Disponibilité vSphere

Update 1

VMware vSphere 8.0
VMware ESXi 8.0
vCenter Server 8.0

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 vSphere

Le document *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.

VMware prend l'intégration au sérieux. Pour promouvoir ce principe au sein de notre communauté de clients, de partenaires et interne, nous créons du contenu à l'aide d'une langue inclusive.

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 document 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.

Continuité d'activité et minimisation des interruptions de service

1

Qu'elles soient prévues ou non, 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, vous pouvez augmenter 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 haute disponibilité indépendamment du matériel, du système d'exploitation et des applications.
- Réduire les interruptions de service prévues pour les opérations de maintenance courantes.
- 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 vSAN. 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.

Protection de vCenter Server avec vCenter High Availability

vCenter High Availability (vCenter HA) protège non seulement contre les défaillances matérielles et de l'hôte mais également contre les défaillances de l'application vCenter Server. Grâce au basculement automatisé entre actif et passif, vCenter HA prend en charge la haute disponibilité avec un temps d'arrêt minimal.

Vous configurez vCenter HA à partir de vSphere Client. L'assistant de configuration offre les options suivantes.

Option	Description
Automatique	L'option automatique clone le nœud actif en nœud passif et en nœud témoin, et configure le nœud pour vous. Si votre environnement répond aux exigences suivantes, vous pouvez utiliser cette option. ■ L'instance de vCenter Server qui devient le nœud actif gère son propre hôte ESXi et sa propre machine virtuelle. Cette configuration de vCenter Server est parfois appelée gestion automatique.
Manuel	L'option Manuel offre davantage de souplesse. Vous pouvez utiliser cette option tant que votre environnement satisfait les configurations matérielles et logicielles requises. Si vous sélectionnez cette option, vous devez cloner le nœud actif sur le nœud passif et sur le nœud témoin. Vous devez également effectuer une configuration de mise en réseau.

Protection de vCenter Server avec VMware Service Lifecycle Manager

La disponibilité de vCenter Server est fournie par VMware Service Lifecycle Manager.

Si le service vCenter échoue, VMware Service Lifecycle Manager le redémarre. VMware Service Lifecycle Manager surveille la santé des services et exécute une action corrective préconfigurée en cas de détection de panne. Le service ne redémarre pas en cas de plusieurs tentatives de correction de panne.

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)

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

L'hôte principal d'un cluster a plusieurs responsabilités :

- Surveiller l'état des hôtes secondaires. Si un hôte secondaire est défaillant ou devient inaccessible, l'hôte principal identifie les machines virtuelles qui doivent être redémarrées.
- Surveiller l'état d'alimentation de toutes les machines virtuelles protégées. Si une machine virtuelle est défaillante, l'hôte principal assure son redémarrage. Grâce à un moteur de placement local, l'hôte principal détermine également l'endroit où le redémarrage a 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, les machines virtuelles enregistrées sur cet hôte ne sont pas protégées par vSphere HA.

Types de pannes d'hôte

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

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

- Panne : un hôte cesse de fonctionner.
- Isolation : un hôte se retrouve isolé sur le réseau.
- Partition. Un hôte perd sa 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 défaillant. Le contrôle de réactivité effectué par l'hôte principal permet de déterminer si l'hôte secondaire échange des signaux de pulsation avec une des banques de données. Reportez-vous à la section Signal de pulsation de banque de données . Par ailleurs, l'hôte principal vérifie si l'hôte répond aux pings ICMP envoyés à ses adresses IP de gestion.

Si un hôte principal ne peut pas communiquer directement avec l'agent sur un hôte secondaire, celui-ci ne répond pas aux commandes ping ICMP. Si l'agent n'émet pas de pulsations, il est considéré comme défaillant. Les machines virtuelles des hôtes sont redémarrées sur d'autres hôtes. Si cet hôte secondaire échange des signaux de pulsation avec une banque de données, l'hôte principal suppose que l'hôte secondaire se trouve dans une partition du réseau ou est isolé du réseau. L'hôte principal continue donc à 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 cette commande ping échoue également, l'hôte déclare qu'il est isolé du réseau.

L'hôte principal surveille les machines virtuelles qui s'exécutent sur un hôte isolé. Si l'hôte principal remarque que les machines virtuelles se mettent hors tension et qu'il en est responsable, il les redémarre.

Note Si vous vous assurez que l'infrastructure réseau est suffisamment redondante et qu'au moins un chemin d'accès au réseau est toujours disponible, l'isolation du réseau de l'hôte est moins susceptible de se produire.

Pannes de Proactive HA

Une panne de Proactive HA se produit lorsqu'un composant hôte est défaillant, ce qui entraîne une perte de redondance ou une panne non grave. Cependant, le comportement de fonctionnement des machines virtuelles qui résident sur l'hôte n'est pas affecté. Par exemple, si une alimentation électrique sur l'hôte tombe en panne, mais que les autres alimentations sont disponibles, il s'agit d'une panne de Proactive HA.

En cas de panne de Proactive HA, vous pouvez automatiser la mesure corrective prise dans la section Disponibilité vSphere de vSphere Client. Les machines virtuelles sur l'hôte concerné peuvent être évacuées vers d'autres hôtes et l'hôte est mis en mode de quarantaine ou de maintenance.

Note Pour que la surveillance des pannes de Proactive HA fonctionne, votre cluster doit utiliser vSphere DRS.

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 .

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 réponse d'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. L'état de surveillance de l'hôte est désactivé. Les réponses d'isolation d'hôte sont également interrompues. 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.

Dépendances des machines virtuelles

Vous pouvez créer des dépendances entre les groupes de machines virtuelles. Pour cela, vous devez d'abord créer les groupes de VM dans vSphere Client en accédant à l'onglet **Configurer** du cluster et en sélectionnant **Groupes de VM/Hôte**. Une fois les groupes créés, vous pouvez créer des règles de redémarrage des dépendances entre les groupes en accédant à l'onglet **Règles de VM/Hôte** et en sélectionnant dans le menu déroulant **Machines virtuelles vers machines virtuelles**. Ces règles peuvent spécifier que certains groupes de VM ne peuvent pas être redémarrés tant que d'autres groupes spécifiés n'ont pas été démarrés en premier.

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.

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 invité 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.

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 d'échec	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.

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 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 d'hôte ou Priorité de redémarrage des 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 fonctions 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 VMware vSphere® High Availability ne peut pas communiquer avec un hôte secondaire sur le réseau de gestion, l'hôte principal utilise le signal de pulsation de banque de données pour déterminer si l'hôte secondaire est défaillant, s'il se trouve dans une partition de réseau ou 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.

VMware 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 2 Go et l'utilisation type est 3 Mo. Avec vmfs5, l'utilisation maximale et classique est 3 Mo. L'utilisation des banques de données par vSphere HA n'entraîne qu'un dépassement de mémoire négligeable et n'a aucun impact sur les performances des autres opérations des banques 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 les machines virtuelles que jusqu'à cette limite.

Note Une banque de données de vSAN 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 accessible par un autre chemin réseau indépendant de vSAN, 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, 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 ESXi, vSphere HA écrit dans `/var/log/vmware/fdm` sur le disque local, ainsi que syslog si il est configuré.

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 du système vCenter Server est désactivée à ce moment-là, vérifiez le nouveau certificat et reconfigurez vSphere HA sur l'hôte.

Contrôle d'admission vSphere HA

vSphere HA utilise le contrôle d'admission pour s'assurer que des ressources suffisantes sont réservées à la récupération des machine virtuelles en cas de défaillance d'un hôte.

Le contrôle d'admission impose des contraintes sur l'utilisation des ressources. Les actions qui risquent d'enfreindre ces contraintes ne sont pas autorisées. Les actions qui peuvent ne pas être autorisées incluent les exemples suivants :

- Mise sous tension d'une machine virtuelle
- Migration d'une machine virtuelle
- Augmentation de la réserve de CPU ou de mémoire d'une machine virtuelle

La base du contrôle d'admission vSphere HA est le nombre de défaillances d'hôte que le cluster est autorisé à tolérer et qui continue à garantir le basculement. La capacité de basculement des hôtes peut être définie de trois manières différentes :

- Pourcentage de ressources du cluster
- Stratégie d'emplacement

- Hôtes de basculement dédiés

Note Vous pouvez désactiver le contrôle d'admission de vSphere HA. 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 définitivement le contrôle d'admission.

Note Dans un cluster, désactivez temporairement le contrôle d'admission HA pour laisser vSphere vMotion poursuivre. Cette action permet d'éviter les interruptions de service des machines sur les hôtes que vous corrigez. La désactivation du contrôle d'admission HA avant de corriger un cluster à deux nœuds entraîne la perte de quasiment toutes ses garanties de haute disponibilité. Cela est dû au fait que lorsque l'un des deux hôtes passe en mode de maintenance, vCenter Server ne peut pas basculer les machines virtuelles vers cet hôte et les basculements HA ne réussissent jamais.

Quelle que soit l'option de contrôle d'admission choisie, un seuil de réduction des ressources de VM existe également. Ce paramètre permet de spécifier le pourcentage de dégradation des ressources pouvant être toléré, mais il n'est pas disponible si vSphere DRS n'est pas activé.

Le calcul de la réduction des ressources est vérifié pour le CPU et la mémoire. Il prend en compte la mémoire réservée d'une machine virtuelle et la surcharge de la mémoire pour décider de l'autoriser ou non à être mise sous tension, migrée ou à modifier sa réservation. La mémoire réelle utilisée par la machine virtuelle n'est pas prise en compte dans le calcul, car la réservation de mémoire ne correspond pas toujours à l'utilisation réelle de la mémoire de la machine virtuelle. Si l'utilisation réelle est supérieure à la mémoire réservée, la capacité de basculement disponible est insuffisante, ce qui entraîne la dégradation des performances lors du basculement.

La définition d'un seuil de réduction des performances vous permet de spécifier l'incidence d'un problème de configuration. Par exemple :

- La valeur par défaut est 100 %, qui ne produit pas d'avertissements.
- Si vous réduisez le seuil à 0 %, un avertissement est généré dès que l'utilisation du cluster est supérieure à la capacité disponible.
- Si vous réduisez le seuil à 20 %, la réduction des performances pouvant être tolérée est calculée de la manière suivante : `performance reduction = current utilization * 20%`. Lorsque l'utilisation actuelle moins la réduction des performances dépasse la capacité disponible, une notification concernant la configuration est émise.

Contrôle d'admission Pourcentage de ressources de cluster

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.

Avec ce type de contrôle d'admission, vSphere HA vérifie qu'un pourcentage spécifié de ressources cumulées de CPU et de mémoire est réservé au basculement.

Lorsque l'option de pourcentage de ressources de cluster est configurée, vSphere HA met en œuvre le contrôle d'admission de la manière suivante :

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 L'option de pourcentage de ressources de cluster du contrôle d'admission vérifie 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.

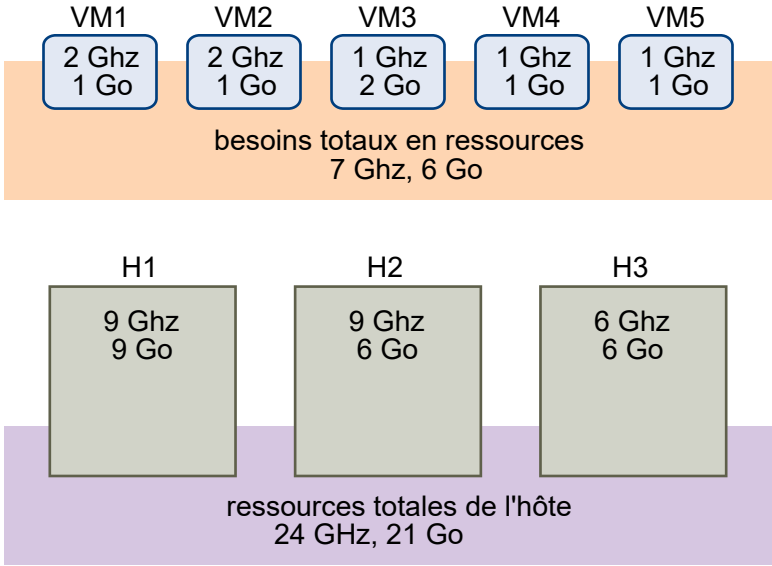
La Capacité CPU de basculement actuelle est calculée en soustrayant les besoins totaux en ressources CPU des ressources CPU totales des hôtes et en divisant le résultat par les ressources CPU totales des hôtes. La Capacité mémoire de basculement actuelle est calculée de la même manière.

Exemple : Contrôle d'admission en utilisant un pourcentage de ressources de cluster

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 2-1. 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.

Contrôle d'admission Stratégie d'emplacement

Lorsque l'option de stratégie d'emplacement est configurée, 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 depuis ces hôtes.

Avec la stratégie d'emplacement, 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 Client

Calcul de la taille d'emplacement

 (Taille d'emplacement et contrôle d'admission de vSphere HA)

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 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 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.

