FlexPod DataCenter con NetApp SnapMirror Business Continuity y ONTAP 9.10

FlexPod

NetApp
March 25, 2024

Tabla de contenidos

FlexPod DataCenter con NetApp SnapMirror Business Continuity y ONTAP 9.10

TR-4920: Continuidad del negocio de FlexPod Datacenter con NetApp SnapMirror y ONTAP 9.10

Jyh-shing Chen, NetApp

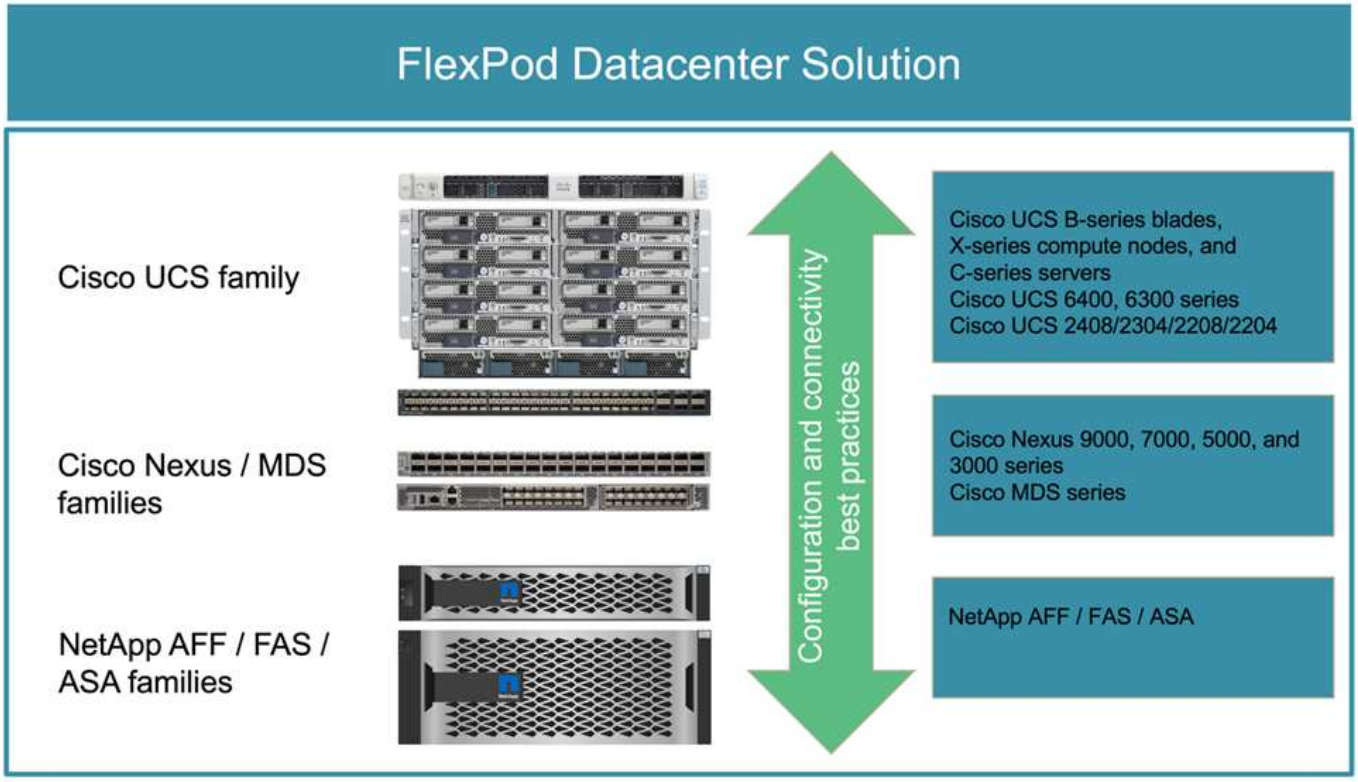
Introducción

Solución de FlexPod

FlexPod es una arquitectura de centro de datos de infraestructura convergente que incluye los siguientes componentes de Cisco y NetApp:

- Sistema de computación unificada de Cisco (Cisco UCS)
- Familias de switches Cisco Nexus y MDS
- Sistemas de cabinas FAS, AFF de NetApp y All SAN (ASA) de NetApp

En la siguiente figura, se describen algunos de los componentes utilizados para crear soluciones de FlexPod. Estos componentes están conectados y configurados según las prácticas recomendadas de Cisco y NetApp, a fin de proporcionar una plataforma ideal para ejecutar diversas cargas de trabajo empresariales con total confianza.



Hay disponible una amplia cartera de diseños validados por Cisco (CVD) y arquitecturas verificadas por NetApp (NVA). Estos CVD y NVA cubren todas las principales cargas de trabajo de los centros de datos y son

el resultado de colaboraciones e innovaciones continuas entre NetApp y Cisco en soluciones FlexPod.

Incorporando pruebas y validaciones en su proceso de creación, los CVD y NVA de FlexPod proporcionan diseños de arquitectura de la solución de referencia y guías de puesta en marcha paso a paso para ayudar a los partners y a los clientes a poner en marcha y adoptar soluciones FlexPod. Al utilizar estos CVD y NVA como guías para el diseño y la implementación, las empresas pueden reducir los riesgos, reducir los tiempos de inactividad de la solución y aumentar la disponibilidad, la escalabilidad, la flexibilidad y la seguridad de las soluciones FlexPod que implementan.

Cada una de las familias de componentes de FlexPod mostradas (Cisco UCS, switches Cisco Nexus/MDS y almacenamiento de NetApp) ofrece opciones de plataformas y recursos para escalar la infraestructura de forma horizontal o vertical, al tiempo que admiten las características y la funcionalidad necesarias en las prácticas recomendadas de configuración y conectividad de FlexPod. FlexPod también se puede escalar horizontalmente para entornos que requieran varias puestas en marcha consistentes al implementar pilas FlexPod adicionales.

Continuidad del negocio y recuperación tras desastres

Las empresas pueden adoptar varios métodos para asegurarse de que pueden recuperar rápidamente sus servicios de datos y aplicaciones tras un desastre. Tener un plan de recuperación ante desastres (DR) y continuidad del negocio (BC), implementar una solución que cumpla con los objetivos empresariales y realizar pruebas regulares de los escenarios de desastre permite a las empresas recuperarse de un desastre y continuar con servicios empresariales críticos después de que se produzca una situación de desastre.

Es posible que las empresas tengan distintos requisitos de recuperación ante desastres y continuidad del negocio para distintos tipos de servicios de datos y aplicaciones. Es posible que algunas aplicaciones y datos no sean necesarios durante una situación de emergencia o desastre, mientras que otras deben estar siempre disponibles para respaldar los requisitos empresariales.

En el caso de servicios de datos y aplicaciones cruciales para la misión que podrían interrumpir su negocio cuando no estén disponibles, es necesario realizar una evaluación cuidadosa para responder a preguntas como qué tipo de situaciones de desastre y mantenimiento tiene que tener en cuenta la empresa, ¿cuántos datos puede permitirse perder los negocios en caso de desastre y con qué rapidez puede y debería producirse la recuperación?

Para las empresas que dependen de los servicios de datos para la generación de ingresos, es posible que los servicios de datos deban protegerse con una solución que pueda resistir no solo varios escenarios de un único punto de fallo, sino también un escenario de desastre de interrupción del servicio del sitio para proporcionar operaciones empresariales continuas.

Objetivo de punto de recuperación y objetivo de tiempo de recuperación

El objetivo de punto de recuperación (RPO) mide cuántos datos, en términos de tiempo, se pueden permitir perder o el punto hasta el que se pueden recuperar los datos. Con un plan de backup diario, una empresa puede perder un día de datos, ya que los cambios realizados en los datos desde el último backup podrían perderse en caso de desastre. En el caso de servicios de datos vitales para el negocio, puede que necesite un objetivo de punto de recuperación cero, así como una planificación e infraestructuras asociadas para proteger los datos sin pérdida alguna.

El objetivo de tiempo de recuperación (RTO) mide cuánto tiempo se puede permitir no tener los datos disponibles o la rapidez con la que se deben recuperar los servicios de datos. Por ejemplo, una empresa puede tener una implementación de backup y recuperación que utilice cintas tradicionales para ciertos conjuntos de datos debido a su tamaño. Como resultado, para restaurar los datos desde las cintas de backup, puede tardar varias horas o incluso días en caso de un fallo de la infraestructura. Además, las consideraciones en cuanto a tiempo deben incluir el tiempo para volver a poner en marcha la infraestructura

además de restaurar los datos. En el caso de los servicios de datos de misión crítica, es posible que necesite un objetivo de tiempo de recuperación muy bajo y, por lo tanto, solo puede tolerar un tiempo de conmutación por error de segundos o minutos para volver a poner los servicios de datos online rápidamente y garantizar la continuidad del negocio.

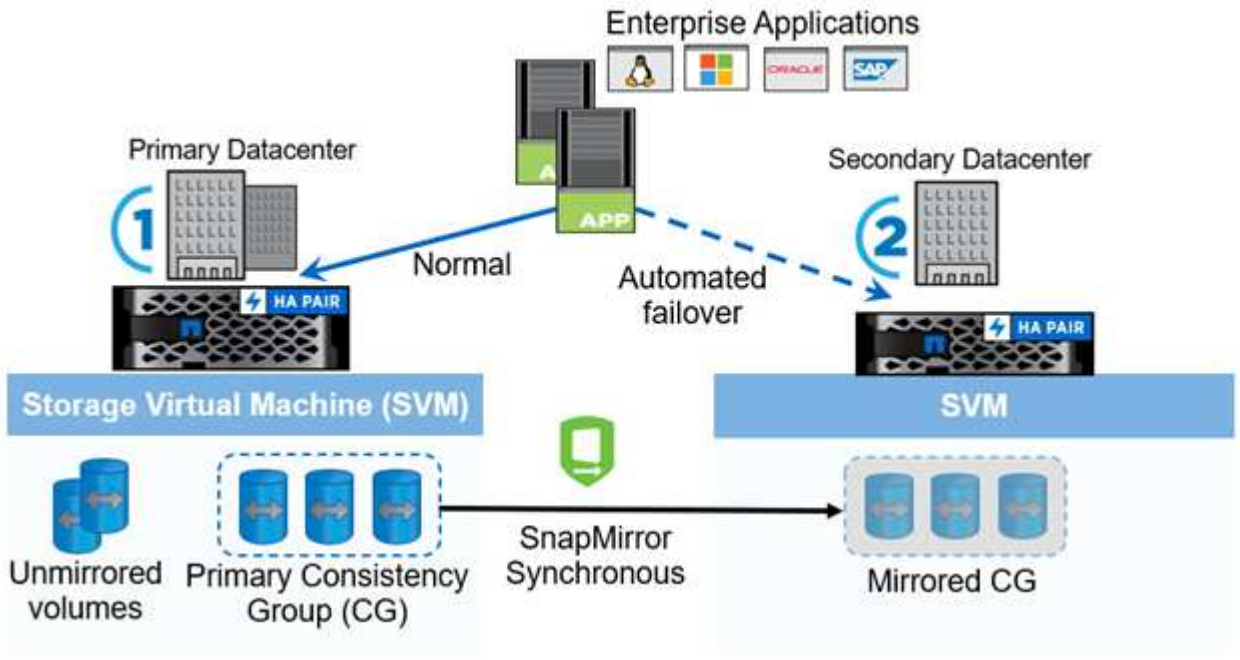
SM-BC

A partir de ONTAP 9.8, puede proteger las cargas DE trabajo SAN para una conmutación por error de aplicaciones transparente con SM-BC de NetApp. Puede crear relaciones de grupos de consistencia entre dos clústeres de AFF o dos clústeres de ASA para que la replicación de datos logre un objetivo de punto de recuperación cero y un objetivo de tiempo de recuperación casi cero.

La solución SM-BC replica los datos mediante la tecnología SnapMirror Synchronous en una red IP. Proporciona granularidad en el nivel de las aplicaciones y conmutación por error automática para proteger los servicios de datos esenciales para la empresa, como Microsoft SQL Server, Oracle, etc., con LUN DE SAN basados en protocolos iSCSI o FC. Un mediador de ONTAP implementado en un centro tercero supervisa la solución SM-BC y permite la recuperación automática tras un desastre en el sitio.

Un grupo de consistencia (CG) es una colección de volúmenes de FlexVol que proporciona una garantía de consistencia de orden de escritura para la carga de trabajo de la aplicación que debe protegerse para la continuidad empresarial. Permite realizar copias Snapshot simultáneas y coherentes con los fallos de una colección de volúmenes en un momento específico. Se establece una relación de SnapMirror, también conocida como una relación de CG, entre un CG de origen y un CG de destino. El grupo de volúmenes que se seleccionó para formar parte de un CG puede asignarse a una instancia de aplicación, a un grupo de instancias de aplicaciones o a una solución completa. Además, las relaciones del grupo de coherencia de SM-BC pueden crearse o eliminarse bajo demanda en función de los requisitos empresariales y cambios.

Como se muestra en la siguiente figura, los datos del grupo de consistencia se replican en un segundo clúster de ONTAP para recuperación ante desastres y continuidad del negocio. Las aplicaciones tienen conectividad con las LUN en ambos clústeres de ONTAP. El clúster principal proporciona I/o y se reanuda automáticamente desde el clúster secundario si se produce un desastre en el principal. Al diseñar una solución SM-BC, se deben observar los números de objetos admitidos para las relaciones de CG (por ejemplo, un máximo de 20 CG y un máximo de 200 extremos) para evitar que se superen los límites admitidos.



"Siguiente: Solución FlexPod SM-BC."

Solución FlexPod SM-BC

"Anterior: Introducción."

Descripción general de la solución

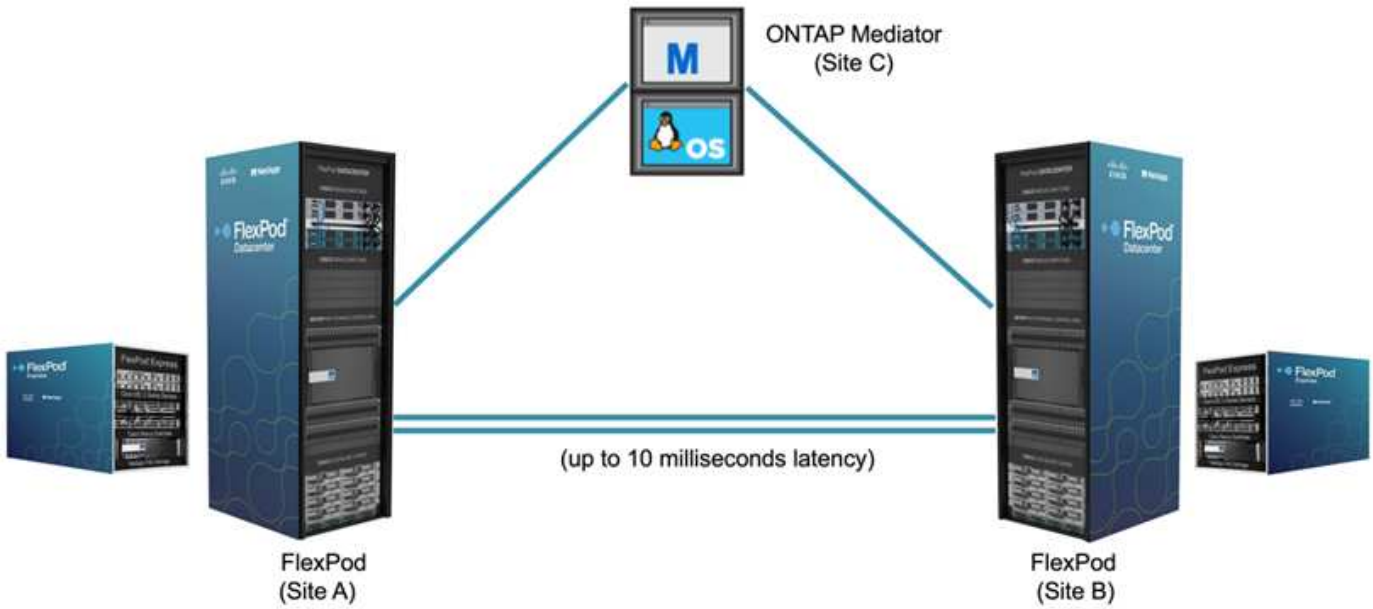
En un nivel superior, una solución FlexPod SM-BC se compone de dos sistemas FlexPod ubicados en dos sitios separados por cierta distancia, conectados y emparejados para ofrecer una solución de centro de datos altamente disponible, flexible y de gran fiabilidad que puede proporcionar continuidad del negocio a pesar de un fallo en el sitio.

Además de poner en marcha dos infraestructuras FlexPod nuevas para crear una solución FlexPod SM-BC, la solución también puede implementarse en dos infraestructuras FlexPod existentes compatibles con SM-BC o agregando una nueva FlexPod a la misma relación con una FlexPod existente.

Los dos sistemas FlexPod en una solución FlexPod SM-BC no necesitan ser idénticos en las configuraciones. Sin embargo, los dos clústeres de ONTAP deben ser de las mismas familias de almacenamiento, ya sea dos sistemas AFF o dos ASA, pero no necesariamente el mismo modelo de hardware. La solución SM-BC no es compatible con los sistemas FAS.

Los dos sitios de FlexPod requieren conectividad de red, lo cual cumple con los requisitos de ancho de banda de la solución y calidad de servicio y tiene una latencia de ida y vuelta de menos de 10 milisegundos (10 ms) entre sitios, según requiera la solución ONTAP SM-BC. Para esta validación de solución FlexPod SM-BC, los dos sitios FlexPod están interconectados mediante una red de capa 2 extendida en el mismo laboratorio.

La solución SM-BC de ONTAP de NetApp proporciona replicación síncrona entre los dos clústeres de almacenamiento de NetApp para lograr una alta disponibilidad y recuperación ante desastres en campus o áreas metropolitanas. El mediador de ONTAP puesto en marcha en un centro tercero supervisa la solución y permite la recuperación automática tras fallos en caso de desastre en el centro. En la siguiente figura, se ofrece una vista general de los componentes de la solución.



Con la solución SM-BC de FlexPod, puede poner en marcha un cloud privado basado en vSphere de VMware en una infraestructura distribuida, pero integrada. La solución integrada permite coordinar varios sitios como

una única infraestructura de soluciones para proteger los servicios de datos de distintos escenarios de un único punto de fallo y un fallo completo del sitio.

En este informe técnico se destacan algunas de las consideraciones de diseño integrales de la solución SM-BC de FlexPod. Se anima a los profesionales a realizar referencias de la información disponible en los distintos CVD y NVA de FlexPod para obtener detalles adicionales sobre la implementación de la solución FlexPod.

A pesar de que la solución se validó por la puesta en marcha de dos sistemas FlexPod basados en prácticas recomendadas de FlexPod tal y como se documenta en CVD, toma en cuenta los requisitos de la solución SM-BC. La solución SM-BC de FlexPod puesta en marcha descrita en este informe se ha validado para lograr resiliencia y tolerancia a fallos durante los distintos escenarios de fallo, así como en un supuesto de fallo simulado del sitio.

Requisitos de la solución

La solución SM-BC de FlexPod ha sido diseñada para responder a los siguientes requisitos clave:

- Continuidad del negocio para aplicaciones vitales para el negocio y servicios de datos en caso de fallo completo del centro de datos (sitio)
- Ubicación flexible y distribuida de las cargas de trabajo con movilidad de cargas de trabajo entre centros de datos
- Afinidad del sitio en la que se accede a los datos de la máquina virtual localmente, desde el mismo centro de datos, durante las operaciones normales
- Recuperación rápida con cero pérdida de datos en caso de fallo en un sitio

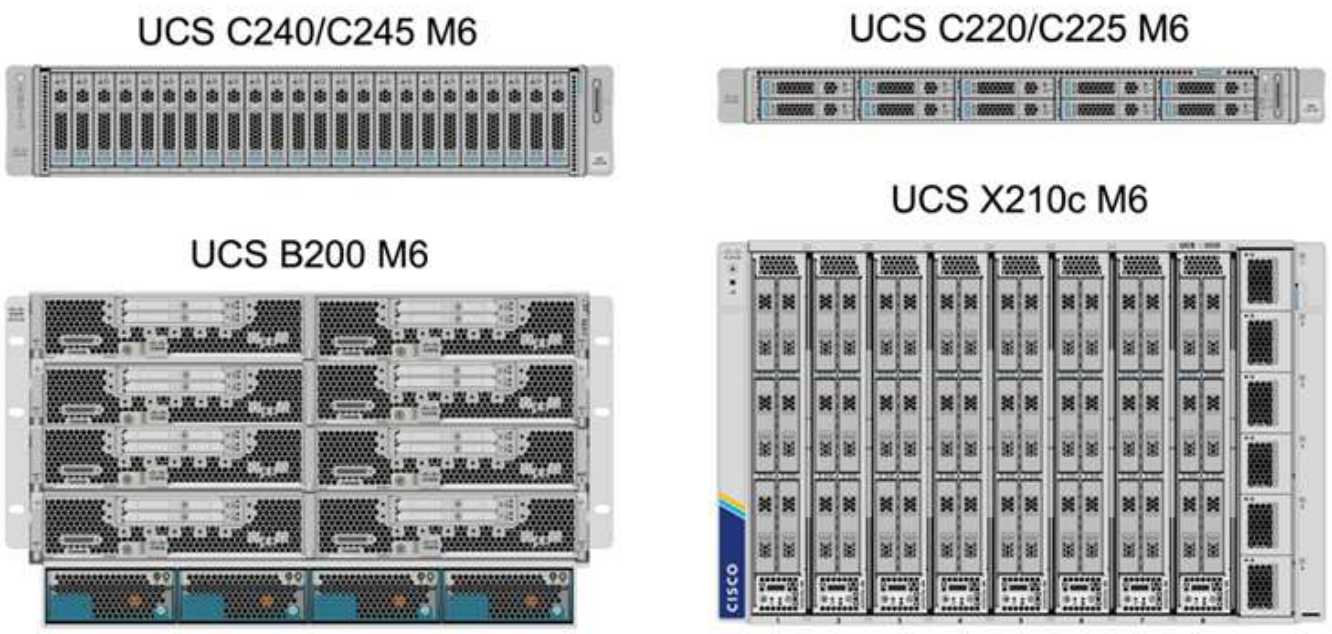
Componentes de la solución

Componentes de computación de Cisco

Cisco UCS es una infraestructura de computación integrada que proporciona recursos informáticos unificados, estructura unificada y gestión unificada. Permite a las empresas automatizar y acelerar la puesta en marcha de aplicaciones, incluidas la virtualización y las cargas de trabajo básicas. Cisco UCS es compatible con una gran variedad de casos de uso de puesta en marcha, incluyendo ubicaciones remotas y sucursales, centros de datos y casos prácticos de cloud híbrido. Dependiendo de los requisitos específicos de la solución, la implementación informática de Cisco de FlexPod puede utilizar una variedad de componentes a diferentes escalas. En las siguientes subsecciones, se proporciona información adicional sobre algunos componentes de UCS.

Nodo de computación y servidor UCS

La siguiente figura muestra algunos ejemplos de componentes de servidor UCS, como los servidores de rack UCS C- Series, el chasis UCS 5108 con servidores blade B-Series y el nuevo chasis UCS X9508 con nodos de computación X-Series. Los servidores en rack Cisco UCS C-Series están disponibles en uno y dos formatos de unidad rack (RU), modelos basados en CPU Intel y AMD, y con distintas velocidades de CPU, núcleos, memoria y opciones de I/O. Los servidores blade Cisco UCS B-Series y los nuevos nodos de computación X-Series también están disponibles con diversas opciones de CPU, memoria e I/o, y todos son compatibles con la arquitectura FlexPod para satisfacer los distintos requisitos empresariales.



Además de los servidores en rack C220/C225/C240/C245 M6 de última generación, los servidores blade B200 M6 y los nodos informáticos X210c que se muestran en esta figura, también pueden utilizarse generaciones anteriores de servidores de rack y blade si siguen siendo compatibles.

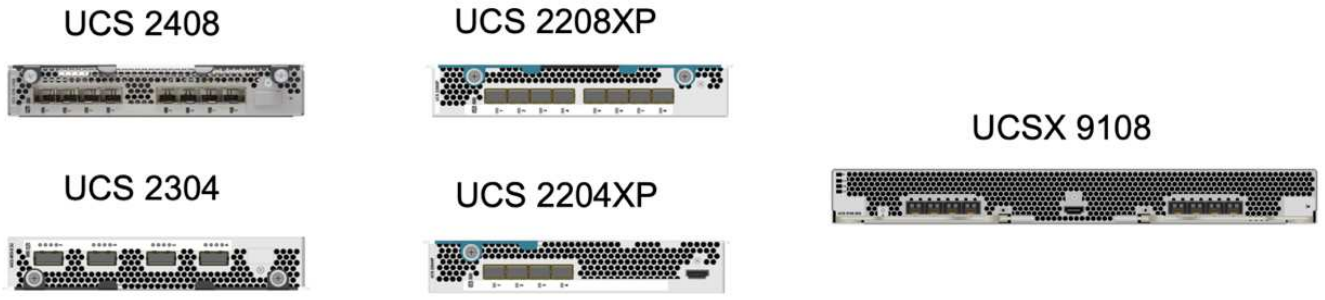
Módulo de I/o y módulo de estructura inteligente

El módulo de E/S (IOM)/extensor de estructura y módulo de estructura inteligente (IFM) proporcionan conectividad de estructura unificada para los chasis de servidor blade Cisco UCS 5108 y los chasis Cisco UCS X9508 de la serie X, respectivamente.

El UCS IOM 2408 de cuarta generación tiene ocho puertos Ethernet unificados de 25 G para conectar el chasis UCS 5108 con interconexión de estructura (FI). Cada 2408 tiene cuatro conectividad Ethernet de plano posterior 10-G a través de la placa media a cada servidor blade del chasis.

El IFM UCSX 9108 25G cuenta con ocho puertos Ethernet unificados de 25-G para conectar los servidores blade en el chasis UCS X9508 con interconexiones de estructura. Cada 9108 tiene cuatro conexiones 25-G hacia cada nodo de computación UCS X210c en el chasis X9108. El 9108 IFM también trabaja conjuntamente con la interconexión de estructuras para gestionar el entorno del chasis.

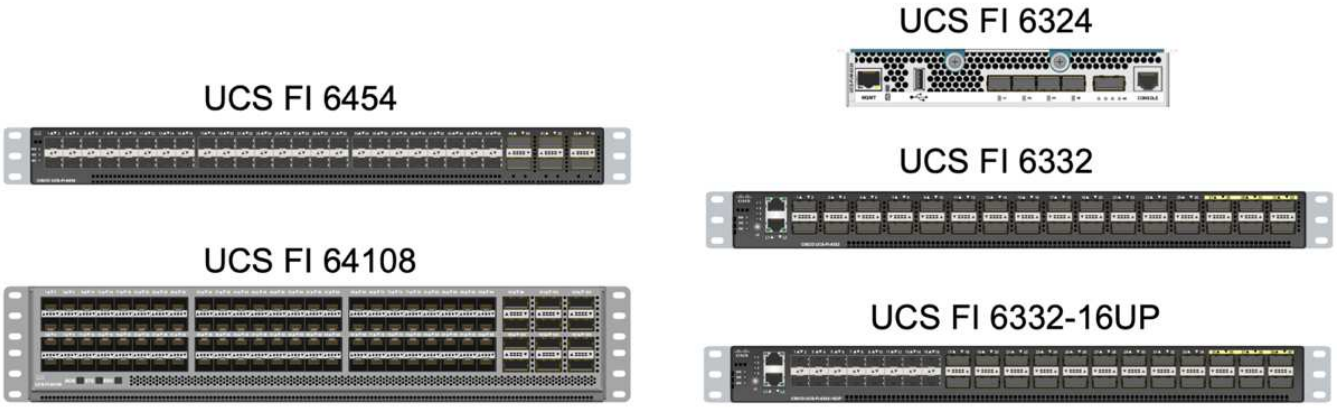
La siguiente figura muestra UCS 2408 y las generaciones de IOM anteriores para el chasis UCS 5108 y el IFM 9108 para el chasis X9508.



Interconexiones de estructura UCS

Los Cisco UCS Fabric Interconnect (FIS) proporcionan conectividad y gestión para todo Cisco UCS. Normalmente implementado como par activo/activo, el FIS del sistema integra todos los componentes en un único dominio de gestión de alta disponibilidad controlado por Cisco UCS Manager o Cisco Intersight. Cisco UCS FIS proporciona una única estructura unificada para el sistema con conmutación de paso de baja latencia e sin pérdidas que admite tráfico LAN, SAN y de gestión mediante un único conjunto de cables.

Hay dos variantes para la cuarta generación de Cisco UCS FIS: UCS FI 6454 y 64108. Incluyen compatibilidad con 10/25 puertos Ethernet de 10 Gbps, puertos Ethernet de 1/25 Gbps, puertos de enlace ascendente Ethernet de 40/100 Gbps y puertos unificados que admiten 10/25 Gigabit Ethernet o Fibre Channel de 8/16/32 Gbps. En la siguiente figura, se muestra el Cisco UCS FIS de cuarta generación junto con los modelos de tercera generación compatibles.

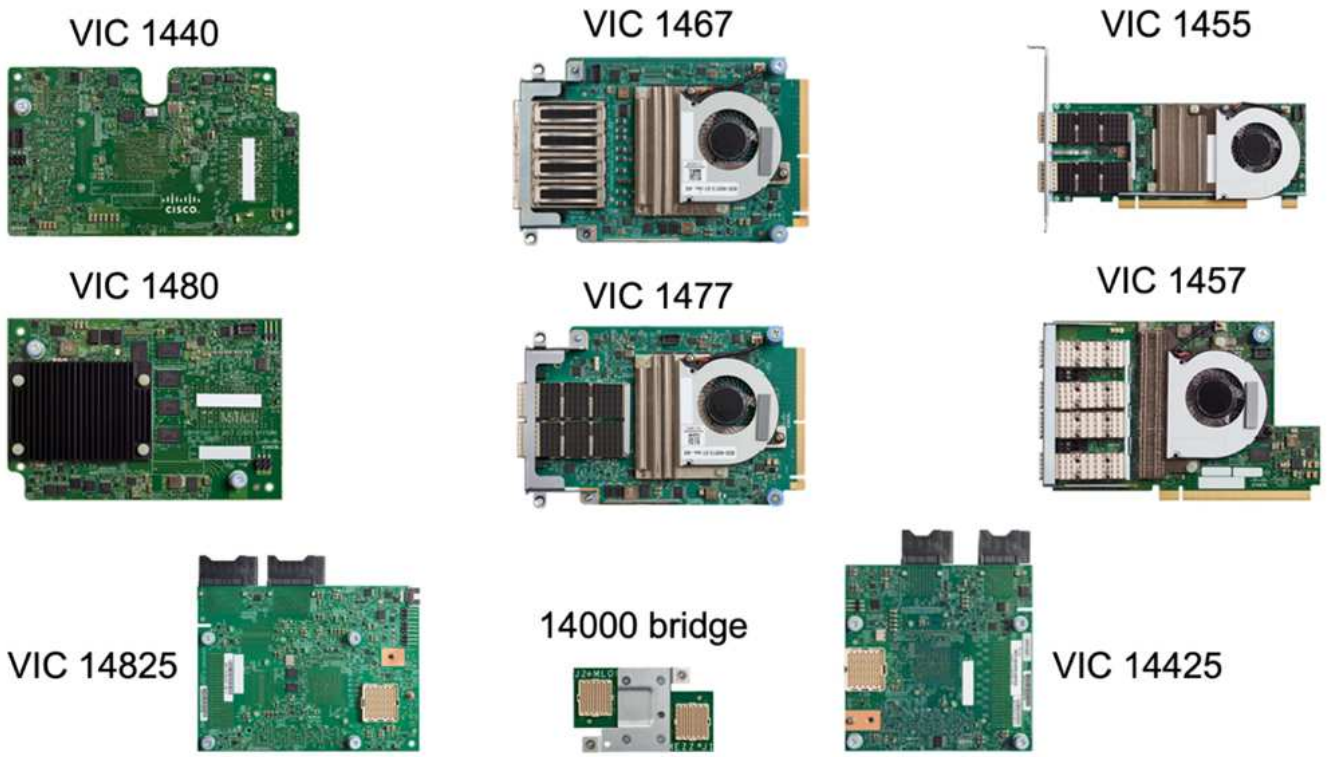


Para admitir el chasis Cisco UCS X-Series, se necesitan interconexiones de estructura de cuarta generación configuradas en el modo gestionado de Intersight (IMM). Sin embargo, es posible ofrecer soporte al chasis Cisco UCS 5108 serie B tanto en modo IMM como en modo gestionado UCSM.

