



Cloud híbrido de FlexPod con Cloud Volumes ONTAP para Epic FlexPod

NetApp
November 04, 2025

This PDF was generated from <https://docs.netapp.com/es-es/flexpod/hybrid-cloud/fhc-cvoe-solution-overview.html> on November 04, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Cloud híbrido de FlexPod con Cloud Volumes ONTAP para Epic	1
TR-4960: Cloud híbrido de FlexPod con Cloud Volumes ONTAP para Epic	1
Destinatarios	2
Ventajas de la solución	2
Topología de la solución	3
Componentes de la solución	3
FlexPod	4
EHR	4
NetApp Console	4
Agente de consola	5
Cloud Volumes ONTAP de NetApp	5
Active IQ Unified Manager de NetApp	6
Cisco Intersight	6
VMware vSphere 7.0	7
Servidor VMware vCenter	7
Revisiones de hardware y software	7
Instalación y configuración	8
Cloud Volumes ONTAP de NetApp	8
Puesta en marcha de FlexPod en las instalaciones	9
Configuración del almacenamiento ONTAP en las instalaciones	10
Agregue almacenamiento FlexPod local a la NetApp Console	12
Configuración de SAN	12
Kit de utilidades de host de NetApp	12
Descubra el almacenamiento de ONTAP	13
Configure el acceso multivía	13
Cree el volumen físico	15
Crear un grupo de volúmenes	15
Crear un volumen lógico	16
Crear sistema de archivos	16
Crear carpeta para montar	17
Monte el sistema de archivos	17
Generación de datos	17
Configurar la replicación de SnapMirror entre ONTAP en las instalaciones y Cloud Volumes ONTAP	18
Validación de la solución	19
Desarrollo y pruebas de aplicaciones (prueba/desarrollo)	20
Recuperación tras siniestros	23
Verificación de los datos en el lugar de producción	26
Conclusión	28
Dónde encontrar información adicional	28
Historial de versiones	29

Cloud híbrido de FlexPod con Cloud Volumes ONTAP para Epic

TR-4960: Cloud híbrido de FlexPod con Cloud Volumes ONTAP para Epic



En colaboración con:

Kamini Singh, NetApp

La clave para llevar a cabo una transformación digital simplemente consiste en hacer más con los datos. Los hospitales generan y requieren grandes cantidades de datos para dirigir su organización y prestar servicio a sus pacientes con eficacia. La información se recopila y procesa cuando se trata a los pacientes y se gestionan los horarios del personal y los recursos médicos.

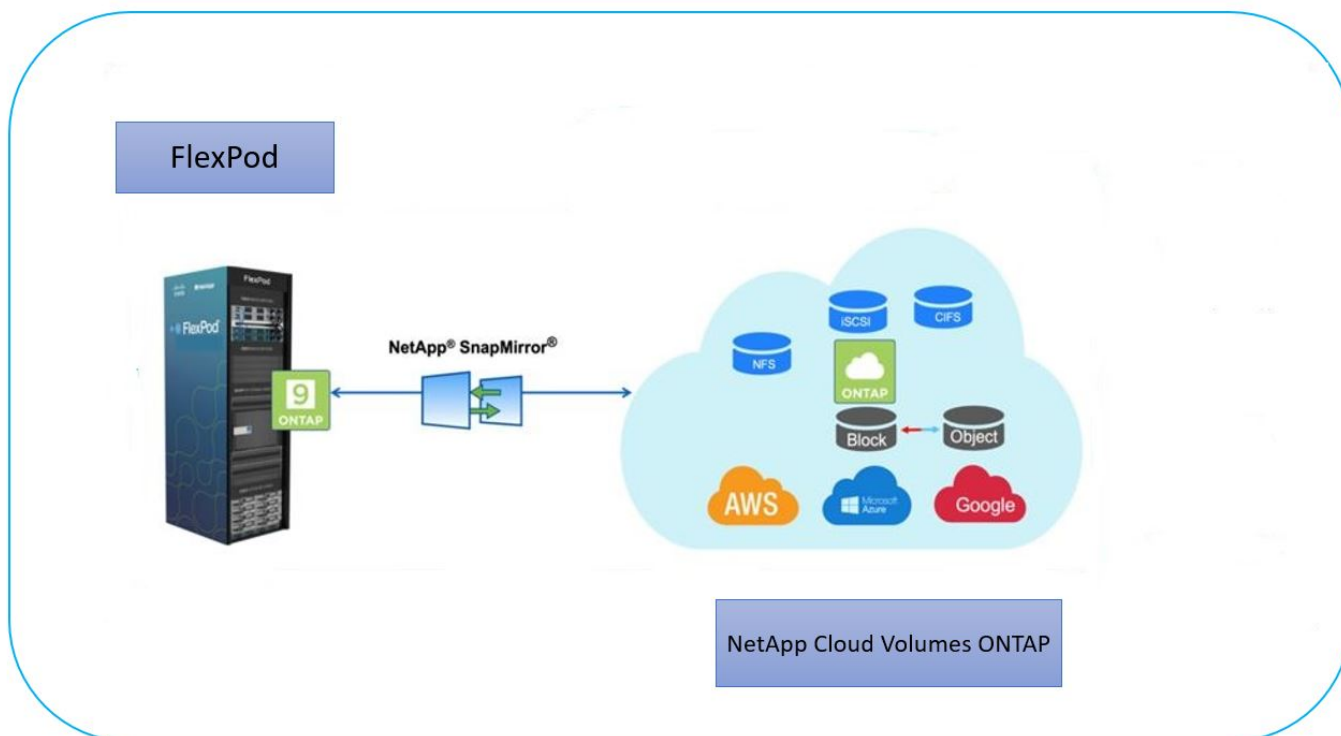
El tamaño cada vez mayor de los datos sanitarios y la valiosa información que estos datos pueden proporcionar hacen que los servicios de datos sanitarios y la protección de datos sean tan cruciales como difíciles. En primer lugar, los datos sanitarios deben estar disponibles y protegidos para cumplir los requisitos de recuperación de datos, continuidad del negocio médico o cumplimiento de normativas.

En segundo lugar, los datos sanitarios deben estar fácilmente disponibles para su análisis. A menudo, este análisis usa enfoques basados en la inteligencia artificial (IA) y el aprendizaje automático (ML) para ayudar a los negocios médicos a mejorar sus soluciones y crear valores empresariales.

En tercer lugar, las infraestructuras de servicios de datos y las metodologías de protección de datos deben adaptarse al crecimiento de los datos del sector sanitario a medida que crece la empresa médica. Además, la movilidad de datos es cada vez más crucial debido a la necesidad de mover datos desde el perímetro en el que se crean al núcleo y al cloud para utilizar los recursos disponibles allí para fines de análisis de datos o archivado.

NetApp ofrece una solución de gestión de datos única para las aplicaciones empresariales, incluido el sector sanitario, y podemos guiar a los hospitales en su viaje hacia la transformación digital. Cloud Volumes ONTAP de NetApp ofrece una solución para la gestión de datos del sector sanitario en la que los datos se pueden replicar de forma eficiente desde un centro de datos de FlexPod a Cloud Volumes ONTAP implementado en un cloud público como AWS.

Al aprovechar los recursos rentables y seguros del cloud público, Cloud Volumes ONTAP mejora la recuperación ante desastres basada en cloud con una replicación de datos muy eficiente, eficiencias de almacenamiento incorporadas y pruebas de recuperación ante desastres sencillas. Estos sistemas se gestionan con el control unificado y la sencillez de arrastrar y soltar, lo que ofrece una protección rentable y a prueba de fallos contra cualquier tipo de error, fallo o desastre. Cloud Volumes ONTAP proporciona la tecnología SnapMirror de NetApp como solución para la replicación de datos a nivel de bloque que mantiene el destino actualizado mediante actualizaciones incrementales.



Destinatarios

Este documento está dirigido a ingenieros de soluciones (se) de NetApp y de partners y personal de servicios profesionales. NetApp asume que el lector tiene los siguientes conocimientos generales:

- Comprensión sólida de los conceptos DE SAN y NAS
- Conocimientos técnicos de los sistemas de almacenamiento ONTAP de NetApp
- Conocimientos técnicos de la configuración y administración del software ONTAP

Ventajas de la solución

El centro de datos FlexPod integrado con Cloud Volumes ONTAP de NetApp ofrece las siguientes ventajas con las cargas de trabajo del sector sanitario:

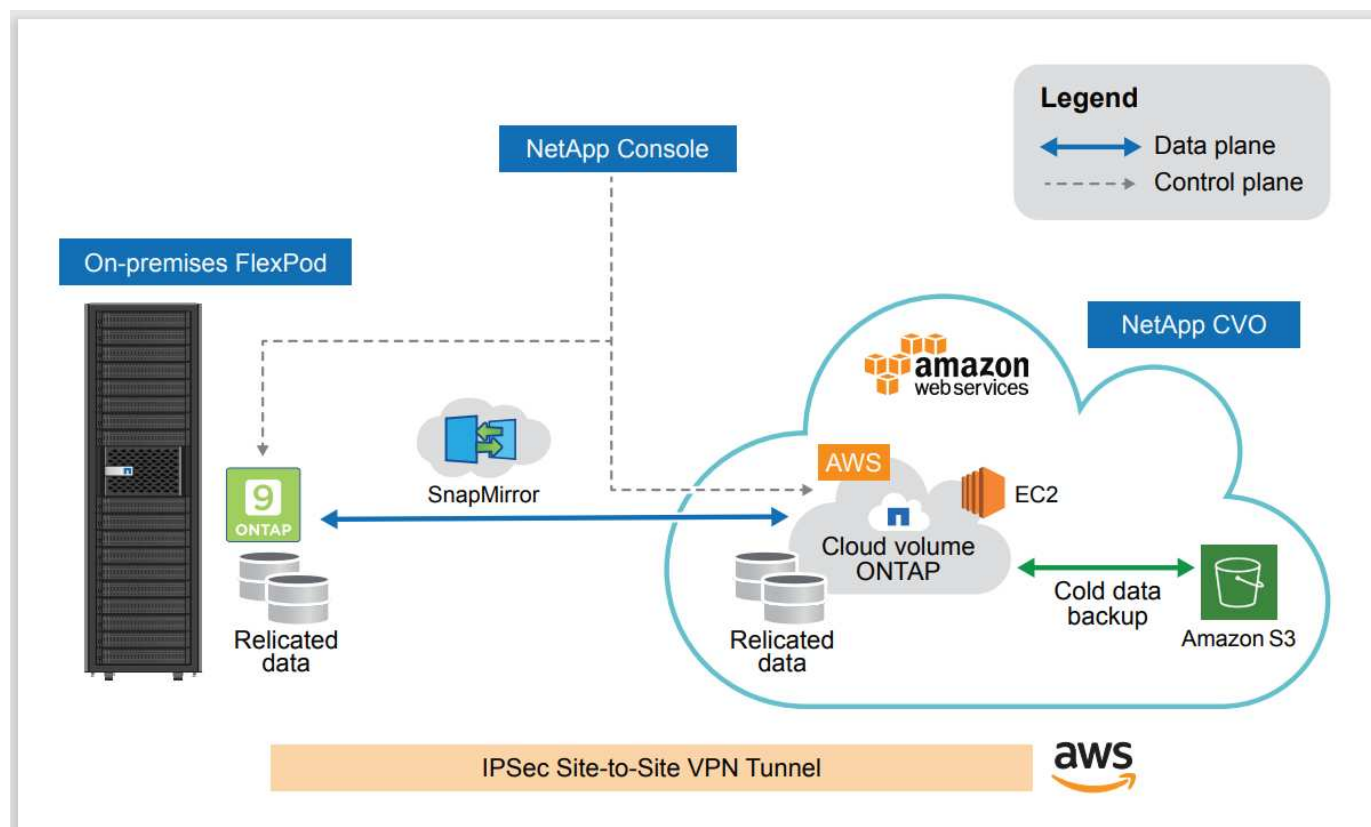
- **Protección personalizada.** Cloud Volumes ONTAP proporciona replicación de datos a nivel de bloque de ONTAP a la nube que mantiene el destino actualizado mediante actualizaciones incrementales. Los usuarios pueden especificar una programación de sincronización para determinar cuándo se transfieren los cambios en el origen. Esto proporciona una protección personalizada para todo tipo de datos sanitarios.
- **Recuperación tras fallos y recuperación tras fallos.** cuando se produce un desastre, los administradores de almacenamiento pueden establecer rápidamente la conmutación por error en los volúmenes en la nube. Cuando se recupera el sitio principal, los datos nuevos creados en el entorno de recuperación ante desastres se vuelven a sincronizar con los volúmenes de origen que permiten restablecer la replicación de datos secundaria. De esta forma, los datos sanitarios se pueden recuperar fácilmente sin interrupciones.
- **Eficiencia.** El espacio de almacenamiento y los costes de la copia secundaria en cloud se optimizan mediante la compresión de datos, el thin provisioning y la deduplicación. Los datos del sector sanitario se transfieren a nivel de bloques de forma comprimida y deduplicado, lo que mejora la velocidad de las transferencias. Los datos también se organizan automáticamente en niveles en un almacenamiento de

objetos de bajo coste y solo se vuelven a almacenamiento de alto rendimiento cuando se accede a ellos, como en un escenario de recuperación ante desastres. De este modo, se reducen significativamente los costes de almacenamiento actuales.

- **Protección contra ransomware.** La protección contra ransomware de NetApp Console analiza las fuentes de datos en entornos locales y en la nube, detecta vulnerabilidades de seguridad y proporciona su estado de seguridad actual y una puntuación de riesgo. A continuación, proporciona recomendaciones prácticas que puede investigar más a fondo y seguir para solucionar el problema. Esto le permite proteger sus datos críticos de atención médica de los ataques de ransomware.

Topología de la solución

Esta sección describe la topología lógica de la solución. La siguiente figura representa la topología de la solución compuesta por el entorno local de FlexPod , NetApp Cloud Volumes ONTAP (CVO) que se ejecuta en Amazon Web Services (AWS) y la plataforma SaaS NetApp Console .



Los planos de control y los planos de datos se indican claramente entre los puntos finales. El plano de datos se ejecuta entre la instancia de ONTAP que se ejecuta en FAS All-Flash en FlexPod y la instancia de CVO de NetApp en AWS mediante una conexión VPN segura de sitio a sitio. La replicación de datos de cargas de trabajo de sanidad desde el centro de datos FlexPod en las instalaciones a Cloud Volumes ONTAP de NetApp se realiza mediante la replicación de SnapMirror de NetApp. Esta solución también admite un backup opcional y una organización en niveles de los datos inactivos que residen en la instancia de CVO de NetApp en AWS S3.

"Siguiente: Componentes de la solución."

Componentes de la solución

"Anterior: Descripción general de la solución."

FlexPod

FlexPod es un conjunto definido de elementos de hardware y software que forma una base integrada para soluciones virtualizadas y no virtualizadas. FlexPod incluye el almacenamiento ONTAP de NetApp, las redes de Cisco Nexus, la red de almacenamiento de Cisco MDS y Cisco Unified Computing System (Cisco UCS).

Las organizaciones sanitarias buscan una solución que facilite su transformación digital y mejore las experiencias y los resultados de los pacientes. Con FlexPod, obtiene una plataforma segura y escalable que aumenta la eficiencia y permite a su personal tomar decisiones más informadas con mayor rapidez para que puedan brindar una mejor atención al paciente.

FlexPod es la plataforma ideal para las necesidades de cargas de trabajo del sector sanitario porque ofrece los siguientes beneficios:

- Optimización de las operaciones para obtener información más rápida y mejores resultados para los pacientes.
- Agilización de las aplicaciones de imágenes con una infraestructura escalable y fiable.
- Puesta en marcha rápida y eficiente con un enfoque demostrado para aplicaciones específicas de sanidad como EHR.

EHR

Electronic Health Records (EHR) fabrica software para grupos médicos de tamaño medio y grande, hospitales y organizaciones sanitarias integradas. Los clientes también incluyen hospitales comunitarios, instalaciones académicas, organizaciones infantiles, proveedores de redes de seguridad y sistemas multihospitalarios. El software integrado en EHR incluye funciones clínicas, de acceso y de ingresos, y se extiende hasta el hogar.

Las organizaciones sanitarias siguen estando presionadas para optimizar las ventajas de sus importantes inversiones en EHR líderes del sector. Cuando los clientes diseñan sus centros de datos para soluciones EHR y aplicaciones de misión crítica, a menudo identifican los siguientes objetivos para su arquitectura de centro de datos:

- Alta disponibilidad de las aplicaciones EHR
- Altas prestaciones
- Facilidad de implementación de EHR en el centro de datos
- Agilidad y escalabilidad para hacer posible el crecimiento con nuevas aplicaciones o lanzamientos de EHR
- Rentabilidad
- Facilidad de administración, estabilidad y soporte
- Sólida protección de datos, backup, recuperación y continuidad del negocio

FlexPod cuenta con la certificación EHR y es compatible con una plataforma que incluye Cisco UCS con procesadores Intel Xeon, Red Hat Enterprise Linux (RHEL) y Cisco con VMware ESXi. Esta plataforma, junto con la alta calificación de nivel de comodidad de EHR para el almacenamiento NetApp que ejecuta ONTAP, le permite ejecutar sus aplicaciones de atención médica en una nube privada totalmente administrada a través de FlexPod , que también se puede conectar a cualquiera de los proveedores de nube pública.

NetApp Console

NetApp Console es una plataforma de gestión empresarial basada en SaaS que permite a los expertos en TI y a los arquitectos de la nube gestionar de forma centralizada su infraestructura híbrida multi-nube utilizando las soluciones en la nube de NetApp . Proporciona un sistema centralizado para visualizar y gestionar su

almacenamiento local y en la nube, compatible con entornos híbridos, múltiples proveedores de nube y cuentas. Para obtener más información, consulte ["Documentación de la NetApp Console"](#).

Agente de consola

Una instancia de agente de consola permite a la consola gestionar recursos y procesos dentro de un entorno de nube pública. Para muchas de las funciones que ofrece la consola se requiere un agente de consola, que puede implementarse en la nube o en la red local.

Un agente de consola es compatible con las siguientes ubicaciones:

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- En el entorno local

["Obtenga más información sobre los agentes de consola"](#).

Cloud Volumes ONTAP de NetApp

Cloud Volumes ONTAP de NetApp es una oferta de almacenamiento definido por software que ejecuta el software de gestión de datos ONTAP en el cloud para proporcionar gestión de datos avanzada para cargas de trabajo de archivos y bloques. Con Cloud Volumes ONTAP, puede optimizar los costes de almacenamiento en cloud y aumentar el rendimiento de las aplicaciones a la vez que mejora la protección de datos, la seguridad y el cumplimiento de normativas.

