Article
Estevan Martinez · Nov 27, 2019 10m read

Mirroring de la base de datos sin una dirección IP virtual

++ Update: August 1, 2018

El uso de la dirección IP virtual (VIP) de InterSystems incorporada en Mirroring de la base de datos de Caché tiene ciertas limitaciones. En particular, solo puede utilizarse cuando los miembros Mirror se encuentran en la misma subred. Cuando se utilizan varios centros de datos, las subredes normalmente no se " extienden " más allá del centro de datos físico debido a la complejidad añadida de la red (puede obtener más información aquí). Por las mismas razones, la IP virtual con frecuencia no puede utilizarse cuando la base de datos se aloja en la nube.

Los dispositivos para la administración del tráfico de red, como los balanceadores de carga (físicos o virtuales), pueden utilizarse para lograr el mismo nivel de transparencia, presentando una dirección única para las aplicaciones o dispositivos del cliente. El administrador para el tráfico de red redirige automáticamente a los clientes hacia la dirección IP real de la Mirror principal actual. La automatización tiene por objeto satisfacer las necesidades tanto de la tolerancia contra fallos de HA como para la promoción de la DR después de un desastre.

Integración de un Administrador de Tráfico de la Red

Hoy en día existen numerosas opciones en el mercado que son compatibles con la redirección del tráfico de red. Cada una de ellas admite metodologías similares e incluso varias para controlar el flujo de la red basada en los requisitos de la aplicación. Para simplificar estas metodologías, consideramos tres categorías: API llamada por el servidor de base de datos, el Sondeo de la Red de Aplicaciones, o una combinación de ambos.

En la siguiente sección se describirá cada una de estas metodologías y se proporcionará orientación sobre la forma en que cada una de ellas puede integrarse con los productos de InterSystems. En todos los escenarios, el árbitro se utiliza para proporcionar decisiones seguras de la tolerancia contra fallos cuando los miembros Mirror no pueden comunicarse directamente. Puede encontrar más información sobre el árbitro aquí .

Para cumplir con los objetivos de este artículo, en los diagramas de ejemplo se mostrarán 3 miembros Mirror: principal, copia de seguridad y DR asíncronos. Sin embargo, reconocemos que su configuración puede ser más grande o menor a esto.

Opción 1: Sondeo de la Red de Aplicaciones (*Recomendado*)

En este método, el dispositivo de red con carga equilibrada utiliza el mecanismo de sondeo incorporado para comunicarse con ambos miembros Mirror con el fin de determinar al miembro Mirror principal.

El método de sondeo que utiliza la página mirrorstatus.cxw de CSP Gateway está disponible en la versión 2017.1, puede utilizarse como método de sondeo en el supervisor de estado del ELB para cada miembro Mirror que se añadió al grupo de servidores del ELB. Únicamente la miembro Mirror principal responderá ' SUCCESS ', dirigiendo así el tráfico de red solo al miembro Mirror principal que esté activo.

En este método no es necesario agregar cualquier lógica a ^ZMIRROR. Tenga en cuenta que la mayoría de los dispositivos de red con carga equilibrada tienen un límite en la frecuencia de ejecución de la comprobación de estado. Normalmente, la frecuencia más alta no es menor de 5 segundos, lo cual es aceptable para admitir la mayoría de los acuerdos en el nivel de servicio para el tiempo de actividad.

Una solicitud HTTP para el siguiente recurso probará cuál es el estado del miembro espejo para la configuración LOCAL de Caché.

/csp/bin/mirrorstatus.cxw

Para todos los demás casos, la ruta hacia estas solicitudes de estado de réplica deben resolverse en el servidor de Caché y en el Namespace apropiados, mediante el mismo mecanismo jerárquico, como el que se utiliza para solicitar páginas reales en el CSP.

Por ejemplo, para probar el estado de configuración de la Mirror que presenta a las aplicaciones en la ruta /csp/user/, se utiliza:

/csp/user/mirrorstatus.cxw

Note: Una licencia CSP no se consume cuando se llama a la comprobación de estado de la Mirror.

Dependiendo de si la instancia de destino es o no un miembro principal activo, la puerta de enlace devolverá alguna de las siguientes respuestas del CSP:

**** Éxito (Es el Miembro Principal)**

==========

HTTP/1.1 200 OK

Content-Type: text/plain

Connection: close

Content-Length: 7

SUCCESS

**** Se produjo un error (no es el Miembro Principal)**

==========

HTTP/1.1 503 Service Unavailable

Content-Type: text/plain

Connection: close

Content-Length: 6

FAILED

**** Se produjo un error (El servidor de Caché no es compatible con la solicitud MirrorStatus.cxw)**

==========

HTTP/1.1 500 Internal Server Error

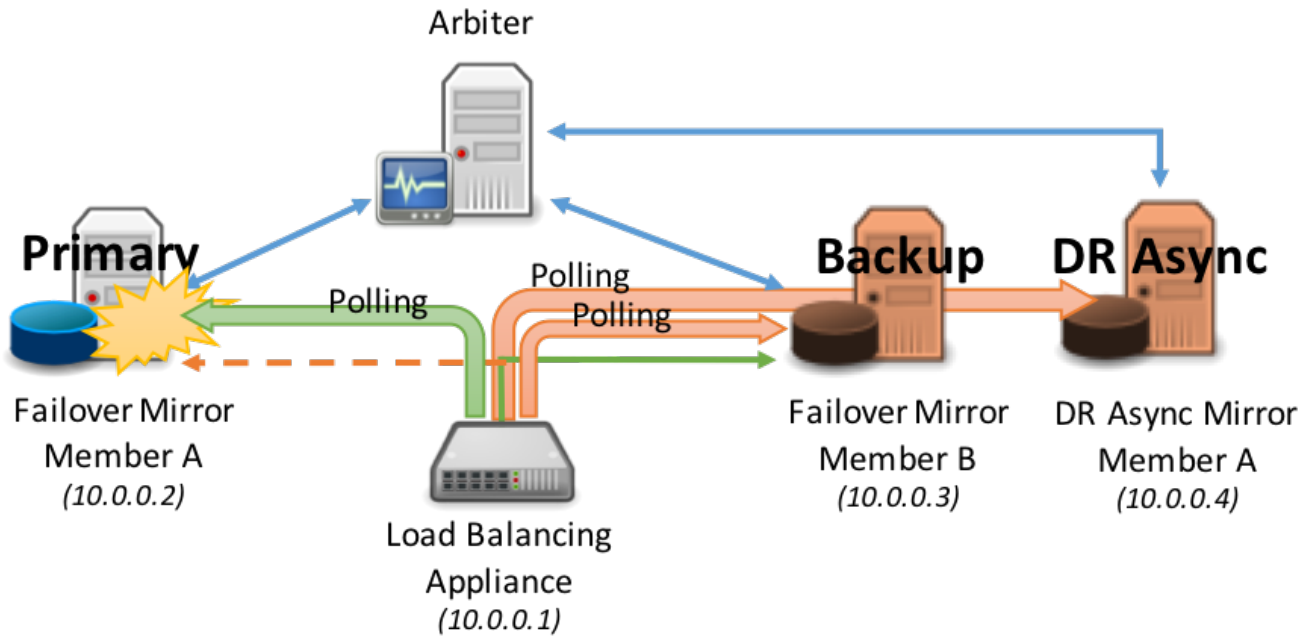
Content-Type: text/plain

Connection: close

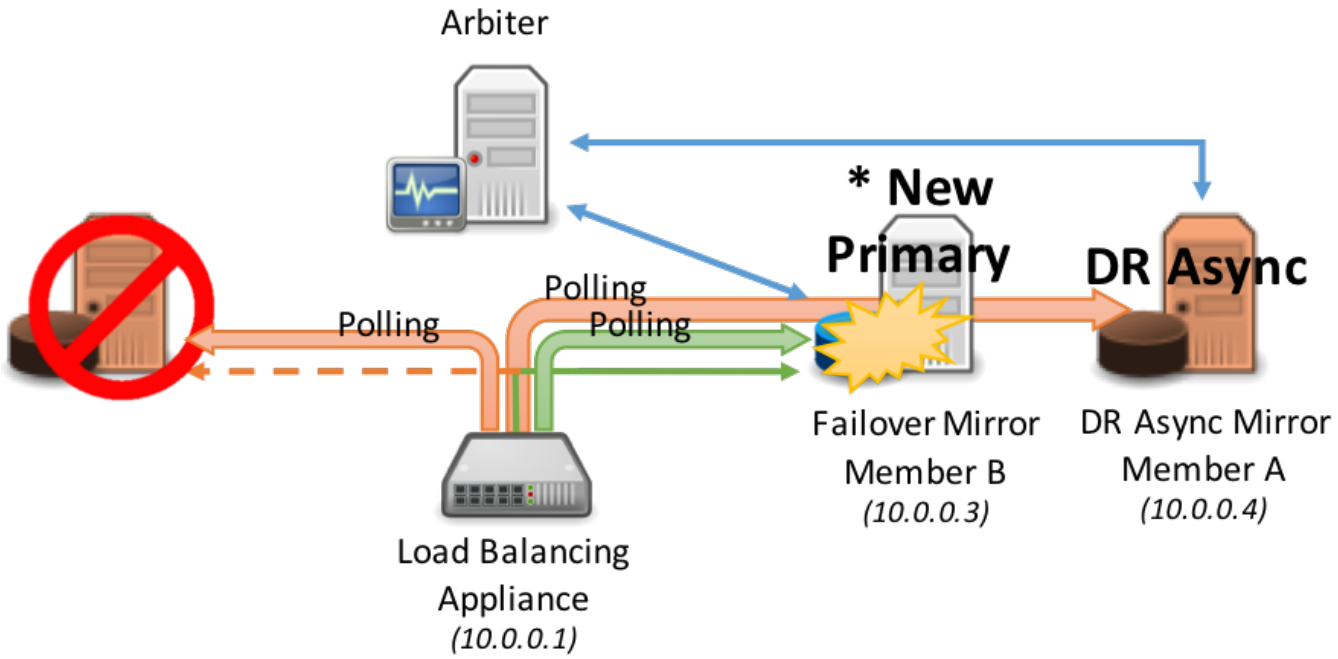
Content-Length: 6

FAILED

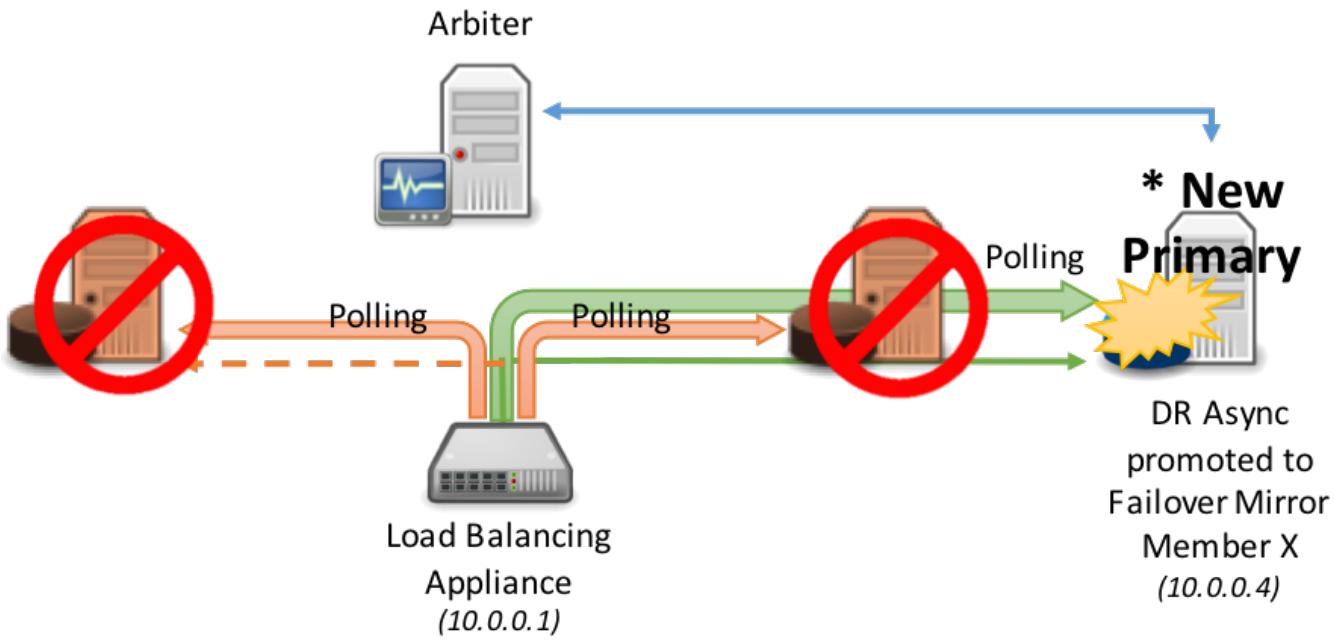
Considere los siguientes diagramas como un ejemplo de sondeo.



La tolerancia contra fallos se produce automáticamente entre los miembros Mirror síncronos de una tolerancia contra fallos:

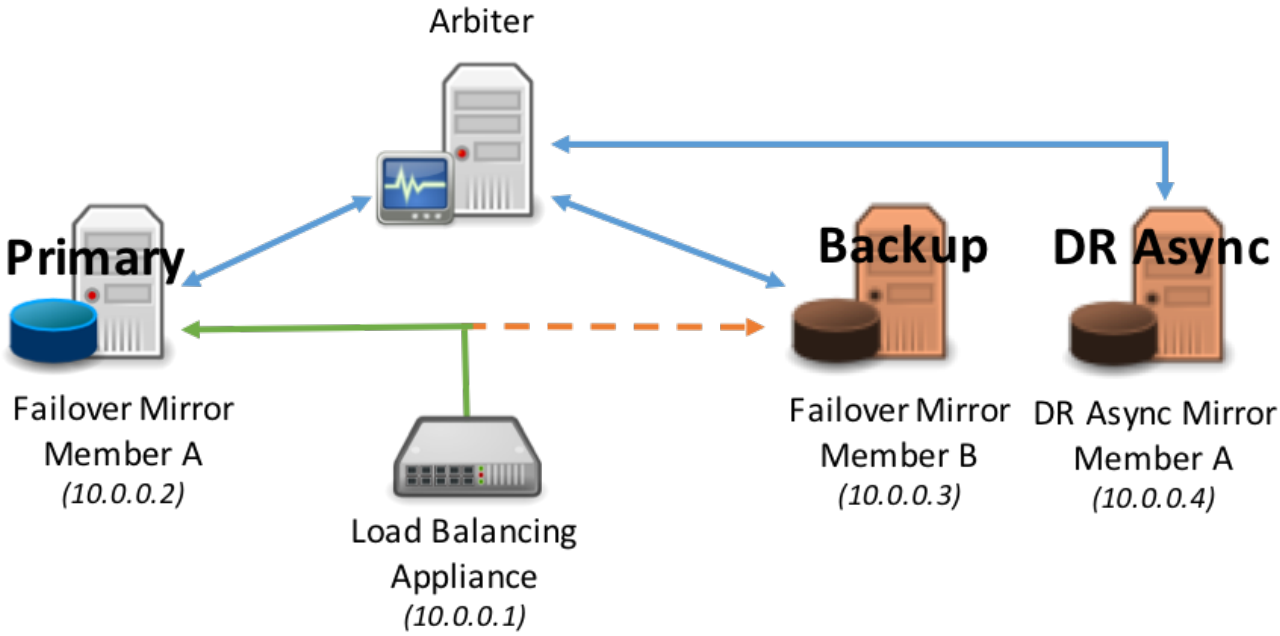


En el siguiente diagrama se muestra la promoción de los miembros Mirror asíncronos en la DR dentro del grupo con cargas equilibradas, esto normalmente asume que el mismo dispositivo de red con carga equilibrada brinda servicio a todos los miembros Mirror (los escenarios que están divididos geográficamente se analizan más adelante en este artículo). Según el procedimiento estándar de la DR, la promoción del miembro de recuperación en caso de desastres implica una decisión humana y luego una simple acción administrativa a nivel de la base de datos. Sin embargo, una vez tomada esta acción, no es necesaria ninguna opción administrativa en el dispositivo de red: descubra automáticamente el nuevo principal.