UCS FI 6324 utiliza el factor de forma IOM y está integrado en un chasis UCS Mini para puestas en marcha que solo requieren un dominio UCS pequeño.

Tarjetas de interfaz virtual UCS

Las tarjetas de interfaz de usuario virtual (VIC) de Cisco UCS unifican la gestión del sistema y la conectividad LAN y SAN para servidores montados en rack y blade. Admite hasta 256 dispositivos virtuales, ya sea como tarjetas de interfaz de red virtuales (vNIC) o como adaptadores de bus host virtual (vHBA) mediante la tecnología Cisco SingleConnect. Como resultado de la virtualización, las tarjetas VIC simplifican en gran medida la conectividad de red y reducen el número de adaptadores de red, cables y puertos de switch necesarios para la puesta en marcha de la solución. En la siguiente figura, se muestran algunos de los ICS de Cisco UCS disponibles para los servidores B-Series y C-Series y los nodos de computación X-Series.



Los diferentes modelos de adaptador admiten diferentes servidores blade y en rack con diferentes recuentos de puertos, velocidades de puerto y factores de forma de LAN modular en placa base (mLOM), tarjetas mezzanine e interfaces PCIe. Los adaptadores admiten algunas combinaciones de Ethernet 10/25/40/100-G y Fibre Channel sobre Ethernet (FCoE). Incorporan la tecnología de adaptador de red convergente (CNA) de Cisco, admiten un conjunto de funciones completo y simplifican la administración de adaptadores y la implementación de aplicaciones. Por ejemplo, el VIC es compatible con la tecnología Data Center Virtual Machine Fabric extender (VM-FEX) de Cisco, que amplía los puertos de interconexión de estructura Cisco UCS a los equipos virtuales, simplificando así la puesta en marcha de la virtualización de servidores.

Gracias a la combinación de Cisco VIC en configuraciones de mLOM, mezzanine, ampliación de puertos y tarjetas de puente, puede aprovechar por completo el ancho de banda y la conectividad disponibles para los servidores blade. Por ejemplo, al utilizar los dos enlaces de 25 G del VIC 14825 (mLOM) y 14425 (entresuelo) y 14000 (tarjeta puente) para el nodo de computación X210c, el ancho de banda combinado VIC es 2 x 50-G + 2 x 50-G, O 100 G por estructura/IFM y 200 G totales por servidor con la configuración de IFM dual.

Para obtener más información sobre las familias de productos Cisco UCS, las especificaciones técnicas y la documentación, consulte "Cisco UCS" sitio web para obtener información.

Componentes de conmutación de Cisco

Switches Nexus

FlexPod usa los switches de la serie Cisco Nexus para proporcionar una estructura de switches Ethernet para la comunicación entre Cisco UCS y las controladoras de almacenamiento de NetApp. Todos los modelos de switch Cisco Nexus admitidos actualmente, incluidas las series Cisco Nexus 3000, 5000, 7000 y 9000, son compatibles con la puesta en marcha de FlexPod.

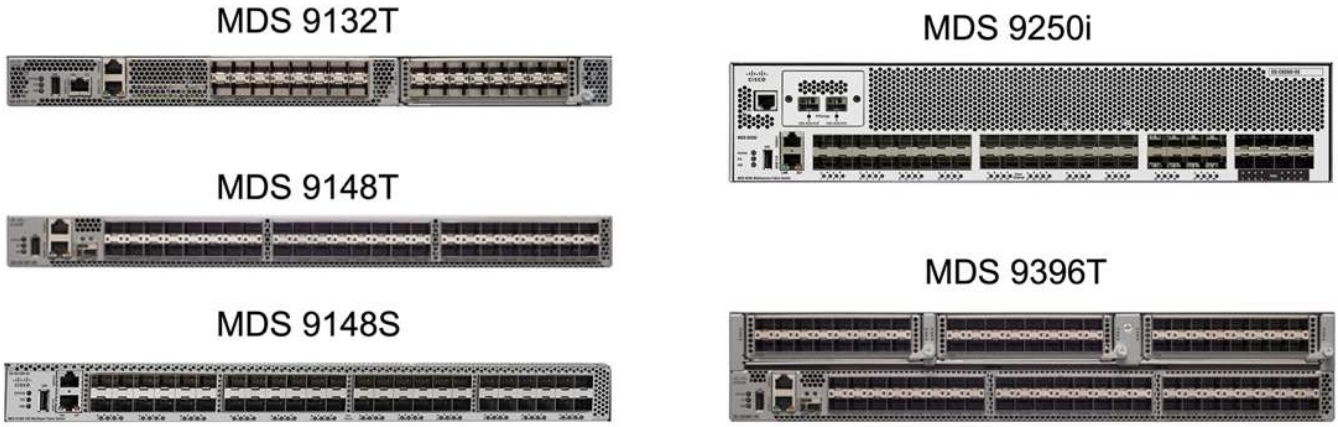
Al seleccionar un modelo de switch para la implementación de FlexPod, hay muchos factores que hay que tener en cuenta, como el rendimiento, la velocidad de puertos, la densidad de puertos y la latencia de conmutación Y protocolos como ACI y VXLAN, para sus objetivos de diseño, así como el tiempo de soporte de los switches.

La validación de muchos CVD de FlexPod recientes utiliza switches Cisco Nexus 9000, como Nexus 9336C-FX2 y Nexus 93180YC-FX3, que proporcionan puertos 40/100G y 10//25G de alto rendimiento, baja latencia y eficiencia energética excepcional en un factor de forma 1U compacto. Se admiten velocidades adicionales mediante puertos de enlace ascendente y cables de desconexión. En la siguiente figura se muestran algunos switches Cisco Nexus 9k y 3k, incluidos los Nexus 9336C-FX2 y el Nexus 3232C utilizados para esta validación.

Consulte "Switches de centro de datos Cisco" Para obtener más información sobre los switches Nexus disponibles y sus especificaciones y documentación.

Switches MDS

Los switches de estructura de las series Cisco MDS 9100/9200/9300 son un componente opcional de la arquitectura FlexPod. Estos switches son de gran fiabilidad, flexibilidad, seguridad y pueden dar visibilidad al flujo de tráfico de la estructura. La siguiente figura muestra algunos ejemplos de switches MDS que se pueden utilizar para crear estructuras FC SAN redundantes para una solución FlexPod con el fin de satisfacer los requisitos empresariales y de las aplicaciones.



Los conmutadores de estructura multicapa Cisco MDS 9132T/9148T/9396T de alto rendimiento 32G son rentables y son altamente fiables, flexibles y escalables. Las funciones y características avanzadas de redes de almacenamiento incluyen facilidad de gestión y son compatibles con toda la cartera de la familia Cisco MDS 9000 para una implementación fiable DE SAN.

Las funcionalidades de análisis y telemetría SAN de vanguardia están integradas en esta plataforma de hardware de nueva generación. Los datos de telemetría extraídos de la inspección de los encabezados de trama se pueden transmitir a una plataforma de visualización de análisis, incluida Cisco Data Center Network Manager. Los switches MDS que admiten 16 G FC, como MDS 9148S, también son compatibles con FlexPod. Además, los switches MDS de múltiples servicios, como MDS 9250i, que admite protocolos FCoE y FCIP

además del protocolo FC, también forman parte de la gama de soluciones FlexPod.

En los switches MDS semimodulares como 9132T y 9396T, se pueden agregar licencias de puerto y módulo de expansión de puerto adicionales para admitir conectividad de dispositivo adicional. En los switches fijos, como 9148T, se pueden agregar licencias de puerto adicionales según sea necesario. Esta flexibilidad, con un sistema de pago por crecimiento, proporciona un componente de gastos operativos que ayuda a reducir los gastos de capital destinados a la implantación y el funcionamiento de la infraestructura SAN basada en switches MDS.

Consulte "Switches Cisco MDS Fabric" Para obtener más información acerca de los switches MDS Fabric disponibles y consulte "IMT de NetApp" y.. "Lista de compatibilidad de hardware y software de Cisco" Si quiere obtener una lista completa de los switches SAN compatibles.

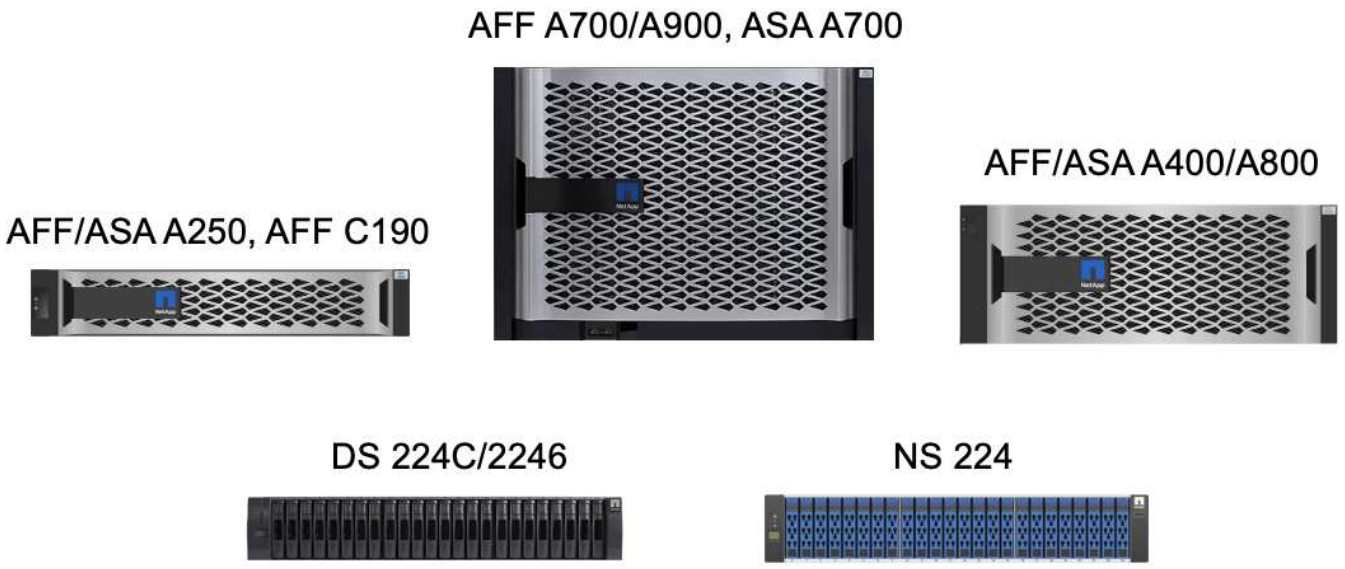
Componentes de NetApp

Para crear una solución AFF SM-BC de FlexPod son necesarias controladoras o ASA redundantes que ejecuten ONTAP Software 9.8 o versiones posteriores. La última versión de ONTAP, actualmente 9.10.1, se recomienda para la puesta en marcha de SM-BC para aprovechar las innovaciones continuas en ONTAP, su rendimiento y calidad, y el mayor número máximo de objetos para soporte SM-BC.

Las controladoras AFF y ASA de NetApp, con un rendimiento e innovaciones líderes del sector, proporcionan protección de datos empresariales y funcionalidades de gestión de datos con gran cantidad de funciones. Los sistemas AFF y ASA admiten tecnologías NVMe integrales, incluidos los SSD conectados a NVMe y la conectividad de host de la interfaz NVMe over Fibre Channel (NVMe/FC). Puede mejorar el rendimiento de su carga de trabajo y reducir la latencia de I/o al adoptar una infraestructura SAN basada en NVMe/FC. Sin embargo, actualmente los almacenes de datos basados en NVMe/FC solo pueden utilizarse para cargas de trabajo no protegidas por SM-BC, ya que en la actualidad la solución SM-BC solo admite los protocolos iSCSI y FC.

Las controladoras de almacenamiento AFF y ASA de NetApp también ofrecen una base para el cloud híbrido que permite a los clientes aprovechar la movilidad de datos fluida que ofrece Data Fabric de NetApp. Con Data Fabric, puede llevar datos fácilmente desde el perímetro donde se generan al núcleo donde se utilizan y al cloud para aprovechar las funcionalidades de computación elástica bajo demanda, IA y APRENDIZAJE AUTOMÁTICO para obtener información muy práctica sobre el negocio.

Como se muestra en la siguiente figura, NetApp ofrece una gran variedad de controladoras de almacenamiento y bandejas de discos para responder a sus requisitos de rendimiento y capacidad. Consulte la siguiente tabla para ver los enlaces a páginas de productos para obtener información sobre las capacidades y especificaciones de las controladoras AFF y ASA de NetApp.

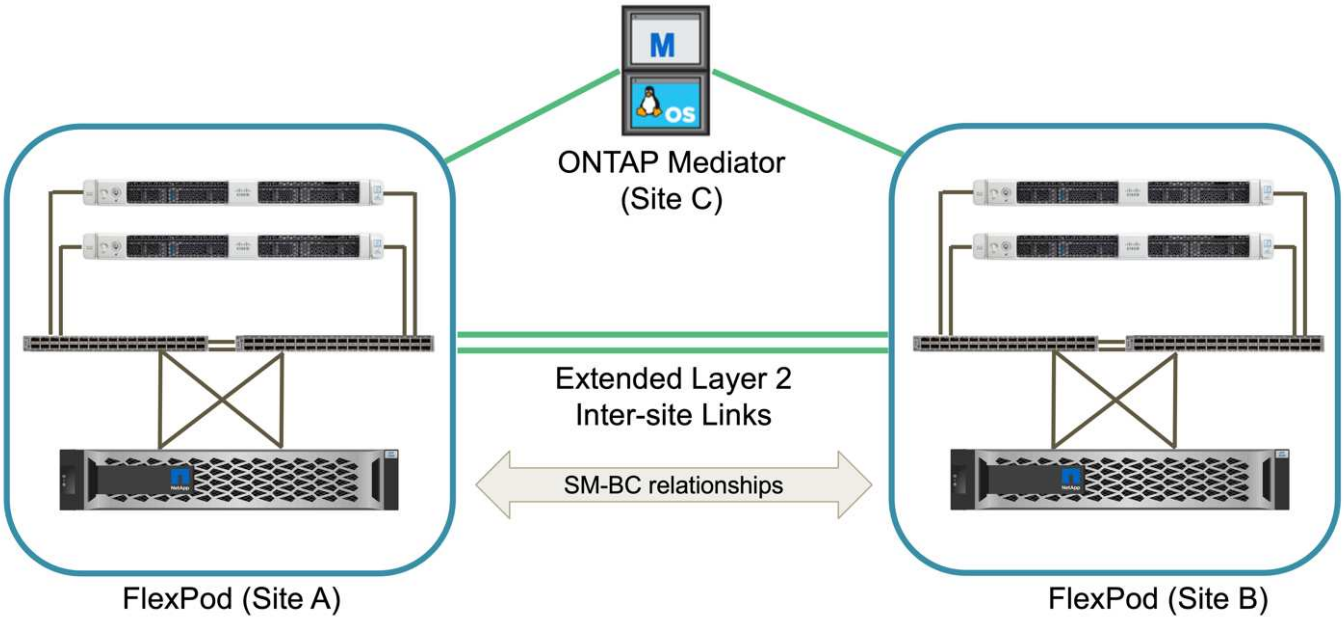


Familia de productos	Especificaciones técnicas
Serie AFF	"Documentación de la serie AFF"
Serie ASA	"Documentación de la serie ASA"

Consulte la "Documentación sobre bandejas de discos y medios de almacenamiento de NetApp" y.. "Hardware Universe de NetApp" para obtener información detallada sobre las bandejas de discos y las bandejas de discos admitidas para cada modelo de controladora de almacenamiento.

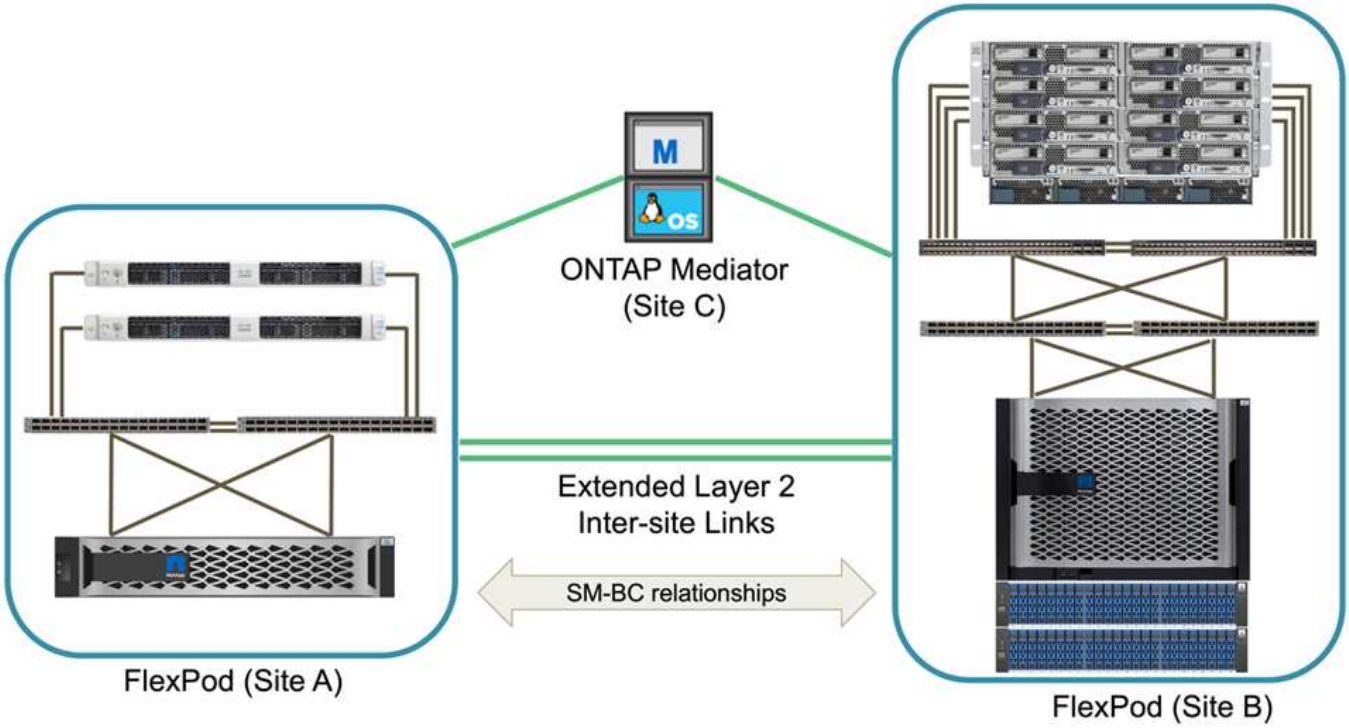
Topologías de soluciones

Las soluciones de FlexPod son flexibles en topología y pueden escalarse vertical u horizontalmente para satisfacer las diferentes necesidades de la solución. Una solución que requiere protección de continuidad del negocio y solo los recursos mínimos de computación y almacenamiento puede usar una topología sencilla de soluciones, como se muestra en la siguiente figura. Esta sencilla topología utiliza los servidores de rack UCS C-Series y las controladoras AFF/ASA con los SSD en la controladora sin bandejas de discos adicionales.



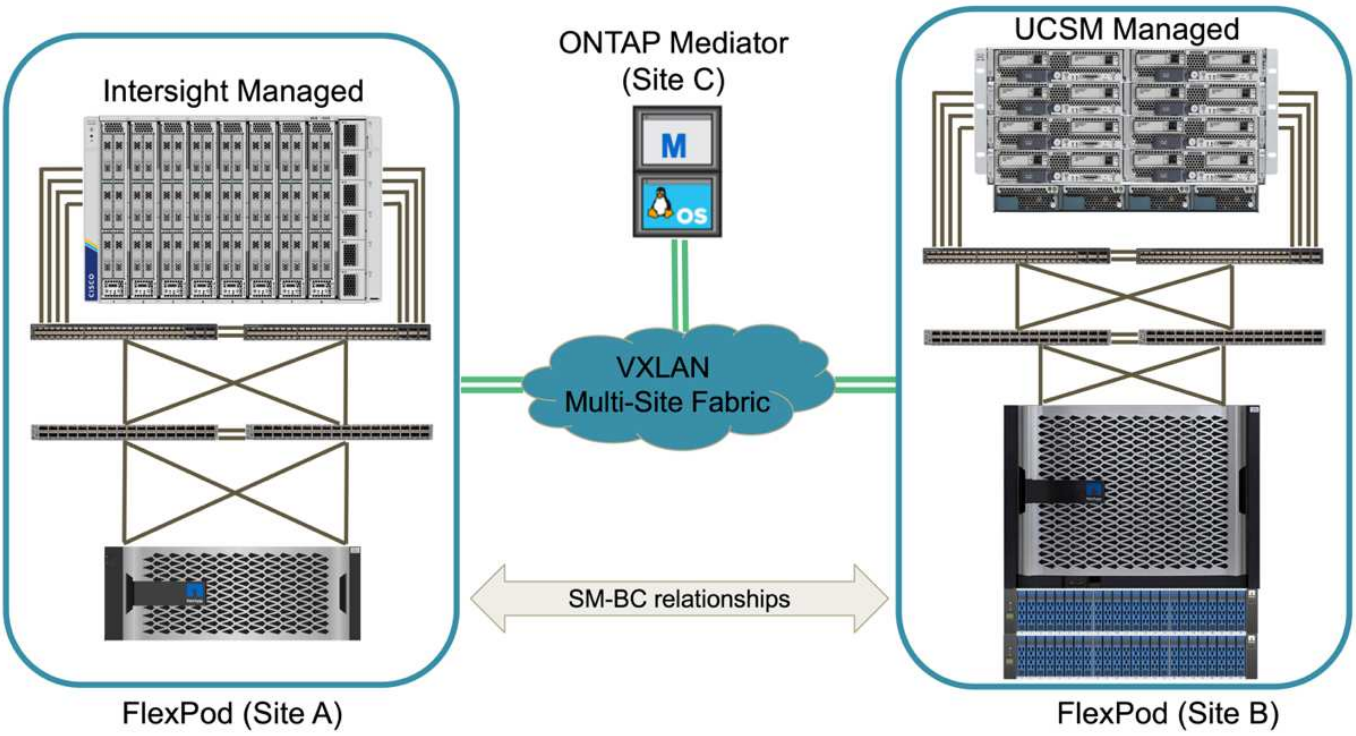
Los componentes redundantes de computación, red y almacenamiento están interconectados con una conectividad redundante entre los componentes. Este diseño de alta disponibilidad proporciona resiliencia de la solución y permite resistir escenarios de un único punto de error. El diseño de varios sitios y las relaciones de replicación de datos síncrona de ONTAP SM-BC proporcionan servicios de datos esenciales para el negocio, a pesar de posibles fallos de almacenamiento en un único sitio.

Una topología de implementación asimétrica que podrían usar las empresas entre un centro de datos y una sucursal en un área metropolitana puede parecerse a la siguiente figura. Para este diseño asimétrico, el centro de datos requiere una FlexPod de mayor rendimiento con más recursos de computación y almacenamiento. Sin embargo, el requisito de la sucursal es menor y puede ser satisfecho por un FlexPod mucho más pequeño.

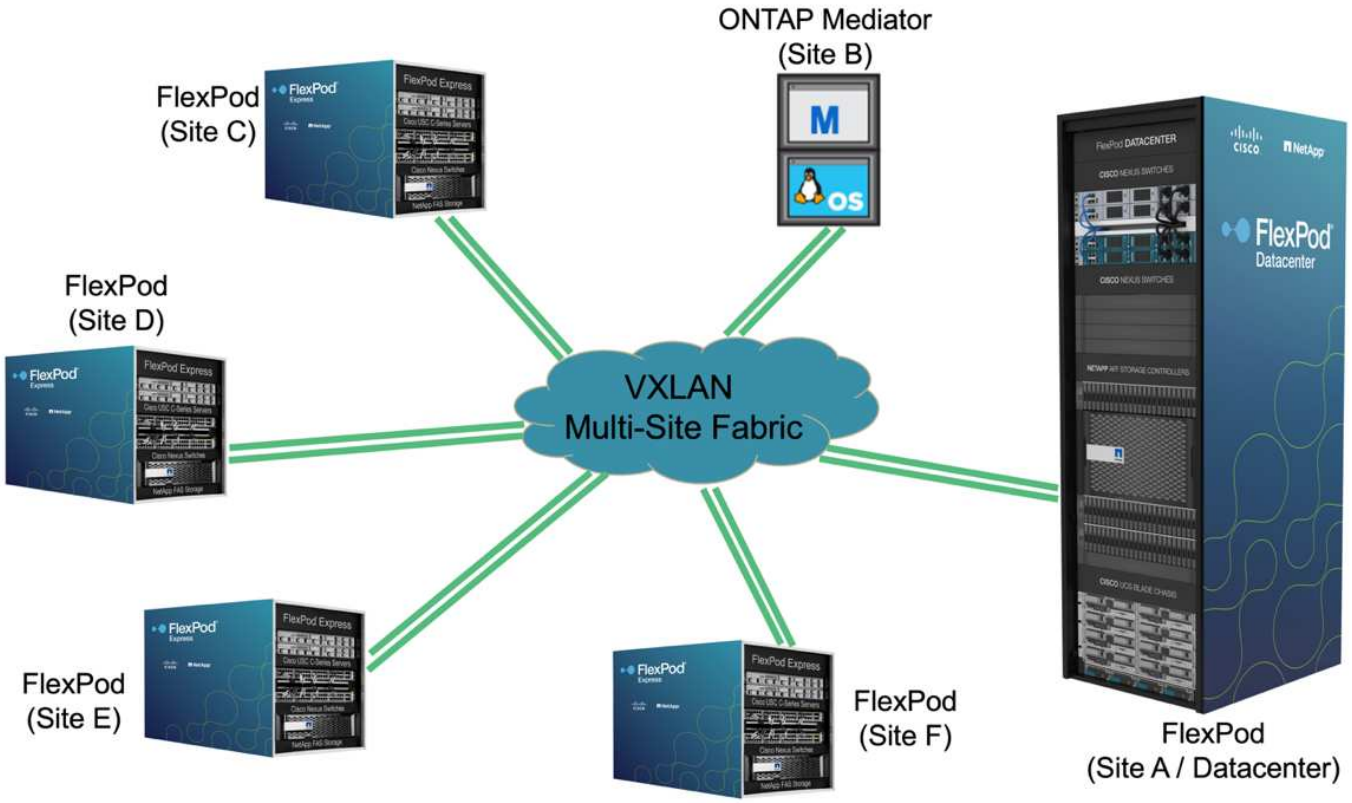


Para las empresas con mayores requisitos de recursos informáticos y de almacenamiento y múltiples sitios, una estructura multisitio basada en VXLAN permite a los múltiples sitios disponer de una estructura de red perfecta para facilitar la movilidad de aplicaciones, de modo que se pueda servir una aplicación desde cualquier sitio.

Puede haber una solución FlexPod existente utilizando los chasis Cisco UCS 5108 y los servidores blade B-Series que deben protegerse con una nueva instancia de FlexPod. La nueva instancia de FlexPod puede utilizar el chasis UCS X9508 más reciente con nodos de computación X210c gestionados por Cisco Intersight, como se muestra en la siguiente figura. En este caso, los sistemas FlexPod de cada site están conectados a una estructura de centro de datos más grande, y los sitios están conectados a través de una red de interconexión para formar una estructura multi-site VXLAN.



Para las empresas que cuentan con un centro de datos y varias sucursales en un área metropolitana que deben protegerse para que proporcione continuidad del negocio La topología de la puesta en marcha de SM-BC de FlexPod mostrada en la siguiente figura puede implementarse para proteger servicios de datos y aplicaciones críticas para alcanzar objetivos de RPO cero y RTO casi cero para todos los sitios de sucursales.



Para este modelo de implementación, cada sucursal establece las relaciones de SM-BC y los grupos de consistencia necesarios con el centro de datos. Debe tener en cuenta los límites de objetos de SM-BC admitidos, de modo que las relaciones generales de los grupos de coherencia y el número de extremos no superen los máximos admitidos en el centro de datos.

"Siguiente: Información general sobre la validación de la solución."

Validación de la solución

Validación de la solución: Información general

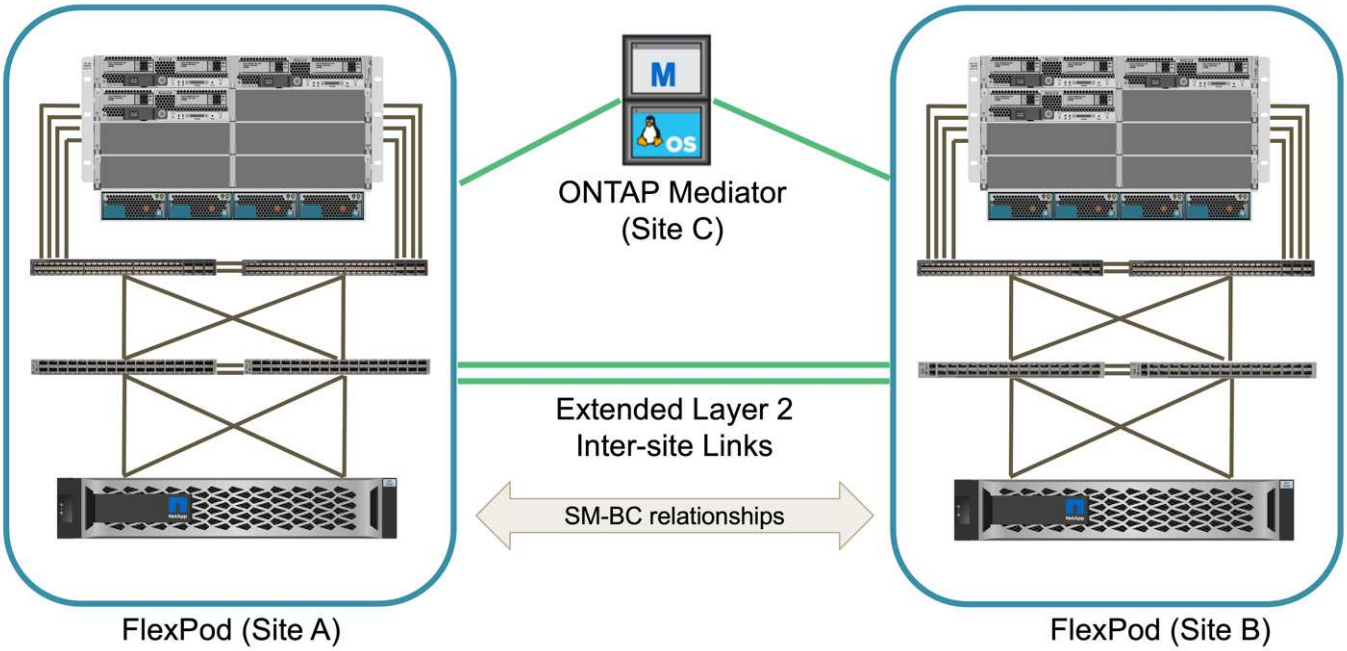
"Anterior: Solución FlexPod SM-BC."

Los detalles de implementación y el diseño de la solución FlexPod SM-BC dependen de los objetivos de solución y configuración de la situación específica de FlexPod. Una vez definidos los requisitos generales de continuidad del negocio, la solución FlexPod SM-BC puede crearse implementando una solución completamente nueva con dos sistemas FlexPod nuevos, añadiendo una FlexPod nueva en otro sitio para emparejarla con una FlexPod existente o emparejando dos sistemas FlexPod existentes.