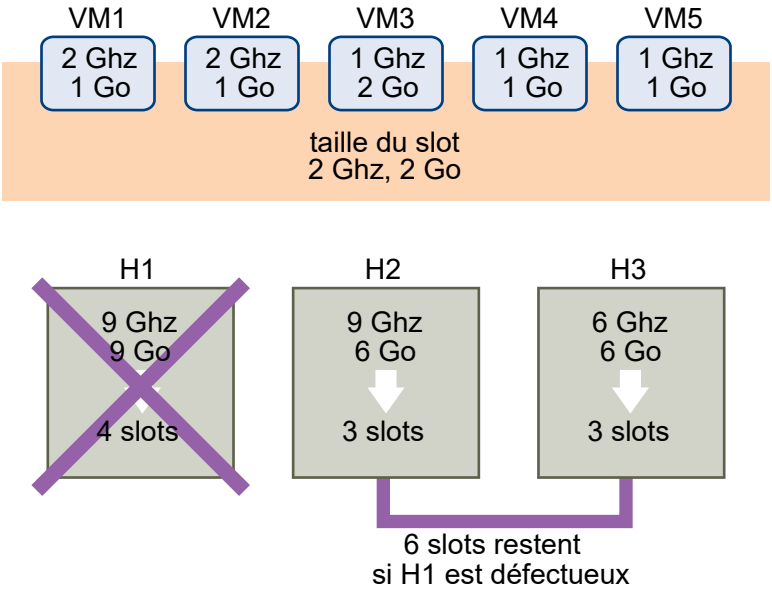
Exemple : Contrôle d'admission en utilisant la stratégie d'emplacement

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 2-2. 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).

Contrôle d'admission sur des hôtes de basculement dédiés

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

Avec le contrôle d'admission sur des hôtes de basculement dédiés, en cas de panne d'un hôte, vSphere HA tente de redémarrer ses machines virtuelles sur un des hôtes de basculement prédéfinis. Si le redémarrage des machines virtuelles est impossible, notamment lorsque les hôtes de basculement sont eux-mêmes en panne ou que leurs ressources sont insuffisantes, 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 le contrôle d'admission sur des hôtes de basculement dédiés 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.

Interopérabilité de vSphere HA

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

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

Utilisation de vSphere HA avec vSAN

Vous pouvez utiliser vSAN comme stockage partagé pour un cluster vSphere HA. S'il est activé, vSAN regroupe les disques de stockage locaux spécifiés qui sont disponibles sur les hôtes dans une banque de données unique partagée par tous les hôtes.

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

Pour plus d'informations sur vSAN, reportez-vous à la section *Administration de VMware vSAN*.

Note Vous pouvez utiliser vSphere HA avec des clusters étendus vSAN.

Conditions requises pour les hôtes ESXI

Pour utiliser vSAN 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

vSAN dispose de son propre réseau. Si vSAN et vSphere HA sont activés sur le même cluster, le trafic entre agents HA circule sur ce réseau de stockage plutôt que sur le réseau de gestion. vSphere HA utilise le réseau de gestion uniquement si vSAN est désactivé. Si vSphere HA est configuré sur un hôte, vCenter Server choisit le réseau approprié.

Note Vous ne pouvez activer vSAN que si vSphere HA est désactivé.

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

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

2 Modifiez le réseau vSAN.

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 dans la mise en réseau vSphere HA, que vSAN soit utilisé ou non.

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

	vSAN activé	vSAN désactivé
Réseau utilisé par vSphere HA	Réseau de stockage vSAN	Réseau de gestion
Banques de données de signaux de pulsation	Toutes les banques de données montées sur plusieurs hôtes, sauf les banques de données vSAN	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 vSAN 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 en utilisant une stratégie de contrôle d'admission, ce paramètre doit être cohérent avec le paramètre de vSAN 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 vSAN 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 vSAN 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 moins de capacité, l'activité de basculement peut s'avérer imprévisible. La réservation d'une capacité trop grande impose une contrainte excessive à l'activation des machines virtuelles et aux migrations vSphere vMotion entre clusters.

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 DPM (Distributed Power Management) 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*.

Note vSphere DRS est une fonctionnalité essentielle de vSphere qui est requise pour maintenir la santé des charges de travail exécutées dans un cluster vSphere. À partir de vSphere 7.0 Update 1, DRS dépend de la disponibilité des machines virtuelles vCLS. Pour plus d'informations, consultez *Services de cluster vSphere (vCLS)* dans *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, vous devez utiliser les options avancées de vSphere HA pour appliquer le comportement de basculement souhaité pour vSphere HA.

- **HA doit respecter les règles d'anti-affinité VM pendant le basculement** : lorsque l'option avancée des règles d'anti-affinité de machine virtuelle est définie, vSphere HA ne bascule pas sur une machine virtuelle s'il viole une règle en le faisant. Au lieu de cela, vSphere HA émet un événement signalant que les ressources sont insuffisantes pour effectuer le basculement.
- **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.

Pour plus d'informations, reportez-vous à la section Options avancées de vSphere HA.

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

Les problèmes et limitations d'interopérabilité suivants affectent VM Component Protection (VMCP) :

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

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 : link-local, ORCHID et link-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 niveau un déploiement IPv4 existant vers IPv6, vous devez d'abord désactiver vSphere HA.

Création 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 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 dans vSphere Client

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 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 vSphere 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.
- Connectez vSphere Client à vCenter Server en utilisant un compte disposant des autorisations d'administrateur de cluster.

Procédure

1. Dans vSphere Client, accédez au centre de données dans lequel vous souhaitez que le cluster réside et cliquez sur **Nouveau 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 Client pour ajouter des hôtes au cluster.
5. Accédez au cluster et activez vSphere HA.
   a. Cliquez sur l'onglet **Configurer**.
   b. Sélectionnez **Disponibilité vSphere** et cliquez sur **Modifier**.
   c. Sélectionnez **vSphere HA**.
6. Sous **Pannes et réponses**, sélectionnez **Activer la surveillance d'hôte**.

   Lorsque l'option de surveillance d'hôte est activée, les hôtes du cluster peuvent échanger des signaux de pulsation réseau et vSphere HA peut 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 de **Surveillance de VM**.

   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 appropriés pour votre cluster.

- Pannes et réponses
- Contrôle d'admission
- banques de données de signaux de pulsation
- Options avancées

Reportez-vous à la section Configuration des paramètres de disponibilité vSphere.

Configuration des paramètres de disponibilité vSphere

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 Client vous pouvez configurer les paramètres vSphere HA suivants :

Pannes et réponses

Fournissez ici les paramètres de réponses aux pannes d'hôte, d'isolation des hôtes, de surveillance des VM et de protection des composants des machines virtuelles.

Contrôle d'admission

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

Banques de données de signaux de pulsation

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.

Configuration des réponses aux pannes

Le volet **Panne et réponses** des paramètres de vSphere HA vous permet de configurer le fonctionnement du cluster lorsque des problèmes se produisent.

Dans cette partie de vSphere Client, vous pouvez déterminer les réponses spécifiques du cluster vSphere HA en cas de pannes ou d'isolation d'un hôte. Vous pouvez également configurer les actions de VM Component Protection (VMCP) lorsque des situations de type PDL (perte de périphérique permanente) et APD (Tous chemins hors service) se produisent et vous pouvez activer la surveillance de VM.

Les tâches suivantes sont disponibles :

Procédure

1 Répondre en cas de panne d'hôte

   Vous pouvez définir des réponses spécifiques en cas de pannes d'un hôte dans votre cluster vSphere HA.

2 Réponse en cas d'isolation d'hôte

   Vous pouvez définir des réponses spécifiques en cas d'isolation d'hôte dans votre cluster vSphere HA.

3 Configurer les réponses de VMCP

   Configurez la réponse de VMCP (VM Component Protection) en cas de défaillance de banque de données avec PDL ou APD.

4 Activer la surveillance de VM

   Vous pouvez activer la surveillance des VM et des applications, et également définir la sensibilité de surveillance de votre cluster vSphere HA.

Répondre en cas de panne d'hôte

Vous pouvez définir des réponses spécifiques en cas de pannes d'un hôte dans votre cluster vSphere HA.

Cette page est modifiable uniquement si vous avez activé vSphere HA.

Procédure

1 Dans vSphere Client, accédez au cluster vSphere HA .

2 Cliquez sur l'onglet **Configurer**.

3 Sélectionnez **Disponibilité vSphere** et cliquez sur **Modifier**.

4 Cliquez sur **Pannes et réponses** et développez l'option **Réponse en cas de panne de l'hôte**

5 Sélectionnez une des options de configuration suivantes.

Option	Description
Réponse en cas de panne	Si vous sélectionnez **Désactivé**, ce paramètre désactive la surveillance et les machines virtuelles ne sont pas redémarrées en cas de panne d'un hôte. Si l'option **Redémarrer les machines virtuelles** est sélectionnée, en cas de panne d'un hôte, les VM sont basculées en fonction de leur priorité de redémarrage.
Priorité de redémarrage des VM par défaut	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. 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.
Condition de priorité de redémarrage des machines virtuelles	Une condition spécifique doit être sélectionnée ainsi que le délai après que cette condition a été remplie, avant que vSphere HA soit autorisé à passer à la priorité de redémarrage de la VM suivante.

6 Cliquez sur **OK**.

Résultats

Vos paramètres de réponse en cas de panne d'hôte sont appliqués.

Réponse en cas d'isolation d'hôte

Vous pouvez définir des réponses spécifiques en cas d'isolation d'hôte dans votre cluster vSphere HA.

Cette page est modifiable uniquement si vous avez activé vSphere HA.

Procédure

1 Dans vSphere Client, accédez au cluster vSphere HA .

2 Cliquez sur l'onglet **Configurer**.

3 Sélectionnez **Disponibilité vSphere** et cliquez sur **Modifier**.

4 Cliquez sur **Pannes et réponses** et développez l'option **Réponse en cas d'isolation d'hôte**.

5 Pour configurer la réponse en cas d'isolation d'hôte, sélectionnez **Désactivé**, **Arrêter et redémarrer les machines virtuelles** ou **Mettre hors tension et redémarrer les VM**.

6 Cliquez sur **OK**.

Résultats

Votre paramètre de réponse en cas d'isolation d'hôte est appliqué.

Configurer les réponses de VMCP

Configurez la réponse de VMCP (VM Component Protection) en cas de défaillance de banque de données avec PDL ou APD.

Cette page est modifiable uniquement si vous avez activé vSphere HA.

Procédure

1 Dans vSphere Client, accédez au cluster vSphere HA .

2 Cliquez sur l'onglet **Configurer**.

3 Sélectionnez **Disponibilité vSphere** et cliquez sur **Modifier**.

4 Cliquez sur **Pannes et réponses** et développez l'option **Banque de données avec PDL** ou **Banque de données avec APD** .

5 Si vous avez cliqué sur **Banque de données avec PDL**, vous pouvez définir la réponse de VMCP pour ce type de problème : **Désactivé**, **Émission d'événements** ou **Mettre hors tension et redémarrer les VM**.

6 Si vous avez cliqué sur **Banque de données avec APD**, vous pouvez définir la réponse de VMCP pour ce type de problème : **Désactivé**, **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**. Vous pouvez également définir l'option **Récupération de réponse**, qui est le nombre de minutes pendant lesquelles VMCP attend avant d'exécuter une action.

7 Cliquez sur **OK**.

Résultats

Vos paramètres de réponse aux défaillances de VMCP sont appliqués.

Activer la surveillance de VM

Vous pouvez activer la surveillance des VM et des applications, et également définir la sensibilité de surveillance de votre cluster vSphere HA.

Cette page est modifiable uniquement si vous avez activé vSphere HA.

Procédure

1 Dans vSphere Client, accédez au cluster vSphere HA .

2 Cliquez sur l'onglet **Configurer**.

3 Sélectionnez **Disponibilité vSphere** et cliquez sur **Modifier**.

4 Cliquez sur **Pannes et réponses** et développez l'option **Surveillance de VM**.

5 Sélectionnez **Surveillance de VM** puis **Surveillance d'application**.

Ces paramètres activent les signaux de pulsation de VMware Tools et des applications, respectivement.

6 Pour définir la sensibilité de surveillance des signaux de pulsation, déplacez le curseur entre **Basse** et **Élevée** ou sélectionnez **Personnalisée** pour fournir des paramètres personnalisés.

7 Cliquez sur **OK**.

Résultats

Vos paramètres de surveillance sont appliqués.

Configurer Proactive HA

Vous pouvez configurer la manière dont Proactive HA répond lorsqu'un fournisseur a signalé la dégradation de sa santé à vCenter, ce qui est le signe d'une panne partielle de cet hôte.

Cette page est modifiable uniquement si vous avez activé vSphere DRS.

