Disponibilidad de vSphere

Actualización 1
VMware vSphere 6.0
VMware ESXi 6.0
vCenter Server 6.0

Este documento admite la versión de todos los productos enumerados y admite todas las versiones posteriores hasta que el documento se reemplace por una edición nueva. Para buscar ediciones más recientes de este documento, consulte http://www.vmware.com/es/support/pubs.

ES-001810-00

vmware®

Puede encontrar la documentación técnica más actualizada en el sitio web de WMware en:

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

En el sitio web de VMware también están disponibles las últimas actualizaciones del producto.

Si tiene algún comentario sobre esta documentación, envíelo a la siguiente dirección de correo electrónico:

docfeedback@vmware.com

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

VMware, Inc.
Paseo de la Castellana 141. Planta 8.
28046 Madrid.
Tel.:+ 34 91 418 58 01
Fax: + 34 91 418 50 55
www.vmware.com/es

Contenido

Acerca de la disponibilidad de vSphere

La *Disponibilidad de vSphere* describe soluciones que ofrecen continuidad del negocio, incluido cómo establecer vSphere® High Availability (HA) y vSphere Fault Tolerance.

Audiencia prevista

La información es para cualquiera que desee proporcionar continuidad del negocio a través de las soluciones vSphere HA y Fault Tolerance. La información de este manual es para administradores expertos de los sistemas Windows y Linux que están familiarizados con la tecnología de máquinas virtuales y las operaciones de centro de datos.

Continuidad del negocio y minimización del tiempo de inactividad

1

El tiempo de inactividad, ya sea planificado o no planificado, acarrea costos considerables. Sin embargo, tradicionalmente las soluciones para asegurar mayores niveles de disponibilidad han sido costosas, difíciles de implementar y complicadas de administrar.

Con el software de VMware resulta más simple y menos costoso proporcionar mayores niveles de disponibilidad para aplicaciones importantes. Con vSphere, las organizaciones pueden aumentar fácilmente el nivel básico de disponibilidad proporcionado para todas las aplicaciones, así como ofrecer mayores niveles de disponibilidad de forma más fácil y rentable. Con vSphere, puede:

- Proporcionar mayor disponibilidad, independiente del hardware, del sistema operativo y de las aplicaciones.
- Reducir el tiempo de inactividad planificado para operaciones comunes de mantenimiento.
- Proporcionar la recuperación automática en caso de errores.

vSphere permite reducir el tiempo de inactividad planificado, evitar el tiempo de inactividad planificado y recuperarse rápidamente de interrupciones.

Este capítulo cubre los siguientes temas:

Reducir el tiempo de inactividad planificado

El tiempo de inactividad planificado suele representar más del 80 % del tiempo de inactividad del centro de datos. El mantenimiento de hardware, la migración de servidores y las actualizaciones de firmware requieren tiempo de inactividad de los servidores físicos. Para minimizar el impacto de este tiempo de inactividad, las organizaciones se ven obligadas a retrasar el mantenimiento hasta encontrarse con períodos de tiempo de inactividad inconvenientes y difíciles de programar.

vSphere permite que las organizaciones puedan reducir en gran medida el tiempo de inactividad planificado. Debido a que las cargas de trabajo en un entorno de vSphere se pueden mover de forma dinámica a servidores físicos diferentes sin tiempo de inactividad o interrupción de servicio, el mantenimiento de servidores se puede realizar sin que se requiera tiempo de inactividad para aplicaciones y servicios. Con vSphere, las organizaciones pueden:

- Eliminar el tiempo de inactividad de las operaciones de mantenimiento comunes.
- Eliminar ventanas de mantenimiento planificadas.

- Realizar mantenimiento en cualquier momento sin interrumpir a los usuarios y servicios.

La funcionalidad vSphere vMotion® y Storage vMotion en vSphere permiten que las organizaciones reduzcan el tiempo de inactividad planificado debido a que las cargas de trabajo en un entorno de VMware se pueden mover de forma dinámica a diferentes servidores o a un almacenamiento subyacente diferente sin interrupción del servicio. Los administradores pueden realizar operaciones de mantenimiento más rápidas y completamente transparentes, sin que se vean obligados a programar períodos de mantenimiento inconvenientes.

Evitar el tiempo de inactividad no planificado

Aunque los hosts ESXi proporcionan una robusta plataforma para ejecutar aplicaciones, las organización también deben protegerse contra el tiempo de inactividad no planificado debido a errores de hardware o aplicaciones. vSphere crea importantes capacidades en la infraestructura de centro de datos que puede ayudarle a prevenir tiempo de inactividad no planificado.

Estas capacidades de vSphere forman parte de infraestructura virtual y son transparentes para el sistema operativo y aplicaciones que se ejecutan en máquinas virtuales. Estas características las pueden configurar y utilizar todas las máquinas virtuales de un sistema físico, lo que reduce el costo y la complejidad que implica proporcionar mayor disponibilidad. Las capacidades clave están integradas en vSphere:

- Almacenamiento compartido. Elimina puntos únicos de error mediante el almacenamiento de archivos de máquina virtual en almacenamiento compartido, como SAN de canal de fibra o iSCSI, o NAS. El uso del reflejo de SAN y las características de replicación se pueden utilizar para mantener copias actualizadas de un disco virtual en sitios de recuperación ante desastres.
- Formación de equipos de interfaz de red. Ofrece tolerancia de errores de tarjetas de red individuales.
- Múltiples rutas alternativas. Tolera errores de ruta de almacenamiento.

Además de estas funcionalidades, las características de vSphere HA y Fault Tolerance pueden minimizar o eliminar el tiempo de inactividad no planificado proporcionando una recuperación rápida ante las interrupciones y una disponibilidad continua, respectivamente.

vSphere HA ofrece una rápida recuperación desde interrupciones

vSphere HA aprovecha varios hosts ESXi configurados como clúster para proporcionar una rápida recuperación desde interrupciones y alta disponibilidad rentable para aplicaciones que se ejecutan en máquinas virtuales.

vSphere HA protege la disponibilidad de aplicaciones de las siguientes formas:

- Protege contra error de un servidor mediante el reinicio de las máquinas virtuales en otros hosts dentro del clúster.
- Protege contra errores de aplicaciones mediante una supervisión continua de una máquina virtual y su restablecimiento en caso de que se detecte un error.
- Protege contra errores de accesibilidad al almacén de datos mediante el restablecimiento de máquinas virtuales afectadas en otros hosts que aún tienen acceso a sus almacenes de datos.
- Protege a máquinas virtuales contra aislamiento de la red mediante el restablecimiento de dichas máquinas en caso de que su host se aísle en la red de administración o de Virtual SAN. Esta protección se proporciona incluso si la red se ha particionado.

A diferencia de otras soluciones de clúster, vSphere HA proporciona la infraestructura para proteger todas las cargas de trabajo con la infraestructura:

- No necesita instalar software especial dentro de la aplicación o máquina virtual. Todas las cargas de trabajo cuentan con protección de vSphere HA. Después de configurar vSphere HA, no se requieren acciones para proteger nuevas máquinas virtuales. Están se encuentran protegidas automáticamente.

- Puede combinar vSphere HA con vSphere Distributed Resource Scheduler (DRS) para proteger contra errores y para proporcionar equilibrio de carga entre los hosts dentro de un clúster.

vSphere HA posee varias ventajas por sobre las soluciones de conmutación por error tradicionales:

Instalación mínima	Después de instalar un clúster de vSphere HA, todas las máquinas virtuales del clúster obtienen compatibilidad para conmutación por error sin una configuración adicional.
Menor costo e instalación de hardware	La máquina virtual actúa como un contenedor portátil para las aplicaciones y puede moverse entre hosts. Los administradores evitan configuraciones duplicadas para varias máquinas. Cuando usa vSphere HA, debe tener suficientes recursos para realizar conmutación por error en la cantidad de hosts que desea proteger con vSphere HA. Sin embargo, el sistema de vCenter Server administra automáticamente recursos y configura clústeres.
Mayor disponibilidad de aplicaciones	Cualquier aplicación que se ejecuta dentro de una máquina virtual tiene acceso a mayor disponibilidad. Debido a que la máquina virtual puede recuperarse de errores de hardware, todas las aplicaciones que se inician en el arranque tienen mayor disponibilidad sin que haya mayores necesidades informáticas, incluso si la aplicación no es en sí una aplicación en clúster. Mediante la supervisión y la respuesta a latidos de VMware Tools y el restablecimiento de máquinas virtuales sin capacidad de respuesta, protege contra fallas del sistema operativo invitado.
Integración de DRS y vMotion	Si hay error en un host y las máquinas virtuales se restablecen en otros hosts, DRS puede proporcionar recomendaciones de migración o migrar máquinas virtuales para asignación de recursos equilibrados. Si se produce error en uno o ambos hosts de origen y destino de una migración, vSphere HA puede ayudar a recuperarse de dicho error.

vSphere Fault Tolerance proporciona disponibilidad continua

vSphere HA ofrece un nivel de protección básico para sus máquinas virtuales mediante un reinicio de ellas en caso de un error del host. vSphere Fault Tolerance proporciona un mayor nivel de disponibilidad, permitiendo que los usuarios puedan proteger cualquier máquina virtual contra un error del host sin perder datos, transacciones o conexiones.

Fault Tolerance proporciona disponibilidad continua al asegurar que los estados de las máquinas virtuales principales y secundarias sean idénticos en cualquier punto de la ejecución de instrucciones de la máquina virtual.

Si se produce un error en el host que ejecuta la máquina virtual principal o en el que ejecuta la máquina virtual secundaria, se produce una conmutación por error inmediata y transparente. El host ESXi en funcionamiento se convierte de forma sencilla en el host de la máquina virtual principal sin perder conexiones de red ni transacciones en curso. Con una conmutación por error transparente, no hay pérdida de datos y las conexiones de red se mantienen. Después de producirse una conmutación por error transparente, reaparece una nueva máquina virtual secundaria y se vuelve a establecer redundancia. El proceso completo es transparente, está completamente automatizado y se produce aunque vCenter Server no esté disponible.

Crear y usar clústeres de vSphere HA 2

Los clústeres de vSphere HA permiten que una colección de hosts ESXi funcionen en conjunto, de manera que, como grupo, proporcionen mayores niveles de disponibilidad para máquinas virtuales de lo que puede proporcionar de forma individual cada host ESXi. Cuando planifique la creación y el uso de un nuevo clúster de vSphere HA, las opciones que seleccione afectarán la manera en que el clúster responde a los errores de los hosts o las máquinas virtuales.

Antes de crear un clúster de vSphere HA, debe saber cómo identifica vSphere HA los errores y el aislamiento de hosts y cómo responder a estas situaciones. También debe saber de qué forma funciona el control de admisión para que pueda elegir la directiva que se ajusta a sus necesidades de conmutación por error. Después de establecer un clúster, puede personalizar su comportamiento con opciones avanzadas y optimizar su rendimiento siguiendo estas prácticas recomendadas.

NOTA: Es posible que reciba un mensaje de error cuando intente usar vSphere HA. Para obtener información sobre los mensajes de error relacionados con vSphere HA, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/1033634.

Este capítulo cubre los siguientes temas:

Funciona vSphere HA

vSphere HA ofrece alta disponibilidad para máquinas virtuales agrupando en un clúster las máquinas virtuales y los hosts en los que residen. Se supervisan los hosts en el clúster y, en caso de un error, las máquinas virtuales en un host con errores se reinician en hosts alternativos.

Cuando se crea un clúster de vSphere HA, se elige un host único automáticamente como el host maestro. El host maestro se comunica con vCenter Server y supervisa el estado de todas las máquinas virtuales protegidas y de los hosts esclavos. Es posible que haya diferentes tipos de errores del host, y el host maestro debe detectar y corregir apropiadamente el error. El host maestro debe distinguir entre un host con errores y uno que está en una partición de red o que ha quedado aislado de la red. Para determinar el tipo de error, el host maestro utiliza la verificación de latidos de la red y del almacén de datos.

Clústeres de Sphere HA (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:vSphereHAClusters)

Hosts maestros y esclavos

Cuando agrega un host a un clúster de vSphere HA, se carga un agente al host que se configura para que se comunique con otros agentes del clúster. Cada host en el clúster funciona como host maestro o host esclavo.

Cuando vSphere HA está habilitado para un clúster, todos los hosts activos (aquellos que no están en modo de espera o mantenimiento ni están desconectados) participan en una elección para escoger el host maestro del clúster. El host que monta la mayor cantidad de almacenes de datos tiene una ventaja en la elección. Comúnmente, solo existe un host maestro por clúster y todos los otros hosts son esclavos. Si el host maestro genera errores, se apaga o se coloca en modo de espera o se quita del clúster, se mantiene una nueva elección.

El host maestro en un clúster tiene varias responsabilidades:

- Supervisar el estado de los hosts esclavos. Si un host esclavo genera errores o no se puede acceder a él, el host maestro identifica cuáles máquinas virtuales tienen que reiniciarse.
- Supervisar el estado de energía de todas las máquinas virtuales protegidas. Si una máquina virtual genera errores, el host maestro se asegura de que se reinicie. Mediante el uso de un motor de colocación local, el host maestro también determina dónde debe realizarse el reinicio.
- Administrar las listas de hosts del clúster y máquinas virtuales protegidas.
- Actuar como la interfaz de administración de vCenter Server con el clúster e informar el estado del clúster.

Los hosts esclavos contribuyen principalmente con el clúster ejecutando máquinas virtuales a nivel local, supervisando sus estados de tiempo de ejecución e informando actualizaciones de estado al host maestro. Un host maestro también puede ejecutar y supervisar máquinas virtuales. Tantos los hosts esclavos como los maestros implementan las características de supervisión de máquina virtual y de aplicaciones.

Una de las funciones que realiza el host maestro es orquestar reinicios de máquinas virtuales protegidas. Una máquina virtual se protege mediante un host maestro después de que vCenter Server observa que el estado de energía de la máquina virtual ha cambiado desde apagado o encendido en respuesta a una acción del usuario. El host maestro mantiene activa la lista de máquinas virtuales protegidas en los almacenes de datos del clúster. Un host maestro elegido recientemente utiliza esta información para determinar cuáles máquinas virtuales hay que proteger.

NOTA: Si desconecta un host de un clúster, todas las máquinas virtuales registradas en ese host quedan sin protección de vSphere HA.

Tipos y detección de errores de los hosts

El host maestro de un clúster de vSphere HA es el responsable de detectar el error de hosts esclavos. Según el tipo de error detectado, es posible que las máquinas virtuales que se ejecutan en los hosts necesiten someterse a conmutación por error.

En un clúster de vSphere HA, se detectan tres tipos de errores de hosts:

- Error: un host deja de funcionar.
- Aislamiento: un host se aísla de la red.
- Partición: un host pierde conectividad de red con el host maestro.

El host maestro supervisa la ejecución de los hosts esclavos en el clúster. Esta comunicación se realiza a través del intercambio de latidos de la red cada segundo. Cuando el host maestro deja de recibir estos latidos de un host esclavo, comprueba la ejecución del host antes de declarar que el host tiene errores. La comprobación de ejecución que realiza el host maestro se hace para determinar si el host esclavo está intercambiando latidos con uno de los almacenes de datos. Consulte "Latidos del almacén de datos," página 19. Igualmente, el host maestro comprueba si el host responde a los pings de ICMP enviados a sus direcciones IP de administración.

Si un host maestro no puede comunicarse directamente con el agente en un host esclavo, este host no responde a los pings de ICMP y el agente no emite latidos si considera que tiene errores. Las máquinas virtuales del host se reinician en hosts alternativos. Si dicho host esclavo intercambia latidos con un almacén de datos, el host maestro da por hecho que está en una partición de red o en una red aislada y por ello continúa supervisando el host y sus máquinas virtuales. Consulte "Particiones de red," página 19.

El aislamiento de la red del host se produce cuando un host sigue en ejecución, pero ya no puede observarse tráfico de los agentes de vSphere HA en la red de administración. Si un host deja de observar este tráfico, intenta hacer ping a las direcciones de aislamiento del clúster. Si esto también genera errores, el host se declara como aislado de la red.

El host maestro supervisa las máquinas virtuales que se están ejecutando en un host aislado, y si observa que se apagan y el host maestro es responsable de las máquinas virtuales, las reinicia.

NOTA: Si asegura que la infraestructura de la red es lo bastante redundante y que hay disponible todo el tiempo al menos una ruta de acceso de la red, entonces sería raro que ocurriera un aislamiento de la red del host.

Determinar respuestas a problemas del host

Si se produce un error en un host y es necesario reiniciar sus máquinas virtuales, puede controlar el orden en el cual se reinician mediante la configuración de prioridad de reinicio de máquinas virtuales. También puede configurar de qué forma responde vSphere HA si los hosts pierden conectividad de red de administración con otros hosts mediante el uso de la configuración de respuesta para el aislamiento del host. También se consideran otros factores cuando vSphere HA reinicia una máquina virtual después de un error.

La siguiente configuración se aplica a todas las máquinas virtuales en el clúster en caso de un error o aislamiento del host. También es posible configurar excepciones para máquinas virtuales específicas. Consulte "Personalizar una máquina virtual individual," página 41.

VM Restart Priority (Prioridad de reinicio de máquina virtual)

La prioridad de reinicio de máquina virtual determina el orden relativo en el cual las máquinas virtuales reciben recursos después de un error del host. Dichas máquinas virtuales se asignan a hosts con capacidad sin reservar, donde las máquinas virtuales con la mayor prioridad se colocan primero y se continúa con aquellas con menor prioridad hasta que, bien se hayan colocado todas las máquinas virtuales, bien no haya más capacidad del clúster disponible para cumplir con las reservas o la sobrecarga de memoria de las máquinas virtuales. A continuación, un host reinicia las máquinas virtuales que tiene asignadas en orden de prioridad. Si no hay suficientes recursos, vSphere HA espera que haya disponible más capacidad sin reservar (por ejemplo, debido a que un host vuelve a estar en línea) y luego vuelve a intentar la colocación de estas máquinas virtuales. Para reducir la posibilidad de que se produzca esta situación, configure el control de admisión de vSphere HA para reservar más recursos para errores. El control de admisión permite controlar cuánta capacidad del clúster reservan la máquinas virtuales, que no está disponible para cumplir con las reservas y sobrecarga de memoria de las máquinas virtuales en caso de que haya un error.

Los valores para esta configuración son Disabled (Deshabilitada), Low (Baja), Medium (Media), que es el valor predeterminado, y High (Alta). La característica de supervisión de máquinas virtuales y aplicaciones de vSphere HA pasa por alto la configuración Disabled (Deshabilitada), ya que esta característica protege a las máquinas virtuales contra errores a nivel de sistema operativo y no errores de máquina virtual. Cuando se produce un error a nivel de sistema operativo, vSphere HA reinicia el sistema operativo y la máquina virtual queda funcionando en el mismo host. Puede cambiar esta configuración para máquinas virtuales individuales.

NOTA: El restablecimiento de una máquina virtual provoca un reinicio en frío del sistema operativo invitado, pero no realiza el ciclo de energía de la máquina virtual.

La configuración de prioridad de reinicio para máquinas virtuales varía según las necesidades del usuario. Asigne una prioridad de reinicio mayor a las máquinas virtuales que proporcionen los servicios más importantes.

Por ejemplo, en caso de una aplicación de varios niveles, puede que tenga que clasificar asignaciones de acuerdo con las funciones alojadas en las máquinas virtuales.

- High (Alta). Servidores de base de datos que proporcionan datos para aplicaciones.
- Medium (Mediana). Servidores de aplicaciones que consumen datos en la base de datos y proporcionan resultados en páginas web.
- Low (Baja). Servidores web que reciben solicitudes de usuarios, transmiten las consultas a servidores de aplicaciones y devuelven los resultados a los usuarios.

Si se produce un error en un host, vSphere HA intenta registrar en un host activo las máquinas virtuales afectadas que estaban encendidas y que tienen una prioridad de reinicio de Disabled (Deshabilitada), o que estaban apagadas.