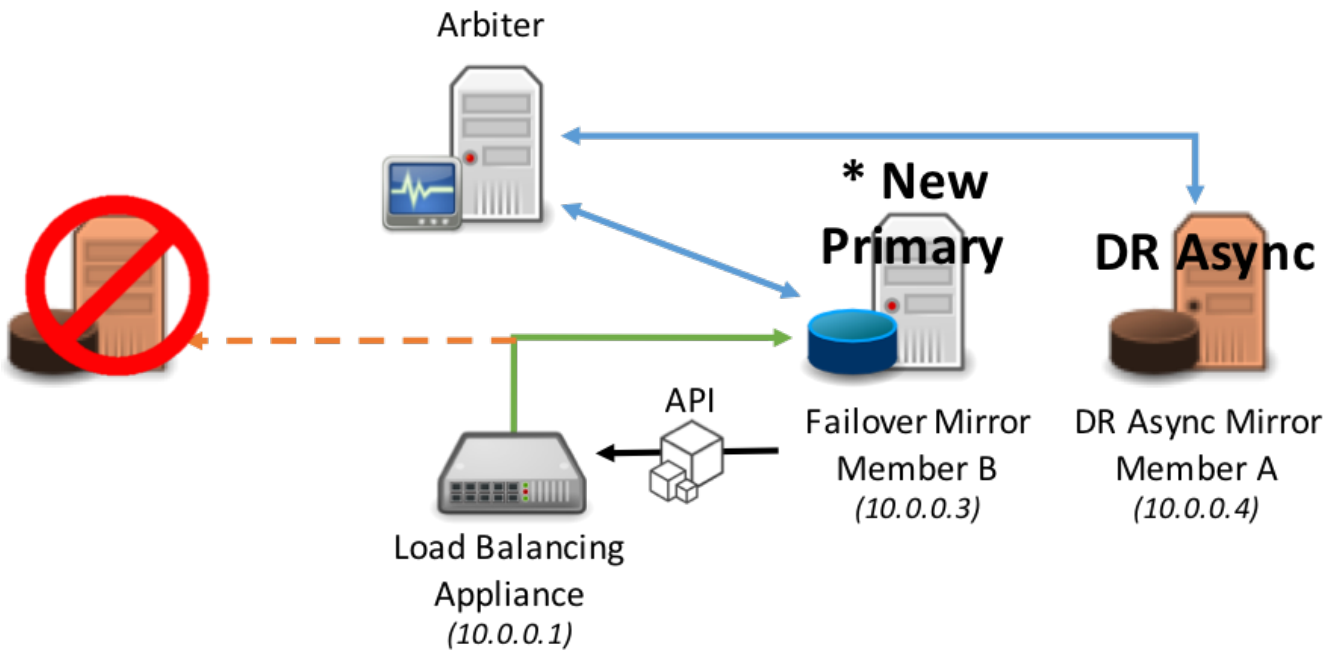


Opción 2: API llamada por el servidor de base de datos

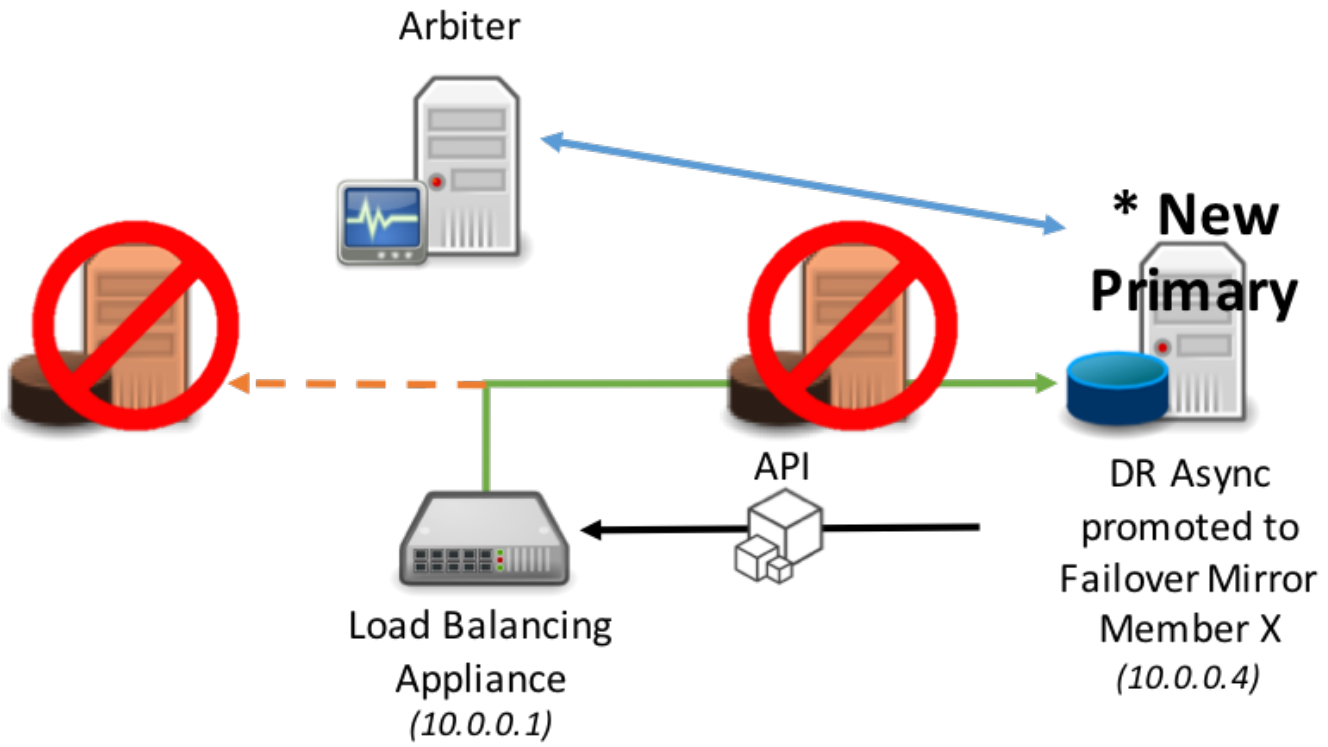
En este método se utiliza el dispositivo para administrar el tráfico de red y tiene un grupo de servidores definido tanto con miembros Mirror de una tolerancia contra fallos como miembros Mirror de una DR asíncrona.



