nombres de machines virtuelles sont mis à jour de manière dynamique à chaque fois qu'une modification est observée dans le nombre de machines virtuelles pour lesquelles une opération de redémarrage est en cours. Le problème de configuration est effacé une fois que vSphere HA a redémarré toutes les machines virtuelles ou a arrêté d'essayer.

Dans vSphere 5.5 ou version antérieure, un événement par machine virtuelle est déclenché en cas d'échec de la tentative de redémarrage de la machine virtuelle. Cet événement est désactivé par défaut dans vSphere 6.x et peut être activé en définissant l'option avancée de vSphere HA `das.config.fdm.reportfailoverfailevent` sur 1.

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'option avancée `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. Paramètres de surveillance des machines virtuelles. 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**.

Note 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.

Si une machine virtuelle rencontre un problème d'accessibilité à la banque de données (Tous chemins hors service ou Perte de périphérique permanente), le service de surveillance de machine virtuelle interrompt sa réinitialisation jusqu'à ce que le problème ait été résolu.

VM Component Protection

Si VM Component Protection (VMCP) est activé, vSphere HA peut détecter les erreurs d'accessibilité à la banque de données et fournir une récupération automatisée pour les machines virtuelles concernées.

VMCP offre une protection contre les erreurs d'accessibilité à la banque de données qui affectent une machine virtuelle s'exécutant sur un hôte dans un cluster vSphere HA. En cas d'erreur d'accessibilité à une banque de données, l'hôte affecté ne peut plus accéder au chemin de stockage d'une banque de données spécifique. Vous pouvez déterminer la réaction de vSphere HA face à cette erreur, depuis la création d'alarmes d'événement jusqu'au redémarrage de la machine virtuelle sur d'autres hôtes.

Note Pour utiliser la fonctionnalité VM Component Protection, la version de vos hôtes ESXi doit être 6.0 ou une version ultérieure.

Types d'erreurs

Il existe deux types d'erreurs d'accessibilité à une banque de données :

PDL

PDL (perte de périphérique permanente) est une perte d'accessibilité irrécupérable qui se produit lorsqu'un périphérique de stockage signale que la banque de données n'est plus accessible à l'hôte. Cette condition ne peut pas être rétablie sans mettre hors tension les machines virtuelles.

APD

APD (Tous chemins hors service) représente une perte d'accessibilité temporaire ou inconnue, ou tout autre retard non identifié dans le traitement des E/S. Ce type d'erreur d'accessibilité est récupérable.

Configuration de VMCP

La fonctionnalité VM Component Protection est configurée dans vSphere Web Client. Accédez à l'onglet **Configurer** et cliquez sur **Disponibilité vSphere**, puis cliquez sur **Modifier**. Sous **Pannes et réponses**, vous pouvez sélectionnez l'option **Banque de données avec PDL** ou **Banque de données avec APD**. Les niveaux de protection du stockage que vous pouvez sélectionner et les actions de correction de la machine virtuelle disponibles varient selon le type d'erreur d'accessibilité à la base de données.

Erreurs PDL

Sous **Banque de données avec PDL**, vous pouvez sélectionner l'option **Émission d'événements** ou **Mettre hors tension et redémarrer les VM**.

Erreurs APD

La réponse aux événements APD est plus complexe et, en fonction de la configuration, est définie avec une plus grande précision. Vous pouvez sélectionner l'option **Émission d'événements**, **Mettre hors tension et redémarrer les VM : stratégie de redémarrage modérée** ou **Mettre hors tension et redémarrer les VM : stratégie de redémarrage agressive**.

Note Si les paramètres Surveillance VM ou Priorité redémarrage VM sont désactivés, VMCP ne peut pas redémarrer la machine virtuelle. Toutefois, la santé du stockage peut toujours être surveillée et les événements être émis.

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 fonctionnalités de gestion du cluster. Réparez le cluster partitionné dès que possible.

- Protection des machines virtuelles. vCenter Server permet de mettre sous tension une machine virtuelle, mais celle-ci ne peut être 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 des clusters. vCenter Server peut communiquer avec l'hôte principal, mais uniquement un sous-ensemble des hôtes secondaires. 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.

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 a échoué, s'il se trouve dans une partition de réseau ou s'il est isolé du réseau. 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'option avancée `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.

Note 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 gérer l'hôte. vCenter Server crée un mot de passe aléatoire pour ce compte et modifie régulièrement le mot de passe. 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 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.

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 de manière permanente, 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 ou de l'application d'un correctif sur des hôtes ESXi 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.

Note 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 tolérer un nombre spécifié de pannes d'hôte. 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.

Note 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

Taille d'emplacement et contrôle d'admission de vSphere HA (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_q744qxvn/uiConfId/49694343/)

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'option avancée `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 options avancées `das.slotcpuinmhz` ou `das.slotmeminmb`. Reportez-vous à la section Options avancées de vSphere HA.

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.

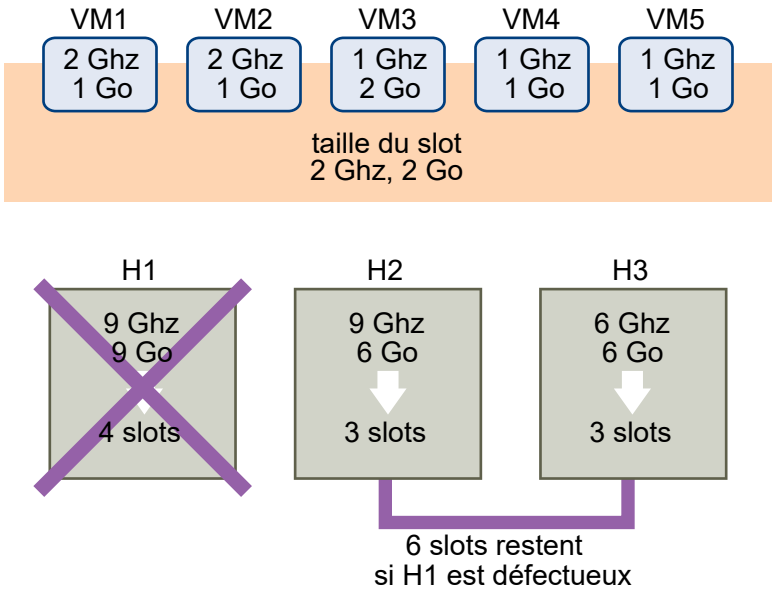
Exemple : Stratégie de contrôle d'admission Défaillances d'hôte tolérées par le cluster

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 slots, 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 slot disponible (les six slots de H2 et H3 moins les cinq slots utilisés).