Entre las ventajas clave se incluyen las siguientes:

- **Eficiencia del almacenamiento.** Aproveche la deduplicación de datos integrada, la compresión de datos, el thin provisioning y la clonación instantánea para minimizar los costes de almacenamiento.
- **Alta disponibilidad.** proporcione fiabilidad empresarial y operaciones continuas en caso de fallos en su entorno de nube.
- **Protección de datos.** Cloud Volumes ONTAP utiliza SnapMirror, la tecnología de replicación de NetApp líder en el sector, para replicar datos en las instalaciones al cloud de forma que sea fácil disponer de copias secundarias para diversos casos de uso. Cloud Volumes ONTAP también se integra con Cloud Backup para proporcionar funcionalidades de backup y restauración para la protección, y archivado a largo plazo de sus datos en el cloud.
- **Niveles de datos.** cambie entre grupos de almacenamiento de alto y bajo rendimiento bajo demanda sin desconectar las aplicaciones.
- **Consistencia de las aplicaciones.** consistencia de las copias Snapshot de NetApp mediante la tecnología SnapCenter de NetApp.
- **Seguridad de datos.** Cloud Volumes ONTAP es compatible con el cifrado de datos y proporciona protección contra virus y ransomware.
- **Controles de cumplimiento de la privacidad.** la integración con Cloud Data Sense le ayuda a comprender el contexto de los datos e identificar datos confidenciales.

Para obtener información más detallada, consulte ["Cloud Volumes ONTAP"](#) .

Active IQ Unified Manager de NetApp

Active IQ Unified Manager de NetApp permite supervisar sus clústeres de almacenamiento de ONTAP desde una única interfaz intuitiva, rediseñada que proporciona inteligencia a partir de los conocimientos de la comunidad y los análisis de IA. Proporciona información exhaustiva sobre operaciones, rendimiento y proactiva del entorno de almacenamiento y las máquinas virtuales que se ejecutan en él. Cuando se produce un problema en la infraestructura de almacenamiento, Unified Manager puede informarle de los detalles del problema para ayudar a identificar la causa raíz. La consola de equipos virtuales le ofrece una vista de las estadísticas de rendimiento de la máquina virtual de manera que puede investigar toda la ruta de I/O desde el host vSphere hasta la red y, finalmente, hasta el almacenamiento.

Algunos eventos también proporcionan acciones correctivas que se pueden tomar para rectificar el problema. Puede configurar alertas personalizadas para los eventos de modo que, cuando se produzcan problemas, se les notifique a través de correo electrónico y capturas SNMP. Active IQ Unified Manager le permite planificar los requisitos de almacenamiento de los usuarios mediante el pronóstico de las tendencias de capacidad y uso para que pueda actuar antes de que surjan problemas, lo que evita decisiones reactivas a corto plazo que puedan provocar problemas adicionales a largo plazo.

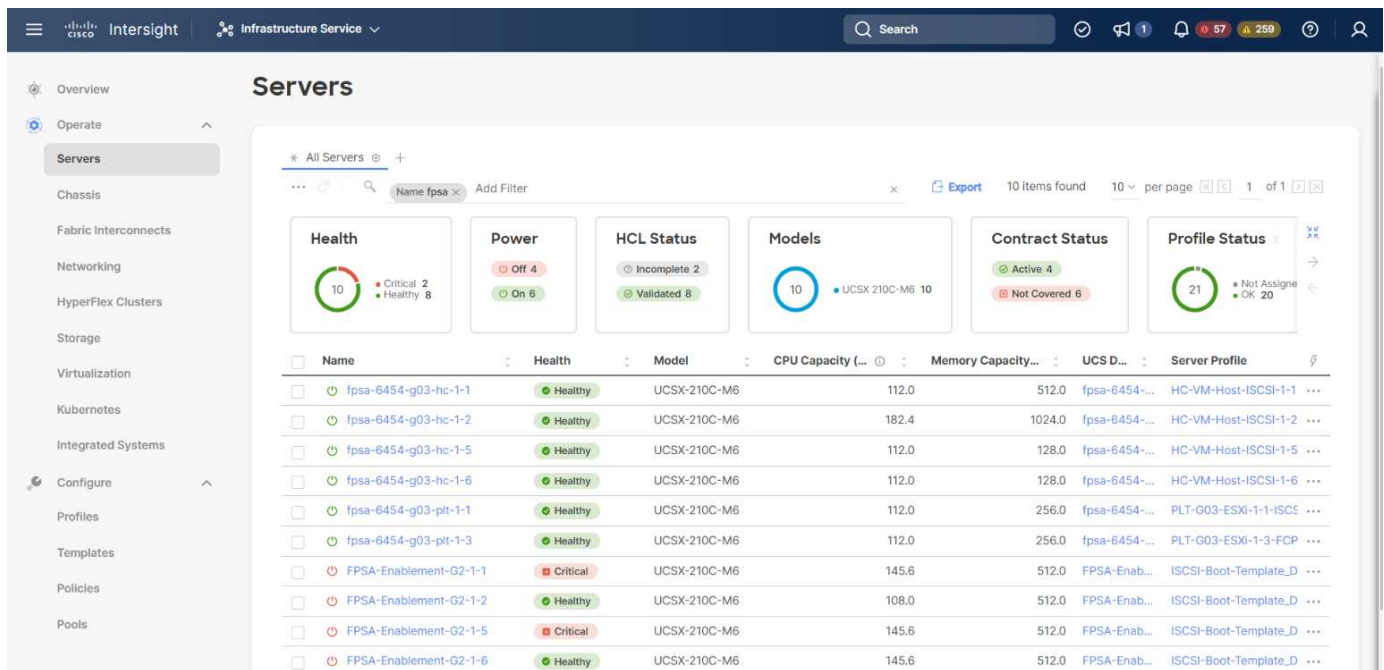
Para obtener más información, consulte ["Active IQ Unified Manager"](#).

Cisco Intersight

Cisco Intersight es una plataforma SaaS que proporciona automatización inteligente, capacidad de observación y optimización para aplicaciones e infraestructuras tradicionales y nativas del cloud. La plataforma ayuda a impulsar el cambio con los equipos DE TECNOLOGÍA y ofrece un modelo operativo diseñado para el cloud híbrido. Cisco Intersight proporciona las siguientes ventajas:

- **Entrega más rápida.** Intersight se entrega como un servicio desde la nube o en el centro de datos del cliente con actualizaciones frecuentes y una innovación continua, gracias a un modelo de desarrollo de software ágil. De esta forma, el cliente puede centrarse en satisfacer las necesidades esenciales del negocio.
- **Operaciones simplificadas.** Intersight simplifica las operaciones utilizando una única herramienta segura suministrada por SaaS con inventario, autenticación y API comunes para funcionar a través de toda la pila y todas las ubicaciones, eliminando así los silos entre equipos. Esto le permite gestionar servidores físicos e hipervisores en las instalaciones, a equipos virtuales, K8s, sin servidor, automatización optimización y control de costes, tanto en las instalaciones como en los clouds públicos.
- *** Optimización continua.*** puede optimizar continuamente su entorno utilizando la inteligencia proporcionada por Cisco Intersight en cada capa, así como por Cisco TAC. Esta inteligencia se convierte en acciones recomendadas y automatizables para que usted pueda adaptarse en tiempo real a cualquier cambio: Desde mover cargas de trabajo y supervisar el estado de los servidores físicos a recomendaciones de reducción de costes para los clouds públicos con los que trabaja.

Intersight de Cisco dispone de dos modos de operaciones de gestión: Modo gestionado UCSM (UMM) y modo gestionado de Intersight (IMM). Puede seleccionar el modo gestionado nativo UCSM (UMM) o el modo gestionado de Intersight (IMM) para sistemas Cisco UCS conectados a la estructura durante la configuración inicial de las interconexiones de estructura. En esta solución, se utiliza IMM nativa. La siguiente figura muestra el panel de Cisco Intersight.



VMware vSphere 7.0

VMware vSphere es una plataforma de virtualización para gestionar de forma integral grandes conjuntos de infraestructuras (incluidas CPU, almacenamiento y redes) como un entorno operativo fluido, versátil y dinámico. A diferencia de los sistemas operativos tradicionales que gestionan una máquina individual, VMware vSphere agrega la infraestructura de todo un centro de datos para crear un único centro de datos con recursos que se pueden asignar de forma rápida y dinámica a cualquier aplicación que lo necesite.

Para obtener más información sobre VMware vSphere y sus componentes, consulte ["vSphere de VMware"](#).

Servidor VMware vCenter

VMware vCenter Server proporciona una gestión unificada de todos los hosts y equipos virtuales desde una única consola y agrega la supervisión del rendimiento de clústeres, hosts y equipos virtuales. VMware vCenter Server proporciona a los administradores una información exhaustiva sobre el estado y la configuración de clústeres de computación, hosts, máquinas virtuales, almacenamiento, el sistema operativo invitado, y otros componentes críticos de una infraestructura virtual. VMware vCenter gestiona el conjunto completo de funciones disponibles en un entorno VMware vSphere.

Para obtener información detallada, consulte ["VMware vCenter"](#).

Revisiones de hardware y software

Esta solución de nube híbrida se puede extender a cualquier entorno FlexPod que ejecute versiones compatibles de software, firmware y hardware, tal como se define en el documento ["Herramienta de matriz de interoperabilidad de NetApp"](#), ["Compatibilidad de hardware y software de UCS"](#), y ["Guía de compatibilidad de VMware"](#).

La siguiente tabla muestra las revisiones de software y hardware de FlexPod en las instalaciones.