Cuando un miembro Mirror se convierte en el miembro Mirror principal se realiza una llamada de API al dispositivo de red para ajustar la prioridad o ponderación e indicar inmediatamente al dispositivo de red que dirija el tráfico al nuevo miembro Mirror principal.



El mismo modelo se aplica a la promoción de un miembro Mirror de una DR asíncrona en el caso de que los miembros Mirror principal y copia de seguridad dejen de estar disponibles.



Esta API se define en la rutina ^ZMIRROR, específicamente como parte de la llamada al procedimiento: ***$$CheckBecomePrimaryOK^ZMIRROR()***

Dentro de esta llamada de procedimiento, inserte cualquier lógica de API y métodos disponibles para el dispositivo de red correspondiente, como API REST, interfaz de línea de comandos, etc. Al igual que con la IP virtual, este es un cambio abrupto en la configuración de la red y no implica ninguna lógica en las aplicaciones para informar a los clientes que ya existen y están conectados al miembro Mirror principal que el error está sucediendo en la tolerancia contra fallos. Dependiendo de la naturaleza del error, esas conexiones pueden terminar como resultado del error en sí mismo, debido al tiempo de espera o error de la aplicación, debido a que el principal nuevo obliga al

principal antiguo a detenerse, o debido al vencimiento del temporizador de mantenimiento TCP utilizado por el cliente.

Como resultado, es posible que los usuarios tengan que volver a conectarse e iniciar sesión. El comportamiento de su aplicación determinaría este comportamiento.

Opción 3: Implementaciones Geográficamente Dispersas

En configuraciones con varios centros de datos y posiblemente implementaciones geográficamente dispersas, tales como implementaciones en nube con varias zonas de disponibilidad y zonas geográficas, surge la necesidad de tener en cuenta las prácticas de redireccionamiento geográfico en un modelo simple y fácilmente compatible que utiliza tanto el balanceo de cargas basado en DNS como el balanceo de cargas local.

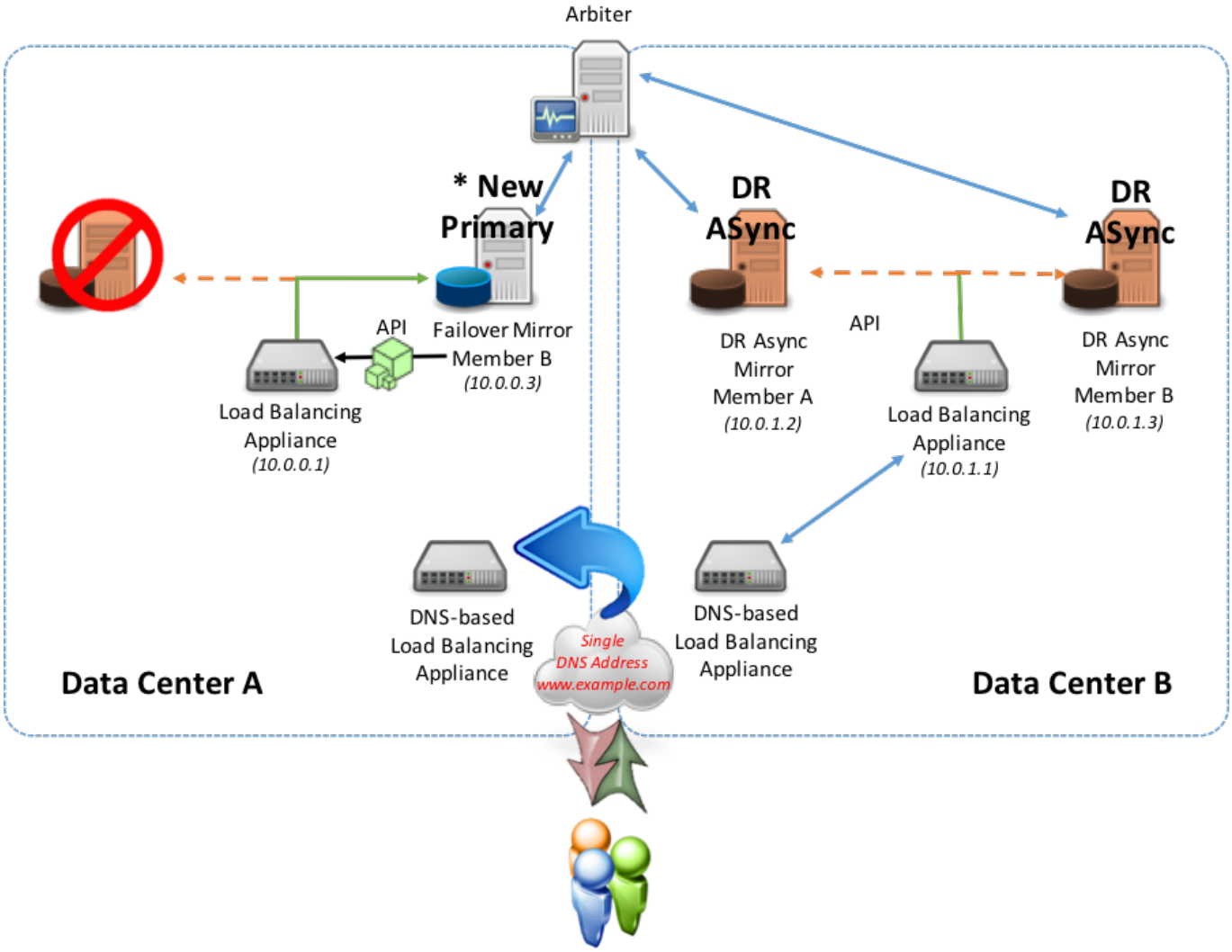
Con este modelo de combinación, se introduce un dispositivo de red adicional que funciona con servicios DNS como Amazon Route 53, F5 Global Traffic Manager, Balanceador de carga global del servidor Citrix NetScaler o Cisco Global Site Selector en combinación con balanceadores de carga de red en cada centro de datos, zona de disponibilidad o georregión de nube.

