

11 Tecnología de Recuperación ante Desastres y sus Aplicaciones

www.huawei.com



Prefacio

- Este módulo introduce principalmente:
 - La definición del sistema de recuperación ante desastres y su importancia hacia la continuidad del negocio empresarial.
 - Soluciones comunes de recuperación ante desastres.
 - Tecnologías comunes de recuperación ante desastres.
 - Historia de éxito de soluciones de recuperación ante desastres.



Objetivos

- Al finalizar este módulo, usted será capaz de:
 - Describir los conceptos y la importancia de la recuperación ante desastres.
 - Diferenciar las ventajas y desventajas de las soluciones comunes de recuperación ante desastres.
 - Comprender los principios técnicos de las soluciones de recuperación ante desastres.
 - Aprender a implementar una solución de recuperación ante desastres mediante el caso práctico de la aplicación típica de la solución de recuperación ante desastres.



Contenidos

1. **Descripción general de la solución de recuperación ante desastres.**
2. Arquitectura de la Solución de Recuperación ante Desastres.
3. Tecnologías comunes de recuperación ante desastres.
4. Caso práctico de la aplicación de recuperación ante desastres.

Demanda de recuperación ante desastres



- Tres riesgos principales: Pérdida de datos, Corrupción de datos, Interrupción del servicio. Cada hora de interrupción del servicio puede causar pérdidas por valor de millones de dólares para las empresas.
- Cumplimiento normativo: Cumplimiento financiero, Protección de Nivel 3, Aislamiento de Seguridad, 3DC, Alta Continuidad del Negocio
- Operación y mantenimiento de TI: El sistema es tolerante a desastres y está listo para su uso, simplifica el funcionamiento y el mantenimiento de TI y evita el impacto de desastres repentinos.

Desafíos de la recuperación ante desastres

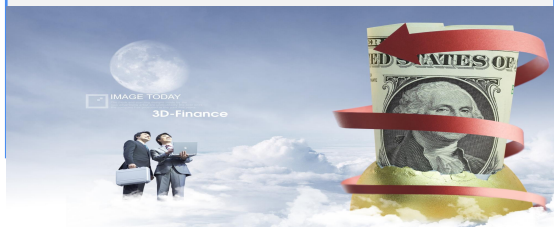
Inversión costosa

ALTO CAPEX

- Alto costo de infraestructura, servidores, almacenamiento y software.
- Alto costo de construcción de salas de servidores e instalaciones.

Alto OPEX

- Soporte profesional de O&M (Implement/Train/Live Support)
- Inversiones a largo plazo para recursos como el agua y la electricidad.



Gestión de complejos

Múltiples dispositivos y administración no unificada

- Los medios de almacenamiento, los servidores y la administración de red son flujos de trabajo independientes, complejos y de baja eficiencia.

Expansión compleja

- El ciclo de expansión en línea es demasiado largo cuando la capacidad es baja y requiere expansión automática.



Capacidad limitada

Capacidades insuficientes de seguridad y DR

- Los datos de copia de seguridad no están fuera del centro de datos y los errores de infraestructura pueden conducir fácilmente a condiciones extremas.

Flexibilidad insuficiente

- La recuperación ante desastres, el uso compartido de datos y otras capacidades están limitadas por la ubicación física de los datos. Las aplicaciones y los datos no se pueden separar y, por lo tanto, no se pueden crear aplicaciones ágiles y mejores características de recuperación ante desastres.



¿Qué es HA?

- **HA (Alta Disponibilidad)** se refiere a la capacidad de proporcionar acceso continuo a las aplicaciones en caso de un error de un solo componente en el sistema local. No importa este fallo es un fallo de los procesos de negocio, las instalaciones físicas o el hardware/software de TI.
- La mejor alta disponibilidad es cuando una máquina en el centro de datos está inactivo, pero los usuarios que utilizan los servicios del centro de datos no son completamente conscientes de ello. Sin embargo, cuando la máquina del centro de datos está inactivo, la conmutación por error del servicio para los servicios que se ejecutan en la máquina generalmente lleva algún tiempo, lo que conduce a la percepción del cliente del tiempo de inactividad.
- El indicador clave de HA es la usabilidad. Su fórmula de cálculo es $[1 - (\text{tiempo de inactividad}) / (\text{tiempo de inactividad} + \text{tiempo de actividad})]$. A menudo usamos unos 9s para la medición de disponibilidad:
 - Cuatro 9s: 99,99% a 0,01% * 365 * 24 * 60 a 52,56 minutos/año de inactividad.
 - Cinco 9s: 99.999% a 0.001% * 365 a 5.265 minutos/año de inactividad.
 - Seis 9s: 99.9999% a 0.0001% * 365 a 31 segundos/año de inactividad.
- Para HA, a menudo se utiliza almacenamiento compartido. En este caso, RPO n.o 0. Al mismo tiempo, el modo HA activo/activo (clúster activo-activo) se utiliza a menudo para hacer RTO casi 0. Si se utiliza el modo activo/pasivo HA, entonces el RTO es necesario ser reducido al mínimo.

¿Qué es la recuperación ante desastres (DR)?

- El desastre es causado por razones artificiales o naturales, causando un grave fallo o corrupción de un sistema de información dentro de un centro de datos, que suspende las funciones de servicio soportadas por el sistema de información, o causa niveles de servicio inaceptables durante un período de tiempo específico que ocurrió en un evento repentino. Esto a menudo conduce a un sistema de información que necesita ser cambiado a un sitio alternativo para su funcionamiento.
- La recuperación ante desastres se refiere a la capacidad de recuperar datos, aplicaciones o servicios en centros de datos en diferentes ubicaciones cuando un desastre destruye un centro de producción.
- La recuperación ante desastres significa que, además del sitio de producción, los sitios redundantes establecidos por los usuarios, cuando se produce un desastre y el sitio de producción está dañado, los sitios redundantes pueden hacerse cargo de los servicios normales de los usuarios y lograr servicios ininterrumpidos. Con el fin de lograr una mayor disponibilidad, muchos usuarios incluso configuran varios sitios redundantes.

La relación entre HA y DR (1)

- Los dos están relacionados entre sí, se complementan entre sí y se entrelazan entre sí, pero al mismo tiempo tienen diferencias significativas entre ellos:

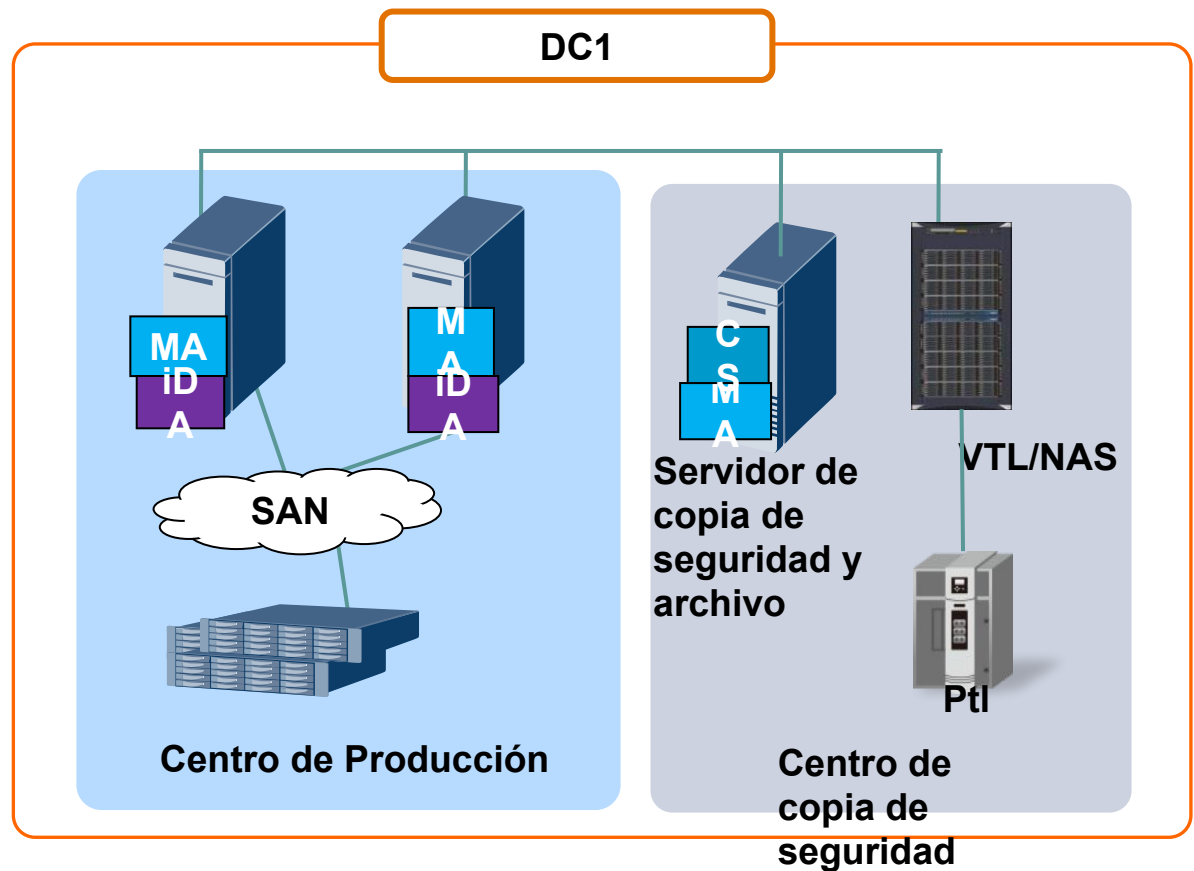
Dimensión	HA (alta disponibilidad)	DR (Recuperación ante Desastres)
Escenarios	HA se refiere al sistema local de alta disponibilidad, lo que significa que en el caso de varios servidores que ejecutan una o más aplicaciones, debe asegurarse de que cuando se produce un error en cualquiera de los servidores, la aplicación que se ejecuta no se interrumpirá, y la aplicación y el sistema deben ser capaces de cambiar rápidamente para operar en otro servidor. Que reside dentro de el clúster del sistema local y	DR se refiere a sistemas de alta disponibilidad en diferentes lugares (en la misma ciudad o en diferentes lugares), lo que indica la capacidad de recuperar datos, aplicaciones y servicios en caso de desastre.

La relación entre HA y DR (2)

Dimensión	HA (alta disponibilidad)	DR (Recuperación ante desastres)
Almacenamiento	HA a menudo utiliza el almacenamiento compartido, lo que significa que no hay pérdida de datos (RPO=0), más consideraciones están en el RTO debido al período de tiempo tomado para la conmutación de servicio/conmutación por error.	La recuperación de datos de recuperación ante desastres fuera del sitio utiliza la replicación de datos. Según las diferentes tecnologías de replicación de datos utilizadas (sincrónica y asincrónica), la pérdida de datos a menudo da lugar a $RPO > 0$; mientras que la conmutación de aplicaciones fuera del sitio a menudo toma más tiempo, por lo que $RTO > 0$.
Fallas	Principalmente controla los errores de un solo componente que provocan que la carga cambie entre los servidores del clúster.	Copes con errores a gran escala que hacen que la carga cambie entre centros de datos.
Red	Las tareas de escalado LAN están dentro de la categoría de HA.	Las tareas de escalado WAN están dentro de la categoría de recuperación ante desastres.
Nube	HA es un mecanismo para garantizar la continuidad del negocio dentro de un entorno de nube.	DR es un mecanismo para garantizar la continuidad del negocio entre varios entornos de nube.

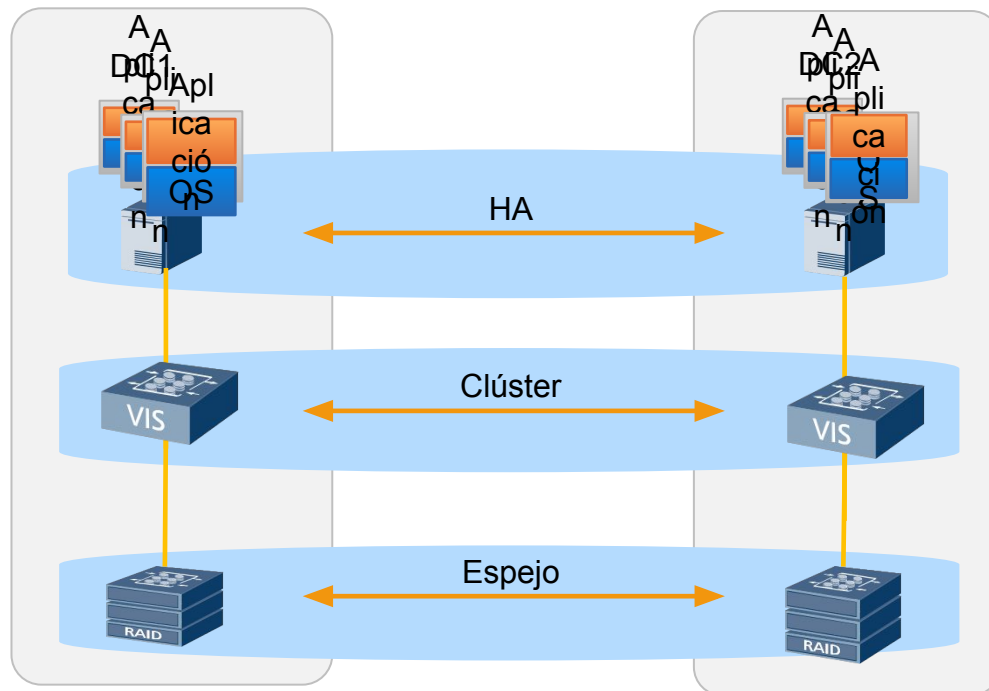
Diferencias entre DR & Copias de seguridad (1)

- **copia de seguridad:** La copia de seguridad es la base fundamental de la recuperación ante desastres, se refiere principalmente al proceso en el que todos o parte de los datos recopilados del disco duro del host de la aplicación o de los arreglos de discos de almacenamiento se replican en otros medios de almacenamiento.



Diferencias entre DR & Copias de seguridad (2)

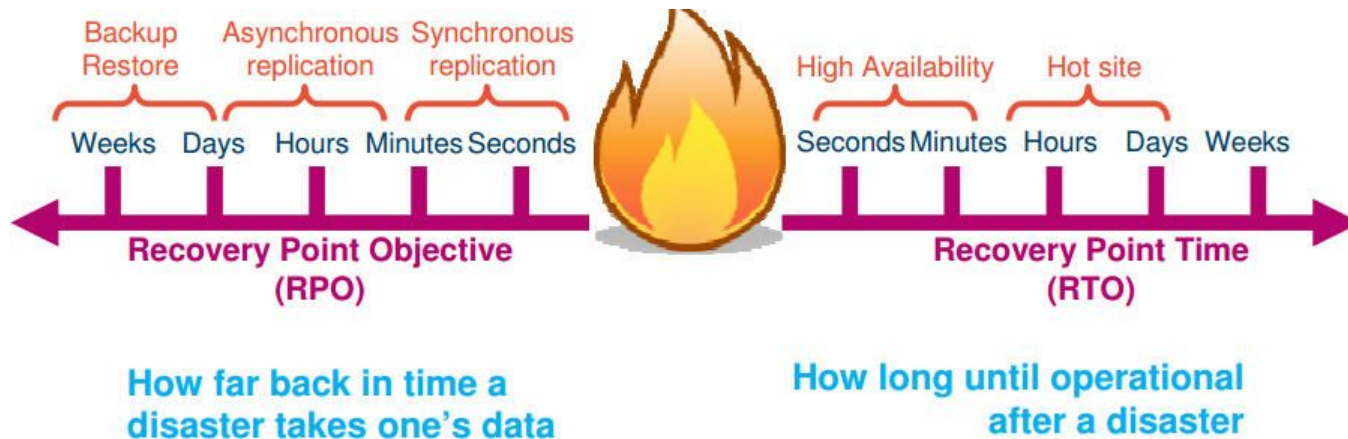
- **Recuperación ante desastres:** El sistema de recuperación ante desastres se refiere al establecimiento de dos o más conjuntos de sistemas de TI con la misma función en ubicaciones remotas separadas entre sí. La supervisión del estado de mantenimiento y la conmutación de funciones se pueden realizar entre ellos. Cuando un sistema deja de funcionar debido al caso de desastre (como incendio, terremoto), todo el sistema de aplicación se puede cambiar a otro lugar para que la función del sistema pueda seguir funcionando normalmente.



- Por lo general, la recuperación ante desastres se refiere a la copia de seguridad de datos o sistemas de aplicaciones que no están en la misma sala de servidores o ubicación. Copia de seguridad hace referencia a datos locales o copias de seguridad del sistema.
- En general, la recuperación ante desastres combina la recuperación ante desastres con la copia de seguridad local, es decir, la copia de seguridad local combinada con la replicación remota de datos para lograr una protección de datos perfecta.

Indicadores clave para medir el rendimiento del sistema de DR

- RPO (Objetivo de punto de recuperación) representa la cantidad de datos que se pueden perder cuando se produce un desastre.
- RTO (Objeto de tiempo de recuperación) representa el tiempo de recuperación del sistema.
- Cuanto menor sea el RPO y el RTO, mayor será la disponibilidad del sistema y mayor será la inversión requerida por el usuario.