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

Il est possible de configurer 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.

Note 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'option avancée `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.

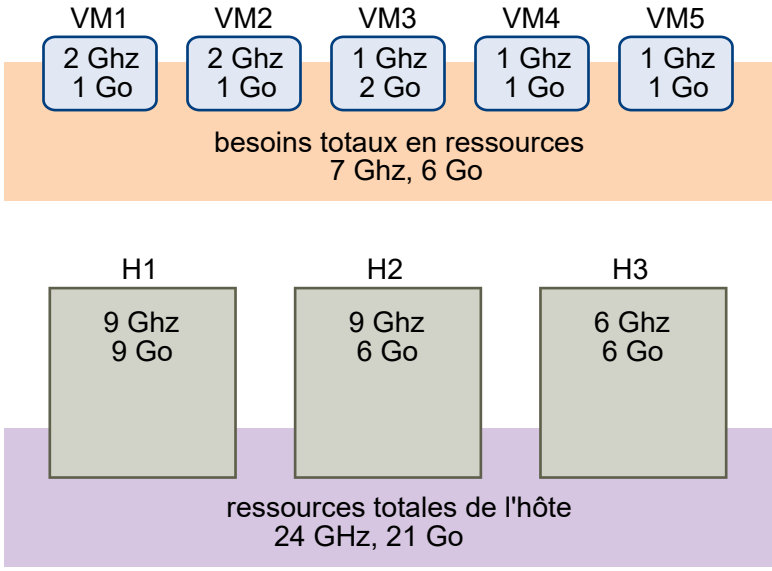
La Capacité CPU de basculement actuelle est calculée en soustrayant les besoins totaux en ressources CPU des ressources CPU totales des hôtes et en divisant le résultat par les ressources CPU totales des hôtes. La Capacité mémoire de basculement actuelle est calculée de la même manière.

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.

Note 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.

Note 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.

Interopérabilité de vSphere HA

vSphere HA peut interagir avec de nombreuses autres fonctionnalités, comme DRS et Virtual SAN.

Avant de configurer vSphere HA, vous devez connaître les limitations de son interopérabilité avec ces autres fonctionnalités ou produits.

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 *VMware Virtual SAN*.

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.

Note 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 pour vSphere HA**.

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

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

Règles d'affinités de vSphere HA et DRS

Si vous créez une règle d'affinité DRS pour votre cluster, vous pouvez indiquer de quelle manière vSphere HA doit appliquer cette règle en cas de basculement d'une machine virtuelle.

Les deux types de règles pour lesquelles vous pouvez le comportement de vSphere HA en cas de basculement sont les suivants :

- Les règles d'anti-affinité de machine virtuelle contraignent les machines virtuelles spécifiées à rester séparées pendant les opérations de basculement.
- Les règles d'affinité machine virtuelle/hôte placent les machines virtuelles spécifiées sur un hôte particulier ou un membre d'un groupe d'hôtes défini pendant les opérations de basculement.

Lorsque vous modifiez une règle d'affinité DRS, cochez la ou les cases appliquant le comportement de basculement souhaité pour vSphere HA.

- **HA doit respecter les règles d'anti-affinité VM pendant le basculement** : si les machines virtuelles avec cette règle sont placées ensemble, le basculement est abandonné.
- **HA devrait respecter les règles d'anti-affinité VM pendant le basculement** : vSphere HA tente de placer les machines virtuelles soumises à cette règle sur les hôtes spécifiés le cas échéant.

Note vSphere HA peut redémarrer une machine virtuelle dans un cluster sur lequel DRS est désactivé, en remplaçant un mappage de règles d'affinité machine virtuelle/hôte si l'échec de l'hôte a lieu rapidement (par défaut en moins de 5 minutes) après avoir défini la règle.

Autres problèmes d'interopérabilité de vSphere HA

Pour utiliser vSphere HA, vous devez connaître les problèmes d'interopérabilité supplémentaires suivants.

VM Component Protection

VM Component Protection (VMCP) connaît les problèmes et limitations de l'interopérabilité suivants :

- VMCP ne prend pas en charge vSphere Fault Tolerance. Si VMCP est activé pour cluster utilisant Fault Tolerance, les machines virtuelles FT affectées recevront automatiquement des remplacements qui désactivent VMCP.
- VMCP ne détecte pas ni ne réagit aux problèmes d'accessibilité des fichiers situés sur les banques de données Virtual SAN. Si la configuration et les fichiers VMDK d'une machine virtuelle sont situés uniquement sur des banques de données Virtual SAN, ils ne sont pas protégés par VMCP.

- VMCP ne détecte pas ni ne réagit aux problèmes d'accessibilité des fichiers situés sur les banques de données de volume virtuel. Si la configuration et les fichiers VMDK d'une machine virtuelle sont situés uniquement sur des banques de données de volume virtuel, ils ne sont pas protégés par VMCP.
- VMCP ne protège pas contre le mappage de périphérique brut (Raw Device Mapping, RDM) inaccessible.

IPv6

vSphere HA peut être utilisé avec des configurations réseau IPv6, qui sont entièrement pris en charge si les considérations suivantes sont prises en compte :

- Le cluster contient uniquement des hôtes ESXi 6.0 ou version ultérieure.
- Le réseau de gestion de tous les hôtes dans le cluster doit être configuré avec la même version d'adresse IP, IPv6 ou IPv4. Les clusters vSphere HA ne peuvent pas contenir les deux types de configuration de la mise en réseau.
- Les adresses d'isolation réseau utilisées par vSphere HA doivent correspondre à la version de l'adresse IP utilisée par le cluster pour son réseau de gestion.
- IPv6 ne peut pas être utilisé dans les clusters vSphere HA qui utilisent également Virtual SAN.

