Soluciones FlexPod

FlexPod

NetApp
April 02, 2025

This PDF was generated from https://docs.netapp.com/es-es/flexpod/index.html on April 02, 2025.
Always check docs.netapp.com for the latest.

Tabla de contenidos

Soluciones FlexPod . . . 1
Definición de FlexPod . . . 2
Especificaciones técnicas de FlexPod Express . . . 2
TR-4293: Especificaciones técnicas de FlexPod Express . . . 2
Plataformas FlexPod . . . 2
Reglas de FlexPod . . . 2
Compatible con configuraciones de FlexPod validadas frente a las validadas . . . 2
Software de almacenamiento . . . 3
Requisitos mínimos de hardware . . . 3
Requisitos mínimos de software . . . 4
Requisitos de conectividad . . . 5
Otros requisitos . . . 6
Equipo existente . . . 6
Información adicional . . . 7
Especificaciones técnicas de FlexPod Datacenter . . . 8
TR-4036: Especificaciones técnicas de FlexPod Datacenter . . . 8
Plataformas FlexPod . . . 8
Reglas de FlexPod . . . 9
Compatible con configuraciones de FlexPod validadas frente a las validadas . . . 9
ONTAP de NetApp . . . 9
Modos de funcionamiento de switches de Cisco Nexus . . . 9
Requisitos mínimos de hardware . . . 10
Requisitos mínimos de software . . . 11
Requisitos de conectividad . . . 11
Otros requisitos . . . 12
Funciones opcionales . . . 12
Componentes de Cisco . . . 27
Componentes de NetApp . . . 32
Requisitos de alimentación y cableado . . . 34
Especificaciones técnicas y referencias . . . 36
Equipo existente . . . 43
Dónde encontrar información adicional . . . 44
Centro de datos FlexPod . . . 45
FlexPod DataCenter con NetApp SnapMirror Business Continuity y ONTAP 9.10 . . . 45
TR-4920: Continuidad del negocio de FlexPod Datacenter con NetApp SnapMirror y ONTAP 9.10 . . . 45
Introducción . . . 45
Solución FlexPod SM-BC . . . 48
Validación de la solución . . . 58
Conclusión . . . 101
Dónde encontrar información adicional e historial de versiones . . . 102
FlexPod Datacenter con VMware vSphere 7,0 y NetApp ONTAP 9,7: Puesta en marcha . . . 105
FlexPod Datacenter con Cisco Intersight y NetApp ONTAP 9,7: Diseño . . . 106
FlexPod Datacenter con Cisco Intersight y NetApp ONTAP 9,7: Puesta en marcha . . . 106

FlexPod Datacenter con Cisco Intersight y NetApp ONTAP 9,7: Diseño . . . 107
FlexPod Datacenter con VMware vSphere 6,7 U2, Cisco UCS fouth-generation Fabric y NetApp ONTAP 9,6 . . . 107
FlexPod Datacenter con VMware vSphere 6,7 U1, la estructura de cuarta generación de Cisco UCS y AFF A-Series de NetApp: Diseño . . . 108
FlexPod Datacenter con VMware vSphere 6,7 U1, la estructura de cuarta generación de Cisco UCS y AFF A-Series de NetApp . . . 108
FlexPod Datacenter con Cisco ACI Multi-Pod, MetroCluster IP de NetApp y VMware vSphere 6,7: Diseño . . . 109
FlexPod Datacenter con Cisco ACI Multi-Pod con NetApp MetroCluster IP y VMware vSphere 6,7: Puesta en marcha . . . 109
Cloud híbrido . . . 110
Cloud híbrido de FlexPod con Cloud Volumes ONTAP para Epic . . . 110
TR-4960: Cloud híbrido de FlexPod con Cloud Volumes ONTAP para Epic . . . 110
Componentes de la solución . . . 112
Instalación y configuración . . . 117
Configuración de SAN . . . 122
Validación de la solución . . . 135
Conclusión . . . 145
Dónde encontrar información adicional . . . 146
Cloud híbrido de FlexPod para Google Cloud Platform con Cloud Volumes ONTAP de NetApp y Cisco Intersight . . . 147
TR-4939: Cloud híbrido de FlexPod para Google Cloud Platform con Cloud Volumes ONTAP de NetApp y Cisco Intersight . . . 147
Componentes de la solución . . . 149
Instalación y configuración . . . 154
Validación de la solución . . . 221
Conclusión . . . 229
Cloud híbrido de FlexPod con NetApp Astra y Cisco Intersight para Red Hat OpenShift . . . 232
TR-4936: Cloud híbrido de FlexPod con NetApp Astra y Cisco Intersight para Red Hat OpenShift . . . 232
Componentes de la solución . . . 235
Instalación y configuración . . . 243
Validación de la solución . . . 266
Conclusión . . . 287
Cloud Insights de NetApp para FlexPod . . . 289
TR-4868: Cloud Insights de NetApp para FlexPod . . . 289
Casos de uso . . . 289
Arquitectura . . . 290
Consideraciones de diseño . . . 292
Ponga en marcha Cloud Insights para FlexPod . . . 293
Casos de uso . . . 305
Vídeos y demostraciones . . . 313
Información adicional . . . 314
FlexPod con FabricPool: Organización en niveles de datos inactiva en Amazon AWS S3 . . . 314
TR-4801: FlexPod con FabricPool: Organización en niveles de datos inactivos en Amazon AWS S3 . . . 314

Información general y arquitectura de FlexPod . . . 315
FabricPool . . . 317
Requisitos de FabricPool . . . 322
Configuración . . . 326
Consideraciones de rendimiento . . . 337
Coste de propiedad . . . 338
Conclusión . . . 338
Dónde encontrar información adicional . . . 338
FlexPod Datacenter para cloud híbrido con CloudCenter de Cisco y almacenamiento privado de NetApp - Diseño . . . 339
Bases de datos empresariales . . . 340
SAP . . . 340
Introducción a SAP en FlexPod . . . 340
FlexPod Datacenter para una solución SAP mediante FibreChannel SAN con Cisco UCS Manager 4,0 y NetApp ONTAP 9,7 . . . 340
White paper SAP no HANA con SQL: Diseño . . . 340
FlexPod Datacenter para solución SAP con la estructura de tercera generación de Cisco UCS y NetApp AFF A-Series . . . 341
FlexPod Datacenter para la solución SAP mediante FibreChannel SAN con Cisco UCS Manager 4,0 y NetApp ONTAP 9,7: Diseño . . . 341
Solución FlexPod Datacenter para SAP con Cisco ACI, Cisco UCS Manager 4,0 y AFF A-Series de NetApp: Diseño . . . 342
FlexPod Datacenter para SAP con Cisco ACI, Cisco UCS Manager 4,0 y AFF A-Series de NetApp: Puesta en marcha . . . 342
FlexPod Datacenter para la solución SAP con Cisco UCS Manager 4,0 y NetApp AFF A–Series: Diseño . . . 342
FlexPod Datacenter para la solución SAP con Cisco ACI en servidores Cisco UCS M5 con SLES 12 SP3 y RHEL 7,4 . . . 343
FlexPod Datacenter para la solución SAP con almacenamiento basado en IP usando AFF A-Series de NetApp y Cisco UCS Manager 3,2 . . . 343
FlexPod Datacenter para una solución SAP mediante FibreChannel SAN con Cisco UCS Manager 4,0 y NetApp ONTAP 9,7 . . . 343
Pon en marcha servidores de aplicaciones SAP en FlexPod con SQL . . . 344
FlexPod Datacenter para SAP con Cisco ACI, Cisco UCS Manager 4,0 y AFF A-Series de NetApp . . . 344
Solución FlexPod Datacenter para SAP con Cisco ACI, Cisco UCS Manager 4,0 y AFF A-Series de NetApp: Diseño . . . 345
FlexPod Datacenter para solución SAP con la estructura de tercera generación de Cisco UCS y NetApp AFF A-Series . . . 345
FlexPod Datacenter para la solución SAP con Cisco UCS Manager 4,0 y NetApp AFF A–Series: Diseño . . . 345
Oracle . . . 346
Centro de datos FlexPod con bases de datos RAC de Oracle en Cisco UCS y AFF A-Series de NetApp . . . 346
Centro de datos FlexPod con Oracle RAC en Oracle Linux . . . 347
Centro de datos FlexPod con bases de datos RAC de Oracle en Cisco UCS y AFF A-Series de

NetApp . . . 347
Microsoft SQL Server . . . 348
FlexPod Datacenter para Microsoft SQL Server 2019 y VMware vSphere 6.7 . . . 348
FlexPod Datacenter con Microsoft SQL Server 2016 y VMware vSphere 6.5 . . . 348
FlexPod Datacenter con Microsoft SQL Server 2017 sobre Linux VM ejecutándose en VMware y Hyper-V. . . . 349
FlexPod Datacenter con Microsoft SQL Server 2017 sobre Linux VM ejecutándose en VMware y Hyper-V. . . . 349
Sector sanitario . . . 350
FlexPod para genomas . . . 350
TR-4911: Genómica de FlexPod . . . 350
Ventajas de la puesta en marcha de cargas de trabajo genómicos en FlexPod . . . 352
Infraestructura de la solución componentes de hardware y software . . . 358
Genómica - instalación y ejecución de GATK . . . 362
Salida para la ejecución de GATK utilizando el archivo JAR . . . 372
Salida para la ejecución de GATK usando el script ./gatk . . . 374
Salida para la ejecución del GATK utilizando el motor Cromwell . . . 377
Configuración de GPU . . . 381
Conclusión . . . 390
Guía de tamaños direccionales de FlexPod para MEDITECH . . . 392
TR-4774: FlexPod para el dimensionamiento direccional de MEDITECH . . . 392
Descripción general de la carga de trabajo de MEDITECH . . . 394
Especificaciones técnicas para arquitecturas pequeñas, medianas y grandes . . . 398
Información adicional . . . 403
Reconocimientos . . . 404
Guía de puesta en marcha de FlexPod Datacenter para MEDITECH . . . 404
TR-4753: Guía de puesta en marcha de FlexPod Datacenter para MEDITECH . . . 404
Diseño . . . 416
Puesta en marcha y configuración . . . 419
Módulos y componentes de MEDITECH . . . 433
Reconocimientos . . . 434
Dónde encontrar información adicional . . . 434
FlexPod para exploración médica . . . 436
TR-4865: FlexPod para imágenes médicas . . . 436
Arquitectura . . . 449
Infraestructura de la solución componentes de hardware y software . . . 460
Ajuste del tamaño de la solución . . . 462
Mejores prácticas . . . 465
Conclusión . . . 470
Información adicional . . . 470
Infraestructura de puestos de trabajo virtuales . . . 472
FlexPod Datacenter con Citrix Virtual Apps & Desktops 1912 LTSR y VMware vSphere 7 para un máximo de 6000 puestos . . . 472
FlexPod Datacenter con VMware Horizon View 7,10, VMware vSphere 6,7 U2, Cisco UCS Manager 4,0 y NetApp ONTAP 9,6 para un máximo de 6700 puestos . . . 472

Visualización de gráficos 3D con Citrix y NVIDIA - Documento técnico . . . 472
FlexPod Datacenter con Citrix XenDesktop/XenApp 7,15 y VMware vSphere 6,5 Update 1 para 6000 puestos . . . 473
FlexPod Datacenter con VMware Horizon View 7,3 y VMware vSphere 6,5 Update 1 con Cisco UCS Manager 3,2 para 5000 puestos . . . 473
FlexPod Datacenter con VMware Horizon View 7,10, VMware vSphere 6,7 U2, Cisco UCS Manager 4,0 y NetApp ONTAP 9,6 para un máximo de 6700 puestos . . . 473
Aplicaciones modernas . . . 475
Centro de datos FlexPod para IA y ML combinados con Cisco UCS 480 ML para aprendizaje profundo: Diseño . . . 475
Ponga en marcha el complemento Trident CSI de NetApp en Cisco Container Platform con FlexPod . . . 475
FlexPod Datacenter para OpenShift Container Platform 4: Puesta en marcha . . . 475
FlexPod Datacenter con Docker Enterprise Edition para la gestión de contenedores . . . 476
FlexPod Datacenter para OpenShift Container Platform 4: Diseño . . . 476
Visualización de gráficos 3D con VMware y NVIDIA en Cisco UCS: Whitepaper . . . 477
Visualización de gráficos 3D con Citrix y NVIDIA - Documento técnico . . . 477
FlexPod Express . . . 478
Guía de diseño de FlexPod Express con Cisco UCS C-Series y la serie AFF C190 de NetApp . . . 478
Diseño de la arquitectura NVA-1139: FlexPod Express con Cisco UCS C-Series y AFF C190 Series de NetApp . . . 478
Resumen del programa . . . 478
Requisitos tecnológicos . . . 481
Opciones de diseño . . . 482
Conclusión . . . 488
Dónde encontrar información adicional . . . 488
Guía de puesta en marcha de FlexPod Express con Cisco UCS C-Series y la serie AFF C190 de NetApp . . . 489
NVA-1142-PUESTA en MARCHA: FlexPod Express con Cisco UCS C-Series y AFF C190 Series de NetApp: Puesta en marcha NVA . . . 489
Descripción general de la solución . . . 489
Requisitos tecnológicos . . . 492
Información sobre el cableado exprés de FlexPod . . . 493
Procedimientos de implantación . . . 496
Conclusión . . . 585
Reconocimientos . . . 585
Dónde encontrar información adicional . . . 586
Historial de versiones . . . 586
Guía de diseño de FlexPod Express con Cisco UCS C-Series y AFF A220 Series . . . 586
Diseño NVA-1125: FlexPod Express con Cisco UCS C-Series y AFF A220 Series . . . 586
Resumen del programa . . . 586
Descripción general de la solución . . . 588
Requisitos tecnológicos . . . 589
Opciones de diseño . . . 590
Verificación de la solución . . . 595
Conclusión . . . 596

Dónde encontrar información adicional . . . 596
Guía de puesta en marcha de FlexPod Express con Cisco UCS C-Series y AFF A220 Series . . . 596
NVA-1123-PUESTA en MARCHA: FlexPod Express con VMware vSphere 6.7 y la guía de puesta en marcha de AFF A220 de NetApp . . . 596
Descripción general de la solución . . . 597
Requisitos tecnológicos . . . 600
Información sobre el cableado exprés de FlexPod . . . 601
Procedimientos de implantación . . . 603
Conclusión . . . 677
Dónde encontrar información adicional . . . 677
FlexPod Express con VMware vSphere 6.7U1 y NetApp AFF A220 con almacenamiento basado en IP directamente incluido . . . 678
NVA-1131-DEPLOY: FlexPod Express con VMware vSphere 6.7U1 y NetApp AFF A220 con almacenamiento basado en IP directamente incluido . . . 678
Descripción general de la solución . . . 678
Requisitos tecnológicos . . . 681
Información de cableado exprés de FlexPod . . . 683
Procedimientos de implantación . . . 684
Conclusión . . . 789
Información adicional . . . 790
FlexPod Express para VMware vSphere 7,0 con Cisco UCS Mini y NetApp AFF/FAS - NVA - Deployment . . . 790
FlexPod y Seguridad . . . 791
FlexPod, la solución a ransomware . . . 791
TR-4802: FlexPod, la solución para ransomware . . . 791
Información general de FlexPod . . . 794
Medidas de protección contra ransomware . . . 795
Proteja y recupere datos en FlexPod . . . 797
Continuar las operaciones de negocios sin pagar el rescate . . . 810
Conclusión . . . 810
Reconocimientos . . . 811
Información adicional . . . 811
Solución FlexPod para el sector sanitario conforme a la seguridad FIPS 140-2-2 . . . 811
TR-4892: Solución FlexPod para el sector sanitario conforme a la seguridad FIPS 140-2-2 . . . 811
Amenazas de ciberseguridad en sanidad . . . 812
Información general de FIPS 140-2 . . . 815
Plano de control frente al plano de datos . . . 816
Computación Cisco UCS de FlexPod y FIPS 140-2 . . . 816
Redes Cisco de FlexPod y FIPS 140-2 . . . 818
Almacenamiento ONTAP de FlexPod y FIPS 140-2 . . . 823
Ventajas para las soluciones de la infraestructura convergente de FlexPod . . . 829
Otras consideraciones de seguridad de FlexPod . . . 832
Conclusión . . . 833
Agradecimientos, historial de versiones y dónde encontrar información adicional . . . 834
Cisco Intersight con el almacenamiento ONTAP de NetApp . . . 837

Guía de inicio rápido de Cisco Intersight con el almacenamiento de NetApp . . . 837
Introducción . . . 837
Lo nuevo . . . 837
A enero de 2024 . . . 837
Noviembre de 2023 . . . 837
Agosto de 2023 . . . 838
Julio de 2023 . . . 838
Junio de 2023 . . . 839
Abril de 2023 . . . 839
Enero de 2023 . . . 839
Agosto de 2022 . . . 839
Julio de 2022 . . . 840
Abril de 2022 . . . 840
Enero de 2022 . . . 841
Octubre de 2021 . . . 841
Problemas conocidos . . . 842
Requisitos . . . 842
Requisitos de hardware y software . . . 842
Requisitos para la licencia de Cisco Intersight . . . 842
Antes de empezar . . . 843
Instale o actualice Active IQ Unified Manager de NetApp . . . 843
Instale el dispositivo virtual Cisco Intersight Assist . . . 843
Configure el servidor proxy de mensajería unificada de AIQ para el servicio IMT . . . 848
Objetivos de reclamaciones . . . 849
Supervise el almacenamiento de NetApp de Cisco Intersight . . . 850
Información general del inventario de almacenamiento . . . 850
Widgets de almacenamiento . . . 851
Casos de uso . . . 853
Caso de uso 1: Supervisión del inventario y los widgets de almacenamiento de NetApp . . . 853
Caso de uso 2: Orquestación de almacenamiento de NetApp mediante flujos de trabajo de referencia 853
Caso de uso 3: Flujos de trabajo personalizados utilizando un formulario sin diseñador . . . 854
De almacenamiento . . . 857
NVMe integral para FlexPod con Cisco UCSM, VMware vSphere 7.0 y ONTAP 9 de NetApp . . . 857
TR-4914: NVMe integral para FlexPod con Cisco UCSM, VMware vSphere 7.0 y ONTAP 9 de NetApp 857
Método de prueba . . . 859
Resultados de la prueba . . . 862
Conclusión . . . 865
Avisos legales . . . 868
Derechos de autor . . . 868
Marcas comerciales . . . 868
Estadounidenses . . . 868
Política de privacidad . . . 868

Soluciones FlexPod

Definición de FlexPod

Especificaciones técnicas de FlexPod Express

TR-4293: Especificaciones técnicas de FlexPod Express

Karthick Radhakrishnan, Arvind Ramakrishnan, Lindsey Street, Savita Kumari, NetApp

FlexPod Express es una arquitectura diseñada previamente y basada en mejores prácticas que se basa en Cisco Unified Computing System (Cisco UCS) y la familia de switches Cisco Nexus, y la capa de almacenamiento se crea con FAS de NetApp o el almacenamiento E-Series de NetApp. FlexPod Express es una plataforma adecuada para ejecutar diversos hipervisores de virtualización, sistemas operativos de configuración básica (OS) y cargas de trabajo empresariales.

FlexPod Express no solo ofrece una configuración básica, sino también la flexibilidad necesaria para ajustar el tamaño y optimizarse con el objetivo de acomodar distintos casos de uso y requisitos. Este documento categoriza las configuraciones exprés de FlexPod según el sistema de almacenamiento utilizado, FlexPod Express con FAS de NetApp y FlexPod Express con E-Series.

Plataformas FlexPod

Existen tres plataformas FlexPod:

- **FlexPod Datacenter.** esta plataforma es una infraestructura de centro de datos virtual escalable de forma masiva adaptada a aplicaciones empresariales con carga de trabajo, virtualización, VDI y cloud público y privado. FlexPod Datacenter tiene sus propias especificaciones, documentadas en "TR-4036: Especificaciones técnicas de FlexPod Datacenter".
- **FlexPod Express.** esta plataforma es una infraestructura convergente compacta que está destinada a casos de uso de oficinas remotas y periféricos.

Este documento proporciona las especificaciones técnicas de la plataforma FlexPod Express.

Reglas de FlexPod

El diseño de FlexPod proporciona una infraestructura flexible que abarca muchos componentes y versiones de software diferentes.

Utilice los conjuntos de reglas como guía para crear o ensamblar una configuración de FlexPod válida. Las cifras y reglas que se enumeran en este documento son los requisitos mínimos para el FlexPod; pueden ampliarse a las familias de productos incluidas según sea necesario para diferentes entornos y casos de uso.

Compatible con configuraciones de FlexPod validadas frente a las validadas

La arquitectura de FlexPod está definida por el conjunto de reglas que se describe en este documento. Los componentes de hardware y las configuraciones de software deben ser compatibles con la Lista de compatibilidad de hardware (HCL) de Cisco y con el "Herramienta de matriz de interoperabilidad de NetApp (IMT)".

Cada Cisco Validated Design (CVD) o NetApp Verified Architecture (NVA) es una posible configuración de FlexPod. Cisco y NetApp documentan estas combinaciones de configuración y las validan mediante una exhaustiva prueba de extremo a extremo. Las instalaciones de FlexPod que se desvían de estas configuraciones son totalmente compatibles si siguen las directrices de este documento y todos los componentes aparecen como compatibles en Cisco HCL y NetApp "IMT".

Por ejemplo, añadir controladoras de almacenamiento adicionales o servidores Cisco UCS y actualizar software a versiones más nuevas es totalmente compatible si el software, el hardware y las configuraciones cumplen las directrices definidas en este documento.

Software de almacenamiento

FlexPod Express es compatible con sistemas de almacenamiento que ejecutan sistemas operativos ONTAP o SANtricity de NetApp.

ONTAP de NetApp

El software ONTAP de NetApp es el sistema operativo que se ejecuta en sistemas de almacenamiento AFF y FAS. ONTAP ofrece una arquitectura de almacenamiento altamente escalable que permite operaciones no disruptivas, actualizaciones no disruptivas y una infraestructura de datos ágil.

Para obtener más información acerca de ONTAP, consulte "Página de productos ONTAP".

Software SANtricity E-Series

El software SANtricity de E-Series es el sistema operativo que se ejecuta en sistemas de almacenamiento E-Series. SANtricity proporciona un sistema altamente flexible que satisface diversas necesidades de aplicaciones y ofrece alta disponibilidad incorporada y una amplia variedad de funciones de protección de datos.

Para obtener más información, consulte "Página de productos SANtricity".

Requisitos mínimos de hardware

En esta sección se describen los requisitos mínimos de hardware para las distintas versiones de FlexPod Express.

FlexPod Express con FAS de NetApp

Los requisitos de hardware de las soluciones Express de FlexPod que utilizan las controladoras FAS de NetApp para almacenamiento subyacente incluyen las configuraciones que se describen en esta sección.

Configuración basada en CIMC (servidores en rack independientes)

La configuración de Cisco Integrated Management Controller (CIMC) incluye los siguientes componentes de hardware:

- Dos switches Ethernet estándar de 10 Gbps en una configuración redundante (se recomienda Cisco Nexus 31108, y se admiten los modelos Cisco Nexus 3000 y 9000)
- Servidores en rack independientes Cisco UCS C-Series
- Dos controladoras AFF C190, AFF A250, FAS2600 o FAS serie 2700 en una configuración de pareja de alta disponibilidad (ha) puesta en marcha como clúster de dos nodos

Configuración gestionada por Cisco UCS

La confirmación gestionada por Cisco UCS incluye los siguientes componentes de hardware:

- Dos switches Ethernet estándar de 10 Gbps en una configuración redundante (se recomienda Cisco Nexus 3524)
- Un chasis de servidor blade de corriente alterna (CA) Cisco UCS 5108
- Dos interconexiones de estructura Cisco UCS 6324
- Servidores Cisco UCS B-Series (al menos cuatro servidores blade Cisco UCS B200 M5)
- Dos controladoras AFF C190, AFF A250, FAS2750 o FAS2720 en una configuración de par de alta disponibilidad (requiere dos puertos de adaptador de destino unificado disponibles 2 [UTA2] por controladora).

FlexPod Express con E-Series

Los requisitos de hardware para la configuración inicial de FlexPod Express con E-Series incluyen:

- Dos interconexiones de estructura Cisco UCS 6324
- Un chasis Cisco UCS Mini 5108 AC2 o DC2 (las interconexiones de estructura Cisco UCS 6324 solo son compatibles con los chasis AC2 y DC2)
- Servidores Cisco UCS B-Series (al menos dos servidores blade Cisco UCS B200 M4)
- Una configuración de par de alta disponibilidad de un sistema de almacenamiento E-Series E2824 cargado con un mínimo de 12 unidades de disco
- Dos switches Ethernet estándar de 10 Gbps en una configuración redundante (se pueden utilizar los switches existentes del centro de datos)

Estos componentes de hardware son necesarios para crear una configuración inicial de la solución; se pueden agregar servidores blade y unidades de disco adicionales según sea necesario. El sistema de almacenamiento E-Series E2824 puede sustituirse por una plataforma superior, y también puede ejecutarse como un sistema all-flash.

Requisitos mínimos de software

En esta sección se describen los requisitos mínimos de software para las distintas versiones de FlexPod Express.

Requisitos de software para FlexPod Express con AFF o FAS de NetApp

Entre los requisitos de software de FlexPod Express con FAS de NetApp se incluyen:

- ONTAP 9.1 o posterior
- Cisco NX-OS versión 7.0(3)I6(1) o posterior
- En la configuración gestionada por Cisco UCS, Cisco UCS Manager UCS 4.0(1b)

Todo el software debe aparecer y ser compatible con la "IMT de NetApp". Algunas funciones de software pueden requerir versiones de código más recientes que los mínimos indicados en arquitecturas anteriores.

Requisitos de software para FlexPod Express con E-Series

Los requisitos de software de FlexPod Express con E-Series incluyen:

- Software SANtricity de E-Series 11.30 o posterior
- Cisco UCS Manager 4.0(1b).

Todo el software debe aparecer y ser compatible con la "IMT de NetApp".

Requisitos de conectividad

En esta sección se describen los requisitos de conectividad para las distintas versiones de FlexPod Express.

Requisitos de conectividad de FlexPod Express con FAS de NetApp

Entre los requisitos de conectividad de FlexPod Express con FAS de NetApp se incluyen:

- Las controladoras de almacenamiento FAS de NetApp deben estar conectadas directamente a los switches Cisco Nexus, excepto en la configuración gestionada por Cisco UCS, donde las controladoras de almacenamiento están conectadas a las interconexiones de estructura.
- No se puede colocar ningún equipo adicional entre los componentes FlexPod principales.
- Se necesitan canales de puertos virtuales (VPC) para conectar los switches Cisco Nexus serie 3000/9000 a las controladoras de almacenamiento de NetApp.
- Aunque no es necesario, se recomienda habilitar la compatibilidad con tramas gigantes en todo el entorno.

Requisitos de conectividad de FlexPod Express con E-Series de NetApp

Entre los requisitos de conectividad de FlexPod Express con E-Series se incluyen:

- Las controladoras de almacenamiento E-Series deben estar conectadas directamente a las interconexiones de estructura.
- No se debe colocar ningún equipo adicional entre los componentes FlexPod principales.
- Los ordenadores virtuales son necesarios entre las interconexiones de estructura y los switches Ethernet.

Requisitos de conectividad de FlexPod Express con AFF de NetApp

Entre los requisitos de conectividad de FlexPod Express con AFF de NetApp se incluyen:

- Las controladoras de almacenamiento AFF de NetApp se deben conectar directamente a los switches Cisco Nexus, excepto en la configuración gestionada por Cisco UCS, donde las controladoras de almacenamiento están conectadas al entramado. interconexiones.
- No se puede colocar ningún equipo adicional entre los componentes FlexPod principales.
- Se necesitan canales de puertos virtuales (VPC) para conectar los switches Cisco Nexus serie 3000/9000 a las controladoras de almacenamiento de NetApp.
- Aunque no es necesario, se recomienda habilitar la compatibilidad con tramas gigantes en todo el entorno.

Otros requisitos

Entre los requisitos adicionales de FlexPod Express se incluyen los siguientes:

- Se requieren contratos de soporte válidos para todo el equipo, incluidos:
  - SMARTnet admite el equipo de Cisco
  - Soporte de SupportEdge Advisor o SupportEdge Premium para equipos de NetApp
- Todos los componentes de software deben aparecer y admitidos en la "IMT de NetApp".
- Todos los componentes de hardware de NetApp deben aparecer y ser compatibles en "Hardware Universe de NetApp".
- Todos los componentes de hardware de Cisco deben aparecer y ser compatibles en "Cisco HCL".

Equipo existente

La siguiente tabla enumera las opciones de la controladora de almacenamiento heredada de NetApp.

Controladora de almacenamiento	Número de referencia de FAS	Especificaciones técnicas
FAS2520	Según las opciones individuales elegidas	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS2552	Según las opciones individuales elegidas	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS2554	Según las opciones individuales elegidas	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS8020	Según las opciones individuales elegidas	http://www.netapp.com/us/products/storage-systems/fas8000/fas8000-tech-specs.aspx

En la siguiente tabla se enumeran las opciones de bandeja de discos heredada de NetApp para FAS de NetApp.

Bandeja de discos	Número de pieza	Especificaciones técnicas
DE1600	E-X5682A-DM-0E-R6-C	"Especificaciones técnicas de las bandejas de discos unidades compatibles con Hardware Universe de NetApp"
DE5600	E-X4041A-12-R6	"Especificaciones técnicas de las bandejas de discos unidades compatibles con Hardware Universe de NetApp"

Bandeja de discos	Número de pieza	Especificaciones técnicas
DE6600	X-48564-00-R6	"Especificaciones técnicas de las bandejas de discos unidades compatibles con Hardware Universe de NetApp"

Controladoras FAS heredadas de NetApp

En la siguiente tabla aparecen las opciones de la controladora FAS de NetApp heredada.

Componente actual	FAS2554	FAS2552	FAS2520
Configuración	2 controladoras en un chasis de 4U	2 controladoras en un chasis de 2U	2 controladoras en un chasis de 2U
Capacidad bruta máxima	576 TB	509 TB	336 TB
Unidades internas	24	24	12
Número máximo de unidades (internas y externas)	144	144	84
Tamaño de volumen máximo	60 TB		
Tamaño máximo de agregado	120 TB		
Número máximo de LUN	2,048 por controladora		
Redes de almacenamiento compatibles	ISCSI, FC, FCoE, NFS y CIFS		ISCSI, NFS y CIFS
Número máximo de volúmenes FlexVol de NetApp	1,000 por controladora		
El número máximo de copias Snapshot de NetApp	255,000 por controladora		

Para obtener más modelos FAS de NetApp, consulte "Sección FAS modela" En la Hardware Universe.

Información adicional

Si quiere obtener más información sobre la información descrita en este documento, consulte los siguientes documentos y sitios web:

- Centro de documentación de los sistemas AFF y FAS

  "https://docs.netapp.com/platstor/index.jsp"

- Recursos de documentación de AFF

  "https://www.netapp.com/us/documentation/all-flash-fas.aspx"

- Página de recursos de documentación de FAS Storage Systems

  "https://www.netapp.com/us/documentation/fas-storage-systems.aspx"

- FlexPod

  "https://flexpod.com/"

- Documentación de NetApp

  "https://docs.netapp.com"

Especificaciones técnicas de FlexPod Datacenter

TR-4036: Especificaciones técnicas de FlexPod Datacenter

Arvind Ramakrishnan y Jyh-shing Chen, NetApp

La plataforma FlexPod es una arquitectura de centro de datos prediseñada con las mejores prácticas que se basa en Cisco Unified Computing System (Cisco UCS), la familia de switches Cisco Nexus y las controladoras de almacenamiento de NetApp (sistemas AFF, ASA o FAS).

FlexPod es una plataforma adecuada para ejecutar diversos hipervisores de virtualización, así como sistemas operativos con configuración básica y cargas de trabajo empresariales. FlexPod ofrece no solo una configuración básica, sino también la flexibilidad necesaria para ajustar el tamaño y optimizarse con el objetivo de acomodar distintos casos de uso y requisitos.

> Antes de solicitar una configuración FlexPod completa, consulte "Infraestructura convergente de FlexPod" página en netapp.com para la última versión de estas especificaciones técnicas.

"Siguiente: Plataformas FlexPod."

Plataformas FlexPod

Existen dos plataformas FlexPod:

- **FlexPod Datacenter.** esta plataforma es una infraestructura de centro de datos virtual enormemente escalable, adecuada para aplicaciones empresariales con cargas de trabajo; virtualización; infraestructura de escritorios virtuales (VDI); y cargas de trabajo de cloud público, privado e híbrido.
- **FlexPod EXPRESS.** Esta plataforma es una infraestructura convergente compacta pensada para casos de uso perimetrales y de oficinas remotas. FlexPod Express cuenta con sus propias especificaciones que se documentan en la "Especificaciones técnicas de FlexPod Express."

Este documento proporciona las especificaciones técnicas para la plataforma del centro de datos FlexPod.

Reglas de FlexPod

El diseño de FlexPod permite una infraestructura flexible que abarca muchos componentes y versiones de software diferentes.

Utilice los conjuntos de reglas como guía para crear o ensamblar una configuración de FlexPod válida. Los números y las reglas que se enumeran en este documento son los requisitos mínimos para una configuración de FlexPod. Pueden ampliarse en las familias de productos incluidas según sea necesario para diferentes entornos y casos de uso.

Compatible con configuraciones de FlexPod validadas frente a las validadas

La arquitectura de FlexPod está definida por el conjunto de reglas que se describen en este documento. Los componentes de hardware y las configuraciones de software deben ser compatibles con "Lista de compatibilidad de hardware y software de Cisco UCS" y la "Herramienta de matriz de interoperabilidad de NetApp (IMT)".

Cada Cisco Validated Design (CVD) o NetApp Verified Architecture (NVA) es una posible configuración de FlexPod. Cisco y NetApp documentan estas combinaciones de configuración y las validan mediante una exhaustiva prueba de extremo a extremo. Las instalaciones de FlexPod que no se puedan implementar con estas configuraciones son totalmente compatibles si siguen las directrices de este documento y si todos los componentes aparecen como compatibles en la lista de compatibilidad de hardware y software de Cisco UCS y NetApp "IMT".

Por ejemplo, añadir más controladoras de almacenamiento o servidores Cisco UCS y actualizar software a versiones más nuevas es totalmente compatible si el software, el hardware y las configuraciones cumplen las directrices definidas en este documento.

ONTAP de NetApp

El software ONTAP de NetApp está instalado en todos los sistemas de cabinas FAS, AFF y AFF All SAN (ASA). FlexPod se ha validado con el software ONTAP, por lo que proporciona una arquitectura de almacenamiento altamente escalable que permite operaciones no disruptivas, actualizaciones no disruptivas y una infraestructura de datos ágil.

Para obtener más información acerca de ONTAP, consulte "Software de gestión de datos ONTAP" página de producto.

Modos de funcionamiento de switches de Cisco Nexus

Puede utilizarse una variedad de productos Cisco Nexus como componente de conmutación de una determinada puesta en marcha de FlexPod. La mayoría de estas opciones aprovechan el SO Cisco Nexus o el software NX-OS tradicional. La familia de switches Cisco Nexus ofrece distintas funcionalidades dentro de sus líneas de productos. Estas funcionalidades se detallan más adelante en este documento.

La oferta de Cisco en el espacio de red definido por software se llama Application Centric Infrastructure (ACI). La línea de productos Cisco Nexus que admite el modo ACI, también llamado modo de estructura, es la serie Cisco Nexus 9300. Estos switches también se pueden poner en marcha en NX-OS o en modo independiente.

Cisco ACI se dirige a las puestas en marcha de centros de datos que se centran en los requisitos de una aplicación específica. Las aplicaciones se crean instancias mediante una serie de perfiles y contratos que permiten la conectividad desde el host o la máquina virtual (VM) hasta el almacenamiento a través de la red.

FlexPod está validado con ambos modos de funcionamiento de los switches Cisco Nexus. Para obtener más información acerca de los modos ACI y NX-OS, consulte las siguientes páginas Cisco:

- "Infraestructura centrada en aplicaciones de Cisco"
- "Software Cisco NX-OS"

Requisitos mínimos de hardware

Una configuración de FlexPod Datacenter tiene requisitos mínimos de hardware, incluidos, entre otros, switches, interconexiones de estructura, servidores y controladoras de almacenamiento de NetApp.

Se deben usar los servidores Cisco UCS. En los diseños validados se han utilizado tanto los servidores C-Series como los B-Series. Los extensores de estructura Cisco Nexus (FEXs) son opcionales con los servidores C-Series.

Una configuración FlexPod tiene los siguientes requisitos mínimos de hardware:

- Dos switches Cisco Nexus en una configuración redundante. Esta configuración puede consistir en dos switches redundantes de las series Cisco Nexus 5000, 7000 o 9000. Los dos conmutadores deben tener el mismo modelo y deben configurarse en el mismo modo de funcionamiento.

  Si va a implementar una arquitectura ACI, debe cumplir los siguientes requisitos adicionales:

  - Implemente los switches de la serie Cisco Nexus 9000 en una topología hoja-espina.
  - Utilice tres controladores de infraestructura de políticas de aplicaciones (APIC) de Cisco.
- Dos interconexiones de estructura de las series Cisco UCS 6200, 6300 o 6400 en una configuración redundante.
- Servidores Cisco UCS:
  - Si la solución utiliza servidores B-Series, un chasis de servidor blade Cisco UCS 5108 B-Series más dos servidores blade Cisco UCS B-Series más dos módulos de I/o 2104, 2204/8, 2408 o 2304 (IOM).
  - Si la solución utiliza servidores C-Series, dos servidores en rack Cisco UCS C-Series.

    Para puestas en marcha de servidores en rack Cisco UCS C-Series, puede elegir un par de módulos FEX 2232PP. Sin embargo, el 2232PP no es un requisito de hardware.
- Dos controladoras de almacenamiento de NetApp en una configuración de parejas de alta disponibilidad (ha):

  Esta configuración puede consistir de cualquier controladora de almacenamiento FAS, AFF o ASA de NetApp admitida. Consulte "Hardware Universe de NetApp" Aplicación para una lista actual de los modelos de controladoras FAS, AFF y ASA compatibles.

  - La configuración de alta disponibilidad requiere dos interfaces redundantes por controladora para el acceso a datos; las interfaces pueden ser FCoE, FC o Ethernet de 10/25 GB (GbE).
  - Si la solución utiliza ONTAP de NetApp, se requiere una topología de interconexión de clúster aprobada por NetApp. Para obtener más información, consulte "Interruptores" De Hardware Universe

de NetApp.

- Si la solución utiliza ONTAP, se requieren al menos dos puertos 10/25 GbE adicionales por controladora para acceder a los datos.
- En el caso de clústeres ONTAP con dos nodos, puede configurar un clúster sin switches de dos nodos.
- En el caso de los clústeres ONTAP con más de dos nodos, se necesitan algunos switches de interconexión de clúster.

- Una bandeja de discos de NetApp con cualquier tipo de disco compatible. Consulte la pestaña bandejas de "Hardware Universe de NetApp" para una lista actual de los modelos de bandejas de discos admitidos.

Requisitos mínimos de software

Una configuración de FlexPod tiene los siguientes requisitos mínimos de software:

- ONTAP de NetApp:
  - La versión del software ONTAP requiere ONTAP 9.1 o posterior
- Versiones de Cisco UCS Manager:
  - Interconexión de estructuras Cisco UCS de la serie 6200: 2.2 (8a)
  - Interconexión de estructuras Cisco UCS de la serie 6300: 3.1 (1e)
  - Interconexión de estructuras Cisco UCS de la serie 6400: 4.0(1)
- Modo gestionado por Cisco Intersight:
  - Interconexión de estructuras Cisco UCS de la serie 6400: 4.1(2)
- Para los switches Cisco Nexus serie 5000, la versión 5.0(3)N1(1c) o posterior del software Cisco NX-OS, incluida NX-OS 5.1.x.
- Para switches Cisco Nexus serie 7000:
  - El chasis de 4 ranuras requiere la versión 6.1(2) o posterior del software Cisco NX-OS
  - El chasis de 9 ranuras requiere la versión 5.2 o posterior del software Cisco NX-OS
  - El chasis de 10 ranuras requiere la versión 4.0 o posterior del software Cisco NX-OS
  - El chasis de 18 ranuras requiere la versión 4.1 o posterior del software Cisco NX-OS
- Para los switches de la serie Cisco Nexus 9000, la versión 6.1(2) o posterior del software Cisco NX-OS

> El software que se usa en una configuración FlexPod debe aparecer y ser compatible en NetApp "IMT". Es posible que algunas funciones requieran versiones más recientes del software que las enumeradas.

Requisitos de conectividad

Una configuración FlexPod tiene los siguientes requisitos de conectividad:

- Se requiere una red de gestión fuera de banda Ethernet de 100 Mbps y 1 GB independiente para todos los componentes.
- NetApp recomienda que habilite la compatibilidad con las tramas gigantes en todo el entorno, pero no es necesario.
- Los puertos de la aplicación Cisco UCS Fabric Interconnect solo se recomiendan para conexiones iSCSI y NAS.

- No se puede colocar ningún equipo adicional en línea entre los componentes principales de FlexPod.

Conexiones de enlace ascendente:

- Los puertos de las controladoras de almacenamiento de NetApp deben estar conectados a los switches de las series Cisco Nexus 5000, 7000 o 9000 para permitir la compatibilidad con los canales de puertos virtuales (VPC).
- Los ordenadores virtuales se requieren desde los switches de las series Cisco Nexus 5000, 7000 o 9000 a las controladoras de almacenamiento de NetApp.
- Los ordenadores virtuales se necesitan desde los switches de las series Cisco Nexus 5000, 7000 o 9000 a las interconexiones de estructura.
- Se requieren al menos dos conexiones para un VPC. Es posible aumentar el número de conexiones dentro de un VPC en función de los requisitos de carga de las aplicaciones y de rendimiento.

Conexiones directas:

- Los puertos de las controladoras de almacenamiento de NetApp que están conectados directamente a las interconexiones estructurales pueden agruparse para habilitar un canal de puertos. VPC no es compatible con esta configuración.
- Se recomiendan canales de puertos FCoE para diseños FCoE integrales.

Arranque SAN:

- Las soluciones FlexPod están diseñadas en torno a una arquitectura DE arranque SAN mediante los protocolos iSCSI, FC o FCoE. El uso de tecnologías "arranque desde SAN" proporciona la configuración más flexible de la infraestructura del centro de datos y permite disponer de las completas funciones de cada componente de la infraestructura. Aunque el arranque desde SAN es la configuración más eficiente, el arranque desde el almacenamiento de servidor local es una configuración válida y compatible.
- No se admite el arranque SAN sobre FC-NVME.

Otros requisitos

Una arquitectura de FlexPod tiene los siguientes requisitos adicionales de interoperabilidad y soporte:

- Todos los componentes de hardware y software deben aparecer y ser compatibles con NetApp "IMT", la "Lista de compatibilidad de hardware y software de Cisco UCS"Y la herramienta de matriz de interoperabilidad de hardware y software Cisco UCS.
- Se requieren contratos de soporte válidos para todo el equipo, incluidos:
  - Soporte de Smart Net total Care (SmartNet) para equipos de Cisco
  - Soporte de SupportEdge Advisor o SupportEdge Premium para equipos de NetApp

Si quiere más información, consulte NetApp "IMT".

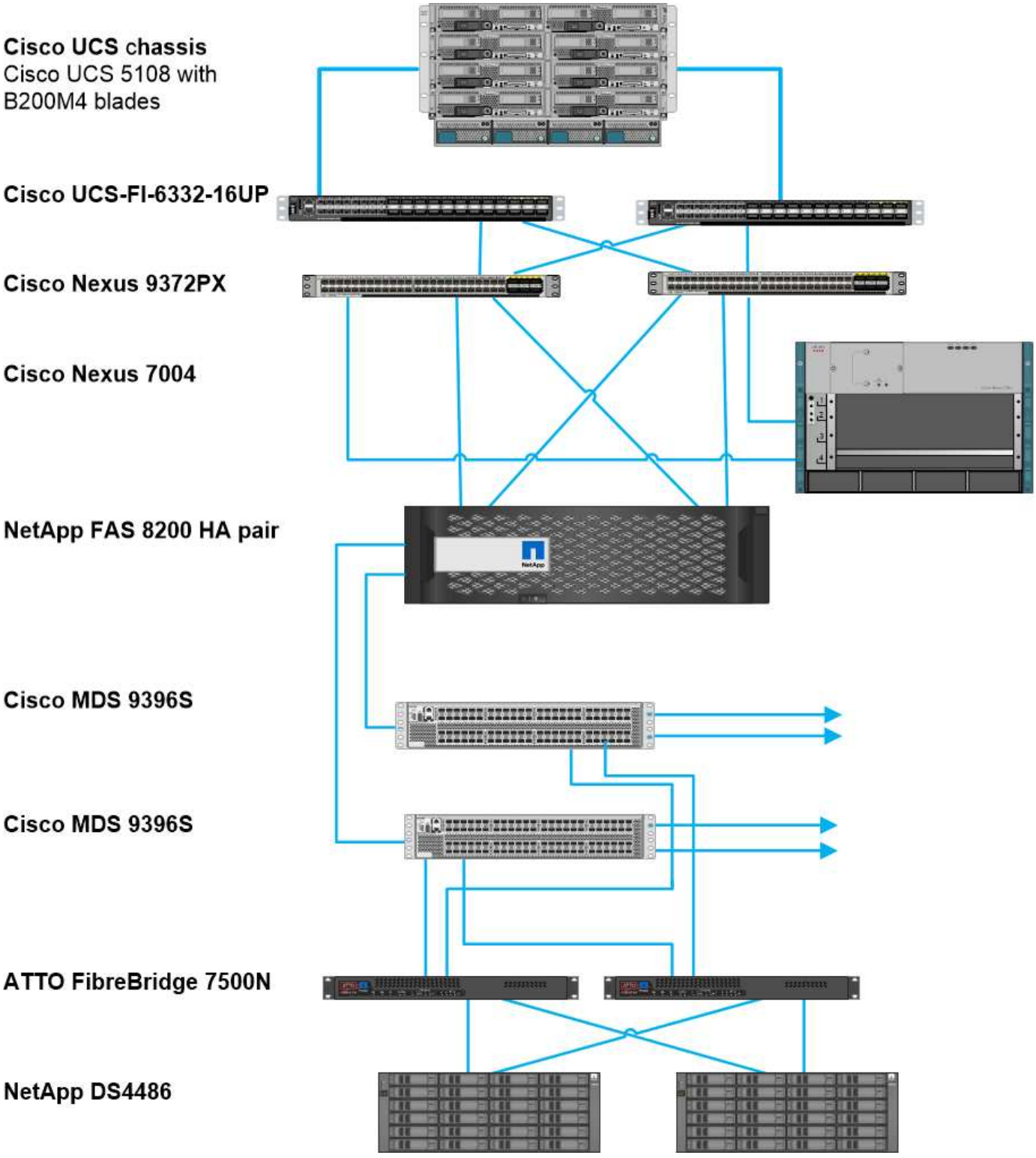
Funciones opcionales

NetApp admite varios componentes opcionales para mejorar aún más las arquitecturas de centros de datos de FlexPod. Los componentes opcionales se describen en las subsecciones siguientes.

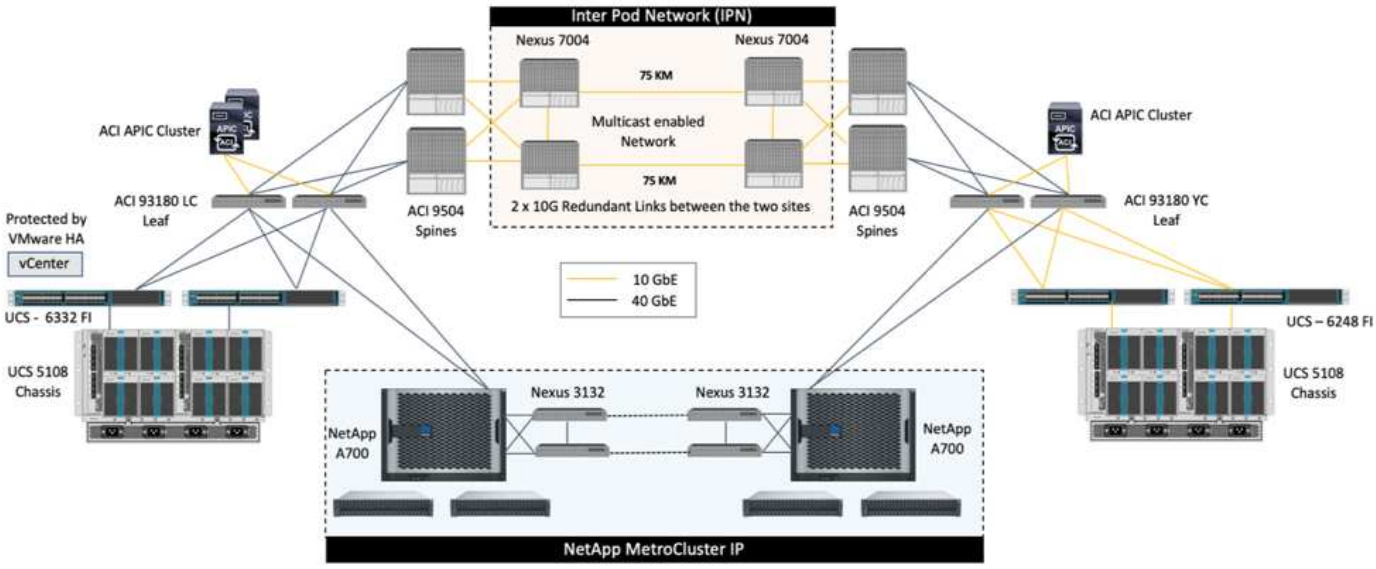
MetroCluster

FlexPod es compatible con ambas variantes del software MetroCluster de NetApp para una disponibilidad continua, en configuraciones de clústeres de dos o cuatro nodos. MetroCluster proporciona replicación síncrona para cargas de trabajo cruciales. Requiere una configuración de sitio doble conectada con switches de Cisco. La distancia máxima admitida entre los sitios es aproximadamente de 300 km (186 millas) para MetroCluster FC y aumenta a 700 km (435 millas) aproximadamente para MetroCluster IP. Las siguientes figuras ilustran un centro de datos FlexPod con arquitectura MetroCluster de NetApp y el centro de datos FlexPod con arquitectura MetroCluster IP de NetApp, respectivamente.

La figura siguiente muestra el centro de datos FlexPod con la arquitectura MetroCluster de NetApp.

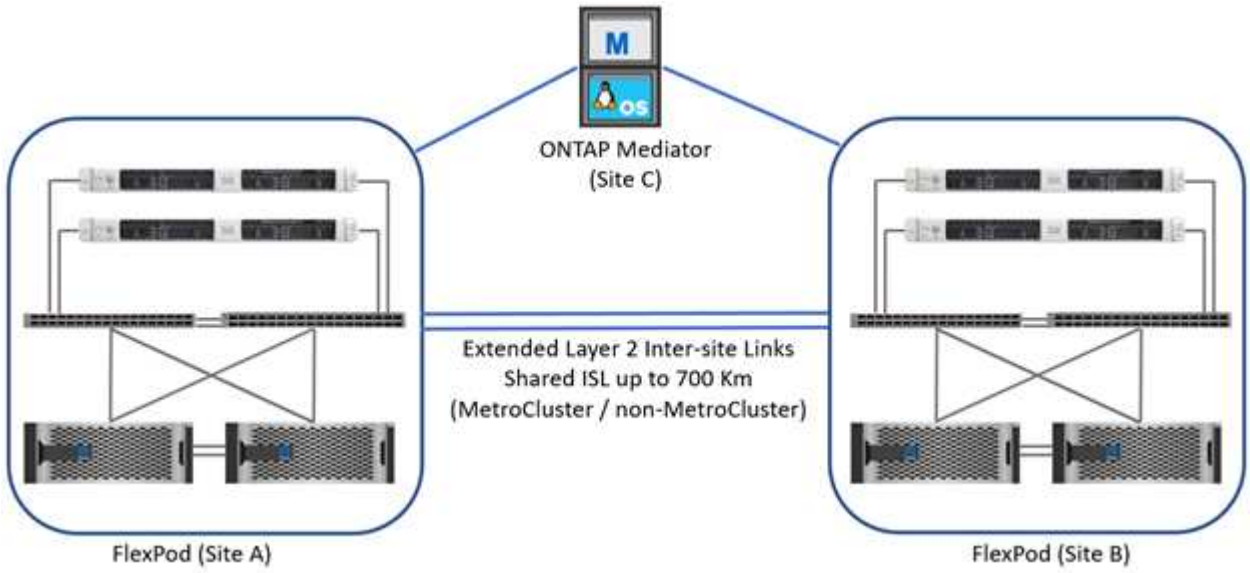


La siguiente figura muestra el centro de datos FlexPod con la arquitectura IP de MetroCluster de NetApp.



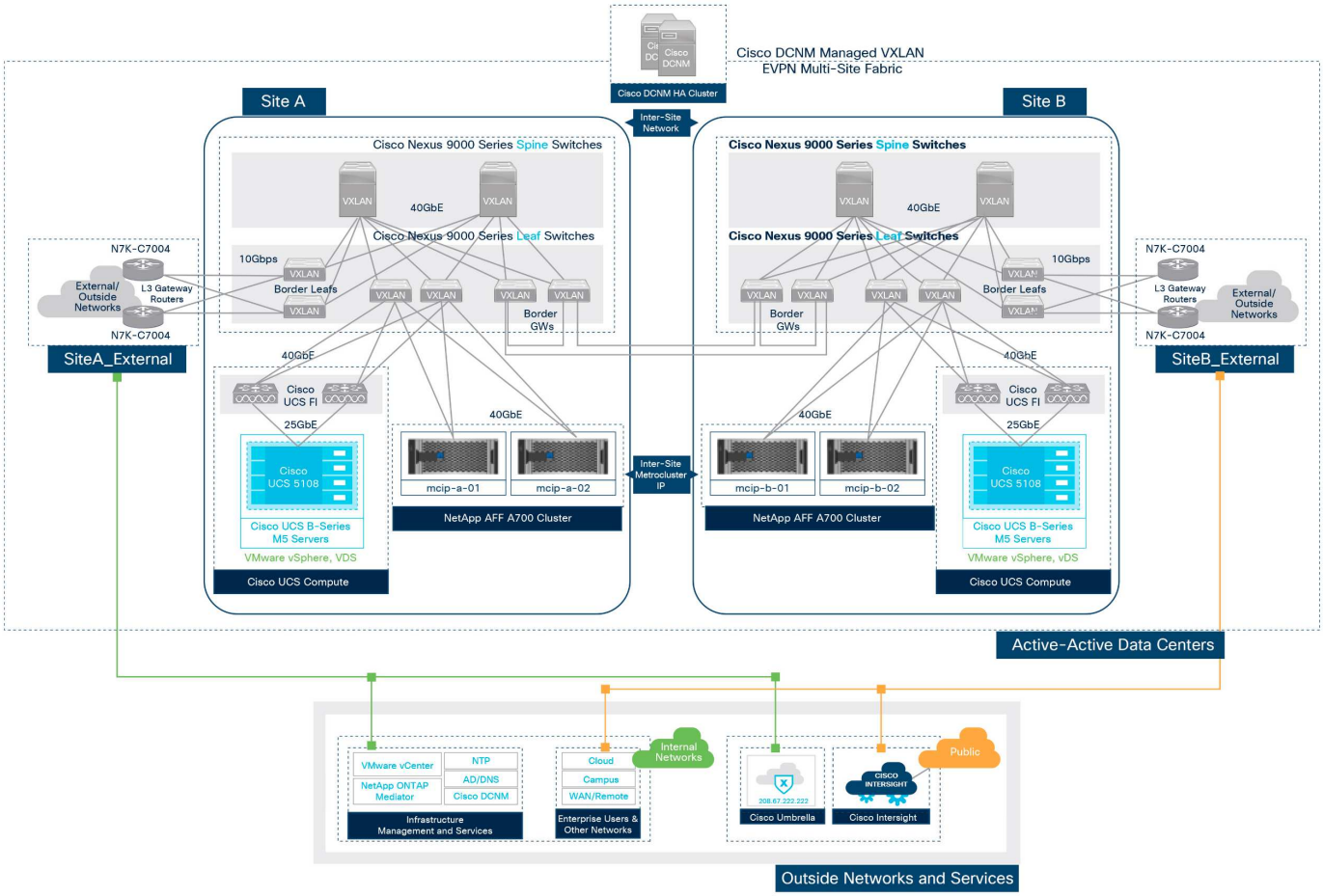
A partir de ONTAP 9.8, ONTAP Mediator se puede instalar en un tercer sitio para supervisar la solución IP de MetroCluster y facilitar una conmutación de sitios no planificada automática cuando se produce un desastre en el sitio.

Para la puesta en marcha de una solución IP de FlexPod MetroCluster con conectividad de sitio a sitio de capa 2 ampliada, se puede lograr una reducción de costes al compartir ISL y utilizar switches FlexPod como switches IP de MetroCluster compatibles si el ancho de banda y los switches de red cumplen los requisitos tal y como se muestra en la siguiente figura. Que muestra la solución IP de FlexPod MetroCluster con el uso compartido de ISL y switches conformes con la normativa.

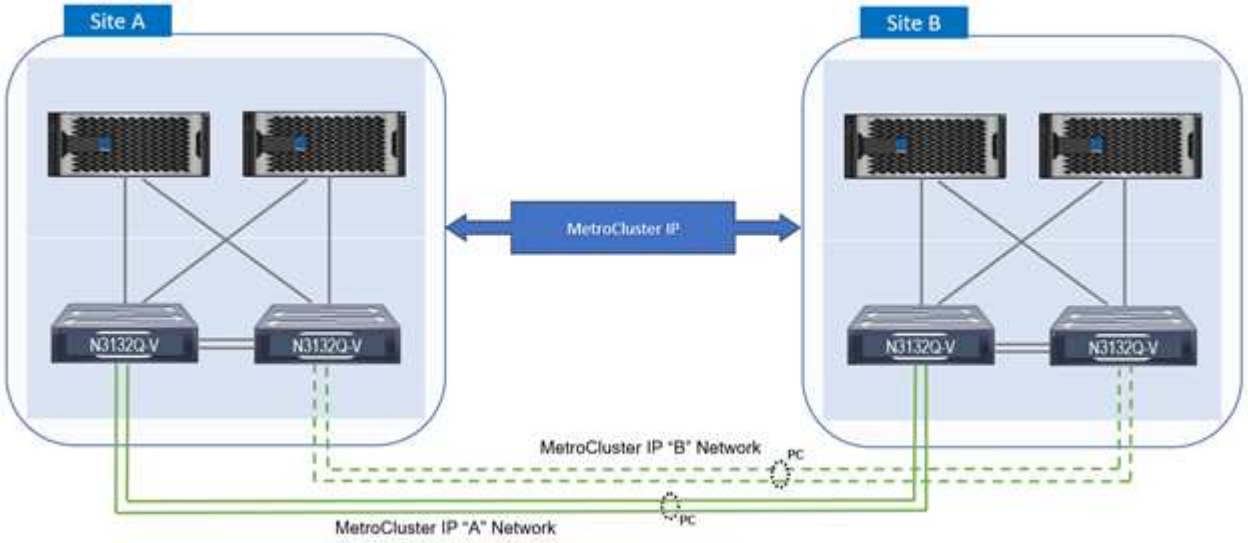


Las dos figuras siguientes muestran la estructura multisitio VXLAN y la estructura de almacenamiento IP MetroCluster para una solución IP FlexPod MetroCluster con implementación de estructura multisitio VXLAN.

- Solución de estructura multisitio VXLAN para FlexPod MetroCluster IP



- Estructura de almacenamiento IP de MetroCluster para solución FlexPod MetroCluster IP



FC-NVMe integral

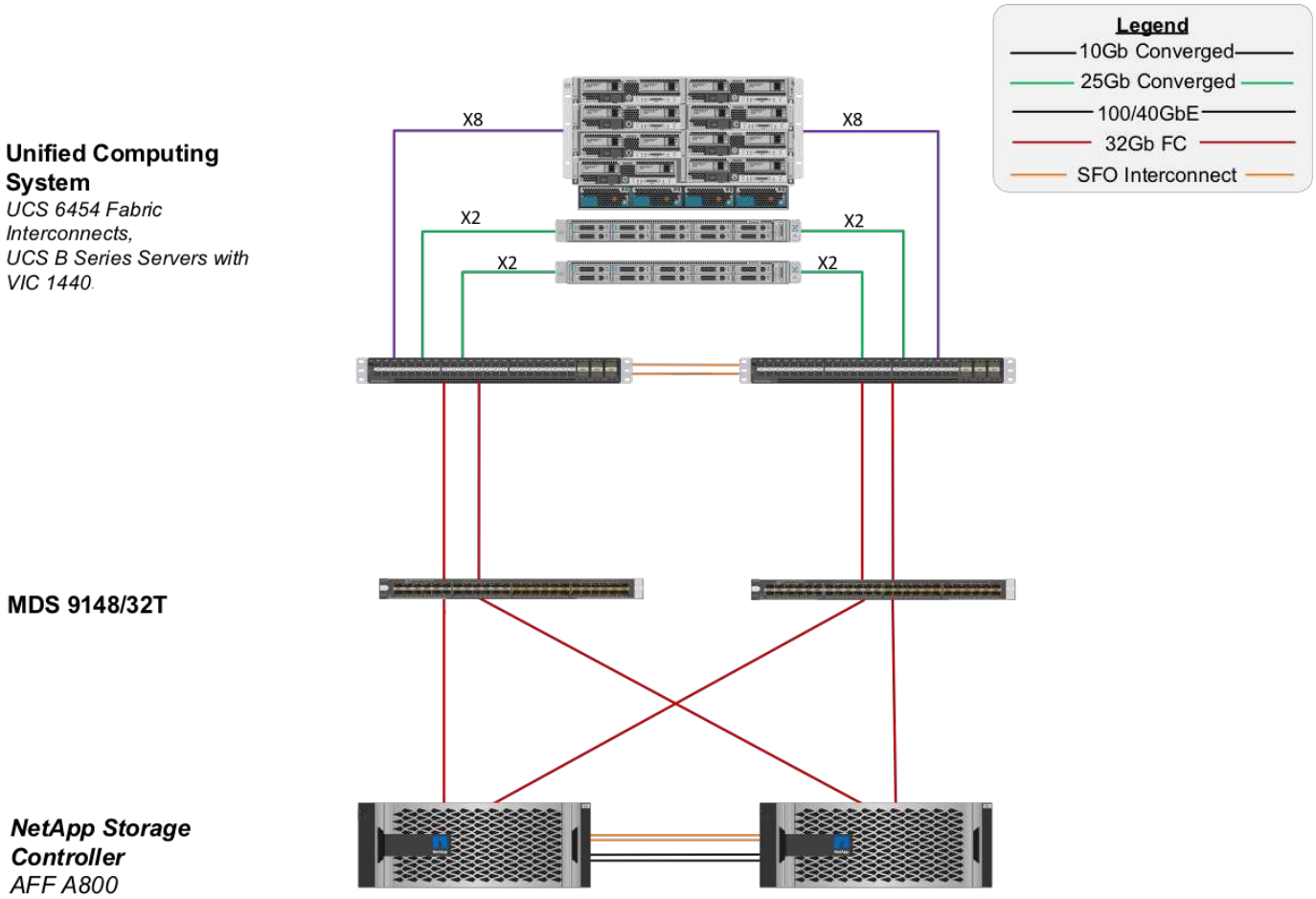
Un FC-NVMe integral amplía sin problemas la infraestructura SAN existente del cliente para aplicaciones en tiempo real a la vez que ofrece una tasa de IOPS y un rendimiento mejorados con una latencia reducida.

Se puede utilizar un transporte SAN FC de 32 GB existente para transportar simultáneamente cargas de trabajo tanto NVMe como SCSI.

La siguiente figura muestra el centro de datos FlexPod para FC con Cisco MDS.

Si desea obtener más información sobre las configuraciones de FlexPod y las ventajas de rendimiento, consulte "Presentación del whitepaper integral sobre NVMe para FlexPod."

Para obtener más información sobre la implantación de ONTAP, consulte "TR-4684: Implementación y configuración de San modernas con NVMe".



Arranque FC SAN mediante Cisco MDS

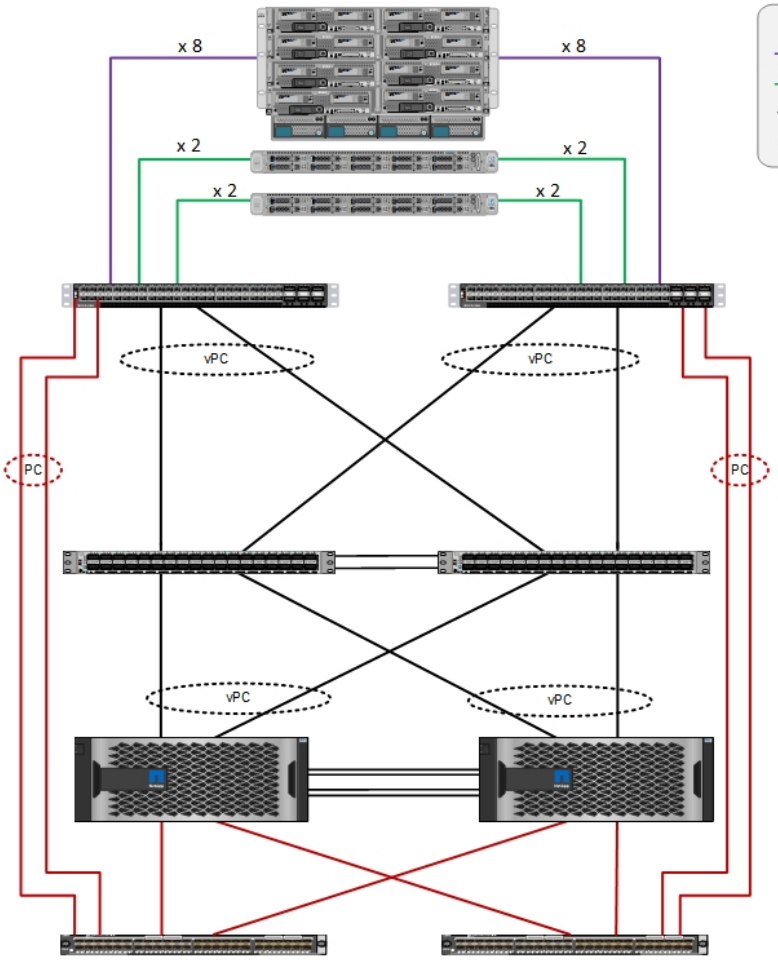
Para proporcionar una mayor escalabilidad mediante el uso de una red SAN dedicada, FlexPod admite switches FC a través de switches Cisco MDS y switches Nexus con compatibilidad con FC como Cisco Nexus 93108TC-FX. La opción de arranque SAN FC a través de Cisco MDS tiene los siguientes requisitos de licencia y hardware:

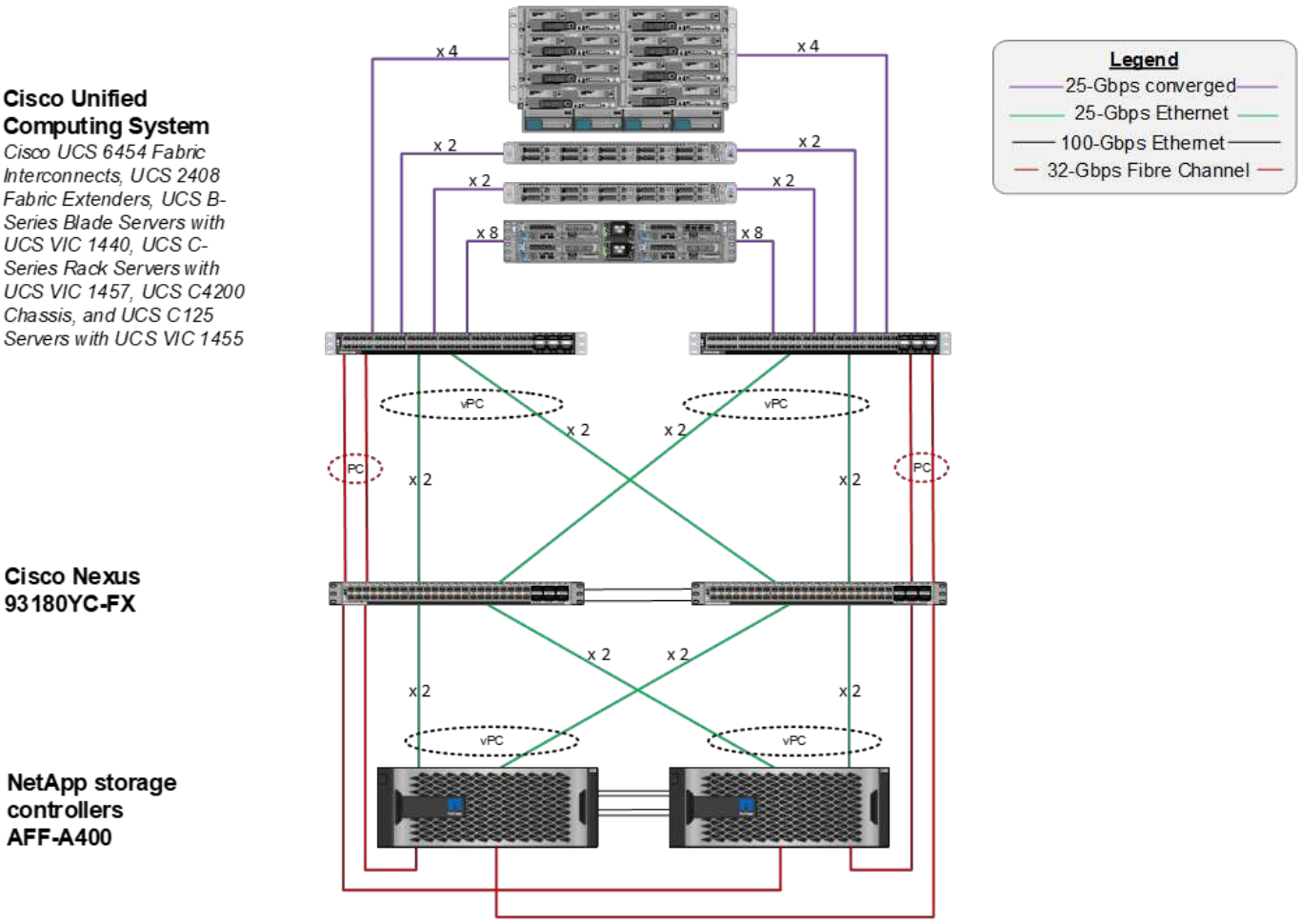
- Un mínimo de dos puertos FC por controladora de almacenamiento de NetApp; un puerto por cada estructura DE SAN
- Una licencia de FC en cada controladora de almacenamiento de NetApp
- Los switches Cisco MDS y las versiones de firmware compatibles con NetApp "IMT"

Para obtener más información sobre un diseño basado en MDS, consulte el CVD "Guía de implementación de FlexPod Datacenter con VMware vSphere 6.7U1: Fibre Channel e iSCSI".

Las siguientes figuras muestran un ejemplo de centro de datos FlexPod para FC con conectividad MDS y de

centro de datos FlexPod para FC con Cisco Nexus 93180YC-FX, respectivamente.





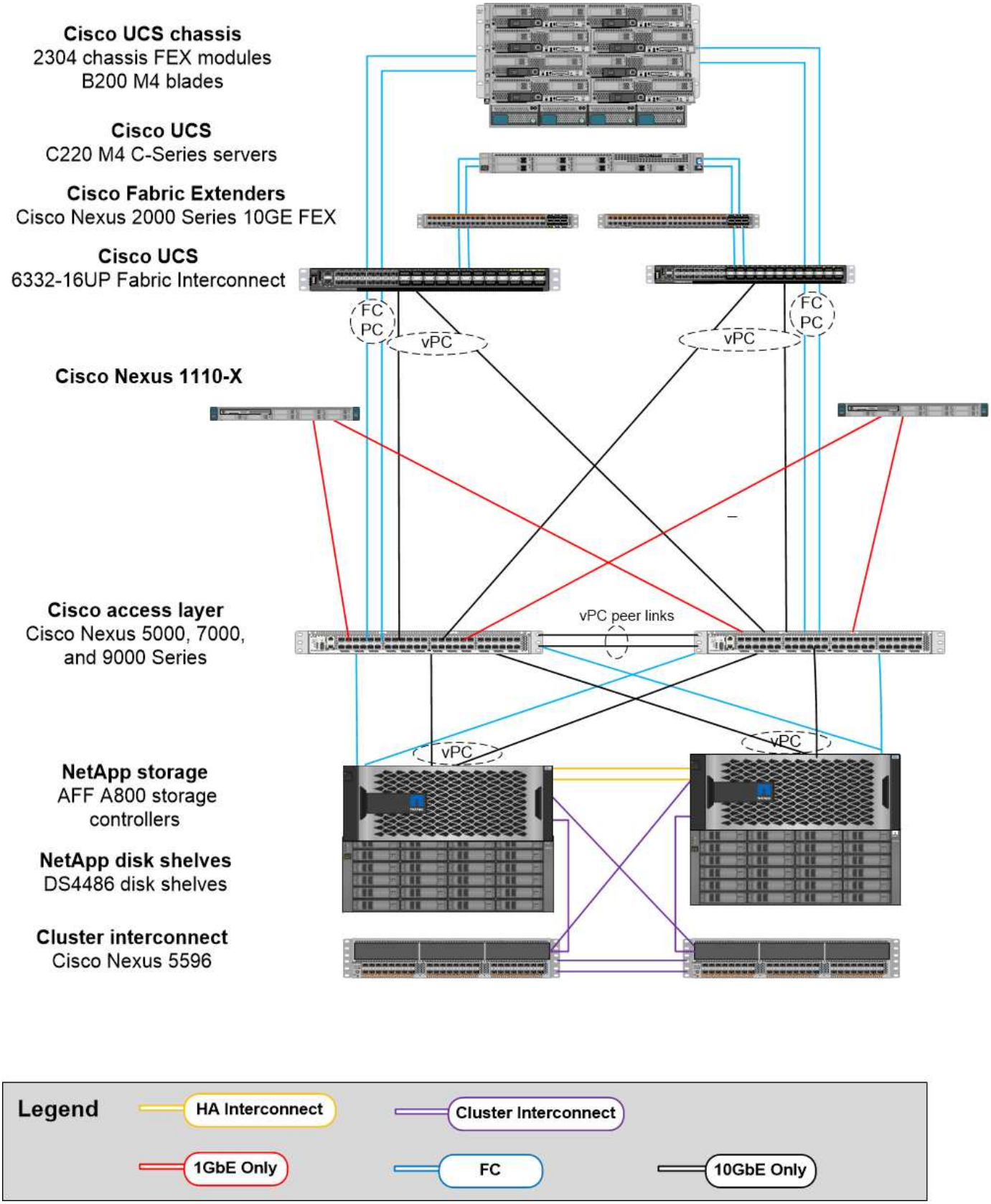
Arranque SAN FC con Cisco Nexus

La opción de arranque SAN FC clásica tiene los siguientes requisitos de licencia y hardware:

- Cuando se realiza la división en zonas de FC en el switch Cisco Nexus 5000 Series, se requiere una licencia del paquete de servicios de protocolos de almacenamiento para los switches Cisco Nexus 5000 Series (FC_FEATURES_PKG).
- Cuando se realiza la división en zonas de FC en el switch Cisco Nexus 5000 Series, se requieren enlaces SAN entre la interconexión de estructura y el switch Cisco Nexus 5000 Series. Para obtener redundancia adicional, se recomiendan canales DE puertos SAN entre los enlaces.
- Los switches Cisco Nexus 5010, 5020 y 5548P requieren un módulo de puerto FC o universal (SUPERIOR) independiente para la conectividad con la interconexión de estructura Cisco UCS y con la controladora de almacenamiento de NetApp.
- Cisco Nexus 93180YC-FX requiere una licencia de características de FC para poder habilitar FC.
- Cada controladora de almacenamiento de NetApp requiere un mínimo de dos puertos FC de 8/16 GB para conectividad.
- Se requiere una licencia de FC en la controladora de almacenamiento de NetApp.

> El uso de la familia de switches Cisco Nexus 7000 o 9000 impide el uso de FC tradicional a menos que se realice la división en zonas de FC en la interconexión de estructura. En ese caso, no se admiten los vínculos superiores SAN al switch.

La siguiente figura muestra una configuración de conectividad de FC.



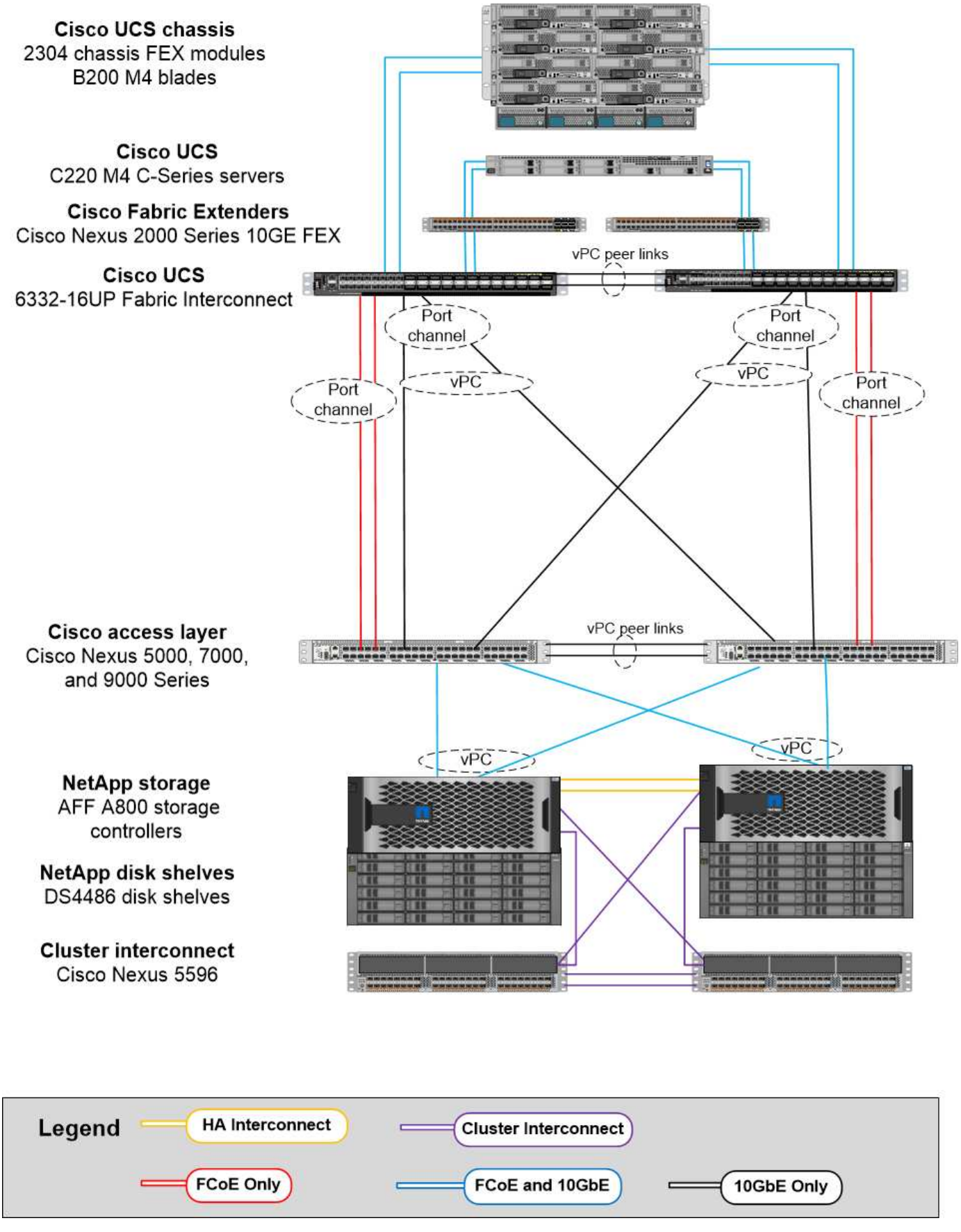
Opción de arranque FCoE SAN

La opción de arranque SAN FCoE tiene los siguientes requisitos de licencia y hardware:

- Cuando se realiza una división en zonas de FC en el switch, una licencia del paquete de servicio de protocolos de almacenamiento para los switches de las series Cisco Nexus 5000 o 7000 (`FC_FEATURES_PKG`) es necesario.
- Cuando se realiza la división en zonas de FC en el switch, se necesitan enlaces ascendentes FCoE entre la interconexión de estructura y los switches de las series Cisco Nexus 5000 o 7000. Para obtener redundancia adicional, también se recomiendan canales de puertos FCoE entre los enlaces.
- Cada controladora de almacenamiento de NetApp requiere al menos una tarjeta complementaria de adaptador de objetivo unificado (UTA) de doble puerto para conectividad FCoE, a menos que haya puertos presentes el adaptador de destino unificado 2 (UTA2) integrados.
- Esta opción requiere una licencia de FC en la controladora de almacenamiento de NetApp.
- Si utiliza los switches Cisco Nexus serie 7000 y la división en zonas de FC se lleva a cabo en el switch, es necesaria una tarjeta de línea capaz de admitir FCoE.

> El uso de switches de la serie Cisco Nexus 9000 excluye el uso de FCoE, a menos que se realice la división en zonas de FC en la interconexión de estructura y el almacenamiento esté conectado a las interconexiones de estructura con puertos del dispositivo. En ese caso, no se admiten los enlaces ascendentes FCoE para el switch.

En la siguiente figura se muestra un escenario de arranque FCoE.


Cisco UCS chassis
2304 chassis FEX modules
B200 M4 blades
Cisco UCS
C220 M4 C-Series servers
Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX
Cisco UCS
6332-16UP Fabric Interconnect
vPC peer links
Port channel
Port channel
Port channel
vPC
vPC
Port channel
Cisco access layer
Cisco Nexus 5000, 7000, and 9000 Series
vPC peer links
vPC
vPC
NetApp storage
AFF A800 storage controllers
NetApp disk shelves
DS4486 disk shelves
Cluster interconnect
Cisco Nexus 5596
Legend
HA Interconnect
Cluster Interconnect
FCoE Only
FCoE and 10GbE
10GbE Only

Opción de arranque iSCSI

La opción de arranque iSCSI tiene los siguientes requisitos de licencia y hardware:

- Se requiere una licencia de iSCSI en la controladora de almacenamiento de NetApp.
- Se requiere un adaptador en el servidor Cisco UCS que sea capaz de arrancar iSCSI.
- Se requiere un adaptador Ethernet de dos puertos 10 Gbps en la controladora de almacenamiento de NetApp.

La siguiente figura muestra una configuración solo Ethernet que se inicia utilizando iSCSI.

Cisco UCS chassis
2304 Chassis FEX modules
B200 M4 blades

Cisco UCS
C220 M4 C-Series servers

Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX

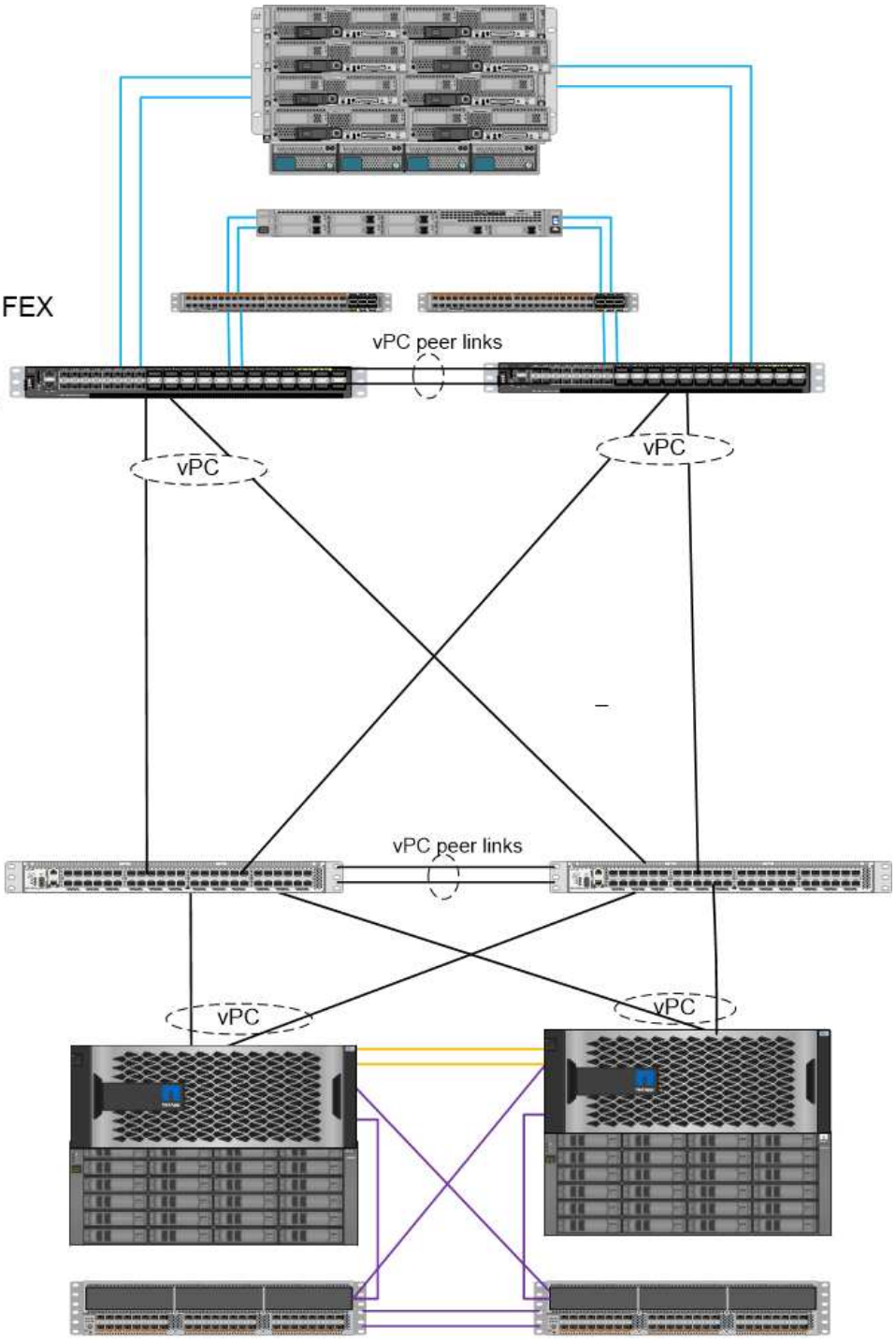
Cisco UCS
6332-16UP Fabric Interconnect

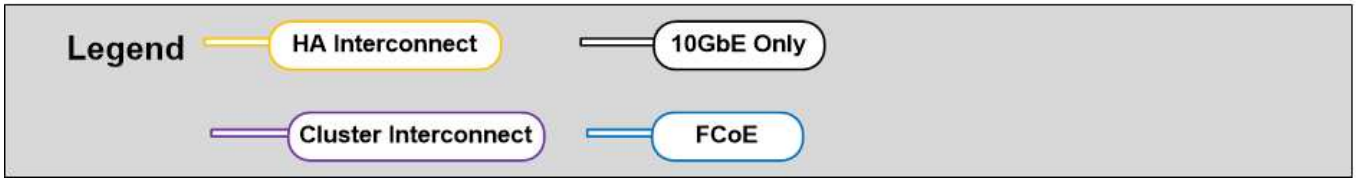
Cisco access layer
Cisco Nexus 5000, 7000, and 9000 Series

NetApp storage
AFF A800 storage controllers

NetApp disk shelves
DS4486 Disk shelves

Cluster Interconnect
Cisco Nexus 5596





Cisco UCS se conecta directamente con el almacenamiento de NetApp

Las controladoras AFF y FAS de NetApp se pueden conectar directamente a las interconexiones de estructura de Cisco UCS sin tener que hacer ningún switch SAN aguas arriba.

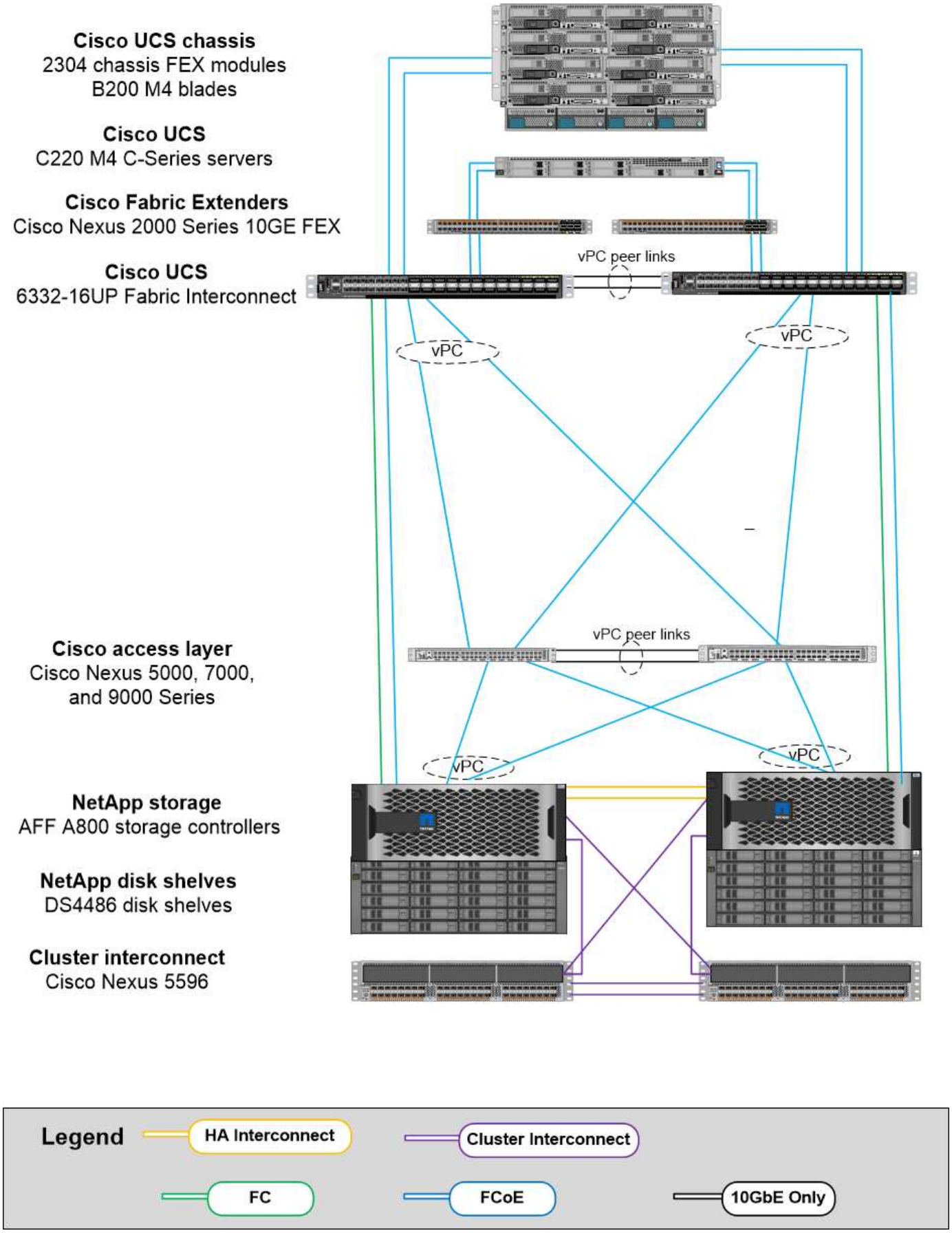
Se pueden utilizar cuatro tipos de puertos Cisco UCS para conectarse directamente con el almacenamiento de NetApp:

- **Puerto FC de almacenamiento.** Conecte directamente este puerto a un puerto FC en el sistema de almacenamiento NetApp.
- **Puerto FCoE de almacenamiento.** Conecte directamente este puerto a un puerto FCoE en el sistema de almacenamiento NetApp.
- **Puerto del dispositivo.** Conecte directamente este puerto a un puerto 10GbE en almacenamiento NetApp.
- **Puerto de almacenamiento unificado.** Conecte directamente este puerto a un UTA de NetApp.

Los requisitos de licencia y hardware son los siguientes:

- Se requiere una licencia de protocolo en la controladora de almacenamiento de NetApp.
- Se requiere un adaptador (iniciador) de Cisco UCS en el servidor. Para obtener una lista de adaptadores de Cisco UCS compatibles, consulte NetApp "IMT".
- Se requiere un adaptador de destino en la controladora de almacenamiento de NetApp.

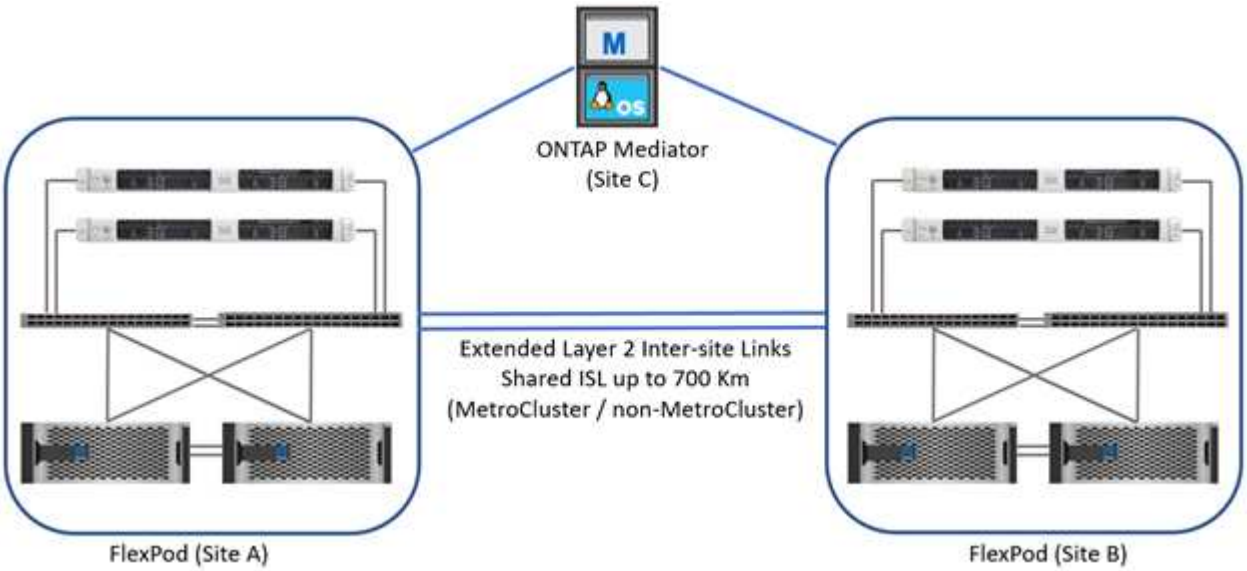
En la siguiente figura se muestra una configuración de conexión directa FC.


Cisco UCS chassis
2304 chassis FEX modules
B200 M4 blades
Cisco UCS
C220 M4 C-Series servers
Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX
Cisco UCS
6332-16UP Fabric Interconnect
vPC peer links
vPC
vPC
Cisco access layer
Cisco Nexus 5000, 7000,
and 9000 Series
vPC peer links
vPC
vPC
NetApp storage
AFF A800 storage controllers
NetApp disk shelves
DS4486 disk shelves
Cluster interconnect
Cisco Nexus 5596
Legend
HA Interconnect
Cluster Interconnect
FC
FCoE
10GbE Only

Notas:

- Cisco UCS se configura en modo de conmutación FC.
- Los puertos FCoE de destino a las interconexiones de estructura se configuran como puertos de almacenamiento FCoE.
- Los puertos FC del destino a las interconexiones de estructura se configuran como puertos de almacenamiento FC.

En la siguiente figura se muestra una configuración de conexión directa iSCSI/Unified IP.



Notas:

- Cisco UCS se configura en el modo de conmutación Ethernet.
- Los puertos iSCSI del destino a las interconexiones de estructura se configuran como puertos de almacenamiento Ethernet para datos iSCSI.
- Los puertos Ethernet del destino a las interconexiones de estructura se configuran como puertos de almacenamiento Ethernet para datos CIFS/NFS.

Componentes de Cisco

Cisco ha contribuido de forma sustancial al diseño y la arquitectura de FlexPod, que abarcan tanto las capas de computación como de red de la solución. En esta sección se describen las opciones de Cisco UCS y Cisco Nexus disponibles para FlexPod. FlexPod es compatible con los servidores Cisco UCS B-Series y C-Series.

Opciones de interconexión de estructura Cisco UCS

Se necesitan interconexiones de estructura redundantes en la arquitectura de FlexPod. Cuando se añaden varios chasis Cisco UCS a un par de interconexiones de estructura, recuerde que el número máximo de chasis de un entorno está determinado por el límite de arquitectura y de puerto.

Los números de pieza que se muestran en la siguiente tabla son para las interconexiones de la estructura base. No incluyen la unidad de suministro de alimentación (PSU) o los módulos de ampliación SFP+, QSFP+ o . Se admiten interconexiones de estructura adicionales. Consulte "IMT de NetApp" para ver una lista completa.

Interconexión de estructura Cisco UCS	Número de pieza	Especificaciones técnicas
Cisco UCS 6332UP	UCS-FI-6332-UP	"Interconexión de estructura Cisco UCS 6332"
Cisco UCS 6454	UCS-FI-6454-U	"Interconexión de estructura Cisco UCS 6454"

Cisco UCS 6454

Cisco UCS 6454 Series ofrece conectividad Ethernet y FCoE de 10/25/40 GbE sin pérdidas, con velocidad de línea y baja latencia, así como puertos unificados capaces de funcionar Ethernet o FC. Los puertos de 44 10 Gbps pueden funcionar como Ethernet convergente de 10 Gbps o 25 Gbps, de los cuales ocho son puertos unificados que pueden funcionar a 8/16 Gbps para FC. Cuatro puertos operan a 1/10 Gbps para la conectividad anterior, y seis puertos QSFP sirven como puertos de enlace ascendente 40/100 Gbps o puertos de arranque. Puede establecer una conectividad de red integral de 100 Gbps con controladoras de almacenamiento de NetApp que admitan adaptadores de 100 Gbps. Para conocer los adaptadores y el soporte de la plataforma, consulte "Hardware Universe de NetApp".

Para obtener detalles acerca de los puertos, consulte "Interconexión de estructura Cisco UCS 6454" Ficha técnica.

Para obtener especificaciones técnicas sobre los módulos de datos QSFP de 100 GB, consulte "Especificaciones técnicas de los módulos QSFP Cisco 100GBASE".

Opción de chasis Cisco UCS B-Series

Para usar blades Cisco UCS B-Series, debe tener un chasis Cisco UCS B-Series. La tabla siguiente describe la opción de chasis Cisco UCS BSeries.

Chasis Cisco UCS B-Series	Número de pieza	Especificaciones técnicas
Cisco UCS 5108	N20-C6508	"Chasis de servidor blade Cisco UCS serie 5100"

Cada chasis blade Cisco UCS 5108 debe tener dos IOM de la serie Cisco UCS 2200/2300/2400 para proporcionar conectividad redundante a las interconexiones de estructura.

Opciones del servidor blade Cisco UCS serie B

Los servidores blade Cisco UCS B-Series están disponibles en variedades de ancho medio y ancho total con diversas opciones de CPU, memoria e I/O. Los números de pieza que se enumeran en la tabla siguiente son para el servidor base. No incluyen la CPU, la memoria, las unidades ni las tarjetas adaptadoras mezzanine. La arquitectura FlexPod admite varias opciones de configuración.

Blade Cisco UCS serie B	Número de pieza	Especificaciones técnicas
CISCO UCS B200 M6	UCSB-B200-M6	"Servidor blade Cisco UCS B200 M6"

Las generaciones anteriores de blades Cisco UCS B-Series pueden utilizarse en la arquitectura FlexPod, si son compatibles con la "Lista de compatibilidad de hardware y software de Cisco UCS". Los servidores blade Cisco UCS B-Series también deben tener un contrato de soporte SmartNet válido.

Opción de chasis Cisco UCS X-Series

Para usar nodos de computación Cisco UCS X-Series, debe tener un chasis Cisco UCS X-Series. En la siguiente tabla se describe la opción del chasis Cisco UCS X-Series.

Blade Cisco UCS serie X	Número de pieza	Especificaciones técnicas
Cisco UCS 9508 M6	UCSX-9508	"Chasis Cisco UCX9508 de la serie X."

Cada chasis Cisco UCS 9508 debe tener dos módulos de estructura inteligente (IFMS) Cisco UCS 9108 para proporcionar conectividad redundante a las interconexiones de estructura.

Opciones de dispositivos Cisco UCS X-Series

Los nodos de computación Cisco UCS X-Series están disponibles con diversas opciones de CPU, memoria e I/O. Los números de pieza enumerados en la siguiente tabla son para el nodo base. No incluyen la CPU, la memoria, las unidades ni las tarjetas adaptadoras mezzanine. La arquitectura FlexPod admite varias opciones de configuración.

Nodos de computación Cisco UCS X-Series	Número de pieza	Especificaciones técnicas
Cisco UCS X210c M6	UCSX-210C-M6	"Nodo de computación Cisco UCS X210c M6"

Opciones del servidor de montaje en rack Cisco UCS C-Series

Los servidores en rack Cisco UCS C-Series están disponibles en una y dos variedades de unidad de rack (RU) con varias opciones de CPU, memoria e I/O. Los números de pieza que se enumeran en la segunda tabla siguiente son para el servidor base. No incluyen CPU, memoria, unidades, tarjetas Peripheral Component Interconnect Express (PCIe) ni Cisco Fabric extender. La arquitectura FlexPod admite varias opciones de configuración.

En la siguiente tabla se enumeran las opciones del servidor en rack Cisco UCS C-Series.

Servidor de montaje en rack Cisco UCS C-Series	Número de pieza	Especificaciones técnicas
CISCO UCS C220 M6	UCSC-C220-M6	"Servidor en rack Cisco UCS C220 M6"
CISCO UCS C225 M6	UCSC-C225-M6	"Servidor en rack Cisco UCS C225 M6"
CISCO UCS C240 M6	UCSC-C240-M6	"Servidor en rack Cisco UCS C240 M6"
CISCO UCS C245 M6	UCSC-C245-M6	"Servidor en rack Cisco UCS C245 M6"

Las generaciones anteriores de servidores Cisco UCS C-Series pueden utilizarse en la arquitectura FlexPod, si son compatibles con "Lista de compatibilidad de hardware y software de Cisco UCS". Los servidores Cisco UCS C-Series también deben tener un contrato de soporte SmartNet válido.

Opciones del switch Cisco Nexus serie 5000

Se necesitan switches redundantes de la serie Cisco Nexus 5000, 7000 o 9000 en la arquitectura FlexPod. Los números de pieza que se enumeran en la tabla siguiente son para el chasis de la serie Cisco Nexus 5000; no incluyen módulos SFP, módulos FC adicionales o módulos Ethernet.

Switch Cisco Nexus 5000 Series	Número de pieza	Especificaciones técnicas
Cisco Nexus 56128P	N5K-C56128P	"Switches de la plataforma Cisco Nexus 5600"
Cisco Nexus 5672UP de 16 G	N5K-C5672UP-16G	
Cisco Nexus 5596UP	N5K-C5596UP-FA	"Switches Cisco Nexus 5548 y 5596"
Cisco Nexus 5548UP	N5K-C5548UP-FA	

Opciones de switch Cisco Nexus serie 7000

Se necesitan switches redundantes de la serie Cisco Nexus 5000, 7000 o 9000 en la arquitectura FlexPod. Los números de pieza que se enumeran en la siguiente tabla son para el chasis Cisco Nexus serie 7000; no incluyen módulos SFP, tarjetas de línea ni suministros de alimentación, pero incluyen bandejas de ventiladores.

Switch Cisco Nexus 7000 Series	Número de pieza	Especificaciones técnicas
Cisco Nexus 7004	N7K-C7004	"Switch Cisco Nexus de 7000 4 ranuras"
Cisco Nexus 7009	N7K-C7009	"Switch Cisco Nexus de 7000 9 ranuras"
Cisco Nexus 7702	N7K-C7702	"Switch Cisco Nexus 7700 de 2 ranuras"
Cisco Nexus 7706	N77-C7706	"Switch Cisco Nexus de 7700 6 ranuras"

Opciones de switch Cisco Nexus serie 9000

Se necesitan switches redundantes de la serie Cisco Nexus 5000, 7000 o 9000 en la arquitectura FlexPod. Los números de pieza que se enumeran en la tabla siguiente son para el chasis de la serie Cisco Nexus 9000; no incluyen módulos SFP ni módulos Ethernet.

Switch Cisco Nexus 9000 Series	Número de pieza	Especificaciones técnicas
Cisco Nexus 93180YC-FX	N9K-C93180YC-FX	"Switches Cisco Nexus serie 9300"
Cisco Nexus 93180YC-EX	N9K-93180YC-EX	
Troncal de Cisco Nexus 9336PQ ACI	N9K-C9336PQ	
Cisco Nexus 9332PQ	N9K-C9332PQ	
Cisco Nexus 9336C-FX2	N9K-C9336C-FX2	
Cisco Nexus 92304QC	N9K-C92304QC	"Switches Cisco Nexus serie 9200"
Cisco Nexus 9236C	N9K-9236C	

Algunos switches de la serie Cisco Nexus 9000 tienen variantes adicionales. Estas variantes son compatibles como parte de la solución FlexPod. Para obtener una lista completa de los switches de la serie Cisco Nexus 9000, consulte "Switches Cisco Nexus serie 9000" En el sitio web de Cisco.

Opciones APIC de Cisco

Al implementar Cisco ACI, debe configurar los tres APIC de Cisco además de los elementos de la sección "Switches Cisco Nexus serie 9000". Para obtener más información sobre los tamaños de la APIC de Cisco, consulte "Especificaciones técnicas de Cisco Application Centric Infrastructure."

Si quiere más información sobre las especificaciones de producto de la APIC, consulte la tabla 1 a la tabla 3 en la "Hoja de datos del controlador de infraestructura de políticas de aplicaciones de Cisco".

Opciones del extensor de estructura de Cisco Nexus

Se recomiendan las FEXs redundantes de montaje en rack de la serie Cisco Nexus 2000 para las arquitecturas FlexPod de gran tamaño que utilizan servidores C-Series. La siguiente tabla describe algunas opciones de Cisco Nexus FEX. También se admiten modelos FEX alternativos. Para obtener más información, consulte "Lista de compatibilidad de hardware y software de Cisco UCS".

FEX para montaje en rack Cisco Nexus	Número de pieza	Especificaciones técnicas
Cisco Nexus 2232PP	N2K-C2232PP	"Extensores estructurales Cisco Nexus serie 2000"
Cisco Nexus 2232TM-E	N2K-C2232TM-E	
Cisco Nexus 2348UPQ	N2K-C2348UPQ	"Extensores estructurales de la plataforma Cisco Nexus 2300"
Cisco Nexus 2348TQCisco Nexus 2348TQ-E	N2K-C2348TQN2K-C2348TQ-E	

Opciones de Cisco MDS

Los switches Cisco MDS son un componente opcional de la arquitectura FlexPod. Se necesitan estructuras de switch SAN redundantes cuando se implementa el switch Cisco MDS para FC SAN. En la siguiente tabla se enumeran los números de pieza y los detalles de un subconjunto de los switches Cisco MDS admitidos. 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.

Switch Cisco MDS 9000 Series	Número de pieza	Descripción
Cisco MDS 9148T	DS-C9148T-24IK	"Switches Cisco MDS 9100 Series"
Cisco MDS 9132T	DS-C9132T-MEK9	
Cisco MDS 9396S	DS-C9396S-K9	"Switches Cisco MDS 9300 Series"

Opciones de licencias de software de Cisco

Se necesitan licencias para habilitar protocolos de almacenamiento en los switches Cisco Nexus. Todas las series de switches Nexus 5000 y 7000 de Cisco requieren una licencia de servicios de almacenamiento para habilitar el protocolo FC o FCoE para implementaciones DE arranque SAN. Los switches de la serie Nexus 9000 de Cisco actualmente no son compatibles con FC o FCoE.

Las licencias necesarias y los números de pieza de estas licencias varían en función de las opciones seleccionadas para cada componente de la solución de FlexPod. Por ejemplo, los números de referencia de las licencias del software varían en función del número de puertos y los switches de las series Cisco Nexus 5000 o 7000 que elija. Consulte a su representante de ventas para obtener los números de pieza exactos. En la siguiente tabla se enumeran las opciones de licencias de software de Cisco.

Licencias de software de Cisco	Número de pieza	Información de licencia
Licencia de almacenamiento de Cisco Nexus 5500, 8, 48 y 96 puertos	N55-8P-SSK9/N55-48P-SSK9/N55-96P-SSK9	"Características del software Cisco NX-OS con licencia"
Licencia de protocolos de almacenamiento de Cisco Nexus 5010/5020	N5010-SSK9/N5020-SSK9	
Licencia de protocolos de almacenamiento de Cisco Nexus 5600	N56-16P-SSK9/N5672-72P-SSK9/N56128-128P-SSK9	
Licencia empresarial de almacenamiento de Cisco Nexus 7000	N7K-SAN1K9	
Licencia de Cisco Nexus 9000 Enterprise Services	N95-LAN1K9/N93-LAN1K9	

Opciones de licencias de soporte de Cisco

Se requieren contratos de soporte de SmartNet válidos en todos los equipos de Cisco de la arquitectura FlexPod.

El representante de ventas debe verificar las licencias necesarias y los números de pieza para dichas licencias porque pueden variar para diferentes productos. En la siguiente tabla se enumeran las opciones de licencias de soporte de Cisco.

Licencias de soporte de Cisco	Guía de licencias
Smart Net total Care in situ Premium	"Servicio Cisco Smart Net total Care"

Componentes de NetApp

Las controladoras de almacenamiento de NetApp proporcionan la base sobre la que se basa la arquitectura FlexPod tanto para el almacenamiento de datos de arranque como de aplicaciones. Los componentes de NetApp incluyen controladoras de almacenamiento, switches de interconexión de clúster, bandejas de unidades y discos, y opciones de licencias.

Opciones de la controladora de almacenamiento de NetApp

Se necesitan controladoras redundantes FAS, AFF o AFF ASA de NetApp en la arquitectura de FlexPod. Las controladoras ejecutan el software ONTAP. Cuando se solicitan las controladoras de almacenamiento, es posible precargar la versión de software preferida en las controladoras. Para ONTAP, se solicita un clúster completo. Un clúster completo incluye un par de controladoras de almacenamiento y una interconexión de clúster (switch o sin switch).

Existen diferentes opciones y configuraciones disponibles, según la plataforma de almacenamiento seleccionada. Consulte a su representante de ventas para obtener información sobre estos componentes adicionales.

Las familias de controladoras enumeradas en la siguiente tabla son adecuadas para usar en una solución de centros de datos de FlexPod porque su conexión con los switches Cisco Nexus es fluida. Consulte "Hardware Universe de NetApp" para obtener detalles específicos de compatibilidad de cada modelo de controladora.

Familia de controladoras de almacenamiento	Especificaciones técnicas
AFF a-Series	"Documentación de AFF a-Series"
AFF ASA a-Series	"Documentación de AFF ASA a-Series"
Serie FAS	"Documentación de la serie FAS"

Opciones del switch de interconexión de clúster

La siguiente tabla enumera los switches de interconexión de clústeres Nexus disponibles para las arquitecturas FlexPod. Además, FlexPod admite todos los switches de clúster compatibles con ONTAP, incluidos los switches que no sean de Cisco, siempre y cuando la versión de ONTAP que se esté poniendo en marcha sea compatible. Consulte "Hardware Universe de NetApp" para obtener detalles de compatibilidad adicionales para modelos de switch específicos.

Switch de interconexión de clúster	Especificaciones técnicas
Cisco Nexus 3132Q-V	"Documentación de NetApp: Switches Cisco Nexus 3132Q-V."
Cisco Nexus 9336C-FX2	"Documentación de NetApp: Switches Cisco Nexus 9336C-FX2"

Opciones de unidades y bandeja de discos de NetApp

Se requiere un mínimo de una bandeja de discos NetApp para todas las controladoras de almacenamiento.

El tipo de bandeja de NetApp seleccionado determina los tipos de unidad disponibles en esa bandeja.

> Para obtener todos los números de pieza de disco y bandejas de discos, consulte a su representante de ventas.

Si desea más información sobre las unidades compatibles, haga clic en el enlace NetApp Hardware Universe de la siguiente tabla y, a continuación, seleccione unidades admitidas.

Bandeja de discos	Especificaciones técnicas
DS224C	"Unidades compatibles con bandejas de discos y medios de almacenamiento en Hardware Universe de NetApp"
DS212C	
DS460C	
NS224	

Opciones de licencias de software de NetApp

La siguiente tabla enumera las opciones de licencias del software de NetApp que están disponibles para la arquitectura del centro de datos de FlexPod. El software de NetApp cuenta con la licencia a nivel de controladora FAS y AFF.

Licencias de software de NetApp	Número de pieza	Especificaciones técnicas
SW, PAQUETE completo (controlador), -C.	SW-8XXX-COMP-BDL-C.	"Biblioteca de productos A–Z"
SW, ONTAP Essentials (controlador), -C.	SW-8XXX-ONTAP9-C	

Opciones de licencias de soporte de NetApp

Las licencias de NetApp SupportEdge Premium son necesarias para la arquitectura de FlexPod, pero los números de pieza de dichas licencias varían en función de las opciones seleccionadas en el diseño de FlexPod. Por ejemplo, los números de referencia de la licencia del software varían en función de la controladora de FAS que elija. Consulte a su representante de ventas para obtener información acerca de los números de pieza exactos de las licencias de soporte individuales. La siguiente tabla muestra un ejemplo de una licencia de SupportEdge.

Licencias de soporte de NetApp	Número de pieza	Especificaciones técnicas
SupportEdge Premium 4 horas in situ—meses: 36	CS-O2-4HR	"SupportEdge Premium de NetApp"

Requisitos de alimentación y cableado

Un diseño de FlexPod tiene requisitos mínimos de alimentación y cableado.

Requisitos de alimentación

Los requisitos de alimentación del centro de datos de FlexPod difieren en función de la ubicación en la que se ha instalado la configuración del centro de datos de FlexPod.

Para obtener más datos acerca de la potencia máxima necesaria y para obtener otra información detallada sobre la alimentación, consulte las especificaciones técnicas de cada componente de hardware enumerado en la sección "Especificaciones técnicas y referencias: Componentes de hardware".

Para obtener información detallada sobre los datos de alimentación de Cisco UCS, consulte "Calculadora de potencia de Cisco UCS".

Para ver los datos de alimentación de la controladora de almacenamiento de NetApp, consulte "Hardware Universe de NetApp". En Platforms, seleccione la plataforma de almacenamiento que desee utilizar en la configuración (FAS/V-Series o AFF). Seleccione la versión de ONTAP y la controladora de almacenamiento y haga clic en el botón Mostrar resultados.

Requisitos mínimos de cable

La cantidad y el tipo de cables y adaptadores necesarios varían en función de la puesta en marcha del centro de datos de FlexPod. El tipo de cable, el tipo de transceptor y el número se determinan durante el proceso de diseño en función de sus necesidades. En la tabla siguiente se indica el número mínimo de cables necesarios.

Hardware subyacente	Número de modelo	Cables necesarios
Chasis Cisco UCS	Cisco UCS 5108	Al menos dos cables twinaxiales por módulo Cisco UCS 2104XP, 2204XP o 2208XP
Cisco UCS Fabric Interconnect	Cisco UCS 6248UP	• Dos cables CAT5e para puertos de gestión • Dos cables CAT5e para las interconexiones L1, L2 por par de interconexiones de estructura • Al menos cuatro cables twinaxiales por interconexión de estructura • Al menos cuatro cables FC por interconexión de estructura
	Cisco UCS 6296UP	Cisco UCS 6332-16UP
	Cisco UCS 6454	Cisco UCS 6332
	• Dos cables CAT5e para puertos de gestión • Dos cables CAT5e para las interconexiones L1, L2 por par de interconexiones de estructura • Al menos cuatro cables twinaxiales por interconexión de estructura	Cisco UCS 6324
	• Dos puertos de gestión de 10/100 Mbps • Al menos dos cables twinaxiales por interconexión de estructura	Switches de las series Cisco Nexus 5000 y 7000
	Serie Nexus 5000 de Cisco	
• Al menos dos cables twinaxial o de fibra de 10 GbE por switch • Al menos dos cables FC por switch (si se requiere conectividad FC/FCoE)	Serie Nexus 7000 de Cisco	Switches Cisco Nexus serie 9000

Hardware subyacente	Número de modelo	Cables necesarios
Serie Nexus 9000 de Cisco	Al menos dos cables de 10 GbE por switch	Controladoras FAS de NetApp
AFF a-Series	• Un par de cables SAS o SATA por controladora de almacenamiento • Al menos dos cables FC por controladora, si se utiliza FC existente • Al menos dos cables de 10 GbE por controladora • Al menos un cable GbE para gestión por controladora • Para ONTAP, se necesitan ocho cables twinaxiales cortos por par de switches de interconexión de clúster	
Serie FAS	Bandejas de discos de NetApp	DS212C
Dos cables SAS, SATA o FC por bandeja de discos		DS224C
		DS460C
		NS224

Especificaciones técnicas y referencias

Las especificaciones técnicas ofrecen detalles sobre los componentes de hardware de una solución FlexPod, como chasis, FEXs, servidores, conmutadores, y las controladoras de almacenamiento.

Chasis de servidor blade Cisco UCS serie B

Entre las especificaciones técnicas del chasis de servidor blade Cisco UCS B-Series, como se muestra en la siguiente tabla, se incluyen los siguientes componentes:

- Número de unidades rack
- Número máximo de palas
- Funcionalidad de estructura unificada
- Ancho de banda de I/o de plano medio por servidor
- Número de bahías de E/S para FEXs

Componente	Chasis de servidor blade Cisco UCS serie 5100
Unidades de rack	6
Hojas de anchura completa máxima	4
Hojas de media anchura máxima	8

Componente	Chasis de servidor blade Cisco UCS serie 5100
Con capacidad de Unified Fabric	Sí
I/o del plano medio	Hasta 80 Gbps de ancho de banda de I/o por servidor
Bahías de E/S para FEXs	Dos bahías para Cisco UCS 2104XP, 2204/8XP, 2408XP y 2304 FEXs

Para obtener más información, consulte "Especificaciones técnicas del chasis de servidor blade Cisco UCS serie 5100".

Servidores blade Cisco UCS serie B

Entre las especificaciones técnicas de los servidores blade Cisco UCS serie B, como se muestra en la siguiente tabla, se incluyen los siguientes componentes:

- Número de zócalos de procesador
- Compatibilidad con procesadores
- Capacidad de memoria
- Tamaño y velocidad
- Soporte de arranque SAN
- Número de ranuras del adaptador intermedio
- Máximo rendimiento de I/O.
- Factor de forma
- Número máximo de servidores por chasis

Componente	Especificaciones técnicas de Cisco UCS
CISCO UCS B200 M6	"Servidor blade Cisco UCS B200 M6"

Servidores de montaje en rack Cisco UCS C-Series

Las especificaciones técnicas de los servidores de rack Cisco UCS C-Series incluyen compatibilidad con procesador, capacidad de memoria máxima, número de ranuras PCIe y tamaño del factor de forma. Para obtener información adicional sobre modelos de servidores UCS compatibles, consulte "Compatibilidad con hardware de Cisco" lista. En las siguientes tablas se ilustran las especificaciones técnicas de los servidores en rack C-Series y la opción de chasis Cisco UCS C-Series, respectivamente.

Componente	Especificaciones técnicas de Cisco UCS
CISCO UCS C220 M6	"Servidor en rack Cisco UCS C220 M6"
CISCO UCS C225 M6	"Servidor en rack Cisco UCS C225 M6"
CISCO UCS C240 M6	"Servidor en rack Cisco UCS C240 M6"
CISCO UCS C245 M6	"Servidor en rack Cisco UCS C245 M6"

Chasis Cisco UCS X-Series

Entre las especificaciones técnicas del chasis Cisco UCS X-Series, como se muestra en la siguiente tabla, se

incluyen los siguientes componentes:

- Número de unidades rack
- Número máximo de nodos
- Funcionalidad de estructura unificada
- Número de bahías de E/S para IFMS

Componente	Chasis de nodos de computación Cisco UCS 9508 X-Series
Unidades de rack	7
Número máximo de nodos	8
Con capacidad de Unified Fabric	Sí
Bahías de E/S para IFMS	Dos bahías para módulos de estructura inteligente (IFMS) Cisco UCS 9108

Para obtener más información, consulte "Especificaciones técnicas del chasis Cisco UCS X9508 X-Series".

Nodo de computación Cisco UCS X-Series

Entre las especificaciones técnicas del nodo de computación Cisco UCS X-Series, como se muestra en la siguiente tabla, se incluyen los siguientes componentes:

- Número de zócalos de procesador
- Compatibilidad con procesadores
- Capacidad de memoria
- Tamaño y velocidad
- Soporte de arranque SAN
- Número de ranuras del adaptador intermedio
- Máximo rendimiento de I/O.
- Factor de forma
- Número máximo de nodos de computación por chasis

Componente	Especificaciones técnicas de Cisco UCS
Cisco UCS X210c M6	"Nodo de computación Cisco UCS X210c M6"

Recomendación de GPU para IA FlexPod, ML y DL

Los servidores en rack Cisco UCS C-Series enumerados en la tabla a continuación pueden utilizarse en una arquitectura de FlexPod para alojar cargas de trabajo de IA, ML y DL. Los servidores Cisco UCS C480 ML M5 están diseñados específicamente para cargas de trabajo de IA, ML y DL y utilizan las GPU basadas en SXM2 de NVIDIA, mientras que los otros servidores utilizan GPU basadas en PCIe.

La tabla que se muestra a continuación también enumera las GPU recomendadas que se pueden utilizar con estos servidores.

Servidor	GPU
CISCO UCS C220 M6	NVIDIA T4
CISCO UCS C225 M6	NVIDIA T4
CISCO UCS C240 M6	NVIDIA TESLA A10, A100
CISCO UCS C245 M6	NVIDIA TESLA A10, A100

Adaptadores de Cisco UCS VIC para servidores blade de la serie B de Cisco UCS

Las especificaciones técnicas de los adaptadores de tarjeta de interfaz virtual (VIC) Cisco UCS para los servidores blade Cisco UCS B-Series incluyen los siguientes componentes:

- Número de puertos de enlace ascendente
- Rendimiento por puerto (IOPS)
- Potencia
- Número de puertos blade
- Descarga del hardware
- Compatibilidad con la virtualización de entrada/salida raíz única (SR-IOV)

Todas las arquitecturas de FlexPod validadas actualmente utilizan un VIC de Cisco UCS. Los demás adaptadores son compatibles si aparecen en la lista de NetApp "IMT" Y son compatibles con la puesta en marcha de FlexPod, pero es posible que no ofrezcan todas las funciones descritas en las arquitecturas de referencia correspondientes. La tabla siguiente ilustra las especificaciones técnicas del adaptador VIC de Cisco UCS.

Componente	Especificaciones técnicas de Cisco UCS
Adaptadores de interfaz virtual Cisco UCS	"Especificaciones técnicas de VIC de Cisco UCS"

Interconexiones de estructura Cisco UCS

Las especificaciones técnicas de las interconexiones de estructura Cisco UCS incluyen el tamaño del factor de forma, el número total de puertos y ranuras de expansión y la capacidad de rendimiento. La siguiente tabla muestra las especificaciones técnicas de interconexión de estructura Cisco UCS.

Componente	Especificaciones técnicas de Cisco UCS
Cisco UCS 6248UP	"Interconexiones de estructuras Cisco UCS de la serie 6200"
Cisco UCS 6296UP	
Cisco UCS 6324	"Interconexión de estructura Cisco UCS 6324"
Cisco UCS 6300	"Interconexiones de estructuras Cisco UCS de la serie 6300"
Cisco UCS 6454	"Interconexiones de estructuras Cisco UCS de la serie 6400"

Switches Cisco Nexus 5000 Series

Las especificaciones técnicas de los switches Cisco Nexus serie 5000, incluido el tamaño de factor de forma, el número total de puertos y la compatibilidad con módulos y tarjetas hijas de capa 3, se incluyen en la hoja de datos de cada familia de modelos. Estas hojas de datos se pueden encontrar en la siguiente tabla.

Componente	Especificaciones técnicas de Cisco Nexus
Cisco Nexus 5548UP	"Switch Cisco Nexus 5548UP"
Cisco Nexus 5596UP (2U)	"Switch Cisco Nexus 5596UP"
Cisco Nexus 56128P	"Switch Cisco Nexus 56128P"
Cisco Nexus 5672UP	"Switch Cisco Nexus 5672UP"

Switches Cisco Nexus 7000 Series

Las especificaciones técnicas de los switches Cisco Nexus serie 7000, incluido el tamaño del factor de forma y el número máximo de puertos, se incluyen en la hoja de datos de cada familia de modelos. Estas hojas de datos se pueden encontrar en la siguiente tabla.

Componente	Especificaciones técnicas de Cisco Nexus
Cisco Nexus 7004	"Switches Cisco Nexus serie 7000"
Cisco Nexus 7009	
Cisco Nexus 7010	
Cisco Nexus 7018	
Cisco Nexus 7702	"Switches Cisco Nexus serie 7700"
Cisco Nexus 7706	
Cisco Nexus 7710	
Cisco Nexus 7718	

Switches Cisco Nexus 9000 Series

Las especificaciones técnicas de los switches de la serie 9000 de Cisco Nexus se incluyen en la hoja de datos de cada modelo. Las especificaciones incluyen el tamaño del factor de forma; el número de supervisores, el módulo de tela y las ranuras para tarjetas de línea; y el número máximo de puertos. Estas hojas de datos se pueden encontrar en la siguiente tabla.

Componente	Especificaciones técnicas de Cisco Nexus
Serie Nexus 9000 de Cisco	"Switches Cisco Nexus serie 9000"
Serie Nexus 9500 de Cisco	"Switches Cisco Nexus serie 9500"
Serie Nexus 9300 de Cisco	"Switches Cisco Nexus serie 9300"
Switch troncal de Cisco Nexus 9336PQ ACI	"Switch troncal de Cisco Nexus 9336PQ ACI"
Serie Nexus 9200 de Cisco	"Switches de la plataforma Cisco Nexus 9200"

Controlador de infraestructura de políticas de aplicaciones de Cisco

Al implementar Cisco ACI, además de los elementos de la sección "Switches Cisco Nexus serie 9000", Debe configurar tres APIC de Cisco. La siguiente tabla enumera las especificaciones técnicas de Cisco APIC.

Componente	Especificaciones técnicas de la infraestructura de políticas de aplicaciones de Cisco
Controlador de infraestructura de políticas de aplicaciones de Cisco	"Especificaciones técnicas de Cisco APIC"

Detalles del extensor de estructura Cisco Nexus

Las especificaciones técnicas de Cisco Nexus FEX incluyen velocidad, número de puertos y enlaces fijos y tamaño de factor de forma.

La siguiente tabla muestra las especificaciones técnicas de FEX de Cisco Nexus 2000.

Componente	Especificaciones técnicas del extensor de estructura Cisco Nexus
Extensores estructurales Cisco Nexus serie 2000	"Especificaciones técnicas de FEX de la serie Nexus 2000"

Módulos SFP

Si desea más información sobre los módulos SFP, consulte los siguientes recursos:

- Para obtener información sobre el SFP de 10 GB de Cisco, consulte "Módulos Cisco 10 Gigabit".
- Para obtener información sobre el SFP de 25 GB de Cisco, consulte "Módulos Cisco 25 Gigabit".
- Para obtener información sobre el módulo Cisco QSFP, consulte "Especificaciones técnicas de los módulos QSFP Cisco 40GBASE".
- Para obtener información sobre el SFP 100 GB de Cisco, consulte "Módulos Cisco 100 Gigabit".
- Para obtener información acerca del módulo SFP FC de Cisco, consulte "Hoja de datos de los transceptores conectables de la familia Cisco MDS 9000".
- Para obtener información sobre todos los módulos de transceptor y SFP de Cisco admitidos, consulte "Notas de instalación del módulo de transceptores Cisco SFP y SFP+" y.. "Módulos de transceptores Cisco".

Controladoras de almacenamiento de NetApp

Las especificaciones técnicas de las controladoras de almacenamiento de NetApp incluyen los siguientes componentes:

- Configuración del chasis
- Número de unidades rack
- Cantidad de memoria
- Almacenamiento en caché Flash Cache de NetApp
- Tamaño del agregado
- Tamaño del volumen

- Número de LUN
- Almacenamiento en red compatible
- Número máximo de volúmenes FlexVol de NetApp
- Número máximo de hosts SAN admitidos
- El número máximo de copias de Snapshot

Serie FAS

Todos los modelos disponibles de controladoras de almacenamiento de FAS se admiten para usar en un centro de datos FlexPod. En la, encontrará especificaciones detalladas de todas las controladoras de almacenamiento de la serie FAS "Hardware Universe de NetApp". Consulte la documentación específica de la plataforma que se incluye en la tabla siguiente para obtener información detallada sobre un modelo de FAS específico.

Componente	Documentación de la plataforma de la controladora FAS Series
Serie FAS9000	"Especificaciones técnicas de la serie FAS9000"
Serie FAS8700	"Hoja de datos de la serie FAS8700"
Serie FAS8300	"Especificaciones técnicas de la serie FAS8300"
Serie FAS500f	"Hoja de datos de la serie FAS500f"
Serie FAS2700	"Especificaciones técnicas de la serie FAS2700"

AFF a-Series

Todos los modelos actuales de las controladoras de almacenamiento AFF a-Series de NetApp son compatibles para su uso en FlexPod. Puede encontrar información adicional en "Especificaciones técnicas de AFF" la hoja de datos y en la "Hardware Universe de NetApp". Consulte la documentación específica de la plataforma que se muestra en la tabla siguiente para obtener información detallada acerca de un modelo AFF específico.

Componente	Documentación de la plataforma de controladoras AFF a-Series
AFF A800 de NetApp	"Documentación de la plataforma A800 de AFF"
AFF A700 de NetApp	"Documentación de la plataforma A700 de AFF"
AFF A700s de NetApp	"Documentación de la plataforma AFF A700s"
AFF A400 de NetApp	"Documentación de la plataforma AFF A400"
AFF A250 de NetApp	"Documentación de la plataforma AFF A250"

AFF ASA a-Series

Todos los modelos actuales de las controladoras de almacenamiento AFF ASA a-Series de NetApp son compatibles para su uso en FlexPod. Puede encontrar más información en el informe técnico sobre los recursos de documentación de la cabina All SAN, el sistema de la cabina All SAN ONTAP AFF y en Hardware Universe de NetApp. Consulte la documentación específica de la plataforma que se muestra en la tabla siguiente para obtener información detallada sobre un modelo AFF específico.

Componente	Documentación de la plataforma de controladoras AFF a-Series
AFF ASA A800 de NetApp	"Documentación de la plataforma A800 de AFF ASA"
AFF ASA A700 de NetApp	"Documentación de la plataforma A700 de AFF ASA"
AFF ASA A400 de NetApp	"Documentación de la plataforma AFF ASA A400"
AFF ASA A250 de NetApp	"Documentación de la plataforma AFF ASA A250"
AFF ASA A220 de NetApp	"Documentación de la plataforma AFF ASA A220"

Bandejas de discos de NetApp

Las especificaciones técnicas de las bandejas de discos de NetApp incluyen el tamaño del factor de forma, el número de unidades por compartimento y los módulos de I/o de la bandeja; esta documentación se puede encontrar en la siguiente tabla. Para obtener más información, consulte "Especificaciones técnicas de bandejas de discos y medios de almacenamiento de NetApp" y la "Hardware Universe de NetApp".

Componente	Documentación de la bandeja de discos FAS/AFF de NetApp
Bandeja de discos DS212C de NetApp	"Documentación de DS212C Disk Shelf"
Bandeja de discos DS224C de NetApp	"Documentación de la bandeja de discos DS224C"
Bandeja de discos DS460C de NetApp	"Documentación de la bandeja de discos DS460C"
Bandeja de discos NS224 NVMe-SSD de NetApp	"Documentación de la bandeja de discos NS224"

Unidades de NetApp

Las especificaciones técnicas de las unidades de NetApp incluyen el tamaño del factor de forma, la capacidad de disco, los RPM del disco, las controladoras compatibles y los requisitos de versión de ONTAP. Estas especificaciones se pueden encontrar en la sección Drives de la "Hardware Universe de NetApp".

Equipo existente

FlexPod es una solución flexible que le permite utilizar su equipo existente y el nuevo equipo a la venta actualmente por Cisco y NetApp. Ocasionalmente, algunos modelos de equipo de Cisco y NetApp están designados como fin de su vida útil (EOL).

Aunque estos modelos de equipos ya no están disponibles, si ha adquirido uno de estos modelos antes de la fecha de finalización de la disponibilidad (EOA), puede utilizar dicho equipo en una configuración de FlexPod. Puede consultar una lista completa de los modelos de equipo heredado que son compatibles con FlexPod y que ya no están a la venta en la "Índice de fin de disponibilidad de los programas de productos de servicio y soporte de NetApp".

Si quiere más información sobre equipos antiguos de Cisco, consulte los avisos de fin de vida útil y fin de disponibilidad de Cisco de "Servidores en rack Cisco UCS serie C", "Servidores blade Cisco UCS serie B", y. "Switches Nexus".

La compatibilidad con la estructura FC heredada incluye lo siguiente:

- Tejido de 2 GB

- Estructura de 4 GB

El software heredado incluye lo siguiente:

- Sistema operativo Data ONTAP de NetApp en 7-Mode, 7.3.5 y versiones posteriores
- ONTAP 8.1.x a 9.0.x
- Cisco UCS Manager 1.3 y posterior
- Cisco UCS Manager 2.1 a 2.2.7

Dónde encontrar información adicional

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

- Documentación de productos de NetApp

  "https://docs.netapp.com/"

- Comunicaciones de soporte de NetApp

  "https://mysupport.netapp.com/info/communications/index.html"

- Herramienta de matriz de interoperabilidad de NetApp (IMT)

  "https://mysupport.netapp.com/matrix/#welcome"

- Hardware Universe de NetApp

  "https://hwu.netapp.com/"

- Soporte de NetApp

  "https://mysupport.netapp.com/"

Centro de datos FlexPod

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

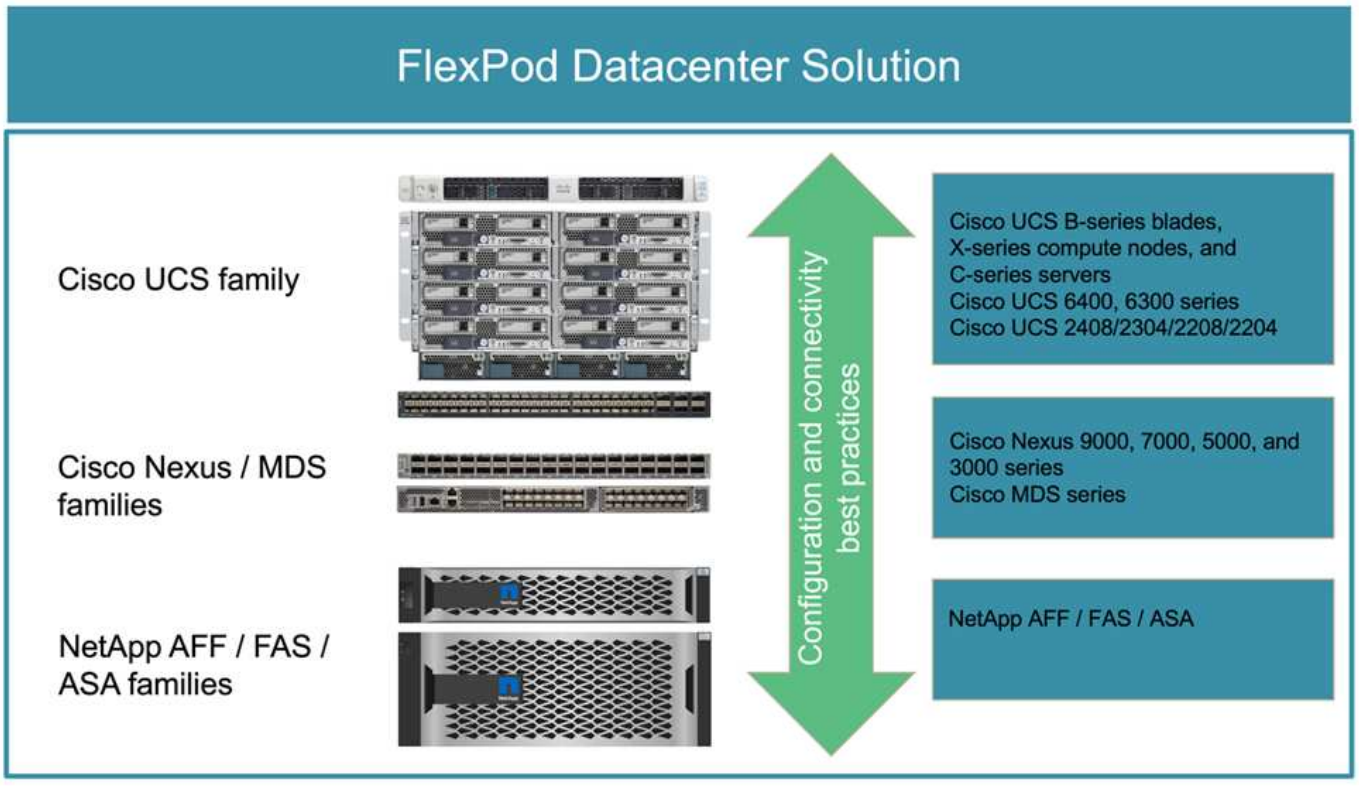
Introducción

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.

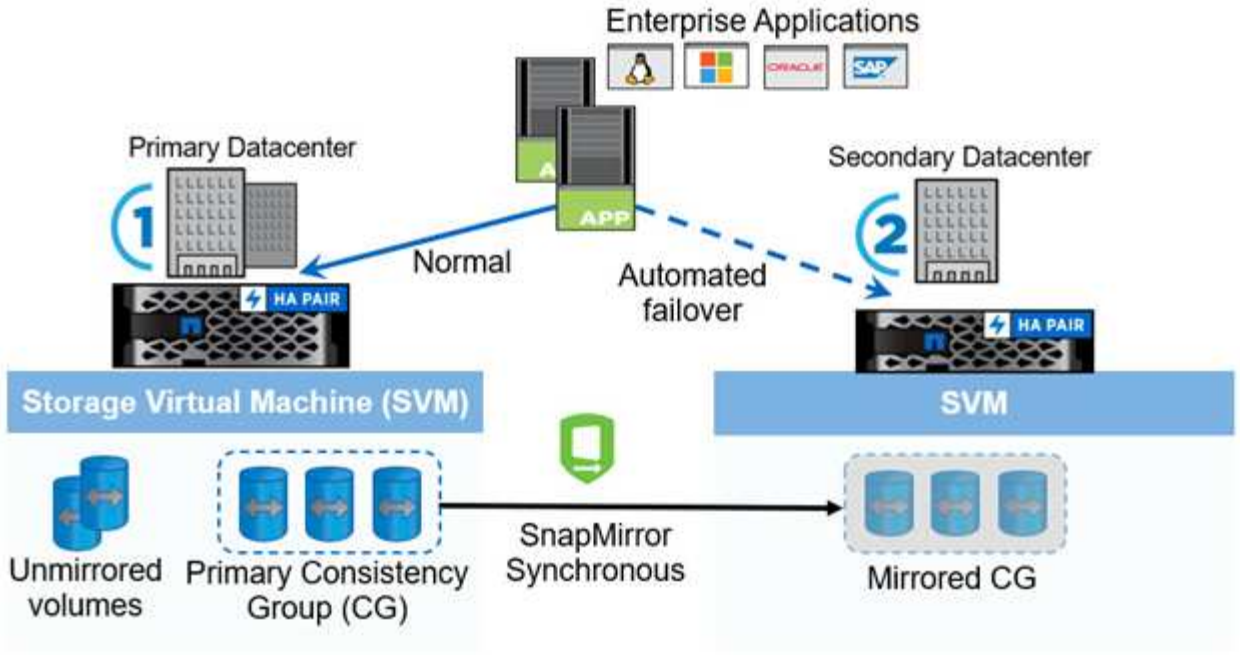
SM-BC

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

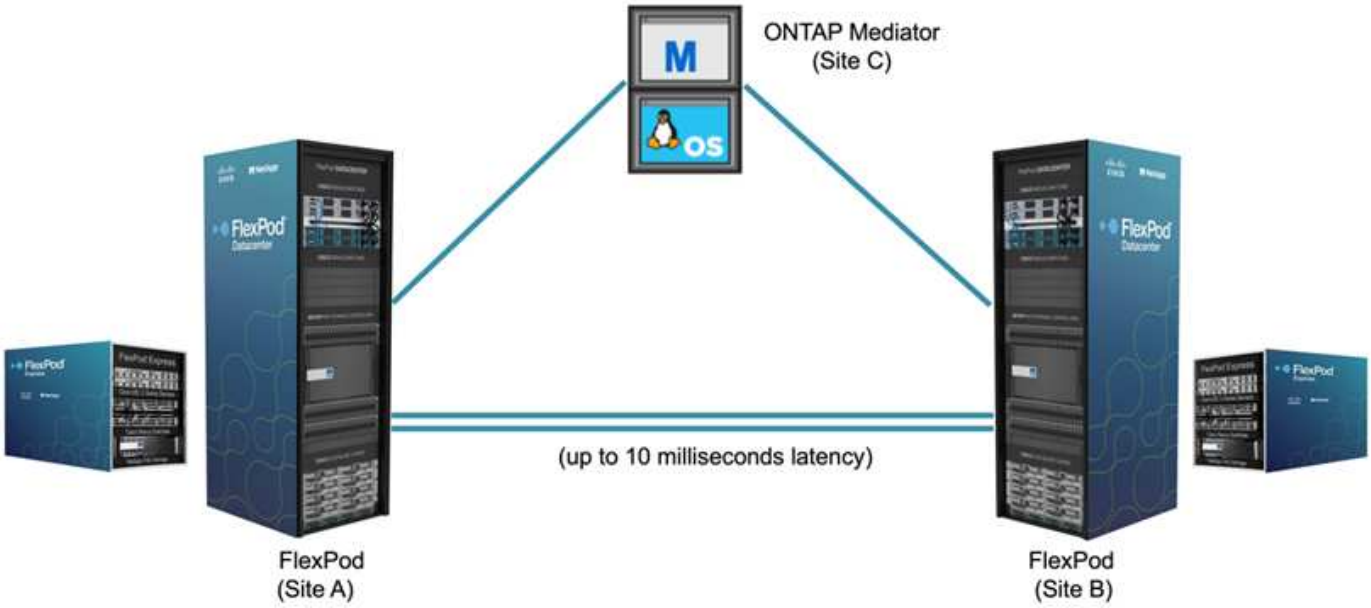
En un nivel superior, una solución FlexPod SM-BC se compone de dos sistemas FlexPod ubicados en dos sitios separados por cierta distancia, conectados y emparejados para ofrecer una solución de centro de datos altamente disponible, flexible y de gran fiabilidad que puede proporcionar continuidad del negocio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

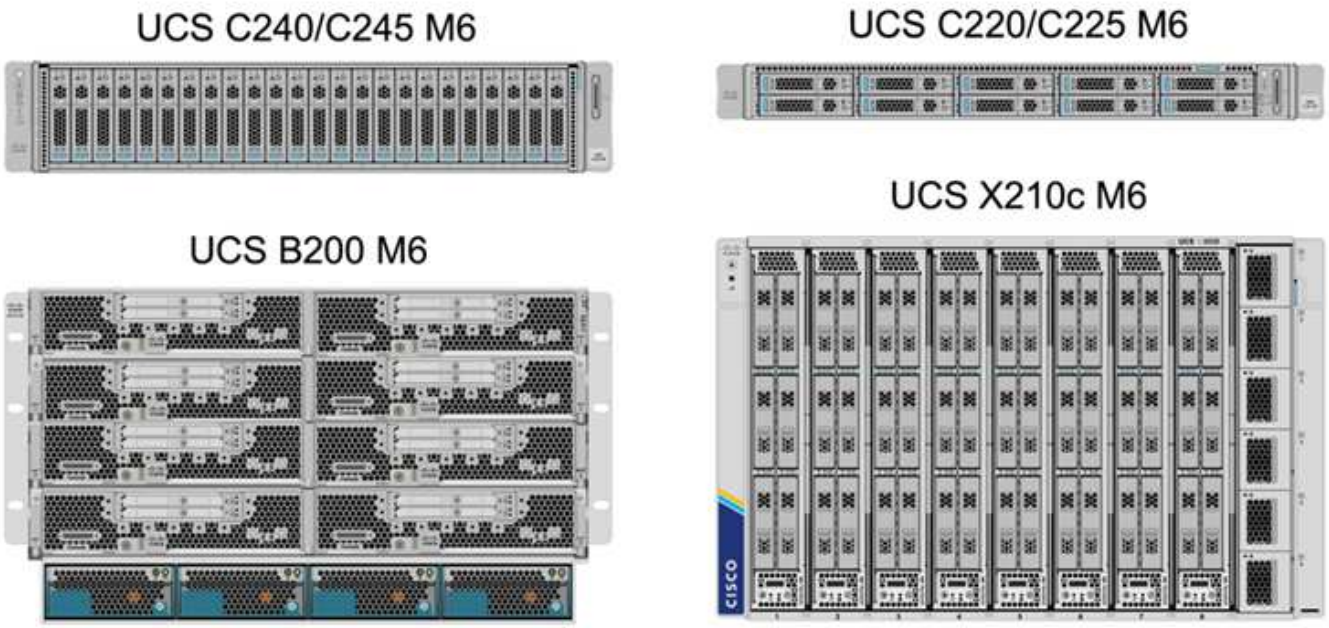
Componentes de computación de Cisco

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.

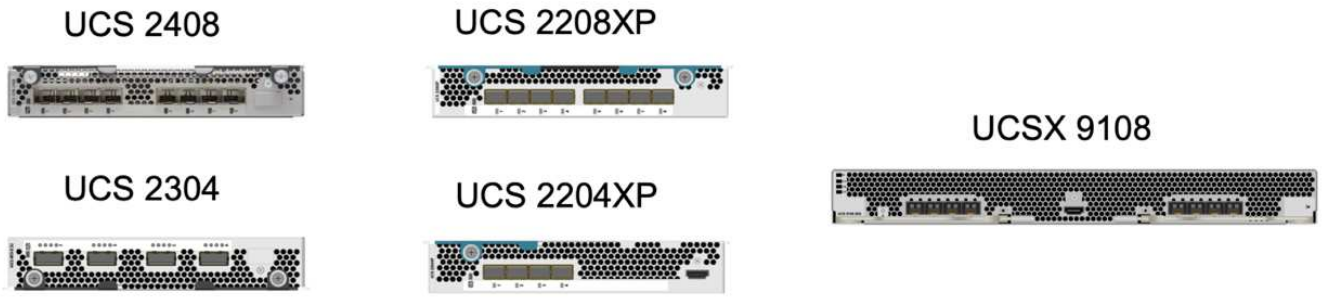
Módulo de I/o y módulo de estructura inteligente

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.

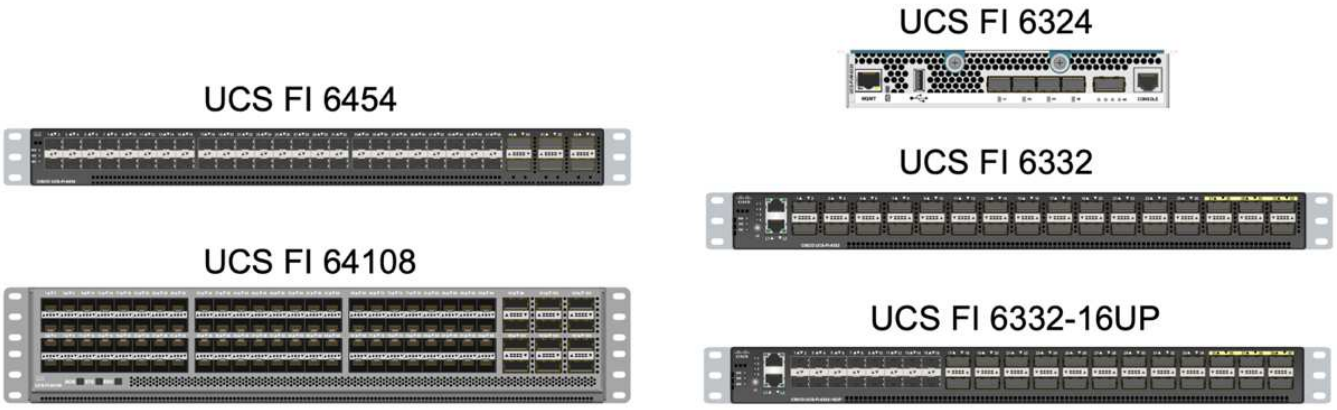
La siguiente figura muestra UCS 2408 y las generaciones de IOM anteriores para el chasis UCS 5108 y el IFM 9108 para el chasis X9508.



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.



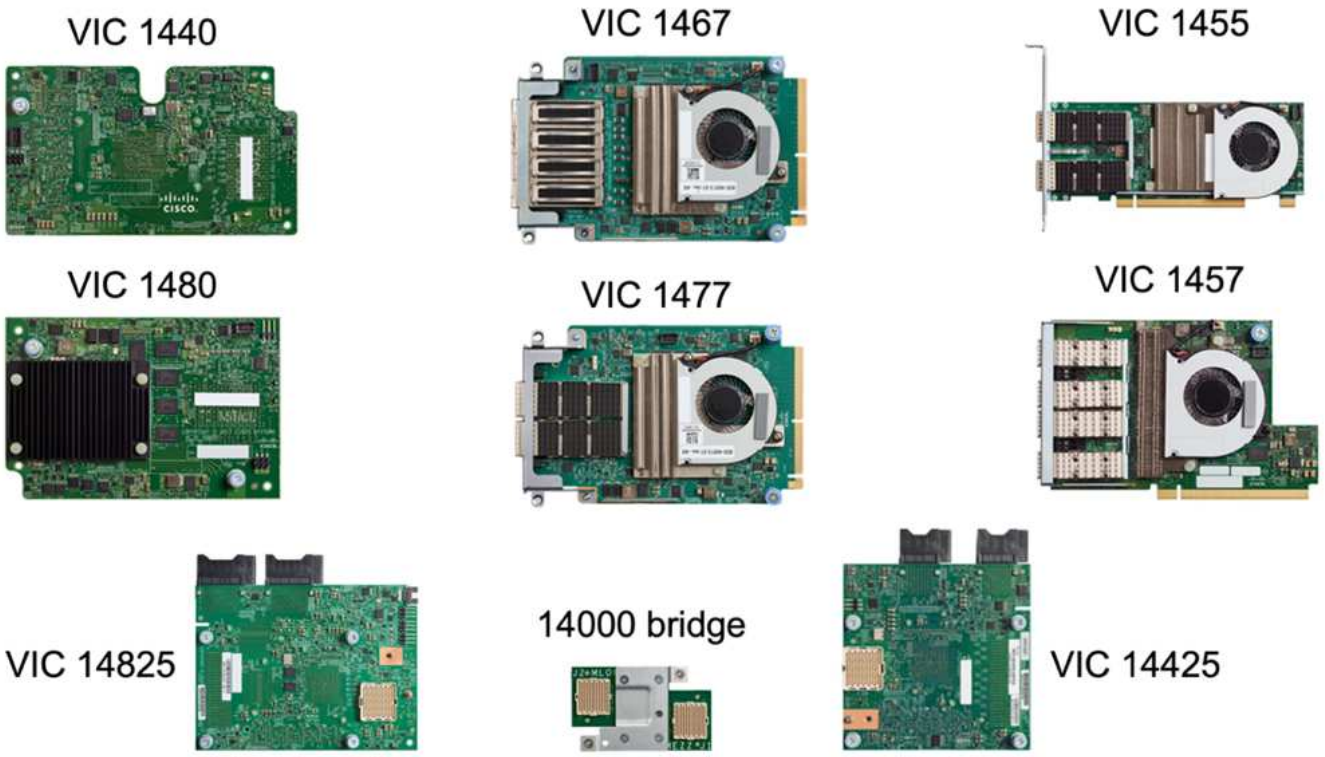
Para admitir el chasis Cisco UCS X-Series, se necesitan interconexiones de estructura de cuarta generación configuradas en el modo gestionado de Intersight (IMM). Sin embargo, es posible ofrecer soporte al chasis Cisco UCS 5108 serie B tanto en modo IMM como en modo gestionado UCSM.

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

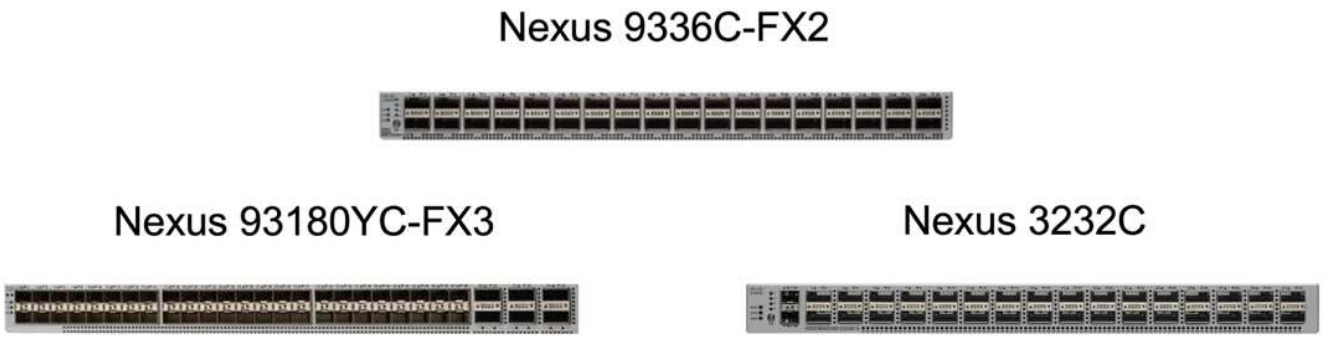
Switches Nexus

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.

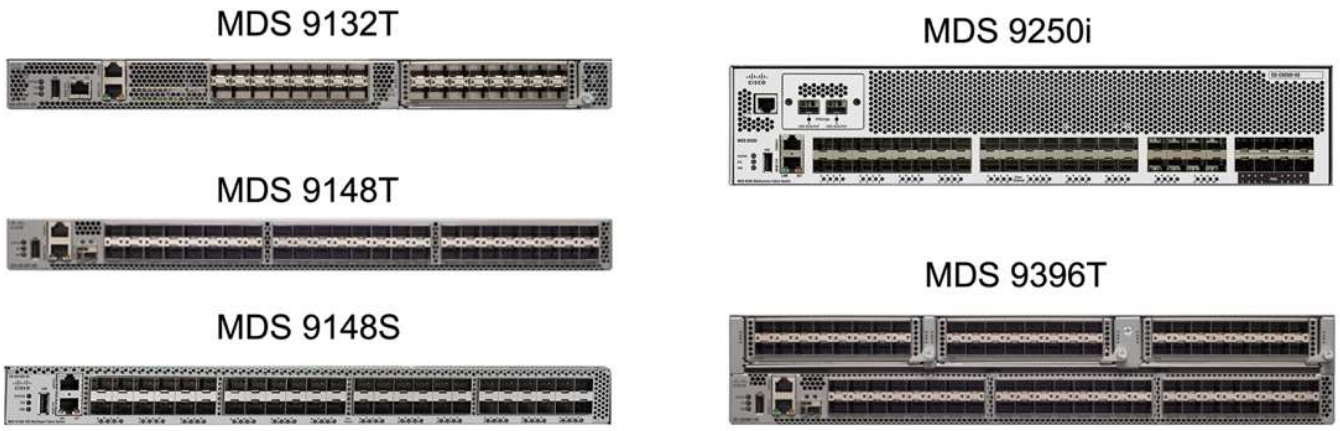
La validación de muchos CVD de FlexPod recientes utiliza switches Cisco Nexus 9000, como Nexus 9336C-FX2 y Nexus 93180YC-FX3, que proporcionan puertos 40/100G y 10//25G de alto rendimiento, baja latencia y eficiencia energética excepcional en un factor de forma 1U compacto. Se admiten velocidades adicionales 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.