Componente	Producto	Versión
Informática	Cisco UCS X210c M6	5.0(1b)

Componente	Producto	Versión
	Interconexiones de estructura Cisco UCS 6454	4.2(2a)
Red	Cisco Nexus 9336C-FX2 NX-OS	9.3(9)
Reducida	AFF A400 de NetApp	ONTAP 9.11.1P2
	Herramientas de ONTAP de NetApp para VMware vSphere	9.11
	Plugin NFS de NetApp para VAAI de VMware	2.0
	Active IQ Unified Manager de NetApp	9.11P1
De NetApp	VSphere de VMware	7.0(U3)
	Controlador Ethernet nenic VMware ESXi	1.0.35.0
	Dispositivo VMware vCenter	7.0.3
	Dispositivo virtual Cisco Intersight Assist	1.0.9-342

La siguiente tabla muestra las versiones de Cloud Volumes ONTAP .

Proveedor	Producto	Versión
NetApp	Consola	3.9.24
	Cloud Volumes ONTAP	ONTAP 9.11

["Siguiente: Instalación y configuración."](#)

Instalación y configuración

["Anterior: Componentes de la solución."](#)

Cloud Volumes ONTAP de NetApp

Complete los pasos siguientes para configurar la instancia de Cloud Volumes ONTAP:

1. Preparar el entorno de proveedor de servicios de cloud público.

Debe capturar los detalles del entorno de su proveedor de servicios de cloud público para la configuración de la solución. Por ejemplo, para la preparación del entorno de Amazon Web Services (AWS), necesita la clave de acceso de AWS, la clave secreta de AWS y otros detalles de red como región, VPC, subred, etc.

2. Configure la puerta de enlace del extremo VPC.

Se requiere una puerta de enlace de extremo de VPC para habilitar la conexión entre el VPC y el servicio de AWS S3. Se utiliza para habilitar la copia de seguridad en CVO, un extremo con el tipo de puerta de enlace.

3. Acceda a la NetApp Console.

Para acceder a la consola y otros servicios en la nube, debe registrarse en ["NetApp Console"](#) . Para configurar espacios de trabajo y usuarios en la cuenta de la consola, consulte ["Configuración y administración de la NetApp Console"](#) . Necesitas una cuenta que tenga permiso para implementar el agente de la consola en tu proveedor de nube directamente desde la consola. Para obtener los permisos que necesita, consulte ["Resumen de permisos para la NetApp Console"](#) .

4. Implementar agente de consola.

Antes de agregar un sistema Cloud Volume ONTAP , debe implementar un agente de consola. La consola le avisará si intenta crear su primer sistema Cloud Volumes ONTAP sin un agente de consola instalado. Para implementar un agente de consola en AWS desde la consola, consulte la ["Opciones de instalación del agente de consola en AWS"](#) .

5. Inicie Cloud Volumes ONTAP en AWS.

Puede iniciar Cloud Volumes ONTAP en una configuración con un único sistema o como par de alta disponibilidad en AWS. ["Lea las instrucciones paso a paso"](#).

Para obtener información detallada sobre estos pasos, consulte ["Guía de inicio rápido para Cloud Volumes ONTAP en AWS"](#).

En esta solución, hemos implementado un sistema Cloud Volumes ONTAP de un solo nodo en AWS.

Puesta en marcha de FlexPod en las instalaciones

Para comprender los detalles sobre el diseño de FlexPod con UCS X-Series, VMware y ONTAP de NetApp, consulte ["Centro de datos FlexPod con Cisco UCS X-Series"](#) guía de diseño. Este documento proporciona directrices de diseño para incorporar la plataforma Cisco Intersight-Series gestionada UCS X-Series en la infraestructura de centro de datos FlexPod.

Para implementar la instancia de FlexPod en las instalaciones, consulte ["esta guía de implementación"](#).

Este documento proporciona directrices de puesta en marcha para incorporar la plataforma Cisco Intersight-Series gestionada por UCS X-Series en una infraestructura de centro de datos FlexPod. El documento abarca tanto las configuraciones como las mejores prácticas para una correcta puesta en marcha.

FlexPod se puede implementar tanto en UCS Managed Mode como en Cisco Intersight Managed Mode (IMM). Si va a implementar FlexPod en UCS Managed Mode, consulte este tema ["guía de diseño"](#) y esto ["guía de puesta en marcha"](#).

La puesta en marcha de FlexPod se puede automatizar con Infraestructura como código con Ansible. A continuación puede ver los enlaces a los repositorios de GitHub para una puesta en marcha completa de FlexPod:

- Podemos ver la configuración de Ansible de FlexPod con Cisco UCS en el modo gestionado de UCS, ONTAP de NetApp y VMware vSphere ["aquí"](#).
- Podrá ver la configuración de Ansible de FlexPod con Cisco UCS en IMM, ONTAP de NetApp y VMware vSphere ["aquí"](#).

Configuración del almacenamiento ONTAP en las instalaciones

En esta sección se describen algunos de los pasos importantes para la configuración de ONTAP específicos de esta solución.

1. Configure una SVM con el servicio iSCSI en ejecución.

```
1. vserver create -vserver Healthcare_SVM -rootvolume
Healthcare_SVM_root -aggregate aggr1_A400_G0312_01 -rootvolume-security
-style unix
2. vserver add-protocols -vserver Healthcare_SVM -protocols iscsi
3. vserver iscsi create -vserver Healthcare_SVM
```

To verify:

```
A400-G0312::> vserver iscsi show -vserver Healthcare_SVM
Vserver: Healthcare_SVM
Target Name:
iqn.1992-08.com.netapp:sn.1fbf00f438c111ed866cd039ea91fb56:vs.3
Target Alias: Healthcare_SVM
Administrative Status: up
```

Si no se instaló la licencia iSCSI durante la configuración del clúster, asegúrese de instalar la licencia antes de crear el servicio iSCSI.

2. Cree un volumen de FlexVol.

```
1. volume create -vserver Healthcare_SVM -volume hc_iscsi_vol -aggregate
aggr1_A400_G0312_01 -size 500GB -state online -policy default -space
guarantee none
```

3. Añada interfaces para el acceso iSCSI.

```

1. network interface create -vserver Healthcare_SVM -lif iscsi-lif-01a
   -service-policy default-data-iscsi -home-node <st-node01> -home-port
   a0a-<infra-iscsi-a-vlan-id> -address <st-node01-infra-iscsi-a-ip>
   -netmask <infra-iscsi-a-mask> -status-admin up
2. network interface create -vserver Healthcare_SVM -lif iscsi-lif-01b
   -service-policy default-data-iscsi -home-node <st-node01> -home-port
   a0a-<infra-iscsi-b-vlan-id> -address <st-node01-infra-iscsi-b-ip>
   -netmask <infra-iscsi-b-mask> -status-admin up
3. network interface create -vserver Healthcare_SVM -lif iscsi-lif-02a
   -service-policy default-data-iscsi -home-node <st-node02> -home-port
   a0a-<infra-iscsi-a-vlan-id> -address <st-node02-infra-iscsi-a-ip>
   -netmask <infra-iscsi-a-mask> -status-admin up
4. network interface create -vserver Healthcare_SVM -lif iscsi-lif-02b
   -service-policy default-data-iscsi -home-node <st-node02> -home-port
   a0a-<infra-iscsi-b-vlan-id> -address <st-node02-infra-iscsi-b-ip>
   -netmask <infra-iscsi-b-mask> -status-admin up

```

En esta solución, creamos cuatro interfaces lógicas iSCSI (LIF), dos en cada nodo.

Una vez que la instancia de FlexPod está en funcionamiento con vCenter implementada y todos los hosts ESXi añadidos, debemos poner en marcha una máquina virtual Linux que actúa como un servidor que se conecta y accede al almacenamiento ONTAP de NetApp. En esta solución, hemos instalado una instancia de CentOS 8 en vCenter.

4. Cree una LUN.

```

1. lun create -vserver Healthcare_SVM -path /vol/hc_iscsi_vol/iscsi_lun1
   -size 200GB -ostype linux -space-reserve disabled

```

En el caso de una base de datos operativa EHR (ODB), un diario y cargas de trabajo de aplicaciones, EHR recomienda presentar almacenamiento a los servidores como LUN iSCSI. NetApp también admite el uso de FCP y NVMe/FC si tiene versiones de AIX y los sistemas operativos RHEL que sean compatibles, lo que mejora el rendimiento. FCP y NVMe/FC pueden coexistir en la misma estructura.

5. Cree un igroup.

```

1. igroup create -vserver Healthcare_SVM -igroup ehr -protocol iscsi
   -ostype linux -initiator iqn.1994-05.com.redhat:8e91e9769336

```

Los iGroups se utilizan para permitir el acceso del servidor a las LUN. Para el host Linux, el IQN del servidor se puede encontrar en el archivo `/etc/iscsi/initiatorname.iscsi`.

6. Asigne la LUN al igroup.

```
1. lun mapping create -vserver Healthcare_SVM -path  
/vol/hc_iscsi_vol/iscsi_lun1 -igroup ehr -lun-id 0
```

Agregue almacenamiento FlexPod local a la NetApp Console

Complete los siguientes pasos para agregar su almacenamiento FlexPod al sistema mediante la consola.

1. Desde el menú de navegación, seleccione **Almacenamiento > Sistemas**.
2. En la página Sistemas, haga clic en **Agregar sistema** y seleccione **Local**.
3. Seleccione **On-local ONTAP**. Haga clic en **Siguiente**.
4. En la página ONTAP Cluster Details, introduzca la dirección IP de administración del clúster y la contraseña de la cuenta de usuario de administrador. A continuación, haga clic en **Agregar**.
5. En la página Detalles y credenciales, introduzca un nombre y una descripción para el entorno de trabajo y, a continuación, haga clic en **Ir**.