Procédure

1. Dans vSphere Client, accédez au cluster Proactive HA.
2. Cliquez sur l'onglet **Configurer**.
3. Sélectionnez **Disponibilité vSphere** et cliquez sur **Modifier**.
4. Sélectionnez **Activer Proactive HA**.
5. Cliquez sur **Pannes et réponses de Proactive HA**
6. Sélectionnez une des options de configuration suivantes.

Option	Description
Niveau d'automatisation	Déterminez si le mode de quarantaine ou de maintenance des hôtes et les migrations de VM sont des recommandations ou des réponses automatiques. ■ **Manuel**. vCenter Server suggère des recommandations de migration pour les machines virtuelles. ■ **Automatisé**. Les machines virtuelles sont migrées vers des hôtes sains et les hôtes dégradés sont mis en quarantaine ou en mode de maintenance selon la configuration du niveau d'automatisation de Proactive HA.
Correction	Déterminez ce qui se produit pour les hôtes partiellement dégradés. ■ **Mode Quarantaine pour toutes les pannes**. Maintient un équilibre entre performances et disponibilité, en évitant l'utilisation d'hôtes partiellement dégradés tant que les performances des machines virtuelles ne sont pas affectées. ■ **Mode de quarantaine pour les pannes modérées et mode de maintenance pour les pannes graves (mixte)**. Maintient un équilibre entre performances et disponibilité, en évitant l'utilisation d'hôtes modérément dégradés tant que les performances des machines virtuelles ne sont pas affectées. Garantit que les machines virtuelles ne s'exécutent pas sur des hôtes présentant une panne sévère. ■ **Mode Maintenance pour toutes les pannes**. Garantit que les machines virtuelles ne s'exécutent pas sur des hôtes présentant une panne partielle. Les privilèges `Host.Config.Quarantine` et `Host.Config.Maintenance` doivent mettre les hôtes respectivement en mode de quarantaine et en mode de maintenance.

Pour activer les fournisseurs Proactive HA pour ce cluster, cochez les cases. Des fournisseurs s'affichent lorsque leur plug-in vSphere Client correspondant a été installé et que les fournisseurs surveillent chaque hôte du cluster. Pour afficher ou modifier les conditions de panne prises en charge par le fournisseur, cliquez sur le lien de modification.

7 Cliquez sur **OK**.

Configurer le contrôle d'admission

Après avoir créé un cluster, vous pouvez configurer le contrôle d'admission afin de spécifier si les machines virtuelles peuvent être démarrées si elles ne respectent pas 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 d'admission apparaît uniquement si vous avez activé vSphere HA.

Procédure

1 Dans vSphere Client, accédez au cluster vSphere HA .

2 Cliquez sur l'onglet **Configurer**.

3 Sélectionnez **Disponibilité vSphere** et cliquez sur **Modifier**.

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

5 Sélectionnez un nombre dans **Pannes de l'hôte tolérées par le cluster**. Il s'agit du nombre maximal de pannes de l'hôte dont le cluster peut récupérer ou pour lesquelles il peut garantir le basculement.

6 Sélectionnez une option pour **Définir la capacité de basculement de l'hôte par**.

Option	Description
Pourcentage de 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.
Stratégie d'emplacement (VM sous tension)	Sélectionnez une stratégie de taille d'emplacement qui couvre toutes les machines virtuelles sous tension ou qui correspond à une taille fixe. Vous pouvez également calculer le nombre de machines virtuelles qui ont besoin d'emplacements multiples.
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.
Désactivé	Sélectionnez cette option pour désactiver le contrôle d'admission et autoriser la mise sous tension des machines virtuelles qui enfreignent les contraintes de disponibilité.

7 Définissez le pourcentage pour **Dégradation des performances tolérées par les VM**.

Ce paramètre détermine quel pourcentage de dégradation des performances les machines virtuelles du cluster sont autorisées à tolérer lors d'une panne.

8 Cliquez sur **OK**.

Résultats

Vos paramètres de contrôle d'admission sont appliqués.

Configurer les banques de données de signal de pulsation

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. Avec le signal de pulsation des banques de données, vSphere HA peut surveiller les hôtes en cas de partitionnement du réseau de gestion et continuer à répondre aux pannes.

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

Procédure

1 Dans vSphere Client, accédez au cluster vSphere HA .

2 Cliquez sur l'onglet **Configurer**.

3 Sélectionnez **Disponibilité vSphere** et cliquez sur **Modifier**.

4 Cliquez sur **Banques de données de signal de pulsation** pour afficher les options de configuration de signal de pulsation des banques de données.

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

Tableau 2-3.

Options de signal de pulsation de banque de données
Sélectionner automatiquement les banques de données accessibles depuis l'hôte
Utiliser uniquement les banques de données de la liste spécifiée
Utiliser les banques de données de la liste spécifiée, puis compléter automatiquement si nécessaire

6 Dans le volet Banques de données des signaux de pulsation disponibles, sélectionnez 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 Client, accédez au cluster vSphere HA .
2. Cliquez sur l'onglet **Configurer**.
3. Sélectionnez **Disponibilité vSphere** et cliquez 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 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.
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.

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

Option	Description
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 défini sur n'importe quelle valeur supérieure ou égale à 0. Définir la valeur 0 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. La valeur par défaut est « true » et 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. Cette option peut également être définie sur « false », auquel cas les règles ne sont pas appliquées. Pour plus d'informations sur les règles d'anti-affinité, reportez-vous à *Gestion des ressources vSphere*.
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.

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

Option	Description
das.config.fdm.reportfailoverfailevent	Lorsque 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.
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.reregisterrestartdisabledvms	Lorsque vSphere HA est désactivé sur une machine virtuelle spécifique, cette option garantit que la machine virtuelle est enregistrée sur un autre hôte après une panne. Vous pouvez ainsi mettre cette machine virtuelle sous tension sans devoir la réenregistrer manuellement. **Note** Lorsque cette option est utilisée, vSphere HA ne met pas la machine virtuelle sous tension, mais l'enregistre uniquement.
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 6.5 ou version ultérieure, la valeur par défaut est « true ». Cette valeur ne peut pas être visiblement définie dans les options HA avancées du cluster. Si vous souhaitez désactiver l'option, vous devez manuellement définir cette option en tant que « false » 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 Client, accédez au cluster vSphere HA .
2. Cliquez sur l'onglet **Configurer**.
3. Sous Configuration, sélectionnez **Remplacements de 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 modifier d'autres paramètres, comme **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.

Recommandations pour les clusters VMware vSphere® High Availability

Pour garantir des performances optimales des clusters vSphere HA, vous devez observer certaines recommandations. 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 fonctionnalité 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 pannes 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, vous devez 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 du flux réseau, les cartes vmkNIC utilisées par vSphere HA et par les autres fonctionnalités doivent se trouver 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. Utilisez 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. En outre, 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 peut être attribuée à une interface réseau donnée utilisée pour 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 l’interopérabilité entre vSphere HA et d'autres fonctionnalités.

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

Dans les clusters où les hôtes ESXi 5.x et ESX/ESXi 4.1 ou des hôtes de version antérieure sont présents, et où Storage vMotion est largement utilisé ou Storage DRS est activé, ne déployez pas vSphere HA. vSphere HA peut répondre à une panne de l'hôte en redémarrant une machine virtuelle présente sur un hôte ayant une version d'ESXi différente de celle sur laquelle la machine virtuelle s'exécutait avant la panne. Un problème peut se produire si, au moment de la panne, la machine virtuelle était impliquée dans une action de Storage vMotion sur un hôte ESXi 5.x et que vSphere HA redémarre la machine virtuelle sur un hôte d’une version antérieure à ESXi 5.0. Bien que la machine virtuelle puisse démarrer, les tentatives de mise sous tension suivantes lors d’opérations de snapshot peuvent corrompre l’état 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 provisionne les hôtes lorsqu'ils démarrent. 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 des hôtes d'un cluster à l'aide de vSAN

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 vSAN, suivez ce processus.

1 Mettez à niveau tous les hôtes.

2 Désactiver vSphere HA

3 Activer vSAN.

4 Réactivez vSphere HA.

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.

Modification du comportement des VIB HA

Dans vSphere 7.0 ou version ultérieure, les VIB HA peuvent parfois être supprimés lorsque HA est activé sur un cluster Lifecycle Manager (vLCM). Dans les versions précédentes, vCenter ne tentait pas de supprimer les VIB HA des hôtes ESXi.

Cette situation peut se produire uniquement sur les clusters vLCM sur lesquels vSphere HA est activé. Lorsqu'une opération de **Correction** de vLCM se produit (en tant qu'opération lancée par l'utilisateur ou en cas d'appel d'API), les VIB de vSphere HA peuvent être supprimés après la désactivation de vSphere HA sur le cluster.

Note Cette modification du comportement est inoffensive, car vCenter transfère les VIB vSphere HA requis lorsque HA est activé de nouveau.

Assurer Fault Tolerance des machines virtuelles

3

Vous pouvez utiliser vSphere Fault Tolerance pour vos machines virtuelles, afin d'assurer la continuité avec des niveaux supérieurs de disponibilité et de protection des données.

Fault Tolerance est basée sur la plate-forme hôte ESXi et elle fournit une disponibilité 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 votre cluster et sur des machines virtuelles, et de connaître les meilleures pratiques pour son utilisation.

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. La machine virtuelle principale est répliquée en permanence sur la machine virtuelle secondaire de sorte que la machine virtuelle secondaire peut prendre le relais à tout moment, favorisant ainsi la protection Fault Tolerant.

Les machines virtuelles principale et secondaire surveillent continuellement l'état l'une de l'autre pour vérifier que Fault Tolerance est maintenu. Un basculement transparent se produit si l'hôte exécutant la machine virtuelle principale échoue ou rencontre une erreur matérielle irrémédiable dans la mémoire de la machine virtuelle principale, auquel 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 de 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 8 vCPU.

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. Le basculement assuré par vSphere HA redémarre les machines virtuelles affectées par une panne.

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.

- Applications qui doivent toujours être disponibles, notamment les applications présentant de longues connexions client que les utilisateurs souhaitent maintenir pendant les pannes matérielles.
- 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. Par exemple, vous pouvez exécuter un rapport trimestriel dont l'interruption peut retarder la mise à disposition d'informations cruciales. 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.

Configuration requise

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 des machines virtuelles Fault Tolerance doivent être compatibles avec vSphere vMotion. 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 machines virtuelles Fault Tolerance autorisées sur un hôte dans le cluster. La valeur par défaut est 4. Il n'y a pas de nombre maximal de machines virtuelles FT par hôte, vous pouvez utiliser des nombres plus importants si la charge de travail s'exécute correctement dans les machines virtuelles FT. Vous pouvez désactiver la vérification en définissant la valeur sur **0**.

das.maxftvcpusperhost

Nombre maximal de vCPU agrégés sur toutes les machines virtuelles tolérantes aux pannes sur un hôte. La valeur par défaut est 8. Il n'y a pas de nombre maximal de vCPU FT par hôte, vous pouvez utiliser des nombres plus importants si la charge de travail fonctionne correctement. Vous pouvez désactiver la vérification en définissant la valeur sur **0**.

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 8 vCPU

Note FT est prise en charge dans les éditions vSphere Standard, vSphere Enterprise et vSphere Enterprise Plus.

Interopérabilité de Fault Tolerance

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

Fonctions vSphere non prises en charge par Fault Tolerance

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.

Note Pour les versions antérieures à vSphere 7.0 Update 2, le chiffrement de machines virtuelles vSphere n'était pas pris en charge avec FT.

- 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.

- Storage 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.
- Banques de données Virtual Volumes.
- Gestion de stratégie basée sur le stockage. Les stratégies de stockage sont prises en charge pour le stockage vSAN.
- Filtres d'E/S.
- Machines virtuelles avec VBS activée

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.

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

Fonction ou périphérique incompatible	Action corrective
Périphérique USB et audio.	Déconnectez ces périphériques de la machine virtuelle.
Virtualisation d'identification N-Port (NPIV).	Désactivez la configuration NPIV de la machine virtuelle.
relais d'adaptateurs réseau	Cette fonction n'est pas prise en charge par Fault Tolerance et doit donc être désactivée.
Connexion de périphériques à chaud	La fonctionnalité de plug 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.
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).

Les machines virtuelles FT ne nécessitent pas qu'EVC prenne en charge DRS. Vous pouvez utiliser FT avec DRS sur des hôtes vSphere 6.5 et 6.0 qui sont gérés par un vSphere 6.7 ou une version de VC plus élevée.

Note vSphere DRS est une fonctionnalité essentielle de vSphere qui est requise pour maintenir la santé des charges de travail exécutées dans un cluster vSphere. À partir de vSphere 7.0 Update 1, DRS dépend de la disponibilité des machines virtuelles vCLS. Pour plus d'informations, consultez *Services de cluster vSphere (vCLS)* dans *Gestion des ressources vSphere*.