En este modelo, el sondeo (recomendado) o los métodos de API descritos anteriormente se utilizan de forma local para ubicar la operación de cualquiera de los miembros Mirror (tolerancia contra fallos o DR asíncrono). Se utiliza para informar al dispositivo de red geográfica/global si puede dirigir el tráfico a cualquiera de los centros de datos. También, en esta configuración, el dispositivo de administración para el tráfico de la red local presenta su propio VIP al dispositivo de red geográfica/global.

En un estado normal de equilibrio, el miembro Mirror principal activo informa al dispositivo de red local que es principal y proporciona un estado “ Up ” . Este estado “ Up ” se transmite al dispositivo geográfico/global para ajustar y mantener el registro DNS con el fin de reenviar todas las solicitudes a este miembro Mirror principal activo.

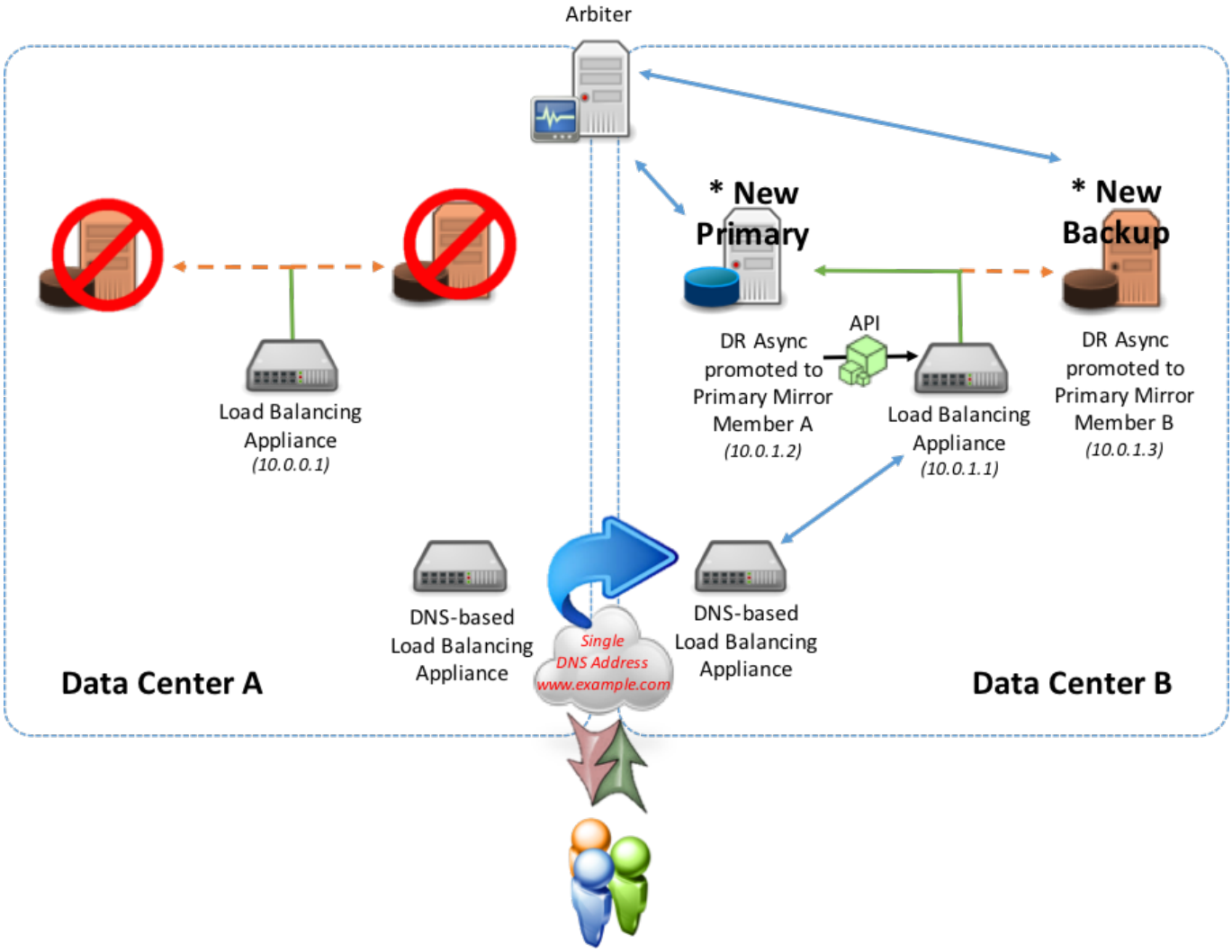
En un escenario de tolerancia contra fallos dentro del mismo centro de datos (el miembro Mirror síncrono de la copia de seguridad se convierte en principal), se utiliza una API o un método de sondeo con el balanceador de cargas local para ahora redirigirlo al nuevo miembro Mirror principal dentro del mismo centro de datos. No se realizan cambios en el dispositivo geográfico/global ya que el balanceador de carga local sigue respondiendo con el estado “ Up ” porque el nuevo miembro espejo principal está activo.

Con el fin de cumplir los objetivos de este ejemplo, el método API se utiliza en el siguiente diagrama para la integración local en el dispositivo de red.



En un escenario de tolerancia contra fallos a un centro de datos diferente (ya sea una miembro Mirror síncrona o un miembro Mirror de una DR asíncrona en un centro de datos alternativo) que utiliza la API o los métodos de sondeo, el miembro Mirror principal recién promovido comienza a informar como principal al dispositivo de red local.