En plus des restrictions précédentes, les types suivants d'adresses IPv6 ne sont pas pris en charge pour être utilisés avec l'adresse d'isolation ou le réseau de gestion vSphere HA : adresse de lien local, ORCHID et adresse de lien local avec indices de zone. De plus, le type d'adresse loopback ne peut pas être utilisé pour le réseau de gestion.

Note Pour mettre à jour le déploiement de l'IPv4 vers l'IPv6, vous devez d'abord désactiver vSphere HA.

Création et configuration d'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.

Note 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.

Liste de contrôle de vSphere HA

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

Consultez cette liste avant de configurer un cluster vSphere HA. Pour plus d'informations, suivez les références croisées appropriées.

- Tous les hôtes doivent disposer d'une licence pour vSphere HA.
- Un cluster doit contenir au moins deux hôtes.
- Tous les hôtes doivent être configurés avec des adresses IP statiques. Si vous utilisez DHCP, vérifiez que l'adresse de chaque hôte est conservée après les redémarrages.
- Tous les hôtes doivent avoir au moins un réseau de gestion en commun. Il est recommandé d'avoir au moins deux réseaux de gestion en commun. Vous devez utiliser le réseau VMkernel avec la case **Trafic de gestion** cochée. Les réseaux doivent être accessibles l'un à l'autre et vCenter Server et les hôtes doivent être accessibles les uns aux autres sur les réseaux de gestion. Reportez-vous à Meilleures pratiques pour la mise en réseau.
- Pour vous assurer que toutes les machines virtuelles peuvent s'exécuter sur n'importe quel hôte du cluster, tous les hôtes doivent avoir accès aux même réseaux et banques de données 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.

  Note vSphere HA utilise le signal de pulsation de banque de données pour différencier les hôtes partitionnés, isolés ou défaillants. Par conséquent, s'il y a 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 de VMware tools. Reportez-vous à Surveillance des VM et applications.
- vSphere HA prend en charge IPv4 et IPv6. Voir Autres problèmes d'interopérabilité de vSphere HA pour consulter les considérations à prendre en compte lors de l'utilisation d'IPv6.
- Pour que VM Component Protection fonctionne, la fonctionnalité de délai d'expiration Tous les chemins hors service (All Paths Down, APD) doit être activée.

- Pour utiliser VM Component Protection, les clusters doivent comporter des hôtes ESXi 6.0 hosts ou version ultérieure.
- Seuls les clusters vSphere HA contenant des hôtes ESXi 6.0 ou version ultérieure peuvent être utilisés pour activer VMCP. Les clusters contenant des hôtes d'une version antérieure ne peuvent pas activer VMCP et ne peuvent pas être ajoutés à un cluster sur lequel VMCP est activé.
- Si votre cluster utilise des banques de données de volume virtuel, lorsque vSphere HA est activé, un configuration de volume virtuel est créée sur chaque banque de données par vCenter Server. Dans ces conteneurs, vSphere HA stocke les fichiers qu'il utilise pour protéger les machines virtuelles. vSphere HA ne fonctionne pas correctement si vous supprimez ces conteneurs. Un seul conteneur est créé par banque de données de volume virtuel.

Créer un cluster vSphere HA

Pour activer votre cluster pour vSphere HA, vous devez d'abord 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.

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

Conditions préalables

- Vérifiez que toutes les machines virtuelles et leurs fichiers de configuration résident sur des stockages partagés.
- Vérifiez que les hôtes sont configurés pour accéder au 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.
- Vérifiez que vous utilisez des connexions réseau de gestion redondant pour vSphere HA. Pour plus d'informations sur la configuration d'un réseau redondant, consultez la rubriqueMeilleures pratiques pour la mise en réseau.
- Vérifiez que vous avez configuré les hôtes avec au moins deux banques de données afin de fournir de la redondance au signal de pulsation de la banque de données vSphere HA.
- Connecter vSphere Web Client au vCenter Server en utilisant un compte disposant des autorisations d'administrateur de cluster.

Procédure

1. Dans vSphere Web Client, accédez au centre de données où vous voulez que le cluster réside et cliquez sur **Créer un cluster**.
2. Complétez le paramètre de l'assistant **Nouveau cluster**.

   Ne pas mettre sous tension vSphere HA (ou DRS).
3. Cliquez sur **OK** pour fermer l'assistant et créer un cluster vide.

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

5 Accédez au cluster et activez vSphere HA.

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

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

   c Sélectionnez **Activer vSphere HA**.

6 Sélectionner **Surveillance de l'hôte**

   L'activation de la surveillance de l'hôte permet aux hôtes du cluster d'échanger des signaux de pulsation réseau et à vSphere HA d'agir lorsqu'il détecte des pannes. La surveillance d'hôte est aussi requise pour le bon fonctionnement du processus de récupération de vSphere Fault Tolerance.

7 Sélectionnez un paramètre pour la **Surveillance machines virtuelles**.

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

8 Cliquez sur **OK**.

Résultats

Vous disposez désormais d'un cluster vSphere HA rempli d'hôtes.

Étape suivante

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

- Conditions de défaillance et réponse VM
- Contrôle d'admission
- Banque de données dédiée à l'émission de signaux de pulsations
- Options avancées

Reportez-vous à Configuration des paramètres du cluster vSphere HA.

Configuration des paramètres du cluster vSphere HA

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 :

Conditions de défaillance et réponse VM

C'est ici que vous fournissez les paramètres concernant la priorité de redémarrage des machines virtuelles, la réaction à l'isolation des hôtes, la sensibilité de surveillance des machines virtuelles et les paramètres de VM Component Protection.

Contrôle d'admission

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

Banque de données dédiée à l'émission de signaux de pulsations

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.

Note Vous pouvez vérifier l'état des tâches de configuration de vSphere HA sur chacun des hôtes dans la console Tâches de vSphere Web Client.