Dado que las soluciones de FlexPod son de naturaleza flexible en sus configuraciones, es posible utilizar todas las configuraciones y componentes de FlexPod compatibles. El resto de esta sección proporciona información para las validaciones de implementación realizadas para una solución de infraestructura virtual basada en VMware. Excepto en los aspectos relacionados con SM-BC, la implementación sigue los procesos estándar de implementación de FlexPod. Consulte los CVD y NVA de FlexPod disponibles adecuados para sus configuraciones específicas para obtener detalles generales de la implementación de FlexPod.

Topología de validación

Para validar la solución FlexPod SM-BC, se utilizan componentes tecnológicos compatibles de NetApp, Cisco y VMware. La solución incluye pares de alta disponibilidad AFF A250 de NetApp que ejecutan ONTAP 9.10.1, switches Cisco Nexus 9336C-FX2 duales en el centro A y switches Cisco Nexus 3232C duales en el centro B, Cisco UCS 6454 FIS en ambos sitios, Y tres servidores Cisco UCS B200 M5 en cada sitio que ejecuta VMware vSphere 7.0u2 y gestionados por UCS Manager y VMware vCenter Server. La siguiente figura muestra la topología de validación de soluciones a nivel de componentes con dos sistemas FlexPod que se ejecutan en el centro A y el sitio B conectados mediante enlaces entre sitios de capa 2 extendidos y Mediador ONTAP que se ejecuta en el centro C.



Hardware y software

En la siguiente tabla se enumeran el hardware y el software empleados para la validación de la solución. Cabe destacar que Cisco, NetApp y VMware cuentan con matrices de interoperabilidad que se utilizan para determinar la compatibilidad con cualquier implementación específica de FlexPod:

- "http://support.netapp.com/matrix/"
- "Herramienta de interoperabilidad de hardware y software Cisco UCS"
- "http://www.vmware.com/resources/compatibility/search.php"

Categoría	Componente	Versión de software	Cantidad
Informática	Interconexión de estructura Cisco UCS 6454	4.2(1f)	4 (2 por sitio)
	Servidores Cisco UCS B200 M5	4.2(1f)	6 (3 por sitio)
	CISCO UCS IOM 2204XP	4.2(1f)	4 (2 por sitio)
	CISCO VIC 1440 (PID: UCSB-MLOM-40G-04)	5.2(1a)	2 (1 por sitio)

Categoría	Componente	Versión de software	Cantidad
	CISCO VIC 1340 (PID: UCSB-MLOM-40G-03)	4.5(1a)	4 (2 por sitio)
Red	Cisco Nexus 9336C-FX2	9.3(6)	2 (centro A)
	Cisco Nexus 3232C	9.3(6)	2 (sitio B)
Reducida	AFF A250 de NetApp	9.10.1	4 (2 por sitio)
	System Manager de NetApp	9.10.1	2 (1 por sitio)
	Active IQ Unified Manager de NetApp	9.10	1
	Herramientas de ONTAP de NetApp para VMware vSphere	9.10	1
	Complemento SnapCenter de NetApp para VMware vSphere	4.6	1
	Mediador ONTAP de NetApp	1.3	1
	NAbox	3.0.2	1
	Cosecha de NetApp	21.11.1-1	1
Virtualización	VMware ESXi	7.0U2	6 (3 por sitio)
	Controlador Ethernet nenic VMware ESXi	1.0.35.0	6 (3 por sitio)
	VMware vCenter	7.0U2	1
	Plugin NFS de NetApp para VAAI de VMware	2.0	6 (3 por sitio)
Pruebas	Microsoft Windows	2022	1
	Microsoft SQL Server	2019	1
	Microsoft SQL Server Management Studio	18.10	1
	HammerDB	4.3	1
	Microsoft Windows	10	6 (3 por sitio)
	Iometer	1.1.0	6 (3 por sitio)

"Siguiente: Validación de soluciones - Computación."

Validación de soluciones: Computación

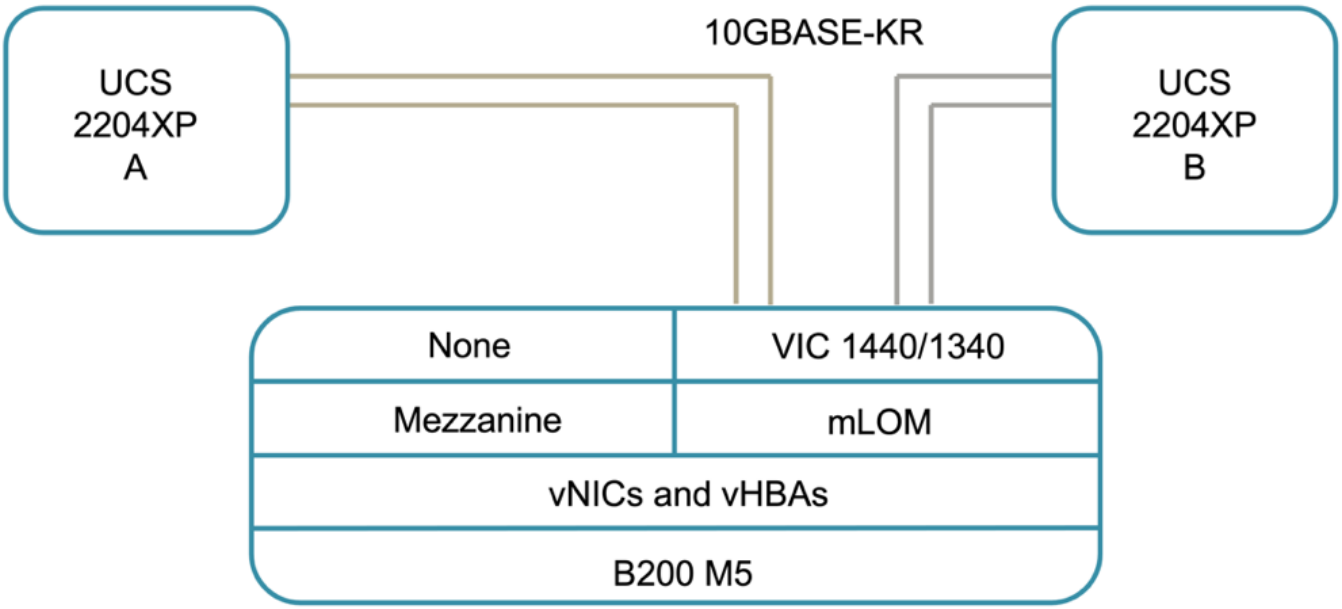
"Preivous: Validación de la solución - Descripción general."

La configuración informática de la solución FlexPod SM-BC sigue las prácticas

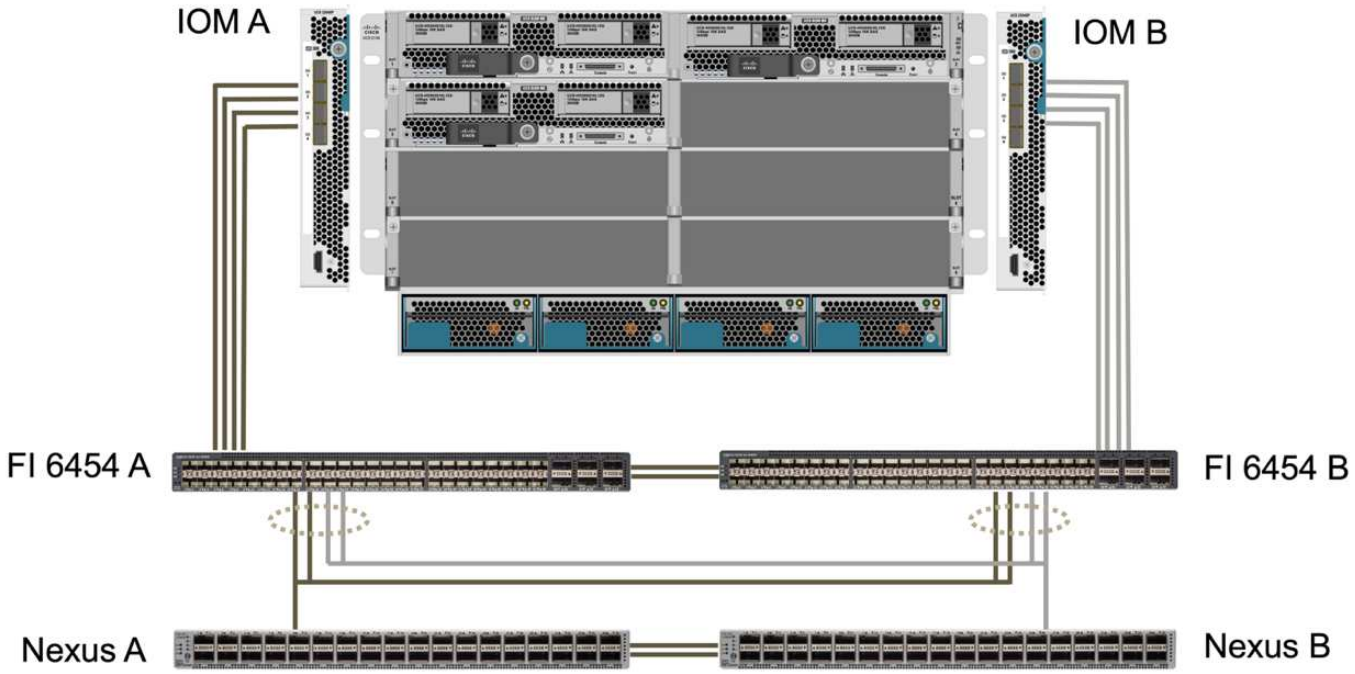
recomendadas habituales de la solución FlexPod. En las siguientes secciones se destacan algunas de las configuraciones y conectividad utilizadas para la validación. También se destacan algunas de las consideraciones relacionadas con SM-BC para proporcionar referencias y orientación de implementación.

Conectividad

La conectividad entre los servidores blade UCS B200 y los IOM es proporcionada por la tarjeta UCS VIC a través de las conexiones de plano posterior del chasis UCS 5108. Los extensores de estructura UCS 2204XP utilizados para la validación tienen dieciséis puertos 10 G cada uno para conectarse con los ocho servidores blade de media anchura, por ejemplo, dos para cada servidor. Para aumentar el ancho de banda de la conectividad del servidor, se puede agregar un VIC basado en mezzanine para conectar el servidor a la IOM de UCS 2408 alternativa, que proporciona cuatro conexiones de 10 G a cada servidor.



La conectividad entre el chasis UCS 5108 y UCS 6454 FIS utilizados para la validación está proporcionada por el IOM 2204XP que utiliza cuatro conexiones 10G. Los puertos FI 1 a 4 se configuran como puertos de servidor para estas conexiones. Los puertos FI 25 a 28 se configuran como puertos de enlace ascendente de red al conmutador Nexus A y B del sitio local. La siguiente figura y tabla proporcionan el diagrama de conectividad y los detalles de conexión de puertos para la conexión de la controladora FIS UCS 6454 con el fin de conectarse al chasis UCS 5108 y a los switches Nexus.



Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
UCS 6454 FI A	1	IOM A	1
	2		2
	3		3
	4		4
	25	Nexus a	1/13/1
	26		1/13/2
	27	Nexus B	1/13/3
	28		1/13/4
	L1	UCS 6454 FI B	L1
	L2		L2
UCS 6454 FI B	1	IOM B	1
	2		2
	3		3
	4		4
	25	Nexus a	1/13/3
	26		1/13/4
	27	Nexus B	1/13/1
	28		1/13/2
	L1	UCS 6454 FI A	L1

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
	L2		L2

Las conexiones anteriores son similares para los dos sitios A y B, a pesar del sitio A que utiliza switches Nexus 9336C-FX2y el sitio B mediante switches Nexus 3232C. Los cables de salida DE 40 G a 4 10 G se utilizan para las conexiones Nexus a FI. LAS conexiones FI a Nexus utilizan canales de puertos y los canales de puertos virtuales se configuran en los switches Nexus para agregar las conexiones a cada RED.

Cuando se utilice una combinación diferente de componentes del switch IOM, FI y Nexus, asegúrese de utilizar los cables y la velocidad de puerto adecuados para la combinación de entorno.

Se puede lograr un ancho de banda adicional usando componentes que admitan conexiones de mayor velocidad o más conexiones. Se puede lograr redundancia adicional agregando conexiones adicionales con componentes que los admitan.

Perfiles de servicio

Un chasis de servidor blade con interconexiones de estructura gestionadas por UCS Manager (UCSM) o Cisco Intersight pueden abstraer los servidores utilizando los perfiles de servicio disponibles en UCSM y los perfiles de servidor de Intersight. Esta validación emplea perfiles UCSM y de servicio para simplificar la gestión de servidores. Con los perfiles de servicio, la sustitución o actualización de un servidor se puede realizar simplemente asociando el perfil de servicio original con el nuevo hardware.

Los perfiles de servicio creados admiten lo siguiente para los hosts VMware ESXi:

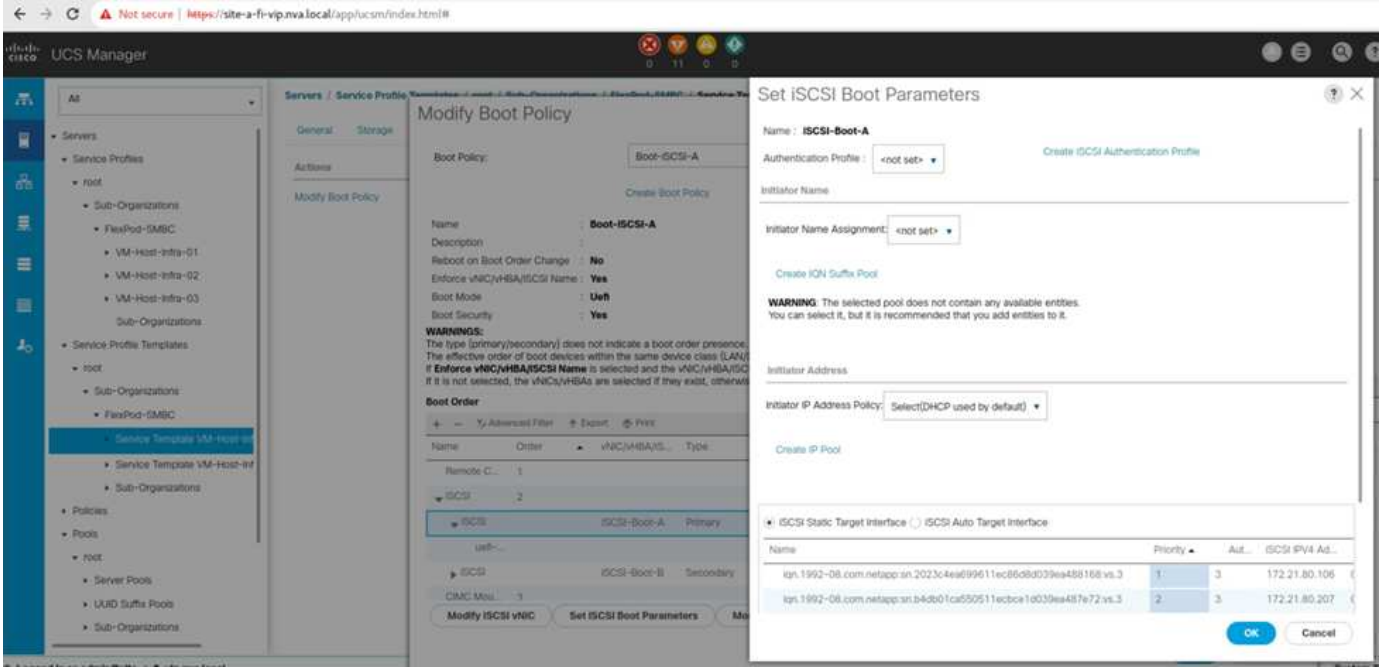
- Arranque SAN desde el almacenamiento A250 de AFF en cualquiera de las ubicaciones mediante el protocolo iSCSI.
- Se crean seis vNIC para los servidores en los que:
  - Dos NIC redundantes (vSwitch0-A y vSwitch0-B) transportan tráfico de gestión en banda. Opcionalmente, estos vNIC también pueden ser utilizados por datos del protocolo NFS que no están protegidos por SM-BC.
  - El switch distribuido de vSphere utiliza dos NIC redundantes (VDS-A y VDS-B) para transportar el tráfico de VMware vMotion y otras aplicaciones.
  - ISCSI-A VNIC utilizado por iSCSI-a vSwitch para proporcionar acceso a la ruta iSCSI-A.
  - VNIC iSCSI-B utilizado por el vSwitch de iSCSI-B para proporcionar acceso a la ruta iSCSI-B.

Arranque SAN

Para la configuración de arranque SAN iSCSI, los parámetros de arranque iSCSI se establecen para permitir el arranque iSCSI desde ambas estructuras iSCSI. Para acomodar la situación de conmutación por error SM-BC en la que un LUN de arranque SAN iSCSI se sirve desde el clúster secundario cuando el clúster primario no está disponible, la configuración de destino estático iSCSI debe incluir destinos tanto del sitio A como del sitio B. Además, para maximizar la disponibilidad del LUN de arranque, configure los parámetros de arranque iSCSI para arrancar desde todas las controladoras de almacenamiento.

El destino estático iSCSI se puede configurar en la política de inicio de las plantillas de perfil de servicio bajo el cuadro de diálogo definir parámetros de arranque iSCSI, como se muestra en la siguiente figura. La

configuración recomendada del parámetro de arranque iSCSI se muestra en la tabla siguiente, que implementa la estrategia de arranque descrita anteriormente para lograr una alta disponibilidad.



Estructura iSCSI	Prioridad	Destino iSCSI	LIF iSCSI
ISCSI a	1	Site un destino iSCSI	Site A Controller 1 iSCSI: LIF
	2	Destino iSCSI del sitio B.	Controladora 2 del centro B iSCSI a LIF
ISCSI B	1	Destino iSCSI del sitio B.	LIF iSCSI B de la controladora del centro B
	2	Site un destino iSCSI	Controladora a del sitio 2 LIF iSCSI B

"Siguiente: Validación de soluciones - Red."

Validación de la solución - Red

"Anterior: Validación de la solución - Computación."

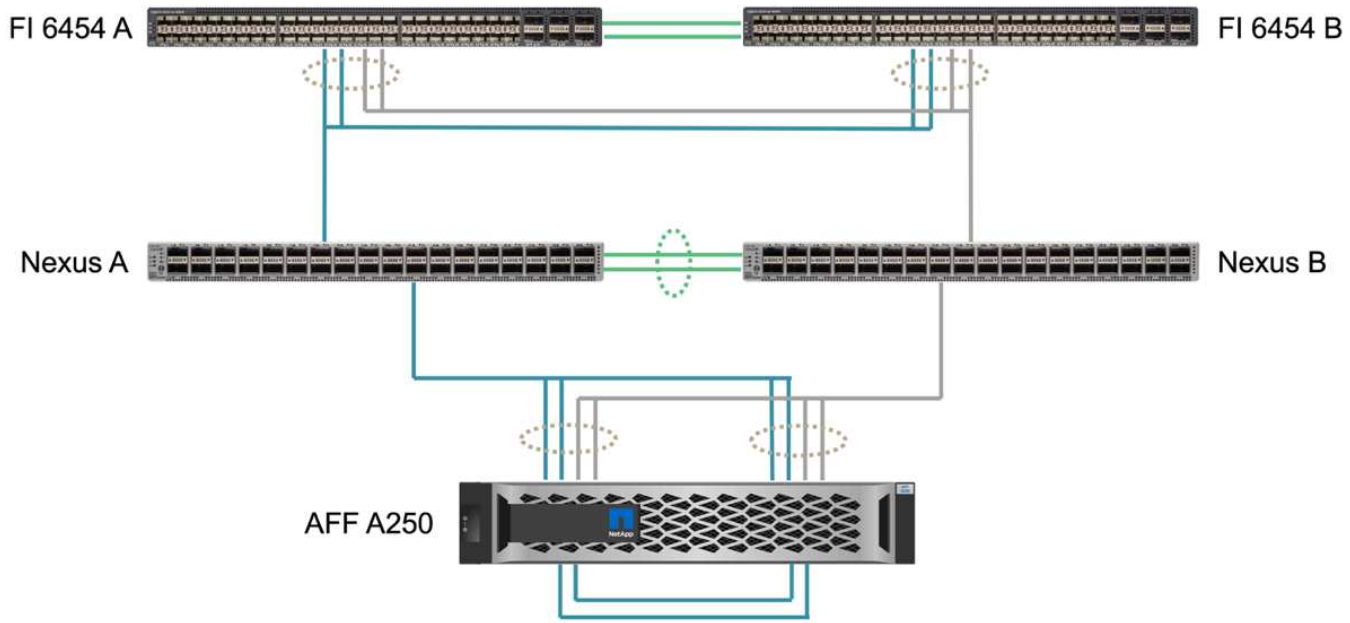
La configuración de red de la solución FlexPod SM-BC sigue las prácticas recomendadas habituales de las soluciones FlexPod en cada site. Para la conectividad entre sitios, la configuración de validación de soluciones conecta los switches Nexus de FlexPod en los dos sitios juntos para proporcionar conectividad entre sitios que amplía las VLAN entre los dos sitios. En las siguientes secciones se destacan algunas de las configuraciones y conectividad utilizadas para la validación.

Conectividad

Los switches FlexPod Nexus de cada sitio proporcionan la conectividad local entre la computación UCS y el almacenamiento ONTAP en una configuración de alta disponibilidad. Los componentes redundantes y la

conectividad redundante proporcionan flexibilidad frente a situaciones de un único punto de error.

El siguiente diagrama muestra la conectividad local del switch Nexus en cada sitio. Además de lo que se muestra en el diagrama, también existen conexiones de red de consola y gestión para cada componente que no se muestra. Se utilizan los cables de arranque de 40 a 4 10G para conectar los switches Nexus a las controladoras de almacenamiento UCS FIS y ONTAP AFF A250. Como alternativa se pueden utilizar cables de arranque DE 100 G a 4 x 25 G para aumentar la velocidad de comunicación entre los switches Nexus y las controladoras de almacenamiento A250 de AFF. Para mayor simplicidad, las dos controladoras AFF A250 se muestran de forma lógica como una cara a cara para la ilustración de cableado. Las dos conexiones entre las dos controladoras de almacenamiento permiten que el almacenamiento forme un clúster sin switches.

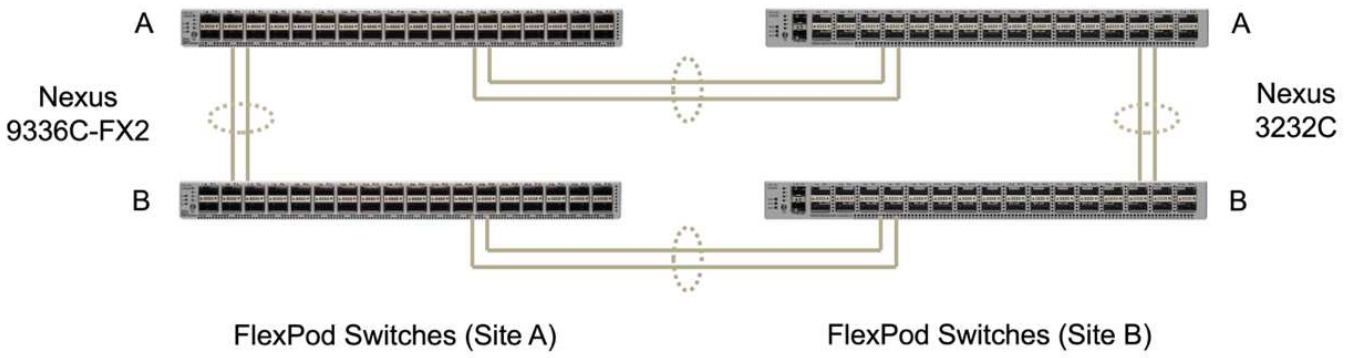


La siguiente tabla muestra la conectividad entre los switches Nexus y las controladoras de almacenamiento A250 de AFF en cada centro.

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Nexus a	1/10/1	AFF A250 A.	e1a
	1/10/2		e1b
	1/10/3	AFF A250 B.	e1a
	1/10/4		e1b
Nexus B	1/10/1	AFF A250 A.	e1c
	1/10/2		e1d
	1/10/3	AFF A250 B.	e1c
	1/10/4		e1d

La conectividad entre los switches FlexPod del sitio A y el sitio B se muestra en la siguiente figura con detalles de cableado que se enumeran en la tabla adjunta. Las conexiones entre los dos switches de cada sitio son para los enlaces del mismo nivel VPC. Por otro lado, las conexiones entre los switches de los sitios proporcionan los enlaces entre sitios. Los enlaces extienden las VLAN a través de varios sitios para la comunicación entre clústeres, la replicación de datos SM-BC, la gestión en banda y el acceso a los datos para

los recursos de sitios remotos.



Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Planta a conmutador	33	Interruptor A de la ubicación B.	31
	34		32
	25	Interruptor B de la planta A	25
	26		26
Interruptor B de la planta A	33	Interruptor B de la ubicación B.	31
	34		32
	25	Planta a conmutador	25
	26		26
Interruptor A de la ubicación B.	31	Planta a conmutador	33
	32		34
	25	Interruptor B de la ubicación B.	25
	26		26
Interruptor B de la ubicación B.	31	Interruptor B de la planta A	33
	32		34
	25	Interruptor A de la ubicación B.	25
	26		26

La tabla anterior enumera la conectividad desde las perspectivas de cada switch FlexPod. Como resultado, la tabla contiene información duplicada para facilitar la legibilidad.

Canal de puertos y canal de puertos virtuales

El canal de puerto permite la agregación de enlaces mediante el protocolo de control de agregación de enlaces (LACP) para la agregación de ancho de banda y la resiliencia de fallos de enlace. El canal de puerto virtual (VPC) permite que las conexiones de canal de puertos entre dos switches Nexus se muestren de forma lógica como una. De este modo, se mejora aún más la resiliencia ante fallos en situaciones como un fallo de enlace único o un fallo de switch único.

El tráfico de servidores UCS al almacenamiento realiza las rutas de IOM A A FI Y de IOM B A FI B antes de llegar a los switches Nexus. Dado que las conexiones FI a los switches Nexus utilizan el canal de puertos en LA parte FI y el canal de puertos virtuales en el lado del switch Nexus, el servidor UCS puede utilizar de manera eficaz rutas a través de ambos switches Nexus y sobrevivir a situaciones de un único punto de error. Entre los dos sitios, los switches Nexus están interconectados como se muestra en la figura anterior. Hay dos enlaces cada uno para conectar los pares de switches entre los sitios y también utilizan una configuración de puerto-canal.

La conectividad entre clústeres y el protocolo de almacenamiento de datos iSCSI/NFS, de gestión en banda, es proporcionada por la interconexión de las controladoras de almacenamiento de cada sitio a los switches Nexus locales en una configuración redundante. Cada controladora de almacenamiento está conectado a dos switches Nexus. Las cuatro conexiones se configuran como parte de un grupo de interfaces en el almacenamiento para proporcionar una mayor resiliencia. En lo que respecta al switch Nexus, esos puertos también forman parte de un VPC entre switches.

En la siguiente tabla se enumeran el ID de canal de puerto y su uso en cada sitio.

Identificador del canal del puerto	Uso
10	Enlace del mismo nivel de Nexus local
15	Interconexión de estructura a enlaces
16	Enlaces B de interconexión de estructura
27	Enlaces de la controladora de almacenamiento A
28	Enlaces de la controladora B de almacenamiento
100	Conmutador inter-site A links
200	Vínculos B del interruptor entre sitios

VLAN

En la siguiente tabla, se enumeran las VLAN configuradas para configurar el entorno de validación de soluciones FlexPod SM-BC junto con su uso.

Nombre	ID DE VLAN	Uso
VLAN nativa	2	VLAN 2 se usa como VLAN nativa en lugar de la VLAN predeterminada (1)
OOB-MGMT-VLAN	3333	VLAN de gestión fuera de banda para dispositivos
IB-MGMT-VLAN	3334	VLAN de gestión en banda para hosts ESXi, gestión de máquinas virtuales, etc.

Nombre	ID DE VLAN	Uso
NFS-VLAN	3335	VLAN NFS opcional para tráfico NFS
ISCSI-A-VLAN	3336	VLAN de estructura iSCSI-a para tráfico de iSCSI
ISCSI-B-VLAN	3337	VLAN de estructura iSCSI-B para tráfico de iSCSI
VMotion: VLAN	3338	VLAN de tráfico de VMware vMotion
VM-Traffic-VLAN	3339	VLAN de tráfico de máquina virtual de VMware
Interconexión de clústeres-VLAN	3340	VLAN de interconexión de clústeres para comunicaciones de paridad de clústeres de ONTAP

Si bien SM-BC no es compatible con los protocolos NFS o CIFS para la continuidad del negocio, puede seguir utilizándolos para cargas de trabajo que no tengan por qué protegerse para la continuidad del negocio. No se crearon almacenes de datos NFS para esta validación.

"Siguiente: Validación de la solución - almacenamiento."

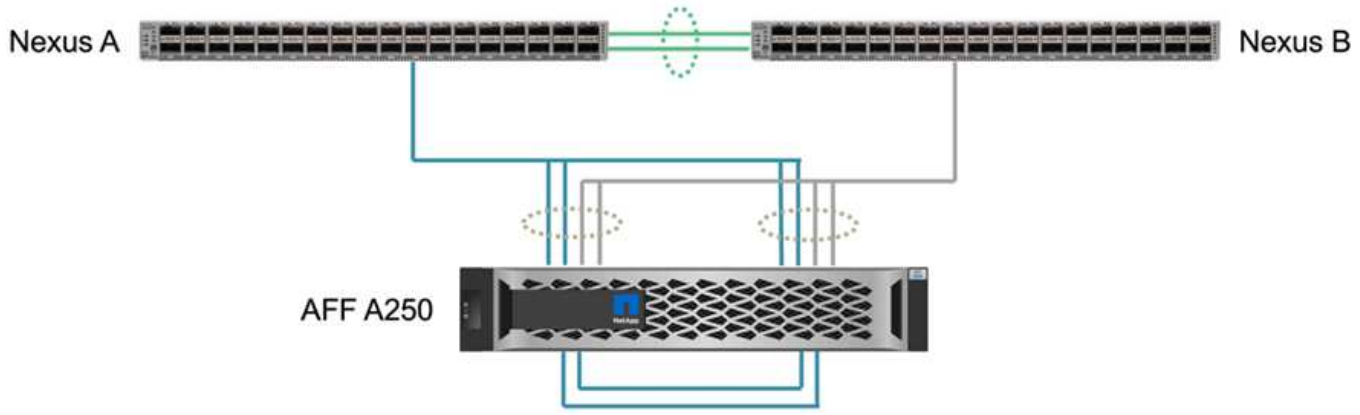
Validación de la solución - almacenamiento

"Anterior: Validación de la solución - Red."

La configuración del almacenamiento de la solución FlexPod SM-BC sigue las prácticas recomendadas habituales de las soluciones FlexPod en cada site. Para los clústeres interpares y la replicación de datos de SM-BC, utilizan los enlaces entre sitios establecidos entre los switches FlexPod en ambos sitios. En las siguientes secciones se destacan algunas de las configuraciones y conectividad utilizadas para la validación.

Conectividad

Los switches Nexus del centro local proporcionan la conectividad del almacenamiento a los FIS y los servidores blade locales UCS. A través de la conectividad del switch Nexus entre sitios, los servidores blade UCS remotos también pueden acceder al almacenamiento. La siguiente figura y tabla muestran el diagrama de conectividad de almacenamiento y una lista de conexiones de las controladoras de almacenamiento en cada sitio.