La consola detecta el clúster ONTAP y lo agrega como sistema en la página Sistemas.

Si quiere más información, consulte la página ["Detectar clústeres de ONTAP en las instalaciones"](#).

["Siguiente: Configuración DE SAN."](#)

Configuración de SAN

["Anterior: Instalación y configuración."](#)

En esta sección, se describe la configuración del host requerida por EHR para permitir que el software se integre mejor con el almacenamiento de NetApp. En este segmento, se trata específicamente de la integración de host para los sistemas operativos Linux. Utilice la ["Herramienta de matriz de interoperabilidad de NetApp \(IMT\)"](#) para validar todas las versiones de software y firmware.



Los siguientes pasos de configuración son específicos del host CentOS 8 que se utilizó en esta solución.

Kit de utilidades de host de NetApp

NetApp recomienda instalar el kit de utilidades de host (Host Utilities) de NetApp en los sistemas operativos de hosts que están conectados a los sistemas de almacenamiento de NetApp y acceden a ellos. Se admite la función de I/O multivía nativa de Microsoft (MPIO). El sistema operativo debe ser compatible con ALUA (acceso asimétrico de unidad lógica) para multivía. La instalación de las utilidades de host configura los ajustes del adaptador de bus de host (HBA) para el almacenamiento de NetApp.

Puede descargar NetApp Host Utilities ["aquí"](#). En esta solución, hemos instalado Linux Host Utilities 7.1 en el host.

```
[root@hc-cloud-secure-1 ~]# rpm -ivh netapp_linux_unified_host_utilities-7-1.x86_64.rpm
```

Descubra el almacenamiento de ONTAP

Asegúrese de que el servicio iSCSI esté en ejecución cuando se supone que se producen los registros. Para establecer el modo de inicio de sesión para un portal específico en un destino o para todos los portales de un destino, utilice `iscsiadm` comando.

```
[root@hc-cloud-secure-1 ~]# rescan-scsi-bus.sh
[root@hc-cloud-secure-1 ~]# iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
[root@hc-cloud-secure-1 ~]# iscsiadm -m node -L all
```

Ahora puede utilizar `sanlun` Para mostrar información sobre las LUN conectadas al host. Asegúrese de que haya iniciado sesión como raíz en el host.

```
[root@hc-cloud-secure-1 ~]# sanlun lun show
controller(7mode/E-Series)/
                                device      host          lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
-----
---
Healthcare_SVM                /dev/sdb host33   iSCSI      200g
cDOT
                                /vol/hc_iscsi_vol/iscsi_lun1

Healthcare_SVM                /dev/sdc host34   iSCSI      200g
cDOT
                                /vol/hc_iscsi_vol/iscsi_lun1
```

Configure el acceso multivía

Device Mapper Multipathing (DM-Multipath) es una utilidad multivía nativa en Linux. Se puede utilizar para la redundancia y para mejorar el rendimiento. Agrega o combina las múltiples rutas de I/O entre los servidores y el almacenamiento, por lo que crea un único dispositivo a nivel de SO.

1. Antes de configurar DM-Multipath en el sistema, asegúrese de que el sistema se haya actualizado e incluya `device-mapper-multipath` paquete.

```
[root@hc-cloud-secure-1 ~]# rpm -qa|grep multipath
device-mapper-multipath-libs-0.8.4-31.el8.x86_64
device-mapper-multipath-0.8.4-31.el8.x86_64
```

2. El archivo de configuración es `/etc/multipath.conf` archivo. Actualice el archivo de configuración como se muestra a continuación.

```
[root@hc-cloud-secure-1 ~]# cat /etc/multipath.conf
defaults {
    path_checker          readsector0
    no_path_retry         fail
}
devices {
    device {
        vendor            "NETAPP  "
        product            "LUN.*"
        no_path_retry      queue
        path_checker        tur
    }
}
```

3. Habilite e inicie los servicios de multivía.

```
[root@hc-cloud-secure-1 ~]# systemctl enable multipathd.service
[root@hc-cloud-secure-1 ~]# systemctl start multipathd.service
```

4. Agregue el módulo de kernel cargable `dm-multipath` y reinicie el servicio multivía. Finalmente, compruebe el estado multivía.

```
[root@hc-cloud-secure-1 ~]# modprobe -v dm-multipath
insmod /lib/modules/4.18.0-408.el8.x86_64/kernel/drivers/md/dm-
multipath.ko.xz

[root@hc-cloud-secure-1 ~]# systemctl restart multipathd.service

[root@hc-cloud-secure-1 ~]# multipath -ll
3600a09803831494c372b545a4d786278 dm-2 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
|+-+ policy='service-time 0' prio=50 status=active
|  `-- 33:0:0:0 sdb 8:16 active ready running
`+-+ policy='service-time 0' prio=10 status=enabled
  `-- 34:0:0:0 sdc 8:32 active ready running
```



Para obtener información detallada sobre estos pasos, consulte ["aquí"](#).

Cree el volumen físico

Utilice la `pvccreate` comando para inicializar un dispositivo de bloques que se usará como volumen físico. La inicialización es análoga al formato de un sistema de archivos.

```
[root@hc-cloud-secure-1 ~]# pvccreate /dev/sdb
Physical volume "/dev/sdb" successfully created.
```

Crear un grupo de volúmenes

Para crear un grupo de volúmenes a partir de uno o más volúmenes físicos, use el `vgcreate` comando. Este comando crea un nuevo grupo de volúmenes por nombre y añade al menos un volumen físico.

```
[root@hc-cloud-secure-1 ~]# vgcreate datavg /dev/sdb
Volume group "datavg" successfully created.
```

La `vgdisplay` el comando se puede usar para mostrar las propiedades del grupo de volúmenes (como el tamaño, las extensiones, la cantidad de volúmenes físicos, etc.) en una forma fija.

```
[root@hc-cloud-secure-1 ~]# vgdisplay datavg
--- Volume group ---
VG Name                datavg
System ID
Format                 lvm2
Metadata Areas         1
Metadata Sequence No   1
VG Access               read/write
VG Status               resizable
MAX LV                 0
Cur LV                0
Open LV                0
Max PV                 0
Cur PV                1
Act PV                 1
VG Size                <200.00 GiB
PE Size                4.00 MiB
Total PE               51199
Alloc PE / Size        0 / 0
Free PE / Size         51199 / <200.00 GiB
VG UUID                C7jmI0-J0SS-Cq91-t6b4-A9xw-nTfi-RXcy28
```

Crear un volumen lógico

Cuando se crea un volumen lógico, se obtiene dicho volumen a partir de un grupo de volúmenes mediante las extensiones libres de los volúmenes físicos que conforman el grupo de volúmenes.

```
[root@hc-cloud-secure-1 ~]# lvcreate -l 100%FREE -n datalv datavg
Logical volume "datalv" created.
```

Este comando crea un volumen lógico llamado `datalv` que utiliza todo el espacio sin asignar en el grupo de volúmenes `datavg`.

Crear sistema de archivos

```
[root@hc-cloud-secure-1 ~]# mkfs.xfs -K /dev/datavg/datalv
meta-data=/dev/datavg/datalv      isize=512    agcount=4, agsize=13106944
blks
        =                        sectsz=4096   attr=2, projid32bit=1
        =                        crc=1          finobt=1, sparse=1, rmapbt=0
        =                        reflink=1       bigtime=0 inobtcount=0
data      =                        bsize=4096   blocks=52427776, imaxpct=25
        =                        sunit=0        swidth=0 blks
naming    =version 2              bsize=4096   ascii-ci=0, ftype=1
log        =internal log          bsize=4096   blocks=25599, version=2
        =                        sectsz=4096   sunit=1 blks, lazy-count=1
realtime  =none                   extsz=4096   blocks=0, rtextents=0
```

Crear carpeta para montar

```
[root@hc-cloud-secure-1 ~]# mkdir /file1
```

Monte el sistema de archivos

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1
```

```
[root@hc-cloud-secure-1 ~]# df -k
```

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
devtmpfs	8072804	0	8072804	0%	/dev
tmpfs	8103272	0	8103272	0%	/dev/shm
tmpfs	8103272	9404	8093868	1%	/run
tmpfs	8103272	0	8103272	0%	/sys/fs/cgroup
/dev/mapper/cs-root	45496624	5642104	39854520	13%	/
/dev/sda2	1038336	258712	779624	25%	/boot
/dev/sda1	613184	7416	605768	2%	/boot/efi
tmpfs	1620652	12	1620640	1%	/run/user/42
tmpfs	1620652	0	1620652	0%	/run/user/0
/dev/mapper/datavg-datalv	209608708	1494520	208114188	1%	/file1

Para obtener información detallada sobre estas tareas, consulte la página ["Administración de LVM con comandos de la CLI"](#).

Generación de datos

`Dgen.pl` Es un generador de datos mediante scripts Perl para el simulador de E/S de EHR (GenerateIO). Los datos dentro de las LUN se generan con el EHR. `Dgen.pl` guion. El script está diseñado para crear datos similares a los de una base de datos EHR.