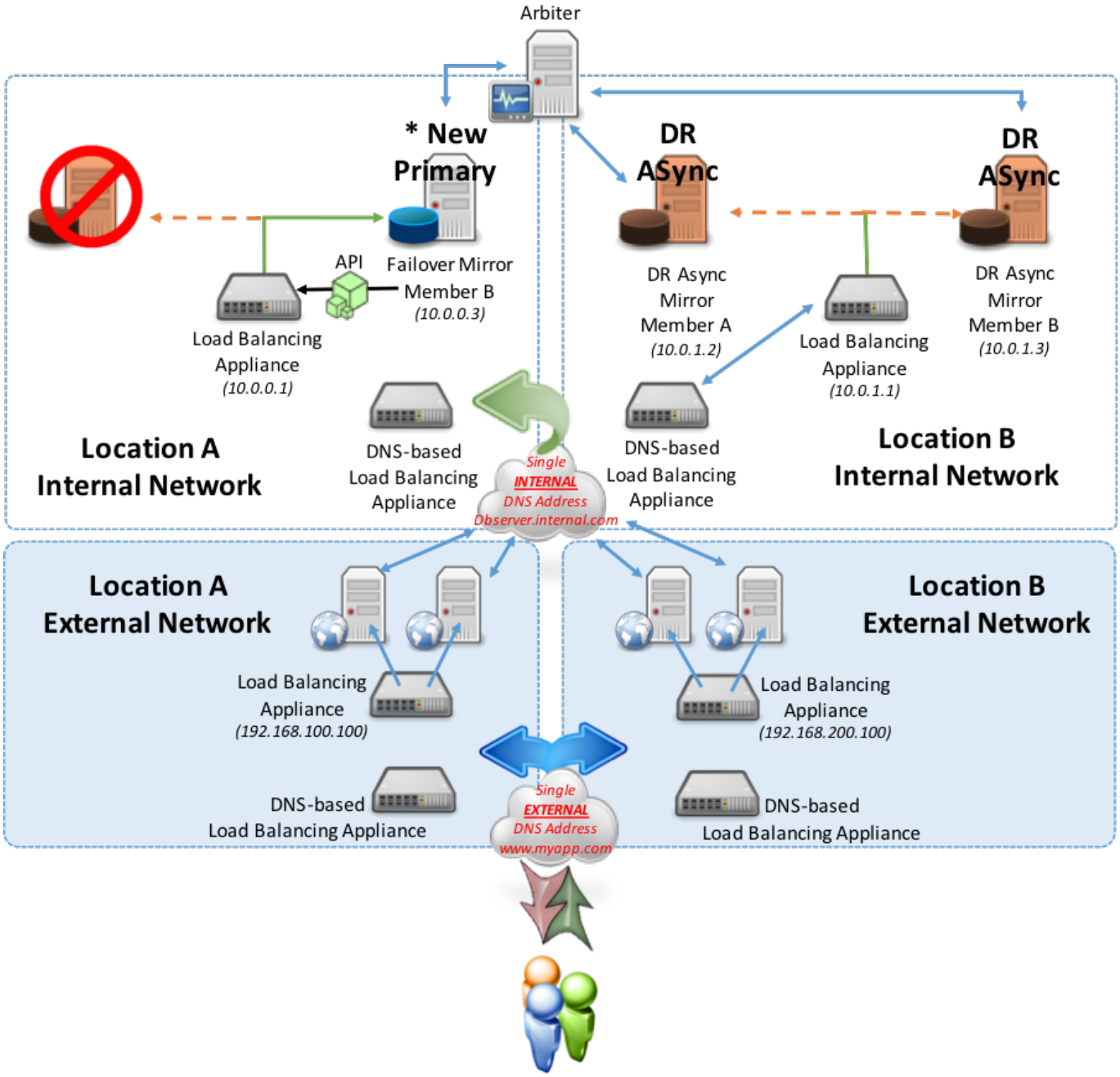
Durante la tolerancia contra fallos, el centro de datos que antes contenía al principal ya no reporta “ Up ” desde el balanceador de carga local al geográfico/global. El dispositivo geográfico/global no dirigirá el tráfico a ese dispositivo local. El dispositivo local del centro de datos alternativo reportará “ Up ” al dispositivo geográfico/global e llamará la actualización del registro DNS ahora directamente a la IP virtual presentada por el balanceador de carga local del centro de datos alternativo.