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 la section Configurer la mise en réseau des machines hôtes.
- Cluster vSphere HA créé et activé. Reportez-vous à la section Création 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 la section Interopérabilité de Fault Tolerance.
- Les fonctions incompatibles ne doivent pas être exécutées avec les machines virtuelles tolérantes aux pannes. Reportez-vous à la section Interopérabilité de Fault Tolerance.
- Les fichiers des machines virtuelles (sauf les fichiers VMDK) doivent être stockés sur le stockage partagé. Les solutions de stockage partagé approuvées comprennent Fibre Channel, iSCSI (matériel et logiciel), vSAN, 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.
- 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 configurer 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. Reportez-vous à la section Configuration requise, limites et licence de Fault Tolerance.

Procédure

1. Dans vSphere Client, accédez à l'hôte.
2. Cliquez sur l'onglet **Configurer**, puis sur **Mise en réseau**.
3. Sélectionnez **Adaptateurs VMkernel**.
4. Cliquez sur l'icône **Ajouter une mise en réseau**.
5. Fournissez les informations appropriées pour votre type de connexion.
6. Cliquez sur **Terminer**.

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 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 Fault Tolerance

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.
- ESXi 6.x ou version ultérieure doit être installé sur l'hôte.
- La machine virtuelle ne doit pas avoir de snapshots.
- La machine virtuelle ne doit pas être un modèle.

- vSphere HA ne doit pas être désactivé sur la machine virtuelle.
- 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 sur lesquels 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 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 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 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 dans le mode maintenance ou le mode 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 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 **Yes**.
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.

Note Les banques de données et la mémoire de machine virtuelle sont répliquées pendant le processus d'activation de Fault Tolerance. Cela peut prendre plusieurs minutes selon la taille des données répliquées. L'état de la machine virtuelle n'apparaît pas comme étant protégé tant que la réplication n'est pas terminée.

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 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 Fault Tolerance**.
3. Cliquez sur **Yes**.

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.

Note Fault Tolerance ne peut pas être désactivé lorsque la machine virtuelle secondaire est en cours de démarrage. Étant donné que cela implique de synchroniser l'état complet de la machine virtuelle principale avec la machine virtuelle secondaire, ce processus peut prendre plus de temps que prévu.

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 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 **Yes**.

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 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 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 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.

Activer le chiffrement Fault Tolerance

Vous pouvez chiffrer le trafic des journaux Fault Tolerance.

vSphere Fault Tolerance effectue régulièrement des vérifications entre une VM principale et une VM secondaire, afin que la VM secondaire puisse reprendre rapidement à partir du dernier point de contrôle réussi. Le point de contrôle contient l'état de la VM qui a été modifié depuis le point de contrôle précédent. Vous pouvez chiffrer le trafic des journaux Fault Tolerance.

Lorsque vous activez Fault Tolerance, le chiffrement FT est défini sur **Opportuniste** par défaut, ce qui signifie qu'il active le chiffrement uniquement si l'hôte principal et l'hôte secondaire sont compatibles avec le chiffrement. Suivez cette procédure si vous devez modifier manuellement le mode de chiffrement FT.

Note Fault Tolerance prend en charge le chiffrement des machines virtuelles vSphere avec vSphere 7.0 Update 2 et versions ultérieures. Le chiffrement invité et basé sur la baie ne dépend pas du chiffrement des machines virtuelles et n'interrompt pas ce dernier. L'utilisation de plusieurs couches de chiffrement requiert des ressources de calcul supplémentaires et peut avoir un impact sur les performances de la machine virtuelle. Cet impact varie selon le matériel, la quantité et le type d'E/S, mais les performances globales ne sont pratiquement pas affectées pour la plupart des charges de travail. L'efficacité et la compatibilité des fonctionnalités de stockage back-end telles que la déduplication, la compression et la réplication peuvent également être affectées par le chiffrement des machines virtuelles.

Conditions préalables

Le chiffrement FT nécessite SMP-FT. Le chiffrement FT hérité (FT d'enregistrement-lecture) n'est pas pris en charge.

Procédure

1 Sélectionnez la VM et choisissez **Modifier les paramètres**.

2 Sous **Options VM**, sélectionnez le menu déroulant **FT chiffrée**.

3 Choisissez l'une des options suivantes :

Option	Description
Désactivé	Ne pas activer la journalisation de FT chiffrée.
Opportuniste	Activez le chiffrement uniquement si les deux côtés sont compatibles. Une VM avec Fault Tolerance est autorisée à se déplacer vers un hôte ESXi qui ne prend pas en charge la journalisation de Fault Tolerance chiffrée.
Requis	Choisissez un hôte principal et un hôte secondaire pour Fault Tolerance qui prennent tous les deux en charge la journalisation de FT chiffrée.

Note Lorsque le chiffrement de la VM est activé, le mode de chiffrement FT est défini sur **Requis** par défaut et ne peut pas être modifié.

Lorsque le mode de chiffrement FT est défini sur **Requis** :

- Lorsque vous activez FT, seuls les hôtes compatibles avec le chiffrement FT sont répertoriés pour le choix d'hôte secondaire FT.
- Le basculement de FT ne peut se produire que sur les hôtes compatibles avec le chiffrement FT.

4 Cliquez sur **OK**.

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 mêmes 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.

Vous pouvez sélectionner plusieurs cartes réseau pour le réseau de journalisation FT. En sélectionnant plusieurs cartes réseau, vous pouvez tirer parti de la bande passante de plusieurs cartes réseau, même si toutes les cartes réseau ne sont pas dédiées à l'exécution de FT.

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.

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 des banques de données vSAN

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

- Un mélange de vSAN et d'autres types de banques de données n'est pas pris en charge pour les machines virtuelles principales et les machines virtuelles secondaires.

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

- vSAN et FT doivent utiliser des réseaux distincts.
- Maintenez les machines virtuelles principales et secondaires dans des domaines de pannes vSAN distincts.

Fault Tolerance héritée

Les machines virtuelles avec FT héritée existent uniquement sur les hôtes ESXi qui sont exécutés sur des versions de vSphere antérieures à la version 6.5.

Les hôtes ESXi antérieurs à la version 6.5 prenait en charge vSphere Fault Tolerance basé sur une technologie différente. Si vous utilisez ce format de Fault Tolerance et que vous devez continuer ainsi, nous vous recommandons de réserver une instance de vCenter 6.0 pour gérer le pool d'hôtes antérieurs à la version 6.5 requis pour exécuter ces machines virtuelles. vCenter 6.0 était la dernière version totalement capable de gérer les VM héritées avec protection FT. Pour plus d'informations sur la fonctionnalité Fault Tolerance héritée, reportez-vous à la documentation de vSphere Availability 6.0.

Dépannage de machines virtuelles tolérantes aux pannes

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

Les rubriques de dépannage traitées concernent des problèmes que vous pourriez rencontrer lors de l'utilisation de la fonction vSphere Fault Tolerance sur vos machines virtuelles. Les rubriques expliquent également comment résoudre les problèmes.

Vous pouvez également consulter l'article dans la base de connaissances VMware accessible à l'adresse http://kb.vmware.com/kb/1033634 pour vous aider à dépanner la fonction de Fault Tolerance. Cet article contient la liste des messages d'erreur pouvant être rencontrés lorsque vous essayez d'utiliser la fonction et, si applicable, conseille comment résoudre chaque erreur.

Virtualisation matérielle non activée

Vous devez activer la Virtualisation matérielle (HV) avant d'utiliser vSphere Fault Tolerance.

Problème

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

Cause

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

Solution

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

Si les composants matériels du serveur ESXi ne prennent pas en charge la virtualisation matérielle, basculez sur des composants matériels utilisant des processeurs qui prennent en charge Fault Tolerance

Hôtes compatibles non disponibles pour les machines virtuelles secondaires

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

Problème

Le message d'erreur suivant peut s'afficher :

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

Cause

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

Solution

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

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

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

Problème

Lorsqu'une machine virtuelle secondaire se trouve sur un hôte fortement chargé, elle peut affecter les performances de la machine virtuelle principale.

Cause

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

Solution

Si la machine virtuelle secondaire se trouve sur un hôte surchargé, vous pouvez la déplacer vers un autre emplacement sans rencontrer de problèmes de conflit de ressources. Autrement dit, procédez comme suit :

- Pour les conflits de mise en réseau FT, utilisez la technologie vMotion pour déplacer la machine virtuelle secondaire vers un hôte disposant d'un nombre moins élevé de machines virtuelles FT présentant un conflit sur le réseau FT. Vérifiez que la qualité de l'accès au stockage de la machine virtuelle n'est pas asymétrique.
- Pour les problèmes de conflit de stockage, désactivez FT et réactivez-le. Lorsque vous recréez la machine virtuelle secondaire, déplacez sa banque de données vers un emplacement avec moins de conflits de ressources et un meilleur potentiel de performance.
- Pour résoudre un problème de ressources de CPU, définissez une réservation de CPU explicite pour la machine virtuelle principale en réglant une valeur en MHz suffisante pour l'exécution de la charge de travail au niveau de performances requis. Cette réservation s'appliquée à la fois aux machines virtuelles principale et secondaire, ce qui garantit qu'elles pourront toutes deux fonctionner à la vitesse spécifiée. Pour vous aider à définir cette réservation, consultez les graphiques de performances de la machine virtuelle (avant l'activation de Fault Tolerance) pour vérifier la quantité de ressources de CPU utilisée dans des conditions normales.

Augmentation de la latence du réseau observée sur les machines virtuelles FT

Si votre réseau de FT n'est pas configuré de manière optimale, vous risquez de rencontrer des problèmes de latence avec les machines virtuelles FT.

Problème

La latence des paquets des machines virtuelles FT peut augmenter de manière variable (environ quelques millisecondes). Les performances des applications qui exigent une latence de paquets réseau ou une gigue très faible (certaines applications en temps réel, par exemple) peuvent être altérées.

Cause

Une certaine augmentation de la latence du réseau est prévue en surcharge pour Fault Tolerance, mais certains facteurs peuvent s'ajouter à cette latence. Par exemple, si le réseau FT se trouve sur un lien de latence particulièrement élevé, cette latence est transmise aux applications. De plus, si la bande passante du réseau FT est insuffisante (moins de 10 Gbps), une latence plus élevée peut se produire.

Solution

Vérifiez que la bande passante du réseau FT est suffisante (au moins 10 Gbps) et utilise un lien à faible latence entre les machines virtuelles principale et secondaire. Ces précautions n'éliminent pas la latence du réseau, mais minimisent son impact potentiel.

Certains hôtes sont surchargés avec des machines virtuelles FT

Vous pouvez rencontrer des problèmes de performance si les machines virtuelles FT ne sont pas réparties de manière uniforme sur les hôtes de votre cluster.

Problème

Certains hôtes du cluster peuvent être surchargés avec des machines virtuelles FT, tandis que d'autres hôtes peuvent disposer de ressources inutilisées.

Cause

vSphere DRS n'équilibre pas la charge des machines virtuelles FT (sauf si elles utilisent l'option FT héritée). Cette limitation peut entraîner la création d'un cluster dans lequel les hôtes sont inégalement répartis avec les machines virtuelles FT.

Solution

Rééquilibrez manuellement les machines virtuelles FT sur le cluster à l'aide de vSphere vMotion. Généralement, moins il y a de machines virtuelles FT sur un hôte, mieux elles fonctionnent, car la contention de la bande passante réseau FT et des ressources de CPU est réduite.

Perte d'accès à la banque de données des métadonnées FT

Il est essentiel de pouvoir accéder à la banque de données des métadonnées Fault Tolerance pour assurer le bon fonctionnement d'une machine virtuelle FT. La perte de cet accès peut provoquer toute une série de problèmes.

Problème

Les problèmes sont les suivants :

- FT peut s'arrêter de manière inattendue.
- Si ni la machine virtuelle principale, ni la secondaire ne peut accéder à la banque de données des métadonnées, les machines virtuelles peuvent échouer de manière inattendue. En général, un échec isolé provoquant l'arrêt de FT se produit également lorsque les deux machines virtuelles perdent l'accès à la banque de données des métadonnées FT. vSphere HA tente ensuite de redémarrer la machine virtuelle principale sur un hôte disposant d'un accès à la banque de données des métadonnées.
- La machine virtuelle peut ne plus être reconnue comme une machine virtuelle FT par vCenter Server. Cet échec de reconnaissance peut autoriser certaines opérations non prises en charge, telles que la création de snapshots sur la machine virtuelle, ce qui peut entraîner des problèmes de fonctionnement.

Cause

L'absence d'autorisations d'accès à la banque de données des métadonnées de Fault Tolerance peut conduire à des résultats indésirables dans la liste précédente.