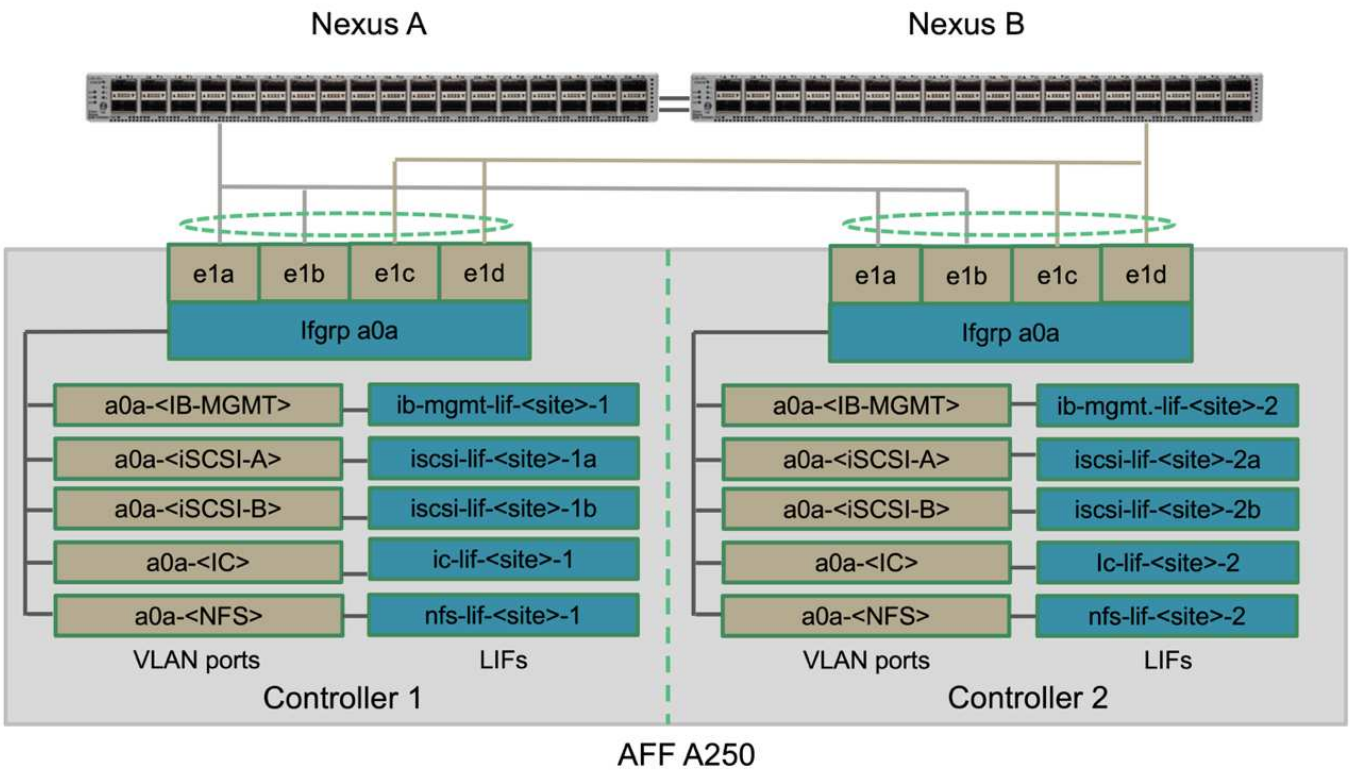


Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
AFF A250 A.	e0c	AFF A250 B.	e0c
	e0d		e0d
	e1a	Nexus a	1/10/1
	e1b		1/10/2
	e1c	Nexus B	1/10/1
	e1d		1/10/2
AFF A250 B.	e0c	AFF A250 A.	e0c
	e0d		e0d
	e1a	Nexus a	1/10/3
	e1b		1/10/4
	e1c	Nexus B	1/10/3
	e1d		1/10/4

Conexiones e interfaces

Para obtener esta validación, se conectan dos puertos físicos por controladora de almacenamiento a cada switch Nexus para añadir ancho de banda y redundancia. Estas cuatro conexiones participan en una configuración de grupo de interfaz en el almacenamiento. Los puertos correspondientes de los switches Nexus participan en un VPC para la agregación y la resiliencia de los enlaces.

Los protocolos de almacenamiento de datos de gestión en banda, entre clústeres y NFS/iSCSI utilizan VLAN. Los puertos VLAN se crean en el grupo de interfaces para segregar los diferentes tipos de tráfico. Las interfaces lógicas (LIF) para las funciones respectivas se crean en la parte superior de los puertos VLAN correspondientes. En la siguiente figura, se muestra la relación entre las conexiones físicas, los grupos de interfaces, los puertos VLAN y las interfaces lógicas.

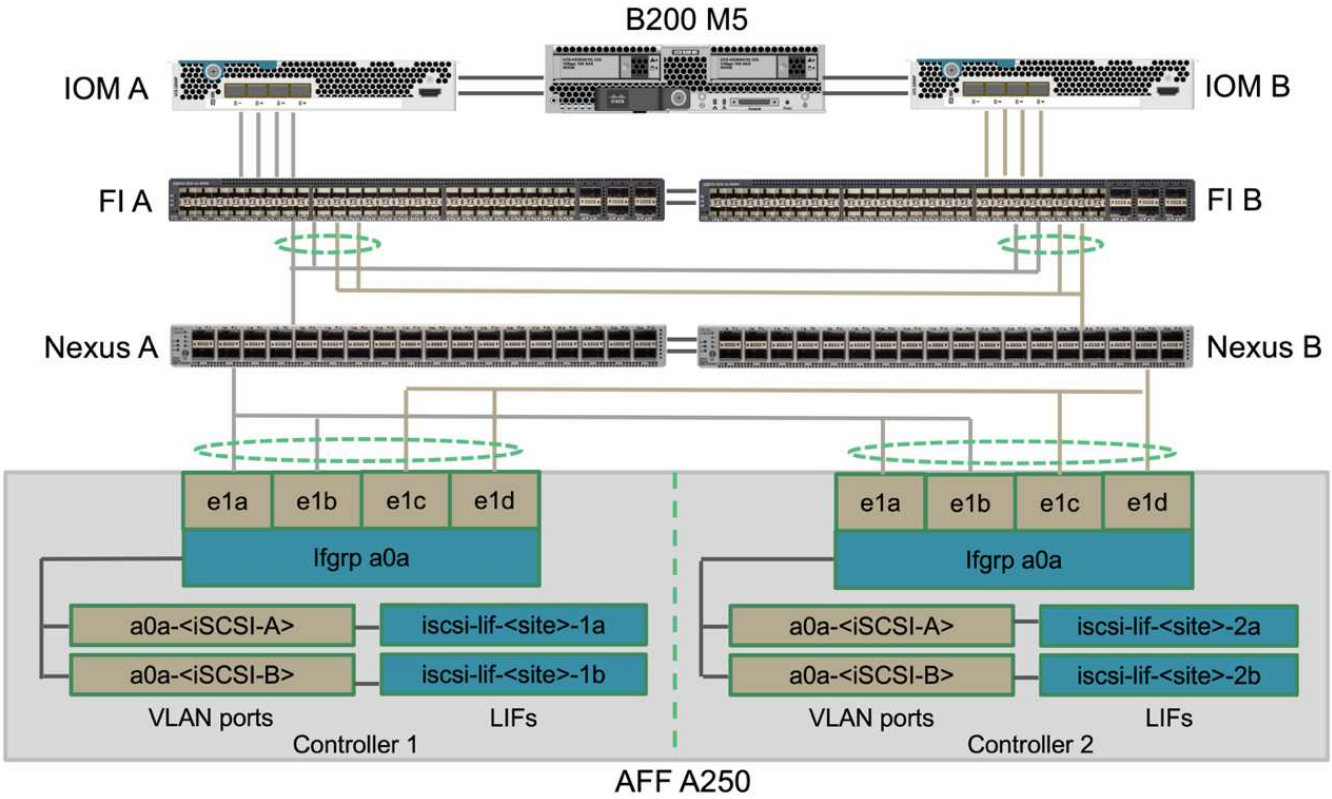


Arranque SAN

NetApp recomienda implementar el arranque SAN para los servidores Cisco UCS en la solución FlexPod. La implementación de arranque SAN permite proteger de forma segura el sistema operativo dentro del sistema de almacenamiento de NetApp, lo que ofrece un mejor rendimiento y flexibilidad. Para esta solución, se validó el arranque SAN de iSCSI.

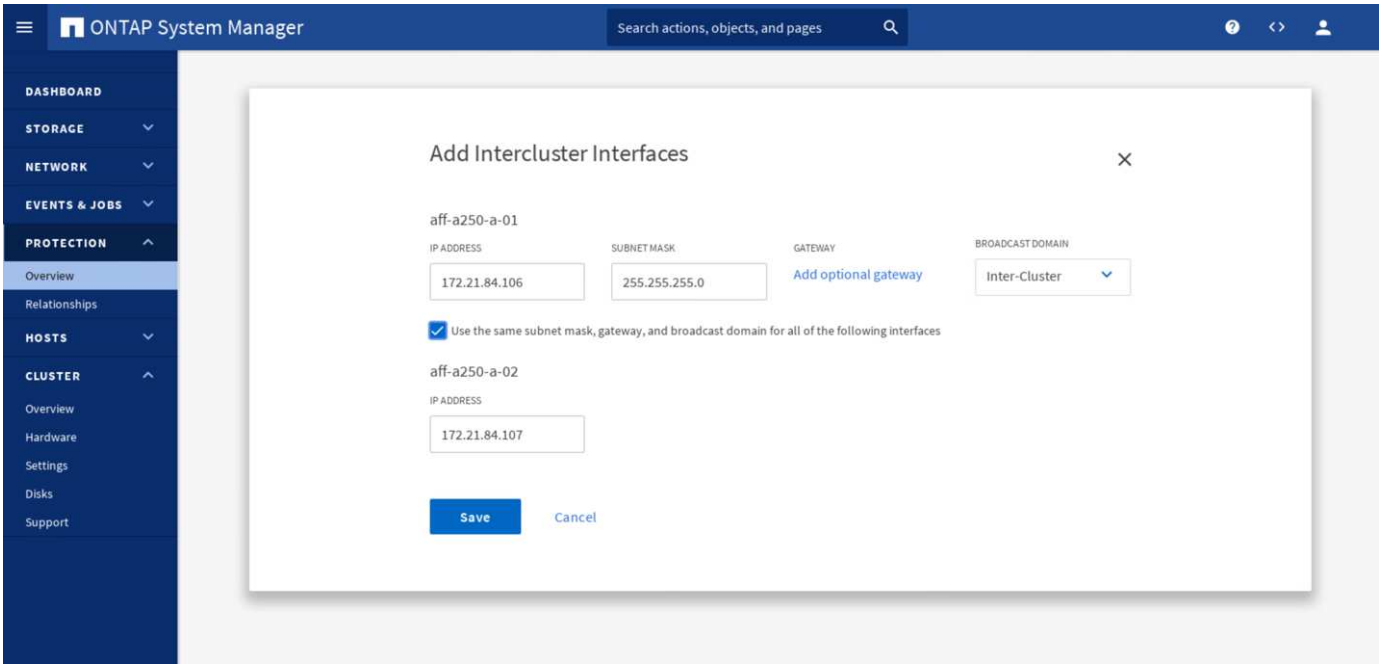
La figura siguiente muestra la conectividad para arranque SAN iSCSI de Cisco UCS Server desde almacenamiento NetApp. En el arranque SAN iSCSI, a cada servidor Cisco UCS se le asignan dos NIC iSCSI (una para cada estructura SAN) que proporcionan conectividad redundante desde el servidor hasta el almacenamiento. Los puertos de almacenamiento Ethernet 10/25-G conectados a los switches Nexus (en este ejemplo, e1a, e1b, e1c y e1d) se agrupan para formar un grupo de interfaces (ifgrp) (en este ejemplo, a0a). Los puertos VLAN iSCSI se crean en ifgrp y los LIF iSCSI se crean en los puertos VLAN iSCSI.

Cada LUN de arranque iSCSI se asigna al servidor que arranca a través de las LIF iSCSI asociando la LUN de arranque con los nombres completos de iSCSI (IQN) del servidor en su igroup de arranque. el igroup de arranque del servidor contiene dos IQN, uno para cada estructura VNIC / SAN. Esta función solo permite que el servidor autorizado tenga acceso a la LUN de arranque creada específicamente para ese servidor.



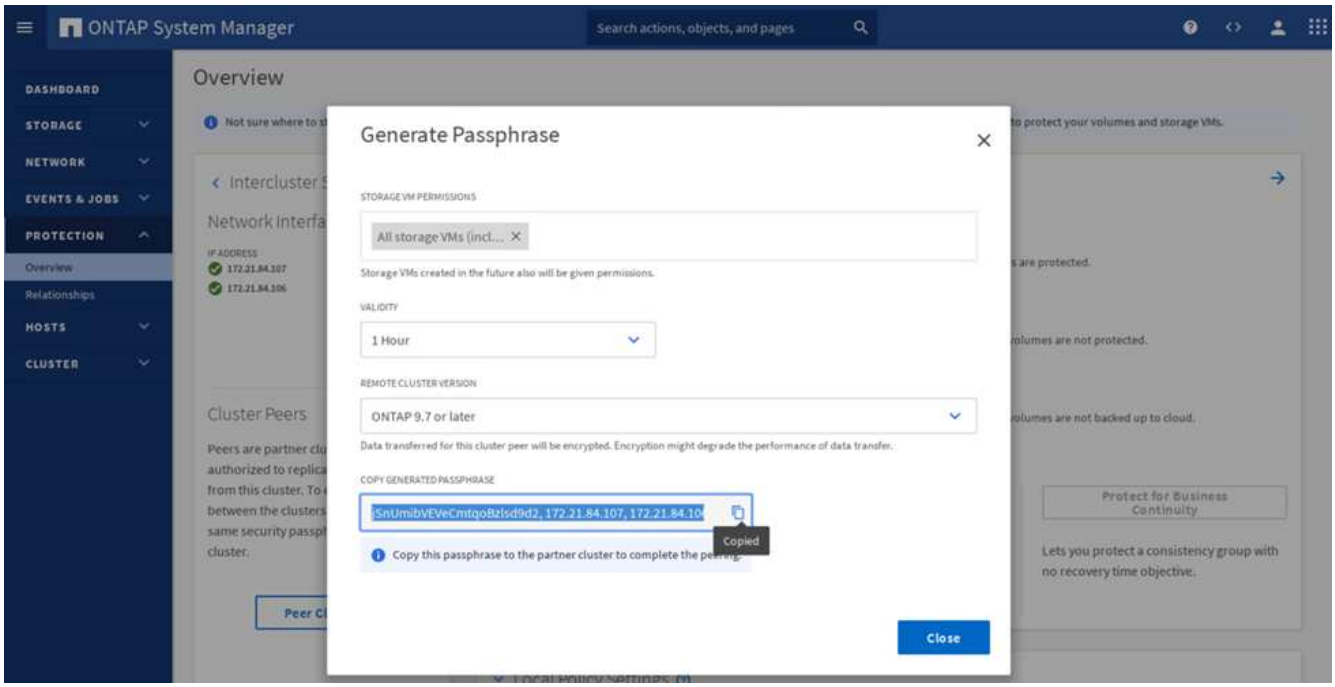
Conexión de clústeres entre iguales

Los clústeres pares de ONTAP se comunican a través de las LIF entre clústeres. Mediante el uso de System Manager de ONTAP para los dos clústeres, puede crear las LIF de interconexión de clústeres necesarias en el panel Protection > Overview.

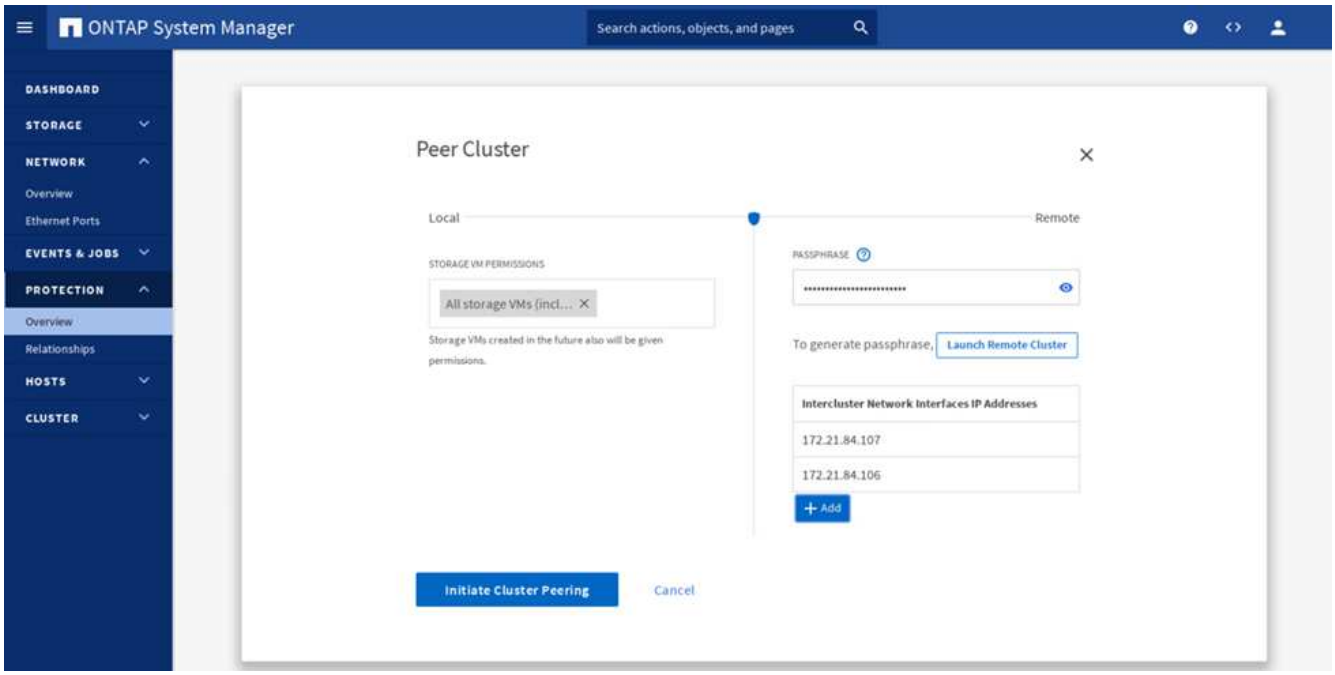


Para conectar los dos clústeres en relación de paridad, complete los siguientes pasos:

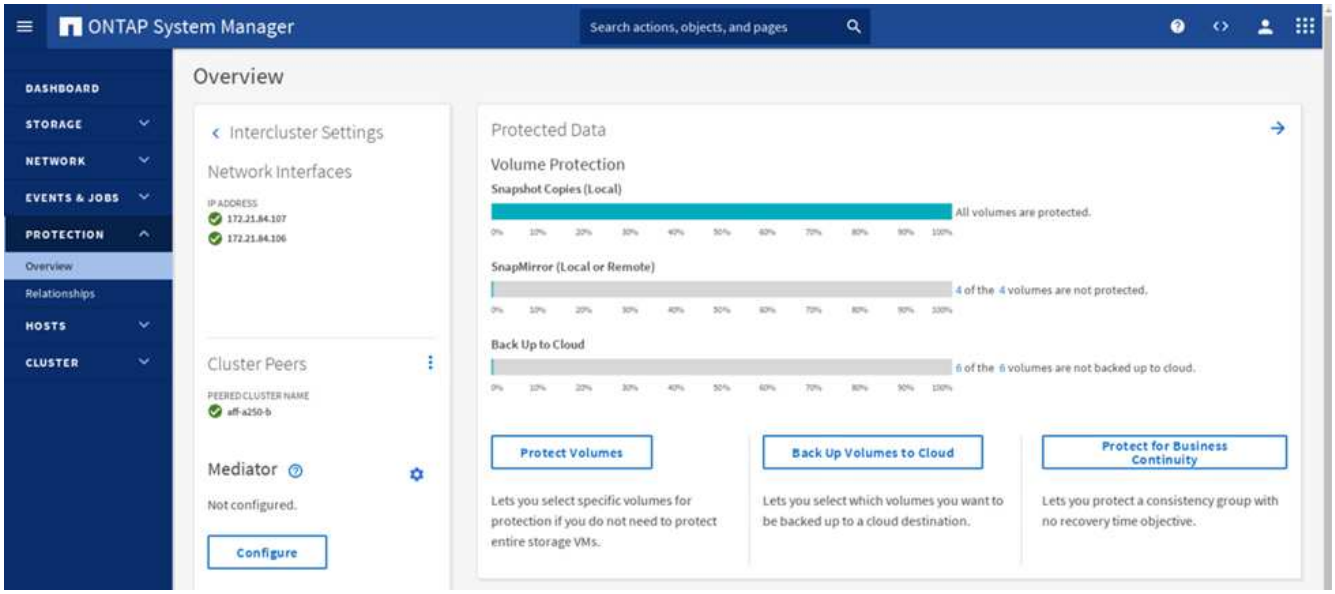
1. Genere una clave de acceso de paridad entre clústeres en el primer clúster.



2. Invoque la opción Peer Cluster en el segundo clúster y proporcione la clave de acceso e información de la LIF entre clústeres.



3. El panel Protección de System Manager > Overview muestra la información de paridad entre clústeres.

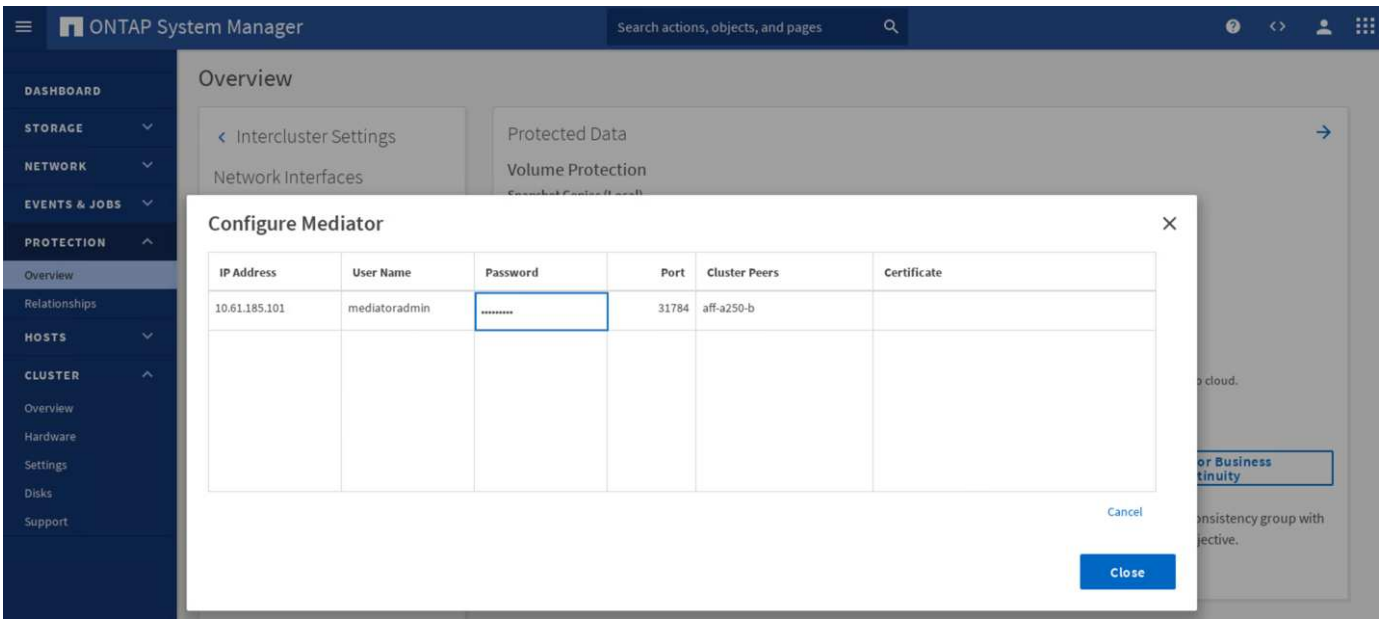


Instalación y configuración del Mediador ONTAP

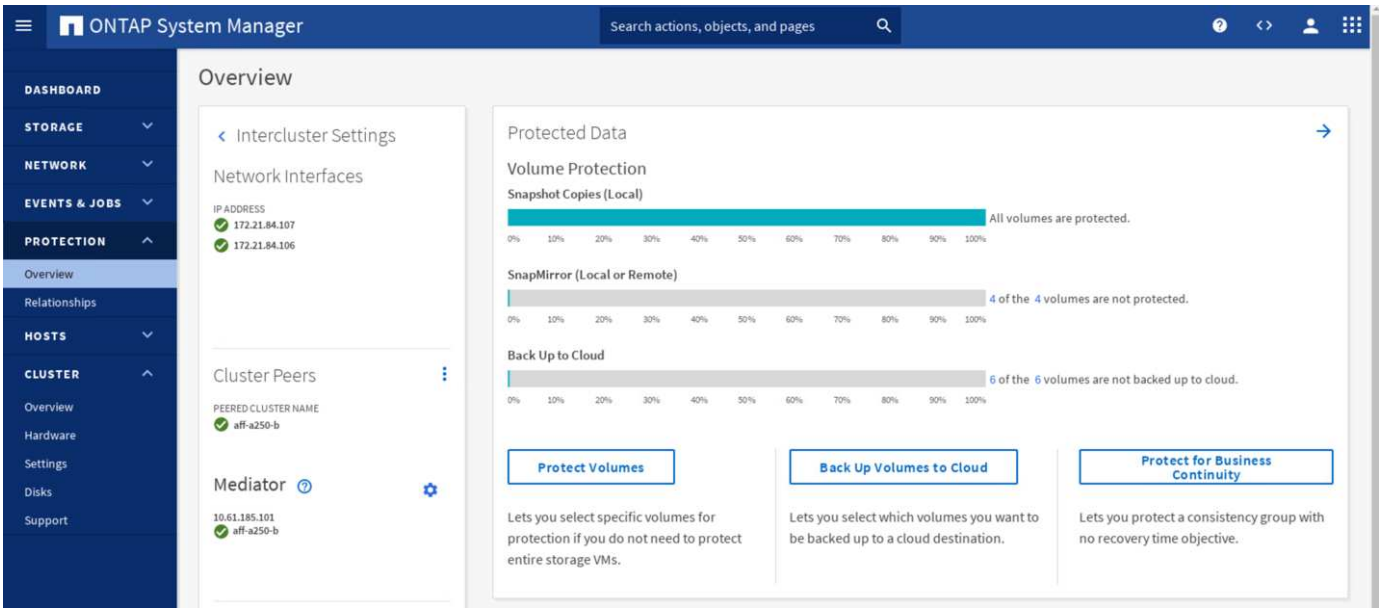
El Mediador ONTAP establece un quórum para los clústeres de ONTAP en una relación de SM-BC. Coordina la conmutación automática al nodo de respaldo cuando se detecta un fallo y ayuda a evitar situaciones de cerebro dividido cuando cada clúster intenta establecer el control simultáneamente como el clúster principal.

Antes de instalar el Mediador ONTAP, consulte "Instale o actualice el servicio Mediator de ONTAP" Página para requisitos previos, versiones compatibles de Linux y procedimientos para instalarlos en los distintos sistemas operativos Linux admitidos.

Una vez instalado el Mediador ONTAP, puede agregar el certificado de seguridad del Mediador ONTAP a los clústeres ONTAP y, a continuación, configurar el Mediador ONTAP en el panel Protección > Descripción general del Administrador del sistema. La siguiente captura de pantalla muestra la GUI de configuración del Mediador ONTAP.



Una vez que proporcione la información necesaria, el Mediador ONTAP configurado aparecerá en el panel Protección de System Manager > Descripción general.



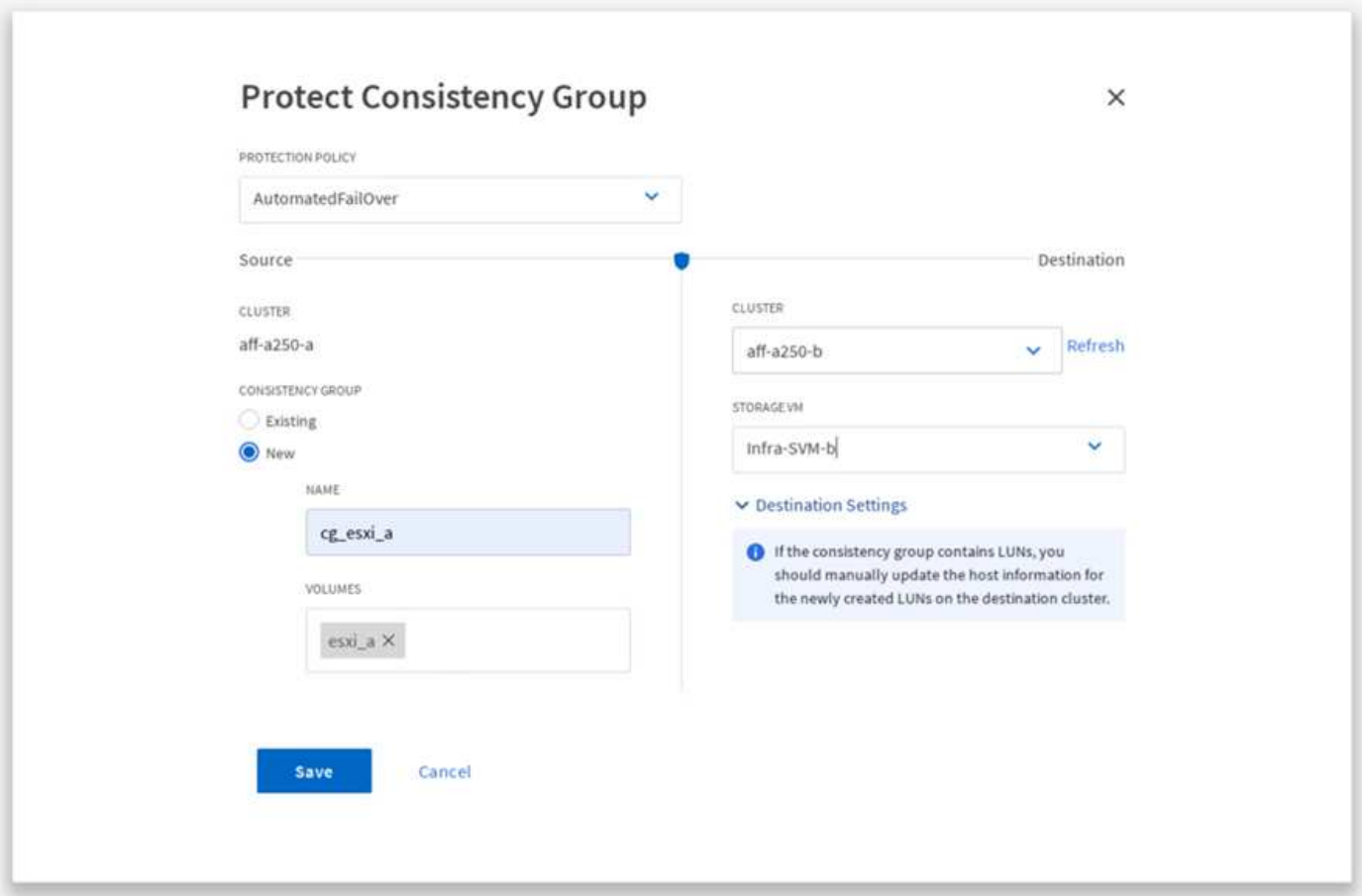
Grupo de consistencia SM-BC

Un grupo de coherencia ofrece una garantía de coherencia de orden de escritura para una carga de trabajo de aplicación que abarca una colección de volúmenes especificados. Para ONTAP 9.10.1, estas son algunas de las restricciones y limitaciones importantes.

- El número máximo de relaciones de grupos de consistencia de SM-BC en un clúster es 20.
- El número máximo de volúmenes admitidos por relación de SM-BC es 16.
- La cantidad máxima de extremos totales de origen y destino en un clúster es 200.

Para obtener más detalles, consulte la documentación de ONTAP SM-BC en "restricciones y limitaciones".

Para la configuración de validación, se utilizó System Manager de ONTAP para crear los grupos de consistencia a fin de proteger los LUN de arranque de ESXi y los LUN de almacenes de datos compartidos en ambos sitios. Para acceder al cuadro de diálogo de creación de grupos de consistencia, vaya a Protection > Overview > Protect for Business Continuity > Protect Consistency Group. Para crear un grupo de consistencia, proporcione la información de la máquina virtual de almacenamiento de destino, clúster de origen y volumen de destino necesarios para la creación.