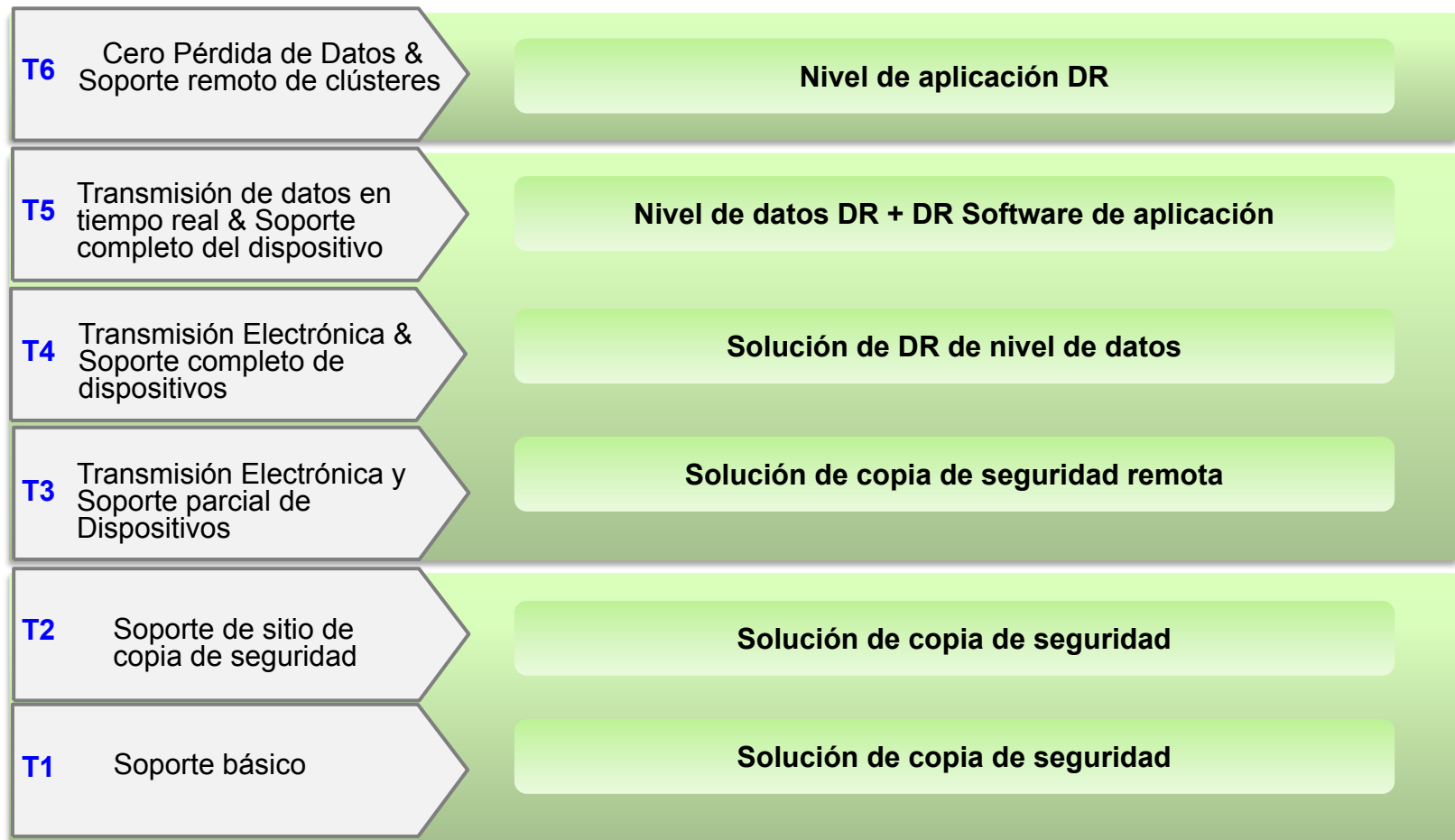
Niveles de Sistemas DR (1)

Nivel	Definición	RTO	TCO
Nivel de datos	<p>Mediante el establecimiento de centros de recuperación ante desastres remotos, se realizará una copia de seguridad remota de los datos para garantizar que los datos originales no se pierdan ni se destruyan después del desastre.</p> <p>En el modo de recuperación ante desastres a nivel de datos, el centro de recuperación ante desastres establecido se puede considerar simplemente como un centro de copia de seguridad de datos remoto. En el nivel de recuperación ante desastres a nivel de datos, las aplicaciones se interrumpen cuando se produce un desastre.</p> <p>La recuperación ante desastres a nivel de datos tiene un tiempo de recuperación largo, pero su costo es menor que otros niveles de recuperación ante desastres y su implementación es relativamente sencilla.</p> <p>Las fuentes de datos son la fuente de vida de todos los sistemas empresariales críticos, por lo que la recuperación ante desastres a nivel de datos es esencial.</p>	<p>El RTO más largo (varios días) porque después del desastre, el Equipo debe volver a implementarse para recuperar los servicios empresariales mediante datos de copia de seguridad.</p>	<p>Menor</p>

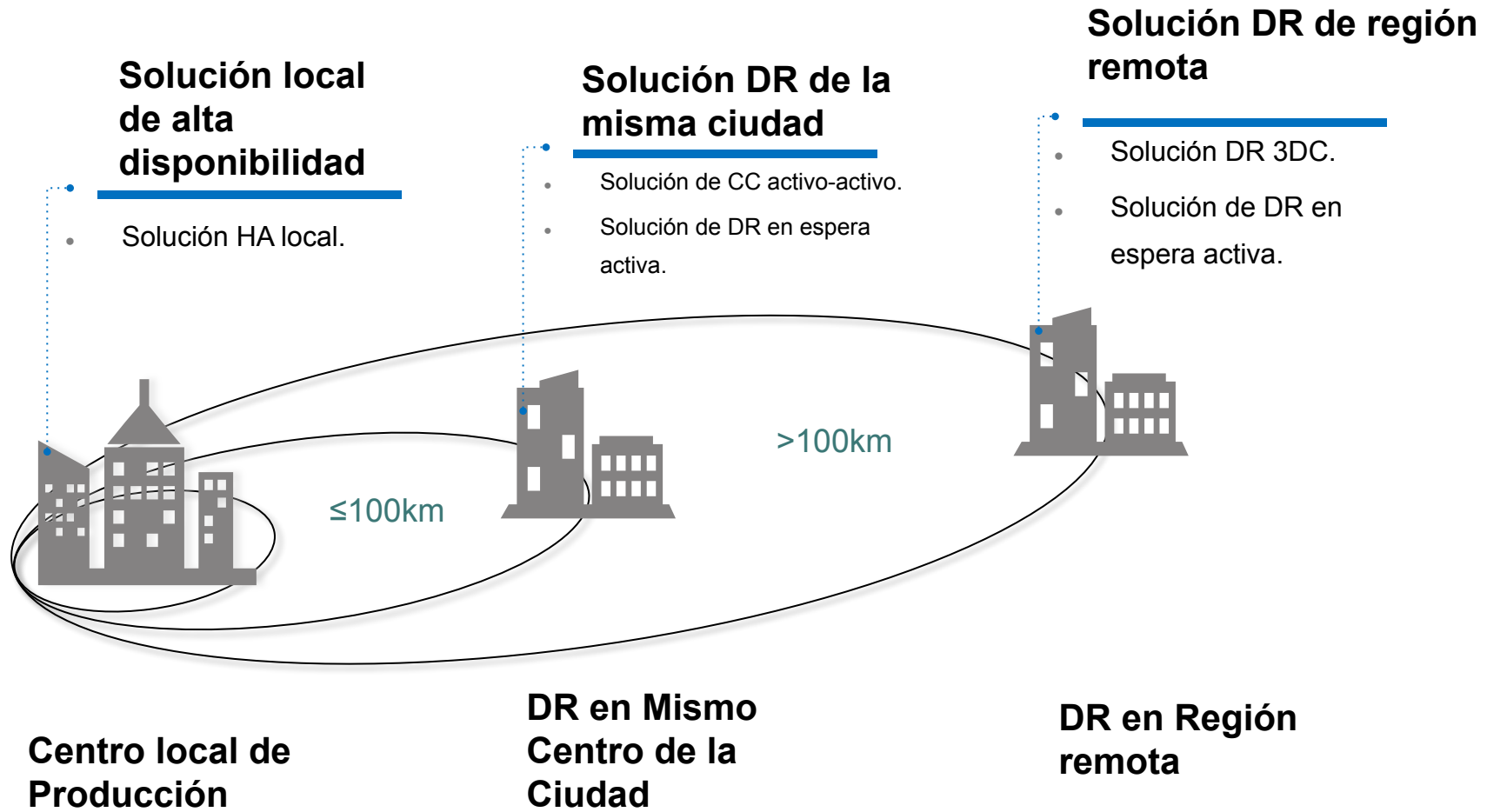
Niveles de sistemas DR (2)

Nivel	Definición	RTO	TCO
Nivel de aplicación	Sobre la base de la recuperación ante desastres a nivel de datos, también se crean conjuntos similares de sistemas de aplicaciones en el sitio de respaldo. A través de la tecnología de replicación síncrona o asíncrona, se puede garantizar que las aplicaciones clave se recuperen dentro del rango de tiempo permitido, minimizando la pérdida causada por los desastres, y permite a los usuarios no estar al tanto del desastre. Por lo tanto, los servicios proporcionados por el sistema son completos, confiables y seguros.	RTO medio (pocas horas)	Medio. El mismo sistema o subsistemas o similares se construye fuera del sitio.
Nivel de servicio	Además de las tecnologías relacionadas con TI necesarias, la recuperación ante desastres de servicio completo requiere una infraestructura completa. La mayoría de sus componentes son sistemas que no son de TI (como teléfonos, oficinas, etc.). Cuando se produce una catástrofe, el espacio de oficina original será destruido. Además de la restauración de datos y aplicaciones, es necesario proporcionar un lugar de trabajo de respaldo para que las empresas se puedan llevar a cabo como de costumbre. .	RTO más pequeño (pocos minutos o Segundos)	Mayor

Análisis de referencia de los niveles de construcción de DR



Panorama de la solución DR

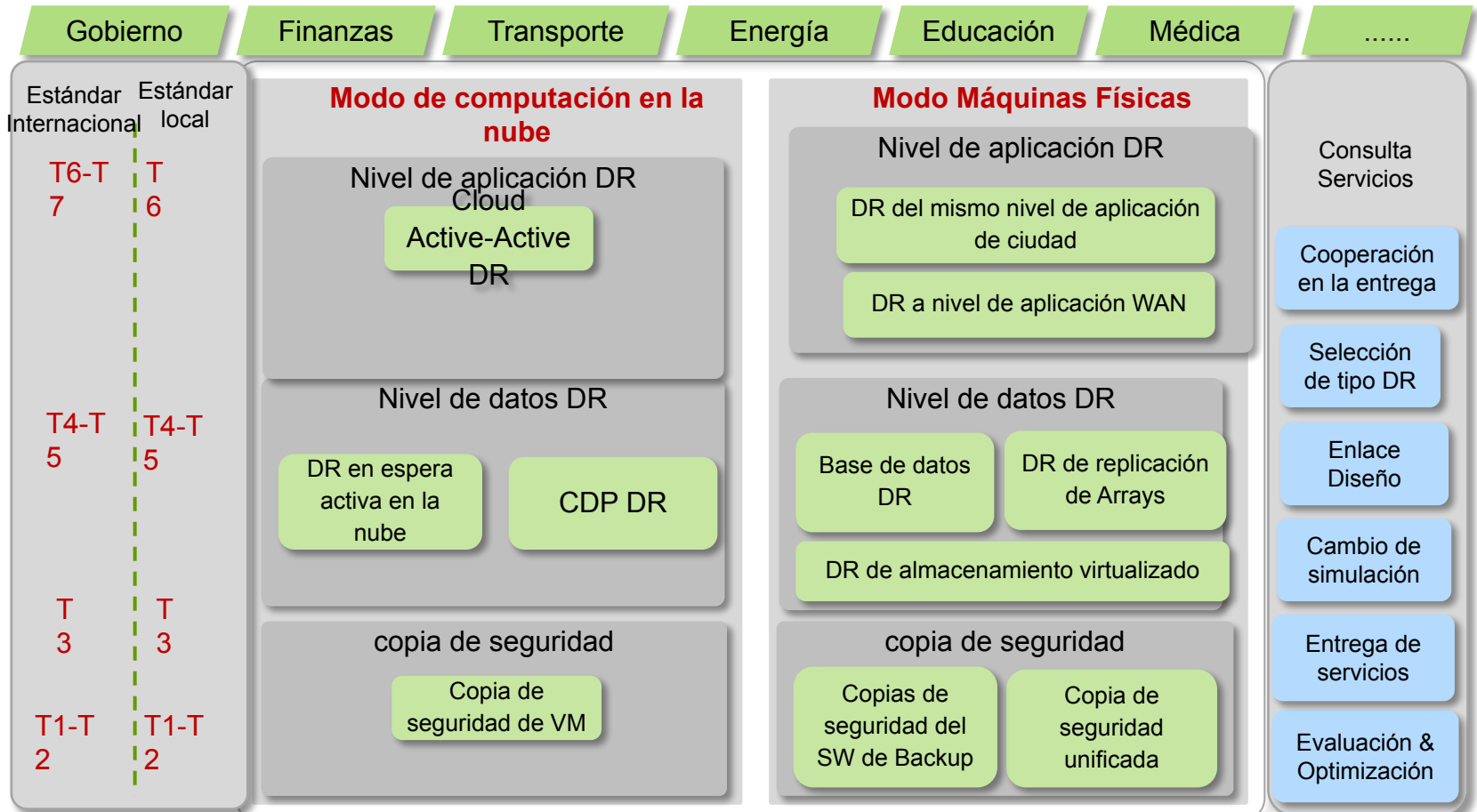




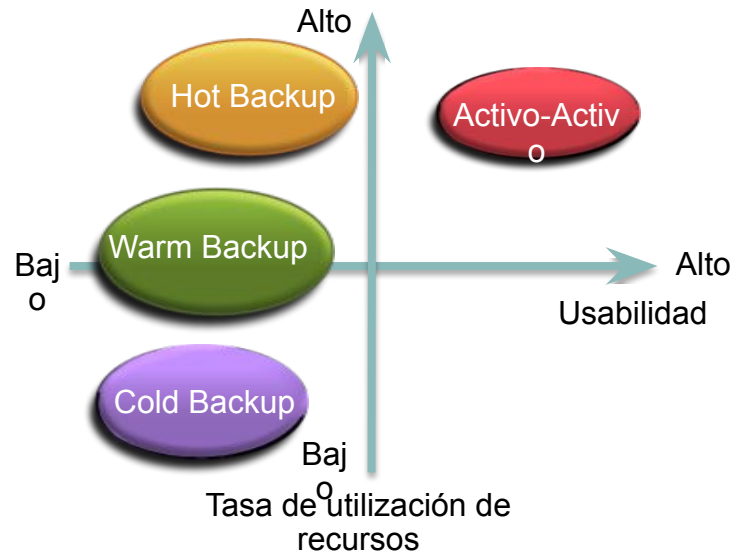
Contenidos

1. Descripción general de la solución de recuperación ante desastres.
2. **Arquitectura de la Solución de Recuperación ante Desastres.**
3. Tecnologías comunes de recuperación ante desastres.
4. Caso práctico de la aplicación de recuperación ante desastres.

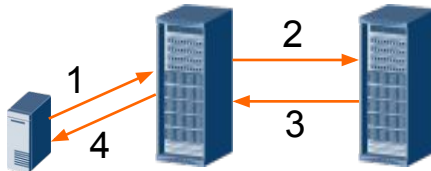
Marco de soluciones de copia de seguridad de recuperación ante desastres



Modelo de diseño DR: Combinación de síncrono & asíncrono (1)

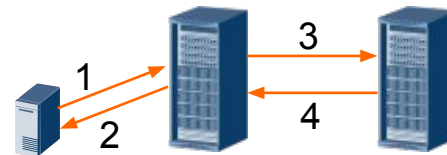


DR síncrono: tiene limitación de distancia



RPO: 0s, 2 espejos idénticos.

DR asíncrono: Sin limitación de distancia

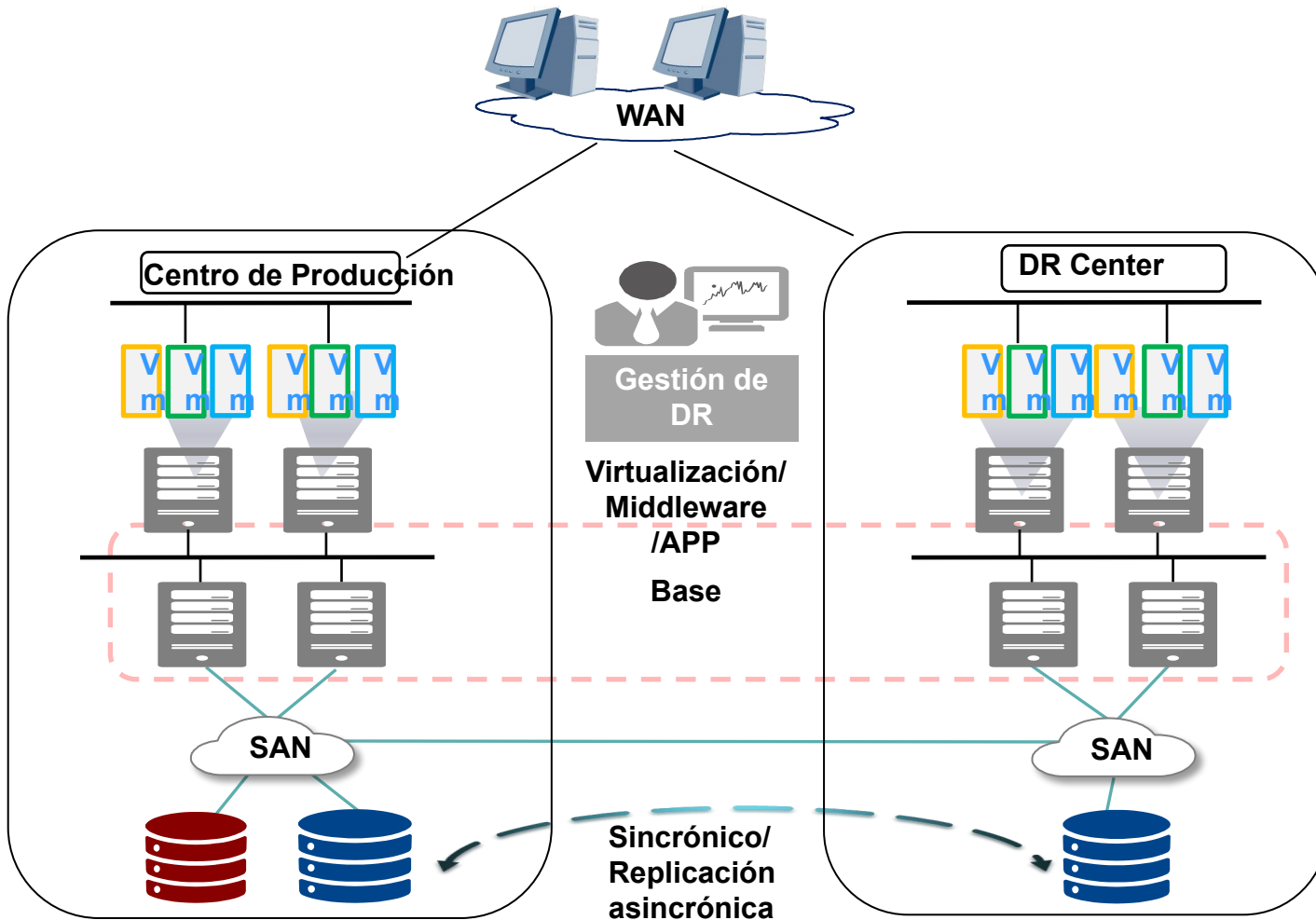


RPO: De 30 minutos a pocas horas, actualiza periódicamente el destino.