Configurer les réactions des machines virtuelles

La page Conditions de défaillance et réponse VM vous permet de sélectionner des paramètres qui déterminent de quelle manière vSphere HA réagit aux échecs et isolements d'hôte. Ces paramètres incluent la priorité de redémarrage des machines virtuelles, la réaction à l'isolation des hôtes, les paramètres de VM Component Protection et la sensibilité de surveillance des machines virtuelles.

La page Réaction des machines virtuelles est uniquement modifiable 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 **Conditions de défaillance et réponse VM** pour afficher les options de configuration.

Option	Description
Priorité de redémarrage des VM	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.
Réponse à l'isolation d'hôte :	La réaction à l'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.
Réponse en cas de banque de données avec perte permanente de périphérique (PDL)	Ce paramètres détermine la réaction de VMCP en cas de perte permanente de périphérique (PDL). Vous pouvez choisir l'**Émission d'événements** ou de **Mettre hors tension et redémarrer les VM**.
Réponse en cas de banque de données avec tous les chemins hors service (APD)	Ce paramètres détermine la réaction de VMCP en cas de panne de tous les chemins d'accès (APD). Vous pouvez choisir l'**Émission d'événements** ou de **Mettre hors tension et redémarrer les VM** avec précaution ou de manière intensive.
Délai de basculement de VM en cas d'APD	Ce paramètre correspond au nombre de minutes pendant lequel VMCP attend avant d'agir.
Réponse en cas de récupération APD après un délai d'expiration APD	Vous pouvez décider si VMCP doit réinitialiser une machine virtuelle ou non dans cette situation.
Sensibilité de surveillance VM	Vous pouvez définir cette fonctionnalité en déplaçant le curseur de **Basse** à **Élevée**. Vous pouvez également sélectionner **Personnalisé** pour fournir des paramètres personnalisés.

5 Cliquez sur **OK**.

Résultats

Les paramètres de réaction de votre machine virtuelle entrent en vigueur.

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**.

Résultats

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

Configurer la banque de données dédiée à l'émission de signaux de pulsations

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 **Banques de données pour le signal de pulsation** 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**.

Définir les options avancées

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

Conditions préalables

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

Note Ces options affectent le fonctionnement de vSphere HA. Modifiez-les donc avec prudence.

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**.

Résultats

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

Étape suivante

Après avoir défini une option avancée vSphere HA, elle est conservée jusqu'à ce que vous procédiez à ce qui suit :

- À l'aide de vSphere Web Client, réinitialisez sa valeur à la valeur par défaut.
- Modifiez ou supprimez manuellement l'option depuis le fichier fdm.cfg sur tous les hôtes du cluster.

Options avancées de vSphere HA

Vous pouvez définir des options avancées qui affectent le comportement du cluster vSphere HA.

Tableau 2-4. Options avancées de vSphere HA

Option	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'isolation (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. Cette option 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.

Tableau 2-4. Options avancées de vSphere HA (suite)

Option	Description
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. **Note** Les valeurs inférieures à 50 ne sont pas recommandées, car elles peuvent entraîner la réinitialisation d'une machine virtuelle par vSphere HA de façon inattendue.
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.
das.config.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*.

Tableau 2-4. Options avancées de vSphere HA (suite)

Option	Description
das.maxresets	Nombre maximal de tentatives de réinitialisation par VMCP. En cas d'échec d'une opération de réinitialisation sur une machine virtuelle affectée par une situation d'APD, VMCP réessaie la réinitialisation plusieurs fois avant d'abandonner.
das.maxterminates	Nombre maximal de tentatives d'arrêt d'une machine virtuelle effectuées par VMCP.
das.terminateretryintervalsec	En cas d'échec de VMCP à arrêter une machine virtuelle, cette option correspond au nombre de secondes pendant lequel le système attend avant de refaire une tentative d'arrêt.
das.config.fdm.reportfailoverfailevent	Quand cette option est définie sur 1, elle permet de générer un événement par machine virtuelle lorsque vSphere HA échoue dans une tentative de redémarrage d'une machine virtuelle. La valeur par défaut est 0. Dans les versions antérieures à vSphere 6.0, cet événement est généré par défaut.
vpxd.das.completemetadataupdateintervalsec	Période (en secondes) après qu'une règle d'affinité machine virtuelle/hôte est définie pendant laquelle vSphere HA peut redémarrer une machine virtuelle dans un cluster sur lequel DRS est désactivé, remplaçant ainsi la règle. La valeur par défaut est de 300 secondes.

Tableau 2-4. Options avancées de vSphere HA (suite)

Option	Description
das.config.fdm.memReservationMB	Par défaut, les agents vSphere HA s'exécutent avec une limite de mémoire configurée de 250 Mo. Un hôte pourrait ne pas autoriser cette réservation si sa capacité réservable est épuisée. Vous pouvez utiliser cette option pour réduire la limite de mémoire et éviter ainsi ce problème. Seuls des nombres entiers supérieurs à 100, qui est la valeur minimale, peuvent être spécifiés. À l'inverse, pour prévenir tout problème lors des élections d'agents principaux dans un cluster volumineux (contenant 6 000 à 8 000 machines virtuelles), cette limite doit être portée à 325 Mo. **Note** Une fois cette limite modifiée, vous devez exécuter une tâche Reconfigurer HA pour tous les hôtes dans le cluster. En outre, lorsqu'un nouvel hôte est ajouté au cluster ou qu'un hôte existant est redémarré, cette tâche doit être exécutée sur ces hôtes afin de mettre à jour ce paramètre de mémoire.
das.respectvmhostsoftaffinityrules	Détermine si vSphere HA redémarre une machine virtuelle correspondante sur un hôte qui appartient au même groupe de VM/hôte. Si aucun hôte n'est disponible ou si la valeur de cette option est définie sur « false », vSphere HA redémarre la machine virtuelle sur n'importe quel hôte disponible dans le cluster. Dans vSphere 6.0, la valeur par défaut est « false ». Cette valeur ne peut pas être visiblement définie dans les options HA avancées du cluster. Si vous souhaitez activer l'option, vous devez manuellement définir cette option en tant que « true » dans les options avancées HA pour le cluster.

Note Si vous modifiez la valeur de l'une des options avancées suivantes, vous devez désactiver, puis réactiver vSphere HA avant que les modifications ne s'appliquent.