Host Isolation Response (Respuesta de aislamiento del host)

La respuesta para el aislamiento del host determina lo que ocurre cuando un host en un clúster de vSphere HA pierde sus conexiones de red de administración, pero sigue ejecutándose. Puede usar la respuesta para aislamiento para que vSphere HA apague máquinas virtuales que se ejecutan en un host aislado y las reinicie en un host que no está aislado. Las respuestas para aislamiento del host requiere que Host Monitoring Status (Estado de supervisión de hosts) esté habilitado. Si está deshabilitado, también se suspenden las respuestas para aislamiento del host. Un host determina que está aislado cuando no puede comunicarse con los agentes que se ejecutan en los otros, y no puede hacer ping a sus direcciones de aislamiento. Después, el host ejecuta su respuesta de aislamiento. Las respuestas son Power off and restart VMs (Apagar y reiniciar máquinas virtuales) o Shutdown and restart VMs (Desactivar y reiniciar máquinas virtuales). Puede personalizar esta propiedad para máquinas virtuales individuales.

NOTA: Si la configuración de prioridad de reinicio de una máquina virtual se establece en Disabled (Deshabilitada), no se realiza ninguna respuesta para aislamiento del host.

Para usar la configuración Shutdown and restart VMs (Desactivar y reiniciar máquina virtual), debe instalar VMware Tools en el sistema operativo invitado de la máquina virtual. La desconexión de la máquina virtual ofrece la ventaja de que mantiene su estado. Desconectar es mejor que apagar la máquina virtual, lo que no purga los cambios más recientes al disco ni confirma transacciones. Las máquinas virtuales que se encuentran en proceso de desconexión ya no pueden realizar conmutación por error mientras se lleva a cabo la desactivación. Las máquinas virtuales que no se han desactivado en 300 segundos o en el tiempo que se haya especificado en la opción avanzada `das.isolationshutdowntimeout`, se apagan.

Después de que crea un clúster de vSphere HA, puede anular la configuración predeterminada del clúster para Restart Priority (Prioridad de reinicio) y Isolation Response (Respuesta para aislamiento) para máquinas virtuales específicas. Dichas anulaciones son útiles para máquinas virtuales que se utilizan para tareas especiales. Por ejemplo, puede que las máquinas virtuales que proporcionan servicios de infraestructura como DNS o DHCP tengan que apagarse antes que otras máquinas virtuales en el clúster.

Cuando un host se aísla o se particiona desde un host maestro, y ese host maestro no puede comunicarse con él mediante almacenes de datos de latidos, se puede producir una condición de "cerebro dividido" de la máquina virtual. En esta situación, el host maestro no puede determinar que el host está activo y, por ello, lo declara inactivo. Luego, el host maestro intenta reiniciar las máquinas virtuales que están ejecutándose en el host aislado o particionado. Este intento se realiza correctamente si las máquinas virtuales siguen ejecutándose en el host aislado o particionado, y si ese host perdió acceso a los almacenes de datos de las máquinas virtuales cuando se aisló o particionó. Entonces, existe una condición de cerebro dividido, ya que hay dos instancias de la máquina virtual. Sin embargo, solo una instancia puede leer o escribir en los discos virtuales de la máquina virtual. Se puede usar máquina virtual Component Protection (Protección de componentes de la máquina virtual) para evitar esta condición de cerebro dividido. Cuando activa la VMCP con la configuración agresiva, supervisa la accesibilidad del almacén de datos de máquinas virtuales encendidas y desconecta aquellas que pierden acceso a sus almacenes de datos.

Para recuperarse de esta situación, ESXi genera una pregunta en la máquina virtual que ha perdido los bloqueos de discos para cuando el host salga del aislamiento y no pueda volver a adquirir dichos bloqueos. vSphere HA responde automáticamente a esta pregunta, lo que permite que la instancia de máquina virtual que perdió los bloqueos de discos se apague, con lo que queda solo la instancia que tiene los bloqueos de discos.

Factores que se consideran para reiniciar máquinas virtuales

Después de un error, el host maestro del clúster intenta reiniciar las máquinas virtuales afectadas mediante la identificación de un host que pueda encenderlas. Cuando se elige dicho host, el host maestro considera varios factores.

Accesibilidad de archivos	Antes de poder iniciar una máquina virtual, sus archivos deben estar accesibles desde uno de los hosts del clúster activo con el que el maestro puede comunicarse a través de la red
Compatibilidad de máquinas virtuales y hosts	Si hay hosts accesibles, la máquina virtual debe ser compatible con al menos uno de ellos. La compatibilidad establecida para una máquina virtual incluye el efecto de cualquier regla de afinidad Máquina virtual-Host requerida. Por ejemplo, si una regla solo permite que se ejecute una máquina virtual en dos hosts, se contempla su colocación en aquellos dos hosts.
Reservas de recursos	De los hosts en los que puede ejecutarse la máquina virtual, al menos uno debe tener suficiente capacidad sin reservar para cumplir con la sobrecarga de memoria de la máquina virtual y cualquier reserva de recursos. Se consideran cuatro tipos de reservas: CPU, memoria, vNIC y flash virtual. Igualmente, debe haber disponibles suficientes puertos de red para encender la máquina virtual.
Límites de hosts	Además de las reservas de recursos, una máquina virtual solo puede colocarse en un host si al hacerlo no se supera la cantidad máxima de máquinas virtuales permitidas o la cantidad de vCPU en uso.
Restricciones de características	Si se ha configurado la opción avanzada que requiere que vSphere HA aplique las reglas de antiafinidad entre máquinas virtuales, vSphere HA no infringe esta regla. También, vSphere HA no infringe ningún límite configurado por host para máquinas virtuales con Fault Tolerance.

Si ningún host satisface las consideraciones anteriores, el host maestro emite un evento que indica que no hay suficientes recursos para que vSphere HA inicie la máquina virtual y vuelve a intentarlo cuando las condiciones del clúster han cambiado. Por ejemplo, si no se puede acceder a la máquina virtual, el host maestro vuelve a intentarlo después de un cambio en la accesibilidad del archivo.

Límites para intentos de reinicio de la máquina virtual

Si el agente maestro de vSphere HA obtiene un error al intentar reiniciar una máquina virtual, lo que implica registrarla y encenderla, este reinicio se vuelve a intentar después de una demora. vSphere HA intenta estos reinicios durante una cantidad máxima de intentos (6 de forma predeterminada), pero no todos los errores en el reinicio se cuentan para este máximo.

Por ejemplo, el motivo más probable para que se produzca un error en un intento de reinicio se debe a que la máquina virtual sigue en ejecución en otro host o a que vSphere HA también intentó reiniciar la máquina virtual poco después de que falló. En esta situación, el agente maestro retrasa el intento de reinicio en dos veces la demora impuesta después del último intento, con una demora mínima de 1 minuto y una demora máxima de 30 minutos. De esta manera, si la demora se establece en 1 minuto, hay un intento inicial en T=0, luego, se realizan intentos adicionales en T=1 (1 minuto), T=3 (3 minutos), T=7 (7 minutos), T=15 (15 minutos) y T=30 (30 minutos). Cada intento de este tipo se cuenta para el límite y solo se hacen seis intentos de forma predeterminada.

Otros errores en el reinicio dan como resultado intentos contabilizables, pero con un diferente intervalo de demora. Un escenario de ejemplo es cuando el host escogido para reiniciar la máquina virtual pierde acceso a uno de los almacenes de datos de la máquina virtual después de que el agente maestro hizo la elección. En este caso, el reintento se hace después de una demora predeterminada de dos minutos. Este intento también se contabiliza para el límite.

Finalmente, algunos intentos no se cuentan. Por ejemplo, si el host en el cual se iba a reiniciar la máquina virtual genera errores antes de que el agente maestro emita la solicitud de reinicio, el reintento se hace después de dos minutos, pero este error no se contabiliza para la cantidad máxima de intentos.

Notificaciones de reinicio de máquina virtual

vSphere HA genera un evento del clúster cuando hay en curso una operación de conmutación por error para máquinas virtuales en el clúster. El evento también muestra un problema de configuración en la pestaña **Cluster Summary** (Resumen del clúster) que indica el número de máquinas virtuales que se van a reiniciar. Existen cuatro categorías diferentes de dichas máquinas virtuales.

- Máquinas virtuales que se colocarán: vSphere HA se encuentra en proceso de intentar reiniciar estas máquinas virtuales.
- Máquinas virtuales en espera de reinicio: se produjo un error en un intento de reinicio anterior y vSphere HA aguarda que caduque un tiempo de espera antes de volver a intentarlo.
- Máquinas virtuales que requieren recursos adicionales: no hay recursos suficientes disponibles para reiniciar estas máquinas virtuales. vSphere HA reintenta cuando hay disponibles más recursos, por ejemplo, que un host vuelva a estar en línea.
- Máquinas virtuales de Virtual SAN inaccesibles: vSphere HA no puede reiniciar estas máquinas virtuales de Virtual SAN, ya que no están accesibles. Lo reintenta cuando cambia la accesibilidad.

Estos conteos de máquinas virtuales se actualizan de forma dinámica cuando se observa un cambio en la cantidad de máquina virtual para las cuales hay en curso una operación de reinicio. El problema de configuración se borra cuando vSphere HA ha reiniciado todas las máquinas virtuales o ha dejado de intentarlo.

En vSphere 5.5 o versiones anteriores, se activa un evento por máquina virtual para un intento incorrecto de reiniciar la máquina virtual. Este evento se deshabilita de forma predeterminada en vSphere 6.x y puede habilitarse configurando la opción avanzada de vSphere HA `das.config.fdm.reportfailoverfailevent` en 1.

Supervisar máquina virtual y aplicaciones

VM Monitoring (Supervisión de máquina virtual) reinicia máquinas virtuales individuales si los latidos de su VMware Tools no se reciben dentro de un tiempo establecido. De forma similar, Application Monitoring (Supervisión de aplicaciones) puede reiniciar una máquina virtual si no se reciben los latidos para una aplicación que está en ejecución. Puede habilitar estas características y configurar la sensibilidad con la cual vSphere HA supervisa la incapacidad de respuesta.

Cuando habilita VM Monitoring (Supervisión de máquina virtual), este servicio (que usa VMware Tools) evalúa si se está ejecutando cada máquina virtual del clúster mediante la comprobación de latidos y actividad de E/S regulares del proceso de VMware Tools que se ejecuta dentro del invitado. Si no se reciben latidos ni actividad de E/S, lo más probable es que esto se deba a que hay errores en el sistema operativo invitado o que no se está asignando nada de tiempo a VMware Tools para completar las tareas. En dicho caso, el servicio VM Monitoring (Supervisión de máquina virtual) determina que la máquina virtual generó errores y que esta se reinicia para restaurar el servicio.

En ocasiones, las máquinas virtuales o las aplicaciones que siguen funcionando adecuadamente dejan de enviar latidos. Para evitar restablecimientos innecesarios, el servicio VM Monitoring (Supervisión de máquina virtual) también supervisa la actividad de E/S de una máquina virtual. Si no se reciben latidos dentro del intervalo de errores, se comprueba el intervalo de estadísticas de E/S (un atributo de nivel de clúster). El intervalo de estadísticas de E/S determina si se ha producido una actividad de disco o de red de la máquina virtual durante los dos minutos anteriores (120 segundos). Si no, la máquina virtual se restablece. Este valor predeterminado (120 segundos) se puede cambiar mediante la opción avanzada `das.iostatsinterval`.

Para habilitar Application Monitoring (Supervisión de aplicaciones), primero debe obtener el SDK adecuado (o usar una aplicación que sea compatible con Application Monitoring [Supervisión de aplicaciones] de VMware) y usarlo para instalar latidos personalizados para las aplicaciones que desea supervisar. Después de que haya hecho esto, Application Monitoring (Supervisión de aplicaciones) funciona de la misma forma que lo hace VM Monitoring (Supervisión de máquina virtual). Si los latidos de una aplicación no se reciben durante un tiempo especificado, su máquina virtual se reinicia.

Puede configurar el nivel de sensibilidad de supervisión. Una supervisión con alta sensibilidad da como resultado una conclusión más rápida de que se produjo un error. Aunque es improbable, la supervisión de alta sensibilidad podría llevar a la identificación incorrecta de errores cuando en realidad la máquina virtual o la aplicación siguen funcionando, pero no se han recibido latidos debido a factores como restricciones de recursos. La supervisión de baja sensibilidad da como resultado interrupciones más prolongadas en el servicio entre errores reales y el restablecimiento de máquinas virtuales. Seleccione una opción que sea un compromiso eficaz para sus necesidades.

La configuración predeterminada para la sensibilidad de supervisión se describe en Tabla 2-1. Para especificar también valores personalizados tanto para la sensibilidad de supervisión como para el intervalo de estadísticas de E/S, puede activar la casilla **Custom** (Personalizar).

Tabla 2-1. Configurar VM Monitoring (Supervisión de máquina virtual)

Configuración	Intervalo de errores (segundos)	Período de restablecimiento
High (Alto)	30	1 hora
Medium (Mediano)	60	24 horas
Low (Bajo)	120	7 días

Una vez que se detectan errores, vSphere HA restablece máquinas virtuales. El restablecimiento asegura que los servicios permanezcan disponibles. Para evitar restablecer máquinas virtuales de forma repetida para errores no transitorios, de forma predeterminada, las máquinas virtuales se restablecerán solo tres veces durante cierto intervalo de tiempo configurable. Después de que las máquinas virtuales se hayan

restablecido tres veces, vSphere HA no realiza nuevos intentos para restablecer las máquinas virtuales después de errores posteriores hasta que haya transcurrido el tiempo especificado. Puede configurar la cantidad de restablecimientos mediante el uso de la configuración personalizada **Maximum per-VM resets** (Restablecimientos máximos por máquina virtual).

NOTA: Las estadísticas de restablecimiento se borran cuando una máquina virtual se apaga y se vuelve a encender, o cuando se migra a otro host mediante el uso de vMotion. Esto hace que se reinicie el sistema operativo invitado, pero no es igual que un "restablecimiento" en el cual el estado de energía de la máquina virtual cambia.

Si una máquina virtual tiene un error de accesibilidad al almacén de datos, ya sea All Paths Down (Todas las rutas de acceso inactivas) o Permanent Device Loss (Pérdida permanente de dispositivos), el servicio VM Monitoring (Supervisión de máquina virtual) suspende el restablecimiento hasta que se haya solucionado el error.

protección de componentes de la máquina virtual

Si la opción Protección de componentes de la máquina virtual (VMCP) está habilitada, vSphere HA puede detectar errores de accesibilidad al almacén de datos y ofrecer recuperación automática para máquinas virtuales afectadas.

VMCP ofrece protección contra errores de accesibilidad al almacén de datos que pueden afectar a una máquina virtual que se ejecuta en un host en un clúster de vSphere HA. Cuando se produce un error de accesibilidad al almacén de datos, el host afectado ya no puede tener acceso a la ruta de acceso del almacén de datos para un almacén de datos específico. Puede determinar la respuesta que tomará vSphere HA para dicho error, que va desde la creación de alarmas de eventos hasta reinicios de máquinas virtuales en otros hosts.

NOTA: Cuando se utiliza la función Protección de componentes de la máquina virtual, los hosts ESXi deben ser versión 6.0 o posterior.

Tipos de error

Existen dos tipos de errores de accesibilidad al almacén de datos:

PDL PDL (Pérdida permanente de dispositivos) es una pérdida irrecuperable de accesibilidad que se produce cuando un dispositivo de almacenamiento informa que el host ya no puede acceder almacén de datos. Esta condición no puede revertirse sin apagar las máquinas virtuales.

APD APD (Todas las rutas de acceso inactivas) representa una pérdida de accesibilidad transitoria o desconocida o cualquier otro retraso sin identificar en el procesamiento de E/S. Este tipo de problema de accesibilidad es recuperable.

Configurar VMCP

La opción Protección de componentes de la máquina virtual se configura en vSphere Web Client. Vaya a la pestaña **Configurar**, haga clic en **Disponibilidad de vSphere** y seleccione **Editar**. En **Errores y respuestas**, puede seleccionar **Almacén de datos con PDL** o **Almacén de datos con APD**. Los niveles de protección de almacenamiento que escoja y las acciones de corrección de máquinas virtuales disponibles pueden ser diferentes dependiendo del tipo de error de accesibilidad de la base de datos.

Errores de PDL

En **Almacén de datos con PDL**, puede seleccionar **Emitir eventos** o **Apagar y reiniciar las máquinas virtuales**.

Errores de APD

Para respuesta a los eventos de APD es más completa y, en consecuencia, la configuración es más refinada. Puede seleccionar **Emitir eventos**, **Apagar y reiniciar las máquinas virtuales (directiva de reinicio conservadora)** o **Apagar y reiniciar las máquinas virtuales (directiva de reinicio agresiva)**

NOTA: Si las configuraciones Supervisión de hosts o Prioridad de restablecimiento de máquina virtual están deshabilitadas, VMCP no puede realizar restablecimientos de máquinas virtuales. Sin embargo, aún puede supervisarse el estado del almacenamiento y se pueden emitir eventos.

Particiones de red

Cuando se produce un error de red de administración para un clúster de vSphere HA, es posible que un subconjunto de los hosts del clúster no pueda comunicarse por la red de administración con los otros hosts. Pueden darse varias particiones en un clúster.

Un clúster particionado conduce a una protección de máquina virtual y funcionalidad de administración de clústeres degradados. Corrija el clúster particionado en cuanto sea posible.

- Protección de máquina virtual. vCenter Server permite que una máquina virtual se encienda, pero solo puede protegerse si se ejecuta en la misma partición que el host maestro del cual es responsable. El host maestro debe comunicarse con vCenter Server. Un host maestro es responsable de una máquina virtual si ha bloqueado exclusivamente un archivo definido por el sistema en el almacén de datos que contiene el archivo de configuración de la máquina virtual.
- Administración de clúster. vCenter Server puede comunicarse con el host maestro, pero solo un subconjunto de los hosts esclavos. Como resultado, es posible que los cambios en la configuración que afecten a vSphere HA no tengan efecto hasta que se resuelva la partición. Este error podría dar como resultado que una de las particiones opere con la configuración antigua, mientras que otra usa la nueva.

Latidos del almacén de datos

Cuando el host maestro en un clúster de vSphere HA no puede comunicarse con un host esclavo a través de la red de administración, el host maestro utiliza la verificación de latido del almacén de datos para determinar si el host esclavo ha generado errores, está en una partición de red o está aislado de la red. Si el host esclavo dejó de verificar latidos del almacén de datos, se considera que se generó un error y las máquinas virtuales se reinician en otra parte.

vCenter Server selecciona un conjunto de almacenes de datos preferidos para verificación de latido. Esta selección se hace para maximizar la cantidad de hosts que tienen acceso a un almacén de datos de verificación de latido y minimizar la probabilidad de que el mismo servidor de LUN o NFS haga copia de seguridad de los almacenes de datos.

Puede usar la opción avanzada `das.heartbeatdsperhost` para cambiar la cantidad de almacenes de datos de latidos que haya seleccionado vCenter Server para cada host. El valor predeterminado es dos y el valor válido máximo es cinco.

vSphere HA crea un directorio en la raíz de cada almacén de datos que se utiliza tanto para verificación de latido del almacén de datos como para mantener activo el conjunto de máquinas virtuales protegidas. El nombre del directorio es `.vSphere-HA`. No elimine ni modifique archivos almacenados en este directorio, ya que esto puede tener un impacto en las operaciones. Debido a que más de un clúster podría usar un almacén de datos, se crean subdirectorios para este directorio para cada clúster. La raíz posee estos directorios y archivos y solo la raíz puede leer y escribir en ellos. El espacio de disco que utiliza vSphere HA depende de varios factores, entre los que se incluyen la versión de VMFS que hay en uso y la cantidad de hosts que utilizan el almacén de datos para verificación de latido. Con vmfs3, el uso máximo es de aproximadamente 2 GB y el uso típico es de cerca de 3 MB. Con vmfs5, el uso máximo y típico es de alrededor de 3 MB. El uso que hace vSphere HA de los almacenes de datos agrega una sobrecarga insignificante y no tiene impacto en el rendimiento en otras operaciones del almacén de datos.

vSphere HA limita la cantidad de máquinas virtuales que pueden tener archivos de configuración en un solo almacén de datos. Consulte *Valores máximos de configuración* para conocer los límites actualizados. Si coloca más de esta cantidad de máquinas virtuales en un almacén de datos y las enciende, vSphere HA protege solo hasta el límite establecido de máquinas virtuales.