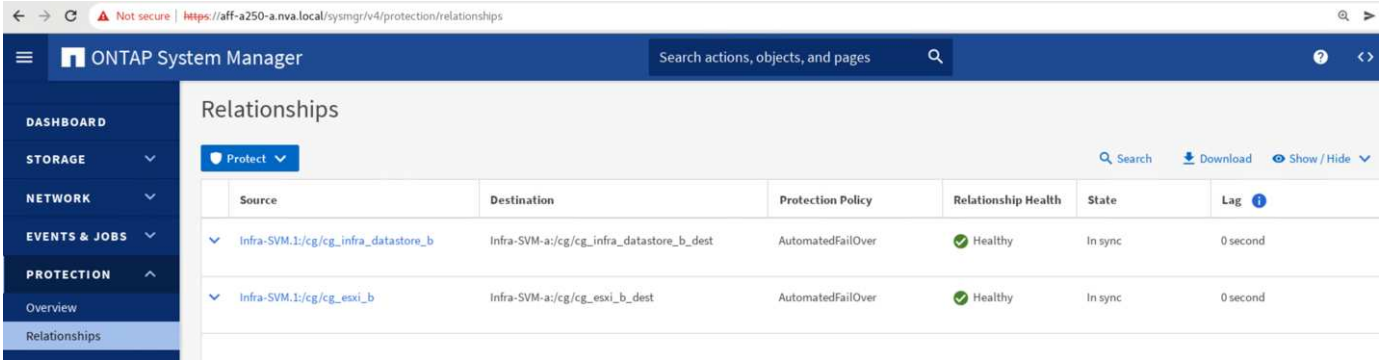


En la siguiente tabla, se enumeran los cuatro grupos de coherencia que se crean y los volúmenes que se incluyen en cada grupo de coherencia para la prueba de validación.

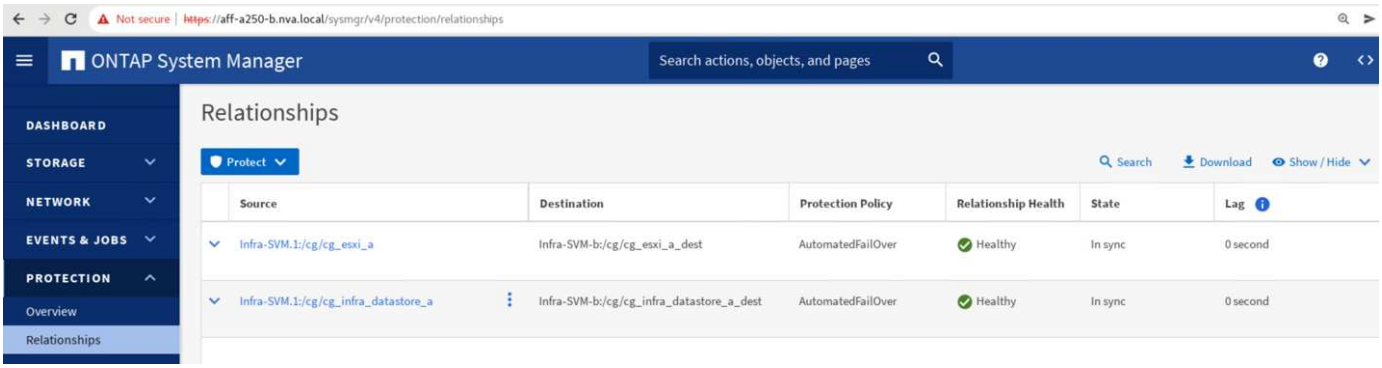
System Manager	Grupo de consistencia	Volúmenes
Centro a	cg_esxi_a	esxi_a
Centro a	cg_infra_datastore_a	infra_datastore_a_01 infra_datastore_a_02
Centro B	cg_esxi_b	esxi_b
Centro B	cg_infra_datastore_b	infra_datastore_b_01 infra_datastore_b_02

Después de crear los grupos de consistencia, se muestran bajo las respectivas relaciones de protección en el sitio A y en el sitio B.

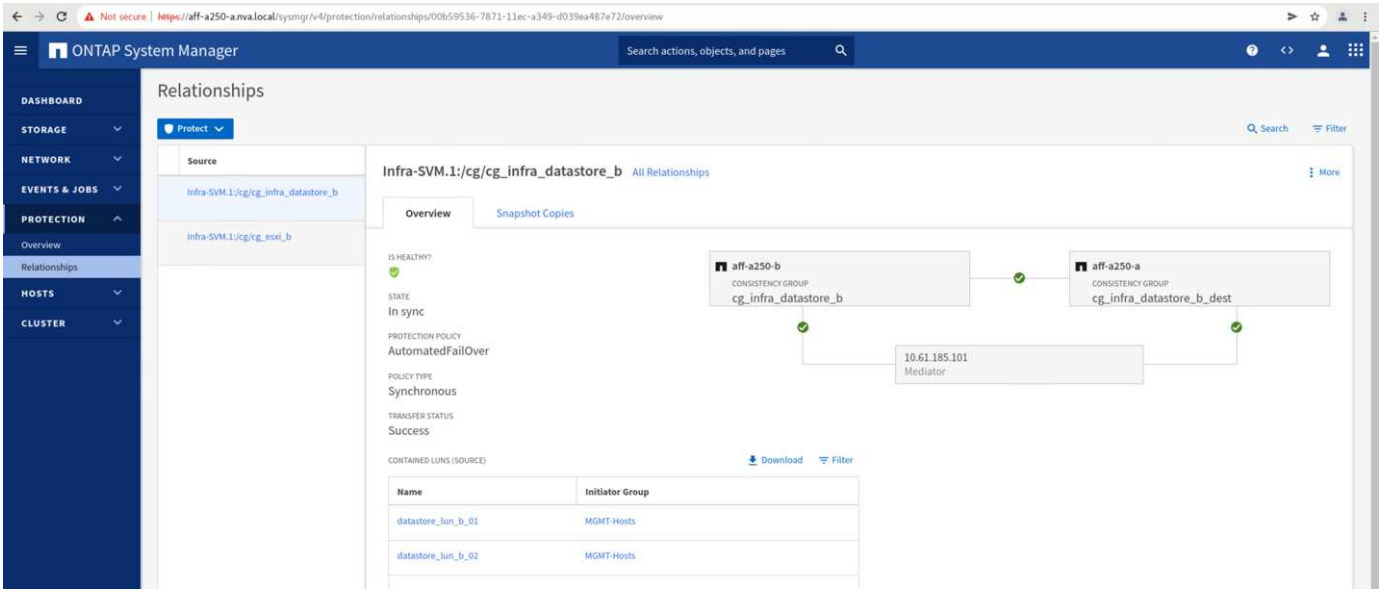
Esta captura de pantalla muestra las relaciones de los grupos de consistencia en la instalación A.



Esta captura de pantalla muestra las relaciones de los grupos de consistencia en la instalación B.



Esta captura de pantalla muestra los detalles de las relaciones del grupo de coherencia para el grupo cg_infra_datastore_b.



Volúmenes, LUN y asignaciones de host

Una vez que se han creado los grupos de coherencia, SnapMirror sincroniza los volúmenes de origen y de destino para que los datos siempre puedan estar sincronizados. Los volúmenes de destino en el sitio remoto transportan los nombres de los volúmenes con el fin _dest. Por ejemplo, para el volumen esxi_a en el sitio a un clúster, hay un volumen de protección de datos (DP) esxi_a_dest correspondiente en el sitio B.

Esta captura de pantalla muestra la información de volumen del sitio A.

```
aff-a250-a::> vol show -vserver Infra-SVM-a
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
Infra-SVM-a esxi_a     aggr1_aff_a250_a_01 online RW     320GB    315.9GB    1%
Infra-SVM-a esxi_b_dest aggr1_aff_a250_a_02 online DP   3.86GB    638.4MB   83%
Infra-SVM-a infra_datastore_a_01 aggr1_aff_a250_a_01 online RW 1TB 717.6GB  29%
Infra-SVM-a infra_datastore_a_02 aggr1_aff_a250_a_02 online RW 1TB 828.4GB  19%
Infra-SVM-a infra_svm_root aggr1_aff_a250_a_01 online RW   1GB    966.5MB    0%
Infra-SVM-a infra_svm_root_m01 aggr1_aff_a250_a_01 online LS 1GB  966.6MB    0%
Infra-SVM-a infra_svm_root_m02 aggr1_aff_a250_a_02 online LS 1GB  966.6MB    0%
Infra-SVM-a vol_infra_datastore_b_01_dest aggr1_aff_a250_a_01 online DP 138.7GB 31.52GB  76%
Infra-SVM-a vol_infra_datastore_b_02_dest aggr1_aff_a250_a_01 online DP 49.37GB 9.03GB  80%
9 entries were displayed.
```

Esta captura de pantalla muestra la información de volumen del sitio B.

```
aff-a250-b::> vol show -vserver Infra-SVM-b
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
Infra-SVM-b esxi_a_dest aggr1_aff_a250_b_02 online DP   4.10GB    768.2MB   80%
Infra-SVM-b esxi_b     aggr1_aff_a250_b_01 online RW     320GB    315.8GB    1%
Infra-SVM-b infra_datastore_b_01 aggr1_aff_a250_b_01 online RW 1TB 911.9GB  10%
Infra-SVM-b infra_datastore_b_02 aggr1_aff_a250_b_02 online RW 1TB 964.0GB   5%
Infra-SVM-b infra_svm_root aggr1_aff_a250_b_01 online RW   1GB    966.9MB    0%
Infra-SVM-b infra_svm_root_m01 aggr1_aff_a250_b_01 online LS 1GB  967.0MB    0%
Infra-SVM-b infra_svm_root_m02 aggr1_aff_a250_b_02 online LS 1GB  967.0MB    0%
Infra-SVM-b vol_infra_datastore_a_01_dest aggr1_aff_a250_b_02 online DP 270.0GB 27.39GB  89%
Infra-SVM-b vol_infra_datastore_a_02_dest aggr1_aff_a250_b_02 online DP 202.8GB 28.20GB  85%
9 entries were displayed.
```

Para facilitar una conmutación por error transparente de aplicaciones, los LUN reflejados de SM-BC también deben asignarse a los hosts del clúster de destino. Esto permite que los hosts vean correctamente las rutas a las LUN desde los clústeres de origen y de destino. La `igroup show` y.. `lun show` Las salidas para el sitio A y el sitio B se capturan en las dos capturas de pantalla siguientes. Con las asignaciones creadas, cada host ESXi del clúster ve su propio LUN de arranque SAN como ID 0 y los cuatro LUN de almacén de datos iSCSI compartidos.

Esta captura de pantalla muestra los iGroups del host y la asignación de LUN para el sitio A un clúster.

```
aff-a250-a::> igroup show
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
Infra-SVM-a MGMT-Hosts iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-a:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:3
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:3
Infra-SVM-a VM-Host-Infra-a-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:1
Infra-SVM-a VM-Host-Infra-a-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:2
Infra-SVM-a VM-Host-Infra-a-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-a VM-Host-Infra-b-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:1
Infra-SVM-a VM-Host-Infra-b-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:2
Infra-SVM-a VM-Host-Infra-b-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:3
7 entries were displayed.

aff-a250-a::> lun show -m
Vserver    Path                                      Igroup   LUN ID  Protocol
---------- ----------------------------------------  -------  ------  --------
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-01           VM-Host-Infra-a-01  0  iscsi
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-02           VM-Host-Infra-a-02  0  iscsi
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-03           VM-Host-Infra-a-03  0  iscsi
Infra-SVM-a /vol/esxi_a/swap_lun_a                   MGMT-Hosts   13  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-01      VM-Host-Infra-b-01  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-02      VM-Host-Infra-b-02  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-03      VM-Host-Infra-b-03  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/swap_lun_b              MGMT-Hosts   23  iscsi
Infra-SVM-a /vol/infra_datastore_a_01/datastore_lun_a_01  MGMT-Hosts  11  iscsi
Infra-SVM-a /vol/infra_datastore_a_02/datastore_lun_a_02  MGMT-Hosts  12  iscsi
Infra-SVM-a /vol/vol_infra_datastore_b_01_dest/datastore_lun_b_01  MGMT-Hosts  21  iscsi
Infra-SVM-a /vol/vol_infra_datastore_b_02_dest/datastore_lun_b_02  MGMT-Hosts  22  iscsi
12 entries were displayed.
```

Esta captura de pantalla muestra los iGroups del host y la asignación de LUN para el clúster del sitio B.

```
aff-a250-b::> igroup show
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
Infra-SVM-b MGMT-Hosts iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-b:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:3
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-b VM-Host-Infra-a-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:1
Infra-SVM-b VM-Host-Infra-a-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:2
Infra-SVM-b VM-Host-Infra-a-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-b VM-Host-Infra-b-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:1
Infra-SVM-b VM-Host-Infra-b-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:2
Infra-SVM-b VM-Host-Infra-b-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:3
7 entries were displayed.

aff-a250-b::> lun show -m
Vserver    Path                                        Igroup   LUN ID  Protocol
---------- ------------------------------------------  -------  ------  --------
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-01      VM-Host-Infra-a-01  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-02      VM-Host-Infra-a-02  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-03      VM-Host-Infra-a-03  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/swap_lun_a              MGMT-Hosts   13  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-01           VM-Host-Infra-b-01  0  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-02           VM-Host-Infra-b-02  0  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-03           VM-Host-Infra-b-03  0  iscsi
Infra-SVM-b /vol/esxi_b/swap_lun_b                   MGMT-Hosts   23  iscsi
Infra-SVM-b /vol/infra_datastore_b_01/datastore_lun_b_01  MGMT-Hosts  21  iscsi
Infra-SVM-b /vol/infra_datastore_b_02/datastore_lun_b_02  MGMT-Hosts  22  iscsi
Infra-SVM-b /vol/vol_infra_datastore_a_01_dest/datastore_lun_a_01  MGMT-Hosts  11  iscsi
Infra-SVM-b /vol/vol_infra_datastore_a_02_dest/datastore_lun_a_02  MGMT-Hosts  12  iscsi
12 entries were displayed.
```

"Siguiente: Validación de la solución - virtualización."

Validación de la solución - virtualización

"Anterior: Validación de la solución - almacenamiento."

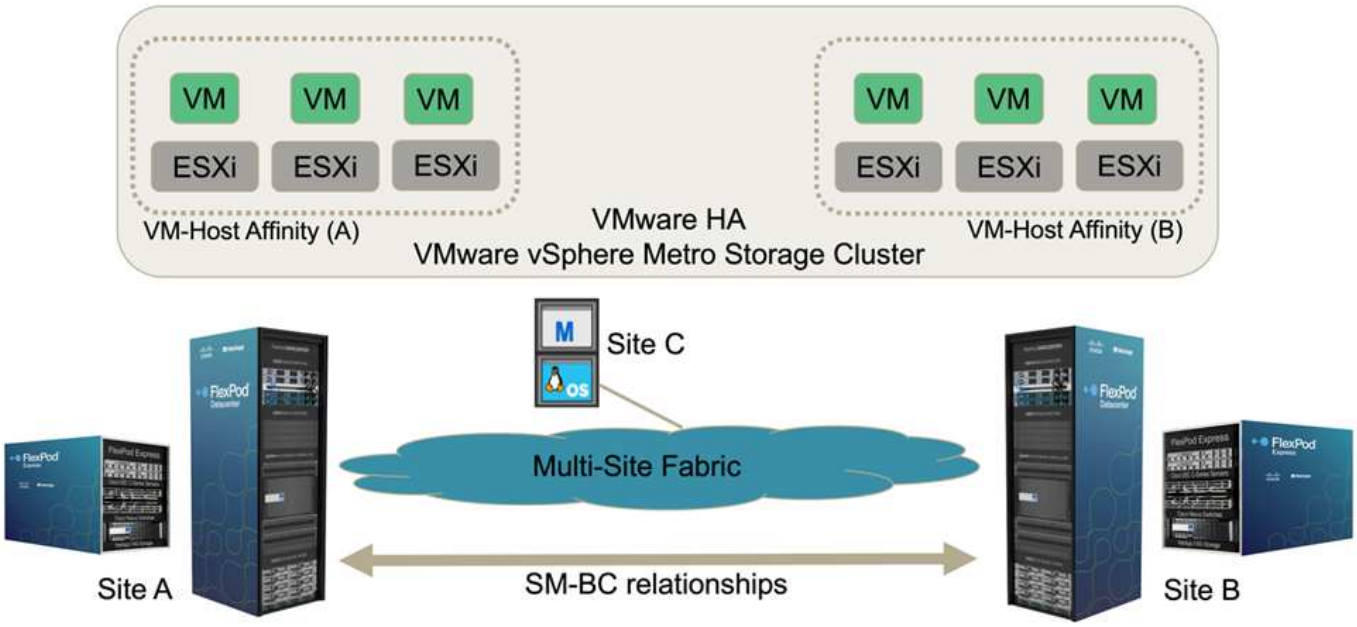
En la solución FlexPod SM-BC multisitio, un solo VMware vCenter gestiona los recursos de infraestructura virtual para toda la solución. Los hosts de ambos centros de datos participan en un único clúster de alta disponibilidad de VMware que abarca ambos centros de datos. Los hosts tienen acceso a la solución SM-BC de NetApp, en la que es posible acceder al almacenamiento con relaciones SM-BC definidas desde ambos sitios.

El almacenamiento de la solución SM-BC cumple con el modelo de acceso uniforme de la función VMware vSphere Metro Storage Cluster (VMSC) para evitar desastres y tiempos de inactividad. Para obtener un rendimiento óptimo de las máquinas virtuales, los discos de máquinas virtuales deben alojarse en los sistemas AFF A250 de NetApp locales para minimizar la latencia y el tráfico por los enlaces WAN bajo un funcionamiento normal.

Como parte de la implementación de diseño, hay que determinar la distribución de las máquinas virtuales en los dos sitios. Puede determinar esta afinidad de sitio de equipos virtuales y la distribución de aplicaciones en los dos sitios de acuerdo con sus preferencias de sitio y requisitos de aplicación. El clúster de VMware VM/grupos de hosts y las reglas de VM/host se usan para configurar la afinidad de VM/host para garantizar que los equipos virtuales se ejecutan en los hosts del sitio deseado.

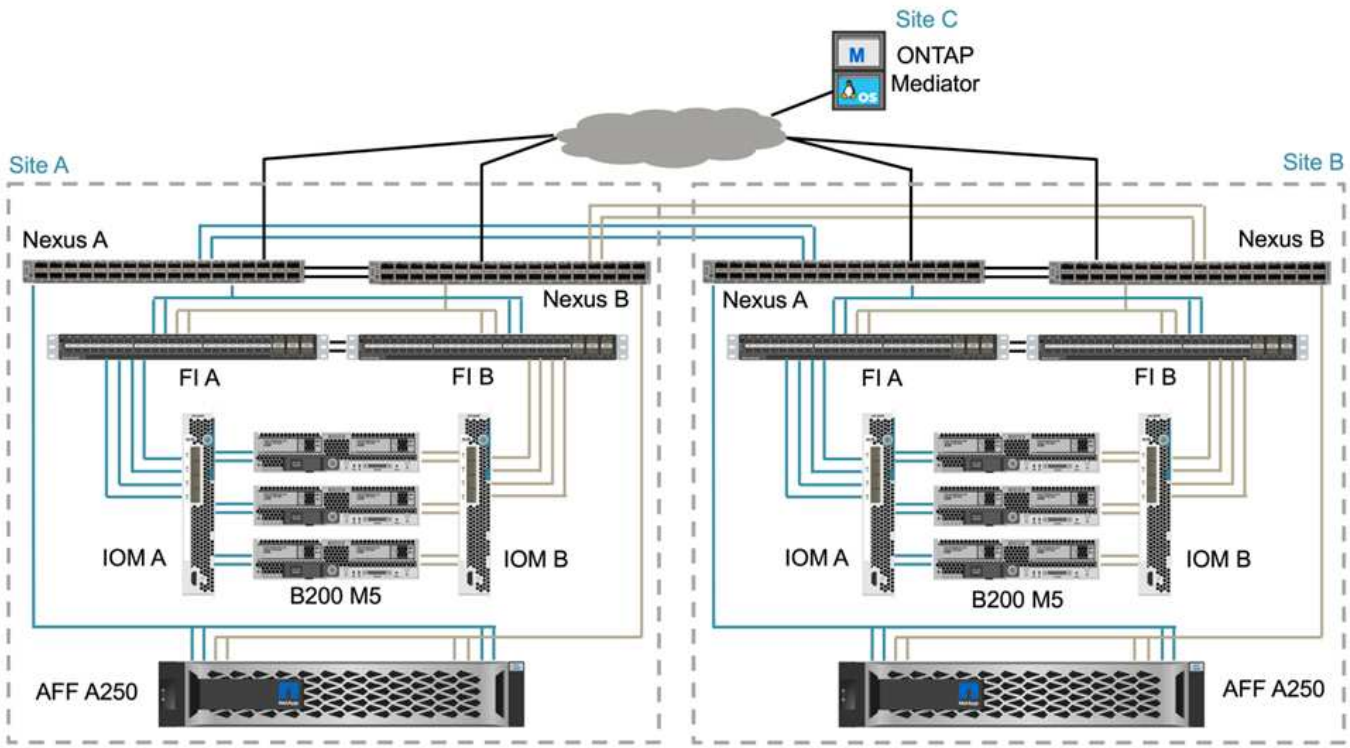
Sin embargo, las configuraciones que permiten que los equipos virtuales se ejecuten en ambos centros asegurarán de que VMware ha puede reiniciar los equipos virtuales en hosts de centro remoto para proporcionar flexibilidad a la solución. Para acomodar máquinas virtuales para ejecutarse en ambos sitios, todos los almacenes de datos compartidos iSCSI deben montarse en todos los hosts ESXi para garantizar un funcionamiento vMotion fluido de las máquinas virtuales entre sitios.

La siguiente figura muestra una vista de virtualización de soluciones FlexPod SM-BC de alto nivel, que incluye funciones de VMware ha y VMSC para proporcionar alta disponibilidad para servicios informáticos y de almacenamiento. La arquitectura de soluciones de centro de datos activo-activo permite la movilidad de las cargas de trabajo entre sitios y proporciona protección ante desastres/continuidad del negocio.



Conectividad de red completa

La solución FlexPod SM-BC incluye infraestructuras FlexPod en cada sitio, conectividad de red entre sitios y el mediador de ONTAP puesto en marcha en un tercer sitio para satisfacer los objetivos de punto de recuperación y de tiempo de recuperación necesarios. En la siguiente figura se muestra la conectividad de red completa entre los servidores Cisco UCS B200M5 de cada sitio y el almacenamiento de NetApp con capacidad SM-BC dentro de un sitio y entre diferentes ubicaciones.



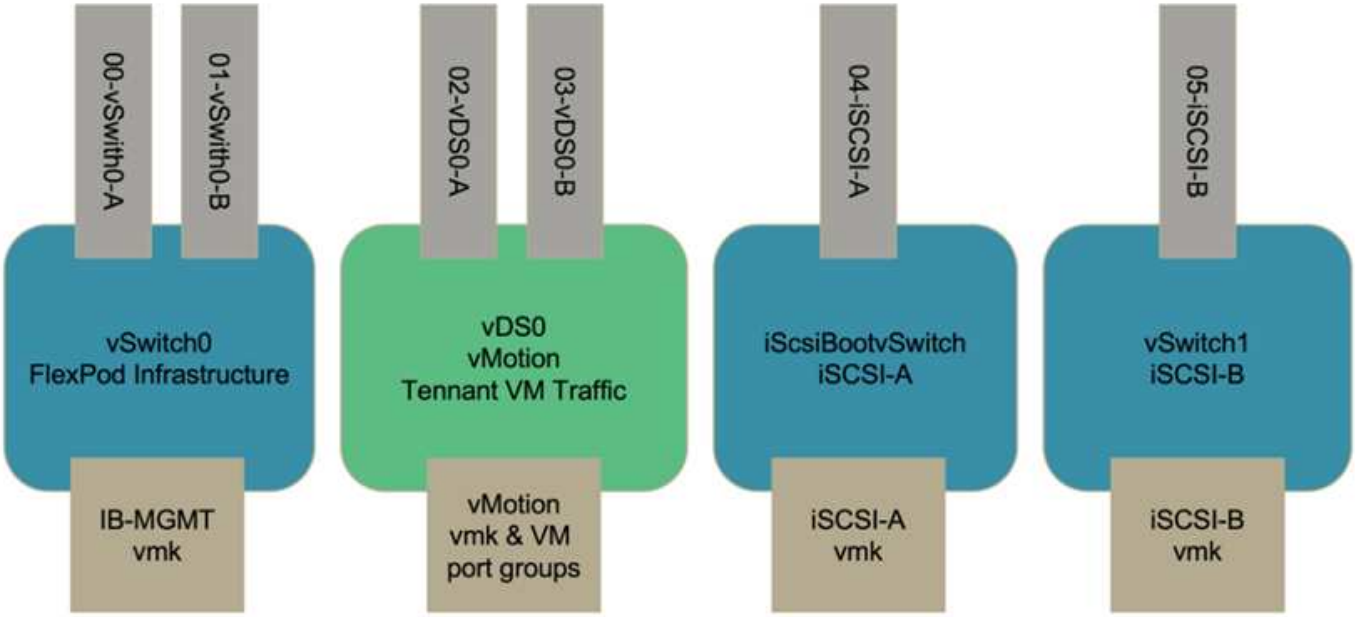
La arquitectura de puesta en marcha de FlexPod es idéntica en cada site para validar esta solución. Sin embargo, la solución admite implementaciones asimétricas y puede añadirse a una solución FlexPod existente si cumple los requisitos.

La arquitectura ampliada de capa 2 se utiliza para una estructura de datos multisitio fluida que proporciona conectividad entre la computación de Cisco UCS y el almacenamiento de NetApp canalizados por puertos en cada centro de datos, así como conectividad entre centros de datos. La configuración del canal de puertos y la configuración del canal de puertos virtuales, cuando corresponda, se utilizan para la agregación de ancho de banda y la tolerancia a fallos entre las capas de cálculo, red y almacenamiento, así como para los enlaces entre sitios. Como resultado, los servidores blade UCS cuentan con conectividad y acceso multivía tanto al almacenamiento de NetApp local como remoto.

Redes virtuales

Cada host del clúster se pone en marcha utilizando redes virtuales idénticas independientemente de su ubicación. El diseño separa los diferentes tipos de tráfico mediante los switches virtuales de VMware (vSwitch) y los switches virtuales distribuidos (VDS) de VMware. El vSwitch de VMware se utiliza principalmente para las redes de infraestructura FlexPod y VDS para las redes de aplicaciones, pero no es necesario.

Los switches virtuales (vSwitch, VDS) se ponen en marcha con dos enlaces de subida por switch virtual; los enlaces ascendentes del hipervisor ESXi se denominan vmnics y NIC virtuales (vNIC) en Cisco UCS Software. Las NIC virtuales se crean en el adaptador Cisco UCS VIC en cada servidor utilizando los perfiles de servicio de Cisco UCS. Se definen seis vNICs, dos para vSwitch0, dos para vDS0, dos para vSwitch1 y dos para los enlaces de subida iSCSI, como se muestra en la siguiente figura.



VSwitch0 se define durante la configuración del host VMware ESXi y contiene la VLAN de gestión de la infraestructura de FlexPod y los puertos del host VMkernel (VMK) de ESXi para la gestión. Un grupo de puertos de máquinas virtuales de gestión de infraestructuras también se encuentra en vSwitch0 para el uso de máquinas virtuales de gestión de infraestructuras clave que sean necesarias.

Es importante colocar estas máquinas virtuales de infraestructura de gestión en vSwitch0, en lugar de en el VDS porque si la infraestructura de FlexPod se apaga o se somete a apagado y encendido/apagado, e intenta activar esa máquina virtual de gestión en un host distinto al host en el que se estaba ejecutando originalmente, Se inicia correctamente en la red de vSwitch0. Este proceso es especialmente importante si VMware vCenter es la máquina virtual de gestión. Si vCenter estaba en el VDS y se movió a otro host y, a continuación, se inició, no se conectaría a la red después de arrancar.

En este diseño se utilizan dos vSwitch de arranque iSCSI. El arranque iSCSI de Cisco UCS requiere NIC independientes para el arranque iSCSI. Estas NIC utilizan VLAN iSCSI de la estructura adecuada como VLAN nativa y se conectan al vSwitch de arranque iSCSI adecuado. También es posible implementar redes iSCSI en VDS si se implementa una instancia nueva de VDS o se utiliza una existente.

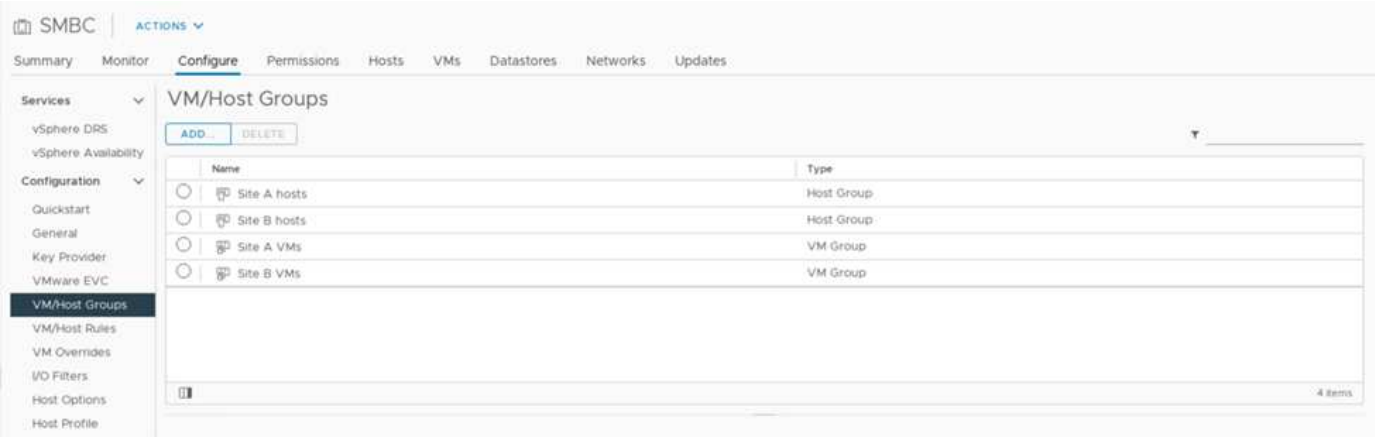
Reglas y grupos de afinidad de VM-Host

Para permitir que las máquinas virtuales se ejecuten en cualquier host ESXi en ambos sitios de SM-BC, todos los hosts ESXi deben montar los almacenes de datos iSCSI desde ambos sitios. Si los almacenes de datos de ambos sitios están correctamente montados por todos los hosts ESXi, puede migrar una máquina virtual entre cualquier host con vMotion y la máquina virtual aún mantiene el acceso a todos sus discos virtuales creados a partir de esos almacenes de datos.