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

Personnaliser une machine virtuelle secondaire

Les paramètres par défaut du cluster relatifs à la priorité de redémarrage, à la réponse d'isolation de l'hôte, à la protection des composants des machines virtuelles 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**, VMCP, **Surveillance VM**, ou **Sensibilité de surveillance VM**.

Note 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**.

Résultats

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 recommandations essentielles concernant un cluster vSphere HA.

Vous pouvez également consulter la publication *Meilleures pratiques du déploiement vSphere High Availability* pour poursuivre la discussion.

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.

Note 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. Pour contenir le trafic vSphere HA en un sous-ensemble de réseaux de la console ESX, utilisez l'option avancée `allowedNetworks`.
- Sur les hôtes ESXi du cluster, les communications vSphere HA, par défaut, sont acheminées via les réseaux VMkernel. Avec un hôte ESXi, si vous souhaitez utiliser un réseau autre que celui employé par vCenter Server pour communiquer avec l'hôte pour vSphere HA, vous devez cocher explicitement la case **Trafic de gestion**.

Pour maintenir le trafic de l'agent vSphere HA sur les réseaux que vous avez spécifiés, configurez les hôtes de façon à ce que les cartes vmkNIC utilisées par vSphere HA 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 si au moins une carte vmkNIC est 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'option avancée `das.isolationaddress[...]` pour ajouter des adresses d'isolation à des réseaux supplémentaires. Reportez-vous à la section Options avancées de vSphere HA.

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 d'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 vous est d'abord possible d'implémenter la redondance du réseau au niveau de l'association de cartes 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 d'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.

Dans la plupart des implémentations, l'association de cartes réseau offre une redondance suffisante, mais il vous est également possible de créer une connexion de réseau de gestion secondaire qui est liée à un commutateur virtuel distinct. 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. 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.

Note 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.

Utilisation des configurations réseau IPv6

Une seule adresse IPv6 doit être attribuée à une interface réseau donnée utilisée par votre cluster vSphere HA. L'attribution de plusieurs adresses IP augmente le nombre de messages de signal de pulsation envoyés par l'hôte principal du cluster sans l'avantage correspondant.

Recommandations concernant l'interopérabilité

Suivez les recommandations suivantes pour permettre une interopérabilité adéquate entre vSphere HA et d'autres fonctionnalités.

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.

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.

Recommandations concernant le contrôle d'admission

Suivez les recommandations suivantes lors de la configuration et de l'utilisation du contrôle d'admission vSphere HA.

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.

Recommandations concernant la surveillance d'un cluster

Suivez les recommandations suivantes lors de la surveillance de l'état et de la validité de votre cluster vSphere HA.

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)

Note 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.

Assurer Fault Tolerance des machines virtuelles

3

Il est possible d'utiliser vSphere Fault Tolerance pour vos 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 basée sur la plate-forme hôte ESXi et elle fournit une disponibilité continue en exécutant des machines virtuelles identiques 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.

Protection Fault Tolerance pour machines virtuelles (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_7ivj3twt/uiConfId/49694343/)

Ce chapitre contient les rubriques suivantes :

Fonctionnement de Fault Tolerance

Il est possible d'utiliser vSphere Fault Tolerance (FT) sur la plupart des machines virtuelles cruciales pour une mission. FT assure la disponibilité continue d'une machine virtuelle de ce type en créant et en maintenant une autre machine virtuelle identique et disponible en permanence pour la remplacer en cas de situation de basculement.

La machine virtuelle protégée s'appelle la machine virtuelle principale. La copie de la machine virtuelle, la machine virtuelle secondaire, est créée et s'exécute sur un autre hôte. L'exécution de la machine virtuelle secondaire est identique à celle de la machine virtuelle principale et elle peut reprendre l'exécution à tout moment sans interruption, assurant ainsi une protection tolérante aux pannes.

Les machines virtuelles principale et secondaire surveillent continuellement l'état l'une de l'autre pour vérifier que la tolérance aux pannes est maintenue. 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'un échec de l'hôte ne peut pas entraîner la perte des deux machines virtuelles.

Note 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.

vSphere Fault Tolerance peut gérer les machines virtuelles à multiprocesseur symétrique (SMP) avec jusqu'à quatre vCPU. Les versions antérieures de vSphere utilisaient une technologie différente pour Fault Tolerance (connue sous le nom de FT héritée), avec différentes conditions requises et caractéristiques (notamment une limitation des vCPU uniques pour les machines virtuelles FT héritée). Si la compatibilité avec ces conditions antérieures est nécessaire, vous pouvez utiliser FT héritée à la place. Toutefois, cela implique la configuration d'une option avancée pour chaque machine virtuelle. Consultez Fault Tolerance héritée pour plus d'informations.

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.

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 d'interrompre 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.

Configuration requise, limites et licence de Fault Tolerance

Avant d'utiliser vSphere Fault Tolerance (FT), tenez compte des conditions requises de niveau supérieur, des limites et de l'attribution de licence qui s'appliquent à cette fonctionnalité.

Exigences

Les conditions de CPU et de mise en réseau requises suivantes s'appliquent à FT.

Les CPU qui sont utilisés sur les machines hôtes pour les machines virtuelles Fault Tolerance doivent être compatibles avec vSphere vMotion ou être améliorées par Enhanced vMotion Compatibility. De plus, les CPU qui prennent en charge la virtualisation du matériel MMU (Intel EPT ou AMD RVI) sont requis. Les CPU suivants sont pris en charge.

- Intel Sandy Bridge ou version ultérieure. Avoton n'est pas pris en charge.
- AMD Bulldozer ou version ultérieure.

Utilisez un réseau de journalisation de 10 Gbits pour FT et vérifiez que la latence du réseau est faible. Un réseau FT dédié est fortement recommandé.

Limites

Dans un cluster configuré pour utiliser Fault Tolerance, deux limites sont appliquées de manière distincte.

das.maxftvmsperhost

Le nombre maximal de machine virtuelles Fault Tolerance autorisées sur un hôte dans le cluster. Les machines virtuelles principale et secondaires sont prises compte vis-à-vis de cette limite. La valeur par défaut est 4.

das.maxftvcpusperhost

Le nombre maximal de vCPU regroupés dans toutes les machines virtuelles Fault Tolerance sur un hôte. Les vCPU des machines virtuelles principale et secondaires sont pris en compte vis-à-vis de cette limite. La valeur par défaut est 8.