NOTA: No se puede usar un almacén de datos de Virtual SAN para verificar latido del almacén de datos. Por lo tanto, si no hay otro almacenamiento compartido accesible para todos los hosts en el clúster, no podrá haber almacenes de datos de latidos en uso. Sin embargo, si tiene un almacenamiento al que pueda acceder mediante una ruta de acceso de red alternativa que sea independiente de la red de Virtual SAN, puede usarlo para instalar un almacén de datos de latidos.

Seguridad de vSphere HA

vSphere HA se mejora a través de varias características de seguridad.

Seleccionar puertos de firewall abiertos

vSphere HA utiliza el puerto TCP y UDP 8182 para comunicación entre agentes. Los puertos de firewall se abren y cierran automáticamente para asegurar que estén abiertos solo cuando sea necesario.

Archivos de configuración protegidos mediante permisos del sistema de archivos

vSphere HA almacena información de configuración en el almacenamiento local o en ramdisk en caso de que no haya un almacén de datos local. Estos archivos se protegen mediante permisos del sistema de archivos y solo el usuario raíz puede acceder a ellos. Los hosts sin almacenamiento local solo son compatibles si los administra Auto Deploy.

Registro detallado

La ubicación donde vSphere HA coloca los archivos de registro depende de las versiones del host.

- Para hosts ESXi 5.x, vSphere HA escribe en syslog solo de manera predeterminada, por lo que los registros se colocan donde syslog está configurado para ponerlos. Los nombres de archivos de registro para vSphere HA vienen antecedidos con `fdm`, fault domain manager, que es un servicio de vSphere HA.
- Para hosts heredados de ESXi 4.x, vSphere HA escribe en `/var/log/vmware/fdm` en el disco local, así como en el syslog si está configurado.
- Para hosts ESX 4.x heredados, vSphere HA escribe en `/var/log/vmware/fdm`.

Inicios de sesión de vSphere HA seguros

vSphere HA inicia sesión en los agentes de vSphere HA mediante una cuenta de usuario, **vpxuser**, creada por vCenter Server. Esta cuenta es la misma que usa vCenter Server para administrar el host. vCenter Server crea una contraseña aleatoria para esta cuenta y cambia dicha contraseña de forma

periódica. El período se establece con la configuración vCenter Server `VirtualCenter.VimPasswordExpirationInDays`. Los usuarios con privilegios administrativos en la carpeta raíz del host pueden iniciar sesión en el agente.

Comunicación segura Toda la comunicación entre el agente de vCenter Server y de vSphere HA se realiza a través de SSL. La comunicación entre agentes también utiliza SSL, excepto para mensajes de elección, que se producen a través de UDP. Los mensajes de elección se verifican a través de SSL de manera que se evite elegir como host maestro solo al host que ejecuta el agente malicioso. En este caso, se emite un problema de configuración para el clúster de manera que el usuario tenga en cuenta el problema.

Se requiere verificación del certificado SSL del host vSphere HA requiere que cada host tenga un certificado SSL verificado. Cada host genera un certificado con autofirma cuando arranca por primera vez. Después, este certificado se puede volver a generar o reemplazar con uno emitido por una entidad. Si se reemplaza el certificado, es necesario volver a configurar vSphere HA en el host. Si un host se desconecta de vCenter Server después de que se actualiza su certificado y se reinicia el agente de host ESXi o ESX, entonces vSphere HA se vuelve a configurar automáticamente cuando el host se conecta de nuevo a vCenter Server. Si la desconexión no se produce debido a que en ese momento está deshabilitada la verificación del certificado SSL del host de vCenter Server, verifique el certificado nuevo y vuelva a configurar vSphere HA en el host.

Control de admisión de vSphere HA

vCenter Server utiliza el control de admisión para asegurar que haya suficientes recursos disponibles en un clúster para proporcionar protección de conmutación por error y asegurar que se respeten las reservas de recursos de máquina virtual.

Hay disponibles tres tipos de control de admisión.

Host Asegura que un host tenga suficientes recursos para satisfacer las reservas de todas las máquinas virtuales que se ejecutan en él.

Grupo de recursos Asegura que un grupo de recursos tenga suficientes recursos para satisfacer las reservas, los recursos compartidos y los límites de todas las máquinas virtuales asociadas a él.

vSphere HA Asegura que haya suficientes recursos en el clúster reservados para la recuperación de máquinas virtuales en caso de error del host.

El control de admisión impone restricciones para el uso de recursos y no se permite ninguna acción que infrinja estas restricciones. Entre los ejemplos de acciones que podrían no permitirse, se encuentran los siguientes:

- Encendido de una máquina virtual.
- Migración de una máquina virtual a un host o a un grupo de clústeres o recursos.
- Aumento de la reserva de CPU o memoria de una máquina virtual.

De los tres tipos de control de admisión, solo se puede deshabilitar el de vSphere HA. Sin embargo, sin él, no hay garantías de que se pueda reiniciar la cantidad esperada de máquinas virtuales después de un error. No deshabilite de forma permanente el control de admisión. Sin embargo, es posible que tenga que hacerlo temporalmente por los siguientes motivos:

- Si necesita infringir las restricciones de conmutación por error cuando no haya suficientes recursos que los admitan, por ejemplo, si va a colocar hosts en modo de espera para probarlos para su uso con Distributed Power Management (DPM).
- Si un proceso automatizado necesita tomar acciones que podrían infringir temporalmente las restricciones de conmutación por error (por ejemplo, como parte de una actualización o revisión de hosts ESXi según lo indica vSphere Update Manager).
- Si necesita realizar operaciones de pruebas o mantenimiento.

El control de admisión reserva la capacidad, pero cuando se produce un error, vSphere HA utiliza cualquier capacidad que haya disponible para los reinicios de máquinas virtuales. Por ejemplo, vSphere HA coloca más máquinas virtuales en un host de las que permitiría el control de admisión para encendidos iniciados por el usuario.

NOTA: Cuando el control de admisión de vSphere HA está deshabilitado, vSphere HA asegura que haya al menos dos hosts encendidos en el clúster aunque DPM esté habilitado y pueda consolidar todas las máquinas virtuales en un solo host. Esto es para asegurar que se pueda realizar la conmutación por error.

Directiva de control de admisión Host Failures Cluster Tolerates (Tolerancias del clúster para errores del host)

Puede configurar vSphere HA para que tolere una cantidad específica de errores del host. Con la directiva de control de admisión Host Failures Cluster Tolerates (Tolerancias del clúster para errores del host), vSphere HA asegura que pueda fallar una cantidad específica de hosts y que permanezcan suficientes recursos en el clúster para realizar conmutación por error en todas las máquinas virtuales desde dichos hosts.

Con la directiva Host Failures Cluster Tolerates (Tolerancias del clúster para errores del host), vSphere HA realiza el control de admisión de la siguiente forma:

1 Calcula el tamaño de ranura.

   Una ranura es una representación lógica de los recursos de memoria y CPU. De forma predeterminada, tiene un tamaño para que satisfaga los requisitos para cualquier máquina virtual encendida en el clúster.

2 Determina cuántas ranuras puede mantener cada host en el clúster.

3 Determina la capacidad actual de conmutación por error del clúster.

   Esta es la cantidad de hosts que pueden tener errores y aún así dejar suficientes ranuras para que atienda a todas las máquinas virtuales encendidas.

4 Determina si la capacidad actual de conmutación por error es inferior a la capacidad configurada de conmutación por error (provista por el usuario).

   Si lo es, el control de admisión no permite la operación.

NOTA: Puede configurar un tamaño de ranura específico tanto para la CPU como la memoria en la sección de control de admisión de la configuración de vSphere HA en vSphere Web Client.

Calcular el tamaño de ranura

Tamaño de ranura y control de admisión de vSphere HA (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vsphere_slot_admission_control)

El tamaño de ranura consta de dos componentes: la CPU y la memoria.

- vSphere HA calcula el componente de CPU obteniendo la reserva de CPU de cada máquina virtual encendida y seleccionando el mayor valor. Si no ha especificado una reserva de CPU para una máquina virtual, se asigna un valor predeterminado de 32 MHz. Puede cambiar este valor usando la opción avanzada `das.vmcpuminmhz`.
- vSphere HA calcula el componente de memoria obteniendo la reserva de memoria, además de la sobrecarga de memoria, de cada máquina virtual encendida y seleccionando el mayor valor. No hay un valor predeterminado para la reserva de memoria.

Si su clúster contiene máquinas virtuales que tienen reservas mucho mayores que las otras, distorsionarán el cálculo del tamaño de ranura. Para evitar esto, puede especificar un límite superior para el componente de CPU o memoria del tamaño de ranura mediante el uso de las opciones avanzadas `das.slotcpuinmhz` o`das.slotmeminmb`, respectivamente. Consulte "Opciones avanzadas de vSphere HA," página 38.

También puede determinar el riesgo de fragmentación de recursos en su clúster viendo la cantidad de máquinas virtuales que requieren varias ranuras. Esto se puede calcular en la sección de control de admisión de la configuración de vSphere HA en vSphere Web Client. Las máquinas virtuales pueden necesitar varias ranuras en caso de que haya especificado un tamaño de ranura fijo o un tamaño de ranura máximo usando opciones avanzadas.

Usar ranuras para calcular la capacidad actual de conmutación por error

Después de calcular el tamaño de ranura, vSphere HA determina los recursos de CPU y memoria de cada host que están disponibles para máquinas virtuales. Estas cantidades son aquellas que están contenidas en el grupo de recursos raíz del host, no los recursos físicos totales del host. Los datos de recursos para un host que utiliza vSphere HA se pueden encontrar en la pestaña **Summary** (Resumen) del host en vSphere Web Client. Si todos los hosts de su clúster son iguales, estos datos se pueden obtener dividiendo las cifras de nivel de clúster por la cantidad de hosts. Los recursos que se van a usar para fines de virtualización no están incluidos. Solo se consideran los hosts que están conectados, que no están en modo de mantenimiento y que no tienen errores de vSphere HA.

Luego, se determina la cantidad máxima de ranuras que puede admitir cada host. Para hacerlo, la cantidad de recursos de CPU del host se divide por el componente de CPU del tamaño de ranura y el resultado se redondea hacia abajo. El mismo cálculo se hace para la cantidad de recursos de memoria del host. Estos números se comparan y el número menor es la cantidad de ranuras que puede admitir el host.

La capacidad actual de conmutación por error se calcula determinando cuántos hosts (comenzando desde el más grande) pueden generar errores y aún dejar suficientes ranuras para atender los requisitos de todas las máquinas virtuales encendidas.

Información de tiempo de ejecución avanzada

Cuando selecciona la directiva de control de admisión Host Failures Cluster Tolerates (Tolerancias del clúster para errores del host), aparece el panel **Advanced Runtime Info** (Información de tiempo de ejecución avanzada) en la sección de vSphere HA de la pestaña **Monitor** (Supervisar) del clúster en vSphere Web Client. Este panel muestra la siguiente información acerca del clúster:

- Slot size (Tamaño de ranura).
- Cantidad total de ranuras en el clúster. La suma de las ranuras que admiten hosts buenos en el clúster.

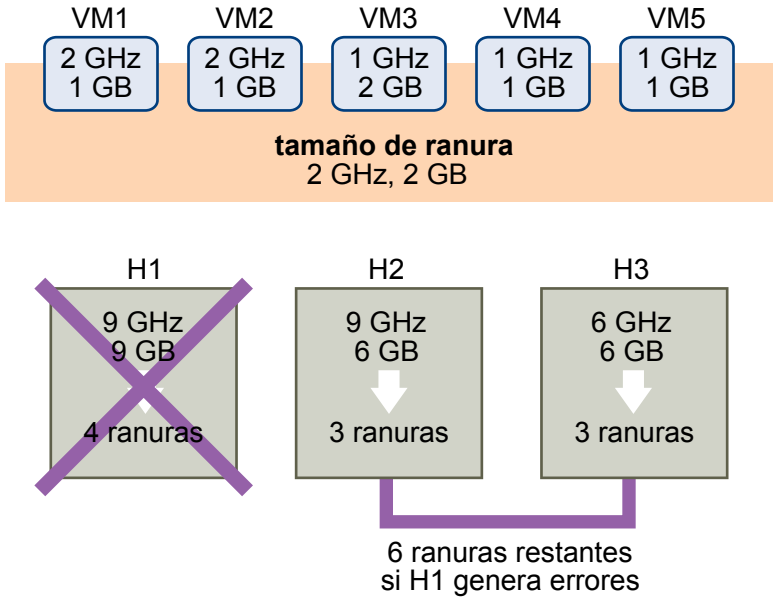
- Used slots (Ranuras utilizadas). La cantidad de ranuras asignadas a máquinas virtuales encendidas. Puede ser mayor que la cantidad de máquinas virtuales encendidas si ha definido un límite superior para el tamaño de ranura mediante las opciones avanzadas. Esto se debe a que algunas máquinas virtuales pueden consumir varias ranuras.
- Available slots (Ranuras disponibles). La cantidad de ranuras disponibles para encender máquinas virtuales en el clúster. vSphere HA reserva la cantidad necesaria de ranuras para conmutación por error. Las ranuras restantes están disponibles para encender máquinas virtuales.
- Failover slots (Slots para conmutación por error). La cantidad total de ranuras sin contar las ranuras usadas o las ranuras disponibles.
- Cantidad total de máquinas virtuales encendidas en el clúster.
- Total number of hosts in cluster (Cantidad total de hosts en el clúster).
- Hosts buenos totales en el clúster. La cantidad de hosts que están conectados, no en modo de mantenimiento, y que no tienen errores de vSphere HA.

Ejemplo: Control de admisión mediante la directiva Host Failures Cluster Tolerates (Tolerancias del clúster para errores del host)

La forma en que se calcula y se usa el tamaño de ranura con esta directiva de control de admisión se muestra en un ejemplo. Haga las siguientes suposiciones sobre un clúster:

- El clúster está compuesto de tres hosts, cada uno con una cantidad diferente de recursos de CPU y de memoria disponibles. El primer host (H1) posee 9 GHz de recursos de CPU disponibles y 9 GB de memoria disponible, en tanto que el host 2 (H2) tiene 9 GHz y 6 GB y el host 3 (H3) cuenta con 6 GHz y 6 GB.
- Existen cinco máquinas virtuales encendidas en el clúster con diferentes requisitos de CPU y memoria. La máquina virtual 1 necesita 2 GHz de recursos de CPU y 1 GB de memoria, en tanto que la máquina virtual 2 requiere 2 GHz y 1 GB, la máquina virtual 3, 1 GHz y 2 GB, la máquina virtual 4 necesita 1 GHz y 1 GB y la máquina virtual 5, 1 GHz y 1 GB.
- Host Failures Cluster Tolerates (Tolerancias del clúster para errores del host) está configurada en uno.

Figura 2-1. Ejemplo de control de admisión con directiva Host Failures Cluster Tolerates (Tolerancias del clúster para errores del host)



1 El tamaño de ranura se calcula comparando tanto los requisitos de CPU como de memoria de las máquinas virtuales y seleccionando el de mayor tamaño.

   El mayor requisito de CPU (compartido por la máquina virtual 1 y la máquina virtual 2) es 2 GHz, en tanto que el mayor requisito de memoria (para la máquina virtual 3) es 2 GB. Basado en esto, el tamaño de ranura es CPU de 2 GHz y memoria de 2 GB.

2 Se determina la cantidad máxima de ranuras que puede admitir cada host.

   H1 puede admitir cuatro ranuras. H2 puede admitir tres ranuras (que es la cantidad menor de 9 GHz/2 GHz y 6 GB/2 GB) y H3 también puede admitir tres ranuras.

3 Se calcula la capacidad actual de conmutación por error.

   El host más grande es el H1 y si genera errores, seis ranuras permanecen en el clúster, lo que es suficiente para las cinco máquinas virtuales encendidas. Si hay error tanto de H1 como de H2, solo quedan tres ranuras, lo que no es suficiente. Por lo tanto, la capacidad actual de conmutación por error es uno.

El clúster tiene una ranura disponible (las seis ranuras en H2 y H3 menos las cinco ranuras usadas).

Directiva de control de admisión Percentage of Cluster Resources Reserved (Porcentaje de recursos del clúster reservados)

Puede configurar vSphere HA para realizar control de admisión mediante la reserva de un porcentaje específico de recursos de CPU y memoria del clúster para recuperación de errores del host.

Con la directiva de control de admisión Percentage of Cluster Resources Reserved (Porcentaje de recursos del clúster reservados), vSphere HA asegura que se reserve un porcentaje específico de recursos de CPU y memoria para conmutación por error.

Con la directiva Cluster Resources Reserved (Recursos del clúster reservados), vSphere HA aplica control de admisión de la siguiente forma:

1 Calcula los requisitos de recursos totales para todas las máquinas virtuales encendidas en el clúster.

2 Calcula los recursos totales del host disponibles para máquinas virtuales.

3 Calcula la capacidad actual de conmutación por error de la CPU y la capacidad actual de conmutación por error de la memoria para el clúster.

4 Determina si la capacidad actual de conmutación por error de la CPU o la capacidad actual de conmutación por error de la memoria es menor que la capacidad de conmutación por error configurada correspondiente (provista por el usuario).

   Si lo es, el control de admisión no permite la operación.

vSphere HA usa las reservas reales de las máquinas virtuales. Si una máquina virtual no tiene reservas, ello significa que la reserva es 0, y se aplica un valor predeterminado de memoria de 0 MB y una CPU de 32 MHz.

NOTA: La directiva de control de admisión Percentage of Cluster Resources Reserved (Porcentaje de recursos del clúster reservados) también comprueba que haya al menos dos hosts habilitados para vSphere HA en el clúster (excluyendo hosts que están entrando en modo de mantenimiento). Si hay solo un host habilitado para vSphere HA, no se permite una operación, incluso si hay suficiente porcentaje de recursos disponibles. El motivo para esta comprobación adicional es que vSphere HA no puede realizar conmutación por error si hay un solo host en el clúster.

Cálcular la capacidad actual de conmutación por error

Los requisitos de recursos totales para las máquinas virtuales encendidas constan de dos componentes: CPU y memoria. vSphere HA calcula estos valores.

- El componente de CPU, sumando las reservas de CPU de las máquinas virtuales encendidas. Si no ha especificado una reserva de CPU para una máquina virtual, se asigna un valor predeterminado de 32 MHz (este valor puede cambiarse usando la opción avanzada `das.vmcpuminmhz`.)
- El componente de memoria, sumando la reserva de memoria (más sobrecarga de memoria) de cada máquina virtual encendida.

Los recursos totales de host disponibles para máquinas virtuales se calculan agregando los recursos de CPU y memoria de los hosts. Estas cantidades son aquellas que están contenidas en el grupo de recursos raíz del host, no los recursos físicos totales del host. Los recursos que se van a usar para fines de virtualización no están incluidos. Solo se consideran los hosts que están conectados, que no están en modo de mantenimiento y que no tienen errores de vSphere HA.

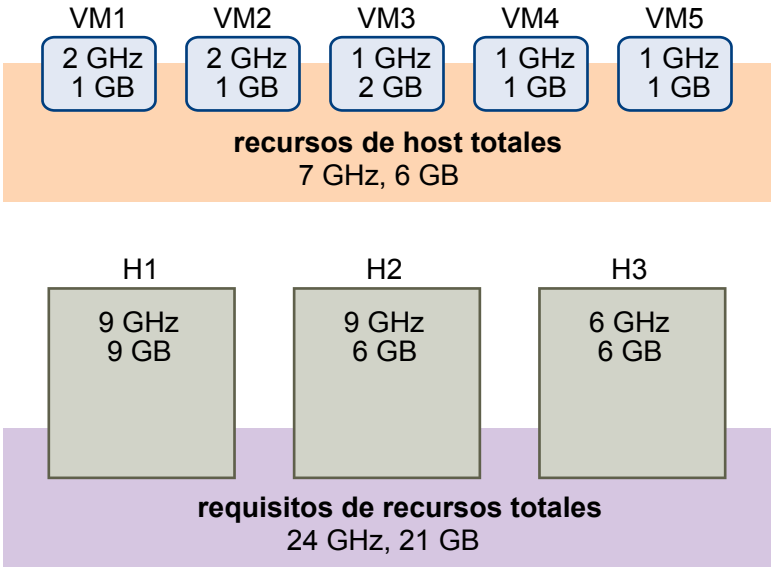
La capacidad actual de conmutación por error de la CPU se calcula restando los requisitos de recursos totales de CPU de los recursos totales de CPU del host y dividiendo el resultado por los recursos totales de CPU del host. La capacidad actual de conmutación por error de la memoria se calcula de forma similar.