Modelo de diseño DR: Combinación de síncrono & asíncrono (2)

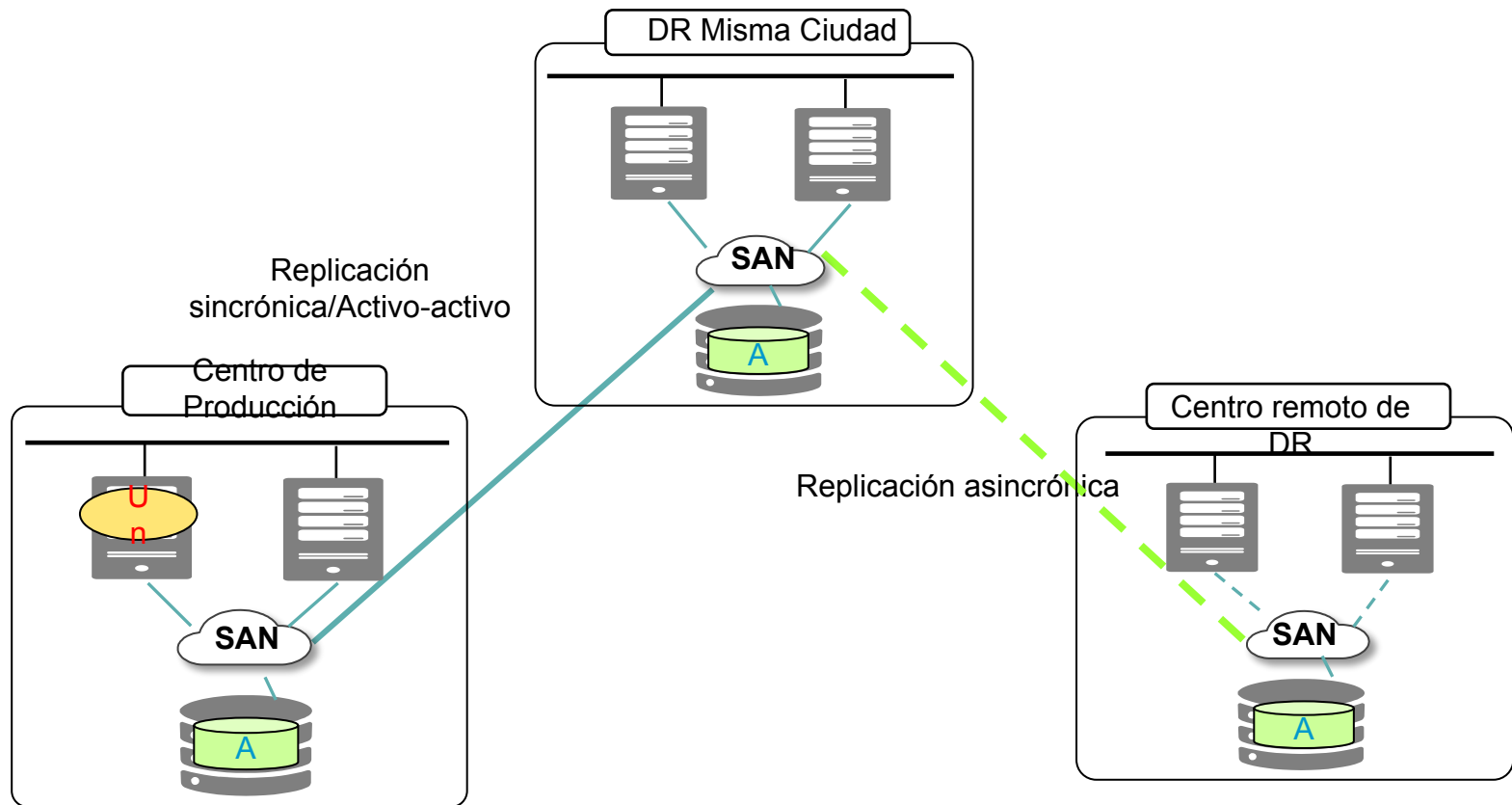
Modo DR	Solución de confiabilidad	Recuperación de DR	Requisitos de copia de seguridad de datos
Activo-Activo	Cluster + Equilibrio de carga	Automático	Replicación síncrona en tiempo real (<100KM)
Copia de seguridad en caliente (Hot)	Clúster	Automático	Replicación síncrona en tiempo real (<100KM)
Copia de seguridad cálida (Warm)	Intervención manual	Manual	Replicación asíncrona (>100KM)
Respaldo en frío (Cold)	Fuerte intervención manual	Manual	Igual que arriba

Activo - Solución de DR en espera

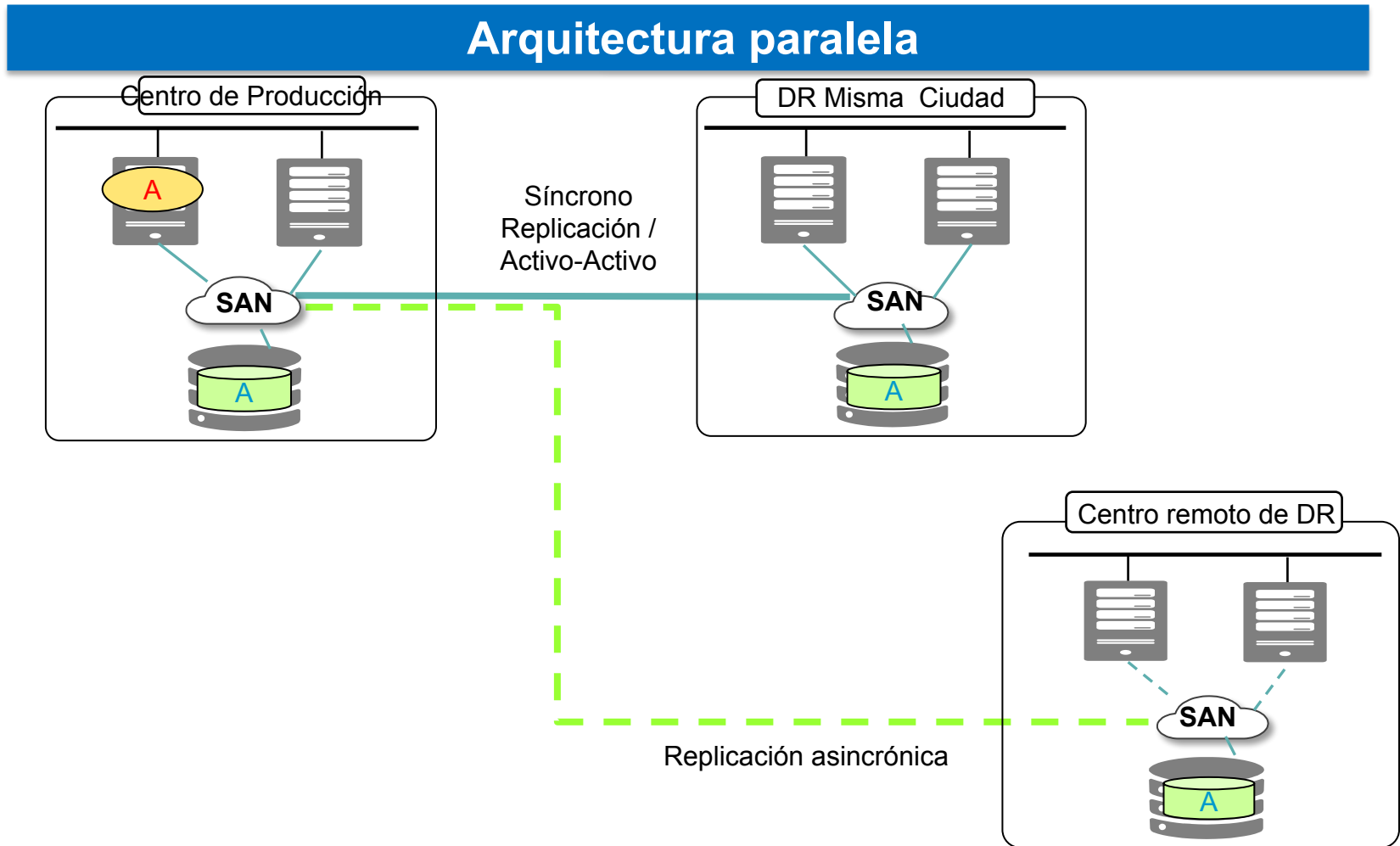


Solución de recuperación ante desastres de tres centros de datos (3DC) (1)

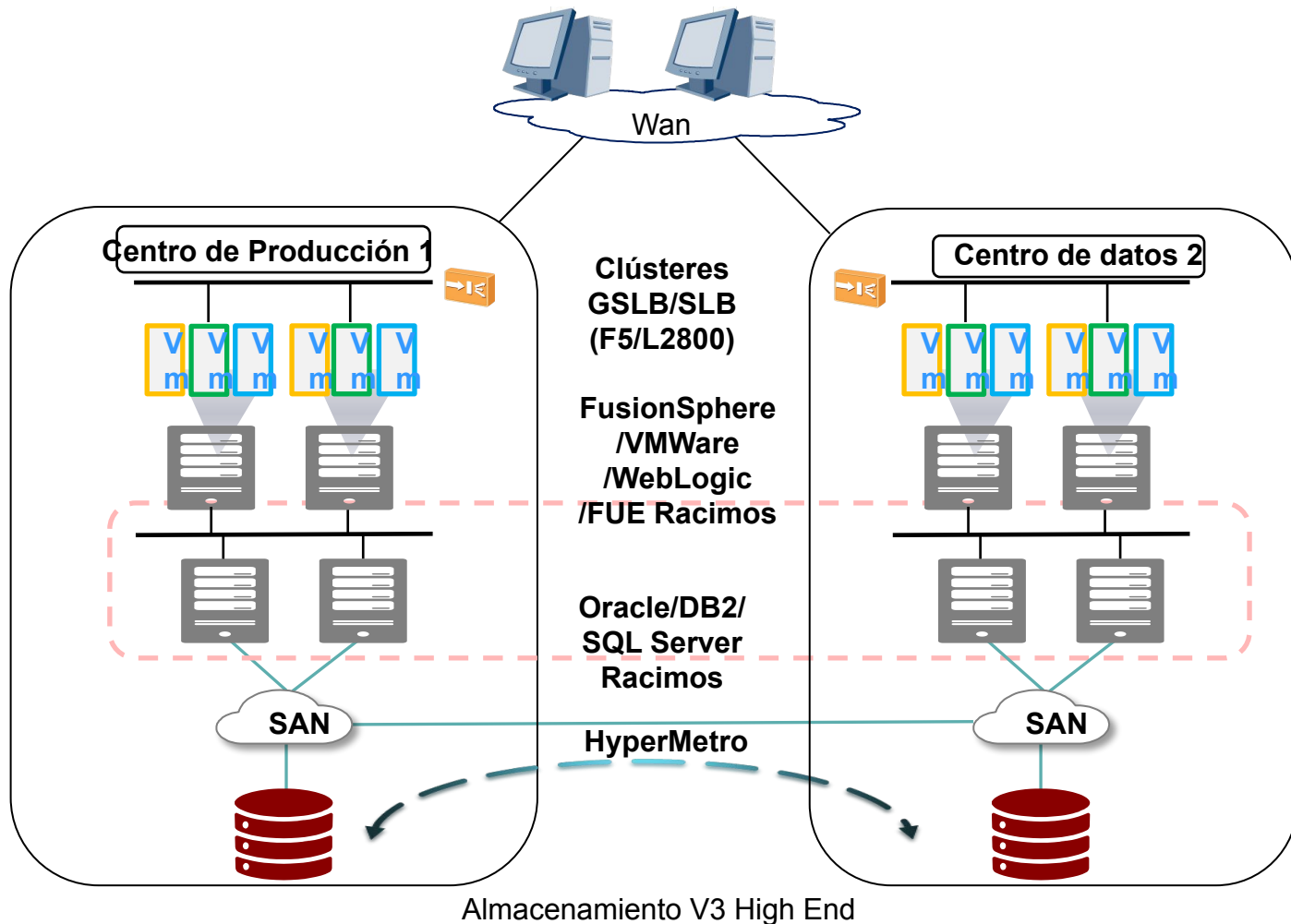
Arquitectura en cascada



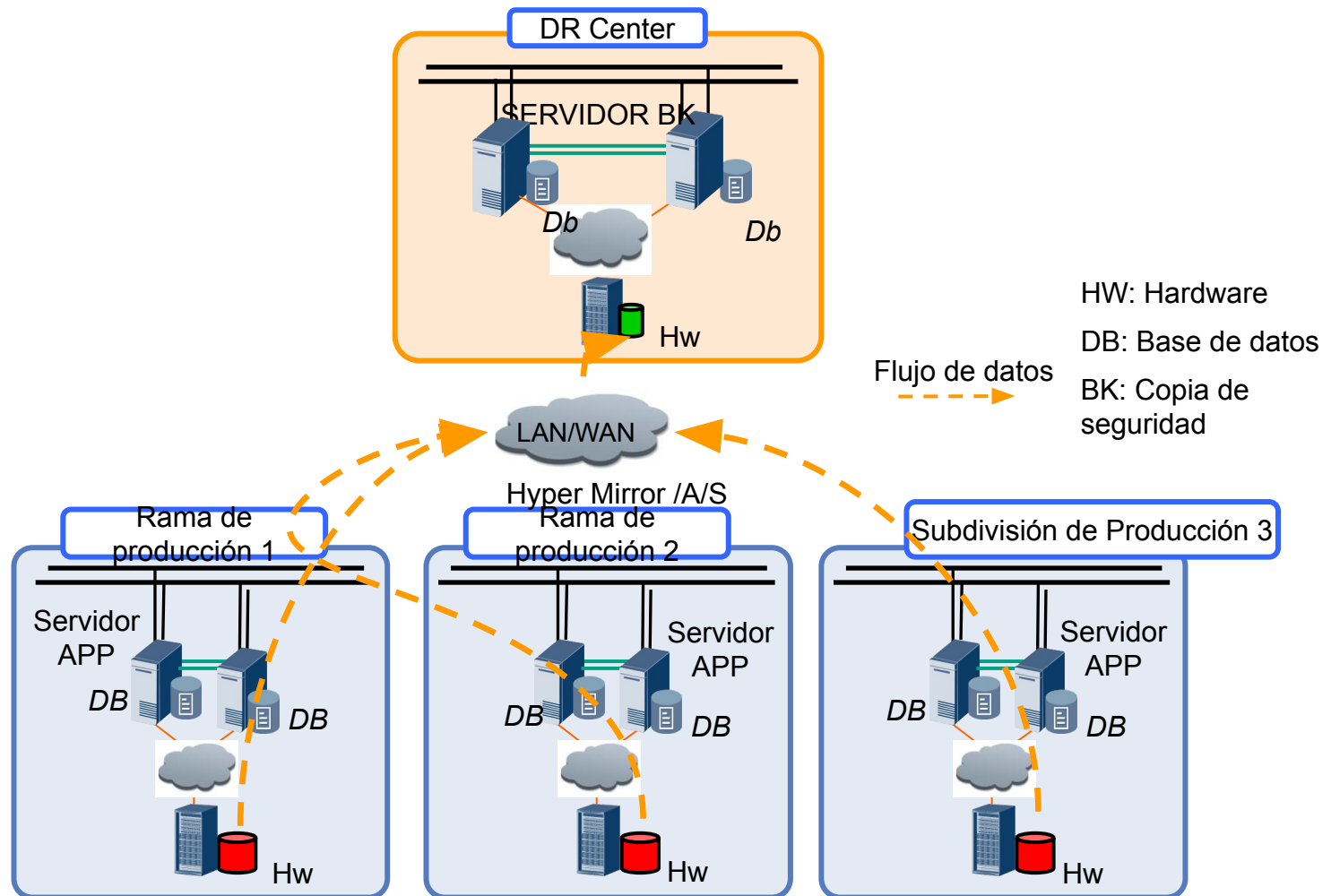
Solución de recuperación ante desastres de tres centros de datos (3DC) (2)