Attribution de licences

Le nombre de vCPU pris en charge par une machine virtuelle unique est limité par le niveau d'attribution de licence acheté pour vSphere. Fault Tolerance est prise en charge comme suit :

- vSphere Standard et Enterprise. Autorise jusqu'à 2 vCPU
- vSphere Enterprise Plus. Autorise jusqu'à 4 vCPU

Note FT et FT héritée ne sont pas prises en charge dans vSphere Essentials et vSphere Essentials Plus.

Interopérabilité de Fault Tolerance

vSphere Fault Tolerance est soumise à certaines limitations concernant les fonctionnalités de vSphere, les périphériques et les autres fonctionnalités avec lesquelles elle peut interagir.

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

Lors de la configuration de votre cluster, vous devez savoir que toutes les fonctionnalités de vSphere ne peuvent pas interagir avec 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.

  Note Les snapshots sur disque uniquement créés pour des sauvegardes de vStorage APIs - Data Protection (VADP) sont pris en charge avec l'option Fault Tolerance. Cependant, la protection FT héritée ne prend pas en charge VADP.

- 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 ni possible d'utiliser Fault Tolerance sur une machine virtuelle qui est un clone lié, ni de créer un clone lié à partir d'une machine virtuelle sur laquelle Fault Tolerance est activée.
- VM Component Protection (VMCP). Si VMCP est activé sur votre cluster, des remplacements sont créés pour les machines virtuelles Fault Tolerance qui désactivent cette fonctionnalité.
- Banques de données à volume virtuel.
- Gestion de stratégie basée sur le stockage.
- Filtres d'E/S.

Fonctions et périphériques incompatibles avec Fault Tolerance

Tous les périphériques, fonctionnalités ou produits tiers ne peuvent pas interagir 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
Mappage disque brut physique (RDM).	Avec la fonctionnalité FT, vous pouvez reconfigurer les machines virtuelles avec des périphériques virtuels pris en charge par des RDM physiques de sorte 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.
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

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

Fonction ou périphérique incompatible	Action corrective
relais de adaptateurs réseau	Cette fonction n'est pas prise en charge par Fault Tolerance et doit donc être désactivée.
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. **Note** 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.
Ports série ou parallèles	Déconnectez ces périphériques de la machine virtuelle.
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.
VMCI (Virtual machine communication interface)	Non prise en charge par Fault Tolerance.
Disque de machine virtuelle de plus de 2 To	Fault Tolerance n'est pas prise en charge sur les disques de machine virtuelle de plus de 2 To.

Utiliser Fault Tolerance avec DRS

Vous pouvez utiliser vSphere Fault Tolerance avec vSphere Distributed Resource Scheduler (DRS) quand la fonctionnalité EVC (Enhanced vMotion Compatibility) est activée. Ce processus permet aux machines Fault Tolerant de bénéficier d'un meilleur placement initial.

Quand la fonctionnalité EVC est activée pour un cluster, DRS émet les recommandations de placement initial pour les machines virtuelles Fault Tolerant et vous permet d'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).

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 et sa machine virtuelle secondaire est placée automatiquement.

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).

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 :

- Vérifiez que vos cluster, vos hôtes et vos machines virtuelles satisfont les conditions requises par la liste de contrôle de Fault Tolerance.
- 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 Activer Fault Tolerance.

Liste de contrôle 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.

Note 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.

- Journalisation de Fault Tolerance et réseau vMotion configuré. Reportez-vous à Configurer la mise en réseau des machines hôtes.
- Cluster vSphere HA créé et activé. Reportez-vous à la section Création et configuration d'un cluster vSphere HA. 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 utiliser des 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 ensembles compatibles Fault Tolerance** pour déterminer si vos hôtes sont certifiés.
- La configuration de chaque hôte implique l'activation de la virtualisation matérielle (HV) dans le BIOS.

Note VMware recommande que les paramètres de gestion de l'alimentation BIOS des hôtes que vous utilisez pour prendre en charge les machines virtuelles Fault Tolerant soient définis sur « Performances maximales » ou « Performances gérées par le système d'exploitation ».

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.

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 Interopérabilité de Fault Tolerance.
- Les fonctions incompatibles ne doivent pas être exécutées avec les machines virtuelles tolérantes aux pannes. Reportez-vous à Interopérabilité de Fault Tolerance.
- 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.

Autres recommandations de configuration

Vous devez respecter les directives suivantes lors de la configuration de Fault Tolerance.

- 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.
- La réservation de mémoire d'une machine virtuelle Fault Tolerant est définie par la taille de la mémoire de la machine virtuelle lorsque Fault Tolerance est activée. Veillez à ce qu'un

pool de ressources contenant des machines virtuelles Fault Tolerance dispose de réserves de mémoire dépassant la capacité de mémoire des machines virtuelles. 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.

Configurer la mise en réseau des machines hôtes

Vous devez configurer deux commutateurs de mise en réseau distincts (vMotion et journalisation de FT) sur chacun des hôtes que vous souhaitez ajouter à un cluster vSphere HA, de sorte que l'hôte puisse prendre en charge vSphere Fault Tolerance.

Pour activer Fault Tolerance sur un hôte, vous devez exécuter cette procédure pour chaque option de groupe de ports (vMotion et journalisation de FT) 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.

Conditions préalables

Des adaptateurs réseau (NIC) de plusieurs giga-octets sont nécessaires. Pour chaque hôte compatible avec Fault Tolerance, il faut au minimum deux cartes réseau physiques. 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.

Note Les cartes réseau de journalisation vMotion et de tolérance aux pannes doivent être sur des sous-réseaux différents. Si vous utilisez la fonctionnalité FT héritée, IPv6 n'est pas pris en charge sur la carte réseau de journalisation de FT.