Ejemplo: Control de admisión usando la directiva Percentage of Cluster Resources Reserved (Porcentaje de recursos del clúster reservados)

La forma en que se calcula y se usa la capacidad actual de conmutación por error con esta directiva de control de admisión se muestra con un ejemplo. Haga las siguientes suposiciones sobre un clúster:

- El clúster está compuesto de tres hosts, cada uno con una cantidad diferente de recursos de CPU y de memoria disponibles. El primer host (H1) posee 9 GHz de recursos de CPU disponibles y 9 GB de memoria disponible, en tanto que el host 2 (H2) tiene 9 GHz y 6 GB y el host 3 (H3) cuenta con 6 GHz y 6 GB.
- Existen cinco máquinas virtuales encendidas en el clúster con diferentes requisitos de CPU y memoria. La máquina virtual 1 necesita 2 GHz de recursos de CPU y 1 GB de memoria, en tanto que la máquina virtual 2 requiere 2 GHz y 1 GB, la máquina virtual 3, 1 GHz y 2 GB, la máquina virtual 4 necesita 1 GHz y 1 GB y la máquina virtual 5, 1 GHz y 1 GB.
- La capacidad configurada de conmutación por error para CPU y memoria está configurada para ambas en 25 %.

Figura 2-2. Ejemplo de control de admisión con la directiva Percentage of Cluster Resources Reserved (Porcentaje de recursos del clúster reservados)



Los requisitos de recursos totales para las máquinas virtuales encendidas son 7 GHz y 6 GB. Los recursos totales del host disponibles para máquinas virtuales son 24 GHz y 21 GB. Basado en esto, la capacidad actual de conmutación por error de la CPU es 70 % ((24 GHz - 7 GHz)/24 GHz). De forma similar, la capacidad actual de conmutación por error de la memoria es de 71 % ((21 GB - 6 GB)/21 GB).

Debido a que la capacidad configurada de conmutación por error del clúster está configurada en 25 %, un 45 % de los recursos totales de CPU del clúster y un 46 % de los recursos de memoria del clúster siguen disponibles para encender máquinas virtuales.

Especificar la directiva de control de admisión de hosts para conmutación por error

Puede configurar vSphere HA para designar hosts específicos como hosts de conmutación por error.

Con la directiva de control de admisión Specify Failover Hosts (Especificar hosts para conmutación por error), cuando un host genera errores, vSphere HA intenta reiniciar sus máquinas virtuales en cualquiera de los hosts para conmutación por error especificados. Si esto no es posible, por ejemplo debido a que los hosts para conmutación por error presentaron error o no tienen suficientes recursos, entonces vSphere HA intenta reiniciar aquellas máquinas virtuales en otros hosts en el clúster.

Para asegurar que haya capacidad disponible en un host para conmutación por error, se evita que encienda máquinas virtuales o use vMotion para migrar máquinas virtuales a un host para conmutación por error. Igualmente, DRS no usa un host para conmutación por error para equilibrio de carga.

NOTA: Si usa la directiva de control de admisión Specify Failover Hosts (Especificar hosts para conmutación por error) y designa varios hosts para conmutación por error, DRS no intenta aplicar las reglas de afinidad Máquina virtual-Máquina virtual para máquinas virtuales que se están ejecutando en hosts para conmutación por error.

Los hosts para conmutación por error actuales aparecen en la sección de vSphere HA de la pestaña **Summary** (Resumen) del clúster. El icono de estado junto a cada host puede estar verde, amarillo o rojo.

- Verde. El host está conectado, no en modo de mantenimiento y no tiene errores de vSphere HA. No hay máquinas virtuales encendidas que residan en el host.
- Amarillo. El host está conectado, no en modo de mantenimiento y no tiene errores de vSphere HA. Sin embargo, hay máquinas virtuales encendidas que residen en el host.

- Rojo. El host está desconectado, en modo de mantenimiento o tiene errores de vSphere HA.

Seleccionar una directiva de control de admisión

Debe elegir una directiva de control de admisión de vSphere HA según sus necesidades de disponibilidad y las características de su clúster. Cuando se elige una directiva de control de admisión, tiene que considerar varios factores.

Evitar la fragmentación de recursos

La fragmentación de recursos se produce cuando hay suficientes recursos en total para realizar la conmutación por error de una máquina virtual. Sin embargo, dichos recursos se encuentran en varios hosts y no se pueden utilizar porque una máquina virtual puede ejecutarse en un host ESXi a la vez. La configuración predeterminada de la directiva Host Failures Cluster Tolerates (Tolerancias del clúster para errores del host) evita la fragmentación de recursos mediante la definición de una ranura como la reserva máxima para máquinas virtuales. La directiva Percentage of Cluster Resources (Porcentaje de recursos del clúster) no soluciona el problema de fragmentación de recursos. Con la directiva Specify Failover Hosts (Especificar hosts para conmutación por error), los recursos no se fragmentan, ya que los hosts están reservados para la conmutación por error.

Flexibilidad de reserva de recursos para la conmutación por error

Las directivas de control de admisión se diferencian en la granularidad de control que le otorgan cuando reserva recursos del clúster para la protección de conmutación por error. La directiva Host Failures Cluster Tolerates (Tolerancias del clúster para errores del host) permite configurar el nivel de conmutación por error en varios hosts. La directiva Percentage of Cluster Resources (Porcentaje de recursos del clúster) le permite designar hasta un 100 % de los recursos de CPU o memoria del clúster para conmutación por error. Con la directiva Specify Failover Hosts (Especificar hosts para conmutación por error) puede especificar un conjunto de hosts de conmutación por error.

Heterogeneidad del clúster

Los clústeres pueden ser heterogéneos en cuanto a reservas de recursos de máquina virtual y las capacidades de recursos totales del host. En un clúster heterogéneo, la directiva Host Failures Cluster Tolerates (Tolerancias del clúster para errores del host) puede ser demasiado conservadora, ya que, cuando define el tamaño de la ranura, solo considera las mayores reservas de máquinas virtuales y da por hecho que los hosts más grandes generarán errores al calcular la capacidad actual de la conmutación por error. Las otras dos directivas de control de admisión no se ven afectadas por la heterogeneidad del clúster.

NOTA: vSphere HA incluye el uso de recursos de máquina virtual secundarias con Fault Tolerance cuando realiza cálculos de control de admisión. Para la directiva Host Failures Cluster Tolerates (Tolerancias del clúster para errores del host), una máquina virtual secundaria tiene asignada una ranura; y para la directiva Percentage of Cluster Resources (Porcentaje de recursos del clúster) se contabiliza el uso de recursos por parte de la máquina virtual secundaria para calcular la capacidad utilizable del clúster.

Interoperabilidad de vSphere HA

vSphere HA puede interoperar con muchas otras funciones, como DRS y Virtual SAN.

Antes de configurar vSphere HA, se deben conocer las limitaciones de su interoperabilidad con estas otras funciones o productos.

Usar vSphere HA con Virtual SAN

Puede usar Virtual SAN como el almacenamiento compartido para un clúster de vSphere HA. Cuando está habilitado, Virtual SAN agrega los discos de almacenamiento local especificados en los hosts en un solo almacén de datos que comparten todos los hosts.

Para usar vSphere HA con Virtual SAN, debe tener en cuenta ciertas consideraciones y limitaciones para la interoperabilidad de estas dos características.

Para obtener información sobre Virtual SAN, consulte *VMware Virtual SAN*.

Requisitos de los hosts ESXi

Puede usar Virtual SAN con un clúster de vSphere HA solamente si se satisfacen las siguientes condiciones:

- Todos los hosts ESXi del clúster deben tener la versión 5.5 o posterior.
- El clúster debe tener un mínimo de tres hosts ESXi.

Diferencias de red

Virtual SAN tiene su propia red. Cuando Virtual SAN y vSphere HA están habilitados para el mismo clúster, el tráfico entre agentes de HA se transmite a través de esta red de almacenamiento en lugar de la red de administración. vSphere HA solo utiliza la red de administración cuando Virtual SAN está deshabilitado. vCenter Server elige la red adecuada cuando vSphere HA está configurado en un host.

NOTA: Virtual SAN solo puede habilitarse cuando vSphere HA está deshabilitado.

Si cambia la configuración de red de Virtual SAN, los agentes de vSphere HA no seleccionan de forma automática la nueva configuración de red. Por lo tanto, para realizar cambios en la red de Virtual SAN, debe llevar a cabo los siguientes pasos en vSphere Web Client:

1 Deshabilite Host Monitoring (Supervisión de hosts) para el clúster de vSphere HA.

2 Realice los cambios de red de Virtual SAN.

3 Haga clic con el botón derecho en el clúster y seleccione **Reconfigure for vSphere HA** (Volver a configurar para vSphere HA).

4 Vuelva a habilitar Host Monitoring (Supervisión de hosts) para el clúster de vSphere HA.

Tabla 2-2 se muestran las diferencias en redes de vSphere HA cuando se usa Virtual SAN o no se usa.

Tabla 2-2. diferencias de red de vSphere HA

	Virtual SAN habilitado	Virtual SAN deshabilitado
Red utilizada por vSphere HA	Red de almacenamiento de Virtual SAN	Red de administración
Almacenes de datos de latidos	Cualquier almacén de datos montado en > 1 host, pero no almacenes de datos de Virtual SAN	Cualquier almacén de datos montado en > 1 host
Host declarado aislado	Direcciones de aislamiento a las que no se puede hacer ping y red de almacenamiento de Virtual SAN inaccesible	No se puede hacer ping a las direcciones de aislamiento y la red de administración no está accesible

Configurar reserva de capacidad

Cuando reserva capacidad para su clúster de vSphere HA con una directiva de control de admisión, esta configuración debe estar coordinada con la configuración de Virtual SAN correspondiente que asegura la accesibilidad de datos cuando haya errores. Específicamente, la configuración Number of Failures Tolerated (Número de errores que se toleran) en el conjunto de reglas de Virtual SAN no debe ser inferior a la capacidad que reserva la configuración de control de admisión de vSphere HA.

Por ejemplo, si el conjunto de reglas de Virtual SAN solamente permite dos errores, la directiva de control de admisión de vSphere HA debe reservar una capacidad que sea equivalente a los errores de solamente un host o dos hosts. Si va a usar la directiva Percentage of Cluster Resources Reserved (Porcentaje de recursos del clúster reservados) para un clúster que tiene ocho hosts, no debe reservar más de un 25 % de los recursos del clúster. En el mismo clúster, con la directiva Host Failures Cluster Tolerates (Tolerancias del clúster para errores del host), la configuración no debe ser mayor a dos hosts. Si vSphere HA reserva menos capacidad, puede que la actividad de conmutación por error sea impredecible, mientras que si se reserva demasiada capacidad se limita excesivamente el encendido de máquinas virtuales y migraciones de vMotion entre clústeres.

Usar vSphere HA y DRS a la vez

El uso de vSphere HA con Distributed Resource Scheduler (DRS) combina la conmutación por error automática con el equilibrio de carga. Mediante esta combinación se puede obtener un clúster más equilibrado después de que vSphere HA haya movido máquinas virtuales a diferentes hosts.

Cuando vSphere HA realiza la conmutación por error y reinicia máquinas virtuales en hosts distintos, su principal prioridad es hacer que todas las máquinas virtuales estén disponibles de inmediato. Después de que se hayan reiniciado las máquinas virtuales, los hosts en los que estaban encendidas podrían verse con carga excesiva, mientras que otros hosts tienen en comparación una carga muy ligera. vSphere HA utiliza la reserva de CPU y memoria y la memoria de sobrecarga de la máquina virtual para determinar si un host tiene suficiente capacidad disponible para incluir la máquina virtual.

En un clúster que utiliza DRS y vSphere HA con control de admisión activado, es posible que las máquinas virtuales no se evacúen de los hosts que entran en modo de mantenimiento. Este comportamiento se produce debido a los recursos reservados para reiniciar máquinas virtuales en caso de un error. Debe migrar manualmente las máquinas virtuales de los hosts mediante el uso de vMotion.

En algunos casos, es posible que vSphere HA no pueda realizar la conmutación por error en máquinas virtuales debido a restricciones de recursos. Esto puede deberse a varios motivos.

- El control de admisión de HA está deshabilitado y Distributed Power Management (DPM) está habilitado. Esto puede provocar que DPM consolide máquinas virtuales en menor cantidad de hosts y que coloque los hosts vacíos en modo de espera, lo que no deja suficiente capacidad de encendido para realizar conmutación por error.
- Las reglas de afinidad Máquina virtual-Host (obligatorias) podrían limitar los hosts en los que se pueden colocar ciertas máquinas virtuales.
- Podría haber suficientes recursos totales, pero estos pueden fragmentarse en varios hosts con el fin de que las máquinas virtuales no puedan usarlos para la conmutación por error.

En dichos casos, vSphere HA puede utilizar DRS para intentar ajustar el clúster (por ejemplo, sacando los hosts del modo de espera o migrando máquinas virtuales para desfragmentar los recursos del clúster), de manera que HA pueda realizar las conmutaciones por error.

Si DPM está en modo manual, puede que tenga que confirmar las recomendaciones de encendido del host. Igualmente, si DRS está en modo manual, es posible que tenga que confirmar las recomendaciones de migración.

Si va a utilizar reglas de afinidad Máquina virtual-Host que son obligatorias, tenga en cuenta que estas no se pueden infringir. vSphere HA no realiza una conmutación por error si el hacerlo implica una infracción de una regla de este tipo.

Para obtener más información sobre DRS, consulte la documentación de *Administración de recursos de vSphere*.

Reglas de afinidad de vSphere HA y DRS

Si crea una regla de afinidad de DRS para su clúster, puede especificar de qué manera vSphere HA aplica esa regla durante la conmutación por error de una máquina virtual.

Los dos tipos de reglas para los cuales puede especificar comportamiento de conmutación por error de vSphere HA son los siguientes:

- Las reglas antiafinidad de la máquina virtual fuerzan a las máquinas virtuales especificadas para que permanezcan separadas durante las acciones de conmutación por error.
- Las reglas de afinidad Máquina virtual-Host colocan máquinas virtuales especificadas en un host particular o un miembro de un grupo definido de hosts durante acciones de conmutación por error.

Cuando edite una regla de afinidad de DRS, active las casillas que aplican el comportamiento de conmutación por error deseado para vSphere HA.

- **HA must respect VM anti-affinity rules during failover** (HA debe respetar las reglas antiafinidad de la máquina virtual durante la conmutación por error): si las máquinas virtuales con esta regla se deben colocar juntas, se cancela la conmutación por error.
- **HA should respect VM to Host affinity rules during failover** (HA debe respetar las reglas de afinidad máquina virtual a host durante la conmutación por error): si es posible, vSphere HA intenta poner las máquina virtual con esta regla en los hosts especificados.

NOTA: vSphere HA puede reiniciar una máquina virtual en un clúster con DRS deshabilitado, con lo que se anula una asignación de reglas de afinidad Máquina virtual-Host si el error del host se produce poco después de configurar la regla (de forma predeterminada, en 5 minutos).

Otros problemas de interoperabilidad de vSphere HA

Para usar vSphere HA, debe tener en cuenta los siguientes problemas de interoperabilidad adicionales.

VM Component Protection (Protección de componentes de la máquina virtual)

VM Component Protection (VMCP) (Protección de componentes de la máquina virtual [VMCP]) tiene los siguientes problemas y limitaciones de interoperabilidad:

- VMCP no es compatible con vSphere Fault Tolerance. Si VMCP se habilita para un clúster mediante Fault Tolerance, las máquinas virtuales con FT afectadas recibirán automáticamente anulaciones que deshabilitan VMCP.
- VMCP no detecta ni responde a problemas de accesibilidad para archivos localizados en almacenes de datos de Virtual SAN. Si los archivos de configuración y VMDK de una máquina virtual están situados solo en almacenes de datos de Virtual SAN, no cuentan con protección de VMCP.
- VMCP no detecta ni responde a problemas de accesibilidad para archivos localizados en almacenes de datos de Virtual Volume. Si los archivos de configuración y VMDK de una máquina virtual están situados solo en almacenes de datos de Virtual Volume no cuentan con protección de VMCP.
- VMCP no protege contra asignación de dispositivos sin formato (RDM) inaccesible.

IPv6

vSphere HA se puede usar con configuraciones de red IPv6, que son plenamente compatibles si se cumplen las siguientes consideraciones:

- El clúster contiene solo hosts ESXi 6.0 o versiones posteriores.
- La red de administración para todos los hosts en el clúster debe configurarse con la misma versión de IP, ya sea IPv6 o IPv4. Los clústeres de vSphere HA no pueden contener ambos tipos de configuración de redes.
- Las direcciones de aislamiento de red que usa vSphere HA deben coincidir con la versión IP que utiliza el clúster para su red de administración.
- IPv6 no se puede usar en clústeres de vSphere HA que también emplean Virtual SAN.

Además de las restricciones anteriores, los siguientes tipos de direcciones IPv6 no son compatibles para usar con la dirección de aislamiento o red de administración de vSphere HA: local de vínculo, ORCHID y local de vínculo con índices de zona. Igualmente, el tipo de dirección de bucle invertido no se puede usar para la red de administración.

NOTA: Para actualizar una implementación existente de IPv4 a IPv6, primero debe deshabilitar vSphere HA.

Crear y configurar un clúster de vSphere HA

vSphere HA opera en el contexto de un clúster de hosts ESXi (o ESX heredado). Debe crear un clúster, rellenarlo con hosts y configurar los parámetros de vSphere HA antes de que pueda establecerse la protección de conmutación por error.

Cuando cree un clúster de vSphere HA, deberá configurar varios parámetros que determinan la manera en que funciona la característica. Antes de hacerlo, identifique los nodos del clúster. Estos nodos son los hosts ESXi que proporcionarán los recursos para admitir máquinas virtuales y que vSphere HA usará para la protección de conmutación por error. Después deberá determinar de qué forma se conectarán estos nodos entre sí y con el almacenamiento compartido donde se encuentran los datos de su máquina virtual. Después de que se instale esa arquitectura de redes, puede agregar los hosts al clúster y concluir la configuración de vSphere HA.

Puede habilitar y configurar vSphere HA antes de agregar nodos de hosts al clúster. Sin embargo, hasta que se agreguen los hosts, su clúster no estará totalmente operativo y parte de la configuración del clúster no estará disponible. Por ejemplo, la directiva de control de admisión Specify a Failover Host (Especificar hosts para conmutación por error) no está disponible hasta que haya un host que pueda designarse como el host para conmutación por error.

NOTA: La característica Virtual Machine Startup and Shutdown (automatic startup) (Inicio y apagado de máquina virtual [inicio automático]) está deshabilitada para todas las máquinas virtuales que residen en hosts que se encuentran en (o se agregan a) un clúster de vSphere HA. El inicio automático no se admite cuando se utiliza con vSphere HA.

Lista de comprobación de vSphere HA

La lista de comprobación de vSphere HA contiene requisitos que debe tener en cuenta antes de crear y utilizar un clúster de vSphere HA.

Repase esta lista antes de configurar un clúster de vSphere HA. Para obtener más información, siga la referencia adecuada.

- Todos los hosts deben tener licencias para vSphere HA.

- Un clúster debe contener al menos dos hosts.
- Todos los hosts deben estar configurados con direcciones IP estáticas. Si utiliza DHCP, debe asegurarse de que la dirección de cada host se mantiene después de los reinicios.
- Todos los hosts deben tener al menos una red de administración en común. La práctica recomendada es tener al menos dos redes de administración en común. Debe utilizar la red VMkernel con la casilla **Management traffic** (Tráfico de administración) habilitada. En las redes de administración, las redes deben poder accederse mutuamente, lo mismo que vCenter Server y los hosts. Consulte "Prácticas recomendadas para redes," página 41.
- Para asegurarse de que cualquier máquina virtual pueda ejecutarse en cualquier host en el clúster, todos los hosts deben tener acceso a las mismas redes y almacenes de datos de las máquinas virtuales. De manera similar, las máquinas virtuales deben estar ubicadas en el almacenamiento compartido, no local. De lo contrario, no podrán realizar conmutación por error en caso de un error en el host.