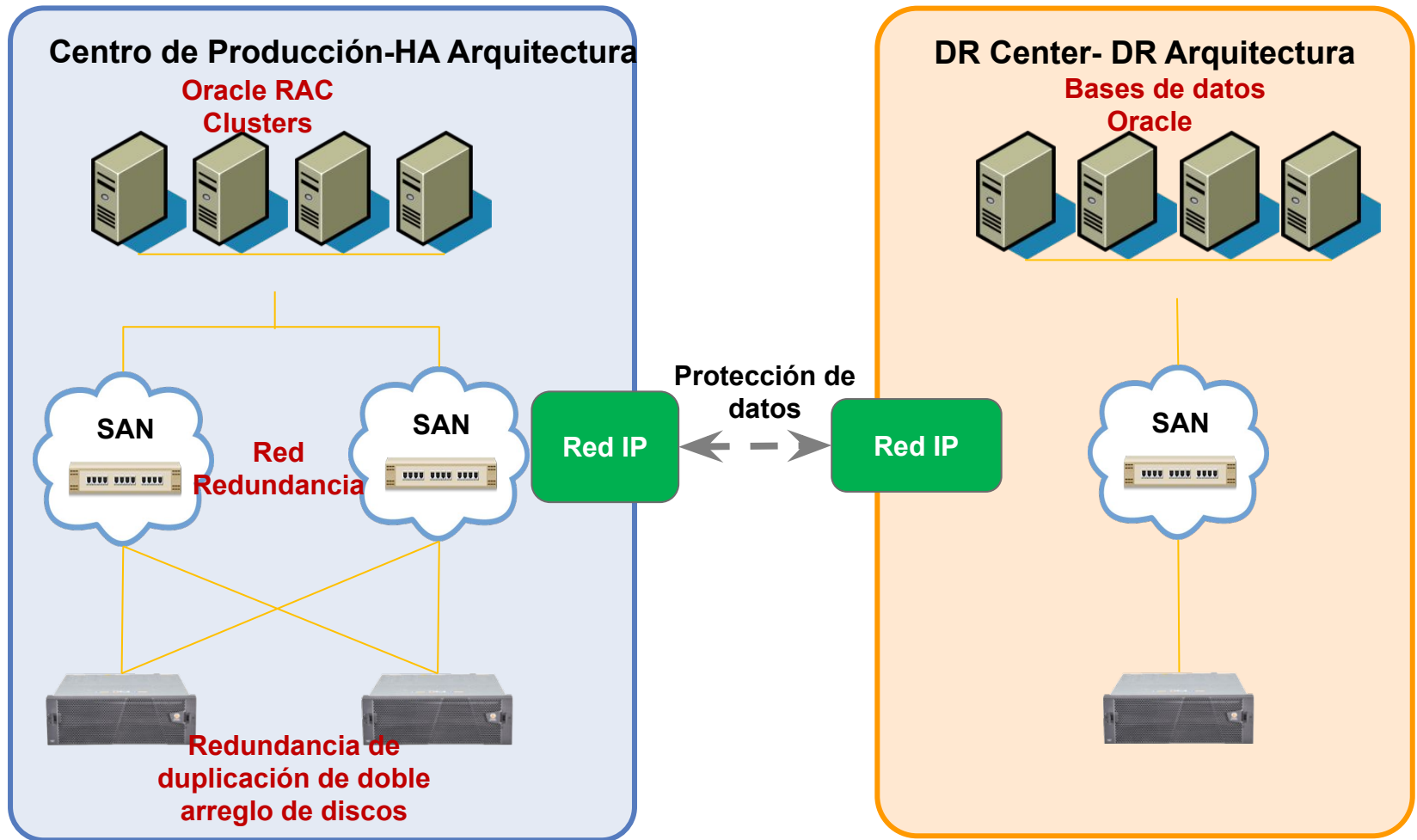
Activo - Solución activa para DR



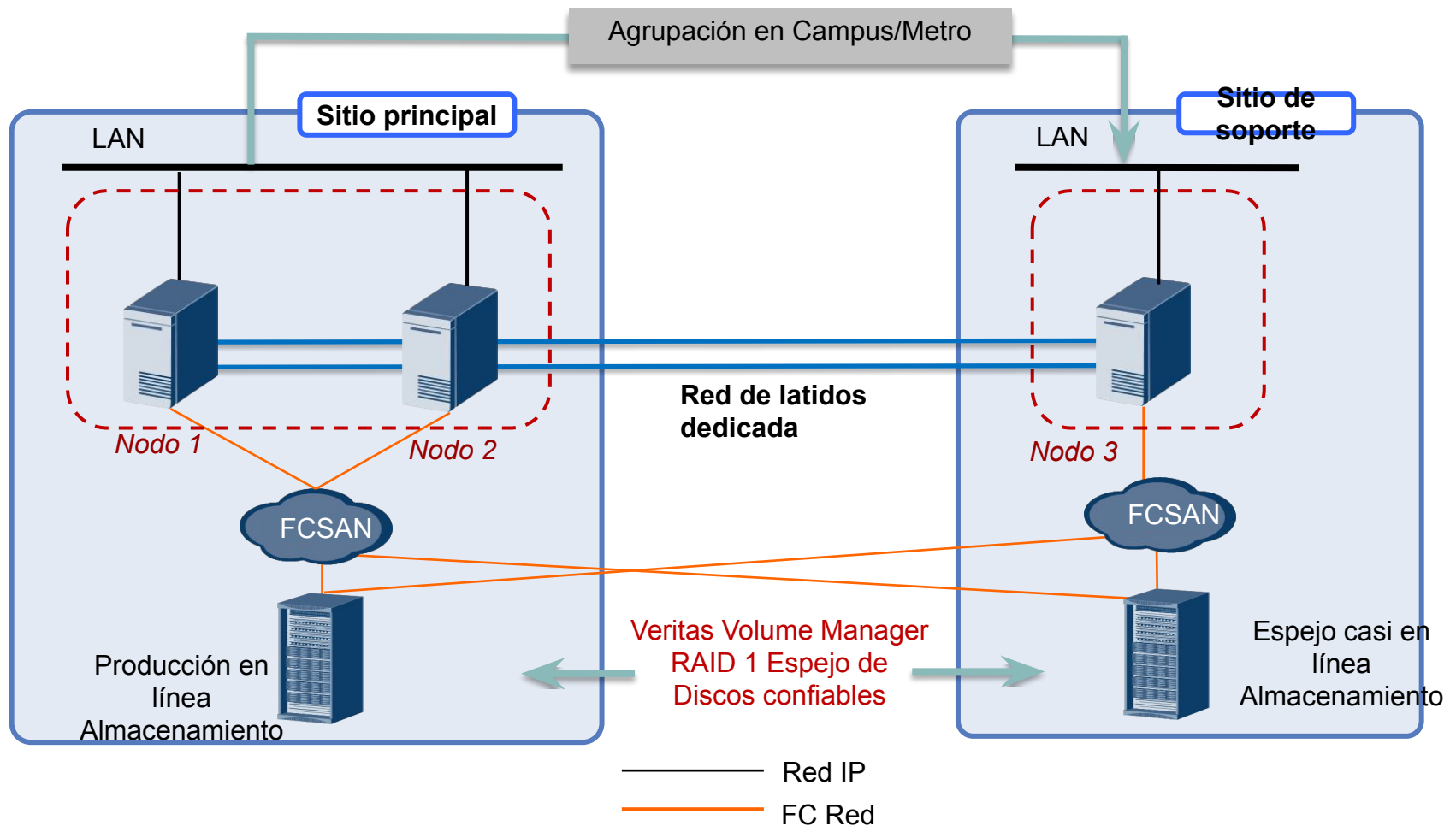
Solución de DR de Replicación de Arreglos



Oracle Database DR

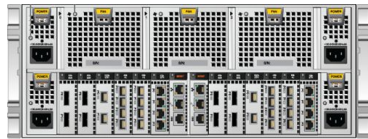


Nivel de aplicación de DR en campus/misma ciudad (modo máquinas físicas)

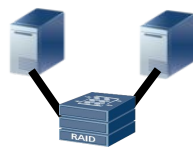


Evolución del nuevo modelo de DR bajo computación en la nube

Modo tradicional de HA local dentro del DC

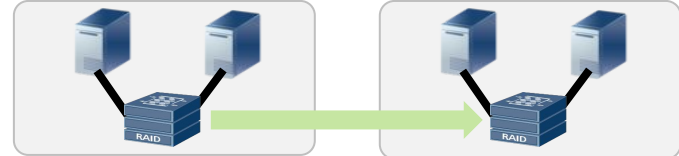


Redundancia de componentes,
Dispositivos altamente
confiables.



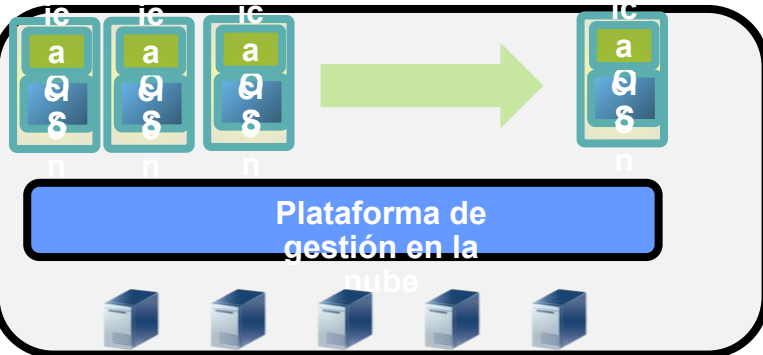
Hot Standby

Modo tradicional de DR de CC cruzada



Principalmente centrados en los servicios de replicación de datos, el proceso es complejo y el ciclo de recuperación es largo.

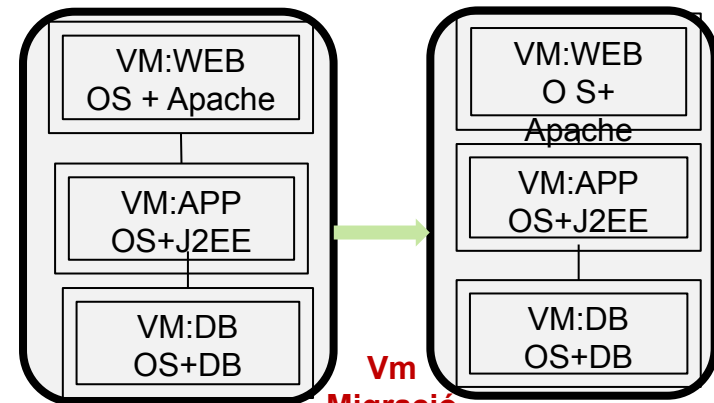
Modo en la nube de HA local dentro del DC



Almacena
miento

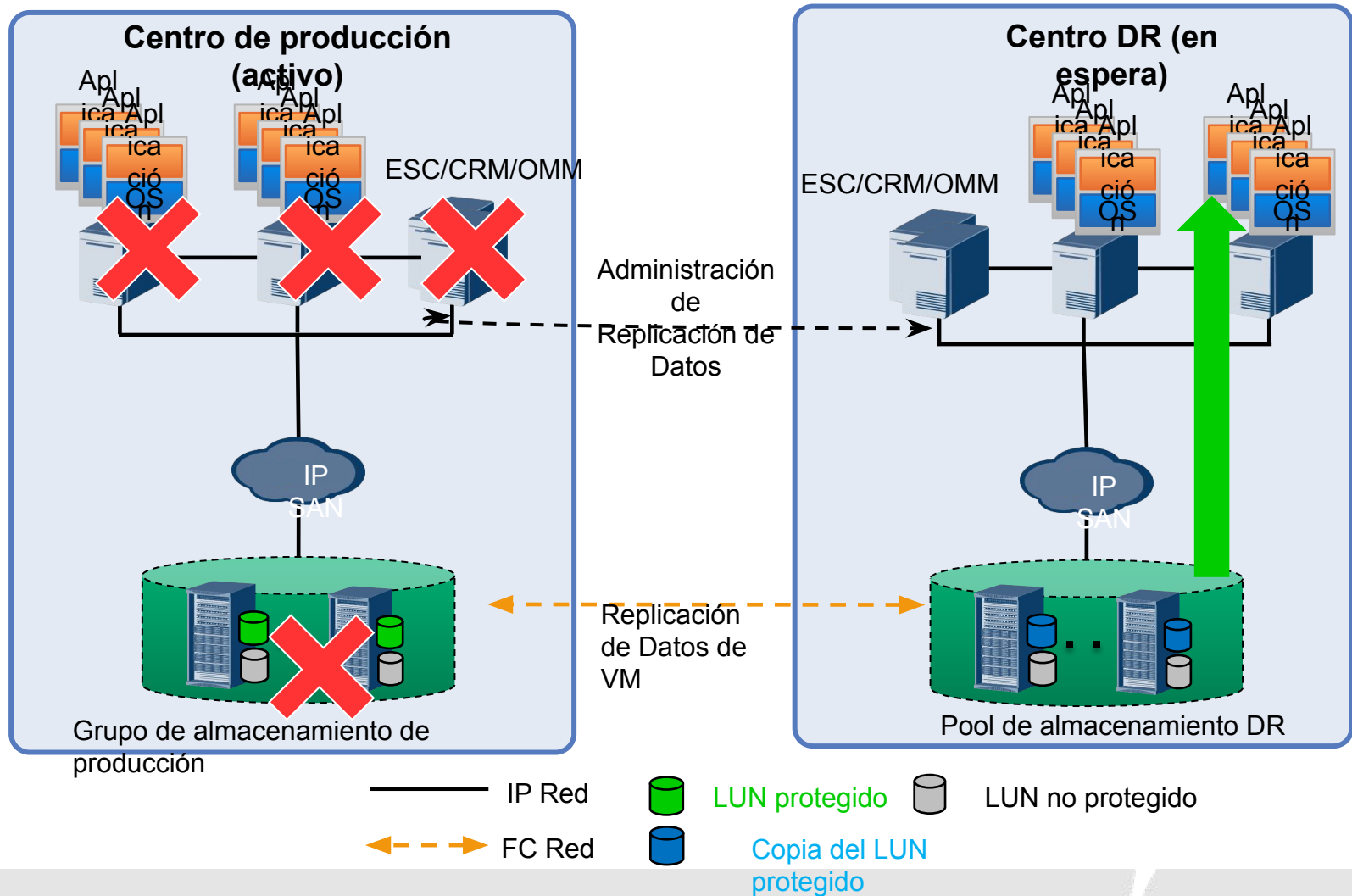
Migración automática de VM (con
servicios)

Modo en la nube de DR Cross DC



Replicación completa de datos de los datos
empresariales y operativos
entorno, gestión unificada, proceso de recuperación
simple,
y un ciclo de recuperación corto.

Cloud Active - Método de implementación de DR de nivel de datos en espera

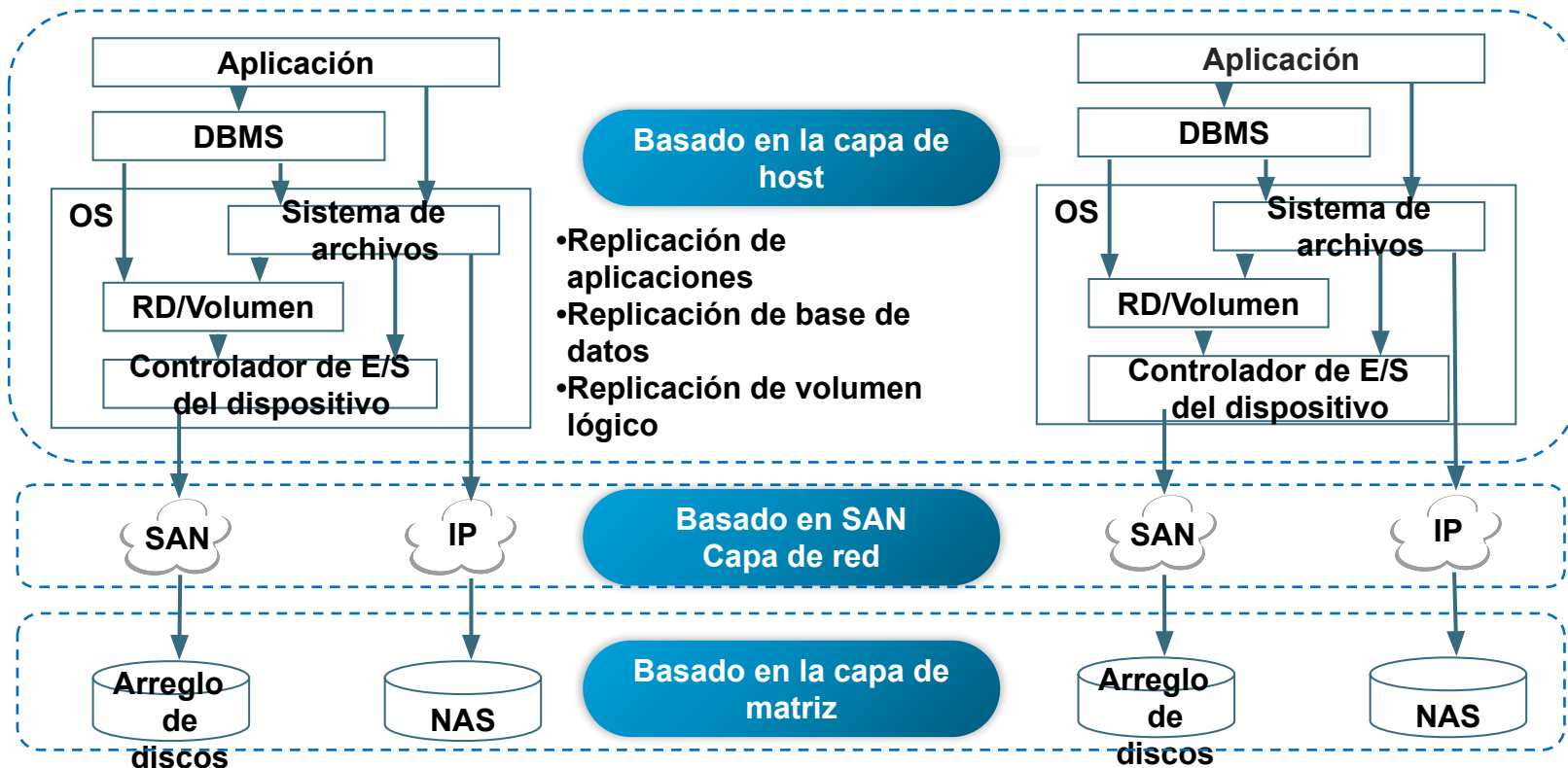




Contenidos

1. Descripción general de la solución de recuperación ante desastres.
2. Arquitectura de la Solución de Recuperación ante Desastres.
3. **Tecnologías comunes de recuperación ante desastres.**
4. Caso práctico de la aplicación de recuperación ante desastres.