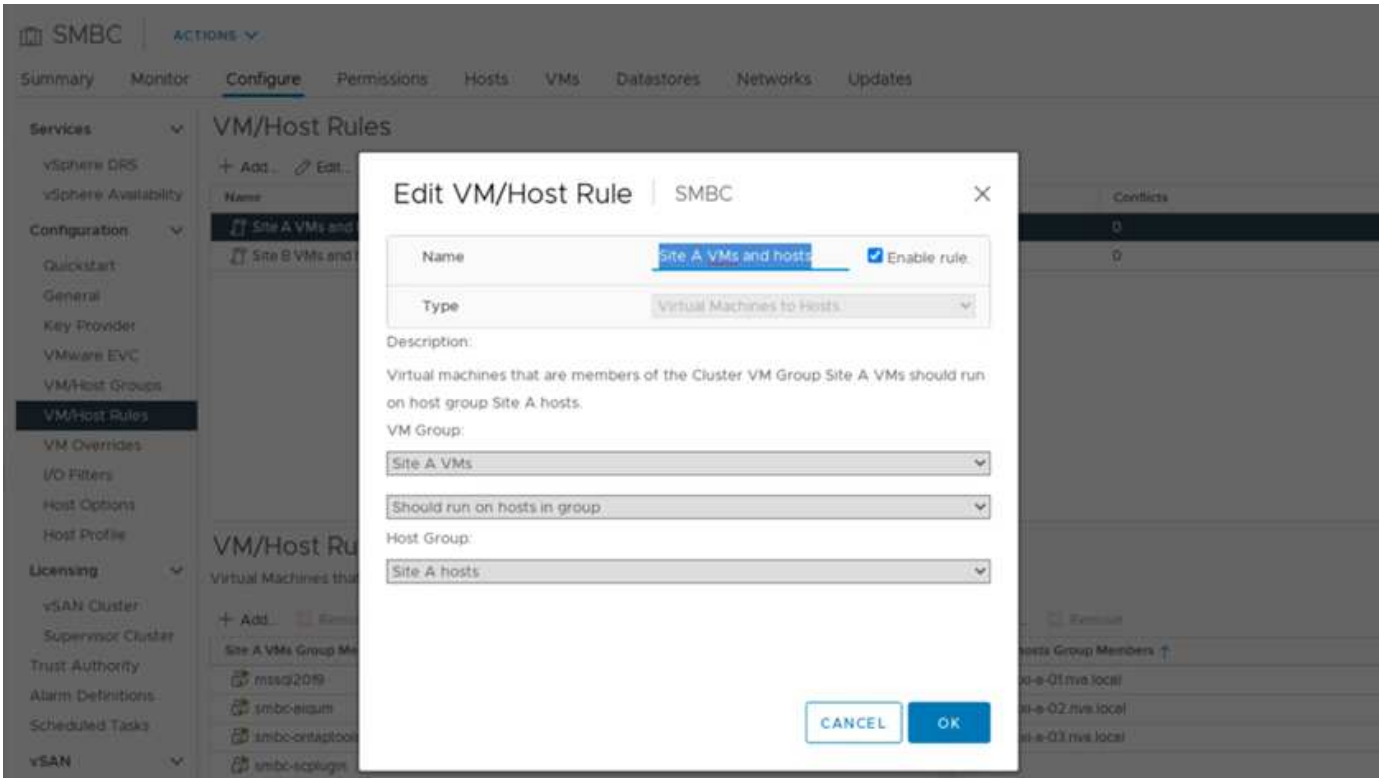
En el caso de una máquina virtual que usa almacenes de datos locales, su acceso a los discos virtuales se convierte en remoto si se migra a un host del sitio remoto y, por lo tanto, se aumenta la latencia de las operaciones de lectura debido a la distancia física entre los sitios. Por lo tanto, se recomienda mantener las máquinas virtuales en los hosts locales y utilizar el almacenamiento local en el sitio.

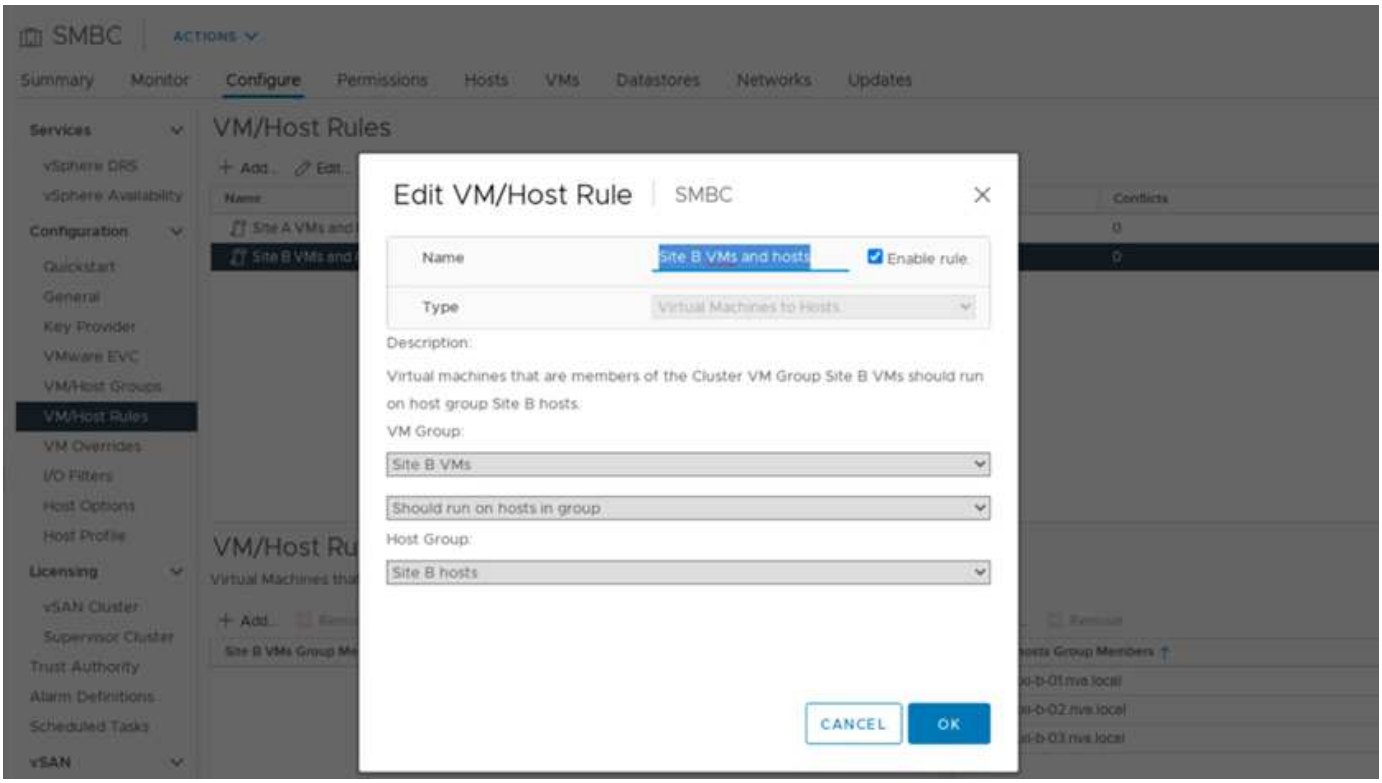
Mediante el uso de un mecanismo de afinidad de VM/host, se puede usar VM/grupos de hosts para crear un grupo de VM y un grupo de hosts para máquinas virtuales y hosts ubicados en un sitio determinado. Con las reglas de host/VM, puede especificar la política que deben seguir las máquinas virtuales y los hosts. Para permitir la migración de máquinas virtuales entre sitios durante un escenario de mantenimiento de sitios o desastres, use la especificación de políticas “debería ejecutarse en hosts en grupo” para esa flexibilidad.

La siguiente captura de pantalla muestra que se crean dos grupos de hosts y dos grupos de equipos virtuales para los hosts y equipos virtuales del sitio a y del sitio B.



Además, las dos figuras siguientes muestran las reglas VM/Host que se crean para que las VM del sitio A y del sitio B se ejecuten en los hosts de sus respectivos sitios utilizando la política “debería ejecutarse en hosts en grupo”.

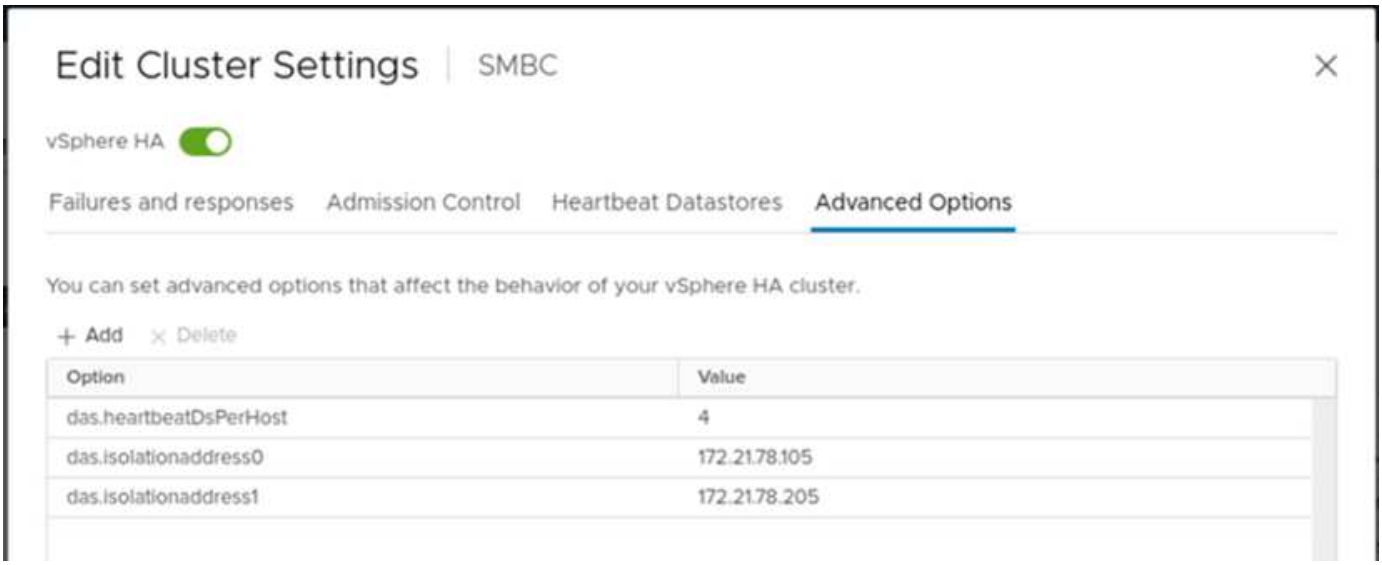




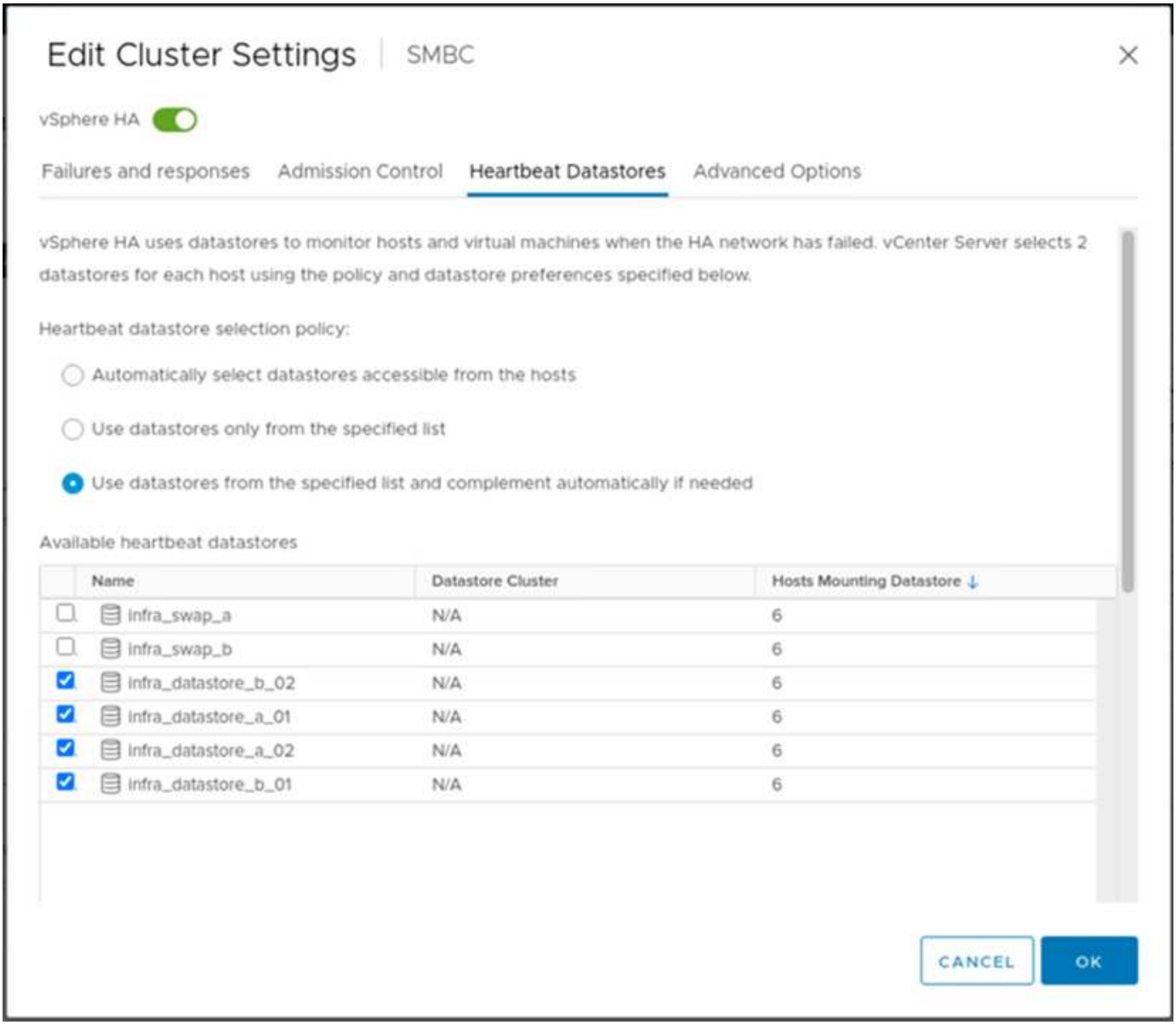
Corazón de vSphere ha

VMware vSphere ha cuenta con un mecanismo de corazón para la validación del estado del host. El mecanismo primario de latidos se realiza mediante redes, mientras que el mecanismo de latidos del corazón secundarios se realiza a través del almacén de datos. Si no se reciben latidos, entonces decide si están aislados de la red haciendo ping a la puerta de enlace predeterminada o a las direcciones de aislamiento configuradas manualmente. Para los latidos del corazón de los almacenes de datos, VMware recomienda aumentar el número de almacenes de datos Heartbeat desde el mínimo de dos a cuatro en un clúster extendido.

Para la validación de soluciones, las dos direcciones IP de administración del clúster de ONTAP se usan como dirección de aislamiento. Además, la opción vSphere ha Advanced recomendada `ds.heartbeatDsPerHost` con un valor de 4 se agregó como se muestra en la siguiente figura.



Para el almacén de datos Heartbeat, especifique los cuatro almacenes de datos compartidos del clúster y complemente automáticamente, como se muestra en la siguiente figura.



Para obtener más información sobre las mejores prácticas y configuraciones para VMware ha Cluster y VMware vSphere Metro Storage Cluster, consulte "Crear y usar clústeres de vSphere ha", "VMware vSphere Metro Storage Cluster (VMSC)" Y la base de conocimientos de VMware para "ONTAP de NetApp con la continuidad empresarial de SnapMirror de NetApp (SM-BC) y VMware vSphere Metro Storage Cluster (VMSC)".

"Siguiente: Validación de la solución - escenarios validados."

Validación de la solución: Situaciones validadas

"Anterior: Validación de la solución - virtualización."

La solución SM-BC de FlexPod Datacenter protege los servicios de datos para numerosos escenarios de fallo de un único punto, así como para un desastre en el sitio. El diseño redundante implementado en cada sitio proporciona alta disponibilidad, y la

implementación de SM-BC con replicación de datos síncrona en sitios protege los servicios de datos de un desastre en todo el sitio de un sitio. La solución puesta en marcha se ha validado para las funciones deseadas y se han utilizado varios escenarios de fallos para los que la solución ha sido diseñada para proteger.

Validación de las funciones de la solución

Se utilizan diversos casos de prueba para verificar las funciones de la solución y simular escenarios de fallo de sitio completos y parciales. Para minimizar la duplicación con las pruebas ya realizadas en las soluciones de centros de datos FlexPod existentes en el programa Cisco Validated Design, este informe se centra en los aspectos relacionados con el SM-BC de la solución. Se incluyen algunas validaciones generales de FlexPod para que los profesionales puedan realizar sus validaciones de implementación.

Para la validación de soluciones, se creó una máquina virtual de Windows 10 por host ESXi en todos los hosts ESXi en ambos sitios. La herramienta Iometer se instaló y se utilizó para generar I/o en dos discos de datos virtuales asignados a partir de los almacenes de datos iSCSI locales compartidos. Los parámetros de carga de trabajo de Iometer configurados eran I/o de 8 KB, 75% de lectura y 50% aleatorio, con 8 comandos de I/o excepcionales para cada disco de datos. En la mayoría de los escenarios de prueba realizados, la continuación de las operaciones de I/o de Iometer sirve como indicador de que el escenario no ha causado una interrupción del servicio de datos.

Dado que SM-BC es fundamental para aplicaciones empresariales como servidores de bases de datos, La instancia de Microsoft SQL Server 2019 en un equipo virtual de Windows Server 2022 también se incluyó como parte de las pruebas para confirmar que la aplicación continúa ejecutándose cuando el almacenamiento de su sitio local no está disponible y el servicio de datos se reanuda en el almacenamiento del centro remoto sin aplicaciones interrupciones.

Prueba de arranque SAN iSCSI del host ESXi

Los hosts ESXi de la solución están configurados para arrancar desde SAN iSCSI. El uso de arranque SAN simplifica la gestión de servidores al sustituir un servidor, ya que el perfil de servicio del servidor puede estar asociado con un nuevo servidor para que arranque sin realizar ningún cambio de configuración adicional.

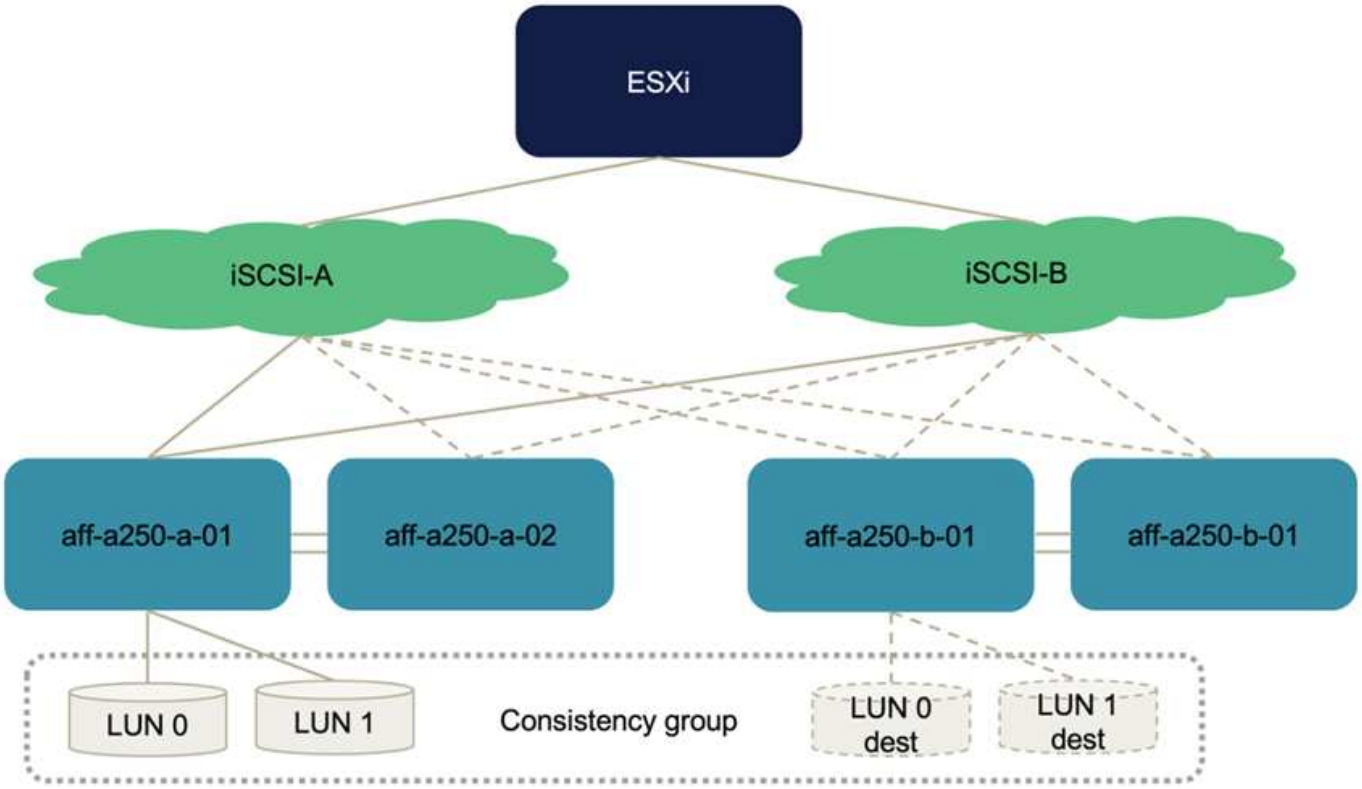
Además de arrancar un host ESXi ubicado en un sitio desde su LUN de arranque iSCSI local, también se llevaron a cabo pruebas para arrancar el host ESXi cuando la controladora de almacenamiento local está en estado de toma de control o cuando su clúster de almacenamiento local no está completamente disponible. Estos escenarios de validación garantizan que los hosts ESXi estén correctamente configurados por diseño y que puedan arrancar durante un caso de mantenimiento del almacenamiento o de desastre en caso de desastre para la recuperación ante desastres, con el fin de proporcionar continuidad empresarial.

Antes de configurar la relación de grupo de consistencia SM-BC, un LUN iSCSI alojado en un par de alta disponibilidad de controladora de almacenamiento tiene cuatro rutas, dos a través de cada estructura iSCSI, según la implementación de las prácticas recomendadas. Un host se puede llegar a la LUN a través de las dos VLAN/estructuras de iSCSI hasta la controladora que aloja LUN, así como a través del partner de alta disponibilidad de la controladora.

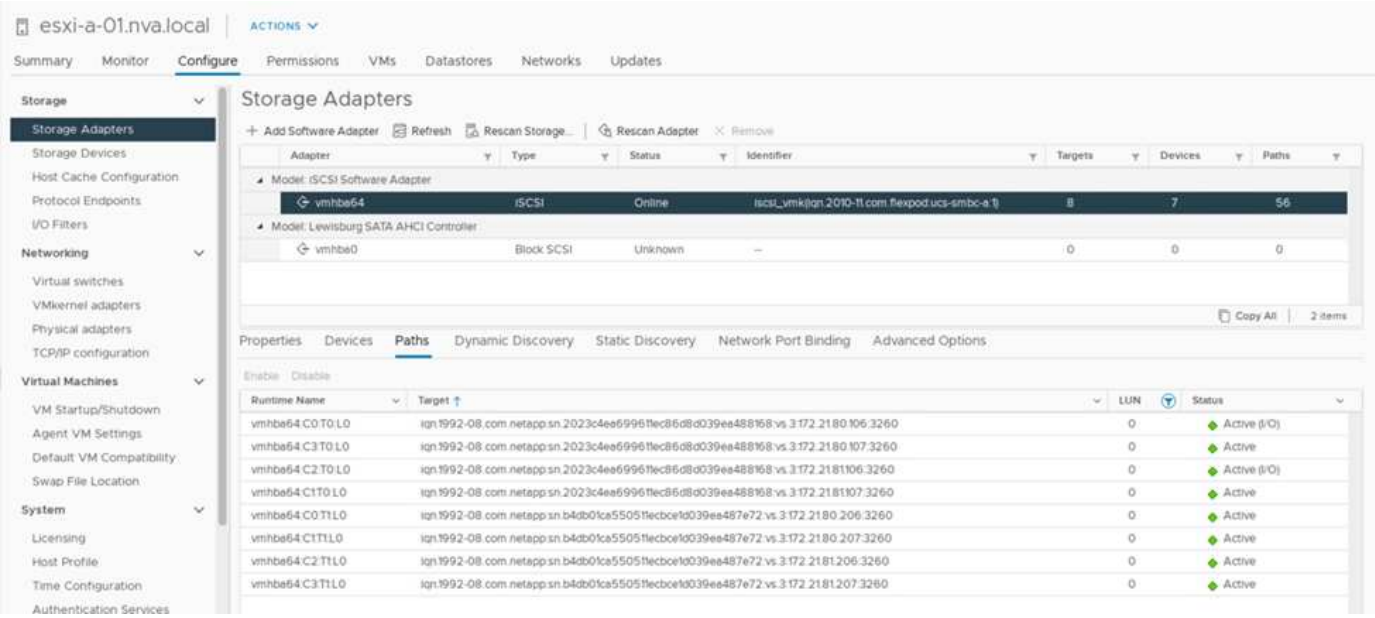
Después de configurar la relación del grupo de consistencia SM-BC y de asignar correctamente las LUN reflejadas a los iniciadores, el número de rutas de la LUN se duplica. Para esta implementación, pasa de tener dos rutas activo/optimizado y dos rutas activo/no optimizadas a tener dos rutas activas/optimizadas y seis rutas activas/no optimizadas.

La siguiente figura muestra las rutas que un host ESXi puede tener para acceder a una LUN, por ejemplo, LUN 0. Como la LUN está conectada al sitio una controladora 01, solo las dos rutas de acceso directamente al LUN a través de dicha controladora están activas/optimizadas y las restantes seis rutas están activas/no

optimizadas.



La siguiente captura de pantalla de la información de la ruta del dispositivo de almacenamiento muestra cómo el host ESXi ve los dos tipos de rutas del dispositivo. Las dos rutas activas/optimizadas se muestran como tienen `active (I/O)` estado de ruta, mientras que las seis rutas activas/no optimizadas sólo se muestran como `active`. Tenga también en cuenta que la columna destino muestra los dos destinos iSCSI y las respectivas direcciones IP de LIF iSCSI para llegar a los destinos.



Cuando una de las controladoras de almacenamiento se desactiva para realizar tareas de mantenimiento o actualización, las dos rutas que llegan a la controladora inactivo ya no están disponibles y se muestran con un estado de ruta de `dead` en su lugar.

Si se produce una conmutación por error del grupo de consistencia en el clúster de almacenamiento principal, ya sea debido a pruebas de conmutación por error manuales o a una conmutación por error automática ante desastres, el clúster de almacenamiento secundario sigue proporcionando servicios de datos para las LUN del grupo de consistencia SM-BC. Dado que las identidades de LUN se conservan y los datos se han replicado de forma síncrona, todos los LUN de arranque de host ESXi protegidos por los grupos de coherencia de SM-BC siguen estando disponibles en el clúster de almacenamiento remoto.

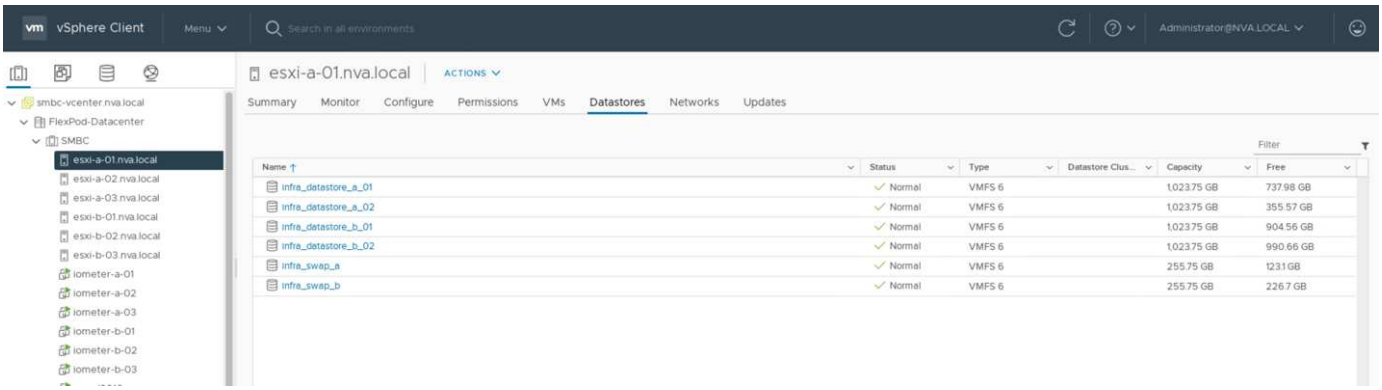
Prueba de afinidad de VMware vMotion y VM/host

Aunque una solución genérica VMware Datacenter de FlexPod admite varios protocolos, como FC, iSCSI, NVMe y NFS, la función de solución FlexPod SM-BC admite los protocolos SAN FC e iSCSI que se suelen utilizar para soluciones vitales para el negocio. Esta validación solo utiliza almacenes de datos basados en protocolo iSCSI y arranque SAN iSCSI.

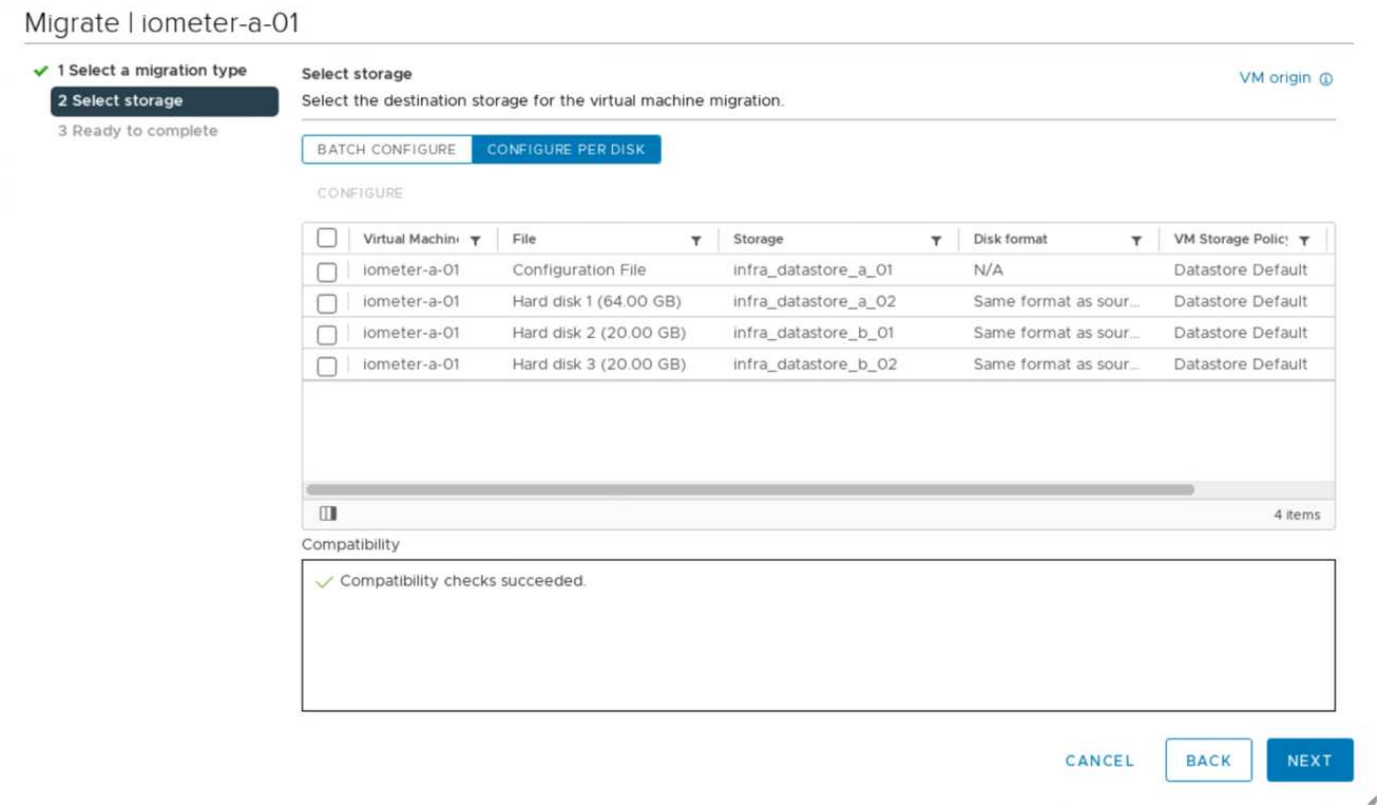
Para que las máquinas virtuales puedan usar servicios de almacenamiento desde un sitio de SM-BC, todos los hosts del clúster deben montar los almacenes de datos iSCSI de ambos sitios para permitir la migración de máquinas virtuales entre los dos sitios y en casos de conmutación por error en caso de desastre.