  NOTA: vSphere HA utiliza latidos del almacén de datos para distinguir entre hosts particionados, aislados y con errores. Por lo tanto, si algunos almacenes de datos son más confiables en el entorno, configure vSphere HA para que les otorgue preferencia.

- Para que la supervisión de máquina virtual funcione, VMware Tools debe estar instalado. Consulte "Supervisar máquina virtual y aplicaciones," página 17.
- vSphere HA es compatible con IPv4 e IPv6. Consulte "Otros problemas de interoperabilidad de vSphere HA," página 31 para ver las consideraciones cuando use IPv6.
- Para que VM Component Protection (Protección de componentes de la máquina virtual) funcione, los hosts deben tener la característica de tiempo de espera de todas las rutas de acceso inactivas (All Paths Down, APD) habilitada.
- Para utilizar VM Component Protection (Protección de componentes de la máquina virtual), los clústeres deben contener hosts ESXi 6.0 o posteriores.
- Solo los clústeres de vSphere HA que contengan hosts ESXi 6.0 o posteriores pueden utilizarse para habilitar VMCP. Los clústeres que contienen hosts de una versión anterior no pueden habilitar VMCP y esos hosts no pueden agregarse a un clúster habilitado para VMCP.
- Si su clúster utiliza almacenes de datos de Virtual Volume, cuando vSphere HA está habilitado, vCenter Server crea Virtual Volume de configuración en cada almacén de datos. En estos contenedores, vSphere HA almacena los archivos que utiliza para proteger las máquinas virtuales. vSphere HA no funciona correctamente si elimina estos contenedores. Solo se crea un contenedor por almacén de datos de Virtual Volume.

Crear un clúster de vSphere HA

Para habilitar su clúster para vSphere HA, primero debe crear un clúster vacío. Después de planificar los recursos y la arquitectura de redes de su clúster, use vSphere Web Client para agregar hosts al clúster y especificar la configuración de vSphere HA del clúster.

El clúster habilitado para vSphere HA es un requisito previo para Fault Tolerance.

Prerequisitos

- Compruebe que todas las máquinas virtuales y sus archivos de configuración residan en el almacenamiento compartido.
- Compruebe que los hosts estén configurados para acceder al almacenamiento compartido, de manera que pueda encender las máquinas virtuales utilizando diferentes hosts en el clúster.
- Compruebe que los hosts estén configurados para tener acceso a la red de máquina virtual.

- Compruebe que está usando conexiones de red de administración redundantes para vSphere HA. Para obtener información acerca de cómo configurar la redundancia de la red, consulte "Prácticas recomendadas para redes," página 41.
- Compruebe que ha configurado hosts con al menos dos almacenes de datos para ofrecer redundancia para la verificación de latidos del almacén de datos de vSphere HA.
- Conecte vSphere Web Client a vCenter Server utilizando una cuenta con permisos de administrador de clúster.

Procedimiento

1 En vSphere Web Client, desplácese hasta el centro de datos donde desea que resida el clúster y haga clic en **Create a Cluster** (Crear un clúster).

2 Complete el asistente New Cluster (Clúster nuevo).

No active vSphere HA (o DRS).

3 Haga clic en **OK** (Aceptar) para cerrar el asistente y crear un clúster vacío.

4 Según su plan para los recursos y la arquitectura de redes del clúster, use vSphere Web Client para agregar hosts al clúster.

5 Desplácese hasta el clúster y habilite vSphere HA.

   a Haga clic en la pestaña **Manage** (Administrar) y en **Settings** (Configuración).

   b Seleccione **vSphere HA** y haga clic en **Edit** (Editar).

   c Seleccione **Turn ON vSphere HA** (Activar).

6 Seleccione **Host Monitoring** (Supervisión de hosts)

Cuando se habilita Host Monitoring (Supervisión de hosts), se permite que los hosts del clúster intercambien latidos de red y que vSphere HA pueda tomar medidas cuando detecta errores. La función de supervisión de host es necesaria para que el proceso de recuperación de vSphere Fault Tolerance funcione correctamente.

7 Elija una configuración para **Virtual Machine Monitoring** (Supervisión de máquinas virtuales).

Seleccione **VM Monitoring Only** (Solo supervisión de máquina virtual) para reiniciar las máquinas virtuales individuales que no emitieron latidos por un tiempo determinado. También puede seleccionar **VM and Application Monitoring** (Supervisión de máquina virtual y aplicaciones) para habilitar la supervisión de aplicaciones.

8 Haga clic en **OK** (Aceptar).

Tiene un clúster de vSphere HA lleno de hosts.

Qué hacer a continuación

Configure las opciones de vSphere HA según sea adecuado para el clúster.

- Failure conditions and VM response (Condiciones de error y respuesta de la máquina virtual)
- Control de admisión
- Datastore for Heartbeating (Almacén de datos para verificar latidos)
- Opciones avanzadas

Consulte "Configurar clúster de vSphere HA," página 35.

Configurar clúster de vSphere HA

Cuando se crea un clúster vSphere HA o se configura un clúster existente, se debe ajustar la configuración que determina cómo funciona la característica.

En vSphere Web Client, puede establecer la siguiente configuración de vSphere HA:

Failure conditions and VM response (Condiciones de error y respuesta de la máquina virtual)	Proporcione aquí la configuración de VM restart priority (Prioridad de reinicio de la máquina virtual), Host isolation response (Respuesta para el aislamiento del host), VM monitoring sensitivity (Sensibilidad de supervisión de máquina virtual) y VM Component Protection (Protección de componentes de la máquina virtual).
Control de admisión	Habilite o deshabilite el control de admisión del clúster vSphere HA y elija una directiva para la manera en que se aplicará.
Datastore for Heartbeating (Almacén de datos para verificar latidos)	Especifique las preferencias de los almacenes de datos que utiliza vSphere HA para los latidos de almacén de datos.
Opciones avanzadas	Personalice el comportamiento de vSphere HA configurando las opciones avanzadas.

NOTA: Puede comprobar el estado de las tareas de configuración de vSphere HA en cada uno de los hosts de la consola Tasks (Tareas) de vSphere Web Client.

Configurar respuestas de máquinas virtuales

La página Failure conditions and VM response (Condiciones de error y respuesta de la máquina virtual) le permite elegir la configuración que determina la manera en que vSphere HA responde a errores de host y aislamientos. Esta configuración incluye la prioridad de reinicio de máquina virtual, la respuesta para el aislamiento del host, la configuración para protección de componentes de la máquina virtual y la sensibilidad de supervisión de la máquina virtual.

La página Virtual Machine Response (Respuesta de la máquina virtual) es editable solo si ha habilitado vSphere HA.

Procedimiento

1 En vSphere Web Client, desplácese hasta el clúster de vSphere HA.

2 Haga clic en la pestaña **Manage** (Administrar) y en **Settings** (Configuración).

3 En Settings (Configuración), seleccione **vSphere HA** y haga clic en **Edit** (Editar).

4 Expanda **Failure Conditions and VM Response** (Condiciones de error y respuesta de la máquina virtual) para visualizar las opciones de configuración.

Opción	Descripción
VM Restart Priority (Prioridad de reinicio de máquina virtual)	La prioridad de reinicio determina el orden en el que se reinician las máquinas virtuales cuando el host falla. Las máquinas virtuales con mayor prioridad se inician primero. Esta prioridad se aplica de forma individual para cada host. Si varios hosts fallan, todas las máquinas virtuales se migran del primer host en el orden de prioridad, después se migran todas las máquinas virtuales del segundo host en el orden de prioridad, etc.
Response for Host Isolation (Respuesta para el aislamiento del host)	La respuesta para el aislamiento del host determina lo que ocurre cuando un host en un clúster de vSphere HA pierde la conexión de red de su consola, pero sigue en funcionamiento.

Opción	Descripción
Response for Datastore with Permanent Device Loss (PDL) (Respuesta para un almacén de datos con pérdida permanente de dispositivos [Permanent Device Loss, PDL])	Esta configuración determina qué hace VMCP en caso de un error de PDL. Puede elegir entre las opciones de **Issue Events** (Emitir eventos) o **Power off and restart VMs** (Apagar y reiniciar las máquinas virtuales).
Response for Datastore with All Paths Down (APD) (Respuesta para almacén de datos con todas las rutas de acceso inactivas [All Paths Down, APD])	Esta configuración determina qué hace VMCP en caso de un error de APD. Puede elegir entre las opciones de **Issue Events** (Emitir eventos) o **Power off and restart VMs** (Apagar y reiniciar las máquinas virtuales) de forma conservadora o agresiva.
Delay for VM failover for APD (Retraso para conmutación por error de la máquina virtual para APD)	Esta configuración corresponde a la cantidad de minutos que VMCP espera antes de tomar medidas.
Response for APD recovery after APD timeout (Respuesta para recuperación de APD después del tiempo de espera de APD)	Puede elegir si VMCP restablece o no una máquina virtual en esta situación.
sensibilidad de la supervisión de la máquina virtual	Para configurar esta opción, mueva el control deslizante entre **Low** (Bajo) y **High** (Alto). También puede seleccionar **Custom** (Personalizado) para proporcionar una configuración personalizada.

5 Haga clic en **OK** (Aceptar).

Se aplicará su configuración de Virtual Machine Response (Respuesta de la máquina virtual).

Configurar el control de admisión

Después de crear un clúster, el control de admisión le permite especificar si se pueden iniciar máquinas virtuales, incluso su infringen restricciones de disponibilidad. El clúster reserva recursos para permitir la conmutación por error de todas las máquinas virtuales en ejecución en la cantidad de hosts especificada.

La página Admission Control (Control de admisión) aparece solo si ha habilitado vSphere HA.

Procedimiento

1 En vSphere Web Client, desplácese hasta el clúster de vSphere HA.

2 Haga clic en la pestaña **Manage** (Administrar) y en **Settings** (Configuración).

3 En Settings (Configuración), seleccione **vSphere HA** y haga clic en **Edit** (Editar).

4 Expanda **Admission Control** (Control de admisión) para visualizar las opciones de configuración.

5 Seleccione una directiva de control de admisión para aplicar al clúster.

Opción	Descripción
Define failover capacity by static number of hosts (Definir la capacidad de conmutación por error mediante una cantidad estática de hosts)	Seleccione la cantidad máxima de errores del host de los que se puede recuperar o de los que desea garantizar la conmutación por error. Igualmente, debe seleccionar una directiva de tamaño de ranura.
Define failover capacity by reserving a percentage of the cluster resources (Definir una capacidad de conmutación por error mediante la reserva de un porcentaje de los recursos del clúster)	Especifique un porcentaje de los recursos de memoria y de CPU del clúster que desea reservar como capacidad de reserva para admitir las conmutaciones por error.

Opción	Descripción
Usar dedicated failover hosts (Usar hosts con conmutación por error dedicados)	Seleccione los hosts que vaya a utilizar para las acciones de conmutación por error. Las conmutaciones por error igual pueden ocurrir en otros hosts en el clúster si un host de conmutación por error predeterminado no tiene suficientes recursos.
Do not reserve failover capacity (No reservar capacidad de conmutación por error)	Esta opción permite encendidos de máquinas virtuales que infringen restricciones de disponibilidad.

6 Haga clic en **OK** (Aceptar).

Admission control (Control de admisión) está habilitado y la directiva que elija entrará en vigor.

Configurar Datastore for Heartbeating (Almacén de datos para verificar latidos)

vSphere HA utiliza latidos de almacén de datos para distinguir entre los hosts con errores y los hosts que residen en una partición de red. Los latidos de almacén de datos permiten que vSphere HA supervise los hosts cuando se produce una partición de red de administración, y para que siga respondiendo a los errores que se producen.

Puede especificar los almacenes de datos que desea que se utilicen para verificar el latido del almacén de datos.

Procedimiento

1 En vSphere Web Client, desplácese hasta el clúster de vSphere HA.

2 Haga clic en la pestaña **Manage** (Administrar) y en **Settings** (Configuración).

3 En Settings (Configuración), seleccione **vSphere HA** y haga clic en **Edit** (Editar).

4 Expanda **Datastore for Heartbeating** (Almacén de datos para verificar latidos) para ver las opciones de configuración para verificar los latidos del almacén de datos.

5 Para proporcionar instrucciones a vSphere HA acerca de cómo seleccionar los almacenes de datos y la manera de tratar las preferencias, elija entre las siguientes opciones:

Tabla 2-3.

Opciones de latidos de almacén de datos
Automatically select datastores accessible from the host (Seleccionar automáticamente almacenes de datos accesibles desde el host)
Use datastores only from the specified list (Utilizar almacenes de datos solo desde la lista especificada)
Use datastores from the specified list and complement automatically if needed (Utilizar almacenes de datos desde la lista y el complemento especificados automáticamente si es necesario)

6 En el panel **Available heartbeat datastores** (Almacenes de datos de latidos disponibles), seleccione los almacenes de datos que desea usar para verificar los latidos.

Los almacenes de datos que figuran son los compartidos por más de un host en el clúster vSphere HA. Cuando se selecciona un almacén de datos, el panel inferior muestra todos los hosts en el clúster vSphere HA que pueden acceder a él.

7 Haga clic en **OK** (Aceptar).

Configurar opciones avanzadas

Para personalizar el comportamiento de vSphere HA, configure las opciones avanzadas de vSphere HA.

Prerequisitos

Compruebe que dispone de privilegios de administrador del clúster.

NOTA: Debido a que estas opciones afectan el funcionamiento de vSphere HA, cámbielas con precaución.

Procedimiento

1 En vSphere Web Client, desplácese hasta el clúster de vSphere HA.

2 Haga clic en la pestaña **Manage** (Administrar) y en **Settings** (Configuración).

3 En Settings (Configuración), seleccione **vSphere HA** y haga clic en **Edit** (Editar).

4 Expanda **Advanced Options** (Opciones avanzadas).

5 Haga clic en **Add** (Agregar) y escriba el nombre de la opción avanzada en el cuadro de texto.

Puede configurar el valor de la opción en el cuadro de texto de la columna Value (Valor).

6 Repita el paso 5 para cada nueva opción que desee agregar y haga clic en **OK** (Aceptar).

El clúster utiliza las opciones que haya agregado o modificado.

Qué hacer a continuación

Una vez que haya configurado una opción avanzada de vSphere HA, se mantendrá hasta que realice una de estas acciones:

- Utilizar vSphere Web Client para restablecer el valor predeterminado.
- Editar o eliminar manualmente la opción del archivo fdm.cfg en todos los hosts del clúster.

Opciones avanzadas de vSphere HA

Puede configurar opciones avanzadas que influyen en el comportamiento del clúster de vSphere HA.

Tabla 2-4. Opciones avanzadas de vSphere HA

Opción	Descripción
`das.isolationaddress[...]`	Determina la dirección a la que se hará ping con el fin de determinar si un host está aislado de la red. Se hace ping a esta dirección solo cuando no se reciben latidos de ningún otro host en el clúster. Si no se especifica, se usa la puerta de enlace predeterminada de la red de administración. Esta puerta de enlace predeterminada tiene que ser una dirección confiable que esté disponible, de manera que el host pueda determina si está aislado de la red. Puede especificar varias direcciones de aislamiento para el clúster (hasta 10): `das.isolationaddressX`, donde X = 0-9. Comúnmente, debe especificar una por red de administración. Si se especifican demasiadas direcciones, la detección de aislamiento tarda demasiado.
`das.usedefaultisolationaddress`	De forma predeterminada, vSphere HA utiliza como dirección de aislamiento la puerta de enlace predeterminada de la red de consola. Esta opción especifica si se usa o no esta puerta de enlace predeterminada (true|false).

Tabla 2-4. Opciones avanzadas de vSphere HA (Continua)

Opción	Descripción
das.isolationshutdowntimeout	El período que espera el sistema para que se desconecte una máquina virtual antes de apagarla. Esto solo se aplica si la respuesta de aislamiento del host es Shut down VM (Apagar máquina virtual). El valor predeterminado es 300 segundos.
das.slotmeminmb	Define el límite máximo del tamaño de ranura de memoria. Si se utiliza esta opción, el tamaño de ranura es el menor valor de este o la reserva de memoria máxima más la sobrecarga de memoria de cualquier máquina virtual encendida en el clúster.
das.slotcpuinmhz	Define el límite máximo del tamaño de ranura de CPU. Si se utiliza esta opción, el tamaño de ranura es el menor valor de este o la reserva de CPU máxima de cualquier máquina virtual encendida en el clúster.
das.vmmemoryminmb	Define el valor de recurso de memoria predeterminado asignado a una máquina virtual en caso de que su reserva de memoria no esté especificada o sea cero. Esto se usa para la directiva de control de admisión Host Failures Cluster Tolerates (Tolerancias del clúster para errores del host). Si no se especifica ninguno, el valor predeterminado es 0 MB.
das.vmcpuminmhz	Define el valor de recurso de CPU predeterminado asignado a una máquina virtual en caso de que su reserva de CPU no esté especificada o sea cero. Esto se usa para la directiva de control de admisión Host Failures Cluster Tolerates (Tolerancias del clúster para errores del host). Si no se especifica ninguno, el valor predeterminado es 32 MHz.
das.iostatsinterval	Cambia el intervalo de estadísticas de E/S predeterminado para sensibilidad de supervisión de la máquina virtual. El valor predeterminado es 120 (segundos). Puede configurarse para cualquier valor igual o superior a 0. Si se configura en 0 se desactiva la comprobación. **NOTA:** No se recomiendan valores inferiores a 50, ya que los valores menores pueden hacer que vSphere HA restablezca de forma inesperada una máquina virtual.
das.ignoreinsufficienthbdatastore	Desactiva problemas de configuración que se crean si el host no tiene suficientes almacenes de datos de latidos para vSphere HA. El valor predeterminado es false.
das.heartbeatdsperhost	Cambia la cantidad de almacenes de datos de latidos que se requieren. Los valores válidos pueden ir entre 2-5 y el valor predeterminado es 2.
fdm.isolationpolicydelaysec	La cantidad de segundos que espera el sistema antes de ejecutar la directiva de aislamiento una vez que se determina que un host está aislado. El valor mínimo es 30. Si se configura en un valor menor a 30, el retraso será de 30 segundos.

Tabla 2-4. Opciones avanzadas de vSphere HA (Continua)

Opción	Descripción
`das.respectvmvmantiaffinityrules`	Determina si vSphere HA aplica las reglas de antiafinidad entre máquinas virtuales. El valor predeterminado es "false", por lo que no se aplican las reglas. También se puede configurar en "true" y las reglas se aplican (incluso si vSphere DRS no está habilitado). En este caso, vSphere HA no realiza conmutación por error en una máquina virtual si ello infringe una regla, pero sí emite un evento que indica que no hay suficientes recursos para ejecutar la conmutación por error. Consulte *Administración de recursos de vSphere* para obtener más información sobre reglas de antiafinidad.
`das.maxresets`	La cantidad máxima de intentos de restablecimiento que hace VMCP. Si se produce un error en una operación de restablecimiento en una máquina virtual afectada por una situación de APD, VMCP reintenta el restablecimiento esta cantidad de veces antes de rendirse.
`das.maxterminates`	La cantidad máxima de reintentos que hace VMCP para finalización de máquinas virtuales.
`das.terminateretryintervalsec`	Si VMCP no finaliza una máquina virtual, esta es la cantidad de segundos que espera el sistema antes de que reintente un intento de finalización.
`das.config.fdm.reportfailoverfailevent`	Cuando está configurado en 1, habilita la generación de un evento por máquina virtual detallado cuando un intento por parte de vSphere HA para reiniciar una máquina virtual no resulte correcto. El valor predeterminado es 0. En versiones anteriores a vSphere 6.0, este evento se genera de forma predeterminada.
`vpxd.das.completemetadataupdateintervalsec`	El período (en segundos) después de que se establece una regla de afinidad Máquina virtual-Host durante el cual vSphere HA puede reiniciar una máquina virtual en un clúster de DRS deshabilitado, con lo que se anula la regla. El valor predeterminado es 300 segundos.
`das.config.fdm.memreservationmb`	De forma predeterminada, los agentes de vSphere HA se ejecutan con un límite de memoria configurado de 250 MB. Puede que un host no permita esta reserva si se ejecuta fuera de la capacidad reservable. Puede usar esta opción avanzada para disminuir el límite de memoria a fin de evitar este problema. Solo es posible especificar números enteros mayores de 100, que es el valor mínimo. Al contario, para evitar problemas durante las elecciones del agente maestro en un clúster grande (que contiene de 6.000 a 8.000 máquinas virtuales), debe elevar este límite a 325 MB. **NOTA:** Una vez que se cambia este límite, debe ejecutar la tarea Reconfigure HA (Volver a configurar alta disponibilidad) para todos los hosts en el clúster. Igualmente, cuando se agrega un nuevo host al clúster o se reinicia el host existente, esta tarea debe realizarse en estos hosts a fin de actualizar esta configuración de memoria.