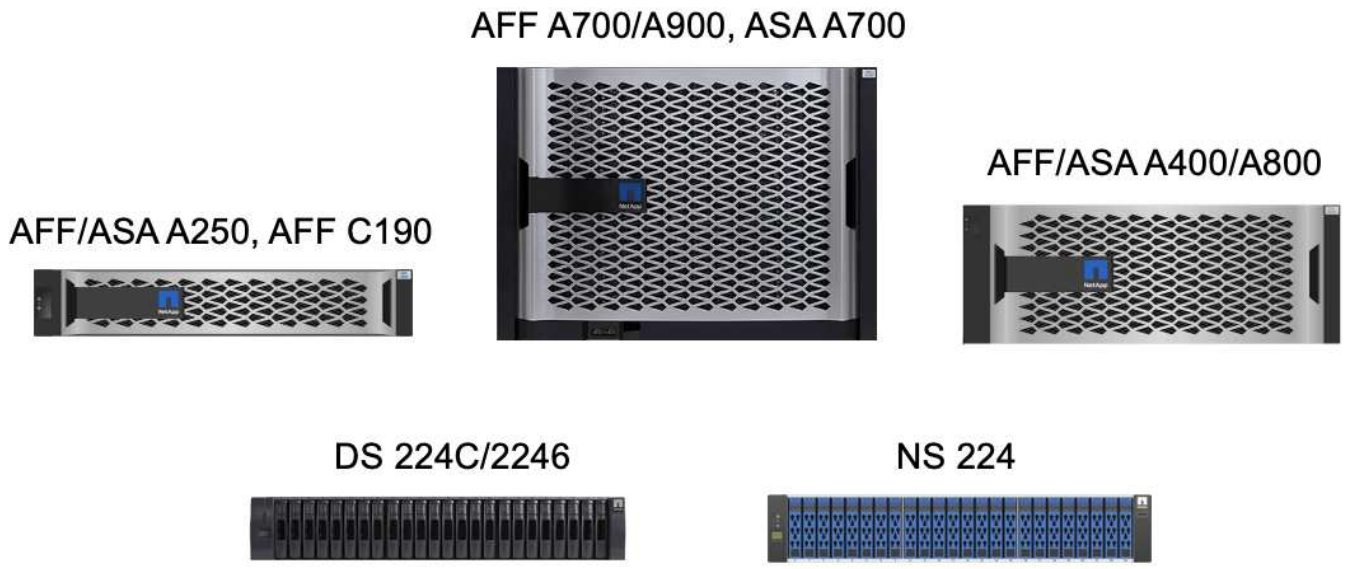
Componentes de NetApp

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.

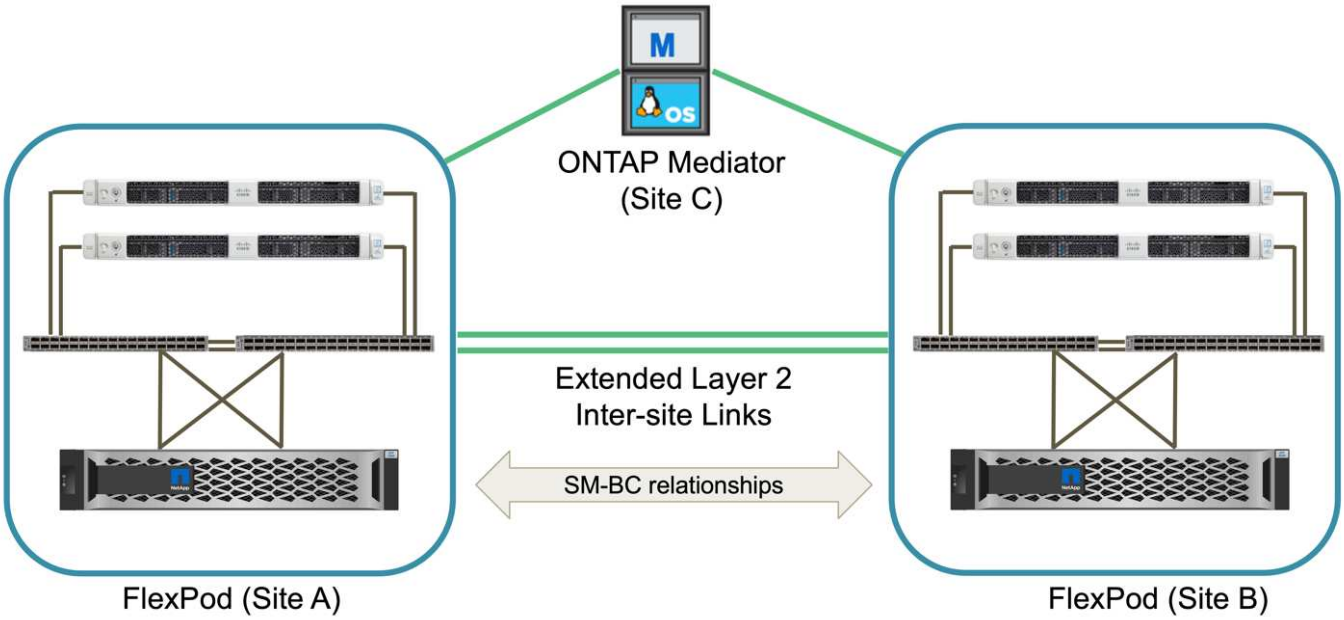


Familia de productos	Especificaciones técnicas
Serie AFF	"Documentación de la serie AFF"
Serie ASA	"Documentación de la serie ASA"

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.

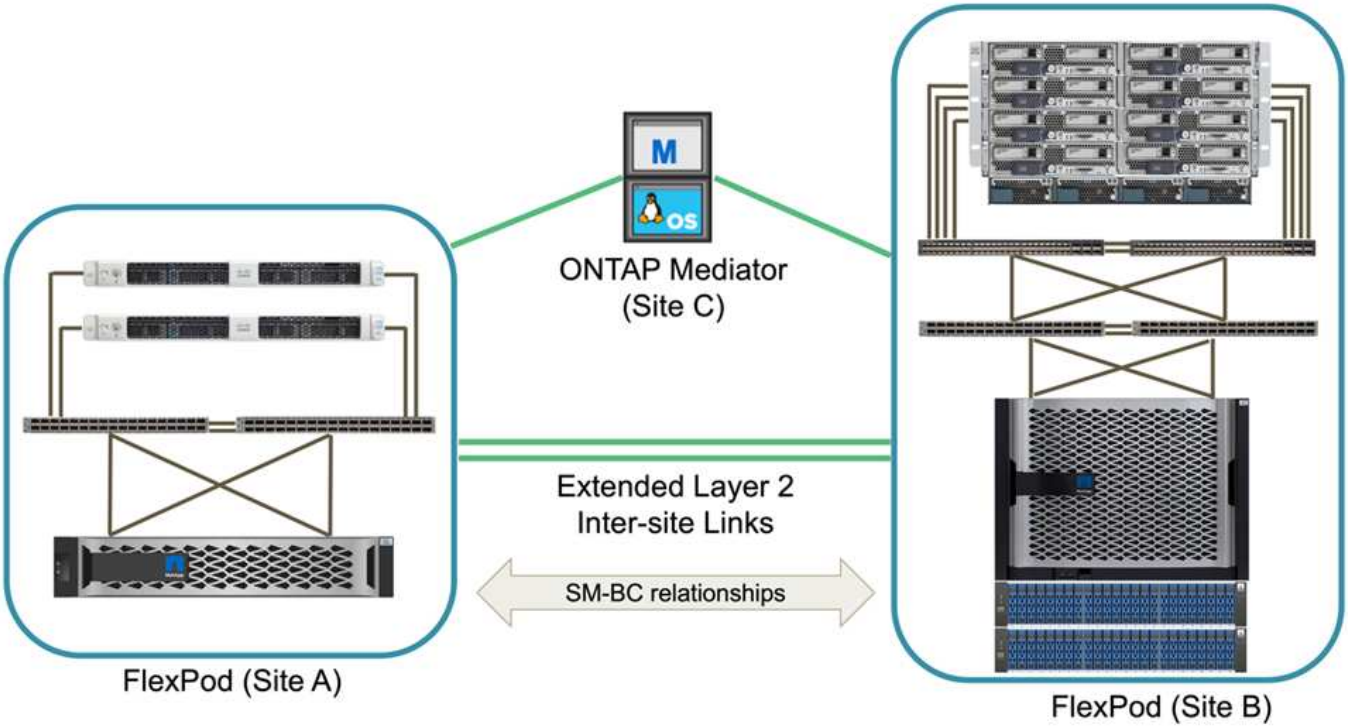
Topologías de soluciones

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.



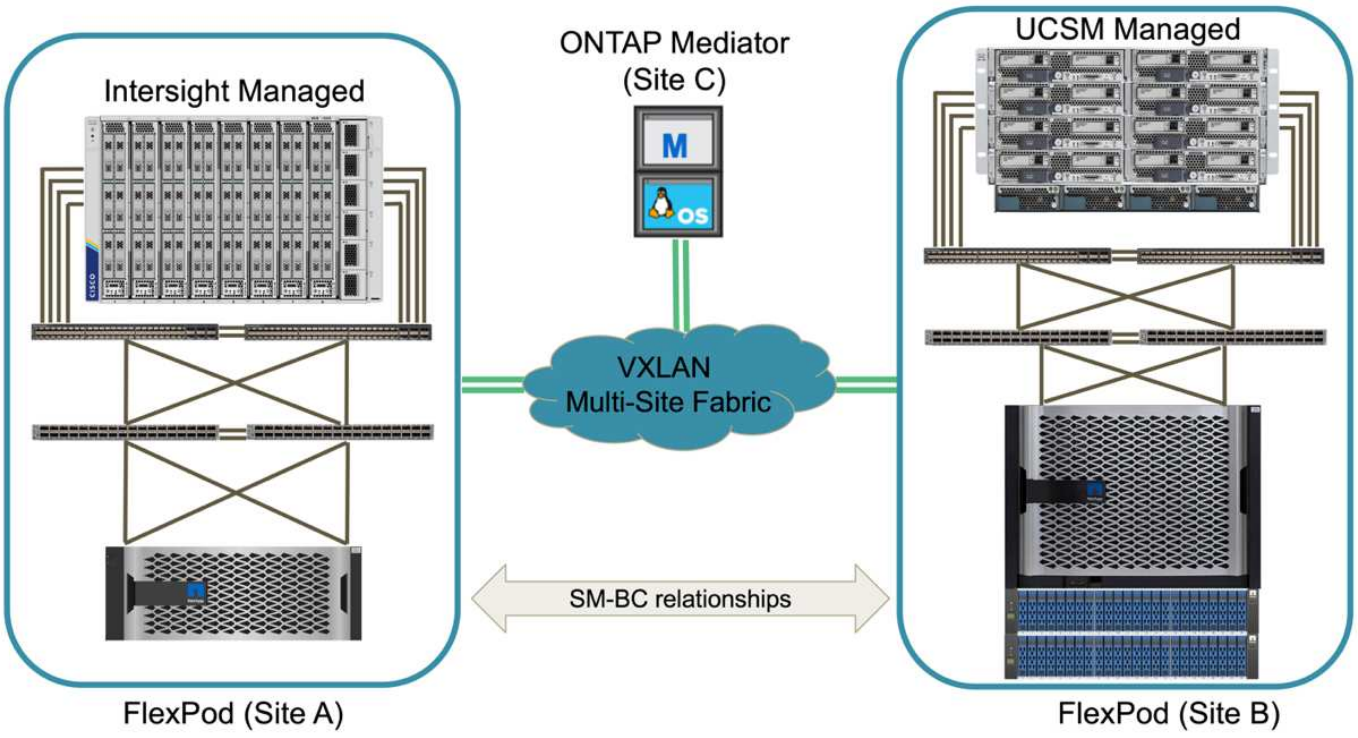
Los componentes redundantes de computación, red y almacenamiento están interconectados con una conectividad redundante entre los componentes. Este diseño de alta disponibilidad proporciona resiliencia de la solución y permite resistir escenarios de un único punto de error. El diseño de varios sitios 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.

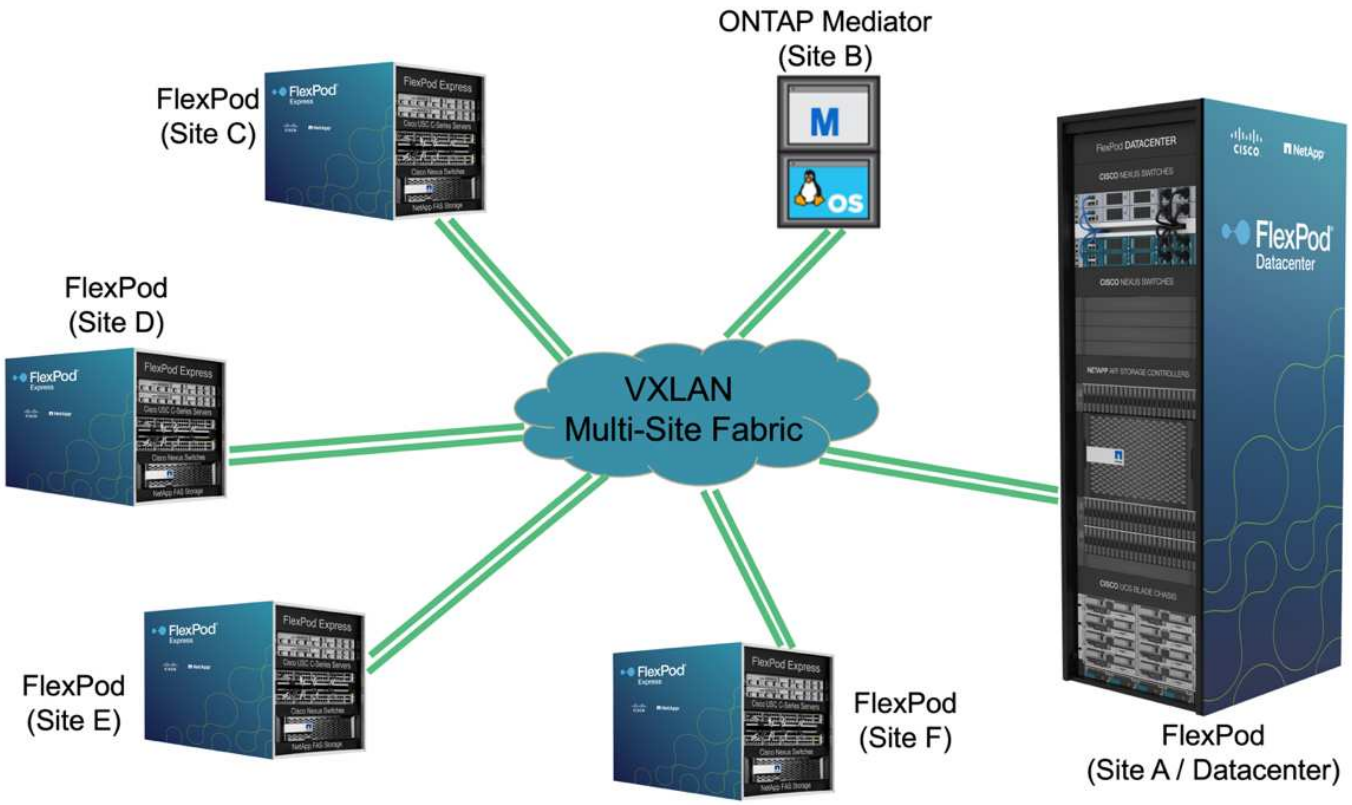


Para las empresas con mayores requisitos de recursos informáticos y de almacenamiento y múltiples sitios, una estructura multisitio basada en VXLAN permite a los múltiples sitios disponer de una estructura de red perfecta para facilitar la movilidad de aplicaciones, de modo que se pueda servir una aplicación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

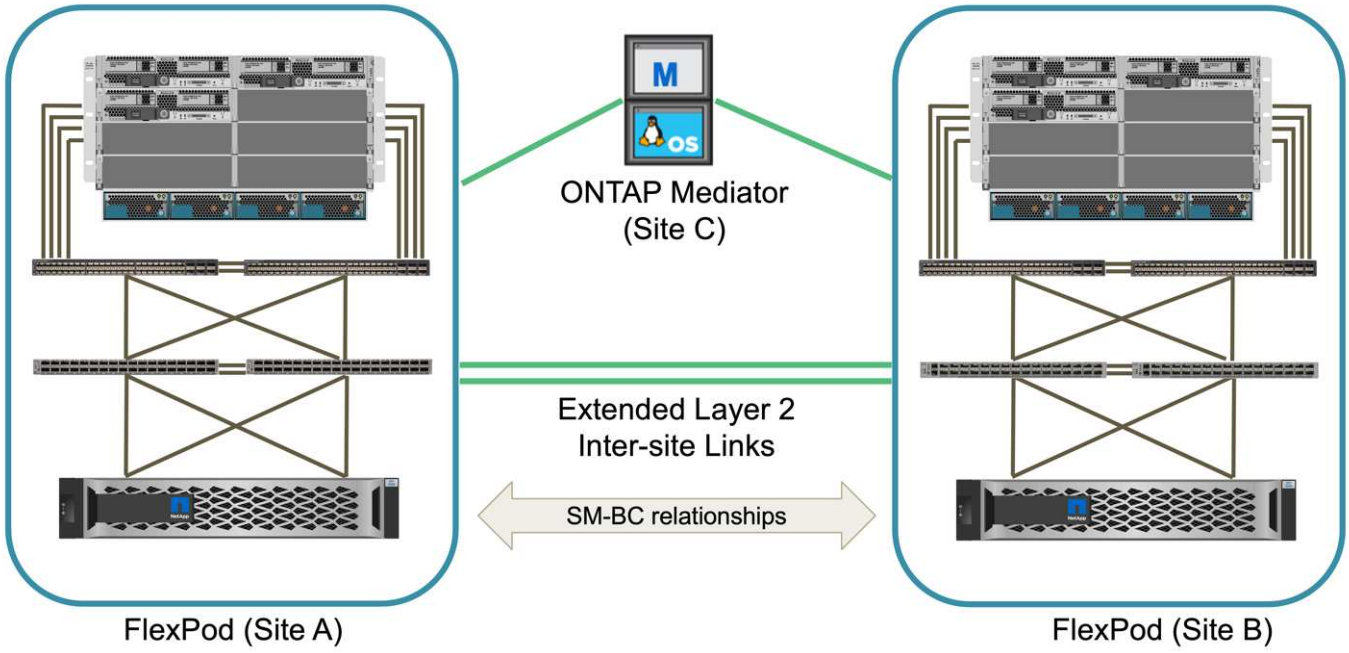
"Anterior: Solución FlexPod SM-BC."

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

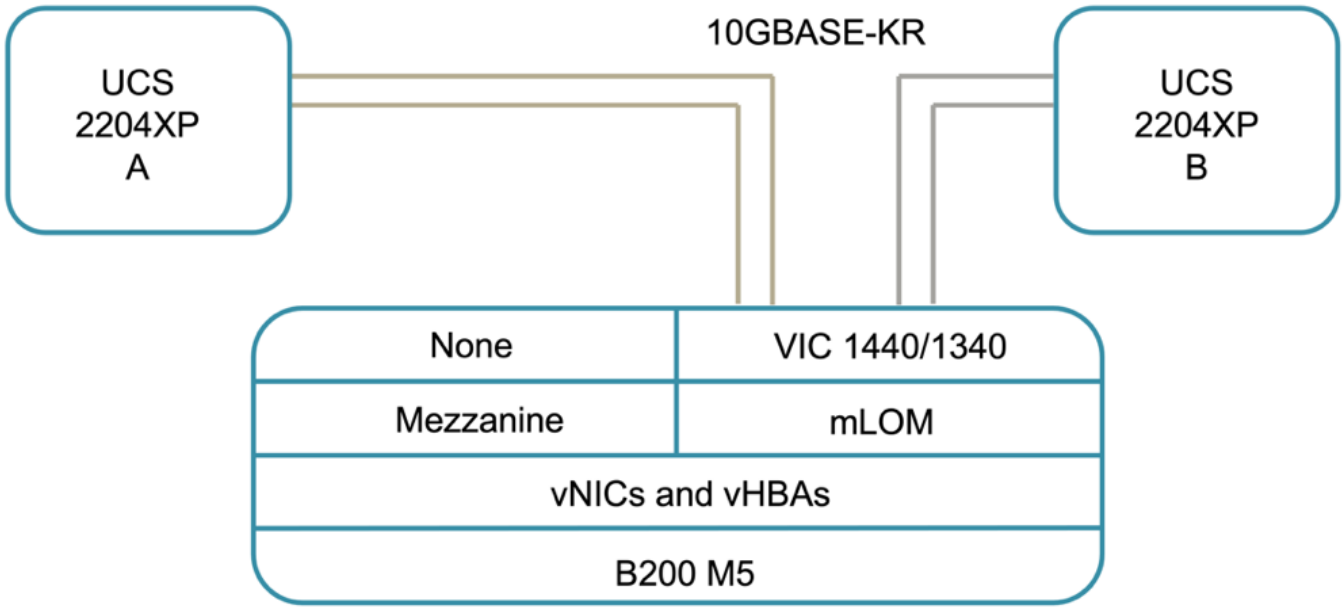
"Preivous: Validación de la solución - Descripción general."

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

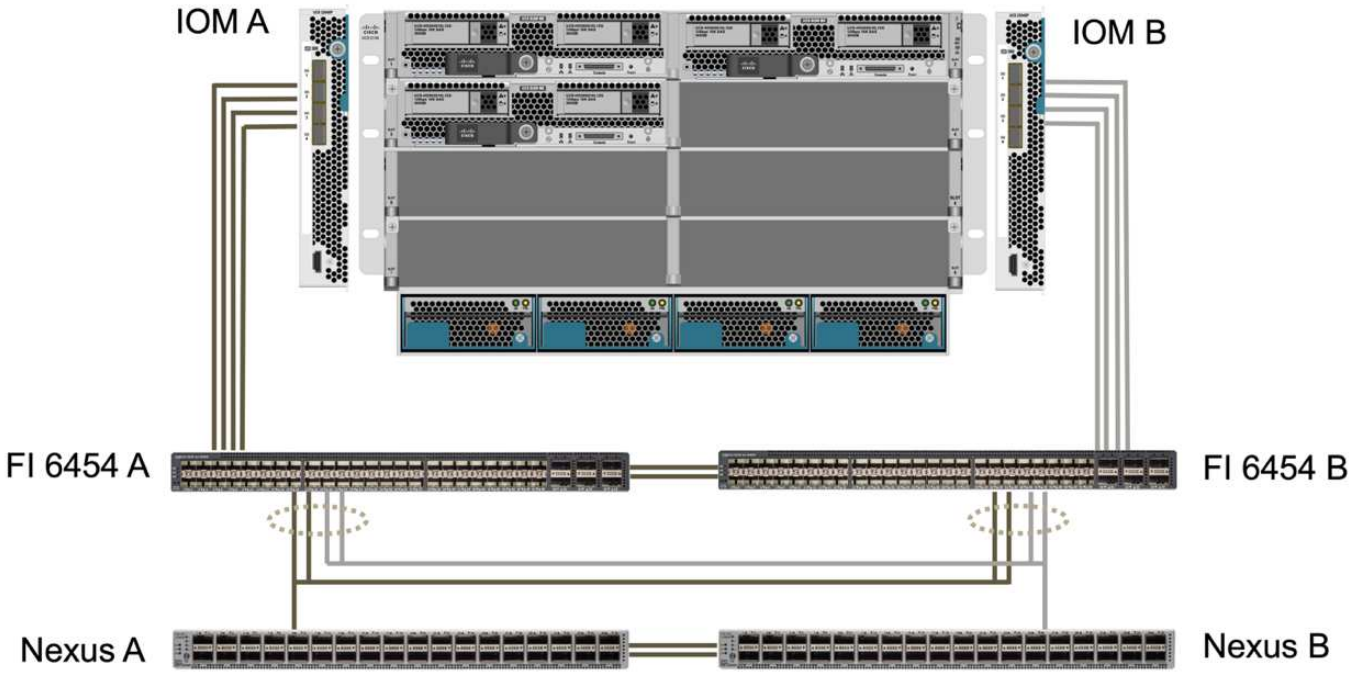
recomendadas habituales de la solución FlexPod. En las siguientes secciones se destacan algunas de las configuraciones y conectividad utilizadas para la validación. También se destacan algunas de las consideraciones relacionadas con SM-BC para proporcionar referencias y orientación de implementación.

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:

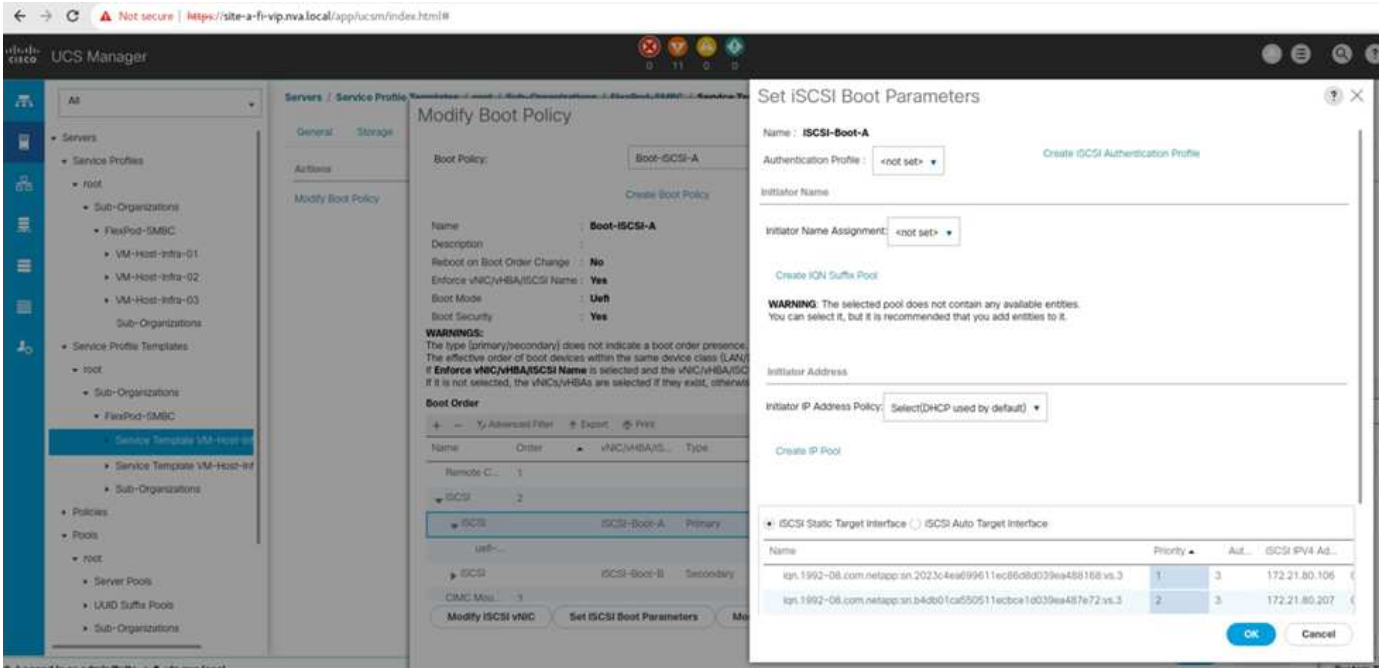
- Arranque SAN desde el almacenamiento A250 de AFF en cualquiera de las ubicaciones mediante el protocolo iSCSI.
- Se crean seis vNIC para los servidores en los que:
  - Dos NIC redundantes (vSwitch0-A y vSwitch0-B) transportan tráfico de gestión en banda. Opcionalmente, estos vNIC también pueden ser 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

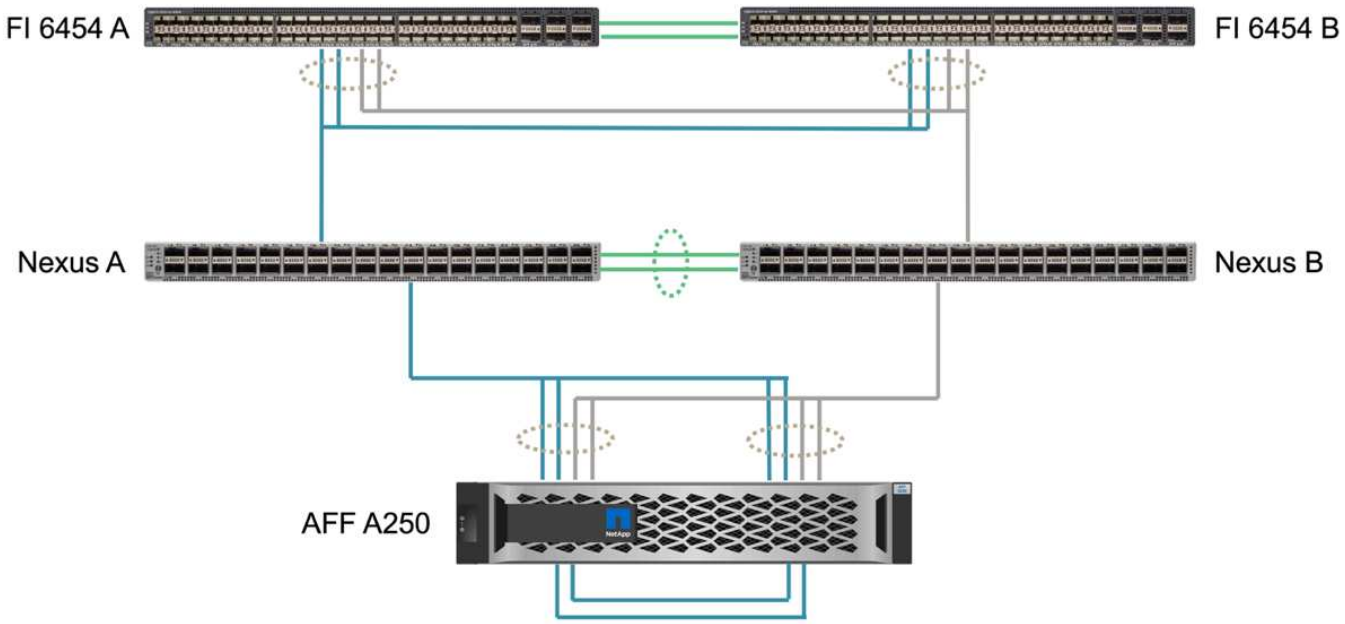
"Anterior: Validación de la solución - Computación."

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.

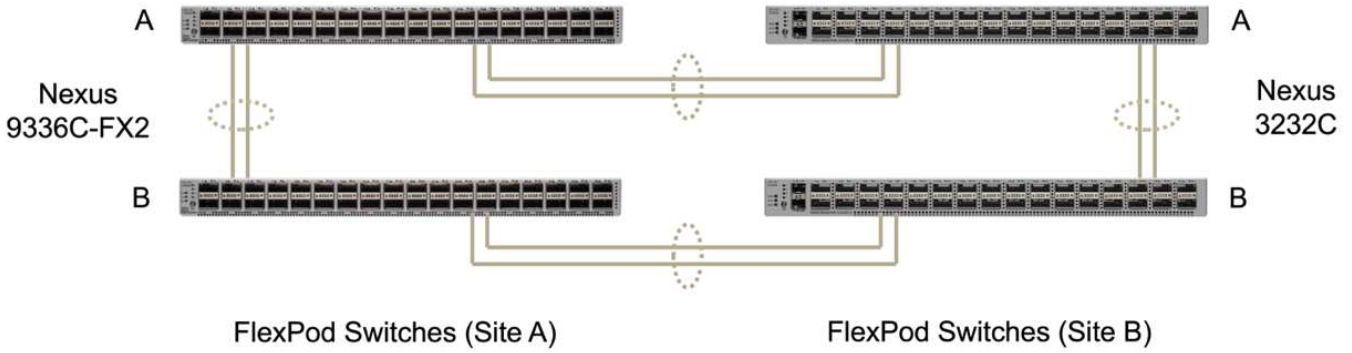
El siguiente diagrama muestra la conectividad local del switch Nexus en cada sitio. Además de lo que se muestra en el diagrama, también existen conexiones de red de consola y gestión para cada componente que no se muestra. Se utilizan los cables de arranque de 40 a 4 10G para conectar los switches Nexus 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.
NFS-VLAN	3335	VLAN NFS opcional para tráfico NFS

Nombre	ID DE VLAN	Uso
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."

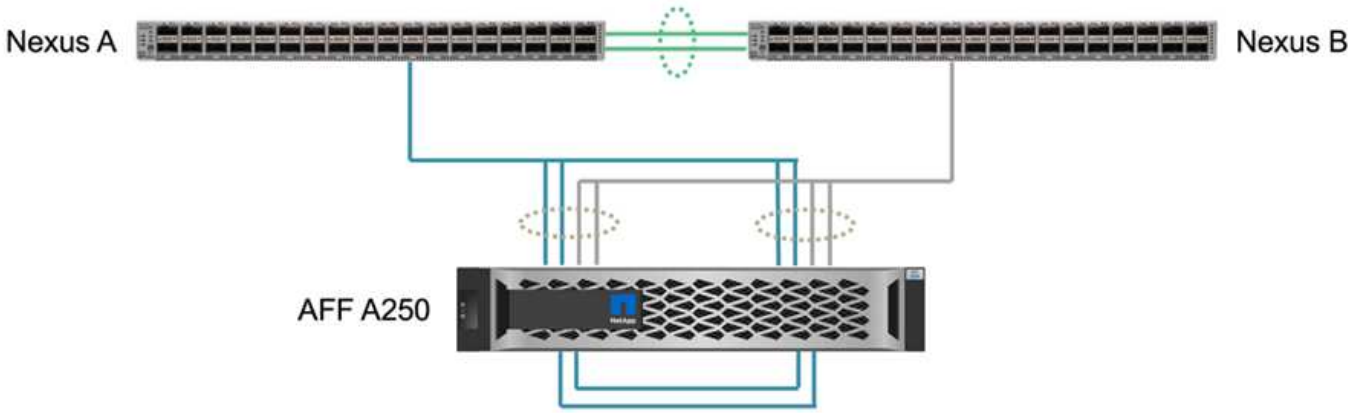
Validación de la solución - almacenamiento

"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.

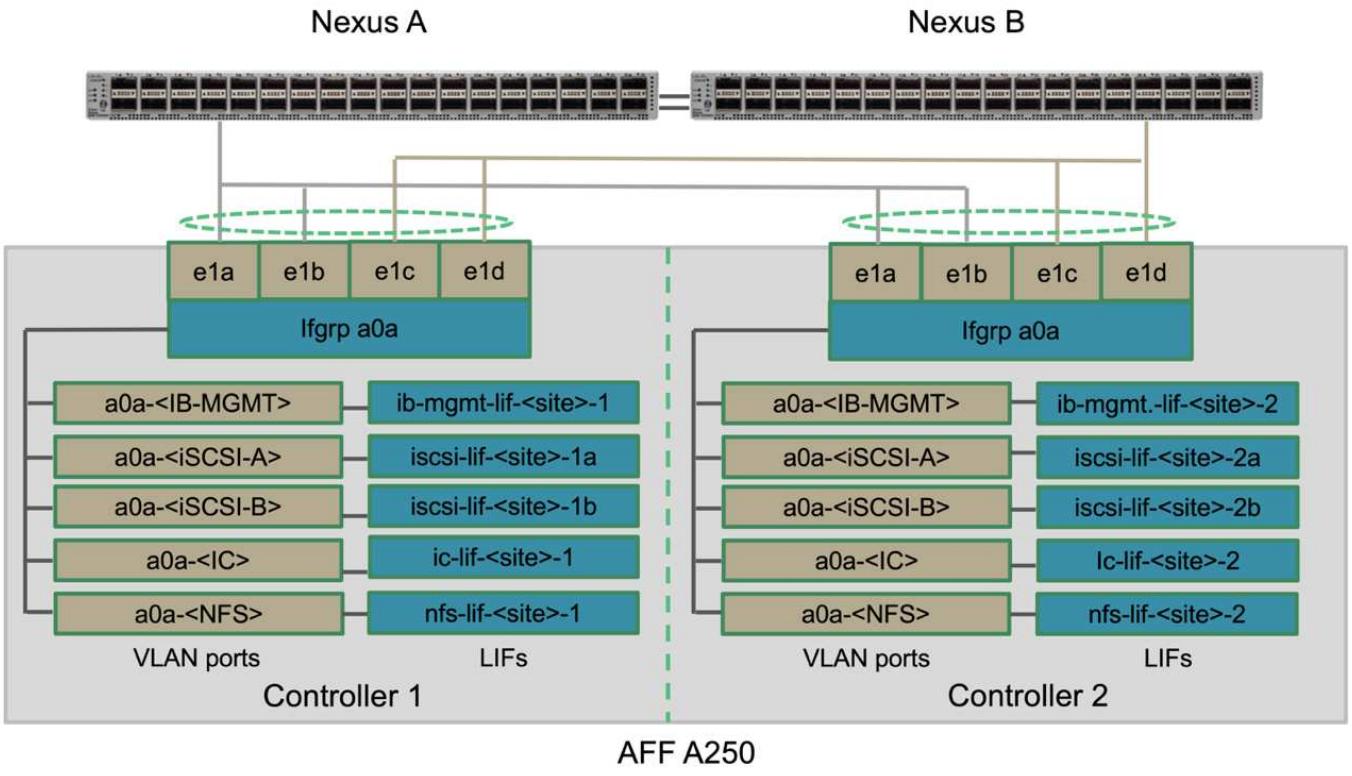


Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
AFF A250 A.	e0c	AFF A250 B.	e0c
	e0d		e0d
	e1a	Nexus a	1/10/1
	e1b		1/10/2
	e1c	Nexus B	1/10/1
	e1d		1/10/2
AFF A250 B.	e0c	AFF A250 A.	e0c
	e0d		e0d
	e1a	Nexus a	1/10/3
	e1b		1/10/4
	e1c	Nexus B	1/10/3
	e1d		1/10/4

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.

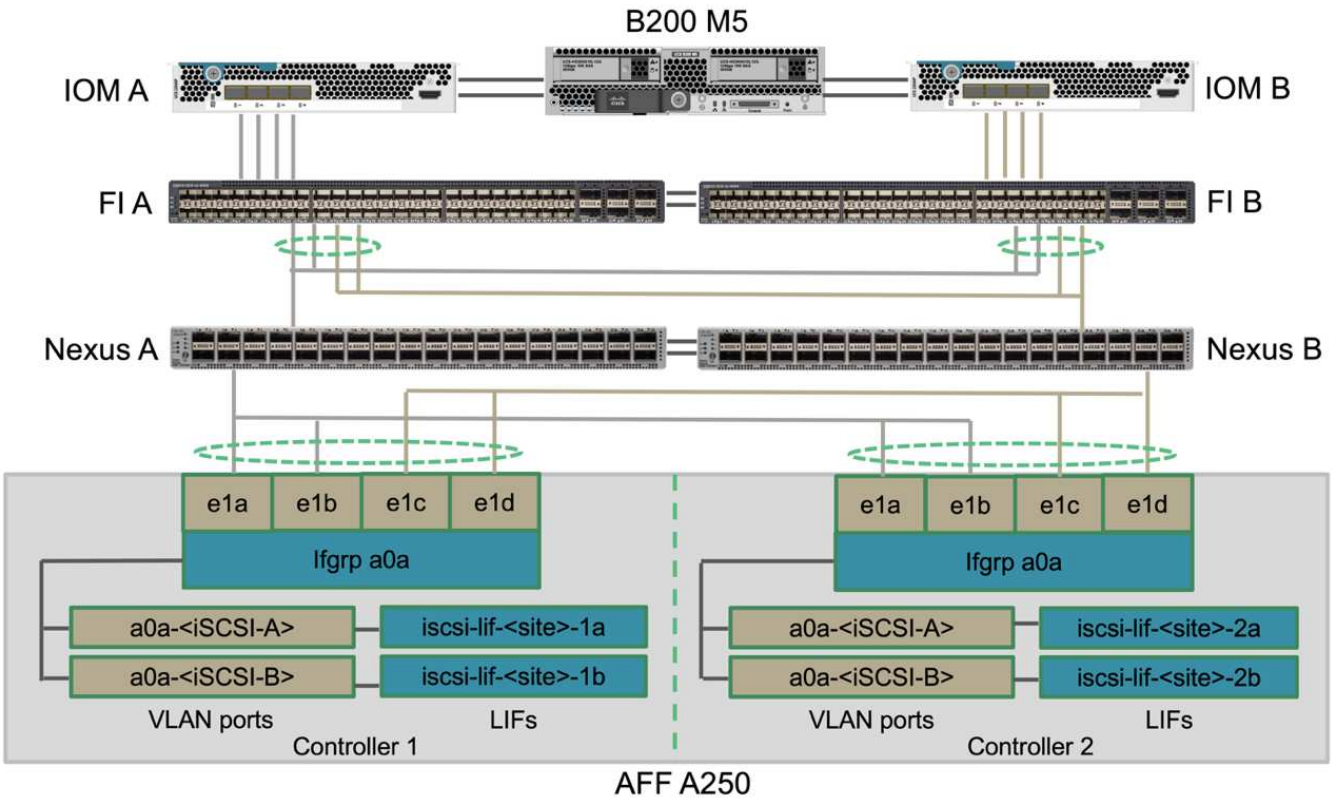


Arranque SAN

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.

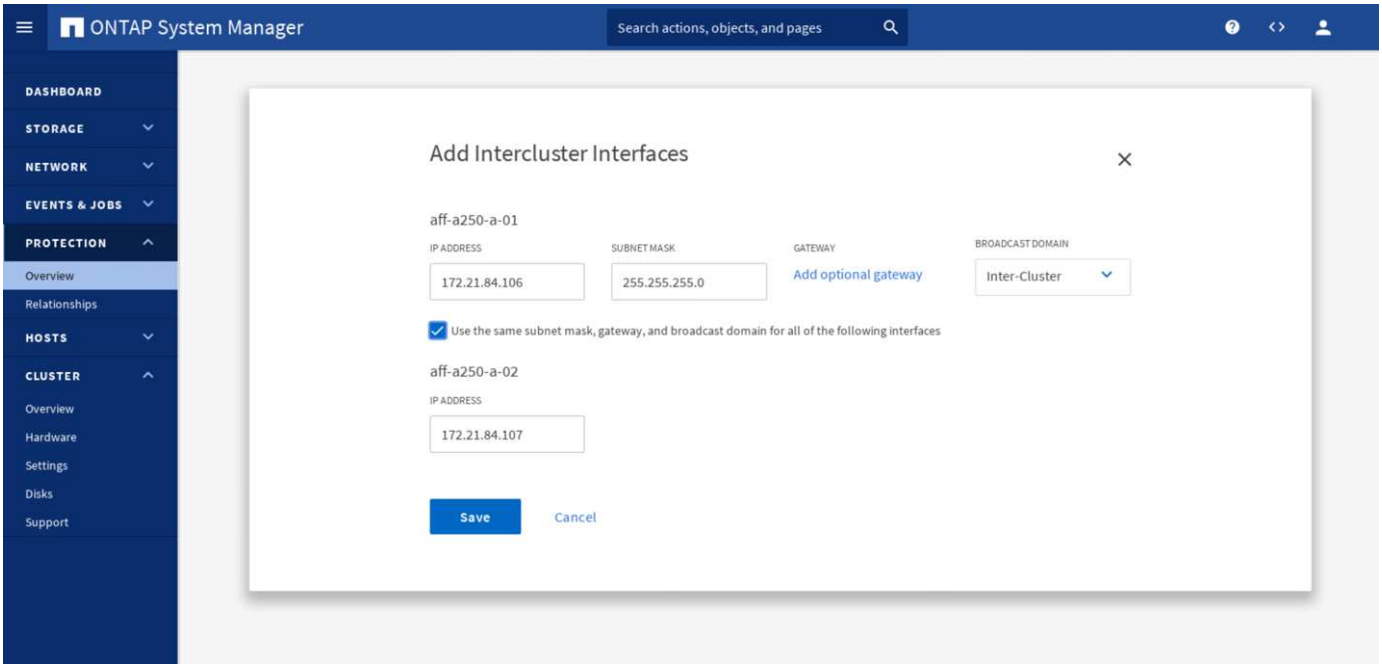
La figura siguiente muestra la conectividad para arranque SAN iSCSI de Cisco UCS Server desde almacenamiento NetApp. En el arranque SAN iSCSI, a cada servidor Cisco UCS se le asignan dos NIC iSCSI (una para cada estructura SAN) que proporcionan conectividad redundante desde el servidor hasta el almacenamiento. 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.



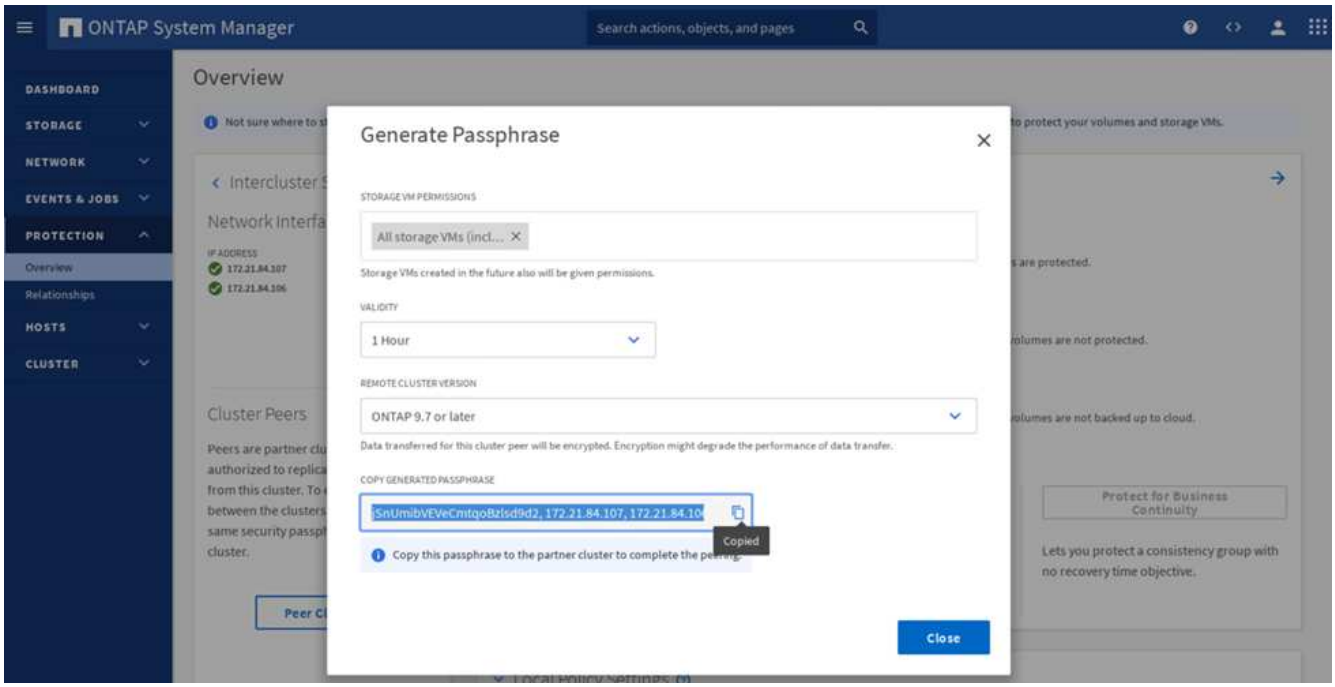
Conexión de clústeres entre iguales

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.

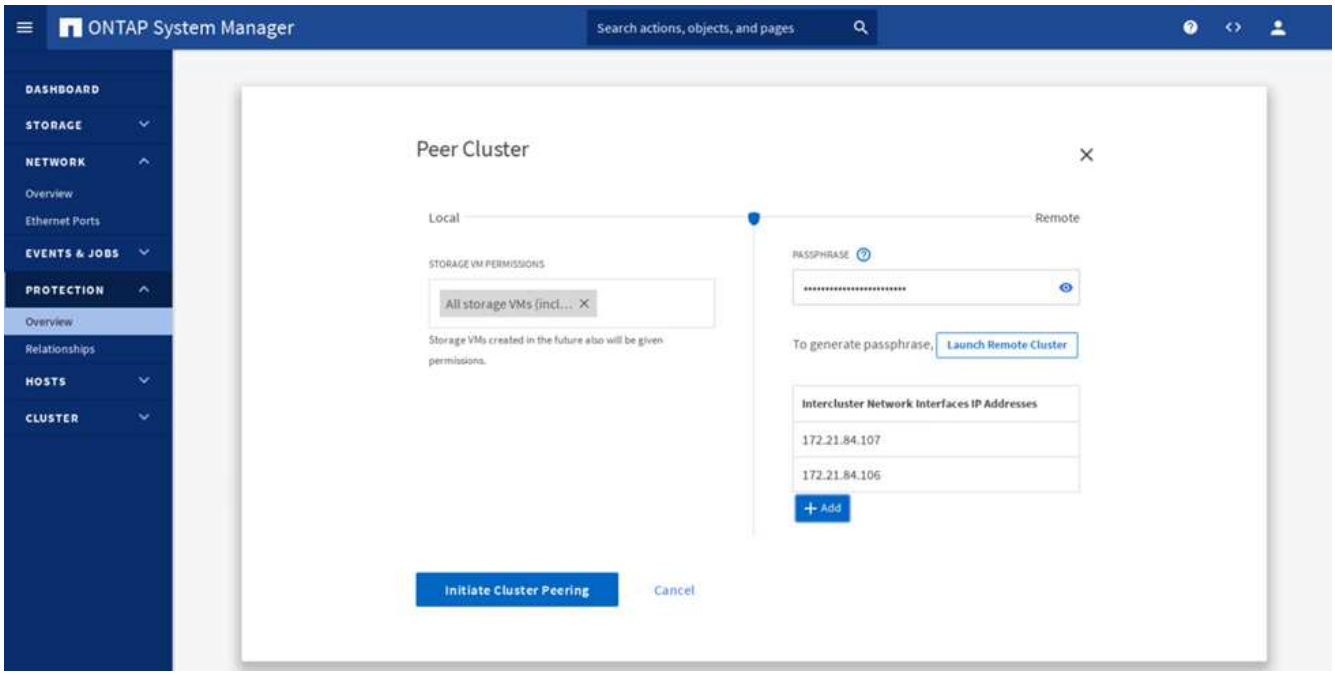


Para conectar los dos clústeres en relación de paridad, complete los siguientes pasos:

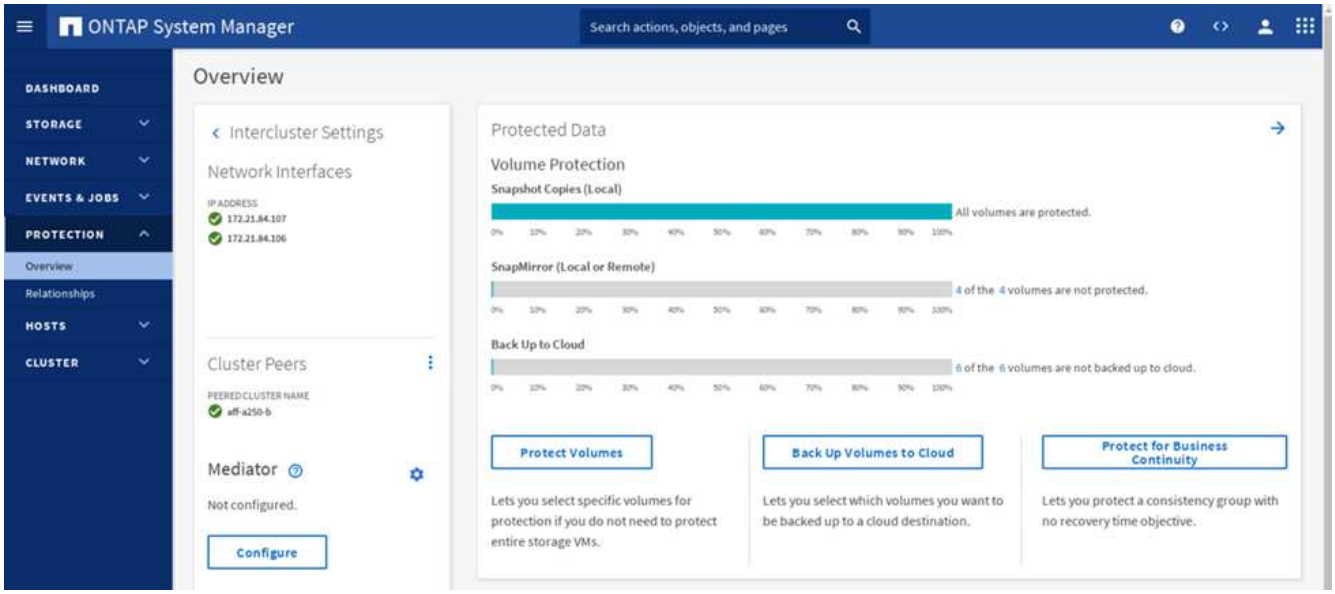
1. Genere una clave de acceso de paridad entre clústeres en el primer clúster.



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.

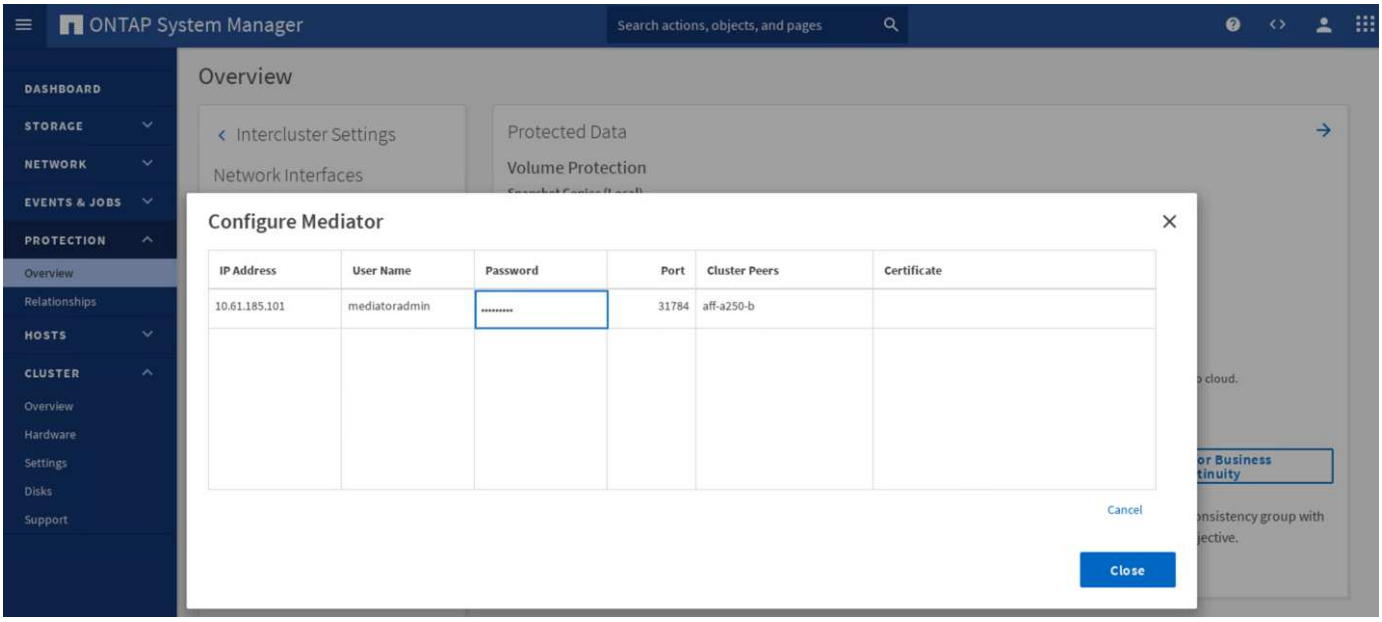


Instalación y configuración del Mediador ONTAP

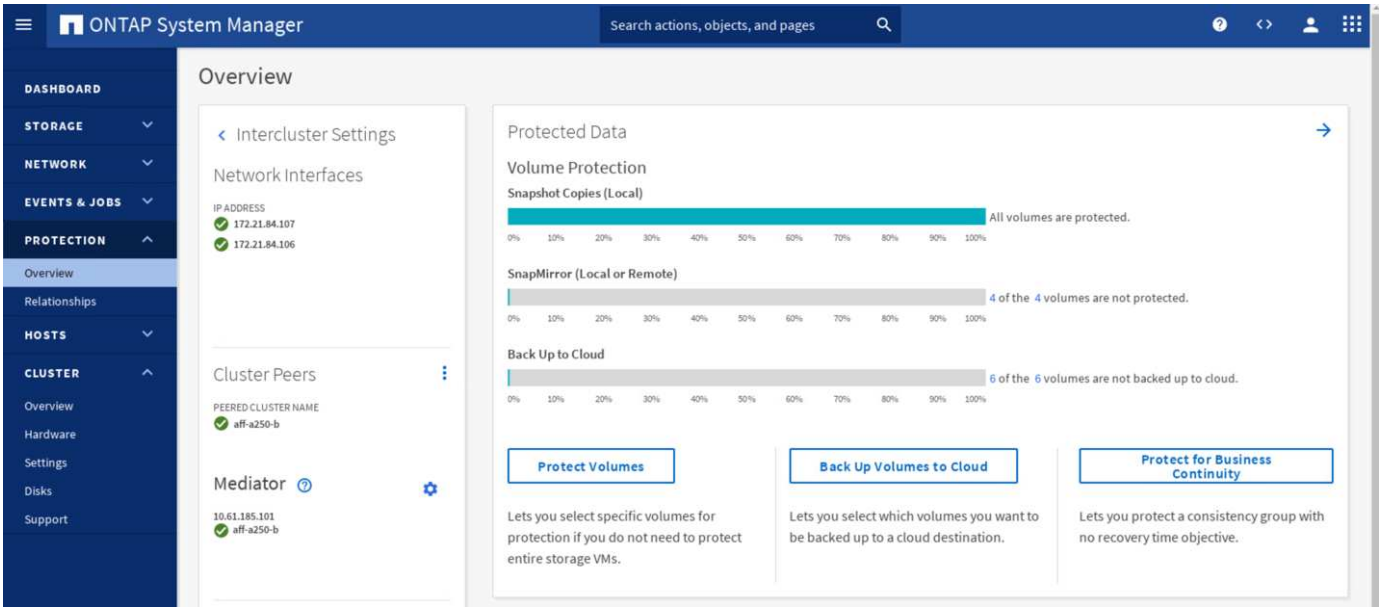
El Mediador ONTAP establece un quórum para los clústeres de ONTAP en una relación de SM-BC. Coordina la conmutación automática al nodo de respaldo cuando se detecta un fallo y ayuda a evitar situaciones de cerebro dividido cuando cada clúster intenta establecer el control simultáneamente como el clúster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



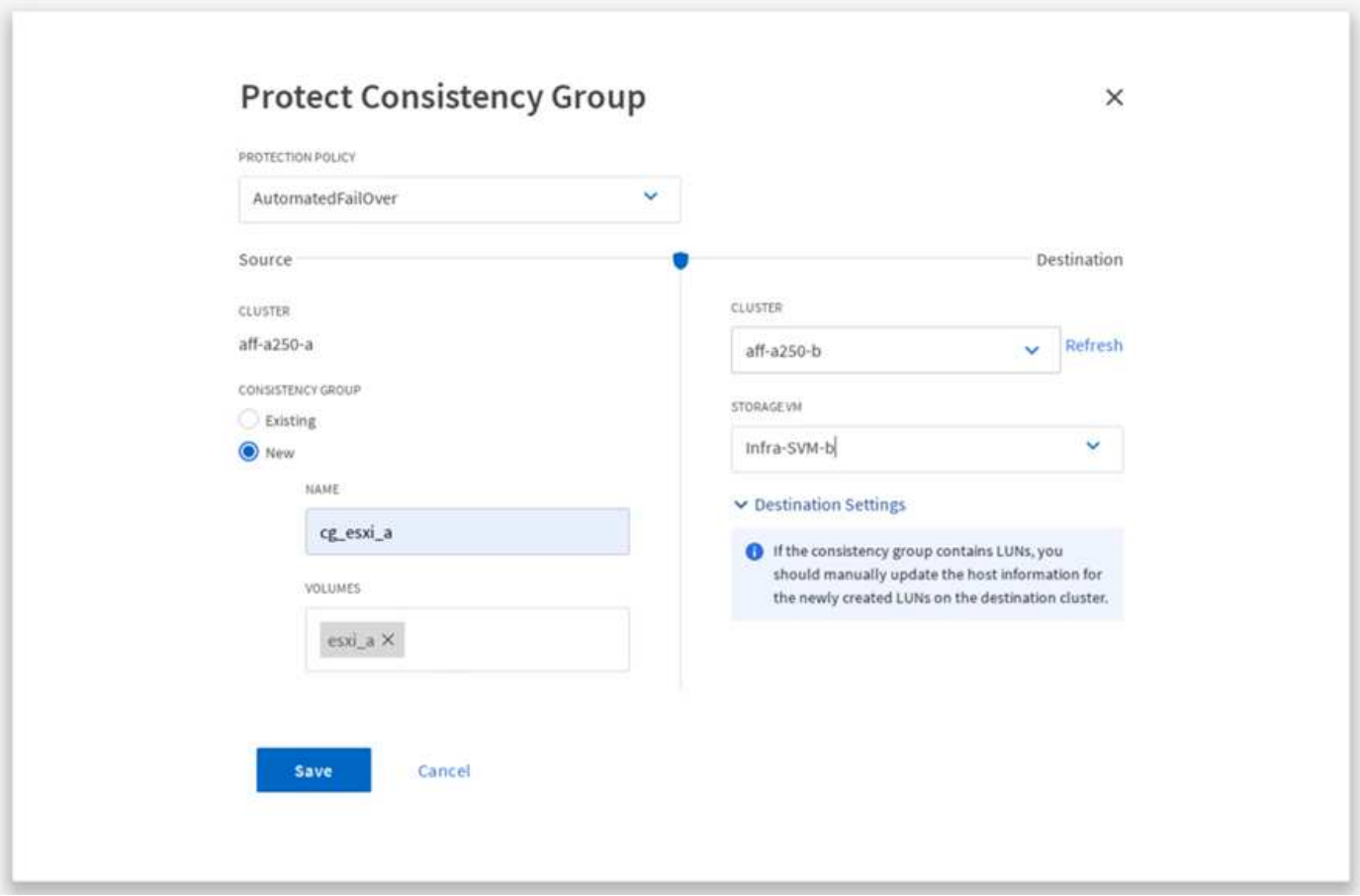
Grupo de consistencia SM-BC

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.

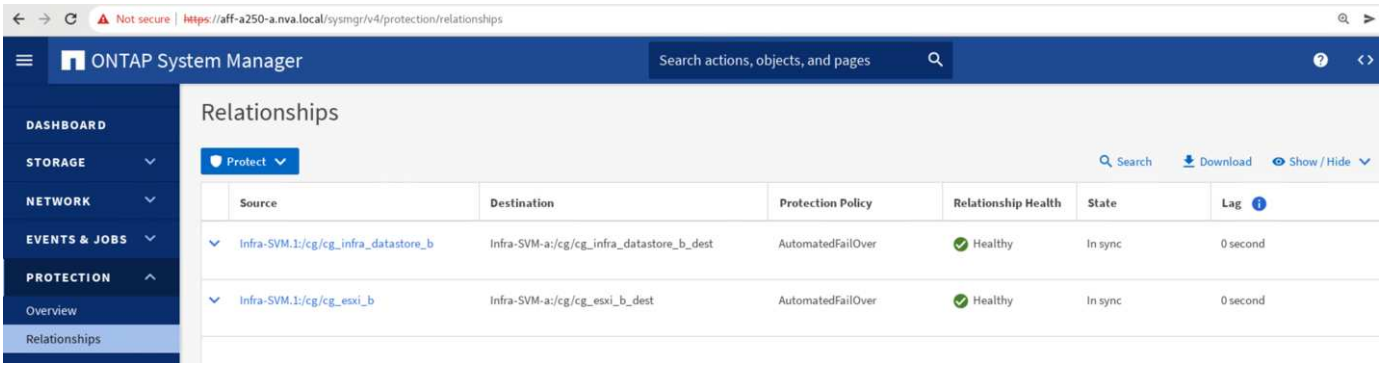


En la siguiente tabla, se enumeran los cuatro grupos de coherencia que se crean y los volúmenes que se incluyen en cada grupo de coherencia para la prueba de validación.

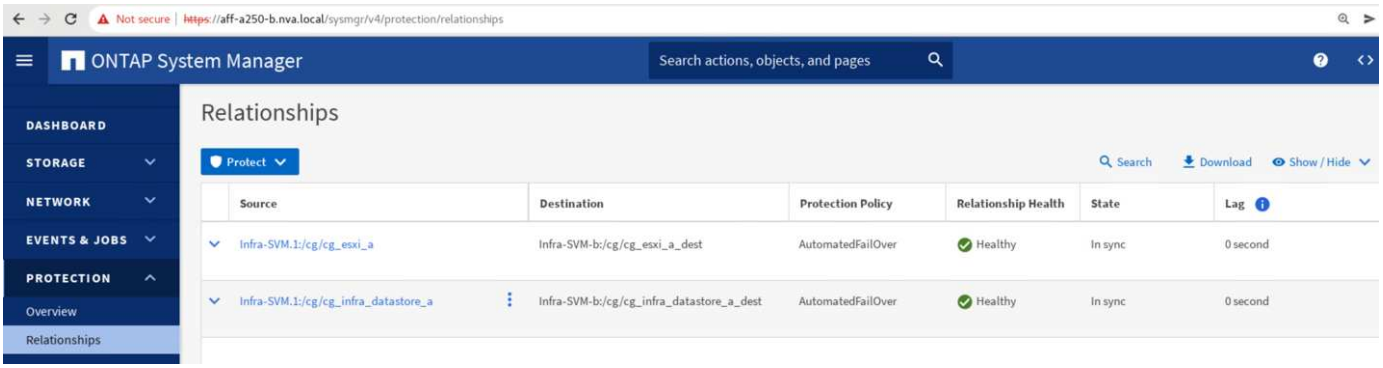
System Manager	Grupo de consistencia	Volúmenes
Centro a	cg_esxi_a	esxi_a
Centro a	cg_infra_datastore_a	infra_datastore_a_01 infra_datastore_a_02
Centro B	cg_esxi_b	esxi_b
Centro B	cg_infra_datastore_b	infra_datastore_b_01 infra_datastore_b_02

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

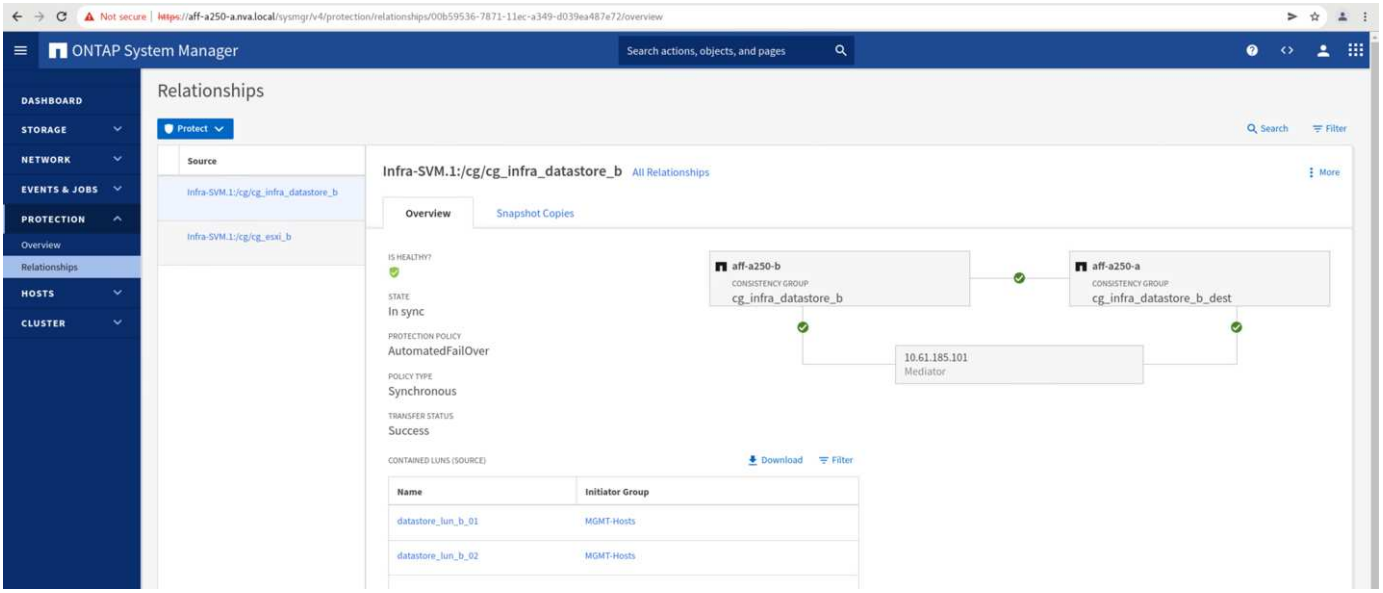
Esta captura de pantalla muestra las relaciones de los grupos de consistencia en la instalación A.



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."

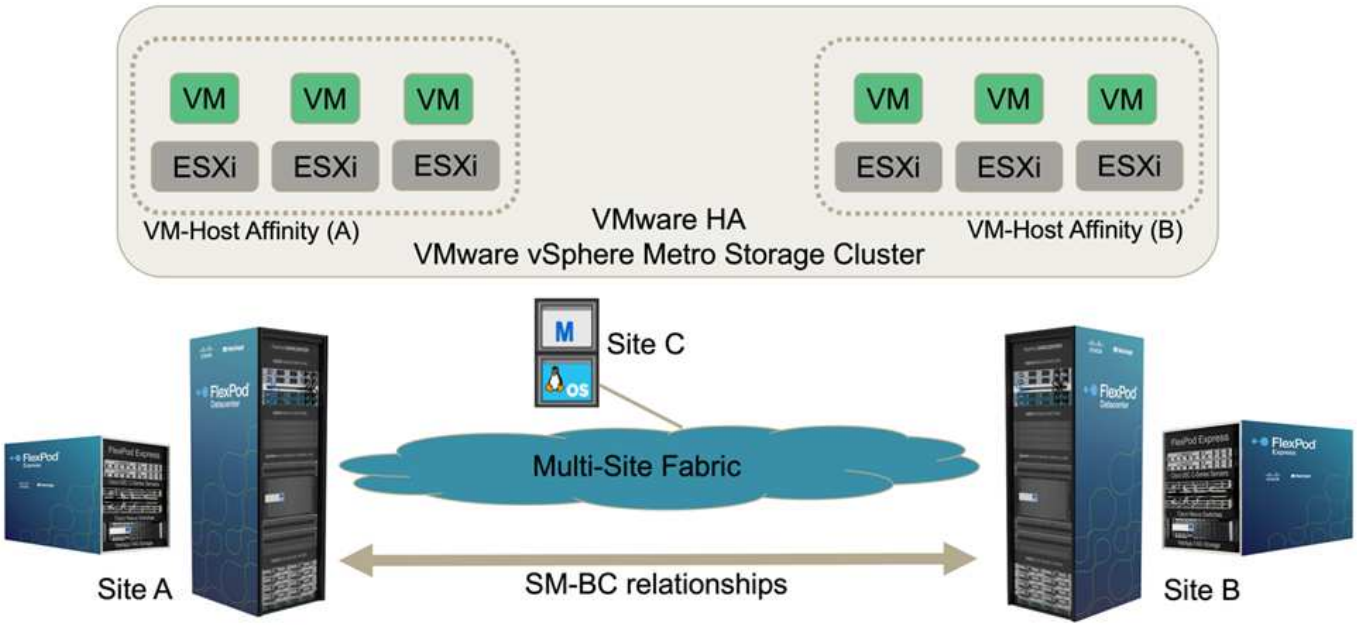
En la solución FlexPod SM-BC multisitio, un solo VMware vCenter gestiona los recursos de infraestructura virtual para toda la solución. Los hosts de ambos centros de datos participan en un único clúster de alta disponibilidad de VMware que abarca ambos centros de datos. Los hosts tienen acceso a la solución 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.

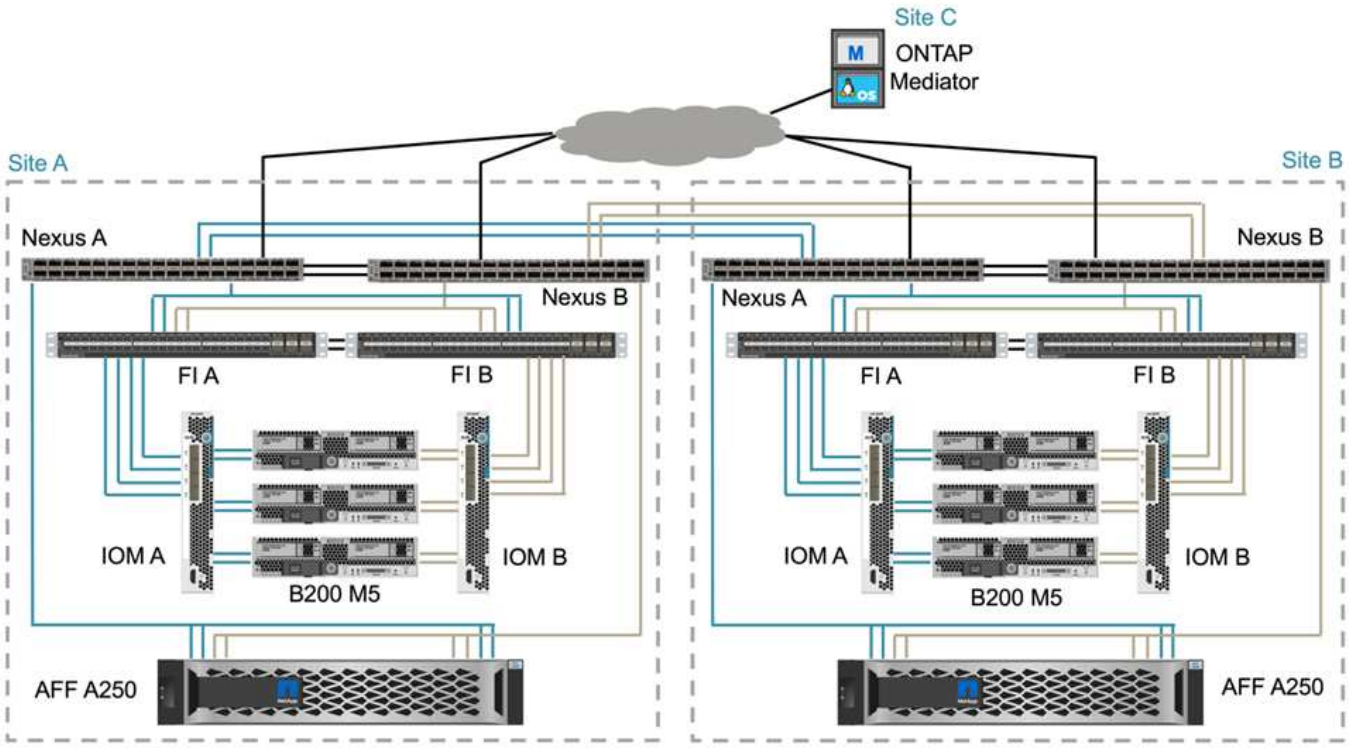
Sin embargo, las configuraciones que permiten que los equipos virtuales se ejecuten en ambos centros asegurarán de que VMware ha puede reiniciar los equipos virtuales en hosts de centro remoto para proporcionar flexibilidad a la solución. Para acomodar máquinas virtuales para ejecutarse en ambos sitios, 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.



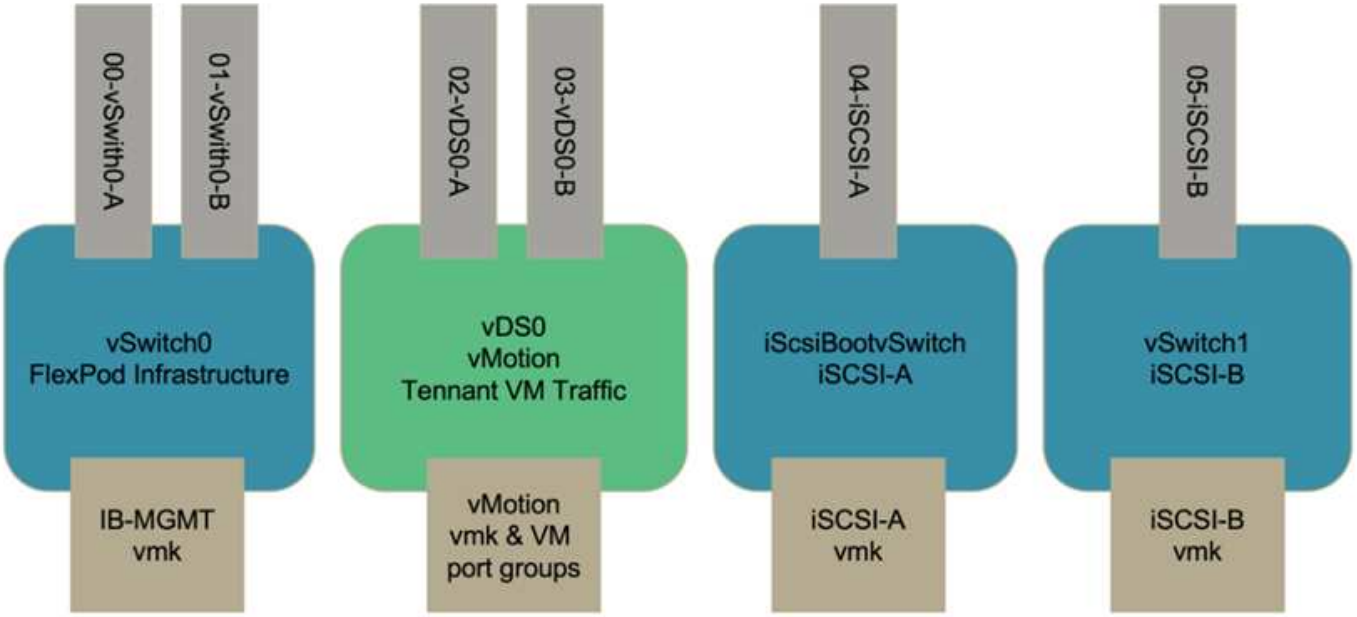
La arquitectura de puesta en marcha de FlexPod es idéntica en cada site para validar esta solución. Sin embargo, la solución admite implementaciones asimétricas y puede añadirse a una solución FlexPod existente si cumple los requisitos.

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.

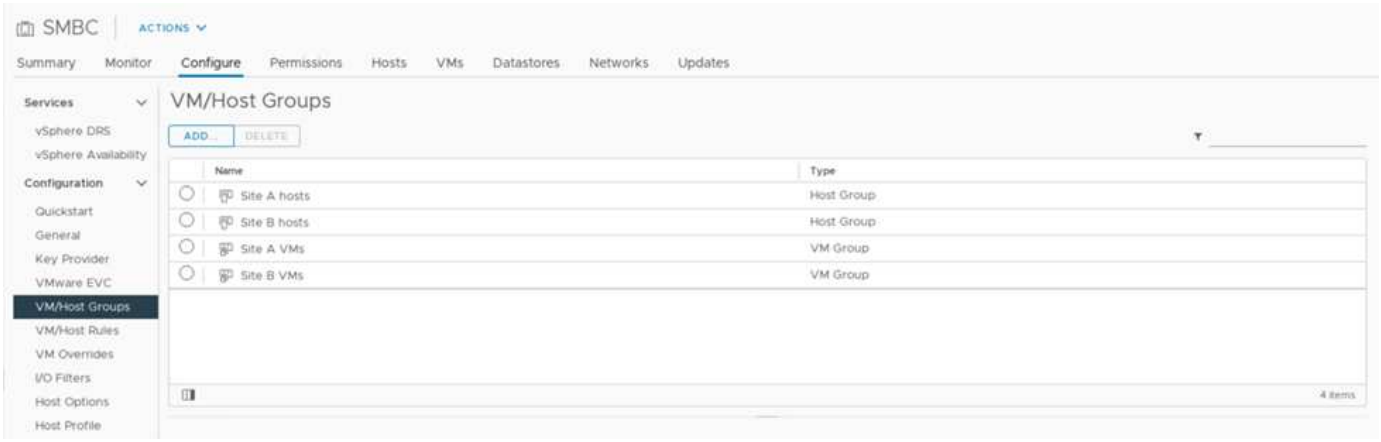
Reglas y grupos de afinidad de VM-Host

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.

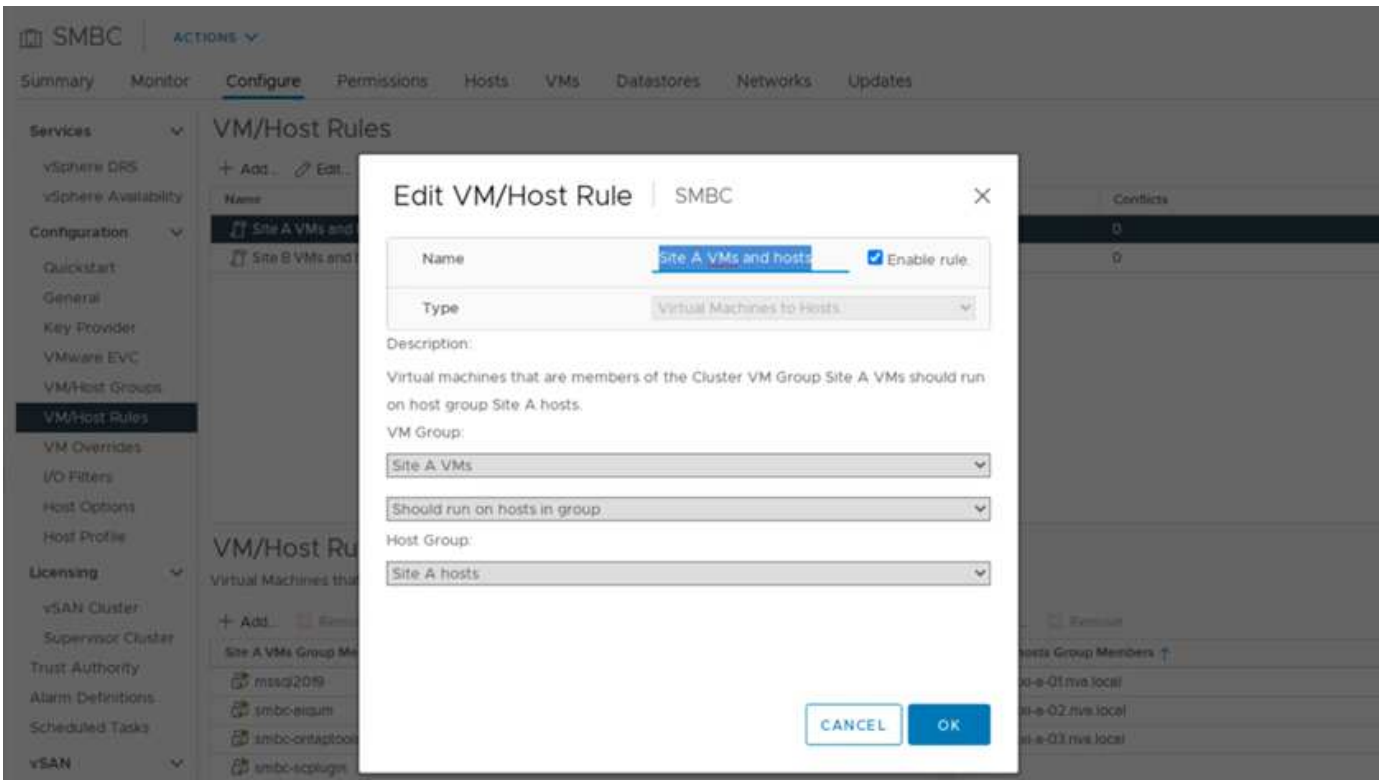
En el caso de una máquina virtual que usa almacenes de datos locales, su acceso a los discos virtuales se convierte en remoto si se migra a un host del sitio remoto y, por lo tanto, se aumenta la latencia de las operaciones de lectura debido a la distancia física entre los sitios. Por lo tanto, se recomienda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

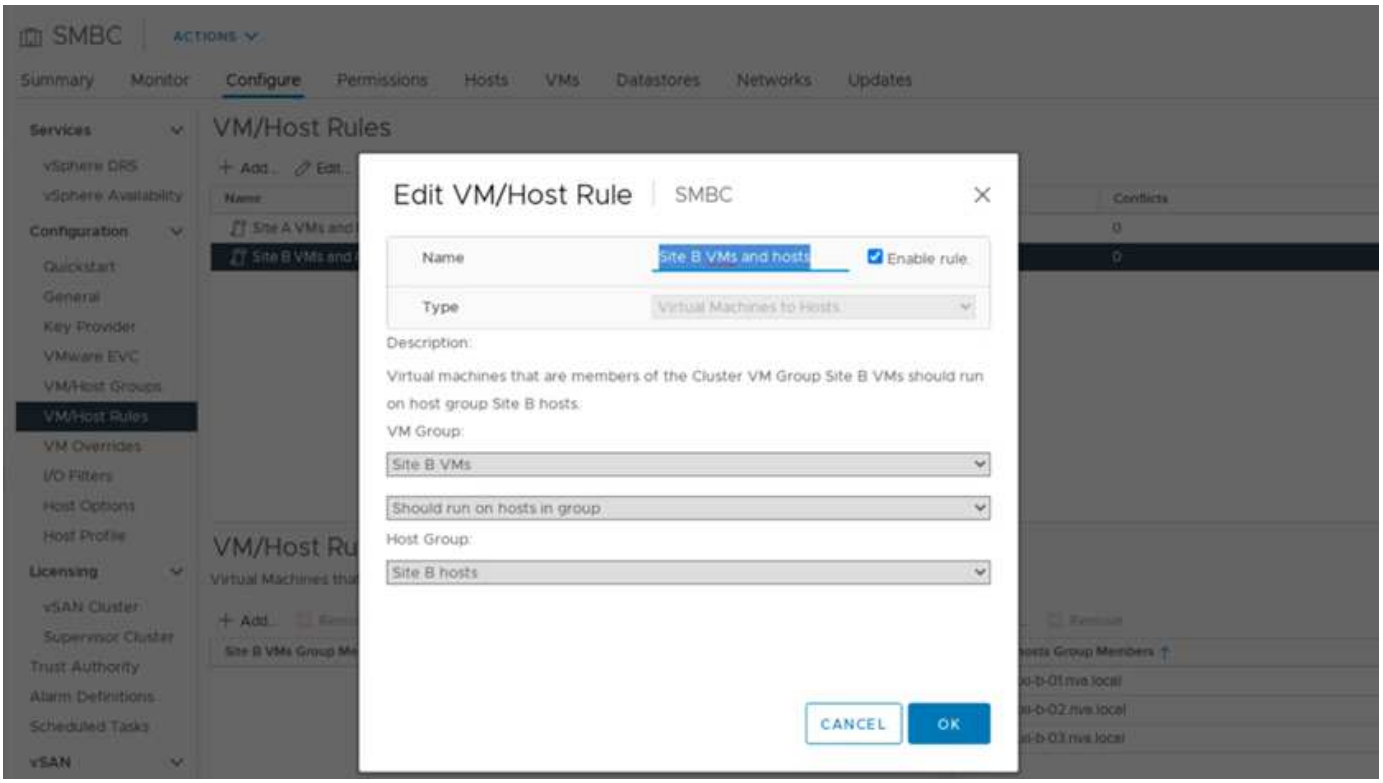
Mediante el uso de un mecanismo de afinidad de VM/host, se puede usar VM/grupos de hosts para crear un grupo de VM y un grupo de hosts para máquinas virtuales y hosts ubicados en un sitio determinado. Con las reglas de host/VM, puede especificar la política que deben seguir las máquinas virtuales y los 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”.

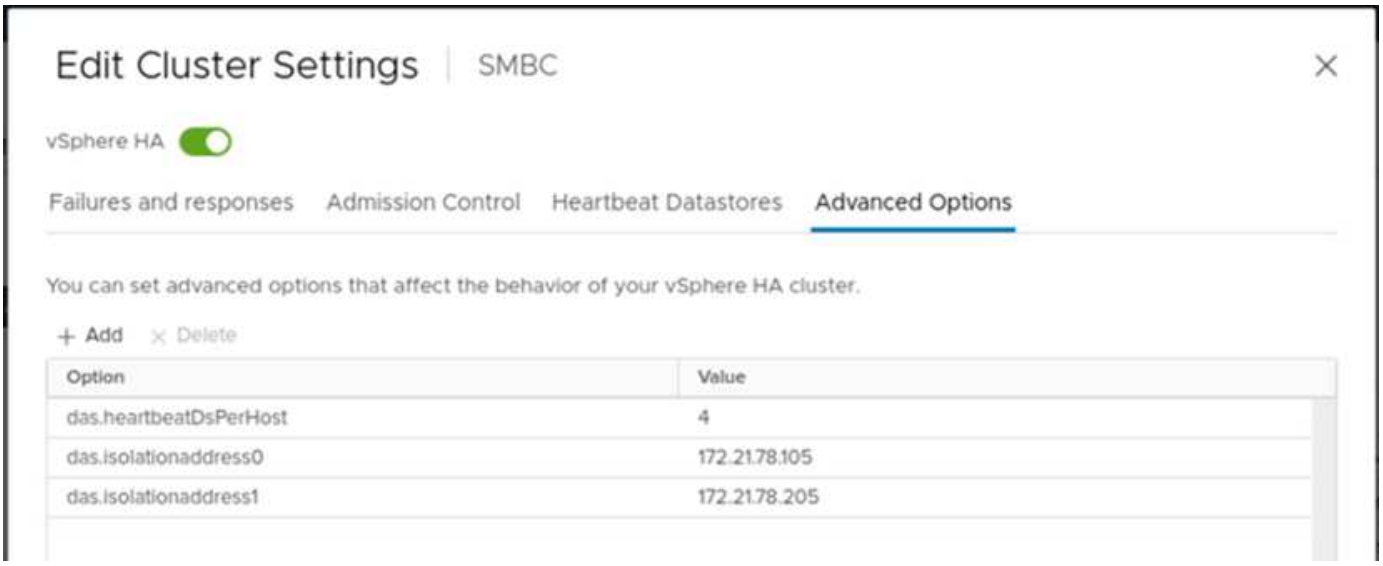




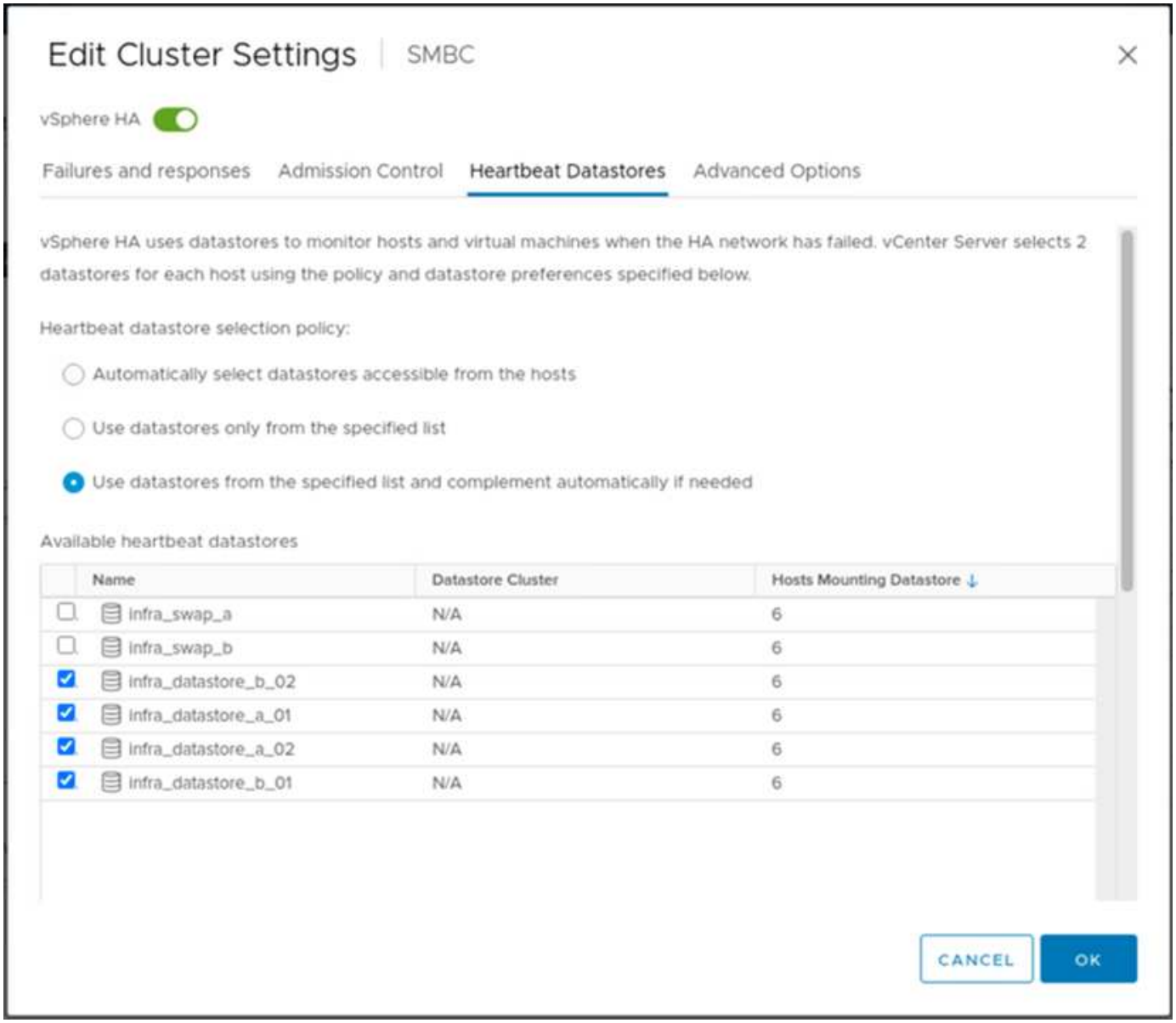
Corazón de vSphere ha

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.

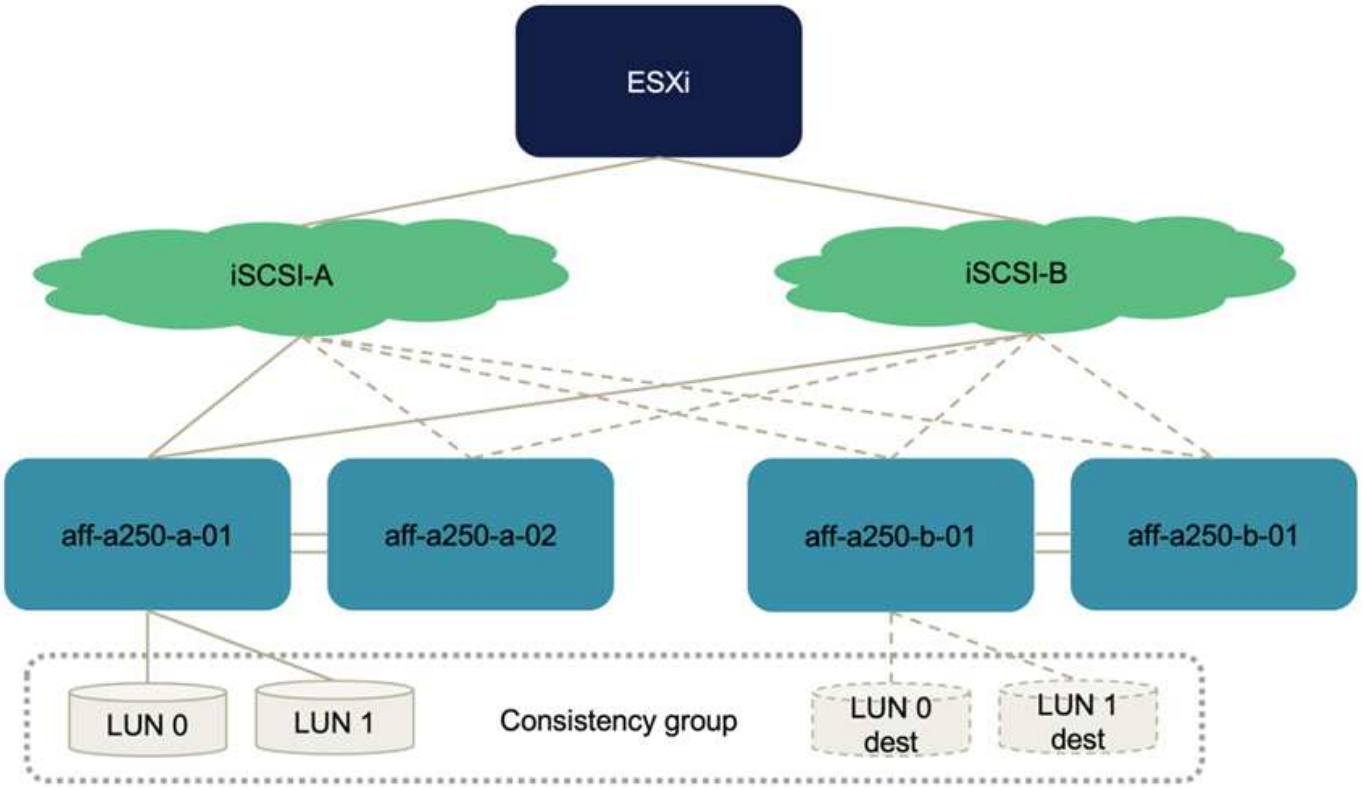
Además de arrancar un host ESXi ubicado en un sitio desde su LUN de arranque iSCSI local, también se llevaron a cabo pruebas para arrancar el host ESXi cuando la controladora de almacenamiento local está en estado de toma de control o cuando su clúster de almacenamiento local no está completamente disponible. 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.

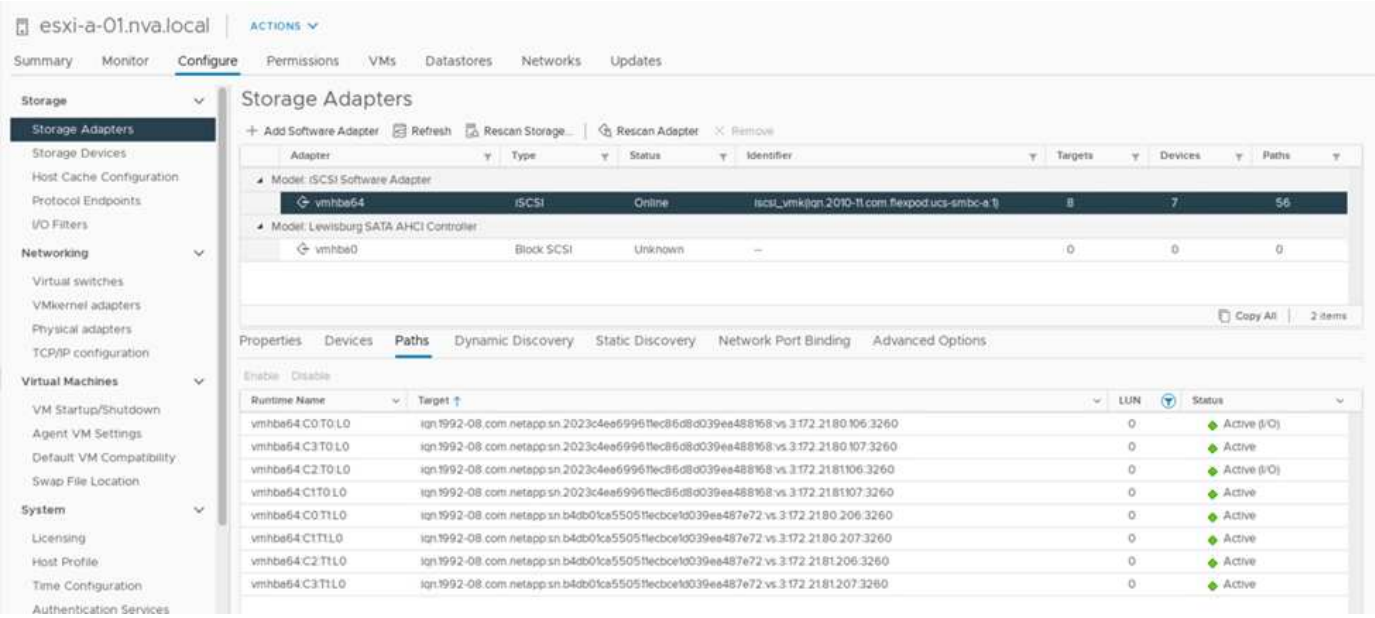
Después de configurar la relación del grupo de consistencia SM-BC y de asignar correctamente las LUN reflejadas a los iniciadores, el número de rutas de la LUN se duplica. Para esta implementación, pasa de tener dos rutas activo/optimizado y dos rutas activo/no optimizadas a tener dos rutas activas/optimizadas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

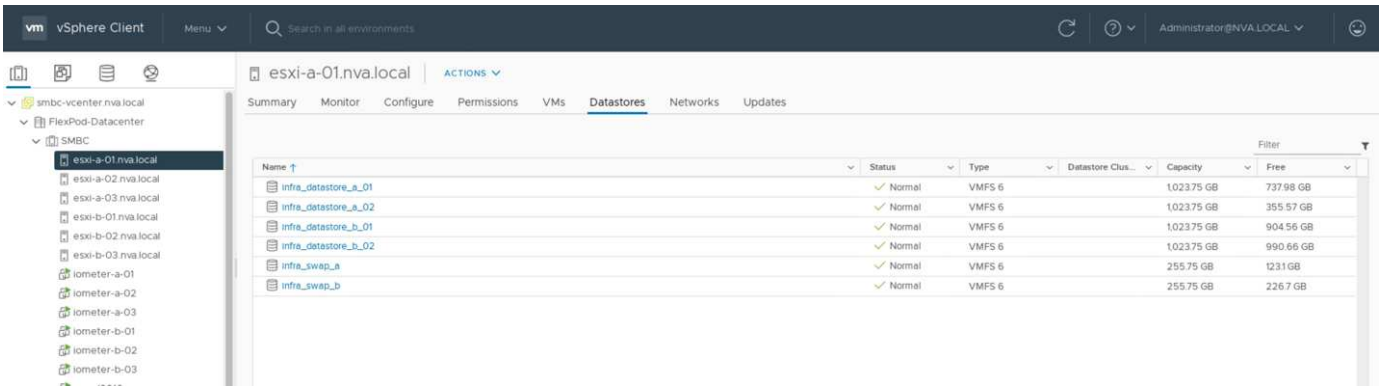
Prueba de afinidad de VMware vMotion y VM/host

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.

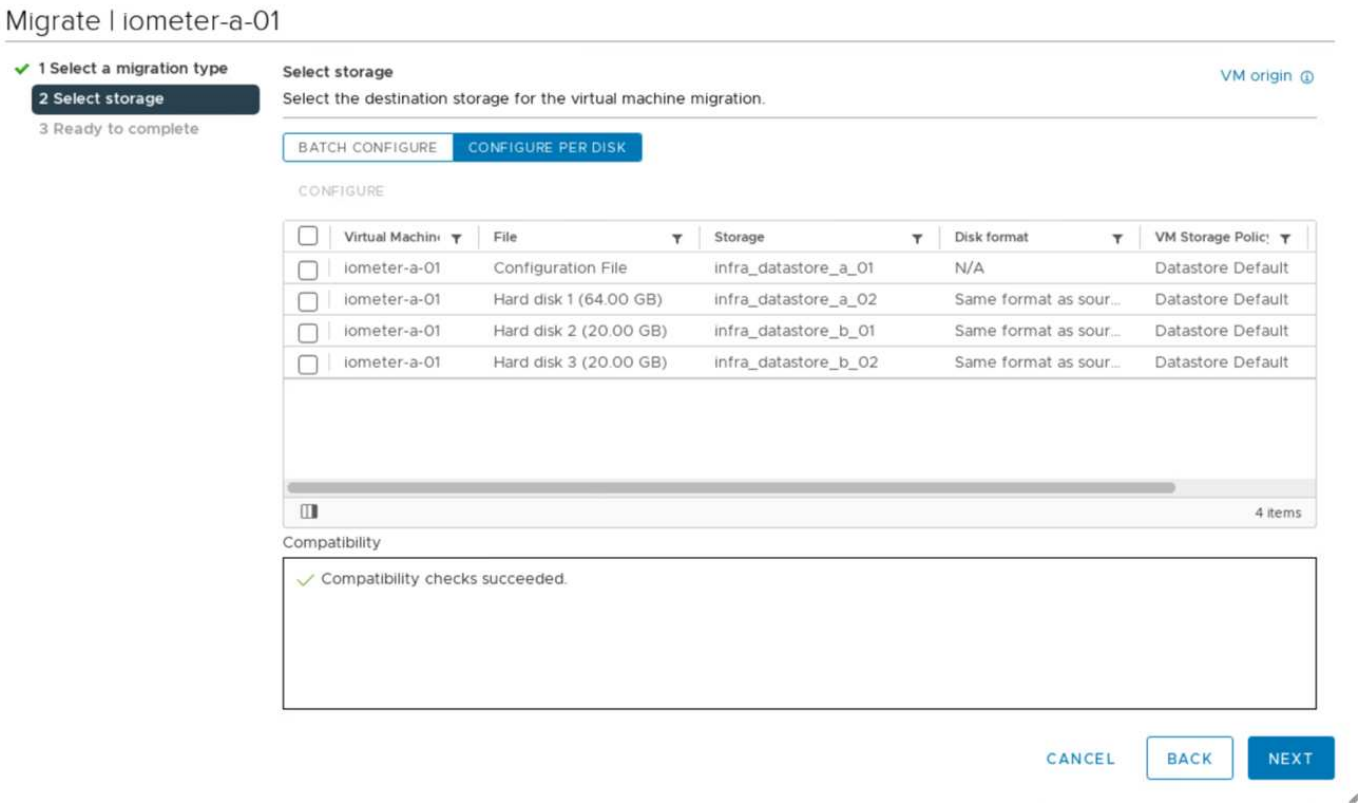
Para que las máquinas virtuales puedan usar servicios de almacenamiento desde un sitio de SM-BC, todos los hosts del clúster deben montar los almacenes de datos iSCSI de ambos sitios para permitir la migración de máquinas virtuales entre los dos sitios y en casos de conmutación por error en caso de desastre.

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.



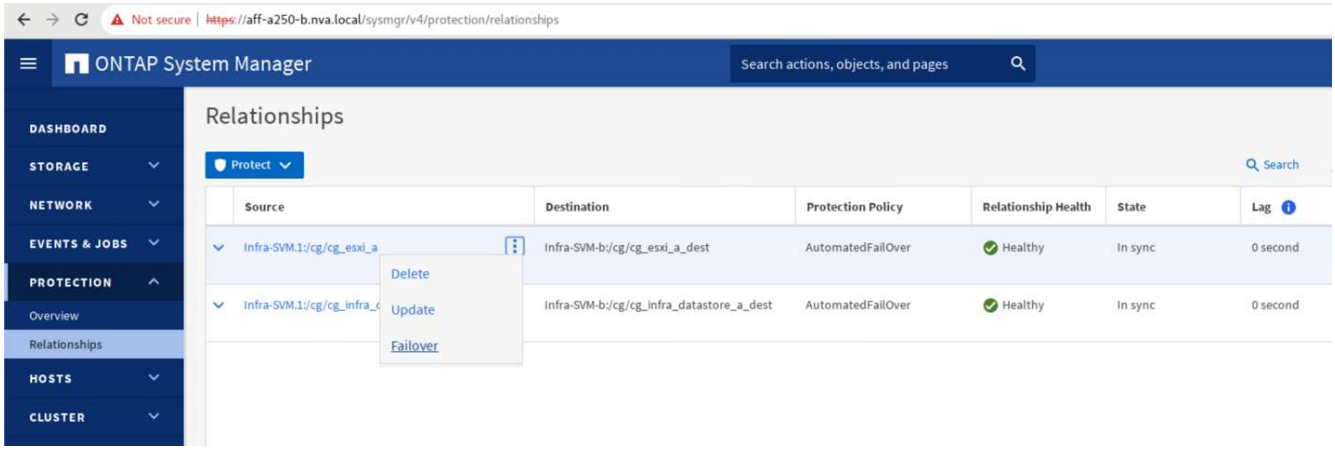
Se llevaron a cabo pruebas de vMotion de máquinas virtuales en un diferente host en el mismo sitio, así como en varios sitios, que se realizaron con éxito. Después de migrar manualmente una máquina virtual entre sitios, la regla de afinidad VM/Host activa y migra la máquina virtual de nuevo al grupo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

Recuperación tras fallos planificada de almacenamiento

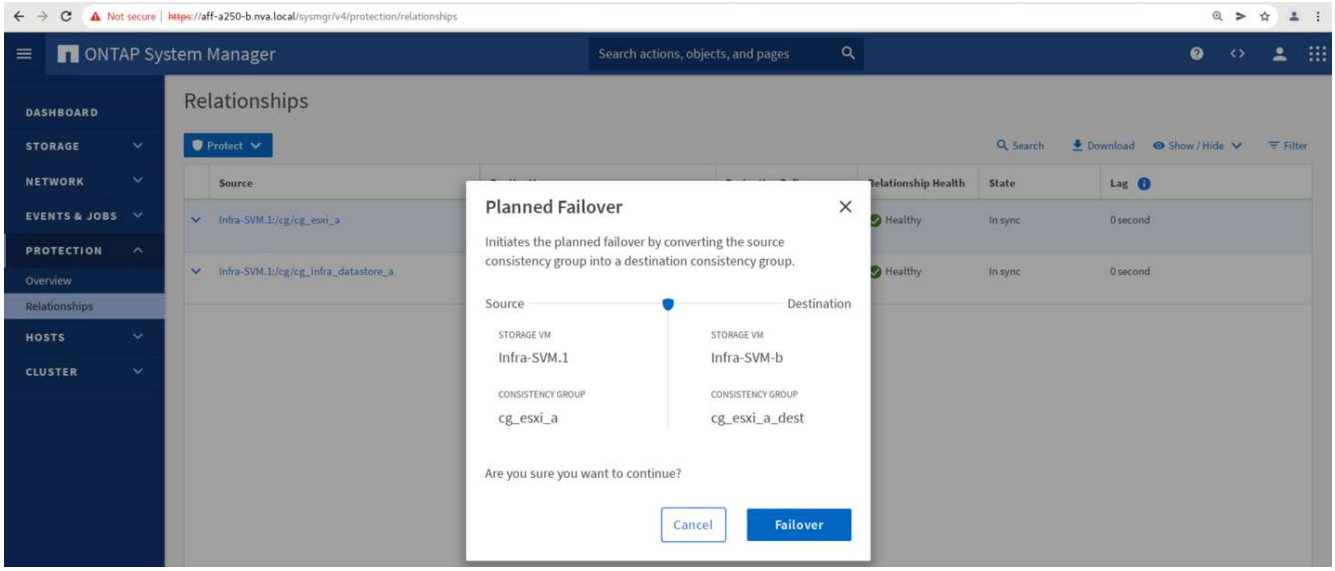
Las operaciones planificadas de conmutación por error del almacenamiento se deben realizar en la solución después de la configuración inicial para determinar si la solución funciona correctamente después de la conmutación por error del almacenamiento. Las pruebas pueden ayudar a identificar cualquier 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.

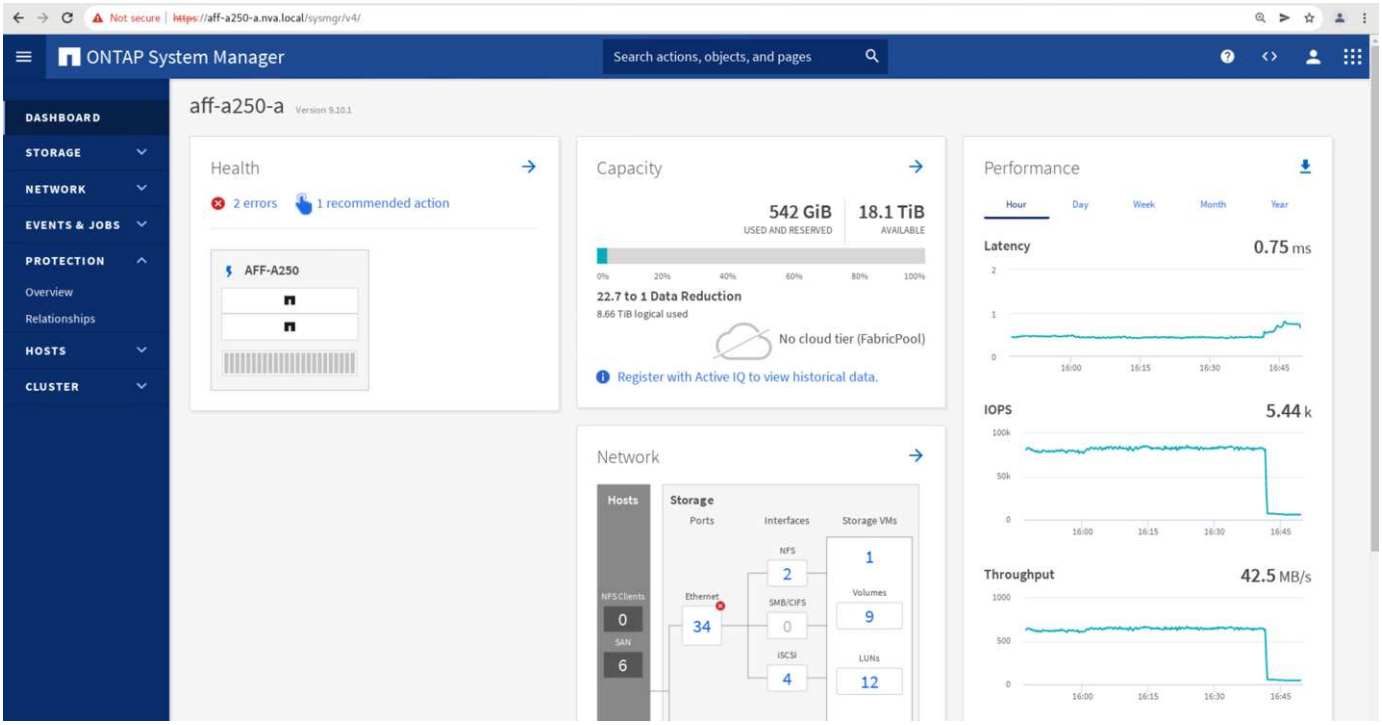
1. Vaya a la pantalla Protection > Relationships para confirmar que el estado de la relación del grupo de coherencia es `In Sync`. Si todavía está en el `Synchronizing` estado, espere a que el estado se convierta `In Sync` antes de realizar una conmutación al respaldo.
2. Expanda los puntos junto al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



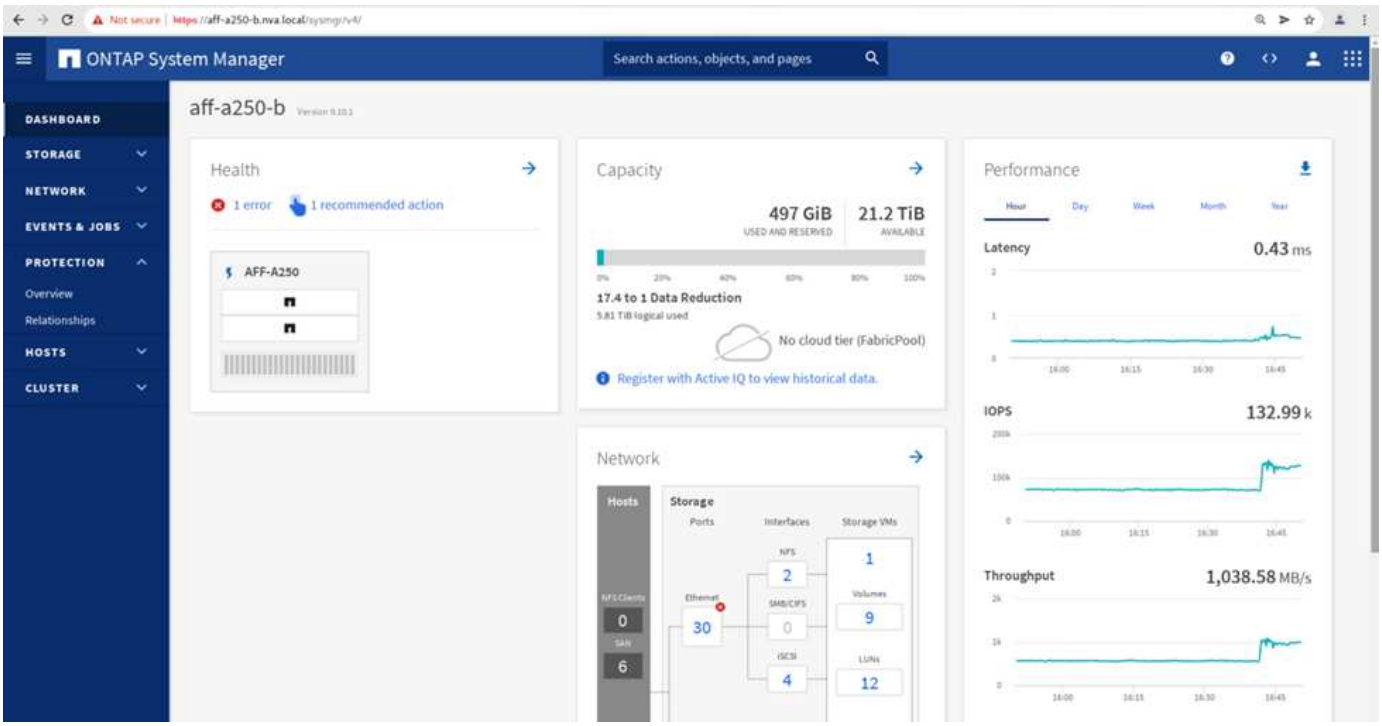
3. Confirme la conmutación por error para el inicio de la acción.



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.

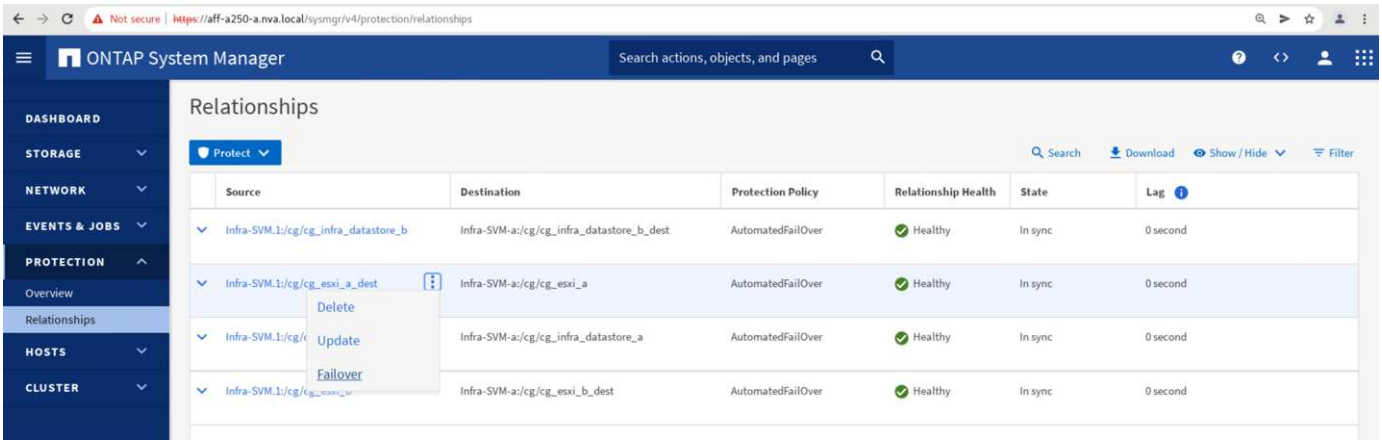


Por otro lado, el panel rendimiento de la consola del administrador del sistema del sitio B muestra un aumento significativo en IOPS, debido al servicio de I/o adicional trasladado desde la instalación A, a aproximadamente 130.000 IOPS, Y llegó a un rendimiento de aproximadamente 1 GB/s, a la vez que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



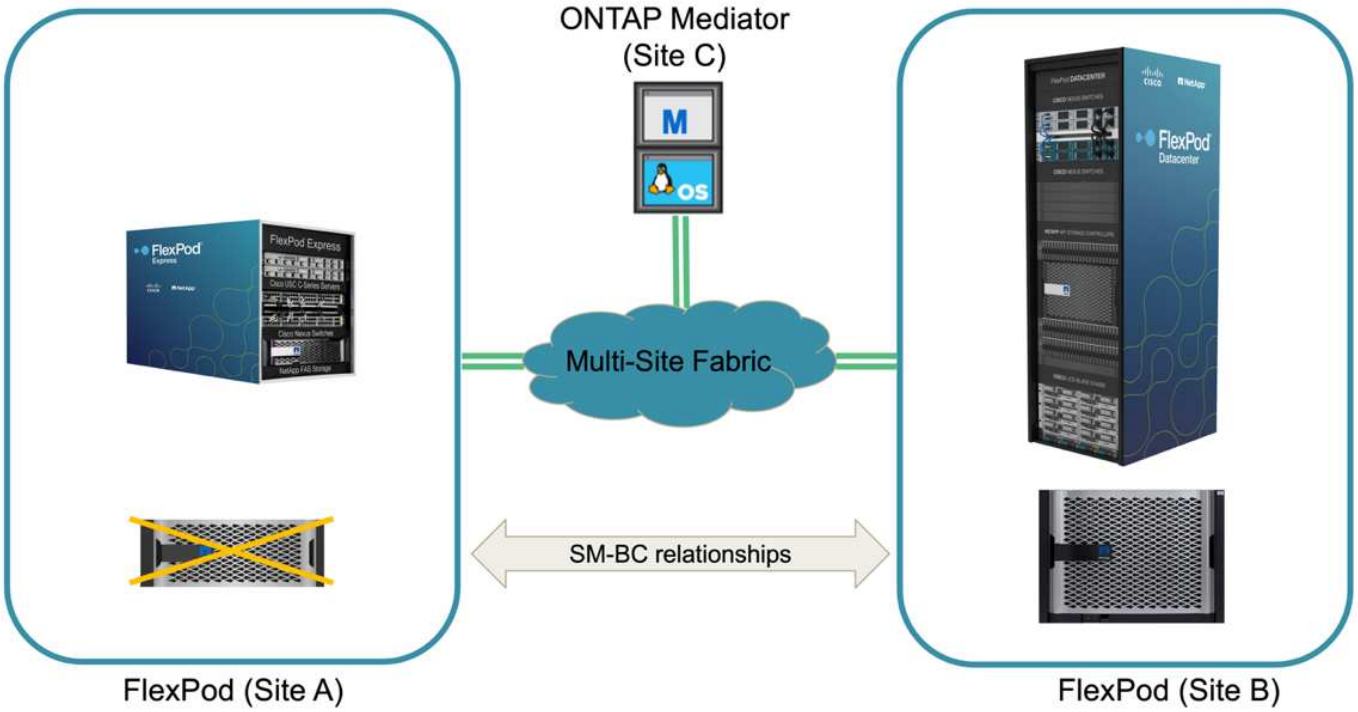
Con la migración transparente de las operaciones De I/o del sitio A al sitio B, ahora es posible desconectar las controladoras De almacenamiento para tareas de mantenimiento programadas. Una vez que se hayan completado el trabajo de mantenimiento o las pruebas y el sitio en el que se cree un clúster 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.



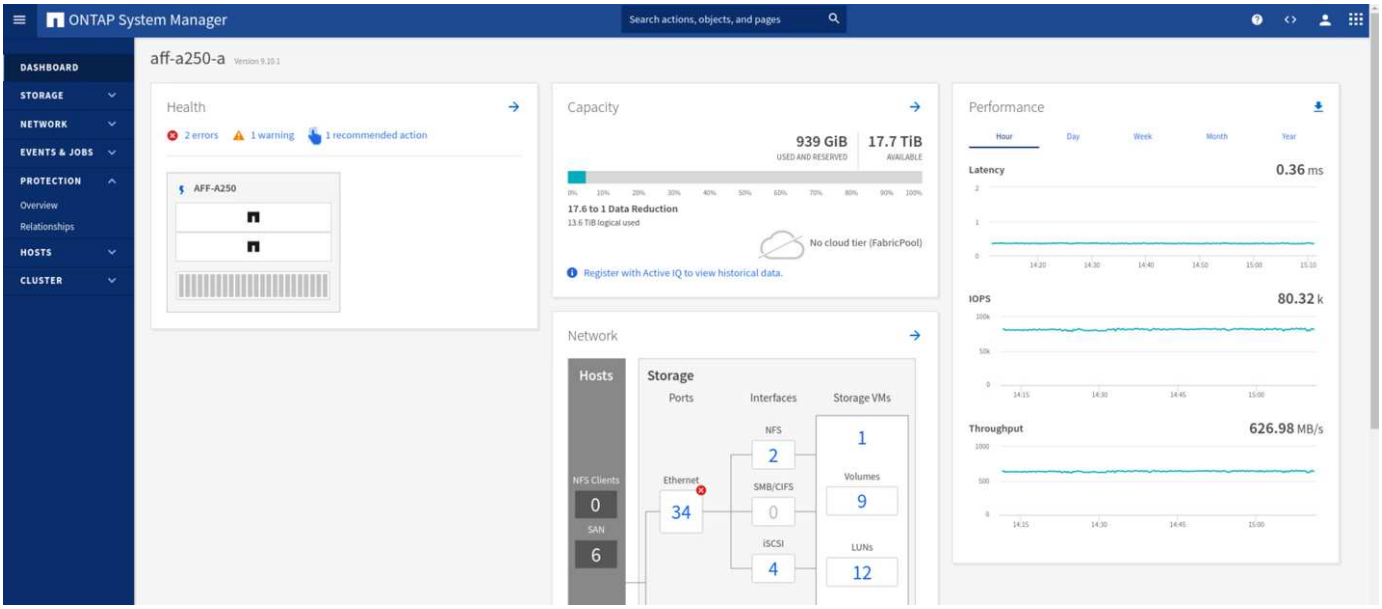
Para simular un desastre de almacenamiento en el centro A, ambas controladoras de almacenamiento en el sitio A pueden apagarse físicamente el switch de alimentación para interrumpir el suministro de alimentación de las controladoras, o mediante el uso del comando de administración de energía del sistema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

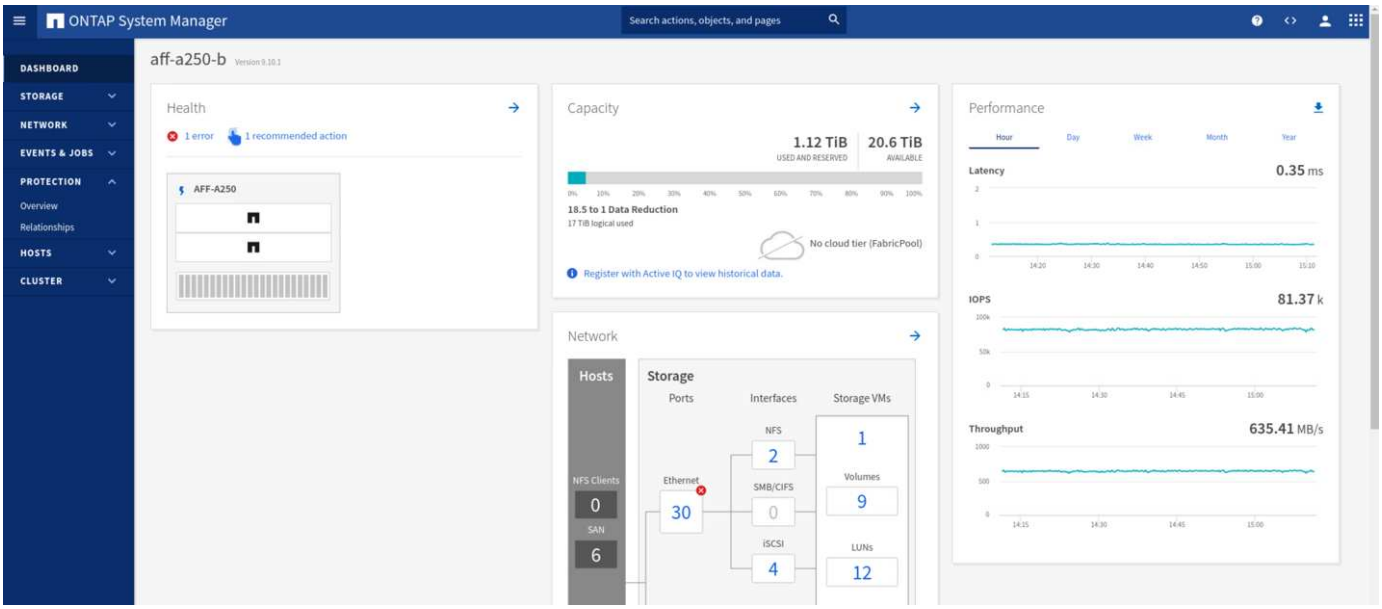
Cuando el clúster de almacenamiento del centro a pierde potencia, hay una parada repentina de los servicios de datos proporcionados por el sitio Un clúster de almacenamiento. Posteriormente, el Mediator de ONTAP, que supervisa la solución SM-BC desde un tercer sitio, detecta el sitio una condición De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

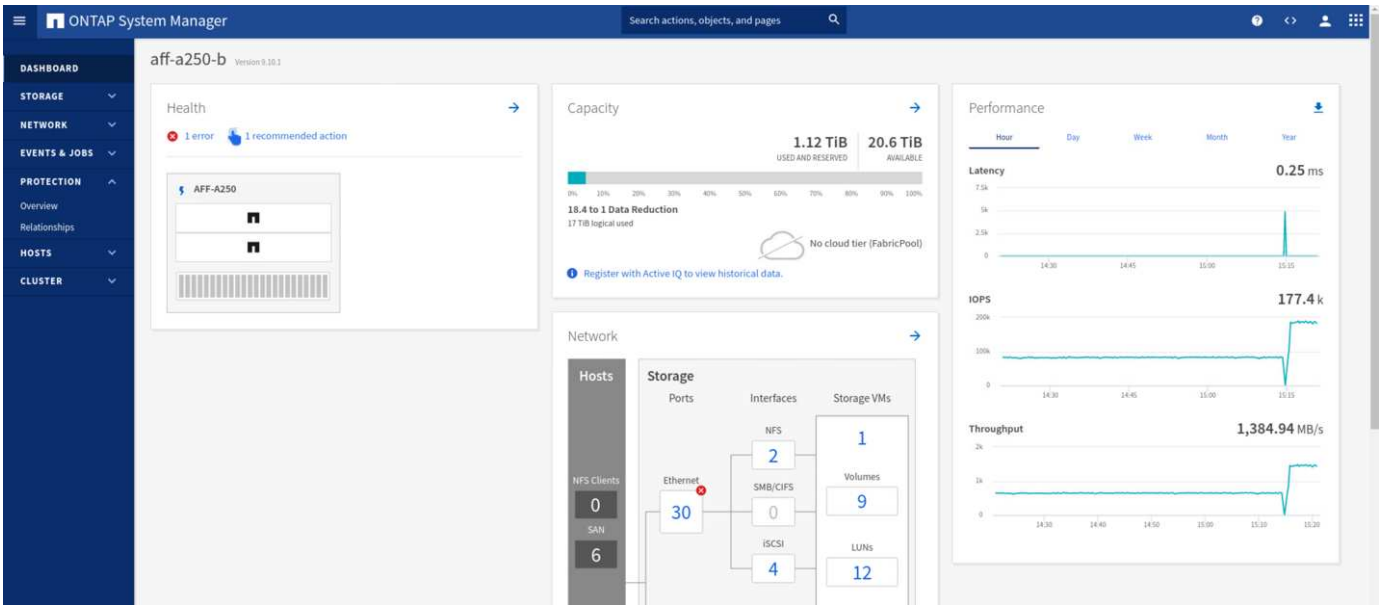
Durante las pruebas de validación, la herramienta de Iometer en los equipos virtuales de ambos sitios genera I/o en sus almacenes de datos locales. Una vez apagado El sitio a un clúster, las operaciones de I/o se pausaron brevemente y, a continuación, se reanudaron. Consulte las dos figuras siguientes 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.



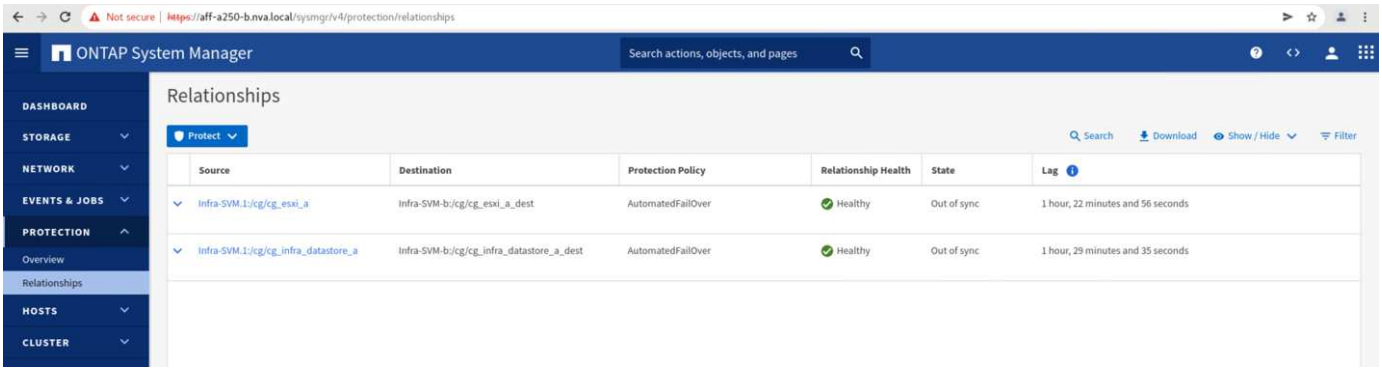


Tras apagar las controladoras de almacenamiento en el sitio A, podemos validar visualmente que las I/o de la controladora de almacenamiento del sitio B aumentaron enormemente para ofrecer servicios de datos adicionales en nombre del sitio A (consulte la siguiente figura). Además, la interfaz gráfica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

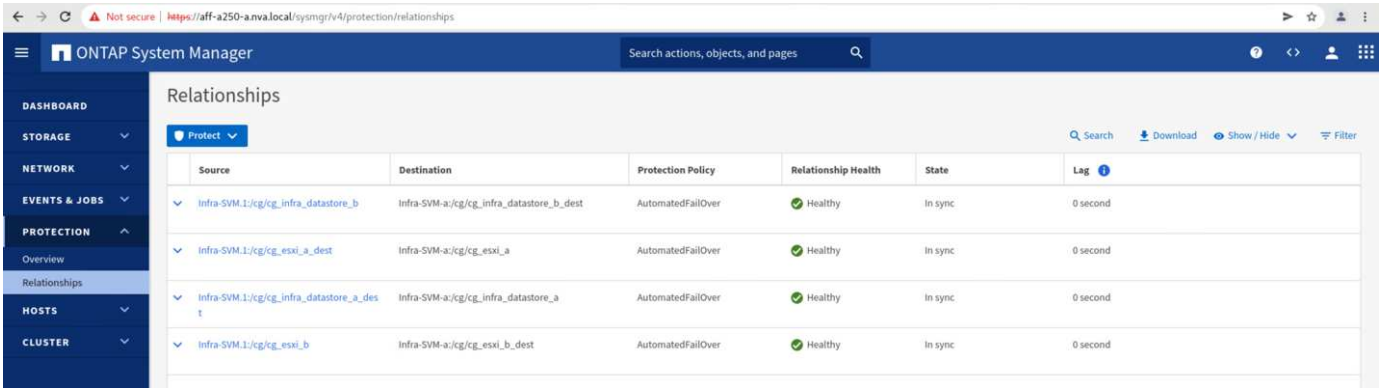
clúster De almacenamiento del sitio. Tenga en cuenta que si hay otros almacenes de datos respaldados por LUN no protegidos mediante relaciones SM-BC, dichos almacenes de datos ya no serán accesibles cuando se produzca un desastre de almacenamiento. Por lo tanto, es importante evaluar las necesidades 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.



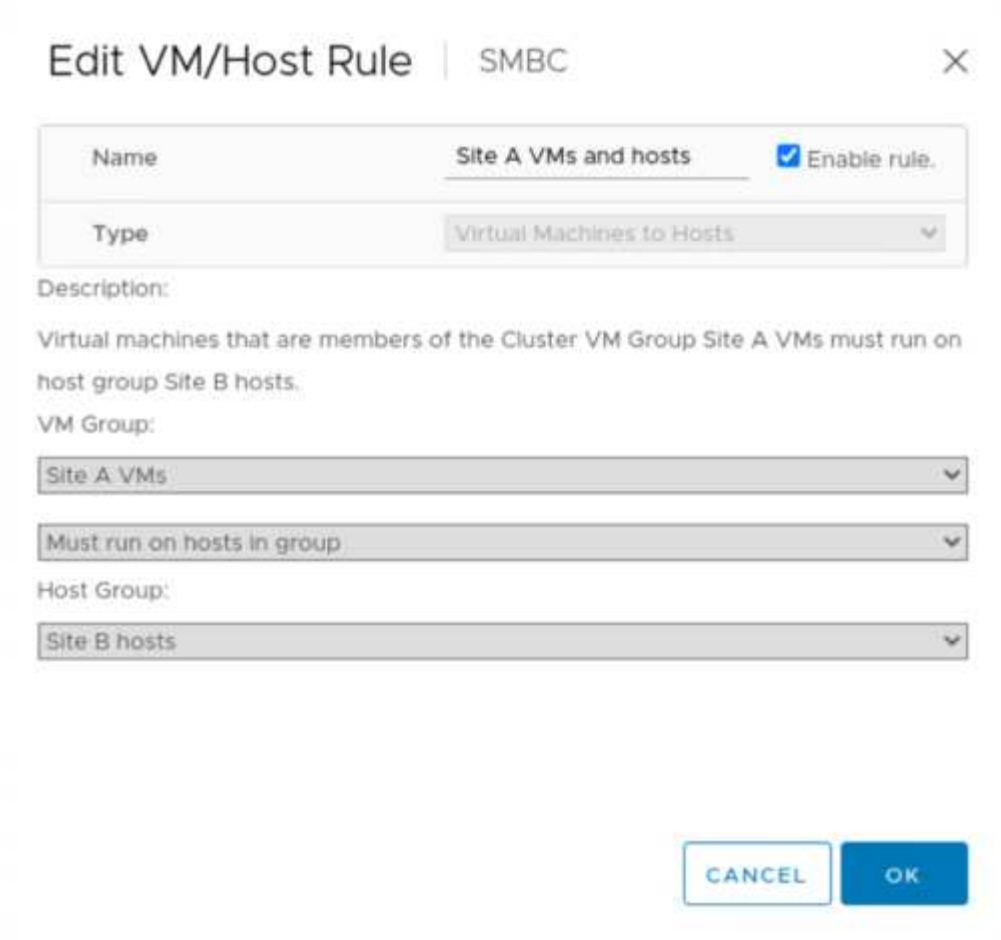
Mantenimiento de sitio completo o errores en el sitio

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.

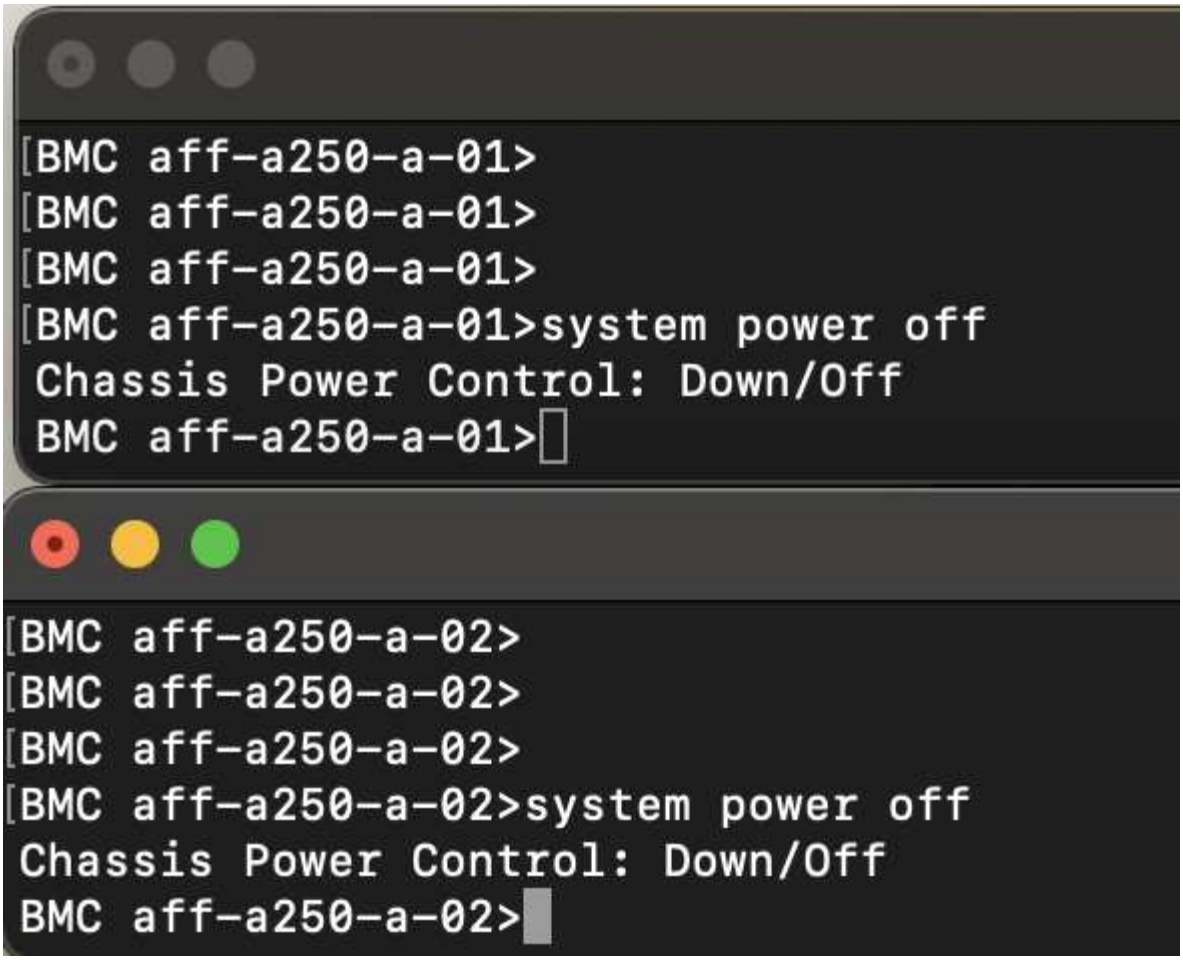
Antes de realizar la migración planificada, actualice la regla de afinidad de equipo virtual/host para que los equipos virtuales que se ejecutan actualmente en el sitio se migren automáticamente fuera del sitio que está experimentando mantenimiento. La siguiente captura de pantalla muestra un ejemplo 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.



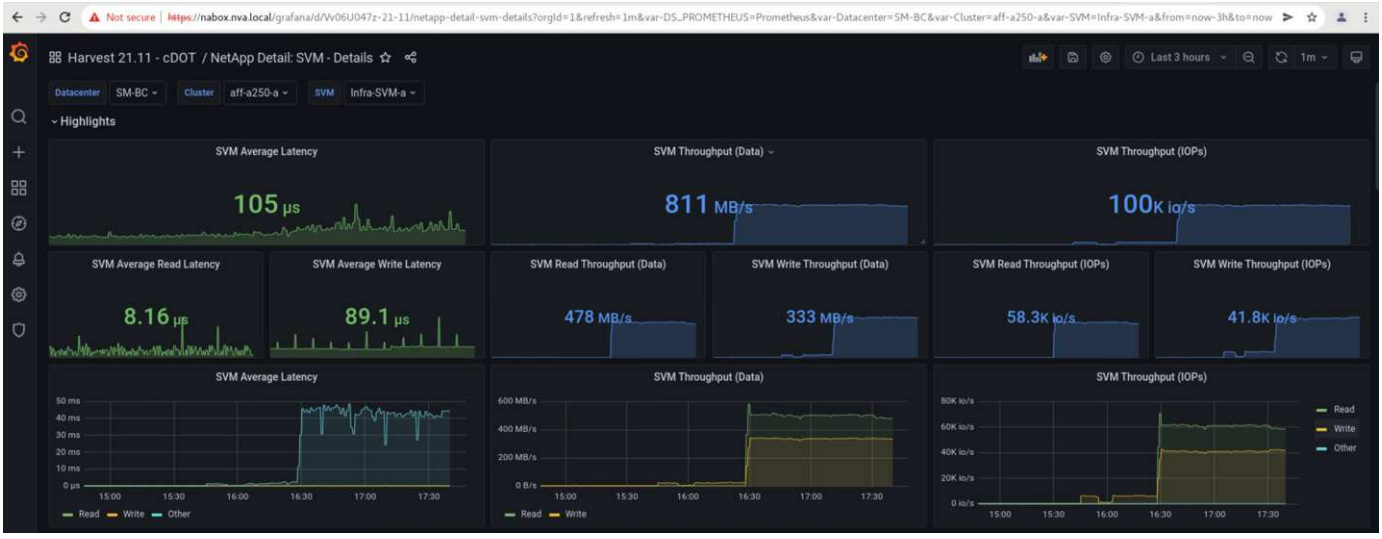
Después de migrar las máquinas virtuales y los servicios de almacenamiento, puede apagar los servidores, las controladoras de almacenamiento, las bandejas de discos y los switches, y realizar las actividades de mantenimiento del sitio que necesite. Cuando se completa el mantenimiento del sitio y se devuelve 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.



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.



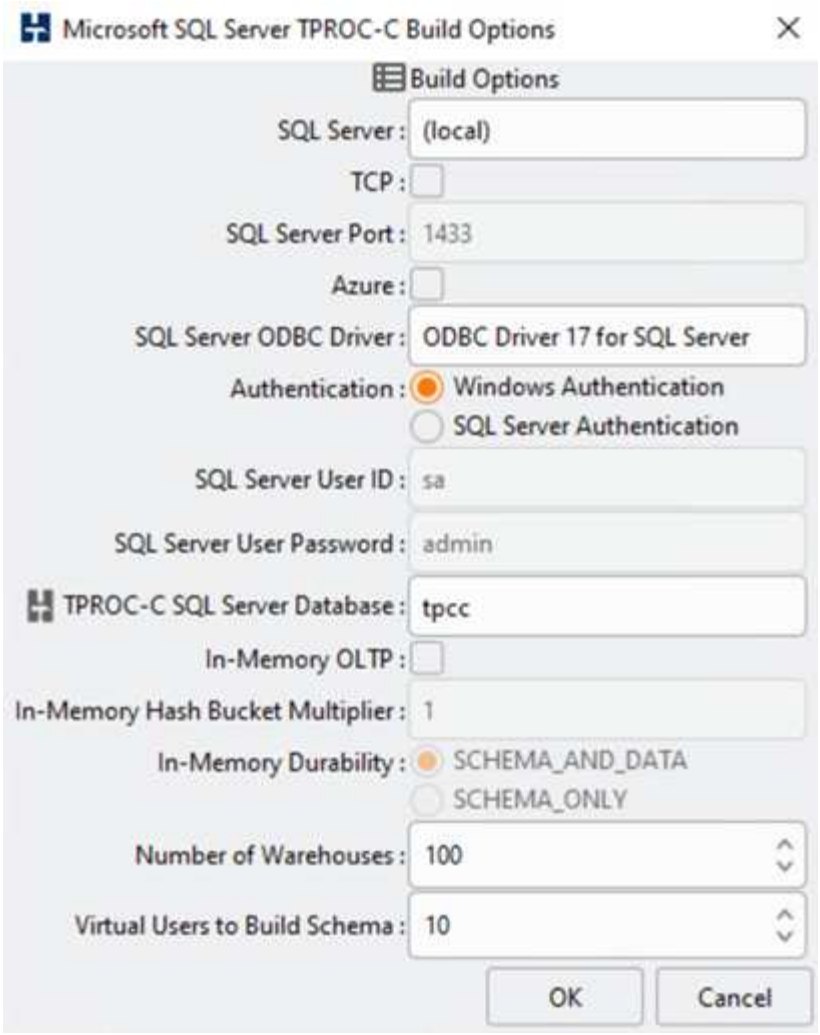


Microsoft SQL Server

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.

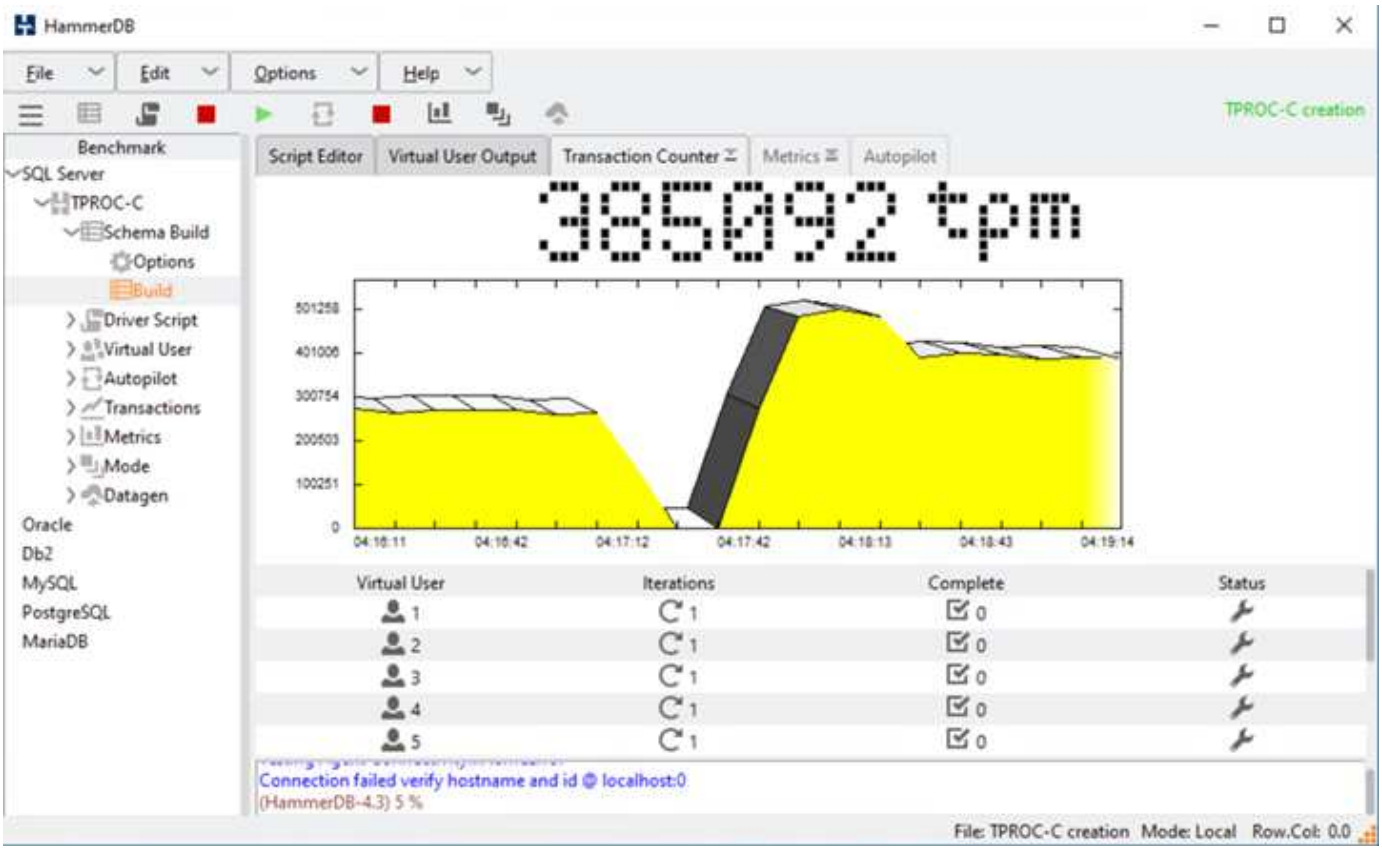
Como parte de la validación de carga de trabajo crítica para el negocio de la solución FlexPod SM-BC, se incluye Microsoft SQL Server 2019 instalado en un equipo virtual de Windows Server 2022 junto con los equipos virtuales de Iometer para pruebas de conmutación al nodo de respaldo del almacenamiento 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.

FlexPod Datacenter con VMware vSphere 7,0 y NetApp ONTAP 9,7: Puesta en marcha

John George, Cisco Sree Lakshmi Lanka, NetApp

Este documento describe FlexPod Datacenter de Cisco y NetApp con ONTAP 9,7 de NetApp en el sistema de almacenamiento all-flash AFF A400 de NetApp, el software unificado Cisco UCS Manager versión 4,1(2) con procesadores escalables Intel Xeon

Scalable de segunda generación y VMware vSphere 7,0. Cisco UCS Manager (UCSM) 4,1(2) proporciona un soporte consolidado para:

- Todos los modelos actuales de interconexión de estructura de Cisco UCS: 6200, 6300, 6324 (Cisco UCS Mini)
- 6400
- IOM de la serie 2200/2300/2400
- Cisco UCS serie B
- Cisco UCS C-Series

También se incluyen las plataformas de gestión de SaaS Cisco Intersight y NetApp Active IQ.

FlexPod Datacenter con NetApp ONTAP 9,7, el software unificado Cisco UCS versión 4,1 (2) y VMware vSphere 7,0 constan de una arquitectura de centro de datos prediseñada y con mejores prácticas integrada en Cisco Unified Computing System (Cisco UCS), la familia de switches Cisco Nexus 9000, switches estructurales MDS 9000 multicapa, Y las cabinas de almacenamiento AFF A-Series de NetApp que ejecutan el software de gestión de datos ONTAP 9,7.

"FlexPod Datacenter con VMware vSphere 7,0 y NetApp ONTAP 9,7: Puesta en marcha"

FlexPod Datacenter con Cisco Intersight y NetApp ONTAP 9,7: Diseño

John George, Cisco Scott Kovacs, NetApp

Este documento describe la solución FlexPod de Cisco y NetApp, la cual es un enfoque validado para poner en marcha tecnologías de Cisco y NetApp como infraestructura de cloud compartida. Este diseño validado proporciona un marco para poner en marcha VMware vSphere, la plataforma de virtualización más popular en centros de datos de clase empresarial en FlexPod.

"FlexPod Datacenter con Cisco Intersight y NetApp ONTAP 9,7: Diseño"

FlexPod Datacenter con Cisco Intersight y NetApp ONTAP 9,7: Puesta en marcha

John George, Cisco Scott Kovacs, NetApp

La tendencia actual del sector en el diseño de los centros de datos reside en las infraestructuras compartidas. Al utilizar la virtualización junto con las plataformas de TI prevalidadas, los clientes empresariales se han embarcado en la transición al cloud abandonando los silos de aplicaciones y dirigiéndose a una infraestructura compartida que se puede poner en marcha rápidamente, lo que aumenta la agilidad y reduce los costes. Cisco y NetApp se han asociado para ofrecer FlexPod, que utiliza los mejores componentes de almacenamiento, servidor y red de su clase para servir de base para una gran variedad de cargas de trabajo, lo que permite diseñar arquitecturas eficientes que se pueden poner en marcha de forma rápida y segura.

"FlexPod Datacenter con Cisco Intersight y NetApp ONTAP 9,7: Puesta en marcha"

FlexPod Datacenter con Cisco Intersight y NetApp ONTAP 9,7: Diseño

John George, Cisco Scott Kovacs, NetApp

Este documento describe una solución validada para poner en marcha tecnologías de Cisco y NetApp como una infraestructura de cloud compartida. Este diseño validado proporciona un marco para poner en marcha VMware vSphere, la plataforma de virtualización más popular en centros de datos de clase empresarial en FlexPod.

FlexPod es una infraestructura integrada líder que admite una amplia gama de cargas de trabajo empresariales y casos prácticos. Esta solución permite a los clientes poner en marcha de forma rápida y fiable un cloud privado basado en vSphere de VMware en una infraestructura integrada.

"FlexPod Datacenter con Cisco Intersight y NetApp ONTAP 9,7: Diseño"

FlexPod Datacenter con VMware vSphere 6,7 U2, Cisco UCS fouth-generation Fabric y NetApp ONTAP 9,6

John George, Cisco Sree Lakshmi Lanka, NetApp

Este documento describe Cisco y NetApp FlexPod Datacenter con NetApp ONTAP 9,6, el software unificado Cisco UCS Manager versión 4,0(4) con procesadores escalables Intel Xeon de segunda generación y VMware vSphere 6,7 U2. Cisco UCS Manager (UCSM) 4,0(4) proporciona un soporte consolidado para:

- Todos los modelos actuales de interconexión de estructura de Cisco UCS: 6200, 6300, 6324 (Cisco UCS Mini)
- 6454
- IOM de la serie 2200/2300/2400
- Cisco UCS serie B
- Cisco UCS C-Series.

FlexPod Datacenter con NetApp ONTAP 9,6, el software unificado Cisco UCS versión 4,0 (4), y VMware vSphere 6,7 U2 es una arquitectura de centro de datos prediseñada y mejor práctica integrada en el sistema Cisco Unified Computing System (Cisco UCS), la familia de switches Cisco Nexus 9000, switches estructurales multicapa MDS 9000, Y las cabinas de almacenamiento AFF A-Series de NetApp que ejecutan ONTAP 9.

"FlexPod Datacenter con VMware vSphere 6,7 U2, Cisco UCS de cuarta generación Fabric y NetApp ONTAP 9,6"

FlexPod Datacenter con VMware vSphere 6,7 U1, la estructura de cuarta generación de Cisco UCS y AFF A-Series de NetApp: Diseño

John George, Cisco Sree Lakshmi Lanka, NetApp

Este documento describe la solución FlexPod de Cisco y NetApp, la cual es un enfoque validado para poner en marcha tecnologías de Cisco y NetApp como infraestructura de cloud compartida. Este diseño validado proporciona un marco para poner en marcha VMware vSphere, la plataforma de virtualización más popular en centros de datos de clase empresarial en FlexPod.