Principales tecnologías para DR

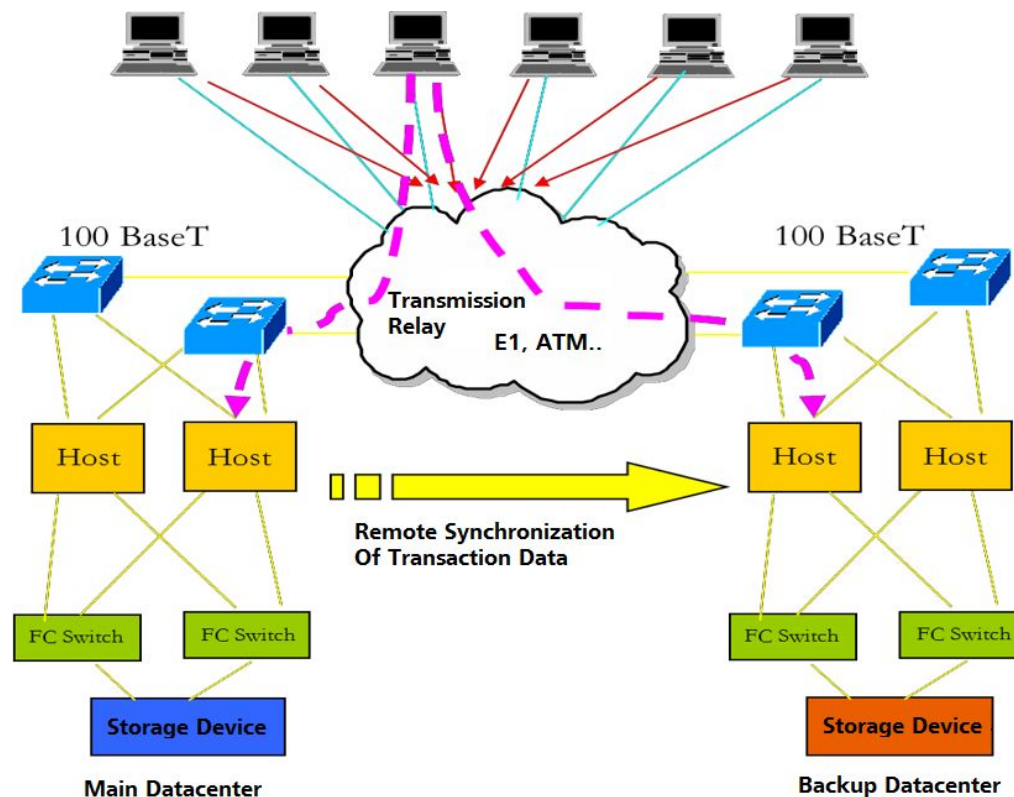


RD: Dispositivo sin procesar

DBMS: Sistema de gestión de bases de datos

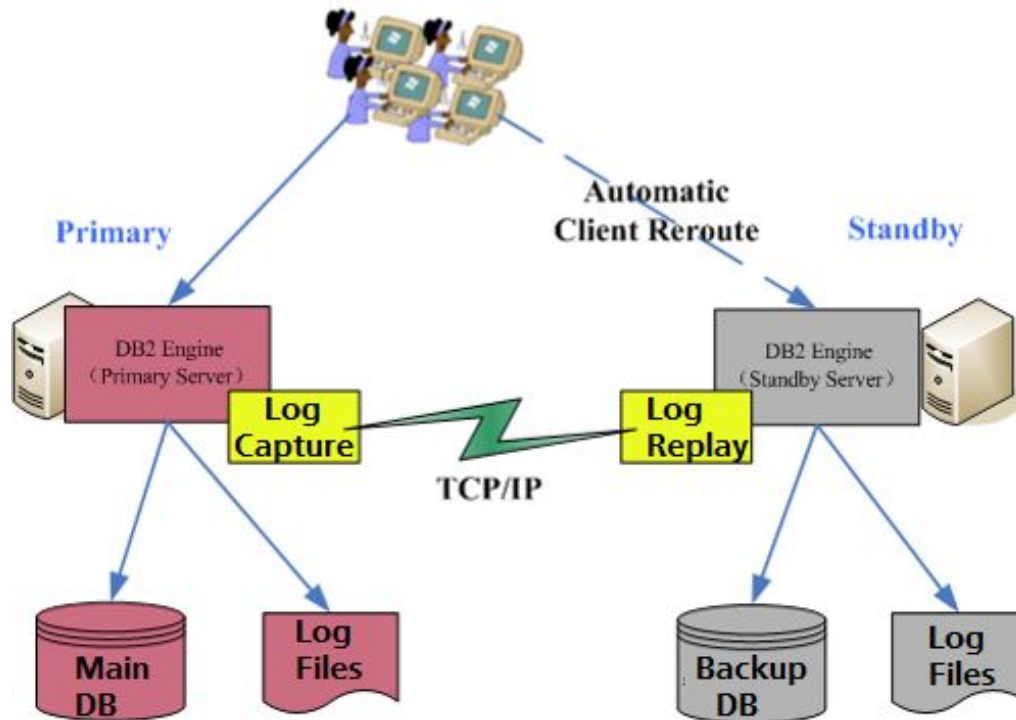
Tecnología DR de Capa de host - Nivel de Aplicación

- La tecnología de recuperación ante desastres a nivel de aplicación permite la replicación remota y la sincronización de datos por software de aplicación. Cuando se produce un error en el centro principal, el sistema de software de aplicación del centro de copia de seguridad de recuperación ante desastres reanuda la operación y se hace cargo de los servicios del centro principal.



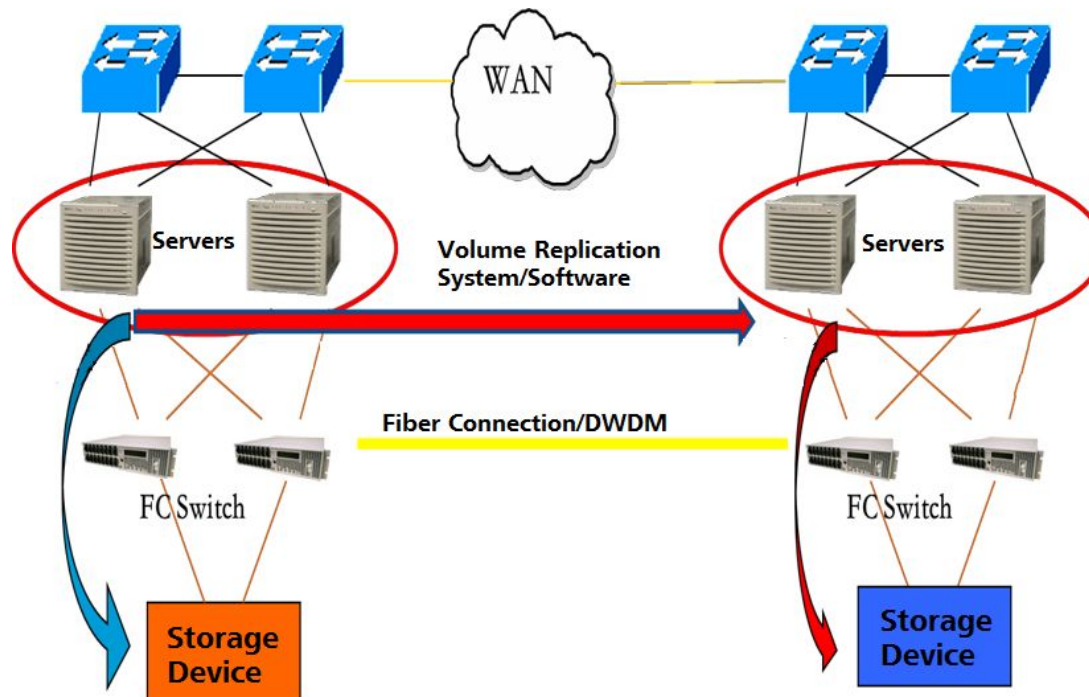
Tecnología DR de capa de host - Nivel de datos

- La tecnología de recuperación ante desastres a nivel de base de datos es una solución de recuperación ante desastres diseñada específicamente para bases de datos. Una base de datos típica suele tener recuperación ante desastres a nivel de base de datos. Por ejemplo: Oracle Data Guard, DB2 HADR, etc. La recuperación ante desastres en el nivel de base de datos se logra principalmente mediante la transferencia de registros de base de datos y la reproducción en sitios de recuperación ante desastres. La tecnología de recuperación ante desastres a nivel de base de datos se puede cambiar sin problemas en caso de desastre.



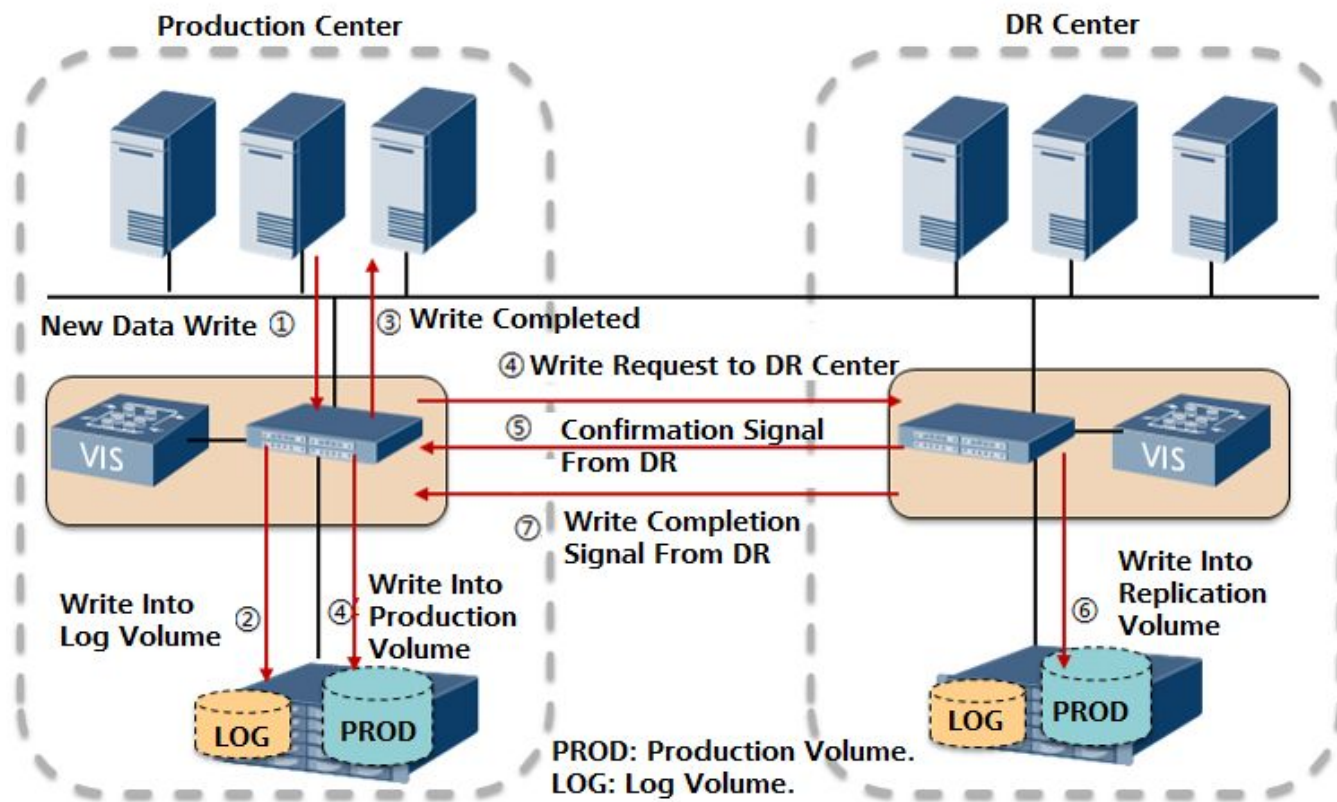
Tecnología DR de capa de host - Nivel de Volumen Lógico

- La replicación remota de datos basada en volúmenes de disco lógico hace referencia a la replicación sincrónica remota (o asincrónica) de uno o varios volúmenes en función de la demanda. La implementación de esta solución se realiza generalmente a través de software.

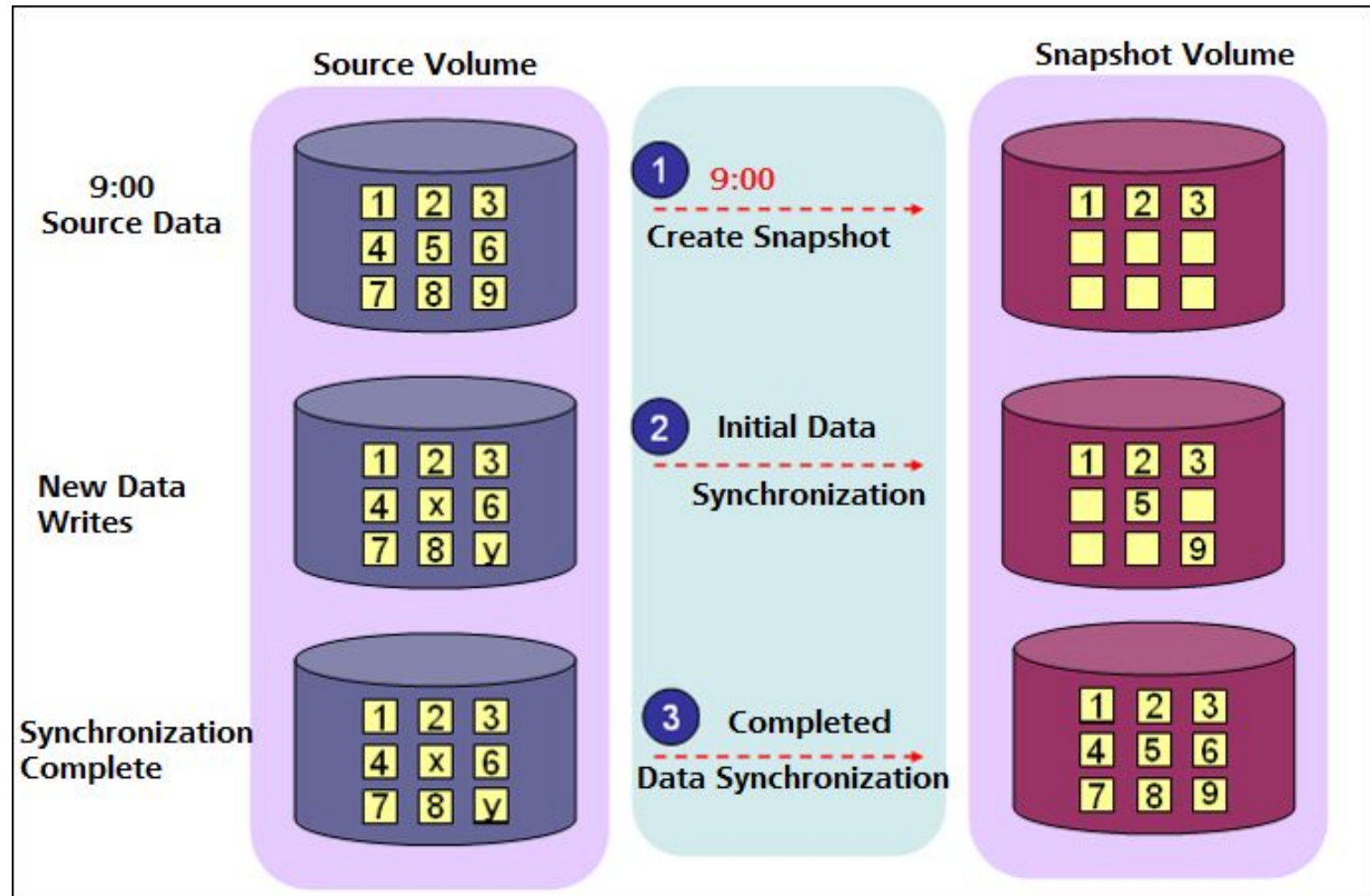


Tecnología DR de capa de red

- La tecnología de replicación de datos basada en SAN es una red de área de almacenamiento (SAN) entre el servidor de aplicaciones front-end y el sistema de almacenamiento back-end. Se agrega una capa de conmutadores inteligentes, donde el front-end está conectado al servidor y los hosts, y el back-end está conectado a los dispositivos de almacenamiento.