Para aplicaciones que se ejecuten en la infraestructura virtual que no requieran la protección de grupos de coherencia de SM-BC en todos los sitios, también pueden usarse el protocolo NFS y almacenes de datos NFS. En este caso, se debe prestar especial atención a la hora de asignar almacenamiento a equipos virtuales para que las aplicaciones vitales para el negocio utilicen correctamente los almacenes de datos SAN protegidos por el grupo de consistencia SM-BC para proporcionar continuidad empresarial.

La siguiente captura de pantalla muestra que los hosts están configurados para montar almacenes de datos iSCSI de ambos sitios.



Existe la opción de migrar discos de máquinas virtuales entre almacenes de datos iSCSI disponibles de ambos sitios, como se muestra en la siguiente figura. Por cuestiones de rendimiento, es óptimo disponer de máquinas virtuales que utilicen almacenamiento de su clúster de almacenamiento local para reducir las latencias de I/o de disco. Esto es especialmente cierto cuando los dos sitios están ubicados a ciertas distancias separadas debido a la latencia de distancia física de ida y vuelta de aproximadamente 1 ms por 100 km de distancia.



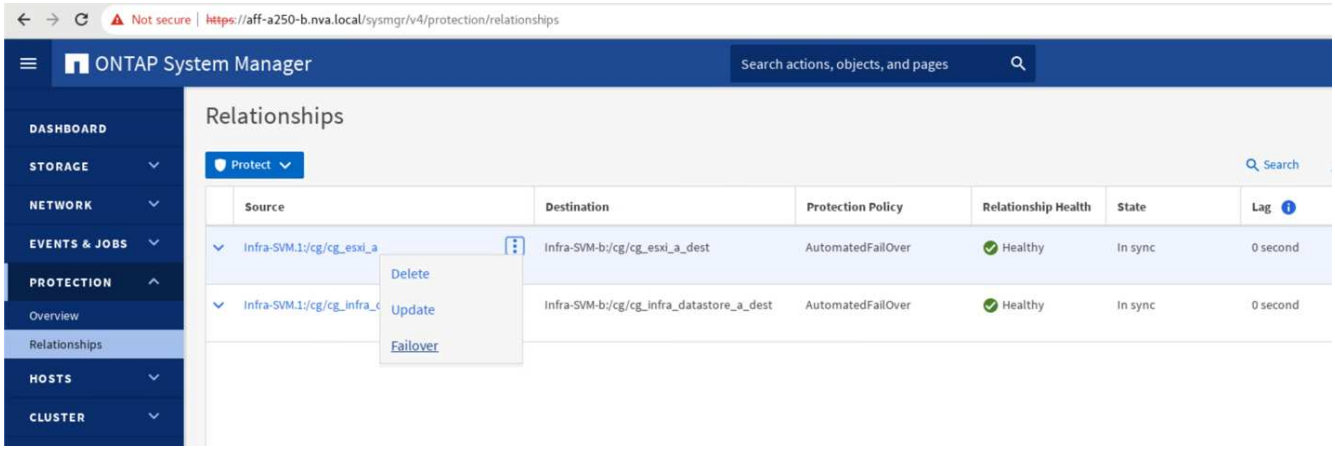
Se llevaron a cabo pruebas de vMotion de máquinas virtuales en un diferente host en el mismo sitio, así como en varios sitios, que se realizaron con éxito. Después de migrar manualmente una máquina virtual entre sitios, la regla de afinidad VM/Host activa y migra la máquina virtual de nuevo al grupo al que pertenece bajo la condición normal.

Recuperación tras fallos planificada de almacenamiento

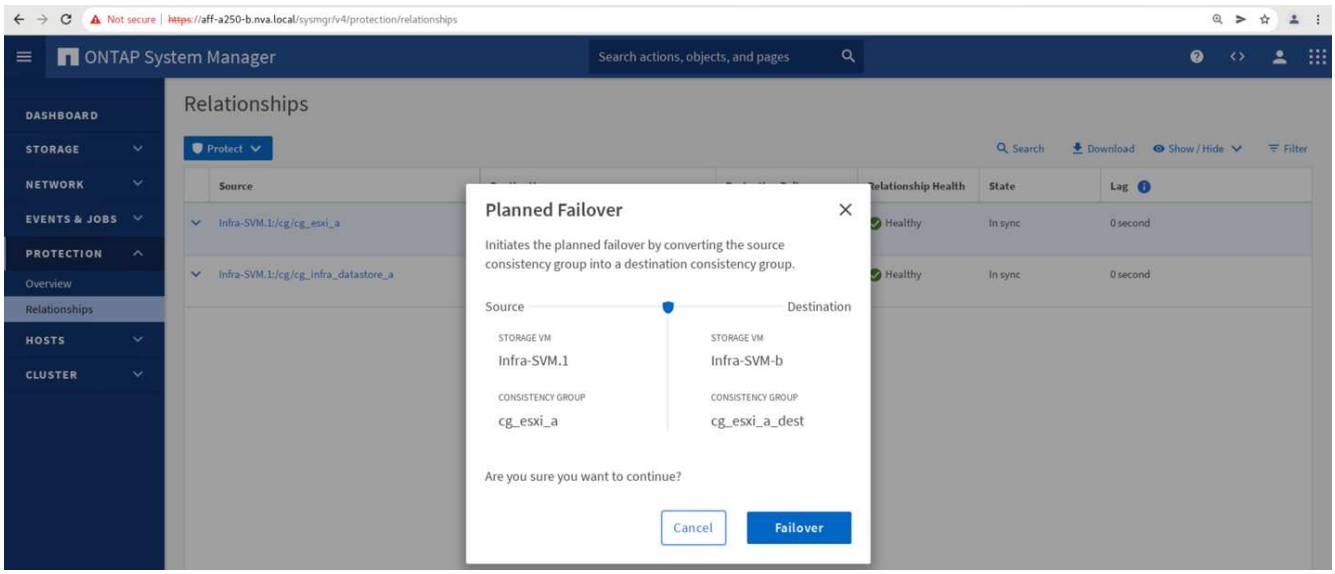
Las operaciones planificadas de conmutación por error del almacenamiento se deben realizar en la solución después de la configuración inicial para determinar si la solución funciona correctamente después de la conmutación por error del almacenamiento. Las pruebas pueden ayudar a identificar cualquier problema de conectividad o configuración que pueda provocar interrupciones de I/O. Probar y solucionar con regularidad cualquier problema de conectividad o configuración ayuda a proporcionar servicios de datos sin interrupciones cuando se produce un desastre en el sitio real. La conmutación por error planificada de almacenamiento también se puede utilizar antes de llevar a cabo una actividad de mantenimiento de almacenamiento programada, de modo que los servicios de datos puedan ofrecerse del sitio no afectado.

Para iniciar una conmutación por error manual del sitio A los servicios de datos de almacenamiento en el sitio B, puede usar el Administrador del sistema ONTAP del sitio B para realizar la acción.

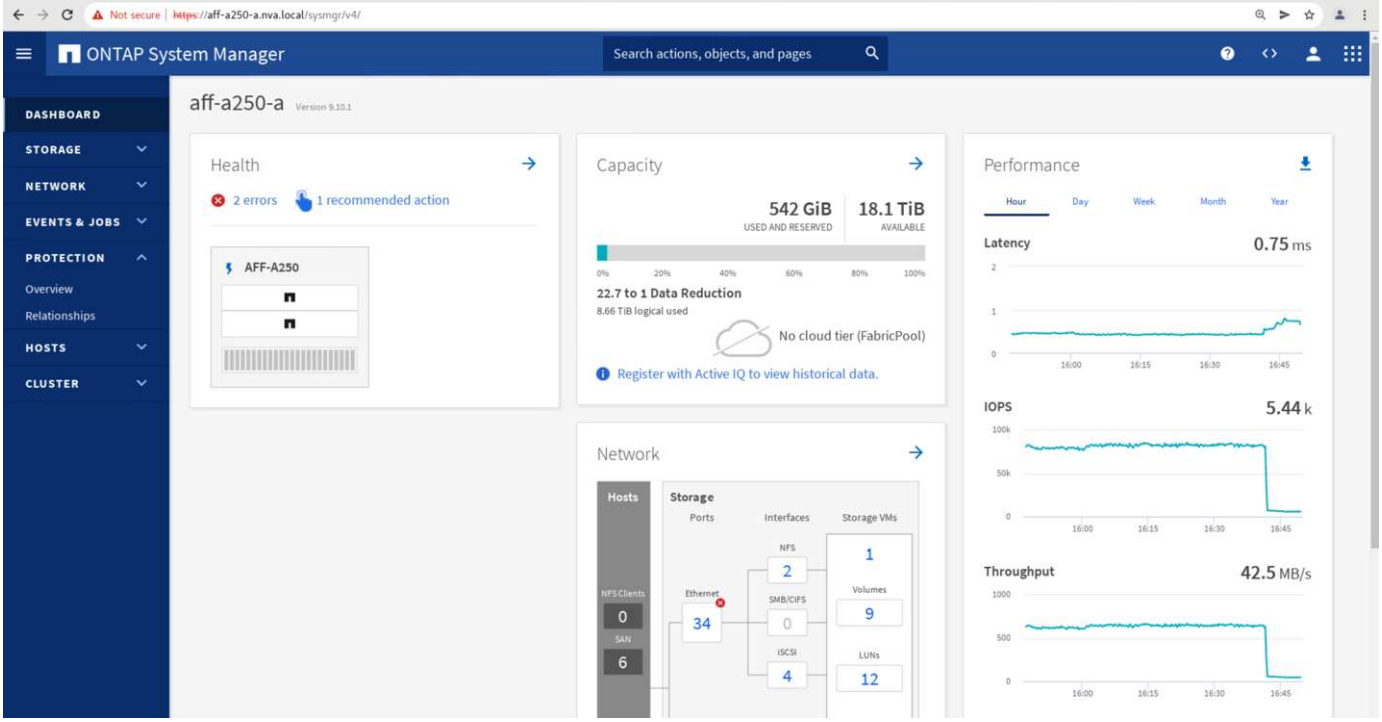
1. Vaya a la pantalla Protection > Relationships para confirmar que el estado de la relación del grupo de coherencia es `In Sync`. Si todavía está en el `Synchronizing` estado, espere a que el estado se convierta `In Sync` antes de realizar una conmutación al respaldo.
2. Expanda los puntos junto al nombre del origen y haga clic en conmutación por error.



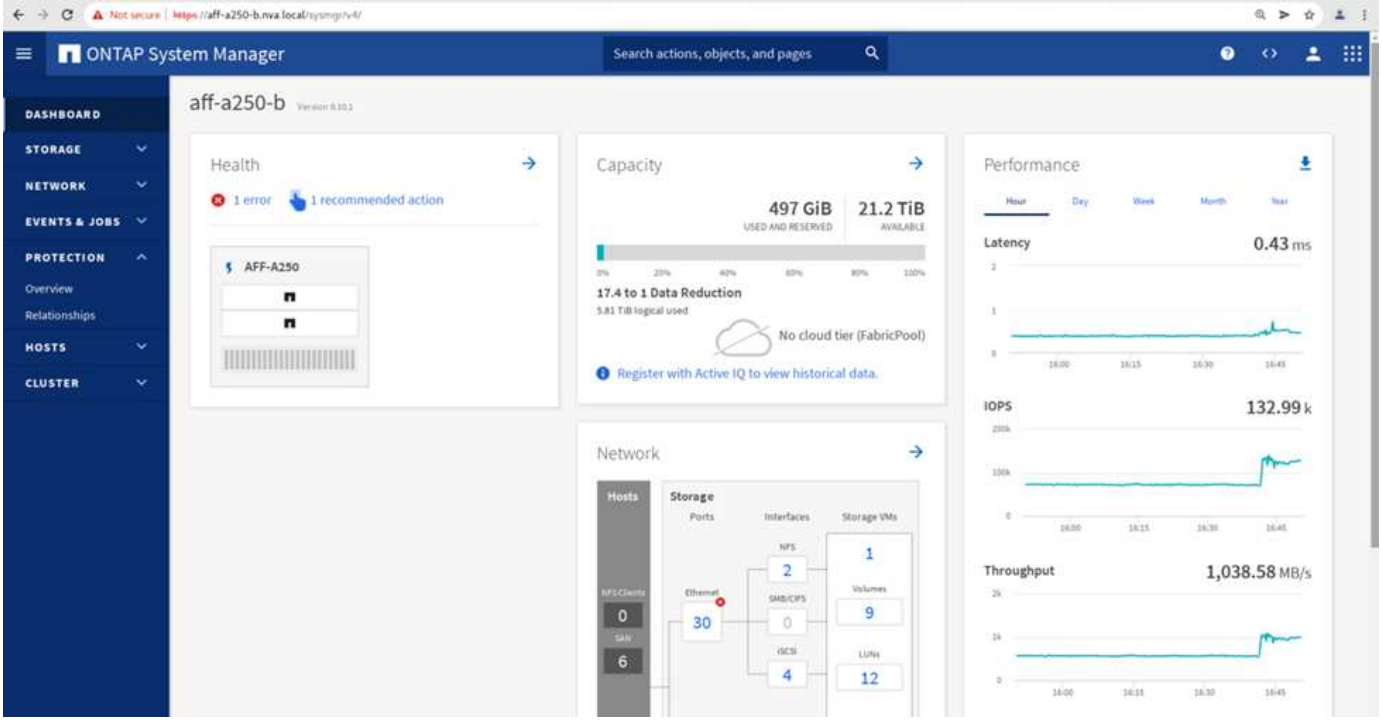
3. Confirme la conmutación por error para el inicio de la acción.



Poco después de iniciar la conmutación por error de los dos grupos de consistencia, `cg_esxi_a` y.. `cg_infra_datastore_a`, En la GUI del Administrador del sistema del sitio B, el sitio a E/S que sirve a esos dos grupos de consistencia movidos al sitio B. Como resultado, la actividad de I/o del sitio se reduce significativamente como se muestra en El panel de rendimiento De System Manager Del sitio.

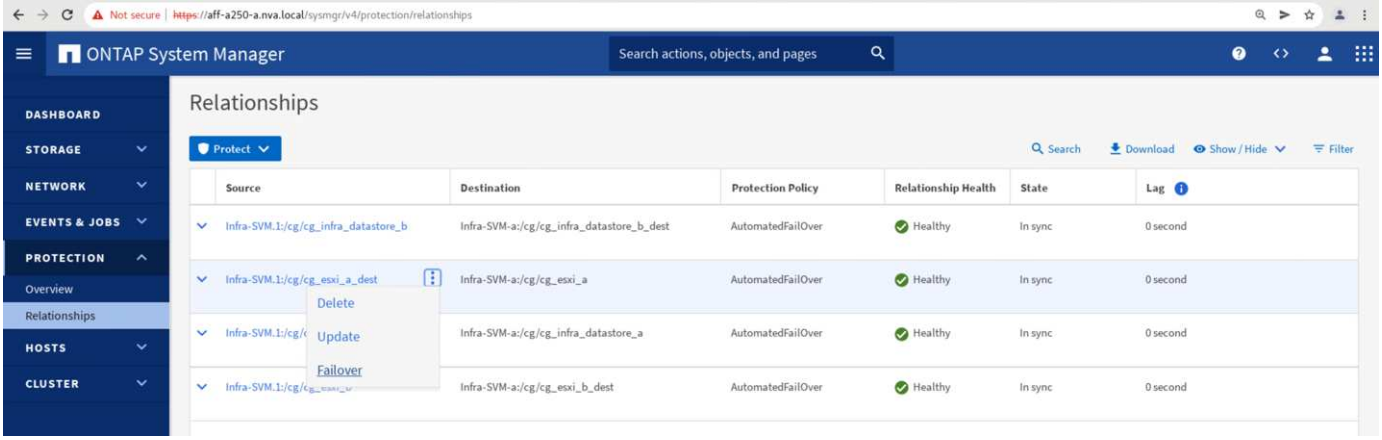


Por otro lado, el panel rendimiento de la consola del administrador del sistema del sitio B muestra un aumento significativo en IOPS, debido al servicio de I/o adicional trasladado desde la instalación A, a aproximadamente 130.000 IOPS, Y llegó a un rendimiento de aproximadamente 1 GB/s, a la vez que mantiene una latencia de I/o inferior a 1 milésima de segundo.



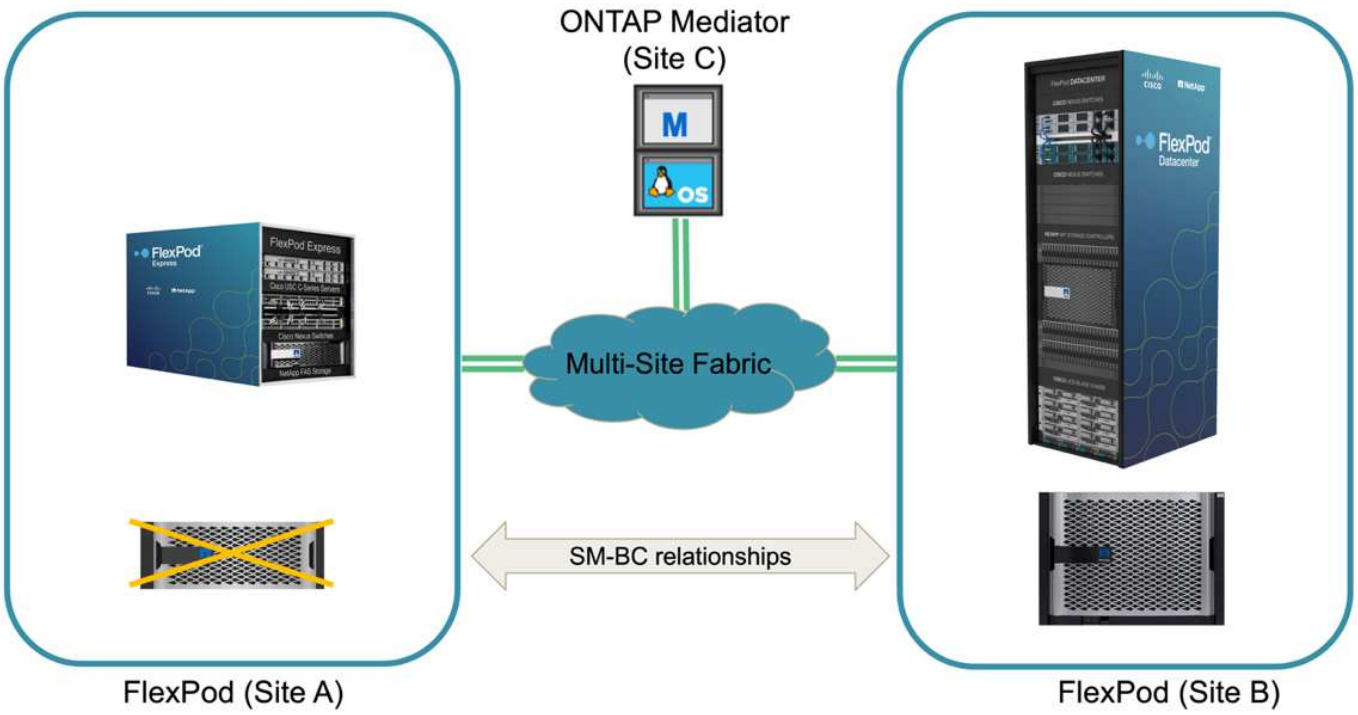
Con la migración transparente de las operaciones De I/o del sitio A al sitio B, ahora es posible desconectar las controladoras De almacenamiento para tareas de mantenimiento programadas. Una vez que se hayan completado el trabajo de mantenimiento o las pruebas y el sitio en el que se cree un clúster de almacenamiento en un backup y en funcionamiento, compruebe y espere a que el estado de protección del grupo de consistencia vuelva a cambiar a. `In sync` Antes de realizar una conmutación al nodo de respaldo para devolver las operaciones de I/o de conmutación al nodo de respaldo del sitio B al sitio A. Tenga en

cuenta que cuanto más tiempo se tarda un sitio en realizarse tareas de mantenimiento o prueba, más tiempo se tarda en sincronizar los datos y el grupo de consistencia se vuelve a la `In sync` estado.



Recuperación no planificada tras fallos de almacenamiento

Se puede producir una conmutación al nodo de respaldo no planificada del almacenamiento cuando se produce un desastre real o durante una simulación de desastre. Por ejemplo, consulte la siguiente figura en la que el sistema de almacenamiento del sitio A experimenta una interrupción del suministro eléctrico, se activa una conmutación por error del almacenamiento no planificada y los servicios de datos de las LUN del sitio A, que están protegidas por las relaciones de SM-BC, continúan en el sitio B.



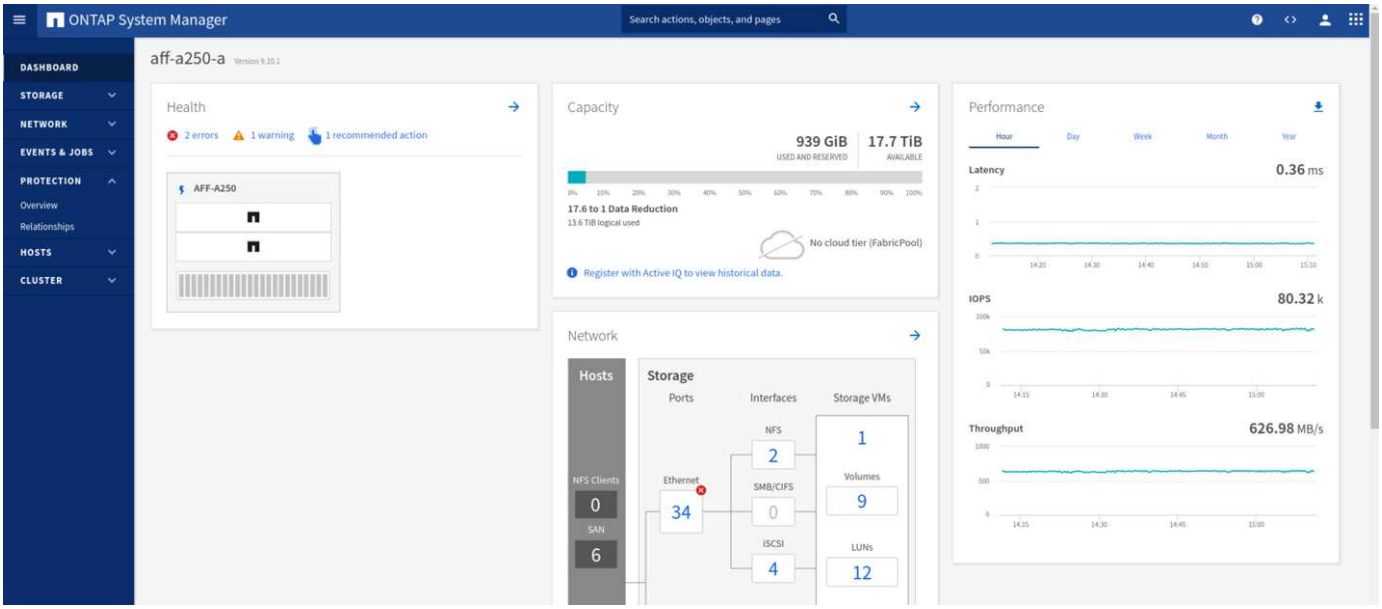
Para simular un desastre de almacenamiento en el centro A, ambas controladoras de almacenamiento en el sitio A pueden apagarse físicamente el switch de alimentación para interrumpir el suministro de alimentación de las controladoras, o mediante el uso del comando de administración de energía del sistema del procesador de servicio de la controladora de almacenamiento para apagar las controladoras.

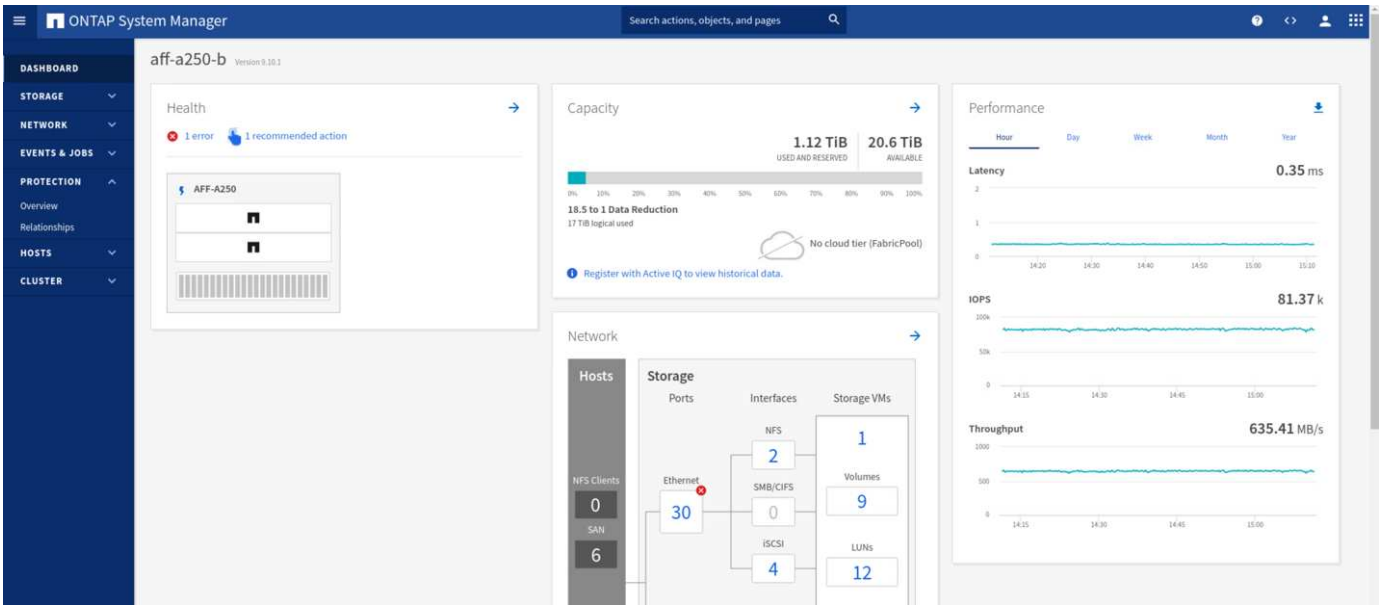
Cuando el clúster de almacenamiento del centro a pierde potencia, hay una parada repentina de los servicios de datos proporcionados por el sitio Un clúster de almacenamiento. Posteriormente, el Mediator de ONTAP, que supervisa la solución SM-BC desde un tercer sitio, detecta el sitio una condición De fallo de

almacenamiento y permite que la solución SM-BC realice una conmutación por error automatizada no planificada. Esto permite que las controladoras de almacenamiento del sitio B continúen los servicios de datos para las LUN configuradas en las relaciones del grupo de consistencia de SM-BC con el sitio A.

Desde la perspectiva de la aplicación, los servicios de datos se hacen una pausa brevemente mientras el sistema operativo comprueba el estado de la ruta de las LUN y, a continuación, reanuda las operaciones de I/o de las rutas disponibles a las controladoras de almacenamiento del sitio B supervivientes.

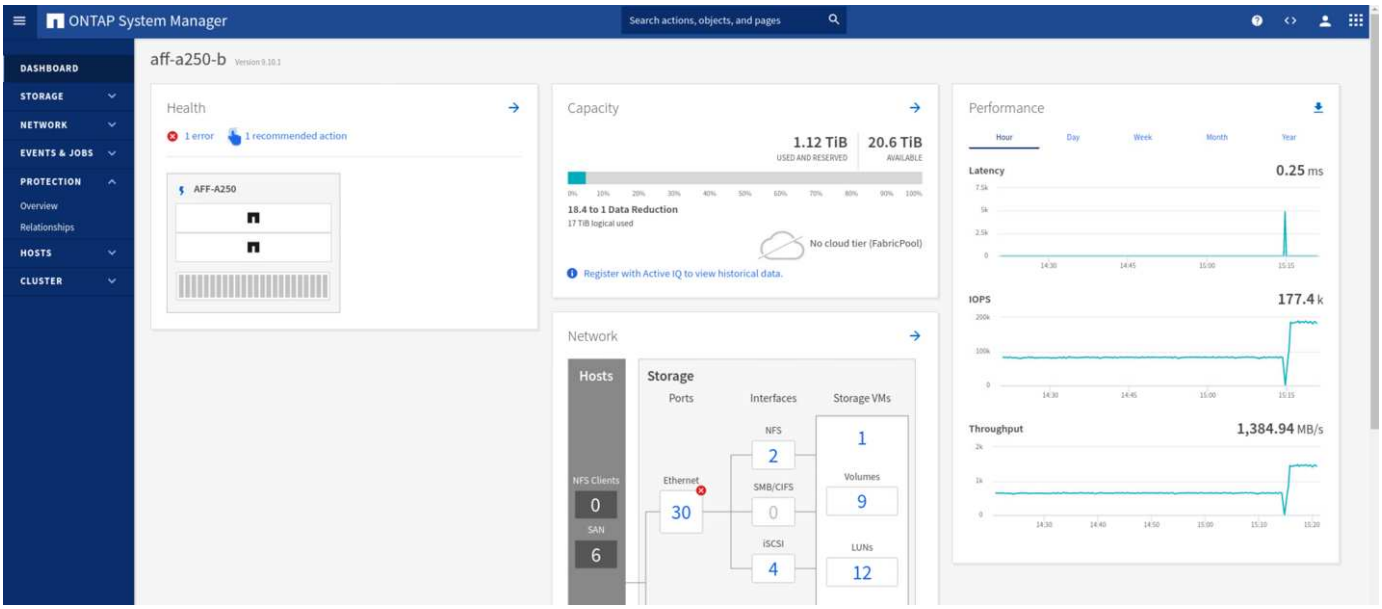
Durante las pruebas de validación, la herramienta de Iometer en los equipos virtuales de ambos sitios genera I/o en sus almacenes de datos locales. Una vez apagado El sitio a un clúster, las operaciones de I/o se pausaron brevemente y, a continuación, se reanudaron. Consulte las dos figuras siguientes para ver los paneles del clúster de almacenamiento en el sitio A y el sitio B respectivamente antes del desastre, que muestran unos 80 000 IOPS y un rendimiento de 600 MB/s en cada centro.



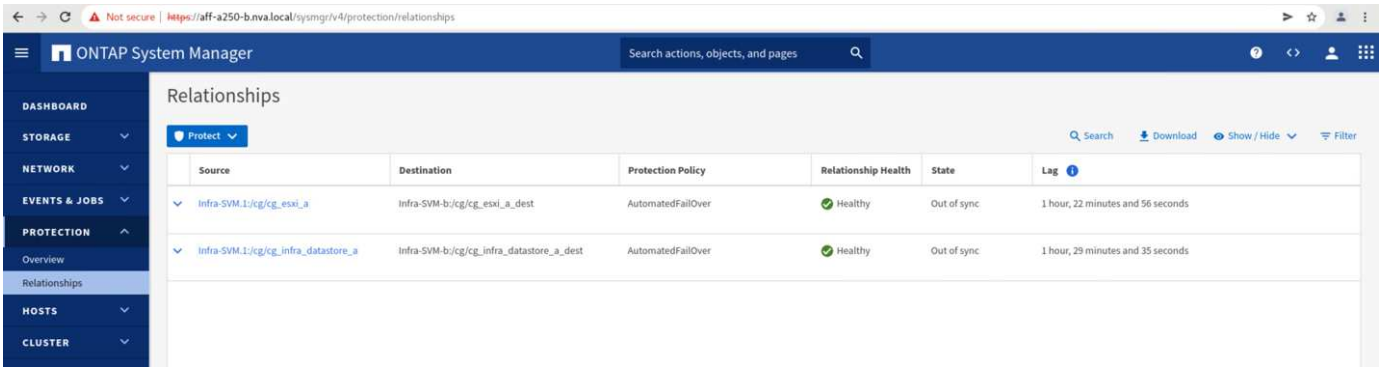


Tras apagar las controladoras de almacenamiento en el sitio A, podemos validar visualmente que las I/o de la controladora de almacenamiento del sitio B aumentaron enormemente para ofrecer servicios de datos adicionales en nombre del sitio A (consulte la siguiente figura). Además, la interfaz gráfica de usuario de los equipos virtuales de Iometer también mostró que la I/o continúa a pesar de la interrupción del servicio en el

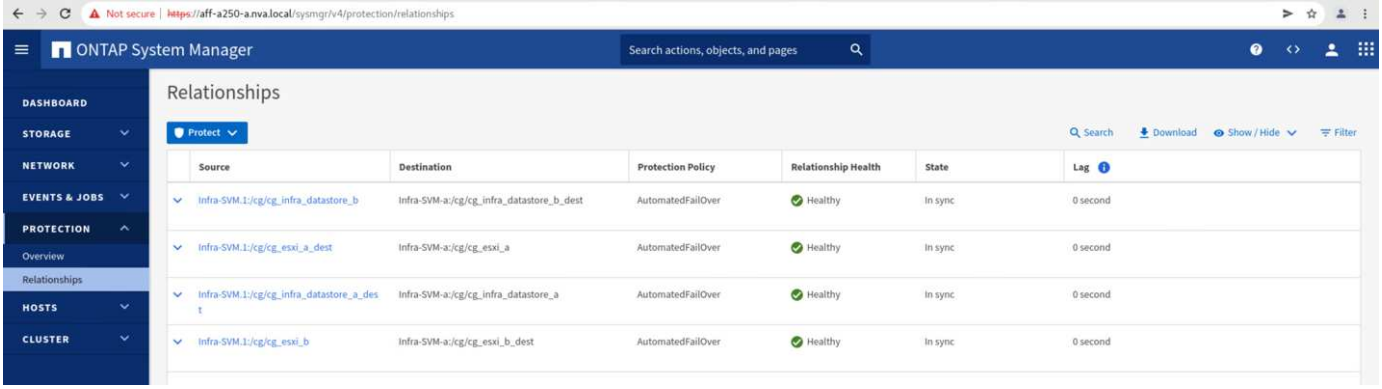
clúster De almacenamiento del sitio. Tenga en cuenta que si hay otros almacenes de datos respaldados por LUN no protegidos mediante relaciones SM-BC, dichos almacenes de datos ya no serán accesibles cuando se produzca un desastre de almacenamiento. Por lo tanto, es importante evaluar las necesidades empresariales de los distintos datos de aplicaciones y colocarlos correctamente en almacenes de datos que estén protegidos por relaciones de SM-BC para proporcionar continuidad de negocio.