FlexPod es una infraestructura integrada líder que admite una amplia gama de cargas de trabajo empresariales y casos prácticos. Esta solución permite a los clientes poner en marcha de forma rápida y fiable cloud privado basado en VMware vSphere en una infraestructura integrada.

La arquitectura de la solución recomendada se basa en Cisco Unified Computing System (Cisco UCS) mediante el lanzamiento de software unificado para admitir las plataformas de hardware de Cisco UCS, incluidos servidores de rack Cisco UCS B-Series y C-Series, interconexiones de estructura Cisco UCS 6454, switches Cisco Nexus 9000 Series, switches Fibre Channel de Cisco MDS, Y cabinas de almacenamiento All Flash Series de NetApp. Además, incluye VMware vSphere 6,7 Update 1, que proporciona una serie de nuevas funciones para optimizar la utilización del almacenamiento y facilitar una nube privada.

"FlexPod Datacenter con VMware vSphere 6,7 U1, la estructura de cuarta generación de Cisco UCS y AFF A-Series de NetApp: Diseño"

FlexPod Datacenter con VMware vSphere 6,7 U1, la estructura de cuarta generación de Cisco UCS y AFF A-Series de NetApp

John George, Cisco Scott Kovacs, NetApp

Este documento describe Cisco y NetApp FlexPod Datacenter con el software unificado Cisco UCS Manager, versión 4,0 (2) y VMware vSphere 6,7 U1. Cisco UCS Manager (UCSM) 4,0(2) proporciona soporte consolidado de todos los modelos actuales de interconexión de estructura de Cisco UCS (6200, 6300, 6324 (Cisco UCS Mini)), IOM de la serie 6454,2200/2300, Cisco UCS B-Series y Cisco UCS C-Series. FlexPod Datacenter con Cisco UCS Unified Software release 4,0(2) y VMware vSphere 6,7 U1 es una arquitectura de centro de datos prediseñada con las mejores prácticas basada en Cisco Unified Computing System (UCS), la familia de switches Cisco Nexus 9000, switches estructurales MDS 9000 multicapa, Asimismo, las cabinas de almacenamiento AFF A-Series de NetApp que ejecutan el sistema operativo de almacenamiento 9 de ONTAP.

"FlexPod Datacenter con VMware vSphere 6,7 U1, la estructura de cuarta generación de Cisco UCS y AFF A-Series de NetApp"

FlexPod Datacenter con Cisco ACI Multi-Pod, MetroCluster IP de NetApp y VMware vSphere 6,7: Diseño

Haseeb Niazi, Cisco Arvind Ramakrishnan, NetApp

Este documento describe la integración de las soluciones multipod de Cisco ACI y MetroCluster IP de NetApp en el centro de datos de FlexPod para ofrecer una solución de centro de datos múltiple de alta disponibilidad. La arquitectura de centro de datos múltiple ofrece la capacidad de equilibrar cargas de trabajo entre dos centros de datos que utilizan la movilidad de cargas de trabajo sin interrupciones, lo que permite la migración de servicios entre sitios sin necesidad de sostener un corte.

La solución de FlexPod con ACI Multi-Pod y MetroCluster IP de NetApp ofrece los siguientes beneficios:

- Movilidad de carga de trabajo fluida entre centros de datos
- Políticas coherentes en todos los sitios
- Extensión de capa 2 en centros de datos geográficamente dispersos
- Prevención mejorada de los tiempos de inactividad durante el mantenimiento
- Prevención y recuperación ante desastres

"FlexPod Datacenter con Cisco ACI Multi-Pod, MetroCluster IP de NetApp y VMware vSphere 6,7: Diseño"

FlexPod Datacenter con Cisco ACI Multi-Pod con NetApp MetroCluster IP y VMware vSphere 6,7: Puesta en marcha

Haseeb Niazi, Cisco Ramesh Issac y Cisco Arvind Ramakrishnan y NetApp

Cisco y NetApp se han asociado para ofrecer una serie de soluciones FlexPod que permiten crear plataformas estratégicas de centros de datos. La solución FlexPod proporciona una arquitectura integrada que incorpora prácticas de diseño recomendadas para informática, almacenamiento y redes, lo que minimiza los riesgos TECNOLÓGICOS gracias a la validación de la arquitectura integrada para garantizar la compatibilidad entre varios componentes. La solución también soluciona los problemas DE TI al proporcionar indicaciones de diseño documentadas, directrices para la puesta en marcha y soporte que se puede utilizar en varias etapas (planificación, diseño e implementación) de una implementación.

"FlexPod Datacenter con Cisco ACI Multi-Pod con NetApp MetroCluster IP y VMware vSphere 6,7: Puesta en marcha"

Cloud híbrido

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.

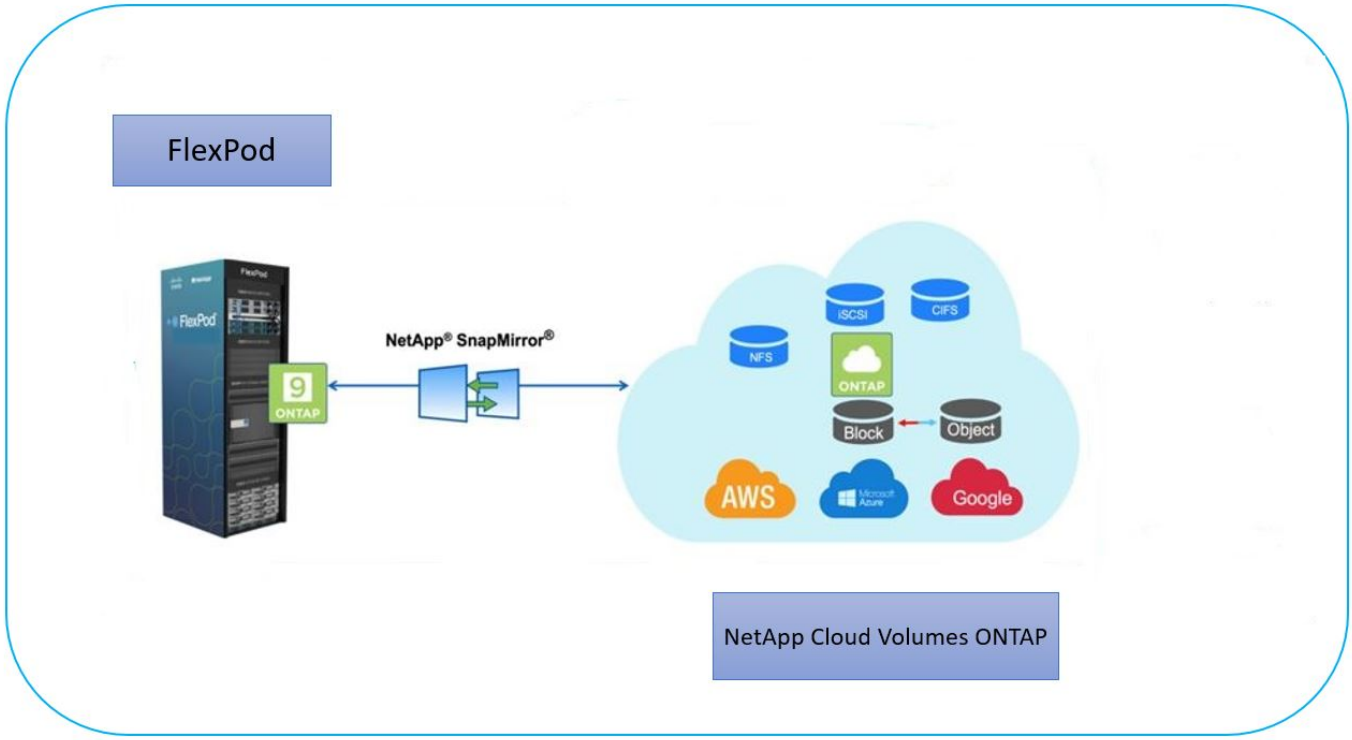
El tamaño cada vez mayor de los datos sanitarios y la valiosa información que estos datos pueden proporcionar hacen que los servicios de datos sanitarios y la protección de datos sean tan cruciales como difíciles. En primer lugar, los datos sanitarios deben estar disponibles y protegidos para cumplir 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:

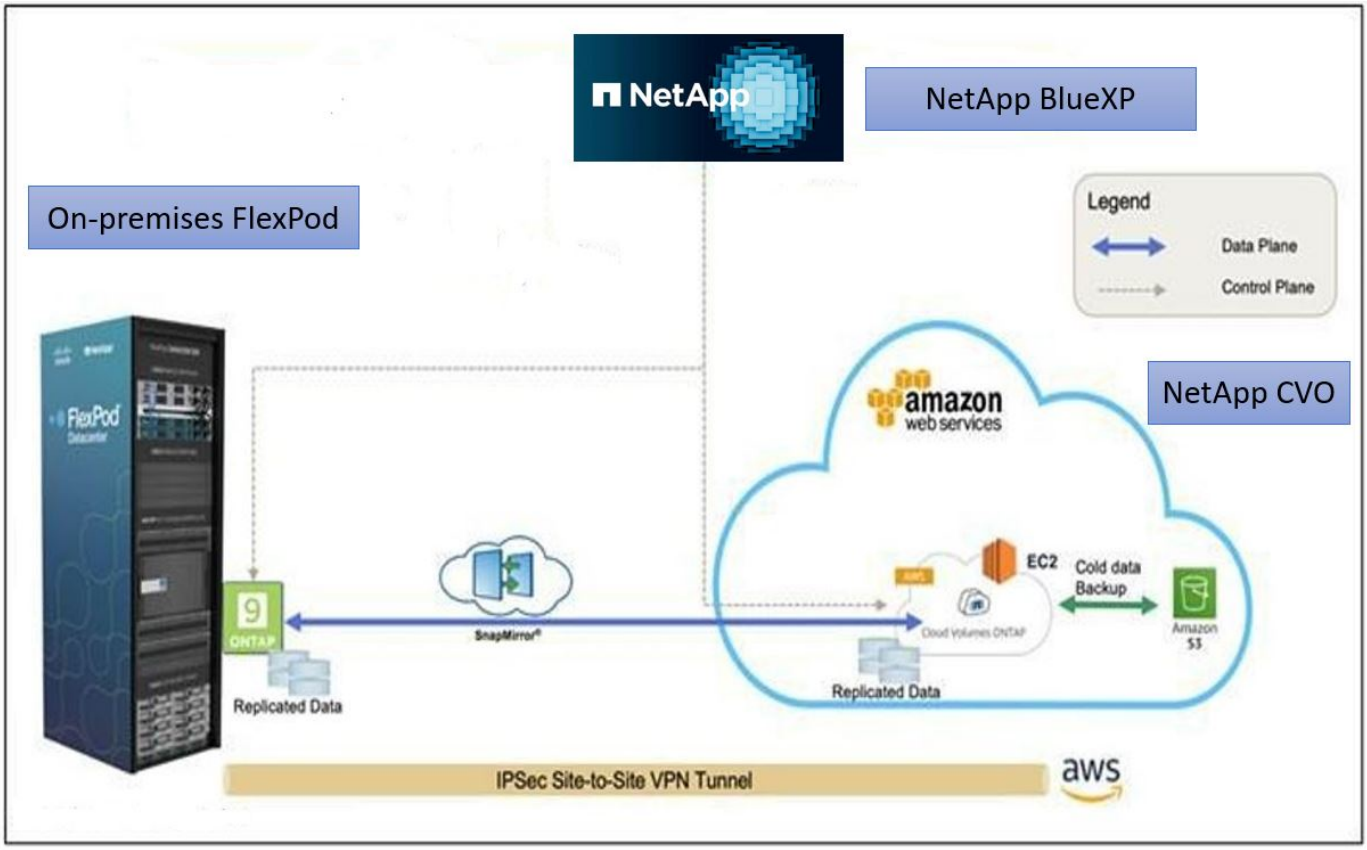
- **Protección personalizada.** Cloud Volumes ONTAP proporciona replicación de datos a nivel de bloque de ONTAP a la nube que mantiene el destino actualizado mediante actualizaciones incrementales. Los usuarios pueden especificar una programación de sincronización para determinar cuándo se transfieren 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 de ransomware de Ransomware.** la protección contra ransomware BlueXP de NetApp analiza orígenes de datos en entornos locales y de cloud, detecta vulnerabilidades de seguridad y proporciona su estado de seguridad actual y su puntuación de riesgos. A continuación, proporciona recomendaciones prácticas que puede investigar más a fondo y seguir para subsanarlas. De esta forma podrá proteger sus datos sanitarios cruciales de ataques de ransomware.

Topología de la solución

En esta sección se describe la topología lógica de la solución. En la siguiente figura se muestra la topología de la solución compuesta por el entorno local de FlexPod, Cloud Volumes ONTAP de NetApp (CVO) ejecutado en Amazon Web Services (AWS) y la plataforma SaaS BlueXP de NetApp.



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 está validado en EHR y es compatible con una plataforma que contiene Cisco UCS con los procesadores Intel Xeon, Red Hat Enterprise Linux (RHEL) y virtualización con VMware ESXi. Esta plataforma, junto con el alto nivel de comodidad de EHR en el almacenamiento de NetApp que se ejecuta en ONTAP, ofrece a los clientes la confianza de que pueden ejecutar sus aplicaciones sanitarias en un cloud privado totalmente gestionado a través de FlexPod, que también se puede conectar a cualquiera de los proveedores de cloud público.

BlueXP de NetApp

BlueXP (anteriormente Cloud Manager de NetApp) es una plataforma de gestión basada en SaaS para empresas que permite a expertos EN TECNOLOGÍA y arquitectos de cloud gestionar de forma centralizada su

infraestructura multicloud híbrida con las soluciones cloud de NetApp. Proporciona un sistema centralizado para ver y gestionar su almacenamiento en las instalaciones y en cloud, que admite cabinas y cuentas de varios proveedores de cloud híbridos. Para obtener más información, consulte "BlueXP".

Conector

Una instancia de conector permite a BlueXP gestionar recursos y procesos dentro de un entorno de nube pública. El conector es necesario para muchas de las características proporcionadas por BlueXP y puede ponerse en marcha en la nube o en la red local.

El conector se admite en las siguientes ubicaciones:

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

Para obtener más información acerca de Connector, consulte "Página de conectores".

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 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.

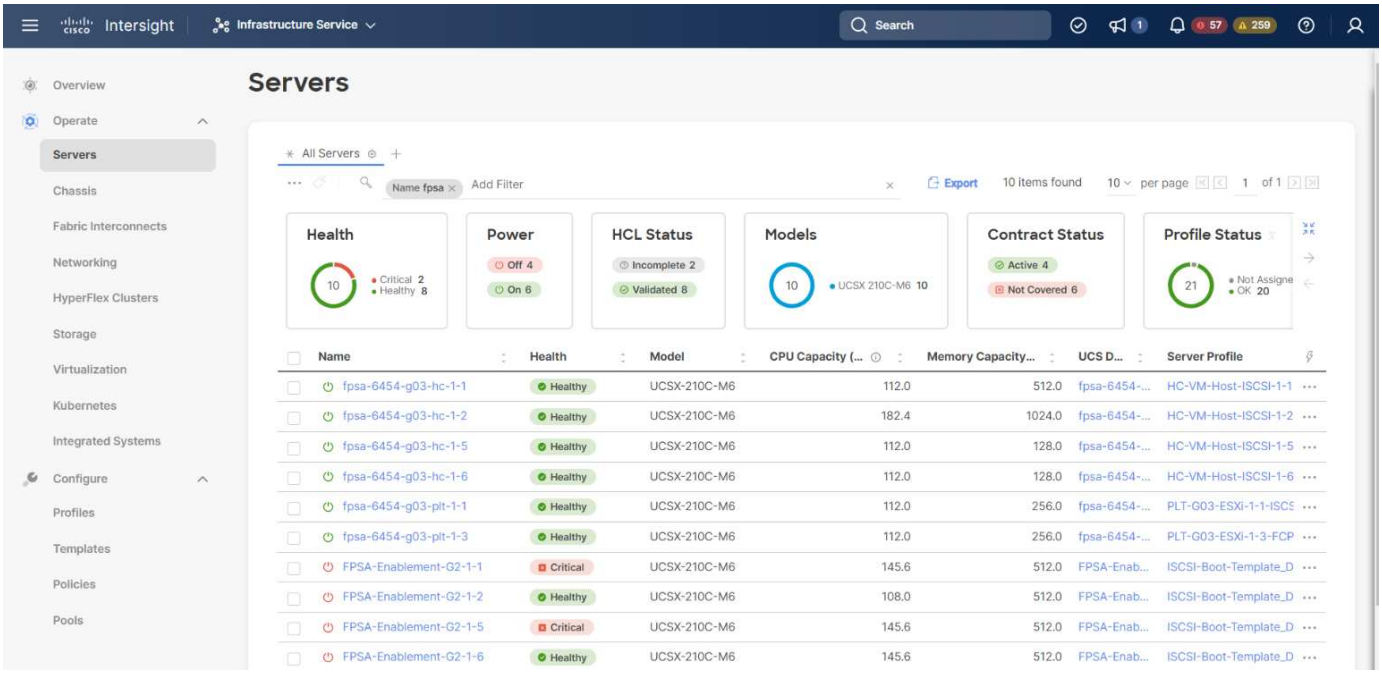
Para obtener más información, consulte "Active IQ Unified Manager".

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 cloud híbrido se puede ampliar a cualquier entorno FlexPod que ejecute versiones compatibles de software, firmware y hardware tal y como se haya definido en "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 BlueXP y Cloud Volumes ONTAP de NetApp.

Proveedor	Producto	Versión
NetApp	BlueXP	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 NetApp BlueXP.

   Para acceder a BlueXP de NetApp y otros servicios cloud, debe registrarse en "BlueXP de NetApp". Para configurar áreas de trabajo y usuarios en la cuenta de BlueXP, haga clic en "aquí". Necesita una cuenta que tenga permiso para implementar el conector en su proveedor de nube directamente desde BlueXP. Puede descargar la política de BlueXP desde "aquí".

4. Despliegue el conector.

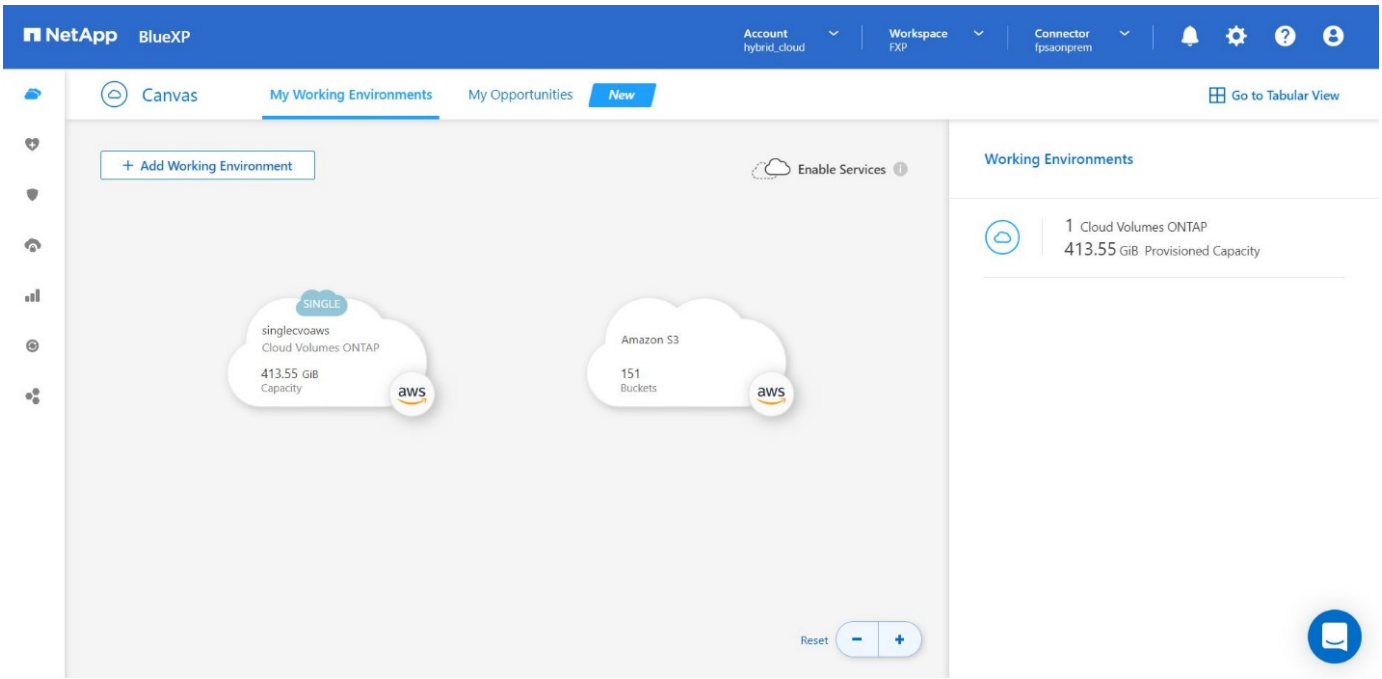
   Antes de añadir un entorno de trabajo de Cloud Volume ONTAP, debe poner en marcha Connector. BlueXP le pregunta si intenta crear su primer entorno de trabajo de Cloud Volumes ONTAP sin conector en su lugar. Para implementar Connector en AWS desde BlueXP, consulte este tema "enlace".

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 puesto en marcha un sistema Cloud Volumes ONTAP de un solo nodo en AWS. En la siguiente figura se muestra la consola BlueXP de NetApp con instancia CVO de un único nodo.



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`.

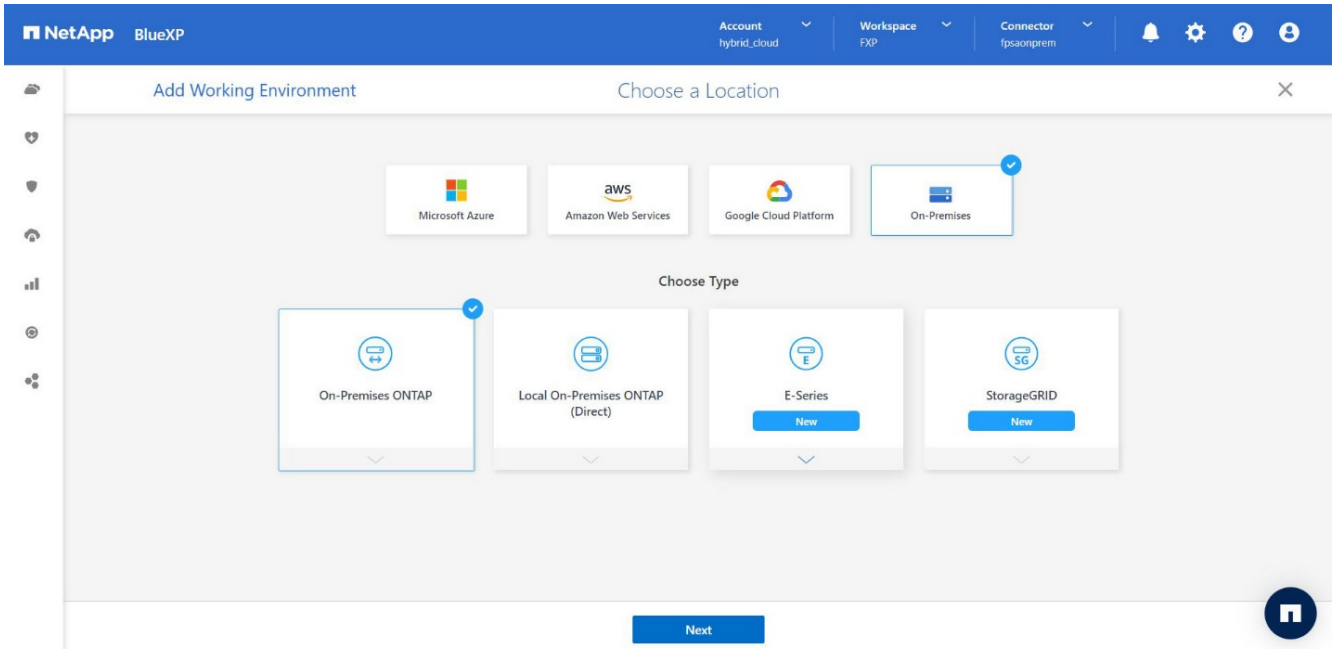
6. Asigne la LUN al igroup.

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

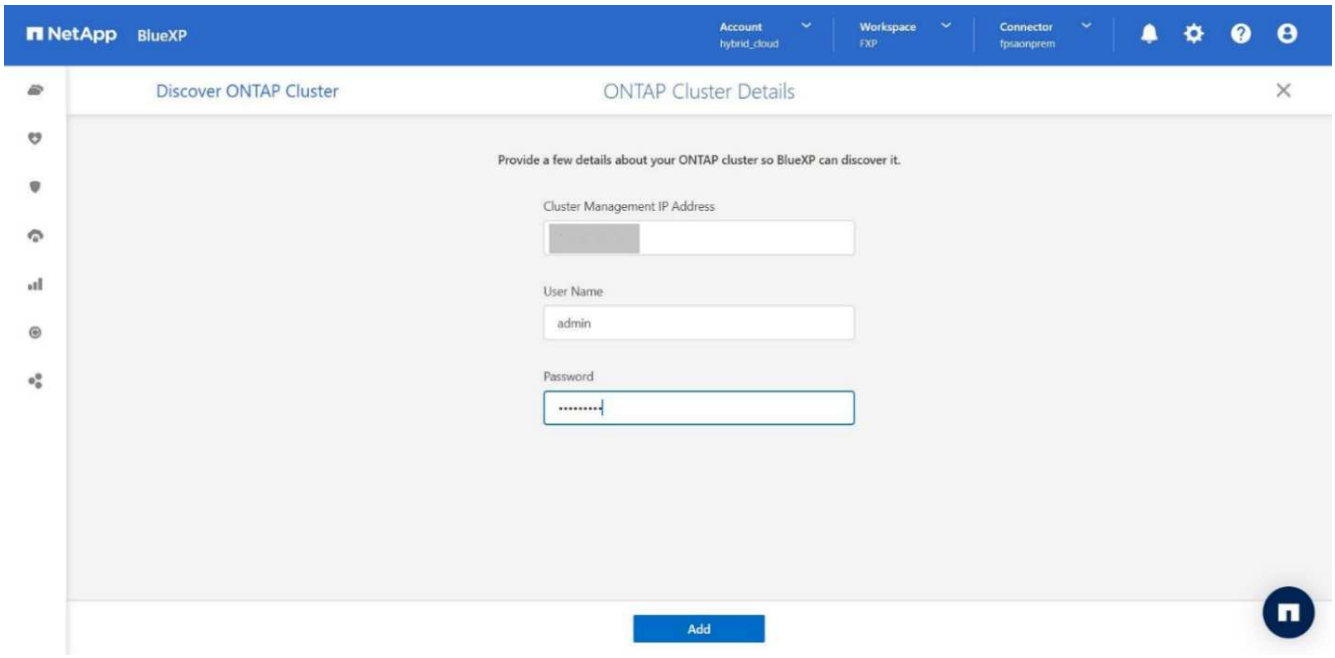
Adición del almacenamiento FlexPod en las instalaciones a BlueXP

Complete los siguientes pasos para añadir su almacenamiento de FlexPod al entorno de trabajo con NetApp BlueXP.

1. En el menú de navegación, selecciona **almacenamiento** > **lienzo**.
2. En la página Canvas, haga clic en **Agregar entorno de trabajo** y seleccione **en las instalaciones**.
3. Seleccione **On-local ONTAP**. Haga clic en **Siguiente**.

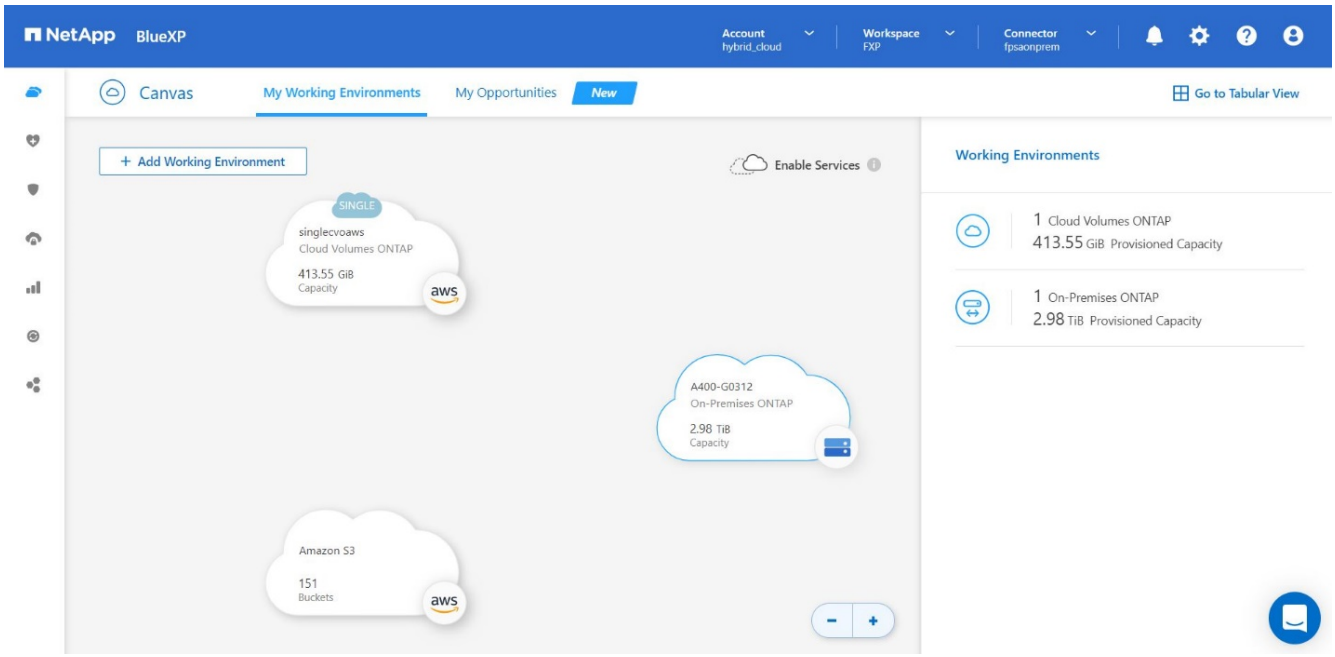


4. En la página ONTAP Cluster Details, introduzca la dirección IP de administración del clúster y la contraseña de la cuenta de usuario de administrador. A continuación, haga clic en **Agregar**.



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**.

   BlueXP descubre el clúster ONTAP y lo añade como un entorno de trabajo en el lienzo.



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 `pvcreate` 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 ~]# pvcreate /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 de secuencias de comandos perl para el simulador de E/S de EHR (GenerateIO). Los datos dentro de las LUN se generan con el EHR `Dgen.pl` guión. El script está diseñado para crear datos similares a los que se encontrarían en 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
```

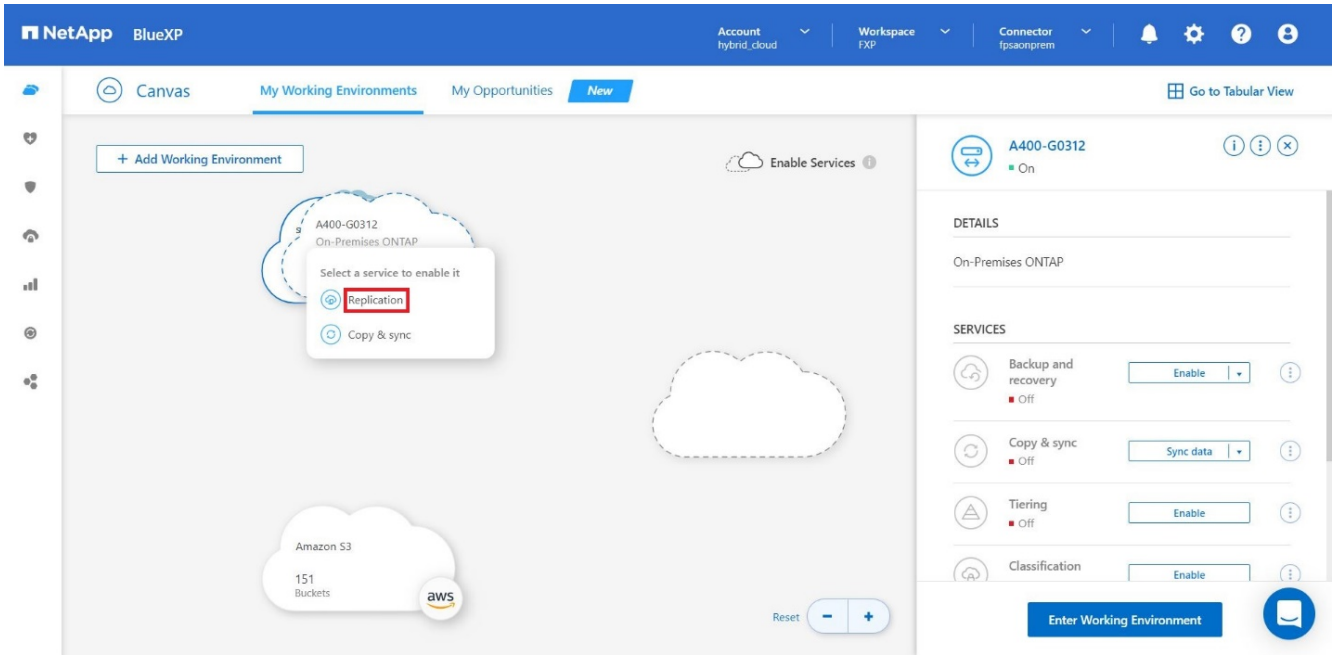
Mientras se ejecuta, la `Dgen.pl` script utiliza el 85% del sistema de archivos para la generación de datos de forma predeterminada.

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.

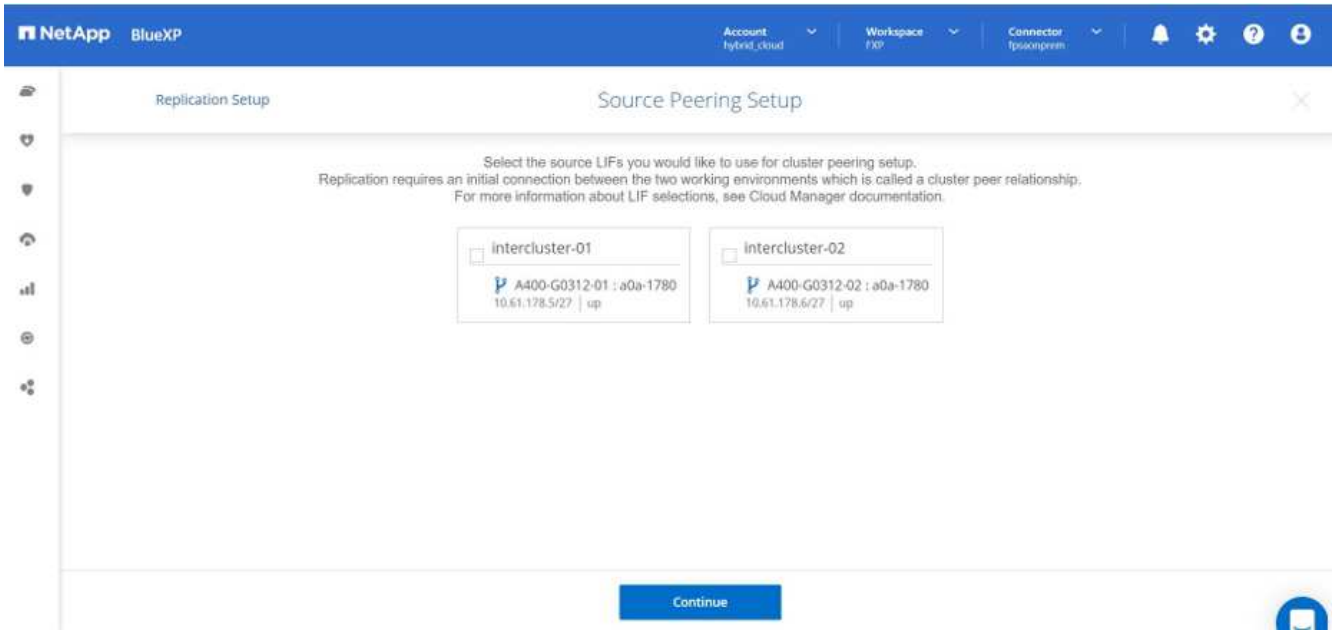
Complete los pasos siguientes para configurar la replicación de SnapMirror entre su sistema ONTAP local y CVO.

1. En el menú de navegación, selecciona **almacenamiento** > **lienzo**.
2. En Canvas, seleccione el entorno de trabajo que contiene el volumen de origen, arrástrelo al entorno de trabajo al que desea replicar el volumen y, a continuación, seleccione **replicación**.

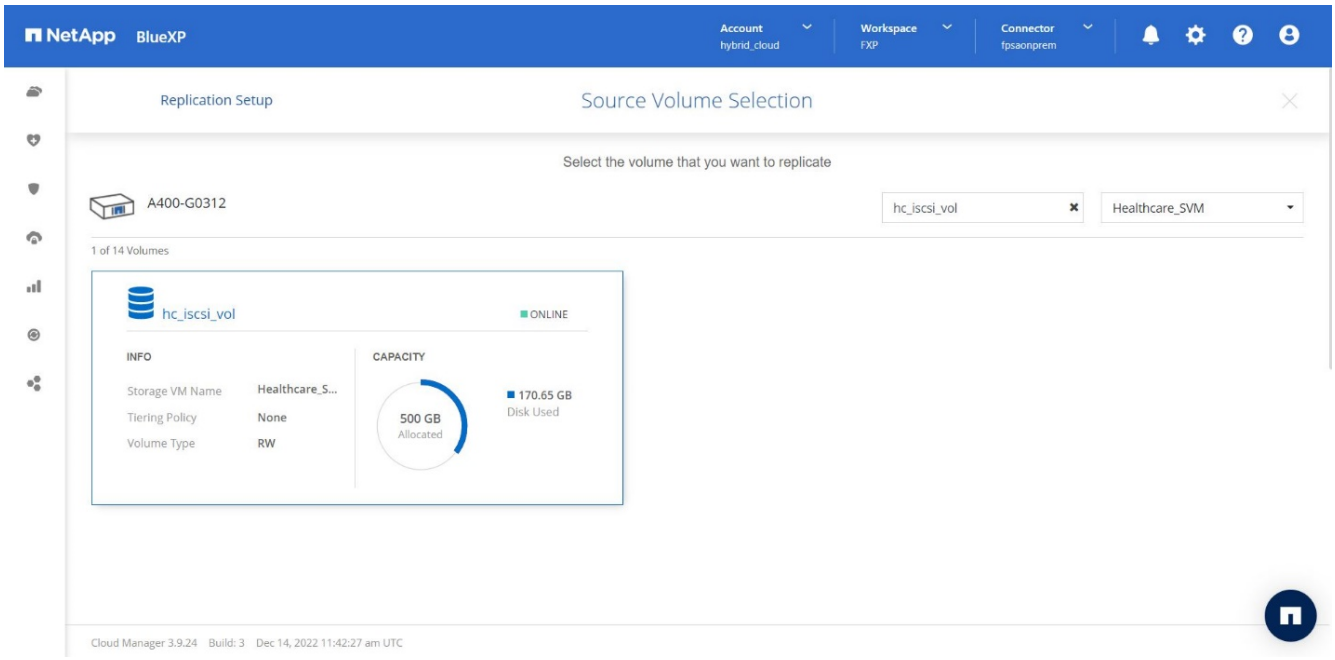


Los pasos restantes explican cómo crear una relación síncrona entre clústeres Cloud Volumes ONTAP y ONTAP en las instalaciones.

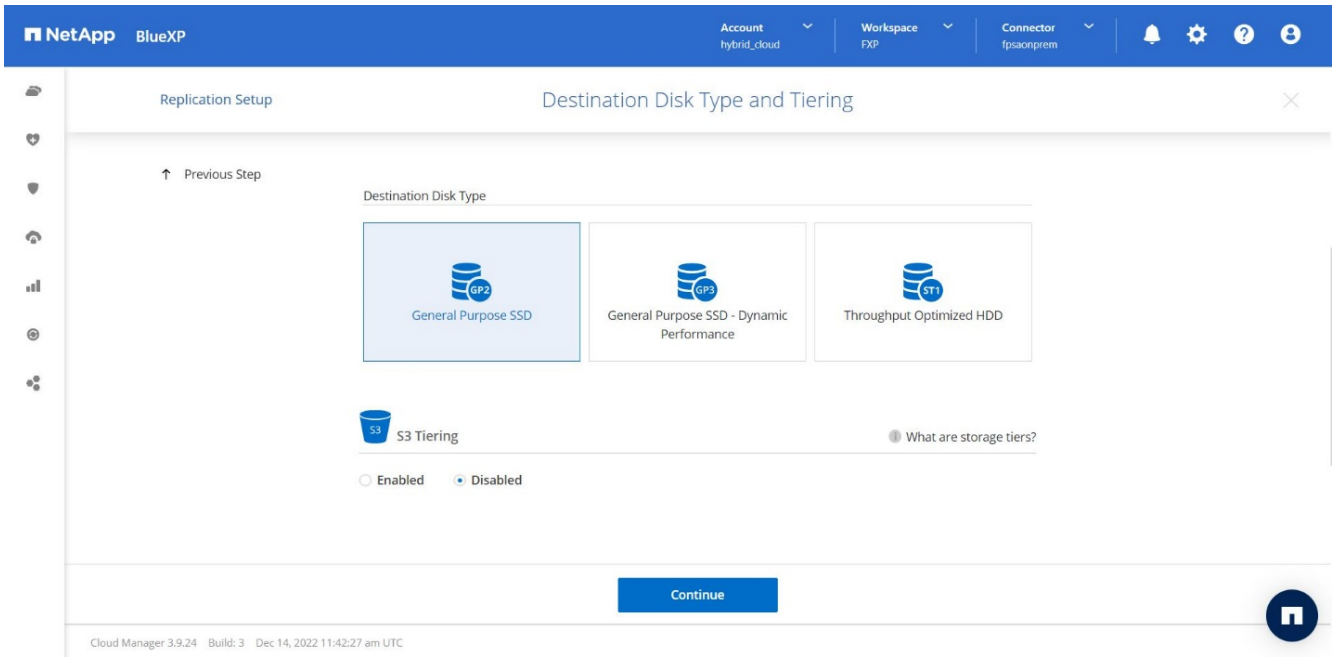
3. **Configuración de relación entre iguales de origen y destino.** Si aparece esta página, seleccione todas las LIF de interconexión de clústeres para la relación entre iguales de clústeres.



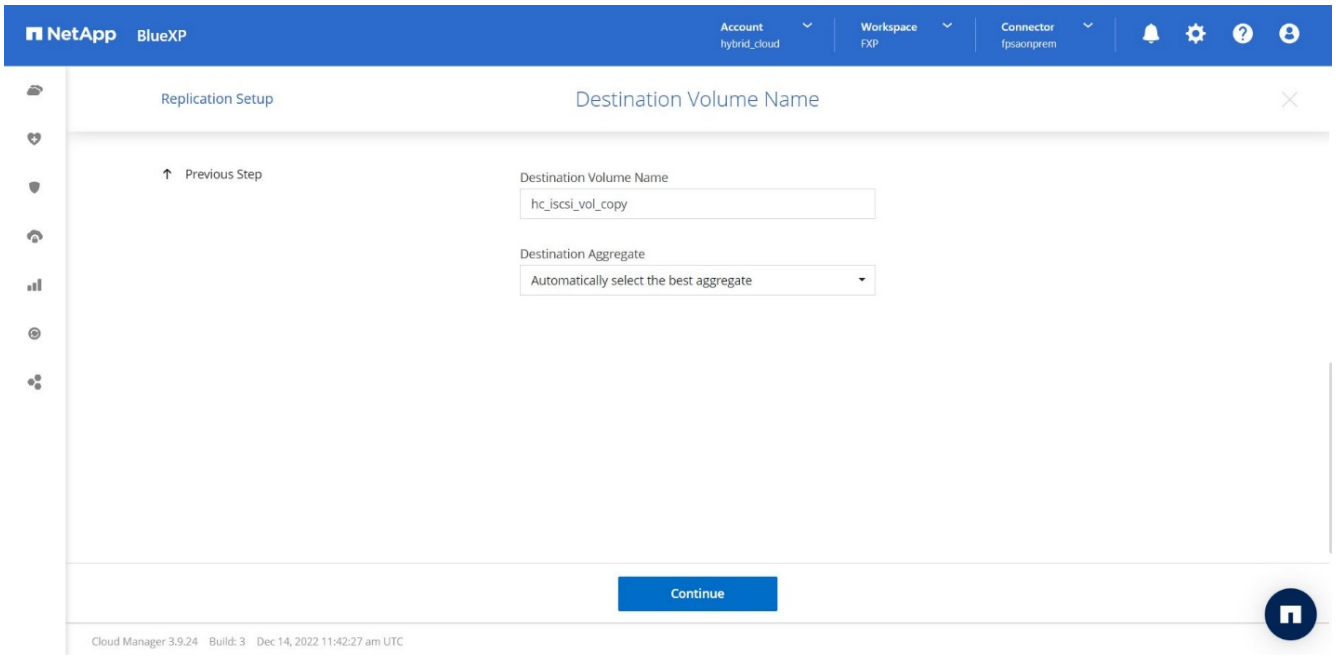
4. **Selección de volumen de origen.** Seleccione el volumen que desea replicar.



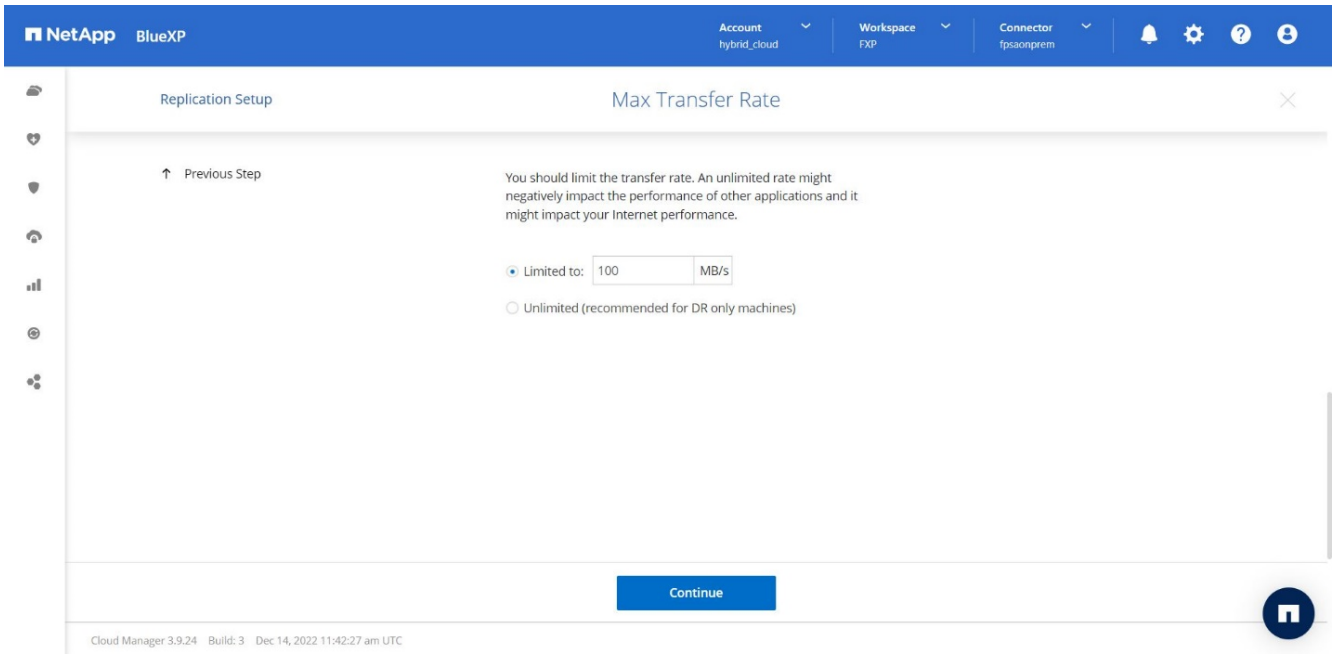
5. **Tipo de disco de destino y clasificación por niveles.** Si el destino es un sistema Cloud Volumes ONTAP, seleccione el tipo de disco de destino y elija si desea habilitar la organización por niveles de datos.



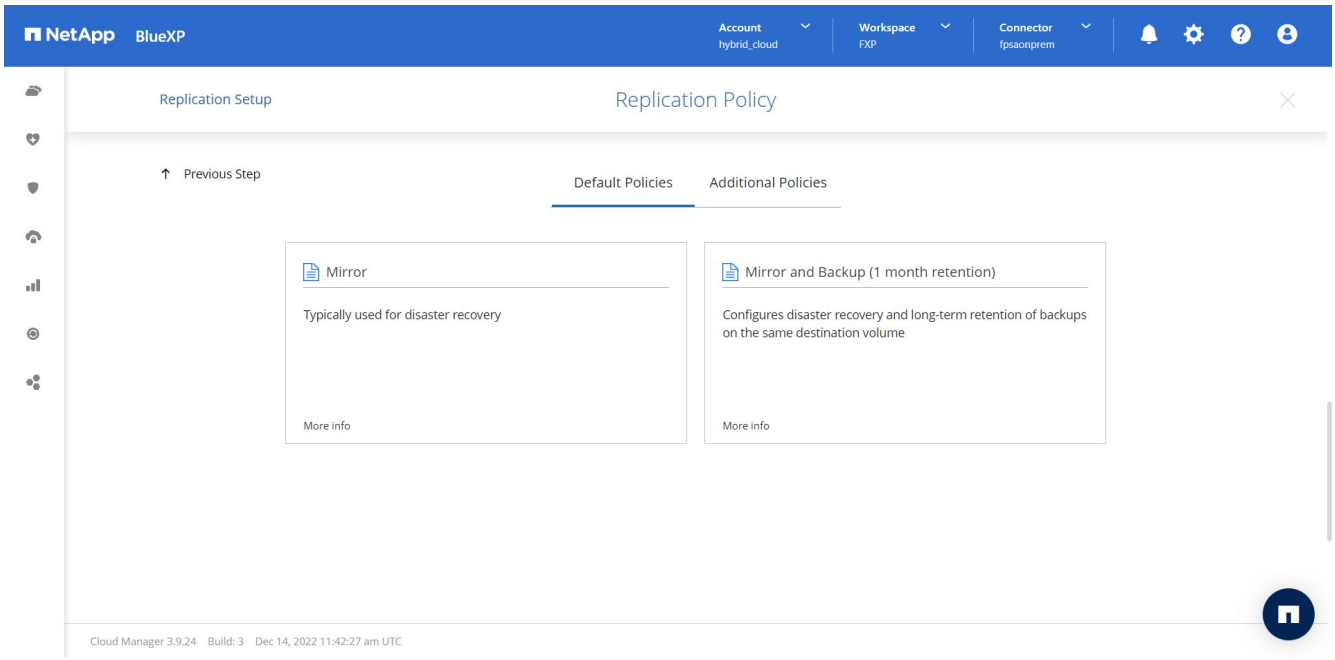
6. **Nombre del volumen de destino:** especifique el nombre del volumen de destino y elija el agregado de destino. Si el destino es un clúster de ONTAP, también debe especificar la máquina virtual de almacenamiento de destino.



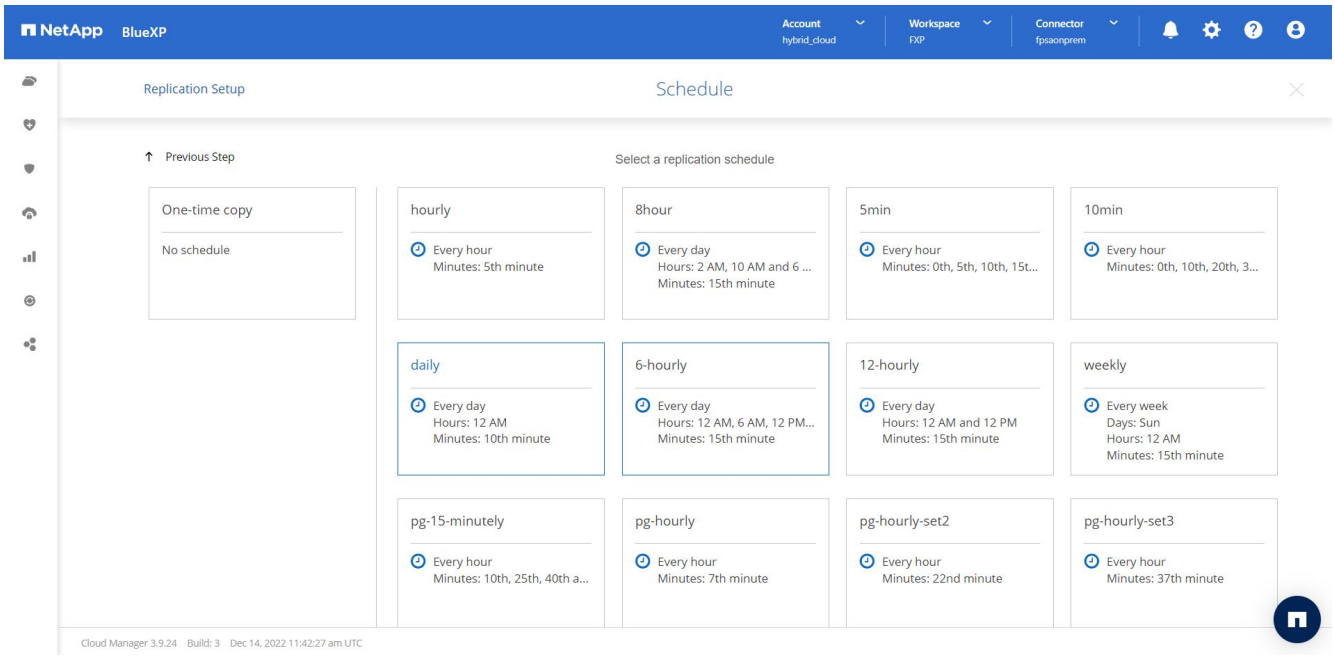
7. **Velocidad máxima de transferencia.** especifique la velocidad máxima (en megabytes por segundo) a la que se pueden transferir los datos.



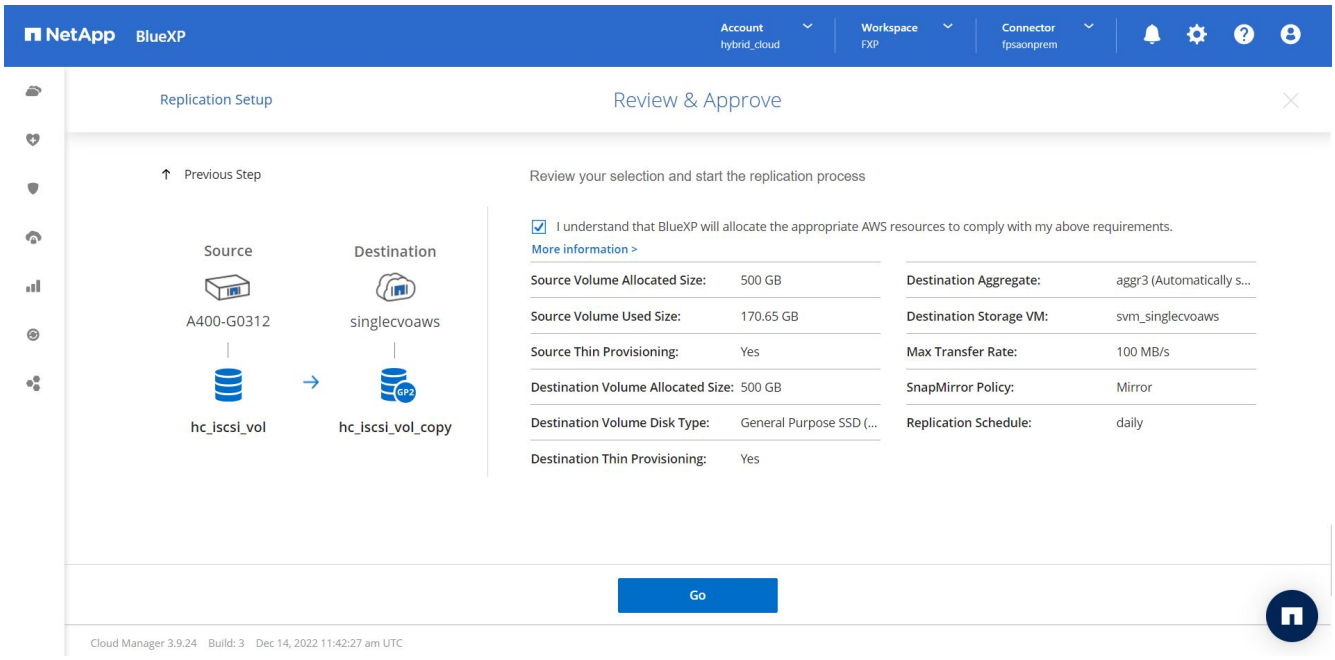
8. **Directiva de replicación.** Seleccione una directiva predeterminada o haga clic en **Directivas adicionales** y, a continuación, seleccione una de las directivas avanzadas. Si necesita ayuda, "obtenga información acerca de las políticas de replicación".



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.

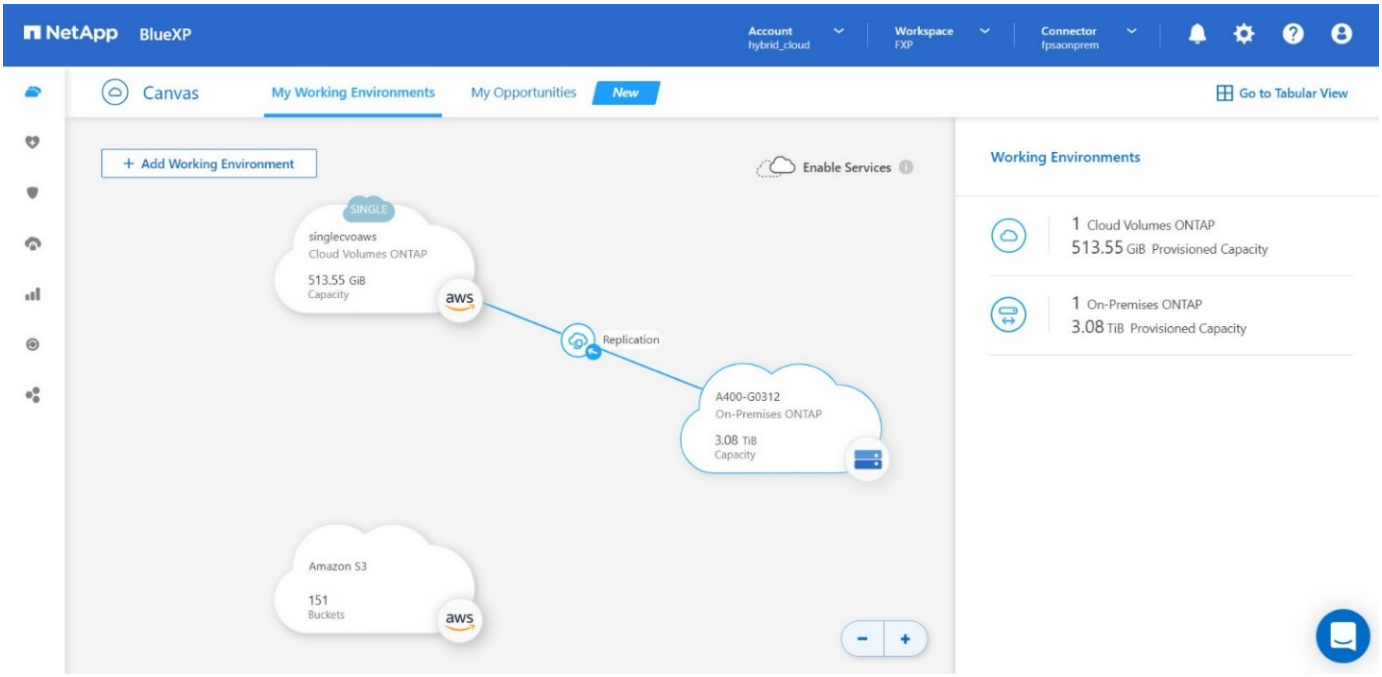


10. **Revisión.** Revise sus selecciones y haga clic en **Ir**.

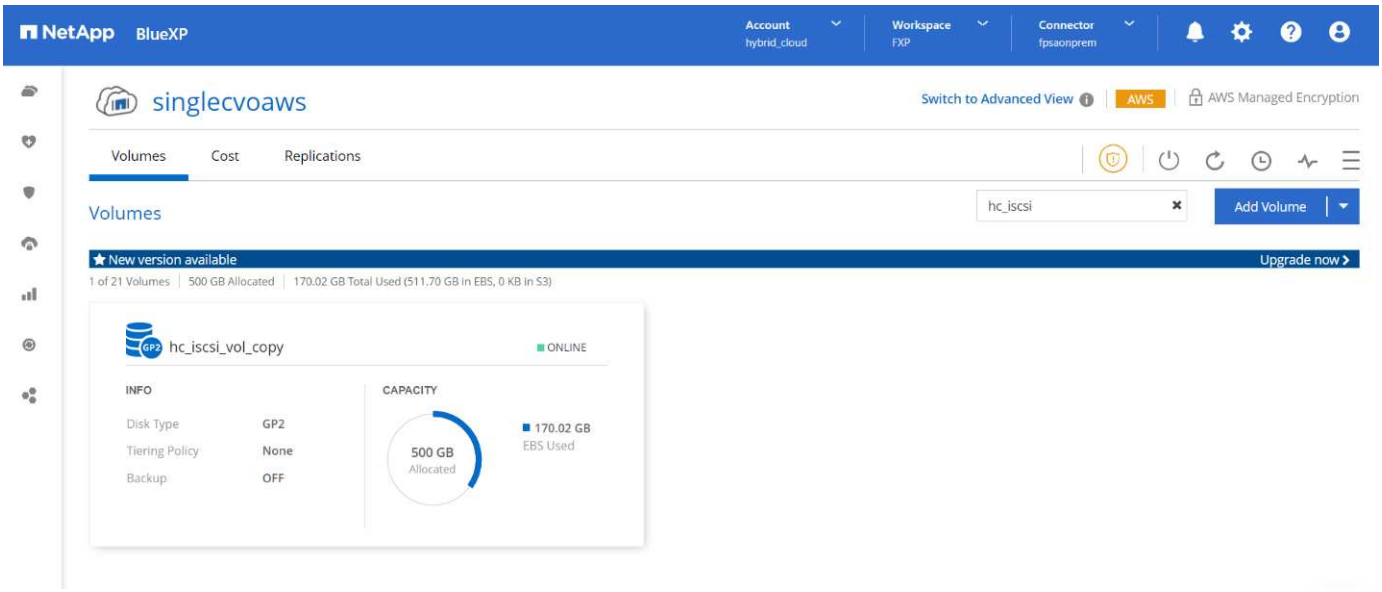


Para obtener información detallada sobre estos pasos de configuración, consulte "aquí".

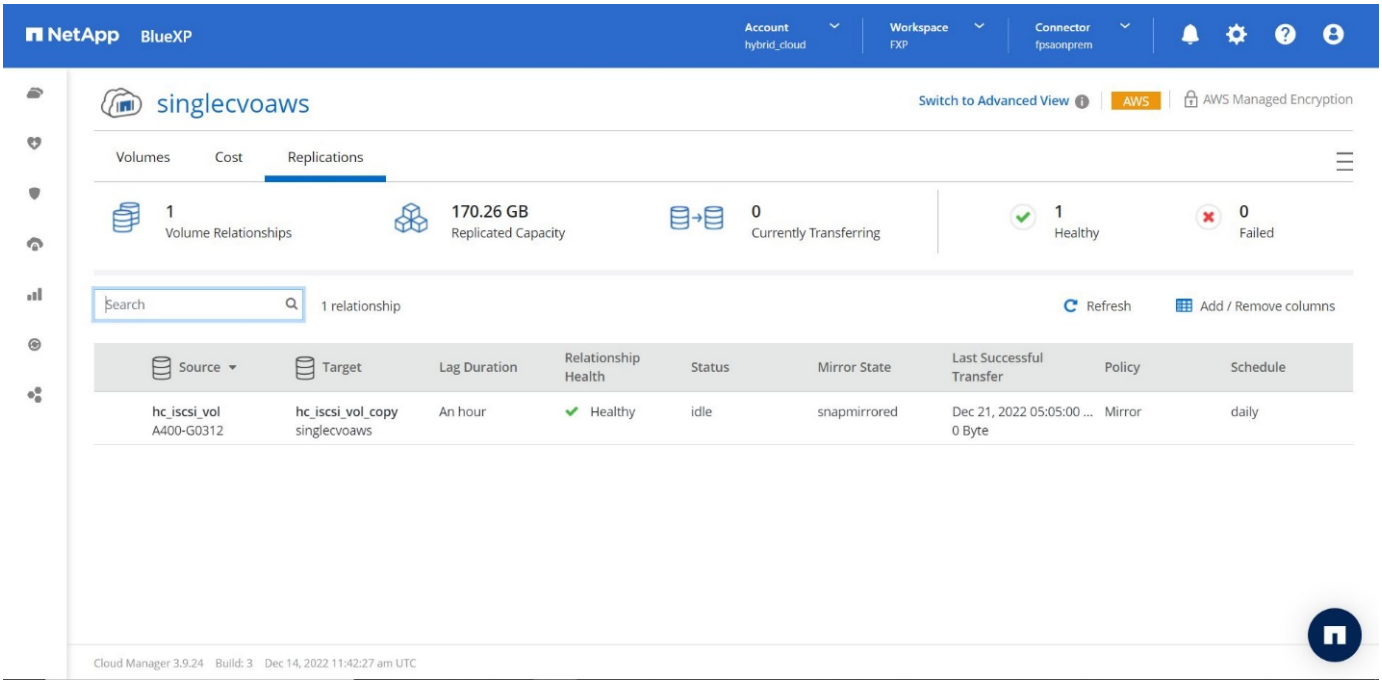
BlueXP inicia el proceso de replicación de datos. Ahora, puede ver el servicio **replicación** que se estableció entre su sistema ONTAP local y Cloud Volumes ONTAP.



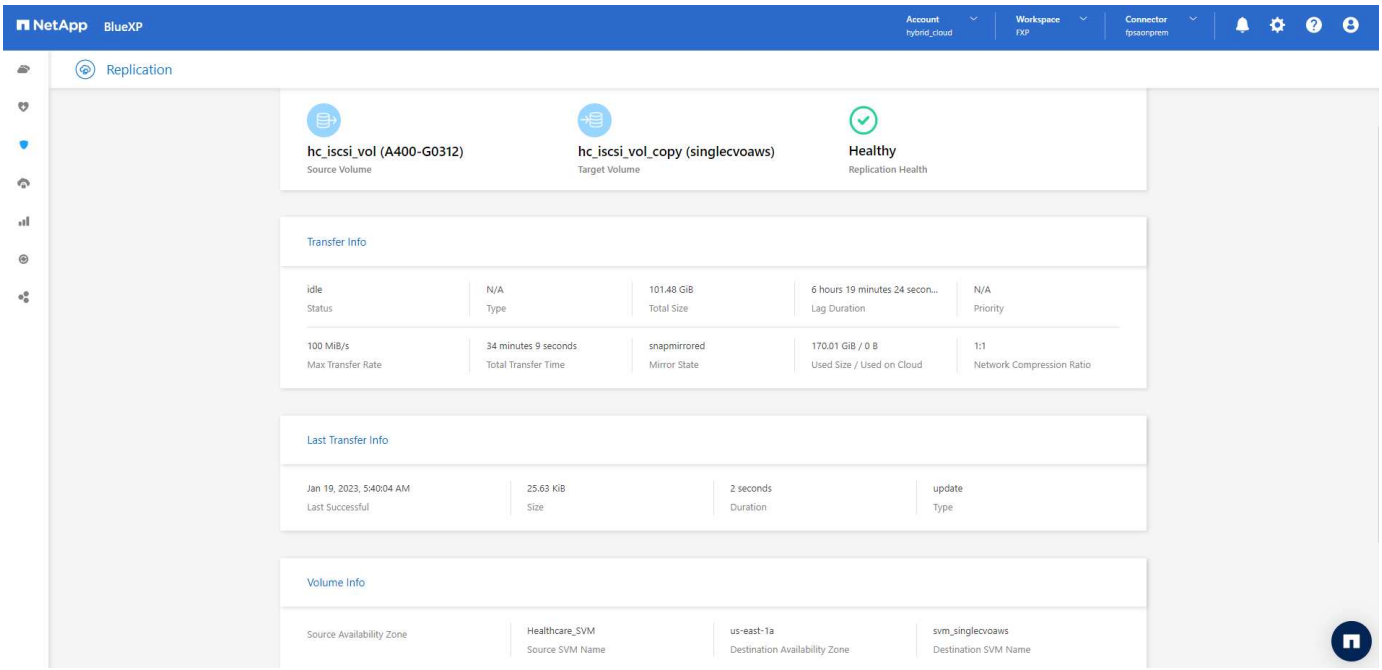
En el clúster de Cloud Volumes ONTAP, puede ver el volumen recién creado.



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 GUI de BlueXP 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.

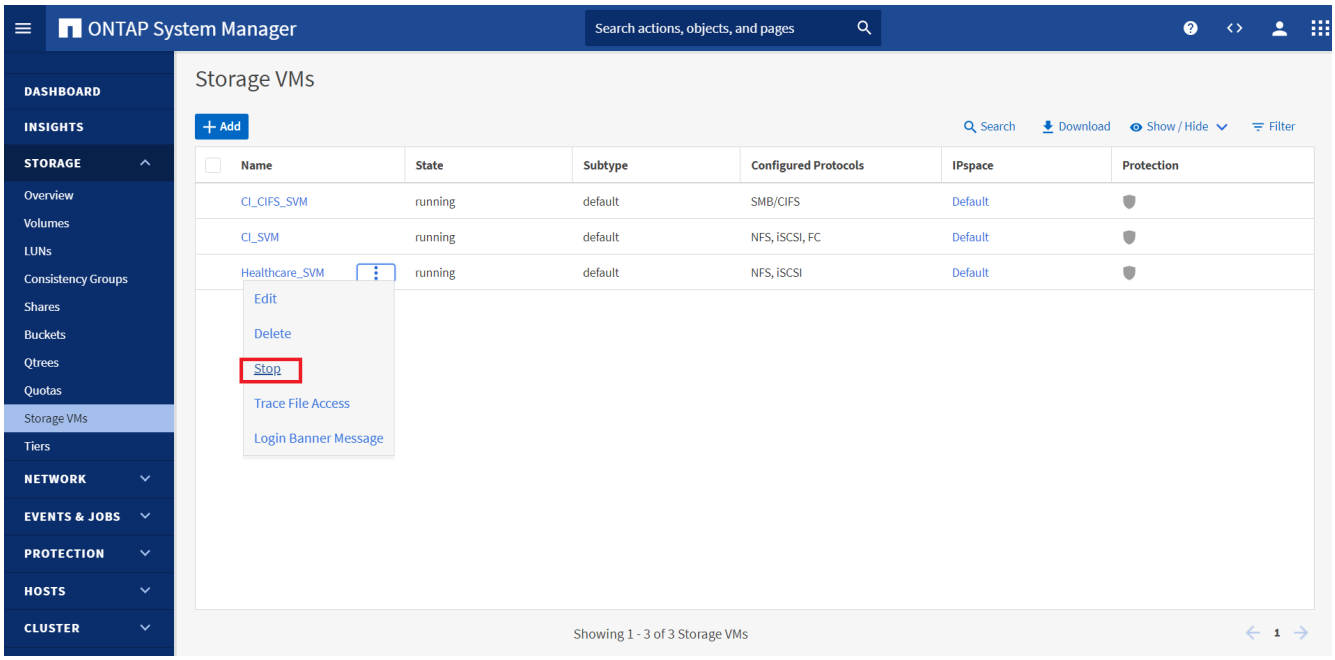
Recuperación tras siniestros

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.

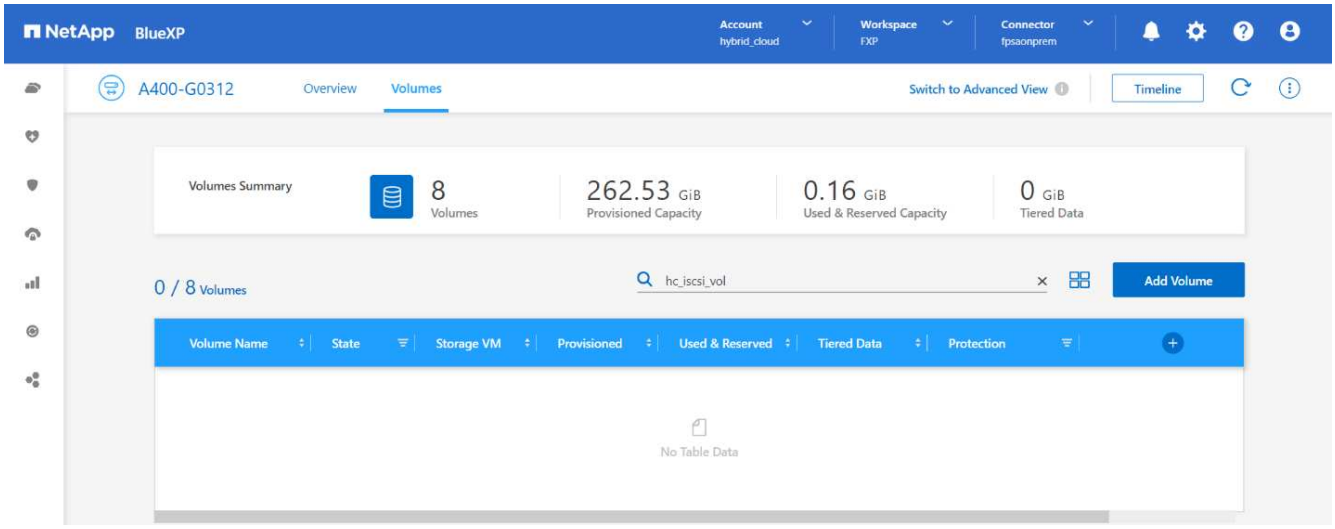
Para realizar la validación de un escenario de recuperación ante desastres correcto, complete los siguientes pasos:

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



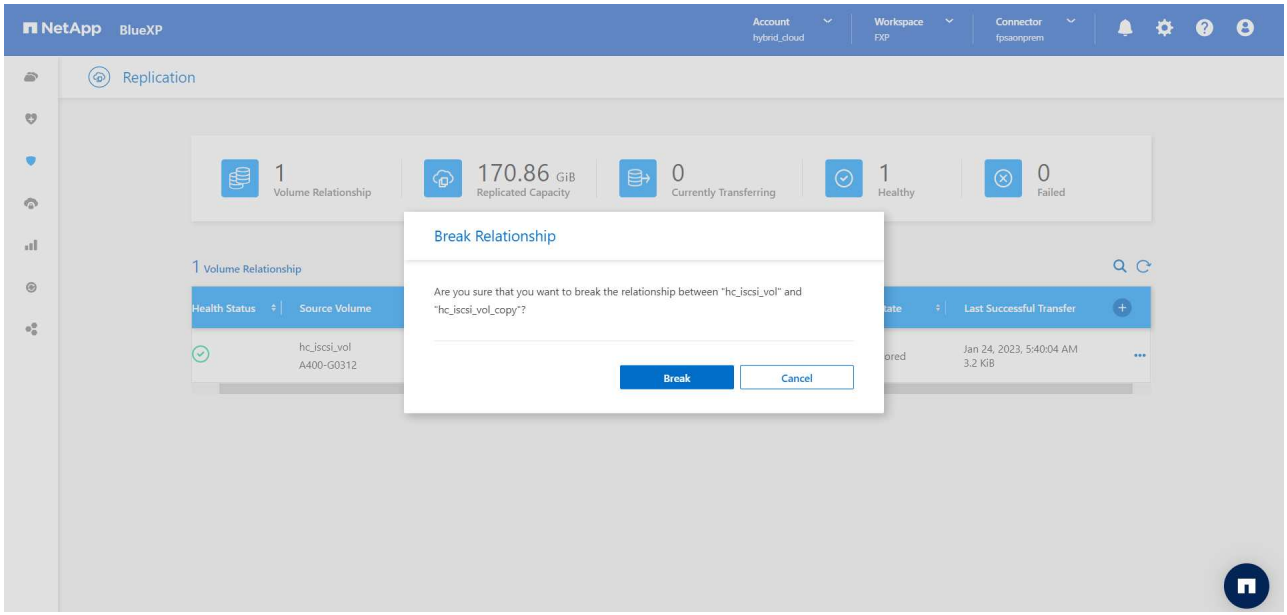
Asegúrese de que la replicación de SnapMirror ya esté configurada entre la ONTAP local en la instancia de FlexPod y Cloud Volumes ONTAP en AWS, para que pueda crear copias de Snapshot de aplicaciones frecuentes.

Una vez detenida la SVM, el `hc_iscsi_vol` El volumen no es visible en BlueXP.



2. Activar DR en CVO.

   a. Rompa la relación de replicación de SnapMirror entre ONTAP en las instalaciones y Cloud Volumes ONTAP y promocione 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_singlecvoaws                    /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
```

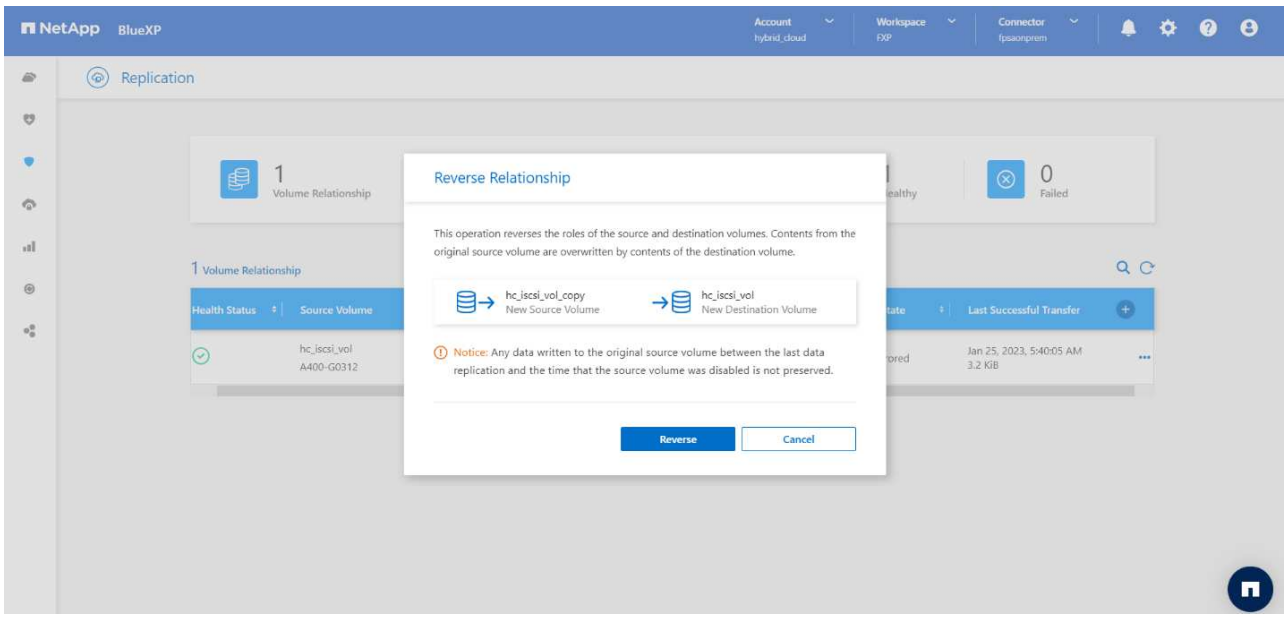
e. Finalmente, monte el sistema de archivos y muestre la información del sistema de archivos.

```
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
```

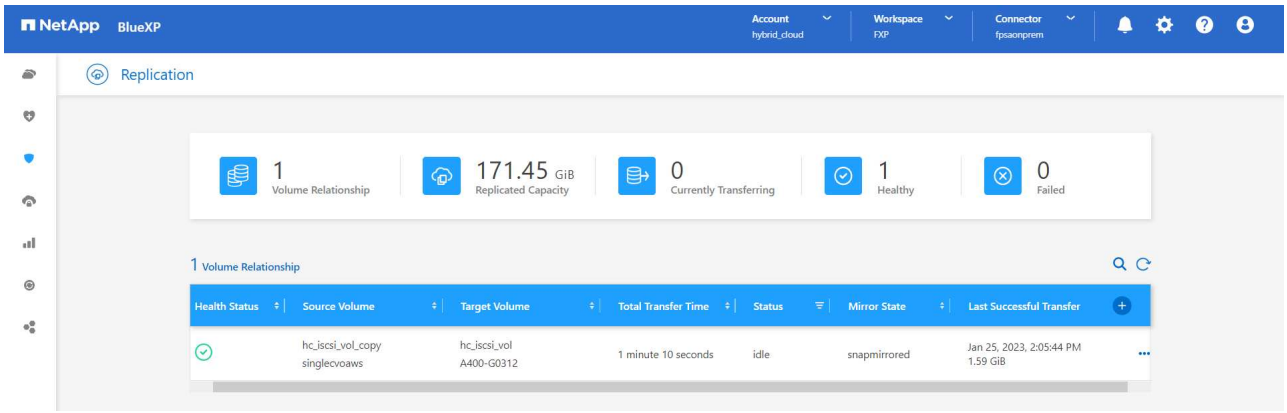
Este resultado muestra que los usuarios pueden acceder a los datos replicados a través de la red hasta la recuperación del centro de producción a partir del desastre.

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.

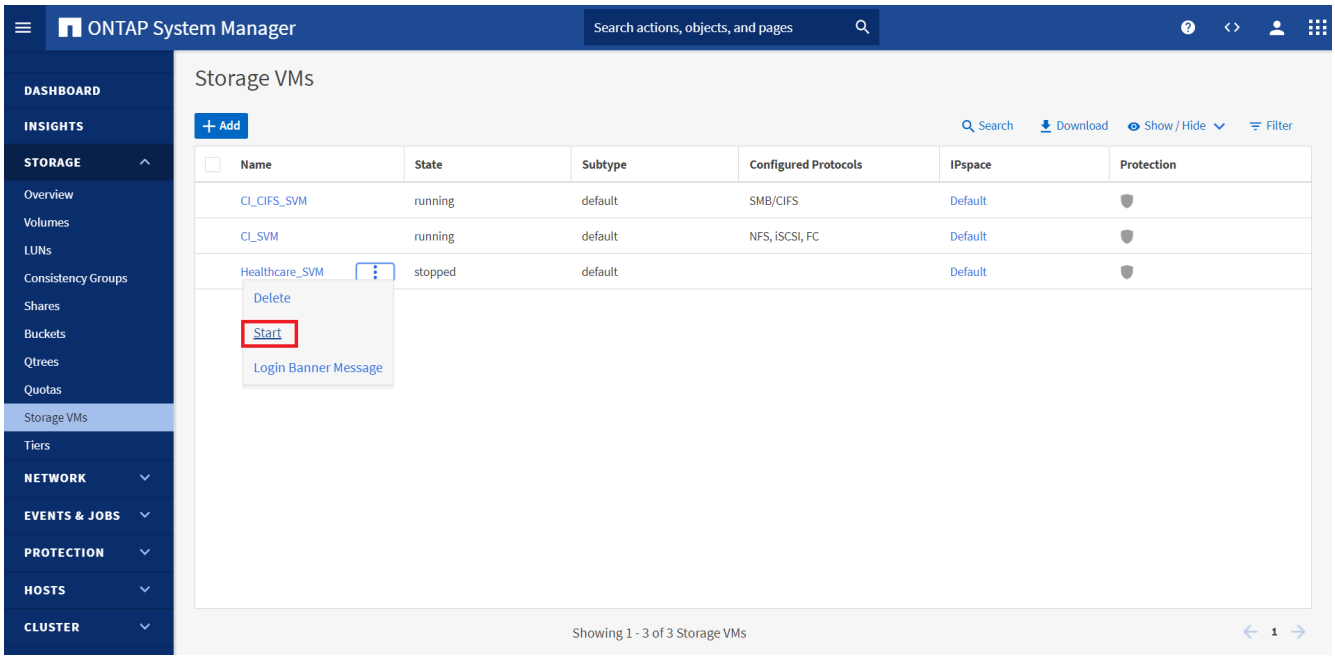
Verificación de los datos en el lugar de producción

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.

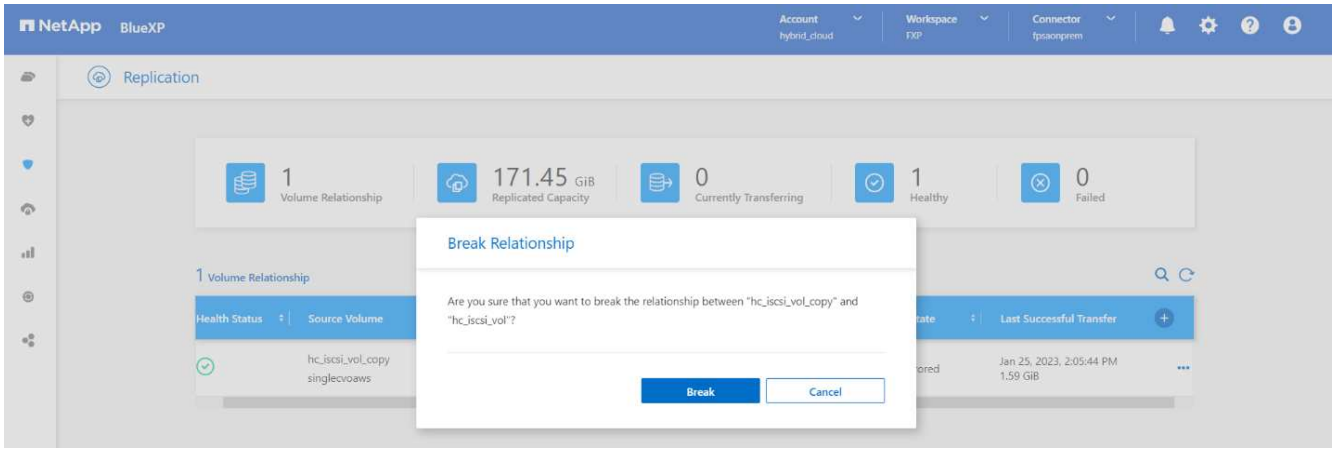
En esta sección, hablamos de poner en el sitio de origen, de restaurar la relación de SnapMirror entre ONTAP y Cloud Volumes ONTAP en las instalaciones, y finalmente realizamos una comprobación de la integridad de los datos en el extremo de la fuente

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`).



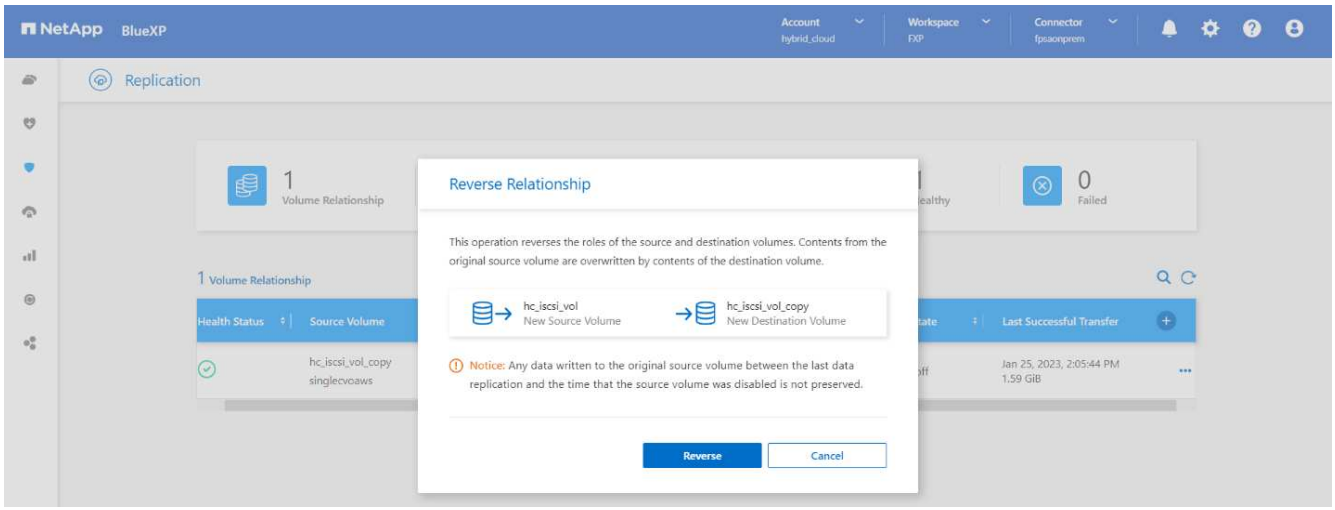
2. Rompa la relación de replicación de SnapMirror entre Cloud Volumes ONTAP y ONTAP en las instalaciones y promocione el volumen en las instalaciones (`hc_iscsi_vol`) volver a la producción.