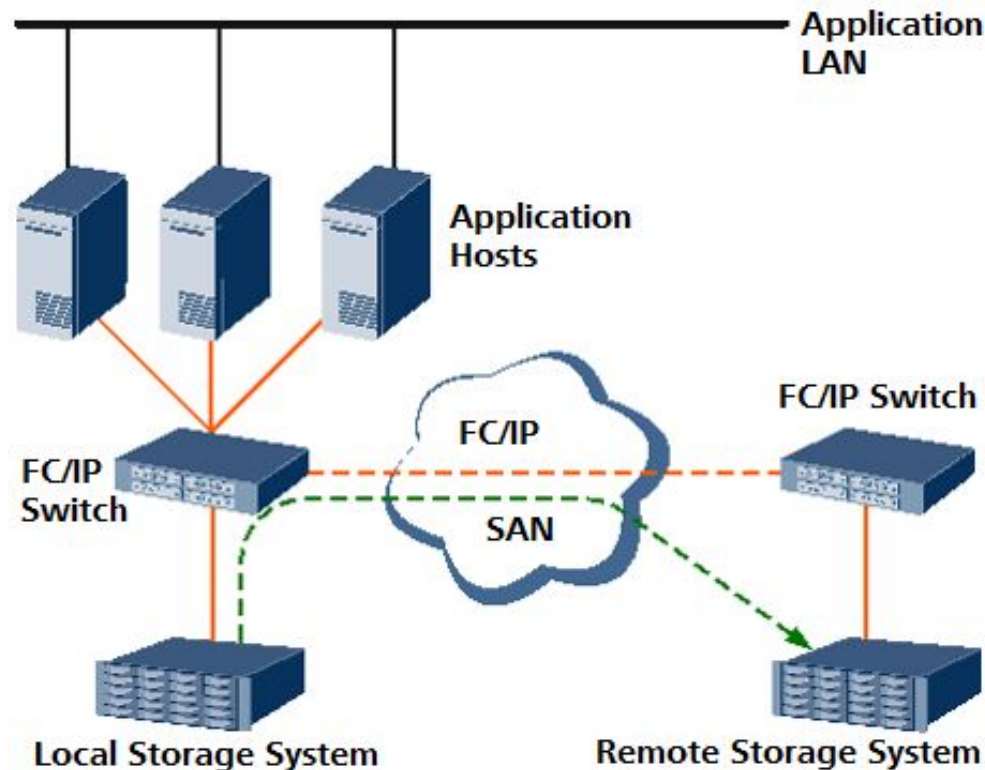


Principio de trabajo de la snapshot de espacio completo de la capa de red

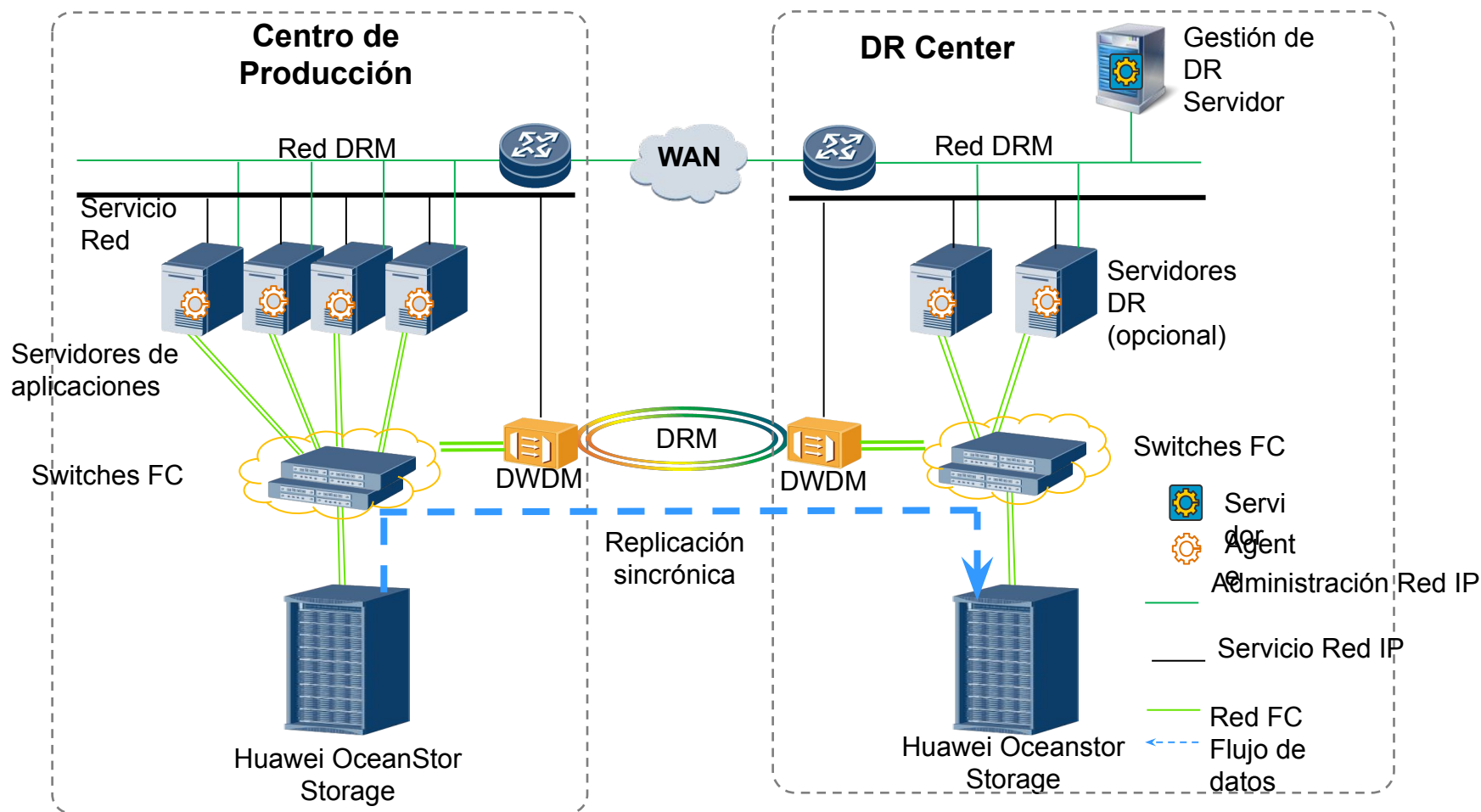


Tecnología DR de nivel de matriz

- La recuperación ante desastres a nivel de matriz se implementa principalmente mediante la tecnología de replicación entre arreglos de discos. Puesto que la replicación de la matriz no pasa a través del host, hay un efecto mínimo en el rendimiento del host.



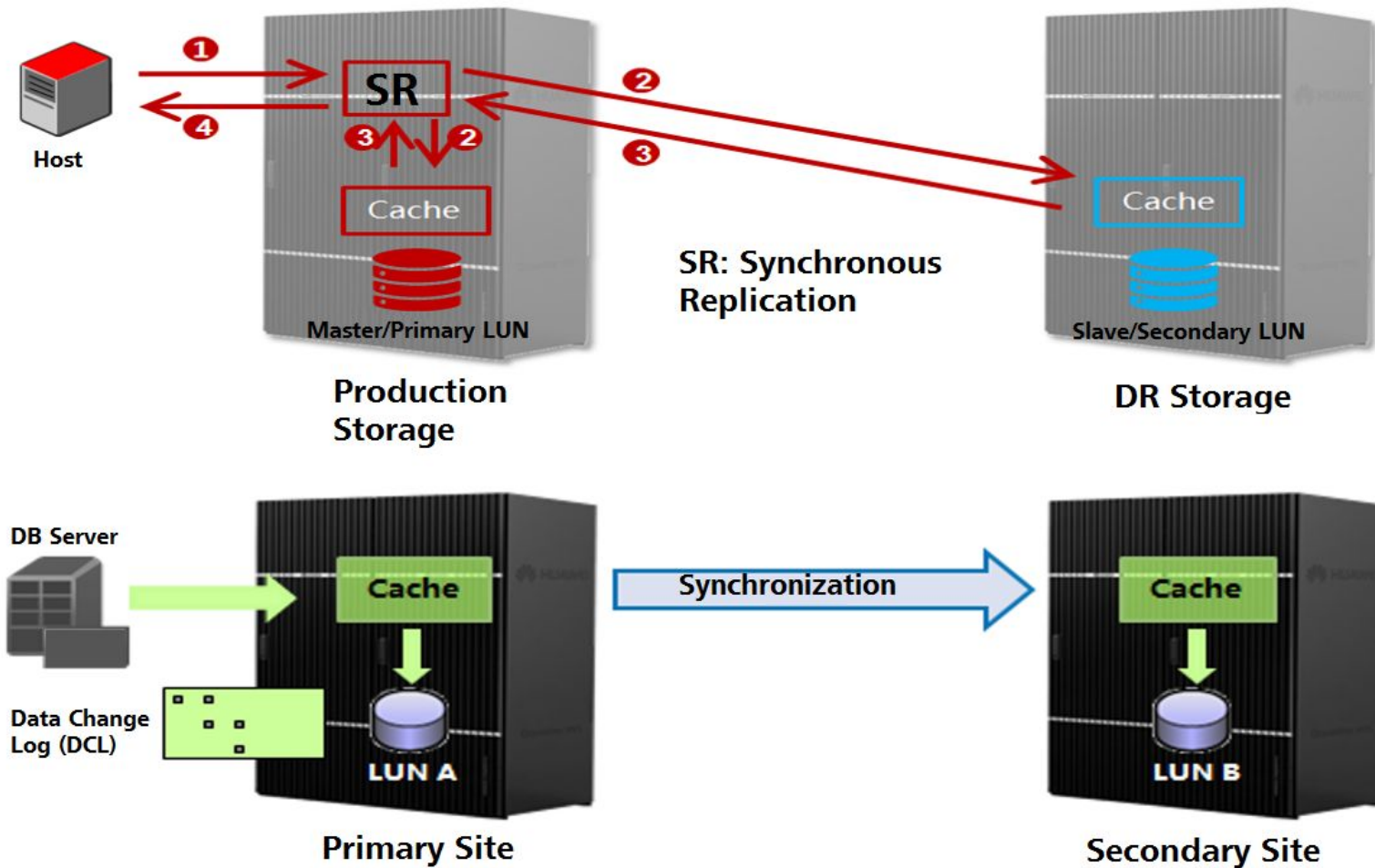
DR de replicación sincrónica de SAN



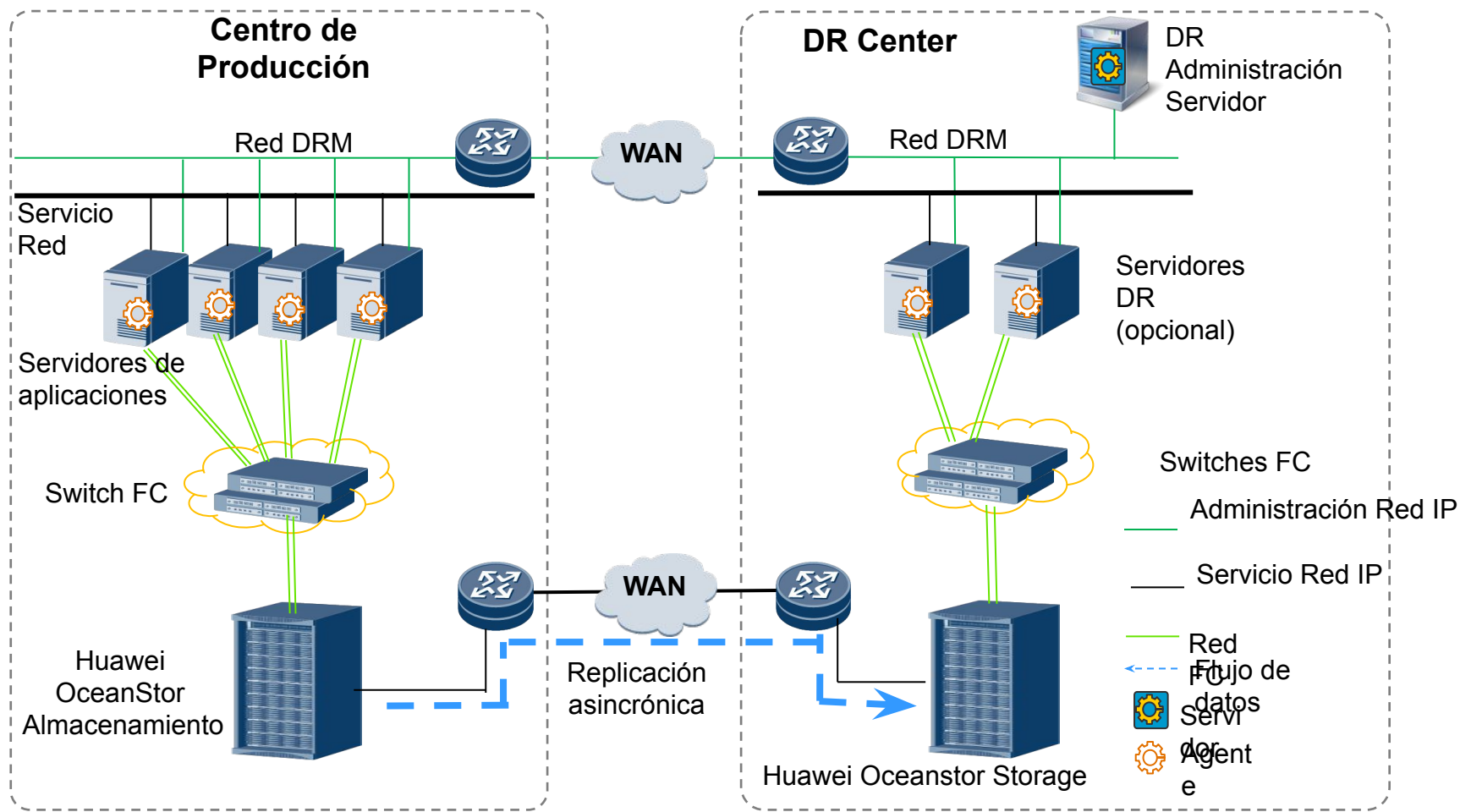
DRM: Gestión de Recuperación ante Desastres.

DRN: Red de replicación de datos.

Principios de trabajo de la replicación sincrónica de SAN

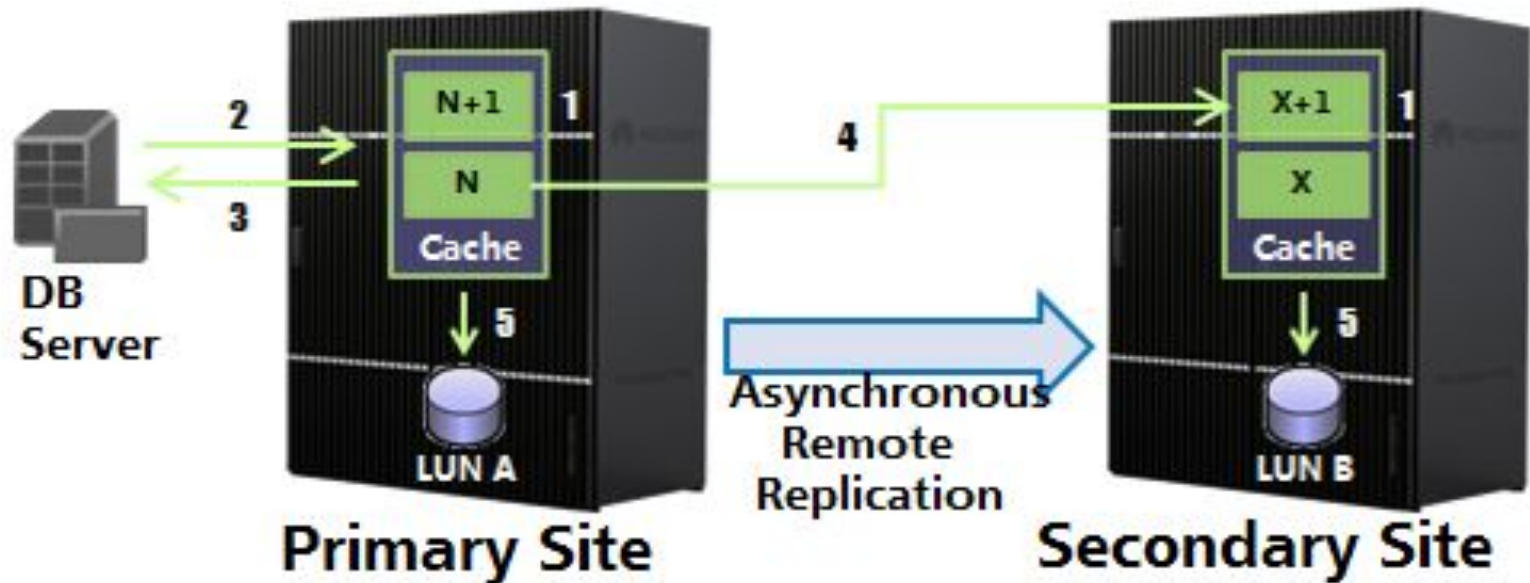


DR de Replicación Asincrónica de SAN

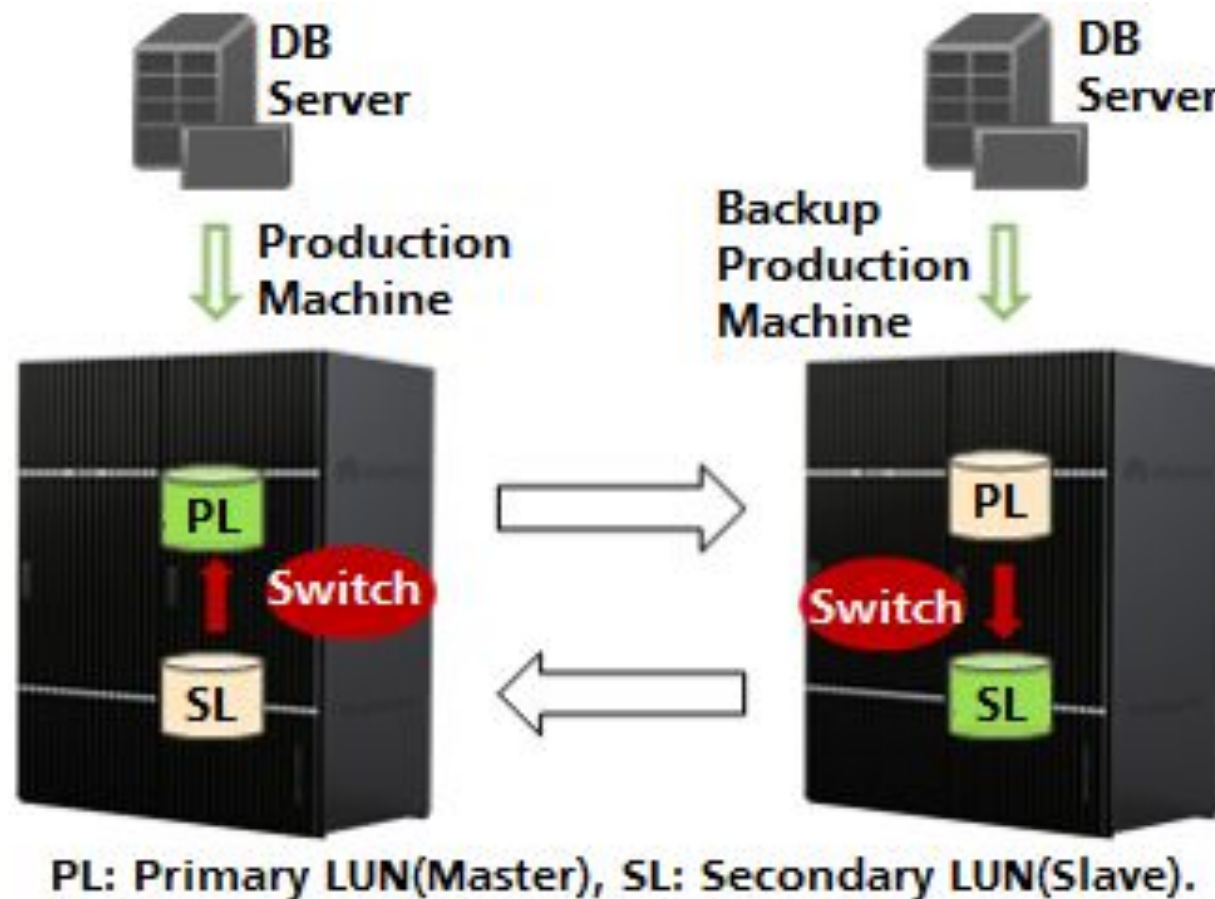


DRM: Gestión de Recuperación ante Desastres.