```
[root@hc-cloud-secure-1 ~]# cd GenerateIO-1.17.3/

[root@hc-cloud-secure-1 GenerateIO-1.17.3]# ./dgen.pl --directory /file1
--jobs 80

[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01  dir05  dir09  dir13  dir17  dir21  dir25  dir29  dir33  dir37
dir41  dir45  dir49  dir53  dir57  dir61  dir65  dir69  dir73  dir77
dir02  dir06  dir10  dir14  dir18  dir22  dir26  dir30  dir34  dir38
dir42  dir46  dir50  dir54  dir58  dir62  dir66  dir70  dir74  dir78
dir03  dir07  dir11  dir15  dir19  dir23  dir27  dir31  dir35  dir39
dir43  dir47  dir51  dir55  dir59  dir63  dir67  dir71  dir75  dir79
dir04  dir08  dir12  dir16  dir20  dir24  dir28  dir32  dir36  dir40
dir44  dir48  dir52  dir56  dir60  dir64  dir68  dir72  dir76  dir80

[root@hc-cloud-secure-1 file1]# df -k .

```

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
/dev/mapper/datavg-datalv	209608708	178167156	31441552	85%	/file1

Mientras se ejecuta, la `Dgen.pl` script utiliza el 85% del sistema de archivos para la generación de datos de forma predeterminada.

Configurar la replicación de SnapMirror entre ONTAP en las instalaciones y Cloud Volumes ONTAP

SnapMirror de NetApp replica los datos a alta velocidad a través de LAN o WAN, de forma que usted obtiene una alta disponibilidad de datos y una rápida replicación de datos tanto en entornos virtuales como tradicionales. Al replicar datos en sistemas de almacenamiento de NetApp y actualizar continuamente los datos secundarios, estos están siempre al día y disponibles cuando los necesite. No se requieren servidores de replicación externos.

Complete los pasos siguientes para configurar la replicación de SnapMirror entre su sistema ONTAP local y CVO.

1. Desde el menú de navegación, seleccione **Almacenamiento > Sistemas**.
2. En Sistemas, seleccione el sistema que contiene el volumen de origen, arrástrelo al sistema en el que desea replicar el volumen y, a continuación, seleccione **Replicación**.

Los pasos restantes explican cómo crear una relación síncrona entre clústeres Cloud Volumes ONTAP y

ONTAP en las instalaciones.

3. **Configuración de relación entre iguales de origen y destino.** Si aparece esta página, seleccione todas las LIF de interconexión de clústeres para la relación entre iguales de clústeres.
4. **Selección de volumen de origen.** Seleccione el volumen que desea replicar.
5. **Tipo de disco de destino y clasificación por niveles.** Si el destino es un sistema Cloud Volumes ONTAP, seleccione el tipo de disco de destino y elija si desea habilitar la organización por niveles de datos.
6. **Nombre del volumen de destino:** especifique el nombre del volumen de destino y elija el agregado de destino. Si el destino es un clúster de ONTAP, también debe especificar la máquina virtual de almacenamiento de destino.
7. **Velocidad máxima de transferencia.** especifique la velocidad máxima (en megabytes por segundo) a la que se pueden transferir los datos.
8. **Directiva de replicación.** Seleccione una directiva predeterminada o haga clic en **Directivas adicionales** y, a continuación, seleccione una de las directivas avanzadas. Si necesita ayuda, ["obtenga información acerca de las políticas de replicación"](#).
9. **Programación.** Elija una copia única o un horario recurrente. Hay varios horarios predeterminados disponibles. Si desea usar otra programación, debe crear una nueva en `destination cluster` Uso de System Manager.
10. **Revisión.** Revise sus selecciones y haga clic en **Ir**.

Para obtener información detallada sobre estos pasos de configuración, consulte ["aquí"](#).

La consola inicia el proceso de replicación de datos. En esta etapa, puede ver el servicio de **Replicación** que se estableció entre su sistema ONTAP local y Cloud Volumes ONTAP.

En el clúster de Cloud Volumes ONTAP, puede ver el volumen recién creado.

También puede verificar que la relación de SnapMirror se haya establecido entre el volumen en las instalaciones y el volumen de cloud.

Puede encontrar más información sobre la tarea de replicación en la ficha **replicación**.

["Siguiente: Validación de la solución."](#)

Validación de la solución

["Anterior: Configuración DE SAN."](#)

En esta sección, revisamos algunos casos de uso de soluciones.

- Uno de los principales casos prácticos de SnapMirror es el backup de datos. SnapMirror se puede utilizar como herramienta de backup principal replicando datos dentro del mismo clúster o en destinos remotos.
- Uso del entorno de recuperación ante desastres para ejecutar pruebas de desarrollo de aplicaciones (prueba/desarrollo).
- Recuperación ante desastres en caso de desastre en la producción.
- Distribución de los datos y acceso remoto a los mismos.

Cabe destacar que los relativamente pocos casos de uso validados en esta solución no representan la funcionalidad completa de la replicación SnapMirror.

Desarrollo y pruebas de aplicaciones (prueba/desarrollo)

Para acelerar el desarrollo de aplicaciones, puede clonar rápidamente los datos replicados en el centro de recuperación ante desastres y utilizarlos para aplicaciones de desarrollo y pruebas. La ubicación de los entornos de recuperación ante desastres y de desarrollo y pruebas en el mismo lugar puede mejorar considerablemente la utilización de las instalaciones de recuperación ante desastres. Además, los clones de desarrollo y pruebas bajo demanda pueden proporcionar tantas copias de datos como sea necesario para iniciar la producción con mayor rapidez.

La tecnología FlexClone de NetApp se puede utilizar para crear rápidamente una copia de lectura y escritura de un volumen FlexVol de destino de SnapMirror en caso de que desee tener acceso de lectura y escritura a la copia secundaria para confirmar si todos los datos de producción están disponibles.

Complete los siguientes pasos para usar el entorno de recuperación ante desastres para realizar pruebas y desarrollo de aplicaciones:

1. Haga una copia de los datos de producción. Para ello, realizar una copia Snapshot de aplicación de un volumen local. La creación Snapshot de aplicaciones consta de tres pasos: Lock, Snap, y. Unlock.
 - a. Ponga en modo inactivo el sistema de archivos para que se suspendan las operaciones de I/O y se mantengan la coherencia de las aplicaciones. Cualquier aplicación escribe golpeando el sistema de archivos permanece en estado de espera hasta que el comando unQUIESCE se emita en el paso c. Los pasos a, b y c se ejecutan a través de un proceso o un flujo de trabajo transparente y no afecta al SLA de la aplicación.

```
[root@hc-cloud-secure-1 ~]# fsfreeze -f /file1
```

Esta opción solicita que el sistema de archivos especificado se congele de nuevas modificaciones. Cualquier proceso que intente escribir en el sistema de archivos bloqueado se bloquea hasta que el sistema de archivos se descongela.

- b. Cree una copia Snapshot del volumen en las instalaciones.

```
A400-G0312::> snapshot create -vserver Healthcare_SVM -volume  
hc_iscsi_vol -snapshot kamini
```

- c. Desactive el sistema de archivos para reiniciar I/O.

```
[root@hc-cloud-secure-1 ~]# fsfreeze -u /file1
```

Esta opción se utiliza para descongelar el sistema de archivos y permitir que las operaciones continúen. Cualquier modificación del sistema de archivos que fue bloqueada por la congelación se desbloquea y se permite completar.

También se puede realizar copias Snapshot coherentes con las aplicaciones usando SnapCenter de NetApp, que tiene una orquestación completa del flujo de trabajo descrito anteriormente como parte de SnapCenter. Para obtener información detallada, consulte ["aquí"](#).

2. Realice una operación de actualización de SnapMirror para mantener sincronizados los sistemas de

producción y de recuperación ante desastres.

```
singlecvoaws::> snapmirror update -destination-path  
svm_singlecvoaws:hc_iscsi_vol_copy -source-path  
Healthcare_SVM:hc_iscsi_vol  
  
Operation is queued: snapmirror update of destination  
"svm_singlecvoaws:hc_iscsi_vol_copy".
```

También se puede realizar una actualización de SnapMirror a través de la interfaz gráfica de usuario (GUI) de la NetApp Console, en la pestaña **Replicación**.

3. Crear una instancia de FlexClone basada en la instantánea de la aplicación que se realizó anteriormente.

```
singlecvoaws::> volume clone create -flexclone kamini_clone -type RW  
-parent-vserver svm_singlecvoaws -parent-volume hc_iscsi_vol_copy  
-junction-active true -foreground true -parent-snapshot kamini  
  
[Job 996] Job succeeded: Successful
```

Para la tarea anterior, también se puede crear una nueva instantánea, pero debe seguir los mismos pasos anteriores para garantizar la coherencia de las aplicaciones.

4. Activar un volumen FlexClone para que la instancia de EHR en el cloud.

```
singlecvoaws::> lun mapping create -vserver svm_singlecvoaws -path  
/vol/kamini_clone/iscsi_lun1 -igroup ehr-igroup -lun-id 0  
  
singlecvoaws::> lun mapping show
```

Vserver	Path	Igroup	LUN ID	Protocol
-----	-----	-----	-----	-----
svm_singlecvoaws	/vol/kamini_clone/iscsi_lun1	ehr-igroup	0	iscsi

5. Ejecute los siguientes comandos en la instancia de EHR en el cloud para acceder a los datos o el sistema de archivos.
 - a. Descubra el almacenamiento de ONTAP. Compruebe el estado de accesos múltiples.

```

sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show

```

Output:

controller(7mode/E-Series)/	device	host	lun
vserver(cDOT/FlashRay)	lun-pathname	filename	adapter protocol size
product			

svm_singlecvoaws	/dev/sda	host2	iSCSI 200g
------------------	----------	-------	------------

cDOT /vol/kamini_clone/iscsi_lun1

```
sudo multipath -ll
```

Output:

```

3600a09806631755a452b543041313053 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running

```

b. Active el grupo de volúmenes.