Procédure

1. Dans vSphere Web Client, accédez à l'hôte
2. Cliquez sur l'onglet **Gérer**, puis cliquez sur **Mise en réseau**.
3. Cliquez sur l'icône **Ajouter mise en réseau d'hôte**.
4. Sélectionnez **Adaptateur de réseau VMkernel** sur la page Sélectionner un type de connexion et cliquez sur **Suivant.**
5. Sélectionnez **Nouveau commutateur standard** puis cliquez sur **Suivant**.
6. Attribuer des adaptateurs réseau 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.

Résultats

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.

Étape suivante

Note Si vous configurez la mise en réseau pour la prise en charge de FT mais que par la suite vous interrompez le port de journalisation de Fault Tolerance, les paires de machines virtuelles Fault Tolerance qui sont déjà sous tension le resteront. 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.

Créer un cluster et vérifier la conformité

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.

Résultats

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

Utilisation de la tolérance aux pannes

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.

Avant de pouvoir activer Fault Tolerance, plusieurs vérifications de validation sont exécutés sur une machine virtuelle.

Après le passage de ces vérifications et après avoir activé vSphere Fault Tolerance pour une machine virtuelle, de nouvelles options sont ajoutées à la section Fault Tolerance de son menu contextuel. Elles comprennent notamment la mise hors tension ou la désactivation de Fault Tolerance, la migration de la machine virtuelle secondaire, le test du basculement et le test du redémarrage de la machine virtuelle secondaire.

Contrôles de validation pour l'activation de Fault Tolerance

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.

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 doit disposer de ESXi 6.x ou version ultérieure (ESX/ESXi 4.x ou version ultérieure pour FT héritée).
- 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.

Vérifications des machines virtuelles activées

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.
- 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 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.).

Placement de la machine virtuelle secondaire

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 tolérance aux pannes 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 tolérance aux pannes 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.

  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 tolérance aux pannes de la machine virtuelle est marqué comme **Protégée**.

Activer Fault Tolerance

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, le nombre de vCPU ou les partages. Il est également impossible d'ajouter ou de supprimer des disques pour la machine virtuelle. 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.

Conditions préalables

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.

Procédure

1. Dans vSphere Web Client, accédez à la VM pour laquelle vous souhaitez activer Fault Tolerance
2. Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Fault Tolerance > Activer Fault Tolerance**.
3. Cliquez sur **Oui**.
4. Choisissez une banque de données sur laquelle placer les fichiers de configuration de la machine virtuelle secondaire. Puis cliquez sur **Suivant**.
5. Choisissez un hôte sur lequel placer la machine virtuelle secondaire. Puis cliquez sur **Suivant**.
6. Passez vos sélections en revue et cliquez sur **Terminer**.

Résultats

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.

Désactiver la Fault Tolerance

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

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

Note 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 tolérance aux pannes**. Dans ce cas, interrompez, puis reprenez Fault Tolerance.

Procédure

1. Dans vSphere Web Client, accédez à la VM pour laquelle vous souhaitez arrêter la tolérance aux pannes.
2. Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Fault Tolerance > Désactiver la Fault Tolerance**.
3. Cliquez sur **Oui**.

Résultats

La tolérance aux pannes est arrêtée pour la machine virtuelle sélectionnée. L'historique, ainsi que la VM secondaire de la VM sélectionnée sont supprimés.

Interrompre Fault Tolerance

L'interruption de vSphere Fault Tolerance pour une machine virtuelle interrompt sa protection Fault Tolerance, mais conserve la machine virtuelle secondaire, sa configuration et l'ensemble de l'historique. Utilisez cette option pour reprendre la protection de Fault Tolerance à l'avenir.

Procédure

1. Dans vSphere Web Client, accédez à la machine virtuelle pour laquelle vous souhaitez interrompre Fault Tolerance.
2. Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Fault Tolerance > Interrompre Fault Tolerance**.
3. Cliquez sur **Oui**.

Résultats

Fault Tolerance est interrompue pour la machine virtuelle sélectionnée. L'historique et la machine virtuelle secondaire de la machine virtuelle sélectionnée sont préservés et seront utilisés si la fonctionnalité est reprise.

Étape suivante

Pour reprendre la fonctionnalité après avoir interrompu Fault Tolerance, sélectionnez **Relancer Fault Tolerance**.

Migration secondaire

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 avec le bouton droit sur la machine virtuelle et sélectionnez **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.

Résultats

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

Tester le basculement

Vous pouvez provoquer une situation de basculement pour une VM principale sélectionnée afin de tester la protection de tolérance aux pannes.

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 sélectionnez **Fault Tolerance > Tester le basculement**.
3. Consultez les détails sur le basculement dans la console de travail.

Résultats

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 secondaire

Vous pouvez provoquer la défaillance d'une VM secondaire afin de tester la protection Tolérance aux pannes 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 sélectionnez **Fault Tolerance > Tester le redémarrage secondaire**.
3. Consultez les détails du test dans la Console des tâches

Résultats

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

Mettre à niveau les hôtes utilisés pour Fault Tolerance

Procédez comme suit pour mettre à niveau les hôtes utilisés pour Fault Tolerance.

Conditions préalables

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.

Note 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. Interrompez Fault Tolerance sur la machine virtuelle principale.
4. Avec vMotion, déplacez la machine virtuelle principale pour laquelle Fault Tolerance a été interrompue vers l'un des hôtes mis à niveau.
5. Reprenez 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.

Résultats

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

Pratiques d'excellence pour Fault Tolerance

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

Les recommandations suivantes concernant la configuration de l'hôte et de la mise en réseau peut améliorer la stabilité et les performances de votre cluster.

Configuration d'hôte

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.

Configuration de la 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 d'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 d'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.

Note 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.

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 :

- Accès commun aux banques de données utilisées par les machines virtuelles.
- La même configuration réseau de machines virtuelles.
- 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 un correctif.

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 . 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) peut 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 trouve dans une partition gérée par un hôte principal qui en est 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.

Utilisation de banques de données Virtual SAN

vSphere Fault Tolerance peut utiliser des banques de données Virtual SAN, mais vous devez observer les restrictions suivantes :

- Un mélange de Virtual SAN et d'autres types de banques de données n'est pas pris en charge pour les VM principales et les VM secondaires.
- Les metro-clusters Virtual SAN ne sont pas pris en charge avec FT.