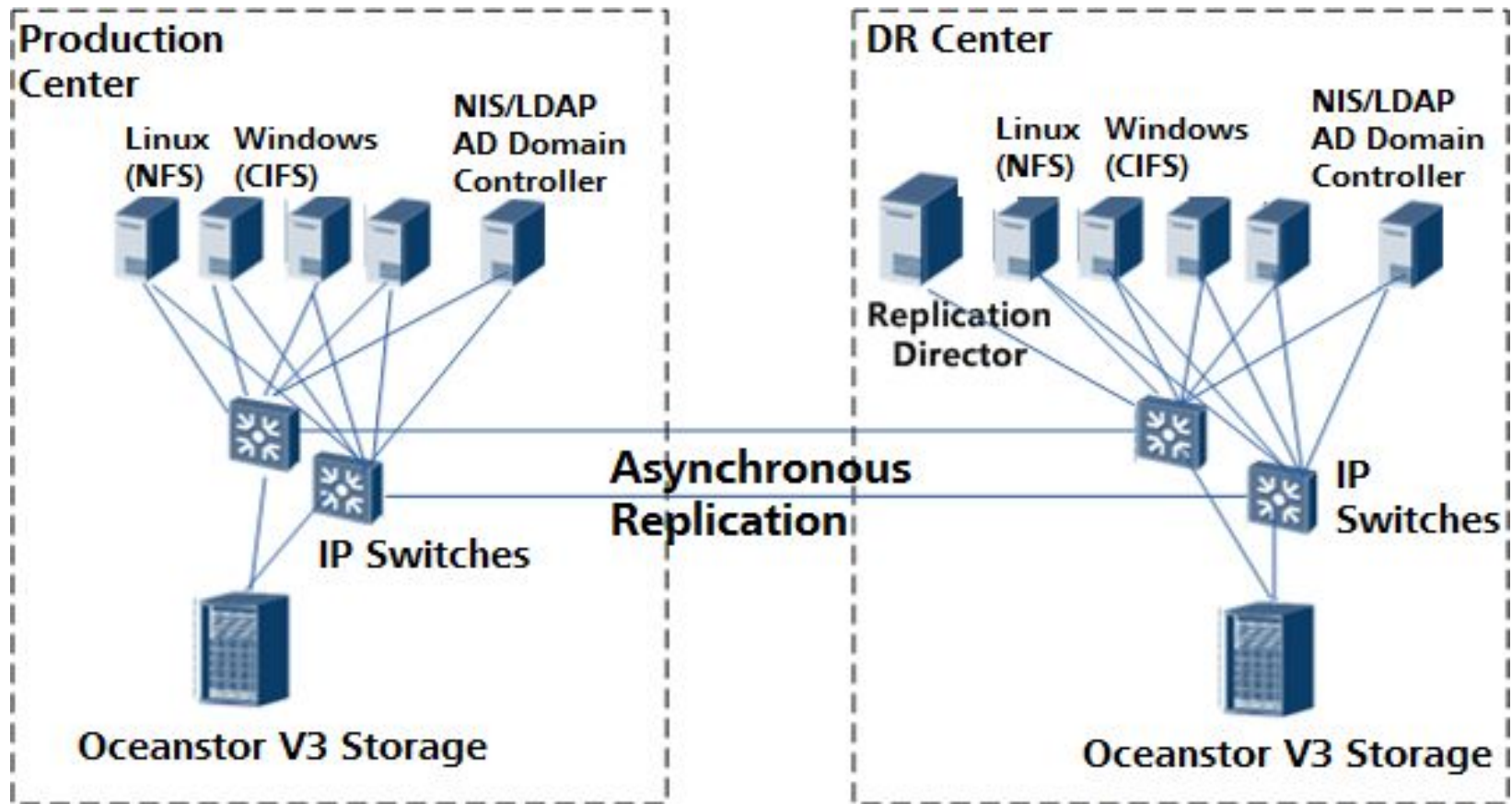
Principio de trabajo de la replicación asincrónica de SAN



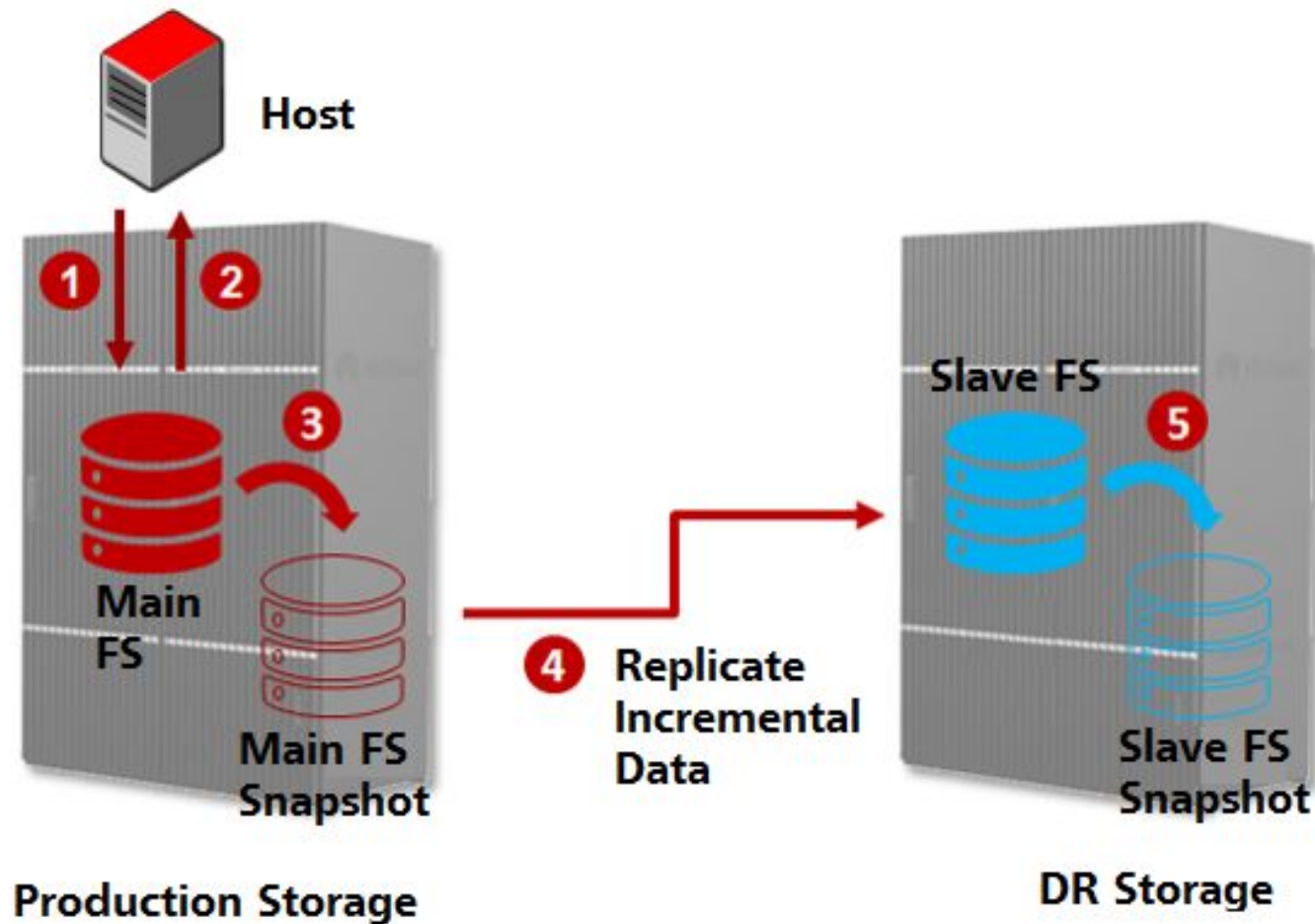
Principio de trabajo de la replicación asincrónica de SAN



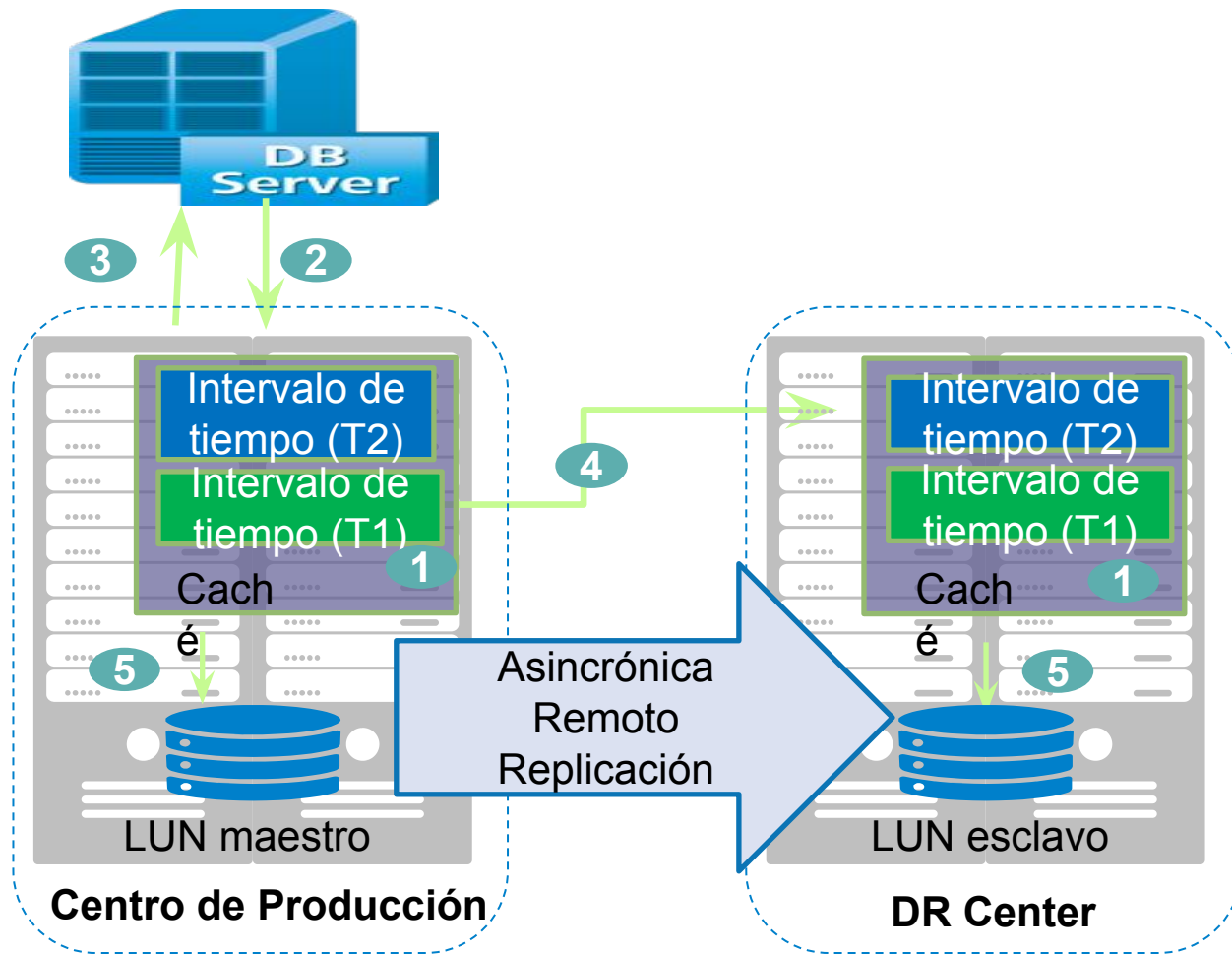
Recuperación de recuperación ante desastres de replicación asincrónica NAS



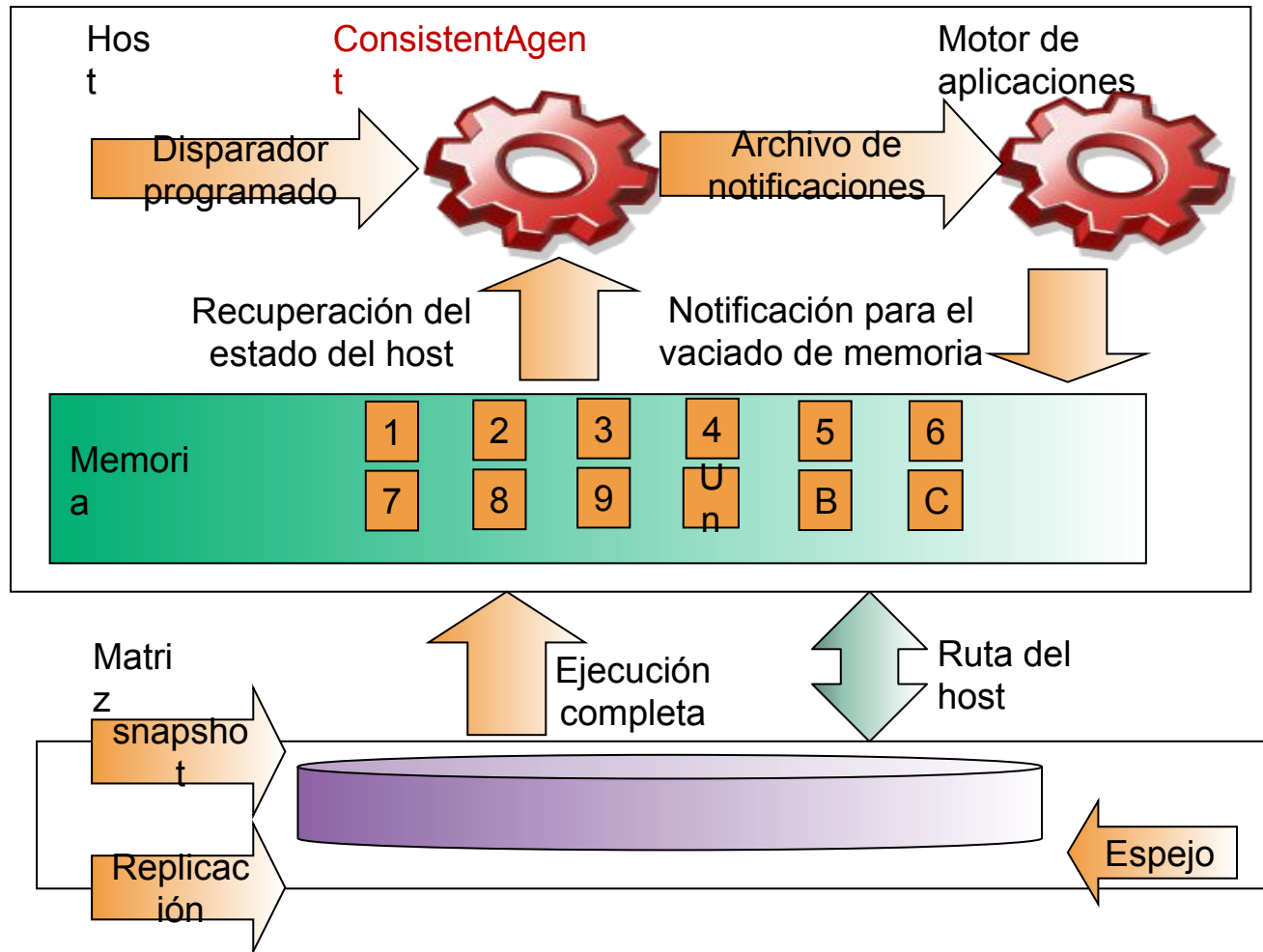
Principios de trabajo de la replicación asincrónica NAS



Replicación remota asincrónica de punto de tiempo múltiple - RPO de nivel de segundos