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
```

3. 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.

4. 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/datavg/datalv /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.

"Siguiente: 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"

- 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"

- BlueXP de NetApp

  "https://bluexp.netapp.com/"

- Cloud Volumes ONTAP de NetApp

  "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"

- Replicación de SnapMirror

  "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"

- FlexPod para Epic

  "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/"

- Herramienta de interoperabilidad de hardware y software Cisco UCS

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- 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	Marzo de 2023	Versión inicial

Cloud híbrido de FlexPod para Google Cloud Platform con Cloud Volumes ONTAP de NetApp y Cisco Intersight

TR-4939: Cloud híbrido de FlexPod para Google Cloud Platform con Cloud Volumes ONTAP de NetApp y Cisco Intersight

Ruchika Lahoti, NetApp

Introducción

La protección de datos con recuperación ante desastres es un objetivo crucial para la continuidad del negocio. La recuperación ante desastres permite a las organizaciones conmutar por error sus operaciones empresariales a una ubicación secundaria y, después, recuperar y recuperar la conmutación tras recuperación en el sitio principal de forma eficiente y fiable. Debido a la existencia de múltiples preocupaciones, como desastres naturales, fallos de red, vulnerabilidades de software y errores humanos, el desarrollo de una estrategia de recuperación ante desastres constituye la principal prioridad EN MATERIA DE TECNOLOGÍA.

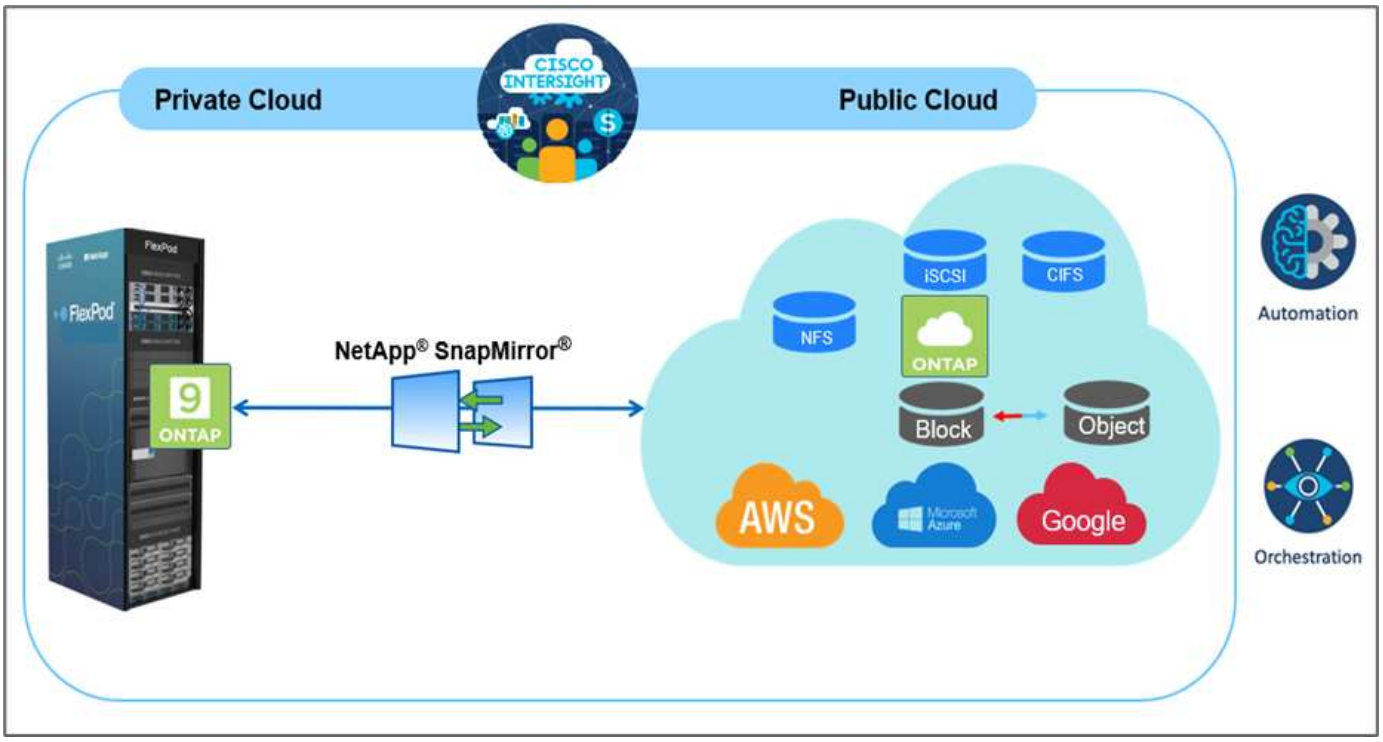
Para la recuperación ante desastres, todas las cargas de trabajo que se ejecuten en el sitio principal se deben reproducir de forma fiel en el sitio de recuperación ante desastres. Una organización también debe disponer de una copia actualizada de todos los datos empresariales, incluidos bases de datos, servicios de archivos, almacenamiento NFS e iSCSI, etc. Dado que los datos del entorno de producción se actualizan constantemente, los cambios deben transferirse al sitio de recuperación tras desastres regularmente.

La implementación de entornos de recuperación ante desastres es un reto para la mayoría de las organizaciones por el requisito de la independencia de la infraestructura y del sitio. El número de recursos necesarios y los costes de configuración, prueba y mantenimiento de un centro de datos secundario pueden ser muy elevados y, normalmente, se acercan al coste de todo el entorno de producción. Resulta difícil mantener un espacio utilizado para datos mínimo con una protección adecuada, a la vez que se sincronizan continuamente los datos y se establece una conmutación por error y conmutación tras recuperación sin problemas. Una vez creado el centro de recuperación ante desastres, el reto se convierte en replicar datos del entorno de producción y mantenerlos sincronizados.

Este informe técnico reúne la solución de infraestructura convergente de FlexPod, Cloud Volumes ONTAP de NetApp en Google Cloud y Cisco Intersight para formar un centro de datos de cloud híbrido para recuperación ante desastres. En esta solución, se trata del diseño y la ejecución de un flujo de trabajo de ONTAP en las instalaciones mediante Cisco Intersight Cloud Orchestrator. También hablamos de la puesta en marcha de Cloud Volumes ONTAP de NetApp y de la coordinación y automatización de la replicación de datos y la recuperación ante desastres entre FlexPod y Cloud Volumes ONTAP mediante el Servicio de interpretación de

Cisco para HashiCorp Terraform.

La siguiente figura muestra una descripción general de la solución.



Esta solución ofrece varias ventajas, como:

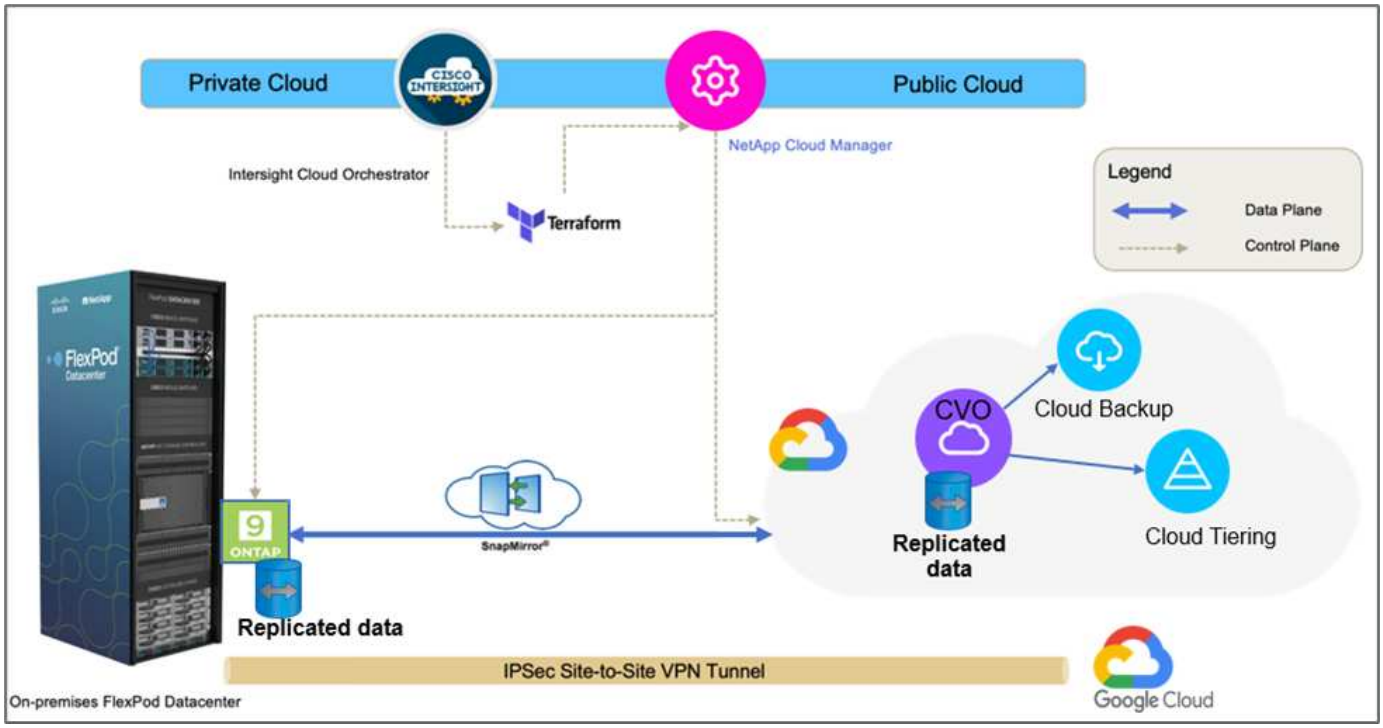
- * Orquestación y automatización.* Cisco Intersight simplifica las operaciones diarias de la infraestructura de cloud híbrido de FlexPod mediante la creación de marcos de coordinación consistentes que se ofrecen a través de la automatización.
- **Protección personalizada.** Cloud Volumes ONTAP proporciona replicación de datos a nivel de bloque de ONTAP a la nube que mantiene el destino actualizado mediante actualizaciones incrementales. Los usuarios pueden especificar un programa de sincronización de cada 5 minutos o cada hora, por ejemplo, según los cambios en el origen que se transfieren.
- **Recuperación tras fallos y recuperación sin problemas.** cuando se produce un desastre, los administradores de almacenamiento pueden recurrir rápidamente a los volúmenes en la nube. Cuando se recupera el sitio principal, los datos nuevos creados en el entorno de recuperación ante desastres se sincronizan de nuevo con los volúmenes de origen, de modo que se vuelve a establecer la replicación de datos secundaria.
- **Eficiencia:** el espacio de almacenamiento y los costes de la copia secundaria de cloud se optimizan mediante el uso de la compresión de datos, el thin provisioning y la deduplicación. Los datos se transfieren en el nivel de bloque en forma comprimida y deduplicado, lo que mejora la velocidad de transferencia. 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.
- **Mayor productividad DE TI.** el uso de Intersight como la única plataforma segura de nivel empresarial para la gestión de la infraestructura y del ciclo de vida de las aplicaciones simplifica la gestión de la configuración y la automatización de las tareas manuales a escala para la solución.

Destinatarios

El público de este documento incluye, sin limitarse a ellos, ingenieros de ventas, consultores de campo, servicios profesionales, gestores DE TECNOLOGÍA, Ingenieros de los partners, ingenieros de fiabilidad del sitio, arquitectos de cloud, ingenieros de cloud y clientes que quieran aprovechar una infraestructura creada para proporcionar eficiencia TECNOLÓGICA y propiciar la innovación TECNOLÓGICA.

Topología de la solución

En esta sección se describe la topología lógica de la solución. La siguiente figura representa la topología de la solución del entorno local de FlexPod, la ejecución de Cloud Volumes ONTAP de NetApp en Google Cloud, Cisco Intersight y Cloud Manager de NetApp.



Los planos de control y los planos de datos se indican claramente entre los puntos finales. El plano de datos utiliza una conexión VPN sitio a sitio segura para conectar la instancia de ONTAP que se ejecuta en All Flash FAS de FlexPod a la instancia de Cloud Volumes ONTAP de NetApp en Google Cloud.

La replicación de datos de carga de trabajo de FlexPod a Cloud Volumes ONTAP de NetApp es gestionada por SnapMirror de NetApp, y el proceso general se orquesta mediante Intersight Cloud Orchestrator de Cisco tanto para los entornos locales como de cloud. Cisco Intersight Cloud Orchestrator consume Terraform Resource Providers para NetApp Cloud Manager para llevar a cabo operaciones relacionadas con la puesta en marcha de Cloud Volumes ONTAP de NetApp y establecer relaciones de replicación de datos.

Esta solución también es compatible con el backup y la organización en niveles opcional de los datos inactivos en la instancia de Cloud Volumes ONTAP de NetApp en Google Cloud Storage.

"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, las redes de almacenamiento de Cisco MDS y Cisco Unified Computing System (Cisco UCS). El diseño es lo suficientemente flexible como para que la red, la informática y el almacenamiento puedan caber en un rack de centro de datos o se puede implementar según el diseño del centro de datos del cliente. La densidad de puertos permite que los componentes de las redes acomoden varias configuraciones.

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.** entrega como 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 acelerar la prestación de la línea de negocio.
- **Operaciones simplificadas.** simplifique las operaciones utilizando una única herramienta segura proporcionada por SaaS con inventario, autenticación y API comunes para trabajar en toda la pila y todas las ubicaciones, eliminando los silos entre equipos. Desde la gestión de servidores físicos e hipervisores en las instalaciones a equipos virtuales, K8s, servidores, automatización optimización y control de costes en los clouds públicos y en las instalaciones.
- **Optimización continua.** Optimice continuamente su entorno mediante la inteligencia proporcionada por Cisco Intersight en todas las capas, así como Cisco TAC. Esta inteligencia se convierte en acciones recomendadas y automatizables para que usted pueda adaptar en tiempo real a cada cambio: Desde mover cargas de trabajo y supervisar el estado de los servidores físicos hasta recomendaciones de reducción de costes 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 UMM o IMM nativos para sistemas Cisco UCS conectados a la estructura durante la configuración inicial de las interconexiones de estructura. En esta solución, se utiliza IMM nativa.

Licencias de Cisco Intersight

Cisco Intersight utiliza una licencia basada en suscripción con varios niveles.

Los niveles de licencias de Cisco Intersight son los siguientes:

- **Cisco Intersight Essentials.** incluye todas las funciones básicas y las siguientes características:
  - Cisco UCS Central
  - Derecho del supervisor Cisco IMC
  - Configuración basada en políticas con Server Profiles
  - Gestión del firmware
  - Valoración de la compatibilidad con la lista de compatibilidad de hardware (HCL)
- **Cisco Intersight Advantage.** incluye las características y funciones de la capa Essentials además de las siguientes características:
  - Widgets, inventario, capacidad, funciones de uso y correlación entre dominios en recursos informáticos físicos, red, almacenamiento, virtualización de VMware y cloud público de AWS.

    - El servicio de asesoría de seguridad de Cisco, en el que los clientes pueden recibir alertas de seguridad importantes y avisos de campo sobre los dispositivos terminales afectados.
- * Cisco Intersight Premier.* Además de las capacidades proporcionadas en el nivel Advantage, Cisco Intersight Premier ofrece lo siguiente:
    - Intersight Cloud Orchestrator (ICO) para Cisco y terceros en informática, redes, almacenamiento, sistemas integrados, virtualización, cloud público y plataformas de cloud público
    - Derecho completo de suscripción para Cisco UCS Director sin coste adicional.

Puede encontrar más información sobre Intersight Licensing y las funciones compatibles con cada licencia "aquí".

> En esta solución utilizamos Intersight Cloud Orchestrator e Intersight Service para HashiCorp Terraform. Estas funciones están disponibles para los usuarios con la licencia Intersight Premier, por lo que este nivel de licencia debe estar activado.

Integración en la nube terraina con ICO

Puede utilizar Cisco Intersight Cloud Orchestrator (ICO) para crear y ejecutar flujos de trabajo que llamen a las API de Terraform Cloud (TFC). La tarea Invoke Web API Request admite Terraform Cloud como destino y se puede configurar con API de Terraform Cloud mediante métodos HTTP. Por lo tanto, el flujo de trabajo puede tener una combinación de tareas que llama a varias API de cloud de Terraform utilizando tareas de API genéricas y otras operaciones. Necesita una licencia Premier para utilizar la función ICO.

Cisco Intersight Assist

Cisco Intersight Assist le ayuda a agregar dispositivos de punto final a Cisco Intersight. Un centro de datos podría tener varios dispositivos que no se conecten directamente con Cisco Intersight. Cualquier dispositivo compatible con Cisco Intersight pero que no se conecte directamente a él requiere un mecanismo de conexión. Cisco Intersight Assist proporciona ese mecanismo de conexión y le ayuda a agregar dispositivos a Cisco Intersight.

Cisco Intersight Assist está disponible en Cisco Intersight Virtual Appliance, que se distribuye como una máquina virtual de implantación que se encuentra en un formato de archivo de Open Virtual Appliance (OVA). Puede instalar el dispositivo en un servidor ESXi. Para obtener más información, consulte "Guía de inicio de Cisco Intersight Virtual Appliance".

Después de solicitar Intersight Assist a Intersight, puede reclamar dispositivos de punto final mediante la opción Claim a través de Intersight Assist. Para obtener más información, consulte "Primeros pasos".

Cloud Volumes ONTAP de NetApp

- Aprovechamiento de las funciones integradas de deduplicación de datos, compresión de datos, thin provisioning y clonado para minimizar los costes en almacenamiento.
- Proporcionando fiabilidad empresarial y operaciones continuas en caso de fallos en su entorno cloud.
- Cloud Volumes ONTAP utiliza SnapMirror de NetApp, la tecnología de replicación líder del sector, para replicar datos en las instalaciones al cloud, por lo que resulta fácil disponer de copias secundarias para diferentes casos de uso.
- Cloud Volumes ONTAP también se integra con Cloud Backup Service para ofrecer funcionalidades de backup y restauración para la protección y el archivado a largo plazo de sus datos en el cloud.
- Cambiar entre pools de almacenamiento de alto y bajo rendimiento bajo demanda sin tener que desconectar las aplicaciones.

- Proporcionar consistencia de copias Snapshot mediante SnapCenter de NetApp.
- Cloud Volumes ONTAP admite el cifrado de datos y proporciona protección contra virus y ransomware.
- La integración con Cloud Data Sense le ayuda a comprender el contexto de los datos e identificar datos confidenciales.

Cloud Central

Cloud Central proporciona una ubicación centralizada para acceder y gestionar los servicios de datos en el cloud de NetApp. Estos servicios le permiten ejecutar aplicaciones críticas en el cloud, crear sitios de recuperación ante desastres automatizados, realizar backups de sus datos SaaS y migrar y controlar datos de forma efectiva entre varios clouds. Para obtener más información, consulte "Cloud Central".

Cloud Manager

Cloud Manager es una plataforma de gestión empresarial basada en SaaS que permite a los expertos EN TECNOLOGÍA y arquitectos de cloud gestionar de forma centralizada su infraestructura multicloud híbrida con las soluciones cloud de NetApp. Proporciona un sistema centralizado para ver y gestionar su almacenamiento en las instalaciones y en cloud, con el fin de dar soporte a varias cuentas y proveedores de cloud híbrido. Para obtener más información, consulte "Cloud Manager".

Conector

Connector permite que Cloud Manager gestione recursos y procesos dentro de un entorno de cloud público. Se requiere una instancia de Connector para utilizar muchas de las funciones proporcionadas por Cloud Manager y que se puede poner en marcha en el cloud o en la red local. El conector se admite en las siguientes ubicaciones:

- AWS
- Microsoft Azure
- Google Cloud
- En el entorno local

Active IQ Unified Manager de NetApp

Active IQ Unified Manager de NetApp le permite supervisar sus clústeres de almacenamiento de ONTAP desde una única interfaz intuitiva y rediseñada que proporciona inteligencia sobre los conocimientos de la comunidad y los análisis de IA. Proporciona información proactiva, operativa y de rendimiento integral del entorno de almacenamiento y de 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 para solucionar el problema que puede tomar. 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 permite planificar los requisitos de almacenamiento de los usuarios al prever las tendencias de uso y capacidad para que actúen de forma proactiva antes de que surjan problemas, evitando la toma de decisiones a corto plazo que puedan dar lugar a problemas adicionales a largo plazo.

VSphere de VMware

VMware vSphere es una plataforma de virtualización para gestionar de forma holística grandes colecciones de infraestructuras (recursos que incluyen 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 agrupa la infraestructura de todo un centro de datos para crear una única usina con recursos que se pueden asignar de forma rápida y dinámica a cualquier aplicación que lo necesite.

Si quiere más información sobre VMware vSphere, siga "este enlace".

VMware vSphere 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.

Versiones de hardware y software

Esta solución de cloud híbrido se puede ampliar a cualquier entorno FlexPod que ejecute versiones compatibles de software, firmware y hardware tal y como se define en la herramienta de matriz de interoperabilidad de NetApp y la lista de compatibilidad de hardware de Cisco UCS.

La solución de FlexPod que se utiliza como plataforma de referencia en nuestro entorno local se puso en marcha de acuerdo con las directrices y especificaciones descritas "aquí".

La red dentro de este entorno se basa en ACI. Para obtener más información, consulte "aquí".

- Consulte los siguientes enlaces para obtener más información:
- "Herramienta de matriz de interoperabilidad de NetApp"
- "Guía de compatibilidad de VMware"
- "Herramienta de interoperabilidad de hardware y software Cisco UCS"

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

Componente	Producto	Versión
Informática	CISCO UCS X210C-M6	5.0(1b)
	Interconexiones de estructura Cisco UCS 6454	4.2(2a)
Red	Cisco Nexus 9332C (espina)	14.2(s)
	Cisco Nexus 9336C-FX2 (Hoja)	14.2(s)
	ACI de Cisco	4.2(s)
Reducida	AFF A220 de NetApp	9.11.1
	Herramientas de ONTAP de NetApp para VMware vSphere	9.10

Componente	Producto	Versión
	Complemento NFS de NetApp para VAAI de VMware	2.0-15
	Active IQ Unified Manager	9.11
De NetApp	VSphere ESXi	7.0(U3)
	Dispositivo VMware vCenter	7.0.3
	Dispositivo virtual Cisco Intersight Assist	1.0.11-306

La ejecución de las configuraciones de Terraform ocurre en la cuenta de Terraform Cloud for Business. La configuración de Terraform utiliza el proveedor de Terraform para NetApp Cloud Manager.

En la siguiente tabla se enumeran los proveedores, productos y versiones.

Componente	Producto	Versión
HashiCorp	Terraform	1.2.7

La siguiente tabla muestra las versiones de Cloud Manager y Cloud Volumes ONTAP.

Componente	Producto	Versión
NetApp	Cloud Volumes ONTAP	9.11
	Cloud Manager	3.9.21

"Siguiente: Instalación y configuración: Implemente FlexPod."

Instalación y configuración

Ponga en marcha FlexPod

"Anterior: Componentes de la solución."

Para comprender los detalles sobre el diseño y la puesta en marcha de FlexPod, incluida la configuración de varios elementos del diseño y las mejores prácticas asociadas, consulte "Diseños validados por Cisco para FlexPod".

FlexPod se puede implementar tanto en UCS Managed Mode como en Cisco Intersight Managed Mode. Si desea implementar FlexPod en UCS Managed Mode, se puede encontrar el diseño validado por Cisco más reciente "aquí".

Cisco Unified Compute System (Cisco UCS) X-Series es un nuevo sistema informático modular, configurado y gestionado desde el cloud. Está diseñado para satisfacer las necesidades de las aplicaciones modernas y mejorar la eficiencia operativa, la agilidad y el escalado mediante un diseño modular adaptable, preparado para el futuro. Se pueden encontrar las directrices de diseño para incorporar la plataforma de la serie X de UCS gestionada por Cisco Intersight en la infraestructura de FlexPod "aquí".

Encontrará FlexPod con la puesta en marcha de Cisco ACI "aquí".

"Siguiente: Configuración de Cisco Intersight."

Configuración de Cisco Intersight

"Anterior: Implementar FlexPod."

Para configurar Cisco Intersight e Intersight Assist, consulte la página de diseños validados por Cisco para FlexPod "aquí".

"Siguiente: Integración cloud Terraform con el requisito previo de la ICO."

Integración en la nube con Terraform requisito previo de la ICO

"Anterior: Configuración de Cisco Intersight."

Procedimiento 1: Conectar Cisco Intersight y Terraform Cloud

1. Reclame o cree un destino cloud de Terraform mediante los detalles pertinentes de la cuenta de Terraform Cloud.
2. Cree un destino de agente de cloud Terraform para clouds privados, de modo que los clientes puedan instalar el agente en el centro de datos y habilitar la comunicación con Terraform Cloud.

   Si desea obtener más información, siga este "este enlace".

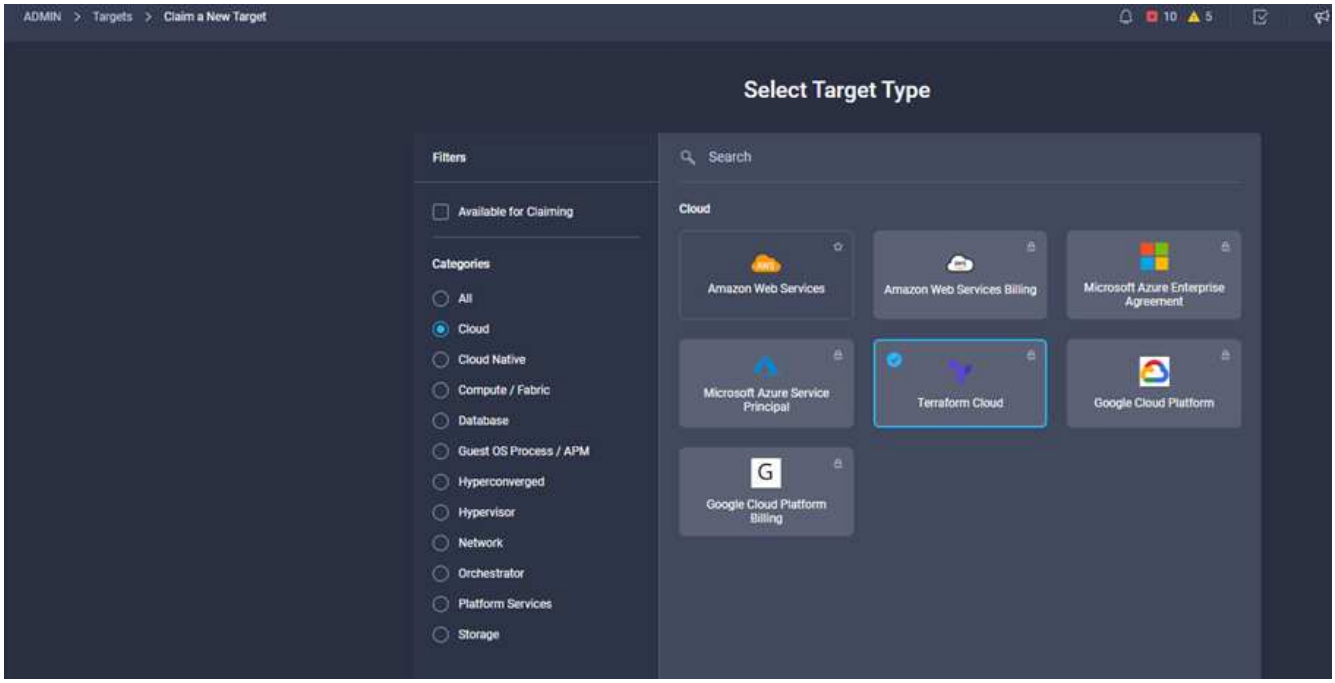
Procedimiento 2: Generar token de usuario

Como parte de la adición de un destino para Terraform Cloud, debe proporcionar el nombre de usuario y el token de API desde la página de configuración de Terraform Cloud.

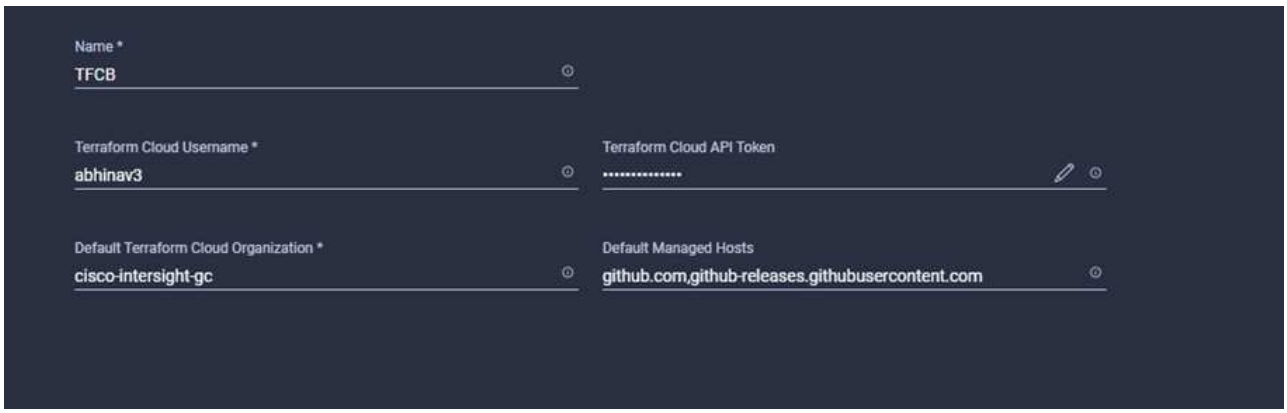
1. Inicie sesión en el cloud de Terraform y vaya a **fichas de usuario**: "https://app.terraform.io/app/settings/tokens".
2. Haga clic en **Crear un nuevo token de API**.
3. Asigne un nombre para recordar y guardar el token en un lugar seguro.

Procedimiento 3: Objetivo de cloud de Terraform de reclamación

1. Inicie sesión en Intersight con privilegios de Administrador de cuentas, Administrador de dispositivos o Técnico de dispositivos.
2. Vaya a **ADMIN > Targets > Claim a New Target**.
3. En **Categorías**, haga clic en **Cloud**.
4. Haga clic en **Nube Terraform** y haga clic en **Inicio**.



5. Escriba un nombre para el destino, el nombre de usuario para Terraform Cloud, el token de API y una organización predeterminada en Terraform Cloud, como se muestra en la siguiente imagen.
6. En el campo **hosts administrados predeterminados**, asegúrese de agregar los siguientes vínculos junto con otros hosts gestionados:
   - github.com
   - github-releases.githubusercontent.com



Si todo se introduce correctamente, verá el destino de Terraform Cloud mostrado en la sección **objetivos de Intersight**.

Procedimiento 4: Agregar agentes de Terraform Cloud

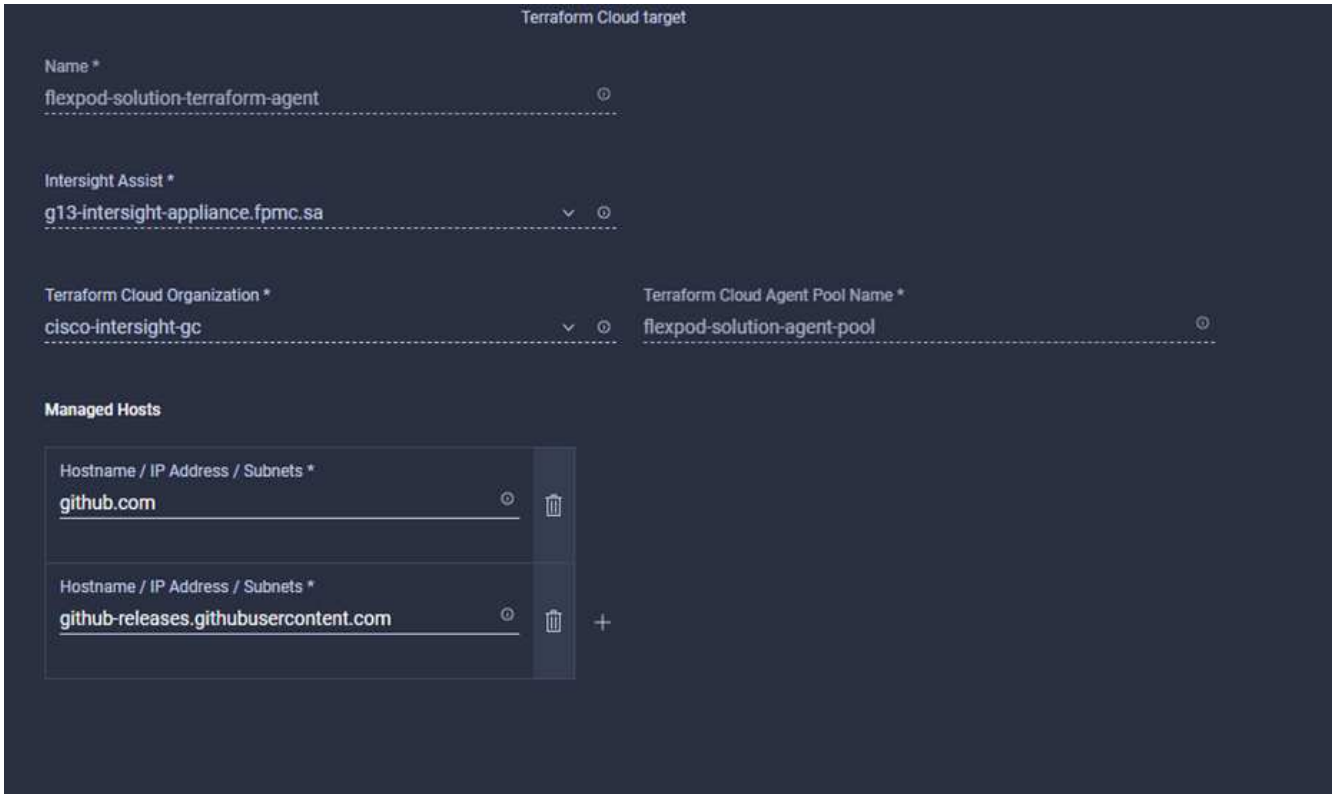
Requisitos previos:

- Destino de cloud Terraform.
- Se ha reclamado Intersight Assist en Intersight antes de implementar el Agente de nube de Terraform.

Sólo puede reclamar cinco agentes por cada ayuda.

Después de crear la conexión a Terraform, debe activar un agente de Terraform para ejecutar el código de Terraform.

1. Haga clic en **Claim Terraform Cloud Agent** en la lista desplegable de su destino de Terraform Cloud.
2. Introduzca los detalles del agente Terraform Cloud. La siguiente captura de pantalla muestra los detalles de configuración del agente Terraform.



Puede actualizar cualquier propiedad Agente de Terraform. Si el objetivo está en el estado **no conectado** y nunca ha estado en el estado **conectado**, no se ha generado un token para el agente Terraform.

Una vez que la validación del agente se realiza correctamente y se genera un token de agente, no podrá volver a configurar la organización ni el grupo de agentes. El despliegue correcto de un agente Terraform se indica mediante un estado de **conectado**.

Después de haber activado y reivindicado la integración de Terraform Cloud, puede implementar uno o más agentes de Terraform Cloud en Cisco Intersight Assist. El agente de Terraform Cloud se modela como un objetivo secundario del destino de Terraform Cloud. Cuando reclama el objetivo de agente, verá un mensaje para indicar que la reclamación de destino está en curso.

Después de unos segundos, el destino se mueve al estado **conectado**, y la plataforma Intersight enruta los paquetes HTTPS desde el agente hasta la puerta de enlace de Terraform Cloud.

Su agente Terraform debe ser reclamado correctamente y debe aparecer en los destinos como **conectado**.

"Siguiente: Configure el proveedor de servicios de cloud público."

Configure el proveedor de servicios de cloud público

"Anterior: Integración cloud Terraform con el requisito previo de la ICO."

Procedimiento 1: Acceder a Cloud Manager de NetApp

Para acceder a Cloud Manager de NetApp y a otros servicios cloud, debe registrarse en "Cloud Central de NetApp".



Para configurar espacios de trabajo y usuarios en la cuenta de Cloud Central, haga clic en "aquí".

Procedimiento 2: Despliegue del conector

Para implementar Connector en Google Cloud, consulte este tema "enlace".

"Siguiente: Puesta en marcha automatizada del almacenamiento de NetApp en el cloud híbrido."

Puesta en marcha automatizada del almacenamiento de NetApp en el cloud híbrido

"Anterior: Configure el proveedor de servicios de cloud público."

Google Cloud

Primero debe habilitar las API y crear una cuenta de servicio que proporcione a Cloud Manager permisos para implementar y gestionar sistemas de Cloud Volumes ONTAP que se encuentren en el mismo proyecto que el conector o en proyectos diferentes.

Antes de implementar un conector en un proyecto de Google Cloud, asegúrese de que el conector no se ejecuta en sus instalaciones o en un proveedor de cloud diferente.

Debe haber dos conjuntos de permisos antes de implementar un conector directamente desde Cloud Manager:

- Necesita implementar Connector con una cuenta de Google que tenga permisos para iniciar la instancia de Connector VM desde Cloud Manager.
- Al implementar Connector, se le solicita que seleccione la instancia de la máquina virtual. Cloud Manager obtiene permisos de la cuenta de servicio para crear y gestionar sistemas de Cloud Volumes ONTAP en su nombre. Los permisos se proporcionan agregando una función personalizada a la cuenta de servicio.debe configurar dos archivos YAML que incluyan los permisos necesarios para el usuario y la cuenta de servicio. Aprenda a usar "Los archivos YAML para configurar permisos" aquí.

Consulte "este vídeo detallado" para todos los requisitos previos requeridos.

Modos de puesta en marcha y arquitectura de Cloud Volumes ONTAP

Cloud Volumes ONTAP está disponible en Google Cloud como sistema de un único nodo y como par de nodos de alta disponibilidad. En función de los requisitos, podemos elegir el modo de puesta en marcha de Cloud Volumes ONTAP. No se admite la actualización de un sistema de un solo nodo a un par de alta disponibilidad. Si desea cambiar entre un sistema de un solo nodo y un par de alta disponibilidad, debe poner en marcha un sistema nuevo y replicar datos desde el sistema existente al nuevo sistema.

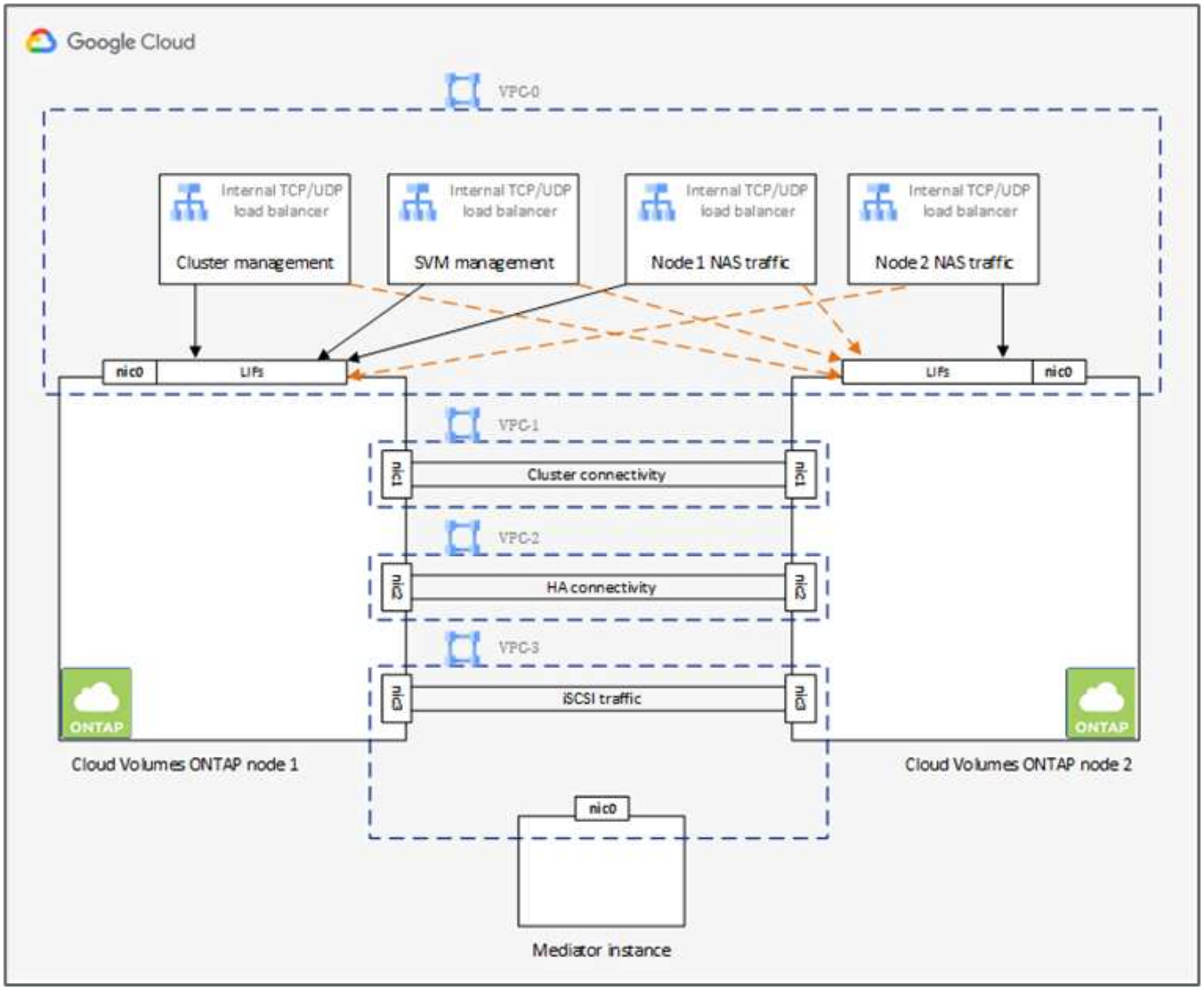
Cloud Volumes ONTAP de alta disponibilidad en Google Cloud

Google Cloud permite la puesta en marcha de recursos entre varias regiones geográficas y varias zonas dentro de una región. La puesta en marcha de alta disponibilidad se compone de dos nodos ONTAP que utilizan potentes tipos de máquinas n1 estándar o n2 disponibles en Google Cloud. Los datos se replican de forma síncrona entre los dos nodos de Cloud Volumes ONTAP para proporcionar disponibilidad en caso de fallo. Para la implementación DE ALTA DISPONIBILIDAD de Cloud Volumes ONTAP se necesitan cuatro PCs y una subred privada en cada VPC. Las subredes de las cuatro VPC deben abasterse con rangos CIDR no superpuestos.

Las cuatro VPC se utilizan con los siguientes fines:

- VPC 0 permite la comunicación entrante hacia los nodos de datos y Cloud Volumes ONTAP.
- VPC 1 proporciona conectividad de clúster entre los nodos de Cloud Volumes ONTAP.
- VPC 2 permite la replicación de RAM no volátil (NVRAM) entre nodos.
- VPC 3 se utiliza para la conectividad a la instancia de mediador de alta disponibilidad y el tráfico de replicación de disco para las recompilaciones de nodos.

La siguiente imagen muestra una Cloud Volumes ONTAP de alta disponibilidad en Gogle Cloud.



Para obtener más información, consulte "este enlace".

Para conocer los requisitos de red de Cloud Volumes ONTAP en Google Cloud, consulte "este enlace".

Para obtener más información sobre la organización en niveles de los datos, consulte "este enlace".

Configure los requisitos previos del entorno

La creación automatizada de clústeres de Cloud Volumes ONTAP, la configuración de SnapMirror entre un volumen en las instalaciones y un volumen de cloud, la creación de un volumen de cloud, etc. se realizan mediante la configuración de Terraform. Estas configuraciones de Terraform se alojan en una cuenta de Terraform Cloud for Business. Con InterSight Cloud Orchestrator, se organizan tareas como crear un espacio de trabajo en una cuenta de Terraform Cloud para Business, agregar todas las variables necesarias al espacio de trabajo, ejecutar un plan de Terraform, etc.

Para estas tareas de automatización y orquestación, se requieren algunos requisitos y datos, como se describe en las siguientes secciones.

Repositorio de GitHub

Necesita una cuenta de GitHub para alojar su código Terraform. Intersight Orchestrator crea un nuevo espacio de trabajo en la cuenta Terraform Cloud para Business. Este espacio de trabajo se configura con un flujo de trabajo de control de versiones. Con este fin, debe mantener la configuración de Terraform en un repositorio de GitHub y proporcionarla como entrada mientras crea el espacio de trabajo.

"Este enlace de GitHub" Proporciona la configuración de Terraform con varios recursos. Puede bifurcar este repositorio y hacer una copia en su cuenta de GitHub.

En este repositorio, `provider.tf` Tiene la definición para el proveedor de Terraform requerido. Se utiliza el proveedor de terraformar para NetApp Cloud Manager.

`variables.tf` tiene todas las declaraciones de variables. El valor de estas variables se introduce como entrada de flujo de trabajo de Intersight Cloud Orchestrator. Esto proporciona una forma cómoda de pasar valores a un área de trabajo y ejecutar la configuración de Terraform.

`resources.tf` Define los diversos recursos necesarios para añadir una ONTAP en las instalaciones al entorno de trabajo, crear un clúster Cloud Volumes ONTAP de un único nodo en Google Cloud, establecer una relación de SnapMirror entre las instalaciones y Cloud Volumes ONTAP, crear un volumen de cloud en Cloud Volumes ONTAP, etc.

En este repositorio:

- `provider.tf` Tiene Cloud Manager de NetApp como definición para el proveedor de Terraform necesario.
- `variables.tf` Tiene las declaraciones de variable que se utilizan como entrada para el flujo de trabajo de Intersight Cloud Orchestrator. Esto proporciona una forma cómoda de pasar valores al espacio de trabajo y ejecutar la configuración de Terraform.
- `resources.tf` Define varios recursos para añadir una ONTAP en las instalaciones al entorno de trabajo, crear un clúster Cloud Volumes ONTAP de un solo nodo en Google Cloud, establecer una relación de SnapMirror entre las instalaciones y Cloud Volumes ONTAP, crear un volumen de cloud en Cloud Volumes ONTAP, etc.

Puede añadir un bloque de recursos adicional para crear varios volúmenes en Cloud Volumes ONTAP o usar o. `for_each` Construcciones de terraformar.

Para conectar espacios de trabajo Terraform, módulos y conjuntos de políticas a repositorios de git que contengan configuraciones de Terraform, Terraform Cloud necesita acceso a su repo de GitHub.

Agregue un cliente y el identificador de token de OAuth del cliente se utiliza como una de las entradas de flujo de trabajo de Intersight Cloud Orchestrator.

1. Inicie sesión en su cuenta de Terraform Cloud for Business. Vaya a **Configuración > proveedores**.
2. Haga clic en **Agregar un proveedor de VCS**.
3. Seleccione su versión.
4. Siga los pasos que se indican en **Configurar proveedor**.
5. Verá el cliente agregado en **proveedores VCS**. Anote el identificador de token de OAuth.

Actualice el token de operaciones de la API de Cloud Manager de NetApp

Además de la interfaz de navegador web, Cloud Manager tiene una API REST que proporciona a los desarrolladores de software acceso directo a la funcionalidad de Cloud Manager a través de la interfaz de SaaS. El servicio Cloud Manager consta de varios componentes distintos que forman conjuntamente una plataforma de desarrollo extensible. El token de actualización permite generar tokens de acceso que agrega al encabezado autorización para cada llamada de API.

Sin llamar a una API directamente, el proveedor de netapp-cloudManager usa un token de actualización y convierte los recursos de Terraform en llamadas API correspondientes. Debe generar un token de actualización para las operaciones de la API de Cloud Manager de NetApp a partir de "Cloud Central de NetApp".

Necesita el ID de cliente de Cloud Manager Connector para crear recursos en Cloud Manager, como crear un clúster de Cloud Volumes ONTAP, configurar SnapMirror, etc.

1. Inicie sesión en Cloud Manager: "https://cloudmanager.netapp.com/".
2. Haga clic en **conector**.
3. Haga clic en **Administrar conectores**.
4. Haga clic en los tres puntos y copie el ID del conector.

Desarrolle el flujo de trabajo de Cisco Intersight Cloud Orchestrator

Cisco Intersight Cloud Orchestrator está disponible en Cisco Intersight si:

- Ha instalado la licencia de Intersight Premier.
- Es administrador de cuentas, administrador de almacenamiento, administrador de virtualización o administrador de servidores y tiene asignado un mínimo de un servidor.

Diseñador de flujos de trabajo

Workflow Designer ayuda a crear nuevos flujos de trabajo (así como tareas y tipos de datos) y a editar los flujos de trabajo existentes para administrar destinos en Cisco Intersight.

Para iniciar Workflow Designer, vaya a **orquestación > flujos de trabajo**. Un panel muestra los siguientes detalles bajo las fichas **Mis flujos de trabajo**, **flujos de trabajo de muestra** y **todos los flujos de trabajo**:

- Estado de validación
- Estado de la última ejecución

- Principales flujos de trabajo por recuento de ejecución
- Principales categorías de flujo de trabajo
- Número de flujos de trabajo definidos por el sistema
- Principales flujos de trabajo por objetivos

Con la consola, puede crear, editar, clonar o eliminar una pestaña. Para crear su propia ficha de vista personalizada, haga clic en **+**, especifique un nombre y, a continuación, seleccione los parámetros necesarios que se deben mostrar en las columnas, las columnas de etiquetas y los widgets. Puede cambiar el nombre de una ficha si no tiene un icono **Bloquear**.

En el panel se encuentra una lista de tablas de flujos de trabajo que muestran la siguiente información:

- Nombre para mostrar
- Descripción
- Definido por el sistema
- Versión predeterminada
- Ejecuciones
- Estado de la última ejecución
- Estado de validación
- Última actualización
- Organización

La columna acciones le permite realizar las siguientes acciones:

- **Ejecutar.** ejecuta el flujo de trabajo.
- **Historial.** muestra el historial de ejecución del flujo de trabajo.
- **Administrar versiones.** cree y administre versiones para flujos de trabajo.
- **Eliminar.** Eliminar un flujo de trabajo.
- **Reintentar.** Reintentar un flujo de trabajo fallido.

Flujo de trabajo

Cree un flujo de trabajo que consta de los siguientes pasos:

- **Definición de un flujo de trabajo.** especifique el nombre para mostrar, la descripción y otros atributos importantes.
- **Definir entradas de flujo de trabajo y salidas de flujo de trabajo.** especifique qué parámetros de entrada son obligatorios para la ejecución del flujo de trabajo y las salidas generadas en la ejecución correcta
- **Agregar tareas de flujo de trabajo.** Agregue una o más tareas de flujo de trabajo en el Diseñador de flujo de trabajo que sean necesarias para que el flujo de trabajo lleve a cabo su función.
- *Validar el flujo de trabajo. *Validar un flujo de trabajo para asegurarse de que no hay errores al conectar entradas y salidas de tareas.

Crear flujos de trabajo para el almacenamiento FlexPod en las instalaciones

Para configurar un flujo de trabajo para el almacenamiento FlexPod en las instalaciones, consulte "este enlace".

"Siguiente: Flujo de trabajo de recuperación ante desastres."

Flujo de trabajo de recuperación ante desastres

"Anterior: Puesta en marcha automatizada de almacenamiento de NetApp en cloud híbrido."

La secuencia de pasos es la siguiente:

1. Defina el flujo de trabajo.
    - Cree un nombre corto y fácil de usar para el flujo de trabajo, como el flujo de trabajo de recuperación ante desastres.
2. Defina la entrada del flujo de trabajo. Las entradas que tomamos para este flujo de trabajo incluyen las siguientes:
    - Opciones de volumen (nombre de volumen, ruta de montaje)
    - Capacidad de un volumen
    - Centro de datos asociado con el almacén de datos nuevo
    - Clúster en el que se aloja el almacén de datos
    - Nombre para el nuevo almacén de datos que se va a crear en vCenter
    - Escriba y la versión del almacén de datos nuevo
    - Nombre de la organización Terraform
    - Espacio de trabajo Terraform
    - Descripción del espacio de trabajo Terraform
    - Variables (sensibles y no sensibles) necesarias para ejecutar la configuración de Terraform
    - Motivo para iniciar el plan
3. Agregue las tareas del flujo de trabajo.

    Entre las tareas relacionadas con operaciones en FlexPod se incluyen las siguientes:

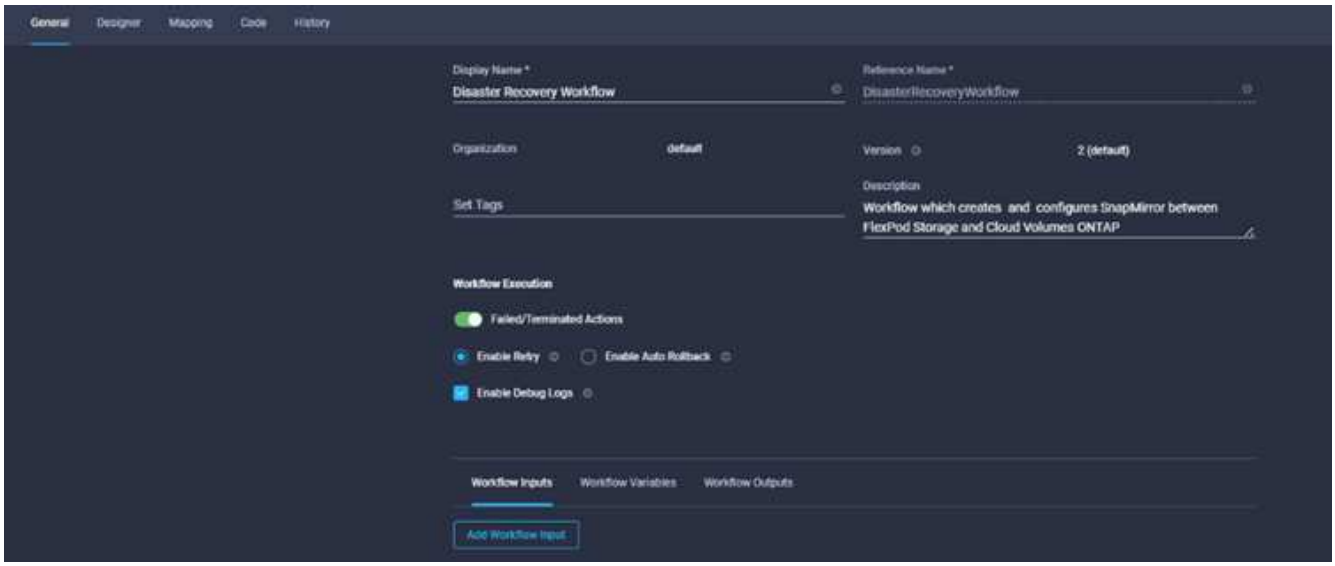
    - Crear volumen en FlexPod.
    - Añada una política de exportación de almacenamiento al volumen creado.
    - Asigne el volumen recién creado a un almacén de datos en VMware vCenter.

      Las tareas relacionadas con la creación del clúster de Cloud Volumes ONTAP:

    - Agregar espacio de trabajo Terraform
    - Agregue variables Terraform
    - Agregue variables sensibles a Terraform
    - Inicie un nuevo plan de Terraform
    - Confirme la ejecución de Terraform
4. Validar el flujo de trabajo.

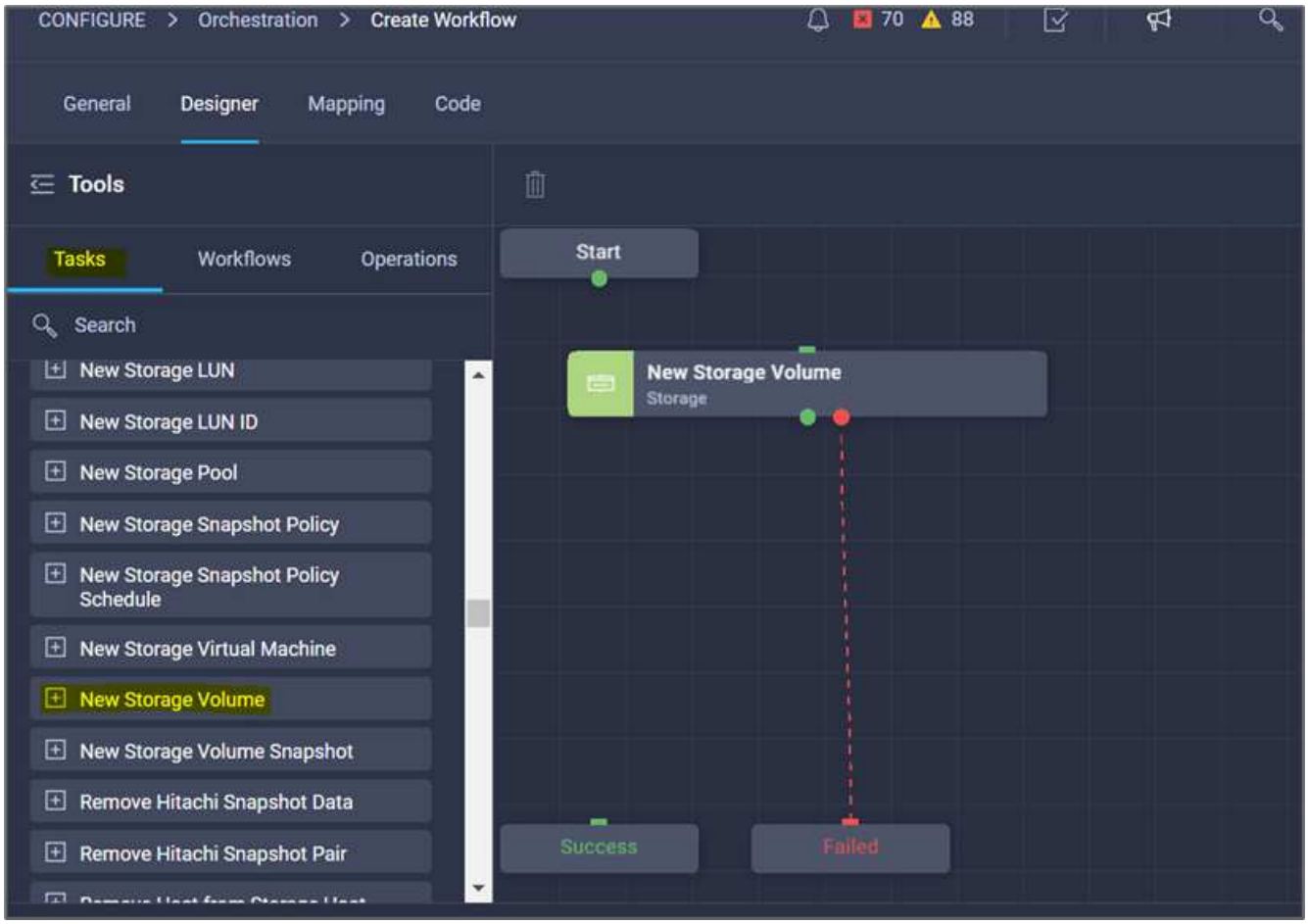
Procedimiento 1: Crear el flujo de trabajo

1. Haga clic en **orquestación** en el panel de navegación de la izquierda y haga clic en **Crear flujo de trabajo**.
2. En la pestaña **General**:
   a. Proporcione el nombre para mostrar (flujo de trabajo de recuperación ante desastres).
   b. Seleccione la organización, establezca etiquetas y proporcione una descripción.
3. Haga clic en Guardar.

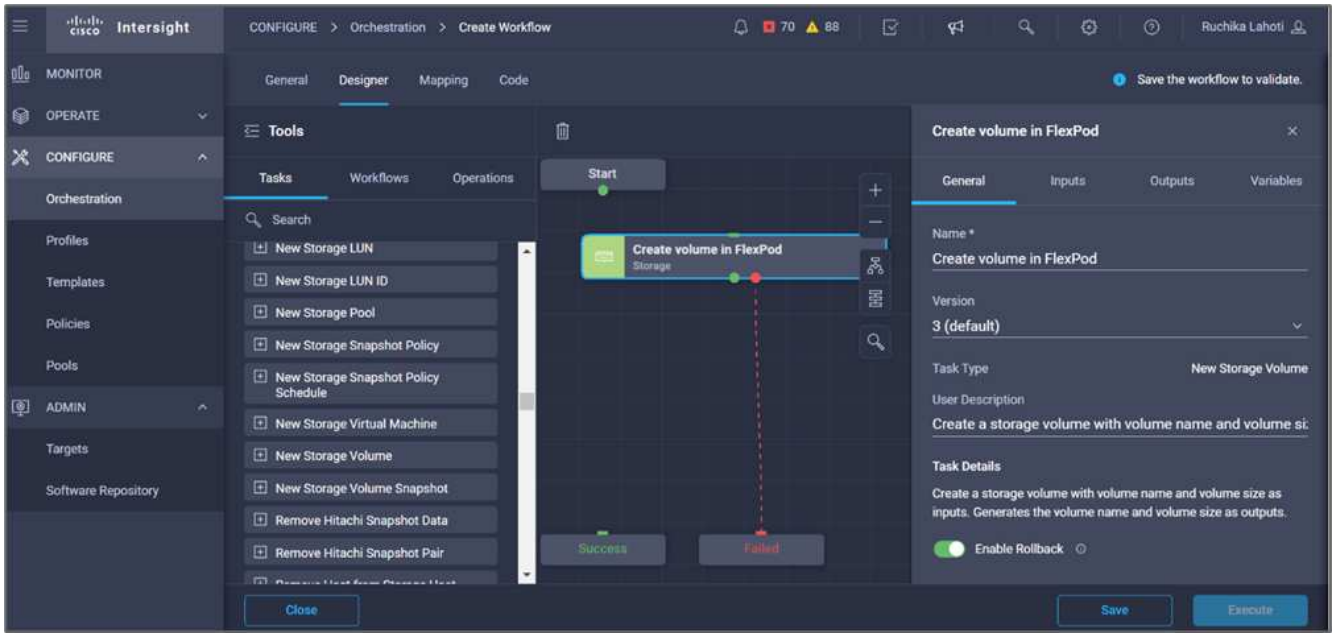


Procedimiento 2. Cree un nuevo volumen en FlexPod

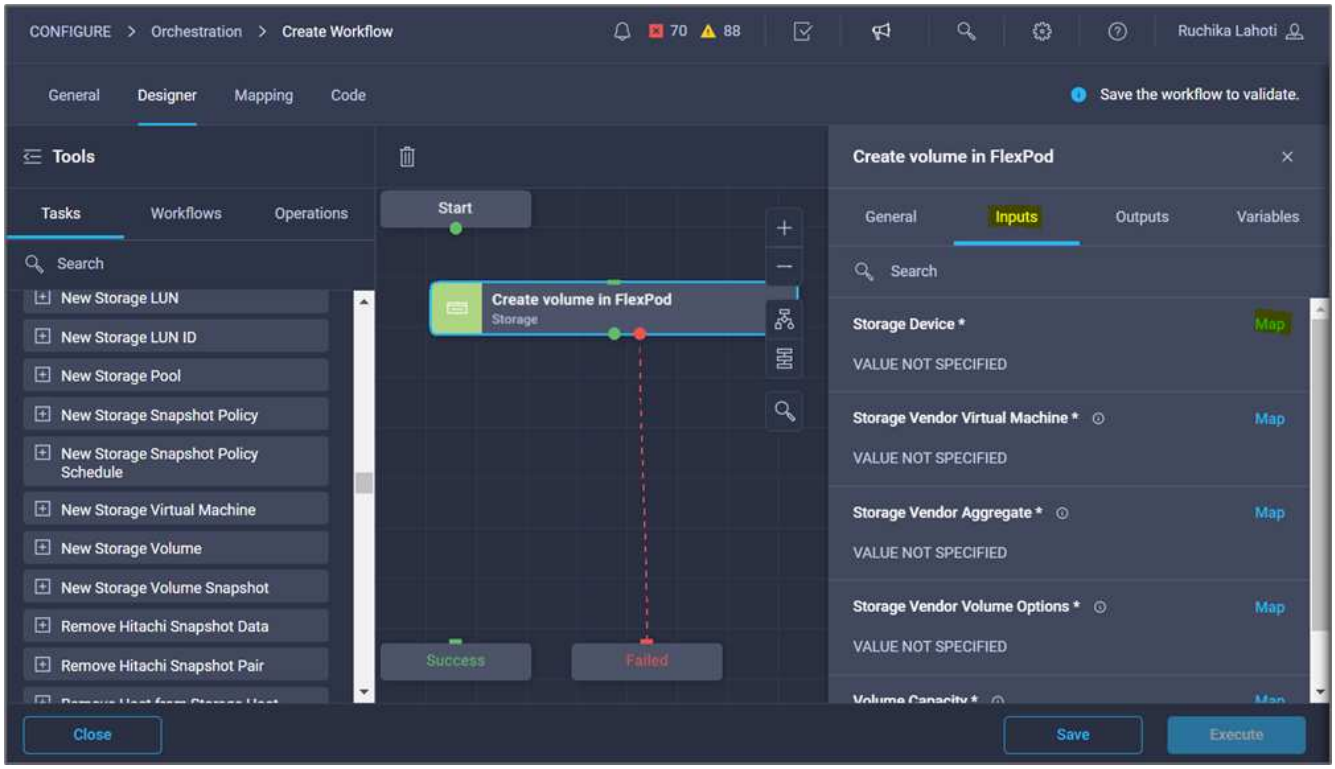
1. Vaya a la ficha **Diseñador** y haga clic en **tareas** en la sección **Herramientas**.
2. Arrastre y suelte la tarea **almacenamiento > Nuevo volumen de almacenamiento** de la sección **Herramientas** en el área **Diseño**.
3. Haga clic en **Nuevo volumen de almacenamiento**.



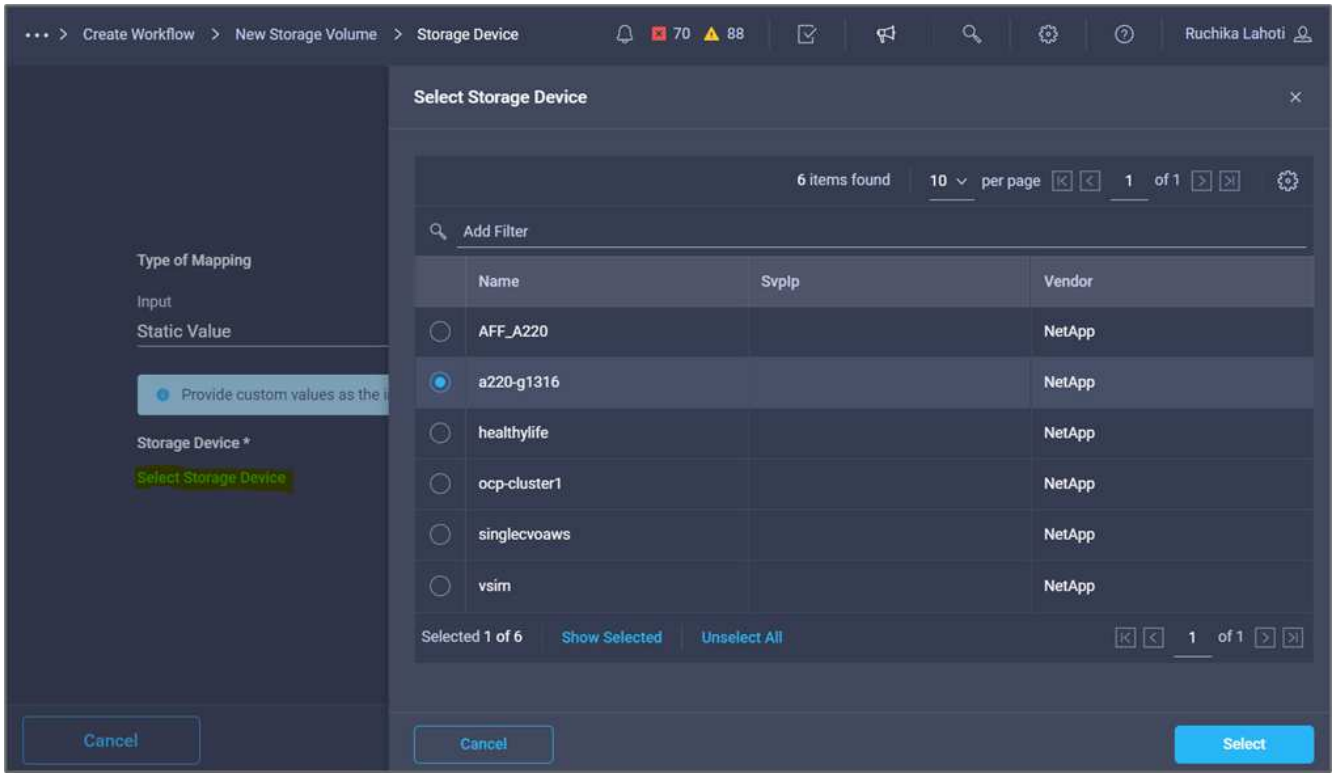
4. En el área **Propiedades de tarea**, haga clic en la ficha **General**. Opcionalmente, puede cambiar el nombre y la descripción de esta tarea. En este ejemplo, el nombre de la tarea es **Crear volumen en FlexPod**.



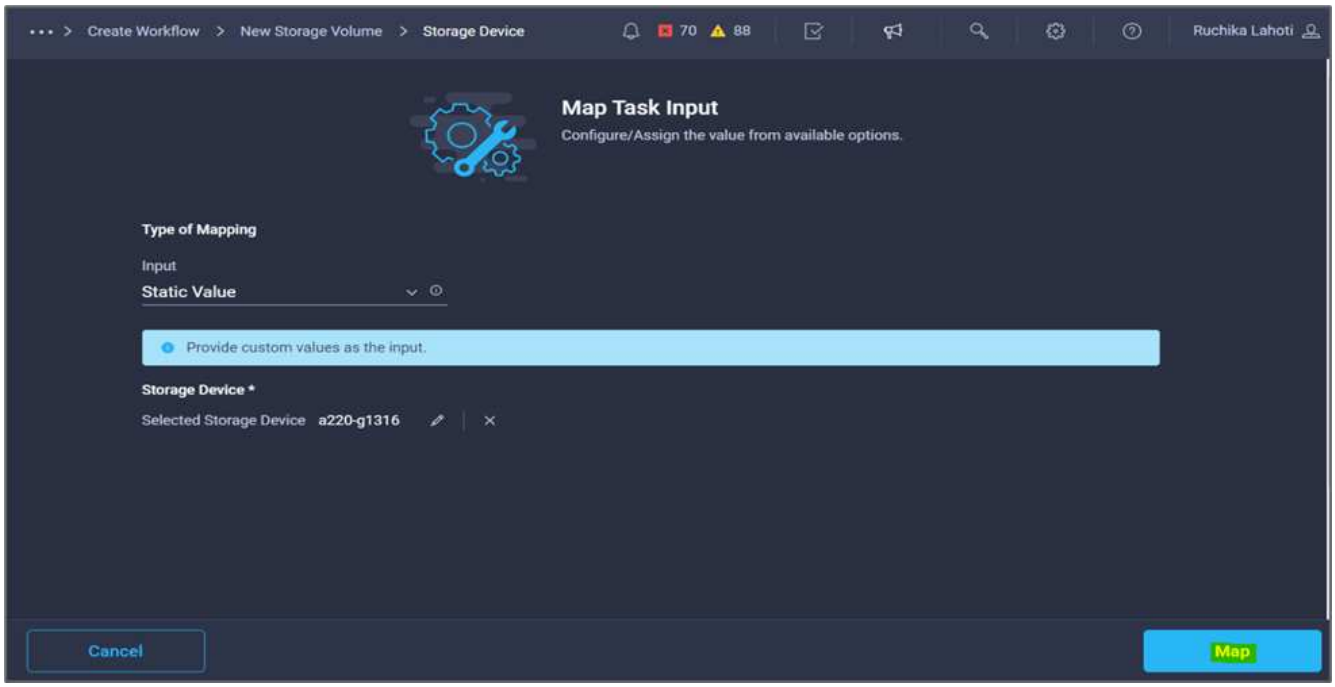
5. En el área **Propiedades de tarea**, haga clic en **Entradas**.
6. Haga clic en **Mapa** en el campo **dispositivo de almacenamiento**.



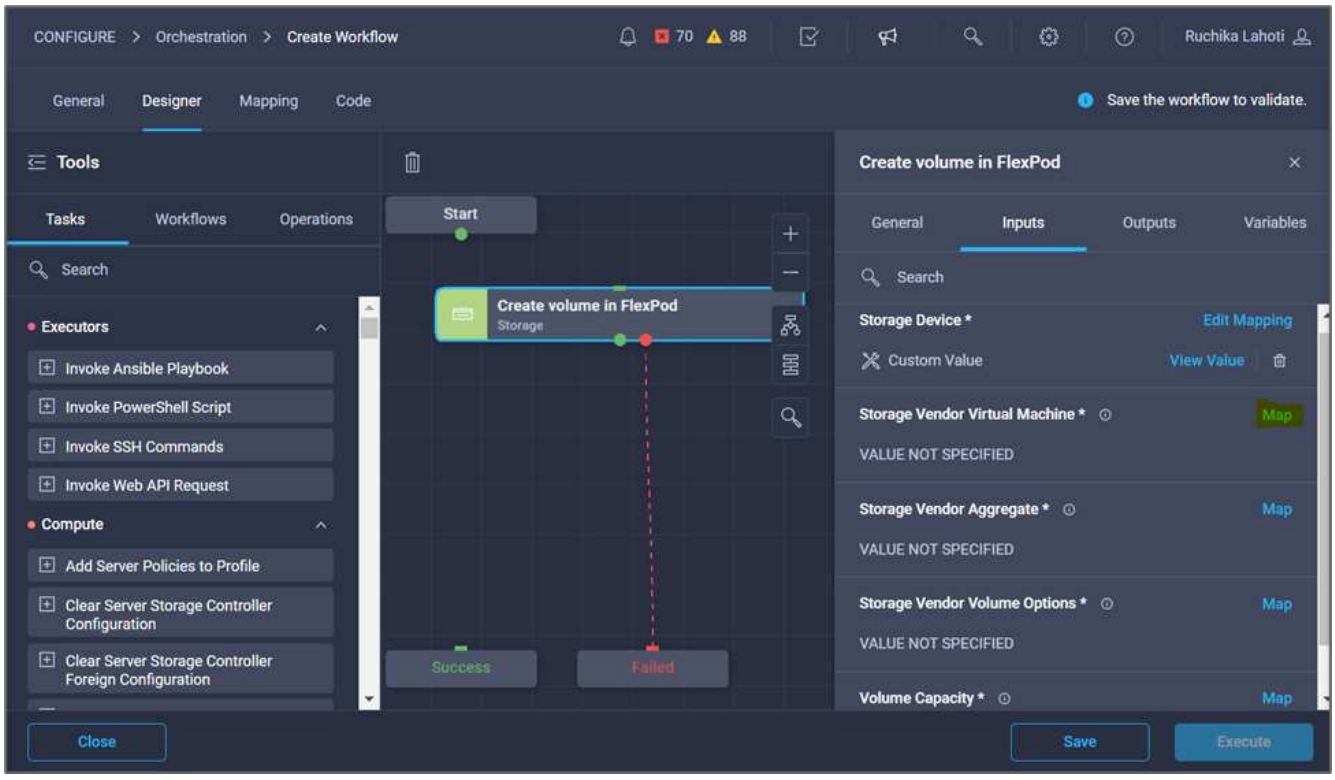
7. Elija **valor estático** y haga clic en **Seleccionar dispositivo de almacenamiento**.
8. Haga clic en el destino de almacenamiento agregado y haga clic en **Seleccionar**.



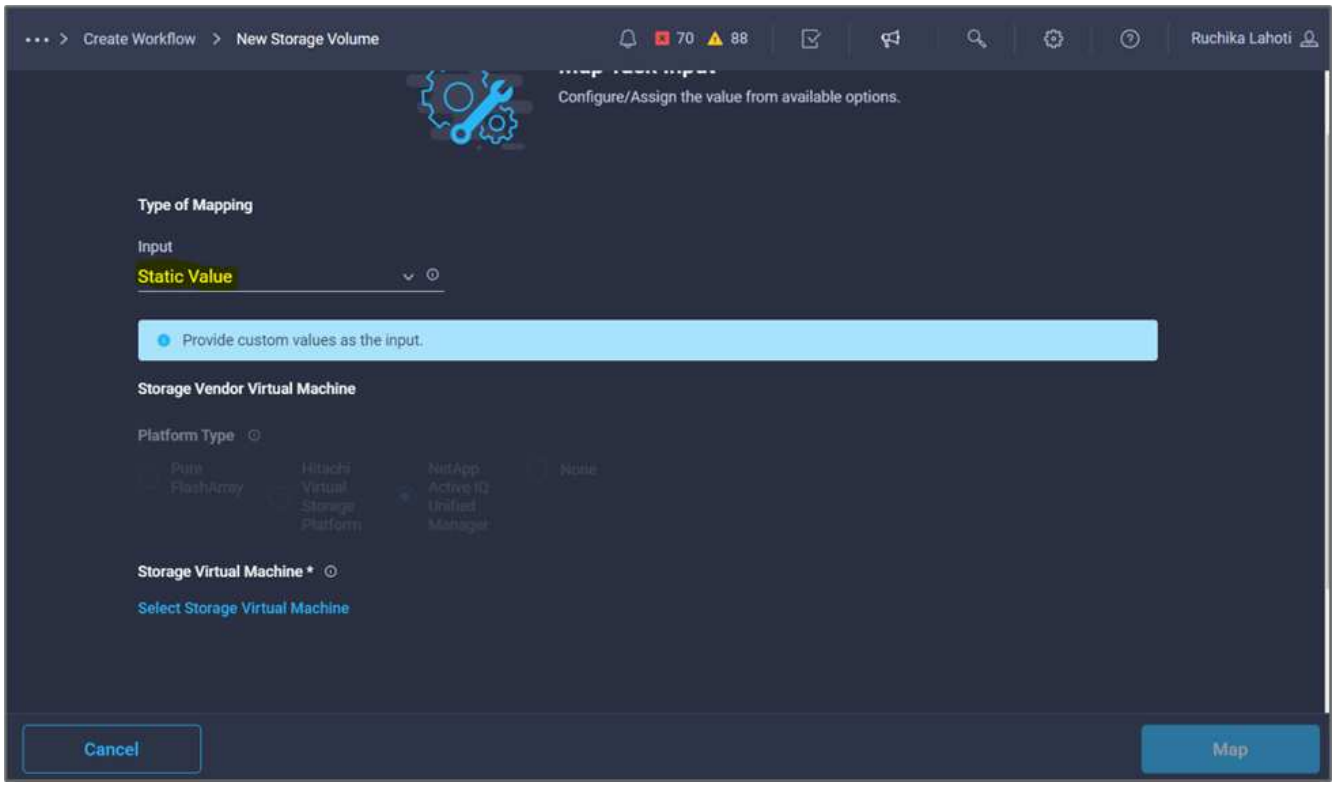
9. Haga clic en **Mapa**.



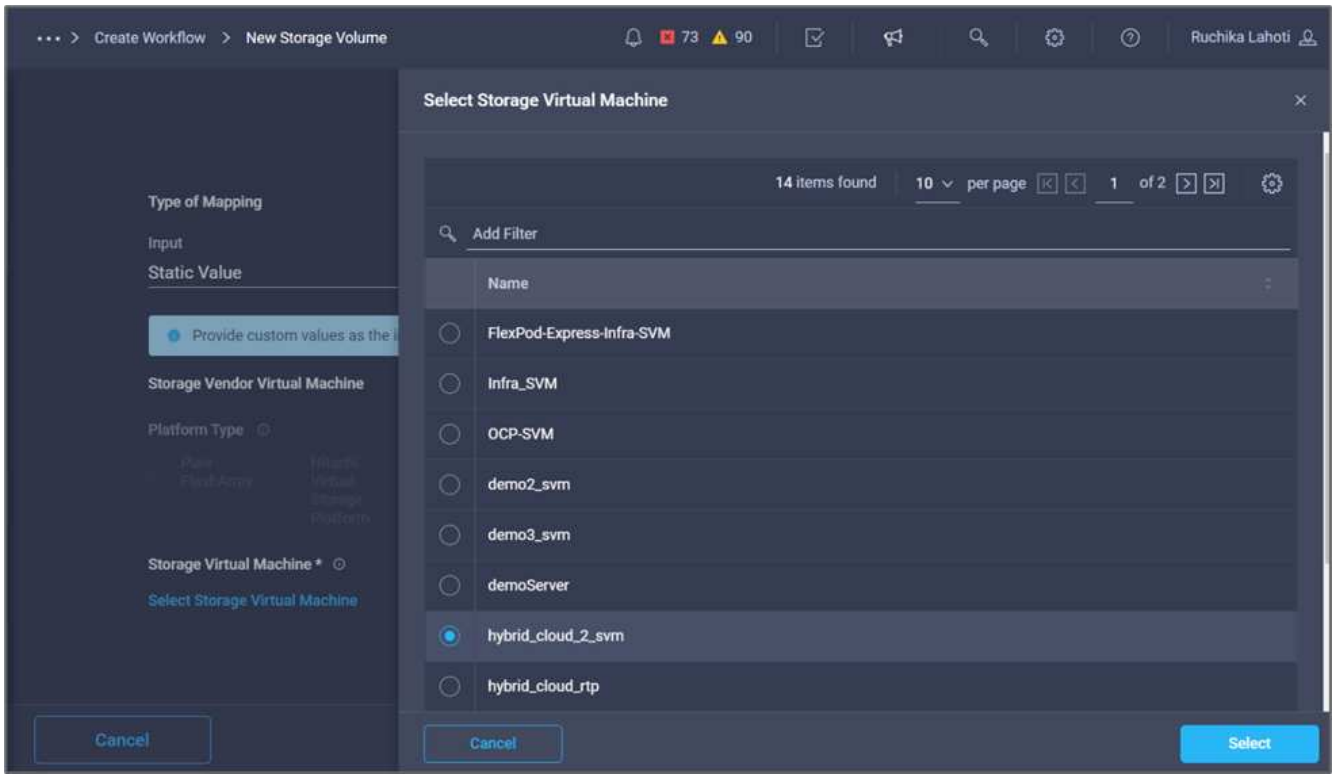
10. Haga clic en **Mapa** en el campo **Storage Vendor Virtual Machine**.



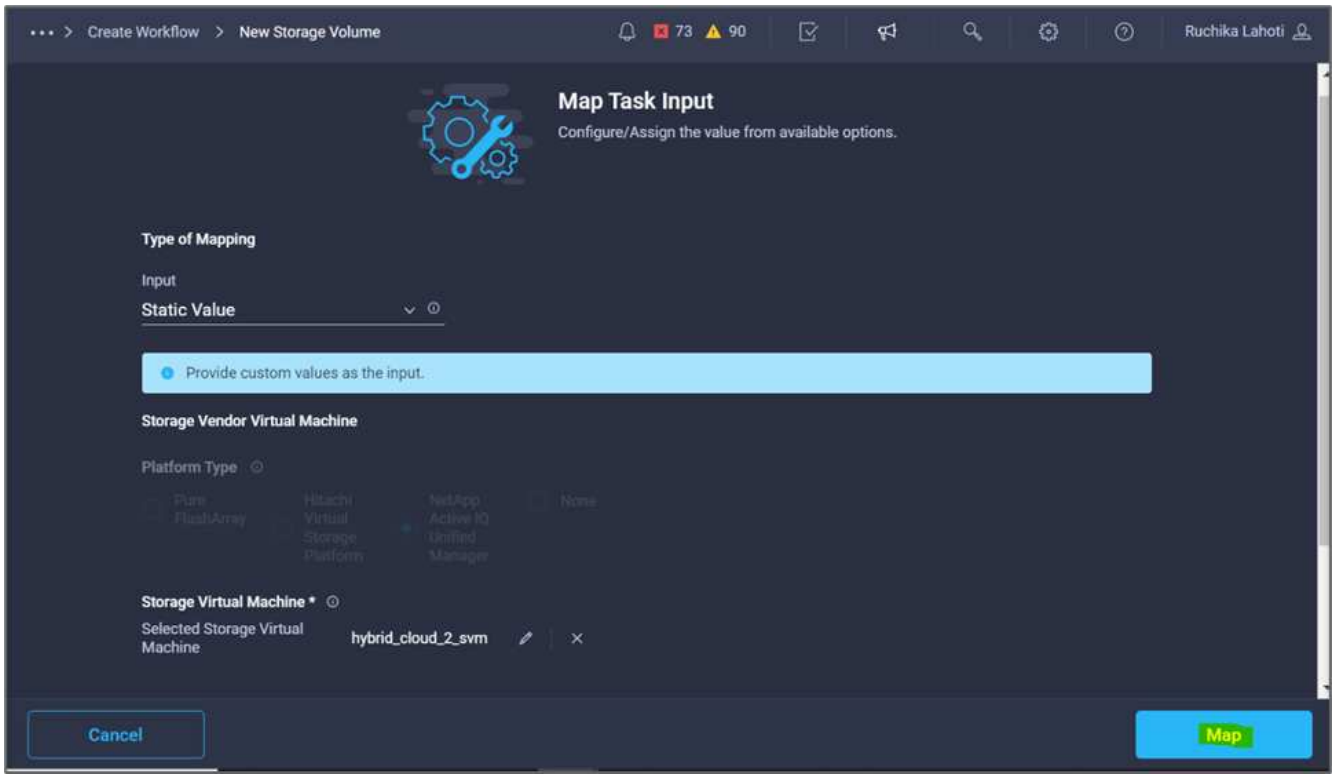
11. Elija **valor estático** y haga clic en **Seleccionar máquina virtual de almacenamiento**.



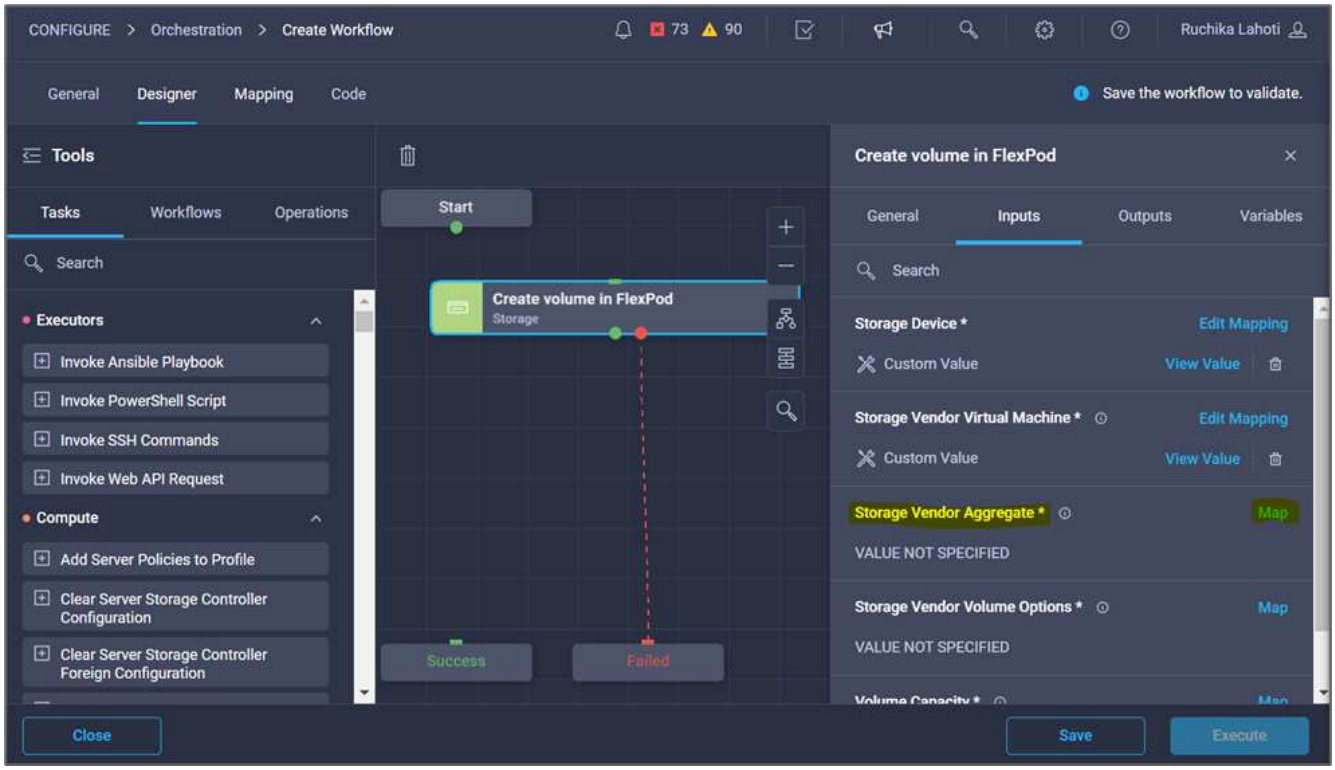
12. Seleccione la máquina virtual de almacenamiento donde se debe crear el volumen y haga clic en **Seleccionar**.



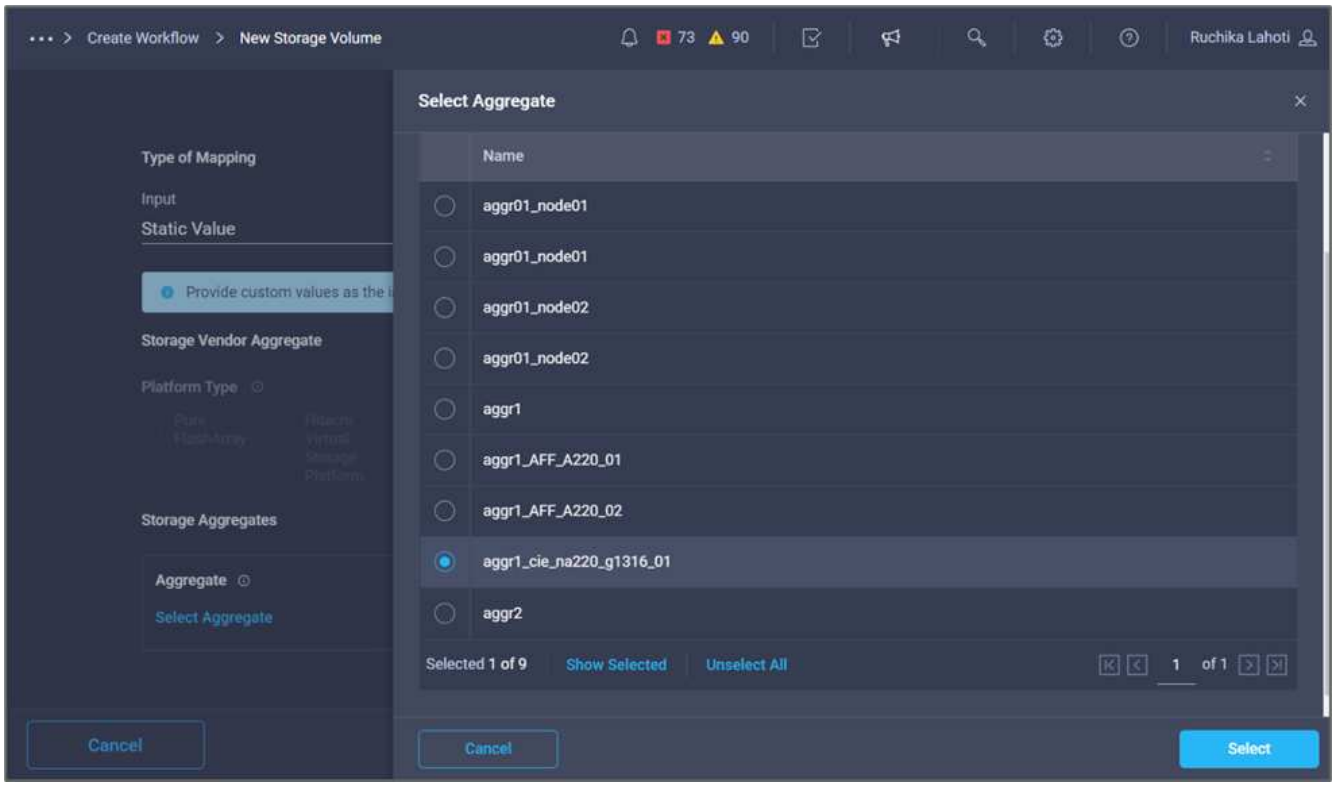
13. Haga clic en **Mapa**.



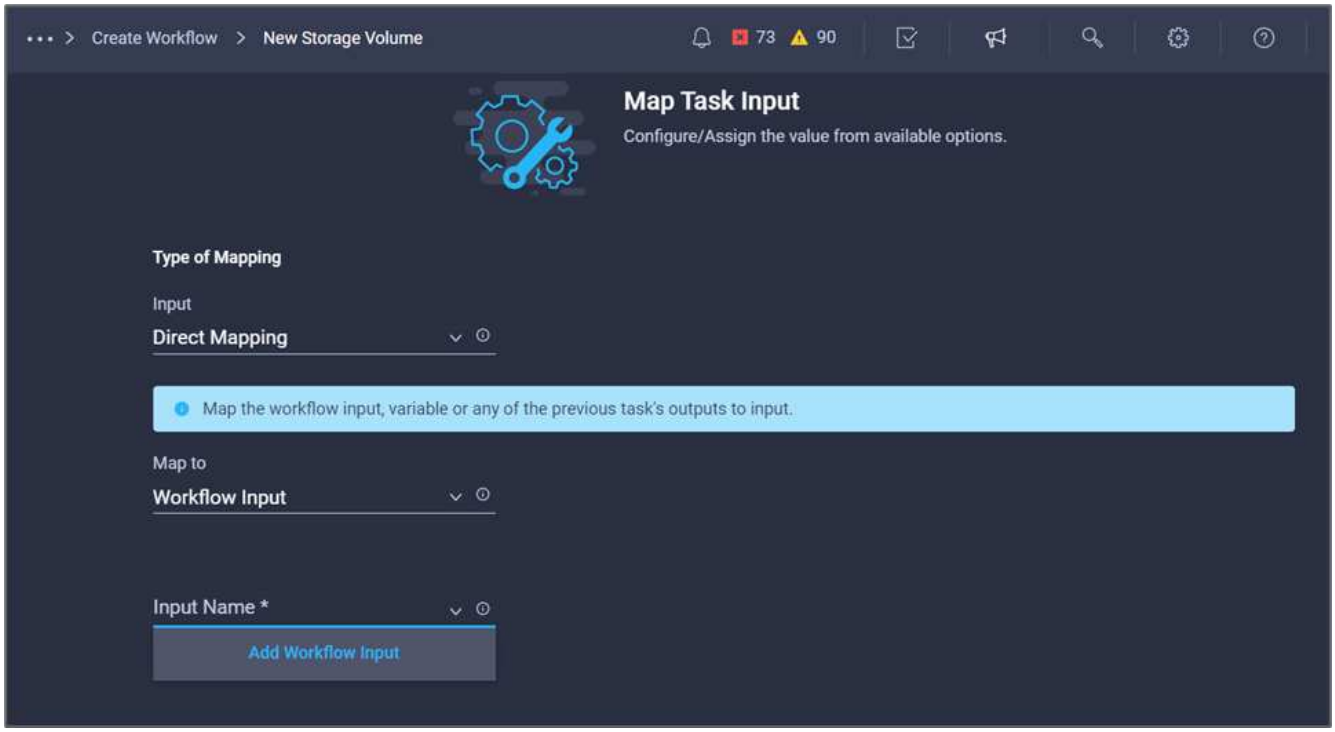
14. Haga clic en **Mapa** en el campo **agregado de proveedores de almacenamiento**.



15. Elija **valor estático** y haga clic en **Seleccionar agregado de almacenamiento**. Seleccione el agregado y haga clic en **Seleccionar**.



16. Haga clic en **Mapa**.
17. Haga clic en **Mapa** en el campo **Opciones de volumen de proveedor de almacenamiento**.
18. Elija **asignación directa** y haga clic en **Entrada de flujo de trabajo**.



19. En el asistente para agregar entrada, lleve a cabo los siguientes pasos:
    a. Proporcione un nombre para mostrar y un nombre de referencia (opcional).
    b. Asegúrese de que **Opciones de volumen de proveedor de almacenamiento** está seleccionada para

Tipo.

c. Haga clic en **establecer valor predeterminado y en Reemplazar**.

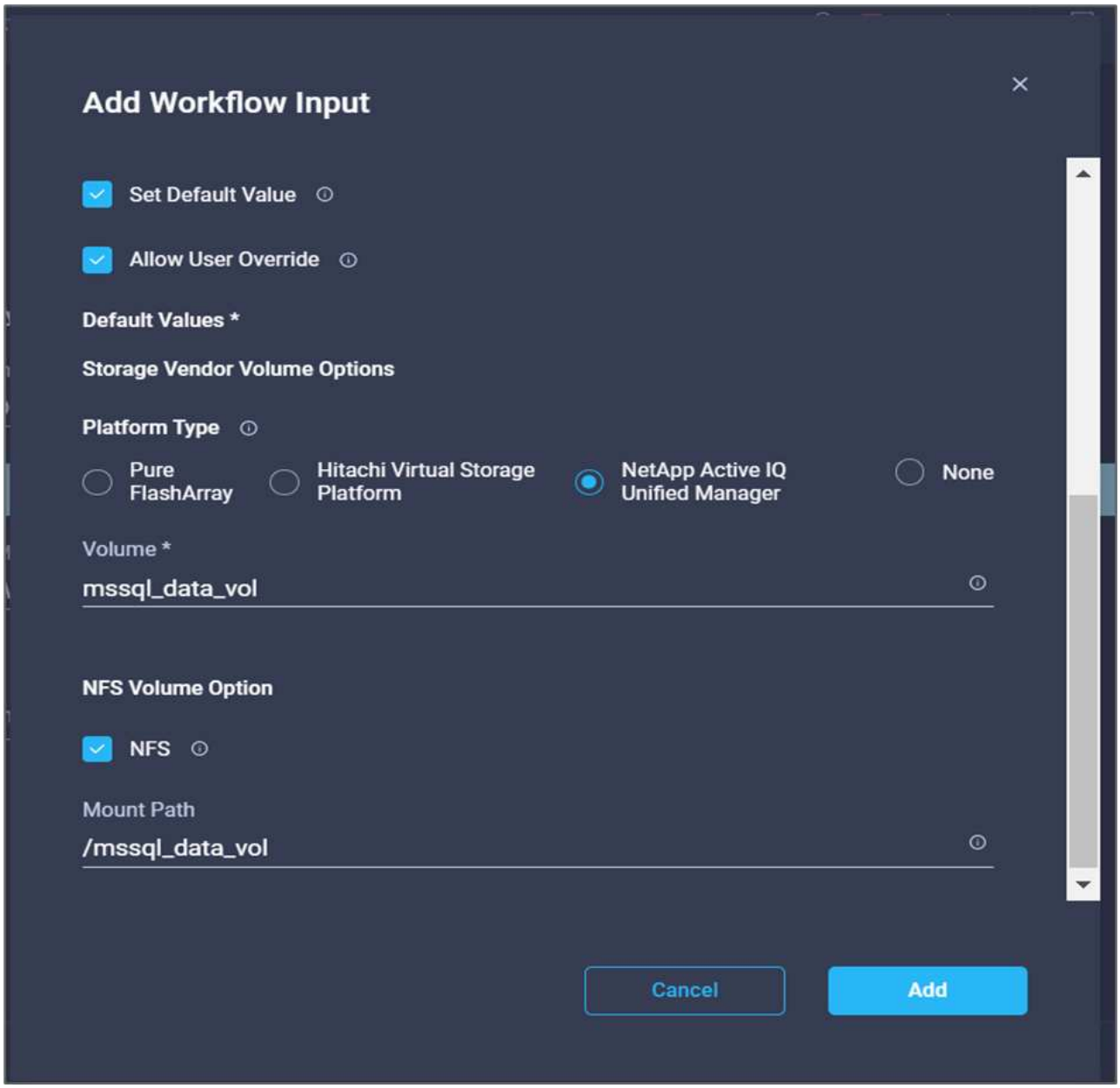
d. Haga clic en **requerido**.

e. Establezca **Tipo de plataforma** en **Active IQ Unified Manager de NetApp**.

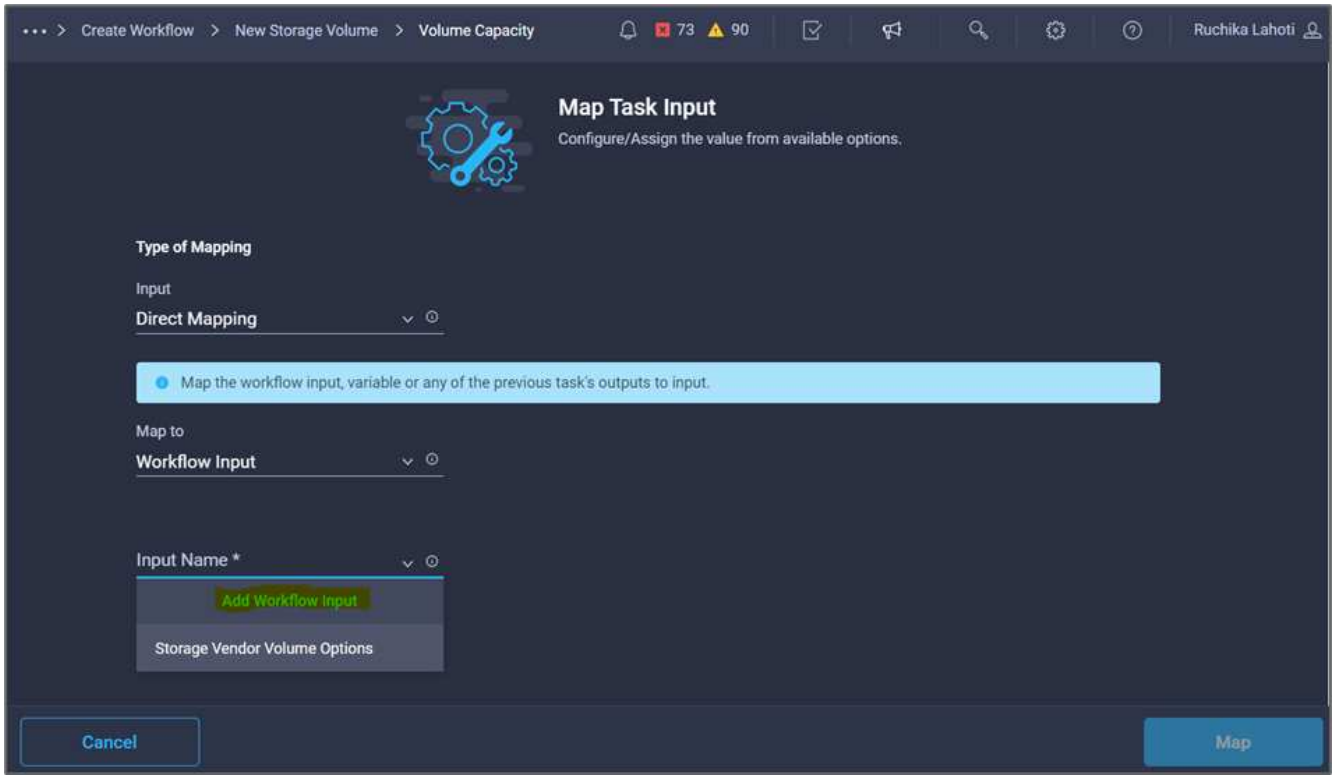
f. Proporcione un valor predeterminado para el volumen creado en **volumen**.

g. Haga clic en **NFS**. Si se establece NFS, se crea un volumen NFS. Si este valor se establece en FALSE, se crea un volumen SAN.

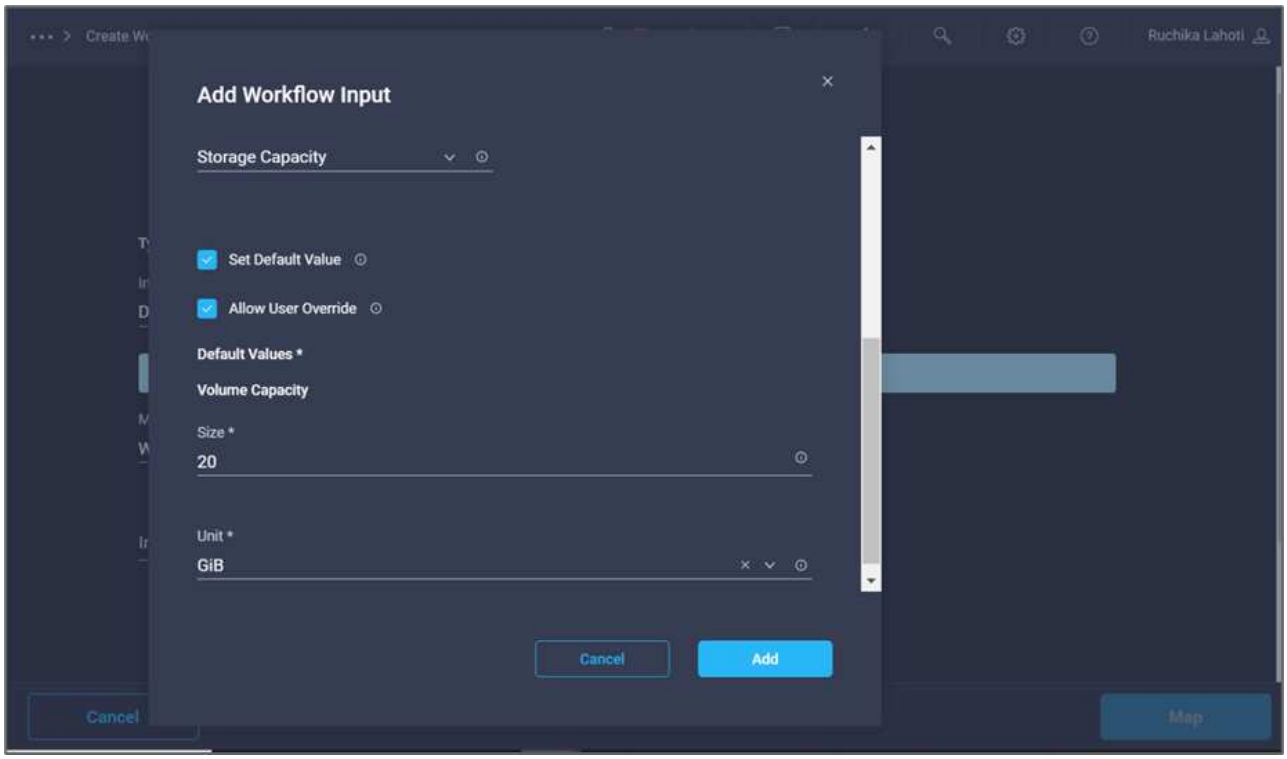
h. Proporcione una ruta de montaje y haga clic en **Agregar**.



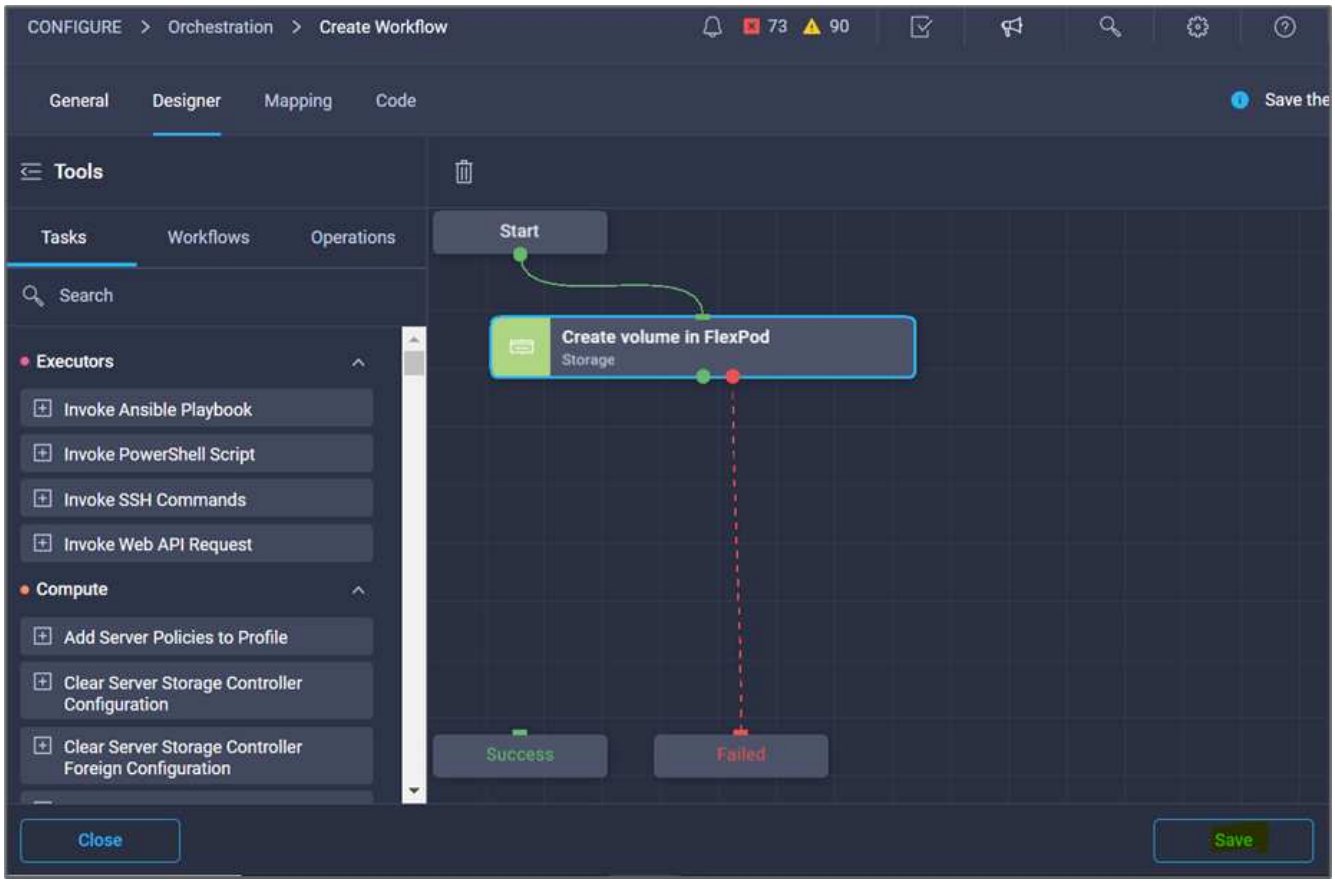
20. Haga clic en **Mapa**.
21. Haga clic en **Mapa** en el campo **capacidad de volumen**.
22. Elija **asignación directa** y haga clic en **Entrada de flujo de trabajo**.
23. Haga clic en **Nombre de entrada** y **Crear entrada de flujo de trabajo**.



24. En el asistente Agregar entrada:
    a. Proporcione un nombre para mostrar y un nombre de referencia (opcional).
    b. Haga clic en **requerido**.
    c. Para **Tipo**, seleccione **capacidad de almacenamiento**.
    d. Haga clic en **establecer valor predeterminado y en Reemplazar**.
    e. Proporcione un valor predeterminado para el tamaño del volumen y la unidad.
    f. Haga clic en **Agregar**.



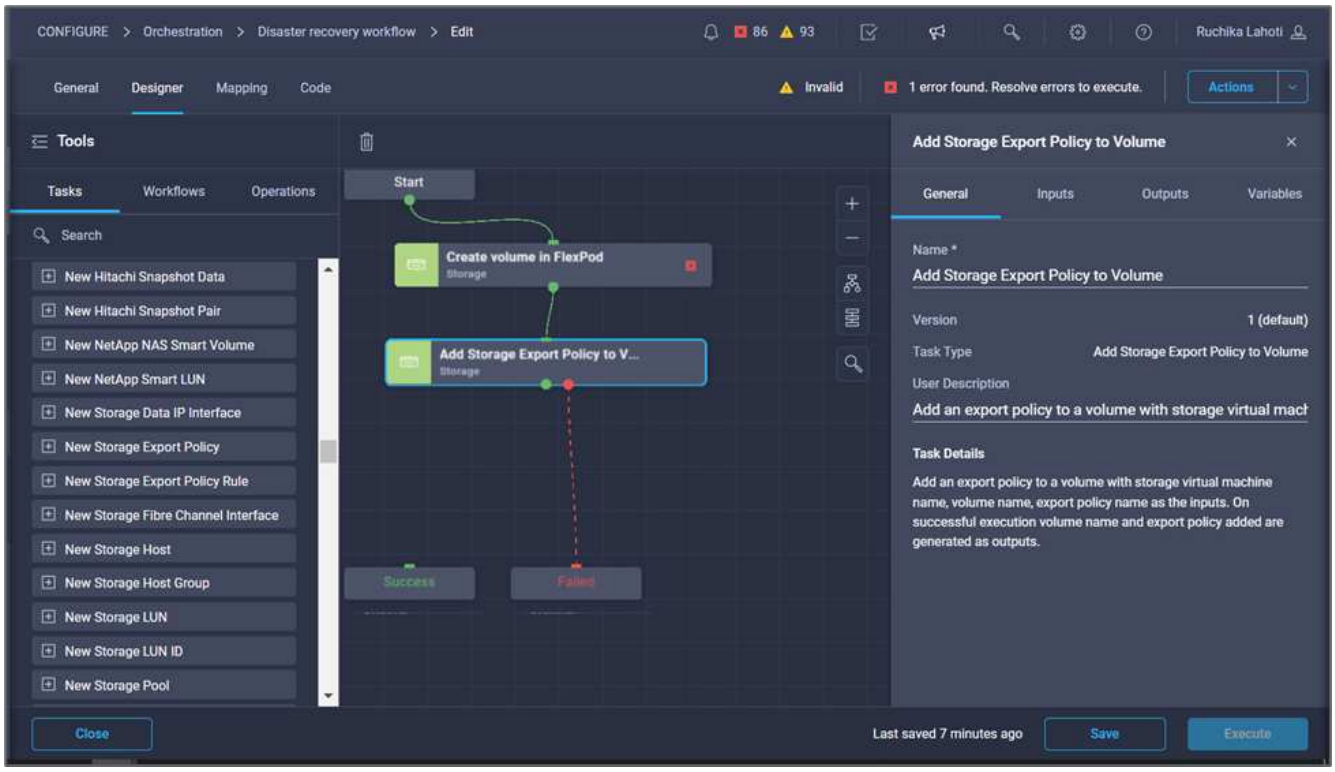
25. Haga clic en **Mapa**.
26. Con conector, cree una conexión entre las tareas **Inicio** y **Crear volumen en FlexPod** y haga clic en **Guardar**.



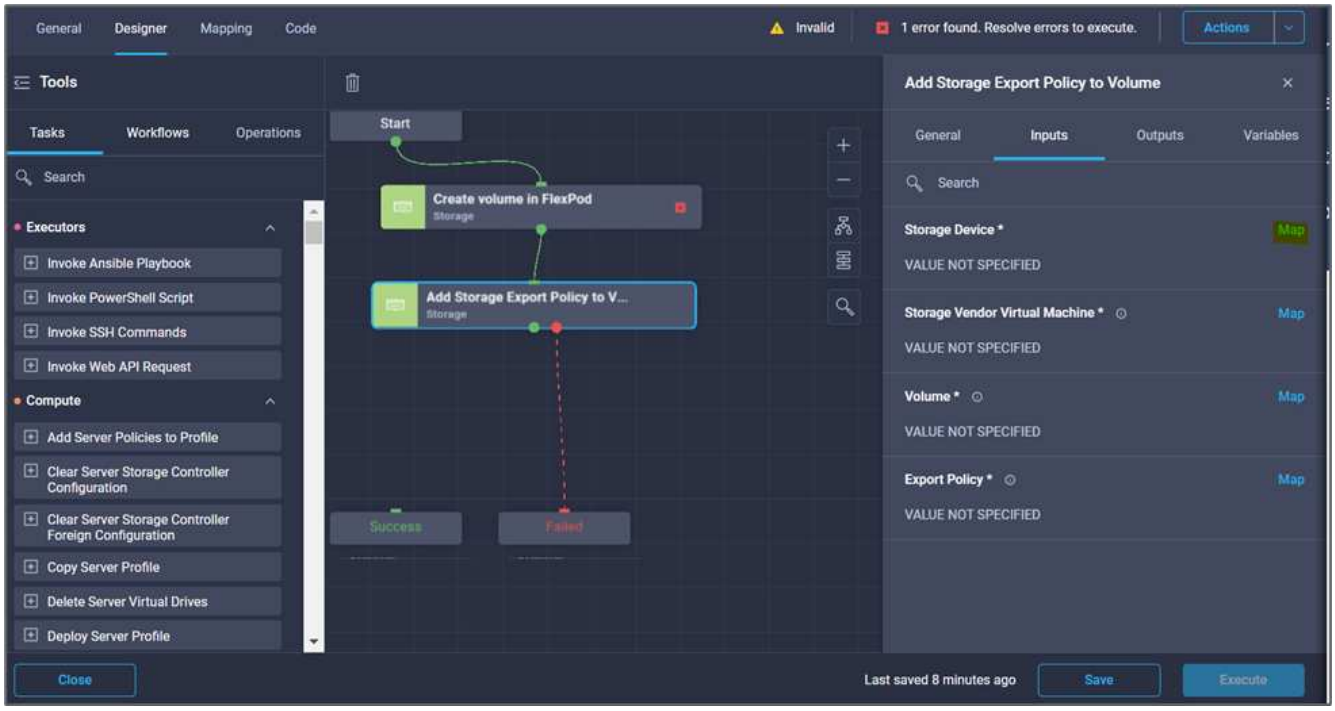
Ignore el error por ahora. Este error se muestra porque no hay conectividad entre las tareas **Crear volumen en FlexPod** y **éxito** que es necesario para especificar la transición correcta.

Procedimiento 3: Añadir la política de exportación de almacenamiento

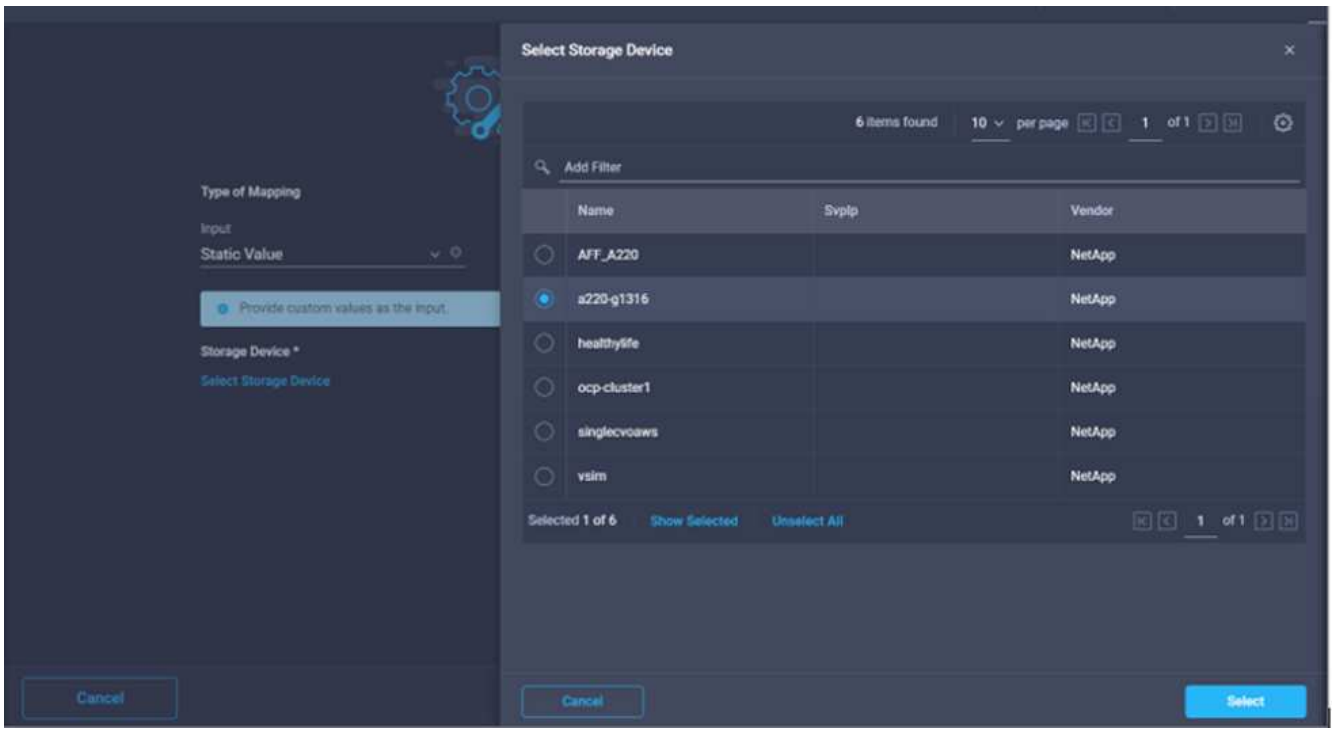
1. Vaya a la ficha **Diseñador** y haga clic en **tareas** en la sección **Herramientas**.
2. Arrastre y suelte la tarea **almacenamiento > Agregar directiva de exportación de almacenamiento al volumen** de la sección **Herramientas** del área **Diseño**.
3. Haga clic en **Agregar directiva de exportación de almacenamiento al volumen**. En el área **Propiedades de tarea**, haga clic en la ficha **General**. Opcionalmente, puede cambiar el nombre y la descripción de esta tarea. En este ejemplo, el nombre de la tarea es Add Storage Export Policy.
4. Utilice conector para establecer una conexión entre las tareas **Crear volumen en FlexPod** y **Agregar directiva de exportación de almacenamiento**. Haga clic en **Guardar**.



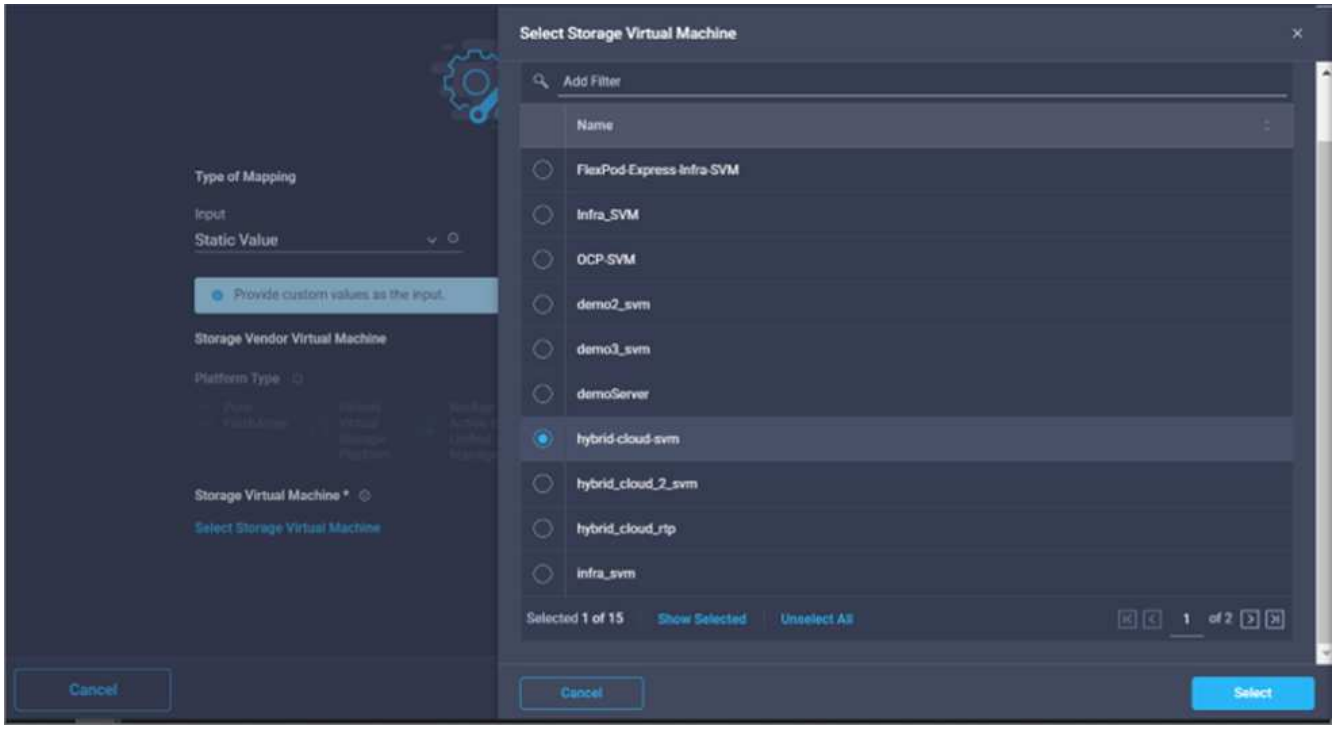
5. En el área **Propiedades de tarea**, haga clic en **Entradas**.
6. Haga clic en **Mapa** en el campo **dispositivo de almacenamiento**.



7. Elija **valor estático** y haga clic en **Seleccionar dispositivo de almacenamiento**. Seleccione el mismo destino de almacenamiento añadido al crear la tarea anterior de crear un nuevo volumen de almacenamiento.
8. Haga clic en **Mapa**.

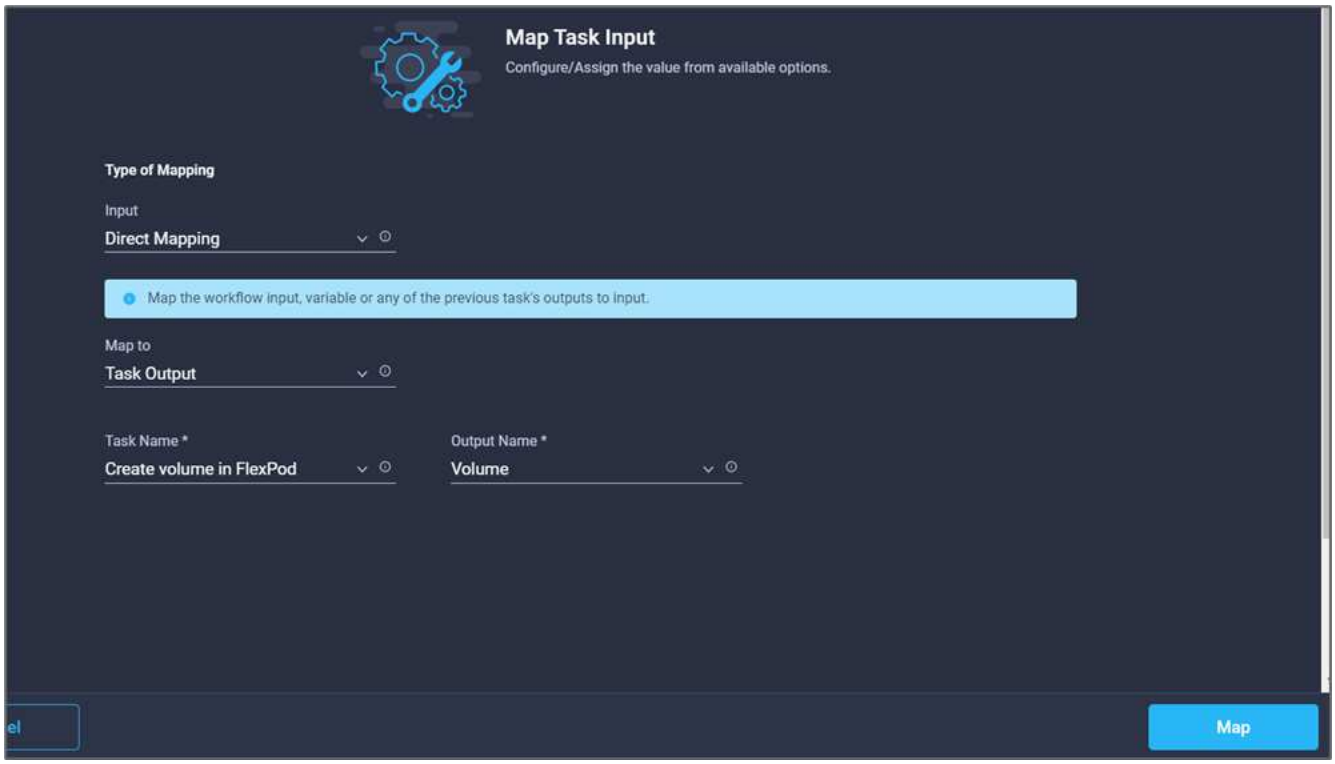


9. Haga clic en **Mapa** en el campo **Storage Vendor Virtual Machine**.
10. Elija **valor estático** y haga clic en **Seleccionar máquina virtual de almacenamiento**. Seleccione la misma máquina virtual de almacenamiento añadida mientras crea la tarea anterior de crear un nuevo volumen de almacenamiento.

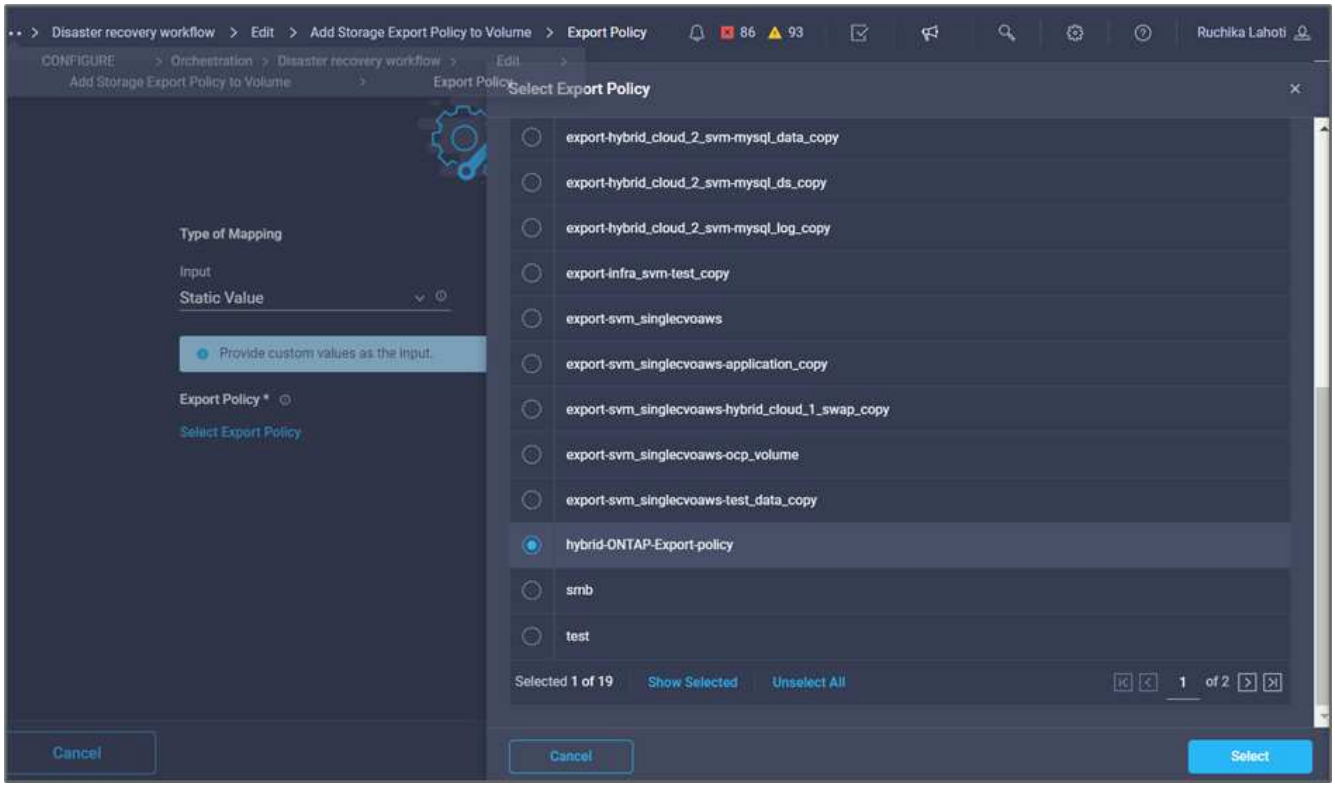


11. Haga clic en **Mapa**.
12. Haga clic en **Mapa** en el campo **volumen**.
13. Haga clic en **Nombre de tarea** y, a continuación, en **Crear volumen en FlexPod**. Haga clic en **Nombre de salida** y, a continuación, en **volumen**.

> En Cisco InterSight Cloud Orchestrator, puede proporcionar el resultado de una tarea anterior como entrada para una nueva tarea. En este ejemplo, los detalles **volumen** se proporcionaron de la tarea **Crear volumen en FlexPod** como entrada para la tarea **Agregar directiva de exportación de almacenamiento**.



14. Haga clic en **Mapa**.
15. Haga clic en **Mapa** en el campo **Política de exportación**.
16. Elija **valor estático** y haga clic en **Seleccionar directiva de exportación**. Seleccione la política de exportación creada.

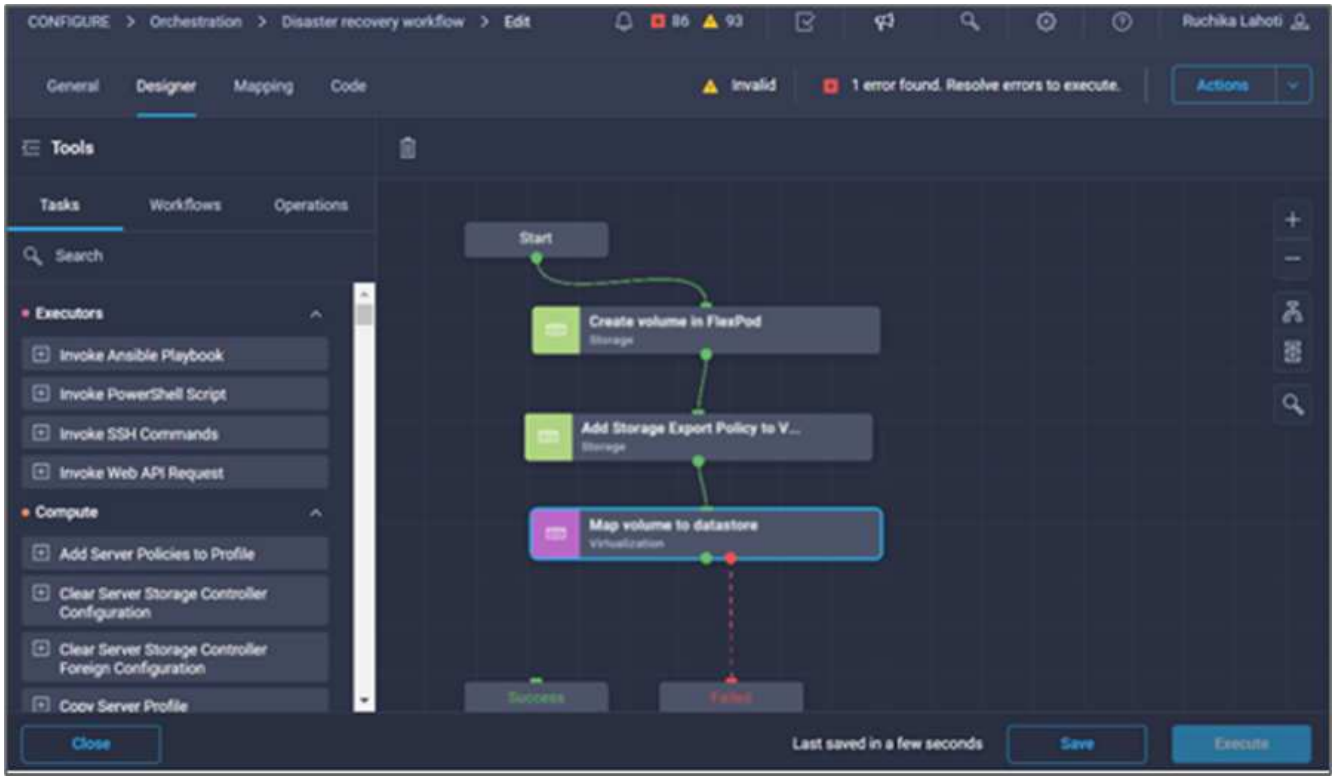


17. Haga clic en **Mapa** y luego en **Guardar**.

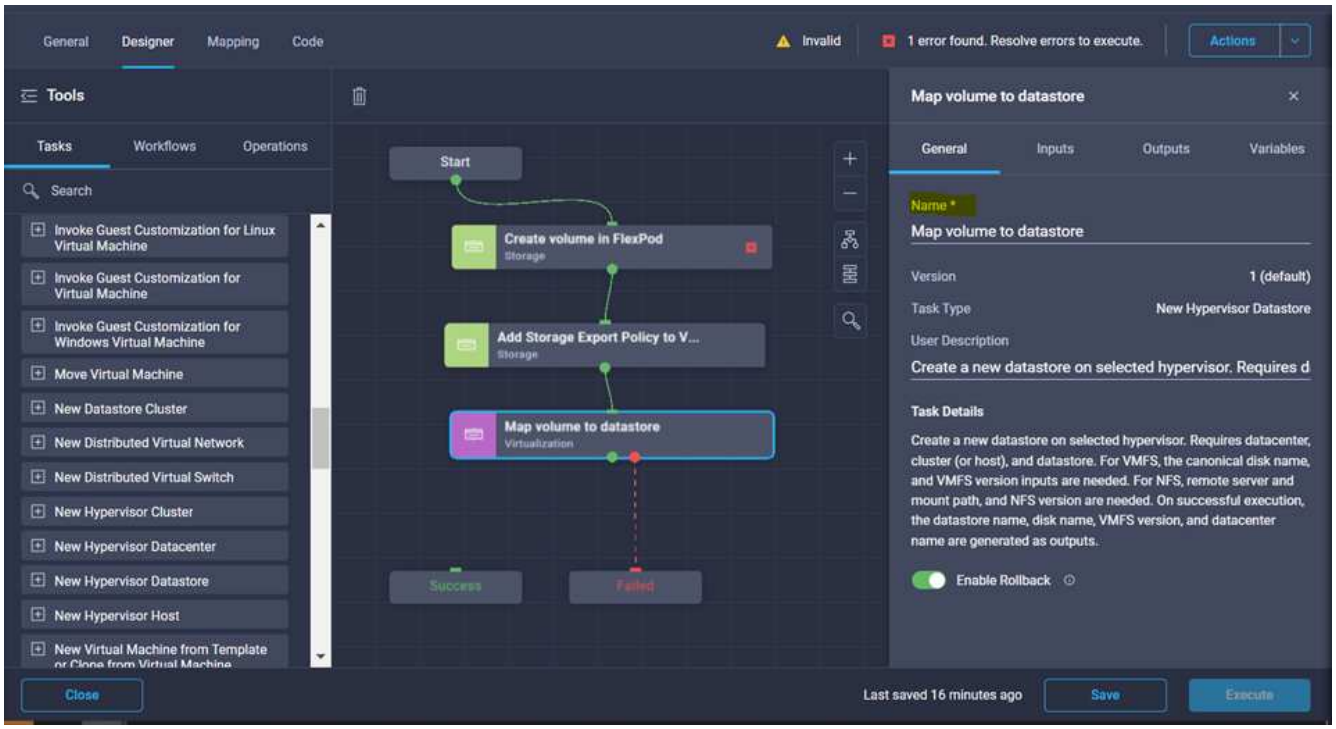
Con esto se completa la adición de una política de exportación al volumen. A continuación, debe crear un nuevo almacén de datos que asigne el volumen creado.

Procedimiento 4: Asignar un volumen de FlexPod a un almacén de datos

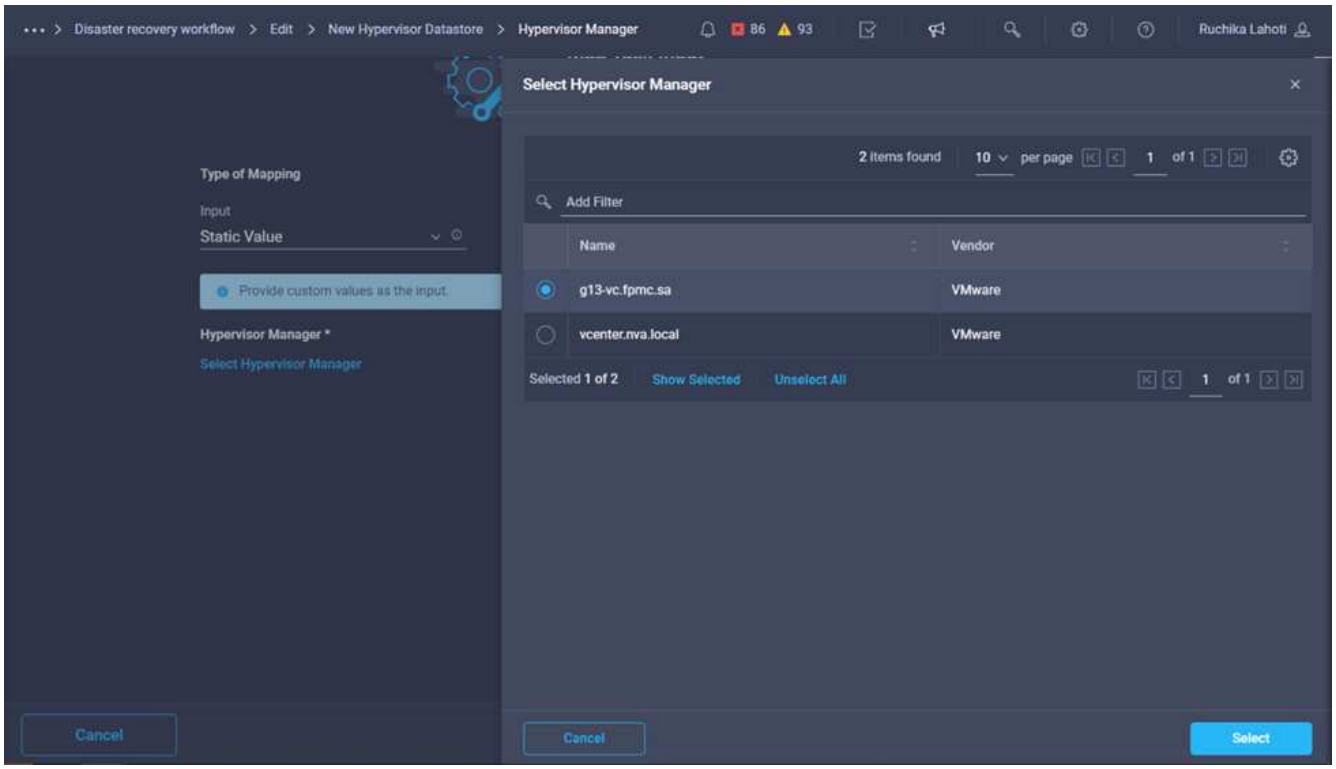
1. Vaya a la ficha **Diseñador** y haga clic en **tareas** en la sección **Herramientas**.
2. Arrastre y suelte la tarea **virtualización > New Hypervisor Datastore** de la sección **Herramientas** del área **Diseño**.
3. Utilice Connector para establecer una conexión entre las tareas **Add Storage Export Policy** y **New Hypervisor Datastore**. Haga clic en **Guardar**.



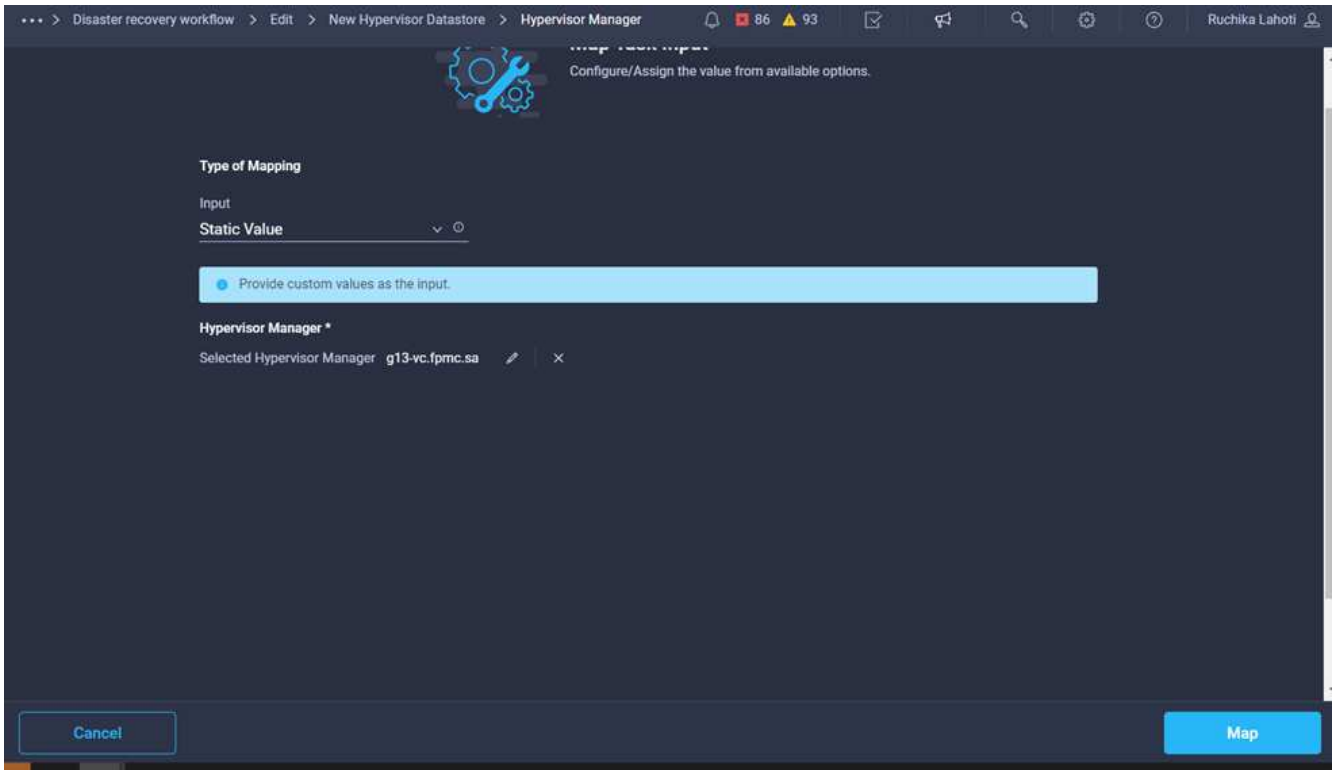
4. Haga clic en **New Hypervisor Datastore**. En el área **Propiedades de tarea**, haga clic en la ficha **General**. Opcionalmente, puede cambiar el nombre y la descripción de esta tarea. En este ejemplo, el nombre de la tarea es **asignar volumen a Datastore**.



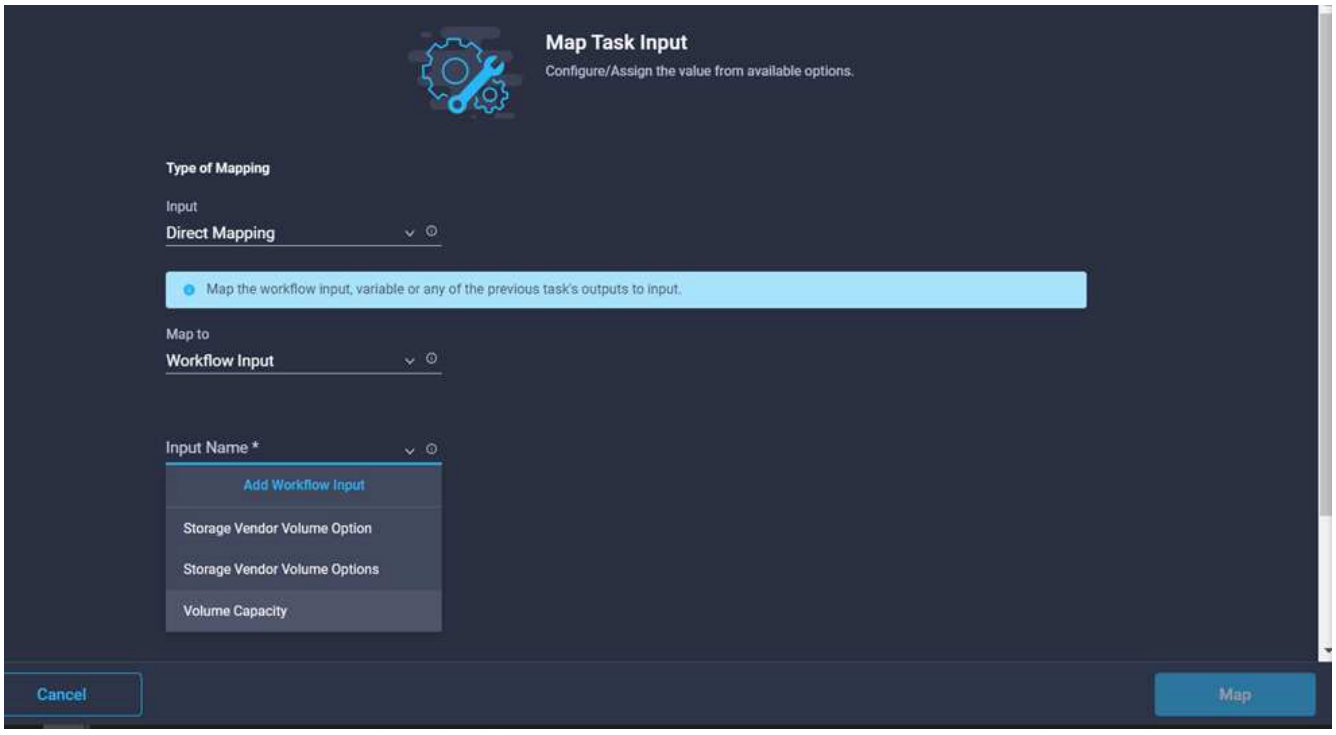
5. En el área **Propiedades de tarea**, haga clic en **Entradas**.
6. Haga clic en **Mapa** en el campo **Hypervisor Manager**.
7. Elija **valor estático** y haga clic en **Select Hypervisor Manager**. Haga clic en el destino de VMware vCenter.



8. Haga clic en **Mapa**.



9. Haga clic en **Mapa** en el campo **Centro de datos**. Este es el centro de datos asociado con el nuevo almacén de datos.
10. Elija **asignación directa** y haga clic en **Entrada de flujo de trabajo**.
11. Haga clic en **Nombre de entrada** y luego en **Crear entrada de flujo de trabajo**.



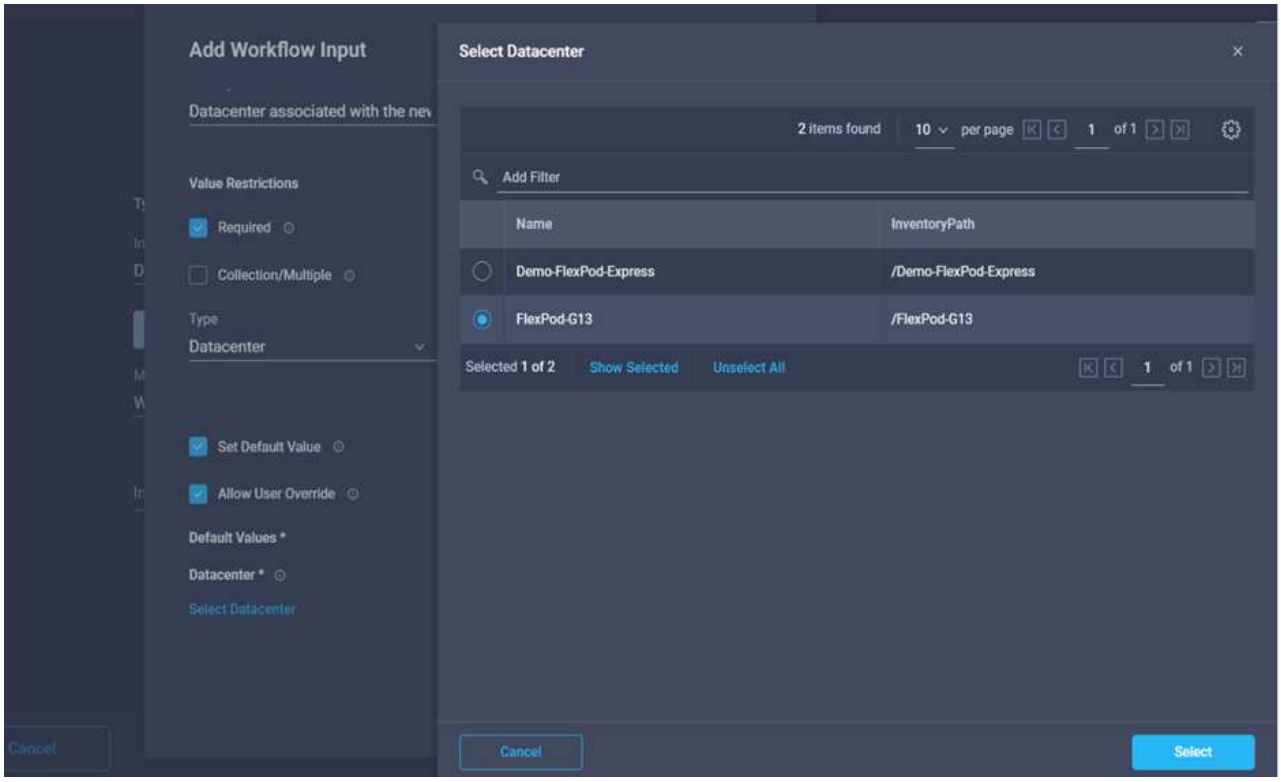
12. En el asistente para agregar entrada, lleve a cabo los siguientes pasos:
    a. Proporcione un nombre para mostrar y un nombre de referencia (opcional).

b. Seleccione **Datacenter** como tipo.

c. Haga clic en **establecer valor predeterminado y en Reemplazar**.

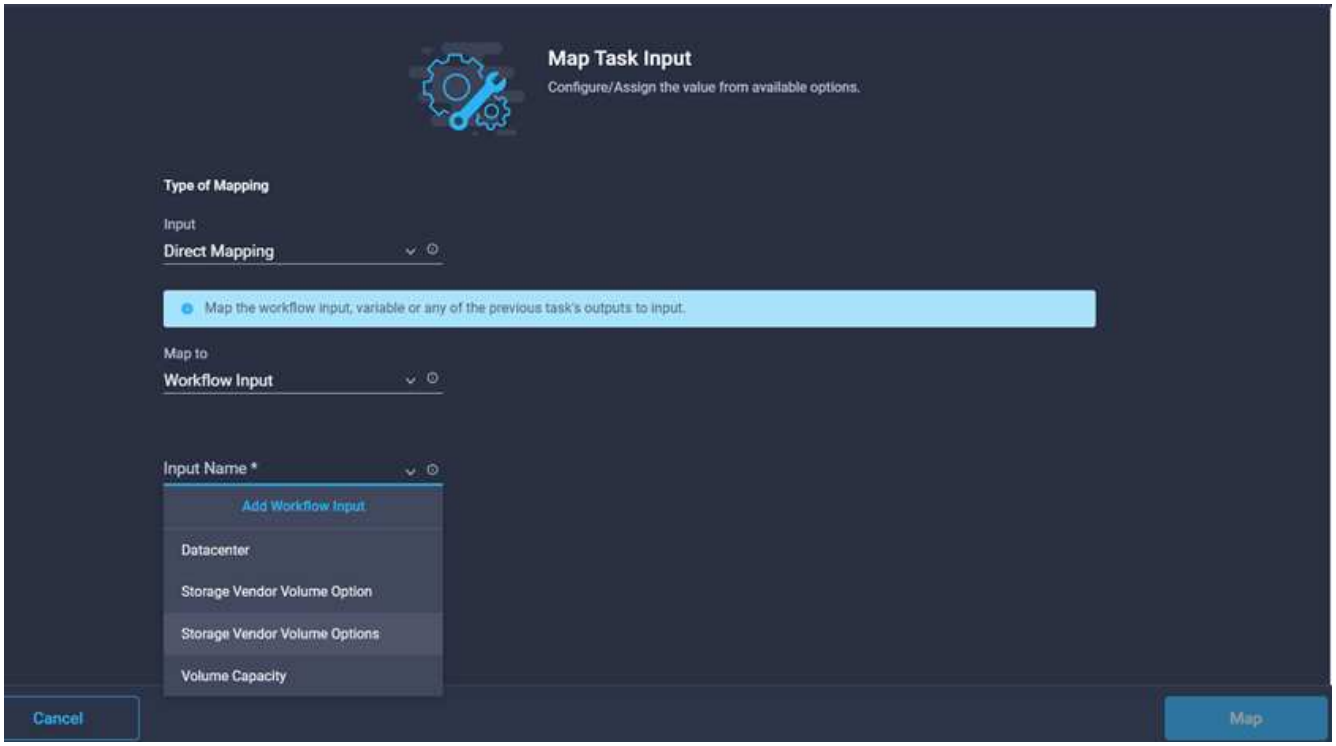
d. Haga clic en **Seleccionar centro de datos**.

e. Haga clic en el centro de datos asociado al nuevo almacén de datos y, a continuación, haga clic en **Select**.

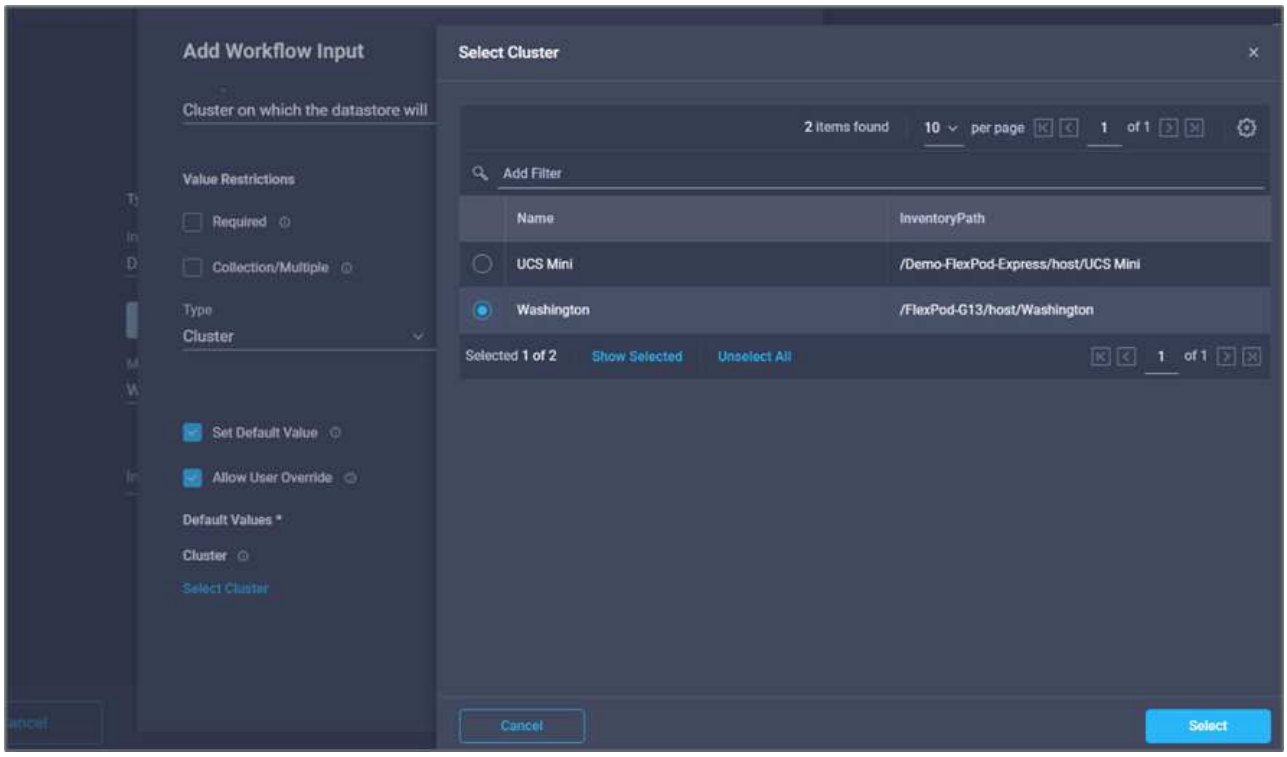


- Haga clic en **Agregar**.

13. Haga clic en **Mapa**.
14. Haga clic en **Mapa** en el campo **clúster**.
15. Elija **asignación directa** y haga clic en **Entrada de flujo de trabajo**.

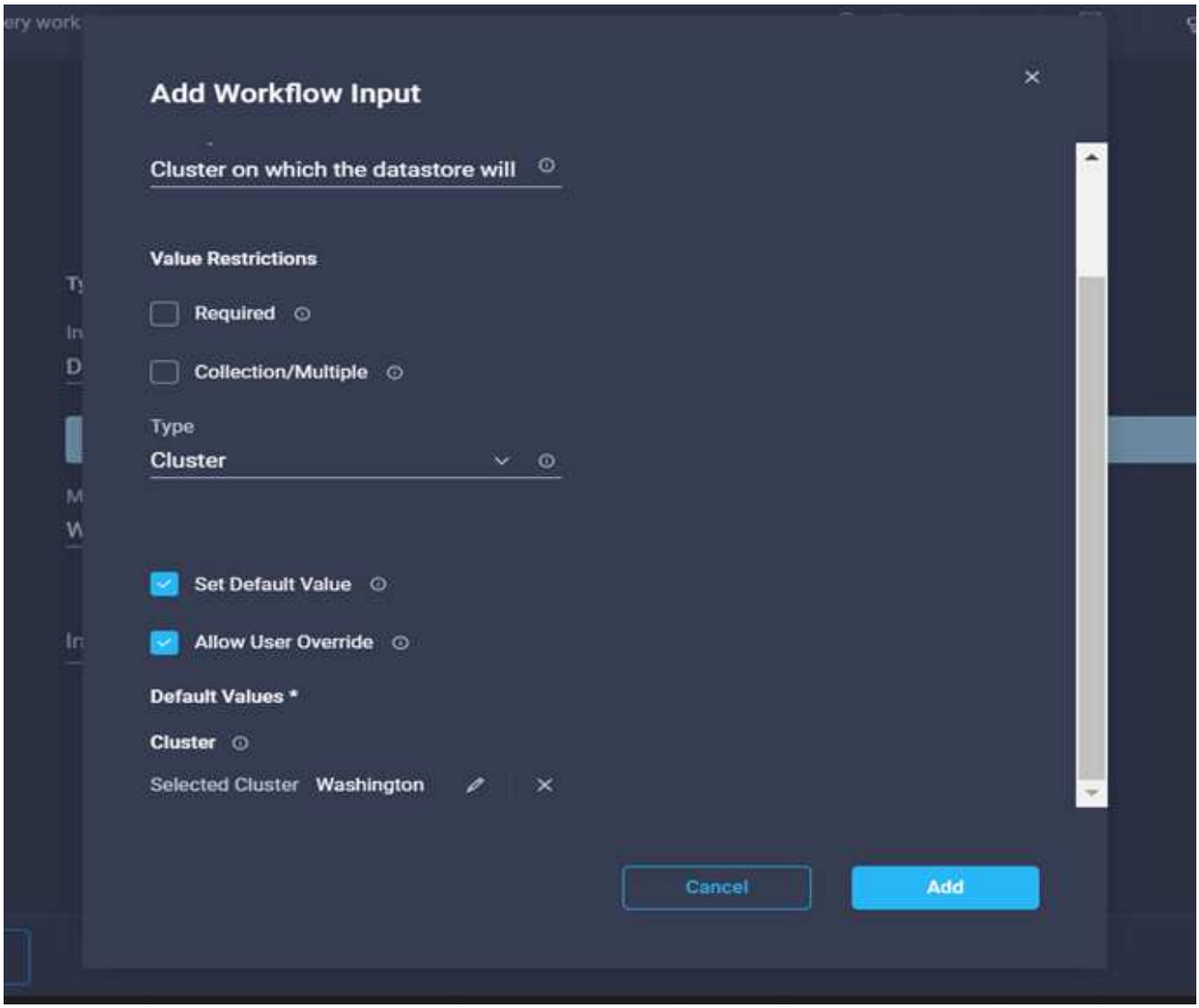


16. En el asistente para agregar entrada, lleve a cabo los siguientes pasos:
    a. Proporcione un nombre para mostrar y un nombre de referencia (opcional).
    b. Haga clic en **requerido**.
    c. Seleccione Cluster como tipo.
    d. Haga clic en **establecer valor predeterminado y en Reemplazar**.
    e. Haga clic en **Seleccionar clúster**.
    f. Haga clic en el clúster asociado con el almacén de datos nuevo.
    g. Haga clic en **Seleccionar**.

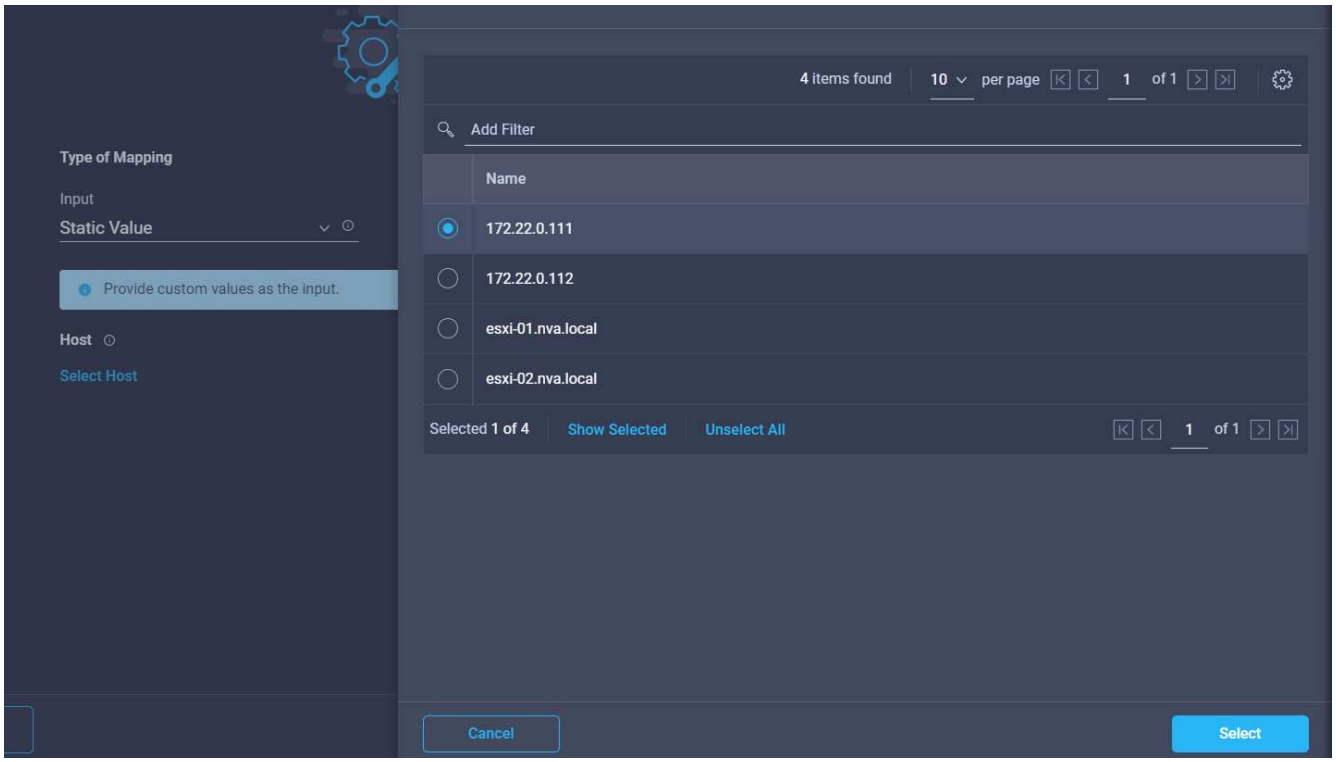


h. Haga clic en **Agregar**.

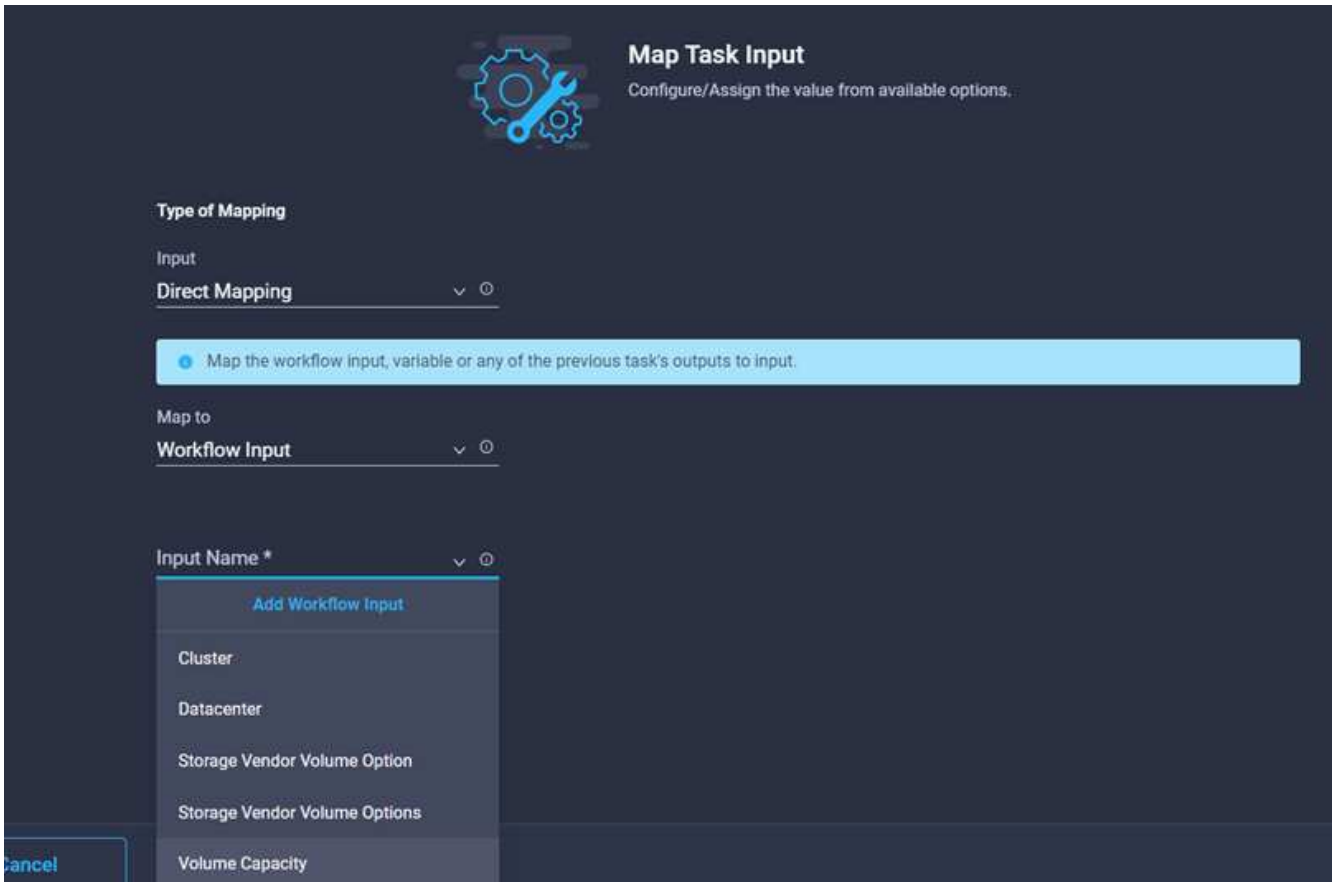
17. Haga clic en **Mapa**.
18. Haga clic en **Mapa** en el campo **Host**.



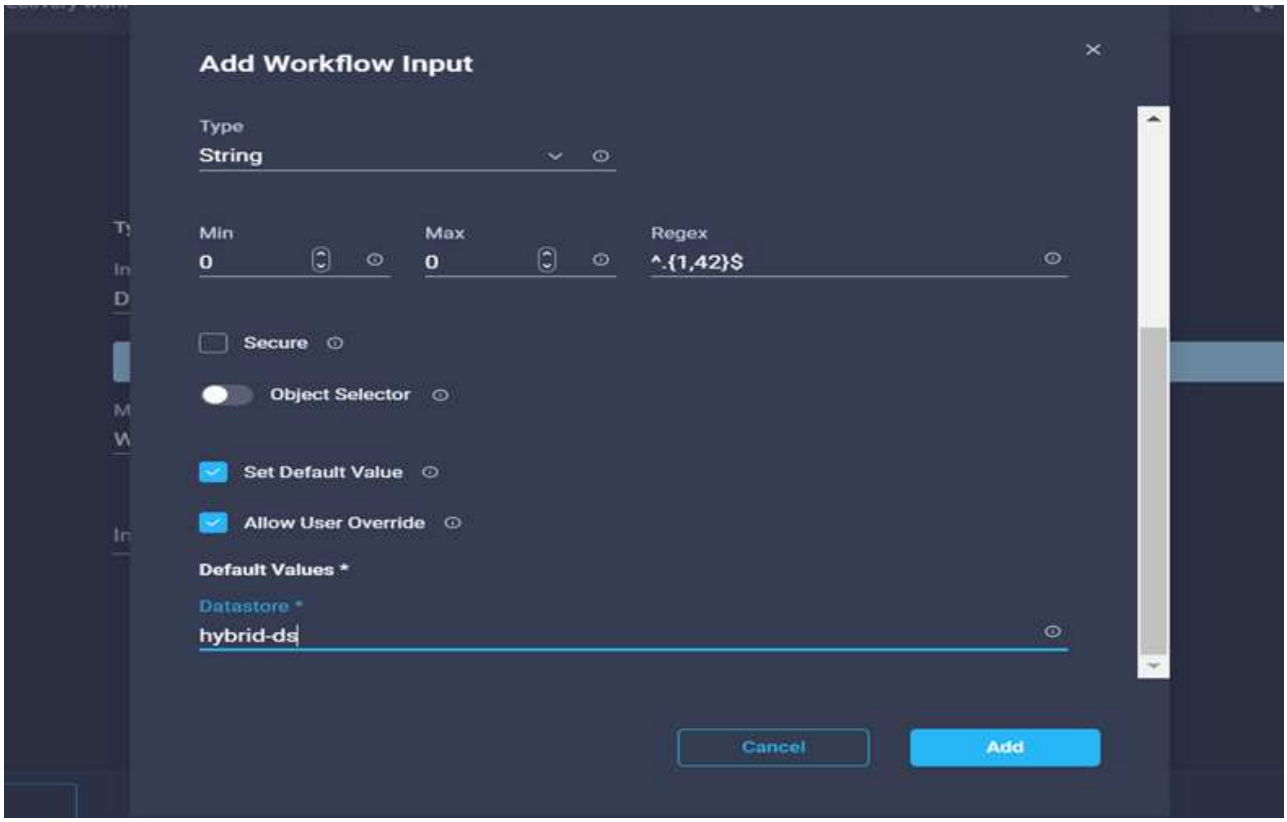
19. Elija **valor estático** y haga clic en el host en el que se alojará el almacén de datos. Si se especifica un clúster, se ignora el host.



20. Haga clic en **Seleccionar y asignar**.
21. Haga clic en **Mapa** en el campo **Datastore**.
22. Elija **asignación directa** y haga clic en **Entrada de flujo de trabajo**.
23. Haga clic en **Nombre de entrada** y **Crear entrada de flujo de trabajo**.



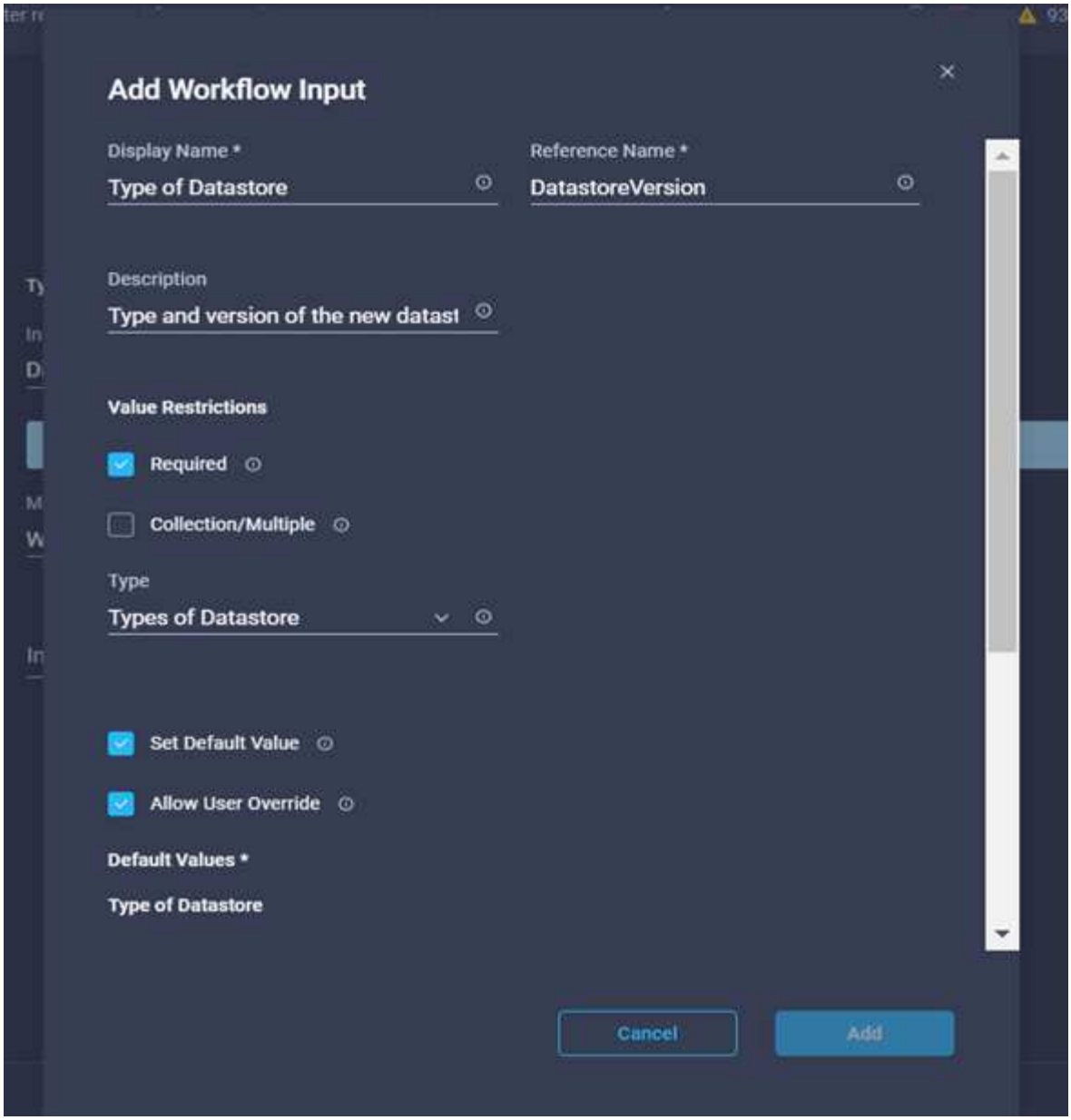
24. En el asistente Agregar entrada:
    a. Proporcione un nombre para mostrar y un nombre de referencia (opcional).
    b. Haga clic en **requerido**.
    c. Haga clic en **establecer valor predeterminado y en Reemplazar**.
    d. Proporcione un valor predeterminado para el almacén de datos y haga clic en **Agregar**.



25. Haga clic en **Mapa**.
26. Haga clic en **Mapa** en el campo de entrada **Tipo de Datastore**.
27. Elija **asignación directa** y haga clic en **Entrada de flujo de trabajo**.
28. Haga clic en **Nombre de entrada** y **Crear entrada de flujo de trabajo**.



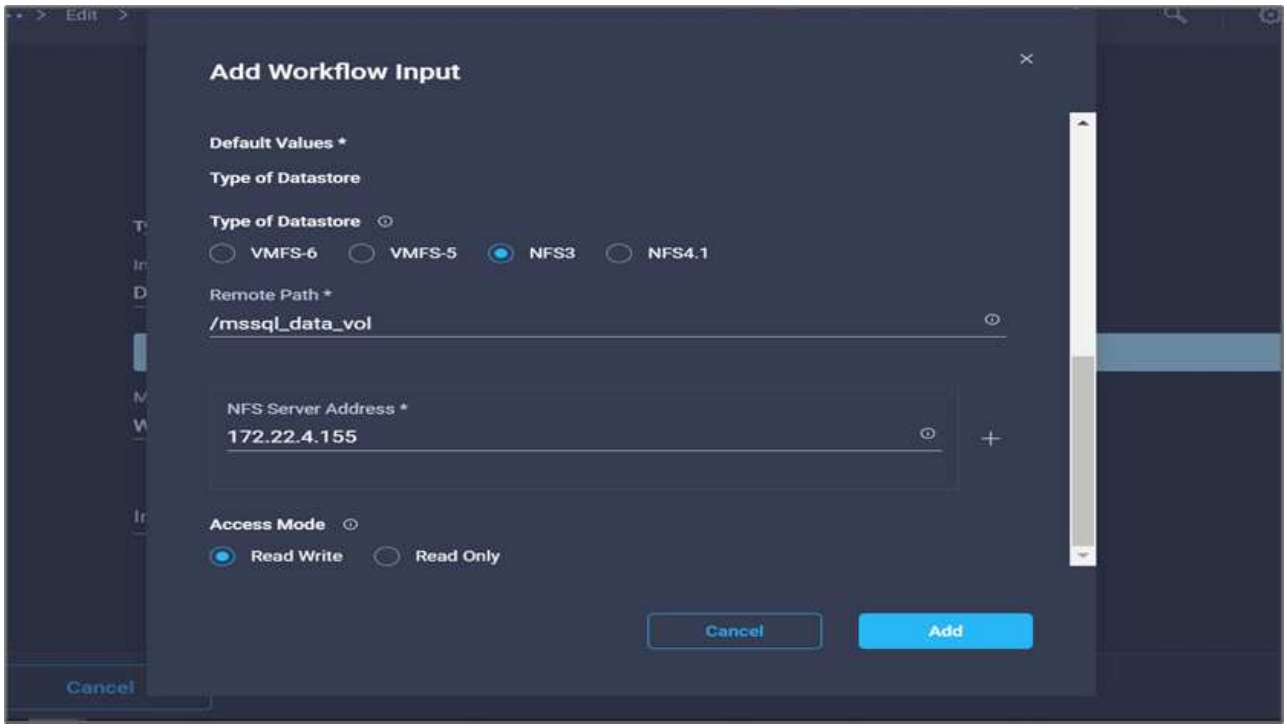
29. En el asistente para agregar entrada, lleve a cabo los siguientes pasos:
    a. Proporcione un nombre para mostrar y un nombre de referencia (opcional) y haga clic en **requerido**.
    b. Asegúrese de seleccionar el tipo **tipos de Datastore** y haga clic en **establecer valor predeterminado y en Anular**.



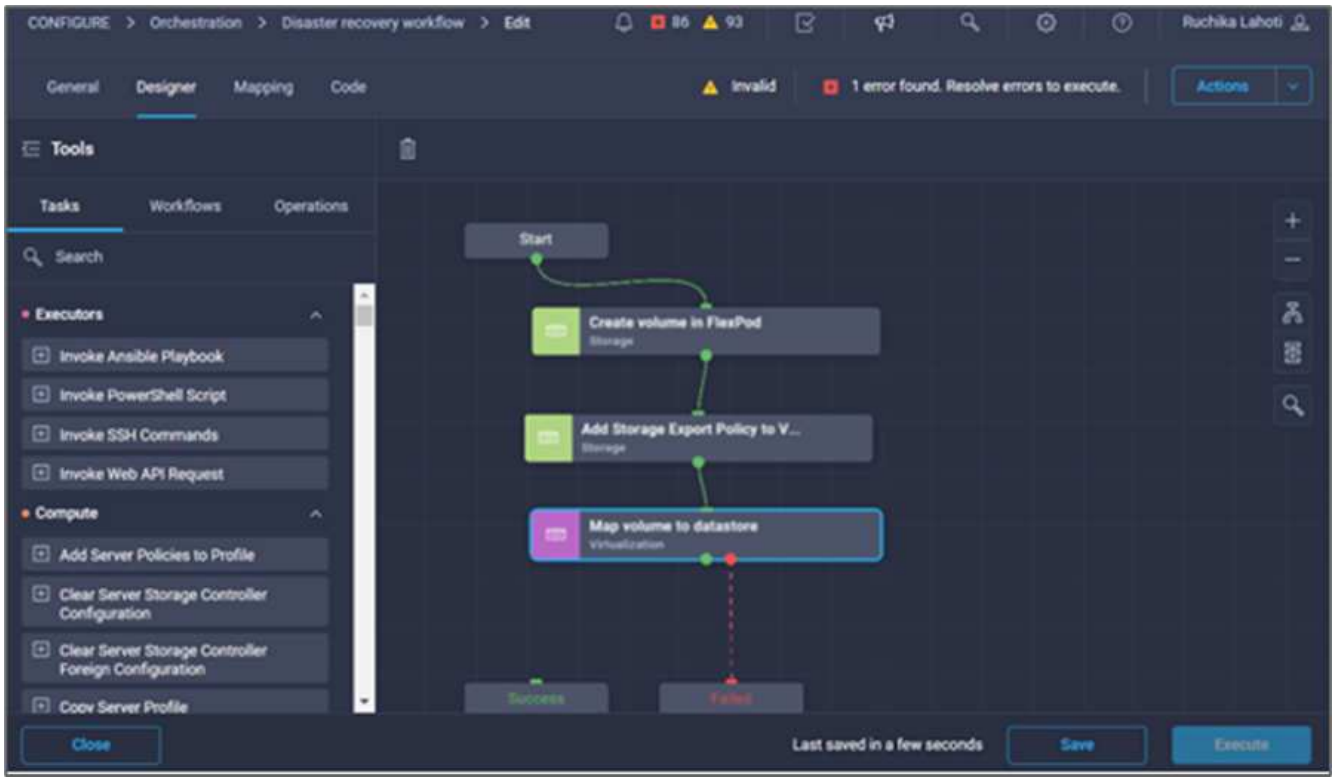
c. Proporcione la ruta remota. Esta es la ruta remota del punto de montaje NFS.

d. Proporcione los nombres de host o las direcciones IP del servidor NFS remoto en la dirección del servidor NFS.

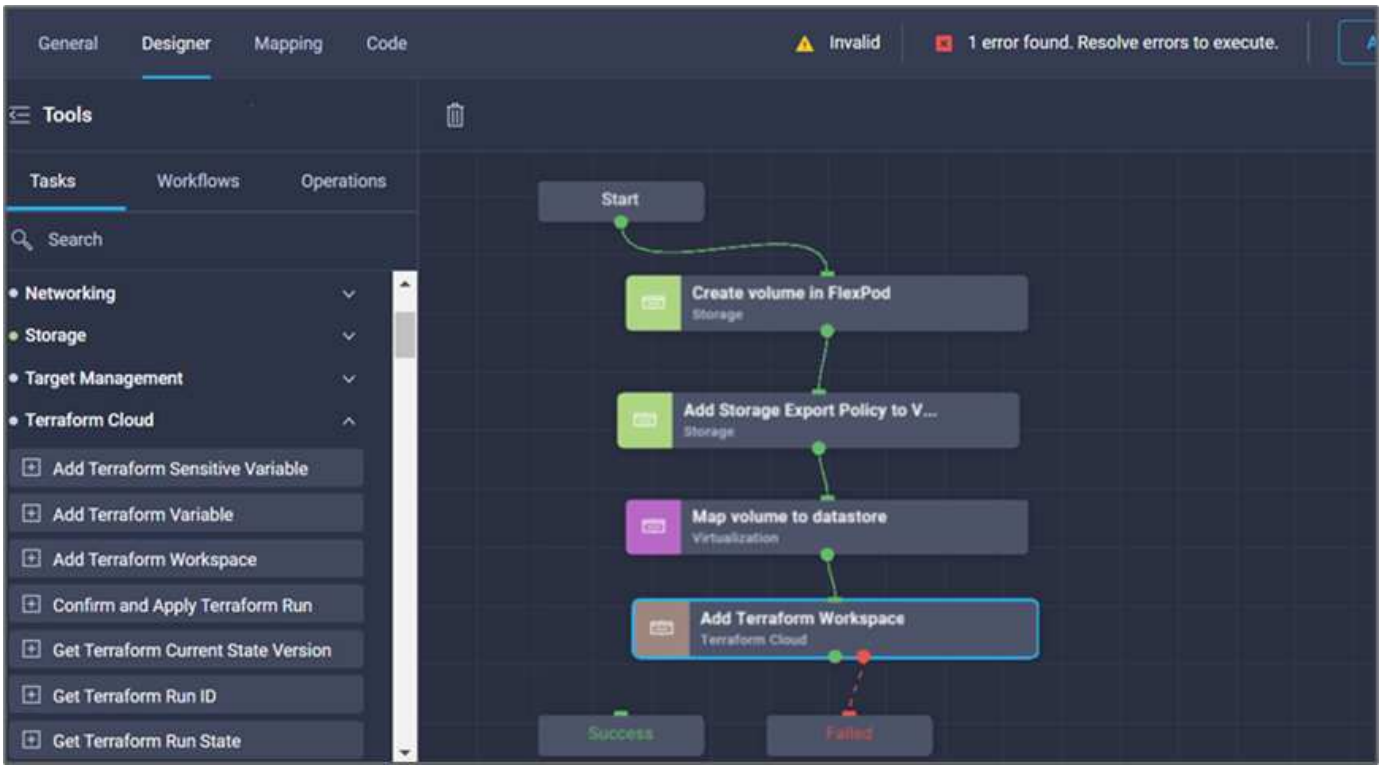
e. Haga clic en **modo de acceso**. El modo Access es para el servidor NFS. Haga clic en sólo lectura si los volúmenes se exportan como de solo lectura. Haga clic en **Agregar**.



30. Haga clic en **Mapa**.
31. Haga clic en **Guardar**.

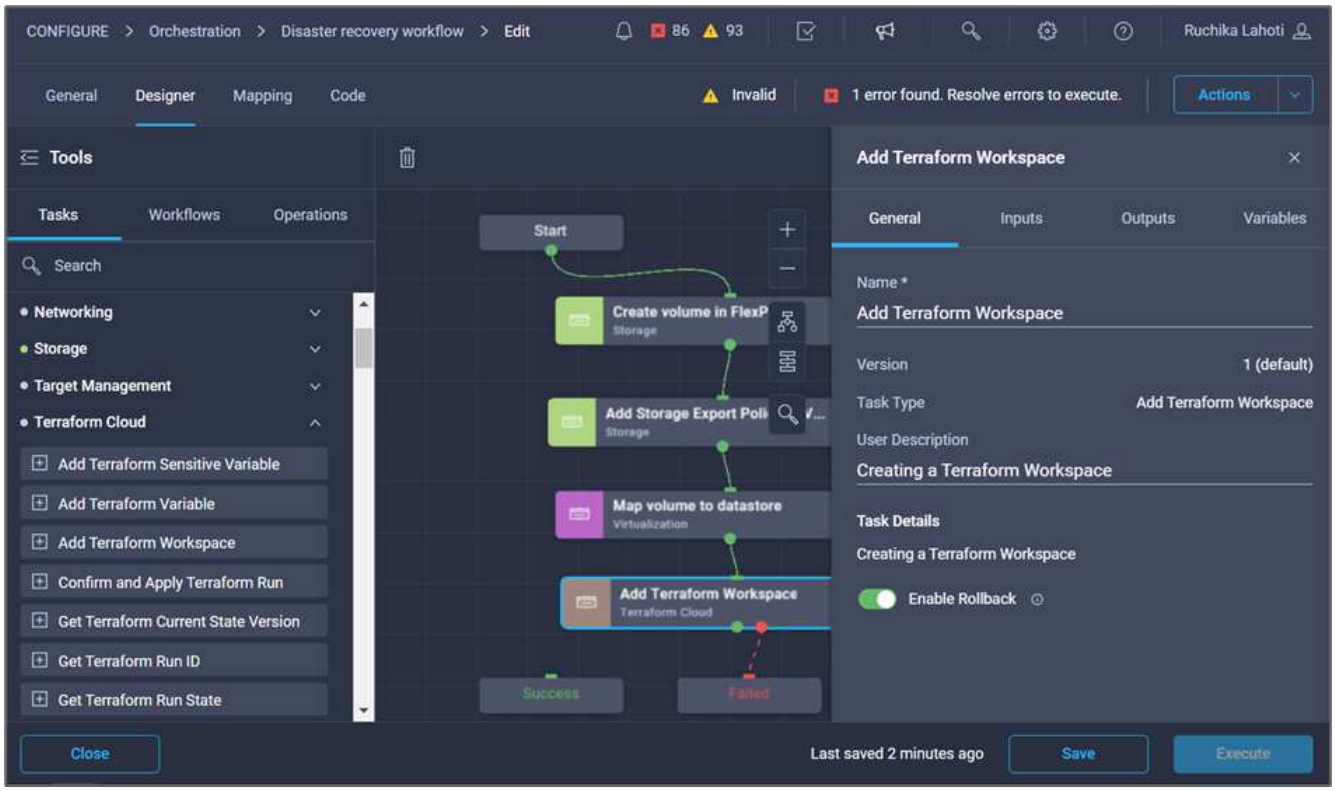


Con esto finaliza la tarea de creación del almacén de datos. Se completan todas las tareas realizadas en el centro de datos FlexPod en las instalaciones.

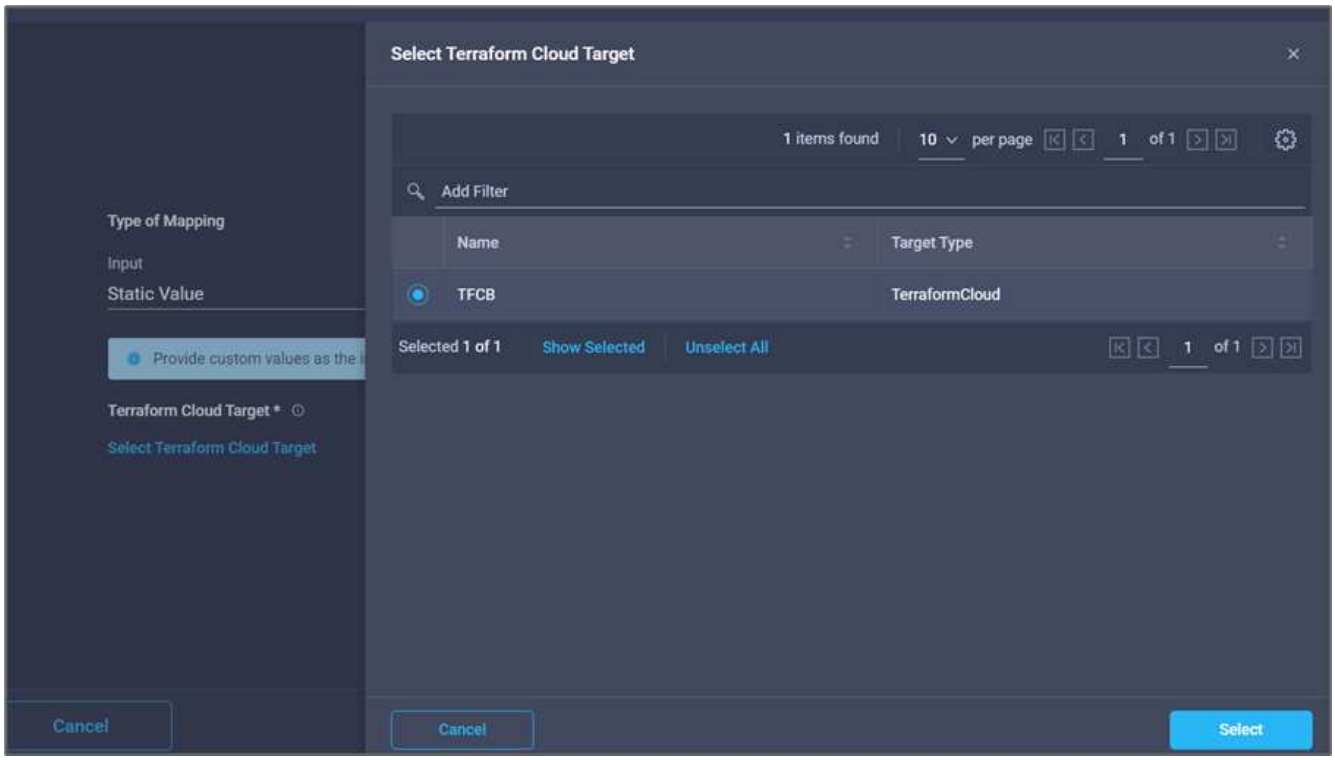


Procedimiento 5: Agregue un nuevo espacio de trabajo Terraform

1. Vaya a la ficha **Diseñador** y haga clic en **tareas** en la sección **Herramientas**.
2. Arrastre y suelte la tarea **Terraform Cloud > Add Terraform Workspace** de la sección Herramientas del área Diseño.
3. Utilice Connector para conectar las tareas **Map volume to Datastore** y **Add Terraform Workspace** y haga clic en **Save**.
4. Haga clic en **Agregar espacio de trabajo de Terraform**. En el área Propiedades de la tarea, haga clic en la ficha **General**. Si lo desea, puede cambiar el nombre y la descripción de esta tarea.

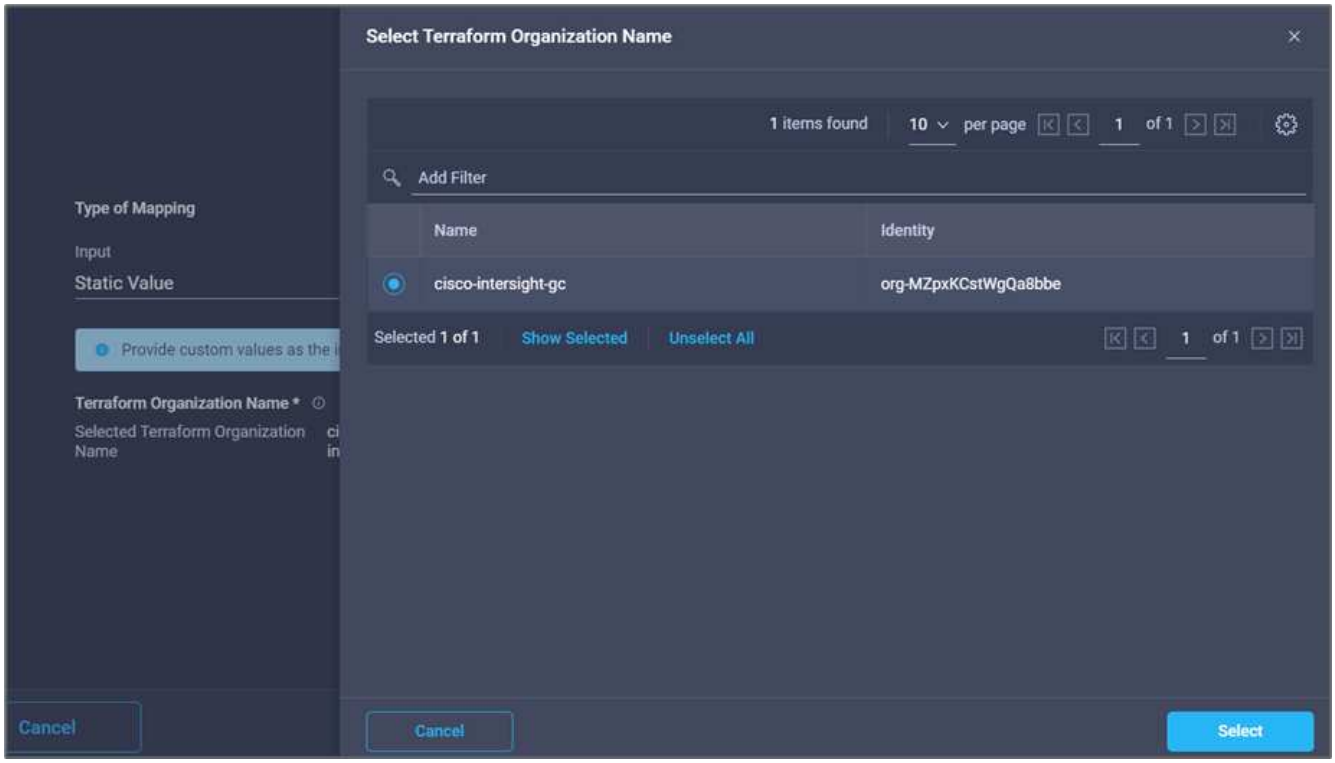


5. En el área Propiedades de la tarea, haga clic en **entradas**.
6. Haga clic en **Mapa** en el campo de entrada **objetivo de nube de Terraform**.
7. Elija **valor estático** y haga clic en **Seleccionar destino de nube de Terraform**. Seleccione la cuenta de Terraform Cloud for Business que se agregó como se explica en "Configure Cisco Intersight Service para HashiCorp Terraform".".

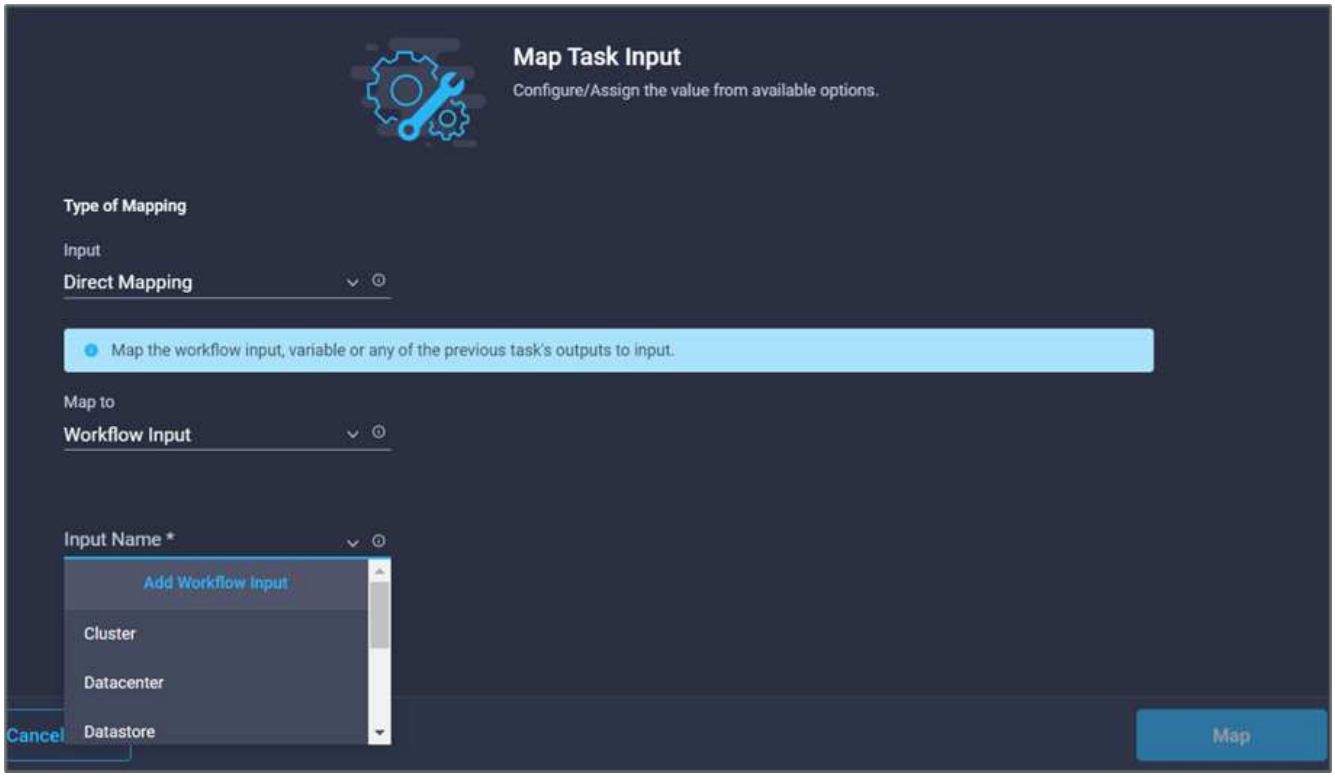


8. Haga clic en **Mapa**.

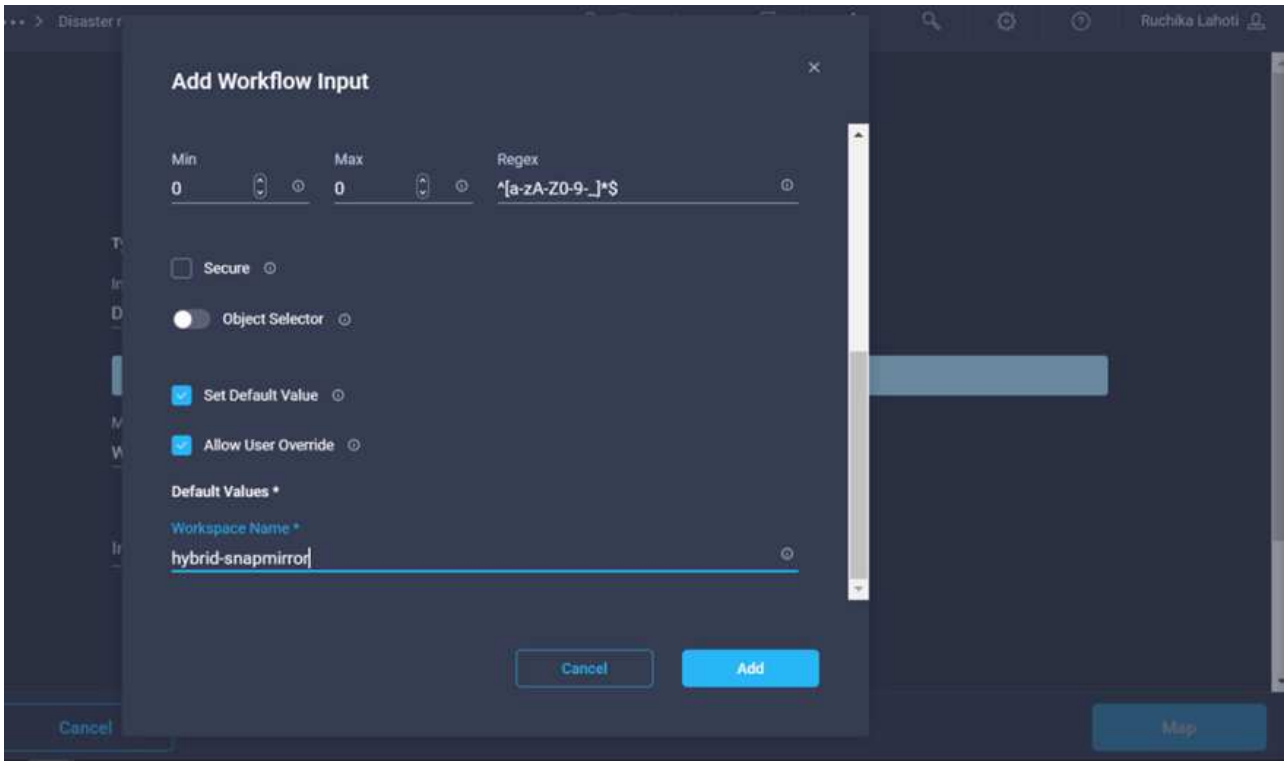
9. Haga clic en **Mapa** en el campo de entrada **Nombre de organización de Terraform**.
10. Elija **valor estático** y, a continuación, haga clic en **Seleccionar organización de Terraform**. Seleccione el nombre de la organización Terraform de la que forma parte en su cuenta de Terraform Cloud for Business.



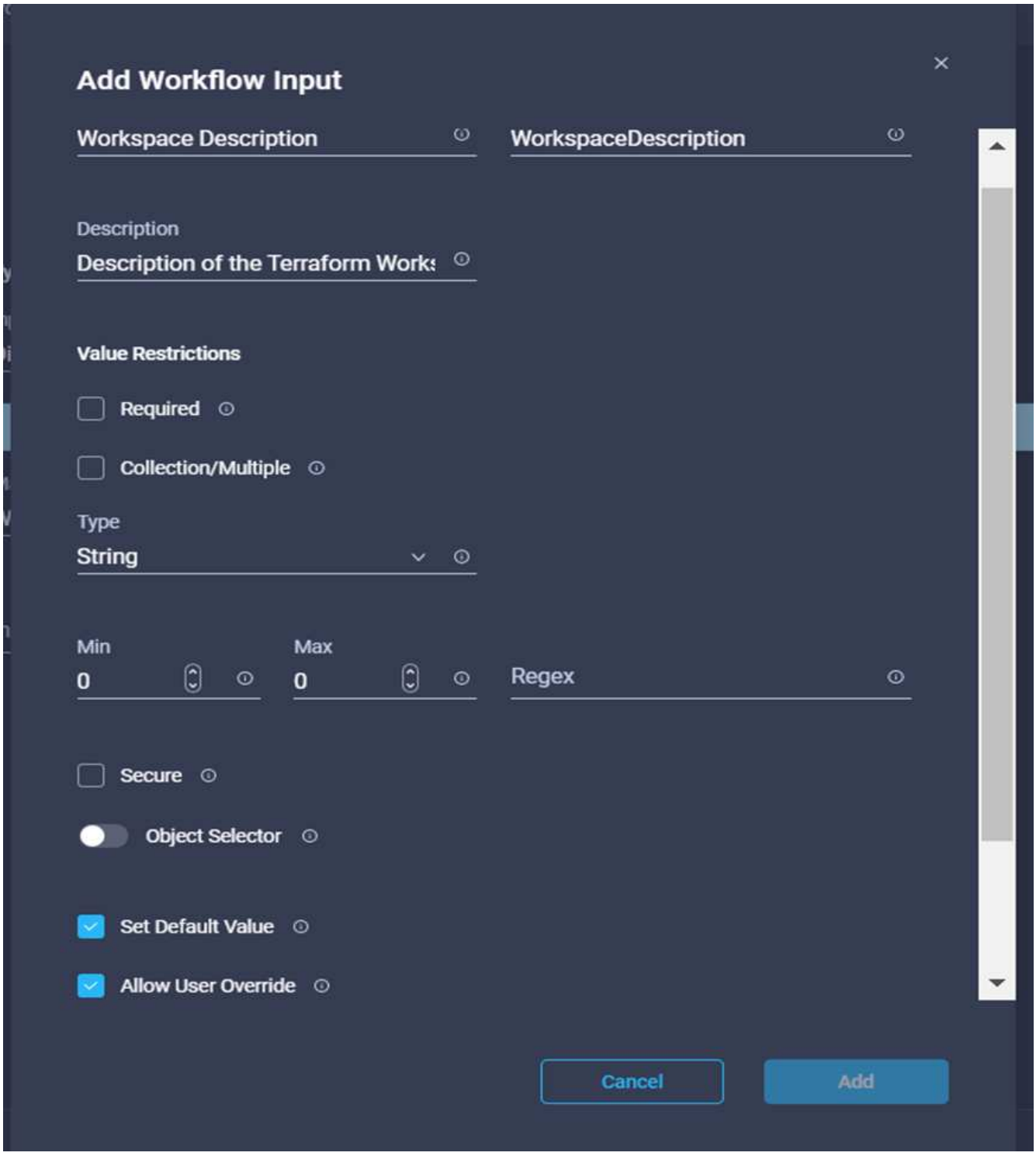
11. Haga clic en **Mapa**.
12. Haga clic en **Mapa** en el campo **Nombre de área de trabajo de Terraform**. Este es el nuevo espacio de trabajo de la cuenta Terraform Cloud para Business.
13. Elija **asignación directa** y haga clic en **Entrada de flujo de trabajo**.
14. Haga clic en **Nombre de entrada** y **Crear entrada de flujo de trabajo**.



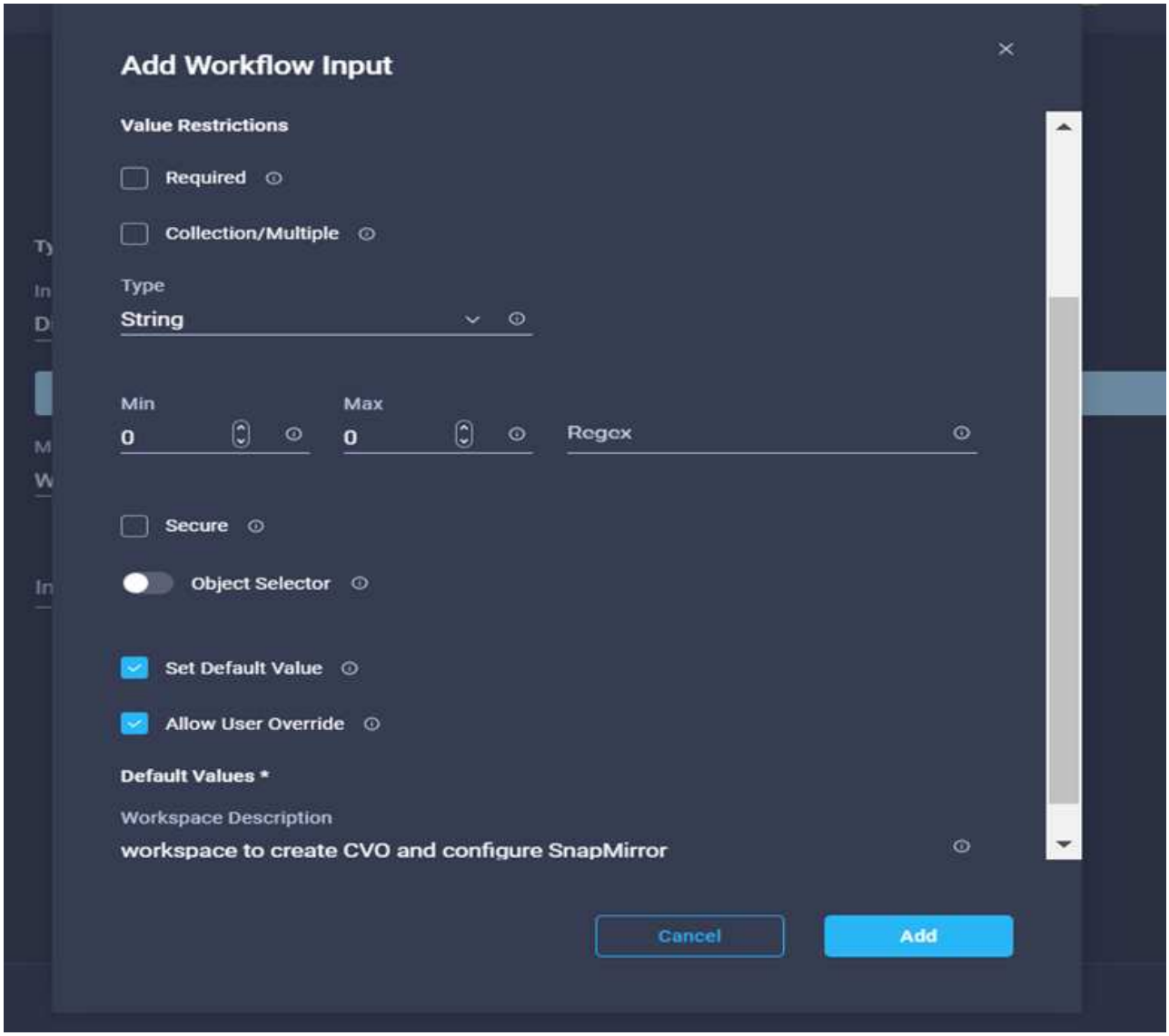
15. En el asistente para agregar entrada, lleve a cabo los siguientes pasos:
    a. Proporcione un nombre para mostrar y un nombre de referencia (opcional).
    b. Haga clic en **requerido**.
    c. Asegúrese de seleccionar **cadena** para **Tipo**.
    d. Haga clic en **establecer valor predeterminado y en Reemplazar**.
    e. Proporcione un nombre predeterminado para el área de trabajo.
    f. Haga clic en **Agregar**.



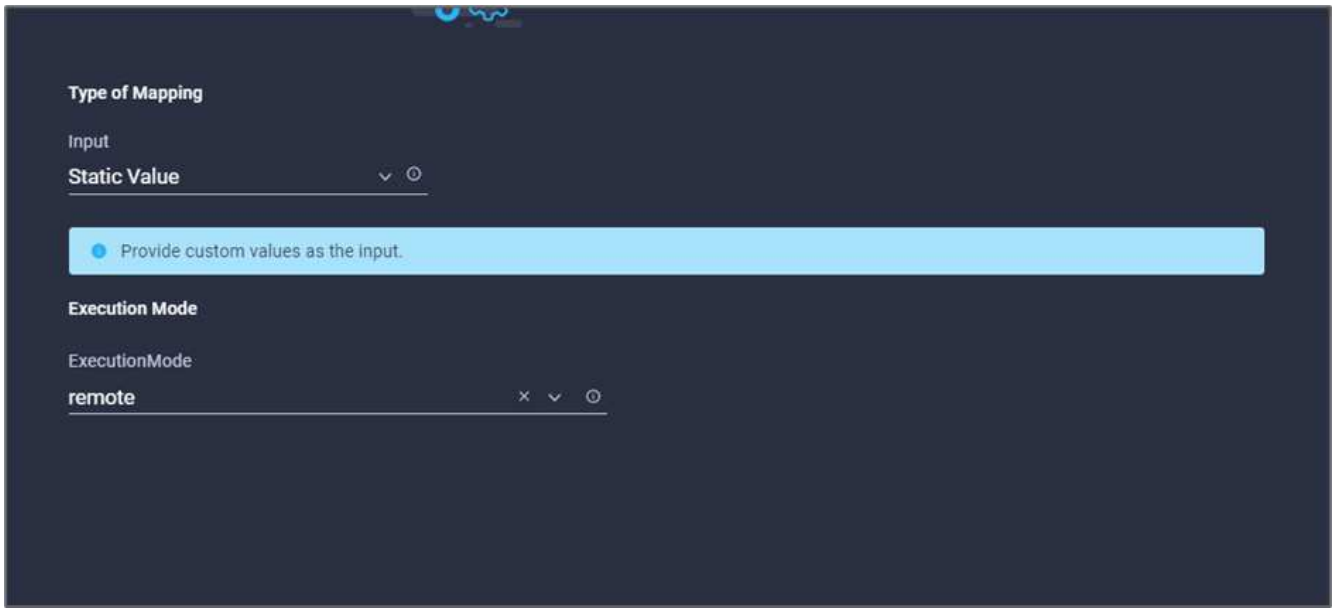
16. Haga clic en **Mapa**.
17. Haga clic en **Mapa** en el campo **Descripción del espacio de trabajo**.
18. Elija **asignación directa** y haga clic en **Entrada de flujo de trabajo**.
19. Haga clic en **Nombre de entrada** y **Crear entrada de flujo de trabajo**.



20. En el asistente para agregar entrada, lleve a cabo los siguientes pasos:
    a. Proporcione un nombre para mostrar y un nombre de referencia (opcional).
    b. Asegúrese de seleccionar **cadena** para **Tipo**.
    c. Haga clic en **establecer valor predeterminado y en Reemplazar**.
    d. Proporcione una descripción del área de trabajo y haga clic en **Agregar**.



21. Haga clic en **Mapa**.
22. Haga clic en **Mapa** en el campo **modo de ejecución**.
23. Elija **valor estático**, haga clic en **modo de ejecución** y, a continuación, haga clic en **remoto**.



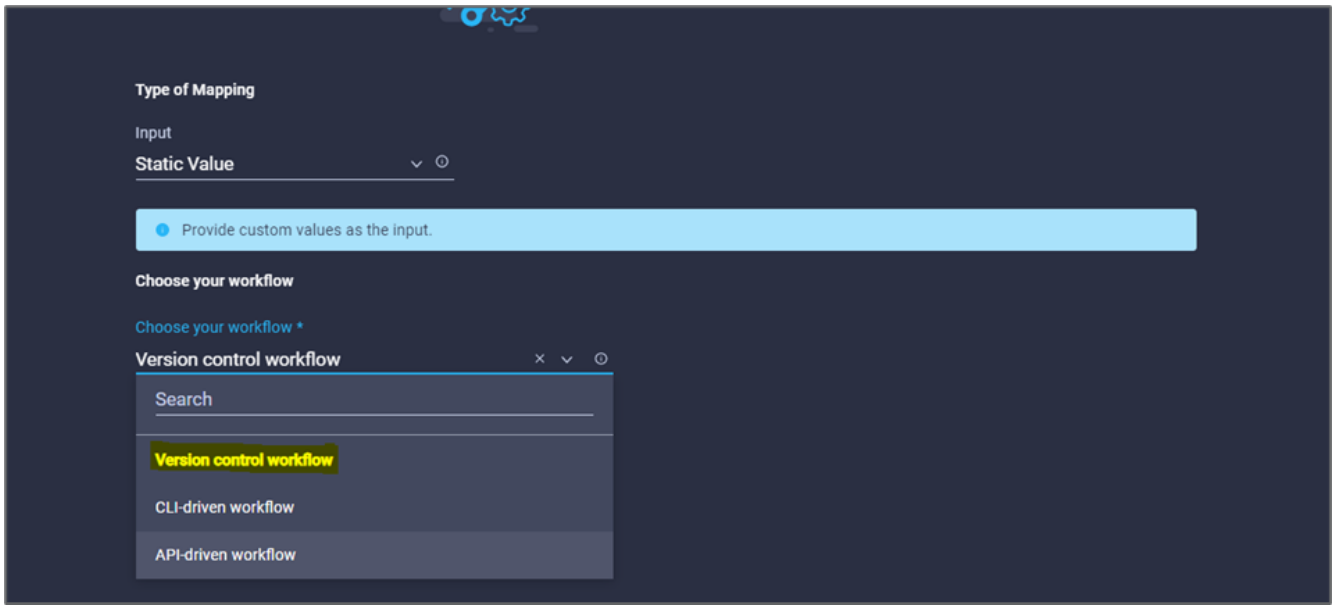
24. Haga clic en **Mapa**.
25. Haga clic en **Mapa** en el campo **aplicar método**.
26. Elija **valor estático** y haga clic en **aplicar método**. Haga clic en **aplicación manual**.



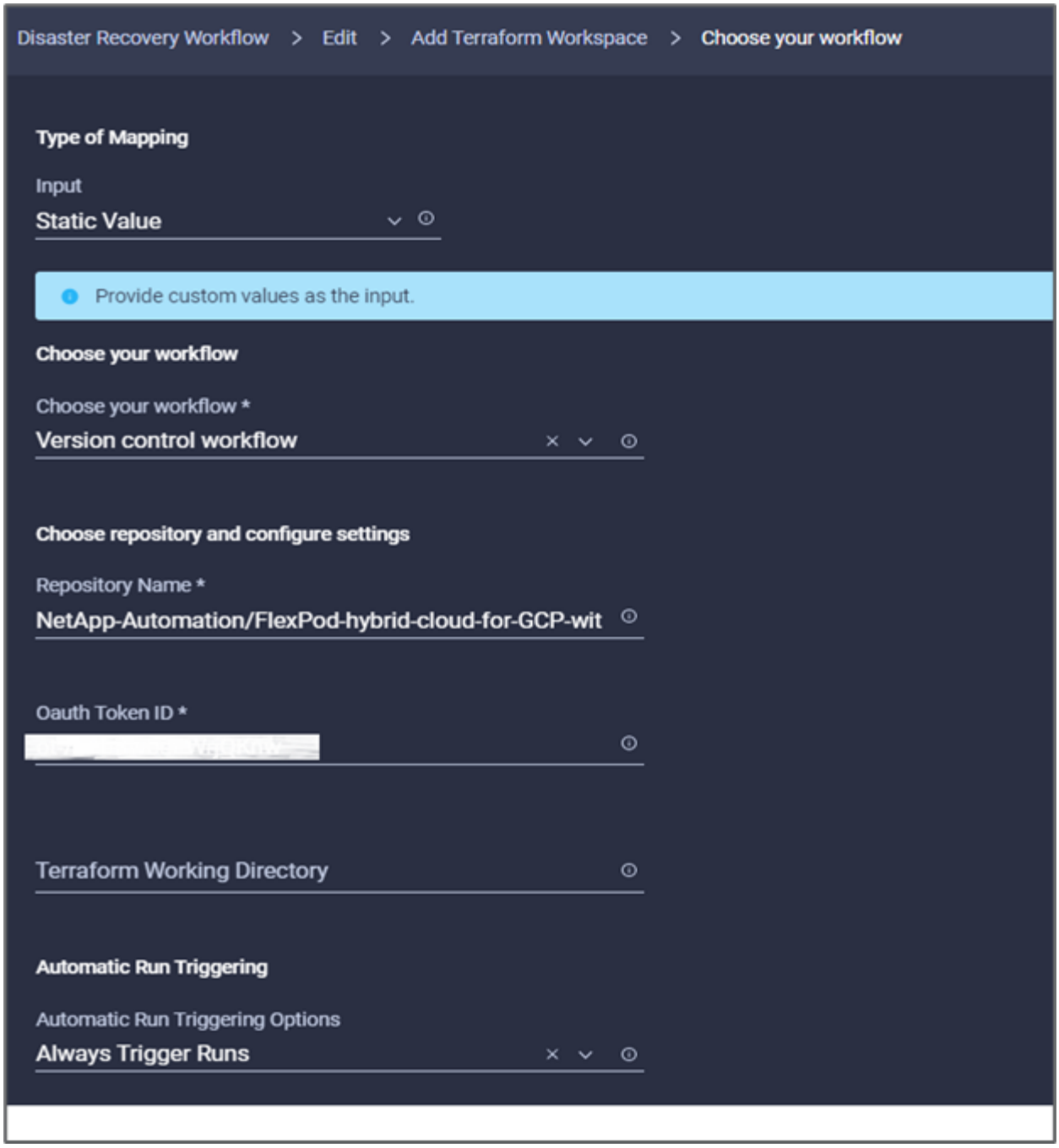
27. Haga clic en **Mapa**.
28. Haga clic en **Mapa** en el campo **interfaz de usuario**.
29. Elija **valor estático** y haga clic en **interfaz de usuario**. Haga clic en **interfaz de usuario de la consola**.



30. Haga clic en **Mapa**.
31. Haga clic en **Mapa** en el campo de entrada y seleccione el flujo de trabajo.
32. Seleccione **valor estático** y haga clic en **Elija el flujo de trabajo**. Haga clic en **flujo de trabajo de control de versiones**.



33. Proporcione los siguientes detalles del repositorio de GitHub:
    a. En **Nombre del repositorio**, introduzca el nombre del repositorio detallado en la sección ""Configuración de requisitos previos del entorno"".
    b. Proporcione el identificador de token de OAuth como se indica en la sección ""Configuración de requisitos previos del entorno"".
    c. Seleccione la opción **disparo automático**.



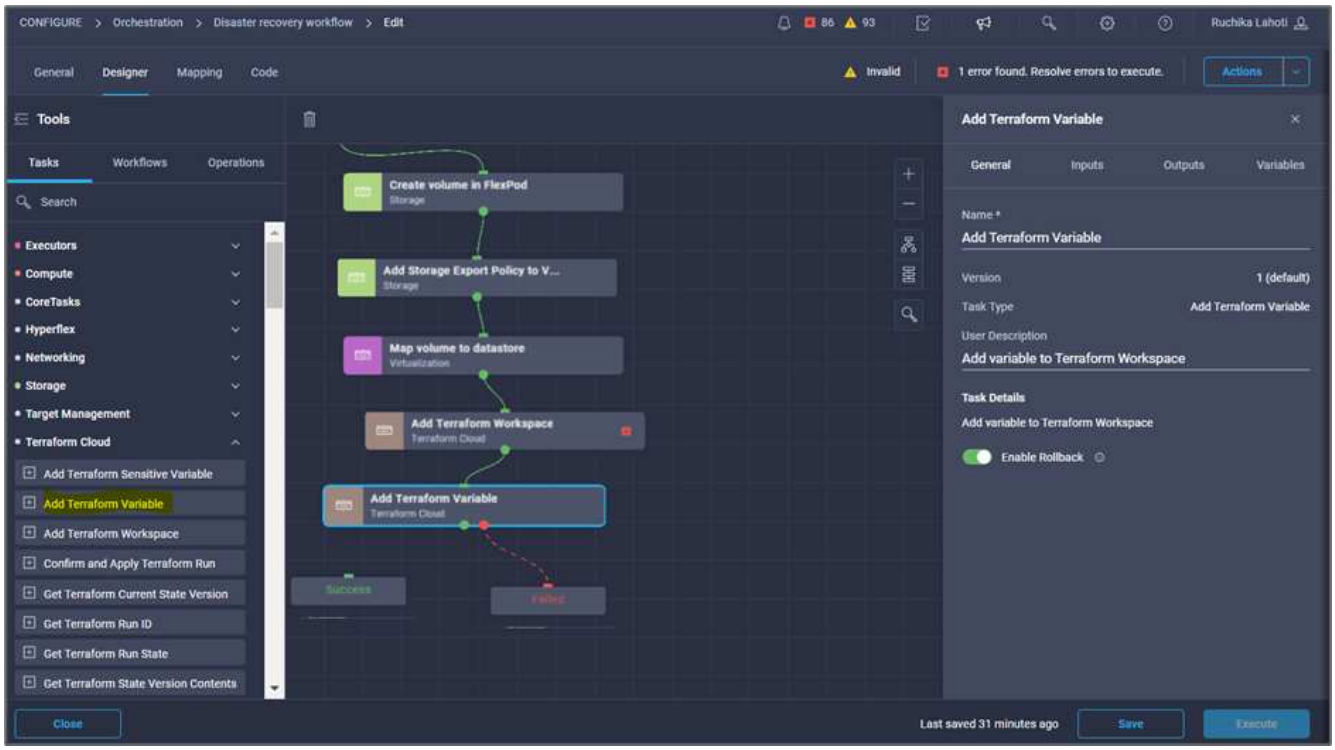
34. Haga clic en **Mapa**.
35. Haga clic en **Guardar**.

De esta forma finaliza la tarea de crear un espacio de trabajo en una cuenta de Terraform Cloud para Business.

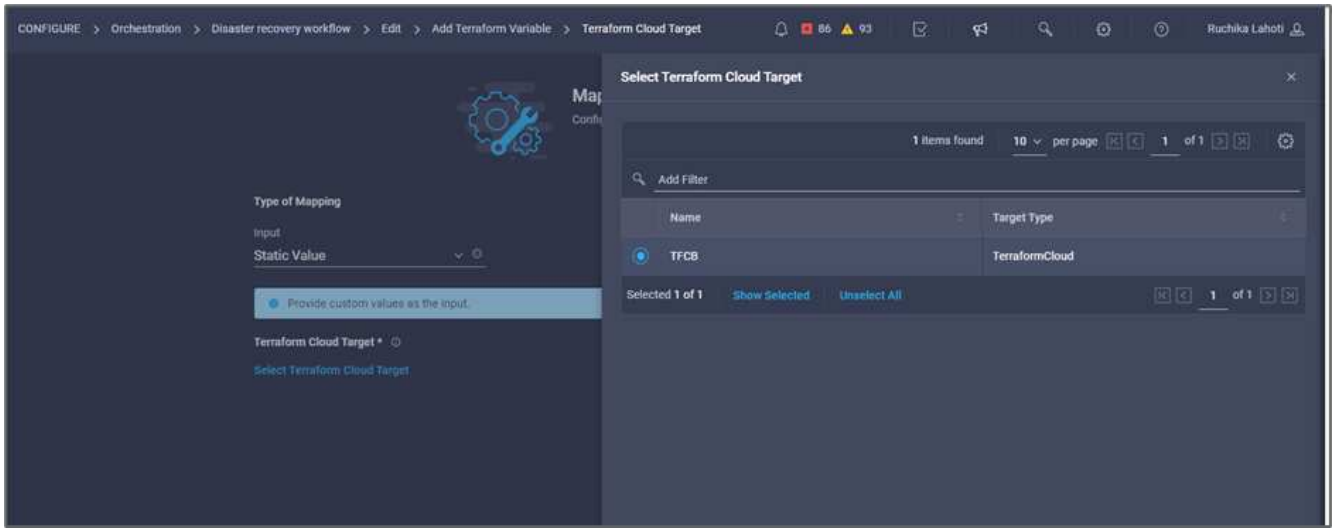
Procedimiento 6: Agregue variables no sensibles al espacio de trabajo

1. Vaya a la ficha **Diseñador** y haga clic en la sección **flujos de trabajo de Herramientas**.
2. Arrastre y suelte el flujo de trabajo **Terraform > Add Terraform variables** de la sección **Herramientas** del área **Diseño**.
3. Utilice Connector para conectar las tareas **Add Terraform Workspace** y **Add Terraform variables**. Haga clic en **Guardar**.

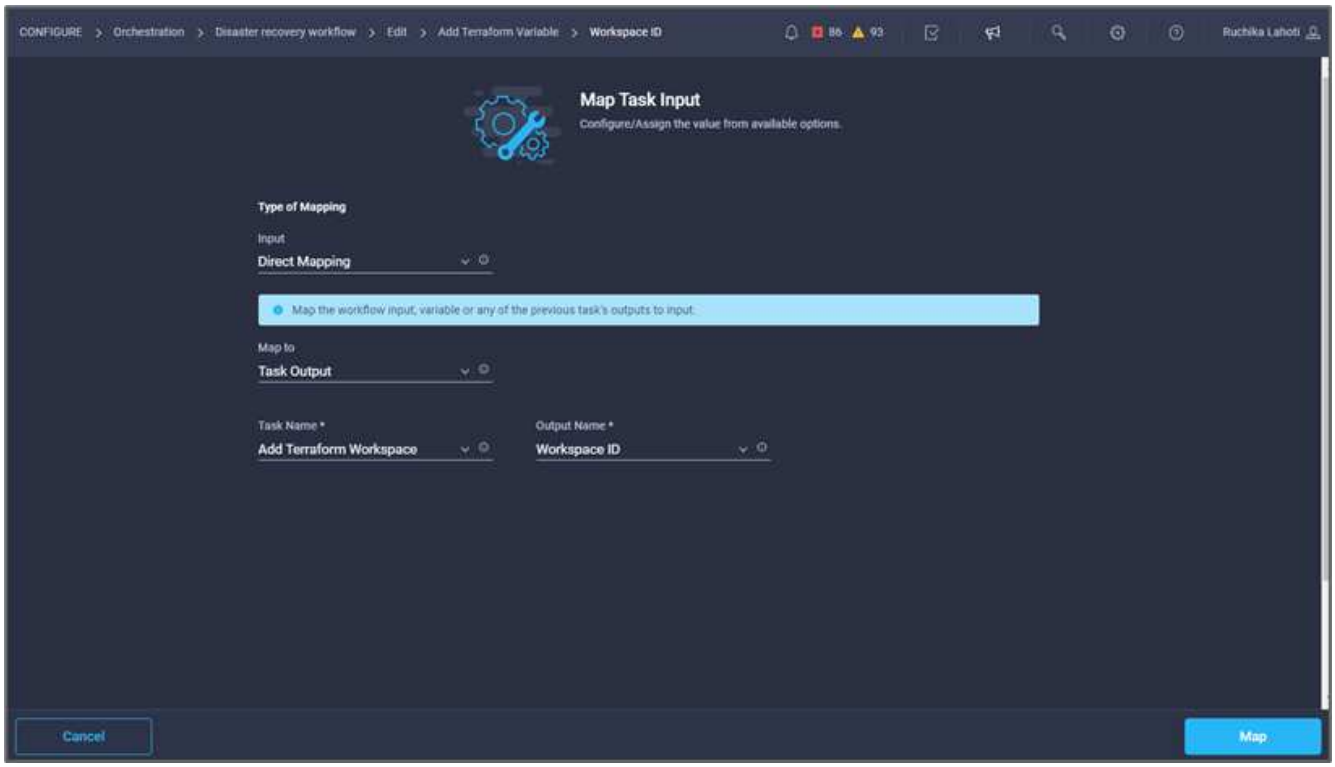
4. Haga clic en **Agregar variables de Terraform**. En el área **Propiedades del flujo de trabajo**, haga clic en la ficha **General**. Opcionalmente, puede cambiar el nombre y la descripción de esta tarea.



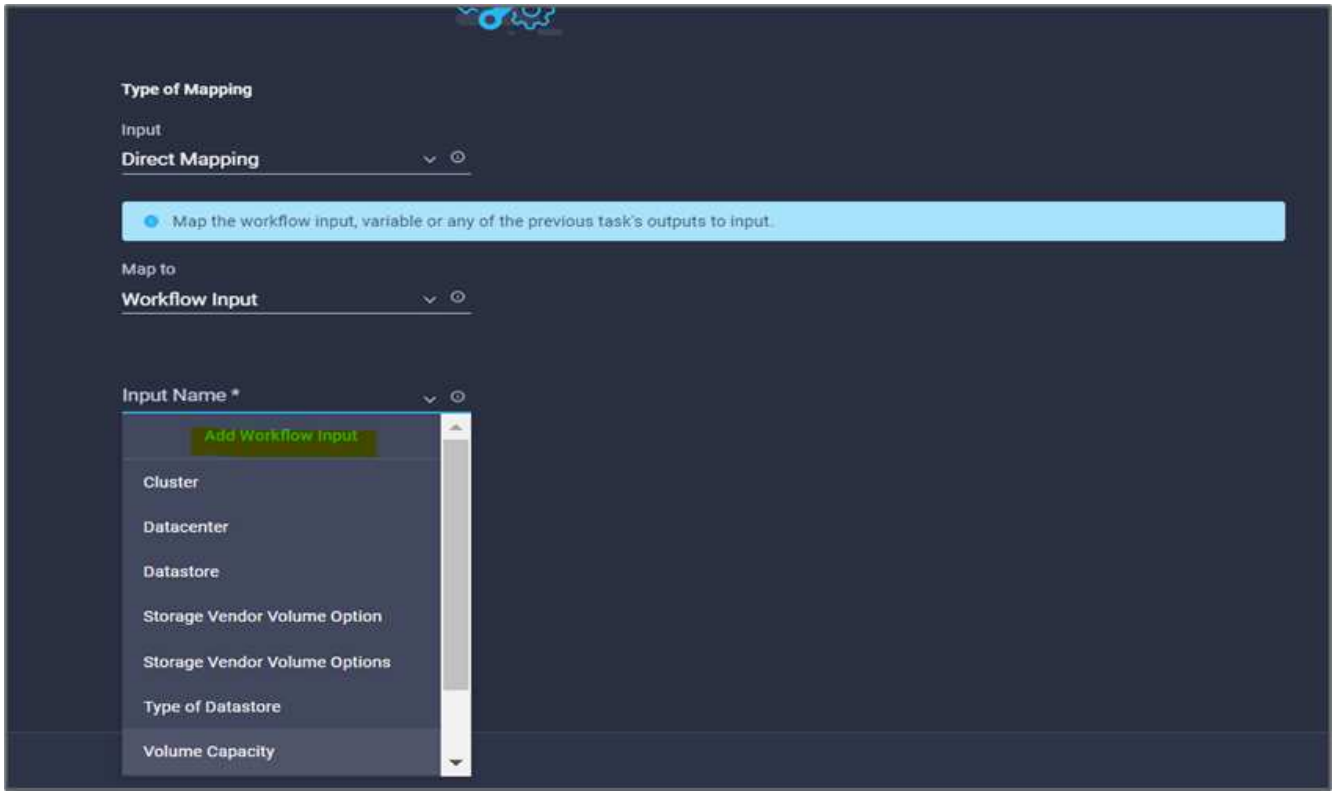
5. En el área **Propiedades del flujo de trabajo**, haga clic en **Entradas**.
6. Haga clic en **Mapa** en el campo **objetivo de la nube Terraform**.
7. Elija **valor estático** y haga clic en **Seleccionar destino de nube de Terraform**. Seleccione la cuenta de Terraform Cloud for Business que se agregó como se explica en "Configure Cisco Intersight Service para HashiCorp Terraform".".



8. Haga clic en **Mapa**.
9. Haga clic en **Mapa** en el campo *Nombre de organización de Terraform *.
10. Elija **valor estático** y haga clic en **Seleccionar organización de Terraform**. Seleccione el nombre de la organización Terraform de la que forma parte en su cuenta de Terraform Cloud for Business.

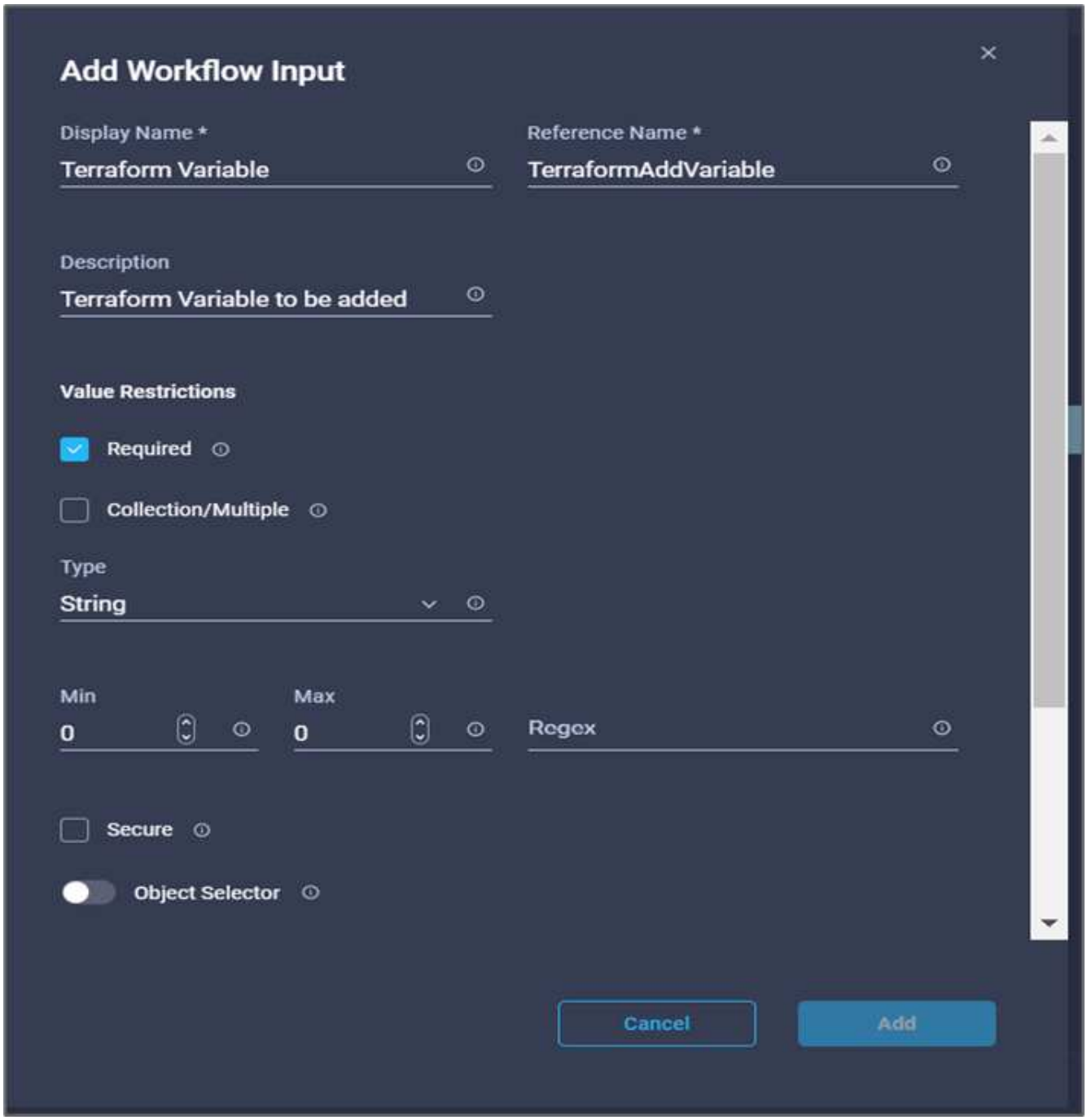


11. Haga clic en **Mapa**.
12. Haga clic en **Mapa** en el campo **Nombre de área de trabajo de Terraform**.
13. Elija **asignación directa** y haga clic en **salida de tareas**.
14. Haga clic en **Nombre de la tarea** y haga clic en **Agregar espacio de trabajo de Terraform**.



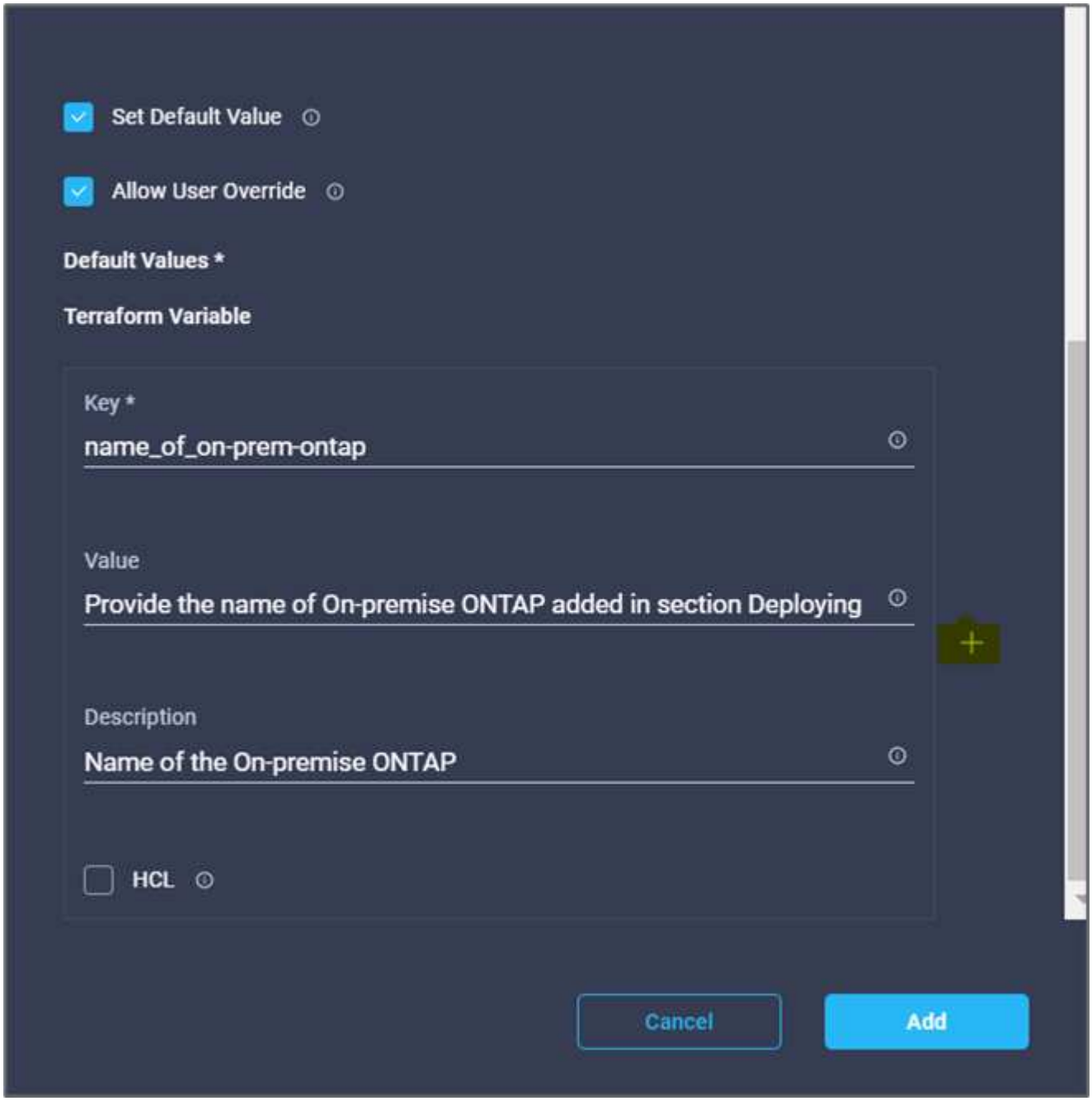
15. Haga clic en **Nombre de salida** y haga clic en **Nombre de área de trabajo**.

16. Haga clic en **Mapa**.
17. Haga clic en **Mapa** en el campo **Opciones de adición de variables**.
18. Elija **asignación directa** y haga clic en **Entrada de flujo de trabajo**.
19. Haga clic en **Nombre de entrada** y **Crear entrada de flujo de trabajo**.



20. En el asistente para agregar entrada, lleve a cabo los siguientes pasos:
    a. Proporcione un nombre para mostrar y un nombre de referencia (opcional).
    b. Asegúrese de seleccionar **String** para **Type**.
    c. Haga clic en **establecer valor predeterminado y en Reemplazar**.
    d. Haga clic en **Tipo de variable** y, a continuación, haga clic en **variables no sensibles**.

21. En la sección **Agregar variables de Terraform**, proporcione la siguiente información:
    - **Clave.** `name_of_on-prem-ontap`
    - **Valor.** proporcione el nombre de ONTAP en las instalaciones.
    - **Descripción.** Nombre del ONTAP en el hotel.
22. Haga clic en **+** para agregar variables adicionales.

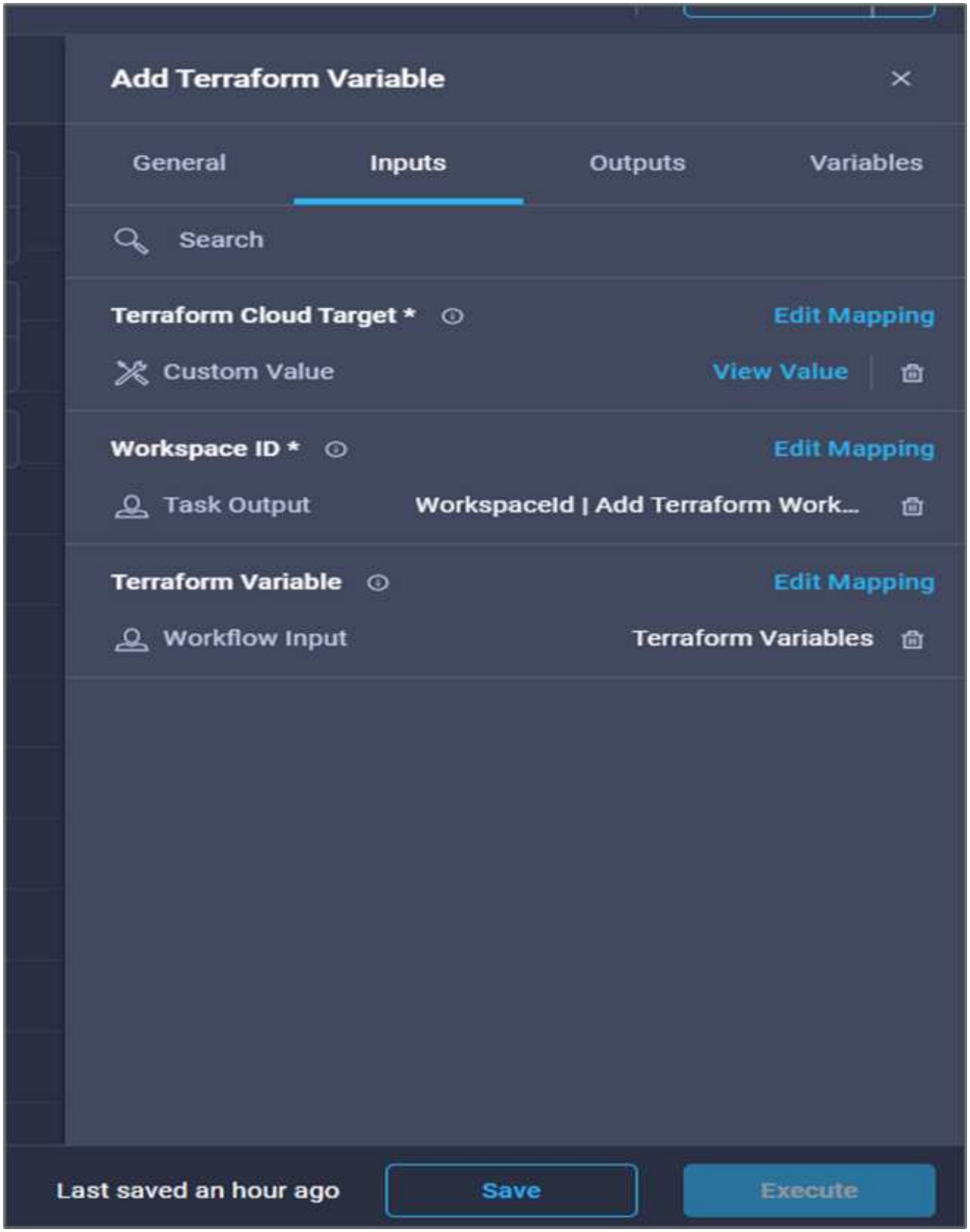


23. Agregue todas las variables Terraform tal y como se muestra en la siguiente tabla. También puede proporcionar un valor predeterminado.

Nombre de la variable Terraform	Descripción
nombre_de_en-local-ontap	Nombre del ONTAP en las instalaciones (FlexPod)

Nombre de la variable Terraform	Descripción
ip_cluster_local-ontap	La dirección IP de la interfaz de gestión del clúster de almacenamiento
on-prem-ontap_user_name	Nombre de usuario de administrador para el clúster de almacenamiento
Zona	Región de GCP donde se creará el entorno de trabajo
id_subred	ID de subred de GCP donde se creará el entorno de trabajo
vpc_id	El ID de VPC donde se creará el entorno de trabajo
nombre_paquete_capacidad	El tipo de licencia que se va a utilizar
volumen_origen	El nombre del volumen de origen
nombre_vm_almacenamiento_origen	El nombre de la SVM de origen
volumen_destino	Nombre del volumen en Cloud Volumes ONTAP
schedule_of_replication	El valor predeterminado es 1 hora
name_of_volume_to_create_on_cvo	El nombre del volumen de cloud
id_espacio_trabajo	Workspace_id donde se creará el entorno de trabajo
ID_proyecto	Project_id donde se creará el entorno de trabajo
nombre_de_cvo_cluster	El nombre del entorno de trabajo de Cloud Volumes ONTAP
gcp_service_account	gcp_service_account del entorno de trabajo de Cloud Volumes ONTAP

24. Haga clic en **Mapa** y luego en **Guardar**.



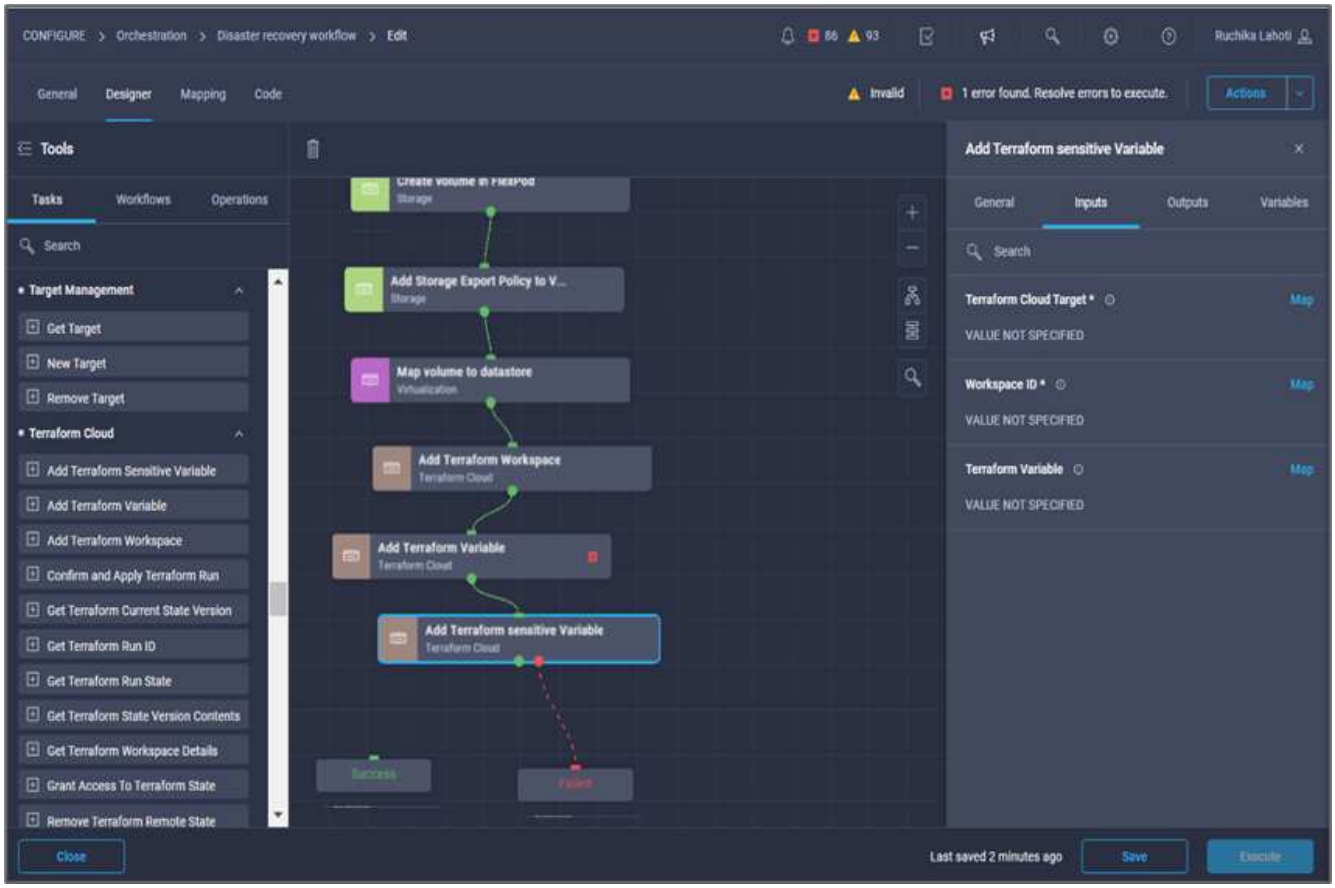
De esta forma, finaliza la tarea de agregar las variables de Terraform necesarias al área de trabajo. A continuación, agregue las variables Terraform sensibles necesarias al espacio de trabajo. También puede combinar ambos en una única tarea.

Procedimiento 7: Agregar variables sensibles a un área de trabajo

1. Vaya a la ficha **Diseñador** y haga clic en **flujos de trabajo** en la sección **Herramientas**.
2. Arrastre y suelte el flujo de trabajo **Terraform > Add Terraform variables** de la sección **Herramientas** del área **Diseño**.
3. Utilice Connector para conectar las dos tareas **Agregar espacio de trabajo de Terraform**. Haga clic en **Guardar**.

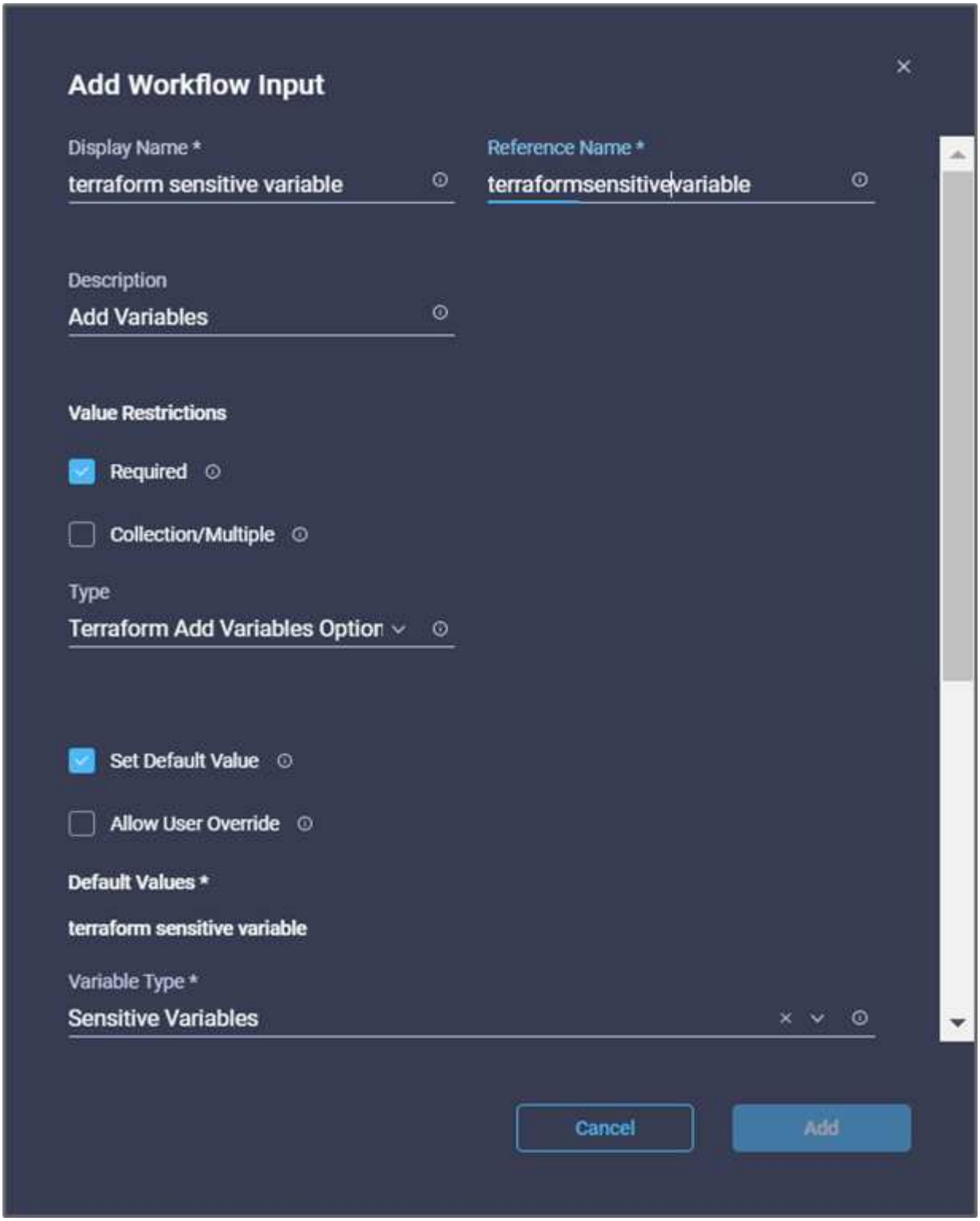
> Aparecerá una advertencia indicando que las dos tareas tienen el mismo nombre. Ignore el error por ahora porque cambia el nombre de la tarea en el paso siguiente.

4. Haga clic en **Agregar variables de Terraform**. En el área **Propiedades del flujo de trabajo**, haga clic en la ficha **General**. Cambie el nombre a **Agregar variables sensibles a Terraform**.



5. En el área **Propiedades del flujo de trabajo**, haga clic en **Entradas**.
6. Haga clic en **Mapa** en el campo **objetivo de la nube Terraform**.
7. Elija **valor estático** y haga clic en **Seleccionar destino de nube de Terraform**. Seleccione la cuenta de Terraform Cloud for Business que se agregó en la sección "Configure Cisco Intersight Service para HashiCorp Terraform".”
8. Haga clic en **Mapa**.
9. Haga clic en **Mapa** en el campo **Nombre de organización de Terraform**.
10. Elija **valor estático** y haga clic en **Seleccionar organización de Terraform**. Seleccione el nombre de la organización Terraform de la que forma parte en su cuenta de Terraform Cloud for Business.
11. Haga clic en **Mapa**.

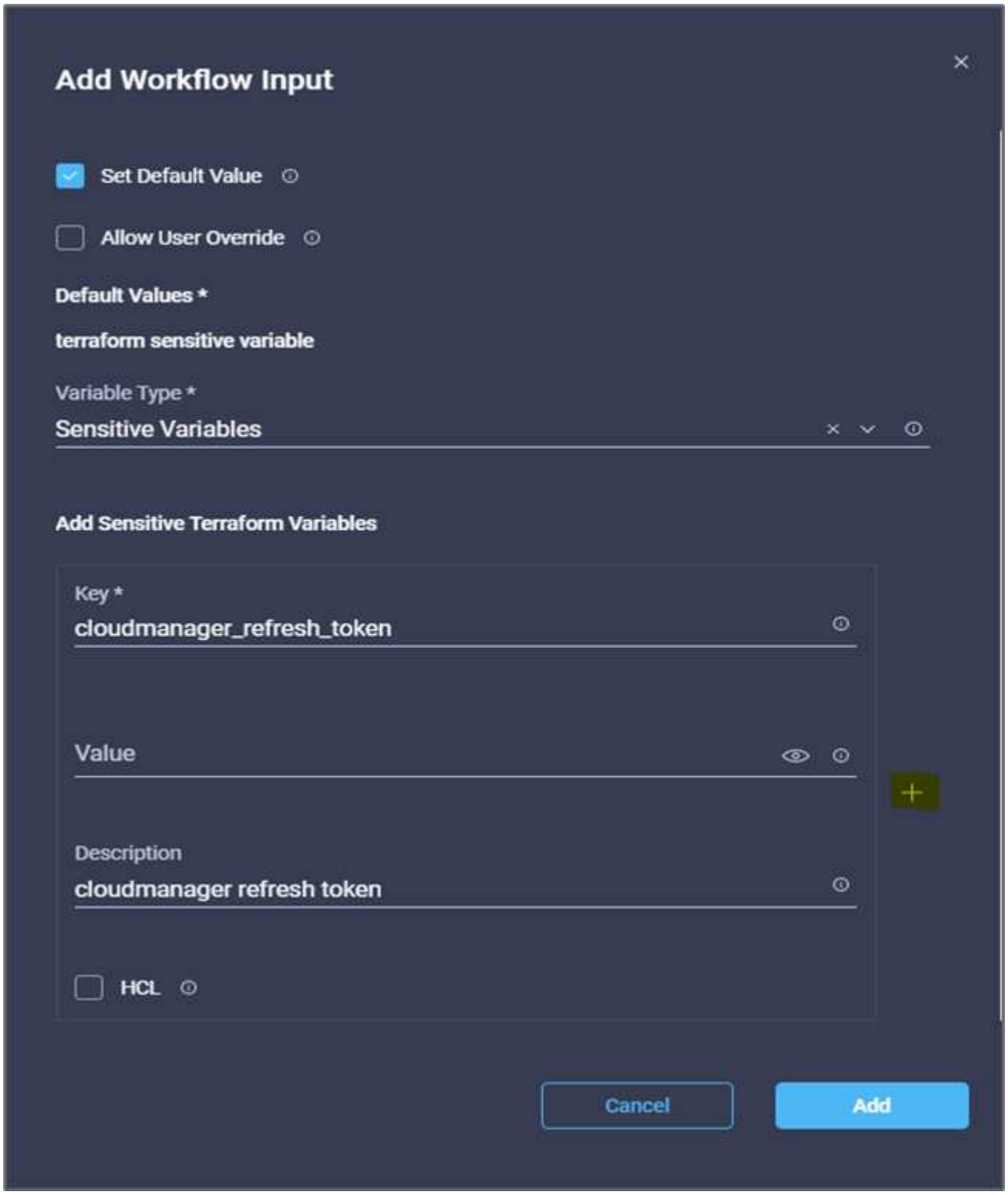
12. Haga clic en **Mapa** en el campo **Nombre de área de trabajo de Terraform**.
13. Elija **asignación directa** y haga clic en **salida de tareas**.
14. Haga clic en **Nombre de la tarea** y, a continuación, haga clic en **Agregar espacio de trabajo de Terraform**.
15. Haga clic en **Nombre de salida** y haga clic en la salida **Nombre de área de trabajo**.
16. Haga clic en **Mapa**.
17. Haga clic en **Mapa** en el campo **Opciones de adición de variables**.
18. Elija **asignación directa** y, a continuación, haga clic en **Entrada de flujo de trabajo**.
19. Haga clic en **Nombre de entrada** y **Crear entrada de flujo de trabajo**.
20. En el asistente para agregar entrada, lleve a cabo los siguientes pasos:
    a. Proporcione un nombre para mostrar y un nombre de referencia (opcional).
    b. Asegúrese de seleccionar **Terraform Agregar variables Opciones** para el tipo.
    c. Haga clic en **establecer valor predeterminado**.
    d. Haga clic en **Tipo de variable** y, a continuación, haga clic en **variables sensibles**.
    e. Haga clic en **Agregar**.



21. En la sección **Agregar variables de Terraform**, proporcione la siguiente información:

    - **Clave.** `cloudmanager_refresh_token`.
    - **Value.** Introduzca el token de actualización para operaciones de la API de Cloud Manager de NetApp.
    - **Descripción.** Actualizar token.

Si quiere más información sobre cómo obtener un token de actualización para las operaciones de la API de Cloud Manager de NetApp, consulte la sección ""“Configuración de requisitos previos del entorno”."



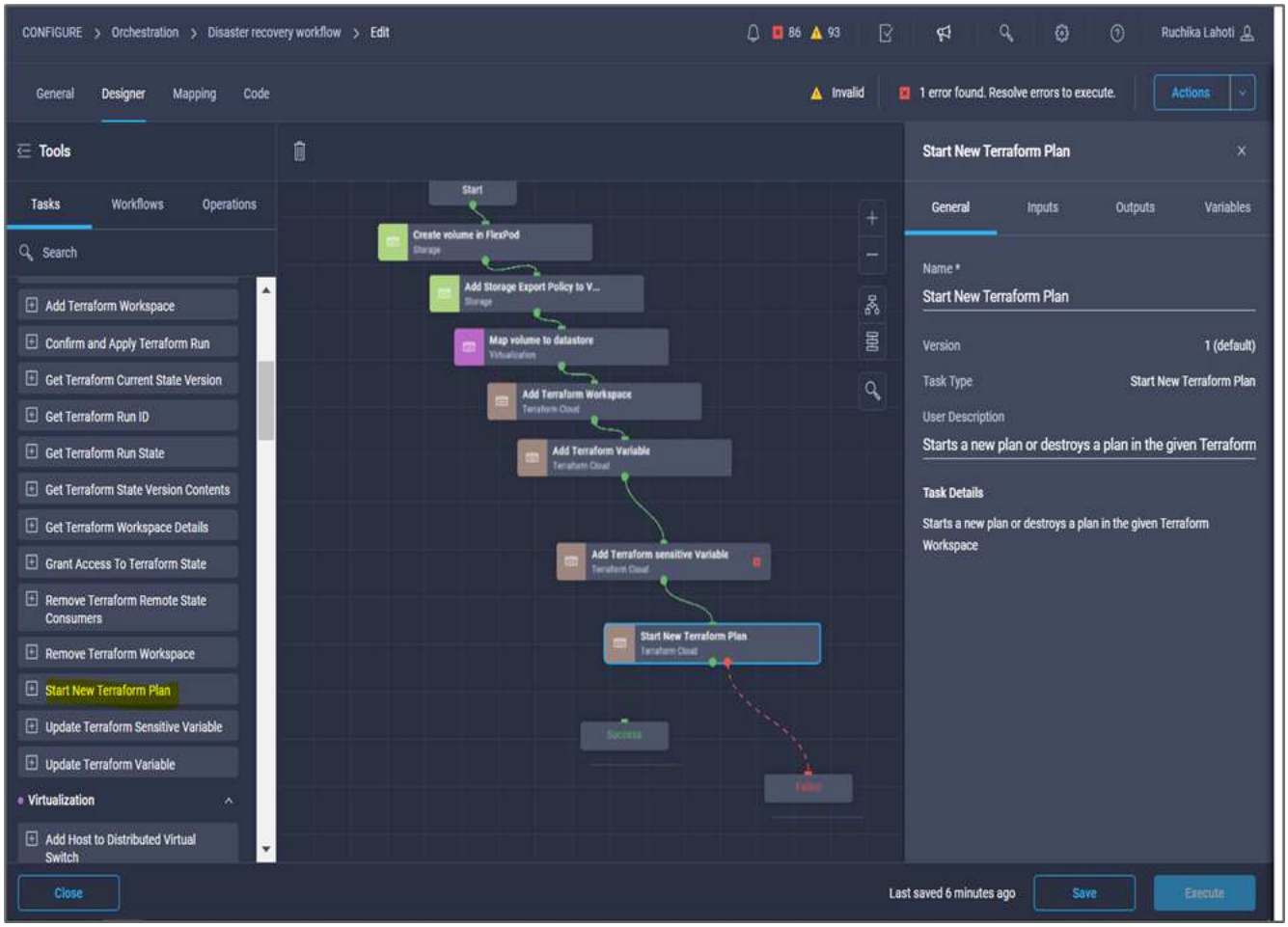
22. Agregue todas las variables sensibles a Terraform tal y como se muestra en la siguiente tabla. También puede proporcionar un valor predeterminado.

Nombre de variable sensible a la Terraform	Descripción
cloudmanager_refresh_token	Actualizar token. Obtenerlo de:
id_conector	El ID de cliente del conector de Cloud Manager. Obtener de
cvo_admin_password	La contraseña de administrador para Cloud Volumes ONTAP
on-prem-ontap_user_password	Contraseña de administrador para el clúster de almacenamiento

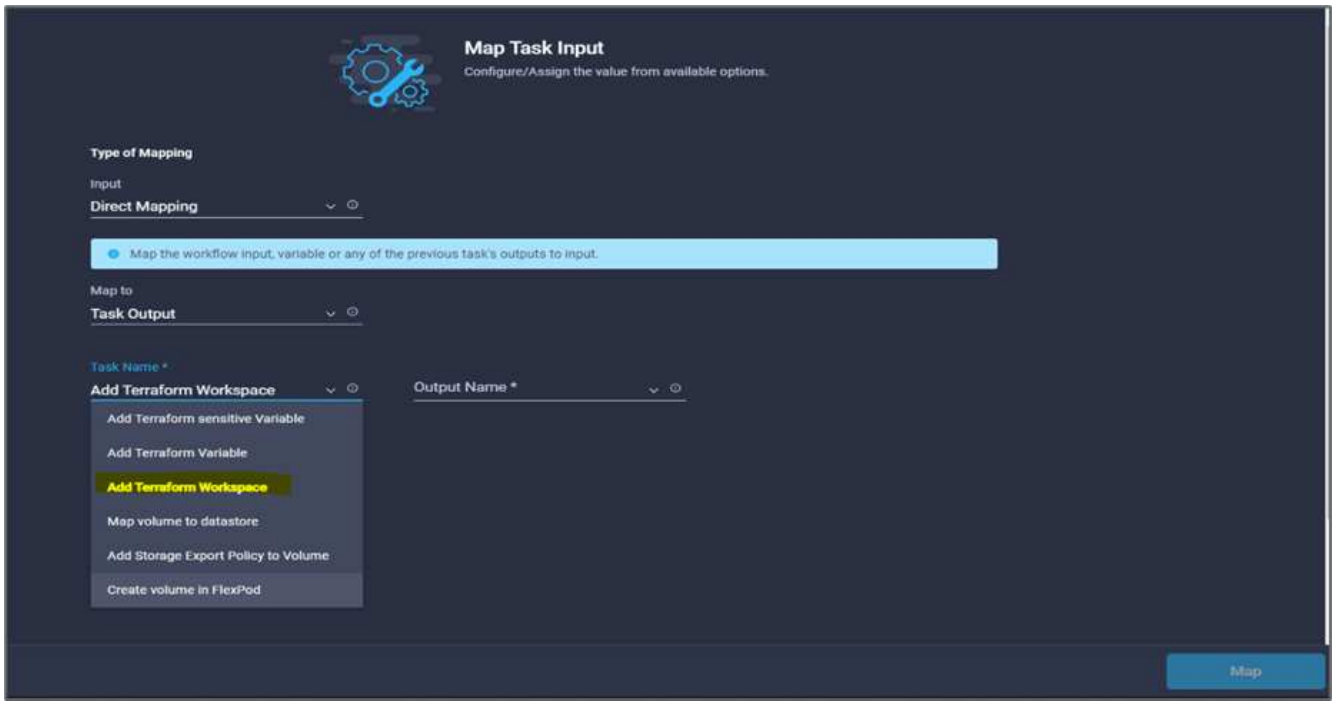
23. Haga clic en **Mapa**.con esto se completa la tarea de agregar las variables sensibles a Terraform necesarias al área de trabajo. A continuación, inicie un nuevo plan Terraform en el área de trabajo configurada.

Procedimiento 8: Iniciar un nuevo plan de Terraform

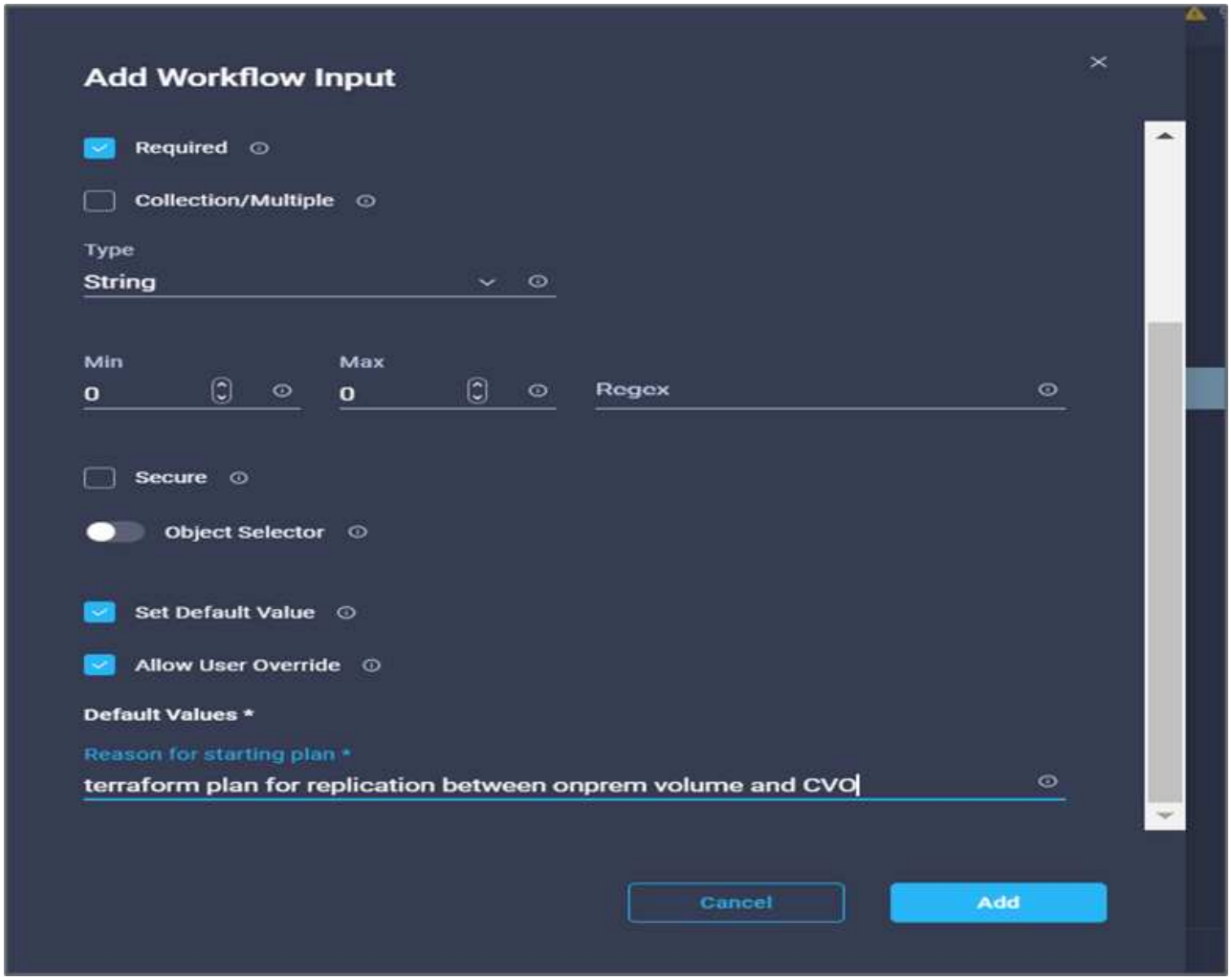
1. Vaya a la ficha **Diseñador** y haga clic en **tareas** en la sección **Herramientas**.
2. Arrastre y suelte la tarea **Terraform Cloud > Iniciar nuevo plan de Terraform** de la sección **Herramientas** del área **Diseño**.
3. Utilice el conector para conectar entre las tareas **Agregar variables sensibles a Terraform** y **Iniciar nuevas tareas del plan de Terraform**. Haga clic en **Guardar**.
4. Haga clic en **Iniciar nuevo plan de Terraform**. En el área **Propiedades de tarea**, haga clic en la ficha **General**. Opcionalmente, puede cambiar el nombre y la descripción de esta tarea.



5. En el área **Propiedades de tarea**, haga clic en **Entradas**.
6. Haga clic en **Mapa** en el campo **objetivo de la nube Terraform**.
7. Elija **valor estático** y haga clic en **Seleccionar destino de nube de Terraform**. Seleccione la cuenta Terraform Cloud for Business que se agregó en la sección “Configuración de Cisco Intersight Service para HashiCorp Terraform”.
8. Haga clic en **Mapa**.
9. Haga clic en **Mapa** en el campo **ID de área de trabajo**.
10. Elija **asignación directa** y haga clic en **salida de tareas**.
11. Haga clic en **Nombre de la tarea** y, a continuación, haga clic en **Agregar espacio de trabajo de Terraform**.



12. Haga clic en **Nombre de salida**, **ID de área de trabajo** y, a continuación, **Mapa**.
13. Haga clic en **Mapa** en el campo **motivo para iniciar el plan**.
14. Elija **asignación directa** y, a continuación, haga clic en **Entrada de flujo de trabajo**.
15. Haga clic en **Nombre de entrada** y luego en **Crear entrada de flujo de trabajo**.
16. En el asistente para agregar entrada, lleve a cabo los siguientes pasos:
    a. Proporcione un nombre para mostrar y un nombre de referencia (opcional).
    b. Asegúrese de seleccionar **String** para **Type**.
    c. Haga clic en **establecer valor predeterminado y en Reemplazar**.
    d. Introduzca un valor predeterminado para **razón para iniciar el plan** y haga clic en **Agregar**.



17. Haga clic en **Mapa**.
18. Haga clic en **Mapa** en el campo **operación del plan**.
19. Elija **valor estático** y haga clic en **operación del plan**. Haga clic en **nuevo plan**.



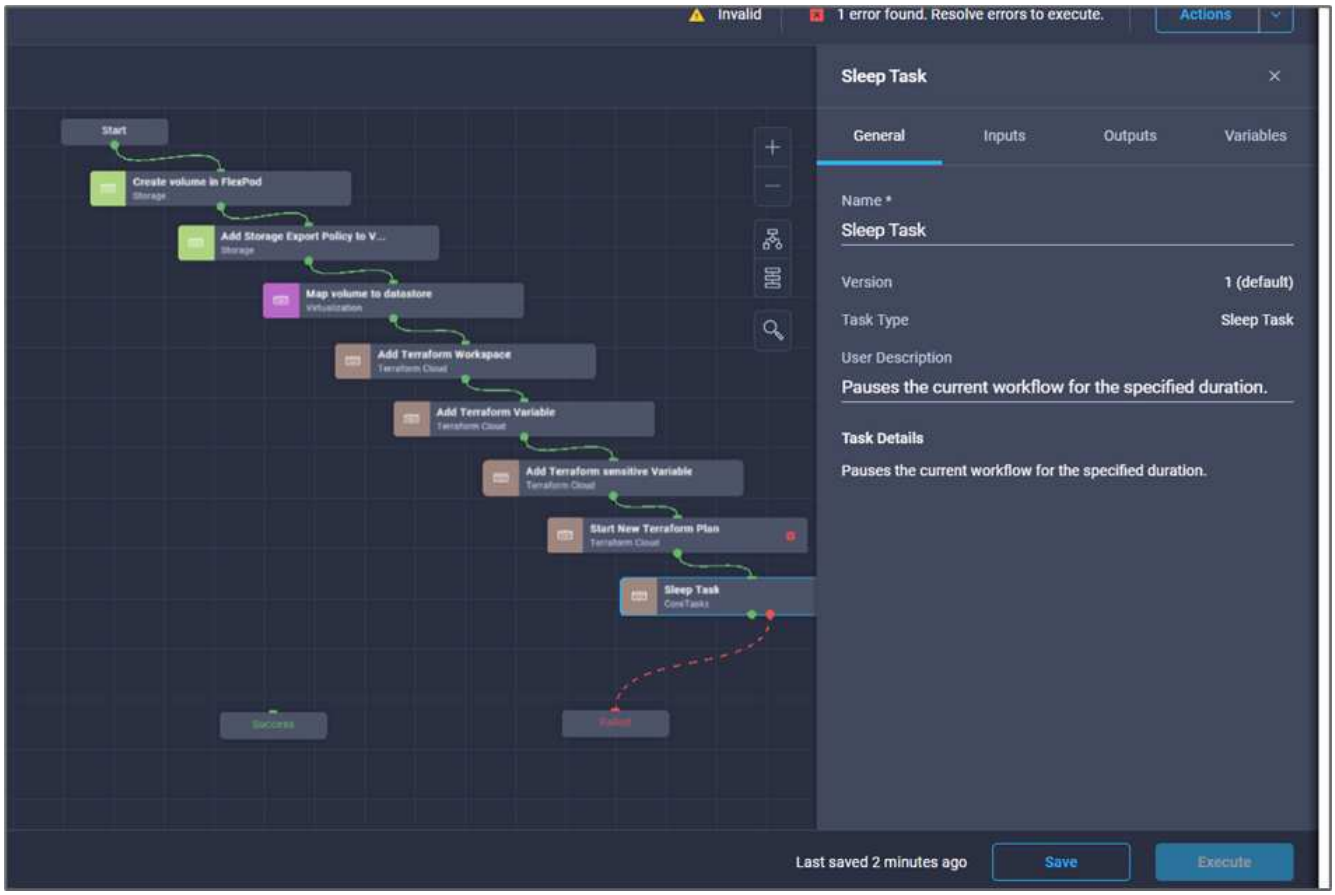
20. Haga clic en **Mapa**.
21. Haga clic en **Guardar**.

Esto completa la tarea de agregar un plan de Terraform en la cuenta de Terraform Cloud para Business. A continuación, cree una tarea de suspensión durante unos segundos.

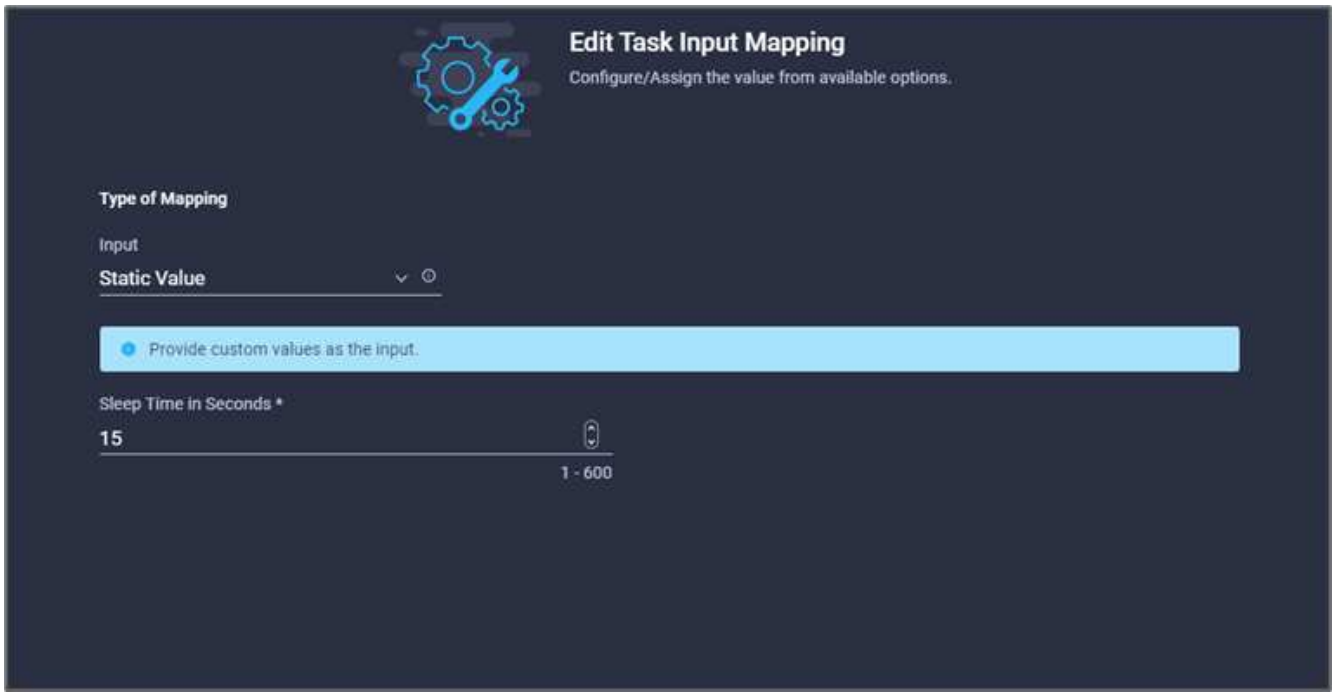
Procedimiento 9: Tarea de reposo para la sincronización

Terraform Apply requiere RunID, que se genera como parte de la tarea Plan Terraform. Esperar unos segundos entre el Plan Terraform y Terraform aplicar acciones evita problemas de tiempo.

1. Vaya a la ficha **Diseñador** y haga clic en **tareas** en la sección **Herramientas**.
2. Arrastre y suelte **tareas principales > tarea de suspensión** de la sección **Herramientas** del área **Diseño**.
3. Utilice el conector para conectar las tareas **Iniciar nuevo plan de Terraform** y **tarea de suspensión**. Haga clic en **Guardar**.



4. Haga clic en **tarea de suspensión**. En el área **Propiedades de tarea**, haga clic en la ficha **General**. Opcionalmente, puede cambiar el nombre y la descripción de esta tarea. En este ejemplo, el nombre de la tarea es **Sincronizar**.
5. En el área **Propiedades de tarea**, haga clic en **Entradas**.
6. Haga clic en **Mapa** en el campo **tiempo de inactividad en segundos**.
7. Seleccione **valor estático** e introduzca **15** en para el **tiempo de inactividad en segundos**.

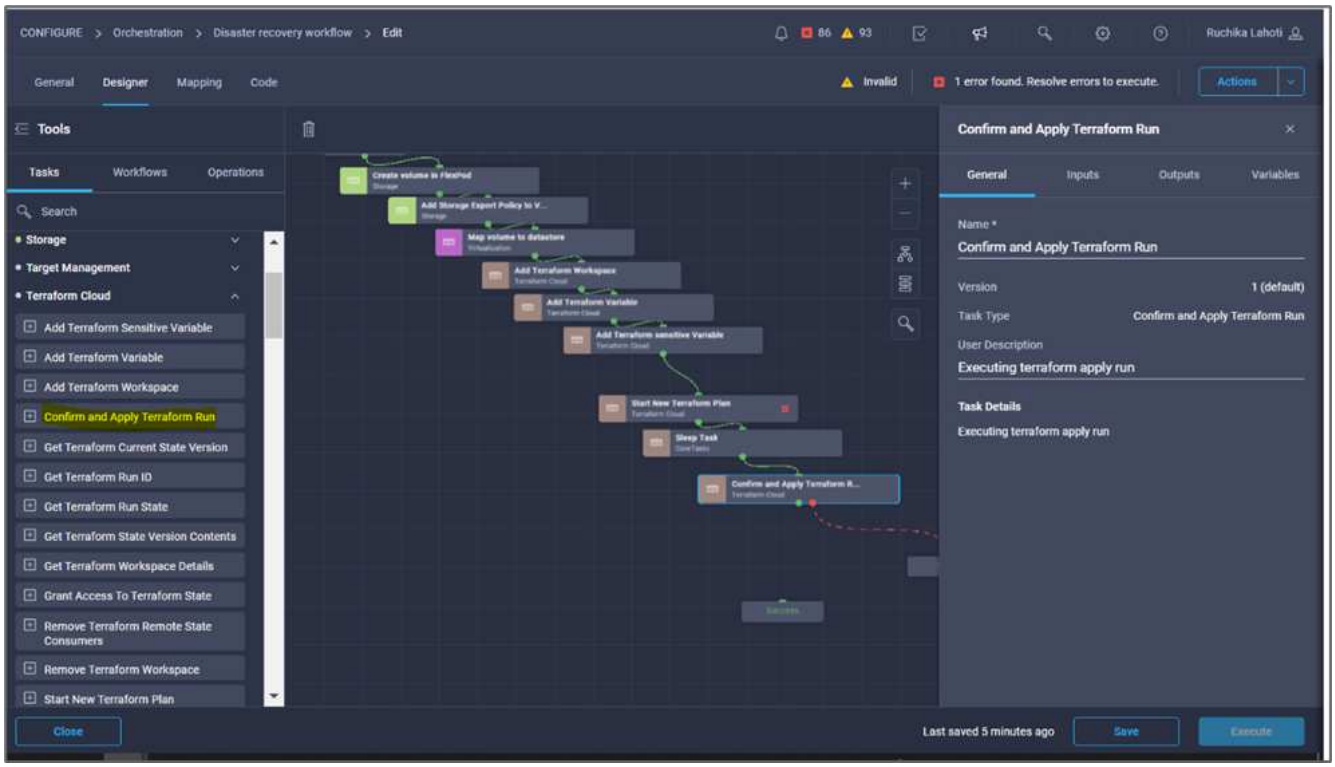


8. Haga clic en **Mapa**.
9. Haga clic en **Guardar**.

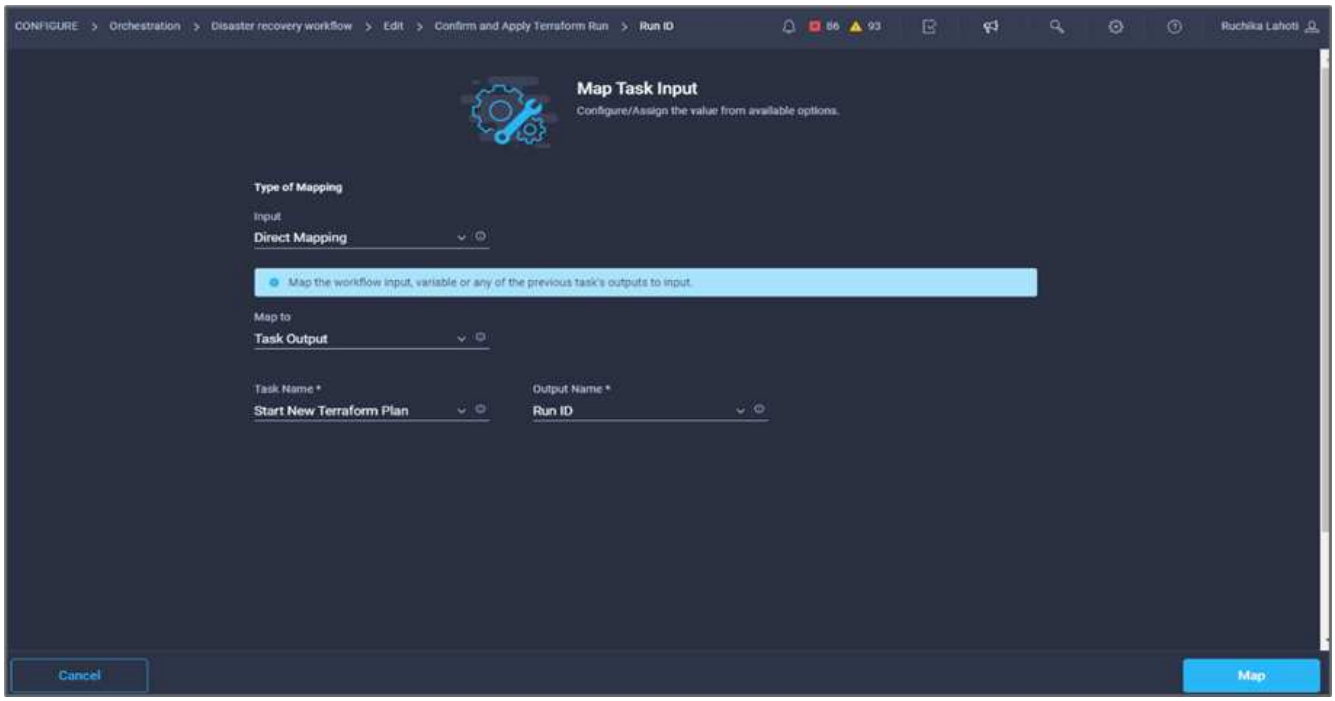
Así finaliza la tarea de suspensión. A continuación, cree la última tarea de este flujo de trabajo, confirmando y aplicando la ejecución de Terraform.

Procedimiento 10: Confirmar y aplicar la ejecución de Terraform

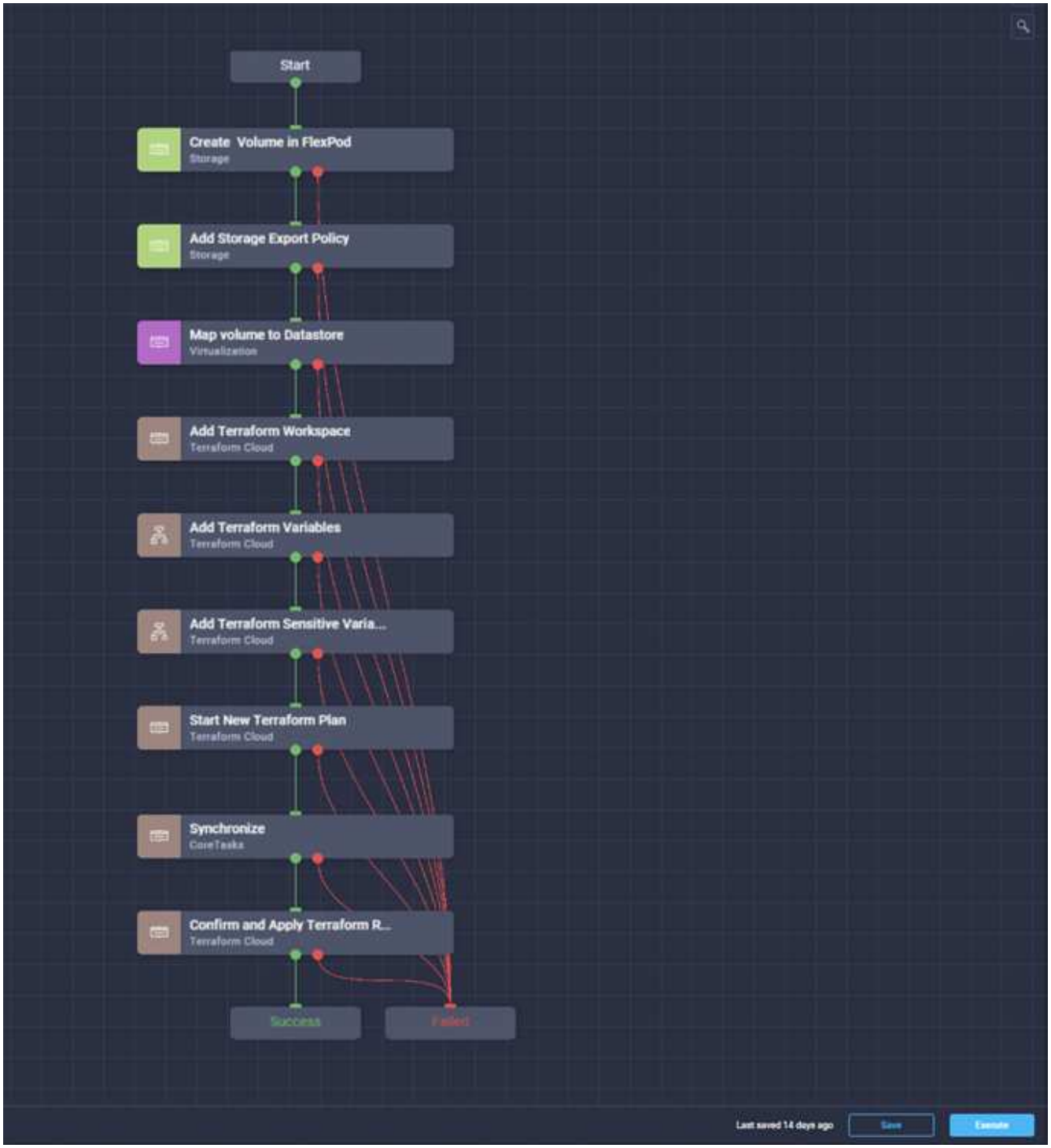
1. Vaya a la ficha **Diseñador** y haga clic en **tareas** en la sección **Herramientas**.
2. Arrastre y suelte la tarea **Terraform Cloud > Confirmar y aplicar ejecución de Terraform** de la sección **Herramientas** del área **Diseño**.
3. Utilice el conector para conectar las tareas **Sincronizar** y **Confirmar y aplicar la ejecución de Terraform**. Haga clic en **Guardar**.
4. Haga clic en **Confirmar** y **aplicar ejecución de Terraform**. En el área **Propiedades de tarea**, haga clic en la ficha **General**. Opcionalmente, puede cambiar el nombre y la descripción de esta tarea.



5. En el área **Propiedades de tarea**, haga clic en **Entradas**.
6. Haga clic en **Mapa** en el campo **objetivo de la nube Terraform**.
7. Elija **valor estático** y haga clic en **Seleccionar destino de nube de Terraform**. Seleccione la cuenta de Terraform Cloud for Business que se agregó en "Configure Cisco Intersight Service para HashiCorp Terraform".”
8. Haga clic en **Mapa**.
9. Haga clic en **Mapa** en el campo **ID de ejecución**.
10. Elija **asignación directa** y haga clic en **salida de tareas**.
11. Haga clic en **Nombre de la tarea** y haga clic en **Iniciar nuevo plan de Terraform**.
12. Haga clic en **Nombre de salida** y, a continuación, haga clic en **ID de ejecución**.



13. Haga clic en **Mapa**.
14. Haga clic en **Guardar**.
15. Haga clic en **flujo de trabajo de alineación automática** para que todas las tareas estén alineadas. Haga clic en **Guardar**.



De esta forma se completa la tarea Confirmar y aplicar ejecución de Terraform. Utilice el conector para conectar entre la tarea **Confirmar y aplicar ejecución de Terraform** y las tareas **éxito** y **fallido**.

Procedimiento 11: Importar un flujo de trabajo generado por Cisco

Cisco InterSight Cloud Orchestrator le permite exportar flujos de trabajo de una cuenta de Cisco Intersight al sistema y, a continuación, importarlos a otra cuenta. Se creó un archivo JSON exportando el flujo de trabajo creado que se puede importar a su cuenta.

Hay disponible un archivo JSON para el componente de flujo de trabajo en la "Repositorio de GitHub".

"Siguiente: Ejecución de Terraform desde la controladora."

Ejecución de Terraform desde la controladora

"Anterior: Flujo de trabajo de recuperación ante desastres."

Podemos ejecutar el plan de Terraform con una controladora. Puede omitir esta sección si ya ha ejecutado su plan de Terraform mediante un flujo de trabajo ICO.

Requisitos previos

La configuración de la solución comienza con una estación de trabajo de gestión que tiene acceso a Internet y con una instalación de Terraform en funcionamiento.

Puede encontrar una guía para instalar Terraform "aquí".

Clonar GitHub repo

El primer paso del proceso es clonar GitHub repo en una nueva carpeta vacía de la estación de trabajo de gestión. Para clonar el repositorio de GitHub, complete los siguientes pasos:

1. Desde la estación de trabajo de gestión, cree una nueva carpeta para el proyecto. Cree una nueva carpeta dentro de esta carpeta llamada `/root/snapmirror-cvo` Y Clone GitHub repo en él.
2. Abra una línea de comandos o una interfaz de consola en la estación de trabajo de administración y cambie los directorios a la nueva carpeta que acaba de crear.
3. Clone la colección GitHub con el siguiente comando:

```
Git clone https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO
```

1. Cambie los directorios a la nueva carpeta llamada `snapmirror-cvo`.

Ejecución de Terraform



- **Init.** inicialice el entorno de Terraform (local). Normalmente se ejecuta sólo una vez por sesión.
- **Plan.** Compare el estado de la terraform con el estado como en la nube y construya y visualice un plan de ejecución. Esto no modifica la implementación (sólo lectura).
- **Aplicar.** aplicar el plan desde la fase del plan. Esto puede cambiar potencialmente la implementación (lectura y escritura).
- **Destruir.** todos los recursos que se rigen por este entorno de Terraform específico.

  Para obtener más información, consulte "aquí".

"Siguiente: Validación de la solución."

Validación de la solución

"Anterior: Ejecución de Terraform desde la controladora."

En esta sección, vamos a revisar la solución con un flujo de trabajo de replicación de datos de muestra y realizamos algunas mediciones para verificar la integridad de la replicación de datos desde la instancia de ONTAP de NetApp que se ejecuta en FlexPod a Cloud Volumes ONTAP de NetApp en Google Cloud.

Utilizamos Cisco Intersight Workflow orchestrator en esta solución y seguiremos utilizándose en nuestro caso de uso.

Cabe destacar que el conjunto limitado de flujos de trabajo de Cisco Intersight utilizados en esta solución no representa el conjunto completo de flujos de trabajo con los que está equipado Cisco Intersight. Puede crear flujos de trabajo personalizados en función de sus requisitos específicos y hacer que se activen desde Cisco Intersight.

Para validar una situación correcta de recuperación ante desastres, mueva primero los datos desde un volumen en ONTAP que forme parte de FlexPod a Cloud Volumes ONTAP mediante SnapMirror. Entonces, puede intentar acceder a los datos desde la instancia de computación en cloud de Google seguida de una comprobación de integridad de los datos.

Los siguientes pasos de alto nivel se utilizan para comprobar los criterios de éxito de esta solución:

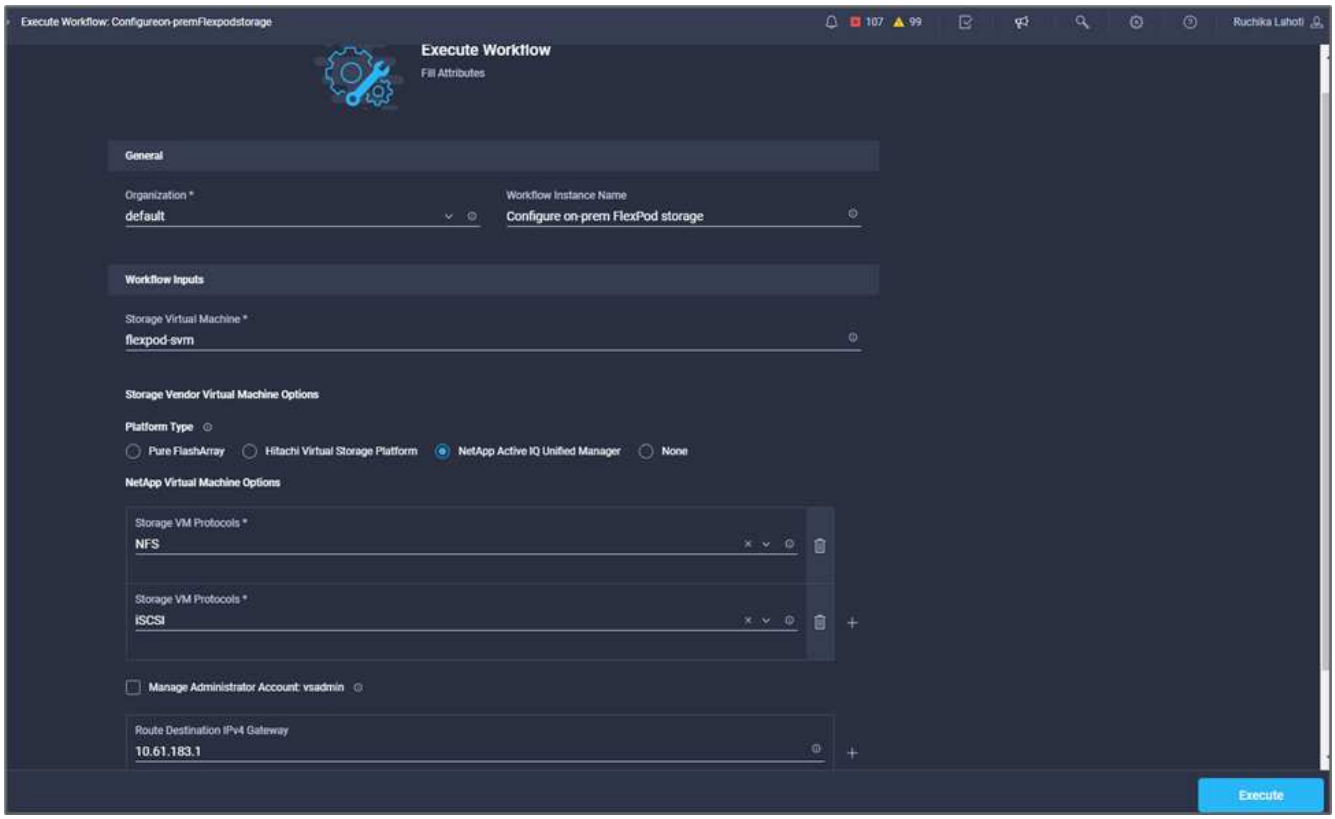
1. Genere una suma de comprobación SHA256 en el conjunto de datos de muestra que está presente en un volumen ONTAP en FlexPod.
2. Configure una relación de SnapMirror para volúmenes entre ONTAP en FlexPod y Cloud Volumes ONTAP.
3. Replique el conjunto de datos de ejemplo de FlexPod en Cloud Volumes ONTAP.
4. Rompa la relación de SnapMirror y promocione el volumen en Cloud Volumes ONTAP a la fase de producción.
5. Asigne el volumen Cloud Volumes ONTAP con el conjunto de datos a una instancia informática en Google Cloud.
6. Genere una suma de comprobación SHA256 en el conjunto de datos de ejemplo en Cloud Volumes ONTAP.
7. Compare la suma de comprobación en el origen y en el destino; presumiblemente, las sumas de comprobación de ambas partes coinciden.

Para ejecutar el flujo de trabajo en las instalaciones, complete los siguientes pasos:

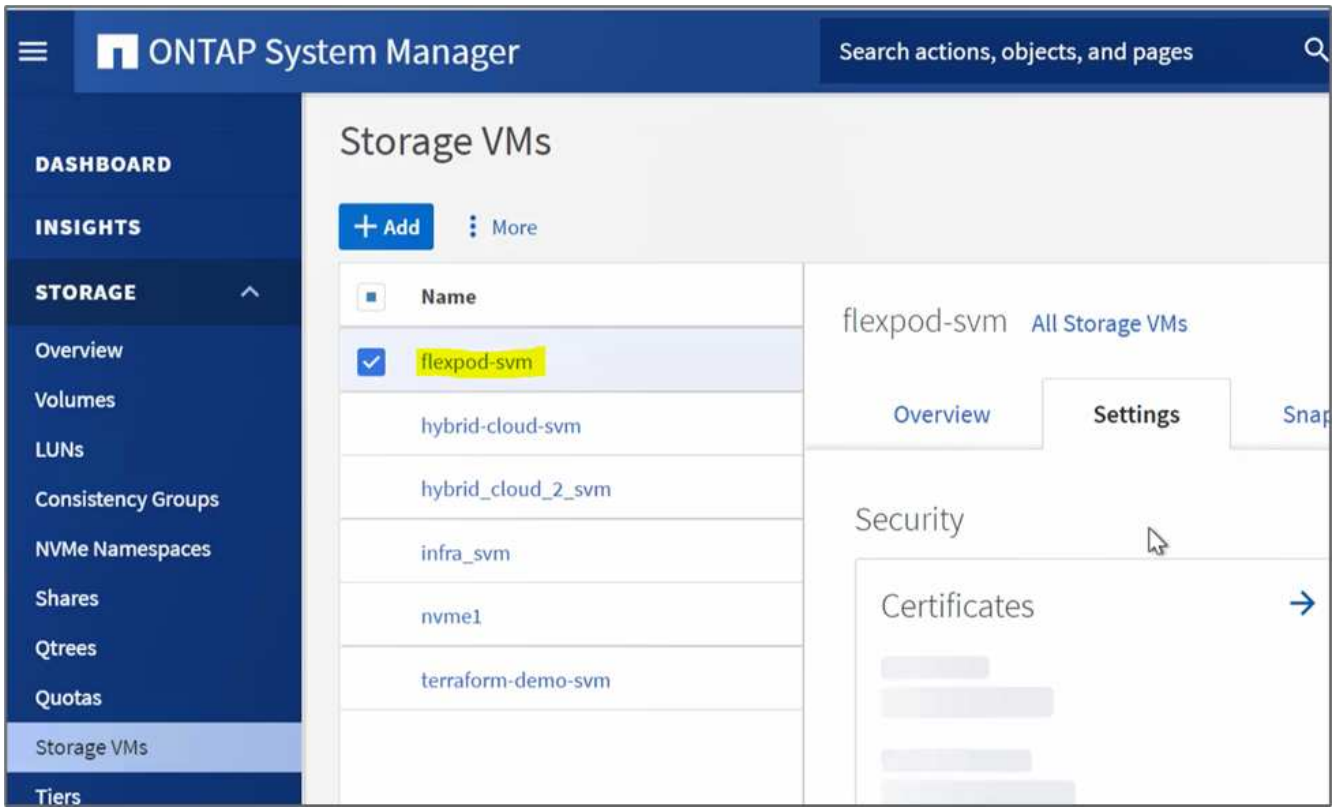
1. Cree un flujo de trabajo en Intersight para FlexPod en las instalaciones.



2. Proporcione las entradas necesarias y ejecute el flujo de trabajo.



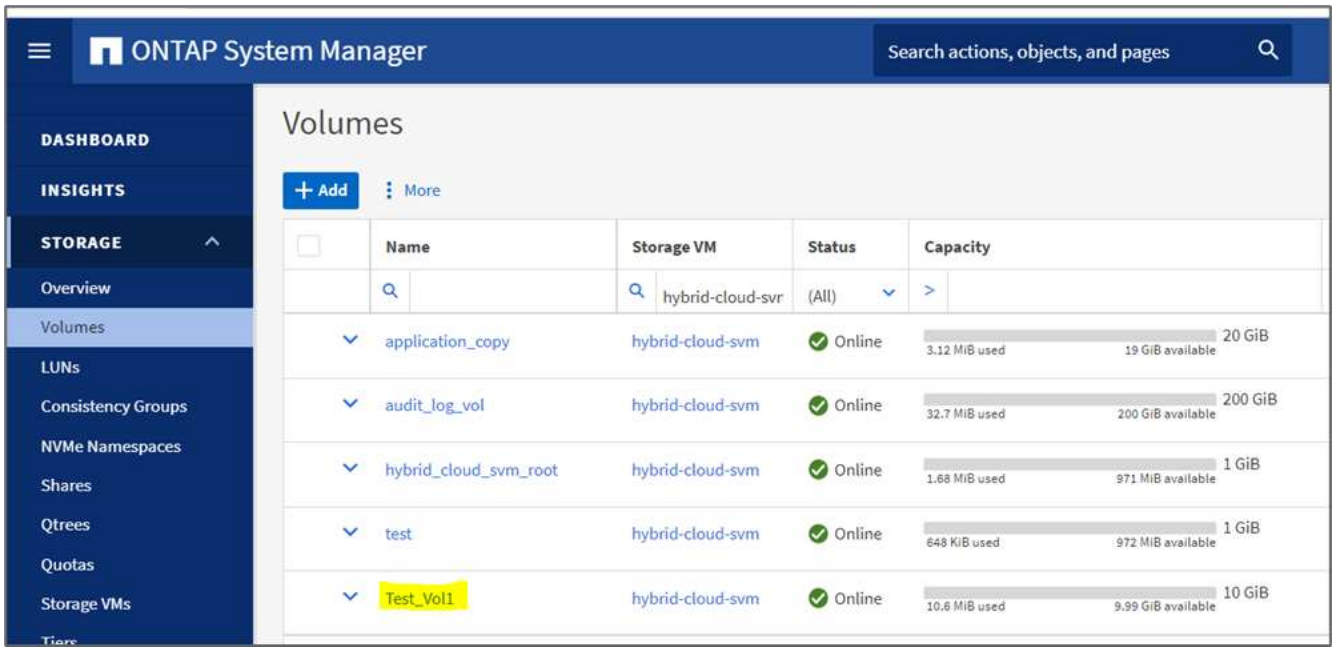
3. Compruebe la SVM recién creada en el administrador del sistema.



4. Cree y ejecute otro flujo de trabajo de recuperación ante desastres para crear un volumen en FlexPod en las instalaciones y establecer una relación de SnapMirror entre este volumen en FlexPod y Cloud Volumes ONTAP.



5. Compruebe el volumen recién creado en el administrador del sistema ONTAP.

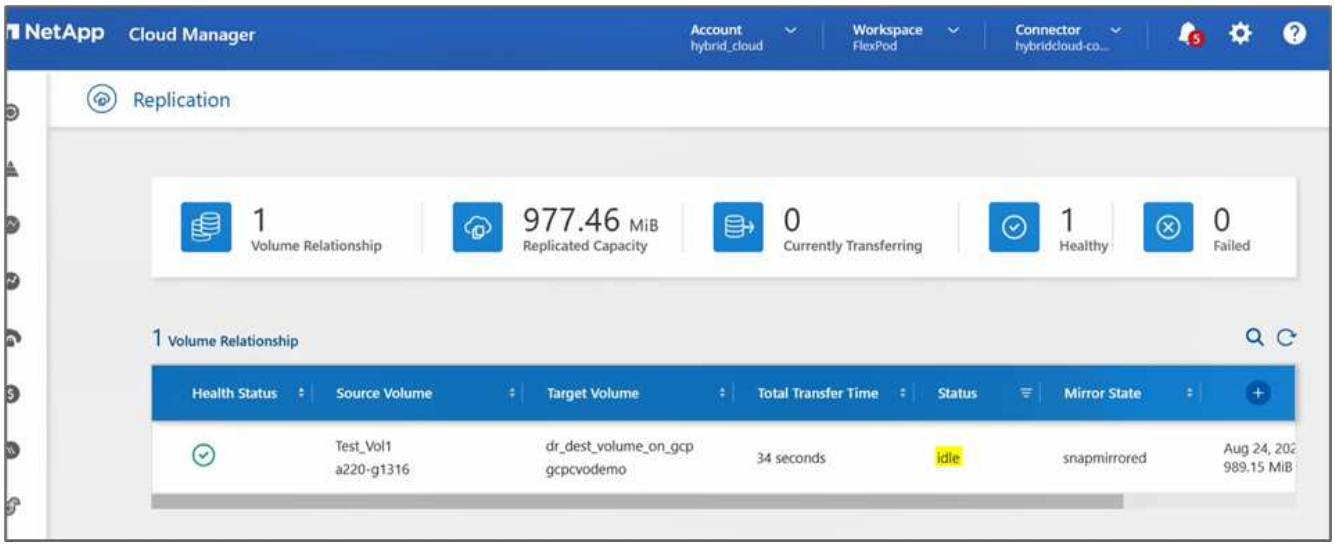


6. Monte el mismo volumen NFS en una máquina virtual local, a continuación, copie el conjunto de datos de muestra y realice la suma de comprobación.

```
root@hybridcloudbackup:/snapmirror_demo# mount -t nfs 172.22.4.157:/Test_Vol1 /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo# df -kh
Filesystem                Size  Used Avail Use% Mounted on
udev                      1.9G     0  1.9G   0% /dev
tmpfs                     394M  1.1M  393M   1% /run
/dev/sda2                  16G   11G  4.2G  72% /
tmpfs                     2.0G     0  2.0G   0% /dev/shm
tmpfs                     5.0M     0  5.0M   0% /run/lock
tmpfs                     2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/loop1                 55M   55M     0 100% /snap/core18/1705
/dev/loop2                 69M   69M     0 100% /snap/lxd/14804
/dev/loop0                 28M   28M     0 100% /snap/snapd/7264
172.22.4.157:/Test_Vol1    10G  512K   10G   1% /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo#
```

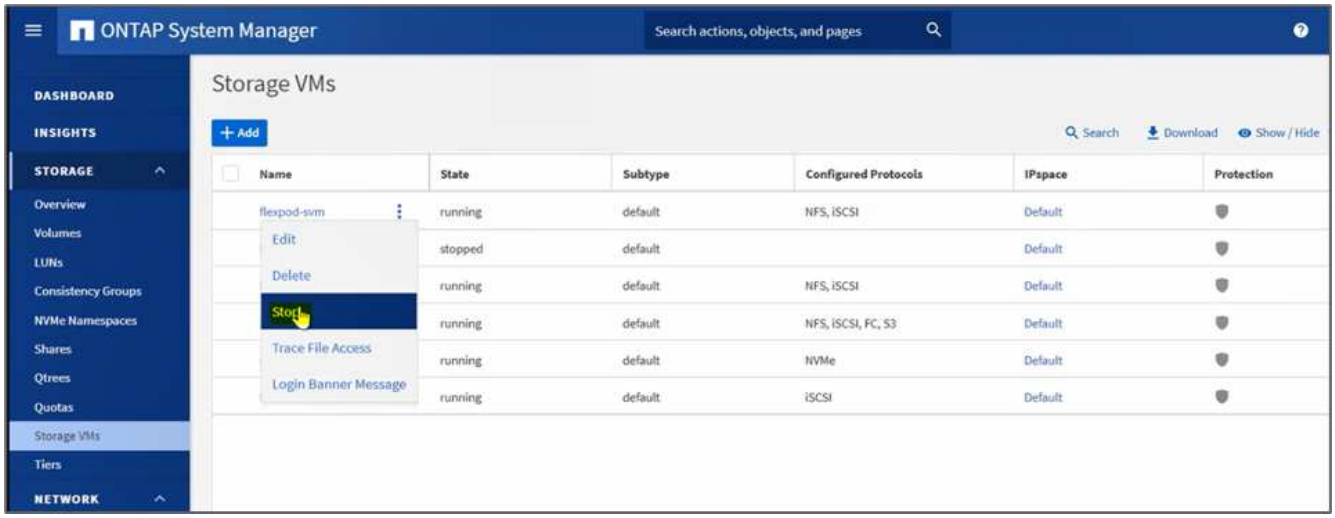
```
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo# sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo#
```

7. Compruebe el estado de replicación en Cloud Manager. La transferencia de datos puede tardar unos minutos en función del tamaño de los datos. Una vez finalizado, puede ver el estado de SnapMirror como **inactivo**.

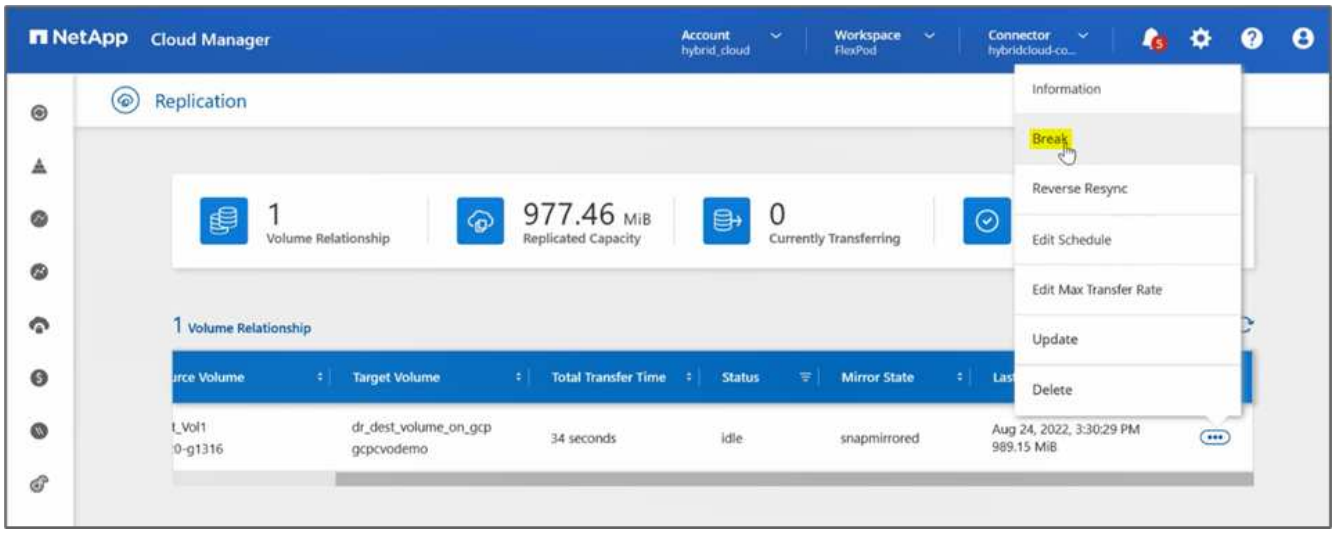


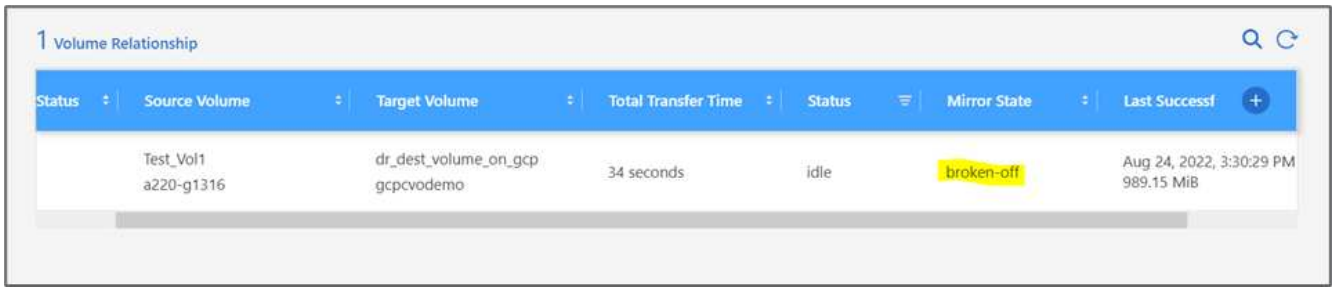
8. Una vez finalizada la transferencia de datos, simule un desastre en el origen deteniendo la SVM que aloja `Test_vol1` volumen.

   Una vez detenida la SVM, el `Test_vol1` El volumen no está visible en Cloud Manager.

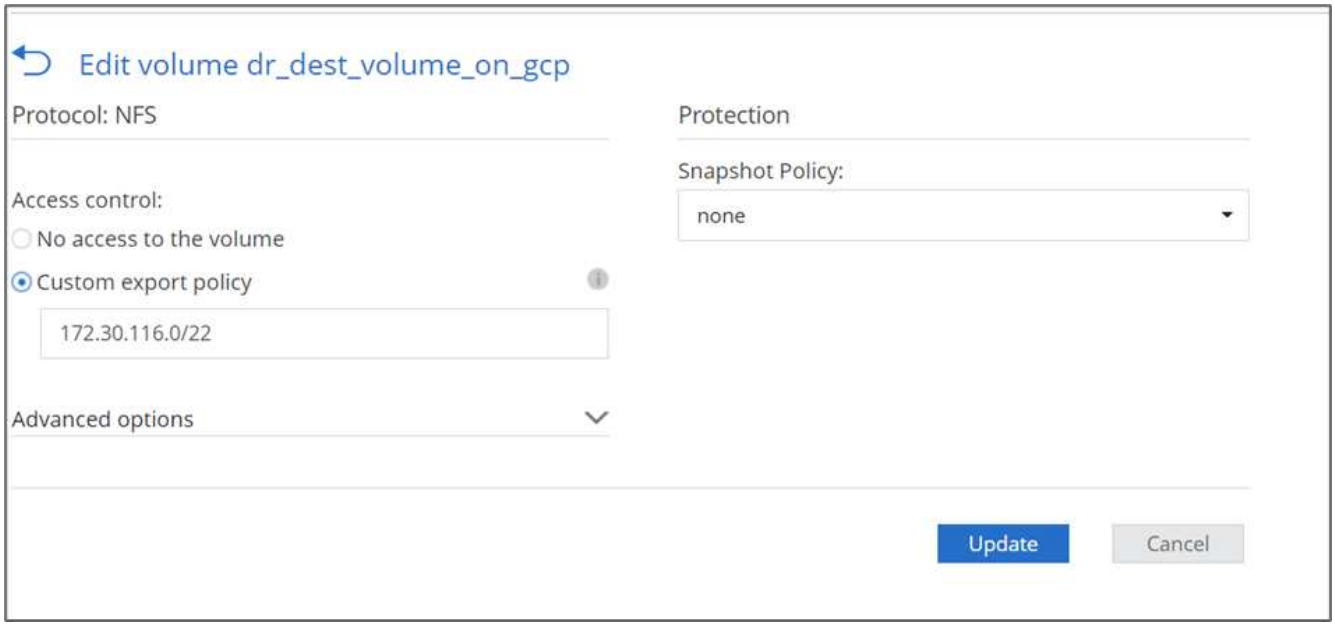


9. Rompa la relación de replicación y promocione el volumen de destino de Cloud Volumes ONTAP a la fase de producción.

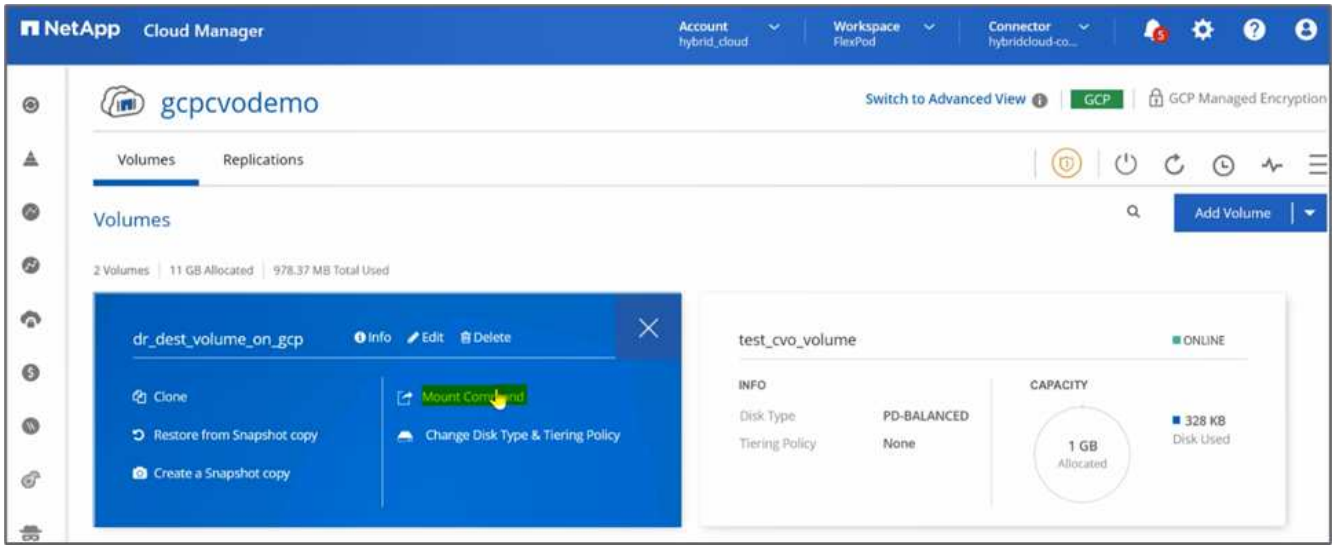




10. Edite el volumen y habilite el acceso del cliente asociándolo a una política de exportación.



11. Obtenga el comando de montaje listo para usar del volumen.





12. Monte el volumen en una instancia de computación, compruebe que los datos están presentes en el volumen de destino y genere la suma de comprobación SHA256 del `sample_dataset_2GB` archivo.

```
drwxr-xr-x 21 root   root            4096 Aug 24 10:20 ../
-rwxr-xr-x  1 nobody 4294967294 1015306240 Aug 24 09:59 test.zip*
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$ sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
```

13. Compare los valores de suma de comprobación tanto en el origen (FlexPod) como en el destino (Cloud Volumes ONTAP).
14. Las sumas de comprobación coinciden con el origen y el destino.

Puede confirmar que la replicación de datos del origen al destino se ha completado correctamente y que se ha mantenido la integridad de los datos. Ahora los datos los pueden consumir las aplicaciones con seguridad para atender a los clientes mientras el sitio de origen pasa por su restauración.

"Siguiente: Conclusión."

Conclusión

"Anterior: Validación de la solución."

En esta solución, el servicio de datos en el cloud de NetApp, la infraestructura de Cloud Volumes ONTAP y el centro de datos de FlexPod se usaron para crear una solución de recuperación ante desastres con un cloud público con la tecnología de Cisco Intersight Cloud Orchestrator. La solución de FlexPod ha evolucionado constantemente para permitir a los clientes modernizar sus aplicaciones y procesos de entrega de negocio. Con esta solución, puede crear un plan BCDR con el cloud público mientras se utiliza la ubicación para un plan de recuperación ante desastres puntual o a tiempo completo, sin por ello dejar de mantener el coste de la solución de recuperación ante desastres bajo.

La replicación de datos entre FlexPod en las instalaciones y Cloud Volumes ONTAP de NetApp se realizó mediante la tecnología SnapMirror contrastada, pero también puede seleccionar otras herramientas de transferencia y sincronización de datos de NetApp como Cloud Sync para sus requisitos de movilidad de datos. Seguridad de los datos en tránsito gracias a las tecnologías de cifrado integradas basadas en TLS/AES.

Independientemente de que tenga un plan temporal de recuperación ante desastres para una aplicación o un plan de recuperación ante desastres a tiempo completo para una empresa, la cartera de productos utilizados en esta solución puede satisfacer ambos requisitos a escala. Con la tecnología de Cisco InterSight Workflow Orchestrator, también se puede automatizar con flujos de trabajo preconfigurados que no solo eliminen la necesidad de reconstruir procesos, sino que también aceleren la implementación de un plan BCDR.

La solución permite la gestión de FlexPod en las instalaciones y la replicación de datos en un cloud híbrido de una forma muy sencilla y cómoda con automatización y orquestación proporcionada por Cisco Intersight Cloud Orchestrator.

Dónde encontrar información adicional

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

GitHub

- Todas las configuraciones de Terraform utilizadas

  "https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO"

- Archivos JSON para la importación de flujos de trabajo

  "https://github.com/ucs-compute-solutions/FlexPod_DR_Workflows"

Cisco Intersight

- Centro de ayuda de Cisco Intersight

  "https://intersight.com/help/saas/home"

- Documentación de Cisco Intersight Cloud Orchestrator:

  "https://intersight.com/help/saas/features/orchestration/configure#intersight_cloud_orchestrator"

- Cisco Intersight Service para la Documentación de Terraform de HashiCorp

  "https://intersight.com/help/saas/features/terraform_cloud/admin"

- Hoja de datos de Cisco Intersight

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html"

- Hoja de datos de Cisco Intersight Cloud Orchestrator

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-cloud-orch-aag-cte-en.html"

- Hoja de datos de Terraform del servicio Cisco Intersight para HashiCorp

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-terraf-ser-aag-cte-en.html"

FlexPod

- Página de inicio de FlexPod

  "https://www.flexpod.com"

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

  "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"

- Centro de datos FlexPod con Cisco UCS X-Series

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

Interoperabilidad

- Herramienta de matriz de interoperabilidad de NetApp

  "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"

- Guía de compatibilidad de VMware

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

Documentos de referencia Cloud Volumes ONTAP de NetApp

- Cloud Manager de NetApp

  "https://docs.netapp.com/us-en/occm/concept_overview.html"

- Cloud Volumes ONTAP

  https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-gcp.html

- Calculadora del coste total de propiedad de Cloud Volumes ONTAP

  https://cloud.netapp.com/google-cloud-calculator

- Dimensionador Cloud Volumes ONTAP

  "https://cloud.netapp.com/cvo-sizer"

- Herramienta de evaluación de cloud

  https://cloud.netapp.com/assessments

- Cloud híbrido de NetApp

  https://cloud.netapp.com/hybrid-cloud

- Documentación sobre API de Cloud Manager

  "https://docs.netapp.com/us-en/occm/reference_infrastructure_as_code.html"

Resolución de problemas

"https://kb.netapp.com/Advice_and_Troubleshooting/Cloud_Services/Cloud_Volumes_ONTAP_(CVO)"

Terraform

- Cloud Terraform

  "https://www.terraform.io/cloud"

- Documentación de Terraform

  "https://www.terraform.io/docs/"

- Registro de Cloud Manager de NetApp

  "https://registry.terraform.io/providers/NetApp/netapp-cloudmanager/lates"

GCP

- Alta disponibilidad de ONTAP para GCP

  "https://cloud.netapp.com/blog/gcp-cvo-blg-what-makes-cloud-volumes-ontap-high-availability-for-gcp-tick"

- GCP perisite

  https://netapp.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=f3d0368b-7165-4d43-a76e-ae01011853d6

Cloud híbrido de FlexPod con NetApp Astra y Cisco Intersight para Red Hat OpenShift

TR-4936: Cloud híbrido de FlexPod con NetApp Astra y Cisco Intersight para Red Hat OpenShift

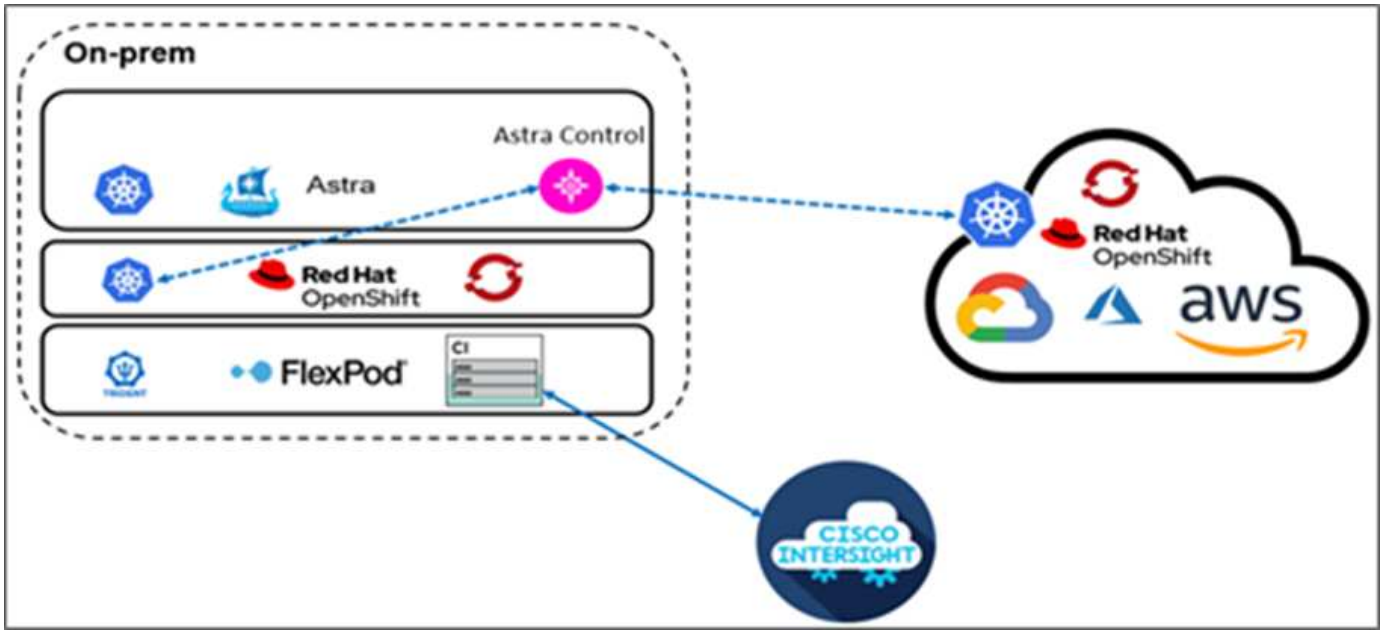
Abhinav Singh

Introducción

A medida que los contenedores y Kubernetes se convierten en la opción de facto para desarrollar, poner en marcha, ejecutar, gestionar y escalar aplicaciones en contenedores, las empresas ejecutan cada vez más aplicaciones vitales para el negocio en ellas. Las aplicaciones vitales para el negocio dependen en gran medida del estado. Una aplicación con estado tiene información de estado, datos y configuración asociada y depende de transacciones de datos anteriores para ejecutar su lógica de negocio. Las aplicaciones vitales para el negocio mientras se ejecuta en Kubernetes siguen teniendo requisitos de disponibilidad y continuidad del negocio, como las aplicaciones tradicionales. Una interrupción del servicio puede afectar seriamente a la pérdida de ingresos, productividad y reputación de la empresa. Por lo tanto, es muy importante proteger, recuperar y mover cargas de trabajo de Kubernetes de forma rápida y sencilla dentro de clústeres, centros de datos en las instalaciones y entornos de cloud híbrido, así como entre ellos. Las empresas han visto en primera línea las ventajas de cambiar su negocio a un modelo de cloud híbrido y modernizar sus aplicaciones a un factor de forma nativo del cloud.

Este informe técnico reúne a Astra Control Center de NetApp con Red Hat OpenShift Container Platform en una solución de infraestructura convergente de FlexPod y se extiende a Amazon Web Services (AWS) para formar un centro de datos de cloud híbrido. Construyendo sobre la familiaridad con "FlexPod y Red Hat OpenShift"En este documento se describe Astra Control Center de NetApp, que empieza con la instalación, la configuración, los flujos de trabajo de protección de aplicaciones y la migración de aplicaciones entre las instalaciones y el cloud. También se tratan las ventajas de las funciones de gestión de datos para aplicaciones (como backup y recuperación de datos, continuidad del negocio) cuando se utiliza Astra Control Center de NetApp para aplicaciones en contenedores que se ejecutan en Red Hat OpenShift.

La siguiente figura muestra la descripción general de la solución.



Destinatarios

La audiencia de destino de este documento incluye directores tecnológicos (directores técnicos), desarrolladores de aplicaciones, arquitectos de soluciones cloud, ingenieros de fiabilidad del sitio (Sres), ingenieros de DevOps, ITOPS y equipos de servicios profesionales que se centran en diseñar, alojar y gestionar aplicaciones en contenedores.

Astra Control de NetApp: Casos prácticos clave

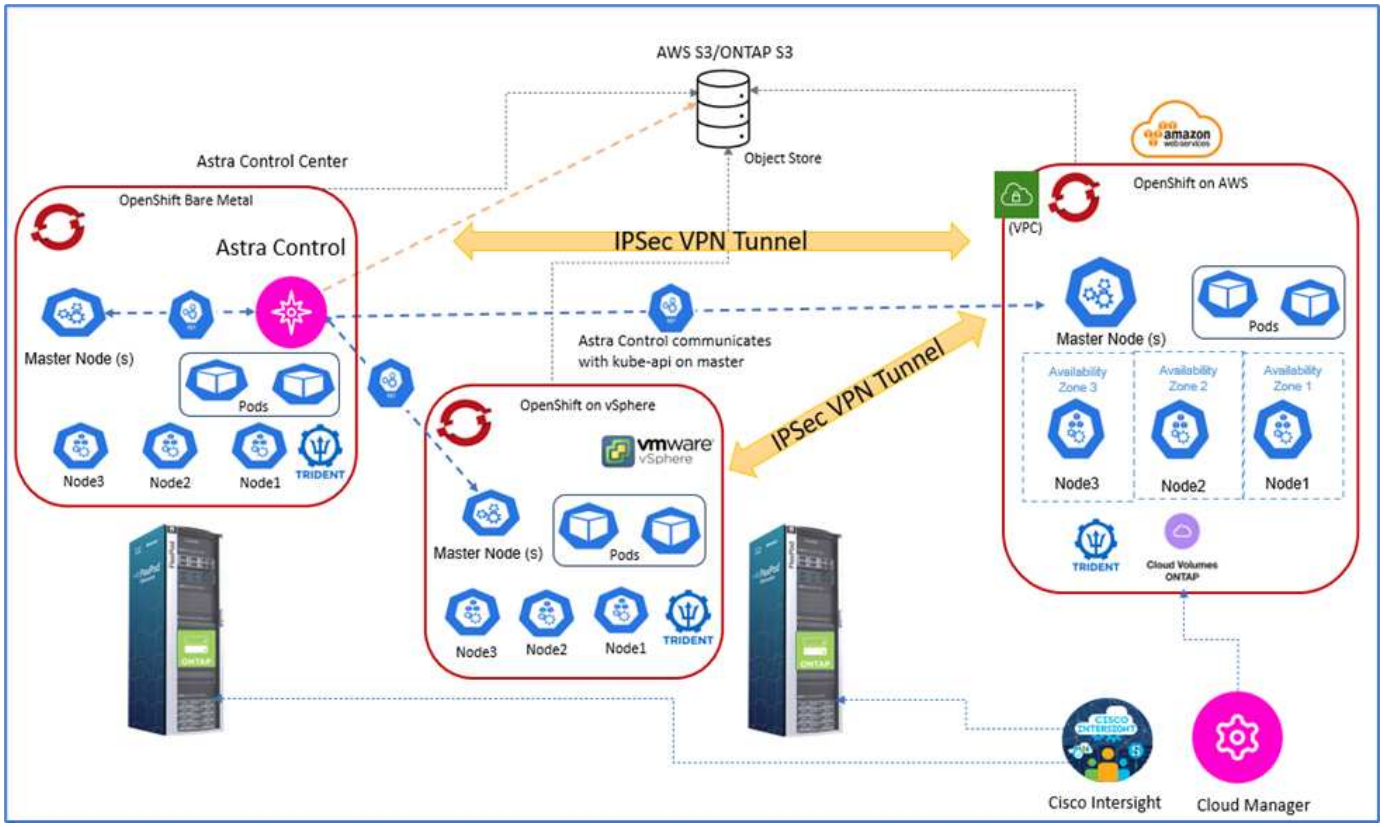
Astra Control de NetApp tiene como objetivo simplificar la protección de aplicaciones para los clientes que tratan con los microservicios nativos del cloud:

- **Representación de la aplicación en un momento específico con snapshots.** con Astra Control puede realizar instantáneas completas de las aplicaciones en contenedores que incluyen los detalles de configuración de la aplicación que se ejecuta en Kubernetes y el almacenamiento persistente asociado. En caso de que se produzca un incidente, las aplicaciones pueden restaurarse a un estado correcto conocido al hacer clic en el botón.
- **Copia completa de seguridad de aplicaciones.** con Astra Control puede realizar una copia de seguridad completa de aplicaciones en un programa predefinido que puede utilizarse para restaurar la aplicación en el mismo clúster K8s o en un clúster K8s diferente a petición de forma automática.
- **Portabilidad de aplicaciones y migración con clones.** con Astra Control puede clonar una aplicación completa junto con sus datos de un clúster de Kubernetes a otro o dentro del mismo clúster K8s. Esta función también ayuda a trasladar o migrar una aplicación a través de los clústeres K8S independientemente de dónde se encuentren los clústeres (simplemente elimine la instancia de la aplicación de origen tras la clonación).
- **Personalice la consistencia de la aplicación.** con Astra Control puede tomar el control de definir estados de inactividad de la aplicación aprovechando los enlaces de ejecución. Borre los enlaces de ejecución ‘pre’ y ‘post’ a los flujos de trabajo de captura y copia de seguridad, las aplicaciones se pondrán en modo inactivo antes de realizar una copia de Snapshot o una copia de seguridad.
- **Automatice la recuperación ante desastres a nivel de aplicación.** con Astra Control puede configurar un plan de recuperación ante desastres de continuidad de negocio (BCDR) para sus aplicaciones contenerizadas. Se utiliza SnapMirror de NetApp en el back-end, y toda la implementación del flujo de trabajo de recuperación ante desastres se ha automatizado.

Topología de la solución

En esta sección se describe la topología lógica de la solución.

En la siguiente ilustración, se muestra la topología de la solución que incluye el entorno local de FlexPod donde se ejecutan clústeres de OpenShift Container Platform y un clúster autogestionado de OpenShift Container Platform en AWS con Cloud Volumes ONTAP de NetApp, Cisco Intersight y la plataforma SaaS Cloud Manager de NetApp.



El primer clúster de OpenShift Container Platform es una instalación básica en FlexPod, el segundo clúster de OpenShift Container Platform se implementa en VMware vSphere ejecutado en FlexPod y el tercer clúster de OpenShift Container Platform se implementa como a "clúster privado" En un cloud privado virtual (VPC) existente en AWS como una infraestructura autogestionada.

En esta solución, FlexPod se conecta a AWS a través de una VPN de sitio a sitio; sin embargo, los clientes también pueden utilizar las implementaciones de conexión directa para extenderse a un cloud híbrido. Cisco Intersight se utiliza para gestionar los componentes de la infraestructura de FlexPod.

En esta solución, Astra Control Center gestiona la aplicación en contenedor alojada en el clúster de la plataforma de contenedores OpenShift que se ejecuta en FlexPod y en AWS. Astra Control Center se instala en la instancia de OpenShift bare-metal que se ejecuta en FlexPod. Astra Control se comunica con kube-api en el nodo maestro y supervisa constantemente el clúster de Kubernetes para detectar posibles cambios. Todas las aplicaciones nuevas que se agreguen al clúster K8S se detectan de forma automática y se ponen a disposición de la administración.

Las representaciones PIT de las aplicaciones contenerizadas se pueden capturar como instantáneas mediante Astra Control Center. Los snapshots de aplicaciones se pueden activar mediante una política de protección programada o bajo demanda. En el caso de las aplicaciones compatibles con Astra, la instantánea es coherente con los fallos. Una copia Snapshot de una aplicación constituye una copia Snapshot de los datos de la aplicación en los volúmenes persistentes, así como los metadatos de la aplicación de los distintos recursos de Kubernetes asociados con dicha aplicación.

Se puede crear una copia de seguridad completa de una aplicación con Astra Control mediante una programación de backup predefinida o bajo demanda. El almacenamiento de objetos se usa para almacenar el backup de los datos de la aplicación. NetApp ONTAP S3, NetApp StorageGRID y cualquier implementación genérica S3 se pueden usar como almacén de objetos.

"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, las redes de almacenamiento de Cisco MDS y Cisco Unified Computing System (Cisco UCS). El diseño es lo suficientemente flexible como para que la red, la informática y el almacenamiento puedan caber en un rack de centro de datos o se puede implementar según el diseño del centro de datos del cliente. La densidad de puertos permite que los componentes de las redes acomoden varias configuraciones.

Control Astra

Astra Control ofrece servicios de protección de datos para aplicaciones para aplicaciones nativas del cloud, que se alojan en clouds públicos y en las instalaciones. Astra Control proporciona funcionalidades de protección de datos, recuperación ante desastres y migración para su aplicación en contenedores que se ejecuta en Kubernetes.

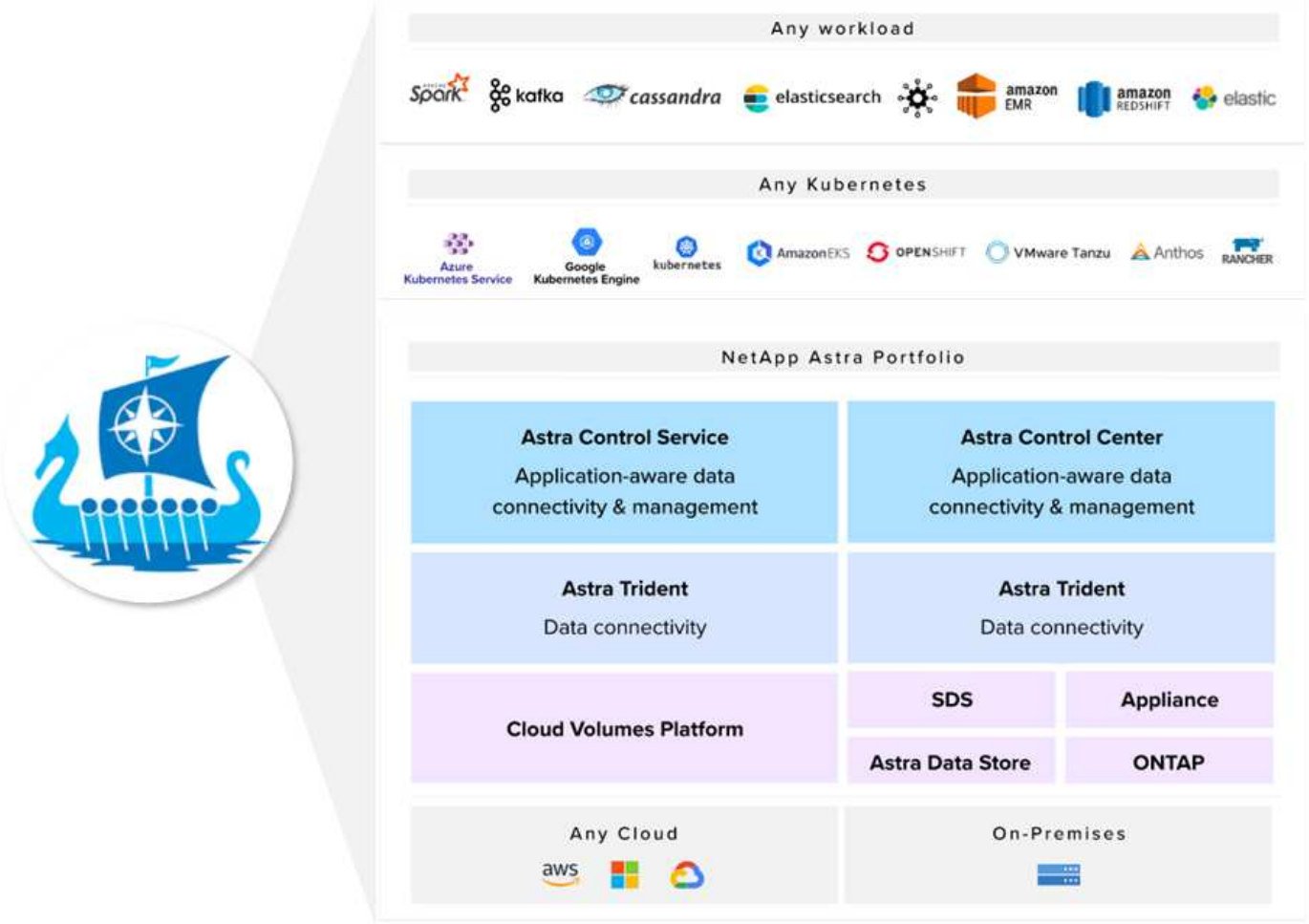
Funciones

Astra Control ofrece funcionalidades cruciales para la gestión del ciclo de vida de los datos de las aplicaciones Kubernetes:

- Gestione automáticamente el almacenamiento persistente
- Crear backups y copias Snapshot bajo demanda coherentes con la aplicación
- Operaciones de backup y Snapshot automatizadas basadas en normativas
- Migre aplicaciones y los datos asociados desde un clúster de Kubernetes a otro en una configuración de cloud híbrido
- Clone una aplicación en el mismo clúster K8s o en otro clúster K8s
- Visualizar el estado de protección de aplicaciones
- Proporciona una interfaz de usuario gráfica y una lista exhaustiva de API DE REST para implementar todos los flujos de trabajo de protección de las herramientas internas existentes.

Astra Control proporciona una visualización en un único panel para sus aplicaciones en contenedores, que incluye una información sobre sus recursos asociados creados en el clúster de Kubernetes. Puede ver todos los clústeres, todas las aplicaciones, en todos los clouds o en todos los centros de datos a través de un portal. Puede utilizar las API Astra Control en todos los entornos (clouds públicos o en las instalaciones) para implementar los flujos de trabajo de gestión de datos.

La siguiente imagen muestra las funciones de Astra Control.



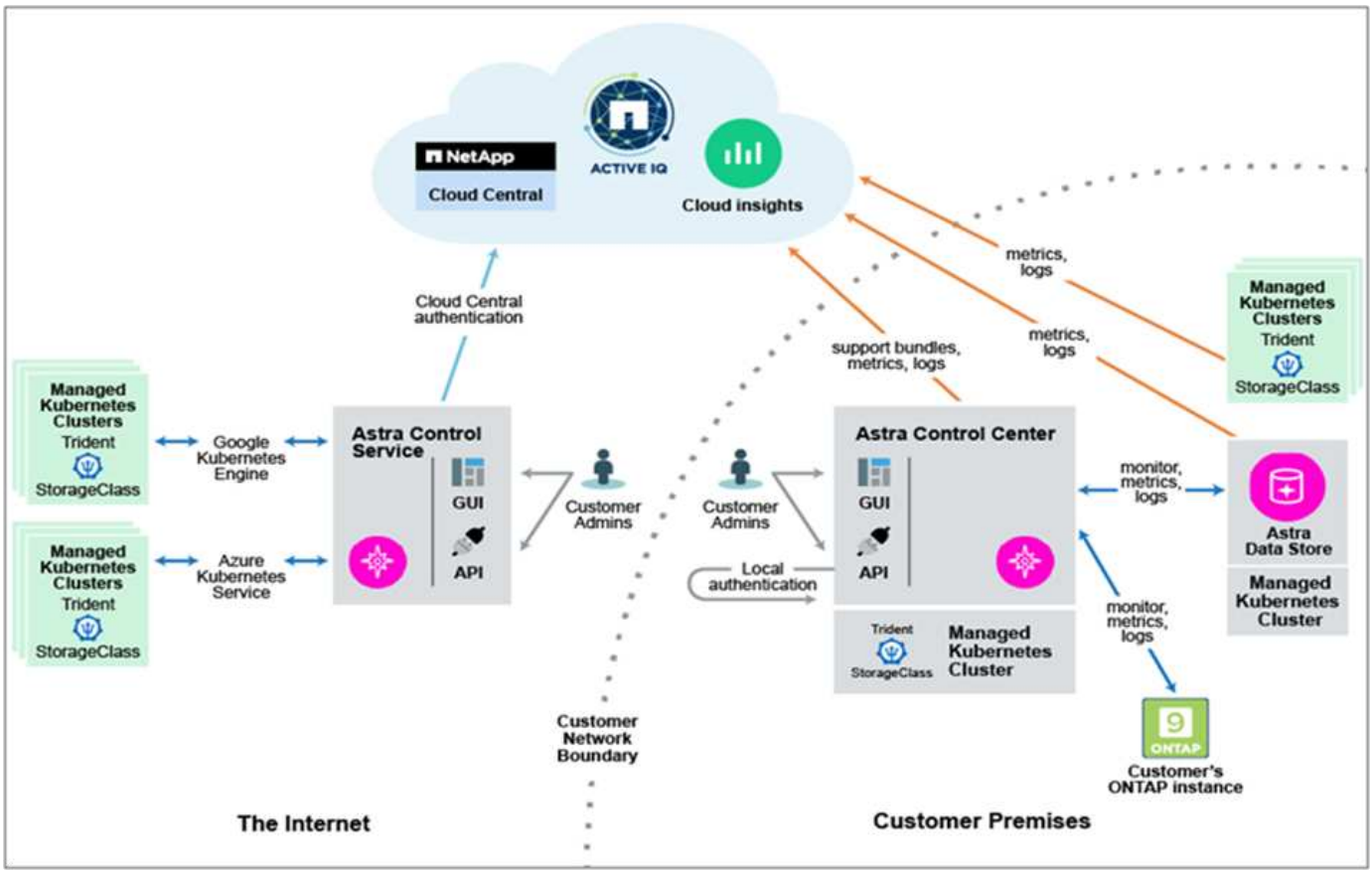
Modelos de consumo de Astra Control

Astra Control está disponible en dos modelos de consumo:

- **Servicio de control de Astra.** un servicio totalmente gestionado que ofrece gestión de datos para aplicaciones de clústeres de Kubernetes en Google Kubernetes Engine (GKE), Azure Kubernetes Service (AKS).
- **Astra Control Center.** Software autogestionado que proporciona gestión de datos para aplicaciones de clústeres de Kubernetes que se ejecutan en su entorno de cloud híbrido y en las instalaciones.

Este informe técnico aprovecha Astra Control Center para la gestión de aplicaciones nativas del cloud que se ejecutan en Kubernetes.

La siguiente imagen muestra la arquitectura Astra Control.



Astra Trident

Astra Trident es un orquestador de almacenamiento de código abierto y totalmente compatible para contenedores y distribuciones de Kubernetes. Se ha diseñado desde el principio para ayudarle a satisfacer las demandas de persistencia de sus aplicaciones en contenedores mediante interfaces estándar del sector, como el "Interfaz de almacenamiento de contenedores (CSI)". Con Astra Trident, los microservicios y las aplicaciones en contenedores pueden aprovechar los servicios de almacenamiento de nivel empresarial que proporciona la cartera de sistemas de almacenamiento de NetApp.

Astra Trident se pone en marcha en clústeres de Kubernetes como pods y proporciona servicios de orquestación de almacenamiento dinámico para sus cargas de trabajo de Kubernetes. Permite que sus aplicaciones en contenedores consuman almacenamiento persistente de una forma rápida y sencilla desde la amplia cartera de NetApp, que incluye ONTAP de NetApp (AFF de NetApp, FAS de NetApp, ONTAP Select de NetApp, cloud, Y Amazon FSX para ONTAP de NetApp), el software de NetApp Element (SolidFire de NetApp), así como el servicio Azure NetApp Files, Cloud Volume Service en Google Cloud y el servicio Cloud Volume Service en AWS. En un entorno de FlexPod, Astra Trident se utiliza para aprovisionar y gestionar de forma dinámica volúmenes persistentes para contenedores que están respaldados por volúmenes y LUN de FlexVol de NetApp, alojados en una plataforma de almacenamiento de ONTAP como los sistemas AFF y FAS de NetApp y Cloud Volumes ONTAP. Trident también desempeña un papel clave en la implementación de los esquemas de protección de aplicaciones que ofrece Astra Control. Si quiere más información sobre Astra Trident, consulte "Documentación de Astra Trident."

Back-end de almacenamiento

Para utilizar Astra Trident, necesita un back-end de almacenamiento compatible. Un back-end de Trident define la relación entre Trident y un sistema de almacenamiento. Indica a Trident cómo se comunica con ese sistema de almacenamiento y cómo debe aprovisionar volúmenes a partir de él. Trident ofrecerá automáticamente pools de almacenamiento de back-ends que coincidan con los requisitos definidos por una

clase de almacenamiento.

- ONTAP AFF y el back-end de almacenamiento de FAS. Como plataforma de software y hardware de almacenamiento, ONTAP proporciona servicios de almacenamiento básicos, compatibilidad con varios protocolos de acceso a almacenamiento y funcionalidad de gestión del almacenamiento, como copias Snapshot de NetApp y mirroring.
- Entorno de administración del almacenamiento de Cloud Volumes ONTAP
- "Almacén de datos Astra" back-end de almacenamiento

Cloud Volumes ONTAP de NetApp

Cloud Volumes ONTAP de NetApp es una oferta de almacenamiento definido por software que ofrece 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.

Sus ventajas clave incluyen:

- Aproveche las funciones integradas de deduplicación de datos, compresión de datos, thin provisioning y clonado para minimizar los costes en almacenamiento.
- Garantice la fiabilidad de su empresa y la continuidad de las operaciones en caso de fallos en su entorno cloud.
- Cloud Volumes ONTAP aprovecha SnapMirror, la tecnología de replicación líder del sector de NetApp, para replicar datos en las instalaciones al cloud de forma que resulta fácil disponer de copias secundarias para varios casos de uso.
- Cloud Volumes ONTAP también se integra con Cloud Backup Service para proporcionar funcionalidades de backup y restauración para la protección y archivado de datos en el cloud a largo plazo.
- Cambie entre pools de almacenamiento de alto y bajo rendimiento bajo demanda sin desconectar las aplicaciones.
- Garantice la consistencia de las copias Snapshot mediante SnapCenter de NetApp.
- Cloud Volumes ONTAP admite el cifrado de datos y proporciona protección contra virus y ransomware.
- La integración con Cloud Data Sense le ayuda a comprender el contexto de los datos e identificar datos confidenciales.

Cloud Central

Cloud Central proporciona una ubicación centralizada para acceder y gestionar los servicios de datos en el cloud de NetApp. Estos servicios le permiten ejecutar aplicaciones críticas en el cloud, crear sitios de recuperación ante desastres automatizados, realizar backups de sus datos y migrar y controlar datos de forma efectiva en varios clouds. Para obtener más información, consulte "Cloud Central."

Cloud Manager

Cloud Manager es una plataforma de gestión basada en SaaS para empresas que permite a expertos EN TECNOLOGÍA Y arquitectos de cloud gestionar de forma centralizada su infraestructura multicloud híbrida con las soluciones cloud de NetApp. Proporciona un sistema centralizado para ver y gestionar su almacenamiento en las instalaciones y en cloud, que admite cabinas y cuentas de varios proveedores de cloud híbridos. Para obtener más información, consulte "Cloud Manager".

Conector

Connector es una instancia que permite a Cloud Manager gestionar recursos y procesos dentro de un entorno de cloud público. Se requiere un conector para utilizar muchas funciones que ofrece Cloud Manager. Un conector puede ponerse en marcha en la nube o en la red local.

El conector se admite en las siguientes ubicaciones:

- AWS
- Microsoft Azure
- Google Cloud
- En sus instalaciones

Para obtener más información acerca de Connector, consulte "este enlace."

Cloud Insights de NetApp

Una herramienta Cloud Insights de supervisión de infraestructura de cloud de NetApp le permite supervisar el rendimiento y la utilización de sus clústeres de Kubernetes gestionados por Astra Control Center. Cloud Insights relaciona el uso del almacenamiento con las cargas de trabajo. Cuando activa la conexión Cloud Insights en Astra Control Center, la información de telemetría se muestra en las páginas de interfaz de usuario de Astra Control Center.

Active IQ Unified Manager de NetApp

Active IQ Unified Manager de NetApp le permite supervisar sus clústeres de almacenamiento de ONTAP desde una única interfaz intuitiva y rediseñada que proporciona inteligencia sobre la comunidad y los análisis de IA. Proporciona información proactiva, operativa y de rendimiento integral 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 que le ayudarán a identificar la causa raíz. La consola de VM le ofrece una vista de las estadísticas de rendimiento de la máquina virtual para poder investigar toda la ruta de I/o desde el host VMware vSphere hacia abajo a través de 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 le notifique a través de correo electrónico y capturas SNMP. Active IQ Unified Manager permite planificar los requisitos de almacenamiento de los usuarios al prever las tendencias de uso y capacidad para que actúen de forma proactiva antes de que surjan problemas, evitando la toma de decisiones a corto plazo que puedan dar lugar a problemas adicionales a largo plazo.

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:

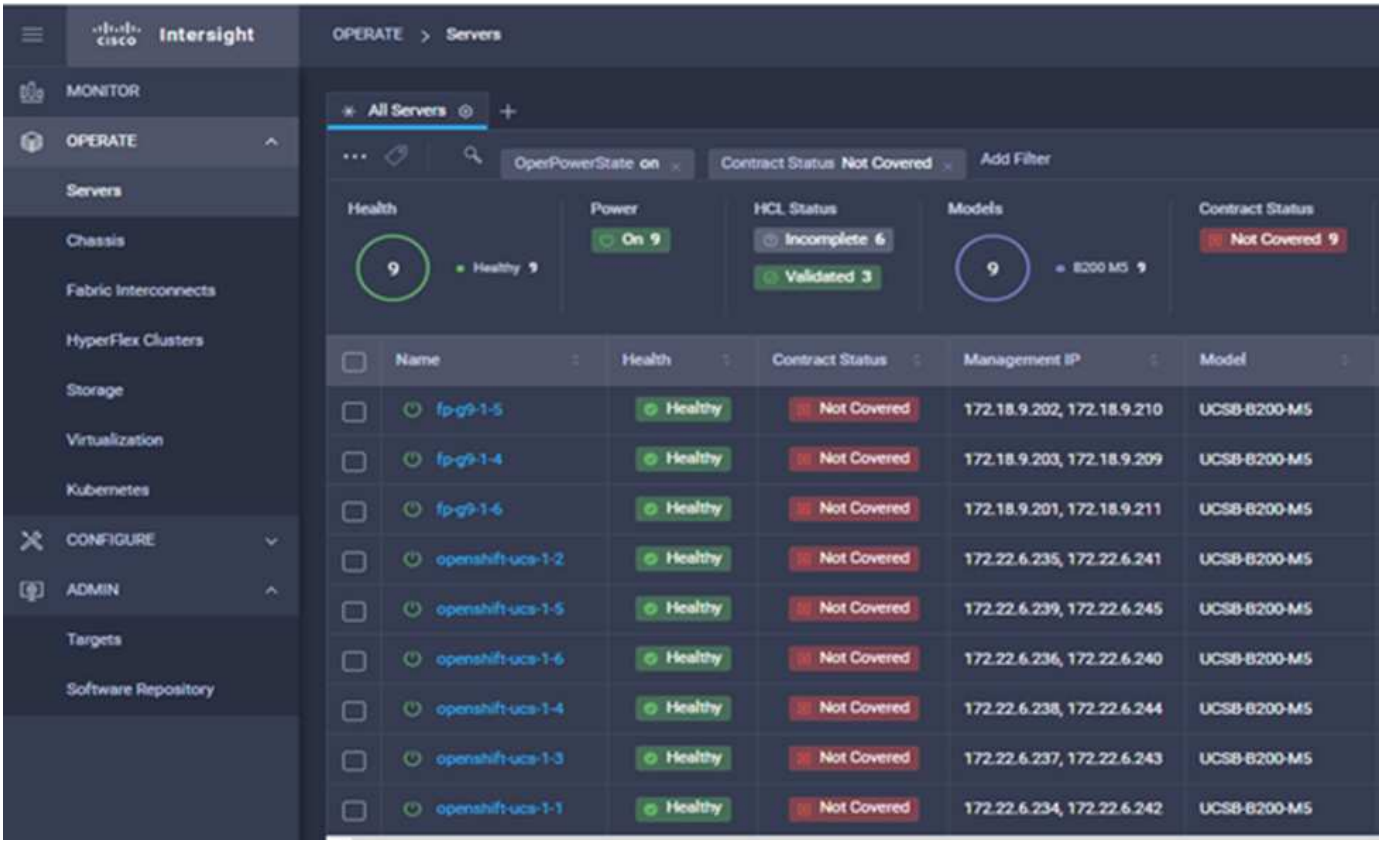
- **Entrega más rápida.** entrega como servicio desde la nube o en el centro de datos del cliente con actualizaciones frecuentes y una innovación continua, gracias a un modelo de desarrollo de software ágil. De esta forma, el cliente solo tiene que centrarse en acelerar la prestación de la línea de negocio.
- **Operaciones simplificadas.** simplifique las operaciones utilizando una única herramienta segura proporcionada por SaaS con inventario, autenticación y API comunes para trabajar en toda la pila y todas

las ubicaciones, eliminando los silos entre equipos. Desde la gestión de servidores físicos e hipervisores en las instalaciones a equipos virtuales, K8s, servidores, automatización optimización y control de costes en los clouds públicos y en las instalaciones.

- **Optimización continua.** Optimice continuamente su entorno mediante la inteligencia proporcionada por Cisco Intersight en todas las capas, así como Cisco TAC. Esta inteligencia se convierte en acciones recomendadas y automatizables para que usted pueda adaptar en tiempo real a cada cambio: Desde mover cargas de trabajo y supervisar el estado de los servidores físicos a ajustar de forma automática el tamaño de los clústeres K8s hasta recomendaciones de reducción de costes 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 LOS MÓDULOS UMM o IMM nativos para los sistemas Cisco UCS conectados a la estructura durante la configuración inicial de las interconexiones de estructura. En esta solución, SE utilizan UMM nativos.

La siguiente imagen muestra el panel de Cisco Intersight.



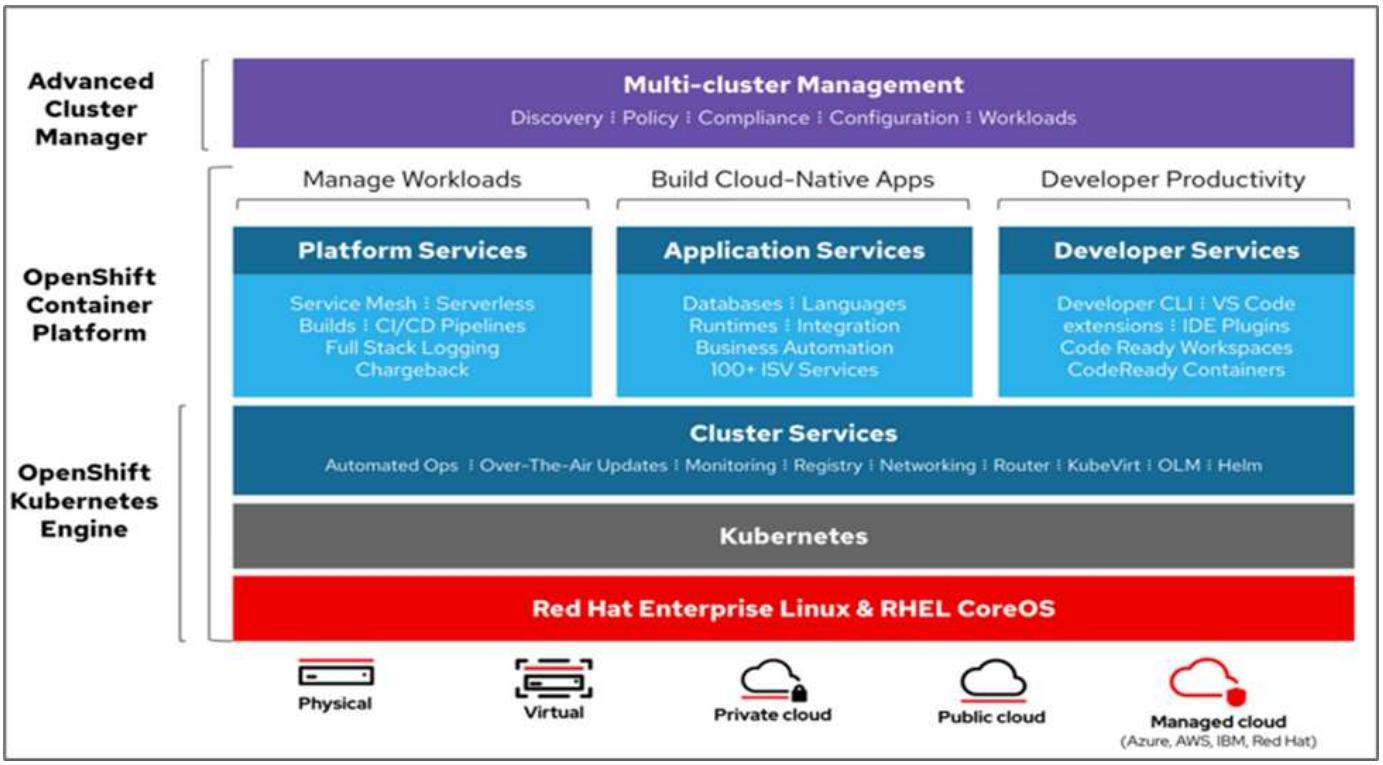
OpenShift Container Platform de Red Hat

Red Hat OpenShift Container Platform es una plataforma de aplicaciones contenedoras que reúne a CRI-o y Kubernetes y proporciona una API e interfaz web para administrar estos servicios. CRI-o es una implementación de Kubernetes Container Runtime Interface (CRI) para permitir el uso de tiempos de ejecución compatibles con Open Container Initiative (OCI). Es una alternativa ligera al uso de Docker como tiempo de ejecución para Kubernetes.

OpenShift Container Platform permite a los clientes crear y administrar contenedores. Los contenedores son procesos independientes que se ejecutan dentro de su propio entorno, independientemente del sistema operativo y la infraestructura subyacente. OpenShift Container Platform ayuda a desarrollar, implementar y administrar aplicaciones basadas en contenedores. Proporciona una plataforma de autoservicio para crear,

modificar e implementar aplicaciones bajo demanda, lo que permite agilizar los ciclos de vida de desarrollo y lanzamiento. OpenShift Container Platform tiene una arquitectura basada en microservicios de unidades pequeñas independientes que funcionan juntas. Se ejecuta sobre un clúster de Kubernetes, con datos sobre los objetos almacenados en etcd, un almacén de claves en clúster de confianza.

La siguiente imagen es una descripción general de la plataforma Red Hat OpenShift Container.



Infraestructura de Kubernetes

Dentro de OpenShift Container Platform, Kubernetes gestiona aplicaciones en contenedores a través de un conjunto de hosts de tiempo de ejecución de CRI-o y proporciona mecanismos para la implementación, el mantenimiento y el escalado de aplicaciones. Los paquetes de servicio CRI-o, crean instancias y ejecutan aplicaciones contenerizadas.

Un clúster de Kubernetes está formado por uno o más maestros y un conjunto de nodos de trabajo. Este diseño de solución incluye la funcionalidad de alta disponibilidad en el hardware y la pila de software. Un clúster de Kubernetes está diseñado para ejecutarse en modo de alta disponibilidad con tres nodos maestros y un mínimo de dos nodos de trabajo para ayudar a garantizar que el clúster no tenga ningún punto único de error.

So Red Hat Core

OpenShift Container Platform utiliza Red Hat Enterprise Linux CoreOS (RHCOS), un sistema operativo orientado a contenedores que combina algunas de las mejores características y funciones de los sistemas operativos CoreOS y Red Hat Atmic Host. RHCOS está específicamente diseñado para ejecutar aplicaciones en contenedores desde OpenShift Container Platform y trabaja con nuevas herramientas para proporcionar una instalación rápida, gestión basada en operadores y actualizaciones simplificadas.

RHCOS incluye las siguientes funciones:

- Ignition, que OpenShift Container Platform utiliza como primera configuración del sistema de arranque para el inicio y configuración de las máquinas.

- CRI-o, una implementación de tiempo de ejecución de contenedor nativo de Kubernetes que se integra estrechamente con el sistema operativo para ofrecer una experiencia de Kubernetes eficiente y optimizada. CRI-o proporciona servicios para ejecutar, detener y reiniciar contenedores. Sustituye por completo el motor de contenedores Docker, que se utilizó en OpenShift Container Platform 3.
- Kubelet, el agente de nodo principal de Kubernetes, es responsable del lanzamiento y la supervisión de contenedores.

VMware vSphere 7.0

VMware vSphere es una plataforma de virtualización para gestionar de forma holística grandes colecciones de infraestructuras (recursos que incluyen 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 agrupa la infraestructura de todo un centro de datos para crear una única usina con recursos que se pueden asignar de forma rápida y dinámica a cualquier aplicación que lo necesite.

Para obtener más información, consulte "VSphere de VMware".

VMware vSphere 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.

Revisiones de hardware y software

Esta solución se puede ampliar a cualquier entorno FlexPod que ejecute versiones compatibles de software, firmware y hardware tal y como se haya definido en el "Herramienta de matriz de interoperabilidad de NetApp" y.. "Lista de compatibilidad de hardware de Cisco UCS." El clúster de OpenShift se instala en FlexPod de forma "Bare Metal" y en VMware vSphere.

Sólo se necesita una única instancia de Astra Control Center para gestionar varios clústeres de OpenShift (k8s), mientras que Trident CSI está instalado en cada clúster de OpenShift. Astra Control Center se puede instalar en cualquiera de estos clústeres de OpenShift. En esta solución, Astra Control Center se instala en el clúster de configuración básica OpenShift.

En la siguiente tabla se enumeran las revisiones de software y hardware de FlexPod para OpenShift.

Componente	Producto	Versión
Informática	Interconexiones de estructura Cisco UCS 6454	4.1(3c)
	Servidores Cisco UCS B200 M5	4.1(3c)
Red	Cisco Nexus 9336C-FX2 NX-OS	9.3(8)
Reducida	AFF A700 de NetApp	9.11.1
	Centro de control de Astra de NetApp	22.04.0
	Complemento NetApp Astra Trident CSI	22.04.0

Componente	Producto	Versión
	Active IQ Unified Manager de NetApp	9.11
De NetApp	Controlador Ethernet nenic VMware ESXi	1.0.35.0
	VSphere ESXi	7.0 (U2)
	Dispositivo VMware vCenter	7.0 U2B
	Dispositivo virtual Cisco Intersight Assist	1.0.9-342
	OpenShift Container Platform	4.9
	Nodo maestro de OpenShift Container Platform	RHCOS 4.9
	OpenShift Container Platform Worker Node	RHCOS 4.9

En la tabla siguiente se enumeran las versiones de software para OpenShift en AWS.

Componente	Producto	Versión
Informática	Tipo de instancia maestra: m5.xlarge	n.a.
	Tipo de instancia de trabajador: m5.Large	n.a.
Red	Puerta de enlace de tránsito de cloud privado virtual	n.a.
Reducida	Cloud Volumes ONTAP de NetApp	9.11.1
	Complemento NetApp Astra Trident CSI	22.04.0
De NetApp	OpenShift Container Platform	4.9
	Nodo maestro de OpenShift Container Platform	RHCOS 4.9
	OpenShift Container Platform Worker Node	RHCOS 4.9

"Siguiente: Instalación básica de FlexPod para OpenShift Container Platform 4."

Instalación y configuración

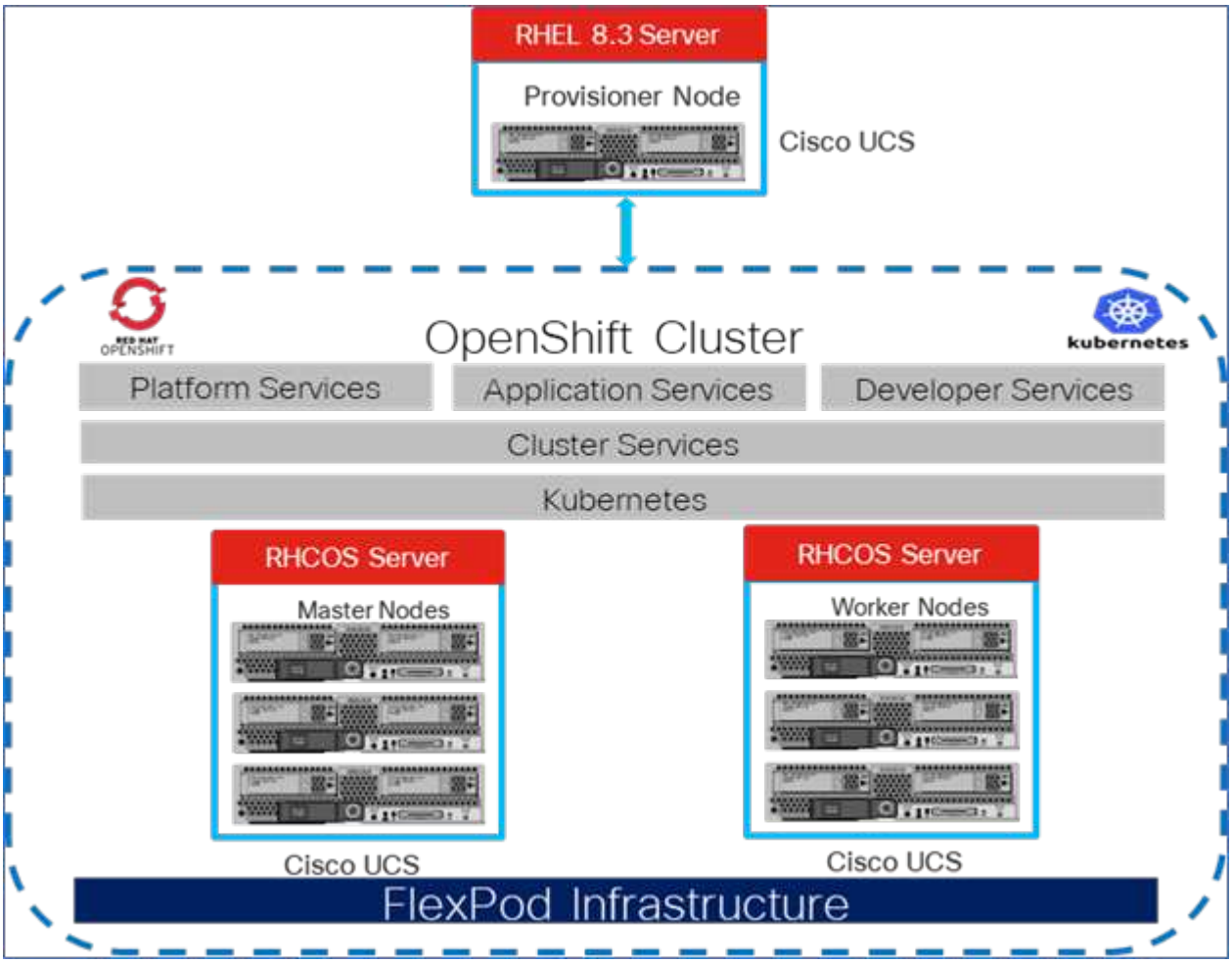
Instalación de configuración básica de FlexPod para OpenShift Container Platform 4

"Anterior: Componentes de la solución."

Para comprender el diseño de configuración básica, los detalles de la implementación y la instalación y la configuración de FlexPod para OpenShift Container Platform 4 de

NetApp Astra Trident, consulte "FlexPod con OpenShift Guía de diseño y puesta en marcha validados de Cisco (CVD)". Este CVD abarca la puesta en marcha de FlexPod y OpenShift Container Platform con Ansible. El CVD también proporciona información detallada sobre la preparación de nodos de trabajo, la instalación de Astra Trident, la configuración de back-end de almacenamiento y clase de almacenamiento, que son los pocos requisitos previos para poner en marcha y configurar Astra Control Center.

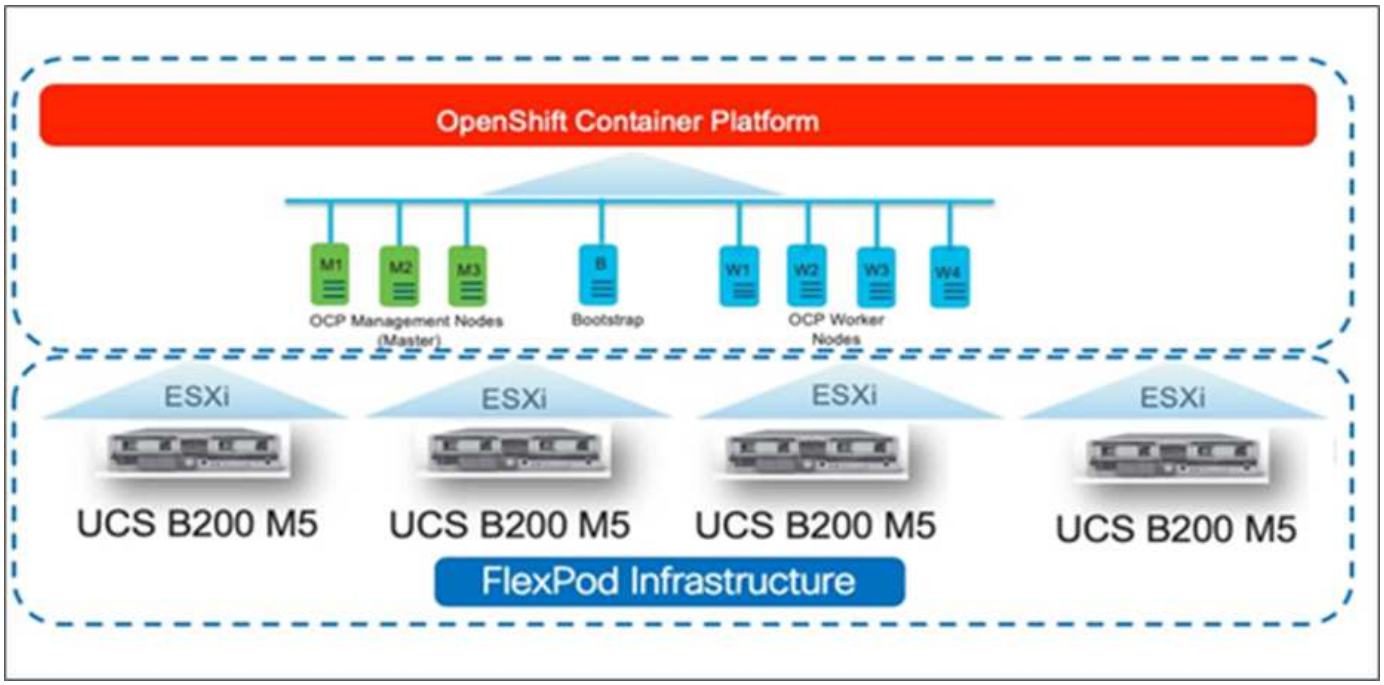
En la siguiente figura se muestra OpenShift Container Platform 4 Bare Metal en FlexPod.



FlexPod para OpenShift Container Platform 4 en una instalación de VMware

Para obtener más información sobre la implementación de Red Hat OpenShift Container Platform 4 en FlexPod con VMware vSphere, consulte "FlexPod Datacenter para OpenShift Container Platform 4".

La siguiente figura ilustra FlexPod para OpenShift Container Platform 4 en vSphere.

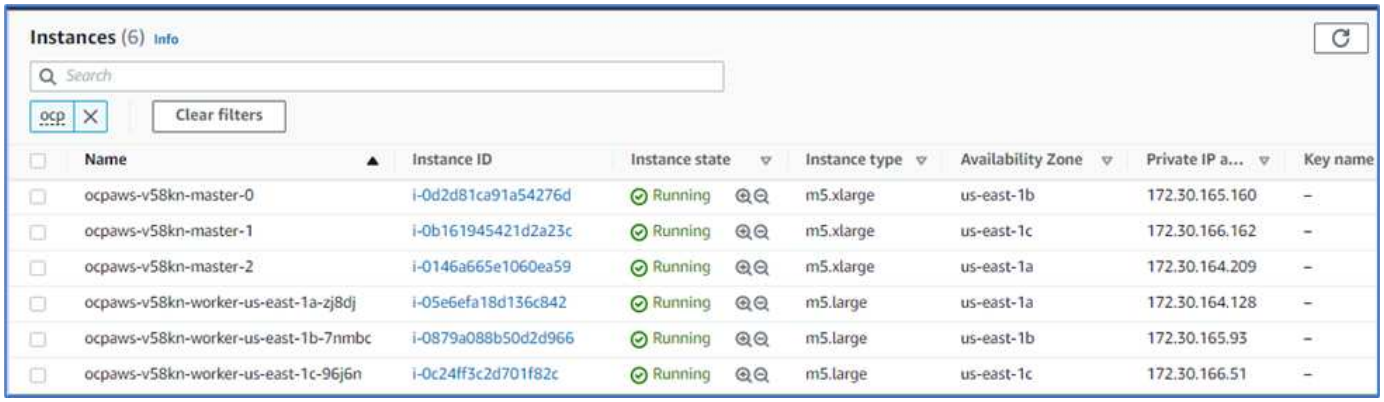


"Siguiente: Red Hat OpenShift en AWS."

Red Hat OpenShift en AWS

"Anterior: Instalación básica de FlexPod para OpenShift Container Platform 4."

Un clúster independiente de OpenShift Container Platform 4 autogestionado se pone en marcha en AWS como sitio de recuperación ante desastres. Los nodos maestro y trabajador abarcan tres zonas de disponibilidad para obtener alta disponibilidad.