Solution

Lors de la planification de votre déploiement FT, placez la banque de données des métadonnées sur un stockage à haut niveau de disponibilité. Lorsque FT est en cours d'exécution, si vous ne parvenez pas à accéder à la banque de données des métadonnées sur la machine virtuelle principale ou secondaire, traitez rapidement le problème de stockage avant que la perte de l'accès provoque l'un des problèmes précédents. Si une machine virtuelle n'est plus reconnue comme une machine virtuelle FT par vCenter Server, n'effectuez aucune opération non prise en charge sur la machine virtuelle. Restaurez l'accès à la banque de données des métadonnées. Après le rétablissement de l'accès aux machines virtuelles FT et à la fin de la période d'actualisation, les machines virtuelles sont reconnaissables.

Échec de l'activation de vSphere FT pour les machines virtuelles sous tension

Si vous tentez d'activer vSphere Fault Tolerance pour une machine virtuelle sous tension, il est possible que l'opération échoue.

Problème

Lorsque vous sélectionnez **Activer Fault Tolerance** pour une machine virtuelle sous tension, l'opération échoue et un message `Erreur inconnue` s'affiche.

Cause

Cette opération peut échouer si l'hôte sur lequel la machine virtuelle s'exécute ne possède pas suffisamment de ressources mémoire pour assurer la protection Fault Tolerance. vSphere Fault Tolerance tente automatiquement d'allouer une réservation de mémoire totale sur l'hôte pour la machine virtuelle. Une capacité supplémentaire de mémoire s'avère nécessaire pour les machines virtuelles avec Fault Tolerance. Elle peut atteindre 1 à 2 Go dans certains cas. Si la machine virtuelle sous tension s'exécute sur un hôte dont les ressources mémoire sont insuffisantes pour gérer la réservation totale et la capacité supplémentaire de mémoire, l'activation de Fault Tolerance échoue. Ensuite, le message `Erreur inconnue` est renvoyé.

Solution

Vous avez le choix entre les solutions ci-dessous :

- Libérez des ressources mémoire sur l'hôte pour prendre en charge la réservation de mémoire de la machine virtuelle et la capacité supplémentaire ajoutée.
- Déplacez la machine virtuelle vers un hôte offrant une grande quantité de ressources mémoire disponibles et réessayez.

Machines virtuelles FT non placées ou supprimées par vSphere DRS

Dans un cluster activé avec vSphere DRS, les machines virtuelles avec FT ne fonctionnent pas correctement si le mode Enhanced vMotion Compatibility (EVC) est actuellement désactivé.

Problème

Comme le mode EVC est requis pour utiliser DRS avec les machines virtuelles avec FT, DRS ne peut pas les placer ni les supprimer si EVC a été désactivé (même s'il est réactivé plus tard).

Cause

Lorsque le mode EVC est désactivé sur un cluster DRS, un remplacement de machine virtuelle qui désactive DRS sur une machine virtuelle avec FT peut être ajouté. Même si le mode EVC est réactivé plus tard, ce remplacement n'est pas annulé.

Solution

Si le mode DRS ne place pas et ne supprime pas les machines virtuelles avec FT dans le cluster, examinez les machines virtuelles pour identifier tout remplacement de machine virtuelle qui désactive DRS. Si vous en trouvez un, supprimez le remplacement qui désactive DRS.

Note Pour plus d'informations sur la modification ou la suppression de remplacements de machine virtuelle, reportez-vous à la section *Gestion des ressources vSphere*.

Basculement d'une machine virtuelle tolérante aux pannes

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

Panne matérielle partielle liée au stockage

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

Panne matérielle partielle liée au réseau

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

Bande passante insuffisante sur le réseau de la carte de journalisation

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

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

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

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

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

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

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

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

vCenter High Availability

4

vCenter High Availability (vCenter HA) protège vCenter Server contre les défaillances matérielles et de l'hôte. L'architecture active-passive de la solution peut également vous aider à réduire considérablement les temps d'arrêt lorsque vous appliquez un correctif à vCenter Server.

Après avoir procédé à la configuration du réseau, vous créez un cluster à trois nœuds qui contient les nœuds actif, passif et témoin. Différents chemins de configuration sont possibles. Ce que vous sélectionnez dépend de votre configuration existante.

Procédure

1 Planifier le déploiement de vCenter HA

Avant de configurer vCenter HA, vous devez prendre en compte plusieurs facteurs. Un déploiement avec des composants utilisant différentes versions de vSphere nécessite une préparation différente d'un déploiement incluant exclusivement des composants vSphere 8.0. Les ressources et les logiciels nécessaires, ainsi que la configuration du réseau, doivent également faire l'objet d'une préparation soigneuse.

2 Configurer le réseau

Quelles que soient l'option de déploiement et la hiérarchie d'inventaire sélectionnée, vous devez définir votre réseau avant de commencer la configuration. Pour définir les fondations du réseau vCenter HA, vous ajoutez un groupe de ports à chaque hôte ESXi.

3 Configurer vCenter HA avec vSphere Client

Lorsque vous utilisez vSphere Client, l'assistant **Configurer vCenter HA** crée et configure un deuxième adaptateur réseau sur vCenter Server, clone le nœud actif et configure le réseau vCenter HA.

4 Gérer la configuration vCenter HA

Après avoir configuré votre cluster vCenter HA, vous pouvez effectuer les tâches de gestion. Ces tâches incluent le remplacement de certificats, le remplacement des clés SSH et la configuration SNMP. Vous pouvez également modifier la configuration du cluster pour désactiver ou activer vCenter HA, passer en mode de maintenance et supprimer la configuration du cluster.

5 Corriger votre environnement vCenter HA

En cas de problème, vous pouvez corriger votre environnement. La tâche que vous devez effectuer dépend des symptômes de la défaillance. Pour en savoir plus sur le dépannage, reportez-vous au système de la base de connaissances VMware.

6 Application de correctifs à un environnement vCenter High Availability

Vous pouvez appliquer un correctif à un dispositif vCenter Server situé dans un cluster vCenter High Availability à l'aide de l'utilitaire **`software-packages`** disponible dans l'interpréteur du dispositif vCenter Server.

Planifier le déploiement de vCenter HA

Avant de configurer vCenter HA, vous devez prendre en compte plusieurs facteurs. Un déploiement avec des composants utilisant différentes versions de vSphere nécessite une préparation différente d'un déploiement incluant exclusivement des composants vSphere 8.0. Les ressources et les logiciels nécessaires, ainsi que la configuration du réseau, doivent également faire l'objet d'une préparation soigneuse.

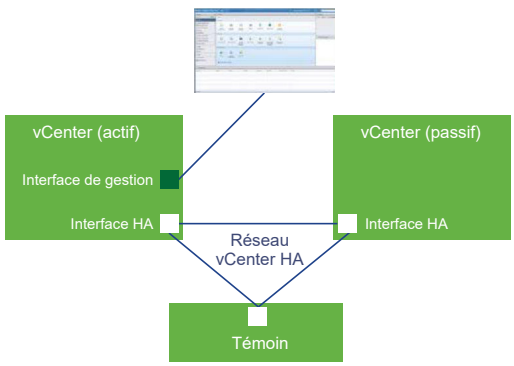
Vue d'ensemble de l'architecture de vCenter

Un cluster vCenter HA comprend trois instances de vCenter Server. La première instance, utilisée à l'origine comme un nœud actif, est clonée deux fois sur un nœud passif et un nœud témoin. Ensemble, ces trois nœuds forment une solution de basculement active-passive.

Le déploiement de chacun des nœuds sur une instance ESXi différente permet de se protéger contre les pannes matérielles. L'ajout des trois hôtes ESXi à un cluster DRS permet de mieux protéger votre environnement.

Une fois la configuration de vCenter HA terminée, seul le nœud actif dispose d'une interface de gestion active (IP public). Les trois nœuds communiquent sur un réseau privé appelé vCenter HA et qui a été défini lors de la configuration. Le nœud actif réplique continuellement les données vers le nœud passif.

Figure 4-1. Cluster vCenter à trois nœuds



Les trois nœuds sont nécessaires pour que cette fonctionnalité fonctionne. Comparez les responsabilités des nœuds.

Tableau 4-1. Nœuds vCenter HA

Nœud	Description
Active	■ Exécute l'instance vCenter Server active ■ Utilise une adresse IP publique pour l'interface de gestion ■ Utilise le réseau vCenter HA pour la réplication des données sur le nœud passif. ■ Utilise le réseau vCenter HA pour communiquer avec le nœud témoin.
Passif	■ Est initialement un clone du nœud actif ■ Il reçoit constamment des mises à jour du nœud actif et synchronise son état avec ce dernier sur le réseau vCenter HA ■ Prend automatiquement le relais en tant que nœud actif en cas de panne
Témoin	■ Clone léger du nœud actif ■ Fournit un quorum afin d'assurer une protection en cas de division

Configurations matérielle et logicielle requises de vCenter HA

Avant de configurer vCenter HA, assurez-vous que vous disposez de suffisamment de ressources de mémoire, de CPU et de banques de données. Assurez-vous également que vous utilisez des versions de vCenter Server et ESXi qui prennent en charge vCenter HA.

Votre environnement doit répondre aux exigences suivantes.

Tableau 4-2. Configuration requise de vCenter HA

Composant	Configuration requise
ESXi	■ ESXi 6.0 ou version plus récente est requis. ■ Un minimum de trois hôtes ESXi est fortement recommandé. Chaque nœud vCenter HA peut ensuite s'exécuter sur un hôte différent pour une meilleure protection.
vCenter Serverde gestion (si utilisé)	Votre environnement peut inclure un système de gestion de vCenter Server ou vous pouvez configurer votre instance de vCenter Server pour gérer l'hôte de ESXi sur lequel elle s'exécute (vCenter Server à gestion automatique) ■ vCenter Server 6.0 ou version plus récente est requis.
vCenter Server	■ vCenter Server 6.5 ou version plus récente est requis. ■ Une taille de déploiement Petite (4 CPU et 16 Go de RAM) ou plus importante est requise pour atteindre l'objectif de temps de récupération. N'utilisez pas la version Minuscule dans les environnements de production. ■ vCenter HA est pris en charge et testé avec les banques de données VMFS, NFS et vSAN. ■ Assurez-vous que vous disposez d'un espace disque suffisant pour collecter et stocker les bundles de support de ces trois nœuds sur le nœud actif. Reportez-vous à la section Collecter des bundles de support pour un nœud vCenter HA.

Tableau 4-2. Configuration requise de vCenter HA (suite)

Composant	Configuration requise
Connexion réseau	■ La latence réseau de vCenter HA entre les nœuds actif, passif et témoin doit être inférieure à 10 ms. ■ Le réseau vCenter HA doit être sur un sous-réseau différent du réseau de gestion.
Gestion des licences requises pour vCenter HA	■ vCenter HA requiert une licence unique vCenter Server. ■ vCenter HA requiert une licence Standard.

Présentation du workflow de configuration dans vSphere Client

Vous pouvez utiliser l'assistant **Configurer vCenter HA** dans vSphere Client pour configurer les nœuds passifs et témoins. L'assistant **Configurer vCenter HA** crée automatiquement les nœuds passifs et témoins dans le cadre de la configuration de vCenter HA. Avec l'option manuelle, il vous incombe de cloner manuellement le nœud actif afin de créer les nœuds passifs et témoins.

Configuration automatique avec vSphere Client

Pour effectuer la configuration automatique, vous devez respecter l'une des exigences suivantes.

- L'instance de vCenter Server, qui deviendra le nœud actif, gère son propre hôte ESXi et sa propre machine virtuelle. Cette configuration de vCenter Server est parfois appelée gestion automatique.

Si vous respectez les exigences, le workflow automatique est le suivant.

1 L'utilisateur déploie le premier dispositif vCenter Server qui deviendra le nœud actif.

2 L'utilisateur ajoute un second réseau (groupe de ports) pour le trafic vCenter HA sur chaque hôte ESXi.

3 L'utilisateur commence à configurer vCenter HA et fournit les adresses IP, l'hôte ESXi cible ou le cluster, et la banque de données pour chaque clone.

4 Le système clone le nœud actif et crée un nœud passif ayant exactement les mêmes paramètres, y compris le même nom d'hôte.

5 Le système clone à nouveau le nœud actif et crée un nœud témoin plus léger.

6 Le système configure le réseau vCenter HA sur lequel les trois nœuds communiquent, par exemple en échangeant des signaux de pulsation et d'autres informations.

Configuration manuelle avec vSphere Client

Si vous souhaitez davantage de contrôle sur votre déploiement, vous pouvez effectuer une configuration manuelle. Avec cette option, il vous incombe de cloner vous-même le nœud actif dans le cadre de la configuration de vCenter HA. Si vous sélectionnez cette option et supprimez ultérieurement la configuration de vCenter HA, il vous incombe de supprimer les nœuds que vous avez créés.

Le workflow de l'option manuelle est le suivant.

1 L'utilisateur déploie le premier dispositif vCenter Server qui deviendra le nœud actif.

2 L'utilisateur ajoute un second réseau (groupe de ports) pour le trafic vCenter HA sur chaque hôte ESXi.

3 L'utilisateur doit ajouter un deuxième adaptateur réseau (NIC) au nœud actif si les informations d'identification de la gestion active vCenter Server sont inconnues.