Opción 4: Implementaciones geográficamente dispersas y en varios niveles

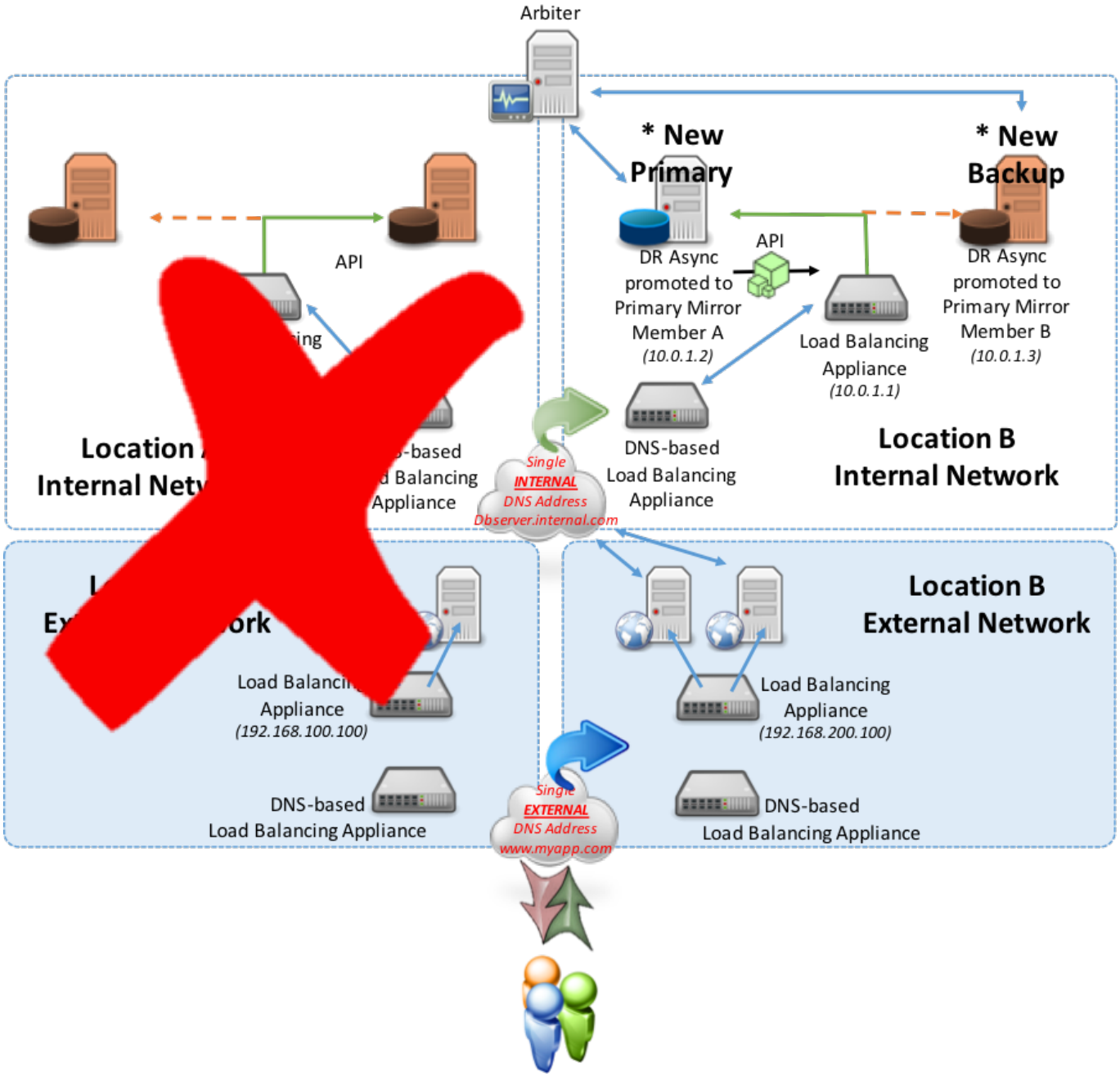
Para llevar la solución un paso más allá, la introducción de un nivel de servidor web separado se realiza como una WAN interna a privada o accesible mediante Internet. Esta opción puede ser un modelo de implementación normal para aplicaciones de grandes empresas.

En el siguiente ejemplo se visualiza una muestra de configuración que utiliza varios dispositivos de red para aislar y dar soporte de forma segura a la web y los niveles de las base de datos. En este modelo se utilizan dos ubicaciones geográficamente dispersas, una de las cuales se considera la ubicación “ principal ” y la otra es puramente de “ recuperación en caso de desastres ” para el nivel de la base de datos. La ubicación de la recuperación en caso de desastres del nivel de la base de datos debe utilizarse en caso de que la ubicación principal esté fuera de servicio por cualquier motivo. Además, el nivel web de este ejemplo se ilustrará como activo-activo, lo cual significa que los usuarios son dirigidos a cualquiera de las dos ubicaciones basándose en varias reglas como la menor latencia, las conexiones menores, los rangos de direcciones IP u otras reglas de enrutamiento que usted considere apropiadas.



Como se muestra en el ejemplo anterior, en el caso de una tolerancia contra fallos dentro de la misma ubicación, se produce una tolerancia contra fallos automática y el dispositivo de red local apunta ahora al nuevo principal. Los usuarios aún se conectan a los servidores web de cualquiera de las dos ubicaciones y los servidores web con su CSP Gateway asociada continúan apuntando a la Ubicación A.

En el siguiente ejemplo, considere una tolerancia contra fallos o una interrupción completa en la Ubicación A en la que tanto el principal o los miembros Mirror de la tolerancia contra fallos en la copia de seguridad estén fuera de servicio. Los miembros Mirror de la DR asíncrona entonces serían promovidos manualmente a principal y miembros Mirror de la tolerancia contra fallos de la copia de seguridad. A partir de esa promoción, el nuevo miembro Mirror principal designado permitirá que el dispositivo de balanceo de carga que se encuentra en la Ubicación B informe “ Up ” mediante el método API discutido anteriormente (el método de sondeo también es una opción). Como resultado del balanceador de carga local que ahora informa “ Up ” , el dispositivo basado en DNS reconocerá y redirigirá el tráfico de la ubicación A a la ubicación B para los servicios en el servidor de base de datos.



Conclusión

Existen muchas permutaciones posibles para diseñar Mirror de una tolerancia contra fallos sin una IP virtual. Estas opciones pueden aplicarse tanto a los escenarios de alta disponibilidad más simples como a las implementaciones en regiones multigeográficas con varios niveles, incluidos los miembros espejo de la DR asíncrona para obtener una solución altamente disponible y tolerante a los desastres que tenga el objetivo de mantener los más altos niveles de resiliencia operativa en sus aplicaciones**.**

Esperamos que este artículo haya proporcionado algo de conocimiento acerca de las diferentes combinaciones y casos de uso posibles para implementar con éxito Mirror de bases de datos con tolerancia contra fallos que sean adecuados para sus necesidades de aplicación y disponibilidad.

#System Administration #High Availability #Failover #Mirroring #Cloud #Caché #Ensemble #InterSystems IRIS

Source URL:https://community.intersystems.com/node/469121