```
[ec2-user@ip-172-30-164-92 ~]$ oc get nodes
NAME                                STATUS   ROLES    AGE   VERSION
ip-172-30-164-128.ec2.internal   Ready    worker   29m   v1.22.8+f34b40c
ip-172-30-164-209.ec2.internal   Ready    master   36m   v1.22.8+f34b40c
ip-172-30-165-160.ec2.internal   Ready    master   33m   v1.22.8+f34b40c
ip-172-30-165-93.ec2.internal    Ready    worker   30m   v1.22.8+f34b40c
ip-172-30-166-162.ec2.internal   Ready    master   36m   v1.22.8+f34b40c
ip-172-30-166-51.ec2.internal    Ready    worker   28m   v1.22.8+f34b40c
```

OpenShift se implementa como un "clúster privado" En un VPC existente en AWS. Un clúster privado de OpenShift Container Platform no expone puntos finales externos y se puede acceder sólo desde una red interna y no es visible para Internet. Se pone en marcha un Cloud Volumes ONTAP de NetApp de un único nodo mediante Cloud Manager de NetApp, que proporciona un back-end de almacenamiento a Astra Trident.

Para obtener más información acerca de la instalación de OpenShift en AWS, consulte "Documentación de OpenShift".

"Siguiente: Cloud Volumes ONTAP de NetApp."

Cloud Volumes ONTAP de NetApp

"Anterior: Red Hat OpenShift en AWS."

La instancia de Cloud Volumes ONTAP de NetApp se pone en marcha en AWS y sirve como almacenamiento de back-end a Astra Trident. Antes de agregar un entorno de trabajo de Cloud Volumes ONTAP, se debe desplegar un conector. Cloud Manager le pregunta si intenta crear el primer entorno de trabajo de Cloud Volumes ONTAP sin un conector en su lugar. Para implementar un conector en AWS, consulte "Cree un conector".

Para implementar Cloud Volumes ONTAP en AWS, consulte "Inicio rápido para AWS".

Después de la puesta en marcha de Cloud Volumes ONTAP, puede instalar Astra Trident y configurar la clase de snapshot y back-end de almacenamiento en el clúster de OpenShift Container Platform.

"Siguiente: Instalación de Astra Control Center en OpenShift Container Platform."

Instalación de Astra Control Center en OpenShift Container Platform

"Anterior: Cloud Volumes ONTAP de NetApp."

Puede instalar Astra Control Center en un clúster OpenShift que se ejecuta en FlexPod o en AWS con un back-end de almacenamiento de Cloud Volumes ONTAP. En esta solución, Astra Control Center se pone en marcha en el clúster de configuración básica OpenShift.

Astra Control Center se puede instalar utilizando el proceso estándar descrito "aquí" O desde Red Hat OpenShift OperatorHub. Astra Control Operator es un operador certificado de Red Hat. En esta solución, Astra Control Center se instala mediante Red Hat OperatorHub.

Requisitos del entorno

- Astra Control Center es compatible con varias distribuciones de Kubernetes; para Red Hat OpenShift, las versiones compatibles incluyen Red Hat OpenShift Container Platform 4.8 o 4.9.
- Astra Control Center requiere los siguientes recursos además de los requisitos de recursos del entorno y de la aplicación del usuario final:

Componentes	Requisito
Capacidad del back-end de almacenamiento	500 GB disponibles como mínimo
Nodos de trabajo	Al menos 3 nodos de trabajo, con 4 núcleos de CPU y 12 GB de RAM cada uno
Dirección del nombre de dominio completo (FQDN)	Una dirección FQDN para Astra Control Center
Astra Trident	Astra Trident 21.04 o posterior instalado y configurado
Controlador de entrada o equilibrador de carga	Configure el controlador de entrada para exponer Astra Control Center con una dirección URL o equilibrador de carga para proporcionar la dirección IP que se resolverá en el FQDN

- Debe tener un registro de imágenes privadas existente en el que pueda insertar las imágenes de creación de Astra Control Center. Debe proporcionar la dirección URL del registro de imágenes donde cargue las imágenes.

> Algunas imágenes se van tirando mientras se ejecutan ciertos flujos de trabajo, y cuando es necesario se crean y destruyen contenedores.

- Astra Control Center requiere que se cree una clase de almacenamiento y se establezca como la clase de almacenamiento predeterminada. Astra Control Center es compatible con los siguientes controladores de ONTAP proporcionados por Astra Trident:
  - ontap-nas
  - ontap-nas-flexgroup
  - san ontap
  - ontap-san-economía

> Asumimos que los clústeres OpenShift puestos en marcha tienen Astra Trident instalado y configurado con un back-end de ONTAP y también se define una clase de almacenamiento predeterminada.

- Para la clonación de aplicaciones en entornos OpenShift, Astra Control Center debe permitir a OpenShift montar volúmenes y cambiar la propiedad de los archivos. Para modificar la política de exportación de ONTAP y permitir estas operaciones, ejecute los siguientes comandos:

```
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -superuser sys
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -anon 65534
```

Para añadir un segundo entorno operativo OpenShift como recurso informático gestionado, asegúrese de que la función Snapshot de Astra Trident Volume esté habilitada. Para habilitar y probar copias Snapshot de volumen con Astra Trident, consulte el funcionario "Instrucciones de Astra Trident".

- A. "VolumeSnapClass" Debe configurarse en todos los clústeres de Kubernetes desde el lugar donde se gestionan las aplicaciones. Esto también podría incluir el clúster K8s en el que está instalado Astra Control Center. Astra Control Center puede gestionar aplicaciones en el clúster K8s en el que se ejecuta.

Y gestión de aplicaciones

- **Licencia.** para gestionar aplicaciones con Astra Control Center, necesita una licencia Astra Control Center.
- **Espacios de nombres.** un espacio de nombres es la entidad más grande que puede ser administrada como una aplicación por Astra Control Center. Puede elegir filtrar componentes según las etiquetas de la aplicación y las etiquetas personalizadas de un espacio de nombres existente y gestionar un subconjunto de recursos como aplicación.
- **StorageClass.** Si instala una aplicación con StorageClass definida explícitamente y necesita clonar la aplicación, el clúster de destino para la operación de clonación debe tener el StorageClass especificado originalmente. Se produce un error al clonar una aplicación con un tipo de almacenamiento establecido explícitamente en un clúster que no tenga el mismo tipo de almacenamiento.
- **Recursos Kubernetes.** las aplicaciones que usan recursos Kubernetes no capturados por Astra Control podrían no tener capacidades completas de gestión de datos de aplicaciones. Astra Control puede capturar los siguientes recursos de Kubernetes:

Recursos de Kubernetes		
Función de clúster	ClusterRoleBinding	ConfigMap
CustomResourceDefinition	Recurso personalizado	Cronjob
DemonSet	HorizontalPodAutocaler	Entrada
DeploymentConfig	MutatingWebhook	Claim persistente
Pod	PodDisruptionBudget	PodTemplate
Política de red	Replicaset	Función
RoleBinding	Ruta	Secreto
ValidadoWebhook		

Instale Astra Control Center utilizando OpenShift OperatorHub

El siguiente procedimiento instala Astra Control Center utilizando Red Hat OperatorHub. En esta solución, Astra Control Center se instala en un clúster OpenShift con configuración básica que se ejecuta en FlexPod.

1. Descargue el paquete Astra Control Center (`astra-control-center-[version].tar.gz`) del "Sitio de soporte de NetApp".
2. Descargue el archivo .zip de los certificados y claves de Astra Control Center desde "Sitio de soporte de NetApp".
3. Verifique la firma del paquete.

```
openssl dgst -sha256 -verify astra-control-center[version].pub
-signature <astra-control-center[version].sig astra-control-
center[version].tar.gz
```

4. Extraiga las imágenes de Astra.

```
tar -vxzf astra-control-center-[version].tar.gz
```

5. Cambie al directorio Astra.

```
cd astra-control-center-[version]
```

6. Agregue las imágenes al registro local.

```
For Docker:
docker login [your_registry_path]OR
For Podman:
podman login [your_registry_path]
```

7. Utilice la secuencia de comandos adecuada para cargar las imágenes, etiquetar las imágenes y empujarlas al registro local.

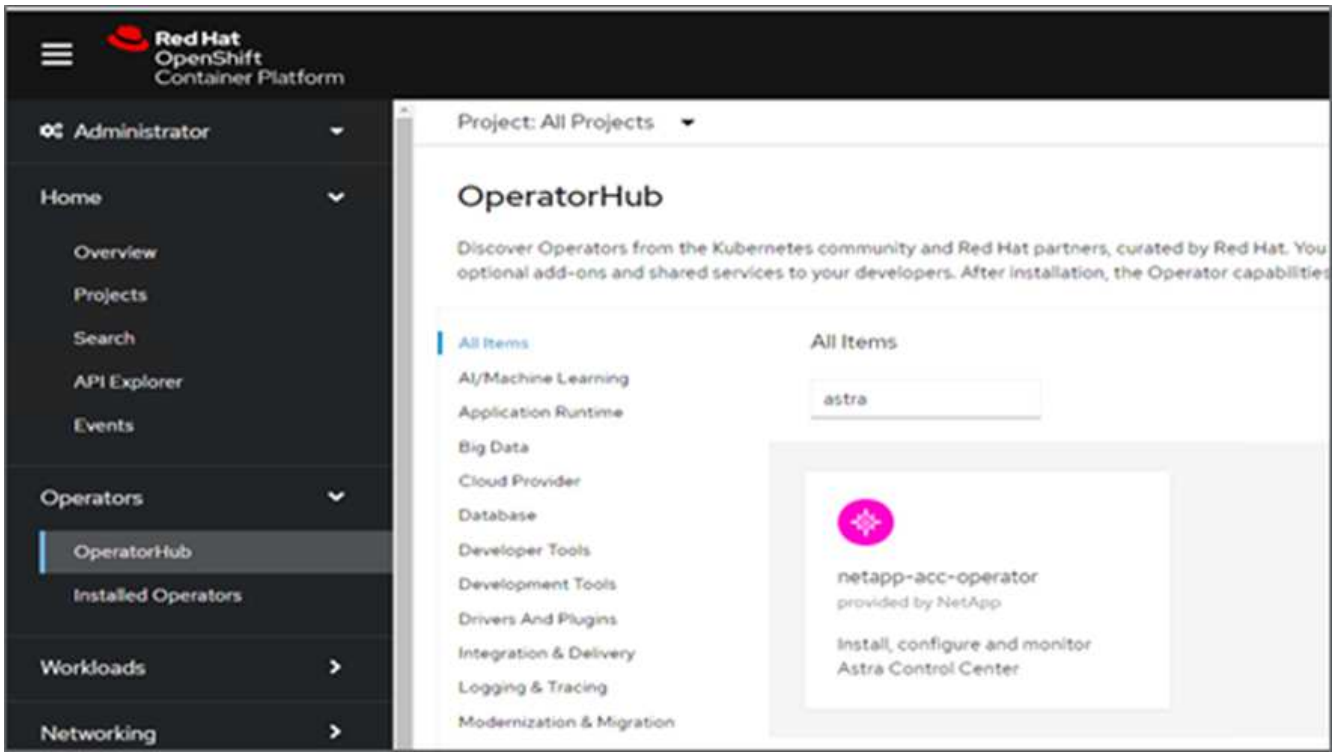
   Para Docker:

```
export REGISTRY=[Docker_registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(docker load --input ${astraImageFile} | sed 's/Loaded
image: //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  docker tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  docker push ${REGISTRY}/${astraImage}
done
```

   Para Podman:

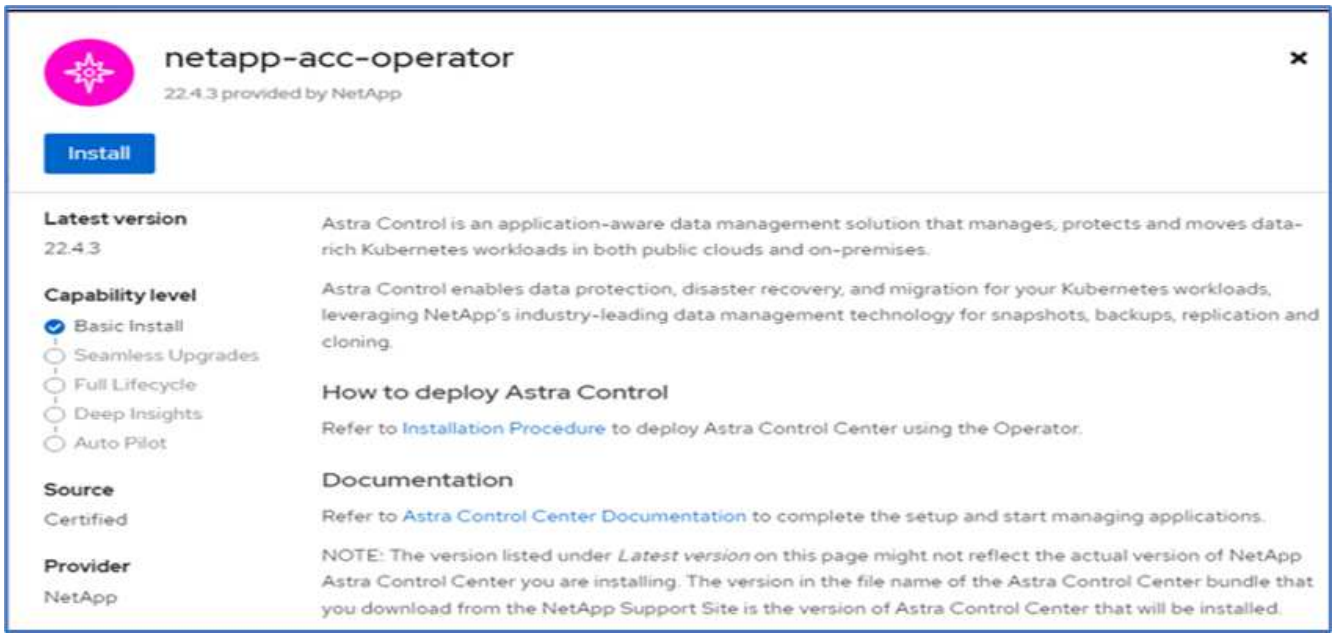
```
export REGISTRY=[Registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  podman push ${REGISTRY}/${astraImage}
done
```

8. Inicie sesión en la consola web de clúster OpenShift con configuración básica. En el menú lateral, seleccione operadores > OperatorHub. Introduzca `astra` para enumerar la `netapp-acc-operator`.

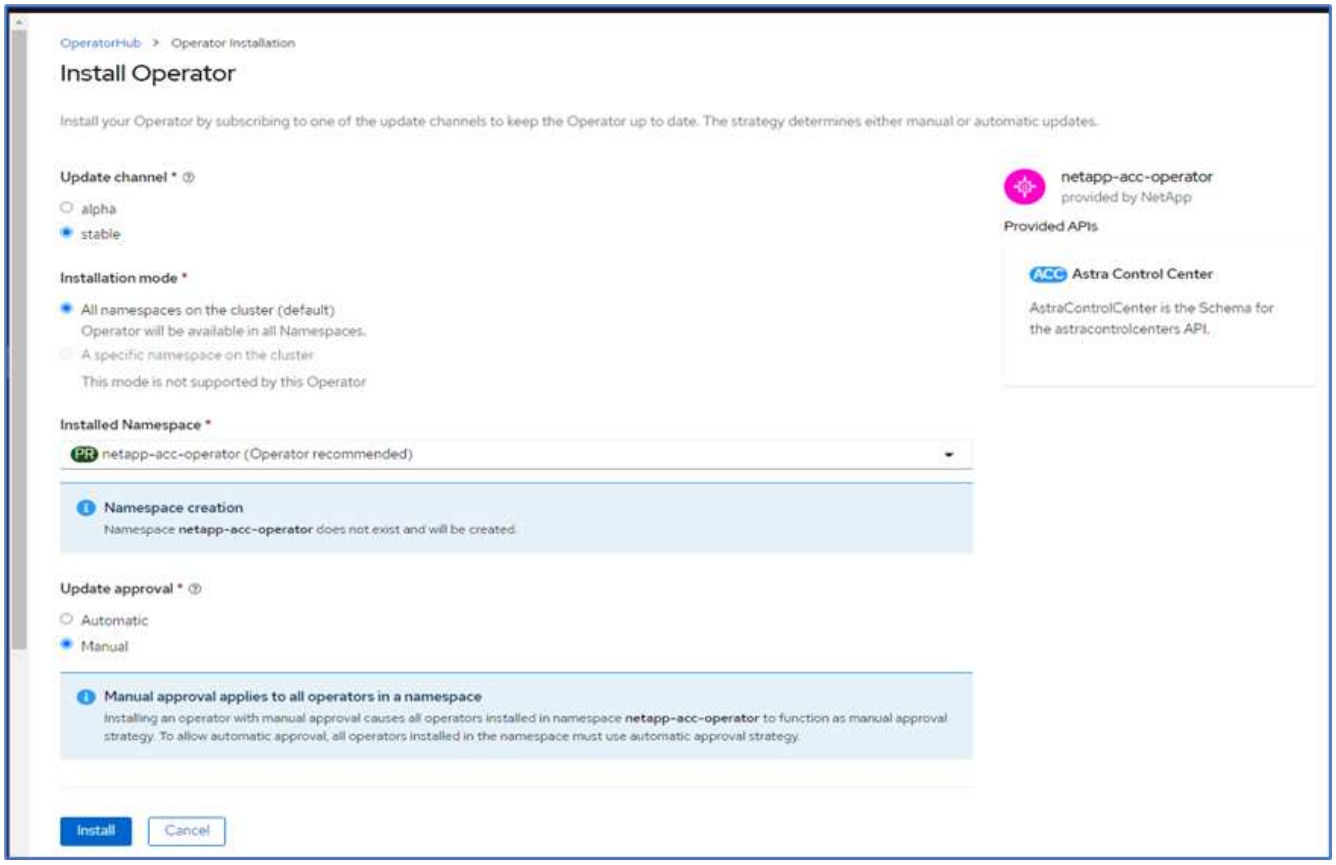


`netapp-acc-operator` Es un operador Red Hat OpenShift certificado y se encuentra en el catálogo de OperatorHub.

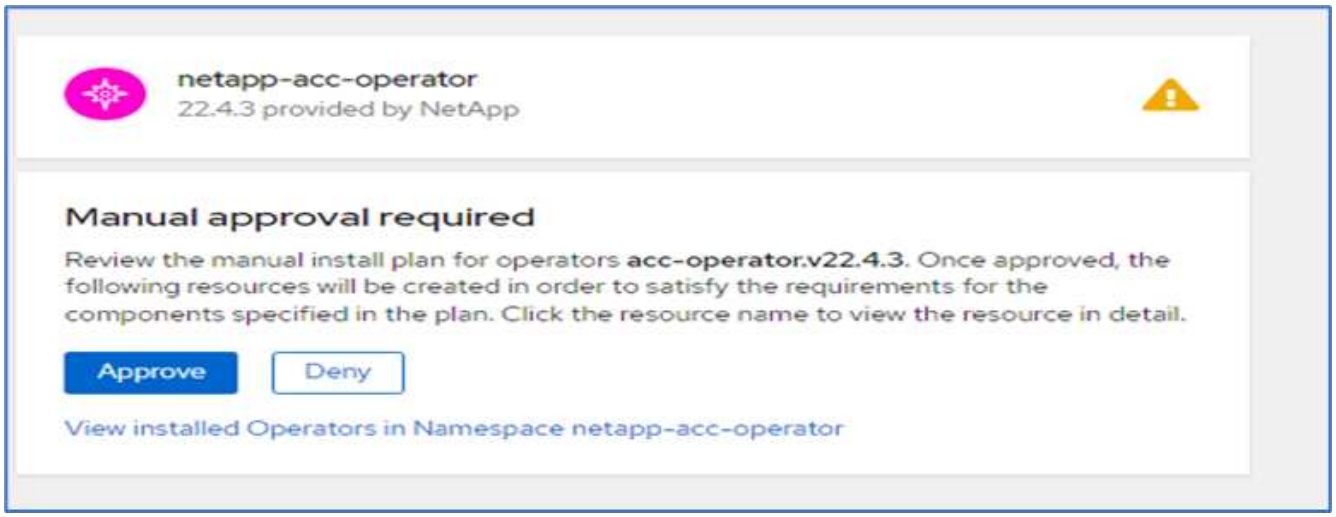
9. Seleccione `netapp-acc-operator` Y haga clic en instalar.



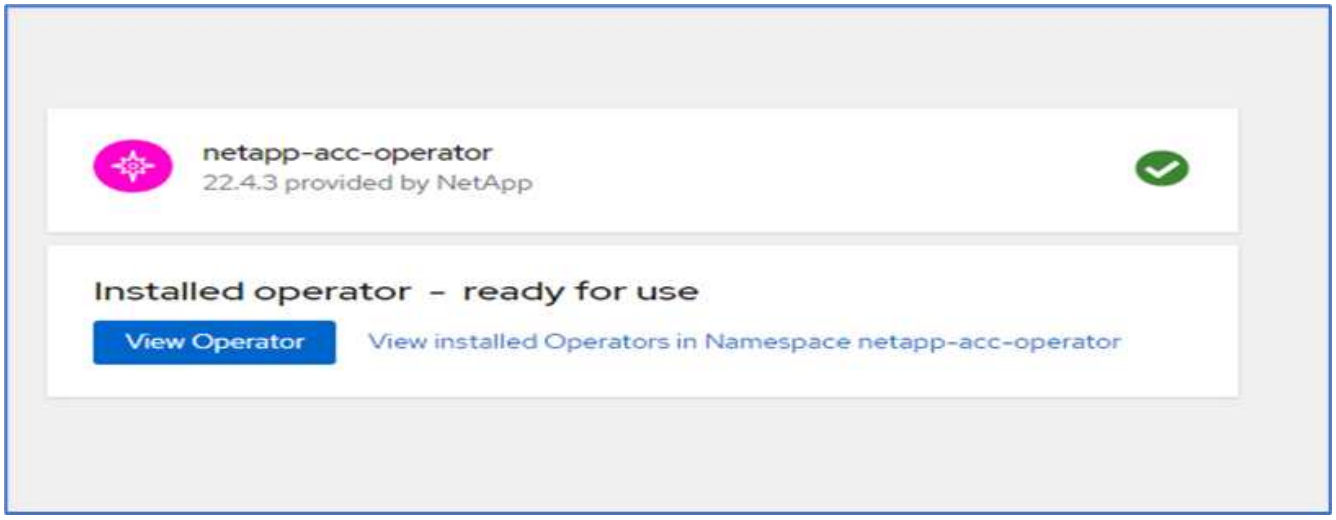
10. Seleccione las opciones adecuadas y haga clic en instalar.



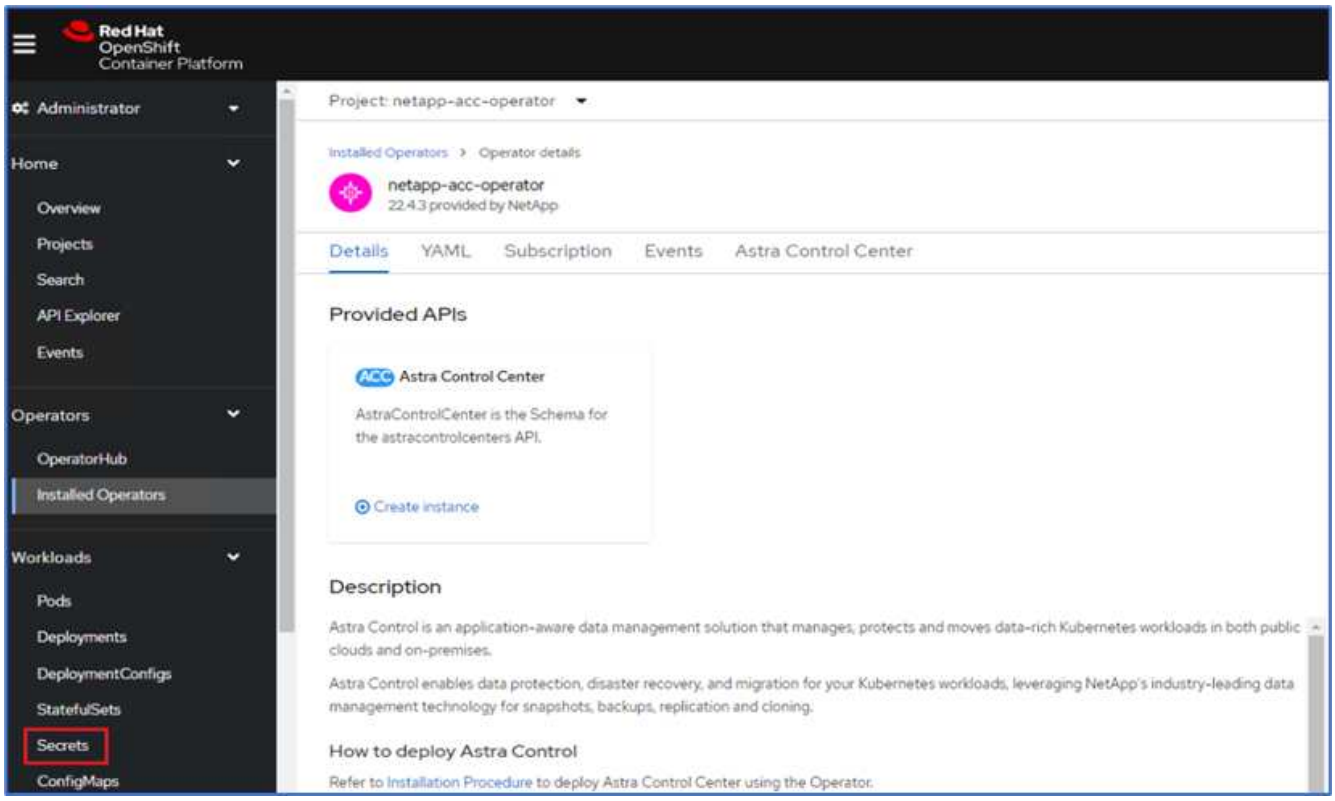
11. Apruebe la instalación y espere a que se instale el operador.



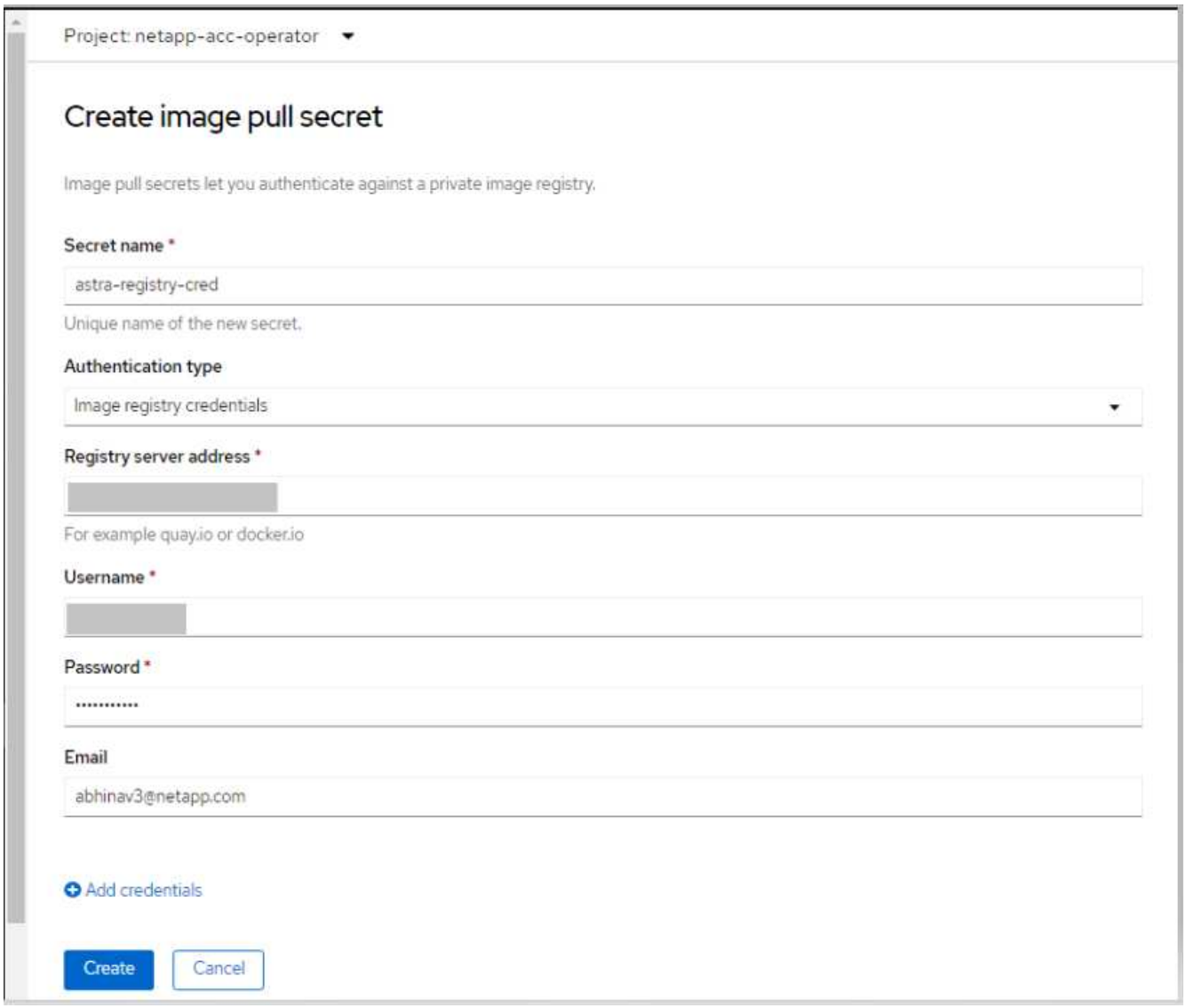
12. En esta fase, el operador se instala correctamente y está listo para su uso. Haga clic en Ver operador para iniciar la instalación de Astra Control Center.



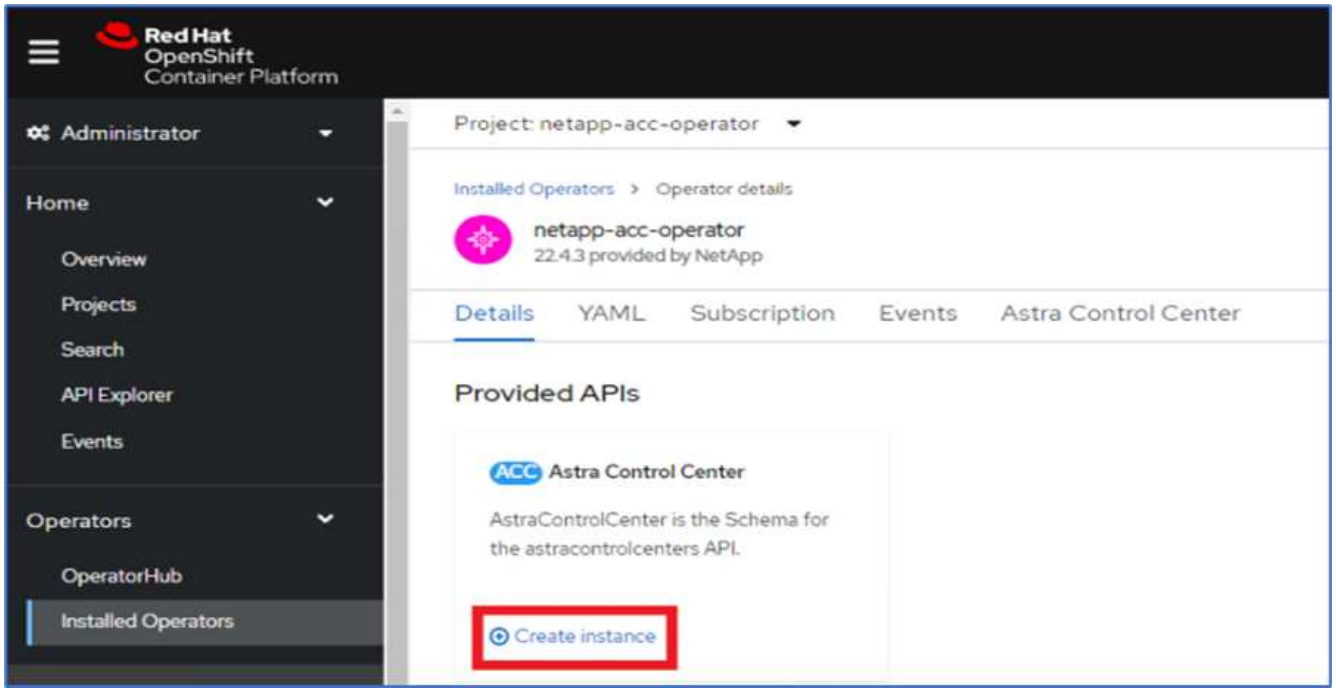
13. Antes de instalar Astra Control Center, cree el secreto de extracción para descargar imágenes Astra del registro Docker que ha introducido anteriormente.



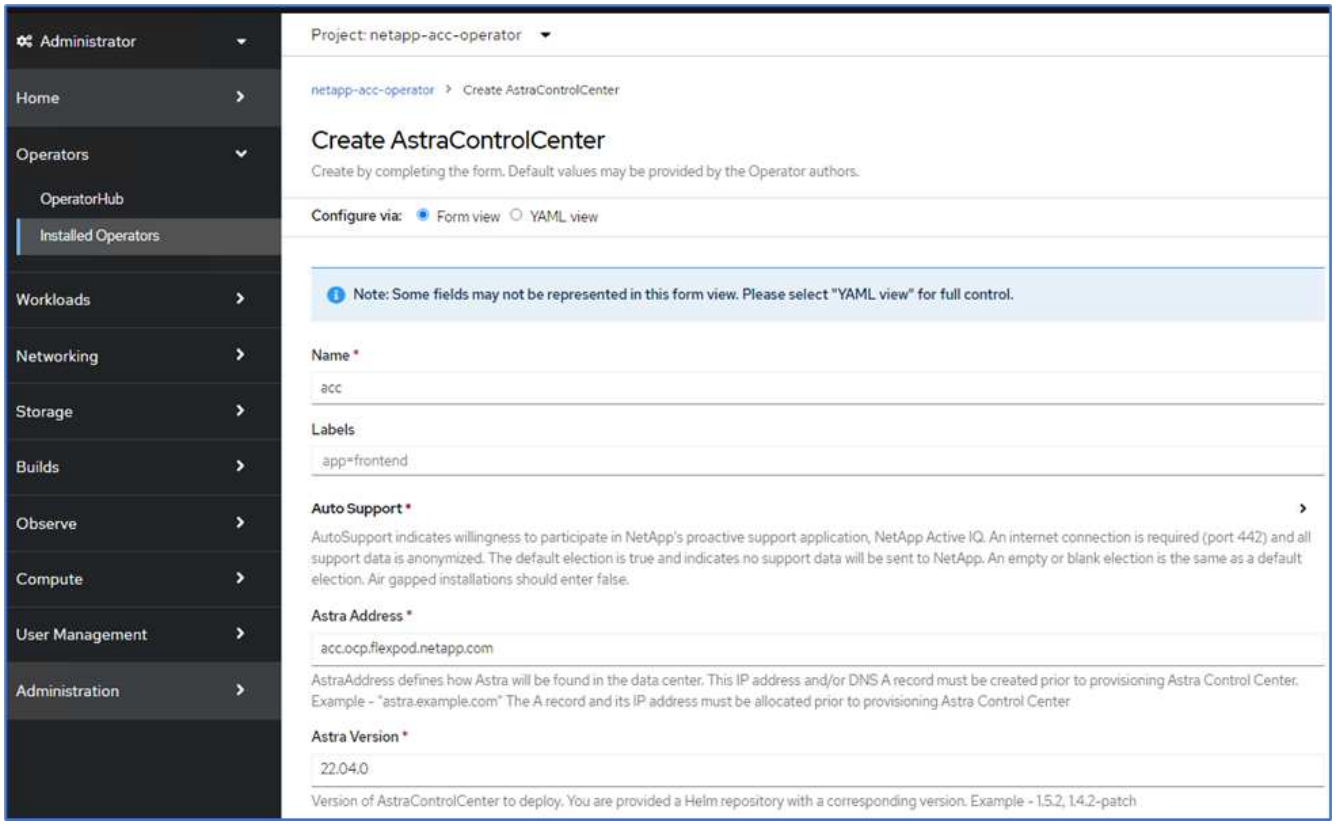
14. Para extraer las imágenes de Astra Control Center de su Docker Private repo, cree un secreto en la `netapp-acc-operator` espacio de nombres. Este nombre secreto se proporciona en el manifiesto Astra Control Center YAML en un paso posterior.



15. En el menú lateral, seleccione operadores > operadores instalados y haga clic en Crear instancia en la sección API que se proporciona.



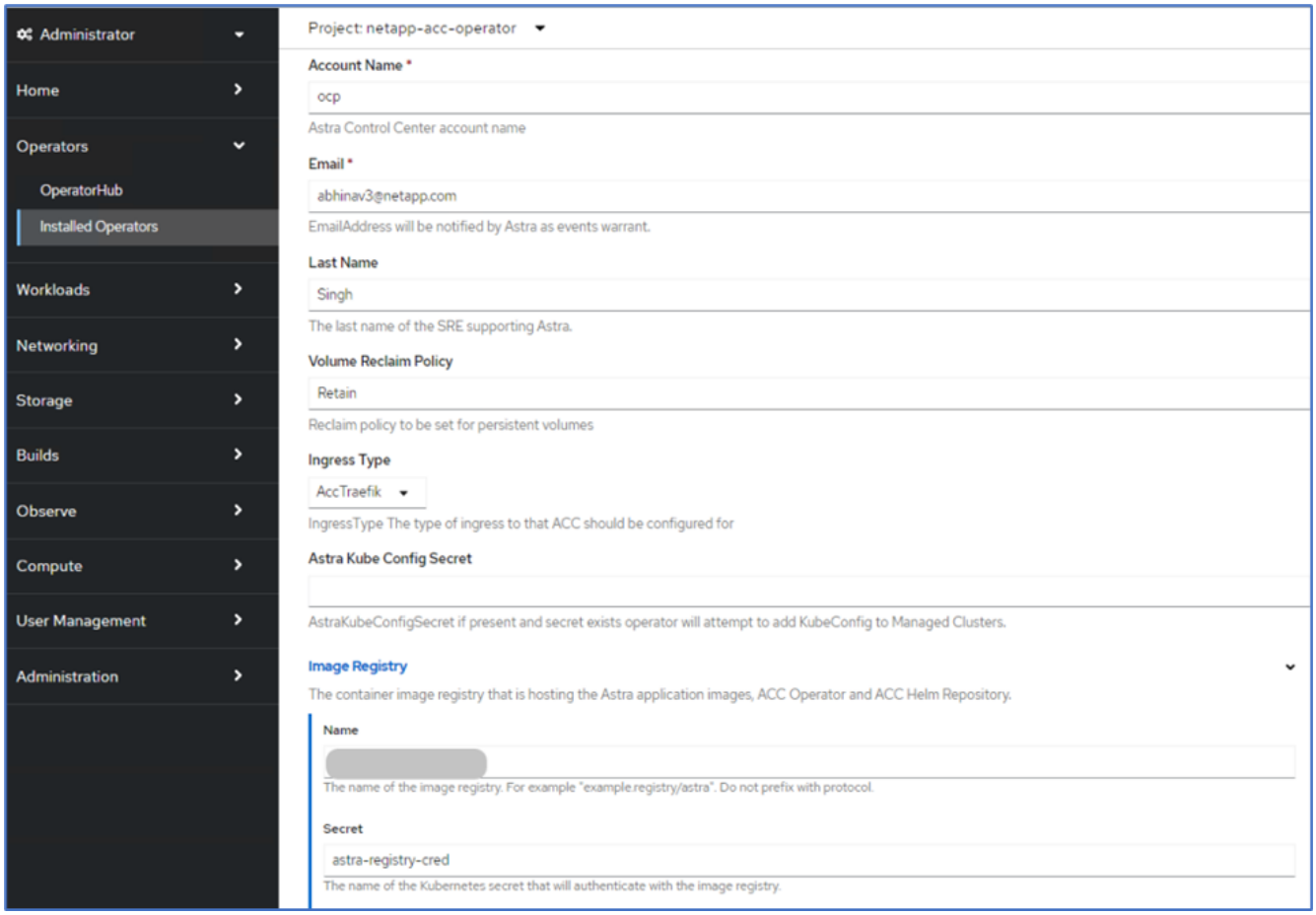
16. Complete el formulario Create AstraControlCenter. Proporcione el nombre, la dirección Astra y la versión Astra.



En Dirección Astra, proporcione la dirección FQDN para Astra Control Center. Esta dirección se utiliza para acceder a la consola web de Astra Control Center. El FQDN también debe resolver una red IP accesible y se debe configurar en el DNS.

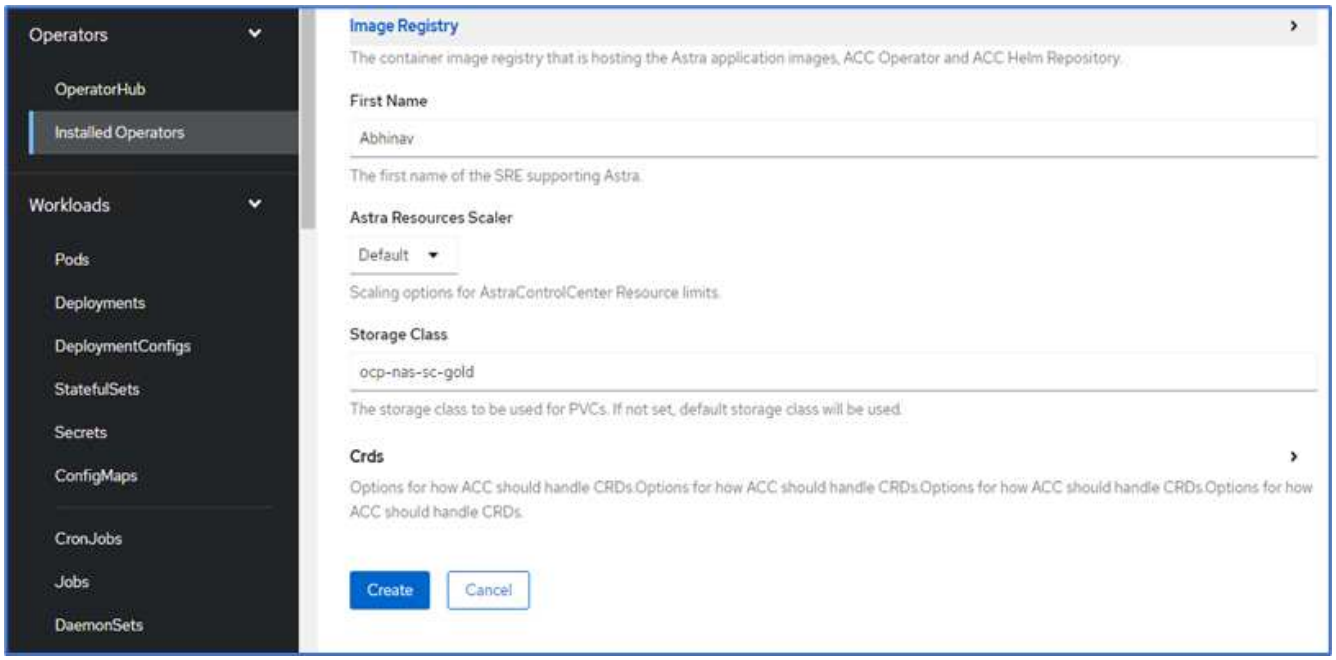
17. Escriba un nombre de cuenta, una dirección de correo electrónico, el apellido del administrador y conserve

la política de reclamación de volumen predeterminada. Si está utilizando un equilibrador de carga, establezca el tipo de entrada en `AccTraefik`. De lo contrario, seleccione Genérico para `Ingress.Controller`. En el Registro de imágenes, introduzca la ruta de acceso y el secreto del Registro de imágenes del contenedor.

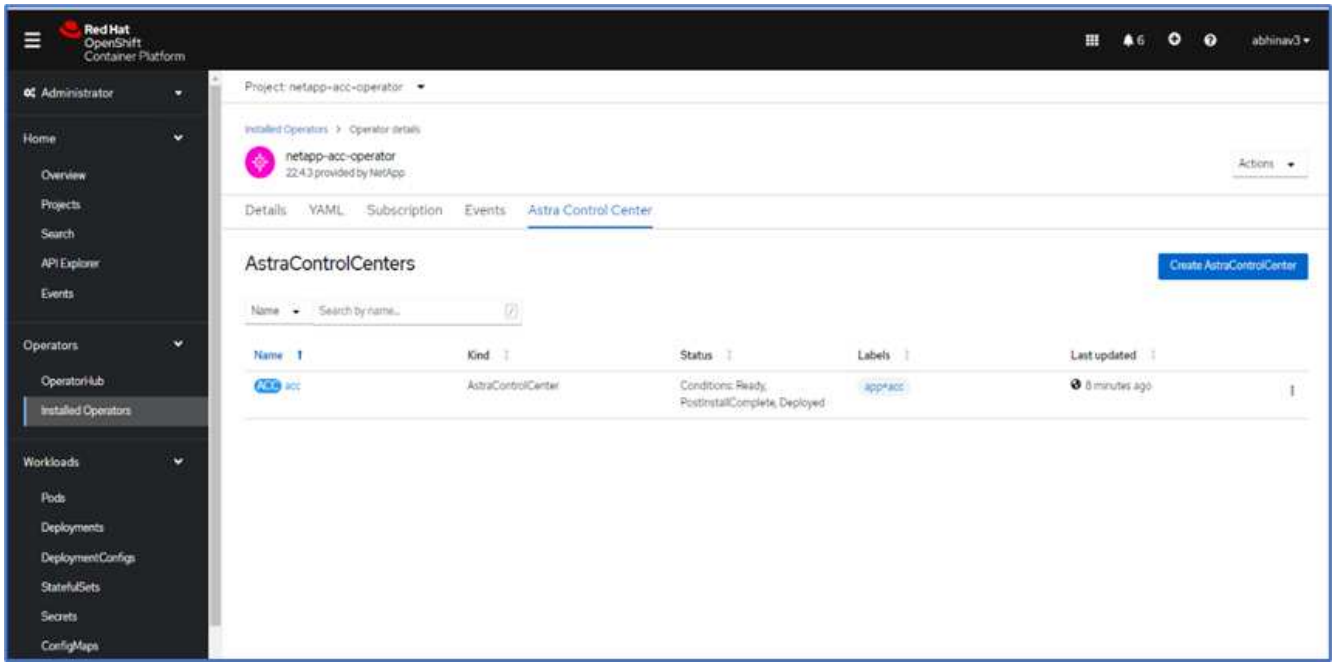


En esta solución, se utiliza el equilibrador de carga de Metallb. Por lo tanto, el tipo de entrada es AccTraefik. De esta forma se expone la puerta de enlace Traefik de Astra Control Center como un servicio Kubernetes de tipo LoadBalancer.

18. Introduzca el nombre del administrador, configure el escalado de recursos y proporcione la clase de almacenamiento. Haga clic en Crear.



El estado de la instancia de Astra Control Center debe cambiar de implementar a preparado.



19. Compruebe que todos los componentes del sistema se hayan instalado correctamente y que todos los pods estén en ejecución.

```
root@abhinav-ansible# oc get pods -n netapp-acc-operator
NAME                                               READY   STATUS
RESTARTS   AGE
acc-helm-repo-77745b49b5-7zg2v                     1/1     Running   0
10m
acc-operator-controller-manager-5c656c44c6-tqnmn   2/2     Running   0
13m
```

```
activity-589c6d59f4-x2sfs                          1/1     Running   0
6m4s
api-token-authentication-4q5lj                     1/1     Running   0
5m26s
api-token-authentication-pzptd                     1/1     Running   0
5m27s
api-token-authentication-tbtg6                     1/1     Running   0
5m27s
asup-669df8d49-qps54                               1/1     Running   0
5m26s
authentication-5867c5f56f-dnpp2                    1/1     Running   0
3m54s
bucketservice-85495bc475-5zcc5                     1/1     Running   0
5m55s
cert-manager-67f486bbc6-txhh6                      1/1     Running   0
9m5s
cert-manager-cainjector-75959db744-4l5p5           1/1     Running   0
9m6s
cert-manager-webhook-765556b869-g6wdf              1/1     Running   0
9m6s
cloud-extension-5d595f85f-txrfl                    1/1     Running   0
5m27s
cloud-insights-service-674649567b-5s4wd            1/1     Running   0
5m49s
composite-compute-6b58d48c69-46vhc                 1/1     Running   0
6m11s
composite-volume-6d447fd959-chnrt                  1/1     Running   0
5m27s
credentials-66668f8ddd-8qc5b                       1/1     Running   0
7m20s
entitlement-fd6fc5c58-wxnmh                        1/1     Running   0
6m20s
features-756bbb7c7c-rgcrm                          1/1     Running   0
5m26s
fluent-bit-ds-278pg                                1/1     Running   0
3m35s
fluent-bit-ds-5pqc6                                1/1     Running   0
3m35s
fluent-bit-ds-8l7cq                                1/1     Running   0
3m35s
fluent-bit-ds-9qbft                                1/1     Running   0
3m35s
fluent-bit-ds-nj475                                1/1     Running   0
3m35s
fluent-bit-ds-x9pd8                                1/1     Running   0
3m35s
```

```
graphql-server-698d6f4bf-kftwc                    1/1     Running   0
3m20s
identity-5d4f4c87c9-wjz6c                         1/1     Running   0
6m27s
influxdb2-0                                       1/1     Running   0
9m33s
krakend-657d44bf54-8cb56                          1/1     Running   0
3m21s
license-594bbdc-rghdg                             1/1     Running   0
6m28s
login-ui-6c65fbbbd4-jg8wz                         1/1     Running   0
3m17s
loki-0                                            1/1     Running   0
9m30s
metrics-facade-75575f69d7-hnlk6                   1/1     Running   0
6m10s
monitoring-operator-65dff79cfb-z78vk              2/2     Running   0
3m47s
nats-0                                            1/1     Running   0
10m
nats-1                                            1/1     Running   0
9m43s
nats-2                                            1/1     Running   0
9m23s
nautilus-7bb469f857-4hlc6                         1/1     Running   0
6m3s
nautilus-7bb469f857-vz94m                         1/1     Running   0
4m42s
openapi-8586db4bcd-gwwvf                          1/1     Running   0
5m41s
packages-6bdb949cfb-nrq8l                         1/1     Running   0
6m35s
polaris-consul-consul-server-0                    1/1     Running   0
9m22s
polaris-consul-consul-server-1                    1/1     Running   0
9m22s
polaris-consul-consul-server-2                    1/1     Running   0
9m22s
polaris-mongodb-0                                 2/2     Running   0
9m22s
polaris-mongodb-1                                 2/2     Running   0
8m58s
polaris-mongodb-2                                 2/2     Running   0
8m34s
polaris-ui-5df7687dbd-trcnf                       1/1     Running   0
3m18s
```

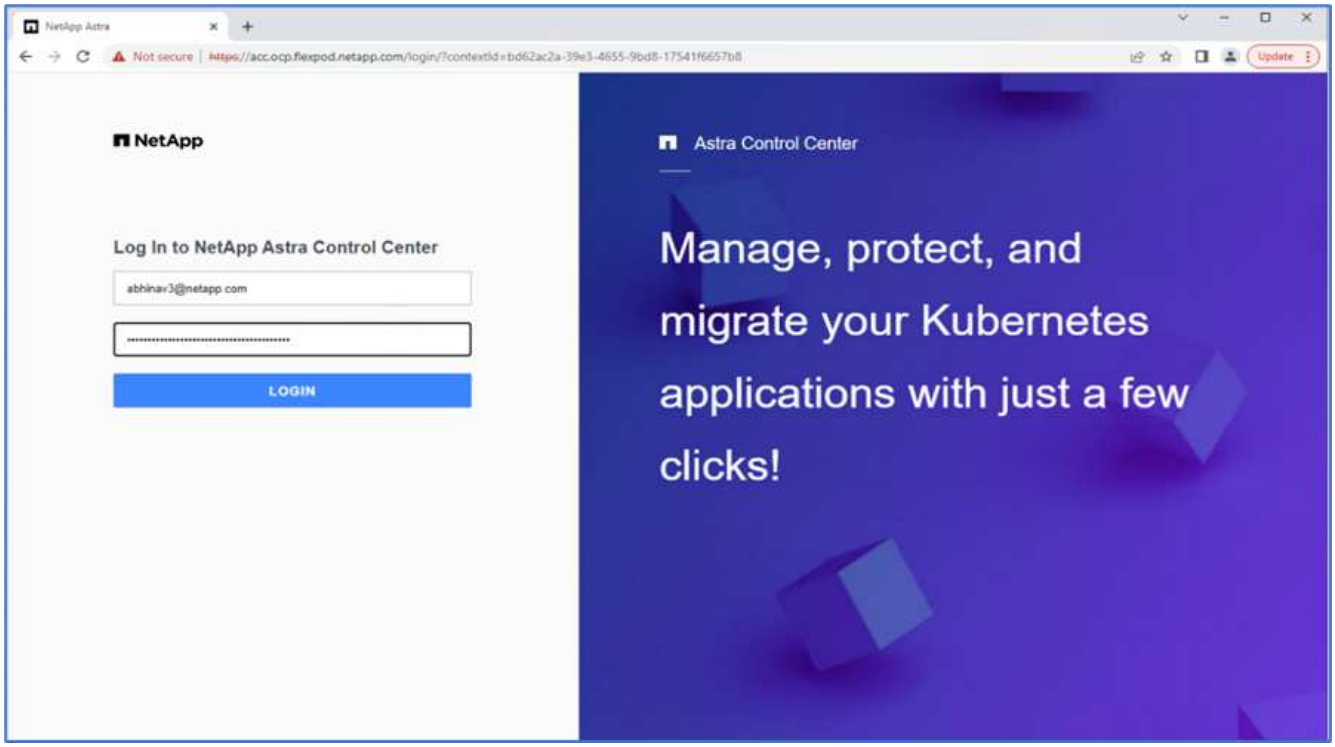
```
polaris-vault-0                                   1/1     Running   0
9m18s
polaris-vault-1                                   1/1     Running   0
9m18s
polaris-vault-2                                   1/1     Running   0
9m18s
public-metrics-7b96476f64-j88bw                   1/1     Running   0
5m48s
storage-backend-metrics-5fd6d7cd9c-vcb4j          1/1     Running   0
5m59s
storage-provider-bb85ff965-m7qrq                  1/1     Running   0
5m25s
telegraf-ds-4zqgz                                 1/1     Running   0
3m36s
telegraf-ds-cp9x4                                 1/1     Running   0
3m36s
telegraf-ds-h4n59                                 1/1     Running   0
3m36s
telegraf-ds-jnp2q                                 1/1     Running   0
3m36s
telegraf-ds-pdz5j                                 1/1     Running   0
3m36s
telegraf-ds-znqtp                                 1/1     Running   0
3m36s
telegraf-rs-rt64j                                 1/1     Running   0
3m36s
telemetry-service-7dd9c74bfc-sfkzt                1/1     Running   0
6m19s
tenancy-d878b7fb6-wf8x9                           1/1     Running   0
6m37s
traefik-6548496576-5v2g6                          1/1     Running   0
98s
traefik-6548496576-g82pq                          1/1     Running   0
3m8s
traefik-6548496576-psn49                          1/1     Running   0
38s
traefik-6548496576-qrkfd                          1/1     Running   0
2m53s
traefik-6548496576-srs6r                          1/1     Running   0
98s
trident-svc-679856c67-78kbt                       1/1     Running   0
5m27s
vault-controller-747d664964-xmn6c                 1/1     Running   0
7m37s
```

Cada pod debe tener el estado de ejecución. Puede tardar varios minutos en implementar los pods del sistema.

20. Cuando todos los pods estén en ejecución, ejecute el siguiente comando para recuperar la contraseña una vez. En la versión YAML de la salida, compruebe la `status.deploymentState` para el valor desplegado y, a continuación, copie el `status.uuid` valor. La contraseña es `ACC-` Seguido del valor UUID. (ACC-[UUID]).

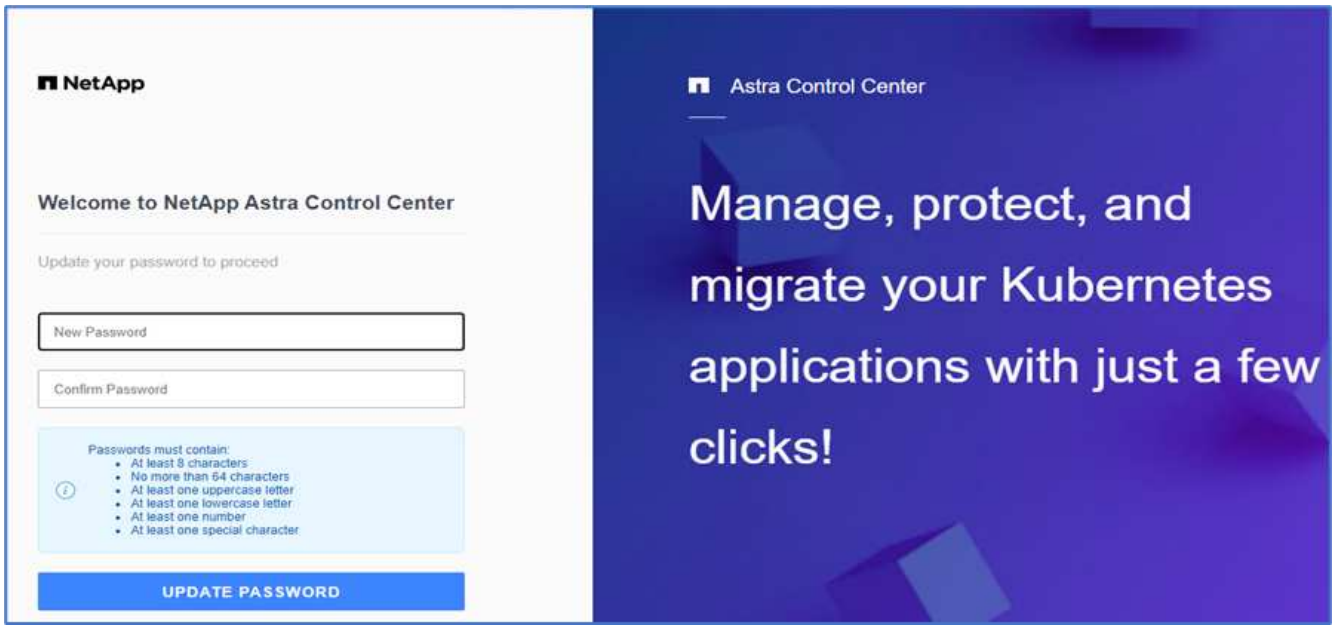
```
root@abhinav-ansible# oc get acc -o yaml -n netapp-acc-operator
```

21. En un explorador, desplácese hasta la URL usando el FQDN que haya proporcionado.
22. Inicie sesión utilizando el nombre de usuario predeterminado, que es la dirección de correo electrónico proporcionada durante la instalación y la contraseña única ACC-[UUID].



Si introduce una contraseña incorrecta tres veces, la cuenta de administrador estará bloqueada durante 15 minutos.

23. Cambie la contraseña y continúe.

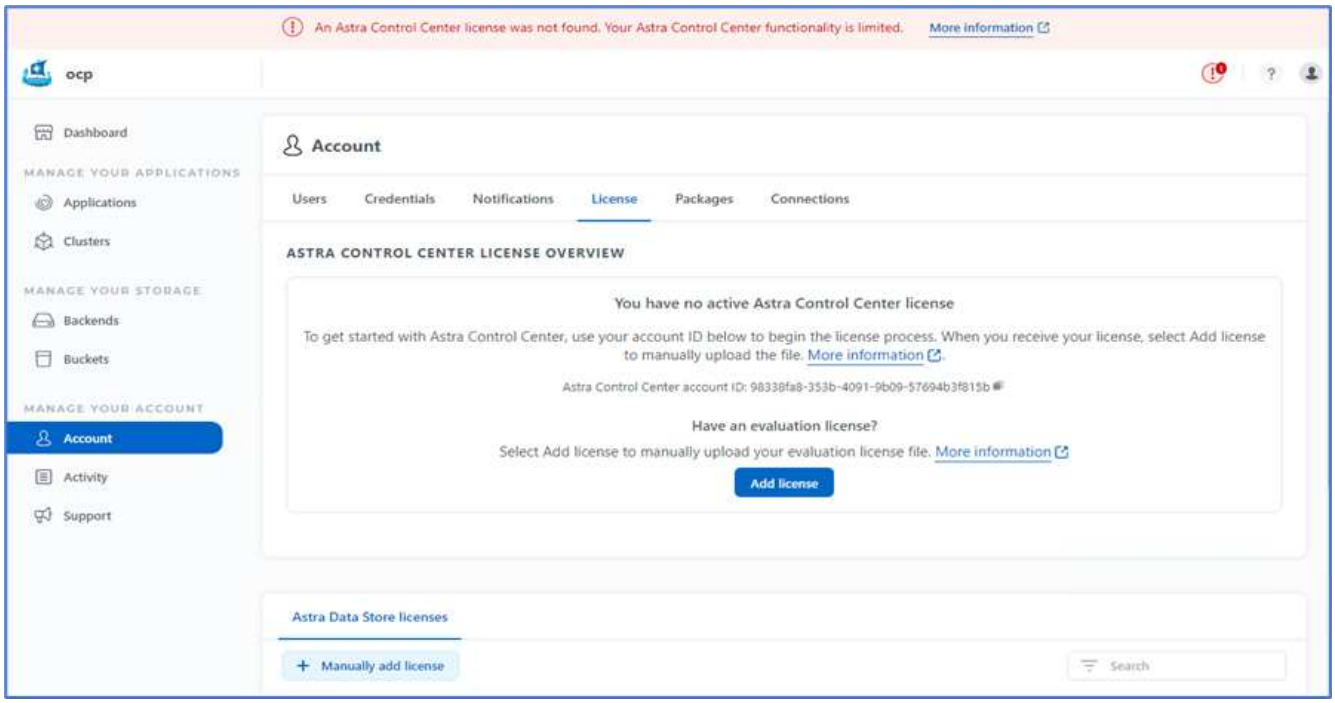


Para obtener más información acerca de la instalación de Astra Control Center, consulte "Descripción general de la instalación de Astra Control Center" página.

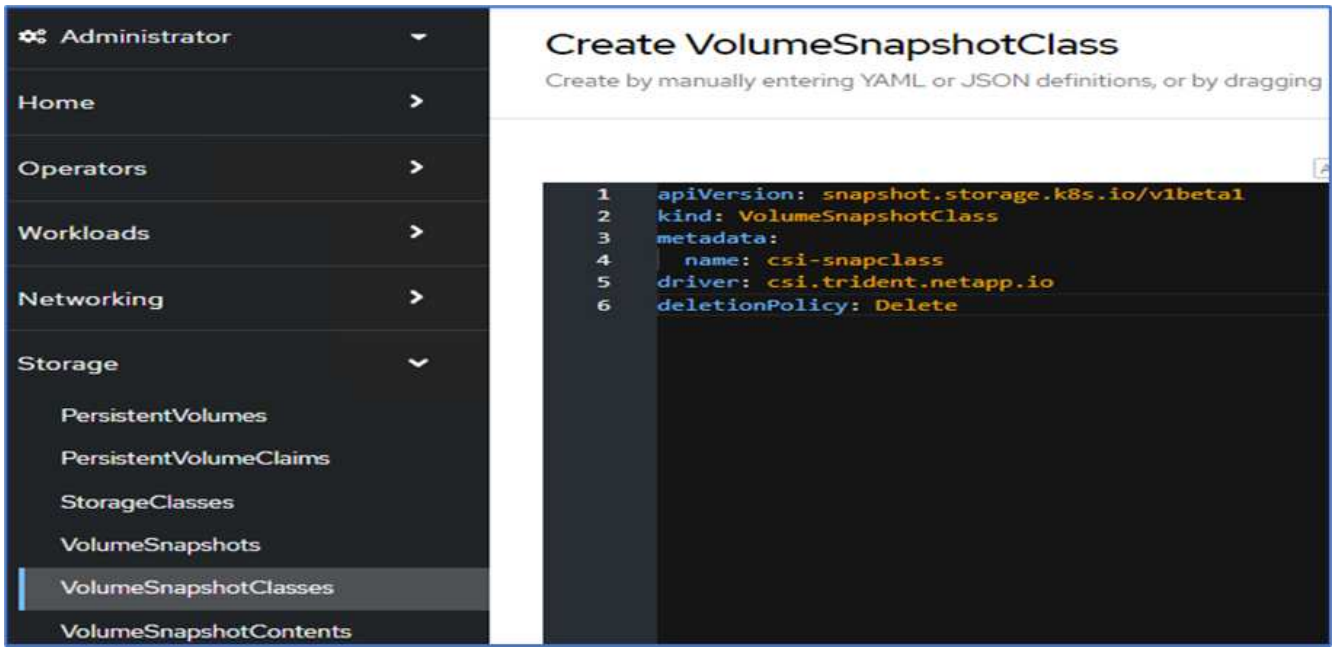
Configure Astra Control Center

Después de instalar Astra Control Center, inicie sesión en la interfaz de usuario, cargue la licencia, añada clústeres, gestione el almacenamiento y añada bloques.

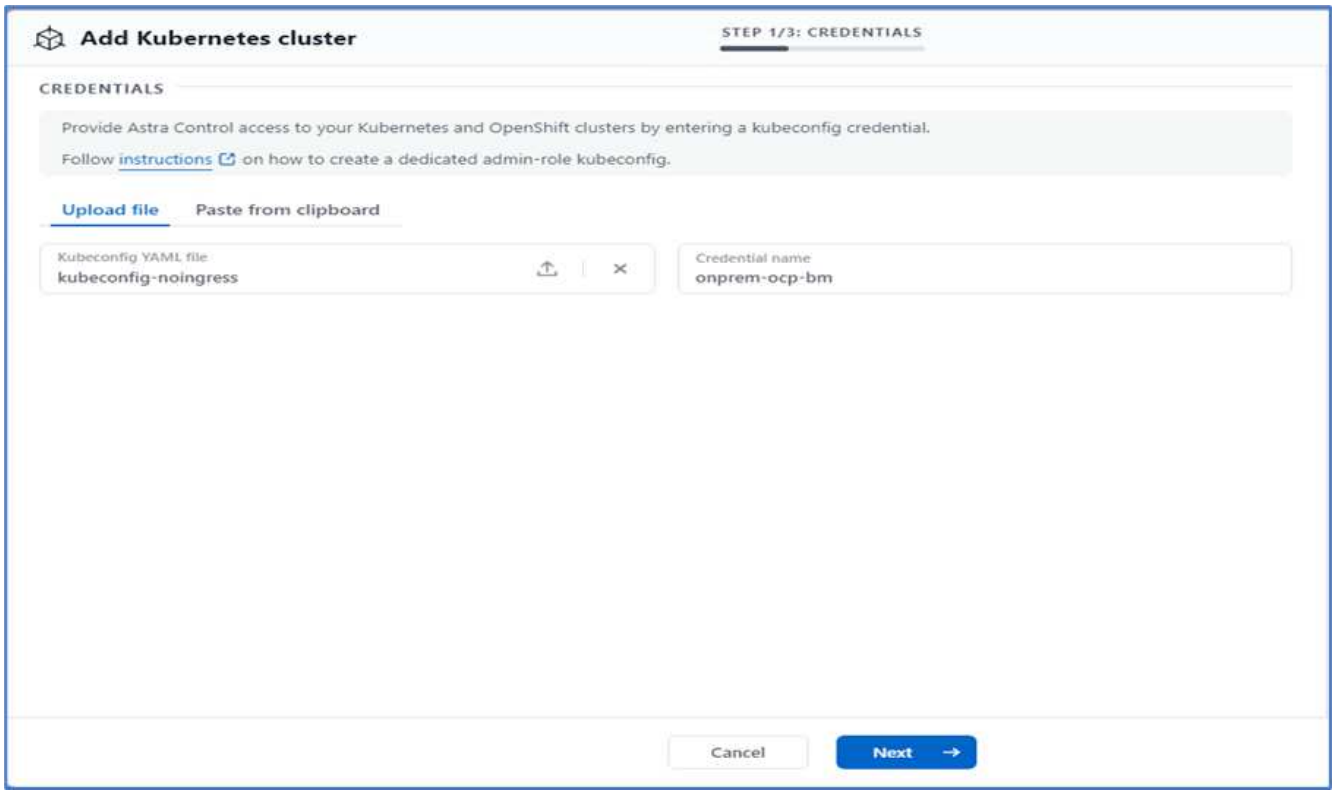
1. En la página de inicio de cuenta, vaya a la ficha Licencia y seleccione Agregar licencia para cargar la licencia Astra.



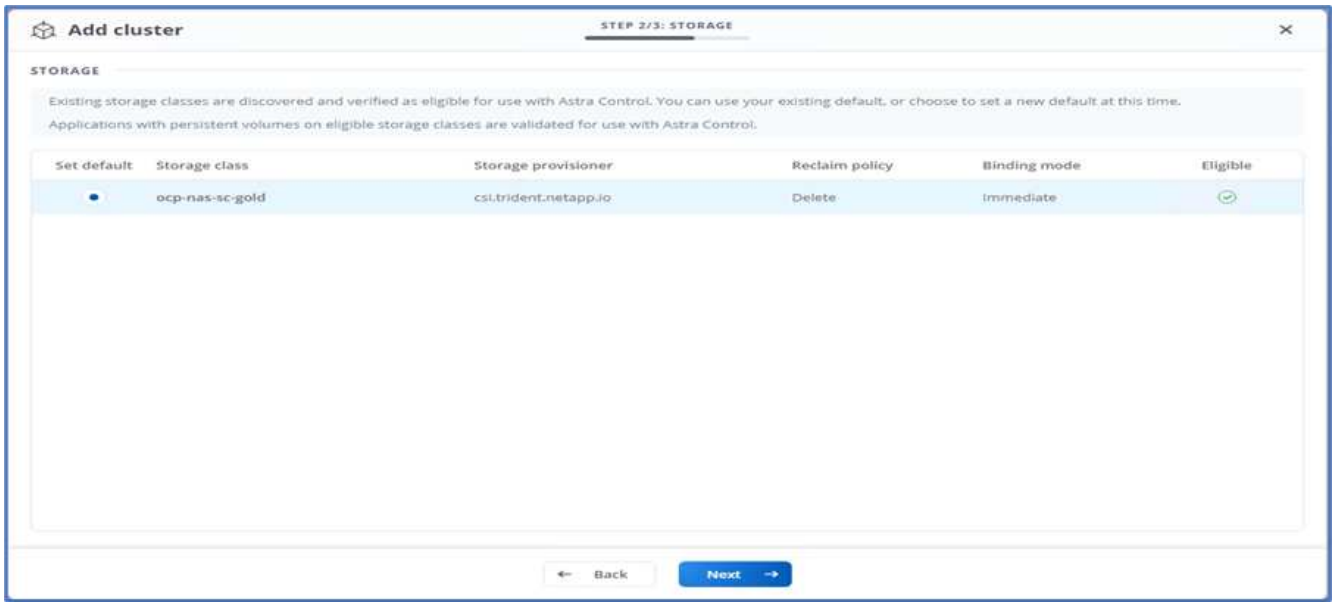
2. Antes de agregar el clúster OpenShift, cree una clase de snapshot Astra Trident Volume desde la consola web de OpenShift. La clase de snapshot Volume se configura con la `csi.trident.netapp.io` controlador.



3. Para añadir el clúster de Kubernetes, vaya a Clusters en la página de inicio y haga clic en Add Kubernetes Cluster. A continuación, cargue el `kubeconfig` archivo para el clúster y escriba un nombre de credencial. Haga clic en Siguiente.



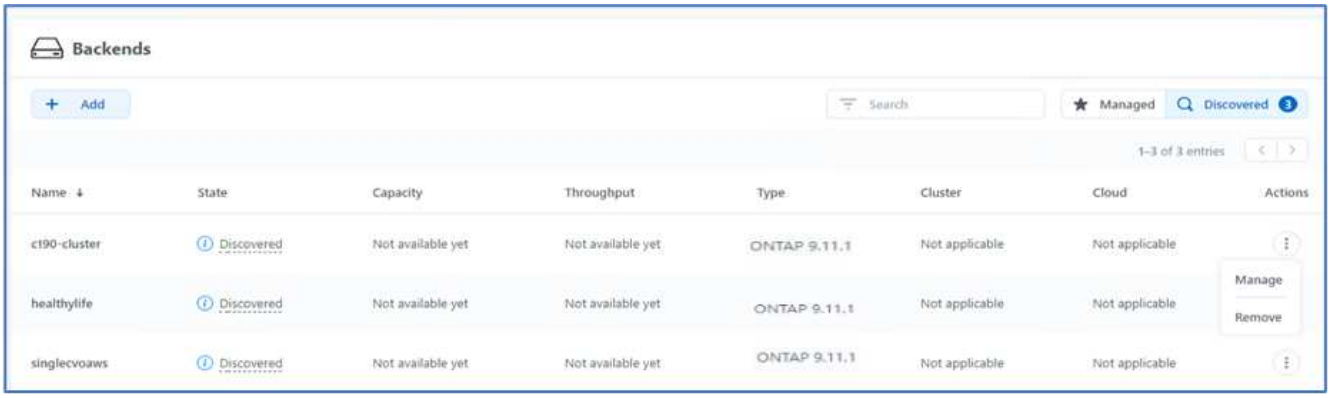
4. Las clases de almacenamiento existentes se detectan de forma automática. Seleccione la clase de almacenamiento predeterminada, haga clic en Next y después en Add cluster.



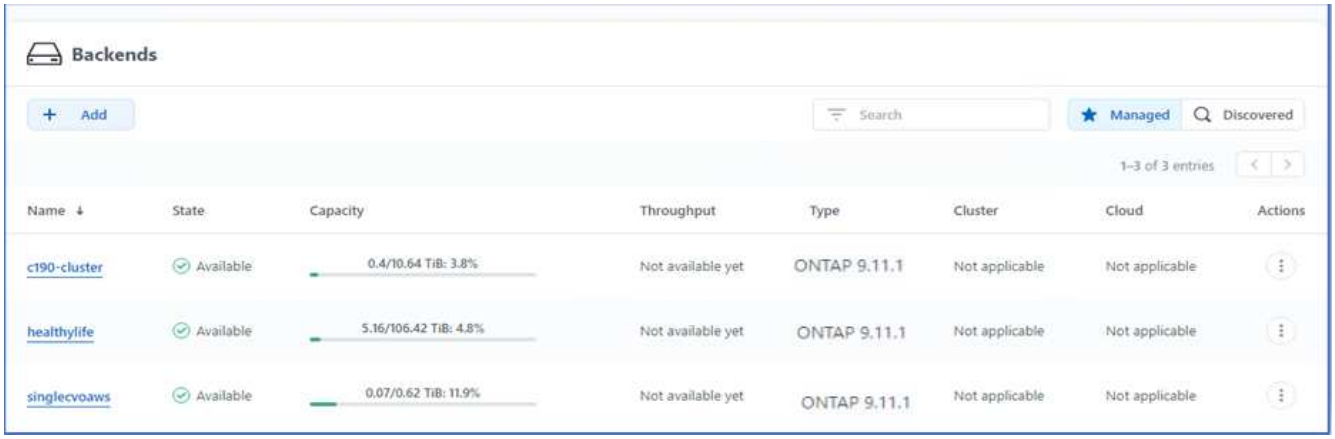
5. El clúster se añade en unos minutos. Para agregar clústeres de OpenShift Container Platform adicionales, repita los pasos 1–4.

> Para añadir un entorno operativo OpenShift adicional como recurso informático gestionado, asegúrese de que Astra Trident "Objetos VolumeSnapshotClass" están definidos.

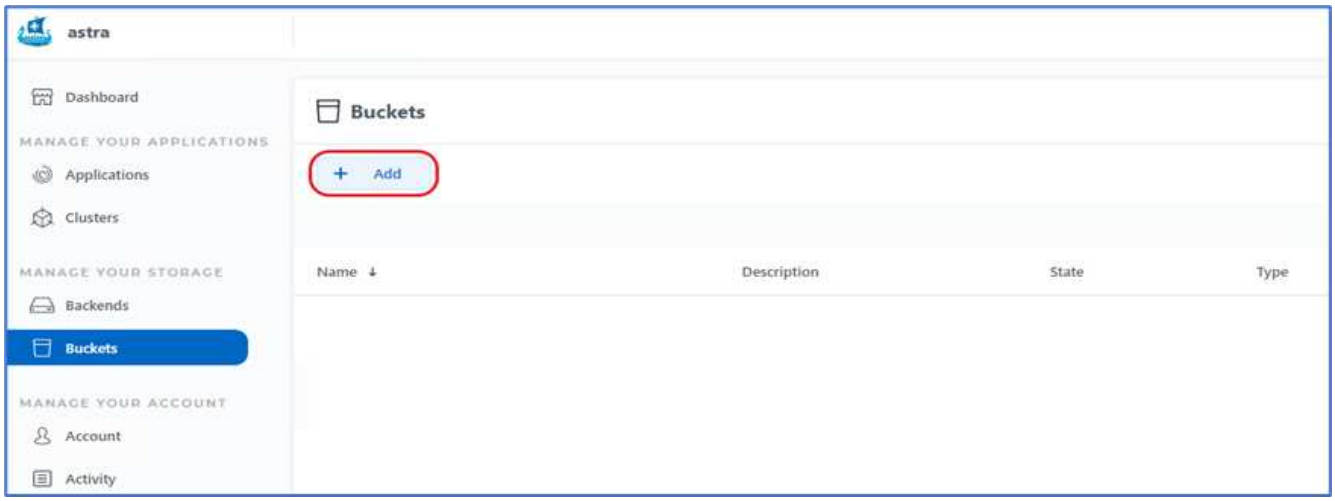
6. Para gestionar el almacenamiento, vaya a backends (backends), haga clic en los tres puntos de la sección Actions (acciones) en el backend que desea gestionar. Haga clic en gestionar.



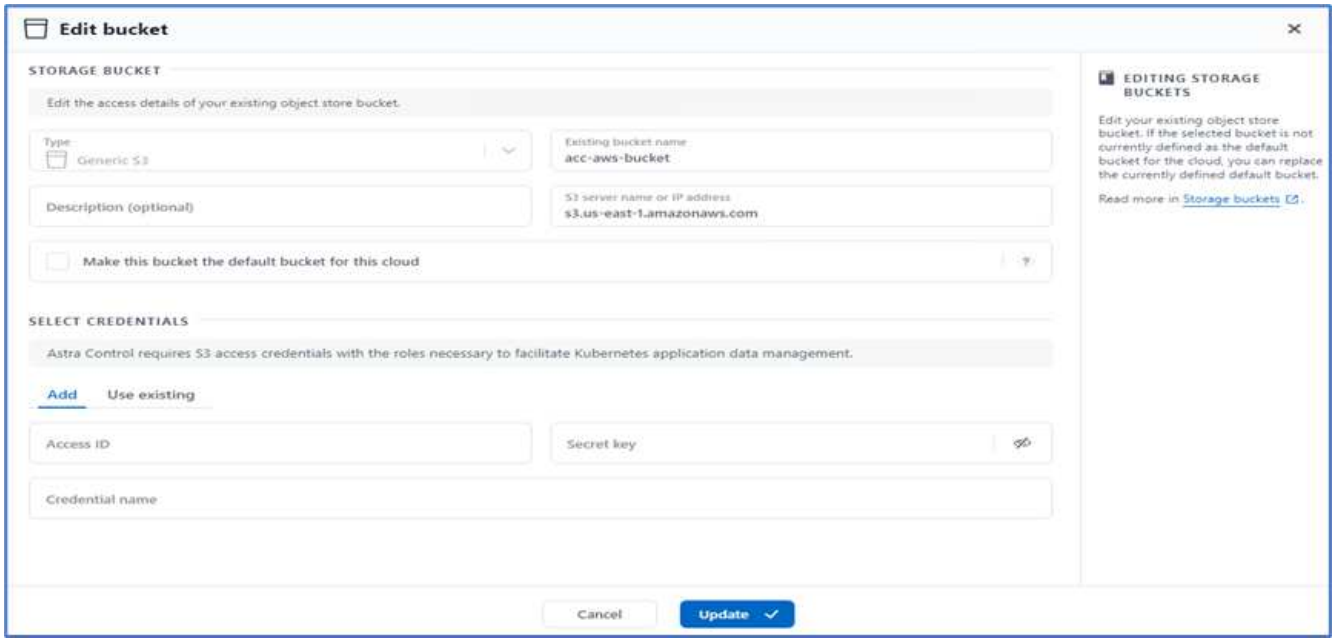
7. Proporcione las credenciales de ONTAP y haga clic en Next. Revise la información y haga clic en Managed. Los back-ends deberían ser el siguiente ejemplo.



8. Para agregar un cucharón a Astra Control, seleccione cucharones y haga clic en Agregar.

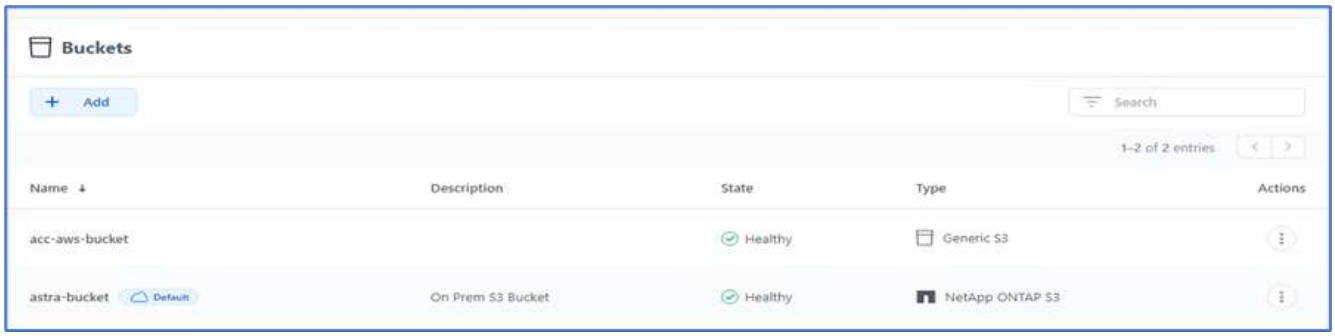


9. Seleccione el tipo de bloque y proporcione el nombre de bloque, el nombre del servidor S3, la dirección IP y la credencial S3. Haga clic en Update.



En esta solución, se usan los bloques AWS S3 y ONTAP S3. También puede utilizar StorageGRID.

El estado de la cuchara debe ser saludable.



Como parte del registro del clúster de Kubernetes con Astra Control Center para la gestión de datos para aplicaciones, Astra Control crea automáticamente vinculaciones de roles y un espacio de nombres de supervisión de NetApp para recopilar métricas y registros de los pods de la aplicación y los nodos de trabajo. Cree una de las clases de almacenamiento basado en ONTAP compatibles por defecto.

Usted primero "Añada un clúster a la gestión de Astra Control", Puede instalar aplicaciones en el clúster (fuera de Astra Control) y, a continuación, ir a la página aplicaciones de Astra Control para gestionar las aplicaciones y sus recursos. Para obtener más información sobre la gestión de aplicaciones con Astra, consulte "Requisitos de gestión de aplicaciones".

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

Validación de la solución

Descripción general

"Anterior: Instalación de Astra Control Center en OpenShift Container Platform."

En esta sección, vamos a revisar la solución con algunos casos de uso:

- Restaurar una aplicación con estado desde una copia de seguridad remota a otro clúster de OpenShift que se ejecuta en la nube.
- Restaurar una aplicación con estado en el mismo espacio de nombres en el clúster de OpenShift.
- Movilidad de aplicaciones mediante la clonación de un sistema FlexPod (OpenShift Container Platform Bare Metal) a otro sistema FlexPod (OpenShift Container Platform en VMware).

Cabe destacar que en esta solución sólo se validan algunos casos de uso. Esta validación no representa en modo alguno toda la funcionalidad de Astra Control Center.

"Siguiente: Recuperación de aplicaciones con backups remotos."

Recuperación de aplicaciones con backups remotos

"Anterior: Información general de validación de la solución."

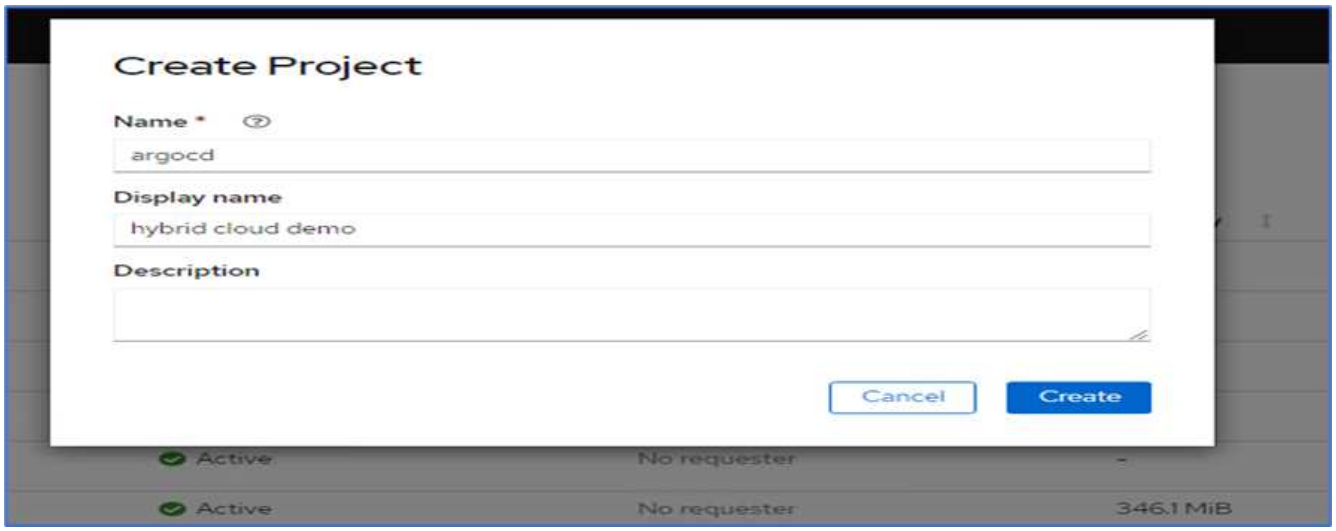
Con Astra, puede realizar un backup completo y consistente con las aplicaciones que

puede utilizar para restaurar su aplicación con sus datos en un clúster de Kubernetes diferente que se ejecute en un centro de datos en las instalaciones o en un cloud público.

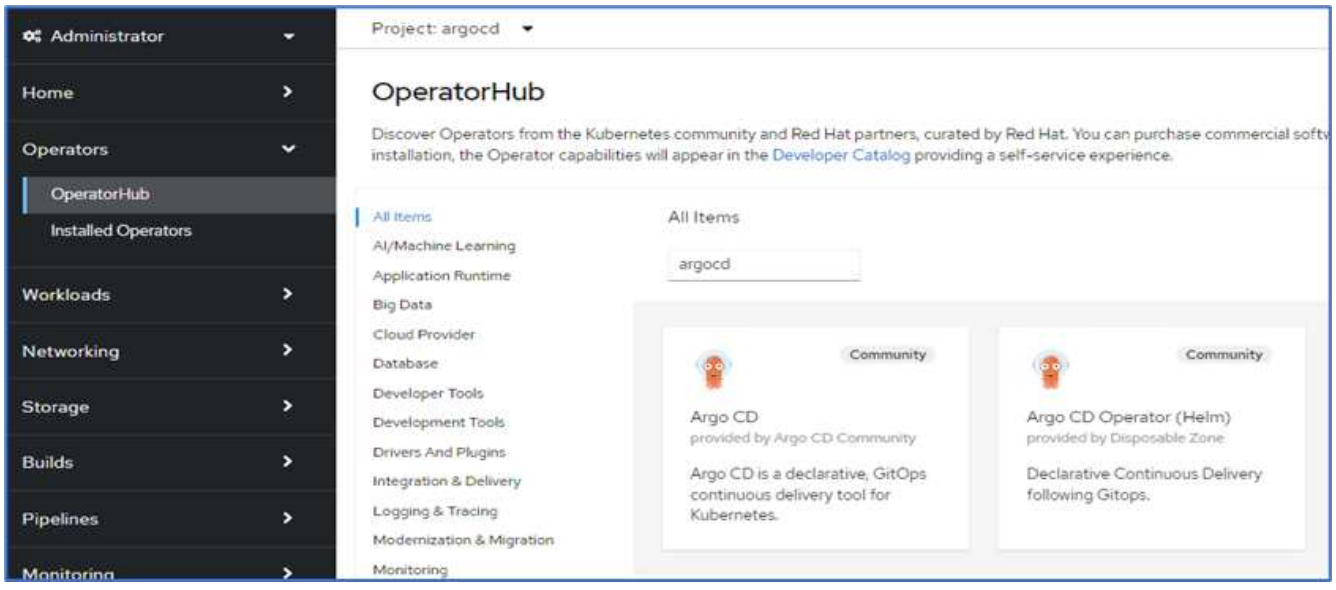
Para validar que la recuperación de aplicaciones se ha realizado correctamente, simule un fallo local de una aplicación que se ejecuta en el sistema FlexPod y restaure la aplicación a un clúster K8s que se ejecuta en el cloud mediante un backup remoto.

La aplicación de ejemplo es una aplicación de lista de precios que utiliza MySQL para la base de datos. Para automatizar la puesta en marcha, usamos "CD Argo" herramienta. Argo CD es una herramienta de entrega continua, declarativa, GitOPS para Kubernetes.

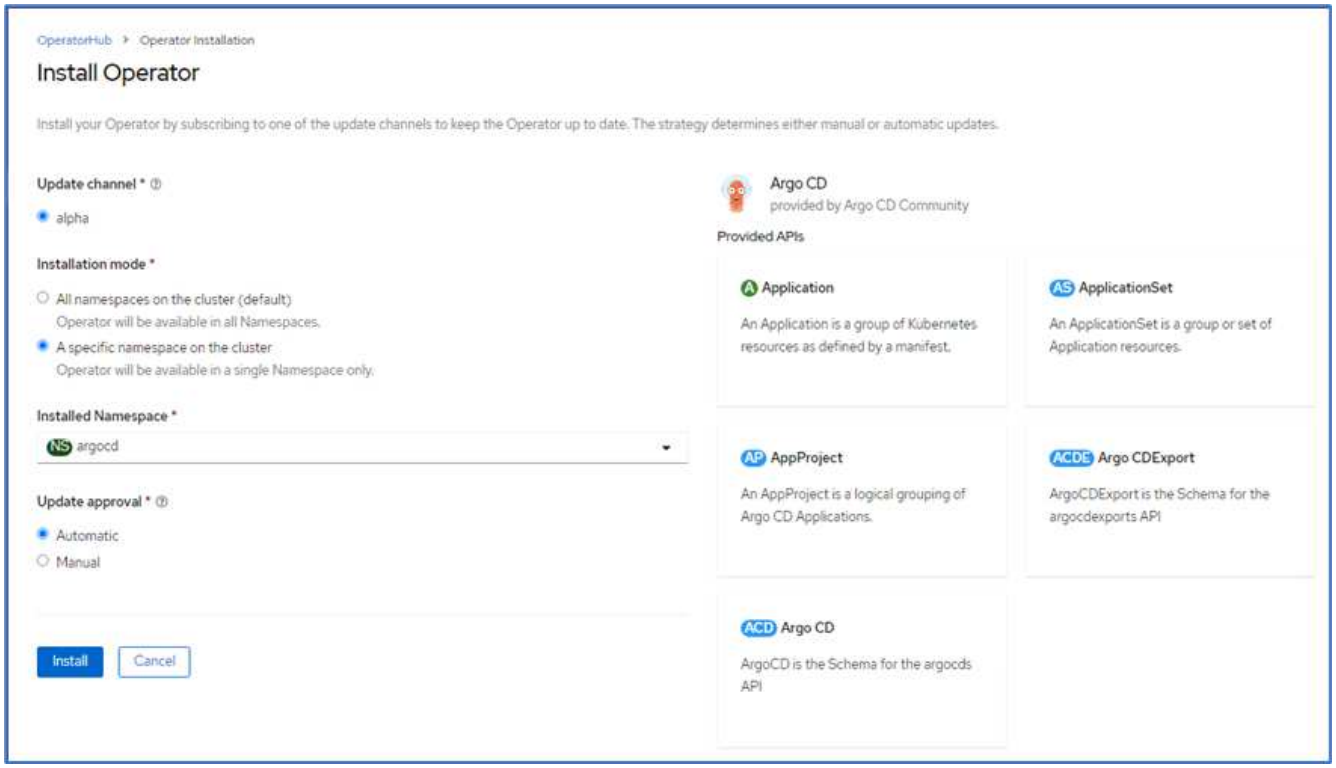
1. Inicie sesión en el clúster OpenShift de las instalaciones y cree un nuevo proyecto con el nombre `argocd`.



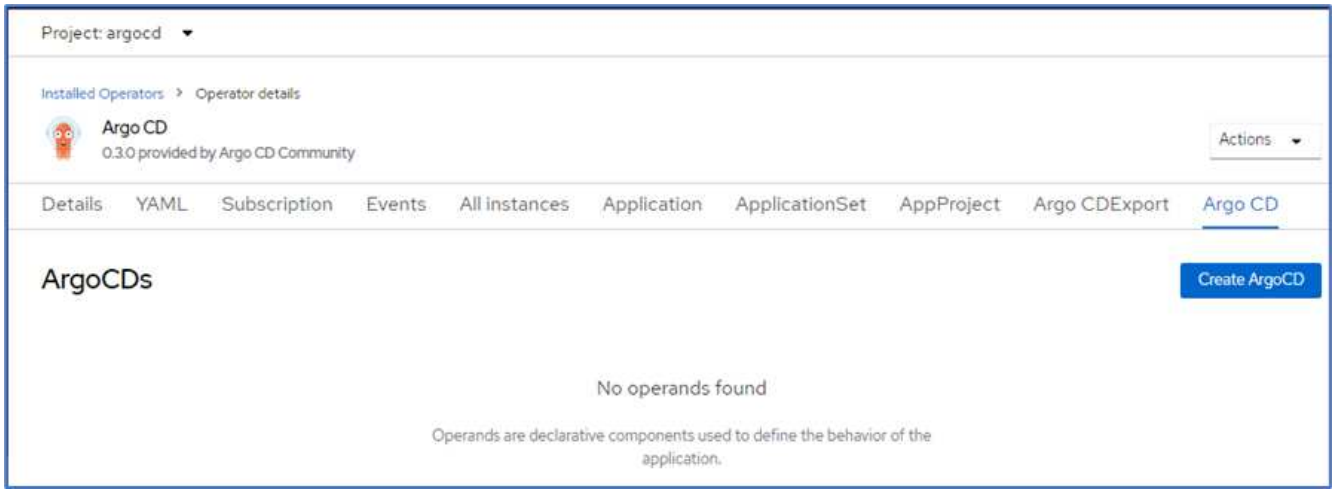
2. En OperatorHub, busque `argocd` Y seleccione operador de Argo CD.



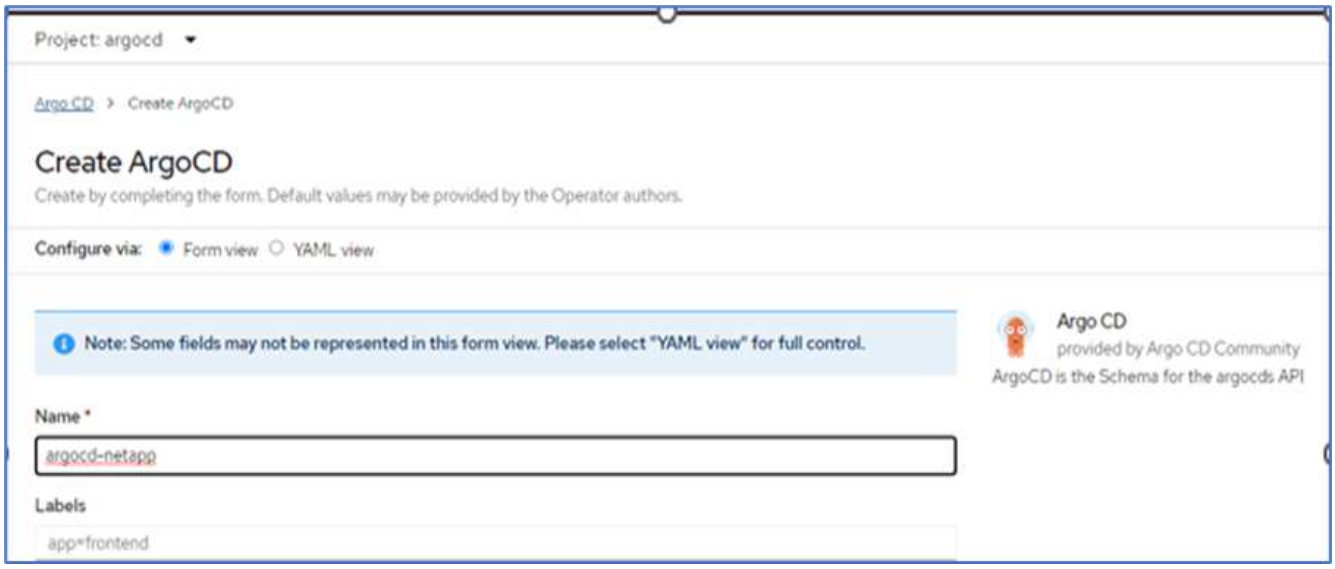
3. Instale el operador en el `argocd` espacio de nombres.



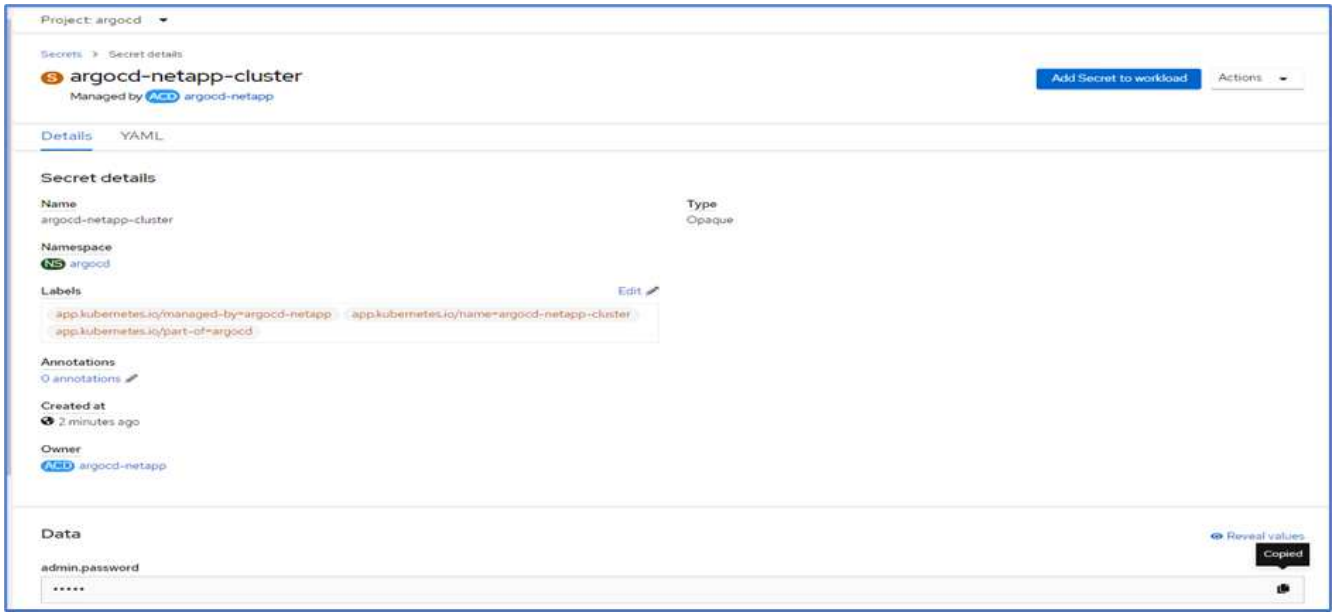
4. Vaya al operador y haga clic en Crear ArgoCD.



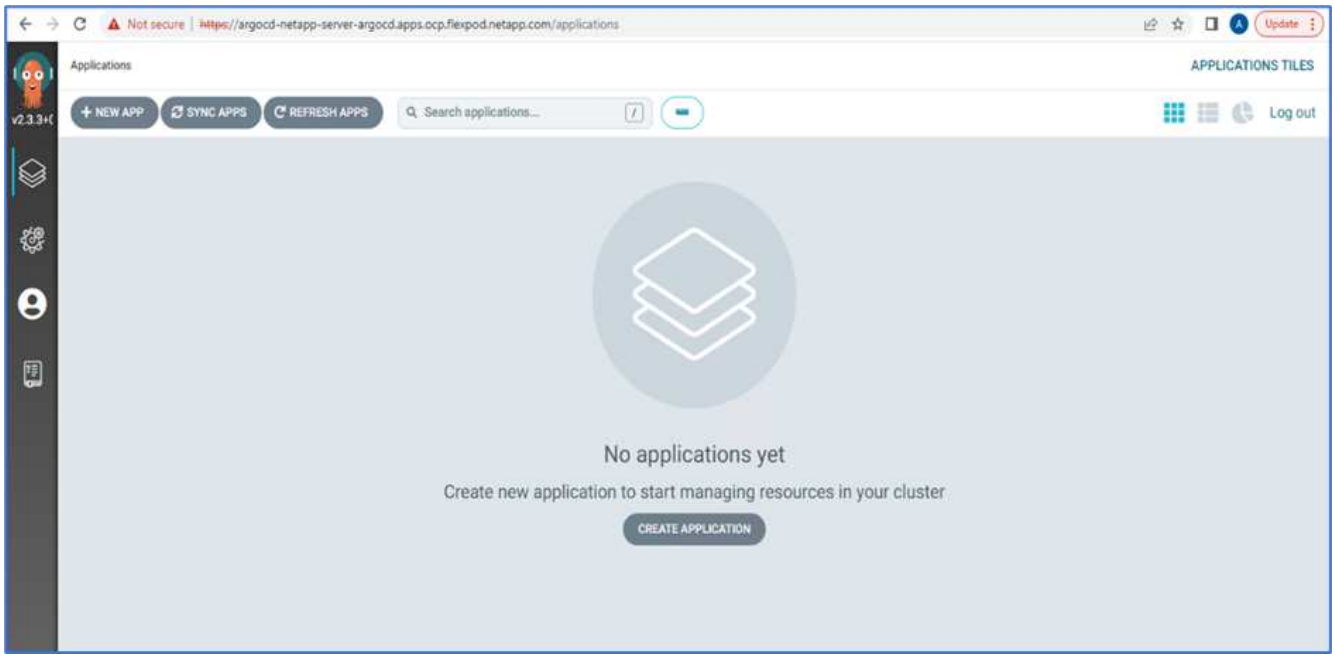
5. Para desplegar la instancia del CD Argo en `argocd` Project, proporcione un nombre y haga clic en Create.



6. Para iniciar sesión en el CD de Argo, el usuario predeterminado es admin y la contraseña está en un archivo secreto con el nombre `argocd-netapp-cluster`.



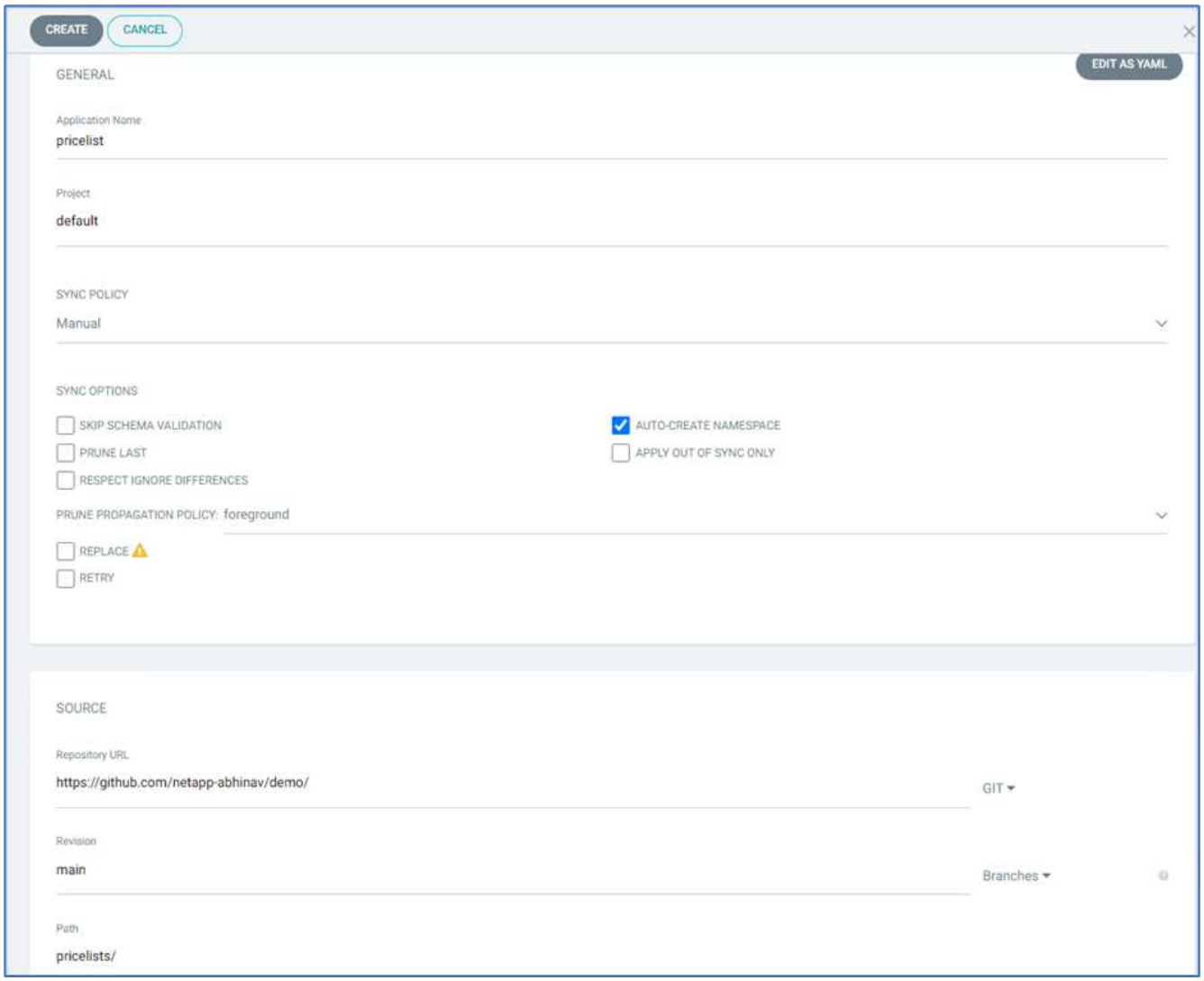
7. En el menú lateral, seleccione rutas > ubicación y haga clic en la dirección URL de `argocd` rutas. Introduzca el nombre de usuario y la contraseña.



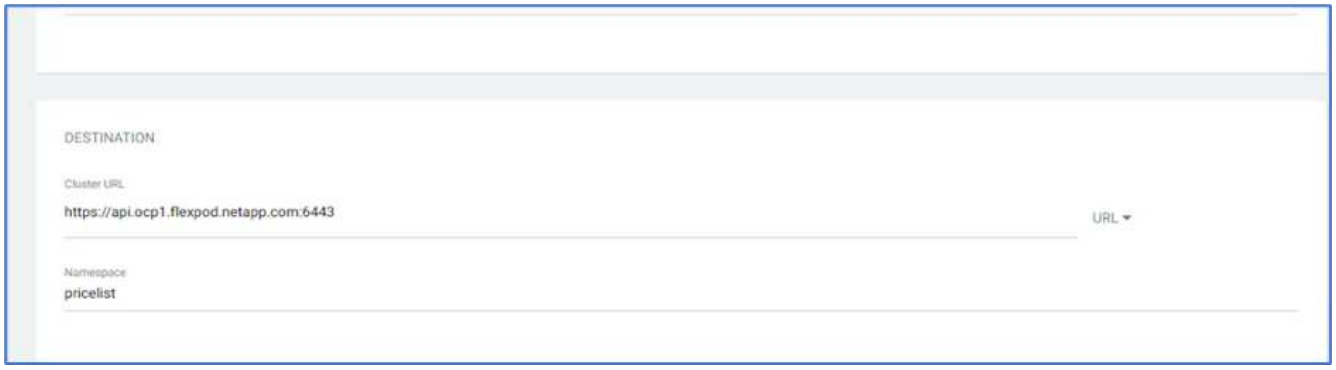
8. Agregue el clúster OpenShift en las instalaciones al CD de Argo a través de la CLI.