NOTA: Si cambia el valor de cualquiera de las siguientes opciones avanzadas, debe deshabilitar y volver a habilitar vSphere HA para que sus cambios surtan efecto.

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

Personalizar una máquina virtual individual

Cada máquina virtual en un clúster de vSphere HA tiene asignada la configuración predeterminada del clúster para VM Restart Priority (Prioridad de reinicio de máquinas virtuales), Host Isolation Response (Respuesta de aislamiento del host), VM Component Protection (Protección de componentes de la máquina virtual) y VM Monitoring (Supervisión de máquinas virtuales). Si se cambian estos valores predeterminados se puede definir el comportamiento específico de cada máquina virtual. Si la máquina virtual sale del clúster, esta configuración se pierde.

Procedimiento

1 En vSphere Web Client, desplácese hasta el clúster de vSphere HA.

2 Haga clic en la pestaña **Manage** (Administrar) y en **Settings** (Configuración).

3 En Settings (Configuración), seleccione **VM Overrides** (Reemplazos por máquina virtual) y haga clic en **Add** (Agregar).

4 Use el botón **+** para seleccionar máquinas virtuales a las cuales aplicar los reemplazos.

5 Haga clic en **OK** (Aceptar).

6 (Opcional) Puede cambiar otra configuración, como **Automation level** (Nivel automático), **VM restart priority** (Prioridad de reinicio de máquinas virtuales), **Host isolation response** (Respuesta para el aislamiento del host), configuración de VMCP,**VM Monitoring** (Supervisión de máquinas virtuales) o la configuración de **VM monitoring sensitivity** (Sensibilidad de la supervisión de las máquinas virtuales).

NOTA: Puede ver los valores predeterminados del clúster para esta configuración expandiendo primero **Relevant Cluster Settings** (Configuración relevante del clúster) y luego ampliando **vSphere HA**.

7 Haga clic en **OK** (Aceptar).

Ahora el comportamiento de la máquina virtual se diferencia de los valores predeterminados del clúster para cada configuración que cambió.

Prácticas recomendadas para clústeres de vSphere HA

Para asegurar un rendimiento óptimo del clúster de vSphere HA, se deben seguir ciertas prácticas recomendadas. En esta sección se destacan algunas de las prácticas recomendadas clave para un clúster de vSphere HA.

También puede consultar la publicación *Prácticas recomendadas para la implementación de vSphere High Availability* para ver un análisis más detallado.

Prácticas recomendadas para redes

Siga las siguientes prácticas recomendadas para la configuración de NIC de host y topología de red para vSphere HA. Las prácticas recomendadas incluyen recomendaciones para los hosts ESXi, y para cableado, conmutadores, enrutadores y firewalls.

Configurar y realizar mantenimiento a la red

Las siguientes sugerencias de mantenimiento de la red pueden ayudarle a evitar la detección accidental de host con error y aislamiento de la red debido a baja de latidos de vSphere HA.

- Cuando se hacen cambios a las redes que en las que se encuentran sus hosts ESXi en clúster, suspenda la característica Host Monitoring (Supervisión de hosts). Si cambia su configuración de hardware de red o de redes, se pueden interrumpir los latidos que vSphere HA usa para detectar errores de host, y esto podría dar como resultado intentos no deseados de realizar conmutación por error en máquinas virtuales.

- Cuando cambia la configuración de redes en los hosts mismos de ESXi, por ejemplo, agregando grupos de puertos o quitando vSwitches, suspenda Host Monitoring (Supervisión de hosts). Después de que haya hecho los cambios de configuración de redes, debe volver a configurar vSphere HA en todos los hosts en el clúster, lo que hace que se vuelva a inspeccionar la información de la red. Luego vuelva a habilitar Host Monitoring (Supervisión de hosts).

NOTA: Debido a que las redes son un componente vital de vSphere HA, si es necesario realiza mantenimiento de red, informe al administrador de vSphere HA.

Redes usadas para comunicaciones de vSphere HA

Para identificar cuáles operaciones de red podrían interrumpir el funcionamiento de vSphere HA, debe saber cuáles redes de administración se están usando para determinación de latidos y otras comunicaciones de vSphere HA.

- En hosts ESX heredados en el clúster, las comunicaciones de vSphere HA pasan por todas las redes que están designadas como redes de consola de servicio. Estos hosts no usan redes de VMkernel para comunicaciones de vSphere HA. Para contener el tráfico de vSphere HA a un subconjunto de las redes de consola de ESX, use la opción avanzada `allowedNetworks`.
- En hosts ESXi en el clúster, las comunicaciones de vSphere HA pasan de forma predeterminada por redes de VMkernel. Con un host ESXi, si desea usar una red diferente a la que utiliza vCenter Server para comunicarse con el host para vSphere HA, debe habilitar explícitamente la casilla **Management traffic** (Tráfico de administración).

Para mantener el tráfico del agente de vSphere HA en las redes que ha especificado, configure hosts de manera que los vmkNIC que usa vSphere HA no compartan subredes con vmkNIC utilizados para otros fines. Los agentes de vSphere HA envían paquetes mediante el uso de cualquier pNIC que está asociado con una subred determinada si también hay al menos un vmkNIC configurado para tráfico de administración de vSphere HA. En consecuencia, para asegurar la separación de flujos de redes, los vmkNIC que emplea vSphere HA y otras características deben estar en subredes diferentes.

Direcciones de aislamiento de la red

Una dirección de aislamiento de la red es una dirección IP a la que se hace ping para determinar si un host está aislado de la red. Se hace ping a esta dirección solo cuando un host ha dejado de recibir latidos de todos los otros hosts en el clúster. Si un host puede hacer ping a su dirección de aislamiento de la red, el host no está aislado de la red y los otros hosts en el clúster han generado errores o están con partición de red. Sin embargo, si el host no puede hacer ping a su dirección de aislamiento, es probable que el host se haya aislado de la red y que no se tome una acción de conmutación por error.

De forma predeterminada, la dirección de aislamiento de la red es la puerta de enlace predeterminada para el host. Solo se especifica una puerta de enlace predeterminada, independientemente de cuántas redes de administración se hayan definido. Debe usar la opción avanzada `das.isolationaddress[...]` para agregar direcciones de aislamiento para redes adicionales. Consulte “Opciones avanzadas de vSphere HA,” página 38.

Redundancia de ruta de acceso de la red

La redundancia de ruta de acceso de la red entre nodos del clúster es importante para la confiabilidad de vSphere HA. Una sola red de administración termina siendo un único punto de error y puede dar como resultado conmutaciones por error aunque solo la red haya generado errores. Si tiene solo una red de administración, cualquier error entre el host y el clúster puede provocar una actividad de conmutación por error innecesaria (o falsa), en caso de que no se mantenga la conectividad del almacén de datos de latidos durante el error de redes. Entre los posibles errores se incluyen errores de NIC, de cables de red, de extracción de cables de red y de restablecimientos de conmutadores. Considere estas posibles fuentes de error entre hosts e intente minimizarlas, comúnmente mediante la entrega de redundancia de red.

La primera forma mediante la cual puede implementar redundancia de red es en el nivel de NIC con formación de equipos de NIC. El uso de un equipo de dos NIC conectadas para separar interruptores físicos separados mejora la confiabilidad de una red de administración. Debido a que los servidores conectados a través de dos NIC (y mediante conmutadores separados) tienen dos rutas de acceso independientes para enviar y recibir latidos, el clúster es más resistente. Para configurar un equipo de NIC para la red de administración, establezca las vNIC en la configuración de vSwitch para una configuración activa o en espera. Los parámetros de configuración recomendados para las vNICs son:

- Default load balancing = route based on originating port ID (Equilibrio de carga predeterminado = ruta basada en el identificador del puerto de origen)
- Failback = No (Conmutación por recuperación = No)

Después de que haya agregado una NIC a un host en su clúster de vSphere HA, debe volver a configurar vSphere HA en ese host.

En la mayoría de las implementaciones, la formación de equipos de NIC ofrece suficiente redundancia de latidos, pero como alternativa, puede crear una segunda conexión de red de administración conectada a un conmutador virtual separado. Las redes de administración redundante permite una detección confiable de errores y evita que se produzcan las condiciones de aislamiento o partición, ya que los latidos pueden enviarse a través de varias redes. La conexión de red de administración original se utiliza para fines de red y de administración. Cuando se crea la segunda conexión de red de administración, vSphere HA envía latidos a través de ambas conexiones de red de administración. Si hay error en una ruta de acceso, vSphere HA sigue enviando y recibiendo latidos a través de la otra ruta de acceso.

NOTA: Configure la menor cantidad posible de segmentos de hardware entre los servidores en un clúster. El objetivo es limitar puntos únicos de error. Además, las rutas con demasiados saltos pueden provocar retrasos de los paquetes de redes para latidos y aumentan los posibles puntos de error.

Usar configuraciones de red IPv6

Solo se debe asignar una dirección IPv6 a una interfaz de red determinada que usa su clúster de vSphere HA. La asignación de varias direcciones IP aumenta la cantidad de mensajes de latidos que envía el host maestro del clúster sin un correspondiente beneficio.

Prácticas recomendadas para la interoperabilidad

Siga estas prácticas recomendadas para permitir una interoperabilidad adecuada entre vSphere HA y otras características.

Interoperabilidad de vSphere HA y Storage vMotion en un clúster mixto

En los clústeres donde hay hosts ESXi 5.x y hosts ESX/ESXi 4.1 o versiones anteriores, y donde Storage vMotion se usa en gran medida o Storage DRS está habilitado, no implemente vSphere HA. vSphere HA podría responder a un error de host reiniciando una máquina virtual en un host con una versión de ESXi diferente de aquella en la que se ejecutaba la máquina virtual antes del error. Se puede producir un problema si, en el momento del error, la máquina virtual participaba en una acción de Storage vMotion en un host ESXi 5.x, y vSphere HA reinicia la máquina virtual en un host con una versión anterior a ESXi 5.0. Aunque es posible que la máquina virtual se encienda, cualquier intento posterior en operaciones de creación de instantáneas podrían dañar el estado del vdisk y dejar la máquina virtual inutilizable.

Usar Auto Deploy con vSphere HA

Puede usar vSphere HA y Auto Deploy de forma conjunta para mejorar la disponibilidad de sus máquinas virtuales. Auto Deploy aprovisiona los hosts cuando se encienden y también se puede configurar para que instale el agente de vSphere HA en aquellos hosts durante el proceso de arranque. Para conocer más detalles, consulte la documentación de Auto Deploy incluida en Instalación y configuración de vSphere.

Actualizar hosts en un clúster mediante Virtual SAN

Si va a actualizar los hosts ESXi en su clúster de vSphere HA a la versión 5.5 o una superior, y también tiene pensado usar Virtual SAN, siga este proceso.

1 Actualice todos los hosts.

2 Deshabilite vSphere HA.

3 Habilite Virtual SAN.

4 Vuelva a habilitar vSphere HA.

Prácticas recomendadas para control de admisión

Siga estas prácticas recomendadas para la configuración y uso de control de admisión para vSphere HA.

Las siguientes recomendaciones son las prácticas recomendadas para control de admisión de vSphere HA.

- Seleccione la directiva de control de admisión Percentage of Cluster Resources Reserved (Porcentaje de recursos del clúster reservados). Esta directiva ofrece la mayor flexibilidad en términos de tamaño de host y de máquina virtual. Cuando configure esta directiva, escoja un porcentaje para CPU y memoria que refleje la cantidad de errores de host que desea admitir. Por ejemplo, si desea que vSphere HA aparte recursos para dos errores de host y tiene diez hosts con igual capacidad en el clúster, entonces especifique 20 % (2/10).
- Asegúrese de asignar un tamaño igual para todos los hosts del clúster. Para la directiva Host Failures Cluster Tolerates (Tolerancias del clúster para errores del host), un clúster desequilibrado da como resultado un exceso de capacidad que se va a reservar para controlar errores debido a que vSphere HA reserva capacidad para los hosts más grandes. Para la directiva Percentage of Cluster Resources (Porcentaje de recursos del clúster), un clúster desequilibrado requiere que especifique mayores porcentajes que de otra manera serían necesarios para reservar suficiente capacidad para el número anticipado de errores de host.
- Si planea usar la directiva Host Failures Cluster Tolerates (Tolerancias del clúster para errores del host), intente mantener los requisitos de tamaño de máquina virtual similares entre todas las máquinas virtuales configuradas. Esta directiva utiliza tamaños de ranura para calcular la cantidad de capacidad necesaria que se debe reservar para cada máquina virtual. El tamaño de ranura se basa en la mayor memoria y CPU reservadas que se necesiten para cualquier máquina virtual. Cuando mezcle máquinas virtuales con diferentes requisitos de CPU y memoria, el cálculo de tamaño de ranura tiene un valor predeterminado del más grande posible, lo que limita la consolidación.
- Si planea usar la directiva Specify Failover Hosts (Especificar hosts para conmutación por error), decida cuántos errores de hosts se admitirán y luego especifique este número de hosts como hosts para conmutación por error. Si el clúster está desequilibrado, los hosts para conmutación por error designados deben ser al menos del mismo tamaño que los hosts sin conmutación por error en su clúster. Esto asegura que haya una capacidad adecuada en caso de error.

Prácticas recomendadas para supervisión de clústeres

Siga estas prácticas recomendadas para supervisar el estado y validez de su clúster de vSphere HA.

Configurar alarmas para supervisar cambios del clúster

Cuando vSphere HA o Fault Tolerance toman medidas para mantener la disponibilidad, por ejemplo, una conmutación por error de máquina virtual, puede recibir notificaciones de dichos cambios. Configure alarmas en vCenter Server para que se activen cuando se produzcan estas acciones y haga que se envíen las alertas (como correos electrónicos) a un conjunto específico de administradores.

Hay varias alarmas predeterminadas de vSphere HA disponibles.

- Recursos insuficientes para conmutación por error (una alarma de clúster)
- No se puede encontrar un maestro (una alarma de clúster)
- Conmutación por error en curso (una alarma de clúster)
- Estado de HA del host (una alarma de host)
- Error de supervisión de máquina virtual (una alarma de máquina virtual)
- Acción de supervisión de máquina virtual (una alarma de máquina virtual)
- Error de conmutación por error (una alarma de máquina virtual)

NOTA: Las alarmas predeterminadas incluyen el nombre de la característica, vSphere HA.

Supervisar la validez del clúster

Un clúster válido es aquel en el cual no se ha infringido la directiva de control de admisión.

Un clúster habilitado para vSphere HA queda invalidado cuando la cantidad de máquinas virtuales encendidas supera los requisitos de conmutación por error, es decir, la capacidad de conmutación por error actual es menor a la capacidad configurada para esto. Si se deshabilita el control de admisión, los clústeres no quedan invalidados.

En vSphere Web Client, seleccione **vSphere HA** en la pestaña **Monitor** (Supervisar) del clúster y luego seleccione **Configuration Issues** (Problemas de configuración). Aparece una lista de problemas actuales de vSphere HA.

El comportamiento de DRS no se ve afectado si un clúster está en rojo debido a un problema de vSphere HA.

Proporcionar Fault Tolerance para máquinas virtuales 3

Es posible utilizar vSphere Fault Tolerance con las máquinas virtuales para garantizar la continuidad del negocio con mayores niveles de disponibilidad y protección de datos que los que ofrece vSphere HA.

Fault Tolerance está integrado en la plataforma de host ESXi y proporciona disponibilidad continua mediante la ejecución de máquinas virtuales idénticas en hosts distintos.

Para lograr resultados óptimos con Fault Tolerance, es necesario familiarizarse con su modo de funcionamiento, la forma de habilitarlo para el clúster y las máquinas virtuales, y las prácticas recomendadas para su utilización.

Protección de Fault Tolerance para máquinas virtuales (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_fault_tolerance_protection_vms)

Este capítulo cubre los siguientes temas:

Funcionamiento de Fault Tolerance

Puede utilizar vSphere Fault Tolerance (FT) para la mayoría de las máquinas virtuales de misión crítica. FT ofrece disponibilidad continua para máquinas virtuales de este tipo mediante la creación y el mantenimiento de máquinas virtuales idénticas y con disponibilidad continua para reemplazarlas en caso de una situación de conmutación por error.

La máquina virtual protegida se conoce como la máquina virtual principal. La máquina virtual duplicada (la secundaria) se crea y ejecuta en otro host. La ejecución de la máquina virtual secundaria es idéntica a la de la máquina virtual principal y puede asumir su control en cualquier punto sin interrupción, con lo que proporciona protección con Fault Tolerance.

Las máquinas virtuales principales y secundarias supervisan de forma continua sus estados mutuos a fin de asegurar que se mantenga Fault Tolerance. Si hay error del host que ejecuta la máquina virtual principal, se produce una conmutación por error transparente, en cuyo caso la máquina virtual secundaria se activa inmediatamente para reemplazar la máquina virtual principal. Se inicia una nueva máquina virtual secundaria y la redundancia de Fault Tolerance se restablece automáticamente. Si se produce un error en el host que ejecuta la máquina virtual secundaria, también se reemplaza de inmediato. En cualquier caso, los usuarios no experimentan interrupción en el servicio ni hay pérdida de datos.

Una máquina virtual con Fault Tolerance y su copia secundaria no deben ejecutarse en el mismo host. Esta restricción asegura que, si hay un error del host, ello no redunde en una pérdida de ambas máquinas virtuales.

NOTA: También puede utilizar las reglas de afinidad Máquina virtual-Host para indicar en qué hosts pueden funcionar las máquinas virtuales designadas. Si utiliza estas reglas, tenga en cuenta que para cualquier máquina virtual principal que se vea afectada por dicha regla, su máquina virtual secundaria asociada también se verá afectada por esa regla. Para obtener más información acerca de reglas de afinidad, consulte la documentación de *Administración de recursos de vSphere*.

Fault Tolerance evita situaciones de "cerebro dividido", lo que puede derivar en dos copias activas de una máquina virtual después de una recuperación de un error. El bloqueo de archivos atómico en almacenamiento compartido se utiliza para coordinar conmutación por error de manera que solo un lado siga en ejecución como la máquina virtual principal y reaparezca automáticamente una nueva máquina virtual secundaria.

vSphere Fault Tolerance puede aceptar máquinas virtuales con multiprocesador simétrico (SMP) con hasta cuatro vCPU. Versiones anteriores de vSphere utilizaban una tecnología diferente para Fault Tolerance (que se conoce como FT heredada), con distintos requisitos y características (incluida una limitación de vCPU únicas para máquinas virtuales de FT heredadas). Si se requiere compatibilidad con estos requisitos anteriores, puede utilizar FT heredada. Sin embargo, esto implica la configuración de una opción avanzada para cada máquina virtual. Consulte "Fault Tolerance heredado," página 61 para obtener más información.

Casos de uso de Fault Tolerance

Hay varias situaciones típicas que pueden aprovechar el uso de vSphere Fault Tolerance.

Fault Tolerance proporciona un mayor nivel de continuidad empresarial que vSphere HA. Cuando se solicita a una máquina virtual secundaria que reemplace a su máquina virtual principal, la máquina virtual secundaria asume de inmediato el control de la función de la máquina virtual principal y se mantiene la totalidad del estado de la máquina virtual. No es necesario volver a introducir o cargar las aplicaciones que ya se estaban ejecutando ni los datos que estaban almacenados en la memoria. Esto es diferente de la conmutación por error proporcionada por vSphere HA, que reinicia las máquinas virtuales que se ven afectadas por un error.

Este mayor nivel de continuidad, así como la protección adicional de la información del estado y de los datos, informa sobre los escenarios en los que es conveniente implementar Fault Tolerance.