4 L'utilisateur se connecte au dispositif vCenter Server (nœud actif) à l'aide de vSphere Client.

5 L'utilisateur démarre la configuration de vCenter HA, coche la case pour configurer manuellement et fournit les adresses IP et les informations de sous-réseau des nœuds passifs et témoins. Éventuellement, l'utilisateur peut remplacer les adresses IP de gestion du basculement.

6 L'utilisateur se connecte à l'instance vCenter Server de gestion et crée deux clones du dispositif vCenter Server (nœud actif).

7 Le système configure le réseau vCenter HA sur lequel les trois nœuds échangent des signaux de pulsation et des informations de réplication.

8 Le dispositif vCenter Server est protégé par vCenter HA.

Reportez-vous à Configurer vCenter HA avec vSphere Client pour plus de détails.

Configurer le réseau

Quelles que soient l'option de déploiement et la hiérarchie d'inventaire sélectionnée, vous devez définir votre réseau avant de commencer la configuration. Pour définir les fondations du réseau vCenter HA, vous ajoutez un groupe de ports à chaque hôte ESXi.

Une fois la configuration terminée, le cluster vCenter HA a deux réseaux, le réseau de gestion sur la première carte réseau virtuelle et le réseau vCenter HA sur la deuxième carte réseau virtuelle.

Réseau de gestion

Le réseau de gestion sert les demandes des clients (IP public). Les adresses IP du réseau de gestion doivent être statiques.

Réseau vCenter HA

Le réseau vCenter HA connecte les nœuds actif, passif et témoin et réplique l'état du serveur. Il surveille également les pulsations.

- Les adresses IP du réseau vCenter HA pour les nœuds actif, passif et témoin doivent être statiques.
- Le réseau vCenter HA doit être sur un sous-réseau différent du réseau de gestion. Les trois nœuds peuvent être sur le même sous-réseau ou sur des sous-réseaux différents.
- La latence du réseau entre les nœuds actif, passif et témoin doit être inférieure à 10 millisecondes.

- Vous ne devez pas ajouter d'entrée de passerelle par défaut pour le réseau du cluster.

Conditions préalables

- vCenter Server qui devient ensuite le nœud actif, est déployé.
- Vous pouvez y accéder et disposez des privilèges de modification de vCenter Server et de l'hôte ESXi sur lequel il s'exécute.
- Pendant la configuration du réseau, vous devez utiliser des adresses IP statiques pour le réseau de gestion. Les adresses des réseaux de gestion et du cluster doivent être de type IPv4 ou IPv6. Les adresses IP du mode ne peuvent pas être mélangées.

Procédure

1. Connectez-vous au vCenter Server de gestion et trouvez l'hôte ESXi sur lequel le nœud actif s'exécute.
2. Ajoutez un groupe de ports à l'hôte ESXi.

   Ce groupe de ports peut figurer sur un commutateur virtuel existant ou, pour une meilleure isolation réseau, vous pouvez créer un nouveau commutateur virtuel. Il doit être différent du réseau de gestion.
3. Si votre environnement inclut les trois hôtes ESXi recommandés, ajoutez le groupe de ports à chacun des hôtes.

Configurer vCenter HA avec vSphere Client

Lorsque vous utilisez vSphere Client, l'assistant **Configurer vCenter HA** crée et configure un deuxième adaptateur réseau sur vCenter Server, clone le nœud actif et configure le réseau vCenter HA.

Conditions préalables

- Déployez l'instance de vCenter Server à utiliser en tant que nœud Actif initial.
  - vCenter Server doit avoir une adresse IP statique.
  - Le mode SSH doit être activé sur vCenter Server.
- Vérifiez que votre environnement respecte les exigences suivantes :
  - L'instance de vCenter Server, qui deviendra le nœud actif, gère son propre hôte ESXi et sa propre machine virtuelle. Cette configuration de vCenter Server est parfois appelée gestion automatique.
- Configurez l'infrastructure du réseau vCenter HA. Reportez-vous à la section Configurer le réseau.

- Identifiez les adresses IP statiques à utiliser pour les deux nœuds vCenter Server qui deviendront les nœuds passif et témoin.

Note Pour utiliser un segment NSX-T sur le nœud actif, vous devez créer NIC2/eth1 à l'aide de l'option **Modifier les paramètres de la VM** pour ajouter la deuxième carte réseau avec le segment NSX-T. Vous n'avez pas besoin de spécifier de ressources pour les nœuds passifs ou témoins, car le clone doit être créé à l'aide de l'option **Cloner la VM** après avoir ajouté les spécifications de personnalisation d'invité nécessaires pour les nœuds passifs et témoins contenant NIC1/eth0 et NIC2/eth1 avec des adresses IP. Lorsque vous configurez des adresses IP VCHA pour eth1 dans l'instance de vCenter Server, eth1 sur le nœud actif est automatiquement renseigné.

Procédure

1. Connectez-vous au nœud actif à l'aide de vSphere Client.
2. Sélectionnez l'objet vCenter Server dans l'inventaire et sélectionnez l'onglet **Configurer**.
3. Sélectionnez **vCenter HA** sous les paramètres.
4. Cliquez sur le bouton **Configurer vCenter HA** pour démarrer l'assistant de configuration.
   - Si l'instance de vCenter Server est à gestion automatique, la page **Paramètres de ressource** s'affiche. Passez à l'étape 7.
   - Si votre instance de vCenter Server est gérée par une autre instance de vCenter Server dans le même domaine SSO, passez à l'étape 7.
   - Si votre instance de vCenter Server est gérée par une autre instance de vCenter Server dans un domaine SSO différent, saisissez l'emplacement et les informations d'identification de l'instance de vCenter Server de gestion.
5. Cliquez sur **Informations d'identification de l'instance de vCenter Server de gestion**. Indiquez le nom de domaine complet ou l'adresse IP de l'instance de vCenter Server de gestion, un nom d'utilisateur et un mot de passe Single Sign-On, puis cliquez sur **Suivant**.

   Si vous n'avez pas les informations d'identification de l'administrateur Single Sign-On, sélectionnez la deuxième puce et cliquez sur **Suivant**.
6. Vous pouvez voir qu'un **Avertissement de certificat** est affiché. Vérifiez l'empreinte SHA1 et sélectionnez **Oui** pour continuer.
7. Dans la section **Paramètres de ressource**, sélectionnez tout d'abord le réseau vCenter HA du nœud actif dans le menu déroulant.

   Note Le sélecteur de réseau n'est plus visible une fois NIC2/eth1 créé.
8. Cochez la case si vous souhaitez créer automatiquement des clones pour les nœuds passif et témoin.

   Note Si vous ne cochez pas la case, vous devez créer manuellement des clones pour les nœuds passifs et témoins après avoir cliqué sur **Terminer**.

9 Pour le nœud passif, cliquez sur **Modifier**.

   a Spécifiez un nom unique et un emplacement cible.

   b Sélectionnez la ressource de calcul de destination pour l'opération.

   c Sélectionnez la banque de données dans laquelle stocker les fichiers de configuration et de disque.

   d Sélectionnez le réseau de gestion des machines virtuelles (NIC 0) et le réseau vCenter HA (NIC 1).

   Si vos sélections provoquent des difficultés, des erreurs ou des avertissements de compatibilité s'affichent.

   e Passez vos sélections en revue et cliquez sur **Terminer**.

10 Pour le nœud témoin, cliquez sur **Modifier**.

   a Spécifiez un nom unique et un emplacement cible.

   b Sélectionnez la ressource de calcul de destination pour l'opération.

   c Sélectionnez la banque de données dans laquelle stocker les fichiers de configuration et de disque.

   d Sélectionnez le réseau vCenter HA (NIC 1).

   Si vos sélections provoquent des difficultés, des erreurs ou des avertissements de compatibilité s'affichent.

   e Passez vos sélections en revue et cliquez sur **Terminer**.

11 Cliquez sur **Suivant**.

12 Dans la section **Paramètres IP**, sélectionnez la version IP dans le menu déroulant.

13 Remplissez les champs Adresse IPv4 (NIC 1) et Masque de sous-réseau ou longueur de préfixe pour les nœuds actif, passif et témoin.

   Vous pouvez modifier les paramètres du réseau de gestion pour le nœud passif. La modification de ces paramètres est facultative. Par défaut, les paramètres du réseau de gestion du nœud actif sont appliqués.

14 Cliquez sur **Terminer**.

Résultats

Les nœuds passif et témoin sont créés. Lorsque vous avez terminé de **configurer vCenter HA**, vCenter Server dispose d'une protection haute disponibilité. Une fois que vCenter HA est activé, vous pouvez cliquer sur **Modifier** pour passer en mode de maintenance, activer ou désactiver vCenter HA. Il existe d'autres boutons pour supprimer vCenter HA ou initier le basculement vCenter HA.

Étape suivante

Reportez-vous à Gérer la configuration vCenter HA pour consulter la liste des tâches de gestion de cluster.

Pour une brève présentation des améliorations apportées à vSphere Client lorsque vous utilisez vCenter HA, consultez la section :

 (Améliorations apportées à l'utilisation de vCenter HA dans vSphere Client)

Gérer la configuration vCenter HA

Après avoir configuré votre cluster vCenter HA, vous pouvez effectuer les tâches de gestion. Ces tâches incluent le remplacement de certificats, le remplacement des clés SSH et la configuration SNMP. Vous pouvez également modifier la configuration du cluster pour désactiver ou activer vCenter HA, passer en mode de maintenance et supprimer la configuration du cluster.

- Configurer des interruptions SNMP

  Vous pouvez configurer des interruptions SNMP (Simple Network Management Protocol) de manière à recevoir des notifications SNMP pour votre cluster vCenter HA.

- Configurer votre environnement pour utiliser des certificats personnalisés

  Le certificat SSL de la machine sur chaque nœud est utilisé pour la communication en matière de gestion du cluster et pour le chiffrement du trafic de réplication. Si vous souhaitez utiliser des certificats personnalisés, vous devez supprimer la configuration vCenter HA, supprimer les nœuds passif et témoin, provisionner le nœud actif avec le certificat personnalisé et reconfigurer le cluster.

- Gérer les clés SSH de vCenter HA

  vCenter HA utilise les clés SSH pour l'authentification sans mot de passe sur les nœuds actif, passif et témoin. L'authentification s'applique pour l'échange des signaux de pulsation et la réplication de fichiers et de données. Pour remplacer les clés SSH dans les nœuds d'un cluster vCenter HA, vous désactivez le cluster, générez de nouvelles clés SSH sur le nœud actif, transférez les clés vers le nœud passif et activez le cluster.

- Initier le basculement de vCenter HA

  Vous pouvez initier manuellement un basculement et faire en sorte que le nœud passif devienne le nœud actif.

- Modifier la configuration d'un cluster vCenter HA

  Lorsque vous modifiez la configuration du cluster vCenter HA, vous pouvez désactiver ou activer le cluster, placer le cluster en mode de maintenance ou supprimer le cluster.

- Effectuer des opérations de sauvegarde et de restauration

  Pour une sécurité supplémentaire, vous pouvez sauvegarder le nœud actif dans le cluster vCenter HA. Vous pouvez ensuite restaurer le nœud en cas de panne catastrophique.

- Supprimer une configuration de vCenter HA

  Vous pouvez supprimer une configuration de vCenter HA de vSphere Client.
- Redémarrer tous les nœuds vCenter HA

  Si vous devez arrêter et redémarrer tous les nœuds dans le cluster, vous devez suivre un ordre spécifique pour l'arrêt afin d'empêcher le nœud passif d'assumer le rôle du nœud actif.
- Modifier l'environnement du serveur

  Lorsque vous déployez un dispositif vCenter Server, vous sélectionnez un environnement. Pour vCenter HA, Petit, Moyen, Grand et Très grand sont pris en charge pour les environnements de production. Si vous avez besoin de plus d'espace et souhaitez modifier l'environnement, vous devez supprimer la machine virtuelle du nœud passif avant de modifier la configuration.
- Collecter des bundles de support pour un nœud vCenter HA

  Collecter un bundle de support à partir de tous les nœuds d'un cluster vCenter HA aide à dépanner les problèmes.

Configurer des interruptions SNMP

Vous pouvez configurer des interruptions SNMP (Simple Network Management Protocol) de manière à recevoir des notifications SNMP pour votre cluster vCenter HA.

Les interruptions sont définies par défaut sur SNMP version 1.

Configurez les interruptions SNMP pour le nœud actif et le nœud passif. Vous indiquez à l'agent où envoyer les interruptions associées en ajoutant une entrée cible à la configuration snmpd.