```
sudo vgchange -ay datavg
```

Output:

```
1 logical volume(s) in volume group "datavg" now active
```

c. Monte el sistema de archivos y muestre el resumen de la información del sistema de archivos.

```
sudo mount -t xfs /dev/datavg/datalv /file1
```

```
cd /file1
```

```
df -k .
```

Output:

Filesystem	1K-blocks	Used	Available	Use%
Mounted on				
/dev/mapper/datavg-datalv	209608708	183987096	25621612	88%
/file1				

Esto valida que puede utilizar el entorno de recuperación ante desastres para desarrollo y pruebas de aplicaciones. La posibilidad de realizar tareas de desarrollo y pruebas de aplicaciones en el sistema de almacenamiento de recuperación ante desastres le permite aprovechar mejor los recursos que, de otro

modo, podrían permanecer inactivos la mayor parte del tiempo.

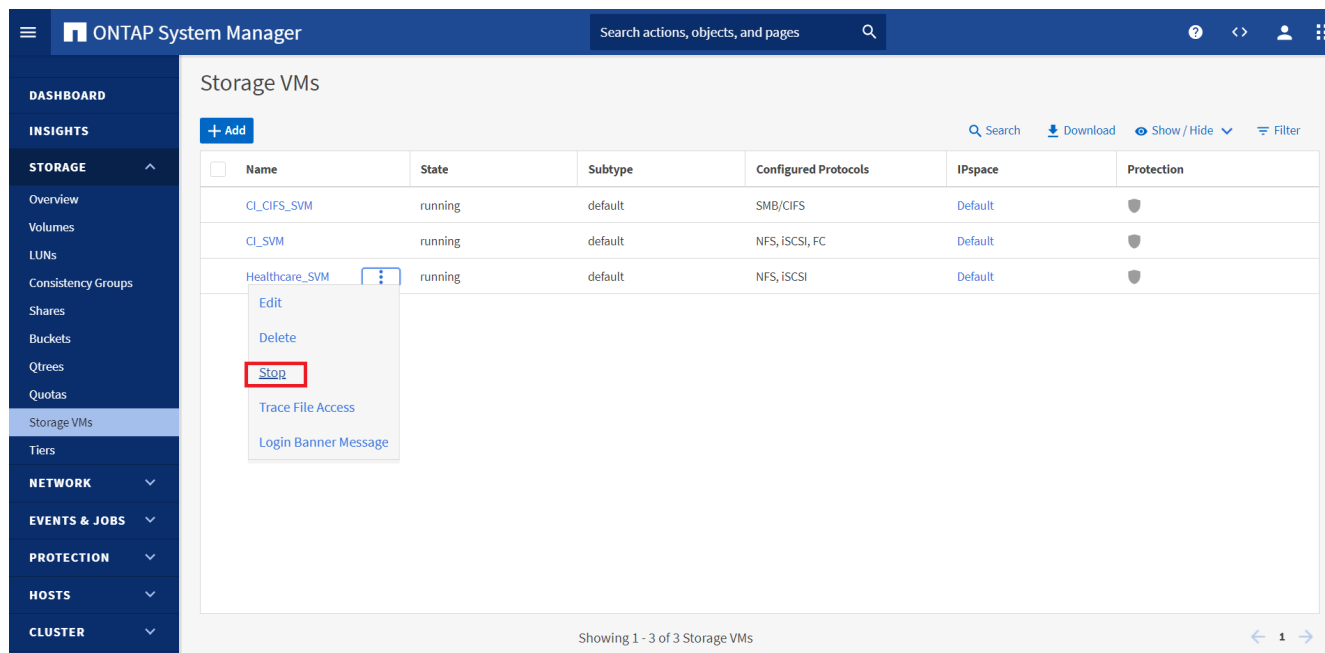
Recuperación tras siniestros

La tecnología SnapMirror también se usa como parte de los planes de recuperación tras desastres. Si los datos clave se replican en una ubicación física diferente, un desastre grave no tendrá que provocar períodos prolongados de falta de disponibilidad de datos para aplicaciones vitales para el negocio. Los clientes pueden acceder a los datos replicados por toda la red hasta que el sitio de producción se recupere de una corrupción, una eliminación accidental o un desastre natural, etc.

En caso de conmutación tras recuperación al sitio principal, SnapMirror ofrece un método eficiente para volver a sincronizar el centro de recuperación ante desastres con el sitio principal y transferir únicamente los datos nuevos o modificados al sitio principal del centro de recuperación ante desastres, simplemente revirtiendo la relación de SnapMirror. Una vez que el centro de producción principal reanuda las operaciones normales de las aplicaciones, SnapMirror continúa la transferencia al centro de recuperación ante desastres sin necesidad de realizar otra transferencia de referencia.

Para realizar la validación de un escenario de recuperación ante desastres correcto, complete los siguientes pasos:

1. Simule un desastre en el origen (producción) deteniendo la SVM que aloja el volumen de ONTAP en las instalaciones (`hc_iscsi_vol`).



The screenshot shows the ONTAP System Manager web interface. The left sidebar contains navigation menus for Dashboard, Insights, Storage, Network, Events & Jobs, Protection, Hosts, and Cluster. The main panel displays the 'Storage VMs' table with columns: Name, State, Subtype, Configured Protocols, IPspace, and Protection. Three rows are listed: 'CL_CIFS_SVM', 'CL_SVM', and 'Healthcare_SVM'. The 'Healthcare_SVM' row is selected, and a context menu is open over it, showing options: Edit, Delete, Stop (highlighted with a red box), Trace File Access, and Login Banner Message. The bottom of the panel indicates 'Showing 1 - 3 of 3 Storage VMs'.

Name	State	Subtype	Configured Protocols	IPspace	Protection
CL_CIFS_SVM	running	default	SMB/CIFS	Default	Shield icon
CL_SVM	running	default	NFS, iSCSI, FC	Default	Shield icon
Healthcare_SVM	running	default	NFS, iSCSI	Default	Shield icon

Asegúrese de que la replicación de SnapMirror ya esté configurada entre la ONTAP local en la instancia de FlexPod y Cloud Volumes ONTAP en AWS, para que pueda crear copias de Snapshot de aplicaciones frecuentes.

Una vez que se ha detenido el SVM, `hc_iscsi_vol` El volumen no se muestra en la consola.

2. Activar DR en CVO.

- a. Rompa la relación de replicación de SnapMirror entre ONTAP en las instalaciones y Cloud Volumes ONTAP y promocióne el volumen de destino de CVO (`hc_iscsi_vol_copy`) a la producción.

Tras romper la relación de SnapMirror, el tipo de volumen de destino cambia de protección de datos (DP) a lectura/escritura (RW).

```
singlecvoaws::> volume show -volume hc_iscsi_vol_copy -fields typev
server          volume          type
-----
svm_singlecvoaws hc_iscsi_vol_copy RW
```

- b. Active el volumen de destino en Cloud Volumes ONTAP para abrir la instancia de EHR en una instancia de EC2 en el cloud.

```
singlecvoaws::> lun mapping create -vserver svm_singlecvoaws -path
/vol/hc_iscsi_vol_copy/iscsi_lun1 -igroup ehr-igroup -lun-id 0

singlecvoaws::> lun mapping show
Vserver      Path                                Igroup    LUN ID
Protocol
-----
svm_singlecvoaws
          /vol/hc_iscsi_vol_copy/iscsi_lun1 ehr-igroup 0    iscsi
```

- c. Para acceder a los datos y el sistema de archivos en la instancia de EHR en el cloud, primero descubra el almacenamiento ONTAP y verifique el estado del acceso multivía.

```

sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show
Output:
controller(7mode/E-Series)/          device      host          lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
-----
-----
svm_singleecvoaws                    /dev/sda  host2      iSCSI      200g
cDOT
                                /vol/hc_iscsi_vol_copy/iscsi_lun1
sudo multipath -ll
Output:
3600a09806631755a452b543041313051 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running

```

d. A continuación, active el grupo de volúmenes.

```

sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active

```

e. Finalmente, monte el sistema de archivos y muestre la información del sistema de archivos.

```

sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                1K-blocks  Used    Available  Use%
Mounted on
/dev/mapper/datavg-datalv  209608708  183987096  25621612   88%
/file1

```

Este resultado muestra que los usuarios pueden acceder a los datos replicados a través de la red hasta la recuperación del centro de producción a partir del desastre.

f. Invierta la relación de SnapMirror. Esta operación revierte los roles de los volúmenes de origen y destino.

Cuando se realiza esta operación, el contenido del volumen de origen original se sobrescribe con el contenido del volumen de destino. Esto es útil cuando se desea reactivar un volumen de origen que se desconectó.

Ahora volumen CVO (`hc_iscsi_vol_copy`) se convierte en el volumen de origen y el volumen en las instalaciones (`hc_iscsi_vol`) se convierte en el volumen de destino.

No se conservan todos los datos escritos en el volumen de origen original entre la última replicación de datos y la hora en la que se deshabilitó el volumen de origen.

- a. Para verificar el acceso de escritura al volumen CVO, cree un nuevo archivo en la instancia de EHR en el cloud.