- Las aplicaciones que deben estar disponibles todo el tiempo, en especial las que tienen conexiones de clientes de larga duración que los usuarios quieren mantener durante los errores de hardware.
- Las aplicaciones personalizadas que no tienen otra forma de agrupar en clústeres.
- Los casos donde podría proporcionarse alta disponibilidad mediante soluciones personalizadas de creación de clústeres, que son demasiado complicadas para configurar y mantener.

Otro caso de uso clave para proteger una máquina virtual con Fault Tolerance puede describirse como On-Demand Fault Tolerance. En este caso, una máquina virtual se protege adecuadamente con vSphere HA durante el funcionamiento normal. Durante ciertos períodos críticos, sería recomendable mejorar la protección de la máquina virtual. Por ejemplo, podría estar ejecutando un informe de fin de trimestre que, si se interrumpe, retrasaría la disponibilidad de información de misión crítica. Con vSphere Fault Tolerance,

puede proteger esta máquina virtual antes de ejecutar este informe y después apagar o suspender Fault Tolerance una vez que se haya generado el informe. Puede usar On-Demand Fault Tolerance para proteger la máquina virtual durante un período de tiempo crítico y volver los recursos a la normalidad durante la operación no crítica.

Requisitos, límites y concesión de licencias de Fault Tolerance

Antes de usar vSphere Fault Tolerance (FT), considere los requisitos, los límites y la concesión de licencias de alto nivel que se aplican a esta característica.

Requisitos

Los siguientes requisitos de CPU y redes se aplican a FT.

Las CPU que se utilizan en máquinas host para máquina virtual con Fault Tolerance deben ser compatibles con vSphere vMotion o estar mejoradas con Enhanced vMotion Compatibility. Igualmente, se requieren CPU que admitan virtualización de MMU de hardware (Intel EPT o RVI AMD). Se admiten las siguientes CPU.

- Intel Sandy Bridge o posterior. Avoton no es compatible.
- AMD Bulldozer o posterior.

Use una red de registro de 10 Gbit para FT y verifique que la red tenga baja latencia. Se recomienda contar con una red de FT dedicada.

Límites

En un clúster configurado para que use Fault Tolerance, se aplican dos límites de forma independiente.

das.maxftvmsperhost	La cantidad máxima de máquinas virtuales con Fault Tolerance que se permiten en un host en el clúster. Tanto las máquinas virtuales principales como las secundarias se contabilizan para este límite. El valor predeterminado es 4.
das.maxftvcpusperhost	La cantidad máxima de CPU que se agregan por todas las máquinas virtuales con Fault Tolerance en un host. Para este límite se contabilizan tanto las vCPU de máquinas virtuales principales como las de máquinas virtuales secundarias. El valor predeterminado es 8.

Licencias

La cantidad de vCPU que admite una sola máquina virtual con Fault Tolerance está limitada por el nivel de licencias que haya adquirido para vSphere. Fault Tolerance se admite de las siguientes maneras:

- vSphere Standard y Enterprise. Permite hasta 2 vCPU.
- vSphere Enterprise Plus. Permite hasta 4 vCPU.

NOTA: FT y FT heredado no se admiten en vSphere Essentials y vSphere Essentials Plus.

Interoperabilidad de Fault Tolerance

vSphere Fault Tolerance se enfrenta a algunas limitaciones con respecto a las características de vSphere, los dispositivos y otras características con las que puede interoperar.

Antes de configurar vSphere Fault Tolerance, debe conocer las funciones y los productos con los que Fault Tolerance no puede interoperar.

Características de vSphere no compatibles con Fault Tolerance

Cuando configure el clúster, debe tener en cuenta que no todas las características de vSphere pueden interoperar con Fault Tolerance.

Las siguientes características de vSphere no son compatibles con las máquinas virtuales con Fault Tolerance.

- Instantáneas. Las instantáneas deben quitarse o confirmarse antes de que sea posible habilitar Fault Tolerance en una máquina virtual. Además, no es posible crear instantáneas de máquinas virtuales en las que esté habilitado Fault Tolerance.

  NOTA: Las instantáneas solo de disco creadas para las copias de seguridad de vStorage APIs - Data Protection (VADP) son compatibles con Fault Tolerance. Sin embargo, FT heredado no es compatible con VADP.

- Storage vMotion. No puede invocar Storage vMotion para máquinas virtuales con Fault Tolerance activado. Para migrar el almacenamiento, debe desactivar temporalmente Fault Tolerance y realizar la acción de vMotion para almacenamiento. Cuando esto haya concluido, puede volver a activar Fault Tolerance.
- Clones vinculados. No puede usar Fault Tolerance en una máquina virtual que sea un clon vinculado, ni tampoco puede crear un clon vinculado a partir de una máquina virtual con FT habilitado.
- VM Component Protection (VMCP) (Protección de componentes de la máquina virtual [VMCP]). Si su clúster tiene VMCP habilitado, se crean anulaciones para las máquinas virtuales con Fault Tolerance que desactivan esta característica.
- Almacenes de datos de Virtual Volumes.
- Administración de directivas basadas en almacenamiento.
- Filtros de E/S.

Características y dispositivos incompatibles con Fault Tolerance

No todos los dispositivos, características o productos de terceros pueden interoperar con Fault Tolerance.

Para que una máquina virtual sea compatible con Fault Tolerance, dicha máquina no debe usar las siguientes características o dispositivos.

Tabla 3-1. Características y dispositivos incompatibles con Fault Tolerance y acciones correctivas

Característica o dispositivo incompatible	Acción correctiva
Asignación de disco sin procesar (RDM) física.	Con FT heredado, puede volver a configurar máquinas virtuales con dispositivos virtuales a los que se les hizo una copia de seguridad con RDM física para usar RMD virtuales en su lugar.
Dispositivos virtuales en CD-ROM y disquete cuya copia de seguridad se hizo mediante un dispositivo físico o remoto.	Quite el dispositivo virtual en CD-ROM o disquete y vuelva a configurar la copia de seguridad con un ISO instalado en el almacenamiento compartido.
Dispositivos USB y de sonido.	Quite estos dispositivos de la máquina virtual
Virtualización de identificador de puerto N (NPIV).	Deshabilite la configuración de NPIV de la máquina virtual.
Acceso directo de la NIC.	Esta característica no es compatible con Fault Tolerance por lo que debe desactivarse.

Tabla 3-1. Características y dispositivos incompatibles con Fault Tolerance y acciones correctivas (Continua)

Característica o dispositivo incompatible	Acción correctiva
Dispositivos de conexión directa.	La característica de conexión en caliente se deshabilita de forma automática para máquinas virtuales con Fault Tolerance. Para conectar dispositivos en caliente (ya sea mediante adición o extracción), debe desactivar temporalmente Fault Tolerance, realizar la conexión directa y luego habilitar Fault Tolerance. **NOTA:** Cuando se utiliza Fault Tolerance, el cambio de la configuración de una tarjeta de red virtual mientras una máquina virtual está en ejecución corresponde a una operación de conexión directa, ya que en necesario "desconectar" la tarjeta de red y luego volver a "conectarla". Por ejemplo, con una tarjeta de red virtual para una máquina virtual en ejecución, si cambia la red a la que está conectada la NIC virtual, primero debe desactivarse FT.
Puertos serie o paralelos	Quite estos dispositivos de la máquina virtual
Dispositivos de vídeo que tienen 3D habilitado.	Fault Tolerance no es compatible con dispositivos de vídeo que tienen 3D habilitado.
Firmware EFI virtual	Asegúrese de que la máquina virtual esté configurada para que utilice firmware del BIOS antes de instalar el sistema operativo invitado.
Interfaz de comunicación de máquina virtual (VMCI)	No compatible con Fault Tolerance.
VMDK de más de 2 TB	Fault Tolerance no es compatible con un VMDK de más de 2 TB.

Usar Fault Tolerance con DRS

Puede usar vSphere Fault Tolerance con vSphere Distributed Resource Scheduler (DRS) solo cuando está habilitada la función Enhanced vMotion Compatibility (EVC). Este proceso permite que las máquinas virtuales con Fault Tolerance se beneficien de una mejor colocación inicial.

Cuando un clúster tiene EVC habilitado, DRS hace las recomendaciones de colocación inicial para las máquinas virtuales con Fault Tolerance y permite asignar un nivel de automatización de DRS a las máquinas virtuales principales (la máquina virtual secundaria siempre supone la misma configuración que su máquina virtual principal asociada).

Cuando vSphere Fault Tolerance se utiliza para máquinas virtuales en un clúster que tiene EVC deshabilitado, se otorgan niveles de automatización de DRS de "disabled" (deshabilitado) a las máquinas virtuales con Fault Tolerance. En dicho clúster, cada máquina virtual principal se enciende solo en su host registrado y su máquina virtual secundaria se coloca automáticamente.

Si utiliza reglas de afinidad con un par de máquinas virtuales con Fault Tolerance, se aplica una regla de afinidad Máquina virtual-Máquina virtual solo a la máquina virtual principal, mientras que una regla de afinidad Máquina virtual-Host se aplica tanto a la máquina virtual principal como a su máquina virtual secundaria. Si se establece una regla de afinidad Máquina virtual-Máquina virtual para una máquina virtual principal, DRS intenta corregir cualquier infracción que se produzca después de una conmutación por error (es decir, después de que la máquina virtual principal se mueve a un nuevo host).

Preparar el clúster y los hosts para Fault Tolerance

Para habilitar vSphere Fault Tolerance en el clúster, debe cumplir con los requisitos previos de la característica y seguir ciertos pasos de configuración en los hosts. Una vez completados esos pasos y creado el clúster, también puede comprobar que la configuración cumpla con los requisitos para habilitar Fault Tolerance.

Las tareas que se deben completar antes de intentar habilitar Fault Tolerance en el clúster son las siguientes:

- Asegúrese de que el clúster, los hosts y las máquinas virtuales cumplan con los requisitos descritos en la lista de comprobación de Fault Tolerance.
- Configure las redes para cada host.
- Cree el clúster de vSphere HA, agregue hosts y compruebe el cumplimiento.

Una vez preparados el clúster y los hosts para Fault Tolerance, ya estará listo para activar Fault Tolerance en las máquinas virtuales. Consulte "Activar Fault Tolerance," página 56.

Lista de comprobación de Fault Tolerance

La siguiente lista de comprobación contiene requisitos de clúster, host y máquina virtual que se deben tener en cuenta antes de utilizar vSphere Fault Tolerance.

Revise la lista antes de configurar Fault Tolerance.

NOTA: La conmutación por error de las máquinas virtuales con tolerancia a errores es independiente de vCenter Server, pero se debe utilizar vCenter Server para configurar los clústeres de Fault Tolerance.

Requisitos de clúster para Fault Tolerance

Se deben cumplir los siguientes requisitos de clúster antes de utilizar Fault Tolerance.

- El registro de Fault Tolerance y las redes de VMotion deben estar configurados. Consulte "Configurar redes para equipos host," página 53.
- Se debe haber creado y habilitado el clúster de vSphere HA. Consulte "Crear y configurar un clúster de vSphere HA," página 32. vSphere HA debe estar habilitado para poder encender las máquinas virtuales con tolerancia a errores o para agregar un host a un clúster que ya admite máquinas virtuales con tolerancia a errores.

Requisitos de host para Fault Tolerance

Se deben cumplir los siguientes requisitos de host antes de utilizar Fault Tolerance.

- Los hosts deben utilizar procesadores compatibles.
- Los hosts deben tener licencia para Fault Tolerance.
- Los hosts deben estar certificados para Fault Tolerance. Consulte http://www.vmware.com/resources/compatibility/search.php y seleccione **Search by Fault Tolerant Compatible Sets** (Buscar por conjuntos compatibles con tolerancia a errores) para determinar si los hosts están certificados.
- La configuración para cada host debe tener habilitada la virtualización de hardware (HV) en el BIOS.

NOTA: VMware recomienda que la configuración de administración de energía del BIOS de los hosts que se utilicen para admitir máquinas virtuales de FT esté definida en "Maximum performance" (Rendimiento máximo) u "OS-managed performance" (Rendimiento administrado por sistema operativo).

Para confirmar la compatibilidad de los hosts en el clúster a fin de admitir Fault Tolerance, se pueden ejecutar comprobaciones de cumplimiento de perfiles como se describe en "Crear un clúster y comprobar el cumplimiento," página 54.

Requisitos de la máquina virtual para Fault Tolerance

Se deben cumplir los siguientes requisitos de máquina virtual antes de utilizar Fault Tolerance.

- No debe haber ningún dispositivo no compatible conectado a la máquina virtual. Consulte "Interoperabilidad de Fault Tolerance," página 49.
- Las características no compatibles no se deben ejecutar en máquinas virtuales con tolerancia a errores. Consulte "Interoperabilidad de Fault Tolerance," página 49.
- Los archivos de máquina virtual se deben almacenar en el almacenamiento compartido. Las soluciones aceptables de almacenamiento compartido incluyen canal de fibra, iSCSI (hardware y software), NFS y NAS.

Otras recomendaciones de configuración

Se deben cumplir las siguientes instrucciones al configurar Fault Tolerance.

- Si se utiliza NFS para acceder al almacenamiento compartido, utilice hardware de NAS dedicado con al menos una NIC de 1 Gbit para obtener el rendimiento de red requerido para que Fault Tolerance funcione correctamente.
- La reserva de memoria de una máquina virtual con tolerancia a errores se establece de acuerdo con el tamaño de memoria de la máquina virtual cuando Fault Tolerance está activado. Compruebe que un grupo de recursos que contenga máquinas virtuales con tolerancia a errores tenga recursos de memoria cuyo tamaño de memoria sea mayor que el de las máquinas virtuales. Sin este exceso en el grupo de recursos, es posible que no haya memoria disponible para utilizar como memoria de sobrecarga.
- Utilice un máximo de 16 discos virtuales por máquina virtual con tolerancia a errores.
- Para garantizar la redundancia y una protección óptima de Fault Tolerance, se deben tener tres hosts en el clúster como mínimo. Durante una situación de conmutación por error, esto proporciona un host que puede alojar la nueva máquina virtual secundaria que se crea.

Configurar redes para equipos host

En cada host que desee agregar a un clúster de vSphere HA, deberá configurar dos conmutadores de redes diferentes (vMotion y registro de FT), de manera que el host pueda admitir vSphere Fault Tolerance.

Para habilitar Fault Tolerance para un host, debe realizar este procedimiento para cada opción de grupo de puertos (vMotion y registro de FT) a fin de asegurar que haya suficiente ancho de banda disponible para el registro de Fault Tolerance. Seleccione una opción, finalice este procedimiento y repítalo una segunda vez seleccionando la otra opción de grupo de puertos.

Prerequisitos

Se requieren tarjetas de interfaz de red (NIC) de varios gigabits. Para cada host compatible con Fault Tolerance, se recomienda un mínimo de dos NIC físicas. Por ejemplo, se necesita una dedicada al registro de Fault Tolerance y una dedicada a vMotion. Utilice tres NIC o más para garantizar la disponibilidad.

NOTA: Las NIC de vMotion y de registro de FT deben estar en diferentes subredes. Si va a utilizar FT heredada, IPv6 no es compatible en la NIC de registro de FT.

Procedimiento

1 En vSphere Web Client, desplácese hasta el host.

2 Haga clic en la pestaña **Manage** (Administrar) y en **Networking** (Redes).

3 Haga clic en el icono **Add host networking** (Agregar redes de host).

4 Seleccione **VMkernel Network Adapter** (Adaptadores de red de VMkernel) en la página Select Connection Type (Seleccionar tipo de conexión) y haga clic en **Next** (Siguiente).

5 Seleccione **New standard switch** (Nuevo conmutador estándar) y haga clic en **Next** (Siguiente).

6 Asigne adaptadores de red físicos al conmutador y haga clic en **Next** (Siguiente).

7 Proporcione una etiqueta de red, habilite los servicios que desea y haga clic en **Next** (Siguiente).

8 Proporcione una dirección IP y una máscara de subred y haga clic en **Finish** (Finalizar) después de revisar su configuración.

Después de crear un conmutador virtual de registro de Fault Tolerance y vMotion, puede crear otros conmutadores virtuales según sea necesario. Agregue el host al clúster y finalice cualquier paso necesario para habilitar Fault Tolerance.

Qué hacer a continuación

NOTA: Si configura redes para admitir FT, pero posteriormente suspende el puerto de registro de Fault Tolerance, los pares de máquinas virtuales de Fault Tolerance, que se enciendan permanecerán encendidos. Si se produce una situación de conmutación por error, cuando la máquina virtual principal se reemplaza con su máquina virtual secundaria, no se inicia una nueva máquina virtual secundaria, con lo que la nueva máquina virtual principal se ejecuta en un estado Not Protected (Sin protección).

Crear un clúster y comprobar el cumplimiento

vSphere Fault Tolerance se utiliza en el contexto de un clúster de vSphere HA. Después de configurar las redes en cada host, cree el clúster de vSphere HA y agréguele hosts. Puede comprobar si el clúster está configurado correctamente y si cumple con los requisitos para la habilitación de Fault Tolerance.

Procedimiento

1 En vSphere Web Client, desplácese hasta el clúster.

2 Haga clic en la pestaña **Monitor** (Supervisar) y luego en **Profile Compliance** (Cumplimiento del perfil).

3 Haga clic en **Check Compliance Now** (Comprobar cumplimiento ahora) para ejecutar las pruebas de cumplimiento.

Aparecen los resultados de la prueba de cumplimiento y se muestra el cumplimiento o el incumplimiento de cada host.

Usar Fault Tolerance

Después de que haya realizado todos los pasos necesarios para habilitar vSphere Fault Tolerance para el clúster, puede utilizar la característica habilitándola para máquinas virtuales individuales.

Antes de que se pueda activar Fault Tolerance, se realizan comprobaciones de validación en una máquina virtual.

Después de pasar las comprobaciones y de activar vSphere Fault Tolerance para una máquina virtual, se agregan nuevas opciones a la sección a la sección de Fault Tolerance de su menú contextual. Entre estas se incluyen la desactivación o deshabilitación de Fault Tolerance, la migración de la máquina virtual secundaria, las pruebas de conmutación por error y las pruebas de reinicio de la máquina virtual secundaria.

Realizar comprobaciones de validación para activación de Fault Tolerance

Si la opción para activar Fault Tolerance se encuentra disponible, esta tarea aún debe validarse y puede generar errores si no se cumplen ciertos requisitos.

Antes de poder activar Fault Tolerance, se realizan varias comprobaciones de validación en una máquina virtual.

- Debe estar activada la comprobación de certificado SSL en la configuración de vCenter Server.
- El host debe estar en un clúster de vSphere HA o un clúster mixto de vSphere HA y DRS.
- El host debe tener ESXi 6.x o una versión superior instalada (ESX/ESXi 4.x o versión superior para FT heredado).
- La máquina virtual no debe tener instantáneas.
- La máquina virtual no debe ser una plantilla.
- La máquina virtual no debe tener vSphere HA deshabilitado.
- La máquina virtual no debe tener un dispositivo de vídeo con 3D habilitado.

Comprobar si existen máquinas virtuales encendidas

Se realizan varias comprobaciones de validación adicionales para máquinas virtuales encendidas (o aquellas que están en proceso de encendido).

- El BIOS de los hosts donde se encuentran las máquinas virtuales con Fault Tolerance deben tener habilitado Hardware Virtualization (HV) (Virtualización de hardware).
- El host que admite la máquina virtual principal debe tener un procesador que sea compatible con Fault Tolerance.
- Su hardware debe contar con certificación de compatibilidad con Fault Tolerance. Para confirmar que la tiene, use la Guía de compatibilidad de VMware en http://www.vmware.com/resources/compatibility/search.php y seleccione **Search by Fault Tolerant Compatible Sets** (Buscar por conjuntos compatibles con Fault Tolerance).
- La configuración de la máquina virtual debe ser válida para usar con Fault Tolerance (por ejemplo, no debe contener ningún dispositivo no compatible).

Colocación de máquina virtual secundaria

Cuando su trabajo de activación de Fault Tolerance para una máquina virtual pasa las comprobaciones de validación, se crea la máquina virtual secundaria. La colocación y estado inmediato de la máquina virtual secundaria depende de si se encendió o apagó la máquina virtual principal cuando encendió Fault Tolerance.