Procédure

1. Connectez-vous au nœud actif en utilisant la console de machine virtuelle ou les clés SSH.
2. Exécutez la commande `vicfg-snmp`, par exemple :

   ```
   vicfg-snmp -t 10.160.1.1@1166/public
   ```

   Dans cet exemple, `10.160.1.1` est l'adresse d'écoute du client, `1166` est le port d'écoute du client et `public` est la chaîne de la communauté.
3. Activez l'agent SNMP (snmpd) en exécutant la commande suivante.

   ```
   vicfg-snmp -e
   ```

Étape suivante

Les commandes suivantes peuvent également être utiles.

- Pour accéder à l'aide complète concernant cette commande, exécutez **`vicfg-snmp -h`**.
- Pour désactiver l'agent SNMP, exécutez **`vicfg-snmp -D`**.

- Pour afficher la configuration de l'agent SNMP, exécutez **`vicfg-snmp -s`**.
- Pour rétablir la configuration par défaut, exécutez **`vicfg-snmp -r`**.

Configurer votre environnement pour utiliser des certificats personnalisés

Le certificat SSL de la machine sur chaque nœud est utilisé pour la communication en matière de gestion du cluster et pour le chiffrement du trafic de réplication. Si vous souhaitez utiliser des certificats personnalisés, vous devez supprimer la configuration vCenter HA, supprimer les nœuds passif et témoin, provisionner le nœud actif avec le certificat personnalisé et reconfigurer le cluster.

Si possible, remplacez les certificats dans vCenter Server qui deviendra le nœud actif, avant de procéder au clonage du nœud.

Procédure

1. Modifiez la configuration du cluster et sélectionnez **Supprimer**.
2. Supprimez le nœud passif et le nœud témoin.
3. Sur le nœud actif, qui est désormais un système vCenter Server autonome, remplacez le certificat SSL de la machine par un certificat personnalisé.
4. Reconfigurez le cluster.

Gérer les clés SSH de vCenter HA

vCenter HA utilise les clés SSH pour l'authentification sans mot de passe sur les nœuds actif, passif et témoin. L'authentification s'applique pour l'échange des signaux de pulsation et la réplication de fichiers et de données. Pour remplacer les clés SSH dans les nœuds d’un cluster vCenter HA, vous désactivez le cluster, générez de nouvelles clés SSH sur le nœud actif, transférez les clés vers le nœud passif et activez le cluster.

Procédure

1. Éditez le cluster et définissez son mode sur **Désactivé**.
2. Connectez-vous au nœud actif en utilisant la console de machine virtuelle ou les clés SSH.
3. Activez l’interpréteur de commandes de dépistage.

   ```
   bash
   ```

4. Exécutez la commande suivante pour générer de nouvelles clés SSH sur le nœud actif.

   ```
   /usr/lib/vmware-vcha/scripts/resetSshKeys.py
   ```

5. Utilisez SCP pour copier les clés sur les nœuds passif et témoin.

   ```
   scp /vcha/.ssh/*
   ```

6 Modifiez la configuration du cluster et définissez le cluster vCenter HA sur **Activé**.

Initier le basculement de vCenter HA

Vous pouvez initier manuellement un basculement et faire en sorte que le nœud passif devienne le nœud actif.

Un cluster vCenter HA prend en charge deux types de basculement.

Basculement automatique

Le nœud passif tente de prendre le relais du nœud actif en cas de panne de celui-ci.

Basculement manuel

L'utilisateur peut forcer un nœud passif à prendre le relais du nœud actif en utilisant l'action Initier le basculement.

Initiez un basculement manuel à des fins de dépannage et de test.

Procédure

1 Connectez-vous au nœud actif de vCenter Server avec vSphere Client et cliquez sur **Configurer** pour le vCenter Server sur lequel vous devez initier le basculement.

2 Dans **Paramètres**, sélectionnez **vCenter HA** et cliquez sur **Initier le basculement**.

3 Cliquez sur **Oui** pour déclencher le basculement.

Une boîte de dialogue qui s'ouvre vous permet de forcer un basculement sans synchronisation. Dans la plupart des cas, il est recommandé d'effectuer tout d'abord la synchronisation.

4 Après le basculement, vous pouvez vérifier que le nœud passif joue le rôle du nœud actif dans vSphere Client.

Modifier la configuration d'un cluster vCenter HA

Lorsque vous modifiez la configuration du cluster vCenter HA, vous pouvez désactiver ou activer le cluster, placer le cluster en mode de maintenance ou supprimer le cluster.

Le mode de fonctionnement d'un dispositif vCenter Server contrôle les capacités de basculement et la réplication de l'état dans un cluster vCenter HA.

Un cluster vCenter HA peut fonctionner dans l'un des modes suivants.

Tableau 4-3. Modes de fonctionnement d'un cluster vCenter HA

Mode	Basculement automatique	Basculement manuel	Réplication	
Activé	Oui	Oui	Oui	Ce mode de fonctionnement par défaut protège le dispositif vCenter Server des défaillances matérielles et logicielles en effectuant un basculement automatique.
Maintenance	Non	Oui	Oui	Utilisé pour les tâches de maintenance. Pour les autres tâches, vous devez désactiver vCenter HA.
Désactivé	Non	Non	Non	Si les nœuds passif et témoin sont perdus ou restaurés suite à une panne, la configuration de vCenter HA peut être désactivée. Le nœud actif continue à s'exécuter en tant que nœud vCenter Server autonome.

Note Si le cluster fonctionne en mode de maintenance ou Désactivé, un nœud actif peut continuer à desservir les requêtes du client même si les nœuds passif et témoin sont perdus ou inaccessibles.

Conditions préalables

Vérifiez que le cluster vCenter HA est déployé et contient les nœuds actif, passif et témoin.

Procédure

1. Connectez-vous au nœud actif vCenter Server à l'aide de vSphere Client et cliquez sur **Configurer**.
2. Sous **Paramètres**, sélectionnez **vCenter HA** et cliquez sur **Modifier**.
3. Sélectionnez l'une des options.

Option	Résultat
Activer vCenter HA	Active la réplication entre les nœuds actif et passif. Si l'état du cluster est sain, votre nœud actif est protégé par le basculement automatique du nœud passif.
Mode maintenance	En mode de maintenance, la réplication est toujours effectuée entre les nœuds actif et passif. Toutefois, le basculement automatique est désactivé.
Désactiver vCenter HA	Désactive la réplication et le basculement. Conserve la configuration du cluster. Vous pourrez ensuite activer vCenter HA à nouveau.
Supprimer le cluster vCenter HA	Supprime le cluster. La réplication et le basculement ne sont plus fournis. Le nœud actif continue à s'exécuter en tant que nœud vCenter Server autonome. Reportez-vous à Supprimer une configuration de vCenter HA pour plus de détails.

4 Cliquez sur OK.

Effectuer des opérations de sauvegarde et de restauration

Pour une sécurité supplémentaire, vous pouvez sauvegarder le nœud actif dans le cluster vCenter HA. Vous pouvez ensuite restaurer le nœud en cas de panne catastrophique.

Note Supprimez la configuration du cluster avant de restaurer le nœud actif. Les résultats sont imprévisibles si vous restaurez le nœud actif alors que le nœud passif est toujours en cours d'exécution ou qu'une autre configuration de cluster est toujours en place.

Conditions préalables

Vérifiez l'interopérabilité de vCenter HA et de la solution de sauvegarde et de restauration. Une solution est la restauration de vCenter Server basée sur un fichier.

Procédure

1 Sauvegardez le nœud actif.

   Ne sauvegardez pas le nœud passif et le nœud témoin.

2 Avant de restaurer le cluster, mettez hors tension et supprimez tous les nœuds vCenter HA.

3 Restaurez le nœud actif.

   Le nœud actif est restauré en tant que dispositif vCenter Server autonome.

4 Reconfigurez vCenter HA.

Supprimer une configuration de vCenter HA

Vous pouvez supprimer une configuration de vCenter HA de vSphere Client.

Procédure

1 Connectez-vous au nœud actif vCenter Server et cliquez sur **Configurer**.

2 Dans la section **Paramètres**, sélectionnez **vCenter HA** et cliquez sur **Supprimer VCHA**.

- La configuration du cluster vCenter HA est supprimée des nœuds actif, passif et témoin.
- Vous pouvez choisir de supprimer les nœuds passif et témoin.
- Le nœud actif continue à s'exécuter en tant que nœud vCenter Server autonome.
- Vous ne pouvez pas réutiliser les nœuds passif et témoin dans une nouvelle configuration de vCenter HA.
- Si vous effectuez une configuration manuelle, ou si les nœuds passif et témoin ne sont pas détectables, vous devez supprimer ces nœuds explicitement.
- Même si la seconde carte réseau virtuelle a été ajoutée par le processus de configuration, le processus de suppression ne supprime pas la carte réseau virtuelle.

Redémarrer tous les nœuds vCenter HA

Si vous devez arrêter et redémarrer tous les nœuds dans le cluster, vous devez suivre un ordre spécifique pour l'arrêt afin d'empêcher le nœud passif d'assumer le rôle du nœud actif.

Procédure

1. Arrêtez les nœuds dans cet ordre.
   - Nœud passif
   - Nœud actif
   - Nœud témoin
2. Redémarrez chaque nœud.

   Vous pouvez redémarrer les nœuds dans n'importe quel ordre.
3. Vérifiez que tous les nœuds joignent le cluster correctement et que le nœud actif précédent reprend ce rôle.

Modifier l'environnement du serveur

Lorsque vous déployez un dispositif vCenter Server, vous sélectionnez un environnement. Pour vCenter HA, Petit, Moyen, Grand et Très grand sont pris en charge pour les environnements de production. Si vous avez besoin de plus d'espace et souhaitez modifier l'environnement, vous devez supprimer la machine virtuelle du nœud passif avant de modifier la configuration.

Procédure

1. Connectez-vous au nœud actif avec vSphere Client, modifiez la configuration du cluster, puis sélectionnez **Désactiver**.
2. Supprimez la machine virtuelle du nœud passif.
3. Modifiez la configuration vCenter Server du nœud actif (par exemple, d'un environnement petit à un environnement moyen).
4. Reconfigurez vCenter HA.

Collecter des bundles de support pour un nœud vCenter HA

Collecter un bundle de support à partir de tous les nœuds d'un cluster vCenter HA aide à dépanner les problèmes.

Lorsque vous collectez un bundle de support sur le nœud actif d'un cluster vCenter HA, le système procède de la façon suivante.

- Il collecte les informations du bundle de support directement sur le nœud actif.

- Il collecte des bundles de support depuis les nœuds passif et témoin, et les place dans le répertoire `commands` du bundle de support du nœud actif.

Note La collecte des bundles de support sur les nœuds passif et témoin se fait dans la mesure du possible et ne peut avoir lieu que si les nœuds sont atteignables.

Corriger votre environnement vCenter HA

En cas de problème, vous pouvez corriger votre environnement. La tâche que vous devez effectuer dépend des symptômes de la défaillance. Pour en savoir plus sur le dépannage, reportez-vous au système de la base de connaissances VMware.

- L'opération de clonage de vCenter HA échoue lors du déploiement

  Si le processus de configuration de vCenter HA ne parvient pas à créer le clone, vous devez résoudre cette erreur de clonage.

- Redéployer le nœud passif ou témoin

  Si le nœud passif ou témoin échoue et que le cluster vCenter HA a été configuré à l'aide de la méthode de clonage automatique, vous pouvez le redéployer dans la page **Paramètres vCenter HA**.

- Le déploiement de vCenter HA échoue avec une erreur

  L'échec du déploiement peut s'expliquer par des problèmes de configuration et en particulier par des incidents lors de la configuration de la mise en réseau.

- Dépannage d'un cluster vCenter HA dégradé

  Pour qu'un cluster vCenter HA soit sain, chacun des nœuds actif, passif et témoin doivent être entièrement opérationnels et accessibles sur le réseau du cluster vCenter HA. En cas de panne d'un nœud, le cluster est considéré comme étant dans un état dégradé.

- Restauration de nœuds vCenter HA isolés

  Si tous les nœuds d'un cluster vCenter HA ne peuvent pas communiquer les uns avec les autres, le nœud actif cesse de desservir les requêtes du client.

- Résolution des défaillances suite à un basculement

  Lorsqu'un nœud passif ne devient pas un nœud actif lors d'un basculement, vous pouvez forcer le passage du nœud passif au nœud actif.

- Alarmes et événements de VMware vCenter® HA

  Si un cluster vCenter HA se trouve dans un état dégradé, les alarmes et événements affichent des erreurs.

L'opération de clonage de vCenter HA échoue lors du déploiement

Si le processus de configuration de vCenter HA ne parvient pas à créer le clone, vous devez résoudre cette erreur de clonage.

Problème

L'opération de clonage échoue.

Note Le clonage d'une machine virtuelle passive ou témoin dans la même banque de données NFS 3.1 en tant que machine virtuelle du nœud actif source échoue lors d'un déploiement VCHA. Vous devez utiliser NFS4 ou cloner les machines virtuelles passives et témoin dans une banque de données différente depuis la machine virtuelle active.