```
cd /file1/  
sudo touch newfile
```

Cuando el sitio de producción está inactivo, los clientes aún pueden acceder a los datos y realizar también escrituras en el volumen Cloud Volumes ONTAP, que ahora es el volumen de origen.

En caso de conmutación tras recuperación al sitio principal, SnapMirror ofrece un método eficiente para volver a sincronizar el centro de recuperación ante desastres con el sitio principal y transferir únicamente los datos nuevos o modificados al sitio principal del centro de recuperación ante desastres, simplemente revirtiendo la relación de SnapMirror. Una vez que el centro de producción principal reanuda las operaciones normales de las aplicaciones, SnapMirror continúa la transferencia al centro de recuperación ante desastres sin necesidad de realizar otra transferencia de referencia.

En esta sección se ilustra la correcta resolución de una situación de recuperación ante desastres cuando el sitio de producción es afectado por un desastre. Ahora los datos pueden ser consumidos con seguridad por aplicaciones que ahora pueden prestar servicio a los clientes mientras el sitio de origen pasa por su restauración.

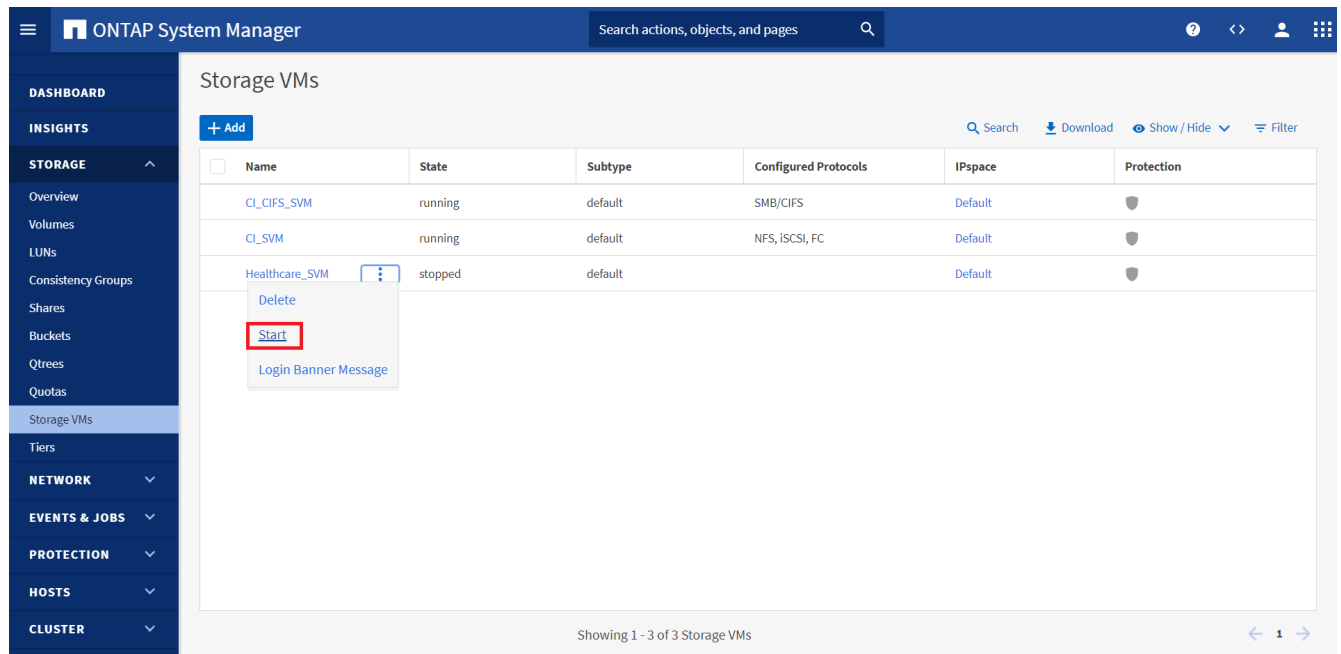
Verificación de los datos en el lugar de producción

Una vez restaurado el sitio de producción, debe asegurarse de que la configuración original se haya restaurado y que los clientes puedan acceder a los datos desde el sitio de origen.

En esta sección, hablamos de poner en el sitio de origen, de restaurar la relación de SnapMirror entre ONTAP y Cloud Volumes ONTAP en las instalaciones, y finalmente realizamos una comprobación de la integridad de los datos en el extremo de la fuente

Para la verificación de los datos en el sitio de producción se puede seguir el siguiente procedimiento:

1. Asegúrese de que el sitio de origen está activo. Para hacerlo, inicie la SVM que aloja el volumen de ONTAP en las instalaciones (`hc_iscsi_vol`).



- Rompa la relación de replicación de SnapMirror entre Cloud Volumes ONTAP y ONTAP en las instalaciones y promocioe el volumen en las instalaciones (hc_iscsi_vol) volver a la producción.

Después de romper la relación de SnapMirror, el tipo de volumen en las instalaciones cambia de la protección de datos (DP) a la de lectura/escritura (RW).

```
A400-G0312::> volume show -volume hc_iscsi_vol -fields type
vserver          volume          type
-----
Healthcare_SVM hc_iscsi_vol RW
```

- Invierta la relación de SnapMirror. Ahora, el volumen de ONTAP en las instalaciones (hc_iscsi_vol) Se convierte en el volumen de origen como lo era antes y el volumen Cloud Volumes ONTAP (hc_iscsi_vol_copy) se convierte en el volumen de destino.

Siguiendo estos pasos, hemos restaurado correctamente la configuración original.

- Reinicie la instancia de EHR en las instalaciones. Monte el sistema de archivos y verifique que newfile Que creó en la instancia de EHR en el cloud cuando la producción no estaba operativa también aquí.

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/dataavg/data1v /file1
[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01 dir05 dir09 dir13 dir17 dir21 dir25 dir29 dir33 dir37 dir41 dir45 dir49 dir53 dir57 dir61 dir65 dir69 dir73 dir77 kamini
dir02 dir06 dir10 dir14 dir18 dir22 dir26 dir30 dir34 dir38 dir42 dir46 dir50 dir54 dir58 dir62 dir66 dir70 dir74 dir78 latest file
dir03 dir07 dir11 dir15 dir19 dir23 dir27 dir31 dir35 dir39 dir43 dir47 dir51 dir55 dir59 dir63 dir67 dir71 dir75 dir79 newfile
dir04 dir08 dir12 dir16 dir20 dir24 dir28 dir32 dir36 dir40 dir44 dir48 dir52 dir56 dir60 dir64 dir68 dir72 dir76 dir80
```

Podemos inferir que la replicación de datos del origen al destino se ha completado correctamente y que se ha mantenido la integridad de los datos. Así finaliza la verificación de los datos en el sitio de producción.

"Siguiente: Conclusión."

Conclusión

"Anterior: Validación de la solución."

Crear un cloud híbrido es un objetivo para la mayoría de las organizaciones sanitarias de proporcionar disponibilidad de datos en cualquier momento. En esta solución, implementamos una solución de cloud híbrido FlexPod con Cloud Volumes ONTAP y utilizamos la tecnología de replicación SnapMirror de NetApp para validar algunos casos prácticos con el fin de realizar backups y recuperar aplicaciones y cargas de trabajo de atención médica.

FlexPod, una infraestructura convergente rigurosamente probada y validada previamente de la alianza estratégica de Cisco y NetApp, ha sido diseñada para proporcionar un rendimiento de sistema de baja latencia predecible y una alta disponibilidad. Este enfoque da como resultado altos niveles de confort de EHR y, en última instancia, el mejor tiempo de respuesta para los usuarios del sistema EHR.

Con NetApp, podrá ejecutar la producción de EHR, la recuperación ante desastres, el backup o la organización en niveles en el cloud tal como lo haría con las funciones de almacenamiento de NetApp en un centro de datos en las instalaciones. Con Cloud Volumes ONTAP de NetApp, NetApp proporciona las funcionalidades de clase empresarial y el rendimiento necesario para ejecutar EHR en el cloud de forma efectiva. Las opciones de cloud de NetApp proporcionan iSCSI de bloque a bloque y SMB o NFS.

Esta solución satisface la necesidad de las organizaciones sanitarias y permite dar un paso adelante hacia su transformación digital. También puede ayudarles a gestionar sus aplicaciones y cargas de trabajo de forma eficiente.

"Siguiendo: Dónde encontrar información adicional."

Dónde encontrar información adicional

"Anterior: Conclusión."

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

- Página de inicio de FlexPod

["https://www.flexpod.com"](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"](https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html)

- NetApp Console

["https://console.netapp.com/"](https://console.netapp.com/)

- Cloud Volumes ONTAP de NetApp

["https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/concept-overview-cvo.html"](https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/concept-overview-cvo.html)

- Inicio rápido para Cloud Volumes ONTAP en AWS

["https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-aws.html"](https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-aws.html)

- Replicación de SnapMirror

["https://docs.netapp.com/us-en/cloud-manager-replication/concept-replication.html"](https://docs.netapp.com/us-en/cloud-manager-replication/concept-replication.html)

- TR-3928: Prácticas recomendadas de NetApp para Epic

<https://www.netapp.com/pdf.html?item=/media/17137-tr3928pdf.pdf>

- TR-4693: Guía de puesta en marcha de FlexPod Datacenter para EHR de Epic

["https://www.netapp.com/media/10658-tr-4693.pdf"](https://www.netapp.com/media/10658-tr-4693.pdf)

- FlexPod para Epic

["https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmw_epic.htm
l"](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmw_epic.html)

- Herramienta de matriz de interoperabilidad de NetApp

["http://support.netapp.com/matrix/"](http://support.netapp.com/matrix/)

- Herramienta de interoperabilidad de hardware y software Cisco UCS

["http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"](http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html)

- Guía de compatibilidad de VMware

["http://www.vmware.com/resources/compatibility/search.php"](http://www.vmware.com/resources/compatibility/search.php)

Historial de versiones

Versión	Fecha	Historial de versiones del documento
Versión 1.0	Marzo de 2023	Versión inicial

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.