Si la máquina virtual principal está encendida:

- Si pasa el control de admisión, se copia el estado completo de la máquina virtual principal y la máquina virtual secundaria se crea, se coloca en un host compatible separado y se enciende.
- El estado de Fault Tolerance que aparece para la máquina virtual es **Protected** (Protegida).

Si la máquina virtual principal está apagada:

- Se crea de inmediato la máquina virtual secundaria y se registra en un host en el clúster (podría volver a registrarse en un host más apropiado cuando se encienda).
- La máquina virtual secundaria no se enciende hasta después de que lo hace la máquina virtual principal.

- El estado de Fault Tolerance que aparece para la máquina virtual es **Not Protected, VM not Running** (No protegido, máquina virtual no está funcionando).
- Cuando intenta encender la máquina virtual principal después de que se ha encendido Fault Tolerance, se realizan las comprobaciones de validación adicionales que se indicaron más arriba.

  Después de pasar todas estas comprobaciones, las máquinas virtuales principales y secundarias se encienden y se colocan en hosts compatibles separados. El estado de Fault Tolerance de la máquina virtual se etiqueta como **Protected** (Protegida).

Activar Fault Tolerance

Puede activar vSphere Fault Tolerance mediante vSphere Web Client.

Cuando Fault Tolerance está activado, vCenter Server restablece el límite de memoria de la máquina virtual y configura la reserva de memoria en el tamaño de memoria de la máquina virtual. Aunque Fault Tolerance permanezca activado, no es posible cambiar la reserva, el tamaño y el límite de memoria, la cantidad de vCPU o los recursos compartidos. Tampoco puede agregar ni quitar discos de la máquina virtual. Cuando Fault Tolerance está apagado, cualquier parámetro que se haya cambiado no se revierte a los valores originales.

Conecte vSphere Web Client a vCenter Server utilizando una cuenta con permisos de administrador de clúster.

Prerequisitos

La opción para activar Fault Tolerance no se encuentra disponible (atenuada) en caso de que se aplique cualquiera de estas condiciones:

- La máquina virtual se encuentra en un host que no tiene una licencia para la característica.
- La máquina virtual se encuentra en un host que está en modo de mantenimiento o de espera.
- La máquina virtual está desconectada o huérfana (no se puede acceder a su archivo .vmx).
- El usuario no tiene permisos para activar la característica.

Procedimiento

1. En vSphere Web Client, desplácese hasta la máquina virtual para la cual desea activar Fault Tolerance.
2. Haga clic con el botón derecho en la máquina virtual y seleccione **Fault Tolerance > Turn On Fault Tolerance (Activar Fault Tolerance)**.
3. Haga clic en **Yes** (Sí).
4. Seleccione un almacén de datos para colocar los archivos de configuración de la máquina virtual secundaria. A continuación, haga clic en **Next** (Siguiente).
5. Seleccione un host en el que colocar la máquina virtual secundaria. A continuación, haga clic en **Next** (Siguiente).
6. Revise las selecciones y, a continuación, haga clic en **Finish** (Finalizar).

La máquina virtual especificada está designada como máquina virtual principal, y una máquina virtual secundaria se establece en otro host. La máquina virtual principal ahora tiene tolerancia a errores.

Desactivar Fault Tolerance

Si se desactiva vSphere Fault Tolerance, se eliminan la máquina virtual secundaria, su configuración y todo el historial.

Utilice la opción **Turn Off Fault Tolerance** (Desactivar Fault Tolerance) si no tiene pensado volver a habilitar la característica. De lo contrario, utilice la opción **Suspend Fault Tolerance** (Suspender Fault Tolerance).

NOTA: Si la máquina virtual secundaria reside en un host que está en modo de mantenimiento, desconectado o que no responde, no se puede utilizar la opción **Turn Off Fault Tolerance** (Desactivar Fault Tolerance). En este caso, debe suspender y reanudar Fault Tolerance.

Procedimiento

1 En vSphere Web Client, desplácese hasta la máquina virtual para la cual desea desactivar Fault Tolerance.

2 Haga clic con el botón derecho en la máquina virtual y seleccione **Fault Tolerance > Turn Off Fault Tolerance (Desactivar Fault Tolerance)**.

3 Haga clic en **Yes** (Sí).

Fault Tolerance se desactiva en la máquina virtual seleccionada. Se eliminarán el historial y la máquina virtual secundaria de la máquina virtual seleccionada.

Suspender Fault Tolerance

La suspensión de vSphere Fault Tolerance para una máquina virtual suspende su protección de Fault Tolerance, pero mantiene la máquina virtual secundaria y todo el historial. Use esta opción para reanudar la protección de Fault Tolerance en el futuro.

Procedimiento

1 En vSphere Web Client, desplácese hasta la máquina virtual para la cual desea suspender Fault Tolerance.

2 Haga clic con el botón derecho en la máquina virtual y seleccione **Fault Tolerance > Suspend Fault Tolerance (Suspender Fault Tolerance)**.

3 Haga clic en **Yes** (Sí).

Fault Tolerance se suspende para la máquina virtual seleccionada. Todo el historial y la máquina virtual secundaria de la máquina virtual seleccionada se mantienen y se usarán en caso de que se reanude la característica.

Qué hacer a continuación

Después de suspender Fault Tolerance, para reanudar la característica, seleccione **Resume Fault Tolerance** (Reanudar Fault Tolerance).

Migrar máquina secundaria

Una vez que vSphere Fault Tolerance se encienda para una máquina virtual principal, podrá migrar su máquina virtual secundaria asociada.

Procedimiento

1 En vSphere Web Client, desplácese hasta la máquina virtual principal para la cual desea migrar su máquina virtual secundaria.

2 Haga clic con el botón derecho en la máquina virtual y seleccione **Fault Tolerance > Migrate Secondary (Migrar máquina secundaria)**.

3 Siga las opciones en el cuadro de diálogo Migrate (Migrar) y confirme los cambios que ha realizado.

4 Haga clic en **Finish** (Finalizar) para aplicar los cambios.

La máquina virtual secundaria asociada a la máquina virtual con tolerancia a errores se migra al host especificado.

Probar conmutación por error

Es posible inducir una situación de conmutación por error de una máquina virtual principal seleccionada a fin de probar la protección de Fault Tolerance.

Esta opción no se encuentra disponible (está atenuada) si la máquina virtual está apagada.

Procedimiento

1 En vSphere Web Client, desplácese hasta la máquina virtual principal en la cual desea probar la conmutación por error.

2 Haga clic con el botón derecho en la máquina virtual y seleccione **Fault Tolerance > Test Failover (Probar conmutación por error)**.

3 Vea detalles sobre la conmutación por error en la consola de la tarea.

Esta tarea induce un error en la máquina virtual principal para garantizar que la máquina virtual secundaria la reemplace. También se inicia una nueva máquina virtual secundaria cuando se vuelve a colocar la máquina virtual principal en estado protegido.

Probar reinicio de la máquina secundaria

Puede inducir el error de una máquina virtual secundaria para probar la protección Fault Tolerance provista para una máquina virtual principal seleccionada.

Esta opción no se encuentra disponible (está atenuada) si la máquina virtual está apagada.

Procedimiento

1 En vSphere Web Client, desplácese hasta la máquina virtual principal en la cual desea realizar la prueba.

2 Haga clic con el botón derecho en la máquina virtual y seleccione **Fault Tolerance > Test Restart Secondary (Probar reinicio de máquina secundaria)**.

3 Vea detalles sobre la prueba en la consola de la tarea.

Esta tarea da como resultado la terminación de la máquina virtual secundaria que brinda protección Fault Tolerance a la máquina virtual principal seleccionada. Se inicia una nueva máquina virtual secundaria, que vuelve a poner la máquina virtual principal en un estado Protected (Protegida).

Actualizar los hosts utilizados para Fault Tolerance

Use el siguiente procedimiento para actualizar los hosts que se usan para Fault Tolerance.

Prerequisitos

Compruebe que dispone de privilegios de administrador del clúster.

Compruebe que tiene conjuntos de cuatro o más hosts ESXi que alojen máquinas virtuales con Fault Tolerance que estén encendidas. Si las máquinas virtuales están apagadas, las máquinas virtuales principales y secundarias se pueden reubicar en hosts con diferentes compilaciones.

NOTA: Este procedimiento de actualización es para un clúster con un mínimo de cuatro nodos. Se pueden seguir las mismas instrucciones para un clúster de menor tamaño, aunque el intervalo sin protección será ligeramente más prolongado.

Procedimiento

1 Utilice vMotion para migrar las máquinas virtuales con Fault Tolerance desde dos hosts.

2 Actualice los dos hosts evacuados a la misma compilación de ESXi.

3 Suspenda Fault Tolerance en la máquina virtual principal.

4 Utilice vMotion para mover la máquina virtual principal para la cual Fault Tolerance se haya suspendido a uno de los hosts actualizados.

5 Reanude Fault Tolerance en la máquina virtual principal que se movió.

6 Repita del Step 1 al Step 5 para tantos pares de máquinas virtuales con Fault Tolerance como se puedan aceptar en los hosts actualizados.

7 Utilice vMotion para redistribuir las máquinas virtuales con Fault Tolerance.

Todos los hosts ESXi de un clúster estarán actualizados.

Prácticas recomendadas de Fault Tolerance

Para garantizar resultados óptimos con Fault Tolerance, se deben seguir ciertas prácticas recomendadas.

Las siguientes recomendaciones para la configuración de hosts y redes pueden ayudar a mejorar la estabilidad y el rendimiento del clúster.

Configuración de hosts

Los hosts que ejecutan las máquinas virtuales principales y secundarias deben operar aproximadamente a la misma frecuencia de procesador. Las características de administración de energía de la plataforma que no se ajusten según la carga de trabajo (por ejemplo, topes de energía y modos de baja frecuencia aplicados para ahorrar energía) pueden provocar una gran variación en la frecuencia del procesador. Si las máquinas virtuales secundarias se reinician de manera regular, deshabilite todos los modos de administración de energía en los hosts que ejecutan máquinas virtuales con tolerancia a errores o compruebe que todos los hosts se ejecuten en los mismos modos de administración de energía.

Configurar redes del host

Las siguientes instrucciones permiten configurar las redes del host para que admitan Fault Tolerance con diferentes combinaciones de tipos de tráfico (por ejemplo, NFS) y números de NIC físicas.

- Distribuya cada equipo de NIC en dos conmutadores físicos para garantizar la continuidad del dominio L2 de cada VLAN entre los dos conmutadores físicos.
- Utilice directivas de formación de equipos determinísticas para garantizar que tipos de tráfico específicos tengan una afinidad con una NIC determinada (activa/en espera) o un grupo de NIC (por ejemplo, identificador de puerto virtual de origen).
- En casos donde se utilicen directivas activas/en espera, vincule los tipos de tráfico para minimizar el impacto en una situación de conmutación por error donde los dos tipos de tráfico comparten una vmnic.

- En casos donde se utilicen directivas activas/en espera, configure todos los adaptadores activos para un tipo de tráfico específico (por ejemplo, registro de FT) en el mismo conmutador físico. Esto minimiza la cantidad de saltos de red y disminuye la posibilidad de que se produzca un exceso de suscripciones del conmutador en vínculos del conmutador.

NOTA: El tráfico de registro de FT entre la máquina virtual principal y la secundaria está descifrado y contiene datos de la red invitada y de la E/S de almacenamiento, como también contenido de memoria del sistema operativo invitado. Este tráfico puede incluir datos sensibles como contraseñas en texto sin formato. Para evitar que estos datos se divulguen, asegúrese de que la red esté protegida, especialmente contra ataques de intermediarios ("Man in the middle"). Por ejemplo, puede utilizar una red privada para el tráfico de registro de FT.

Clústeres homogéneos

vSphere Fault Tolerance puede funcionar en clústeres con hosts no uniformes, pero funciona mejor en clústeres con nodos compatibles. Al construir su clúster, todos los hosts deben tener la siguiente configuración:

- Acceso común a los almacenes de datos utilizados por las máquinas virtuales.
- La misma configuración de red de la máquina virtual.
- La misma configuración del BIOS (administración de energía e hiperproceso) para todos los hosts.

Ejecute **Check Compliance** (Comprobar cumplimiento) para identificar incompatibilidades y corregirlas.

Rendimiento

Para aumentar el ancho de banda disponible para el tráfico de registro entre máquinas virtuales principales y secundarias, se utiliza una NIC de 10 Gbit y se habilita la utilización de tramas gigantes.

ISO en almacenamiento compartido para acceso continuo

Almacene las imágenes ISO a las que acceden las máquinas virtuales con la función Fault Tolerance habilitada en un almacenamiento compartido al que puedan acceder ambas instancias de la máquina virtual con tolerancia a errores. Si se utiliza esta configuración, el CD-ROM de la máquina virtual sigue funcionando con normalidad, incluso cuando ocurre una conmutación por error.

Para máquinas virtuales con la función Fault Tolerance habilitada, se pueden utilizar imágenes ISO que sean accesibles solo para la máquina virtual principal. En este caso, la máquina virtual principal puede acceder a la imagen ISO; pero si se produce una conmutación por error, el CD-ROM informa de errores como si no hubiera soportes físicos. Esta situación puede ser aceptable si el CD-ROM se utiliza para una operación temporal y no crítica (por ejemplo, una revisión).

Evitar particiones de red

Una partición de red se produce cuando un clúster de vSphere HA tiene un error en la red de administración que aísla algunos de los hosts de vCenter Server entre sí. Consulte “Particiones de red,” página 19. Cuando se produce una partición, la protección de Fault Tolerance puede degradarse.

En un clúster de vSphere HA particionado con Fault Tolerance, la máquina virtual principal (o su máquina virtual secundaria) podría terminar en una partición administrada por un host maestro que no es responsable de la máquina virtual. Cuando se necesita una conmutación por error, la máquina virtual secundaria se reinicia solo si la máquina virtual principal estaba en una partición administrada por el host maestro responsable de ella.

Para asegurar que su red de administración tenga menos probabilidades de experimentar un error que lleve a una partición de la red, siga las recomendaciones en “Prácticas recomendadas para redes,” página 41.

Utilizar almacenes de datos de Virtual SAN

vSphere Fault Tolerance puede utilizar almacenes de datos de Virtual SAN, pero se deben tener en cuenta las siguientes restricciones:

- Las máquinas virtuales principales y secundarias no admiten la mezcla de Virtual SAN y otros tipos de almacenes de datos.
- FT no admite clústeres metro de Virtual SAN.

Para aumentar el rendimiento y la confiabilidad mediante FT con Virtual SAN, también se recomiendan las siguientes condiciones.

- Virtual SAN y FT deben utilizar redes distintas.
- Conserve las máquinas virtuales principales y secundarias en dominios de errores de Virtual SAN distintos.

Fault Tolerance heredado

De manera predeterminada, vSphere Fault Tolerance (FT) puede incluir máquinas virtuales con multiprocesador simétrico (SMP) con hasta cuatro vCPU. Sin embargo, si su máquina virtual tiene solo una vCPU, puede usar FT heredado para compatibilidad con versiones anteriores. A menos que sea técnicamente necesario, no se recomienda usar FT heredado.

Para usar Fault Tolerance heredado, debe configurar una opción avanzada para la máquina virtual. Después de concluir esta configuración, la máquina virtual con FT heredado es diferente de cierta forma respecto de otras máquina virtual con Fault Tolerance.

Diferencias de las máquinas virtuales que usan FT heredado

Las máquinas virtuales que usan FT y las máquinas virtuales que utilizan FT heredado se diferencian de varias formas.

Tabla 3-2. Diferencias entre FT heredado y FT

	FT heredado	FT
Tablas de páginas extendidas/Indexación de virtualización rápida (EPT/RVI)	No compatible	Obligatorio
IPv6	No compatibles para NIC de registro de FT heredado.	Compatible para NIC de registro de FT.
DRS	Totalmente compatible para la colocación inicial, el equilibrio de carga y la compatibilidad con modo de mantenimiento.	Solo se admite la colocación de encendido de máquinas virtuales secundarias y el modo de mantenimiento.
API de vStorage - copias de seguridad para protección de datos	No compatible	Compatible
Archivos .vmdk de disco grueso puestos a cero	Obligatorio	No se requiere debido a que FT es compatible con todos los tipos de archivo de disco, incluidos los gruesos y los finos.
Redundancia de .vmdk	Solo una copia	Las máquinas virtuales principales y las secundarias siempre mantienen copias independientes que se pueden colocar en diferentes almacenes de datos para aumentar la redundancia.

Tabla 3-2. Diferencias entre FT heredado y FT (Continua)

	FT heredado	FT
Ancho de banda de la NIC	Se recomienda una NIC dedicada de 1 Gb	Se recomienda una NIC dedicada de 10 Gb
Compatibilidad de CPU y host	Requiere versiones idénticas de modelo y familia de CPU y versiones casi idénticas de vSphere en los hosts.	Las CPU deben ser compatibles con vSphere vMotion o EVC. Las versiones de vSphere en los hosts deben ser compatibles con vSphere vMotion.
Activar FT en máquina virtual en ejecución	No siempre es compatible. Puede que primero necesite apagar la máquina virtual.	Compatible
Storage vMotion	Compatible solo en máquinas virtuales apagadas. vCenter Server desactiva automáticamente FT antes de realizar una acción de Storage vMotion y luego activa FT nuevamente después de que concluya la acción de Storage vMotion.	No compatible. El usuario debe desactivar FT para la máquina virtual antes de realizar la acción de Storage vMotion y luego volver a activar FT.
Controladores de redes de vlance	No compatible	Compatible

Requisitos adicionales para FT heredado

Además de las diferencias que se indican para FT heredado, también tiene los siguientes requisitos únicos.

- Su clúster debe contener al menos dos hosts con certificación de FT que ejecuten la misma versión de Fault Tolerance o el mismo número de compilación de host. El número de versión de Fault Tolerance aparece en la pestaña **Summary** (Resumen) del host en vSphere Web Client.
- Los hosts ESXi deben tener acceso a los mismos almacenes de datos y redes de máquina virtual.
- Las máquinas virtuales deben estar almacenadas en archivos RDM virtuales o archivos de disco de máquina virtual (VMDK) que tienen aprovisionamiento grueso. Si una máquina virtual está almacenada en un archivo de VMDK que tienen aprovisionamiento fino y se hace un intento de usar Fault Tolerance, un mensaje indica que se debe convertir el archivo de VMDK. Para realizar la conversión, debe apagar la máquina virtual.
- Los hosts deben tener procesadores del grupo de procesadores compatibles con FT. Compruebe que los procesadores de los hosts sean compatibles entre sí.
- El host que es compatible con la máquina virtual secundaria debe tener un procesador que sea compatible con Fault Tolerance y que tenga la misma familia o modelo de CPU que el host que admite la máquina virtual principal.
- Cuando actualice hosts que contienen máquinas virtuales con Fault Tolerance, compruebe que las máquinas virtuales principales y secundarias sigan ejecutándose en hosts con el mismo número de versión de FT o número de compilación del host (para hosts anteriores a ESX/ESXi 4.1).

NOTA: Si designó una máquina virtual para que usara FT heredado antes de actualizar los hosts en el clúster, esa máquina virtual sigue utilizando FT heredado después de la actualización del host.

Habilitar Fault Tolerance heredado

Para usar Fault Tolerance heredado, debe configurar una opción avanzada para la máquina virtual.

El FT heredado se puede usar solo con máquinas virtuales que tienen una única vCPU y que aún no utilizan FT. Para habilitar FT heredado para cada máquina virtual que va a utilizarlo, debe configurar la opción avanzada `vm.uselegacyft` en un valor **true**.

Procedimiento

1 En vSphere Web Client, desplácese hasta la máquina virtual.

2 Haga clic con el botón derecho en la máquina virtual y seleccione **Edit Settings** (Editar configuración).

3 Haga clic en la pestaña **VM Options** (Opciones de máquina virtual).

4 Abra la sección **Advanced** (Opciones avanzadas) y, junto a **Configuration Parameters** (Parámetros de configuración), haga clic en **Edit Configuration** (Editar configuración).

5 Haga clic en **Add Row** (Agregar fila) e introduzca `vm.uselegacyft` para Name (Nombre) y **true** para Value (Valor).

6 Haga clic en **OK** (Aceptar).

FT heredado ahora está habilitado para esa máquina virtual.

Índice

R

S

T

V