Cause

Recherchez l'exception de clone. Celle-ci peut indiquer l'un des problèmes suivants.

- Vous avez un cluster sur lequel DRS est activé, mais vous ne disposez pas de trois hôtes.
- La connexion à l'hôte ou à la base de données est perdue.
- L'espace disque est insuffisant.
- Autres erreurs **Cloner une machine virtuelle**

Solution

1. Corrigez l'erreur à l'origine de ce problème.
2. Supprimez le cluster, puis recommencez la configuration.

Redéployer le nœud passif ou témoin

Si le nœud passif ou témoin échoue et que le cluster vCenter HA a été configuré à l'aide de la méthode de clonage automatique, vous pouvez le redéployer dans la page **Paramètres vCenter HA**.

Procédure

1. Connectez-vous au nœud actif à l'aide de vSphere Client.
2. Sélectionnez l'objet vCenter Server dans l'inventaire et sélectionnez l'onglet **Configurer**.
3. Sélectionnez **vCenter HA** sous **Paramètres**.
4. Cliquez sur le bouton **REDÉPLOYER** en regard du nœud pour démarrer l'assistant de redéploiement.
5. - Si votre instance de vCenter Server est gérée par une autre instance de vCenter Server dans le même domaine SSO, passez à l'étape 6.
   - Si votre instance de vCenter Server est gérée par une autre instance de vCenter Server dans un domaine SSO différent, saisissez l'emplacement et les informations d'identification de l'instance de vCenter Server de gestion. Saisissez les informations pour les champs **Nom de domaine complet ou adresse IP du vCenter Server de gestion** et **Single Sign-On**.
6. Spécifiez un nom unique et un emplacement cible.

7 Sélectionnez la ressource de calcul de destination pour l'opération.

8 Sélectionnez la banque de données dans laquelle stocker les fichiers de configuration et de disque.

9 Configurez les réseaux de la machine virtuelle.

- Si vous redéployez le nœud passif, sélectionnez les réseaux Gestion des machines virtuelles (NIC 0) et vCenter HA (NIC 1).
- Si vous redéployez le nœud témoin, sélectionnez le réseau vCenter HA (NIC 1).

Si vos sélections provoquent des difficultés, des erreurs ou des avertissements de compatibilité s'affichent.

10 Vérifiez vos sélections et cliquez sur **Terminer** pour redéployer le nœud.

Le déploiement de vCenter HA échoue avec une erreur

L'échec du déploiement peut s'expliquer par des problèmes de configuration et en particulier par des incidents lors de la configuration de la mise en réseau.

Problème

Vous commencez la configuration d'un cluster vCenter HA, mais celle-ci échoue avec une erreur. L'erreur peut indiquer la cause du problème, par exemple, un message Échec de la connexion SSH peut s'afficher.

Solution

Si le déploiement échoue, prenez les mesures nécessaires pour résoudre les problèmes de réseau.

1 Vérifiez que les nœuds passif et témoin sont accessibles depuis le nœud actif.

2 Vérifiez que le routage entre les nœuds est configuré correctement.

3 Vérifiez le temps de réponse du réseau.

Dépannage d'un cluster vCenter HA dégradé

Pour qu'un cluster vCenter HA soit sain, chacun des nœuds actif, passif et témoin doivent être entièrement opérationnels et accessibles sur le réseau du cluster vCenter HA. En cas de panne d'un nœud, le cluster est considéré comme étant dans un état dégradé.

Problème

Si le cluster est dans un état dégradé, le basculement ne peut pas être effectué. Pour obtenir des informations sur les scénarios de panne lorsque le cluster est dans un état dégradé, reportez-vous à la section Résolution des défaillances suite à un basculement.

Cause

Le cluster peut être dans un état dégradé pour plusieurs raisons.

L'un des nœuds est défaillant

- En cas de panne du nœud actif, un basculement du nœud actif vers le nœud passif est effectué automatiquement. Une fois le basculement effectué, le nœud passif devient le nœud actif.

  Le cluster est alors dans un état dégradé car le nœud actif d'origine n'est pas disponible.

  Après que le nœud défaillant a été rétabli ou mis en ligne, il devient le nouveau nœud passif et le cluster redevient sain une fois que les nœuds actif et passif ont été synchronisés.
- En cas de panne du nœud passif, le nœud actif continue à fonctionner, mais aucun basculement n'est possible et le cluster est dans un état dégradé.

  Si le nœud passif est rétabli ou mis en ligne, il rejoint automatiquement le cluster et l'état de celui-ci est sain une fois que les nœuds actif et passif ont été synchronisés.
- En cas de panne du nœud témoin, le nœud actif continue à fonctionner et la réplication entre les nœuds actif et passif continue, mais aucun basculement ne peut être effectué.

  Si le nœud témoin est rétabli ou mis en ligne, il rejoint automatiquement le cluster et l'état de celui-ci est sain.

La réplication de la base de données échoue

En cas d'échec de la réplication entre les nœuds actif et passif, le cluster est considéré comme étant dégradé. Le nœud actif continue de se synchroniser avec le nœud passif. S'il réussit, le cluster redevient sain. Cet état peut être du à des problèmes au niveau de la bande passante du réseau ou à d'autres manques de ressources.

Problèmes de réplication du fichier de configuration

Si les fichiers de configuration ne sont pas correctement répliqués entre le nœud actif et le nœud passif, le cluster est dans un état dégradé. Le nœud actif continue de tenter de se synchroniser avec le nœud passif. Cet état peut être du à des problèmes au niveau de la bande passante du réseau ou à d'autres manques de ressources.

Solution

La manière de résoudre ce problème dépend de l'origine de l'état de dégradation du cluster. Si le cluster se trouve dans un état dégradé, des événements, des alarmes et des interruptions SNMP affichent des erreurs.

Si l'un des nœuds est en panne, recherchez une éventuelle défaillance matérielle ou une isolation de réseau. Vérifiez si le nœud défaillant est mis sous tension.

En cas de défaillance de la réplication, vérifiez si le réseau vCenter HA dispose d'une bande passante suffisante et assurez-vous que la latence réseau est de 10 ms ou moins.

Restauration de nœuds vCenter HA isolés

Si tous les nœuds d'un cluster vCenter HA ne peuvent pas communiquer les uns avec les autres, le nœud actif cesse de desservir les requêtes du client.

Problème

L'isolation des nœuds est un problème de connectivité réseau.

Solution

1. Essayez de résoudre le problème de connectivité. Si vous parvenez à restaurer la connectivité, les nœuds isolés rejoignent le cluster automatiquement et le nœud actif commence à desservir les requêtes du client.
2. Si vous ne parvenez pas à résoudre le problème de connectivité, vous devez vous connecter directement à la console du nœud actif.
   a. Mettez les machines virtuelles des nœuds passif et actif hors tension, puis supprimez-les.
   b. Connectez-vous au nœud actif en utilisant SSH ou par l'intermédiaire de la console de la machine virtuelle.
   c. Pour activer le shell Bash, entrez **`shell`** à l'invite `appliancesh`.
   d. Exécutez la commande suivante pour supprimer la configuration de vCenter HA.

      ```
      vcha-destroy -f
      ```

   e. Redémarrez le nœud actif.

      Le nœud actif est désormais une instance autonome de vCenter Server.

   f. Procédez de nouveau à la configuration du cluster vCenter HA.

Résolution des défaillances suite à un basculement

Lorsqu'un nœud passif ne devient pas un nœud actif lors d'un basculement, vous pouvez forcer le passage du nœud passif au nœud actif.

Problème

Le nœud passif échoue lorsqu'il tente d'assurer le rôle du nœud actif.

Cause

Un basculement vCenter HA peut échouer pour les raisons suivantes.

- Le nœud témoin devient indisponible alors que le nœud passif tente d'assurer le rôle du nœud actif.
- Il existe un problème de synchronisation de l'état du serveur entre les nœuds.

Solution

Vous pouvez résoudre ce problème de la manière suivante.

1 Si le nœud actif récupère de la défaillance, il redevient le nœud actif.

2 Si le nœud témoin récupère de la défaillance, suivez les étapes ci-dessous.

   a Connectez-vous au nœud passif via la console de la machine virtuelle.

   b Pour activer le shell Bash, entrez **`shell`** à l'invite `appliancesh`.

   c Exécutez la commande suivante.

   ```
   vcha-reset-primary
   ```

   d Redémarrez le nœud passif.

3 Si le nœud actif et le nœud témoin ne peuvent pas récupérer de la défaillance, vous pouvez forcer le passage du nœud passif à une instance autonome de vCenter Server.

   a Supprimez les machines virtuelles du nœud actif et du nœud témoin.

   b Connectez-vous au nœud passif via la console de la machine virtuelle.

   c Pour activer le shell Bash, entrez **`shell`** à l'invite `appliancesh`.

   d Exécutez la commande suivante.

   ```
   vcha-destroy
   ```

   e Redémarrez le nœud passif.

Alarmes et événements de VMware vCenter® HA

Si un cluster vCenter HA se trouve dans un état dégradé, les alarmes et événements affichent des erreurs.

Problème

Tableau 4-4. Les événements suivants déclencheront l'alarme de santé VCHA dans vpxd :

Nom de l'événement	Description de l'événement	Type d'événement	Catégorie
L'état actuel du cluster vCenter HA est sain	L'état actuel du cluster vCenter HA est sain	com.vmware.vcha.cluster.state.healthy	info
L'état actuel du cluster vCenter HA est dégradé	L'état actuel du cluster vCenter HA est dégradé	com.vmware.vcha.cluster.state.degraded	avertissement
L'état actuel du cluster vCenter HA est isolé	L'état actuel du cluster vCenter HA est isolé	com.vmware.vcha.cluster.state.isolated	erreur
Le cluster vCenter HA est détruit	Le cluster vCenter HA est détruit	com.vmware.vcha.cluster.state.destroyed	info

Tableau 4-5. Les événements suivants déclencheront l'alarme de santé PSC HA dans vpxd :

Nom de l'événement	Description de l'événement	Type d'événement	Catégorie
L'état actuel de PSC HA est sain	L'état actuel de PSC HA est sain	com.vmware.vcha.psc.ha.health.healthy	info
L'état actuel de PSC HA est dégradé	L'état actuel de PSC HA est dégradé	com.vmware.vcha.psc.ha.health.degraded	info
PSC HA n'est plus surveillé une fois que le cluster vCenter HA est détruit	L'état de PSC HA n'est pas surveillé	com.vmware.vcha.psc.ha.health.unknown	info

Tableau 4-6. Événements connexes à l'état du cluster

Nom de l'événement	Description de l'événement	Type d'événement	Catégorie
Le nœud {nodeName} a rejoint le cluster	Un seul nœud a rejoint le cluster	com.vmware.vcha.node.joined	info
Le nœud {nodeName} a quitté le cluster	Un seul nœud a quitté le cluster	com.vmware.vcha.node.left	avertissement
Basculement réussi	Basculement réussi	com.vmware.vcha.failover.succeeded	info
Le basculement ne peut pas continuer lorsque le cluster est en mode désactivé	Le basculement ne peut pas continuer lorsque le cluster est en mode désactivé	com.vmware.vcha.failover.failed.disabled.mode	avertissement
Le basculement ne peut pas continuer lorsque le cluster ne dispose pas des trois nœuds connectés	Le basculement ne peut pas continuer lorsque le cluster ne dispose pas des trois nœuds connectés	com.vmware.vcha.failover.failed.node.lost	avertissement
Le basculement ne peut pas continuer lorsque vPostgres sur le nœud passif n'est pas prêt pour la prise en charge	Le basculement ne peut pas continuer lorsque le nœud passif n'est pas prêt pour la prise en charge	com.vmware.vcha.failover.failed.passive.not.ready	avertissement
Le mode du cluster vCenter HA est passé à {clusterMode}	Le mode du cluster vCenter HA a été modifié	com.vmware.vcha.cluster.mode.changed	info

Tableau 4-7. Événements liés à la réplication de la base de données

Nom de l'événement	Description de l'événement	Type d'événement	Catégorie
Le mode de réplication de la base de données est passé à {newState}	L'état de réplication de la base de données a été modifié : synchrone, asynchrone ou aucune réplication	com.vmware.vcha.DB.replication.state.changed	info

Tableau 4-8. Événements liés à la réplication de fichiers

Nom de l'événement	Description de l'événement	Type d'événement	Catégorie
Le dispositif {fileProviderType} est {state}	L'état de réplication du fichier du dispositif a été modifié	com.vmware.vcha.file.replication.state.changed	info

Application de correctifs à un environnement vCenter High Availability

Vous pouvez appliquer un correctif à un dispositif vCenter Server situé dans un cluster vCenter High Availability à l'aide de l'utilitaire **`software-packages`** disponible dans l'interpréteur du dispositif vCenter Server.

Pour plus d'informations, reportez-vous à la section *Corriger un environnement vCenter High Availability* dans *Mise à niveau de vSphere*.