```
####Login to Argo CD####
abhinav3@abhinav-ansible$ argocd-linux-amd64 login argocd-netapp-server-
argocd.apps.ocp.flexpod.netapp.com --insecure
Username: admin
Password:
'admin:login' logged in successfully
Context'argocd-netapp-server-argocd.apps.ocp.flexpod.netapp.com' updated
####List the On-Premises OpenShift cluster####
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add
ERRO[0000] Choose a context name from:
CURRENT  NAME
CLUSTER              SERVER
*        default/api-ocp-flexpod-netapp-com:6443/abhinav3
api-ocp-flexpod-netapp-com:6443
https://api.ocp.flexpod.netapp.com:6443
         default/api-ocp1-flexpod-netapp-com:6443/abhinav3
api-ocp1-flexpod-netapp-com:6443
https://api.ocp1.flexpod.netapp.com:6443
####Add On-Premises OpenShift cluster###
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add default/api-
ocp1-flexpod-netapp-com:6443/abhinav3
WARNING: This will create a service account `argocd-manager` on the
cluster referenced by context `default/api-ocp1-flexpod-netapp-
com:6443/abhinav3` with full cluster level admin privileges. Do you want
to continue [y/N]? y
INFO[0002] ServiceAccount "argocd-manager" already exists in namespace
"kube-system"
INFO[0002] ClusterRole "argocd-manager-role" updated
INFO[0002] ClusterRoleBinding "argocd-manager-role-binding" updated
Cluster 'https://api.ocp1.flexpod.netapp.com:6443' added
```

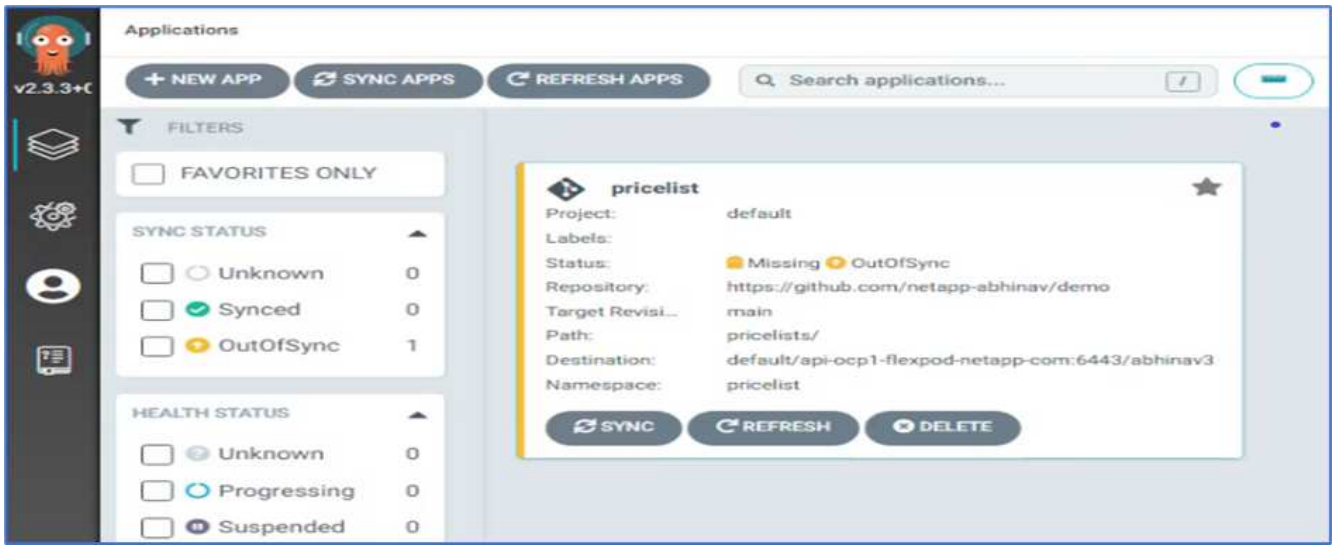
9. En la interfaz de usuario de ArgoCD, haga clic EN LA NUEVA APLICACIÓN e introduzca los detalles sobre el nombre de la aplicación y el repositorio de código.



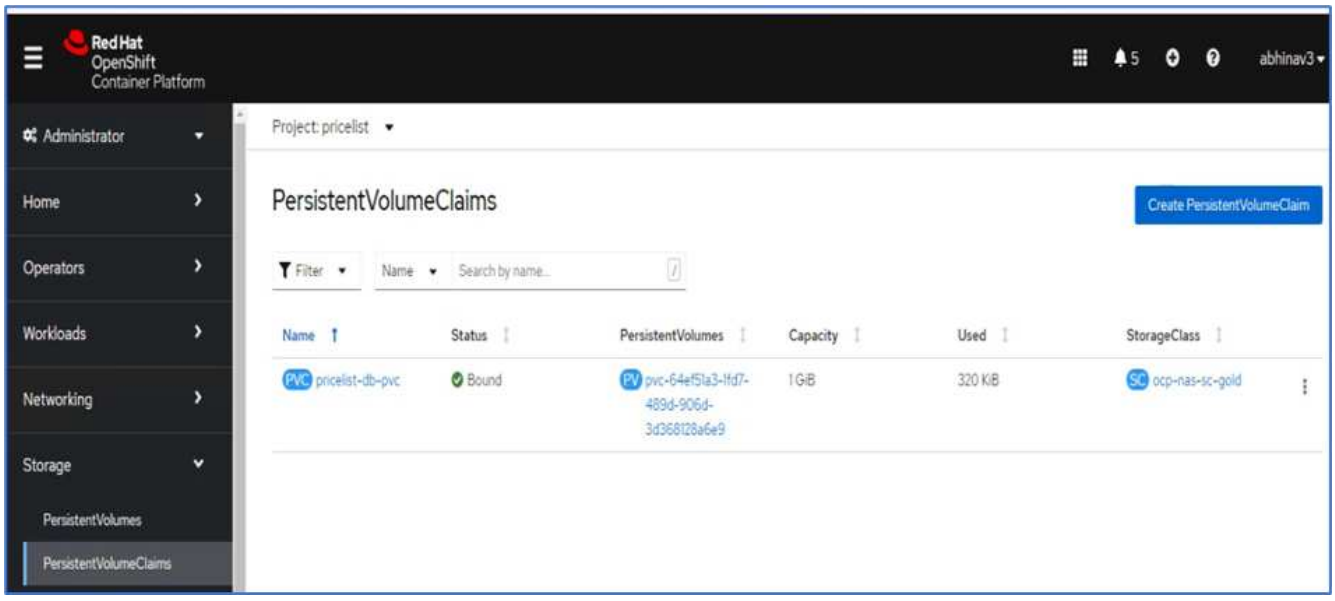
10. Introduzca el clúster OpenShift donde se va a implementar la aplicación junto con el espacio de nombres.



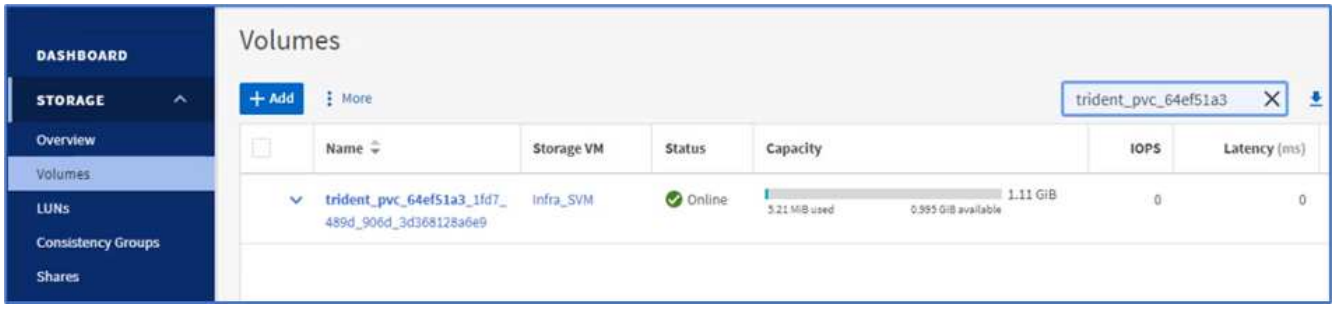
11. Para implementar la aplicación en el clúster OpenShift en las instalaciones, haga clic en SYNC.



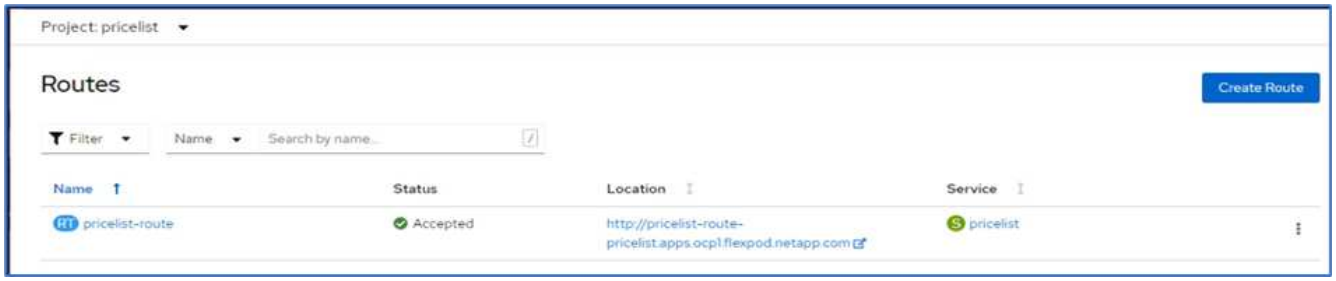
12. En la consola de OpenShift Container Platform, vaya a Lista de precios de proyecto y, en almacenamiento, compruebe el nombre y el tamaño del PVC.



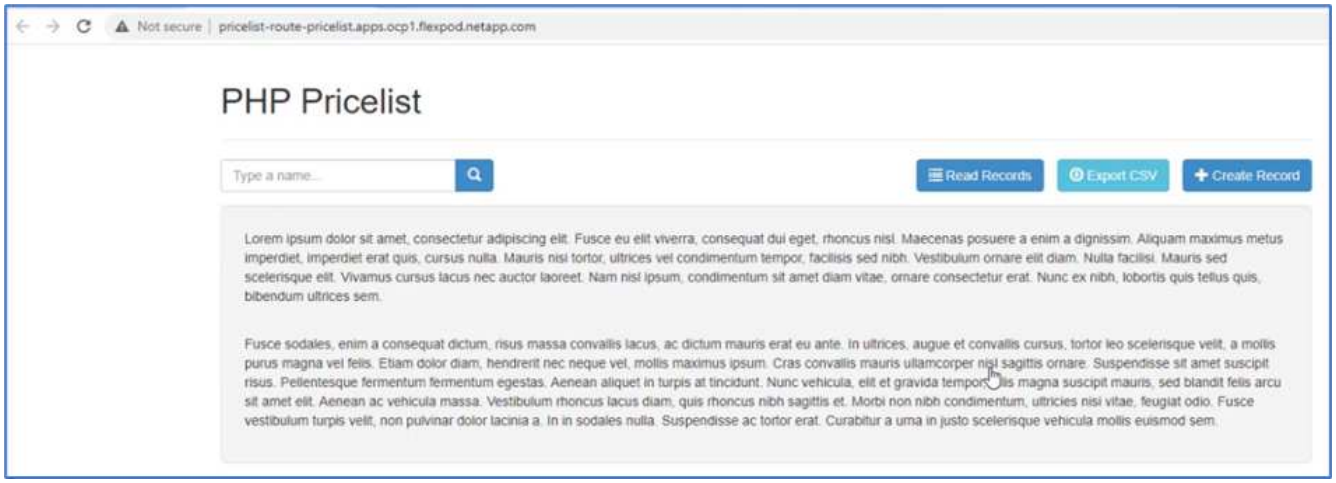
13. Inicie sesión en System Manager y verifique la RVP.



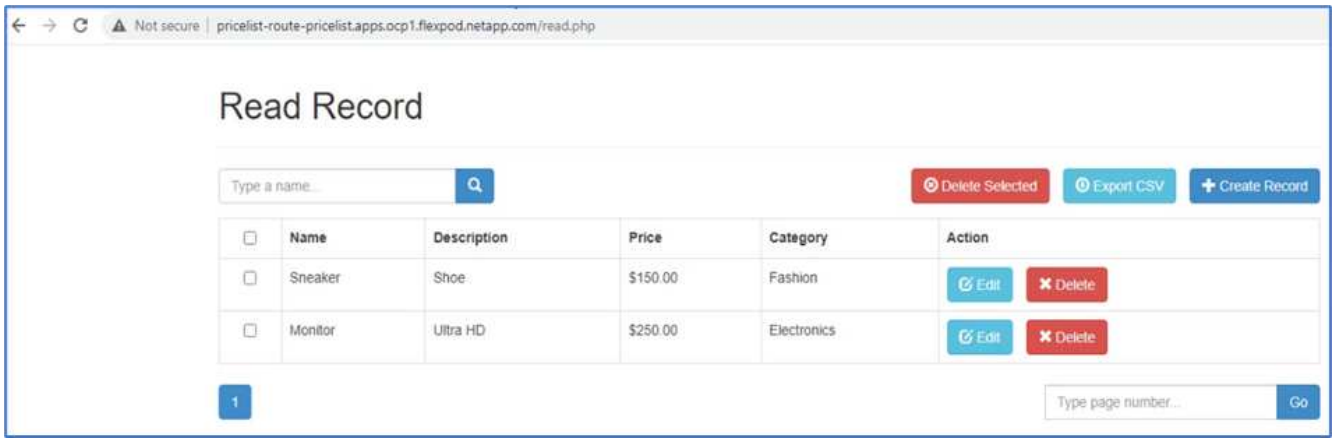
14. Una vez que se estén ejecutando los pods, seleccione Networking > Routes en el menú lateral y haga clic en la dirección URL en ubicación.



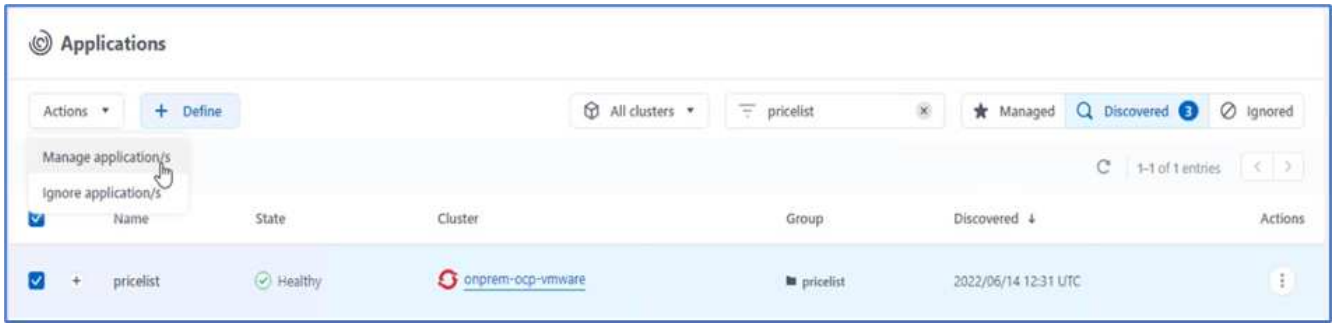
15. Se muestra la página de inicio de la aplicación Lista de precios.



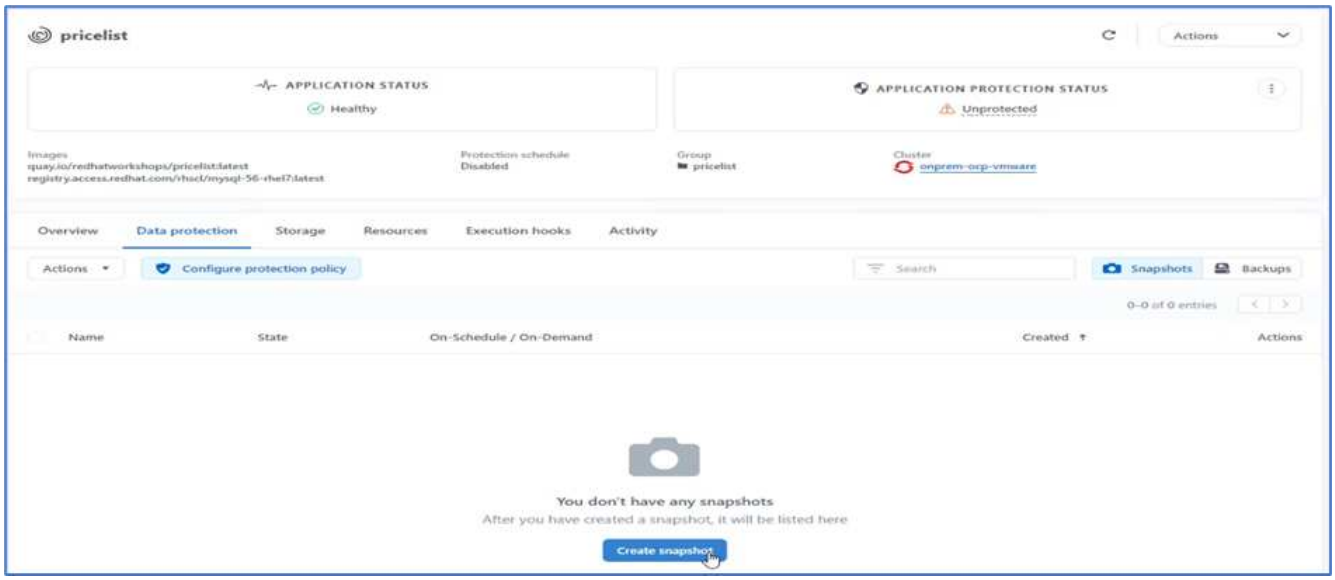
16. Cree algunos registros en la página Web.



17. La aplicación se descubre en Astra Control Center. Para gestionar la aplicación, vaya a aplicaciones > descubiertas, seleccione la aplicación Lista de precios y haga clic en Administrar aplicaciones en acciones.

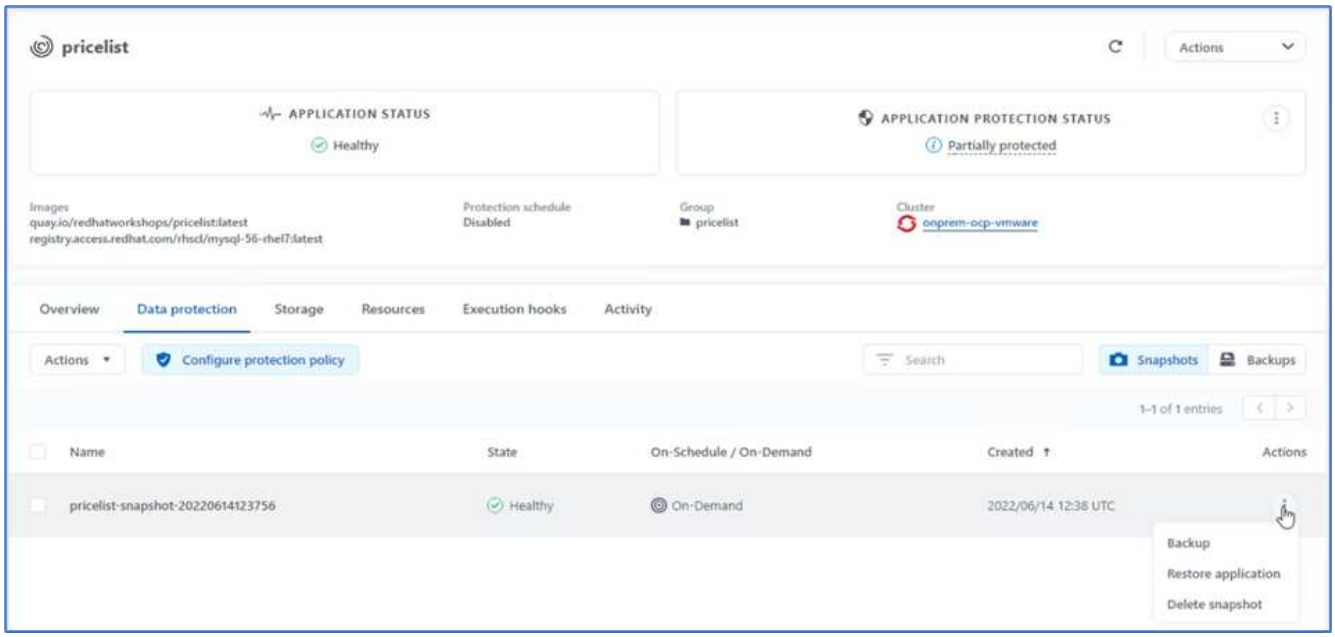


18. Haga clic en la aplicación Lista de precios y seleccione Protección de datos. En este momento, no deben existir copias Snapshot o backups. Haga clic en Create Snapshot para crear una snapshot bajo demanda.

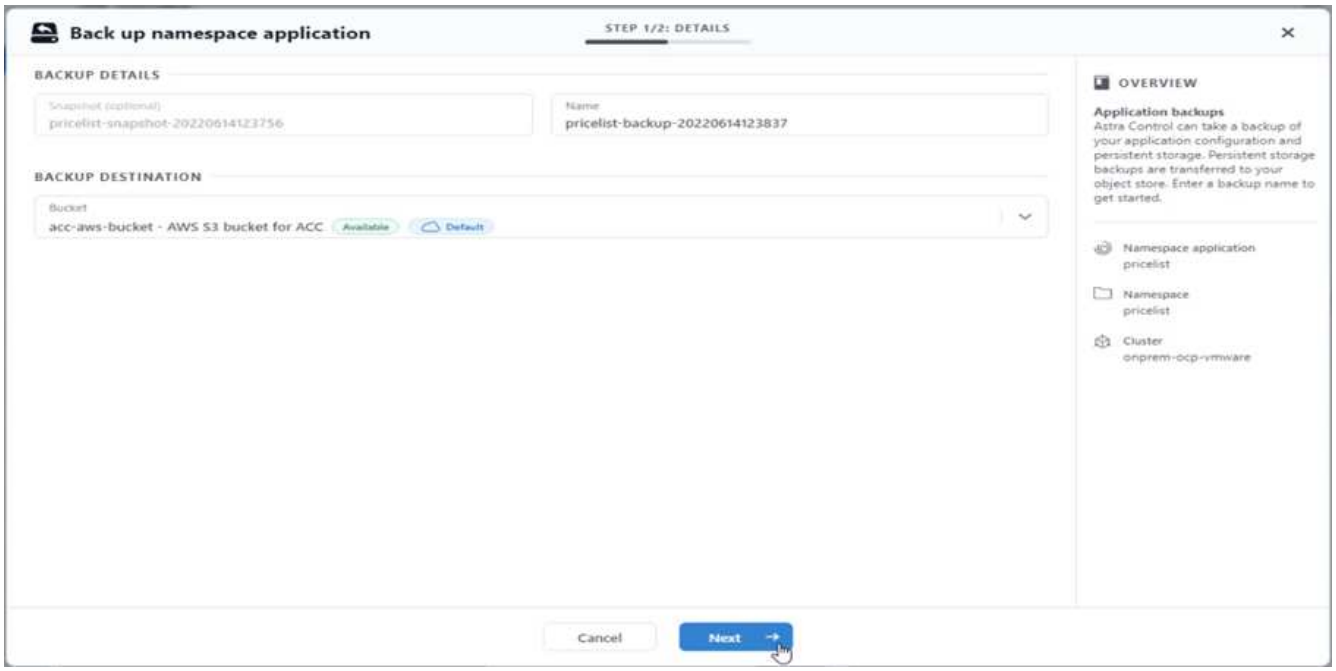


Astra Control Center de NetApp es compatible con copias Snapshot y backups bajo demanda y programadas.

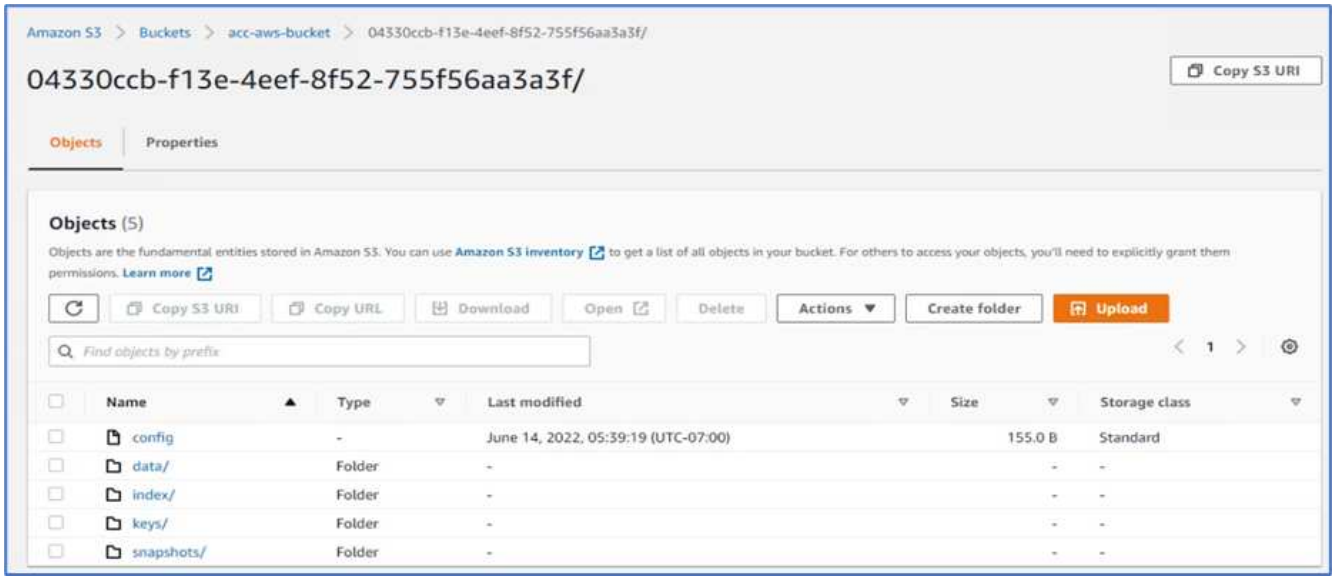
19. Una vez creada la copia de Snapshot y el estado es correcto, cree un backup remoto con esa copia de Snapshot. Este backup se almacena en el bloque de S3.



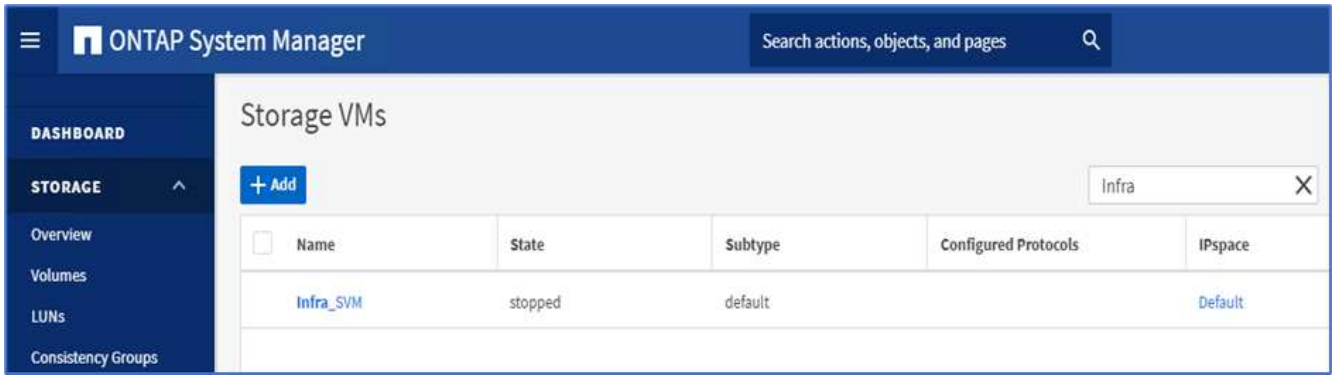
20. Seleccione el bloque de AWS S3 e inicie la operación de backup.



21. La operación de backup debe crear una carpeta con varios objetos en el bloque de AWS S3.



22. Una vez completado el backup remoto, simule un desastre en las instalaciones; para ello, detenga la máquina virtual de almacenamiento (SVM) que aloja el volumen de respaldo del VP.

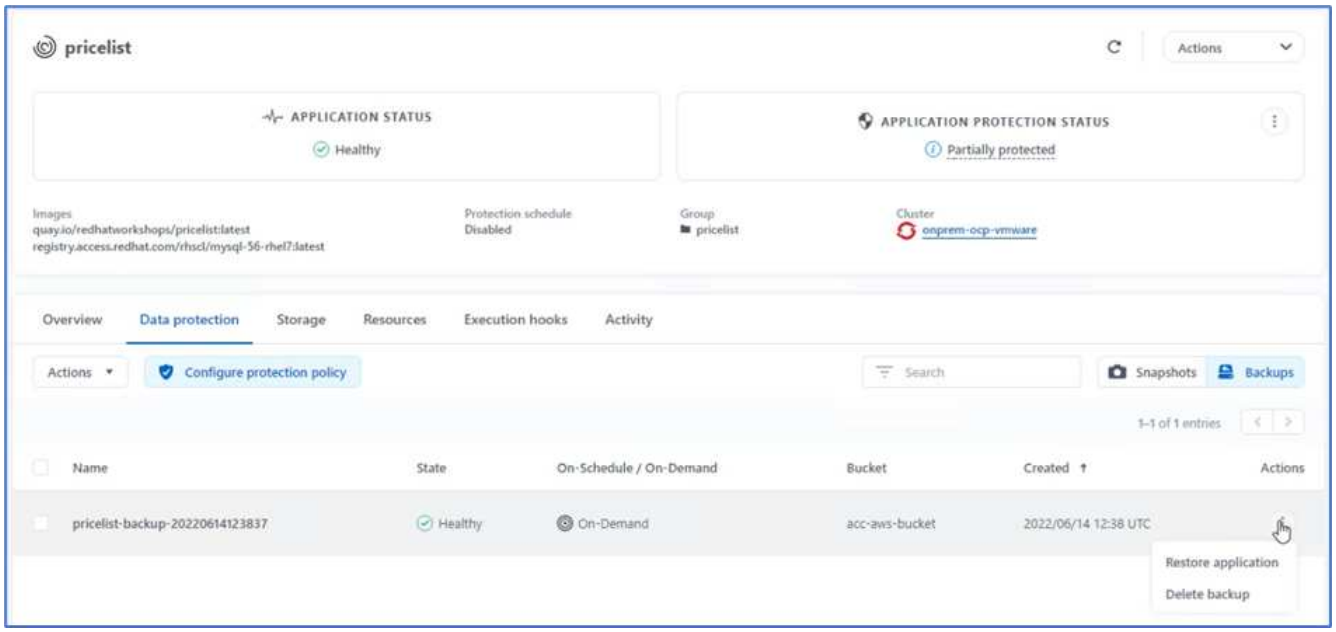


23. Actualice la página web para confirmar la interrupción. La página web no está disponible.

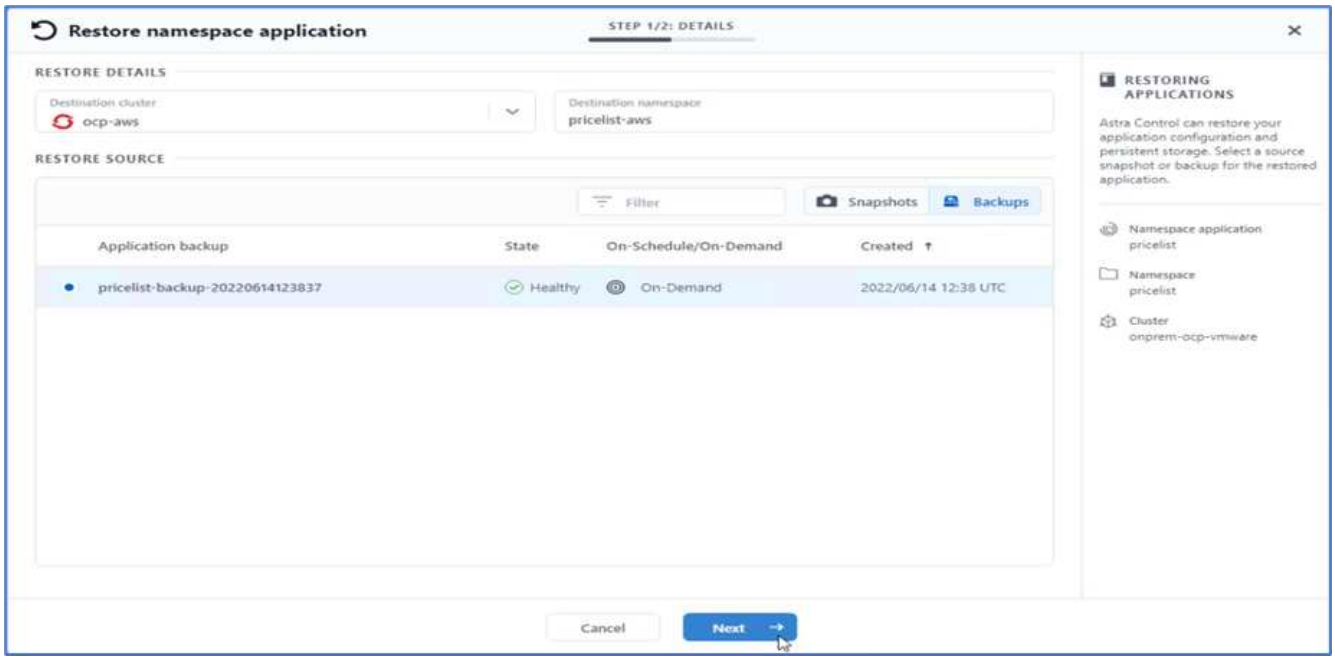


Como se espera, el sitio web está inactivo, por lo que recuperemos rápidamente la aplicación del backup remoto utilizando Astra en el clúster OpenShift que se ejecuta en AWS.

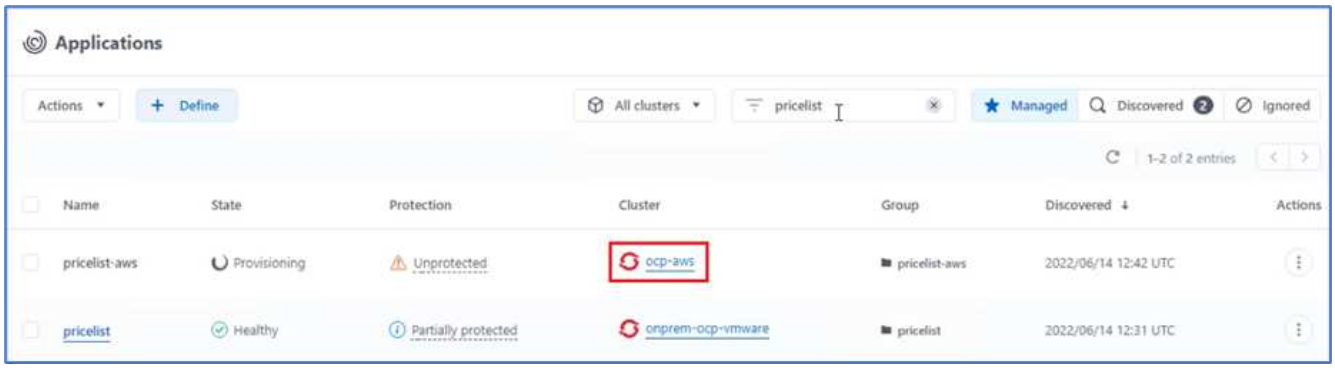
24. En Astra Control Center, haga clic en la aplicación Lista de precios y seleccione Protección de datos > copias de seguridad. Seleccione el backup y haga clic en Restore Application, en Action.



25. Seleccione `ocp-aws` como clúster de destino y asigne un nombre al espacio de nombres. Haga clic en la copia de seguridad bajo demanda, Siguiente y, a continuación, Restaurar.



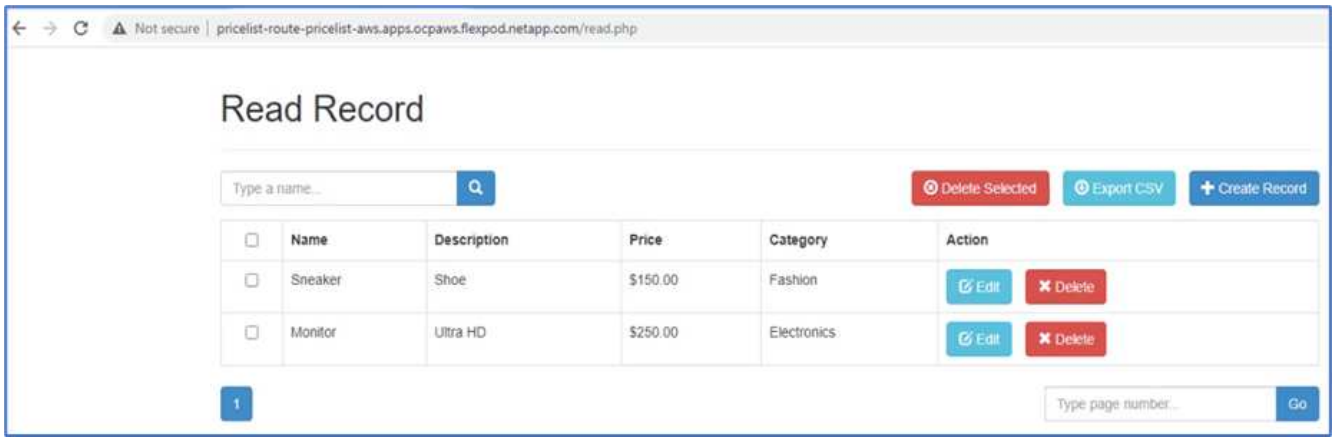
26. Una nueva aplicación con el nombre `pricelist-app` Se provisoned en el clúster OpenShift que se ejecuta en AWS.



27. Compruebe lo mismo en la consola web de OpenShift.



28. Después de todos los pods bajo la `pricelist-aws` Proyecto en ejecución, vaya a rutas y haga clic en la dirección URL para iniciar la página Web.



Este proceso valida que la aplicación de lista de precios se ha restaurado correctamente y que la integridad de los datos se ha mantenido en el clúster OpenShift sin problemas en AWS con la ayuda de Astra Control Center.

Protección de datos con copias Snapshot y movilidad de aplicaciones para DevTest

Este caso de uso consta de dos partes, como se describe en las siguientes secciones.

Parte 1

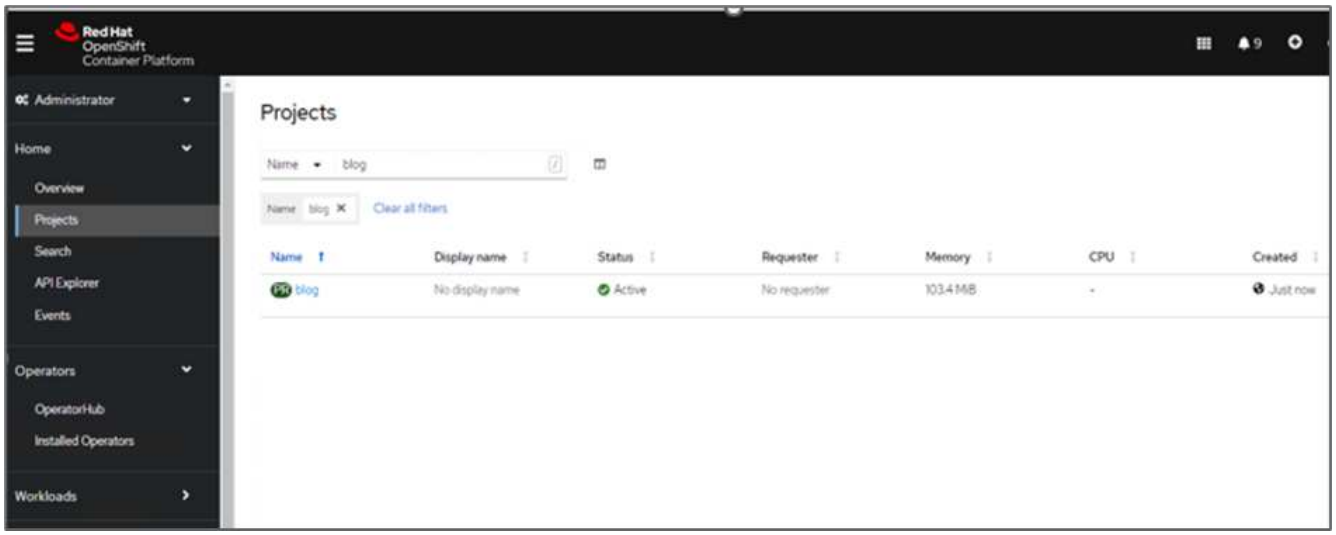
Con Astra Control Center, puede tomar instantáneas en cuenta las aplicaciones para la protección de datos local. Si elimina o corrompe accidentalmente sus datos, puede revertir sus aplicaciones y los datos asociados a un estado correcto conocido utilizando una instantánea registrada previamente.

En este escenario, un equipo de desarrollo y pruebas (DevTest) implementa una aplicación de ejemplo con estado (sitio de blog) que es una aplicación de blog Ghost, agrega algunos contenidos y actualiza la aplicación a la última versión disponible. La aplicación Ghost utiliza SQLite para la base de datos. Antes de actualizar la aplicación, se realiza una instantánea (bajo demanda) con Astra Control Center para la protección de datos. Los pasos detallados son los siguientes:

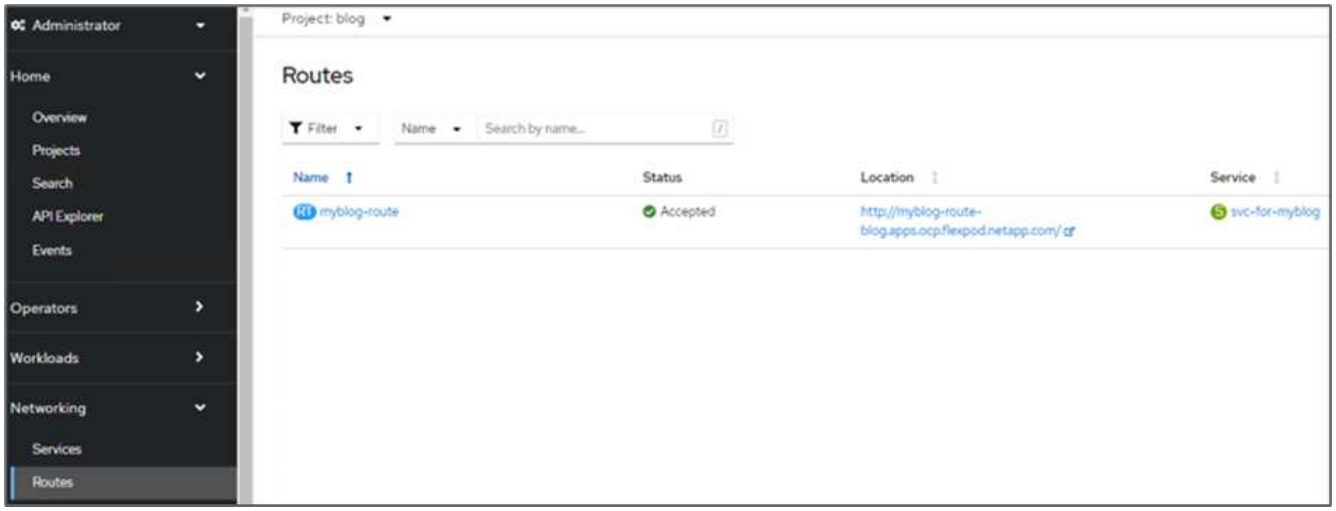
1. Despliegue la aplicación de blogs de ejemplo y sincronícela desde ArgoCD.



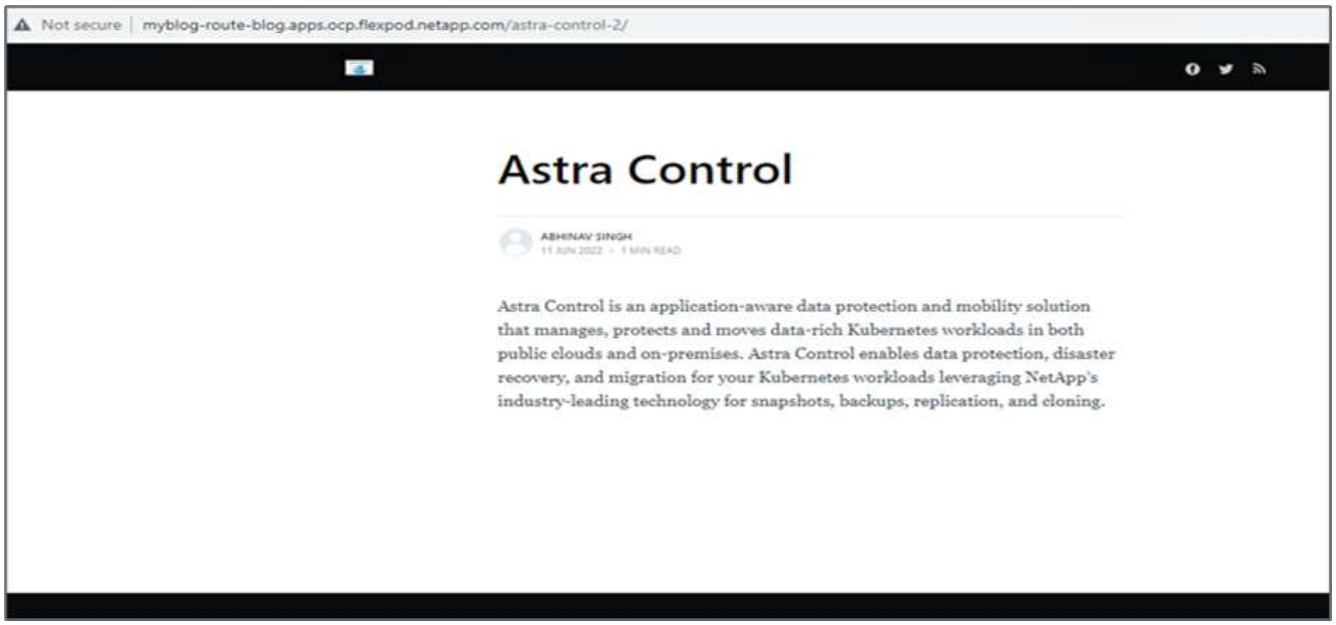
2. Inicie sesión en el primer clúster de OpenShift, vaya a Project y escriba Blog en la barra de búsqueda.



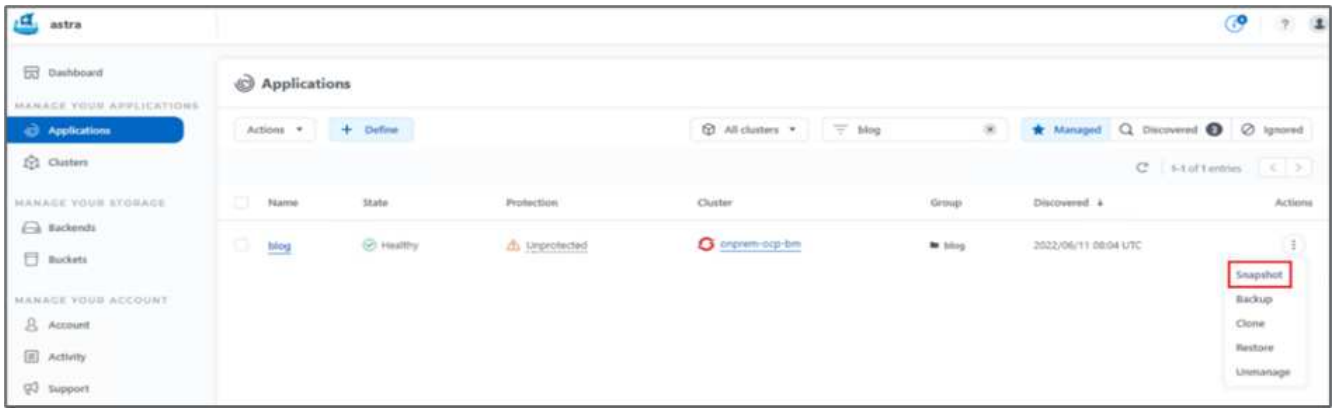
3. En el menú lateral, seleccione redes > rutas y haga clic en la URL.



4. Se muestra la página de inicio del blog. Agregue contenido al sitio del blog y lo publique.



5. Vaya a Astra Control Center. En primer lugar, gestione la aplicación desde la ficha descubierto y, a continuación, realice una copia snapshot.

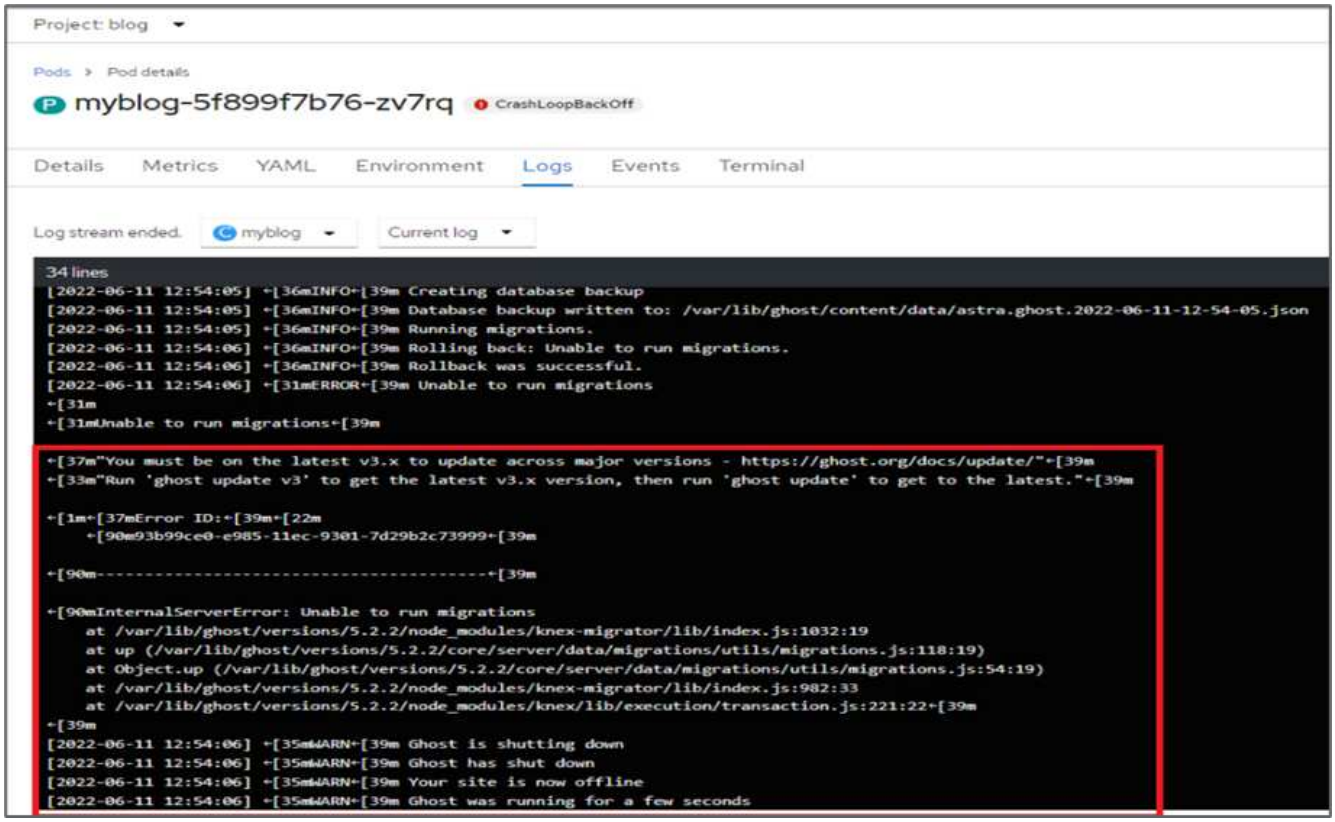


> También puede proteger sus aplicaciones creando instantáneas, copias de seguridad o ambas con una programación definida. Para obtener más información, consulte "Proteja las aplicaciones con snapshots y backups".

6. Una vez creada correctamente la instantánea bajo demanda, actualice la aplicación a la última versión. La versión actual de la imagen es `ghost: 3.6-alpine` y la versión de destino es `ghost:latest`. Para actualizar la aplicación, realice cambios directamente en el repositorio de Git y sincronícelo con el CD de Argo.



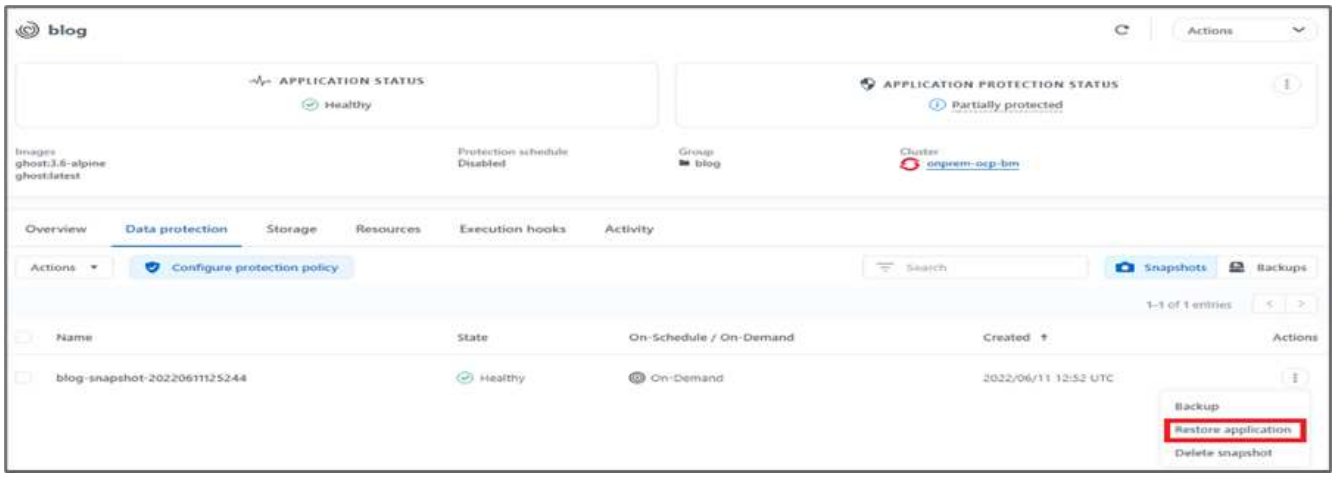
7. Puede ver que la actualización directa a la última versión no es compatible debido a que el sitio de blog está inactivo y a que toda la aplicación está dañada.



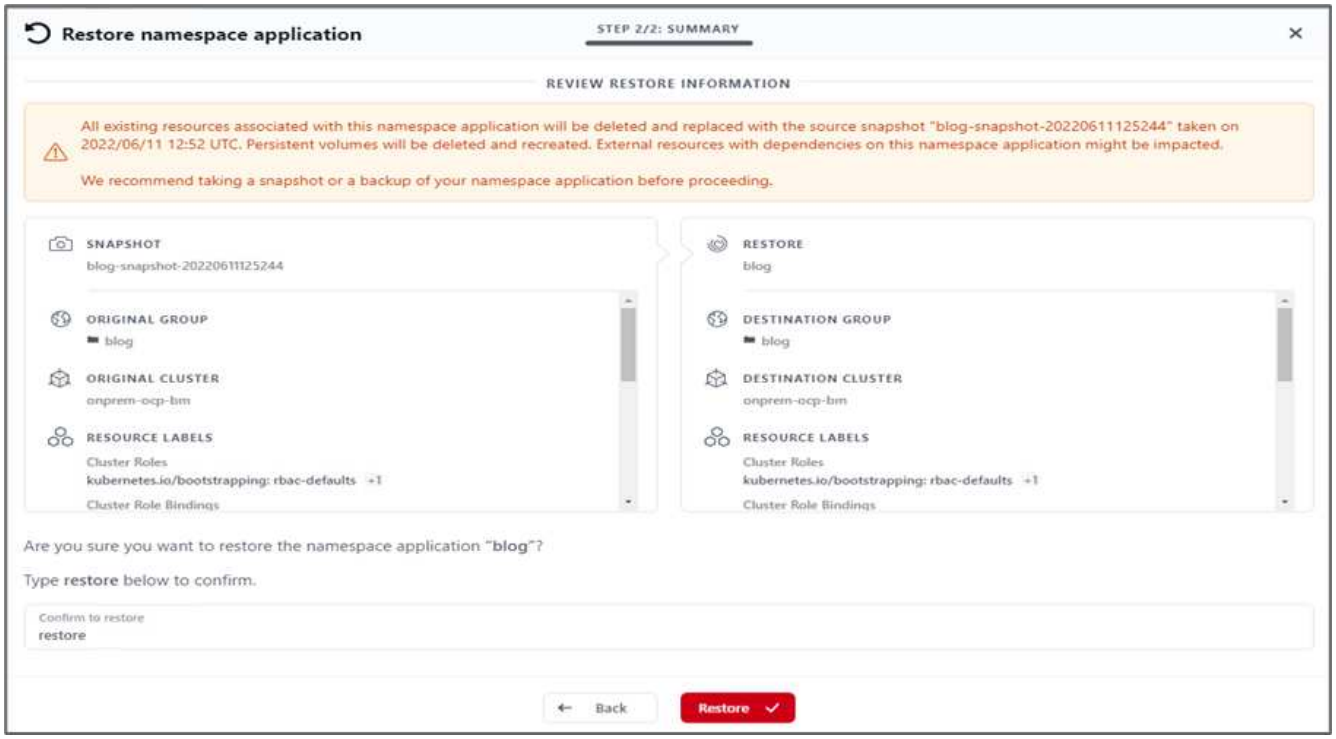
8. Para confirmar que el sitio del blog no está disponible, actualice la dirección URL.



9. Restaurar la aplicación desde la instantánea.



10. La aplicación se restaura en el mismo clúster de OpenShift.



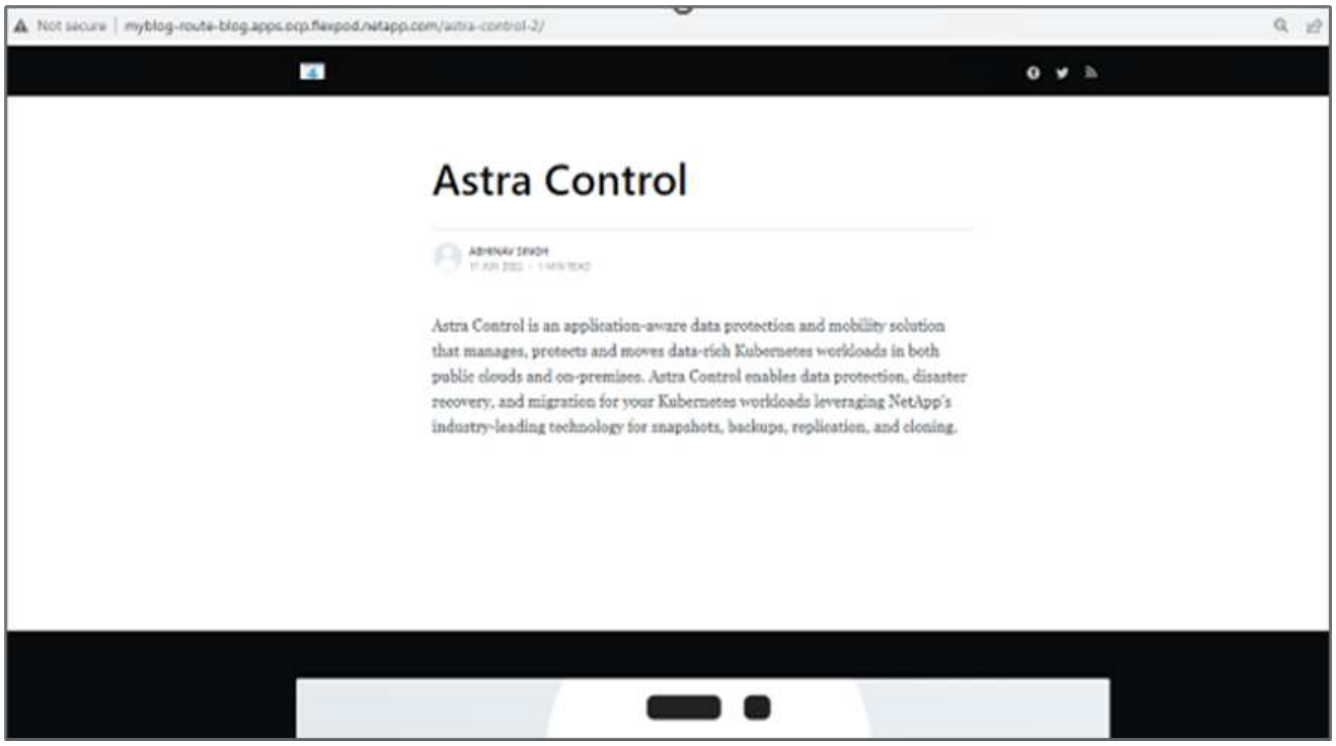
11. El proceso de restauración de aplicaciones se inicia inmediatamente.



12. En unos minutos, la aplicación se restaura correctamente a partir de la instantánea disponible.



13. Para ver si la página web está disponible, actualice la dirección URL.

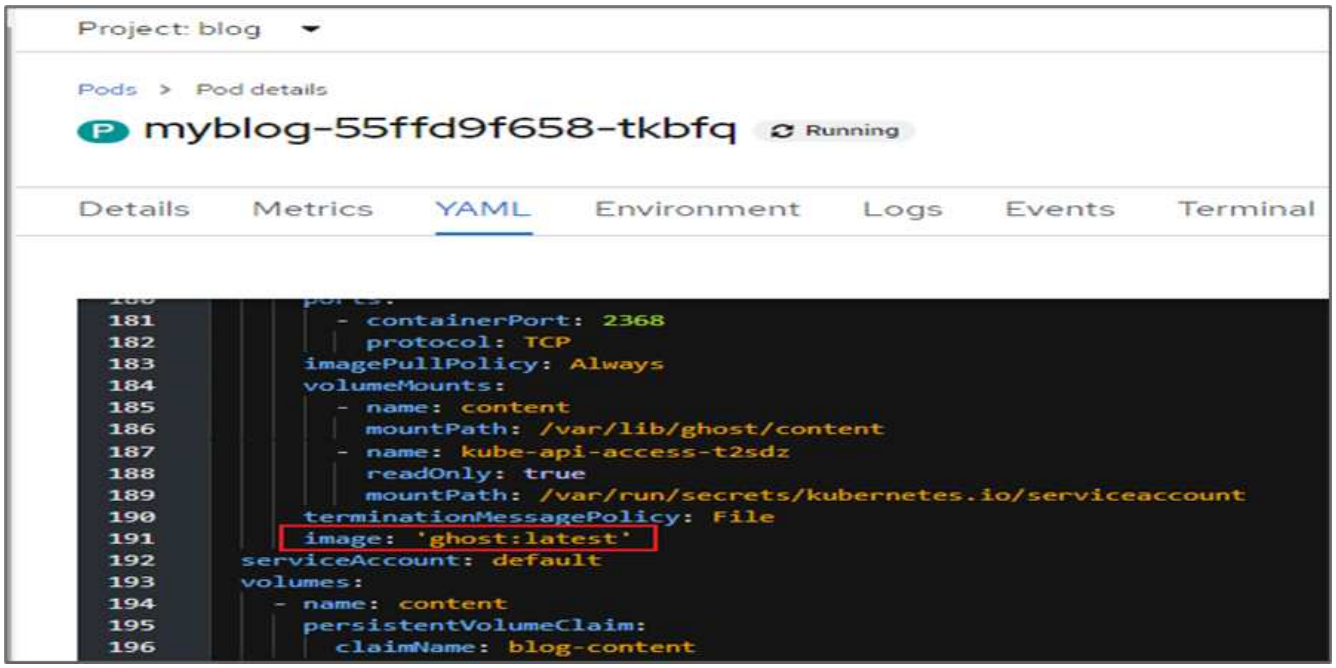


Con la ayuda de Astra Control Center, un equipo de DevTest puede recuperar con éxito una aplicación del sitio de blog y sus datos asociados mediante la instantánea.

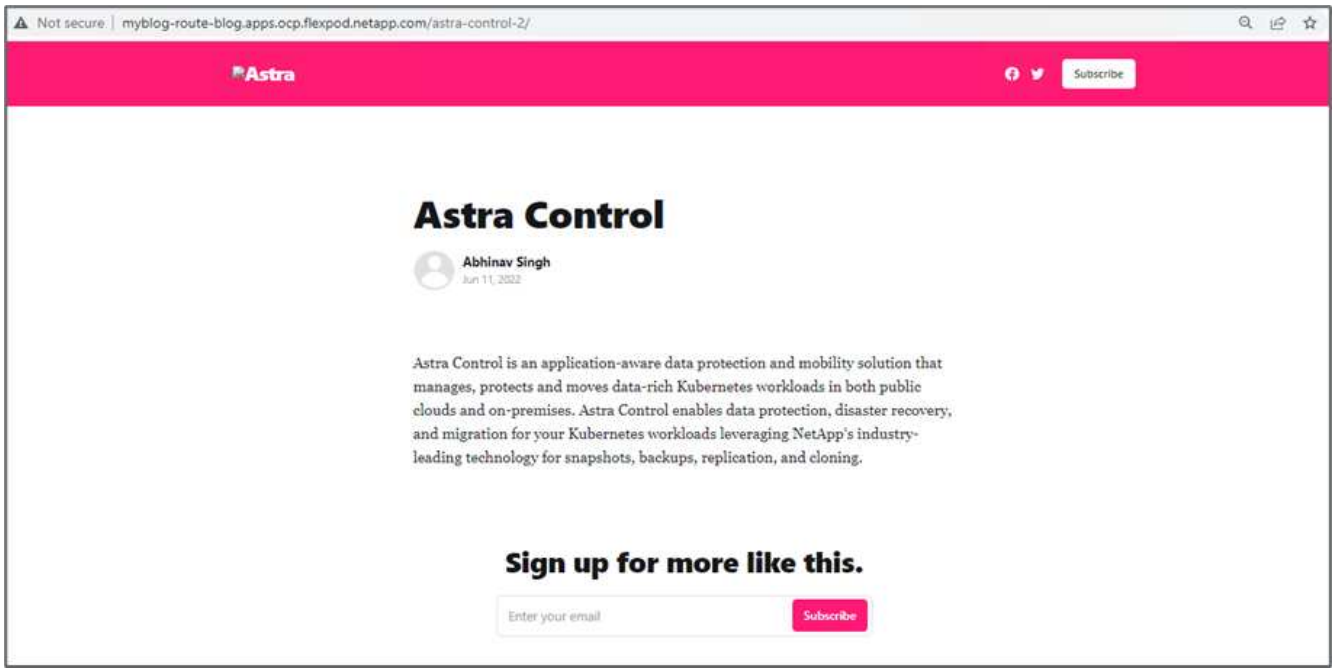
Parte 2

Con Astra Control Center, puede mover toda una aplicación junto con sus datos de un clúster de Kubernetes a otro, independientemente de dónde estén los clústeres (en las instalaciones o en el cloud).

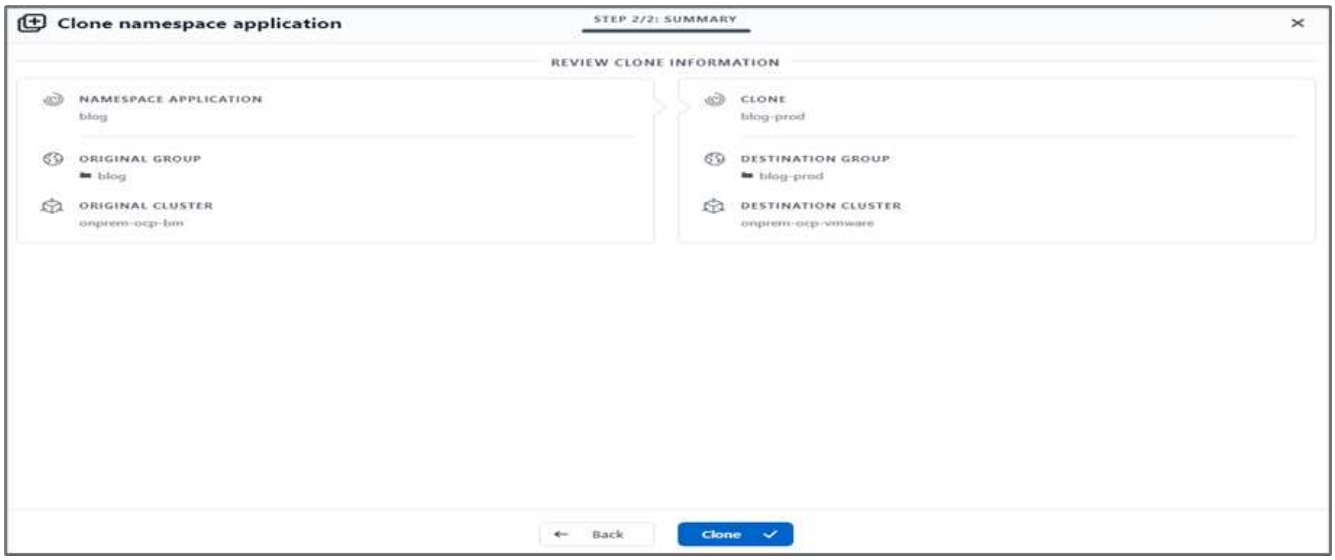
1. El equipo de DevTest actualiza inicialmente la aplicación a la versión compatible (`ghost-4.6-alpine`) antes de actualizar a la versión final (`ghost-latest`) para preparar la producción. A continuación, publican una actualización de la aplicación que se clona en el clúster de producción OpenShift que se ejecuta en un sistema FlexPod diferente.
2. En este momento, la aplicación se actualiza a la versión más reciente y está lista para clonarse en el clúster de producción.



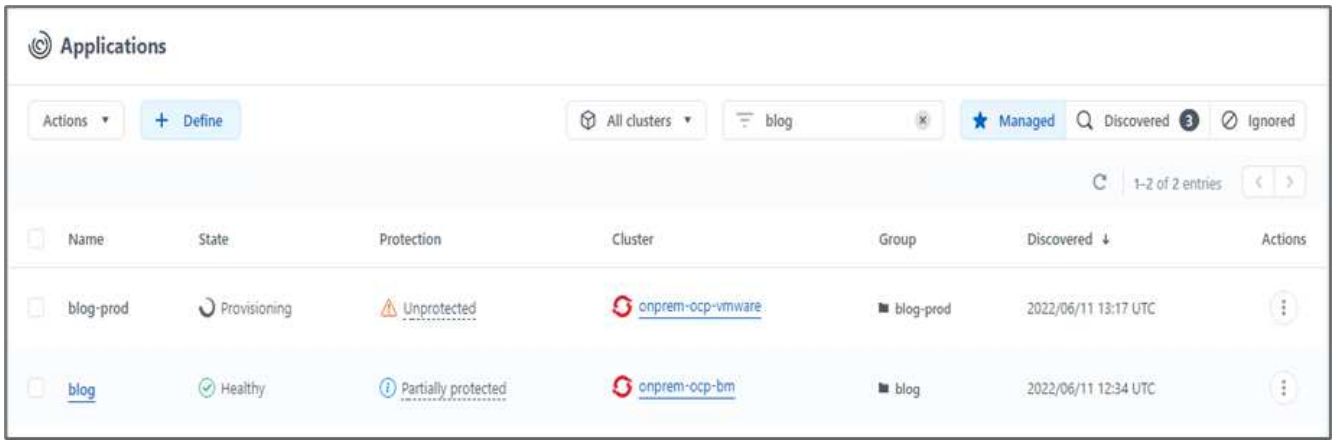
3. Para verificar el nuevo tema, actualice el sitio del blog.



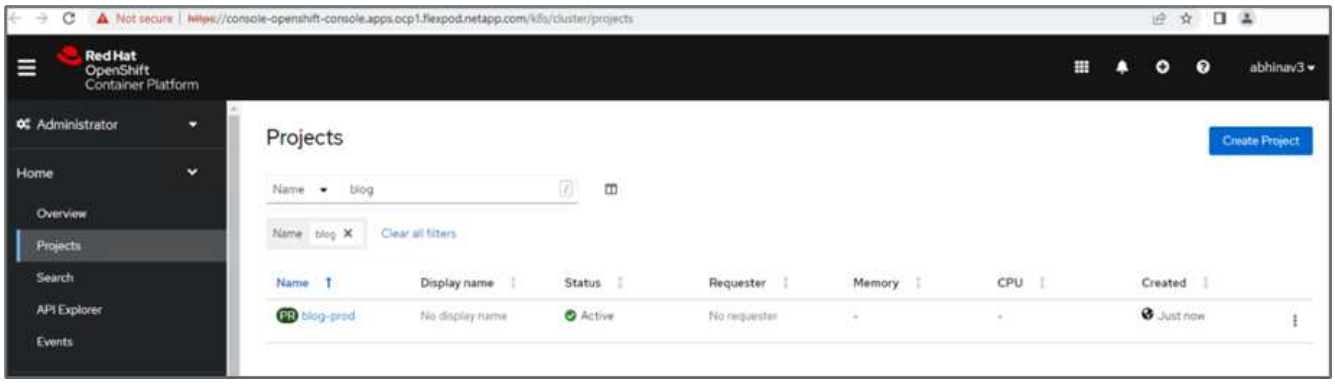
4. En Astra Control Center, clone la aplicación en el otro clúster de producción OpenShift que se ejecuta en VMware vSphere.



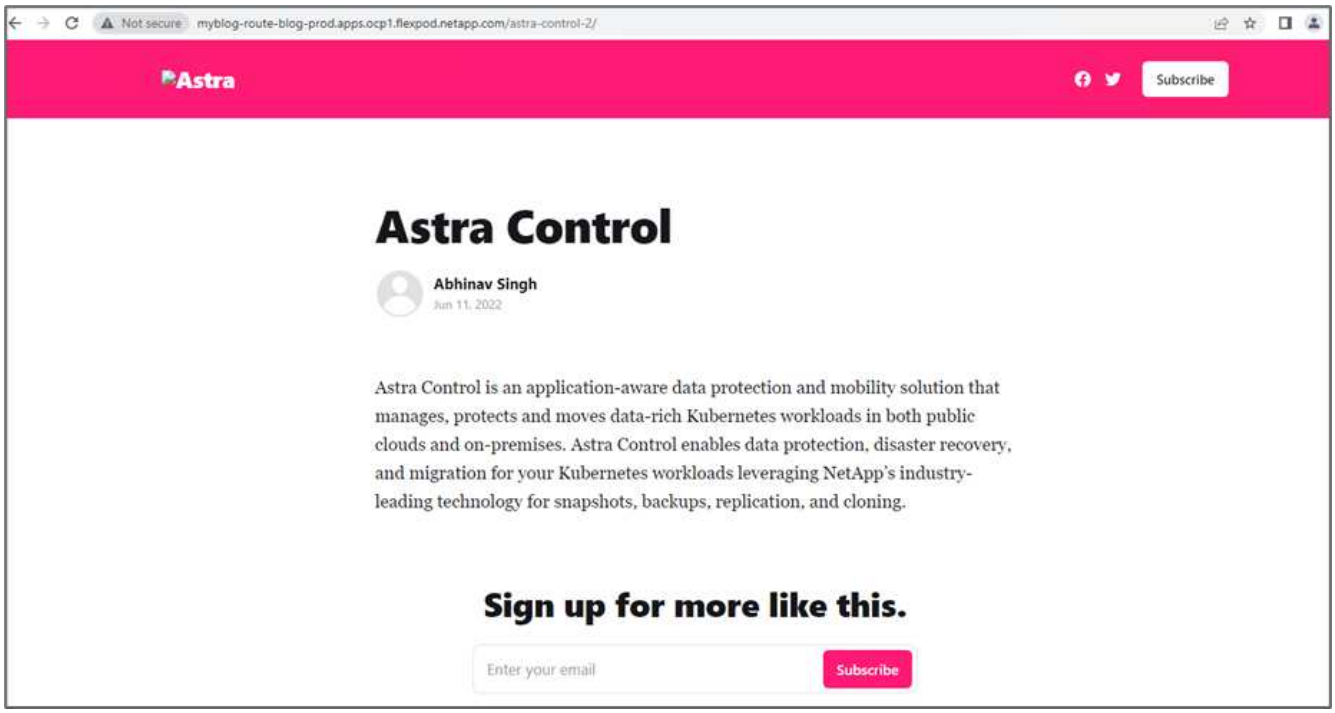
Ahora se aprovisiona un nuevo clon de aplicaciones en el clúster OpenShift de producción.



5. Inicie sesión en el clúster de Production OpenShift y busque el blog del proyecto.



6. En el menú lateral, seleccione redes > rutas y haga clic en la dirección URL en ubicación. Se muestra la misma página de inicio con el contenido.



Con esto concluye la validación de la solución Astra Control Center. Ahora puede clonar una aplicación completa y sus datos de un clúster de Kubernetes a otro, sin importar dónde esté el clúster de Kubernetes.

"Siguiente: Conclusión."

Conclusión

"Anterior: Recuperación de aplicaciones con backups remotos."

En esta solución, implementamos un plan de protección para aplicaciones en contenedores que se ejecutan en FlexPod y AWS mediante la cartera Astra de NetApp. NetApp Astra Control Center y Astra Trident, junto con Cloud Volumes ONTAP, Red Hat OpenShift y la infraestructura de FlexPod, formaron los componentes principales de esta solución.

Demostramos la protección de las aplicaciones capturando copias Snapshot y ejecutamos backups de copias completas para restaurar aplicaciones de distintos clústeres K8s ejecutados en entornos de cloud y en las instalaciones.

También demostramos el clonado de aplicaciones en clústeres K8s, permitiendo a los clientes migrar sus aplicaciones a los clústeres K8s de su elección en las ubicaciones deseadas.

FlexPod ha evolucionado constantemente para que sus clientes puedan modernizar sus aplicaciones y procesos de entrega del negocio. Con esta solución, los clientes de FlexPod pueden crear con confianza su plan BCDR para sus aplicaciones nativas del cloud con el cloud público como ubicación para un plan de recuperación ante desastres puntual o de tiempo completo, sin por ello dejar de mantener el coste de la solución en niveles bajos.

Astra Control le permite mover toda una aplicación junto con sus datos de un clúster de Kubernetes a otro, independientemente de dónde estén los clústeres. También puede ayudarle a acelerar la puesta en marcha, las operaciones y la protección de sus aplicaciones nativas del cloud.

Resolución de problemas

Para obtener instrucciones sobre la solución de problemas, consulte "documentación en línea".

Dónde encontrar información adicional

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"

- 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"

- Puesta en marcha de FlexPod con infraestructura como código para VMware con Ansible

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

- Puesta en marcha de FlexPod con infraestructura como código para configuración básica de Red Hat OpenShift con Ansible

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

- Herramienta de interoperabilidad de hardware y software Cisco UCS

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- Hoja de datos de Cisco Intersight

  "https://intersight.com/help/saas/home"

- Documentación de NetApp Astra

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- Centro de control de Astra de NetApp

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- Astra Trident de NetApp

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

- Cloud Manager de NetApp

  "https://docs.netapp.com/us-en/occm/concept_overview.html"

- Cloud Volumes ONTAP de NetApp

  "https://docs.netapp.com/us-en/occm/task_getting_started_aws.html"

- Red Hat OpenShift

  "https://www.openshift.com/"

- Herramienta de matriz de interoperabilidad de NetApp

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

Historial de versiones

Versión	Fecha	Historial de versiones del documento
Versión 1.0	Julio de 2022	Liberar para ACC 22.04.0.

Cloud Insights de NetApp para FlexPod

TR-4868: Cloud Insights de NetApp para FlexPod

Alan Cowles, NetApp

En colaboración con: 

La solución que se detalla en este informe técnico es la configuración del servicio Cloud Insights de NetApp para supervisar el sistema de almacenamiento AFF A800 de NetApp con ONTAP de NetApp, que se implementa como parte de una solución de centro de datos de FlexPod.

Valor para el cliente

La solución indicada en este documento proporciona valor a los clientes interesados en una solución de supervisión totalmente equipada para sus entornos de cloud híbrido, donde ONTAP se pone en marcha como sistema de almacenamiento principal. Esto incluye entornos FlexPod que usan los sistemas de almacenamiento AFF y FAS de NetApp.

Casos de uso

Esta solución se aplica a los siguientes casos de uso:

- Organizaciones que desean supervisar diversos recursos y utilización de su sistema de almacenamiento de ONTAP puesto en marcha como parte de una solución de FlexPod.
- Organizaciones que quieren solucionar problemas y reducir el tiempo de resolución de los incidentes que se producen en su solución de FlexPod con sus sistemas AFF o FAS.
- Organizaciones interesadas en proyecciones de optimización de costes, incluidos paneles personalizados para proporcionar información detallada sobre el desperdicio de recursos y en dónde se puede obtener un ahorro de costes en su entorno FlexPod, incluido ONTAP.

Público objetivo

El público objetivo de la solución incluye los siguientes grupos:

- Los ejecutivos DE TECNOLOGÍA y los que se preocupan por la optimización de costes y la continuidad del negocio.
- Arquitectos de soluciones interesados en el diseño y la gestión de centros de datos o clouds híbridos.
- Ingenieros de soporte técnico responsables de la solución de problemas y la resolución de incidentes.

Puede configurar Cloud Insights para proporcionar varios tipos de datos útiles que puede utilizar para ayudar en la planificación, la solución de problemas, el mantenimiento y la continuidad del negocio. Supervisando la solución FlexPod Datacenter con Cloud Insights y presentando los datos agregados en paneles personalizados que se pueden digerir fácilmente. no solo es posible predecir cuándo es necesario escalar los recursos en una implementación para cumplir con las exigencias, sino también para identificar aplicaciones o volúmenes de almacenamiento específicos que producen problemas en el sistema. Esto ayuda a garantizar que la infraestructura que se supervisa sea predecible y funcione según las expectativas, lo que permite a una organización cumplir acuerdos de nivel de servicios definidos y escalar la infraestructura según sea necesario, eliminando así los residuos y los costes adicionales.

Arquitectura

En esta sección, revisamos la arquitectura de una infraestructura convergente de centro de datos FlexPod, incluido un sistema AFF A800 de NetApp supervisado por Cloud Insights.

Tecnología de soluciones

Una solución de centro de datos de FlexPod consta de los siguientes componentes mínimos para proporcionar un entorno de infraestructura convergente compatible, validado, escalable y de alta disponibilidad.

- Dos nodos de almacenamiento ONTAP de NetApp (un par de alta disponibilidad)
- Dos switches de red de centro de datos de Cisco Nexus
- Dos switches de estructura Cisco MDS (opcional para puestas en marcha de FC)
- Dos interconexiones de estructura Cisco UCS
- Un chasis blade Cisco UCS con dos servidores blade Cisco UCS serie B

O.

- Dos servidores Cisco UCS C-Series en rack

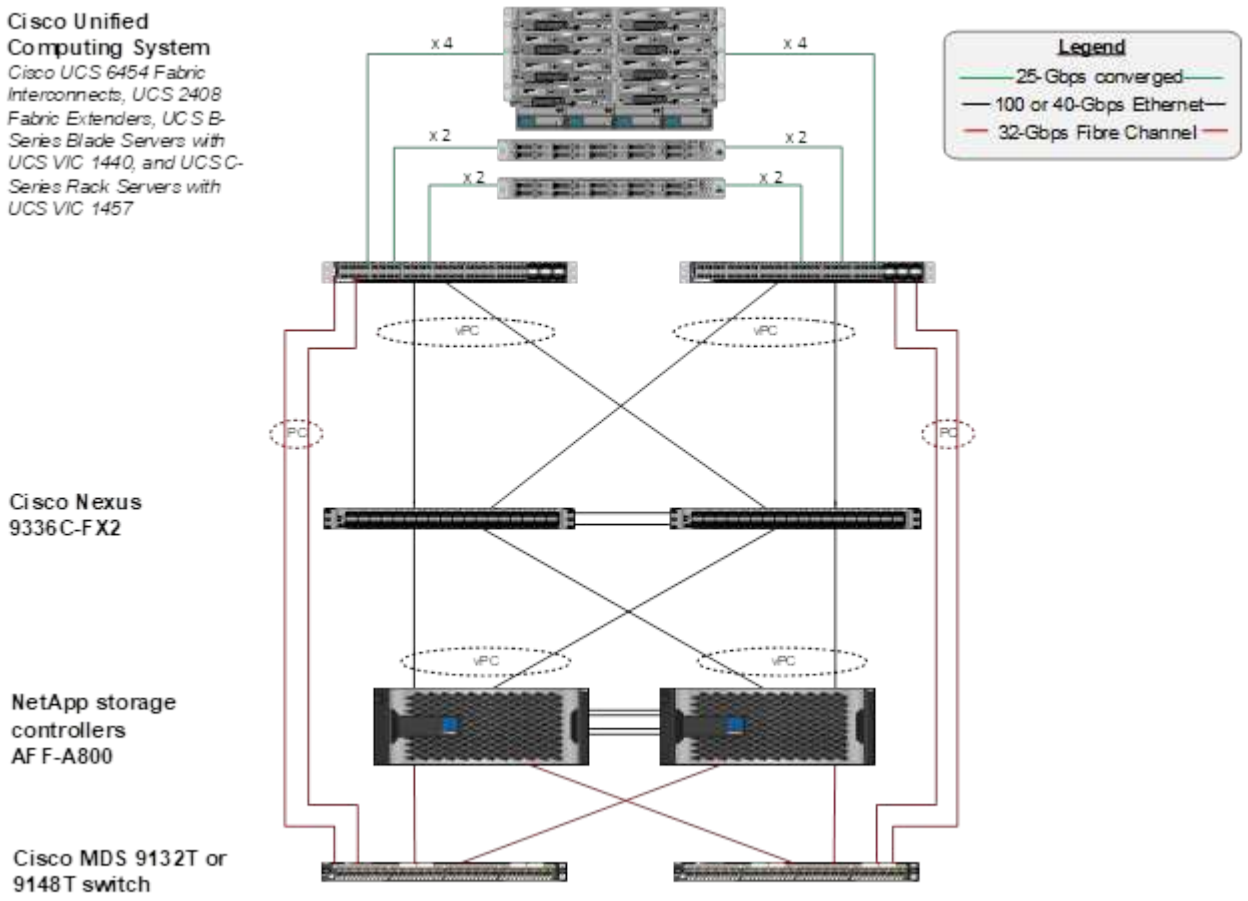
Para que Cloud Insights recopile datos, una organización debe poner en marcha una unidad de adquisición como máquina virtual o física dentro de su entorno del centro de datos FlexPod, o bien en una ubicación en la que pueda contactar con los componentes de los que recopila datos. Puede instalar el software de la unidad de adquisición en un sistema que ejecute varios sistemas operativos Windows o Linux admitidos. En la siguiente tabla se enumeran los componentes de la solución para este software.

De NetApp	Versión
Microsoft Windows	10
Servidor Microsoft Windows	2012, 2012 R2, 2016, 2019

De NetApp	Versión
Red Hat Enterprise Linux	7.2 – 7.6
CentOS	7.2 – 7.6
Oracle Enterprise Linux	7.5
Debian	9
Ubuntu	18.04 LTS

Diagrama arquitectónico

La siguiente figura muestra la arquitectura de la solución.



Requisitos de hardware

En la siguiente tabla se enumeran los componentes de hardware necesarios para implementar la solución. Los componentes de hardware que se usan en cualquier implementación particular de la solución pueden variar en función de las necesidades del cliente.

Hardware subyacente	Cantidad
Cisco Nexus 9336C-FX2	2
Interconexión de estructura Cisco UCS 6454	2
Chasis de servidor Blade UCS 5108 Cisco	1

Hardware subyacente	Cantidad
Extensores de estructura Cisco UCS 2408	2
Blades Cisco UCS B200 M5	2
AFF A800 de NetApp	2

Requisitos de software

En la siguiente tabla se enumeran los componentes de software necesarios para implementar la solución. Los componentes que se usan en cualquier implementación particular de la solución pueden variar en función de las necesidades del cliente.

De NetApp	Versión
Firmware de Cisco Nexus	9.3(5)
Versión de Cisco UCS	4.1(2a)
Versión de ONTAP de NetApp	9.7
Versión de Cloud Insights de NetApp	Septiembre 2020, básico
Red Hat Enterprise Linux	7.6
VSphere de VMware	6.7U3

Detalles de casos de uso

Esta solución se aplica a los siguientes casos de uso:

- El análisis del entorno con los datos proporcionados al asesor digital Active IQ de NetApp para la evaluación de los riesgos del sistema de almacenamiento y recomendaciones para la optimización del almacenamiento.
- Solución de problemas del sistema de almacenamiento de ONTAP puesto en marcha en una solución de centro de datos de FlexPod mediante la examen de las estadísticas del sistema en tiempo real.
- Generar consolas personalizadas para supervisar fácilmente puntos de interés específicos de los sistemas de almacenamiento de ONTAP que se ponen en marcha en una infraestructura convergente de FlexPod Datacenter.

Consideraciones de diseño

La solución FlexPod Datacenter es una infraestructura convergente diseñada por Cisco y NetApp para proporcionar un entorno de centro de datos dinámico, altamente disponible y escalable para la ejecución de cargas de trabajo empresariales. Los recursos de computación y de red de la solución los proporcionan los productos Cisco UCS y Nexus, y el sistema de almacenamiento de ONTAP proporciona los recursos de almacenamiento. El diseño de la solución se mejora regularmente cuando hay disponibles versiones de software y firmware actualizadas de hardware. Estos detalles, junto con las mejores prácticas para el diseño y la puesta en marcha de soluciones, se recogen en documentos de Cisco Validated Design (CVD) o de NetApp Verified Architecture (NVA) y se publican regularmente.

Ya está disponible el documento CVD más reciente que detalla el diseño de la solución para el centro de datos de FlexPod "aquí".

Ponga en marcha Cloud Insights para FlexPod

Para implementar la solución, debe completar las siguientes tareas:

1. Regístrese en el servicio Cloud Insights
2. Cree una máquina virtual de VMware (VM) para configurarla como una unidad de adquisición
3. Instale el host Red Hat Enterprise Linux (RHEL)
4. Cree una instancia de unidad de adquisición en el portal de Cloud Insights e instale el software
5. Añada el sistema de almacenamiento supervisado del centro de datos FlexPod a Cloud Insights.

Regístrese en el servicio Cloud Insights de NetApp

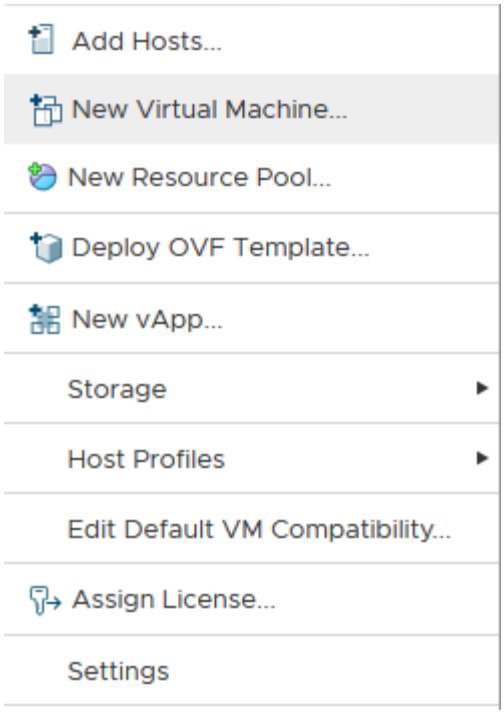
Para registrarse en el servicio Cloud Insights de NetApp, complete los siguientes pasos:

1. Vaya a. "https://cloud.netapp.com/cloud-insights"
2. Haga clic en el botón en el centro de la pantalla para iniciar la prueba gratuita de 14 días o en el enlace de la esquina superior derecha para registrarse o iniciar sesión con una cuenta existente de Cloud Central de NetApp.

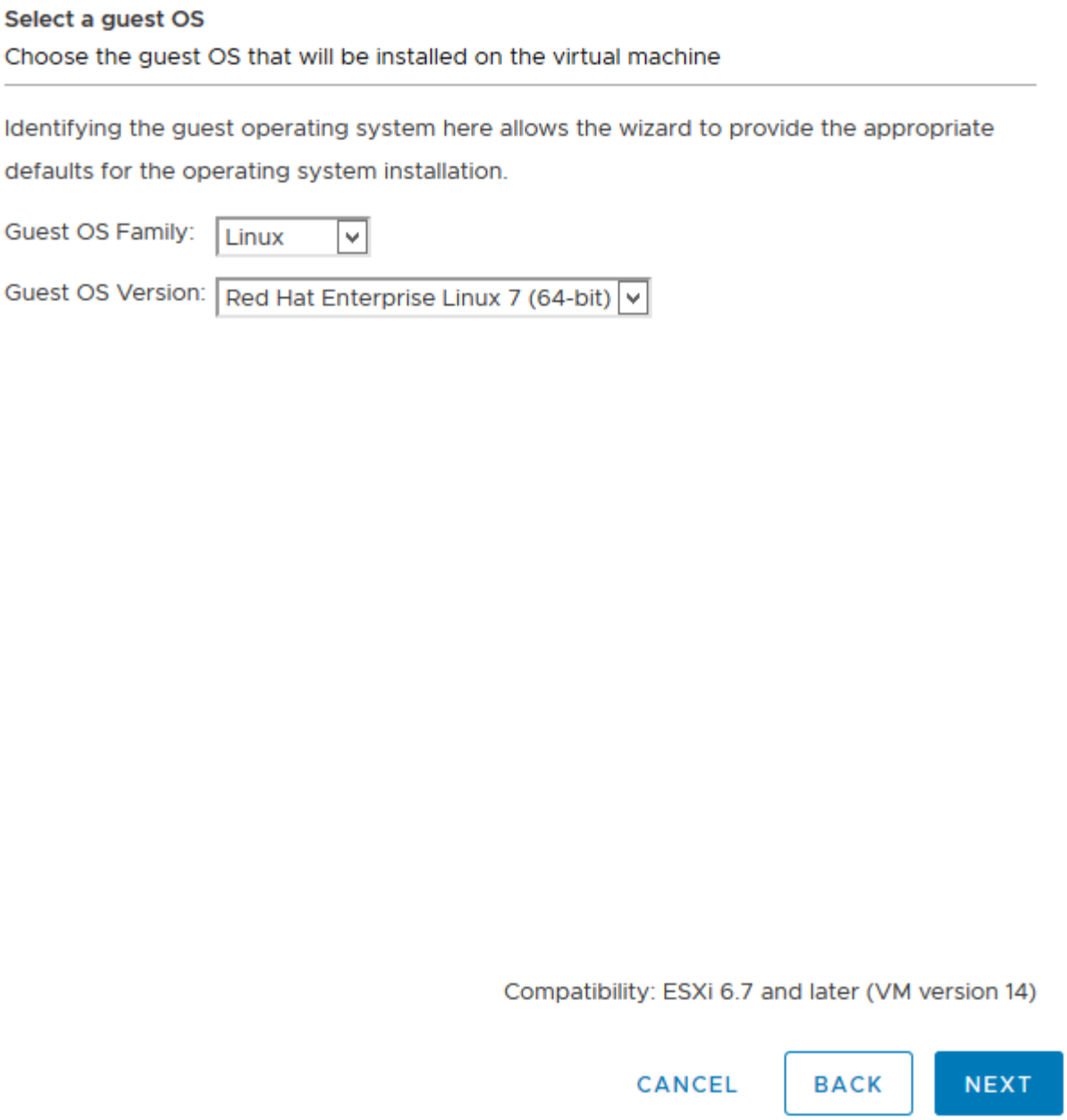
Cree una máquina virtual VMware para configurarla como una unidad de adquisición

Para crear un equipo virtual de VMware para configurarlo como unidad de adquisición, lleve a cabo los siguientes pasos:

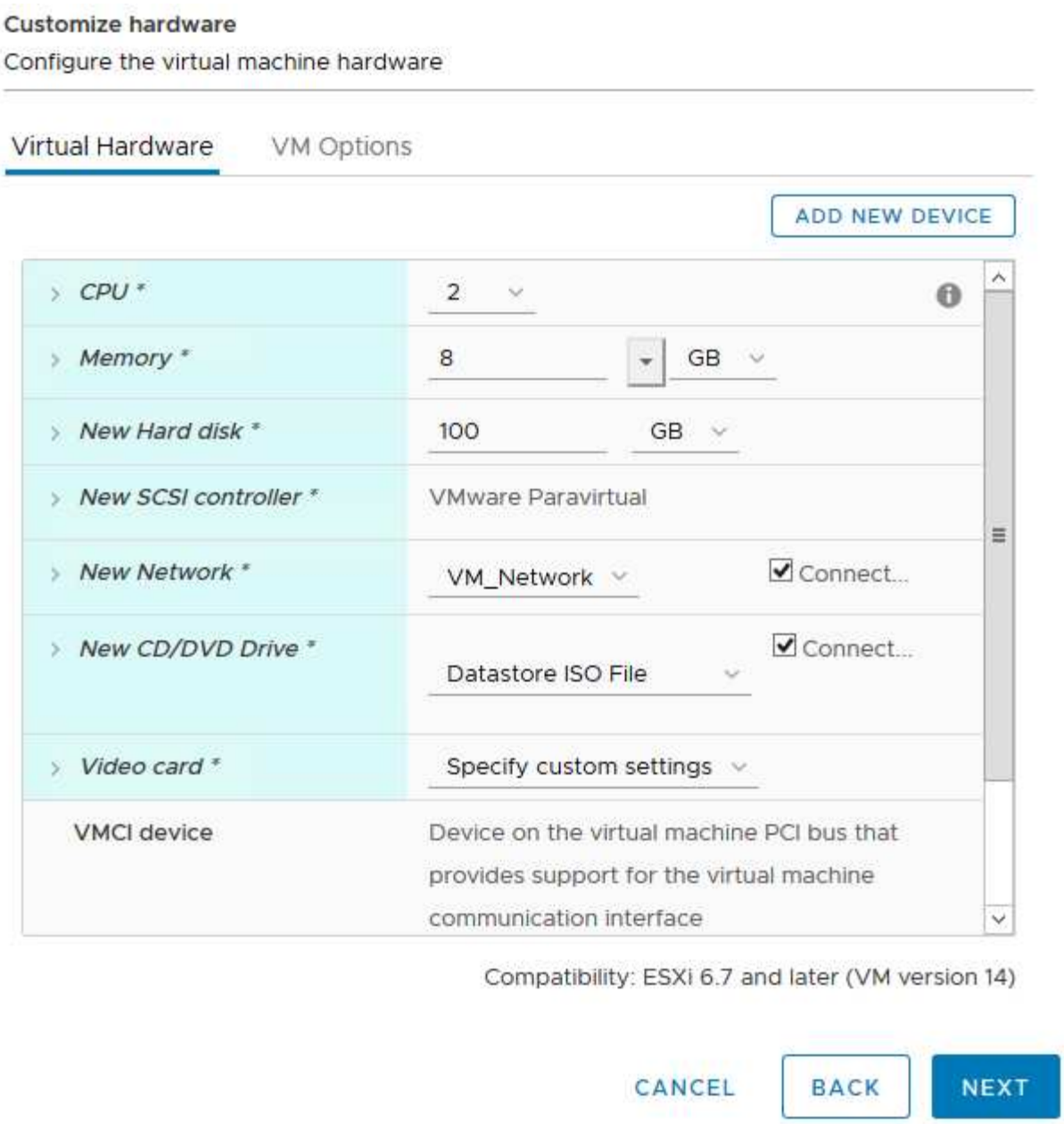
1. Inicie el explorador web e inicie sesión en VMware vSphere y seleccione el clúster que desea alojar una máquina virtual.
2. Haga clic con el botón derecho del ratón en ese clúster y seleccione Crear una máquina virtual en el menú.



3. En el asistente New Virtual Machine, haga clic en Next.
4. Especifique el nombre de la máquina virtual y seleccione el centro de datos en el que desea instalarla y haga clic en Siguiente.
5. En la siguiente página, seleccione el clúster, los nodos o el grupo de recursos en el que desea instalar la máquina virtual y, a continuación, haga clic en Next.
6. Seleccione el almacén de datos compartido que aloja las máquinas virtuales y haga clic en Next.
7. Confirme que el modo de compatibilidad de la máquina virtual se ha establecido en `ESXi 6.7 or later` Y haga clic en Siguiente.
8. Seleccione Guest OS Family Linux, Guest OS Version: Red Hat Enterprise Linux 7 (64 bits).



9. En la siguiente página se puede personalizar los recursos de hardware en el equipo virtual. La Unidad de adquisición de Cloud Insights requiere los siguientes recursos. Una vez seleccionados los recursos, haga clic en Siguiente:
   a. Dos CPU
   b. 8 GB de RAM
   c. 100 GB de espacio en disco duro
   d. Una red que puede acceder a los recursos del centro de datos FlexPod y del servidor Cloud Insights a través de una conexión SSL en el puerto 443.
   e. Imagen ISO de la distribución de Linux elegida (Red Hat Enterprise Linux) desde la que arrancar.

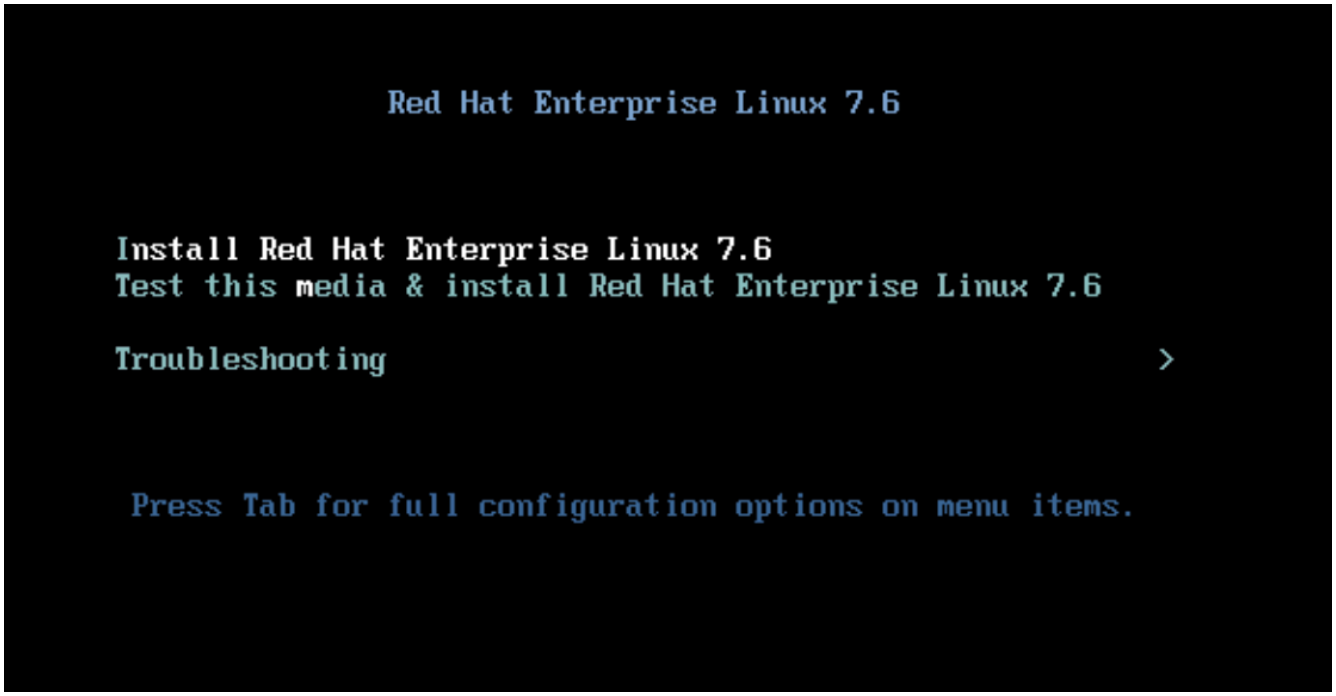


10. Para crear la máquina virtual, en la página Ready to Complete, revise la configuración y haga clic en Finish.

Instale Red Hat Enterprise Linux

Para instalar Red Hat Enterprise Linux, siga estos pasos:

1. Encienda la máquina virtual, haga clic en la ventana para iniciar la consola virtual y, a continuación, seleccione la opción instalar Red Hat Enterprise Linux 7.6.



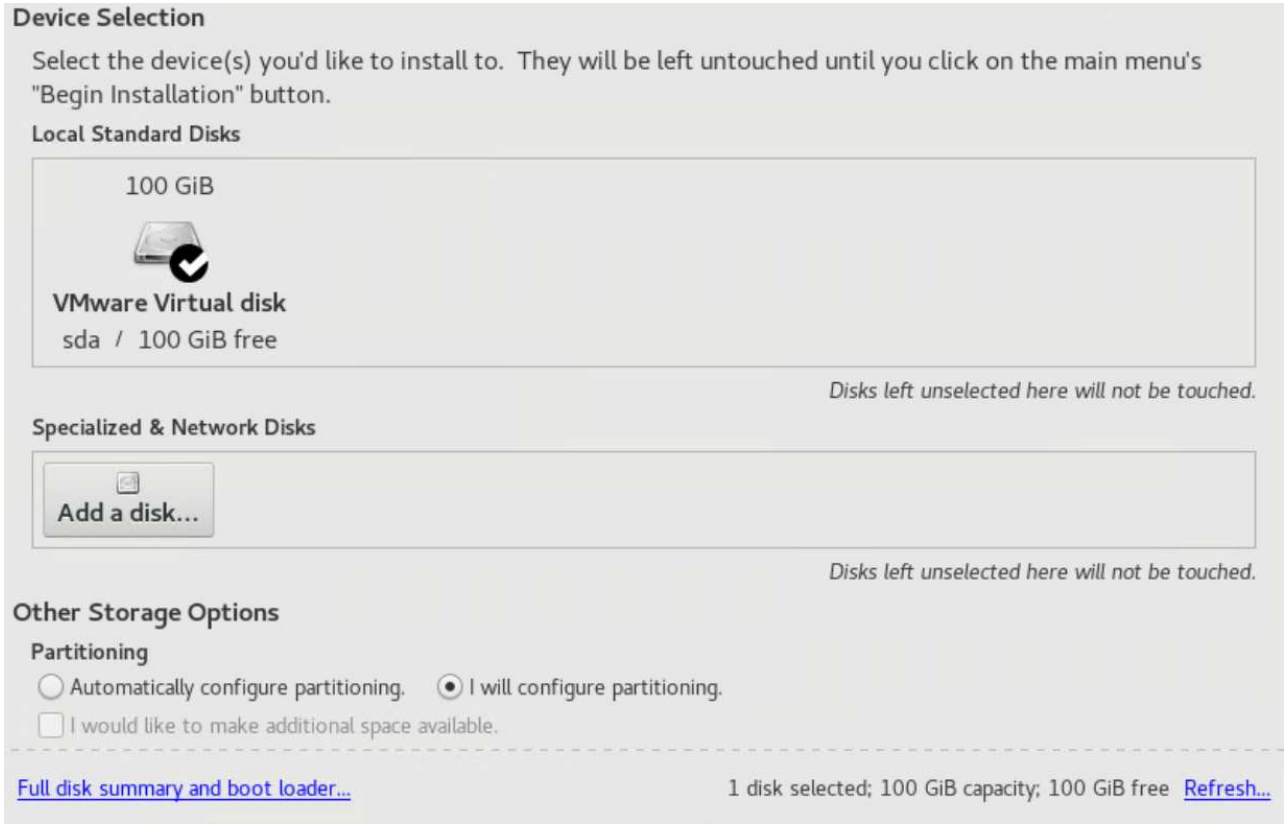
2. Seleccione el idioma preferido y haga clic en Continue.

   La página siguiente es Resumen de la instalación. La configuración predeterminada debería ser aceptable para la mayoría de estas opciones.

3. Debe personalizar el diseño del almacenamiento siguiendo estas opciones:

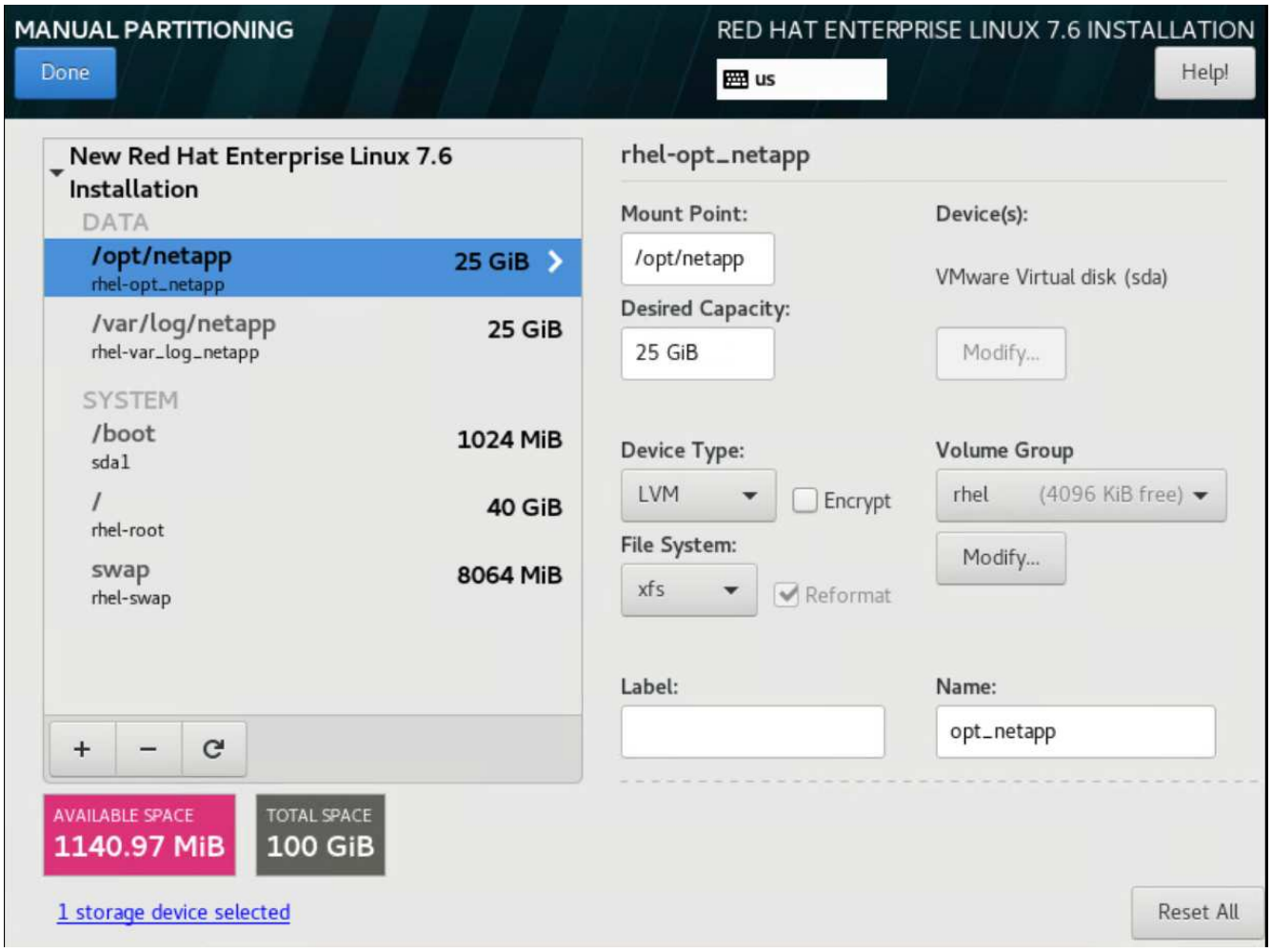
   a. Para personalizar la partición del servidor, haga clic en destino de instalación.

   b. Confirme que el disco virtual de VMware de 100GIB está seleccionado con una Marca de verificación en negro y seleccione el botón de opción I voluntad Configure Partitioning.



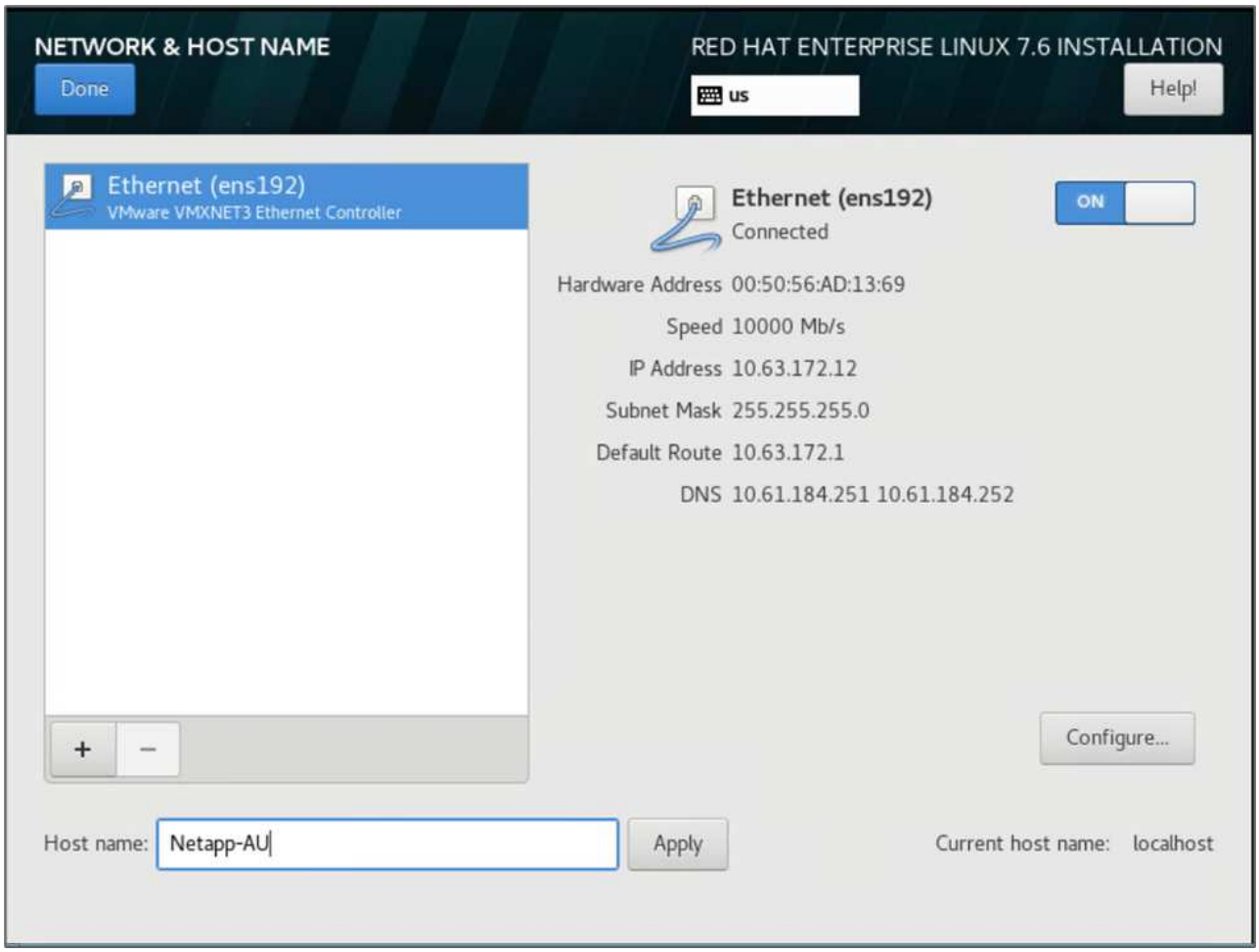
c. Haga clic en Listo.

   Aparecerá un nuevo menú que le permitirá personalizar la tabla de particiones. Dedique 25 GB a cada uno `/opt/netapp` y.. `/var/log/netapp`. Puede asignar automáticamente el resto del almacenamiento al sistema.



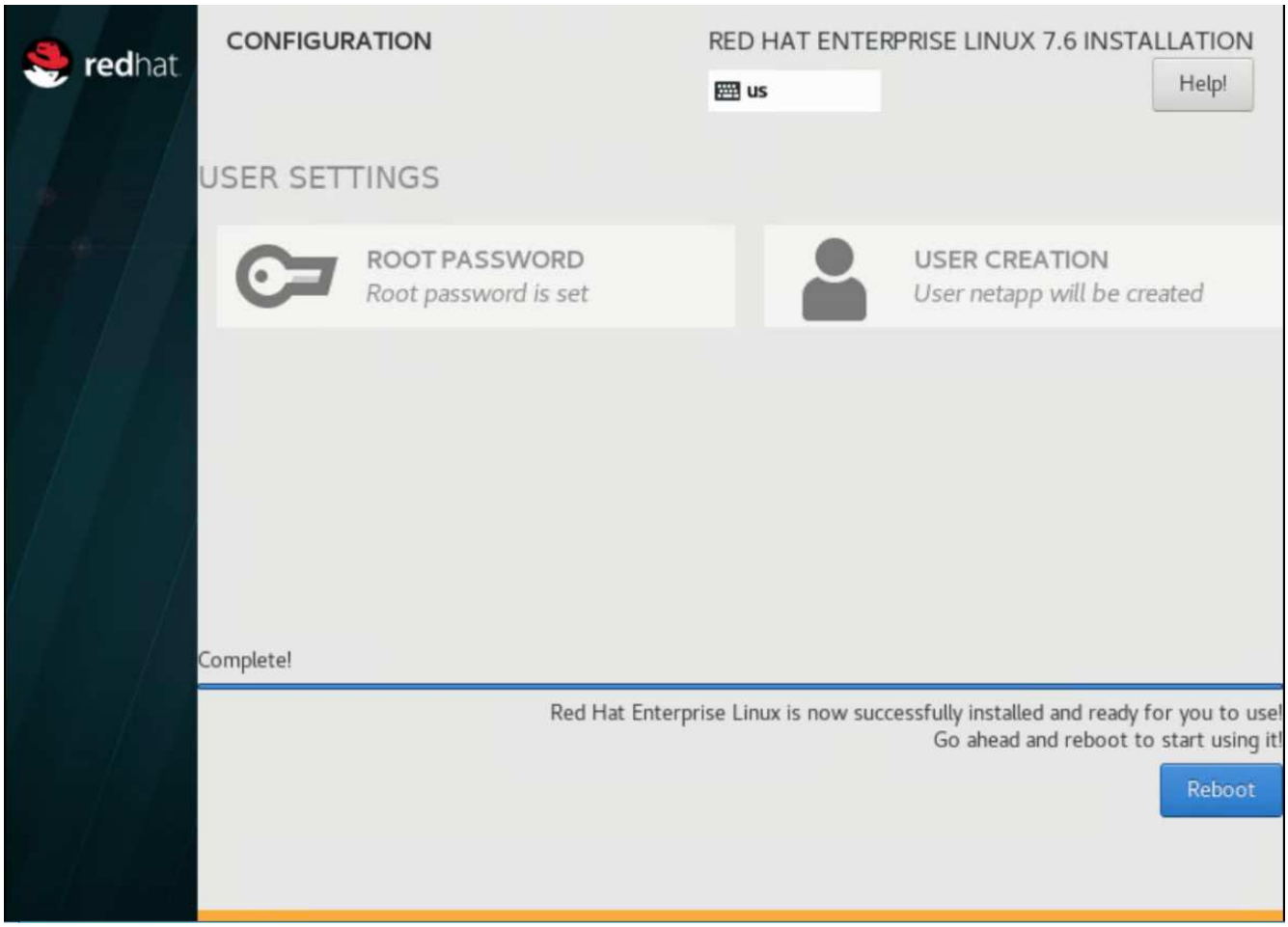
a. Para volver al resumen de la instalación, haga clic en Listo.

4. Haga clic en Network and Host Name.
   a. Introduzca un nombre de host para el servidor.
   b. Active el adaptador de red haciendo clic en el botón deslizante. Si el Protocolo de configuración dinámica de host (DHCP) está configurado en la red, recibirá una dirección IP. Si no lo está, haga clic en Configurar y asigne manualmente una dirección.



c. . Haga clic en Listo para volver al resumen de la instalación.

5. En la página Resumen de la instalación, haga clic en comenzar instalación.
6. En la página progreso de la instalación, puede establecer la contraseña raíz o crear una cuenta de usuario local. Cuando finalice la instalación, haga clic en Reiniciar para reiniciar el servidor.



7. Una vez reiniciado el sistema, inicie sesión en el servidor y regístrelo con Red Hat Subscription Manager.

```
[root@Netapp-AU ~]# subscription-manager register
Registering to: subscription.rhsm.redhat.com:443/subscription
Username: alan.cowles@netapp.com
Password:
The system has been registered with ID: a47f2e7b-81cd-4757-85c7-eb1818c2c2a1
The registered system name is: Netapp-AU
[root@Netapp-AU ~]#
```

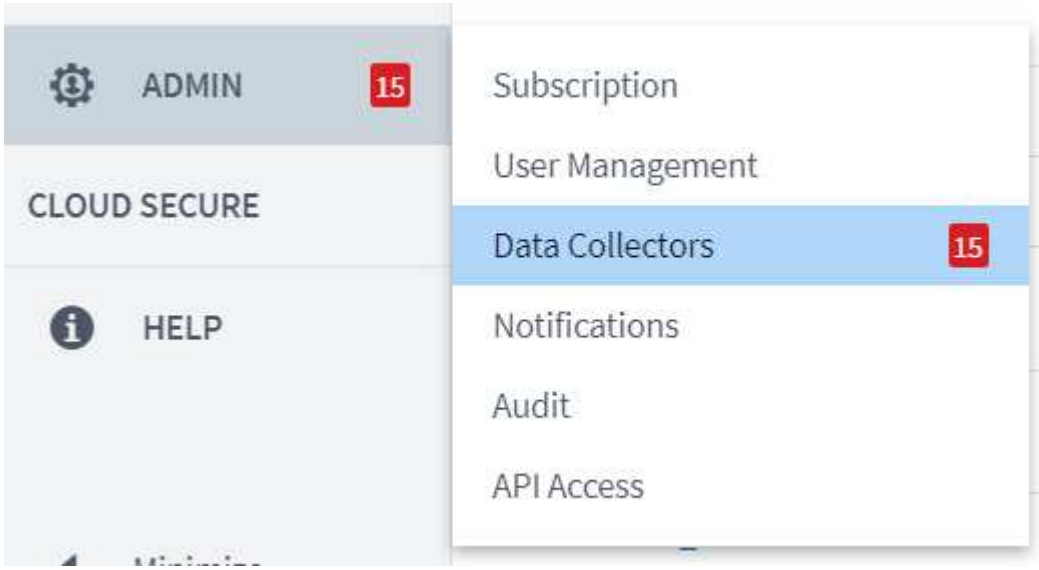
8. Adjunte una suscripción disponible a Red Hat Enterprise Linux.

```
[root@Netapp-AU ~]# subscription-manager attach --pool=8a85f99b710f3b1901713b90b9e154cf
Successfully attached a subscription for: Red Hat Enterprise Linux, Standard Support (128 Sockets, NFR, Partner Only)
[root@Netapp-AU ~]#
```

Cree una instancia de unidad de adquisición en el portal de Cloud Insights e instale el software

Para crear una instancia de unidad de adquisición en el portal de Cloud Insights e instalar el software, lleve a cabo los siguientes pasos:

1. En la página de inicio de Cloud Insights, coloque el cursor sobre la entrada Admin en el menú principal a la izquierda y seleccione colectores de datos en el menú.



2. En el centro superior de la página colectores de datos, haga clic en el vínculo unidades de adquisición.

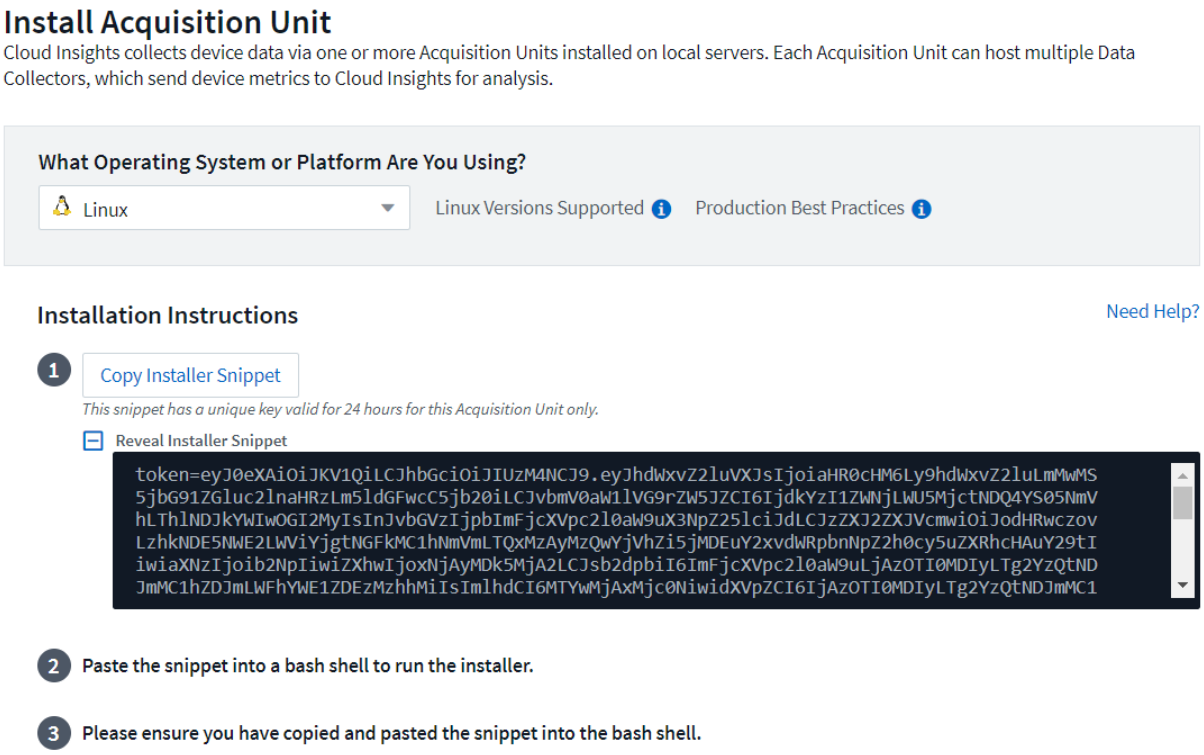


3. Para crear una nueva unidad de adquisición, haga clic en el botón de la derecha.



4. Seleccione el sistema operativo que desea utilizar para alojar la unidad de adquisición y siga los pasos para copiar el script de instalación desde la página Web.

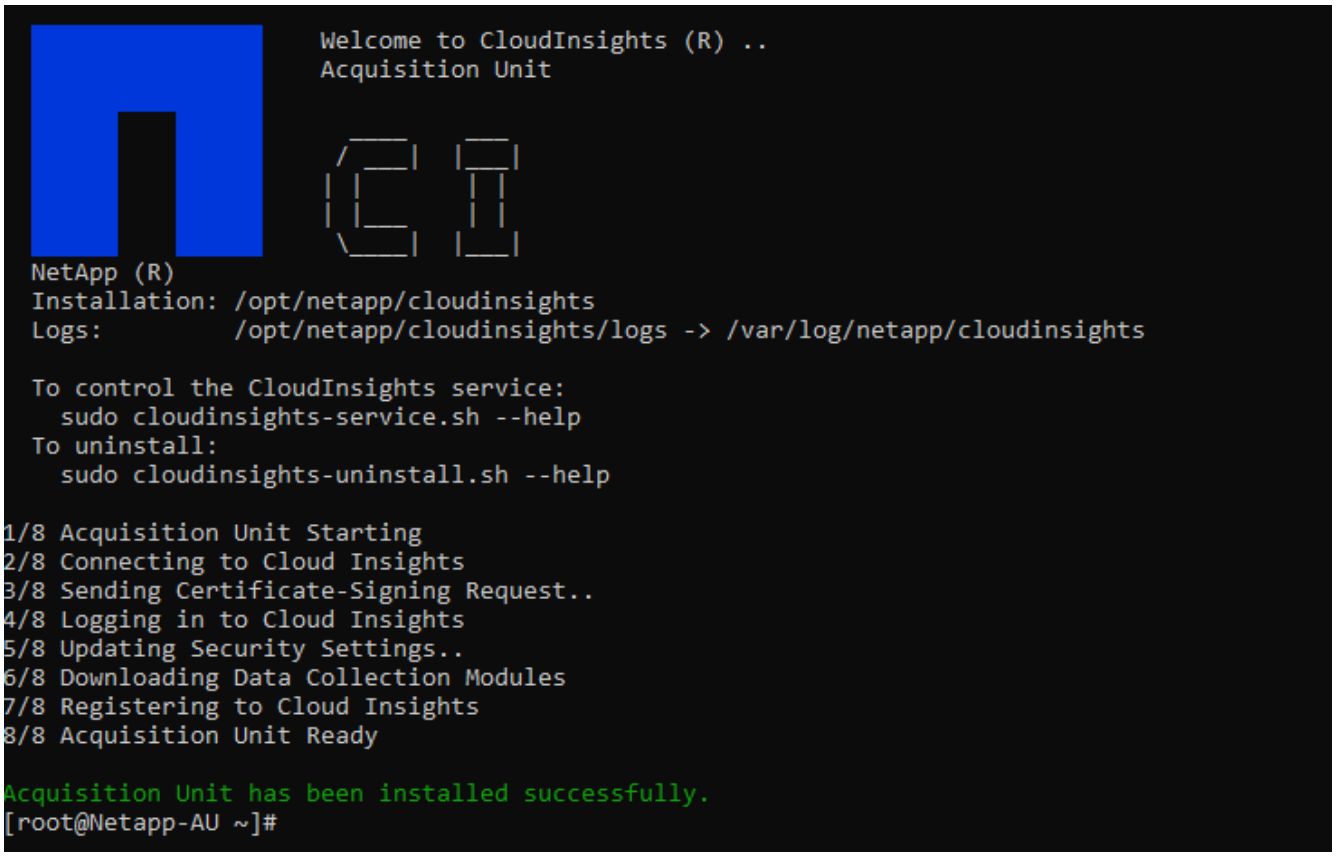
   En este ejemplo, se trata de un servidor Linux, que proporciona un fragmento y un token para pegar en la CLI de nuestro host. La página Web espera a que la unidad de adquisición se conecte.



5. Pegue el fragmento de código en la CLI de la máquina Red Hat Enterprise Linux que se ha aprovisionado y haga clic en Intro.

```
[root@Netapp-AU ~]# token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzM4NCJ9.eyJhdWxvZ2luVXJsIjoiaHR0cHM6Ly9hdWxvZ2luLmMwMS5jbG91ZGluc
2lnaHRzLm5ldGFwcC5jb20iLCJvbmV0aW1lVG9rZW5JZCI6IjQ5ZTY0MGM5LTY5MTItNDQ4Yi04YmI4LTIwNGY2OTQ2YzY1YSIsInJvbGVzIjpbImFjcXVpc
2l0aW9uX3NpZ25lciJdLCJzZXJ2ZXJVcmwiOiJodHRwczovLzhkNDE5NWE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZi5jMDEuY2xvdWRpbnNpZ2h0cy
y5uZXRhcHAuY29tIiwiaXNzIjoib2NpIiwiZXhwIjoxNjAyMTgyNzg2LCJsb2dpbiI6ImFjcXVpc2l0aW9uLjc4MTliZGI3LTk5OWQtNGNiYS05YmU1LTMwZ
TcxZjk0ODRiZCIsImlhdCI6MTYwMjA5NjMyNiwidXVpZCI6Ijc4MTliZGI3LTk5OWQtNGNiYS05YmU1LTMwZTcxZjk0ODRiZCIsInRlbmFudCI6IjhkNDE5N
WE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZiIsInRlbmFudFN1YmRvbWFpbiI6InBzMTMyNSJ9.RvWLR3wH1_k6fIOCiO_h-Wok2STfFPDj7VksmXqw
-GZ-JqSIe8SZE4Sv3DuWrWM6 domainUrl=https://8d4195a6-ebb8-4ad0-a6ef-41302340b5af.c01.cloudinsights.netapp.com/rest/v1/au
version=1.253.0 bootstrap=cloudinsights-au-install-bootstrap.sh && curl $proxy_auth_scheme -H "Authorization: Bearer $to
ken" -o $bootstrap $domainUrl/installerBootstrap && sudo chmod 755 $bootstrap && sudo /bin/bash -c "TOKEN=$token HTTPS_P
ROXY=$https_proxy PROXY_AUTH_SCHEME=$proxy_auth_scheme AU_VERSION=$version INSTALLER_NAME=cloudinsights-linux-au-install
er-$version INSTALLER_URL=$domainUrl/installers/linux/$version ./$bootstrap"
```

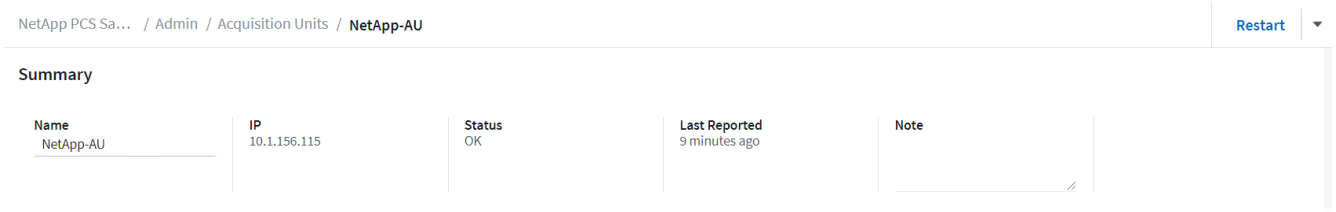
El programa de instalación descarga un paquete comprimido e inicia la instalación. Una vez finalizada la instalación, recibe un mensaje que indica que la unidad de adquisición se ha registrado con Cloud Insights de NetApp.



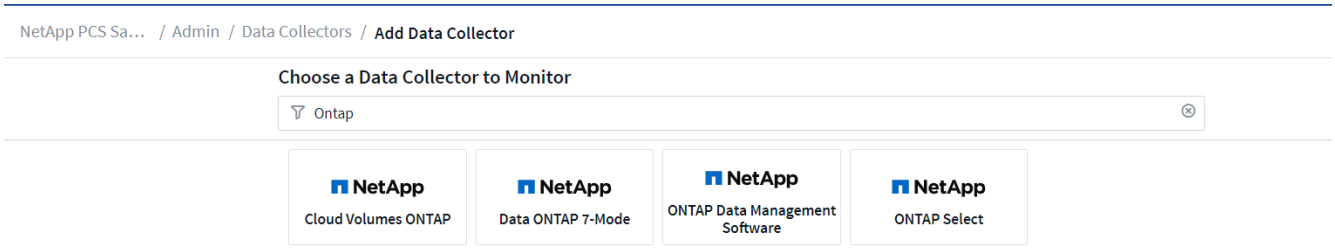
Añada el sistema de almacenamiento supervisado del centro de datos FlexPod a Cloud Insights

Para añadir el sistema de almacenamiento de ONTAP desde una instalación de FlexPod, complete los pasos siguientes:

1. Vuelva a la página unidades de adquisición del portal Cloud Insights y busque la unidad recién registrada. Para ver un resumen de la unidad, haga clic en ella.

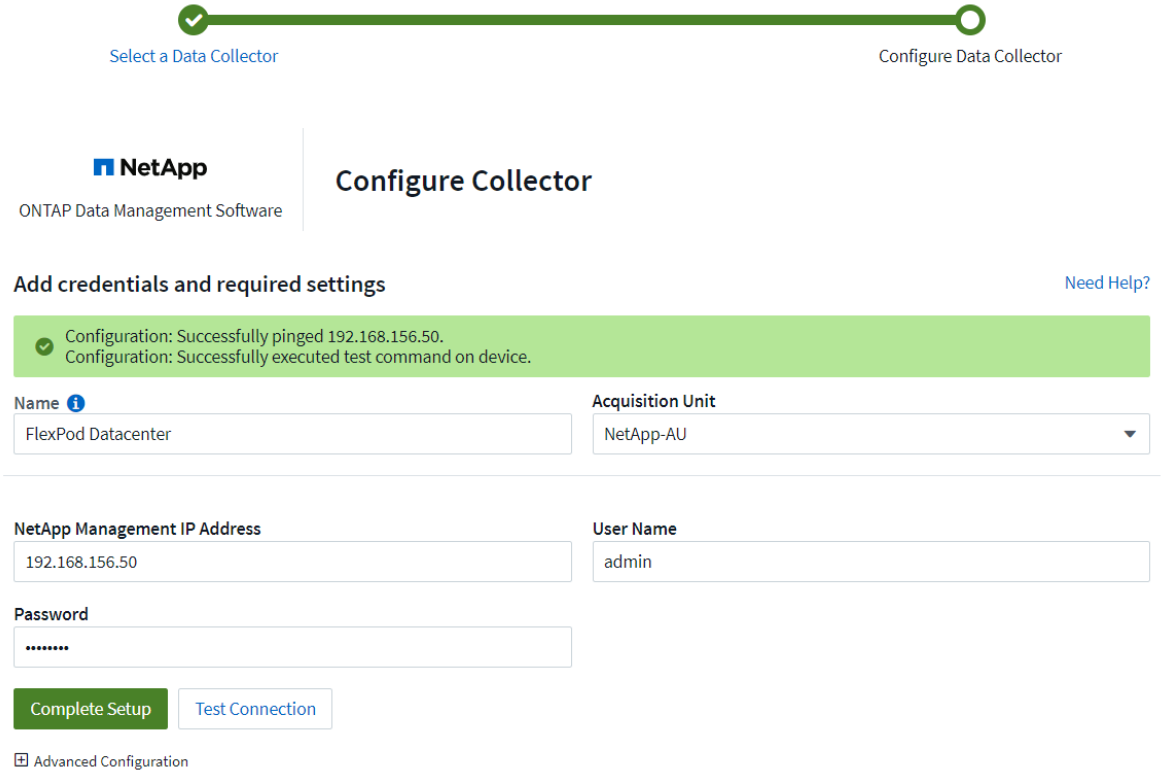


2. Para iniciar un asistente y añadir el sistema de almacenamiento, en la página Summary, haga clic en el botón para crear un recopilador de datos. La primera página muestra todos los sistemas a partir de los cuales se pueden recopilar datos. Utilice la barra de búsqueda para buscar ONTAP.



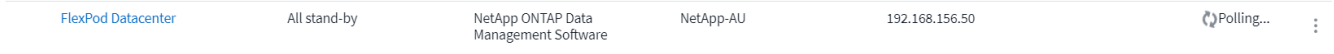
3. Seleccione ONTAP Data Management Software.

   Aparece una página que le permite asignar un nombre a la implementación y seleccionar la unidad de adquisición que desea utilizar. Puede proporcionar la información y las credenciales de conectividad del sistema ONTAP y probar la conexión para confirmarla.



4. Haga clic en Complete Setup.

   El portal vuelve a la página de recopiladores de datos y el recopilador de datos comienza su primer sondeo para recopilar datos del sistema de almacenamiento de ONTAP en el centro de datos de FlexPod.



Casos de uso

Con la instalación y configuración de Cloud Insights para supervisar su solución de

centro de datos de FlexPod, podemos explorar algunas de las tareas que puede realizar en la consola para evaluar y supervisar su entorno. En esta sección, se destacan cinco casos de uso principales para Cloud Insights:

- Integración con Active IQ
- Exploración de paneles en tiempo real
- Creación de paneles personalizados
- Resolución avanzada de problemas
- Optimización del almacenamiento

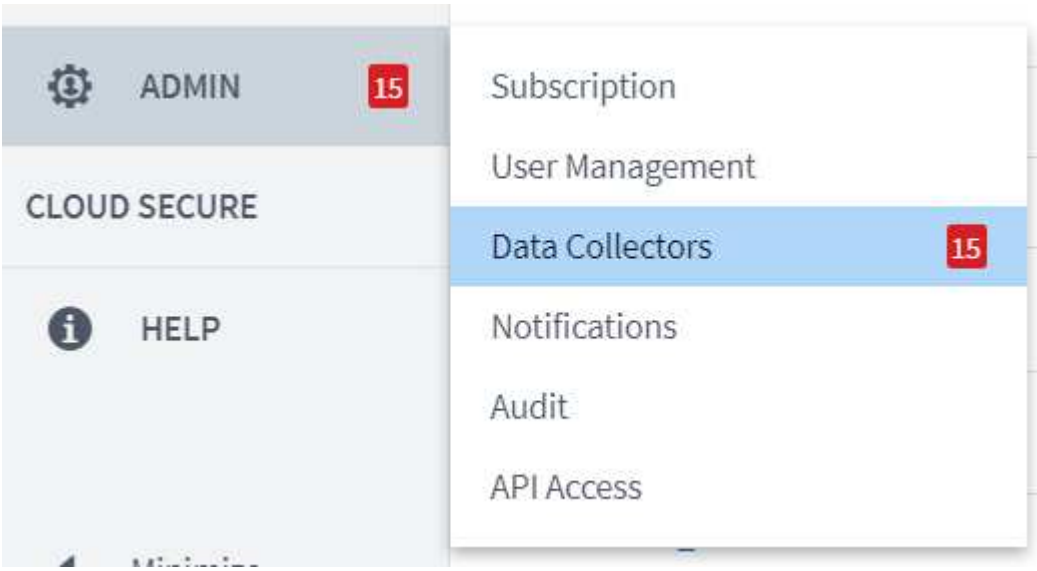
Integración con Active IQ

Cloud Insights está totalmente integrado en la plataforma de supervisión del almacenamiento de Active IQ. Un sistema ONTAP, puesto en marcha como parte de una solución de centro de datos de FlexPod, se configura automáticamente para enviar información de vuelta a NetApp a través de la función AutoSupport, que está integrada en cada sistema. Estos informes se generan de forma programada o dinámica siempre que se detecte un fallo en el sistema. La información que se comunica mediante AutoSupport se agrega y se muestra en consolas con un fácil acceso, en el menú Active IQ de Cloud Insights.

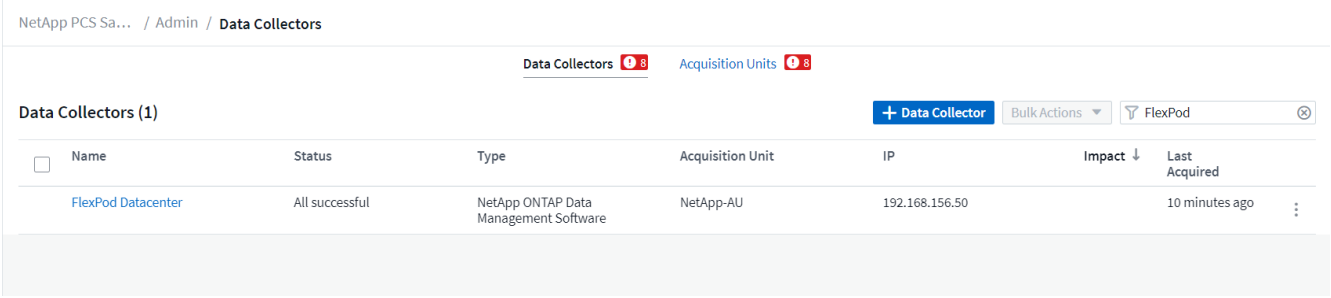
Acceda a la información de Active IQ a través de la consola de Cloud Insights

Para acceder a la información de Active IQ a través de la consola de Cloud Insights, complete los siguientes pasos:

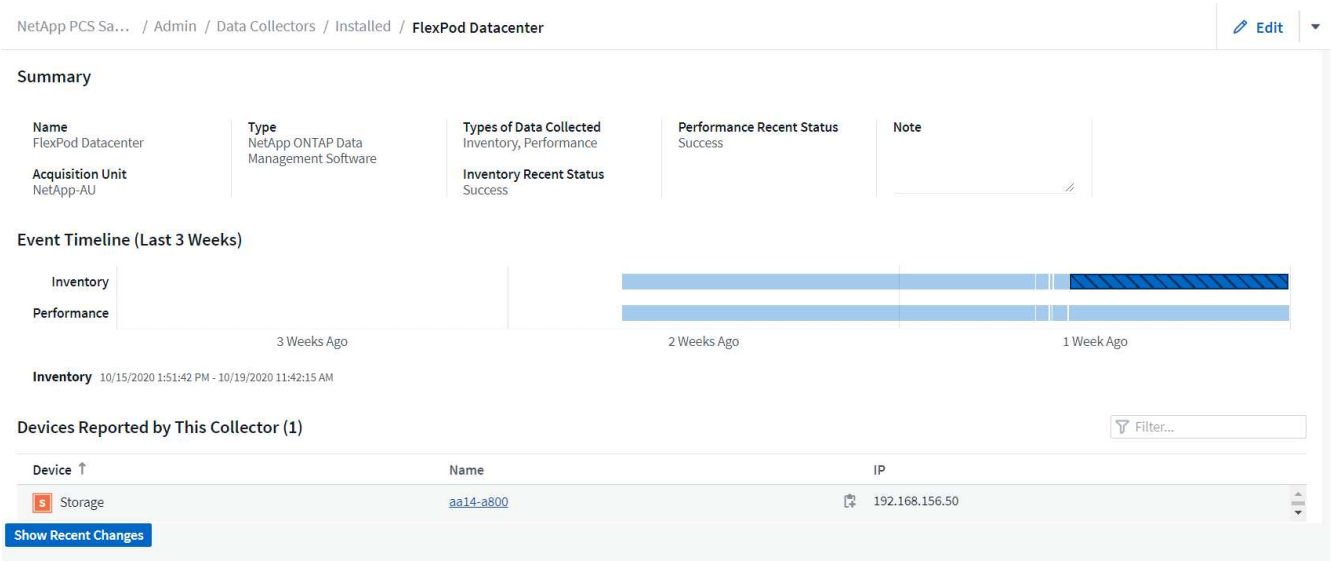
1. Haga clic en la opción colector de datos bajo el menú Admin de la izquierda.



2. Filtro para el recopilador de datos específico de su entorno. En este ejemplo, vamos a filtrar por el término FlexPod.

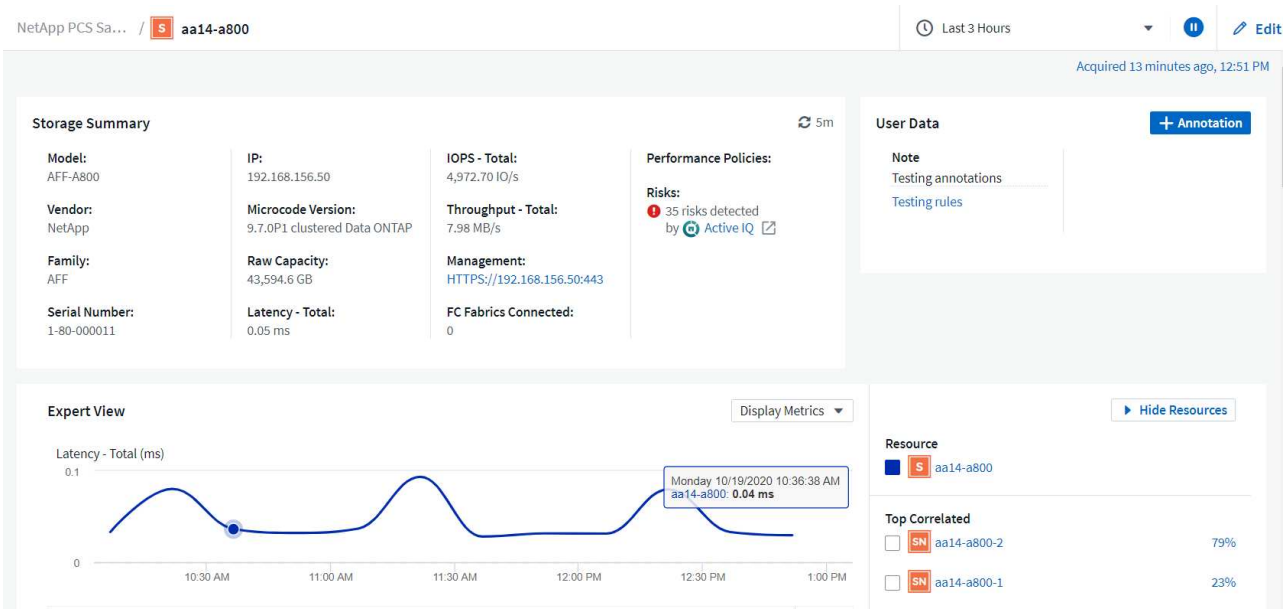


3. Haga clic en el recopilador de datos para obtener un resumen del entorno y los dispositivos que está supervisando el recopilador.

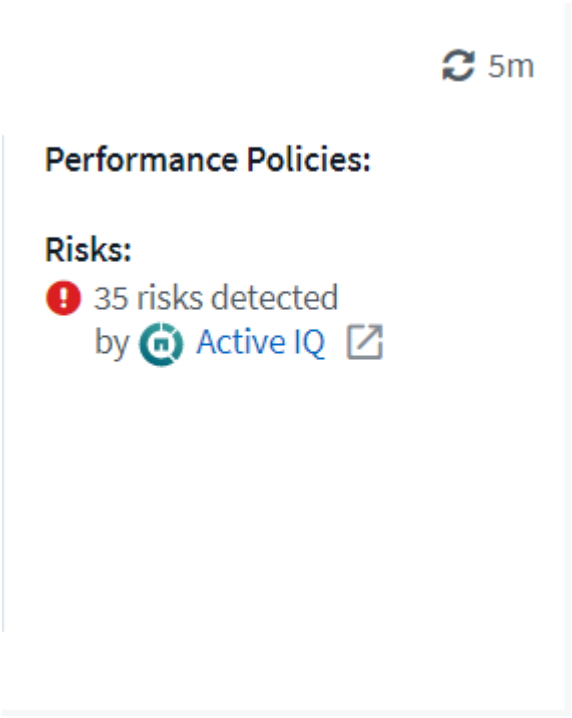


En la lista de dispositivos situada cerca de la parte inferior, haga clic en el nombre del sistema de almacenamiento de ONTAP que se va a supervisar. Esto muestra un tablero de información recopilada sobre el sistema, incluidos los siguientes detalles:

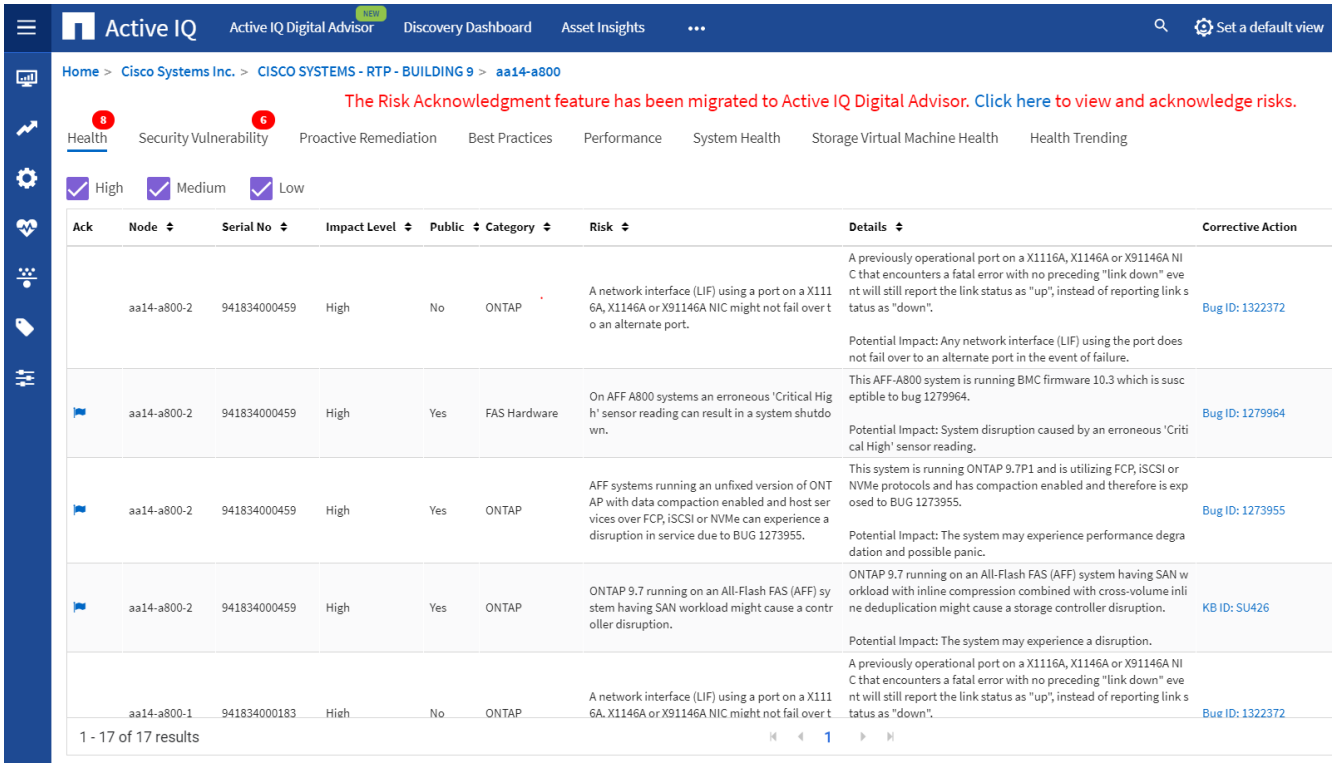
- Modelo
- Familia
- Versión de ONTAP
- Capacidad bruta
- IOPS promedio
- Latencia media
- Rendimiento promedio



Además, en esta página de la sección Performance Policies, puede encontrar un enlace a Active IQ de NetApp.



4. Para abrir una nueva pestaña del navegador y llevarle a la página de reducción de riesgos, en la que se muestran los nodos afectados, qué críticos son los riesgos y cuál es la acción adecuada que se debe realizar para corregir los problemas identificados, haga clic en el enlace de Active IQ.

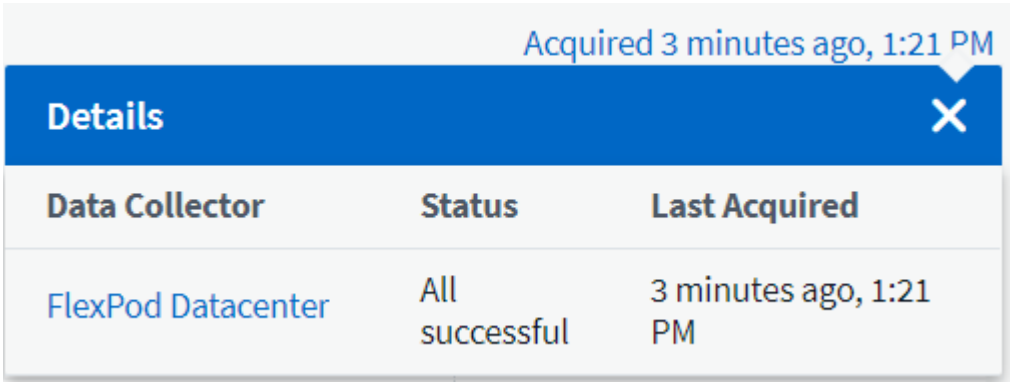


Explore los paneles en tiempo real

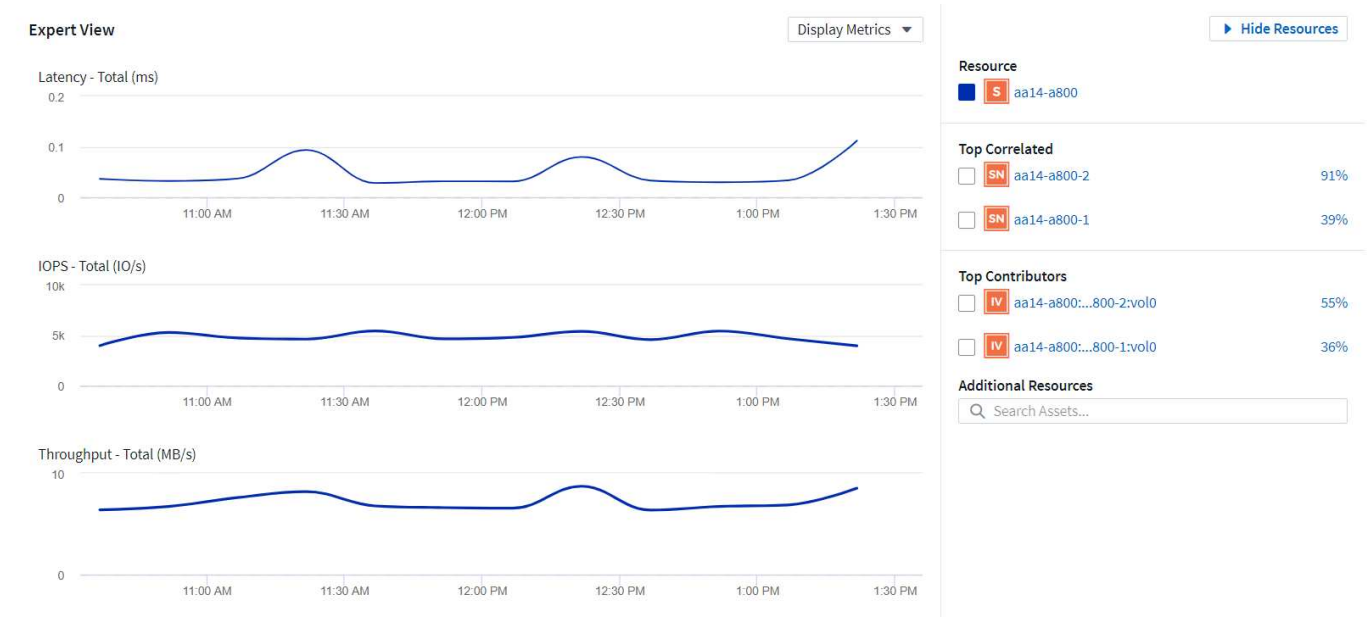
Cloud Insights puede mostrar consolas en tiempo real de la información que se obtuvo en el sondeo del sistema de almacenamiento de ONTAP implementado en una solución para centros de datos de FlexPod. La unidad de adquisición de Cloud Insights recopila datos a intervalos regulares y rellena el panel del sistema de almacenamiento predeterminado con la información recopilada.

Acceda a gráficos en tiempo real a través de la consola de Cloud Insights

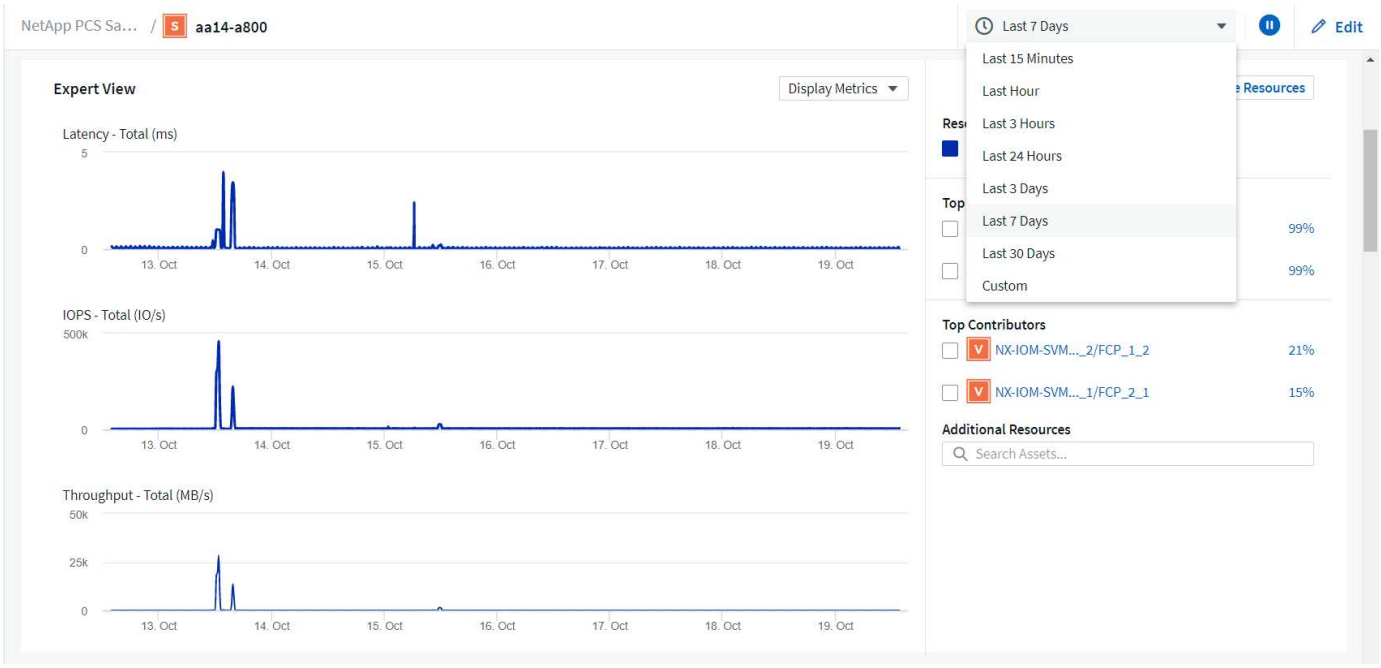
Desde el panel del sistema de almacenamiento, puede ver la última vez que el recopilador de datos actualizó la información. Un ejemplo de esto se muestra en la siguiente figura.



De forma predeterminada, la consola del sistema de almacenamiento muestra varios gráficos interactivos donde se muestran métricas en todo el sistema desde el sistema de almacenamiento en el que se está sondeando o desde cada nodo individual, incluidos: Latencia, IOPS y rendimiento, en la sección Expert View. En la siguiente figura se muestran ejemplos de estos gráficos predeterminados.



De forma predeterminada, los gráficos muestran información de las últimas tres horas, pero puede establecerlos en un número de valores distintos o en un valor personalizado de la lista desplegable, situada cerca de la parte superior derecha del panel del sistema de almacenamiento. Esto se muestra en la siguiente figura.



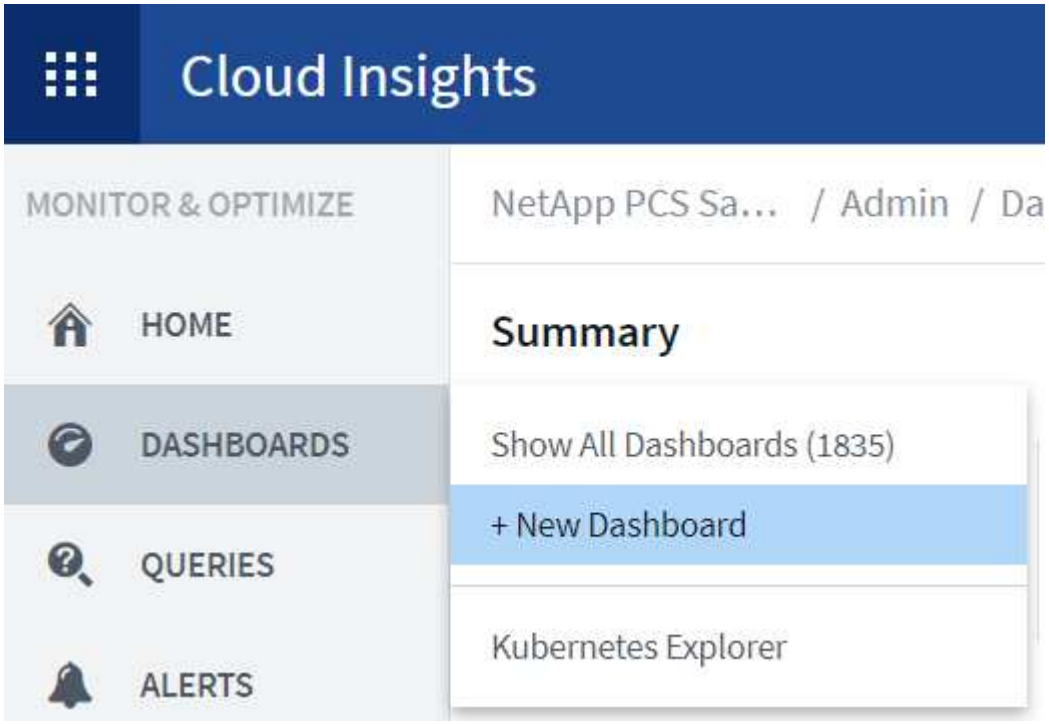
Crear paneles personalizados

Además de utilizar las consolas predeterminadas que muestran información de todo el sistema, puede usar Cloud Insights para crear consolas totalmente personalizadas que le permitirán centrarse en el uso de recursos para volúmenes de almacenamiento específicos de la solución para centros de datos de FlexPod, y, por lo tanto, las aplicaciones puestas en marcha en la infraestructura convergente que dependen de dichos volúmenes para que se ejecuten de forma efectiva. De esta forma, puede ayudarle a crear una mejor visualización de aplicaciones específicas y los recursos que consumen en el entorno del centro de datos.

Cree un panel personalizado para evaluar los recursos de almacenamiento

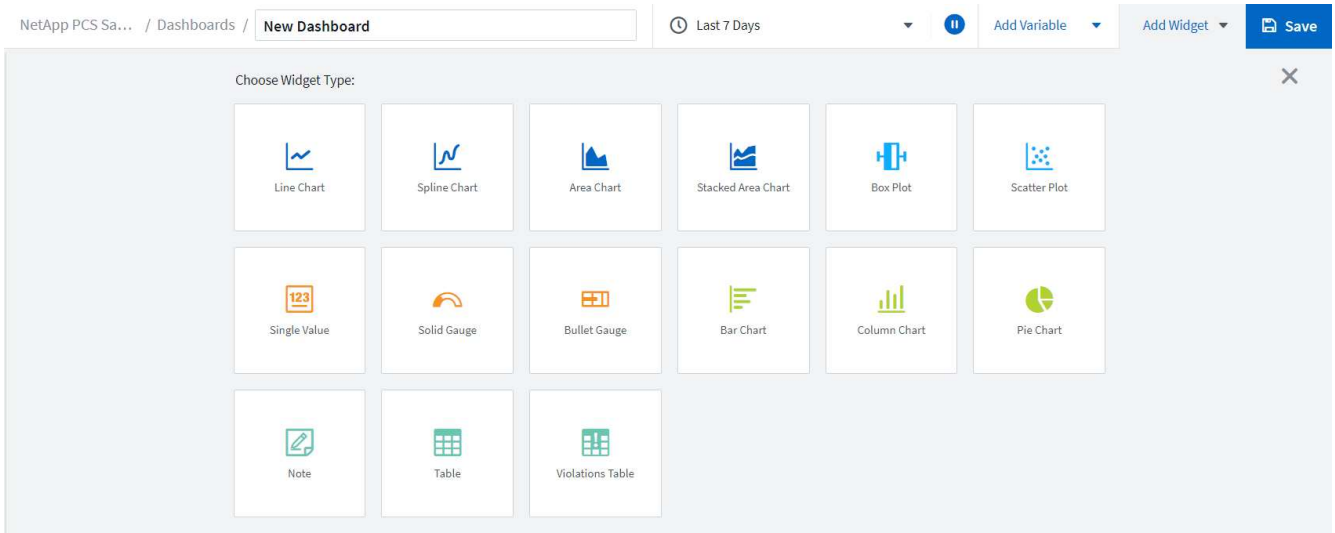
Para crear una consola personalizada para evaluar los recursos de almacenamiento, complete los siguientes pasos:

1. Para crear un panel personalizado, pase el ratón sobre Paneles en el menú principal de Cloud Insights y haga clic en + Nuevo panel en la lista desplegable.



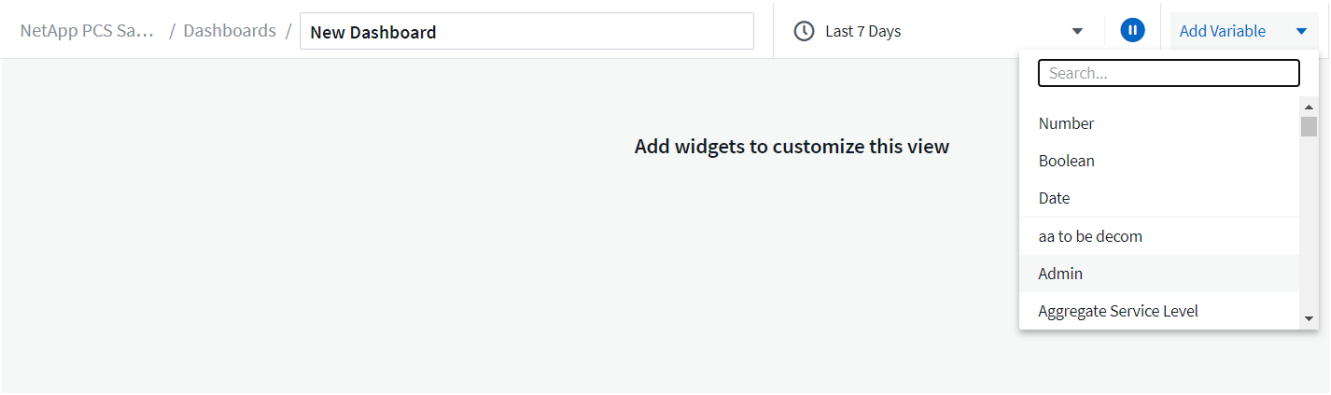
   Se abrirá la ventana Nueva consola.

2. Asigne un nombre al panel y seleccione el tipo de widget utilizado para mostrar los datos. Puede seleccionar entre varios tipos de gráficos, incluso notas o tipos de tablas para presentar los datos recopilados.



3. Elija variables personalizadas en el menú Agregar variable.

   Esto permite que los datos presentados se centren en mostrar factores más específicos o especializados.



4. Para crear una consola personalizada, seleccione el tipo de widget que desea utilizar, por ejemplo, un gráfico circular para mostrar la utilización del almacenamiento por volumen:

   a. Seleccione el widget Gráfico circular de la lista desplegable Agregar widget.

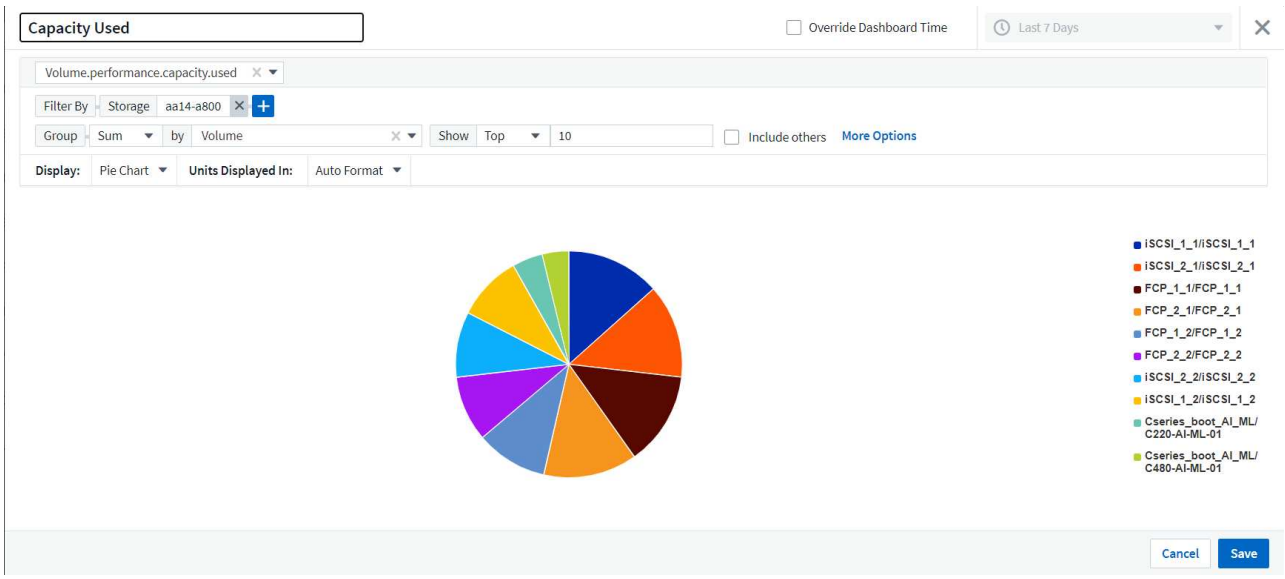
   b. Asigne un nombre al widget con un identificador descriptivo, como `Capacity Used`.

   c. Seleccione el objeto que desea mostrar. Por ejemplo, puede buscar según el término clave volume y seleccionar `volume.performance.capacity.used`.

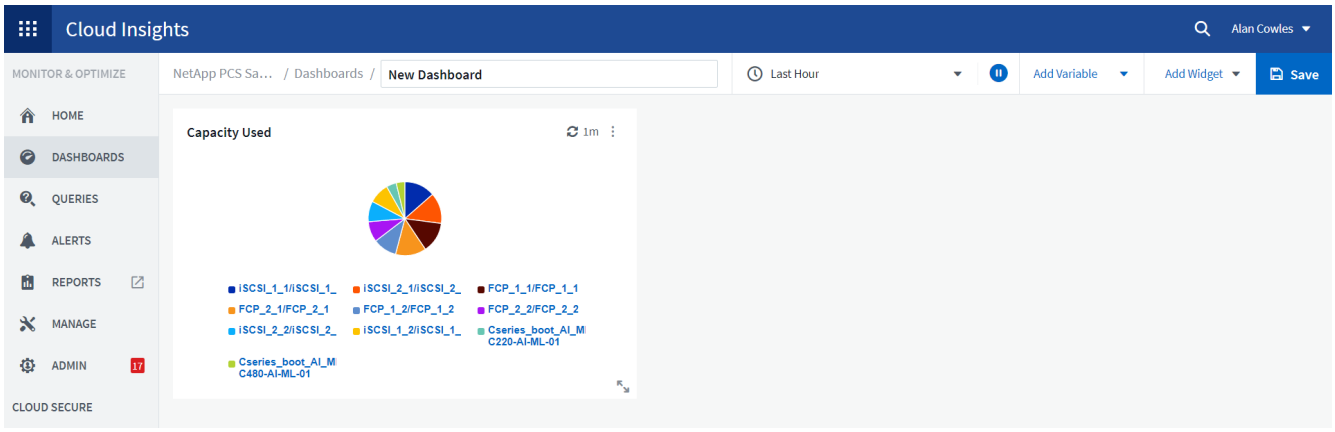
   d. Para filtrar por sistemas de almacenamiento, utilice el filtro y el tipo en el nombre del sistema de almacenamiento en la solución de centro de datos FlexPod.

   e. Personalice la información que se mostrará. De forma predeterminada, esta selección muestra los volúmenes de datos ONTAP y enumera los 10 primeros.

   f. Para guardar el panel personalizado, haga clic en Guardar.



   Después de guardar el widget personalizado, el explorador vuelve a la página New Dashboard donde se muestra el widget recién creado y permite realizar acciones interactivas, como modificar el período de sondeo de datos.



Resolución avanzada de problemas

Cloud Insights permite aplicar métodos avanzados de solución de problemas a cualquier entorno de almacenamiento en una infraestructura convergente de FlexPod Datacenter. Utilizando componentes de cada una de las funciones mencionadas anteriormente: Integración de Active IQ, paneles predeterminados con estadísticas en tiempo real y paneles personalizados, los problemas que pueden surgir se detectan pronto y se resuelven rápidamente. Con la lista de riesgos de Active IQ, un cliente puede encontrar errores de configuración notificados que podrían provocar problemas o detectar errores que se han notificado y parches de versiones de código que pueden remediarlos. Observar los paneles en tiempo real de la página de inicio de Cloud Insights puede ayudar a descubrir patrones en el rendimiento del sistema que podrían ser un indicador temprano de un problema en aumento y ayudar a resolverlo rápidamente. Por último, la posibilidad de crear paneles personalizados permite a los clientes centrarse en los activos más importantes de su infraestructura y supervisar los activos directamente para garantizar que pueden cumplir sus objetivos de continuidad de negocio.

Optimización del almacenamiento

Además de la solución de problemas, es posible usar los datos recopilados por Cloud Insights para optimizar el sistema de almacenamiento de ONTAP puesto en marcha en una solución de infraestructura convergente de FlexPod Datacenter. Si un volumen muestra una alta latencia, quizás porque varias máquinas virtuales con altas demandas de rendimiento comparten el mismo almacén de datos, esa información se muestra en la consola de Cloud Insights. Con esta información, un administrador de almacenamiento puede optar por migrar una o varias máquinas virtuales a otros volúmenes, migrar volúmenes de almacenamiento entre niveles de agregados o entre nodos del sistema de almacenamiento ONTAP, con lo que se obtiene un entorno de rendimiento optimizado. La información obtenida de la integración de Active IQ con Cloud Insights puede destacar los problemas de configuración que provocan un rendimiento más deficiente de lo esperado y ofrecer las acciones correctivas recomendadas que, si se implementan, pueden resolver cualquier problema y garantizar un sistema de almacenamiento perfectamente adaptado.

Vídeos y demostraciones

Puede ver una demostración en vídeo de cómo se usa Cloud Insights de NetApp para evaluar los recursos en un entorno local "aquí".

Puede ver una demostración en vídeo del uso de Cloud Insights de NetApp para supervisar la infraestructura y establecer umbrales de alerta para la infraestructura "aquí".

Puede ver una demostración en vídeo de cómo se utiliza Cloud Insights de NetApp para evaluar las aplicaciones individuales del entorno "aquí".

Información adicional

Si quiere obtener más información sobre la información descrita en este documento, consulte los siguientes sitios web:

- Documentación de productos de Cisco

  "https://www.cisco.com/c/en/us/support/index.html"

- Centro de datos FlexPod

  "https://www.flexpod.com"

- Cloud Insights de NetApp

  "https://cloud.netapp.com/cloud-insights"

- Documentación de productos de NetApp

  "https://docs.netapp.com"

FlexPod con FabricPool: Organización en niveles de datos inactiva en Amazon AWS S3

TR-4801: FlexPod con FabricPool: Organización en niveles de datos inactivos en Amazon AWS S3

Scott Kovacs, NetApp

Los precios del almacenamiento flash siguen bajando, por lo que ponen a disposición de las cargas de trabajo y aplicaciones que anteriormente no se consideraban aptas para el almacenamiento flash. No obstante, para los responsables DE TECNOLOGÍA es fundamental hacer un uso más eficiente de la inversión en almacenamiento. Los departamentos DE TECNOLOGÍA siguen presionándose para ofrecer servicios DE mayor rendimiento con un aumento mínimo o nulo del presupuesto. Para ayudarle a dar respuesta a estas necesidades, FabricPool de NetApp le permite aprovechar la rentabilidad del cloud al mover los datos que se usan con poca frecuencia del costoso almacenamiento flash en las instalaciones a un nivel de almacenamiento más rentable en el cloud público. Mover datos a los que se accede con poca frecuencia al cloud libera espacio de almacenamiento flash muy valioso en sistemas AFF o FAS para ofrecer más capacidad para las cargas de trabajo críticas para el negocio en el nivel flash de alto rendimiento.

En este informe técnico se revisa la función de organización en niveles de datos de FabricPool de ONTAP de NetApp en el contexto de una arquitectura de infraestructura convergente FlexPod de NetApp y Cisco. Debe estar familiarizado con la arquitectura de la infraestructura convergente del centro de datos de FlexPod y el software de almacenamiento de ONTAP para aprovechar completamente los conceptos descritos en este informe técnico. Partiendo de la familiaridad con FlexPod y ONTAP, hablamos de FabricPool, de cómo funciona y de cómo puede utilizarse para lograr un uso más eficiente del almacenamiento flash en las instalaciones. Gran parte del contenido de este informe se trata con mayor detalle en "TR-4598 mejores

prácticas de FabricPool" Y otra documentación de producto de ONTAP. El contenido se ha condensado en una infraestructura de FlexPod y no cubre por completo todos los casos de uso de FabricPool. Todas las características y conceptos examinados están disponibles en ONTAP 9.6.

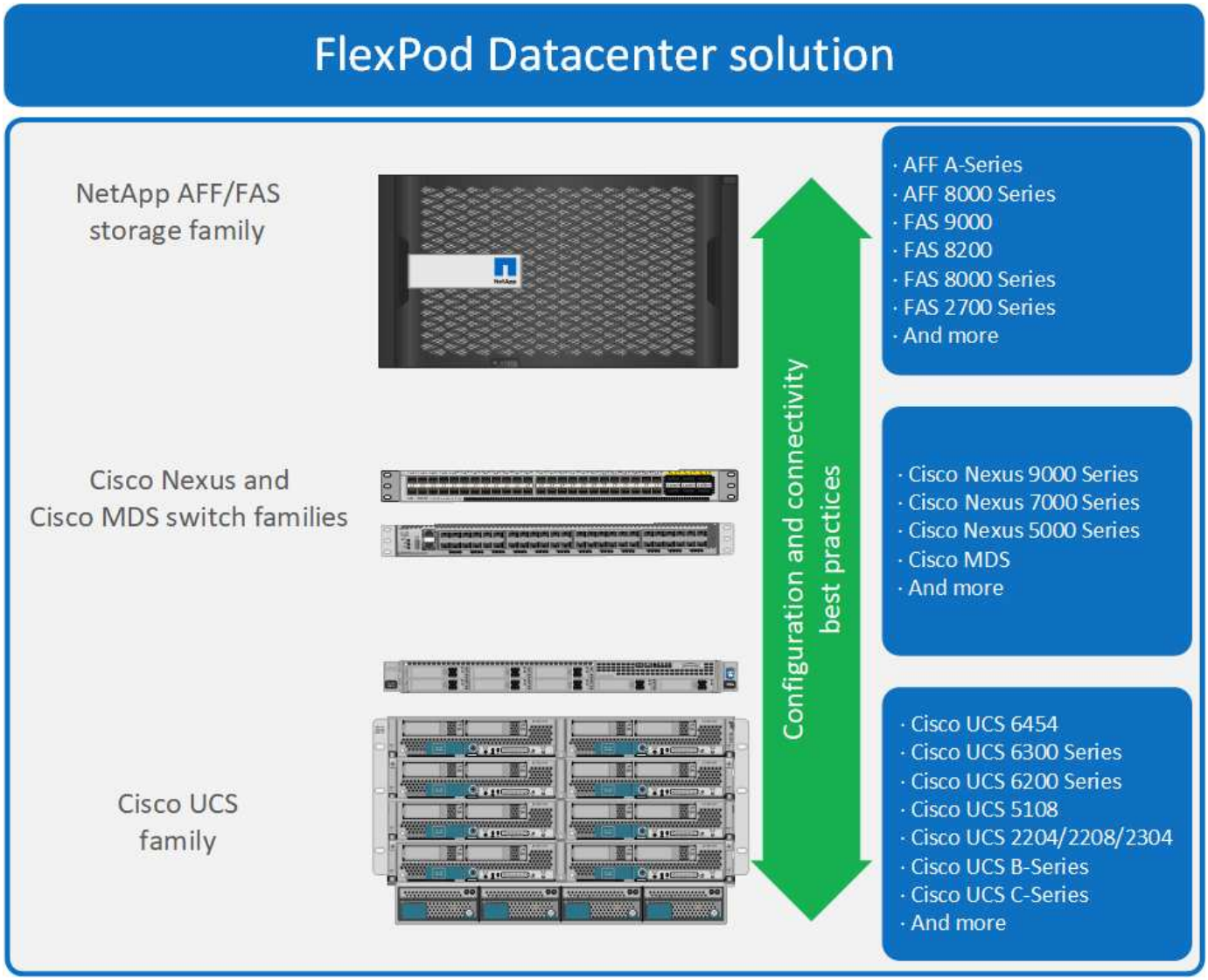
Puede encontrar información adicional sobre FlexPod en "TR-4036 Especificaciones técnicas de FlexPod Datacenter".

Información general y arquitectura de FlexPod

Información general de 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 AFF de NetApp, la conexión a redes Cisco Nexus, la red de almacenamiento de Cisco MDS, Cisco Unified Computing System (Cisco UCS) y el software VMware vSphere en un único paquete. El diseño es lo suficientemente flexible como para que las redes, los recursos informáticos y el almacenamiento puedan encajar en un rack de centro de datos o bien se puede poner en marcha según el diseño de centro de datos del cliente. La densidad de puertos permite que los componentes de las redes acomoden varias configuraciones.

Una de las ventajas de la arquitectura de FlexPod es la capacidad de personalizar o adaptar el entorno para adaptarlo a las necesidades de un cliente. Una unidad FlexPod se puede escalar fácilmente a medida que cambian los requisitos y la demanda. Una unidad se puede escalar tanto de forma vertical (agregando recursos a una unidad FlexPod) como de salida (agregando más unidades FlexPod). La arquitectura de referencia de FlexPod destaca la flexibilidad, los beneficios económicos y la facilidad de instalación de una solución de almacenamiento basada en IP y Fibre Channel. Un sistema de almacenamiento que es capaz de servir diversos protocolos en una única interfaz proporciona a los clientes una opción y protege su inversión, ya que se trata de una arquitectura de conexión única. La siguiente figura muestra muchos de los componentes de hardware de FlexPod.

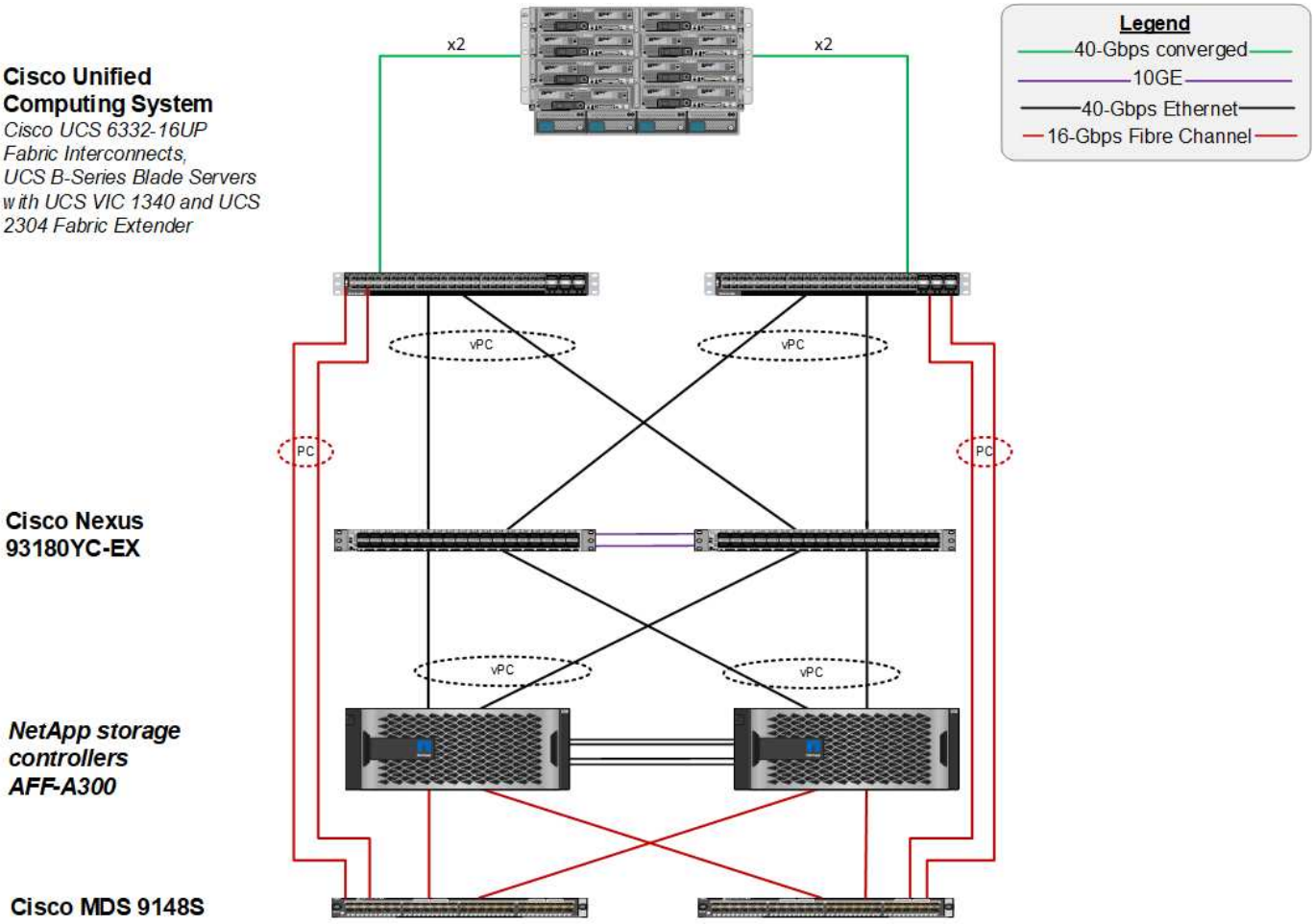


Arquitectura FlexPod

La siguiente figura muestra los componentes de una solución VMware vSphere y FlexPod y las conexiones de red necesarias para las interconexiones de estructura Cisco UCS 6454. Este diseño consta de los siguientes componentes:

- Conexiones Ethernet de 40 GB canalizadas por puerto entre el chasis blade Cisco UCS 5108 y las interconexiones de estructura Cisco UCS
- Conexiones Ethernet de 40 GB entre la interconexión de estructura de Cisco UCS y Cisco Nexus 9000
- Conexiones Ethernet de 40 GB entre Cisco Nesxus 9000 y la cabina de almacenamiento AFF A300 de NetApp

Estas opciones de infraestructura se amplían con la introducción de switches MDS de Cisco que se sitúan entre Cisco UCS Fabric Interconnect y AFF A300 de NetApp. Esta configuración proporciona a los hosts arranque FC un acceso a nivel de bloques FC de 16 GB al almacenamiento compartido. La arquitectura de referencia refuerza la estrategia de conexión única porque, a medida que se añade almacenamiento adicional a la arquitectura, no es necesario realizar ninguna conmutación por los hosts a la interconexión de estructura Cisco UCS.



FabricPool

Información general de FabricPool

FabricPool es una solución de almacenamiento híbrido en ONTAP que utiliza un agregado all-flash (SSD) como nivel de rendimiento y un almacén de objetos en un servicio de cloud público como nivel del cloud. Esta configuración permite el movimiento de datos basado en políticas, en función de si se accede con frecuencia a los datos o no. ONTAP admite FabricPool tanto para agregados AFF como para todos los SSD en plataformas FAS. El procesamiento de datos se realiza a nivel de bloque, con los bloques de datos a los que se accede con frecuencia en el nivel de rendimiento all-flash etiquetados como bloques activos y a los que se accede con poca frecuencia como inactivos.

El uso de FabricPool permite reducir los costes de almacenamiento sin sacrificar rendimiento, eficiencia, seguridad ni protección. FabricPool es transparente para las aplicaciones empresariales y aprovecha las eficiencias del cloud al reducir el TCO del almacenamiento sin tener que rediseñar la arquitectura de la infraestructura de aplicaciones.

FlexPod se puede beneficiar de las funcionalidades de almacenamiento por niveles de FabricPool para hacer un uso más eficiente del almacenamiento flash de ONTAP. Las máquinas virtuales inactivas (VM), las plantillas de máquinas virtuales que se usan con poca frecuencia y los backups de máquinas virtuales de NetApp SnapCenter para vSphere pueden consumir un espacio valioso en el volumen del almacén de datos. El traslado de datos inactivos al nivel de cloud libera espacio y recursos para las aplicaciones de alto rendimiento esenciales que se alojan en la infraestructura de FlexPod.

Los protocolos Fibre Channel e iSCSI suelen tardar más en experimentar un tiempo de espera (de 60 a 120 segundos), pero no se intentan volver a establecer una conexión del mismo modo que lo hacen los protocolos NAS. Si se agota el tiempo de espera de un protocolo SAN, debe reiniciarse la aplicación. Incluso una breve interrupción podría ser desastrosa para las aplicaciones de producción que utilizan protocolos SAN, ya que no hay forma de garantizar la conectividad con los clouds públicos. Para evitar este problema, NetApp recomienda el uso de clouds privados cuando la organización en niveles de los datos a los que acceden los protocolos SAN.

En ONTAP 9.6, FabricPool se integra con todos los principales proveedores de cloud público: Alibaba Cloud Object Storage Service, Amazon AWS S3, Google Cloud Storage, IBM Cloud Object Storage y Microsoft Azure Blob Storage. Este informe se centra en el almacenamiento Amazon AWS S3 como nivel de objetos en el cloud elegido.

El agregado compuesto

Para crear una instancia de FabricPool, se asocia un agregado flash de ONTAP a un almacén de objetos en el cloud, como un bloque de AWS S3, para crear un agregado compuesto. Cuando se crean volúmenes dentro del agregado compuesto, se pueden aprovechar las funcionalidades de organización en niveles de FabricPool. Cuando se escriben datos en el volumen, ONTAP asigna una temperatura a cada uno de los bloques de datos. Cuando el bloque se escribe por primera vez, se le asigna una temperatura de calor. A medida que pasa el tiempo, si no se accede a los datos, se somete a un proceso de refrigeración hasta que finalmente se le asigna un estado de frío. Estos bloques de datos a los que se accede con poca frecuencia se organizan en niveles fuera del agregado de SSD de rendimiento y en el almacén de objetos en el cloud.

El período de tiempo entre el momento en el que un bloque se designa como frío y el momento en el que se mueve al almacenamiento de objetos en cloud se modifica con la política de organización en niveles del volumen en ONTAP. Se logra más granularidad mediante la modificación de la configuración de ONTAP que controla el número de días necesarios para que un bloque quede frío. Los candidatos para la organización en niveles de datos son las copias Snapshot de volúmenes tradicionales, los backups de SnapCenter para vSphere VM y otros backups basados en Snapshot de NetApp, y los bloques que se usan con poca frecuencia en un almacén de datos de vSphere, como las plantillas de máquinas virtuales y los datos de estas máquinas a los que se accede con poca frecuencia.

Generación de informes de datos inactivos

Los informes de datos inactivos (IDR, por sus siglas en inglés) están disponibles en ONTAP para ayudar a evaluar la cantidad de datos inactivos que se pueden organizar en niveles a partir de un agregado. IDR está activado de forma predeterminada en ONTAP 9.6 y utiliza una directiva de refrigeración predeterminada de 31 días para determinar qué datos del volumen están inactivos.

La cantidad de datos inactivos organizados en niveles depende de las políticas de organización en niveles establecidas en el volumen. Esta cantidad puede ser diferente de la cantidad de datos fríos detectados por IDR utilizando el período de enfriamiento predeterminado de 31 días.

Creación de objetos y movimiento de datos

FabricPool funciona con bloques WAFL de NetApp, bloques de refrigeración, concatenarlos y objetos de almacenamiento y migran esos objetos a un nivel de cloud. Cada objeto de FabricPool es de 4 MB y está compuesto por 1,024 bloques de 4 KB. El tamaño del objeto es fijo de 4 MB en función de las recomendaciones de rendimiento de los principales proveedores de cloud y no puede modificarse. Si los bloques inactivos se leen y se activan, solo se recuperan los bloques solicitados del objeto de 4 MB y se vuelven a mover al nivel de rendimiento. Ni el objeto completo ni el archivo completo se vuelven a migrar. Solo

se migran los bloques necesarios.

> Si ONTAP detecta una oportunidad para lecturas secuenciales, solicita bloques del nivel de cloud antes de que se lean para mejorar el rendimiento.

De forma predeterminada, los datos se mueven al nivel de cloud solo cuando se utiliza el agregado de rendimiento superior al 50 %. Este umbral se puede establecer en un porcentaje más bajo para permitir una menor cantidad de almacenamiento de datos en el nivel flash de rendimiento para moverse al cloud. Esto podría resultar útil si la estrategia de organización en niveles consiste en mover datos inactivos solo cuando el agregado está cerca de la capacidad.

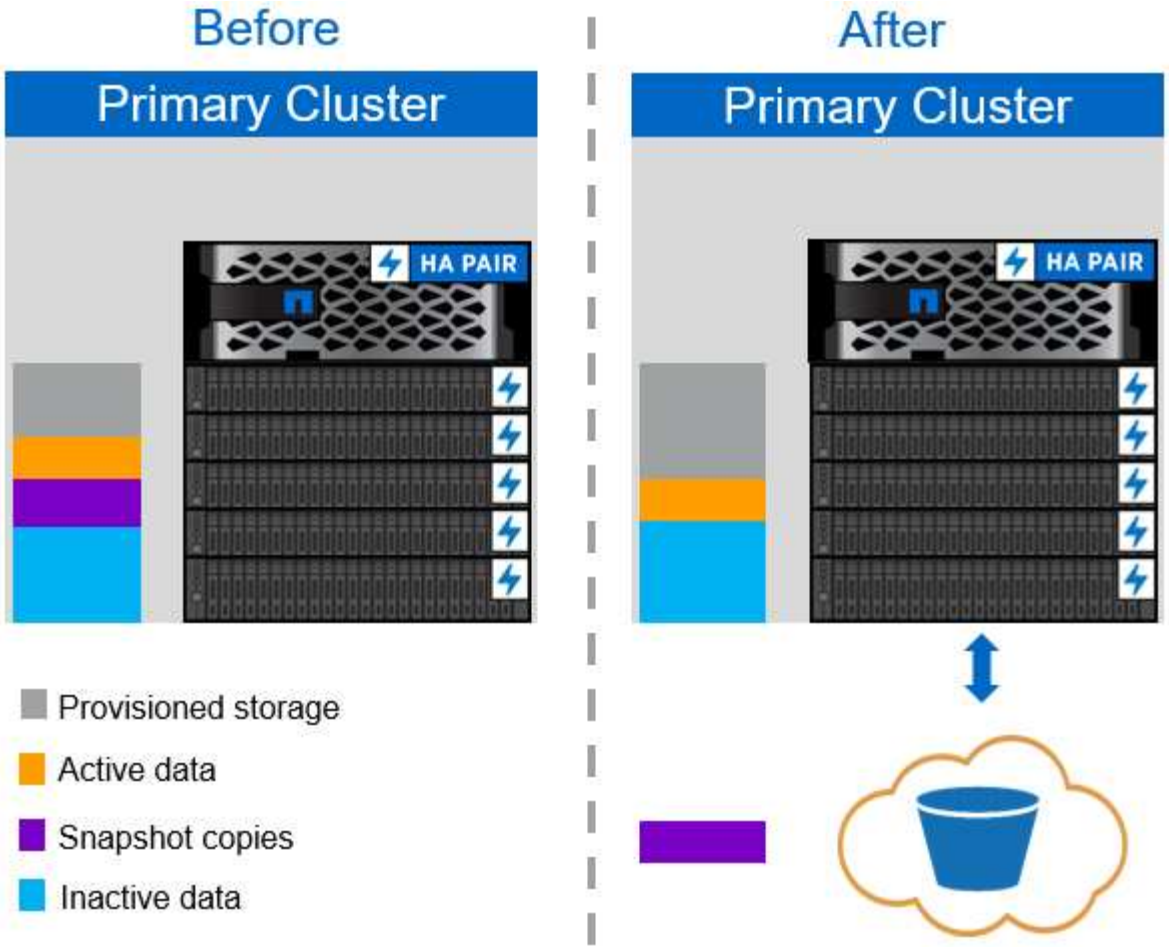
Si el uso del nivel de rendimiento supera el 70 % de la capacidad, los datos inactivos se leen directamente desde el nivel de cloud sin que se vuelvan a escribir en el nivel de rendimiento. Al evitar la escritura de datos fríos en agregados muy utilizados, FabricPool conserva el agregado para los datos activos.

Reclame espacio en el nivel de rendimiento

Como hemos visto anteriormente, el principal caso de uso de FabricPool es facilitar el uso más eficiente del almacenamiento flash local de alto rendimiento. Los datos inactivos en forma de copias Snapshot de volumen y backup de equipos virtuales de la infraestructura virtual de FlexPod pueden ocupar una gran cantidad de almacenamiento flash de elevado coste. El valioso almacenamiento en el nivel de rendimiento se puede liberar implementando una de las dos políticas de almacenamiento por niveles: Solo Snapshot o automático.

Política de organización en niveles solo de Snapshot

La política de organización en niveles de solo Snapshot, que se muestra en la siguiente figura, mueve datos Snapshot de volumen frío y backups de SnapCenter para vSphere de máquinas virtuales que ocupan espacio pero no comparten bloques con el sistema de archivos activo a un almacén de objetos de cloud. La política de organización en niveles solo de Snapshot mueve bloques de datos inactivos al nivel de cloud. Si hace falta una restauración, los bloques fríos en el cloud se activan y vuelven a transferirse al nivel flash de rendimiento de las instalaciones.

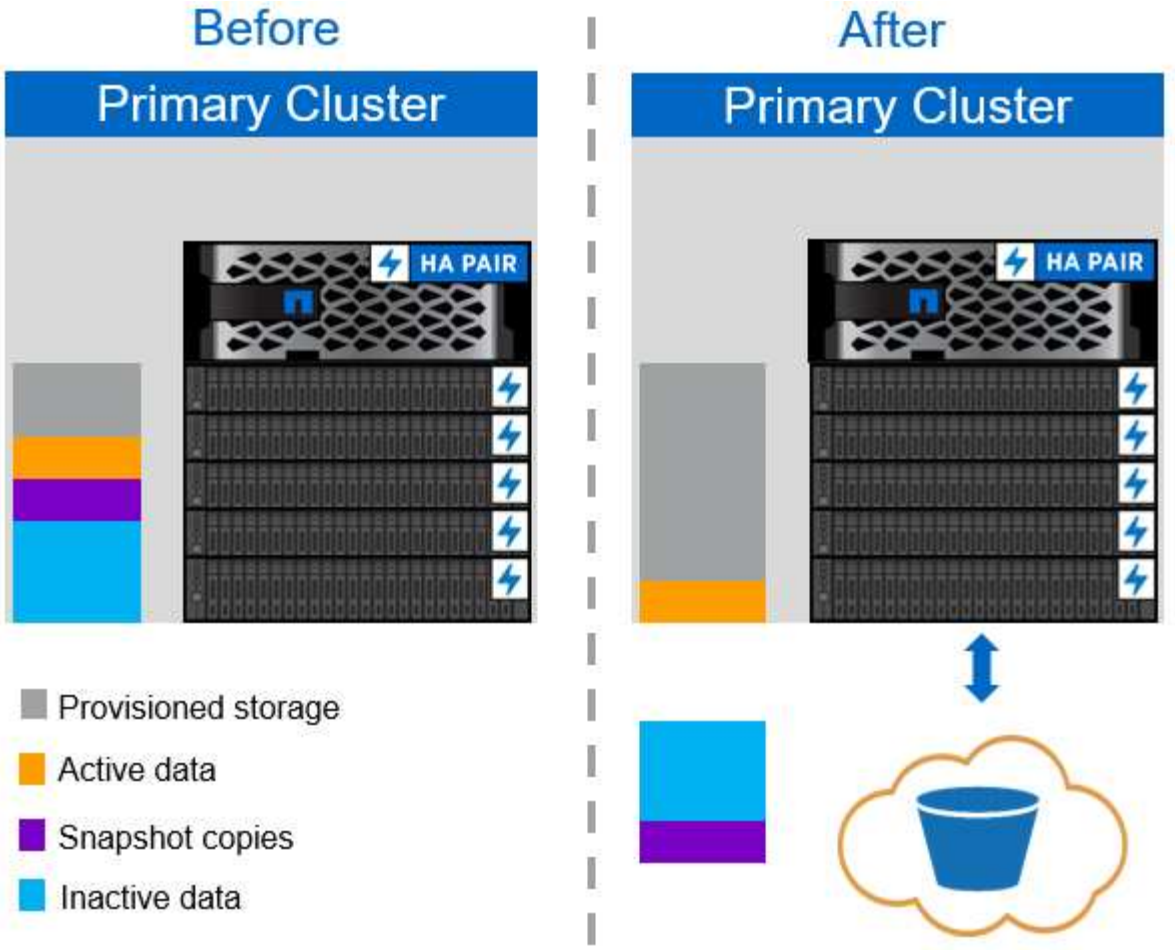


Política de organización automática en niveles

La política de organización en niveles automática de FabricPool, que se muestra en la siguiente figura, no solo mueve bloques de datos de copias snapshot activas al cloud, sino que también mueve bloques de datos inactivos del sistema de archivos activo. Esto puede incluir plantillas de máquina virtual y todos los datos de máquina virtual sin usar en el volumen de almacén de datos. Los bloques fríos que se mueven se controlan mediante el `tiering-minimum-cooling-days` configuración para el volumen. Si una aplicación lee aleatoriamente los bloques inactivos en el nivel de cloud, esos bloques se activan y vuelven a traerlos al nivel de rendimiento. Sin embargo, si un proceso secuencial lee los bloques fríos, como un análisis antivirus, los bloques permanecen inactivos y persisten en el almacén de objetos en la nube, ya que no se mueven de nuevo al nivel de rendimiento.

Cuando se usa la política de organización en niveles automática, los bloques a los que se accede con poca frecuencia se devuelven del nivel de cloud a la velocidad de conectividad del cloud. Esto puede afectar al rendimiento de la VM si la aplicación es sensible a la latencia, que debe tenerse en cuenta antes de usar la política de organización en niveles automática en el almacén de datos. NetApp recomienda colocar LIF de interconexión de clústeres en puertos con una velocidad de 10 GbE para lograr un rendimiento adecuado.

El generador de perfiles de almacén de objetos se debe usar para probar la latencia y el rendimiento del almacén de objetos antes de adjuntarlo a un agregado de FabricPool.



Toda la política de organización en niveles

A diferencia de las políticas Auto y Snapshot, la política de organización en niveles total mueve volúmenes completos de datos inmediatamente al nivel de cloud. Esta política es más adecuada para la protección de datos secundaria o volúmenes de archivado para los que es necesario conservar los datos con fines históricos o normativos, pero a los que no se accede en raras ocasiones. La política todo no se recomienda para los volúmenes de almacenes de datos de VMware, ya que los datos escritos en el almacén de datos se mueven de inmediato al nivel de cloud. Las operaciones de lectura posteriores se realizan desde el cloud y podrían introducir problemas de rendimiento para las máquinas virtuales y las aplicaciones que residen en el volumen del almacén de datos.

Seguridad

La seguridad es una preocupación central para el cloud y FabricPool. Todas las funciones de seguridad nativas de ONTAP son compatibles con el nivel de rendimiento y el movimiento de datos se protege mientras se transfieren al nivel de cloud. FabricPool utiliza la "AES-256-GCM" el algoritmo de cifrado en el nivel de rendimiento y mantiene este cifrado de extremo a extremo en el nivel del cloud. Los bloques de datos que se mueven al almacén de objetos en el cloud están protegidos con seguridad de la capa de transporte (TLS) v1.2 a fin de mantener la confidencialidad y la integridad de los datos entre los niveles de almacenamiento.

NetApp admite la comunicación con el almacén de objetos cloud mediante una conexión no cifrada, pero no la recomienda.

Cifrado de datos

El cifrado de datos es fundamental para la protección de la propiedad intelectual, la información comercial y la información personal del cliente. FabricPool es totalmente compatible tanto con el cifrado de volúmenes de NetApp (NVE) como con el cifrado del almacenamiento de NetApp (NSE) para mantener las estrategias de protección de datos existentes. Todos los datos cifrados en el nivel de rendimiento permanecen cifrados cuando se mueven al nivel de cloud. Las claves de cifrado en el cliente son propiedad de ONTAP, mientras que las claves de cifrado del almacén de objetos en el servidor son propiedad del almacén de objetos en cloud correspondiente. Los datos que no estén cifrados con NVE se cifran con el algoritmo AES-256-GCM. No se admiten otros cifrados AES-256.



El uso de NSE o NVE es opcional y no es obligatorio para utilizar FabricPool.

Requisitos de FabricPool

FabricPool requiere ONTAP 9.2 o posterior y el uso de agregados SSD en cualquiera de las plataformas indicadas en esta sección. Los requisitos adicionales de FabricPool dependen del nivel de cloud que se adjunto. En el caso de plataformas AFF de gama básica con una capacidad fija relativamente pequeña como AFF C190 de NetApp, FabricPool puede ser muy eficaz para mover datos inactivos al nivel de cloud.

Plataformas

FabricPool es compatible con las siguientes plataformas:

- AFF de NetApp
  - A800
  - A700S, A700
  - A320, A300
  - A220 Y A200
  - C190
  - AFF8080, AFF8060 Y AFF8040
- FAS de NetApp
  - FAS9000
  - FAS8200
  - FAS8080, FAS8060 Y FAS8040
  - FAS2750 Y FAS2720
  - FAS2650, FAS2620



Solo los agregados de SSD en las plataformas FAS pueden usar FabricPool.

- Niveles de cloud
  - Servicio de almacenamiento de objetos en cloud de Alibaba (estándar, acceso poco frecuente)
  - Amazon S3 (Estándar, Estándar - IA, One Zone-IA, Intelligent-Tiering)
  - Servicios de cloud comercial de Amazon (C2S)

- Almacenamiento en cloud de Google (Multi-Regional, Regional, Nearline, Coldline)
- Almacenamiento de objetos en cloud de IBM (estándar, almacén, almacén frío, Flex)
- Almacenamiento de Microsoft Azure Blob (Hot and Cool)

LIF de interconexión de clústeres

Los pares de alta disponibilidad en clúster que usan FabricPool requieren dos interfaces lógicas de interconexión de clústeres (LIF) para comunicarse con el nivel de cloud. NetApp recomienda crear una LIF de interconexión de clústeres en pares de alta disponibilidad adicionales para conectar los niveles de cloud sin problemas a agregados de esos nodos.

La LIF que ONTAP utiliza para conectarse con el almacén de objetos AWS S3 debe estar en un puerto de 10 Gbps.

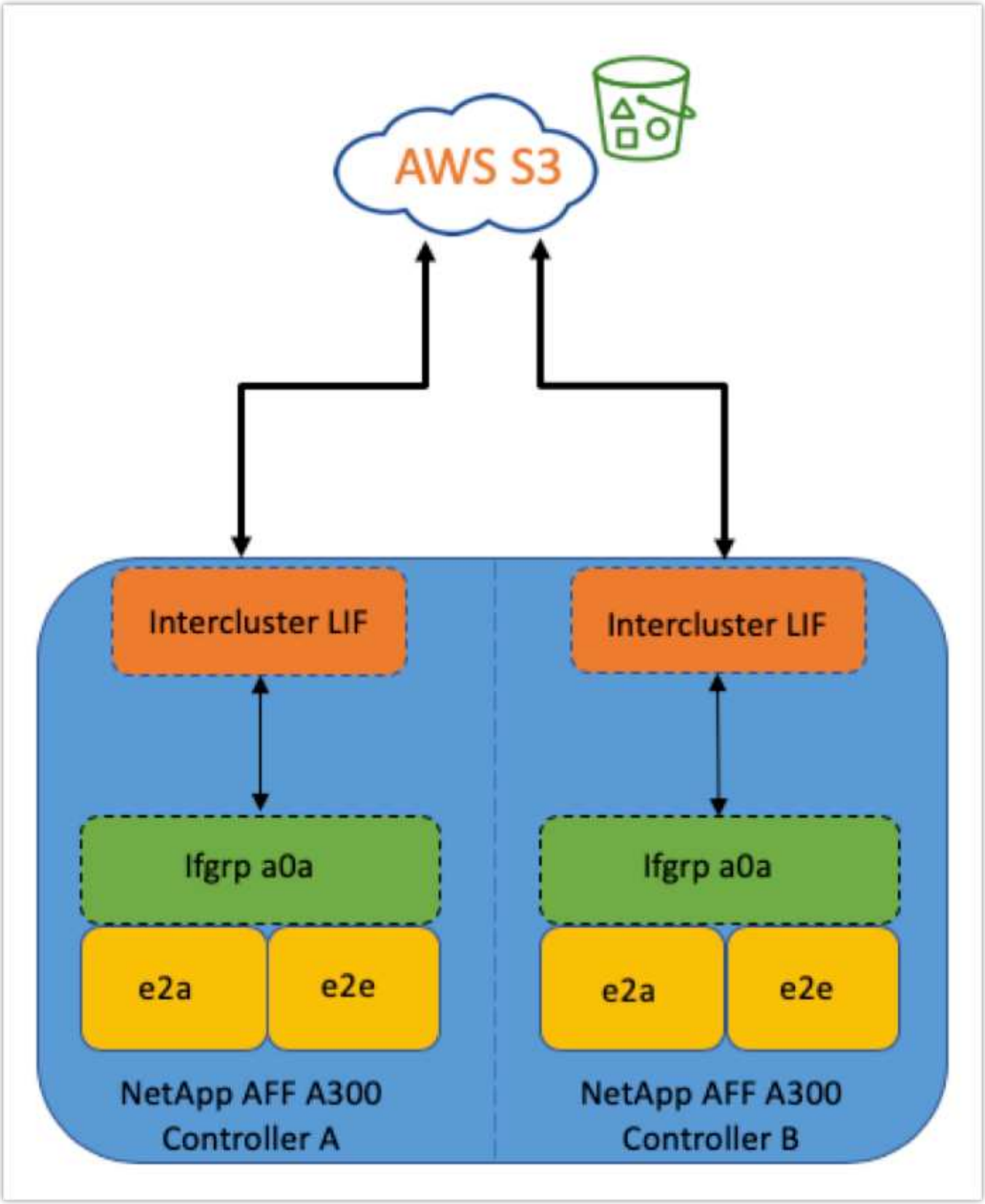
Si se utiliza más de una LIF Intercluser en un nodo con enrutamiento diferente, NetApp recomienda colocarlos en distintos espacios IP. Durante la configuración, FabricPool puede seleccionar entre varios espacios IP, pero no puede seleccionar LIF específicas de interconexión de clústeres dentro de un espacio IP.

Al deshabilitar o eliminar una LIF de interconexión de clústeres, se interrumpe la comunicación al nivel de cloud.

Conectividad

La latencia de lectura de FabricPool es una función de conectividad con el nivel de cloud. Las LIF de interconexión de clústeres mediante puertos de 10 Gbps, que se muestran en la siguiente figura, ofrecen un rendimiento adecuado. NetApp recomienda validar la latencia y el rendimiento del entorno de red específico para determinar el efecto que tiene en el rendimiento de la FabricPool.

Al utilizar FabricPool en entornos de bajo rendimiento, es necesario seguir cumpliendo los requisitos mínimos de rendimiento para las aplicaciones del cliente y ajustar los objetivos de tiempo de recuperación según corresponda.



Perfilador de almacén de objetos

El generador de perfiles de almacén de objetos, un ejemplo de lo cual se muestra a continuación y se encuentra disponible a través de la interfaz de línea de comandos de ONTAP, prueba la latencia y el rendimiento de los almacenes de objetos antes de adjuntarse a un agregado de FabricPool.

El nivel de cloud debe añadirse a ONTAP antes de que se pueda utilizar con el generador de perfiles de almacén de objetos.

Inicie el generador de perfiles del almacén de objetos desde el modo de privilegios avanzado de ONTAP con el siguiente comando:

```
storage aggregate object-store profiler start -object-store-name <name>
-node <name>
```

Para ver los resultados, ejecute el siguiente comando:

```
storage aggregate object-store profiler show
```

Los niveles de cloud no ofrecen un rendimiento similar al del nivel de rendimiento (normalmente GB por segundo). Aunque los agregados FabricPool pueden ofrecer un rendimiento similar al de SATA, también pueden tolerar latencias de hasta 10 segundos y un bajo rendimiento para soluciones de organización en niveles que no requieren un rendimiento similar al de SATA.