Mientras el sitio un clúster está inactivo, se muestran las relaciones de los grupos coherentes `Out of sync` estado como se muestra en la siguiente figura. Una vez que se vuelve a encender la alimentación de las controladoras de almacenamiento en el sitio A, el clúster de almacenamiento se arranca y la sincronización de datos entre el sitio A y el sitio B se produce de forma automática.



Antes de devolver los servicios de datos del sitio B al sitio A, debe comprobar el sitio a con System Manager y asegurarse de que las relaciones de SM-BC se han vuelto a sincronizar y que el estado ha vuelto a estar sincronizado. Después de confirmar que los grupos de consistencia están sincronizados, se puede iniciar una operación manual de conmutación por error para devolver los servicios de datos en las relaciones del grupo de consistencia de nuevo al sitio A.



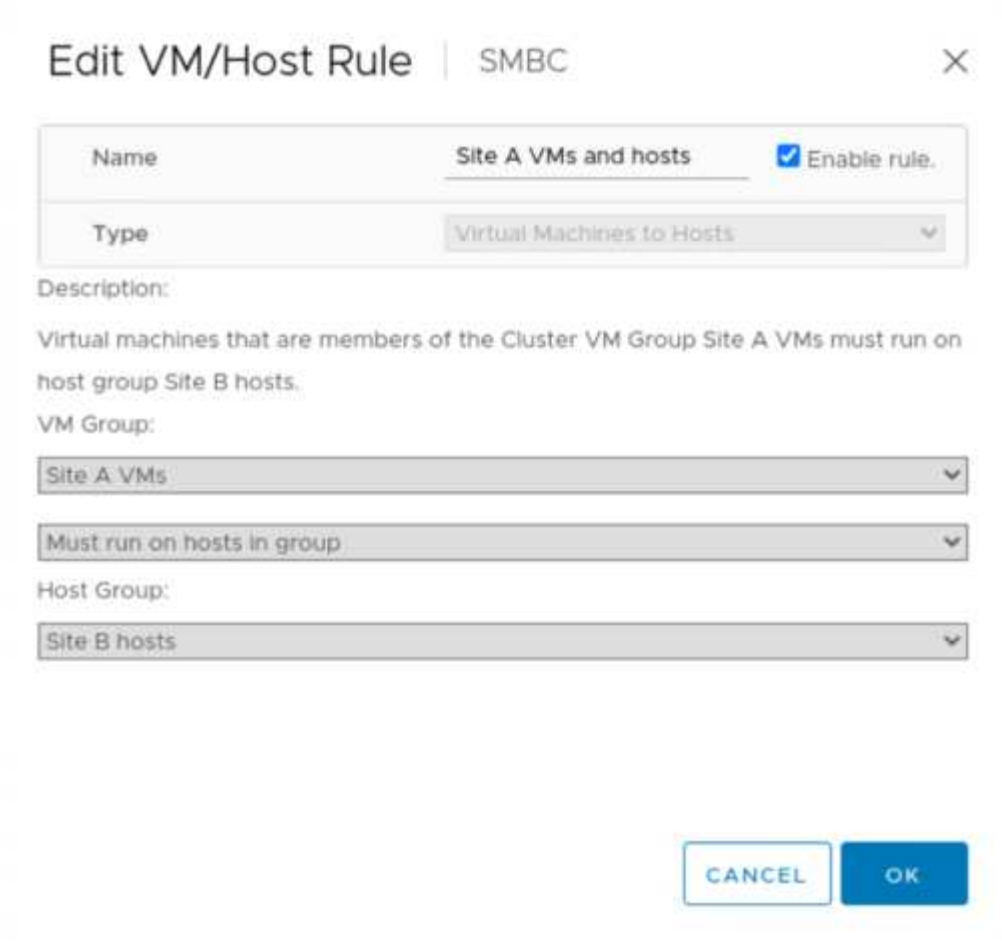
Mantenimiento de sitio completo o errores en el sitio

Un sitio podría necesitar mantenimiento del sitio, experimentar pérdida de energía, o podría ser afectado por un desastre natural como un huracán o un terremoto. Por lo tanto, es crucial que ejercite escenarios de fallos del sitio planificados y no planificados para ayudar a garantizar que su solución FlexPod SM-BC esté correctamente configurada para sobrevivir a estos fallos en todas sus aplicaciones y servicios de datos vitales para el negocio. Se validaron los siguientes escenarios relacionados con el sitio.

- Escenario de mantenimiento planificado del sitio mediante la migración de máquinas virtuales y servicios de datos críticos al otro sitio
- Escenario de interrupción del sitio no planificado apagando servidores y controladoras de almacenamiento para simulación de desastre

Para conseguir que un sitio esté listo para realizar un mantenimiento programado, se necesita una combinación de máquinas virtuales afectadas migradas fuera del sitio con vMotion y una recuperación manual tras fallos de las relaciones de grupos de consistencia de SM-BC para migrar máquinas virtuales y servicios de datos críticos al sitio alternativo. La prueba se realizó en dos pedidos diferentes: VMotion primero seguido de conmutación por error de SM-BC y conmutación por error de SM-BC primero seguido de vMotion, para confirmar que las máquinas virtuales siguen ejecutándose y que los servicios de datos no se interrumpen.

Antes de realizar la migración planificada, actualice la regla de afinidad de equipo virtual/host para que los equipos virtuales que se ejecutan actualmente en el sitio se migren automáticamente fuera del sitio que está experimentando mantenimiento. La siguiente captura de pantalla muestra un ejemplo de cómo modificar el sitio una regla de afinidad de VM/host para que los equipos virtuales migren de la instalación A al sitio B automáticamente. En lugar de especificar que los equipos virtuales ahora deben ejecutarse en el centro B, también puede optar por deshabilitar la regla de afinidad temporalmente para que los equipos virtuales se puedan migrar manualmente.



Después de migrar las máquinas virtuales y los servicios de almacenamiento, puede apagar los servidores, las controladoras de almacenamiento, las bandejas de discos y los switches, y realizar las actividades de mantenimiento del sitio que necesite. Cuando se completa el mantenimiento del sitio y se devuelve la instancia de FlexPod, se puede cambiar la afinidad del grupo de hosts para que los equipos virtuales regresen a su sitio original. Después, debe cambiar la regla de afinidad del sitio VM/host “debe ejecutarse en los hosts del grupo” a “debería ejecutarse en los hosts del grupo”, de modo que se permita que las máquinas virtuales se ejecuten en los hosts del otro sitio en caso de que ocurra un desastre. Para las pruebas de validación, todas las máquinas virtuales se migraron correctamente al otro sitio y los servicios de datos continuaron sin problemas después de realizar una conmutación por error para las relaciones de SM-BC.

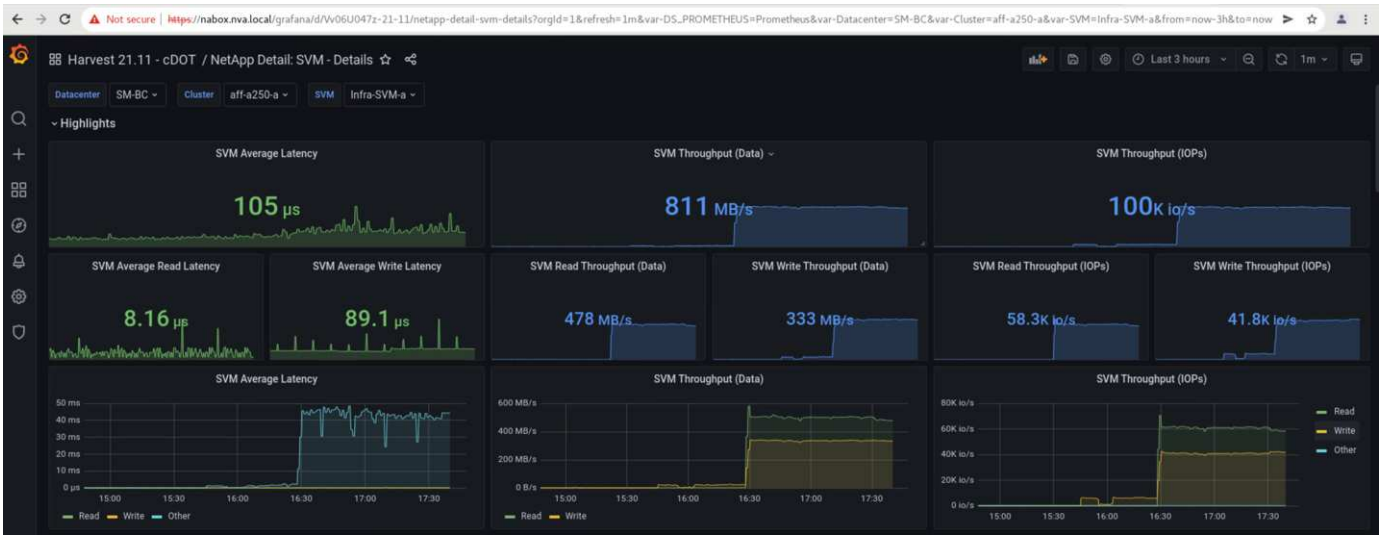
Para la simulación imprevista de desastres del sitio, los servidores y las controladoras de almacenamiento se apagaron para simular un desastre en el sitio. La función de alta disponibilidad de VMware detecta las máquinas virtuales caídos y reinicia esas máquinas virtuales en el sitio superviviente. Además, el Mediador de ONTAP que se ejecuta en un tercer sitio detecta el fallo del sitio y el sitio superviviente inicia una conmutación por error y comienza a proporcionar servicios de datos para el centro según lo esperado.

La siguiente captura de pantalla muestra que la CLI del procesador de servicio de los controladores de almacenamiento se utilizó para apagar el sitio un clúster de forma abrupta para simular un desastre de almacenamiento en el sitio.

```
[BMC aff-a250-a-01>
[BMC aff-a250-a-01>
[BMC aff-a250-a-01>
[BMC aff-a250-a-01>system power off
 Chassis Power Control: Down/Off
 BMC aff-a250-a-01>
```

```
[BMC aff-a250-a-02>
[BMC aff-a250-a-02>
[BMC aff-a250-a-02>
[BMC aff-a250-a-02>system power off
 Chassis Power Control: Down/Off
 BMC aff-a250-a-02>
```

Los paneles de la máquina virtual de almacenamiento de los clústeres de almacenamiento tal y como capturan la herramienta de recogida de datos Harvest de NetApp y se muestran en la consola de Grafana en la herramienta de supervisión de NAbox se muestran en las dos capturas de pantalla siguientes. Como se puede observar en el lado derecho de los gráficos de IOPS y rendimiento, el clúster del sitio B elige Al clúster Una carga de trabajo de almacenamiento inmediatamente después de que el sitio un clúster deja de funcionar.

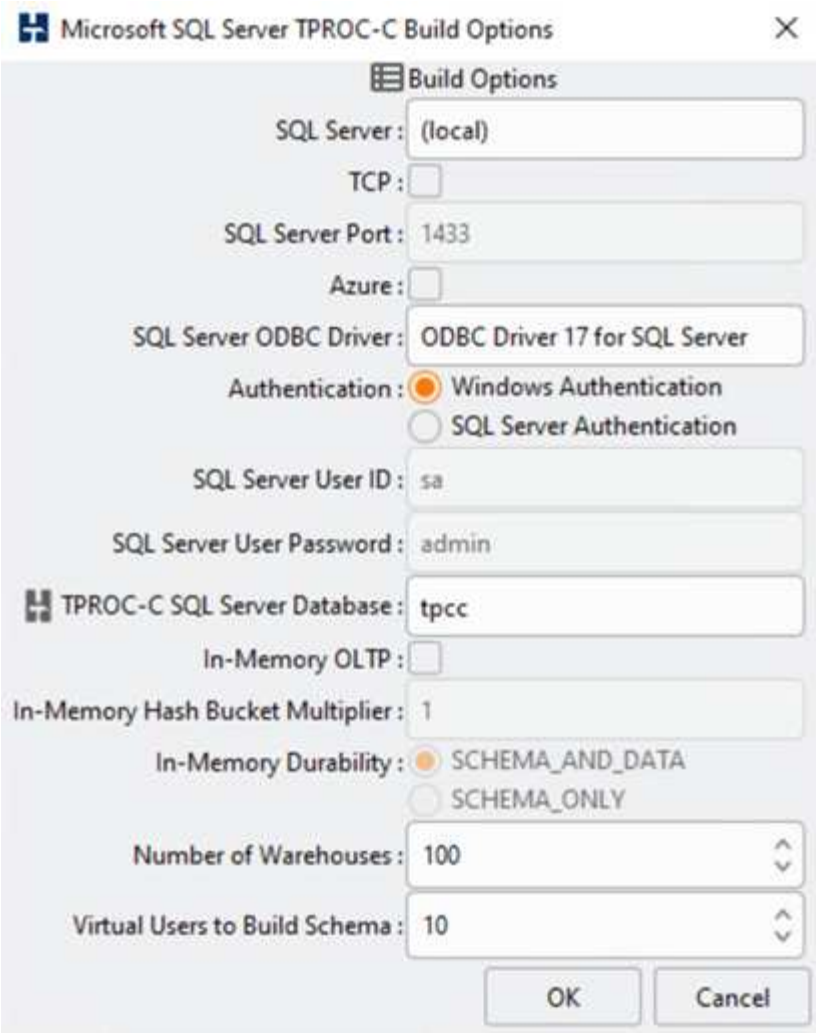


Microsoft SQL Server

Microsoft SQL Server es una plataforma de bases de datos ampliamente adoptada e implementada para LOS departamentos DE TI de las empresas. La versión de Microsoft SQL Server 2019 aporta muchas características y mejoras nuevas a sus motores relacionales y analíticos. Admite cargas de trabajo con aplicaciones que se ejecutan en las instalaciones, en el cloud y en entornos híbridos usando una combinación de ambos. Además, se puede poner en marcha en múltiples plataformas, como Windows, Linux y contenedores.

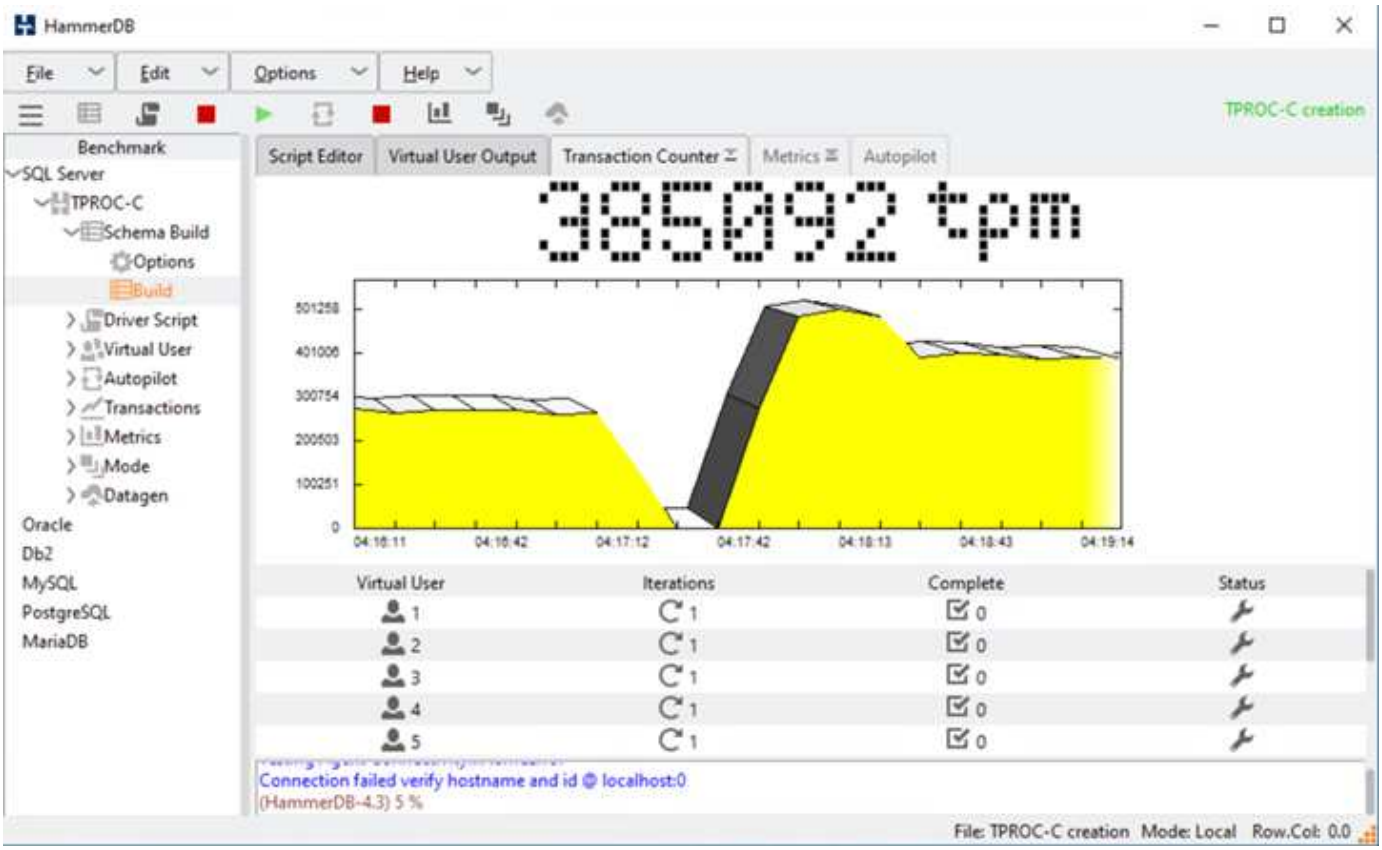
Como parte de la validación de carga de trabajo crítica para el negocio de la solución FlexPod SM-BC, se incluye Microsoft SQL Server 2019 instalado en un equipo virtual de Windows Server 2022 junto con los equipos virtuales de Iometer para pruebas de conmutación al nodo de respaldo del almacenamiento planificadas y no planificadas de SM-BC. En el equipo virtual de Windows Server 2022, SQL Server Management Studio está instalado para administrar SQL Server. Para realizar pruebas, se utiliza la herramienta de base de datos HammerDB para generar transacciones de base de datos.

La herramienta de pruebas de bases de datos de HammerDB se configuró para pruebas con la carga de trabajo TPROC-C de Microsoft SQL Server. Para las configuraciones de creación de esquemas, las opciones se actualizaron para utilizar 100 almacenes con 10 usuarios virtuales, como se muestra en la siguiente captura de pantalla.



Después de actualizar las opciones de creación de esquemas, se inició el proceso de creación de esquemas. Unos minutos más tarde, se introdujo un fallo imprevisto del clúster de almacenamiento del centro B simulado apagando ambos nodos del clúster de almacenamiento A250 de AFF de dos nodos aproximadamente al mismo tiempo mediante los comandos de CLI del procesador del sistema.

Tras una breve pausa de las transacciones de la base de datos, se pateó la conmutación por error automatizada para la corrección de desastre y se reanudaron las transacciones. La siguiente captura de pantalla muestra la captura de pantalla del contador de transacciones de HammerDB en ese momento. Como la base de datos de Microsoft SQL Server normalmente se encuentra en el clúster de almacenamiento del sitio B, la transacción se pausó brevemente cuando el almacenamiento del centro B se interrumpió y, a continuación, se reanudó una vez realizada la conmutación automática al respaldo.



Las medidas del clúster de almacenamiento se obtuvieron utilizando la herramienta NAbox con la herramienta de supervisión Harvest de NetApp instalada. Los resultados se muestran en los paneles predefinidos de Grafana para la máquina virtual de almacenamiento y otros objetos de almacenamiento. El panel proporciona metricas para latencia, rendimiento, IOPS y detalles adicionales con estadísticas de lectura y escritura separadas para el sitio B y el sitio A.

Esta captura de pantalla muestra la consola de rendimiento de NAbox Grafana para el clúster de almacenamiento del sitio B.

La tasa de IOPS del clúster de almacenamiento del sitio B era de aproximadamente 100 000 IOPS antes de que se introdujera el desastre. Luego, las métricas de rendimiento mostraron una caída brusca de cero en el lado derecho de los gráficos debido al desastre. Dado que el cluster de almacenamiento del sitio B estaba

inactivo, no se pudo recopilar nada del cluster del sitio B después de que se introdujera el desastre.

Por otro lado, la tasa de IOPS del sitio que un clúster de almacenamiento recogió las cargas de trabajo adicionales del sitio B después de la conmutación automática al respaldo. La carga de trabajo adicional se puede ver con facilidad en el lado derecho de los gráficos IOPS y rendimiento de la siguiente captura de pantalla, que muestra la consola de rendimiento de NAbox Grafana para ubicar Un clúster de almacenamiento.

El supuesto de prueba de desastre de almacenamiento anterior confirmó que la carga de trabajo de Microsoft SQL Server puede sobrevivir a una interrupción completa del clúster de almacenamiento en el sitio B donde reside la base de datos. La aplicación utilizaba con transparencia los servicios de datos proporcionados por el sitio, un clúster de almacenamiento después de detectar el desastre y de producirse la conmutación por error.

En la capa informática, cuando las máquinas virtuales que se ejecutan en un sitio determinado sufren un fallo del host, las máquinas virtuales están diseñadas para reiniciarse automáticamente con la función de alta disponibilidad de VMware. Para que se produzca una interrupción completa de la tecnología del centro, las reglas de afinidad de VM/host permiten reiniciar los equipos virtuales en el sitio superviviente. Sin embargo, para que una aplicación vital para el negocio proporcione servicios sin interrupciones, se necesita clustering basado en aplicaciones como Microsoft Failover Cluster o la arquitectura de aplicaciones basadas en contenedores de Kubernetes para evitar tiempos de inactividad de las aplicaciones. Consulte el documento pertinente para la implementación de la agrupación en clústeres basada en aplicaciones, que está más allá del alcance de este informe técnico.

"Siguiente: Conclusión."

Conclusión

"Anterior: Validación de la solución - escenarios validados."

El centro de datos FlexPod con SM-BC utiliza un diseño de centro de datos activo-activo para proporcionar continuidad del negocio y recuperación ante desastres para cargas de trabajo vitales para el negocio. Por lo general, la solución interconecta dos centros de datos implementados en ubicaciones separadas y geográficamente dispersas en una zona metropolitana. La solución SM-BC de NetApp utiliza replicación síncrona para proteger los servicios de datos críticos para el negocio frente a un fallo de sitio. La solución requiere que los dos sitios de puesta en marcha de FlexPod tengan una latencia

de red de ida y vuelta inferior a 10 milisegundos.

El Mediador ONTAP de NetApp puesto en marcha en un tercer sitio supervisa la solución SM-BC y permite la conmutación por error automatizada cuando se detecta un desastre en el sitio. La instancia de VMware vCenter con VMware ha y la configuración ampliada de clústeres de almacenamiento Metro de VMware vSphere funcionan sin problemas con el SM-BC de NetApp para permitir que la solución cumpla los objetivos de objetivo de punto de recuperación cero deseados y de objetivo de tiempo de recuperación casi cero.

La solución FlexPod SM-BC también puede ponerse en marcha en infraestructuras FlexPod existentes si cumplen los requisitos o añadiendo una solución FlexPod adicional a un FlexPod existente para alcanzar los objetivos de continuidad del negocio. NetApp y Cisco ofrecen herramientas adicionales de gestión, supervisión y automatización, como Cisco Intersight, Ansible y la automatización basada en HashiCorp Terraform, para que pueda supervisar fácilmente la solución, obtener información sobre sus operaciones y automatizar su puesta en marcha y sus operaciones.

Desde la perspectiva de una aplicación vital para el negocio como Microsoft SQL Server, sigue estando disponible una base de datos que reside en un almacén de datos VMware protegido por una relación de CG de SM-BC de ONTAP a pesar de una interrupción del servicio de almacenamiento del sitio. Tal y como se verificó durante las pruebas de validación, tras una interrupción del suministro eléctrico del clúster de almacenamiento en el que reside la base de datos, se produce una conmutación por error de la relación de CG de SM-BC y las transacciones de Microsoft SQL Server se reanudan sin interrupción de las aplicaciones.

Con la protección de datos granular de aplicaciones, es posible crear las relaciones de CG del SM-BC de ONTAP para sus aplicaciones vitales para el negocio de modo que cumplan con los requisitos de RPO cero y RTO casi cero. Así, que el clúster de VMware en el que se ejecuta la aplicación Microsoft SQL Server puede sobrevivir a una interrupción del almacenamiento del sitio, las LUN de arranque de los hosts ESXi de cada sitio también están protegidas por una relación de CG de SM-BC.

La flexibilidad y la escalabilidad de FlexPod le permite empezar con una infraestructura del tamaño adecuado que puede crecer y evolucionar a medida que cambien los requisitos de su negocio. Este diseño validado le permite poner en marcha de forma fiable un cloud privado basado en vSphere de VMware en una infraestructura distribuida e integrada, por lo que ofrece una solución flexible para numerosos escenarios de un único punto de fallo y fallos en un centro para proteger los servicios de datos empresariales cruciales.

"Siguiente: Dónde encontrar información adicional e historial de versiones."

Dónde encontrar información adicional e historial de versiones

"Anterior: Conclusión."

Si quiere más información sobre el contenido de este documento, consulte los siguientes documentos o sitios web:

FlexPod

- Página de inicio de FlexPod

  "https://www.flexpod.com"

- Guías de puesta en marcha y diseño validado por Cisco para FlexPod

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-

guides.html"

- Servidores Cisco - sistema de computación unificada (UCS)

  "https://www.cisco.com/c/en/us/products/servers-unified-computing/index.html"

- Documentación de productos de NetApp

  "https://www.netapp.com/support-and-training/documentation/"

- Guía de diseño de FlexPod Datacenter con Cisco UCS 4.2(1) en UCS Managed Mode, VMware vSphere 7.0 U2 y NetApp ONTAP 9.9

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2_design.html"

- Guía de puesta en marcha de FlexPod Datacenter con Cisco UCS 4.2(1) en UCS Managed Mode, VMware vSphere 7.0 U2 y NetApp ONTAP 9.9

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2.html"

- Guía de diseño de FlexPod Datacenter con Cisco UCS X-Series, VMware 7.0 U2 y NetApp ONTAP 9.9

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_esxi7u2_design.html"

- Guía de puesta en marcha de FlexPod Datacenter con Cisco UCS X-Series, VMware 7.0 U2 y NetApp ONTAP 9.9

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmware_7u2.html"

- Guía de diseño de FlexPod Express para VMware vSphere 7.0 con Cisco UCS Mini y AFF/FAS NVA de NetApp

  https://www.netapp.com/pdf.html?item=/media/22621-nva-1154-DESIGN.pdf

- Guía de puesta en marcha de FlexPod Express para VMware vSphere 7.0 con Cisco UCS Mini y AFF/FAS NVA de NetApp

  https://www.netapp.com/pdf.html?item=/media/21938-nva-1154-DEPLOY.pdf

- FlexPod MetroCluster IP con estructura de interfaz multisitio VXLAN

  "https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/flexpod-metrocluster-ip-vxlan-multi-site-wp.pdf"

- NAbox

  "https://nabox.org"

- Cosecha de NetApp

  "https://github.com/NetApp/harvest/releases"

SM-BC

- SM-BC

  "https://docs.netapp.com/us-en/ontap/smbc/index.html"

- TR-4878: Continuidad del negocio de SnapMirror (SM-BC) ONTAP 9.8

  https://www.netapp.com/pdf.html?item=/media/21888-tr-4878.pdf

- Cómo eliminar correctamente una relación de SnapMirror con ONTAP 9

  "https://kb.netapp.com/Advice_and_Troubleshooting/Data_Protection_and_Security/SnapMirror/How_to_correctly_delete_a_SnapMirror_relationship_ONTAP_9"

- Conceptos básicos de la recuperación ante desastres de SnapMirror Synchronous

  "https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-synchronous-disaster-recovery-basics-concept.html"

- Conceptos básicos de la recuperación ante desastres de SnapMirror asíncrono

  "https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-disaster-recovery-concept.html#data-protection-relationships"

- Protección de datos y recuperación ante desastres

  "https://docs.netapp.com/us-en/ontap/data-protection-disaster-recovery/index.html"

- Instale o actualice el servicio Mediator de ONTAP

  "https://docs.netapp.com/us-en/ontap/mediator/index.html"

VMware vSphere ha y vSphere Metro Storage Cluster

- Crear y usar clústeres de vSphere ha

  "https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-5432CA24-14F1-44E3-87FB-61D937831CF6.html"

- VMware vSphere Metro Storage Cluster (VMSC)

  "https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-vmsc"

- Prácticas recomendadas para VMware vSphere Metro Storage Cluster

  "https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-recommended-practices"

- ONTAP de NetApp con la continuidad empresarial de SnapMirror de NetApp (SM-BC) con VMware vSphere Metro Storage Cluster (VMSC). (83370)

  "https://kb.vmware.com/s/article/83370"

- Proteja aplicaciones y bases de datos de nivel 1 con el clúster de almacenamiento Metro de VMware vSphere y ONTAP

"https://community.netapp.com/t5/Tech-ONTAP-Blogs/Protect-tier-1-applications-and-databases-with-VMware-vSphere-Metro-Storage/ba-p/171636"

Microsoft SQL y HammerDB

- Microsoft SQL Server 2019

  "https://www.microsoft.com/en-us/sql-server/sql-server-2019"

- Guía de prácticas recomendadas de desarrollo de arquitectura de Microsoft SQL Server en VMware vSphere

  "https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/sql-server-on-vmware-best-practices-guide.pdf"

- Sitio web de HammerDB

  "https://www.hammerdb.com"

Matriz de compatibilidad

- Matriz de compatibilidad de hardware de Cisco UCS

  "https://ucshcltool.cloudapps.cisco.com/public/"

- Herramienta de matriz de interoperabilidad de NetApp

  "https://support.netapp.com/matrix/"

- Hardware Universe de NetApp

  "https://hwu.netapp.com"

- Guía de compatibilidad de VMware

  "http://www.vmware.com/resources/compatibility/search.php"

Historial de versiones

Versión	Fecha	Historial de versiones del documento
Versión 1.0	Abril de 2022	Versión inicial.