Pour augmenter les performances et la fiabilité lors de l'utilisation de FT avec Virtual SAN, les conditions suivantes sont également recommandées.

- Virtual SAN et FT doivent utiliser des réseaux distincts.
- Maintenez les VM principales et secondaires dans des domaines de pannes Virtual SAN distincts.

Fault Tolerance héritée

Par défaut, vSphere Fault Tolerance (FT) peut gérer les machines virtuelles à multiprocesseur symétrique (SMP) avec jusqu'à quatre vCPU. Si votre machine virtuelle dispose d'un vCPU unique, il vous est toutefois possible d'utiliser la fonctionnalité FT héritée à la place de la compatibilité descendante. À moins que ce soit nécessaire d'un point de vue technique, utiliser la FT héritée n'est pas recommandé.

Pour utiliser la fonctionnalité Fault Tolerance héritée, vous devez configurer une option avancée pour la machine virtuelle. Une fois cette configuration terminée, la machine virtuelle avec FT héritée est quelque peu différente des autres machines virtuelles Fault Tolerant.

Différences des machines virtuelles avec FT héritée

Les machines virtuelles avec FT et celles avec FT héritée diffèrent de plusieurs manières.

Tableau 3-2. Différences entre FT héritée et FT

	FT héritée	FT
Extended Page Tables/Rapid Virtualization Indexing (EPT/RVI).	Non pris en charge	Requis
IPv6	Non pris en charge pour les cartes réseau de journalisation avec FT héritée.	Pris en charge pour les cartes réseau de journalisation avec FT.
DRS	Pris entièrement en charge pour le placement initial, l'équilibrage de charge et la prise en charge du mode de maintenance.	Prise en charge uniquement de la mise sous tension lors du placement de la machine virtuelle secondaire et du mode de maintenance.
API vStorage - sauvegarde de la protection des données	Non pris en charge	Pris en charge
Fichiers des disques .vmdk au format Thick eager-zeroed	Requis	Non requis, car FT prend en charge tous les types de disques, notamment les disques dynamiques et statiques
Redondance des fichiers .vmdk	Seulement une copie unique	Les machines virtuelles principales et les machines virtuelles secondaires conservent toujours des copies distinctes qui peuvent être placées dans des différentes banques de données afin d'augmenter la redondance.
Bande passante de la carte réseau	Carte réseau dédiée de 1 Go recommandée	Carte réseau dédiée de 10 Go recommandée
Compatibilité du CPU et de l'hôte	Nécessite un modèle et une famille de CPU identiques et des versions presque identiques de vSphere sur les hôtes.	Les CPU doivent être compatibles avec vSphere vMotion ou EVC. Les versions de vSphere sur les hôtes doivent être compatibles avec vSphere vMotion.

Tableau 3-2. Différences entre FT héritée et FT (suite)

	FT héritée	FT
Activer FT sur les machines virtuelles en cours d'exécution	Pas toujours pris en charge. Il se peut que vous deviez d'abord mettre hors tension la machine virtuelle.	Pris en charge
Storage vMotion	Pris en charge uniquement sur les machines virtuelles hors tension. vCenter Server met automatiquement FT hors tension avant d'exécuter une action de Storage vMotion, puis remet FT sous tension une fois l'action de Storage vMotion terminée.	Non pris en charge. L'utilisateur doit mettre FT hors tension sur la machine virtuelle avant d'exécuter l'action de Storage vMotion, puis remettre FT sous tension.
Pilotes de mise en réseau vlance	Non pris en charge	Pris en charge

Conditions requises supplémentaires pour la fonctionnalité FT héritée

Outre les différences répertoriées concernant la fonctionnalité FT héritée, celle-ci est soumise aux conditions uniques suivantes.

- Votre cluster doit contenir au moins deux hôtes certifiés FT exécutant la même version de Fault Tolerance ou utilisant le même numéro de build d'hôte. Le numéro de version de Fault Tolerance apparaît dans l'onglet **Résumé** d'un hôte dans vSphere Web Client.
- Les hôtes ESXi doivent avoir accès aux mêmes banques de données et réseaux des machines virtuelles.
- 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 stockée dans un fichier VMDK qui est provisionné dynamiquement et que vous tentez d'utiliser 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.
- Les hôtes doivent avoir des processeurs appartenant au groupe de processeurs compatibles avec FT. Vérifiez que les processeurs des hôtes sont compatibles les uns avec les autres.
- 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.
- Lorsque vous mettez à niveau des hôtes qui contiennent des machines virtuelles Fault Tolerant, vérifiez que les machines virtuelles principales et secondaires continuent de s'exécuter sur des hôtes ayant le même numéro de version FT ou de build d'hôte (pour les hôtes antérieurs à ESX/ESXi 4.1).

  Note Si vous avez désigné une machine virtuelle devant utiliser FT avant de mettre à niveau les hôtes dans le cluster, celle-ci continuera d'utiliser la fonctionnalité FT héritée après la mise à niveau de l'hôte.

Activer la fonctionnalité Fault Tolerance héritée

Pour utiliser la fonctionnalité Fault Tolerance héritée, vous devez configurer une option avancée pour la machine virtuelle.

La fonctionnalité FT héritée peut être utilisée uniquement avec des machines virtuelles à vCPU unique qui n'utilisent pas encore FT. Pour activer la fonctionnalité FT héritée pour chaque machine virtuelle qui devra l'utiliser, vous devez définir l'option avancée `vm.uselegacyft` sur une valeur de **true**.

Procédure

1. Dans vSphere Web Client, accédez à la machine virtuelle.
2. Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
3. Cliquez sur l'onglet **Options VM**.
4. Ouvrez la section **Avancésé** et, en regard de **Paramètres de configuration**, cliquez sur **Modifier la configuration**.
5. Cliquez sur **Ajouter ligne** et entrez `vm.uselegacyft` pour Nom et **true** pour Valeur.
6. Cliquez sur **OK**.

Résultats

La fonctionnalité FT héritée est à présent activée pour cette machine virtuelle.