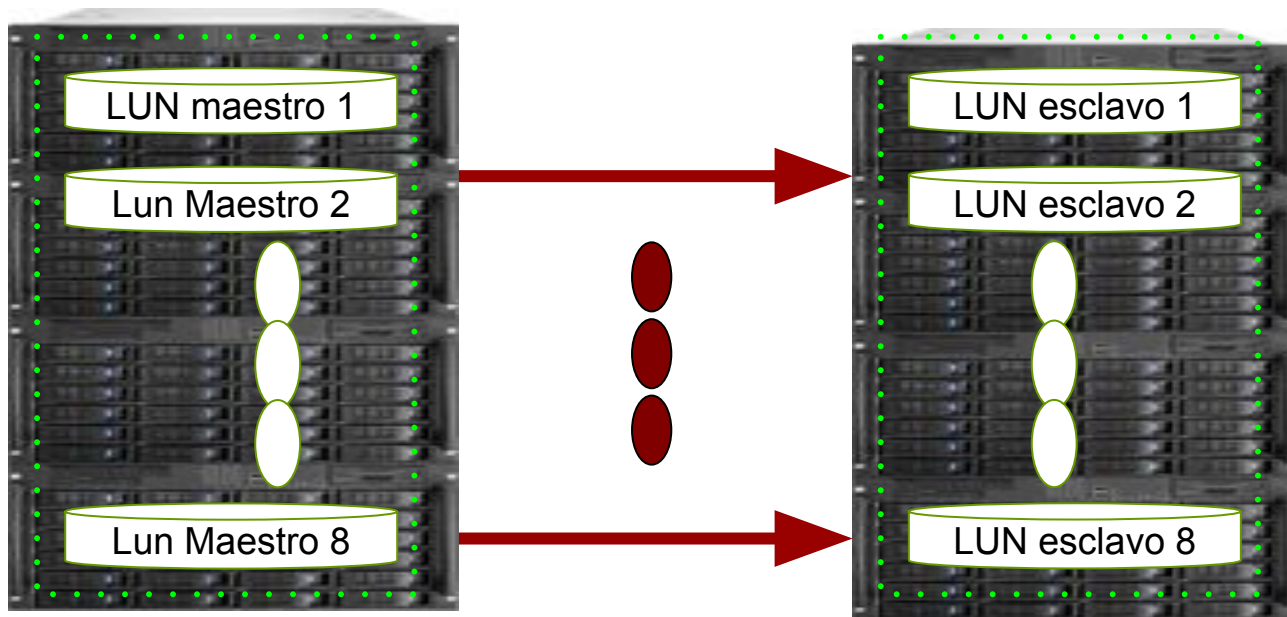


Replicación remota - Consistencia de la aplicación



Replicación remota - Grupo de consistencia

- Se utiliza para mantener la coherencia de tiempo de los datos reflejados de varios LUNs.
- Todos los miembros se sincronizan, dividen, rompen y cambian entre primarios y secundarios juntos al mismo tiempo.



Comparaciones sobre tipos de tecnología DR (1)

Capa Host

(Software de replicación típico como Symantec VVR, Oracle DataGuard, DSG y Quest, etc.)

Pros

- Implementado en el lado del host, no es necesario tener en cuenta la compatibilidad entre los dispositivos subyacentes.
- Cuando se replica la base de datos, el centro de recuperación ante desastres puede tomar parte del trabajo del centro de producción.

Contras

- La replicación de base de datos solo se puede implementar en la base de datos correspondiente.
- La replicación de nivel de host utiliza una cierta cantidad de recursos de host y afecta al sistema de aplicaciones.
- La implementación se implementa completamente en el equipo host. Es más complejo y por lo general requiere la modificación del sistema.

Capa de red

(Ejemplos típicos como IBM SVC, EMC, VPLEX, **Huawei VIS** etc.)

Pros

- Amplia compatibilidad para la integración de recursos de múltiples almacenamientos SAN heterogéneos en el back-end.
- Múltiples arreglos de discos SAN pueden ser tolerantes a desastres al mismo tiempo, eliminando así la necesidad de construir arreglos de discos uno a uno.
- Cree una plataforma básica de recuperación ante desastres con una buena escalabilidad.
- El costo de construcción es independiente del número de hosts y el número de arreglos de discos, lo que simplifica el proceso de cálculo del coste.

Contras

- El costo inicial de construcción es relativamente alto y hay menos proveedores disponibles para proporcionar soluciones.

Comparaciones sobre tipos de tecnología DR (2)

Capa de matriz

(La mayoría de los principales proveedores admiten arreglos de discos habilitados para la creación de reflejo o la replicación, como **Serie Huawei OceanStor V3.**)

Pros

- No tiene ningún impacto en el sistema de aplicación host y tiene un proceso de construcción simple.
- Cuando se produce un error en la matriz de producción, la aplicación se puede cambiar a una matriz tolerante a desastres en un corto período de tiempo.
- Las licencias se basan en la implementación de la matriz subyacente, no según el número de hosts.

Contras

- La matriz en ambos extremos debe ser el mismo producto del fabricante y no puede resolver el problema heterogéneo de la matriz.
- No se puede acceder a los datos del sitio remoto en tiempo real. Los volúmenes de datos deben verse después de promocionarse o visualizarse a través de snapshots.

Solución Típica de Simulación de DR

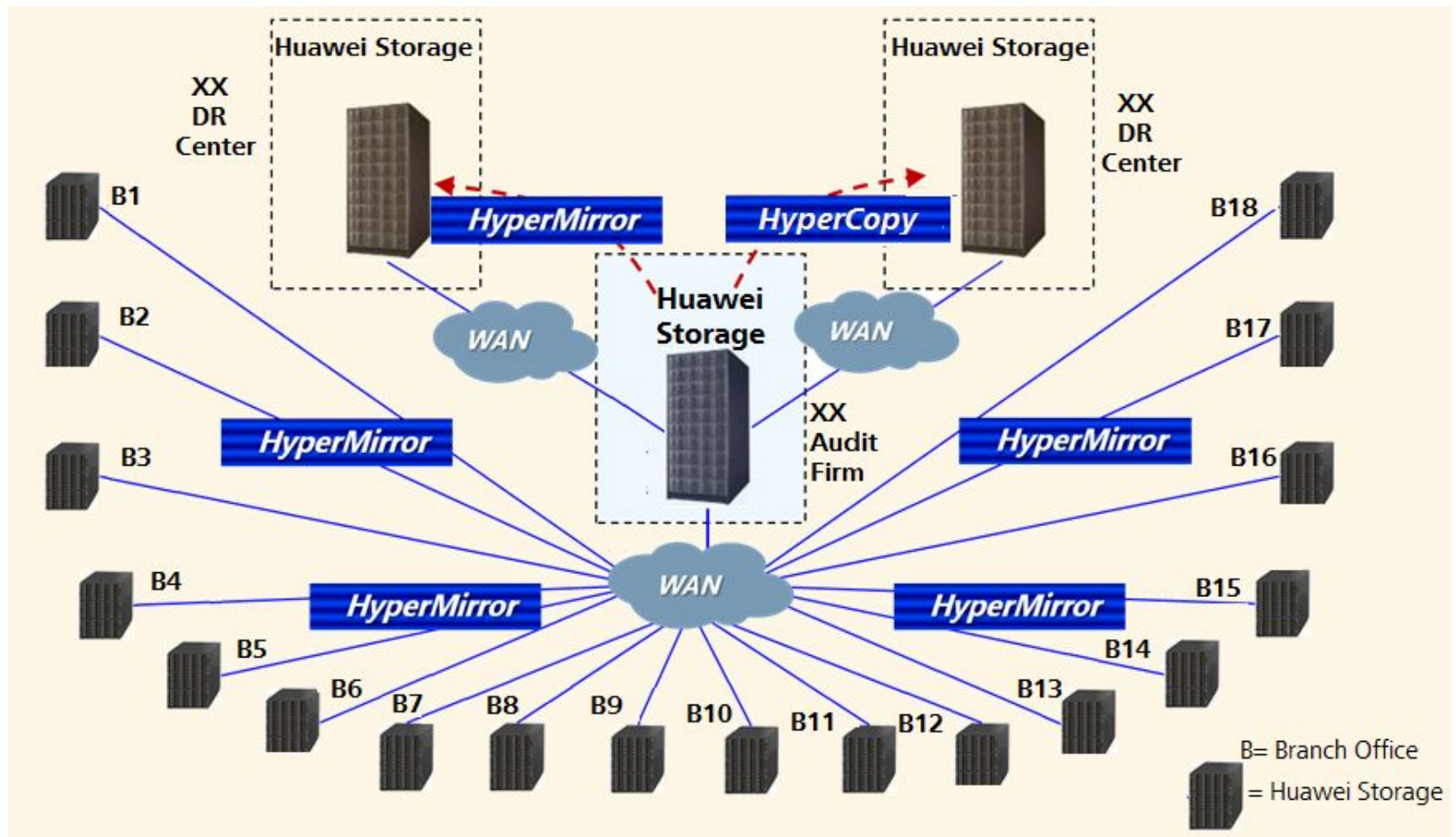




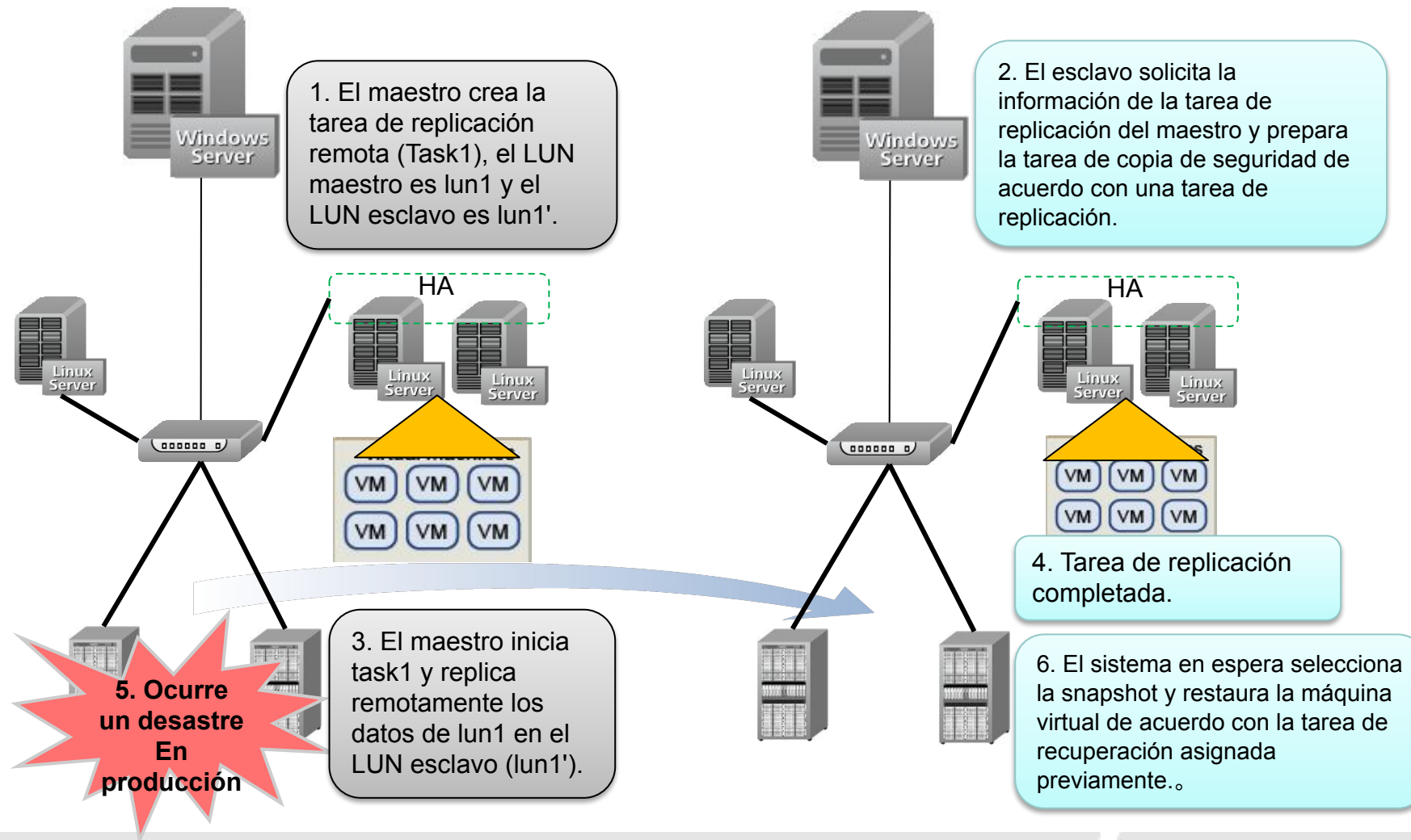
Contenidos

1. Descripción general de la solución de recuperación ante desastres.
2. Arquitectura de la Solución de Recuperación ante Desastres.
3. Tecnologías comunes de recuperación ante desastres.
4. **Caso práctico de la aplicación de recuperación ante desastres.**

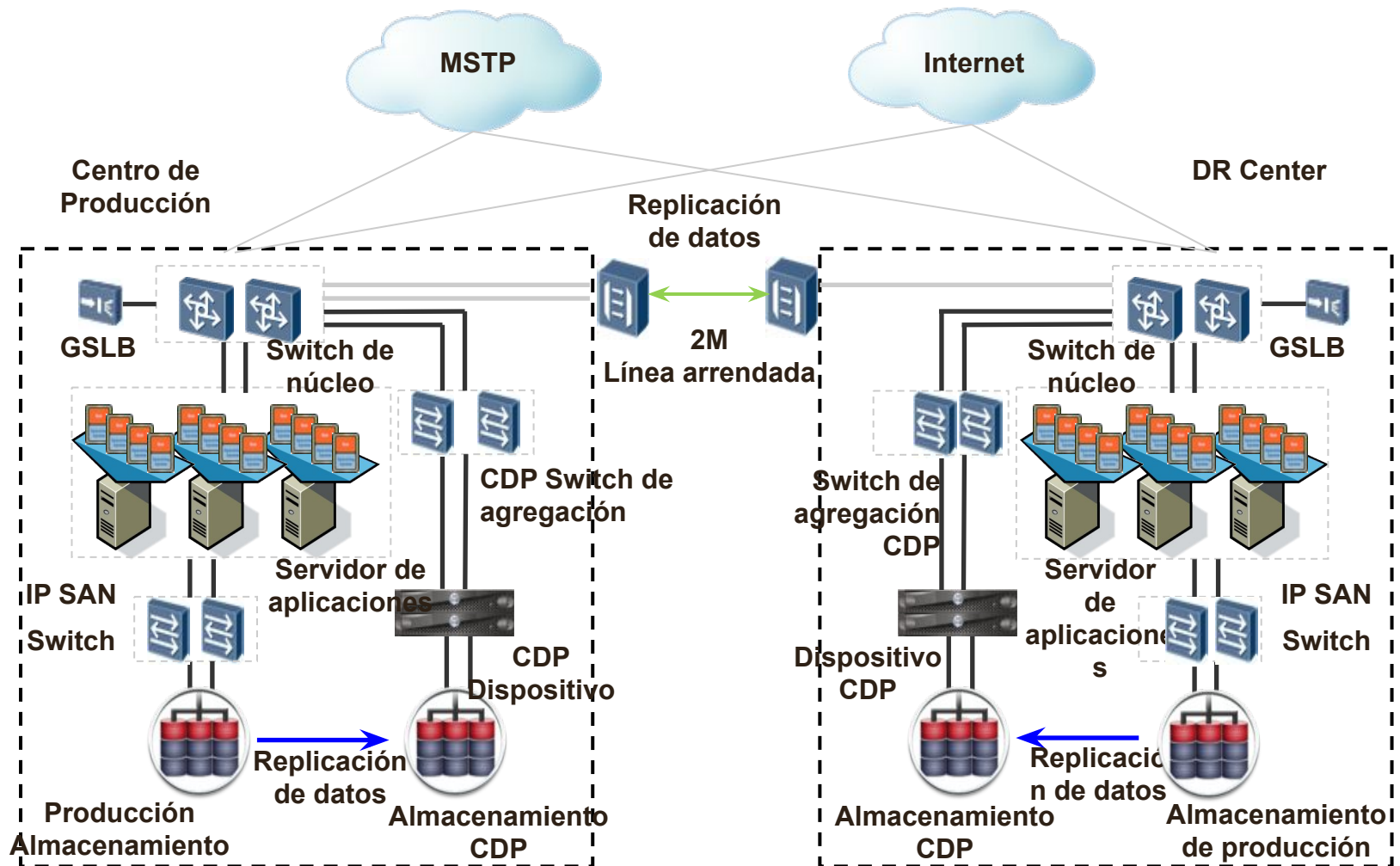
Caso 1:XX Sistema centralizado de DR multiregion



Caso 2:XX Proyecto DR virtualizado



Caso 3: Solución DR de nivel de aplicación





Resumen

- Este módulo principalmente nos permite aprender sobre:
 - Los conceptos de DR y la importancia de construir los sistemas de recuperación ante desastres.
 - Las soluciones comunes de recuperación ante desastres y las ventajas y desventajas de estas soluciones.
 - Las diferentes tecnologías utilizadas para implementar estas soluciones de recuperación ante desastres y los casos de aplicación de recuperación ante desastres típicos.

Quiz

1. (Verdadero o Falso) La replicación remota sincrónica puede lograr RTO-0 y RPO-0. ()
2. (MCQ) El núcleo de la tecnología de recuperación ante desastres es la tecnología de replicación de datos, pero hay muchos tipos de estas tecnologías, por lo que ¿cuáles de las 3 capas siguientes se pueden implementar con dispositivos que implementan la funcionalidad de replicación de datos? ()
 - A. Capa de aplicación.
 - B. Capa Host.
 - C. Capa de red.
 - D. Capa de almacenamiento.

Gracias

www.huawei.com

You