```
bb09-a300-2::*> storage aggregate object-store profiler show
Object store config name: aws_infra_fp_bk_1
Node name: bb09-a300-2-1
Status: Active. Issuing GETs
Start time: 10/3/2019 12:37:24

Op      Size       Total     Failed            Latency(ms)          Throughput
                                          min       max       avg
-------------------------------------------------------------------------------
PUT     4MB        1084      0         336       5951      2817       69.55MB
GET     4KB        158636    0         27        1132      41         32.22MB
GET     8KB        0         0         0         0         0          0B
GET     32KB       0         0         0         0         0          0B
GET     256KB      0         0         0         0         0          0B
5 entries were displayed.
```

Volúmenes

Thin provisioning de almacenamiento es una práctica estándar para el administrador de infraestructura virtual de FlexPod. Virtual Storage Console (VSC) de NetApp aprovisiona volúmenes de almacenamiento para almacenes de datos VMware sin garantía de espacio (thin provisioning) y con configuración de eficiencia del almacenamiento optimizada de acuerdo con las prácticas recomendadas de NetApp. Si se utiliza VSC para crear almacenes de datos de VMware, no es necesario realizar ninguna acción adicional, ya que no se debe asignar ninguna garantía de espacio al volumen de almacenes de datos.

FabricPool no puede asociar un nivel de cloud a un agregado que contenga volúmenes que utilicen una garantía de espacio distinta de ninguna (por ejemplo, volumen).

```
volume modify -space-guarantee none
```

Ajuste de `space-guarantee none` el parámetro proporciona thin provisioning para el volumen. La cantidad de espacio consumido por volúmenes con este tipo de garantía crece a medida que se añaden los datos en lugar de determinarse por un tamaño de volumen inicial. Este enfoque es esencial para FabricPool, ya que el volumen debe admitir datos en el nivel de cloud que se activan y vuelven a estar relacionados con el nivel de rendimiento.

Licencia

FabricPool requiere una licencia basada en capacidad cuando se unen proveedores de almacenamiento de objetos de terceros (como Amazon S3) como niveles de cloud para los sistemas flash híbridos AFF y FAS.

Las licencias de FabricPool están disponibles en formato perpetuo o basado en períodos (de 1 año o 3 años).

La organización en niveles en el nivel de cloud se detiene cuando la cantidad de datos (capacidad utilizada) almacenados en el nivel de cloud alcanza la capacidad con la licencia. Los datos adicionales, incluidas las copias SnapMirror en los volúmenes que utilizan la política de toda la organización en niveles, no se pueden organizar en niveles hasta que se aumente la capacidad de la licencia. Aunque la organización en niveles se detiene, aún se puede acceder a los datos desde el nivel de cloud. Los datos inactivos adicionales permanecen en las unidades SSD hasta que la capacidad con licencia aumenta.

Una licencia de FabricPool basada en un término de 10 TB de capacidad gratuita viene con la compra de un clúster nuevo de ONTAP 9.5 o posterior, si bien puede aplicarse un coste de soporte adicional. Las licencias FabricPool (incluida la capacidad adicional de las licencias existentes) se pueden adquirir en incrementos de 1 TB.

Una licencia de FabricPool solo se puede eliminar de un clúster que no contiene agregados de FabricPool.

> Las licencias de FabricPool son para todo el clúster. Debe tener el UUID disponible al comprar una licencia (`cluster identify show`). Si quiere información adicional sobre licencias, consulte "Base de conocimientos de NetApp".

Configuración

Revisiones de software

En la siguiente tabla se muestran las versiones validadas de software y hardware.

Capa	Dispositivo	Imagen	Comentarios
Reducida	AFF A300 de NetApp	ONTAP 9.6P2	
Informática	Servidores blade Cisco UCS B200 M5 con Cisco UCS VIC 1340	Versión 4.0(4b)	
Red	Interconexión de estructura Cisco Nexus 6332-16UP	Versión 4.0(4b)	
	Switch Cisco Nexus 93180YC-EX en el modo independiente de NX-OS	Versión 7.0(3)I7(6)	
Red de almacenamiento	Cisco MDS 9148S	Versión 8.3(2)	

Capa	Dispositivo	Imagen	Comentarios
Hipervisor		VMware vSphere ESXi 6.7U2	ESXi 6.7.0,13006603
		Servidor VMware vCenter	VCenter Server 6.7.0.30000, compilación 13639309
Proveedor de cloud		Amazon AWS S3	Bloque S3 estándar con opciones predeterminadas

Los requisitos básicos para FabricPool se describen en "Requisitos de FabricPool". Una vez cumplidos todos los requisitos básicos, complete los siguientes pasos para configurar FabricPool:

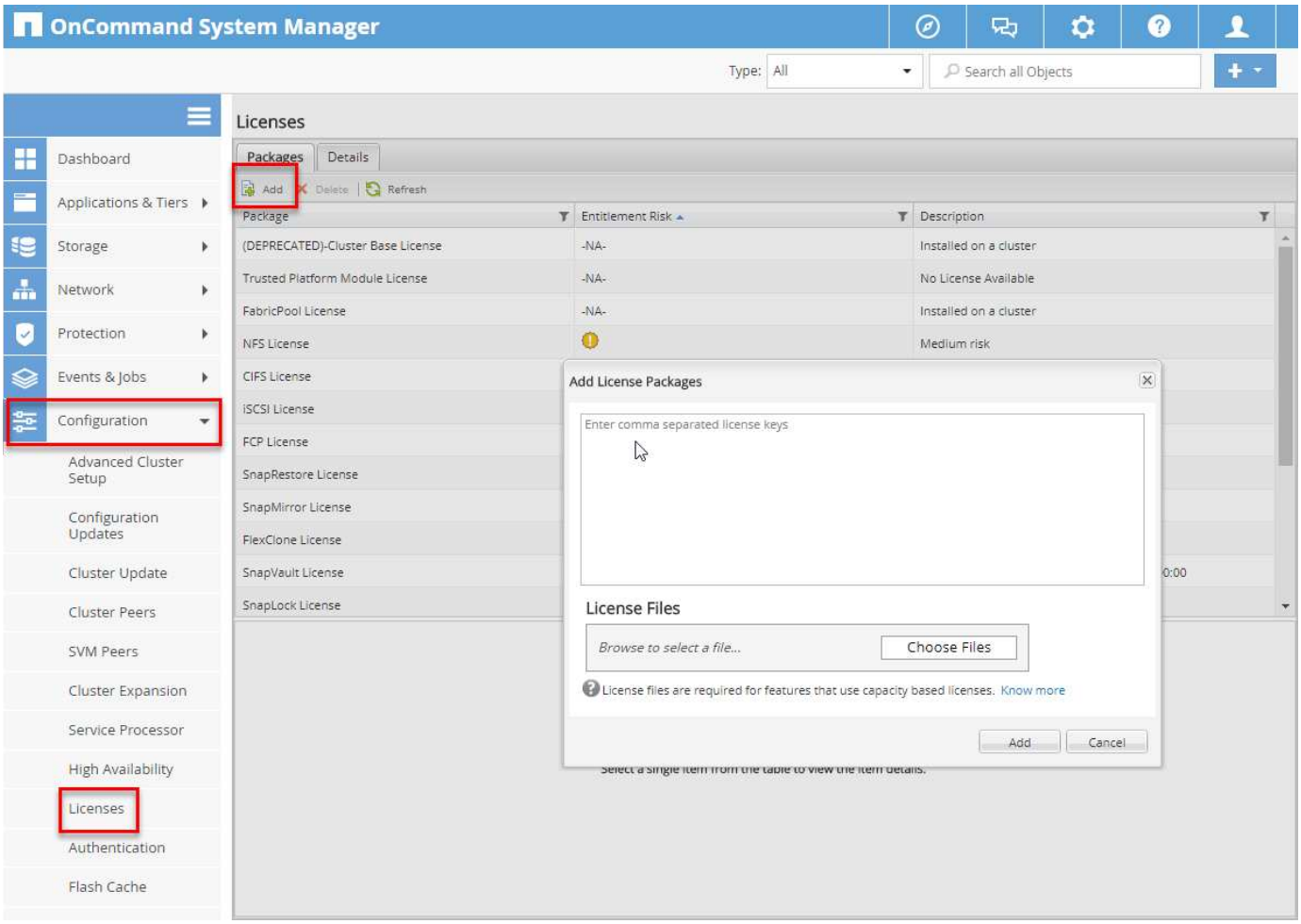
1. Instalar una licencia de FabricPool.
2. Cree un bloque de almacén de objetos AWS S3.
3. Añada un nivel de cloud a ONTAP.
4. Adjunte el nivel de cloud a un agregado.
5. Establezca la política de organización en niveles del volumen.

"Siguiente: Instale la licencia de FabricPool."

Instale la licencia de FabricPool

Después de adquirir un archivo de licencia de NetApp, puede instalarlo con OnCommand System Manager. Para instalar el archivo de licencia, lleve a cabo los siguientes pasos:

1. Haga clic en Configurations.
2. Haga clic en Cluster.
3. Haga clic en Licenses.
4. Haga clic en Añadir.
5. Haga clic en elegir archivos para examinar y seleccionar un archivo.
6. Haga clic en Añadir.



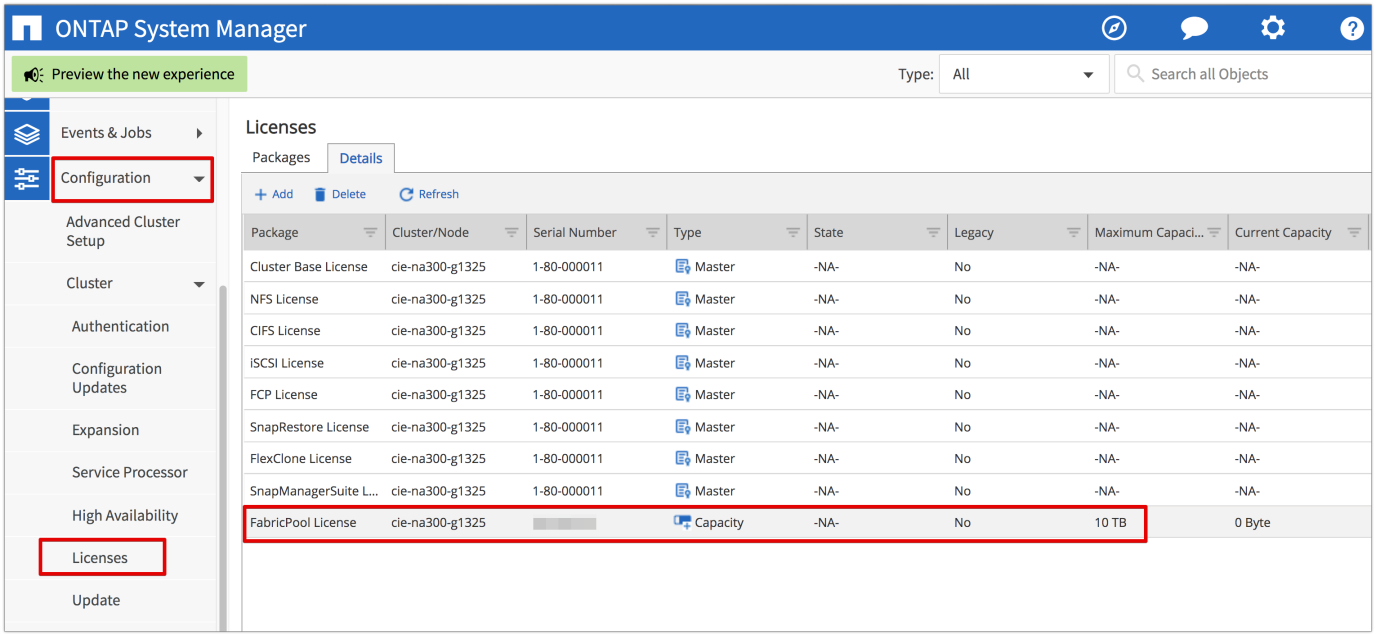
Capacidad de licencia

Es posible ver la capacidad de la licencia mediante la interfaz de línea de comandos de ONTAP o System Manager de OnCommand. Para ver la capacidad con licencia, ejecute el siguiente comando en la CLI de ONTAP:

```
system license show-status
```

En OnCommand System Manager, complete los siguientes pasos:

1. Haga clic en Configurations.
2. Haga clic en Licenses.
3. Haga clic en la pestaña Details.



La capacidad máxima y la capacidad actual se enumeran en la fila Licencia de FabricPool.

"Siguiente: Cree un bloque de AWS S3."

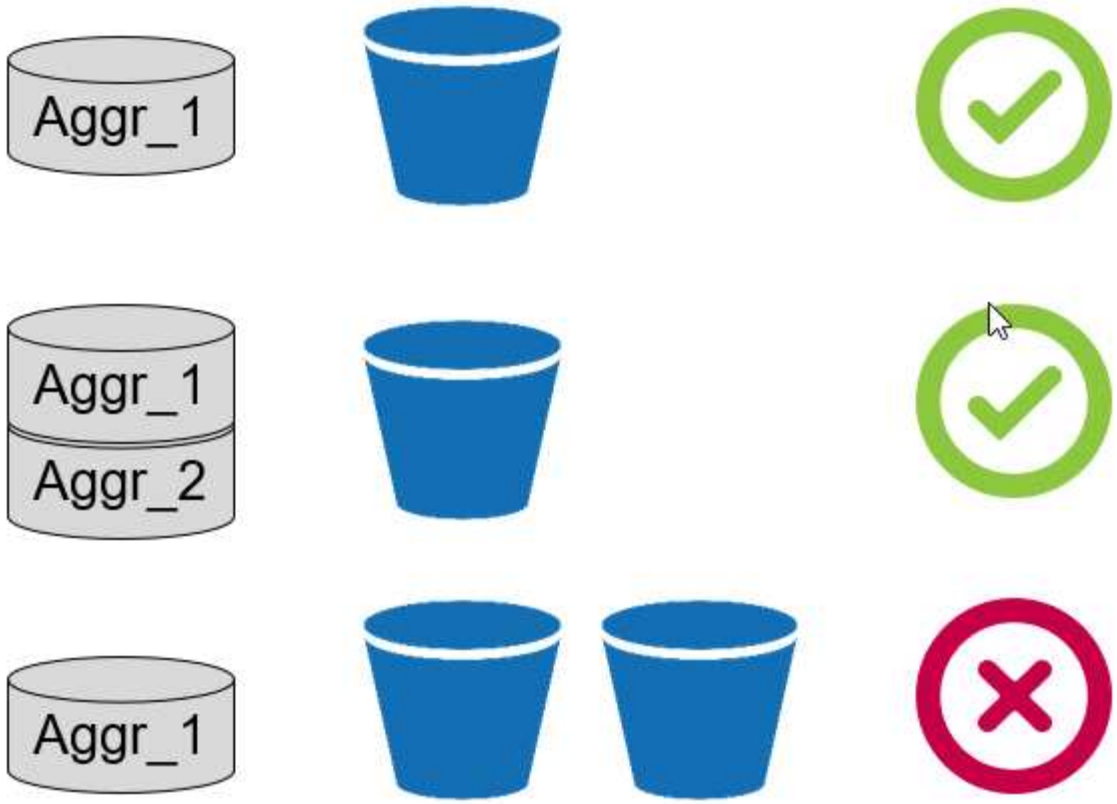
Cree el bloque de AWS S3

Los bloques son contenedores de almacenamiento de objetos que contienen datos. Debe proporcionar el nombre y la ubicación del bloque en el que se almacenan los datos antes de poder agregarse a un agregado como nivel de cloud.

Los bloques no se pueden crear usando System Manager de OnCommand, OnCommand Unified Manager ni ONTAP.

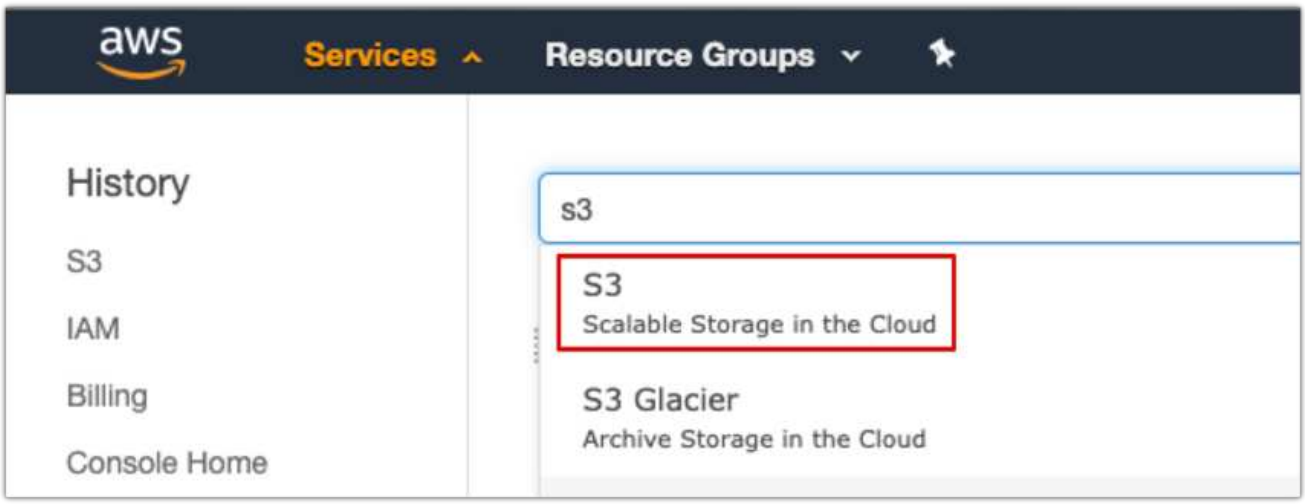
FabricPool admite la conexión de un bloque por agregado, como se muestra en la siguiente figura. Un único bloque se puede conectar a un único agregado, y un único bloque se puede vincular a varios agregados. Sin embargo, un solo agregado no se puede asociar a varios bloques. Aunque un único bloque se puede conectar a varios agregados de un clúster, NetApp no recomienda conectar un único bloque a agregados en varios clústeres.

Al planificar una arquitectura de almacenamiento, tenga en cuenta cómo la relación entre bloques y agregados puede afectar al rendimiento. Muchos proveedores de almacenes de objetos establecen un número máximo de IOPS admitidas a nivel de bloque o contenedor. Los entornos que requieren el máximo rendimiento deben utilizar varios bloques para reducir la posibilidad de que las limitaciones de IOPS del almacén de objetos puedan afectar al rendimiento en varios agregados de FabricPool. Añadir un único bloque o contenedor a todos los agregados de FabricPool de un clúster puede ser más beneficioso para los entornos que valoran la capacidad de gestión por el rendimiento en el nivel cloud.

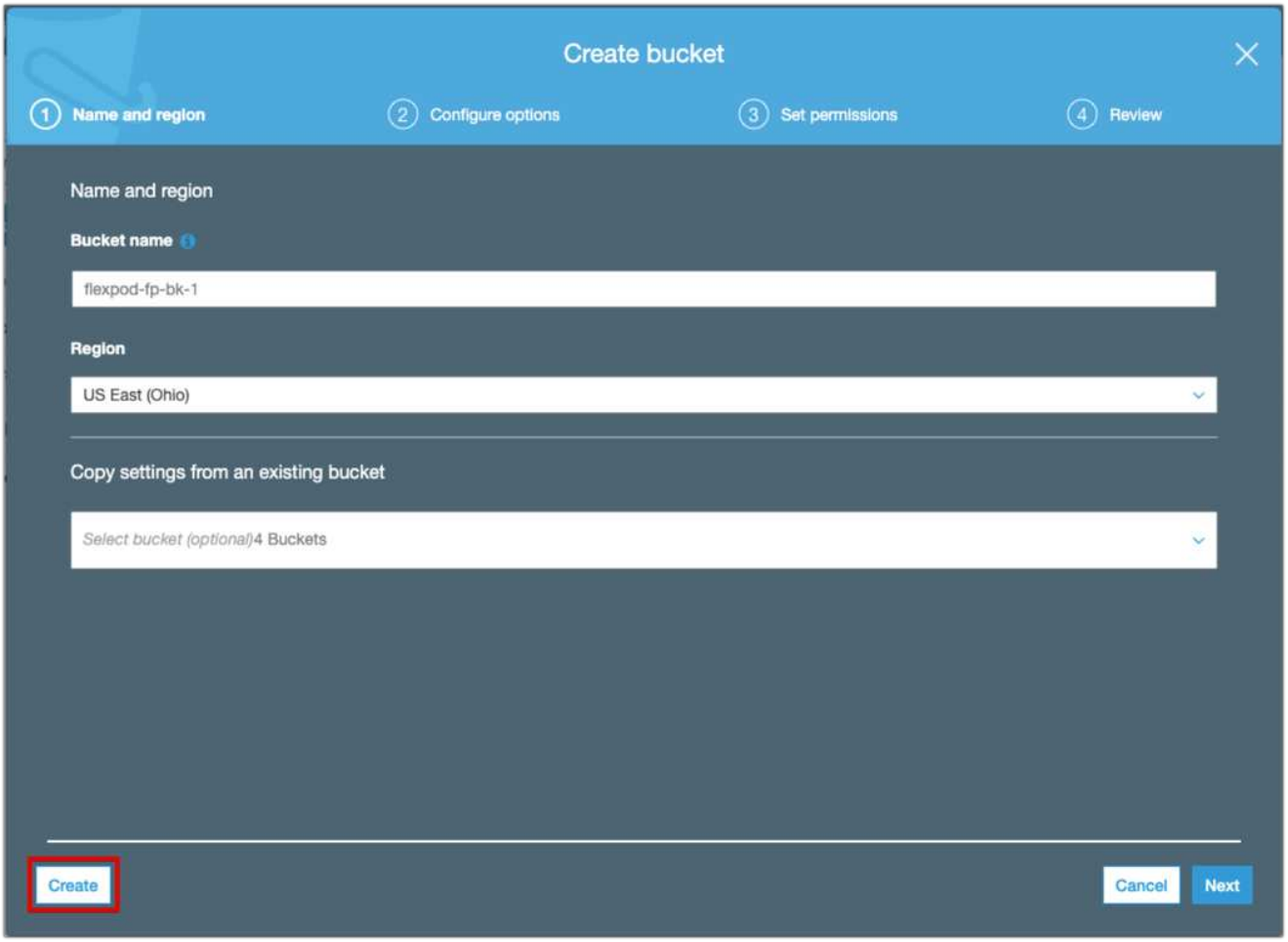


Cree un bloque de S3

1. En la consola de gestión de AWS desde la página de inicio, introduzca S3 en la barra de búsqueda.
2. Seleccione el almacenamiento escalable S3 en el cloud.



3. En la página de inicio de S3, seleccione Create Bucket.
4. Introduzca un nombre compatible con DNS y elija la región para crear el bloque.



5. Haga clic en Create para crear el bloque de almacenamiento de objetos.

"Siguiente: Añada un nivel de cloud a ONTAP"

Añada un nivel de cloud a ONTAP

Antes de que un almacén de objetos se pueda asociar a un agregado, ONTAP debe agregarlo e identificarlo. Esta tarea se puede completar tanto con OnCommand System Manager como con la interfaz de línea de comandos de ONTAP.

FabricPool admite Amazon S3, IBM Object Cloud Storage y almacenes de objetos de almacenamiento blob de Microsoft Azure como niveles de cloud.

Necesita la siguiente información:

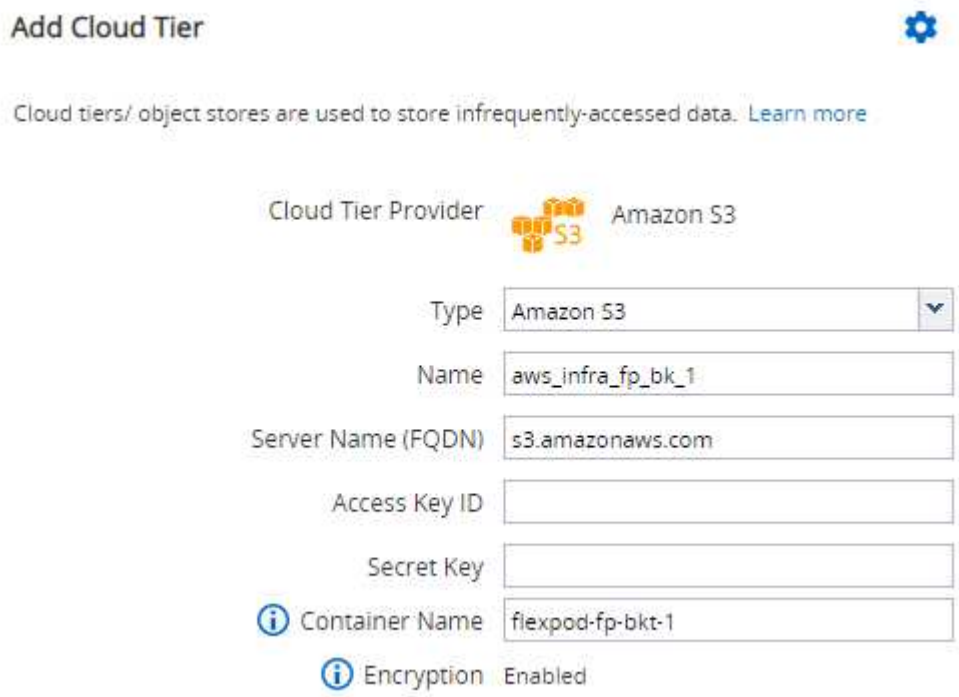
- Nombre del servidor (FQDN); por ejemplo, `s3.amazonaws.com`
- ID de clave de acceso
- Clave secreta
- Nombre de contenedor (nombre de bloque)

System Manager de OnCommand

Para añadir un nivel de cloud con System Manager de OnCommand, complete los siguientes pasos:

1. Inicie OnCommand System Manager.
2. Haga clic en Storage.
3. Haga clic en Aggregates & Disks.
4. Haga clic en Cloud Tiers.
5. Seleccione un proveedor de almacén de objetos.
6. Complete los campos de texto según sea necesario para el proveedor del almacén de objetos.

   En el campo Container Name, introduzca el nombre del contenedor o el bloque del almacén de objetos.
7. Haga clic en Save and Attach Aggregates.



CLI de ONTAP

Para añadir un nivel de cloud con la interfaz de línea de comandos de ONTAP, escriba los siguientes comandos:

```
object-store config create
-object-store-name <name>
-provider-type <AWS>
-port <443/8082> (AWS)
-server <name>
-container-name <bucket-name>
-access-key <string>
-secret-password <string>
-ssl-enabled true
-ipspace default
```

"Siguiente: Adjunte un nivel de cloud a un agregado de ONTAP."

Adjuntar un nivel de cloud a un agregado de ONTAP

Después de que ONTAP haya añadido e identificado un almacén de objetos, se debe vincular a un agregado para crear una FabricPool. Esta tarea se puede completar mediante OnCommand System Manager o la interfaz de línea de comandos de ONTAP.

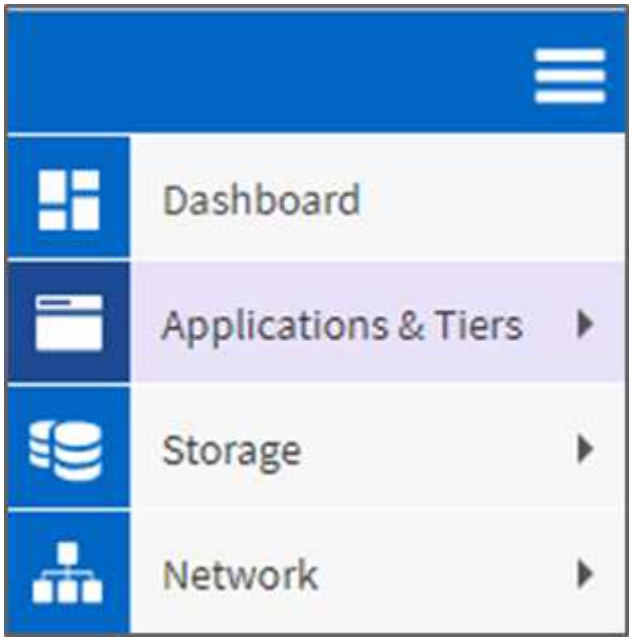
Se puede conectar más de un tipo de almacén de objetos a un clúster, pero solo se puede asociar un tipo de almacén de objetos a cada agregado. Por ejemplo, un agregado puede usar Google Cloud y otro agregado puede usar Amazon S3, pero no se puede vincular un agregado a ambos.

Añadir un nivel de cloud a un agregado es una acción permanente. Un nivel de cloud no se puede desvincular de un agregado al que se haya adjuntado.

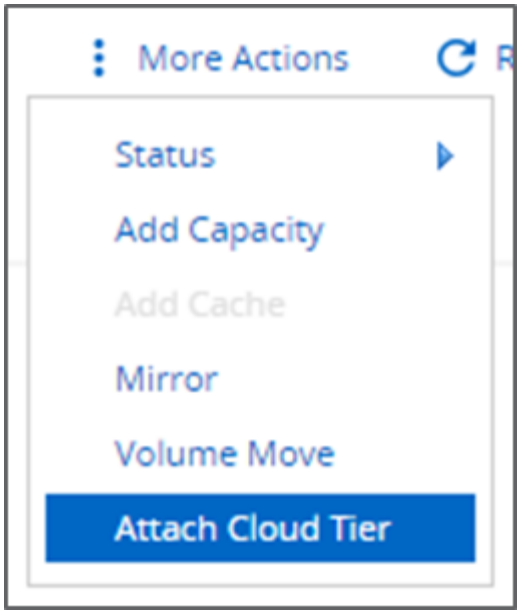
System Manager de OnCommand

Para adjuntar un nivel de cloud a un agregado mediante System Manager de OnCommand, realice los siguientes pasos:

1. Inicie OnCommand System Manager.
2. Haga clic en aplicaciones y niveles.



3. Haga clic en Storage Tiers.
4. Haga clic en un agregado.
5. Haga clic en Actions y seleccione Attach Cloud Tier.



6. Seleccione un nivel de cloud.
7. Consulte y actualice las políticas de organización en niveles de los volúmenes en el agregado (opcional). De forma predeterminada, la política de organización en niveles del volumen se establece como solo Snapshot.
8. Haga clic en Guardar.

CLI de ONTAP

Para adjuntar un nivel de cloud a un agregado mediante la interfaz de línea de comandos de ONTAP, ejecute los siguientes comandos:

```
storage aggregate object-store attach
-aggregate <name>
-object-store-name <name>
```

Ejemplo:

```
storage aggregate object-store attach -aggregate aggr1 -object-store-name
- aws_infra_fp_bk_1
```

"Siguiente: Defina la política de organización en niveles del volumen."

Establezca la política de organización en niveles del volumen

De forma predeterminada, los volúmenes usan la política de organización en niveles None volume. Tras la creación del volumen, la política de organización en niveles del volumen se puede cambiar mediante el Administrador del sistema de OnCommand o la interfaz de línea de comandos de ONTAP.

Cuando se utiliza con FlexPod, FabricPool proporciona tres políticas de organización en niveles de

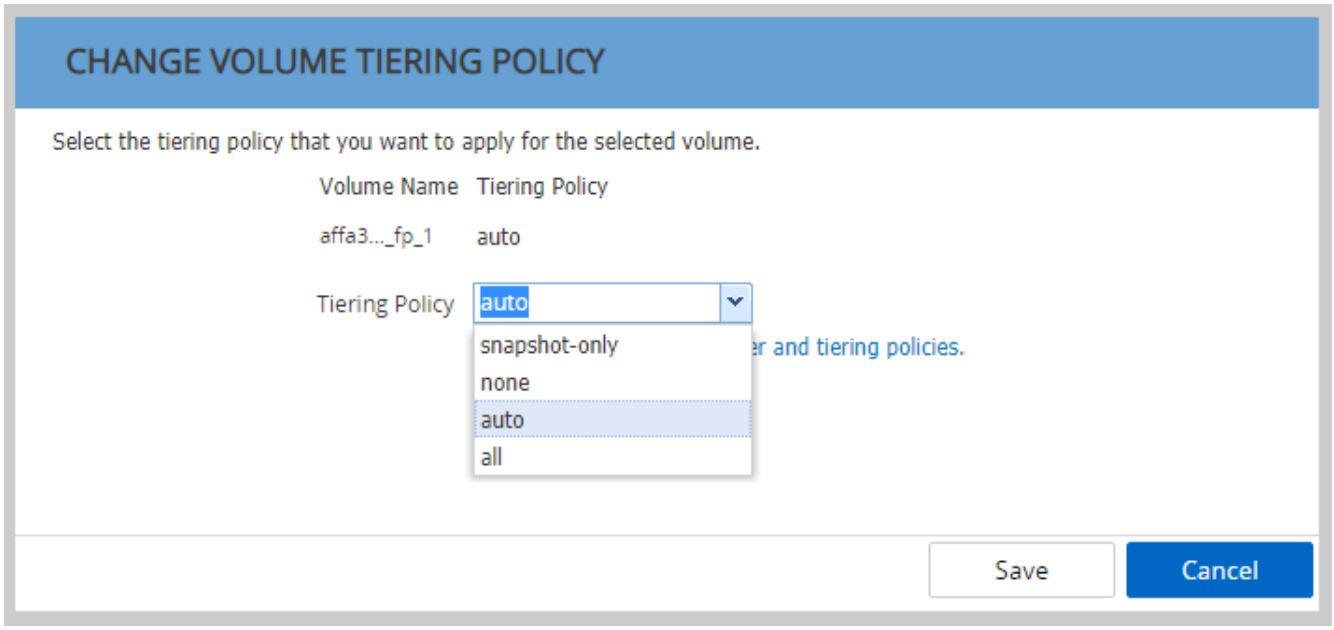
volúmenes, Auto, Snapshot-only y None.

- **Auto**
  - Todos los bloques de datos fríos del volumen se mueven al nivel de cloud. Suponiendo que se utiliza el agregado más del 50%, se necesitan aproximadamente 31 días para que los bloques inactivos queden inactivos. El período de enfriamiento automático se puede ajustar entre 2 días y 63 días mediante el uso del `tiering-minimum-cooling-days` ajuste.
  - Cuando los bloques inactivos de un volumen con una política de organización en niveles configurada en Auto se leen de forma aleatoria, se realizan en caliente y se escriben en el nivel de rendimiento.
  - Cuando los bloques inactivos de un volumen con una política de organización en niveles configurada como Auto se leen de forma secuencial, permanecen inactivos y permanecen en el nivel del cloud. No se escriben en el nivel de rendimiento.
- **Sólo instantánea**
  - Los bloques de instantáneas frías en el volumen que no están compartidos con el sistema de archivos activo se mueven al nivel de cloud. Si asumimos que el agregado está más del 50% utilizado, se tarda aproximadamente 2 días en que los bloques snapshot inactivos permanezcan inactivos. El período de refrigeración solo de Snapshot puede ajustarse de 2 a 63 días con la `tiering-minimum-cooling-days` ajuste.
  - Cuando se leen bloques inactivos de un volumen con una política de organización en niveles establecida en Snapshot únicamente, se realizan caliente y se escriben en el nivel de rendimiento.
- **Ninguno (predeterminado)**
  - Los volúmenes establecidos para usar None, ya que su política de organización en niveles no organiza los datos inactivos en el nivel de cloud.
  - Si se configura la política de organización en niveles en None, se evitará la nueva organización en niveles.
  - Los datos de volumen que se han movido anteriormente al nivel de cloud permanecen en el nivel de cloud hasta que se activan y se vuelven a mover automáticamente al nivel de rendimiento.

System Manager de OnCommand

Para cambiar la política de organización en niveles de un volumen mediante el Administrador del sistema de OnCommand, lleve a cabo los siguientes pasos:

1. Inicie OnCommand System Manager.
2. Seleccionar un volumen.
3. Haga clic en más acciones y seleccione Change Tiering Policy.
4. Seleccione la política de organización en niveles que se aplicará al volumen.
5. Haga clic en Guardar.



CLI de ONTAP

Para cambiar la política de organización en niveles de un volumen mediante la interfaz de línea de comandos de ONTAP, ejecute el siguiente comando:

```
volume modify -vserver <svm_name> -volume <volume_name>
-tiering-policy <auto|snapshot-only|all|none>
```

"Siguiente: Defina los días de enfriamiento mínimos de organización en niveles de volumen."

Establezca los días de enfriamiento mínimos de organización en niveles de volumen

La `tiering-minimum-cooling-days` La configuración determina cuántos días deben pasar antes de que los datos inactivos de un volumen con la política solo de copias Snapshot se consideren inactivos y sean aptos para la organización en niveles.

Automático

El valor predeterminado `tiering-minimum-cooling-days` La configuración de la política de organización automática en niveles es de 31 días.

Como las lecturas mantienen las temperaturas de bloque activas, aumentar este valor puede reducir la cantidad de datos elegibles para la organización en niveles y aumentar la cantidad de datos mantenidos en el nivel de rendimiento.

Si desea reducir este valor desde los 31 días predeterminados, tenga en cuenta que los datos no deben estar activos antes de que se marquen como inactivos. Por ejemplo, si se espera que una carga de trabajo de varios días realice un número significativo de escrituras el día 7, el volumen `tiering-minimum-cooling-days` el ajuste no debe ser inferior a 8 días.

El almacenamiento de objetos no es transaccional, como el almacenamiento de archivos o bloques. La realización de cambios en los archivos que se almacenan como objetos en volúmenes con días mínimos de refrigeración excesivamente agresivos puede provocar la creación de nuevos objetos, la fragmentación de los objetos existentes y la adición de ineficiencias del almacenamiento.

Solo Snapshot

El valor predeterminado `tiering-minimum-cooling-days` La configuración de la política de organización en niveles solo de Snapshot es de 2 días. Un mínimo de 2 días da tiempo adicional a los procesos en segundo plano para proporcionar la máxima eficiencia del almacenamiento y evita que los procesos diarios de protección de datos tengan que leer datos del nivel de cloud.

CLI de ONTAP

Para cambiar el volumen `tiering-minimum-cooling-days` Si configura mediante la CLI de ONTAP, ejecute el siguiente comando:

```
volume modify -vserver <svm_name> -volume <volume_name> -tiering-minimum
-cooling-days <2-63>
```

Se requiere el nivel de privilegio avanzado.

Al cambiar la política de organización en niveles entre Auto y Snapshot-only (o viceversa), se restablece el período de inactividad de los bloques en el nivel de rendimiento. Por ejemplo, un volumen que utilice la política de organización en niveles automática de volumen con los datos en el nivel de rendimiento que ha estado inactivo durante 20 días tendrá la inactividad de los datos en el nivel de rendimiento se restablecerá a 0 días si la política de organización en niveles se establece en solo Snapshot.

Consideraciones de rendimiento

Configure el nivel de rendimiento

Al realizar un dimensionamiento, tenga en cuenta que el nivel de rendimiento debe ser capaz de realizar las siguientes tareas:

- Respaldar los datos activos
- Al admitir datos inactivos hasta que el análisis de organización en niveles mueve los datos al nivel de cloud
- Da soporte a los datos del nivel cloud que se activan y se vuelven a escribir en el nivel de rendimiento
- Compatibilidad con metadatos de WAFL asociados con el nivel de cloud conectado

Para la mayoría de los entornos, una tasa de rendimiento y capacidad de 1:10 en agregados de FabricPool es extremadamente conservadora, al tiempo que ofrece un ahorro significativo en almacenamiento. Por ejemplo, si el objetivo es establecer un nivel de 200 TB en el nivel de cloud, el agregado del nivel de rendimiento debería tener como mínimo 20 TB.

Las escrituras del nivel de cloud al nivel de rendimiento se deshabilitan si la capacidad del nivel de rendimiento es superior al 70 %. Si esto ocurre, los bloques se leen directamente desde el nivel de cloud.

Configure el nivel de cloud

A la hora de ajustar el tamaño, el almacén de objetos que actúe como nivel de cloud debe poder realizar las siguientes tareas:

- Admite lecturas de datos inactivos existentes
- Compatibilidad con escrituras de nuevos datos fríos
- Compatibilidad con la eliminación y desfragmentación de objetos

Coste de propiedad

La "Calculadora de economía de FabricPool" Está disponible a través de la empresa independiente de analistas TECNOLÓGICOS, Evaluator Group, que ayuda a proyectar los ahorros en costes entre las instalaciones y el cloud para el almacenamiento de datos inactivos. La calculadora ofrece una interfaz sencilla para determinar el coste de almacenar datos a los que se accede con poca frecuencia en un nivel de rendimiento en lugar de enviarlos a un nivel de cloud durante el resto del ciclo de vida de los datos. Según un cálculo de 5 años, se utilizan los cuatro factores clave (capacidad de origen, crecimiento de datos, capacidad de snapshot y porcentaje de datos inactivos) para determinar los costes de almacenamiento a lo largo del periodo de tiempo.

Conclusión

La transición a la infraestructura en nube varía entre organizaciones, entre unidades de negocio e, incluso, entre unidades de negocio de las organizaciones. Algunos eligen una adopción rápida, mientras que otros prefieren una estrategia más conservadora. FabricPool encaja en la estrategia cloud de las organizaciones independientemente de su tamaño y de la velocidad de adopción del cloud, lo que demuestra aún más los beneficios de eficiencia y escalabilidad de una infraestructura de FlexPod.

Dónde encontrar información adicional

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

- Prácticas recomendadas de FabricPool

  "www.netapp.com/us/media/tr-4598.pdf"

- Documentación de productos de NetApp

  "https://docs.netapp.com"

- TR-4036: Especificaciones técnicas del centro de datos de FlexPod

"https://www.netapp.com/us/media/tr-4036.pdf"

FlexPod Datacenter para cloud híbrido con CloudCenter de Cisco y almacenamiento privado de NetApp - Diseño

Haseeb Niazi, Cisco David Arnette, NetApp

Los diseños validados por Cisco (CVD) proporcionan sistemas y soluciones diseñados, probados y documentados para facilitar y mejorar las puestas en marcha de los clientes. Estos diseños incorporan una amplia gama de tecnologías y productos en una cartera de soluciones que se han desarrollado para responder a las necesidades empresariales de los clientes y para guiarlos desde el diseño hasta la puesta en marcha.

"FlexPod Datacenter para cloud híbrido con CloudCenter de Cisco y almacenamiento privado de NetApp - Diseño"

Bases de datos empresariales

SAP

Introducción a SAP en FlexPod

La plataforma FlexPod es una arquitectura de centro de datos prediseñada con las mejores prácticas que se basa en Cisco Unified Computing System (Cisco UCS), la familia de switches Cisco Nexus y las controladoras de almacenamiento de NetApp.

FlexPod es una plataforma adecuada para ejecutar aplicaciones SAP, y las soluciones que se proporcionan aquí le permiten poner en marcha SAP HANA de forma rápida y fiable con un modelo de integración personalizada de centro de datos. FlexPod ofrece no solo una configuración básica, sino también la flexibilidad necesaria para ajustar el tamaño y optimizarse con el objetivo de acomodar distintos casos de uso y requisitos.

FlexPod Datacenter para una solución SAP mediante FibreChannel SAN con Cisco UCS Manager 4,0 y NetApp ONTAP 9,7

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Este documento describe Cisco y FlexPod Datacenter de NetApp con ONTAP 9,7 de NetApp en el almacenamiento AFF A400 de NetApp y el software unificado Cisco UCS Manager, versión 4,1(1) con procesadores escalables Intel Xeon de segunda generación para SAP HANA.

FlexPod Datacenter con NetApp ONTAP 9,7 y la versión unificada del software Cisco UCS 4,1 (1) es una arquitectura de centro de datos con mejores prácticas prediseñada desarrollada desarrollada en el sistema Cisco Unified Computing System (Cisco UCS), la familia de switches Cisco Nexus 9000, switches estructurales multicapa MDS 9000, Asimismo, las cabinas de almacenamiento AFF A-Series de NetApp que ejecutan el sistema operativo de almacenamiento 9,7 de ONTAP.

"FlexPod Datacenter para una solución SAP mediante FibreChannel SAN con Cisco UCS Manager 4,0 y NetApp ONTAP 9,7"

White paper SAP no HANA con SQL: Diseño

El sector de LA TECNOLOGÍA actual está siendo testigo de una transformación espectacular en las soluciones de centros de datos. En los últimos años se ha producido un interés considerable en las soluciones de centros de datos prevalidadas y diseñadas. La introducción de la tecnología de virtualización en áreas críticas ha tenido un gran impacto en los principios de diseño y en la arquitectura de estas soluciones. Ha permitido que muchas aplicaciones se ejecuten en sistemas de configuración básica migren a nuevas soluciones virtualizadas integradas. FlexPod es una solución de centro de datos validada previamente y diseñada para responder a las necesidades que cambian rápidamente los departamentos DE TECNOLOGÍA. Cisco y NetApp se han asociado para proporcionar FlexPod, que utiliza componentes informáticos, de redes y almacenamiento de excelente calidad como base para diversas cargas de trabajo empresariales, incluidas bases de datos, planificación de recursos empresariales (ERP),

gestión de relaciones con el cliente (CRM) y aplicaciones web.

La consolidación de las aplicaciones DE TI, en particular las bases de datos, ha generado un interés considerable en los últimos años. La plataforma de bases de datos más adoptada e instalada en los últimos años es Microsoft SQL Server. Las bases de datos de SQL Server con frecuencia se han convertido en sujetos al aumento descontrolado de las bases de datos, lo cual lleva a retos de TI, como servidores infrautilizados, licencias incorrectas, problemas de seguridad, preocupaciones de gestión y enormes costes operativos. Por lo tanto, las bases de datos de SQL Server son buenas candidatas para la consolidación en una plataforma más sólida, flexible y resiliente. Este documento describe la arquitectura de referencia de FlexPod para desplegar y consolidar bases de datos SQL Server.

"White paper SAP no HANA con SQL: Diseño"

FlexPod Datacenter para solución SAP con la estructura de tercera generación de Cisco UCS y NetApp AFF A-Series

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Este documento describe la metodología de puesta en marcha de Cisco y FlexPod Datacenter de NetApp para SAP HANA basado en los procesadores escalables Intel Xeon de segunda generación compatibles con Cisco UCS Computing System (Cisco UCS).

Cisco UCS Manager (UCSM) 4,0(4) proporciona soporte consolidado de todos los modelos actuales de interconexión de estructura de Cisco UCS (6200, 6300, 6324 y 6454), IOM de la serie 2200/2300, blade Cisco UCS B-Series y servidores de factor de forma en rack Cisco UCS C-Series. FlexPod Datacenter con la versión unificada del software Cisco UCS 4,0 (4D) y ONTAP 9,6 de NetApp, es una arquitectura de centro de datos prediseñada con mejores prácticas basada en Cisco UCS, la familia de switches Cisco Nexus 9000 y cabinas de almacenamiento AFF A-Series de NetApp.

"FlexPod Datacenter para solución SAP con Cisco UCS estructura de tercera generación y NetApp AFF A-Series"

FlexPod Datacenter para la solución SAP mediante FibreChannel SAN con Cisco UCS Manager 4,0 y NetApp ONTAP 9,7: Diseño

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Cisco y NetApp se han asociado para ofrecer una serie de soluciones FlexPod que permiten crear plataformas estratégicas de centros de datos. La solución FlexPod proporciona una arquitectura integrada que incorpora prácticas recomendadas de diseño de red, informática y almacenamiento, por lo que minimiza los riesgos RELACIONADOS CON la TECNOLOGÍA mediante la validación de la arquitectura integrada para garantizar la compatibilidad entre los diferentes componentes. La solución también soluciona los problemas DE TI al proporcionar indicaciones de diseño documentadas, directrices para la puesta en marcha y soporte que puede utilizarse en varias etapas (planificación, diseño e implementación) de una implementación.

"FlexPod Datacenter para la solución SAP mediante FibreChannel SAN con Cisco UCS Manager 4,0 y NetApp ONTAP 9,7: Diseño"

Solución FlexPod Datacenter para SAP con Cisco ACI, Cisco UCS Manager 4,0 y AFF A-Series de NetApp: Diseño

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Este documento describe la solución FlexPod integrada de Cisco ACI como enfoque validado para la puesta en marcha de entornos de integración personalizada del centro de datos (TDI) de SAP HANA. Este diseño validado proporciona directrices y un marco para implementar SAP HANA con prácticas recomendadas de Cisco y NetApp.

La arquitectura de la solución recomendada se basa en Cisco Unified Computing System (Cisco UCS) mediante una versión de software unificada para admitir las plataformas de hardware de Cisco UCS que incluyen los siguientes componentes:

- Los servidores blade Cisco UCS B-Series y los servidores en rack Cisco UCS C-Series configurables con la opción Intel Optane Data Center Persistent Memory Module (DCPMM)
- Interconexiones de estructuras Cisco UCS de la serie 6400
- Switches troncales y Cisco Nexus serie 9000
- Cabinas de almacenamiento All Flash Series de NetApp

Además, este documento proporciona validaciones tanto para Red Hat Enterprise Linux como para SUSE Linux Enterprise Server para SAP HANA.

"Solución FlexPod Datacenter para SAP con Cisco ACI, Cisco UCS Manager 4,0 y AFF A-Series de NetApp: Diseño"

FlexPod Datacenter para SAP con Cisco ACI, Cisco UCS Manager 4,0 y AFF A-Series de NetApp: Puesta en marcha

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

En este documento se describen los procedimientos de arquitectura y puesta en marcha para la opción de integración personalizada del centro de datos de SAP HANA en la infraestructura de FlexPod, la cual consta de:

- Cisco UCS Computing System (Cisco UCS) compatible con procesadores escalables Intel Xeon de segunda generación.
- Cambiar productos que aprovechan la infraestructura centrada en aplicaciones (ACI) de Cisco.
- Cabinas AFF A-Series de NetApp.

El objetivo de este documento es mostrar los pasos de configuración detallados para la implementación de SAP HANA

"FlexPod Datacenter para SAP con Cisco ACI, Cisco UCS Manager 4,0 y AFF A-Series de NetApp: Puesta en marcha"

FlexPod Datacenter para la solución SAP con Cisco UCS Manager 4,0 y NetApp AFF A–Series: Diseño

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Este documento describe la solución FlexPod de Cisco y NetApp, la cual es un enfoque validado para la puesta en marcha de entornos de integración personalizada del centro de datos (TDI) de SAP HANA. Este diseño validado proporciona directrices y un marco para implementar SAP HANA con prácticas recomendadas de Cisco y NetApp.

FlexPod es una infraestructura integrada líder que admite una amplia gama de cargas de trabajo empresariales y casos prácticos. Esta solución le permite poner en marcha SAP HANA de forma rápida y fiable con un modelo de modo de integración de centro de datos personalizado.

"FlexPod Datacenter para la solución SAP con Cisco UCS Manager 4,0 y NetApp AFF A–Series: Diseño"

FlexPod Datacenter para la solución SAP con Cisco ACI en servidores Cisco UCS M5 con SLES 12 SP3 y RHEL 7,4

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

En este documento se describen los procedimientos de arquitectura y puesta en marcha para la opción de integración personalizada del centro de datos de SAP HANA en la infraestructura de FlexPod compuesta por productos de computación y switch de Cisco que aprovechan la infraestructura centrada en aplicaciones (ACI) de Cisco, la solución de redes definidas por software (SDN) líder del sector, junto con las cabinas AFF A-Series de NetApp. El objetivo de este documento es mostrar los principios de diseño con los pasos de configuración detallados para la instalación de SAP HANA.

"FlexPod Datacenter para la solución SAP con Cisco ACI en servidores Cisco UCS M5 con SLES 12 SP3 y RHEL 7,4"

FlexPod Datacenter para la solución SAP con almacenamiento basado en IP usando AFF A-Series de NetApp y Cisco UCS Manager 3,2

Shailendra Mruthunjaya, Cisco Ralf Klahr, Cisco Marco Schoen, NetApp

La arquitectura de referencia detallada en este documento destaca la flexibilidad, el beneficio económico y la facilidad de instalación de una solución de almacenamiento basada en IP. Un sistema de almacenamiento capaz de ofrecer varios protocolos en una única interfaz permite a los clientes elegir y proteger la inversión, ya que es una arquitectura realmente única. La solución está diseñada para alojar cargas de trabajo SAP HANA escalables.

"FlexPod Datacenter para la solución SAP con almacenamiento basado en IP usando AFF A-Series de NetApp y Cisco UCS Manager 3,2"

FlexPod Datacenter para una solución SAP mediante FibreChannel SAN con Cisco UCS Manager 4,0 y NetApp ONTAP 9,7

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Este documento describe Cisco y FlexPod Datacenter de NetApp con ONTAP 9,7 de NetApp en el almacenamiento AFF A400 de NetApp y el software unificado Cisco UCS

Manager, versión 4,1(1) con procesadores escalables Intel Xeon de segunda generación para SAP HANA.

FlexPod Datacenter con NetApp ONTAP 9,7 y la versión unificada del software Cisco UCS 4,1 (1) es una arquitectura de centro de datos con mejores prácticas prediseñada desarrollada desarrollada en el sistema Cisco Unified Computing System (Cisco UCS), la familia de switches Cisco Nexus 9000, switches estructurales multicapa MDS 9000, Asimismo, las cabinas de almacenamiento AFF A-Series de NetApp que ejecutan el sistema operativo de almacenamiento 9,7 de ONTAP.

"FlexPod Datacenter para una solución SAP mediante FibreChannel SAN con Cisco UCS Manager 4,0 y NetApp ONTAP 9,7"

Pon en marcha servidores de aplicaciones SAP en FlexPod con SQL

FlexPod es una solución de centro de datos prevalidada y diseñada para responder a los rápidos cambios en las necesidades de los departamentos DE TECNOLOGÍA. Cisco y NetApp se han asociado para proporcionar FlexPod, que utiliza los mejores componentes informáticos, de redes y almacenamiento como base para diversas cargas de trabajo empresariales, como bases de datos, planificación de recursos empresariales (ERP), gestión de relaciones con los clientes (CRM) y aplicaciones web. La consolidación de las aplicaciones DE TI, en particular las bases de datos, ha generado un interés considerable en los últimos años. La plataforma de bases de datos más adoptada e instalada en los últimos años es Microsoft SQL Server. Las bases de datos de SQL Server con frecuencia se han convertido en sujetos al aumento descontrolado de las bases de datos, lo cual lleva a retos de TI, como servidores infrautilizados, licencias incorrectas, problemas de seguridad, preocupaciones de gestión y enormes costes operativos. Por lo tanto, las bases de datos de SQL Server son buenas candidatas para la consolidación en una plataforma más sólida, flexible y resiliente. Este documento describe la arquitectura de referencia de FlexPod para desplegar y consolidar bases de datos SQL Server.

"Pon en marcha servidores de aplicaciones SAP en FlexPod con SQL"

FlexPod Datacenter para SAP con Cisco ACI, Cisco UCS Manager 4,0 y AFF A-Series de NetApp

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

En este documento se describen los procedimientos de arquitectura y puesta en marcha para la opción de integración personalizada del centro de datos de SAP HANA en la infraestructura de FlexPod, la cual consta de:

- Cisco UCS Computing System (Cisco UCS) compatible con procesadores escalables Intel Xeon de segunda generación.
- Cambiar productos que aprovechan la infraestructura centrada en aplicaciones (ACI) de Cisco.
- Cabinas AFF A-Series de NetApp.

"FlexPod Datacenter para SAP con Cisco ACI, Cisco UCS Manager 4,0 y AFF A-Series de NetApp"

Solución FlexPod Datacenter para SAP con Cisco ACI, Cisco UCS Manager 4,0 y AFF A-Series de NetApp: Diseño

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Este documento describe la solución FlexPod integrada de Cisco ACI como enfoque validado para la puesta en marcha de entornos de integración personalizada del centro de datos (TDI) de SAP HANA. Este diseño validado proporciona directrices y un marco para implementar SAP HANA con prácticas recomendadas de Cisco y NetApp.

La arquitectura de la solución recomendada se basa en Cisco Unified Computing System (Cisco UCS) mediante una versión de software unificada para admitir las plataformas de hardware de Cisco UCS que incluyen los siguientes componentes:

- Los servidores blade Cisco UCS B-Series y los servidores en rack Cisco UCS C-Series configurables con la opción Intel Optane Data Center Persistent Memory Module (DCPMM)
- Interconexiones de estructuras Cisco UCS de la serie 6400
- Switches troncales y Cisco Nexus serie 9000
- Cabinas de almacenamiento All Flash Series de NetApp

Además, este documento proporciona validaciones tanto para Red Hat Enterprise Linux como para SUSE Linux Enterprise Server para SAP HANA.

"Solución FlexPod Datacenter para SAP con Cisco ACI, Cisco UCS Manager 4,0 y AFF A-Series de NetApp: Diseño"

FlexPod Datacenter para solución SAP con la estructura de tercera generación de Cisco UCS y NetApp AFF A-Series

Shailendra Mruthunjaya, Cisco Ralf Klahr, Cisco Marco Schoen, NetApp

Este documento describe la metodología de puesta en marcha de Cisco y FlexPod Datacenter de NetApp para SAP HANA basado en el sistema de computación Cisco UCS (Cisco UCS) con el respaldo de los procesadores escalables Intel Xeon de segunda generación.

Cisco UCS Manager (UCSM) 4,0(4) proporciona soporte consolidado de todos los modelos actuales de interconexión de estructura de Cisco UCS (6200, 6300, 6324 y 6454), IOM de la serie 2200/2300, blade Cisco UCS B-Series y servidores de factor de forma en rack Cisco UCS C-Series. FlexPod Datacenter con la versión unificada del software Cisco UCS 4,0 (4D) y ONTAP 9,6 de NetApp, es una arquitectura de centro de datos prediseñada con las mejores prácticas desarrollada sobre Cisco UCS, la familia de switches Cisco Nexus 9000 y cabinas de almacenamiento AFF A-Series de NetApp.

"FlexPod Datacenter para solución SAP con la estructura de tercera generación de Cisco UCS y NetApp AFF A-Series"

FlexPod Datacenter para la solución SAP con Cisco UCS Manager 4,0 y NetApp AFF A–Series: Diseño

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Este documento describe la solución FlexPod de Cisco y NetApp, la cual es un enfoque validado para la puesta en marcha de entornos de integración personalizada del centro de datos (TDI) de SAP HANA. Este diseño validado proporciona directrices y un marco para implementar SAP HANA con prácticas recomendadas de Cisco y NetApp.

FlexPod es una infraestructura integrada líder que admite una amplia gama de cargas de trabajo empresariales y casos prácticos. Esta solución le permite poner en marcha SAP HANA de forma rápida y fiable con un modelo de modo de integración de centro de datos personalizado.

La arquitectura de la solución recomendada se basa en Cisco Unified Computing System (Cisco UCS) mediante una versión de software unificada para admitir las plataformas de hardware de Cisco UCS que incluyen los siguientes componentes:

- Los servidores blade Cisco UCS B-Series y los servidores de montaje en rack Cisco UCS C-Series configurables con la opción Intel Optane Data Center Persistent Memory Module (DCPMM)
- Interconexiones de estructuras Cisco UCS de la serie 6300
- Switches Cisco Nexus 9000 Series
- Cabinas de almacenamiento All Flash Series de NetApp

Además, este documento proporciona validaciones tanto para Red Hat Enterprise Linux como para SUSE Linux Enterprise Server para SAP HANA.

"FlexPod Datacenter para la solución SAP con Cisco UCS Manager 4,0 y NetApp AFF A–Series: Diseño"

Oracle

Centro de datos FlexPod con bases de datos RAC de Oracle en Cisco UCS y AFF A-Series de NetApp

Tushar Patel, Cisco Hardikkumar Vyas, Cisco

Los diseños validados por Cisco incluyen sistemas y soluciones diseñados, probados y documentados para facilitar y mejorar las puestas en marcha de los clientes. Estos diseños incorporan una amplia gama de tecnologías y productos en una cartera de soluciones que se han desarrollado para satisfacer las necesidades empresariales de los clientes. Cisco y NetApp se han asociado para ofrecer FlexPod, que sirve como base para una variedad de cargas de trabajo y permite diseñar arquitecturas eficientes que se basan en los requisitos del cliente. Una solución FlexPod es un enfoque validado para poner en marcha tecnologías de Cisco y NetApp como infraestructura de nube compartida.

El centro de datos FlexPod con el sistema AFF all-flash de NetApp es una plataforma de infraestructura convergente que combina las mejores tecnologías de Cisco y NetApp en una potente plataforma convergente para aplicaciones empresariales. Cisco y NetApp trabajan estrechamente con Oracle para dar cabida a las bases de datos más exigentes en cuanto a tiempos de respuesta y transacciones que requieren las empresas actuales.

Este diseño validado por Cisco (CVD) describe la arquitectura FlexPod Datacenter de referencia usando Cisco UCS y All Flash AFF Storage de NetApp para implementar un entorno de base de datos Oracle RAC de alta disponibilidad. Este documento muestra la configuración de hardware y software de los componentes

involucrados y los resultados de varias pruebas. Además, este documento ofrece directrices de implementación y prácticas recomendadas con servidores de computación Cisco UCS, switches de interconexión de estructura Cisco, switches Cisco MDS, switches Cisco Nexus, almacenamiento AFF de NetApp y base de datos Oracle RAC.

"Centro de datos FlexPod con bases de datos RAC de Oracle en Cisco UCS y AFF A-Series de NetApp"

Centro de datos FlexPod con Oracle RAC en Oracle Linux

Tushar Patel, Cisco Niranjan Mohapatra, Cisco John Elliott, NetApp

Cisco Unified Computing System (Cisco UCS) es una plataforma de centro de datos de próxima generación que condensa los recursos informáticos, la red, el acceso al almacenamiento y la virtualización en un único sistema cohesivo. Cisco UCS es la plataforma ideal para la arquitectura de cargas de trabajo de base de datos cruciales. La combinación de la plataforma Cisco UCS, el almacenamiento de NetApp y la arquitectura Real Application Cluster (RAC) de Oracle puede acelerar su transformación TECNOLÓGICA al posibilitar implementaciones más rápidas, una mayor flexibilidad de elección, eficiencia y menor riesgo. Este diseño validado por Cisco (CVD) destaca una arquitectura de referencia de FlexPod flexible, multitenant, de alto rendimiento y resiliente con la base de datos RAC 12c de Oracle.

La plataforma de FlexPod, desarrollada por NetApp y Cisco, es una solución de infraestructura integrada y flexible que ofrece tecnologías prevalidadas de almacenamiento, redes y servidor. Ha sido diseñada para aumentar la capacidad de respuesta DEL DEPARTAMENTO DE TI ante las necesidades empresariales, a la vez que se reduce el coste general de informática. Considere un tiempo de actividad máximo y un riesgo mínimo. Los componentes de FlexPod están integrados y estandarizados para ayudarle a lograr puestas en marcha puntuales, repetibles y coherentes. Puede planificar con precisión la energía, el espacio, la capacidad útil, el rendimiento y el coste de cada implementación de FlexPod.

FlexPod adopta la tecnología más reciente y simplifica de manera eficiente las cargas de trabajo de los centros de datos que redefinen la forma en que LA TECNOLOGÍA ofrece valor:

- Aproveche la capacidad de las cabinas híbridas FAS de NetApp con flash Pool y proporcione la capacidad de poner en marcha la proporción precisa de flash a medios giratorios para su aplicación o entorno específico.
- Aproveche una plataforma prevalidada para minimizar la interrupción del negocio, mejorar la agilidad TECNOLÓGICA y reducir el tiempo de puesta en marcha de meses a semanas.
- Reduzca el tiempo de administración y el coste total de propiedad (TCO) en un 50 %.
- Cumple o supera las demandas de rendimiento del hardware en constante expansión para las cargas de trabajo de los centros de datos.

"Centro de datos FlexPod con Oracle RAC en Oracle Linux"

Centro de datos FlexPod con bases de datos RAC de Oracle en Cisco UCS y AFF A-Series de NetApp

Tushar Patel, Cisco Hardikkumar Vyas, Cisco

El centro de datos FlexPod con el sistema AFF all-flash de NetApp es una plataforma de

infraestructura convergente que combina las mejores tecnologías de Cisco y NetApp en una potente plataforma convergente para aplicaciones empresariales. Cisco y NetApp trabajan estrechamente con Oracle para dar cabida a las bases de datos más exigentes en cuanto a tiempos de respuesta y transacciones que requieren las empresas actuales.

Este diseño validado por Cisco (CVD) describe la arquitectura FlexPod Datacenter de referencia usando Cisco UCS y All Flash AFF Storage de NetApp para implementar un entorno de base de datos Oracle RAC de alta disponibilidad. Este documento muestra la configuración de hardware y software de los componentes involucrados y los resultados de varias pruebas. Además, este documento ofrece directrices de implementación y prácticas recomendadas con servidores de computación Cisco UCS, switches de interconexión de estructura Cisco, switches Cisco MDS, switches Cisco Nexus, almacenamiento AFF de NetApp y base de datos Oracle RAC.

"Centro de datos FlexPod con bases de datos RAC de Oracle en Cisco UCS y AFF A-Series de NetApp"

Microsoft SQL Server

FlexPod Datacenter para Microsoft SQL Server 2019 y VMware vSphere 6.7

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco Atul Bhalodia y NetApp

Este documento describe una arquitectura de referencia de FlexPod utilizando los productos de hardware y software más recientes, y ofrece recomendaciones de puesta en marcha para alojar bases de datos de Microsoft SQL Server 2019 en entornos virtualizados VMware ESXi. Esta solución también usa Cisco Workload Optimization Manager (CWOM), que proporciona recomendaciones automatizadas para un uso óptimo y eficiente de los recursos tanto para las cargas de trabajo de SQL como para la infraestructura.

La solución se basa en Cisco Unified Computing System (Cisco UCS) utilizando la versión de software unificado 4,1.1c para admitir las plataformas de hardware Cisco UCS, incluidos servidores blade Cisco UCS serie B, interconexiones de estructura Cisco UCS 6400, switches de la serie Cisco Nexus 9000 y cabinas de almacenamiento serie AFF de NetApp.

"FlexPod Datacenter para Microsoft SQL Server 2019 y VMware vSphere 6.7"

FlexPod Datacenter con Microsoft SQL Server 2016 y VMware vSphere 6.5

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco David Arnette y NetApp

Este documento trata una arquitectura de referencia de FlexPod utilizando los productos de hardware y software más recientes, y ofrece recomendaciones de configuración para instalar bases de datos de Microsoft SQL Server en un entorno virtualizado.

La arquitectura de la solución recomendada se basa en Cisco Unified Computing System (Cisco UCS) mediante la versión de software unificado para admitir las plataformas de hardware de Cisco UCS, incluidos servidores blade Cisco UCS B-Series, interconexiones de estructura Cisco UCS 6300, switches de la serie Cisco Nexus 9000 y cabinas de almacenamiento all-flash de NetApp. Además, esta solución incluye VMware vSphere 6,5 y vSphere 6,5, que proporciona varias funciones nuevas para optimizar la utilización del almacenamiento y facilitar un cloud privado.

"FlexPod Datacenter con Microsoft SQL Server 2016 y VMware vSphere 6.5"

FlexPod Datacenter con Microsoft SQL Server 2017 sobre Linux VM ejecutándose en VMware y Hyper-V.

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco Atul Bhalodia y NetApp

Este documento trata una arquitectura de referencia de FlexPod utilizando los productos de hardware y software más recientes y ofrece recomendaciones de puesta en marcha para alojar bases de datos de Microsoft SQL Server en entornos virtualizados de VMware ESXi y Microsoft Windows Hyper-V con compatibilidad de Linux de la puesta en marcha de Microsoft para SQL Server.

La arquitectura de la solución recomendada se basa en el sistema Unified Computing System de Cisco (Cisco UCS) mediante la versión de software unificado 4,0.1c para admitir las plataformas de hardware Cisco UCS, incluidos servidores blade Cisco UCS serie B, interconexiones de estructura Cisco UCS 6300, switches de la serie Cisco Nexus 9000 y cabinas de almacenamiento serie AFF de NetApp.

"FlexPod Datacenter con Microsoft SQL Server 2017 sobre Linux VM ejecutándose en VMware y Hyper-V."

FlexPod Datacenter con Microsoft SQL Server 2017 sobre Linux VM ejecutándose en VMware y Hyper-V.

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco Atul Bhalodia y NetApp

Este documento trata una arquitectura de referencia de FlexPod utilizando los productos de hardware y software más recientes y ofrece recomendaciones de puesta en marcha para alojar bases de datos de Microsoft SQL Server en entornos virtualizados de VMware ESXi y Microsoft Windows Hyper-V con compatibilidad de Linux de la puesta en marcha de Microsoft para SQL Server.

La arquitectura de la solución recomendada se basa en Cisco Unified Computing System (Cisco UCS) mediante la versión de software unificado 4,0.1c para admitir las plataformas de hardware Cisco UCS, incluidos servidores blade Cisco UCS serie B, interconexiones de estructura Cisco UCS 6300, switches de la serie Cisco Nexus 9000 y cabinas de almacenamiento serie AFF de NetApp.

"FlexPod Datacenter con Microsoft SQL Server 2017 sobre Linux VM ejecutándose en VMware y Hyper-V."

Sector sanitario

FlexPod para genomas

TR-4911: Genómica de FlexPod

JayaKishore Esanakula, NetApp

Hay pocos campos de la medicina que son más importantes que la genómica para la salud y las ciencias biológicas, y la genómica se está convirtiendo rápidamente en una herramienta clínica clave para los médicos y las enfermeras. La genómica, cuando se combina con imágenes médicas y patología digital, nos ayuda a entender cómo los genes de un paciente pueden verse afectados por los protocolos de tratamiento. El éxito de la genómica en el sector sanitario depende cada vez más de la interoperabilidad de datos a escala. El objetivo final es comprender los enormes volúmenes de datos genéticos e identificar correlaciones y variantes clínicamente relevantes que mejoran el diagnóstico y hacen realidad la medicina de precisión. La genómica nos ayuda a comprender el origen de los brotes de enfermedades, cómo evolucionan las enfermedades y qué tratamientos y estrategias podrían ser eficaces. Claramente, la genómica tiene muchos beneficios que abarcan la prevención, el diagnóstico y el tratamiento. Las organizaciones de atención médica se enfrentan a varios desafíos, entre ellos los siguientes:

- Calidad de la atención mejorada
- Atención basada en el valor
- Explosión de datos
- Medicina de precisión
- Pandemias
- Prendas tecnológicas, supervisión remota y atención sanitaria
- Seguridad cibernética

Las vías clínicas estandarizadas y los protocolos clínicos son uno de los componentes críticos de la medicina moderna. Uno de los aspectos clave de la estandarización es la interoperabilidad entre los proveedores de atención médica, no solo para los registros médicos, sino también para los datos genómicos. La gran pregunta es ¿las organizaciones sanitarias renunciarán a la propiedad de los datos genómicos en lugar de que los pacientes sean propietarios de los datos personales de su genómica y los registros médicos relacionados?

La interoperabilidad de los datos de los pacientes es fundamental para posibilitar la medicina de precisión, una de las fuerzas que impulsan la reciente explosión del crecimiento de los datos. El objetivo de la medicina de precisión es hacer que el mantenimiento de la salud, la prevención de enfermedades, los diagnósticos y las soluciones de tratamiento sean más eficaces y precisos.

La tasa de crecimiento de los datos ha sido exponencial. A principios de febrero de 2021, los laboratorios estadounidenses secuenciaron aproximadamente 8,000 cepas del COVID-19 por semana. El número de genomas secuenciados había aumentado a 29,000 por semana en abril de 2021. Cada genoma humano secuenciado en su totalidad tiene un tamaño de alrededor de 125 GB. Por lo tanto, a una tasa de 29,000 genomas secuenciados por semana, el almacenamiento total del genoma en reposo sería de más de 180

petabytes al año. Varios países han comprometido recursos a la epidemiología genómica para mejorar la vigilancia genómica y prepararse para la próxima oleada de desafíos mundiales en materia de salud.

La reducción del costo de la investigación genómica está impulsando la investigación y las pruebas genéticas a un ritmo sin precedentes. Los tres P se encuentran en un punto de inflexión: Potencia informática, privacidad de datos y personalización de la medicina. En 2025, los investigadores estiman que se secuenciarán entre 100 y 2 millones de genomas humanos. Para que la genómica sea eficaz y sea una propuesta valiosa, las capacidades de genómica deben ser una parte integral de los flujos de trabajo de atención médica; debe ser fácil de acceder y ser aplicable durante la visita de un paciente. También es igualmente importante integrar los datos de historiales médicos electrónicos de los pacientes con los datos de genomas de los pacientes. Con la llegada de una infraestructura convergente de vanguardia como FlexPod, las organizaciones pueden incorporar sus funcionalidades de genómica en los flujos de trabajo diarios de médicos, enfermeras y gestores clínicos. Para obtener la información más reciente sobre la plataforma FlexPod, consulte este tema "Whitepaper de FlexPod Datacenter con Cisco UCS X-Series".

Para un médico, el verdadero valor de la genómica incluye la medicina de precisión y los planes de tratamiento personalizados basados en los datos genómicos de un paciente. Nunca ha habido tal sinergia entre médicos y científicos de datos en el pasado, y la genómica se está beneficiando de las innovaciones tecnológicas del pasado reciente, así como de asociaciones reales entre organizaciones sanitarias y líderes tecnológicos del sector.

Los centros médicos académicos y otras organizaciones de salud y ciencias de la vida están en camino de establecer el centro de excelencia (COE) en ciencia genómica. Según el Dr. Charlie Gersbach, Dr. Greg Crawford, y Dr. Tim E Reddy, de la Universidad de Duke, “sabemos que los genes no están activados o desactivados por un simple interruptor binario, sino que es el resultado de múltiples interruptores regulatorios genéticos que funcionan juntos. También han determinado que "ninguna de estas partes del genoma trabaja en aislamiento. El genoma es una red muy complicada que la evolución ha tejido” ("ref").

NetApp y Cisco llevan trabajando muy duro para implementar mejoras incrementales en la plataforma de FlexPod durante más de 10 años. Todos los comentarios de los clientes se escuchan, evalúan y están ligados a las fuentes de valor y los conjuntos de funciones de FlexPod. Este continuo bucle de comentarios, colaboración, mejora y celebración diferencia a FlexPod de la plataforma de infraestructura convergente de confianza de todo el mundo. Se ha simplificado y diseñado desde cero para ser la plataforma más fiable, robusta, versátil y ágil para organizaciones sanitarias.

Ámbito

La plataforma de infraestructura convergente FlexPod permite a una organización sanitaria alojar una o más cargas de trabajo genómica, junto con otras aplicaciones clínicas y no clínicas de la sanidad. En este informe técnico se utiliza una herramienta genómica de código abierto estándar en el sector denominada GATK durante la validación de la plataforma FlexPod. Sin embargo, una discusión más profunda sobre genómica o GATK está fuera del alcance de este documento.

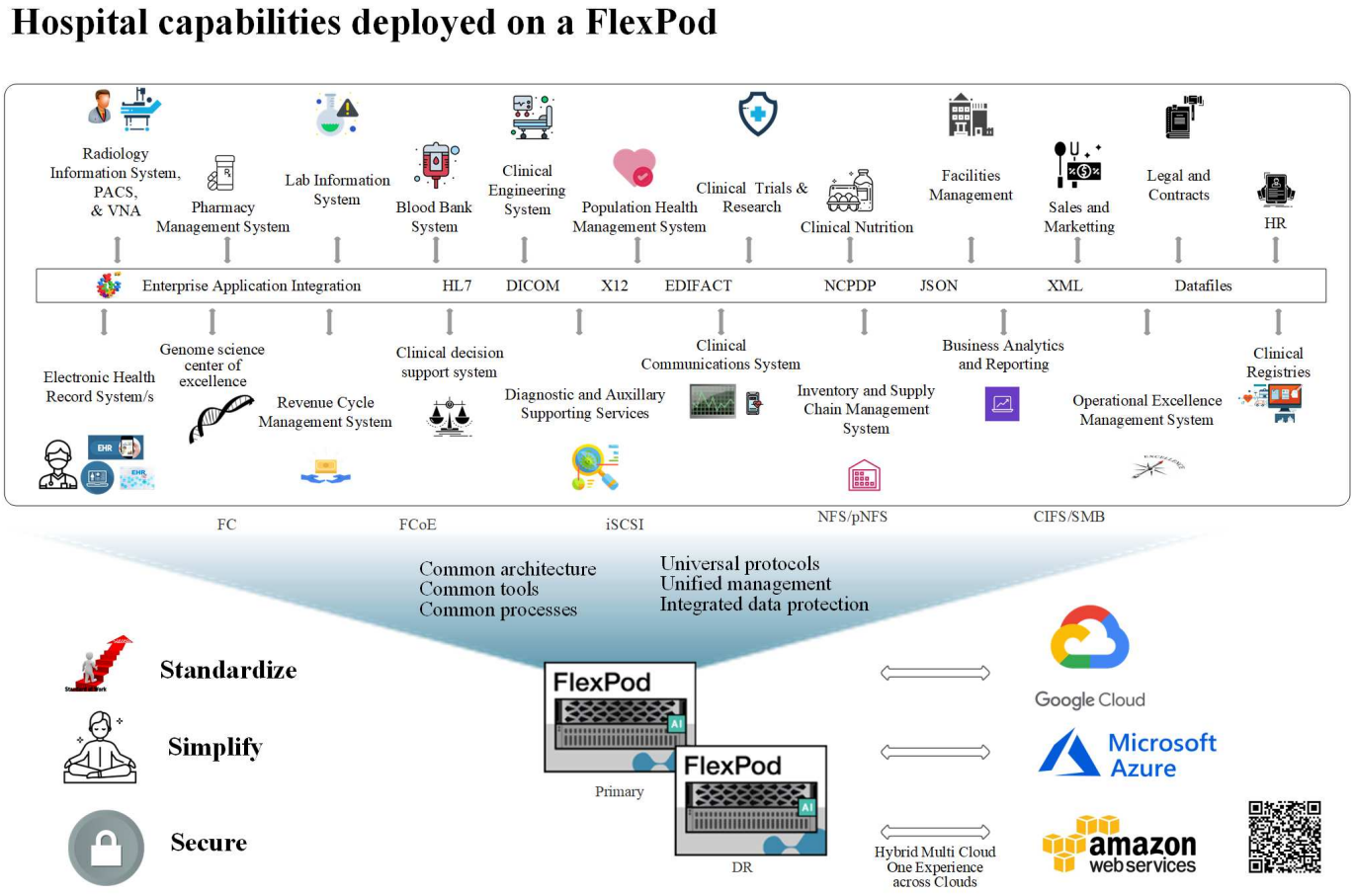
Destinatarios

Este documento está dirigido a líderes técnicos del sector sanitario y a ingenieros de soluciones de partners de Cisco y NetApp y personal de servicios profesionales. NetApp asume que el lector tiene un buen conocimiento de los conceptos de configuración de la computación y el almacenamiento, así como una familiaridad técnica con las amenazas para la salud, la seguridad sanitaria, los sistemas TECNOLÓGICOS para el sector sanitario, Cisco UCS y los sistemas de almacenamiento de NetApp.

Capacidades hospitalarias implementadas en FlexPod

Un hospital típico tiene un conjunto diversificado de sistemas DE TECNOLOGÍA. La mayoría de estos sistemas son adquiridos a un proveedor, mientras que muy pocos son construidos por el sistema hospitalario

interno. Por tanto, el sistema hospitalario debe gestionar distintos entornos de infraestructura en sus centros de datos. Cuando los hospitales unifican sus sistemas en una plataforma de infraestructura convergente como FlexPod, las organizaciones pueden estandarizar sus operaciones de centro de datos. Con FlexPod, las organizaciones sanitarias pueden implementar sistemas clínicos y no clínicos en la misma plataforma, unificando las operaciones del centro de datos.



"Siguiente: Ventajas de la puesta en marcha de cargas de trabajo genómicos en FlexPod"

Ventajas de la puesta en marcha de cargas de trabajo genómicos en FlexPod

"Anterior: Introducción."

En esta sección se proporciona una breve lista de ventajas para ejecutar una carga de trabajo genómica en una plataforma de infraestructura convergente FlexPod. Describiremos rápidamente las capacidades de un hospital. La siguiente vista de arquitectura empresarial muestra las capacidades de un hospital puestas en marcha en una plataforma de infraestructura convergente FlexPod preparada para cloud híbrido.

- * Evitar silos en la salud.* los silos en la salud son una preocupación muy real. A menudo, los departamentos se encuentran organizados en silos en su propio conjunto de hardware y software, no por elección, sino de forma orgánica, por evolución. Por ejemplo, radiología, cardiología, EHR, genómica, análisis, ciclo de ingresos y otros departamentos terminan con su conjunto individual de software y hardware dedicados. Las organizaciones sanitarias mantienen un conjunto limitado de profesionales DE TI para gestionar sus activos de hardware y software. El punto de inflexión se produce cuando se espera que este conjunto de personas gestionen un conjunto de hardware y software muy diversificado. La heterogeneidad se ve agravada por un conjunto incongruente de procesos llevados a la organización

sanitaria por los proveedores.

- **Iniciar pequeño y crecer.** el kit de herramientas GATK está adaptado para la ejecución de CPU, que mejor paquete de plataformas como FlexPod. FlexPod permite una escalabilidad independiente de la red, el entorno informático y el almacenamiento. Empiece con poco y escale a medida que aumenten sus funcionalidades de genómica y el entorno. Las organizaciones sanitarias no tienen que invertir en plataformas especializadas para ejecutar cargas de trabajo genómicas. En su lugar, las organizaciones pueden aprovechar plataformas versátiles como FlexPod para ejecutar cargas de trabajo genómica y no genómicas en la misma plataforma. Por ejemplo, si el departamento de pediatría quiere implementar una capacidad genómica, los líderes TECNOLÓGICOS pueden aprovisionar computación, almacenamiento y redes en una instancia de FlexPod existente. A medida que crece la unidad de negocio genómica, la organización sanitaria puede escalar su plataforma FlexPod según sea necesario.
- **Un único panel de control y una flexibilidad sin igual.** Cisco Intersight simplifica significativamente las operaciones DE TI al unir aplicaciones con la infraestructura, proporcionando visibilidad y gestión desde servidores e hipervisores sin sistema operativo hasta aplicaciones sin servidor, reduciendo así los costes y mitigando el riesgo. Esta plataforma SaaS unificada utiliza un diseño de API abierta unificado que se integra de forma nativa con plataformas y herramientas de terceros. Además, permite la gestión desde su equipo de operaciones de centro de datos in situ o desde cualquier lugar mediante una aplicación móvil.

  Los usuarios liberan rápidamente un valor tangible en su entorno al aprovechar Intersight como su plataforma de gestión. Al permitir la automatización de muchas tareas manuales diarias, Intersight elimina los errores y simplifica las operaciones diarias. Además, las avanzadas capacidades de soporte que ofrece Intersight permiten a los usuarios mantenerse por delante de los problemas y acelerar la resolución de estos. En conjunto, las organizaciones dedican mucho menos tiempo y dinero a la infraestructura de aplicaciones y más tiempo al desarrollo empresarial principal.

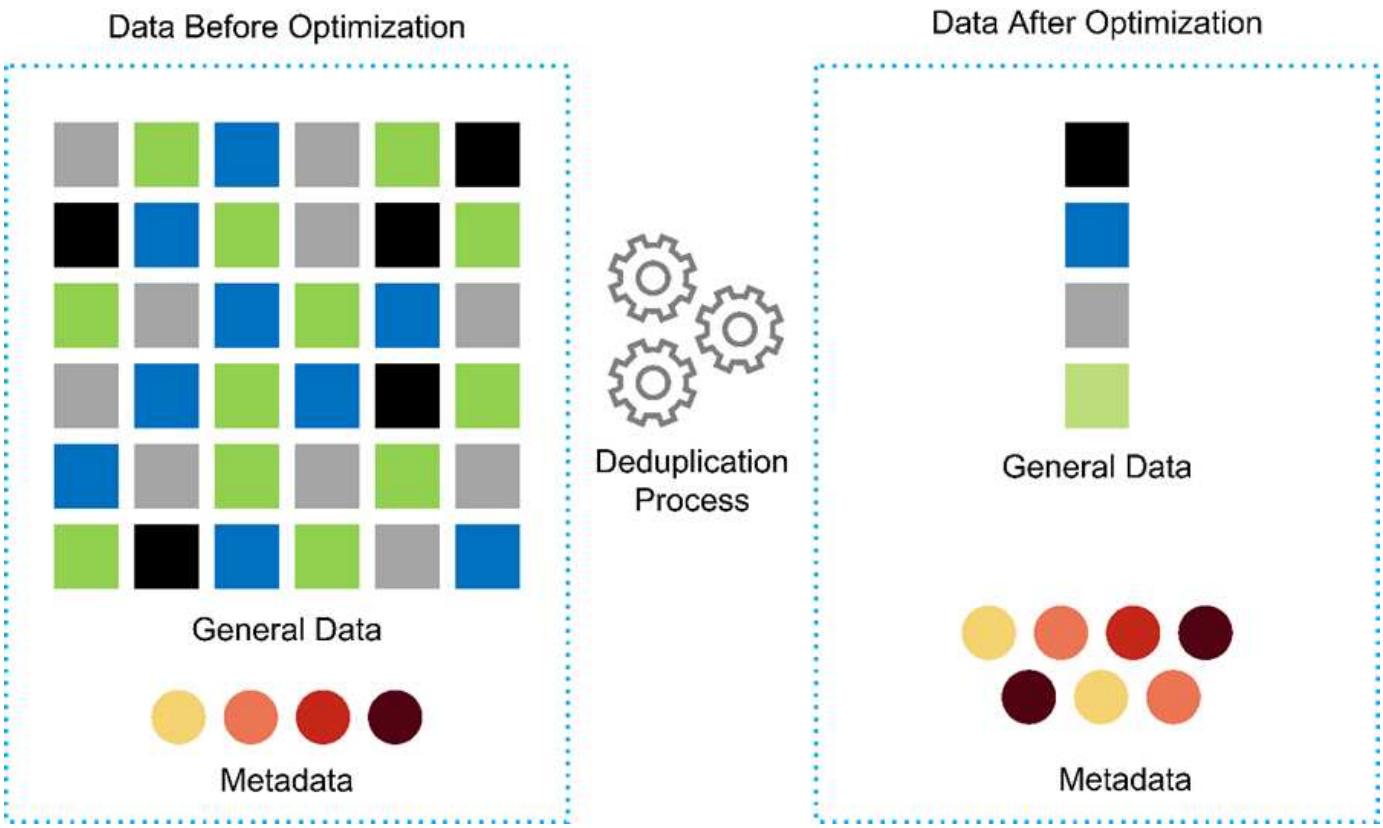
  Aprovechar la gestión de Intersight y la arquitectura de FlexPod, fácilmente escalable, permite a las organizaciones ejecutar varias cargas de trabajo de genoma en una única plataforma FlexPod, lo que aumenta el uso y reduce el coste total de propiedad (TCO). FlexPod permite un dimensionamiento flexible, con opciones que empiezan por nuestro pequeño FlexPod Express y se pueden escalar a implementaciones grandes de centros de datos FlexPod. Con las funcionalidades de control de acceso basadas en funciones integradas en Cisco Intersight, las organizaciones sanitarias pueden implementar mecanismos sólidos de control de acceso, lo que evita la necesidad de pilas de infraestructuras independientes. El uso de varias unidades de negocio en la organización sanitaria puede aprovechar la genómica como una competencia principal.

  En última instancia, FlexPod ayuda a simplificar las operaciones DE TI y a reducir los costos operativos y permite que los administradores de infraestructuras DE TI se centren en tareas que ayudan a los médicos a innovar en lugar de quedar relegados a mantener las operaciones básicas.

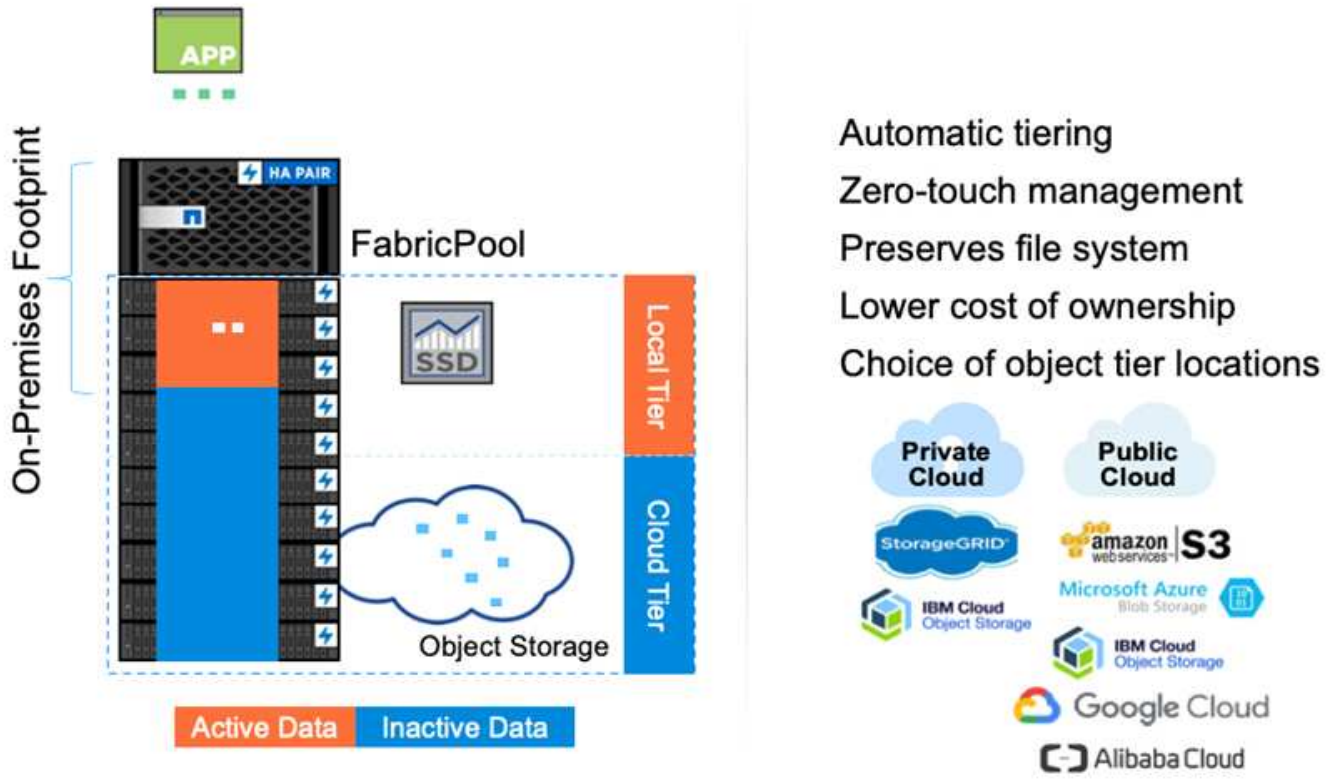
- **Diseño validado y resultados garantizados.** las guías de diseño e implementación de FlexPod se validan para ser repetibles, y cubren detalles completos de la configuración y las mejores prácticas del sector que se necesitan para implementar un FlexPod con confianza. Las guías de diseño validado, las guías de puesta en marcha y las arquitecturas de Cisco y NetApp ayudan a su organización de ciencias biológicas o sanitarias a eliminar las conjeturas de la implantación de una plataforma validada y de confianza desde el principio. Con FlexPod puede acelerar los tiempos de puesta en marcha y reducir costes, complejidad y riesgos. Los diseños validados y las guías de puesta en marcha de FlexPod establecen a FlexPod como la plataforma perfecta para diversas cargas de trabajo de genómica.
- * Innovación y agilidad.* se recomienda FlexPod como una plataforma ideal por EHR como Epic, Cerner, Meditech y sistemas de imagen como Agfa, GE, Philips. Para obtener más información acerca de "Rollo de honor épico" Y la arquitectura de la plataforma de destino; consulte la web de usuarios de Epic. Ejecutando la genómica "FlexPod" permite a las organizaciones sanitarias continuar su camino de innovación con agilidad. Con FlexPod, la implementación del cambio de organización viene de forma natural. Cuando las organizaciones se estandarizan en una plataforma de FlexPod, los expertos EN

TECNOLOGÍA del sector sanitario pueden disponer de tiempo, esfuerzo y recursos para innovar y, por lo tanto, ser tan ágiles como exige el ecosistema.

- **Datos liberados**. Con la plataforma de infraestructura convergente FlexPod y el sistema de almacenamiento ONTAP de NetApp, es posible acceder a los datos genómicos utilizando una amplia variedad de protocolos a escala desde una única plataforma. FlexPod con ONTAP de NetApp ofrece una plataforma de cloud híbrido sencilla, intuitiva y potente. Su Data Fabric, impulsado por ONTAP de NetApp, aúna los datos de distintos sitios, sin que los barreras físicas y de todas las aplicaciones. Su Data Fabric se ha creado pensando en empresas basadas en datos en un mundo donde todo gira alrededor de ellos. Los datos se crean y se usan en varias ubicaciones y, a menudo, hay que aprovecharlos y compartirlos con otras ubicaciones, aplicaciones e infraestructuras. Por tanto, se necesita una forma coherente e integrada de gestionarla. FlexPod controla a su equipo DE TECNOLOGÍA y simplifica la cada vez mayor complejidad TECNOLÓGICA.
- **Multitenancy seguro.** FlexPod utiliza módulos criptográficos compatibles con FIPS 140-2, lo que permite a las organizaciones implementar la seguridad como un elemento fundamental, no como una idea de última hora. FlexPod permite a las organizaciones implantar multi-tenancy seguro desde una única plataforma de infraestructura convergente, independientemente del tamaño de la plataforma. FlexPod con multi-tenancy seguro y calidad de servicio ayudan con la separación de cargas de trabajo y maximizan la utilización. Esto ayuda a evitar que el capital quede atrapado en plataformas especializadas que potencialmente están infrautilizadas y requiere un conjunto de habilidades especializadas para gestionarlas.
- **La eficiencia del almacenamiento.** la genómica requiere que el almacenamiento subyacente tenga las funcionalidades de eficiencia del almacenamiento líderes en el sector. Puede reducir los costes de almacenamiento con funciones de eficiencia del almacenamiento de NetApp como la deduplicación (inline y bajo demanda), la compresión de datos y la compactación de datos ("ref"). La deduplicación de NetApp proporciona deduplicación a nivel de bloque en un volumen FlexVol. En esencia, la deduplicación elimina los bloques duplicados y solo almacena los bloques únicos en el volumen FlexVol. La deduplicación funciona con un alto grado de granularidad y funciona en el sistema de archivos activo del volumen FlexVol. En la siguiente figura se muestra información general sobre el funcionamiento de la deduplicación de NetApp. La deduplicación es transparente para las aplicaciones. Por lo tanto, se puede usar para deduplicar datos originados por cualquier aplicación que utilice el sistema de NetApp. Puede ejecutar la deduplicación del volumen como un proceso en línea y como un proceso en segundo plano. Es posible configurarlo para que se ejecute automáticamente, para que se programe o manualmente a través de la CLI, ONTAP System Manager de NetApp o Active IQ Unified Manager de NetApp.



- **Permitir la interoperabilidad genómica.** ONTAP FlexCache es una capacidad de almacenamiento en caché remoto que simplifica la distribución de archivos, reduce la latencia WAN y reduce los costes de ancho de banda WAN ("ref"). Una de las actividades clave durante la identificación y anotación de variantes genómicas es la colaboración entre los médicos. La tecnología ONTAP FlexCache aumenta el rendimiento de los datos incluso cuando los médicos colaboradores se encuentran en diferentes ubicaciones geográficas. Dado el tamaño típico de un archivo *.BAM (de 1 GB a 100 s de GB), es fundamental que la plataforma subyacente pueda hacer que los archivos estén disponibles para los médicos en diferentes ubicaciones geográficas. FlexPod con ONTAP FlexCache hace que los datos genómicos y las aplicaciones estén realmente listos para los distintos sitios, lo que convierte la colaboración entre investigadores de todo el mundo en un proceso fluido con una baja latencia y un alto rendimiento. Las organizaciones sanitarias que ejecutan aplicaciones de genómica en un entorno multisitio pueden escalarse horizontalmente usando la estructura de datos para equilibrar la capacidad de gestión con el coste y la velocidad.
- **Uso inteligente de la plataforma de almacenamiento.** FlexPod con la organización en niveles automática de ONTAP y la tecnología Fabric Pool de NetApp simplifica la gestión de datos. FabricPool ayuda a reducir los costes de almacenamiento sin comprometer el rendimiento, la eficiencia, la seguridad o la protección. FabricPool es transparente para las aplicaciones empresariales y aprovecha las eficiencias del cloud al reducir el TCO del almacenamiento sin necesidad de rediseñar la arquitectura de la infraestructura de aplicaciones. FlexPod se puede beneficiar de las funcionalidades de almacenamiento por niveles de FabricPool para hacer un uso más eficiente del almacenamiento flash de ONTAP. Para obtener más información, consulte "FlexPod con FabricPool". El siguiente diagrama proporciona una descripción general de alto nivel de FabricPool y sus ventajas.



- **Análisis y anotación de variantes más rápidos.** la plataforma FlexPod es más rápida de implementar y operar. La plataforma FlexPod permite la colaboración entre los médicos, al poner los datos a escala con baja latencia y un mayor rendimiento. Una mayor interoperabilidad permite innovar. Las organizaciones sanitarias pueden ejecutar sus cargas de trabajo genómicos y no genómicas en paralelo, lo que significa que las organizaciones no necesitan plataformas especializadas para iniciar la transición a la genómica.

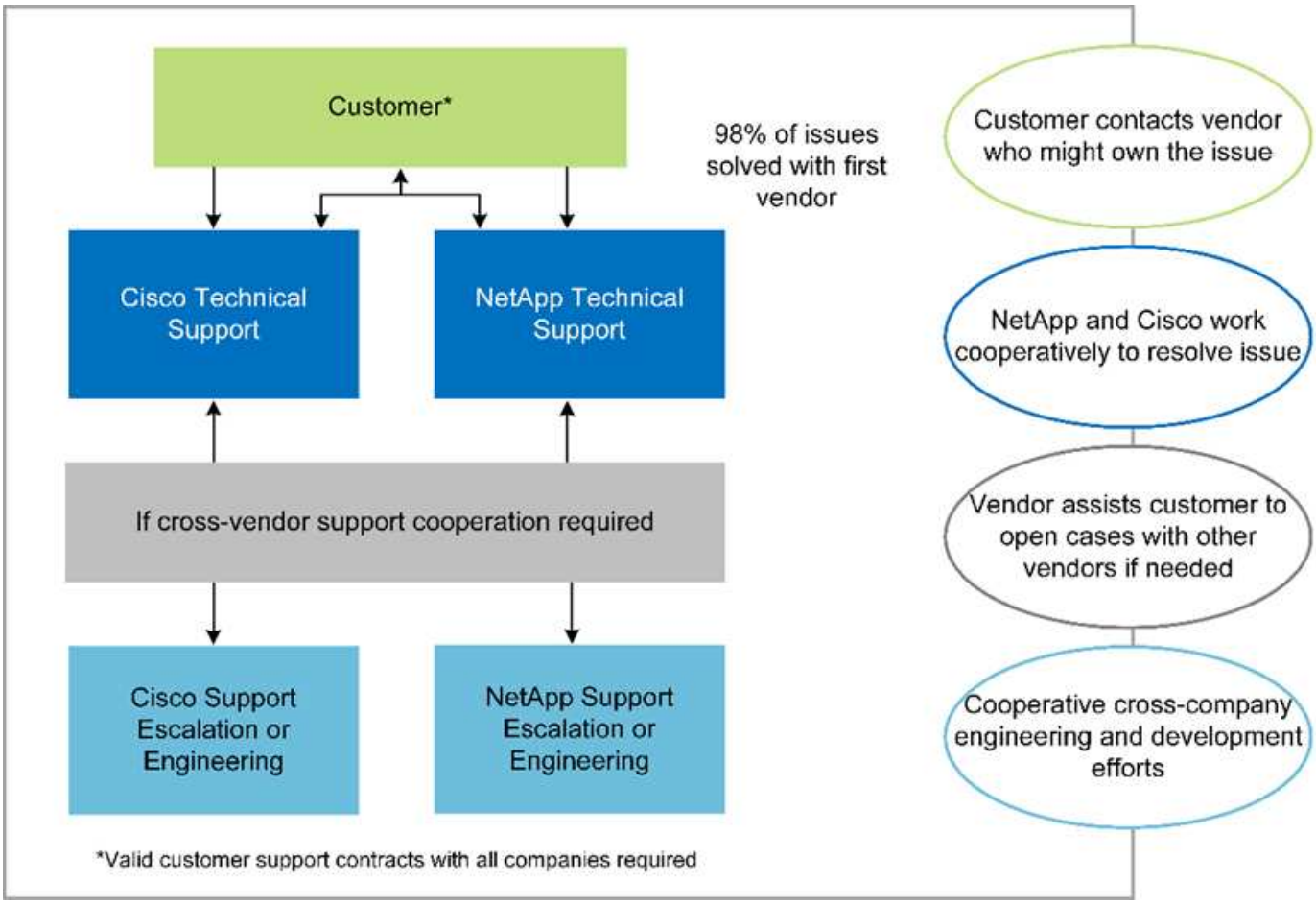
  FlexPod ONTAP añade habitualmente funciones innovadoras a la plataforma de almacenamiento. Centro de datos FlexPod es la base de infraestructura compartida óptima para poner en marcha FC- NVMe para permitir acceso al almacenamiento de alto rendimiento a aplicaciones que lo necesiten. A medida que FC-NVMe evoluciona para incluir alta disponibilidad, multivía y compatibilidad con sistemas operativos adicionales, FlexPod se adapta perfectamente a la plataforma preferida, lo que proporciona la escalabilidad y fiabilidad necesarias para respaldar estas funcionalidades. ONTAP con una I/o más rápida con NVMe integral permite que los análisis de genomas se completen con mayor rapidez ("ref").

  Los datos del genoma en secuencia RAW producen tamaños de archivo grandes, y es importante que estos archivos estén disponibles para los analizadores de variantes para reducir el tiempo total que toma de la colección de muestras a la anotación de variante. NVMe (memoria no volátil rápida) cuando se utiliza como protocolo de acceso al almacenamiento y transporte de datos proporciona niveles de rendimiento sin precedentes y los tiempos de respuesta más rápidos. FlexPod pone en marcha el protocolo NVMe a la vez que accede al almacenamiento flash a través del bus PCI Express (PCIe). PCIe posibilita la implementación de decenas de miles de colas de comandos, lo que aumenta la paralelización y el rendimiento. Un único protocolo del almacenamiento a la memoria acelera el acceso a los datos.

- **Agilidad para la investigación clínica desde el principio.** capacidad de almacenamiento flexible y ampliable y rendimiento permite a las organizaciones de investigación sanitaria optimizar el medio ambiente de una manera elástica o puntual (JIT). Al desacoplar el almacenamiento de la infraestructura informática y de red, la plataforma FlexPod se puede escalar horizontal y verticalmente sin interrupciones. Con Cisco Intersight, la plataforma FlexPod se puede gestionar con flujos de trabajo automatizados integrados y personalizados. Los flujos de trabajo de Cisco Intersight permiten a las organizaciones

sanitarias reducir los tiempos de gestión del ciclo de vida de las aplicaciones. Cuando un centro médico académico exige que los datos de los pacientes se anonimien y pongan a disposición de su centro de investigación informática y/o centro de calidad, su organización DE TI puede aprovechar los flujos de trabajo de Cisco Intersight FlexPod para realizar backups, clonarlos y restaurarlos con seguridad en cuestión de segundos y no de horas. Con Trident y Kubernetes de NetApp, las organizaciones TECNOLÓGICAS pueden suministrar nuevos científicos de datos y hacer que los datos clínicos estén disponibles para el desarrollo de modelos en cuestión de minutos, y en ocasiones incluso en segundos.

- **La protección de datos genómicos.** SnapLock de NetApp proporciona un volumen para una finalidad especial en el que los ficheros se pueden almacenar y realizar transacciones a un estado que no puede borrarse ni escribirse. Los datos de producción del usuario que se encuentran en un volumen FlexVol se pueden duplicar o realizar copias vault en un volumen SnapLock mediante la tecnología SnapMirror o SnapVault de NetApp. Los archivos del volumen de SnapLock, el volumen en sí y su agregado de alojamiento no se pueden eliminar hasta que finalice el período de retención. Mediante el software FPolicy de ONTAP, las organizaciones pueden evitar ataques de ransomware al dejar las operaciones en archivos con extensiones específicas. Es posible activar un evento de FPolicy para operaciones de archivos específicas. El evento está ligado a una política, que llama al motor que necesita utilizar. Puede configurar una política con un conjunto de extensiones de archivo que potencialmente puedan contener ransomware. Cuando un archivo con una extensión no permitida intenta realizar una operación no autorizada, FPolicy impide que esa operación se ejecute ("ref").
- **Soporte conjunto de FlexPod.** NetApp y Cisco han establecido el soporte conjunto de FlexPod, un modelo de soporte sólido, escalable y flexible para cumplir los requisitos de soporte exclusivos de la infraestructura convergente de FlexPod. Este modelo aprovecha la experiencia combinada, recursos y conocimientos de soporte técnico de NetApp y Cisco para ofrecer un proceso optimizado para identificar y solucionar problemas de soporte de FlexPod, independientemente de dónde se encuentre el problema. En la siguiente figura, se ofrece una descripción general del modelo de soporte conjunto de FlexPod. El cliente se pone en contacto con el proveedor que podría ser el propietario del problema y tanto Cisco como NetApp trabajan conjuntamente para resolverlo. Cisco y NetApp cuentan con equipos de desarrollo e ingeniería de múltiples empresas que trabajan conjuntamente para solucionar problemas. Este modelo de soporte reduce la pérdida de información durante la traducción, permite la confianza y reduce el tiempo de inactividad.

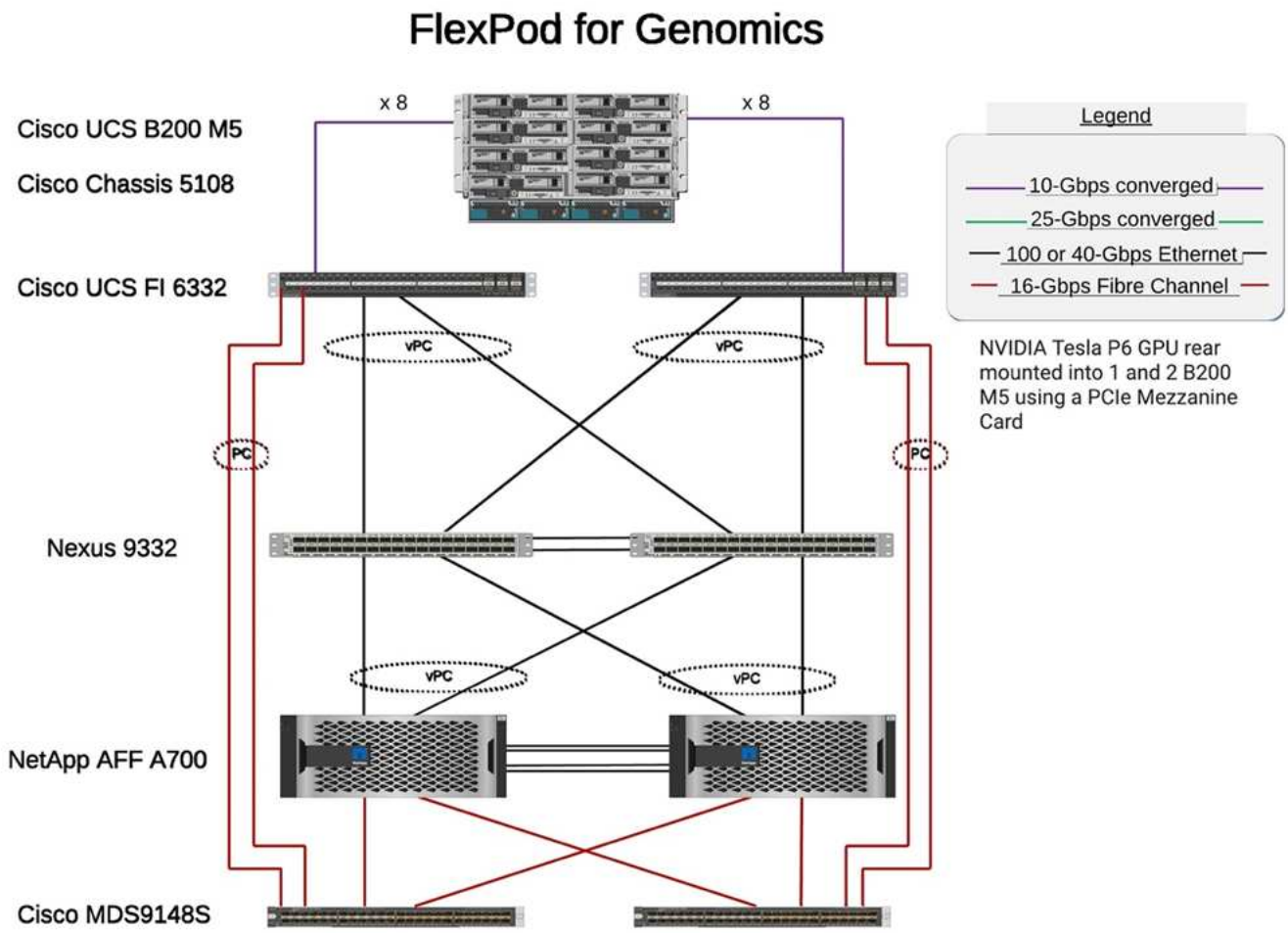


"Siguiente: Componentes de hardware y software de la infraestructura de la solución."

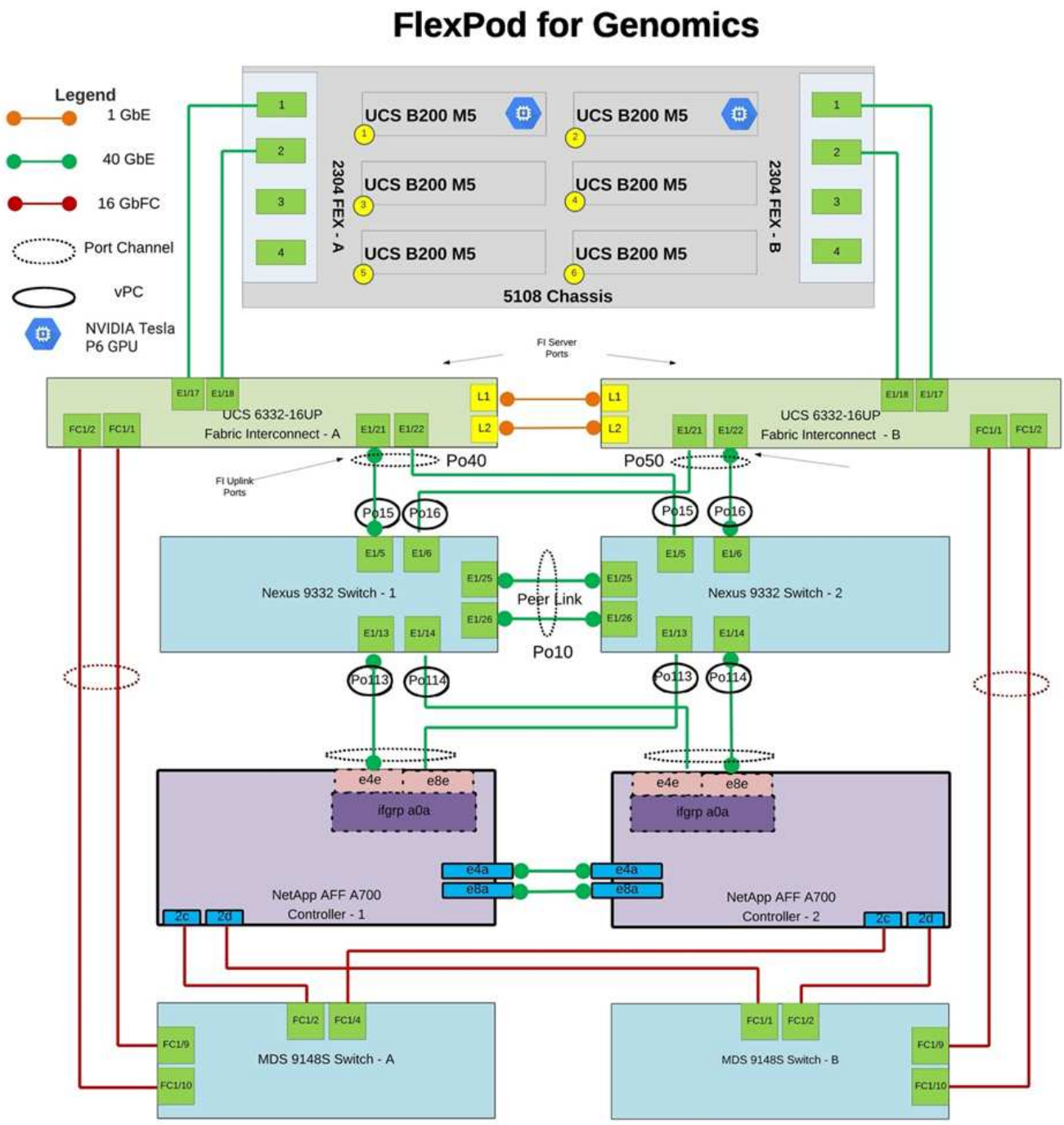
Infraestructura de la solución componentes de hardware y software

"Anterior: Ventajas de la puesta en marcha de cargas de trabajo genómicos en FlexPod"

La siguiente figura muestra el sistema FlexPod utilizado para la instalación y validación de GATK. Nosotros usamos "FlexPod Datacenter con VMware vSphere 7.0 y NetApp ONTAP 9.7 Cisco Validated Design (CVD)" durante el proceso de configuración.



En el siguiente diagrama se describen los detalles del cableado FlexPod.



La siguiente tabla enumera los componentes de hardware utilizados durante la prueba de GATK que se activa en un FlexPod. Aquí está la "Herramienta de matriz de interoperabilidad de NetApp" (IMT) y. "Lista de compatibilidad de hardware (HCL) de Cisco".

Capa	Familia de productos	Cantidad y modelo	Detalles
Informática	Chasis Cisco UCS 5108	1 o 2	
	Servidores blade Cisco UCS	6 B200 M5	Cada uno con 2 20 núcleos o más, 2,7 GHz y 128 GB de RAM

Capa	Familia de productos	Cantidad y modelo	Detalles
	Tarjeta de interfaz virtual (VIC) de Cisco UCS	Cisco UCS 1440	Consulte
	2 interconexiones de estructura Cisco UCS	6332	-
Red	Switches Cisco Nexus	2 switches Cisco Nexus 9332	-
Red de almacenamiento	Red IP para el acceso de almacenamiento mediante protocolos SMB/CIFS, NFS o iSCSI	Los mismos switches de red que se han descrito anteriormente	-
	Acceso a almacenamiento mediante FC	2 Cisco MDS 9148S	-
Reducida	Sistema de almacenamiento all-flash AFF A700 de NetApp	Clúster 1	Clúster con dos nodos
	Bandeja de discos	Una bandeja de discos DS224C o NS224	Totalmente lleno con 24 unidades
	SSD	24, 1,2 TB o más capacidad	-

Esta tabla enumera el software de infraestructura.

De NetApp	Familia de productos	Versión o versión	Detalles
Varios	Linux	RHEL 8.3	-
	Windows	Windows Server 2012 R2 (64 bits)	-
	ONTAP de NetApp	ONTAP 9.8 o posterior	-
	Interconexión de estructura Cisco UCS	Cisco UCS Manager 4.1 o posterior	-
	Switches de las series Cisco Ethernet 3000 o 9000	Para la serie 9000, 7.0(3)I7(7) o posterior para la serie 3000, 9.2(4) o posterior	-
	Cisco FC: Cisco MDS 9132T	8.4(1a) o posterior	-
	Hipervisor	VMware vSphere ESXi 7.0	-
Reducida	Sistema de gestión de hipervisores	VMware vCenter Server 7.0 (vcsa) o versiones posteriores	-
Red	Virtual Storage Console (VSC) de NetApp	VSC 9.7 o posterior	-

De NetApp	Familia de productos	Versión o versión	Detalles
	SnapCenter de NetApp	SnapCenter 4.3 o posterior	-
	Administrador de Cisco UCS	4.1(3c) o posterior	
Hipervisor	ESXi		
Gestión	Sistema de gestión del hipervisor VMware vCenter Server 7.0 (vcsa) o versiones posteriores		
	Virtual Storage Console (VSC) de NetApp	VSC 9.7 o posterior	
	SnapCenter de NetApp	SnapCenter 4.3 o posterior	
	Administrador de Cisco UCS	4.1(3c) o posterior	

"Siguiente: Genómica - instalación y ejecución de GATK."

Genómica - instalación y ejecución de GATK

"Anterior: Componentes de hardware y software de la infraestructura de la solución."

Según el Instituto Nacional de Investigación del Genoma humano ("NHGRI"), “la genómica es el estudio de todos los genes de una persona (el genoma), incluyendo las interacciones de estos genes entre sí y con el medio ambiente de una persona. ”

Según la "NHGRI", “El ácido Deoxirribonucleico (ADN) es el compuesto químico que contiene las instrucciones necesarias para desarrollar y dirigir las actividades de casi todos los organismos vivos. Las moléculas de ADN están hechas de dos filamentos de torsión, emparejados, a menudo llamados como una hélice doble". “El conjunto completo de ADN de un organismo se llama su genoma”.

La secuenciación es el proceso de determinar el orden exacto de las bases en una cadena de ADN. Uno de los tipos más comunes de secuenciación utilizados hoy se llama secuenciación por síntesis. Esta técnica usa la emisión de señales fluorescentes para ordenar las bases. Los investigadores pueden usar la secuenciación del ADN para buscar variaciones genéticas y cualquier mutación que pueda desempeñar un papel en el desarrollo o progresión de una enfermedad mientras una persona todavía está en la etapa embrionaria.

De muestra a identificación de variante, anotación y predicción

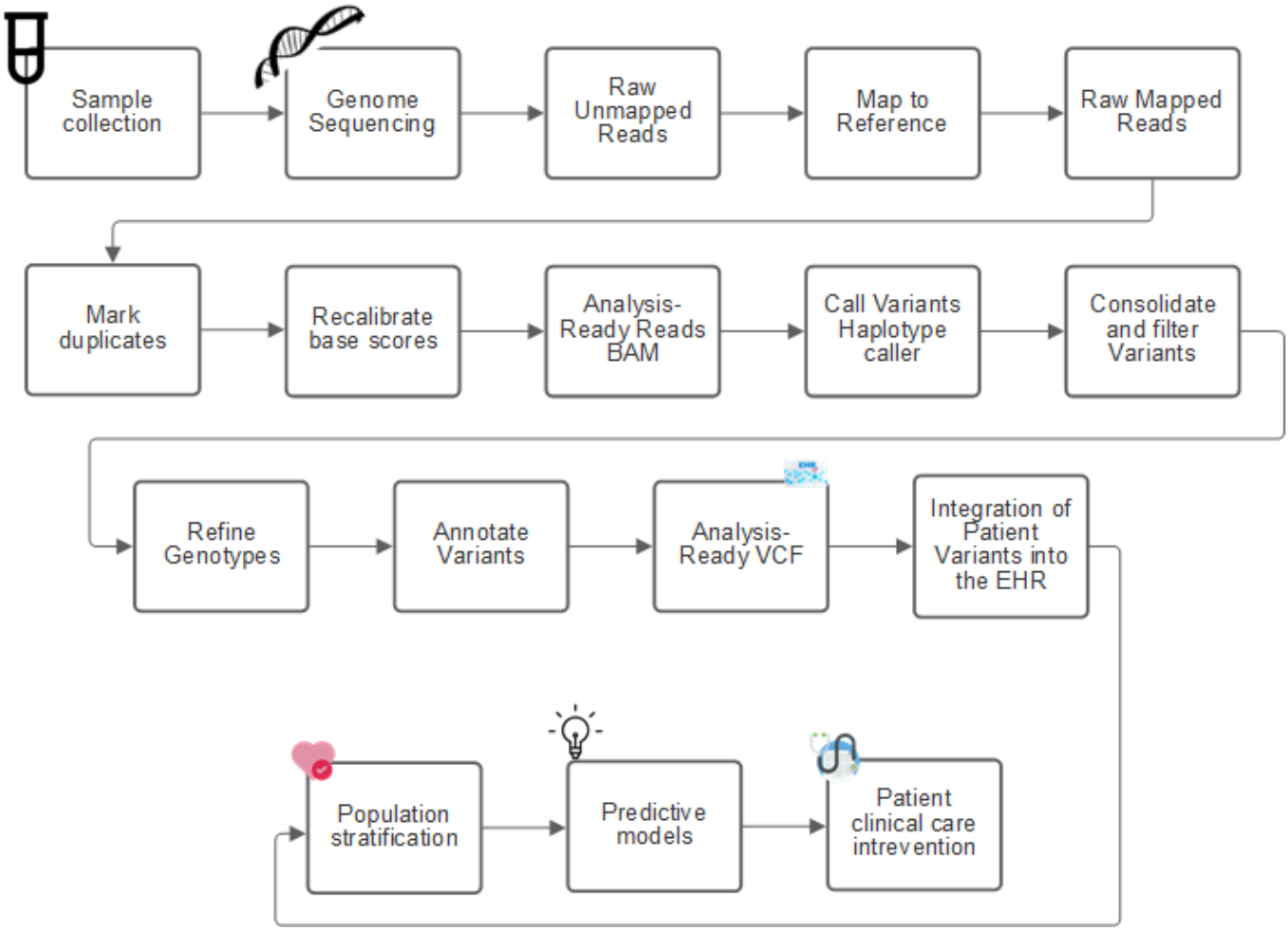
En líneas generales, la genómica se puede clasificar en los siguientes pasos. Esta no es una lista exhaustiva:

1. Recogida de muestras.
2. "Secuenciación genómica" uso de un secuenciador para generar los datos sin procesar.
3. Preprocesamiento. Por ejemplo: "deduplicación" uso "Picard".
4. Análisis genómico.
    a. Asignación a un genoma de referencia.

b. "Variante" La identificación y la anotación se realizan normalmente con GATK y herramientas similares.

5. Integración en el sistema de historiales médicos electrónicos (EHR).
6. "Estratificación poblacional" e identificación de la variación genética a través de la ubicación geográfica y el origen étnico.
7. "Modelos predictivos" utilizando un polimorfismo significativo de un solo nucleótido.
8. "Validación".

En la siguiente figura se muestra el proceso desde el muestreo hasta la identificación de variantes, la anotación y la predicción.



El proyecto Genoma humano se completó en abril de 2003 y el proyecto hizo una simulación de muy alta calidad de la secuencia del genoma humano disponible en el dominio público. Este genoma de referencia inició una explosión en la investigación y el desarrollo de capacidades de genómica. Prácticamente cada dolencia humana tiene una firma en los genes de ese ser humano. Hasta hace poco, los médicos estaban aprovechando los genes para predecir y determinar defectos de nacimiento como la anemia drepanocítica, que es causada por un cierto patrón de herencia causado por un cambio en un solo gen. El tesoro de los datos que el proyecto del genoma humano ha puesto a su disposición llevó a la llegada del estado actual de las capacidades genómicas.

La genómica ofrece un amplio conjunto de ventajas. A continuación se presenta un pequeño conjunto de beneficios en los ámbitos de la salud y las ciencias de la vida:

- Mejor diagnóstico en el punto de atención

- Mejor pronóstico
- Medicina de precisión
- Planes de tratamiento personalizados
- Mejor control de enfermedades
- Reducción de acontecimientos adversos
- Mejora del acceso a las terapias
- Mejor control de enfermedades
- Participación efectiva en ensayos clínicos y mejor selección de pacientes para ensayos clínicos basados en genotipos.

La genómica es un "bestia con cuatro cabezas," debido a las demandas computacionales que se encuentran a lo largo del ciclo de vida de un conjunto de datos: adquisición, almacenamiento, distribución y análisis.

Kit de herramientas de análisis de genoma (GATK)

GATK fue desarrollado como una plataforma de ciencia de datos en el "Instituto amplio". GATK es un conjunto de herramientas de código abierto que permiten el análisis del genoma, específicamente el descubrimiento de variantes, la identificación, la anotación y el genotipado. Una de las ventajas de GATK es que el conjunto de herramientas y comandos se pueden encadenar para formar un flujo de trabajo completo. Los principales desafíos que enfrenta el instituto general son los siguientes:

- Entender las causas profundas y los mecanismos biológicos de las enfermedades.
- Identificar las intervenciones terapéuticas que actúen en la causa fundamental de una enfermedad.
- Entender la línea de visión de las variantes a la función en la fisiología humana.
- Crear estándares y políticas "marcos de trabajo" para representación de datos genómicos, almacenamiento, análisis, seguridad, etc.
- Estandarizar y socializar las bases de datos de agregación de genomas interoperables (gnomAD).
- Monitoreo, diagnóstico y tratamiento basados en el genoma de pacientes con mayor precisión.
- Ayudar a implementar herramientas que predicen enfermedades mucho antes de que aparezcan los síntomas.
- Crear y empoderar a una comunidad de colaboradores interdisciplinarios para ayudar a enfrentar los problemas más difíciles e importantes de la biomedicina.

Según GATK y el instituto general, la secuenciación del genoma debe ser tratada como un protocolo en un laboratorio de patología; cada tarea está bien documentada, optimizada, reproducible y consistente entre muestras y experimentos. El siguiente es un conjunto de pasos recomendados por el Instituto amplio, para más información, ver el "Sitio web de GATK".

Configuración de FlexPod

La validación de cargas de trabajo genómica incluye una configuración desde cero de una plataforma de infraestructura FlexPod. La plataforma FlexPod tiene una alta disponibilidad y se puede escalar de forma independiente; por ejemplo, red, almacenamiento y recursos informáticos se pueden escalar de forma independiente. Utilizamos la siguiente guía de diseño validado por Cisco como documento de arquitectura de referencia para configurar el entorno FlexPod: "FlexPod Datacenter con VMware vSphere 7.0 y ONTAP 9.7 de NetApp". Consulte los aspectos destacados de la siguiente configuración de la plataforma FlexPod:

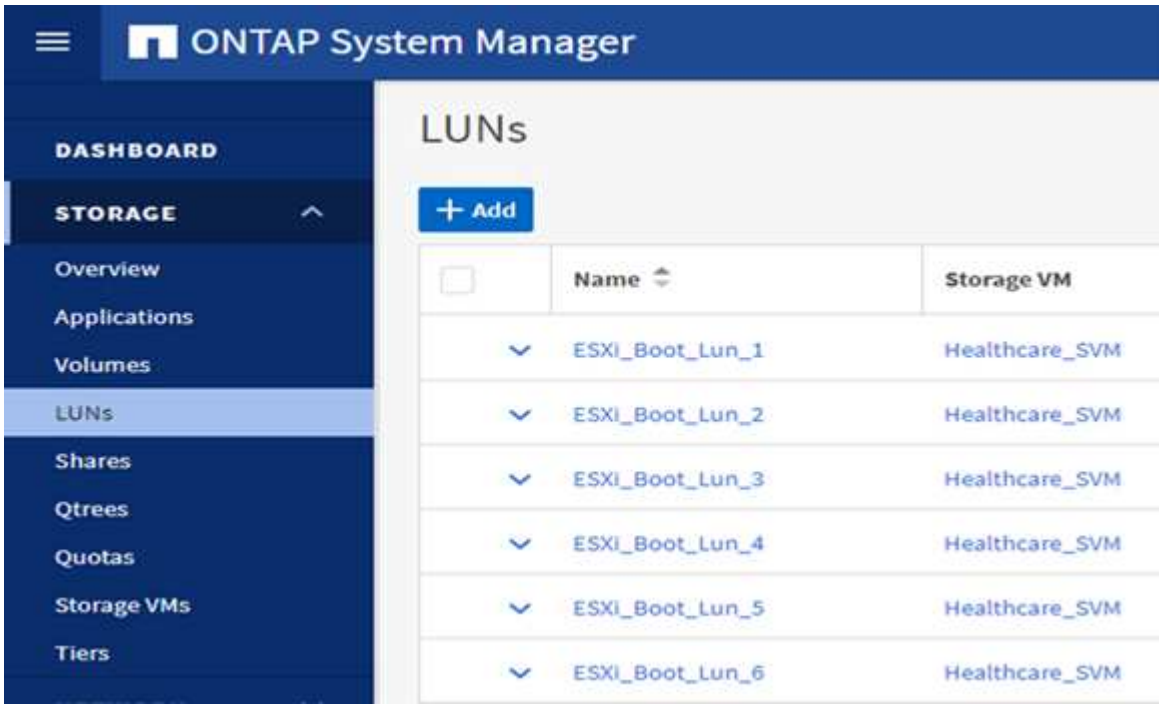
Para realizar la configuración de FlexPod Lab, realice los siguientes pasos:

1. La configuración y validación de FlexPod Lab utiliza las siguientes reservas IP4 y VLAN.

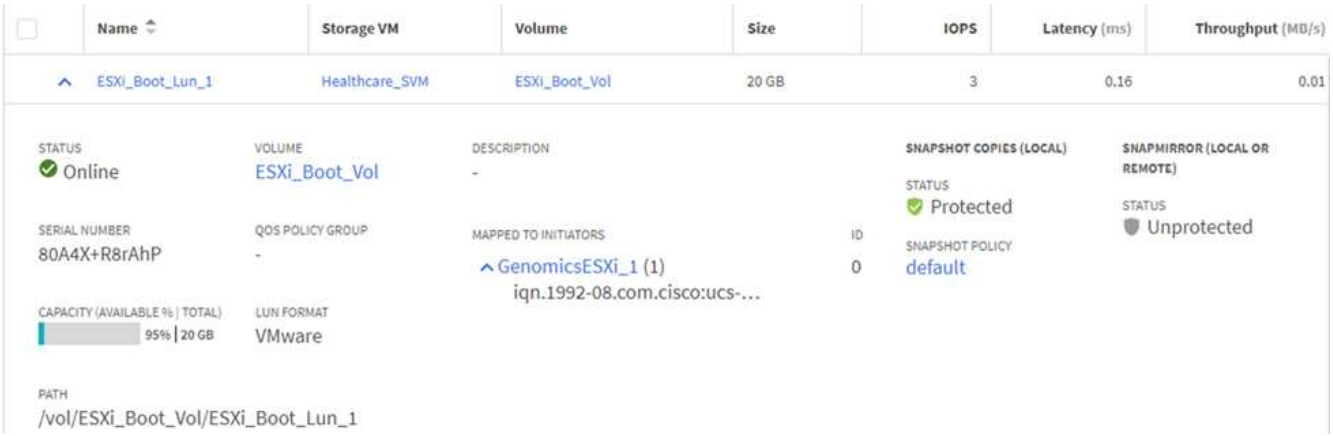
IP Reservations

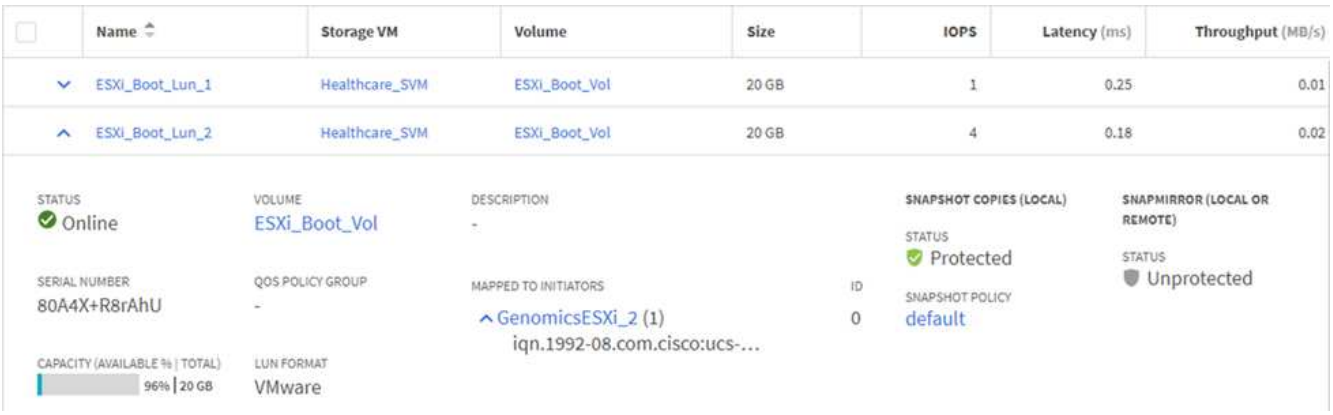
VLAN	IP Range	Subnet Mask	Purpose
3281	172.21.25 /24	255.255.255.0	IB-MGMT
3282	172.21.26 /24	255.255.255.0	vMotion
3283	172.21.27 /24	255.255.255.0	VM
3284	172.21.28 /24	255.255.255.0	NFS
3285	172.21.29 /24	255.255.255.0	iSCSI-A
3286	172.21.30 /24	255.255.255.0	iSCSI-B

2. Configure los LUN de arranque basados en iSCSI en la SVM ONTAP.



3. Asigne LUN a iGroups iSCSI.

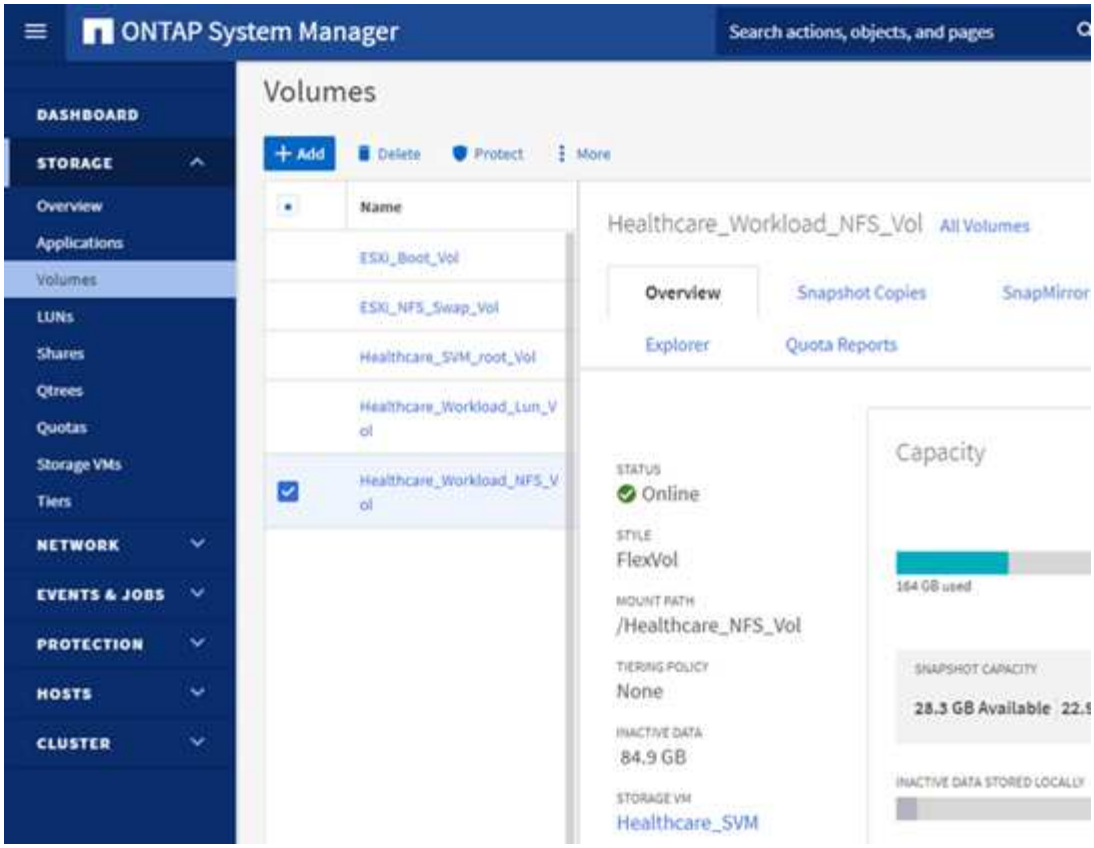




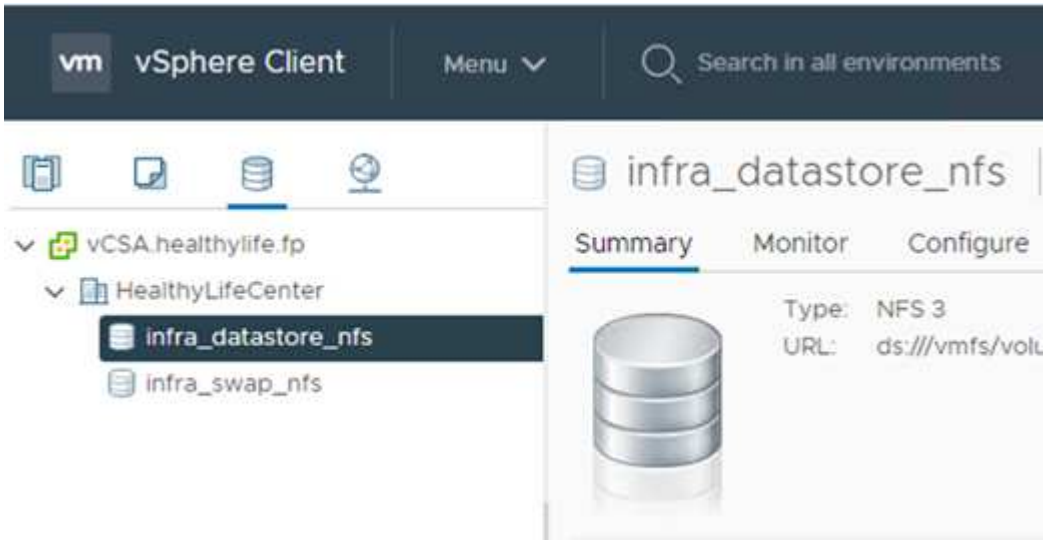
4. Instale vSphere 7.0 con arranque iSCSI.
5. Registre hosts ESXi en vCenter.



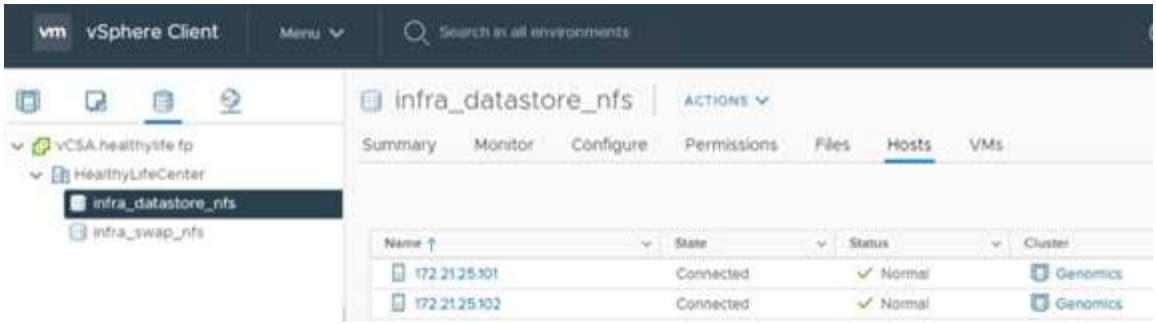
6. Aprovisione un almacén de datos NFS `infra_datastore_nfs` En el almacenamiento de ONTAP.



7. Añada el almacén de datos a vCenter.



8. Con vCenter, añada un almacén de datos NFS a los hosts ESXi.



9. Mediante el para vCenter, cree un equipo virtual Red Hat Enterprise Linux (RHEL) 8.3 para ejecutar GATK.
10. Un almacén de datos NFS se presenta a la máquina virtual y se monta en `/mnt/genomics`, Que se utiliza para almacenar ejecutables de GATK, secuencias de comandos, archivos de mapa de alineación binaria (BAM), archivos de referencia, archivos de índice, archivos de diccionario y archivos de salida para llamadas de variante.

```
[root@genomics1 genomics]# df | grep genomics
/dev/sdb              308587328  5699492 287142812   2% /mnt/genomics
[root@genomics1 genomics]#
```

Configuración y ejecución de GATK

Instale los siguientes requisitos previos en Red Hat Enterprise 8.3 Linux VM:

- Java 8 o SDK 1.8 o posterior
- Descargue GATK 4.2.0.0 de The Broad Institute "El sitio de GitHub". Los datos de la secuencia del genoma se almacenan generalmente en forma de una serie de columnas ASCII delimitadas por tabulaciones. Sin embargo, ASCII toma demasiado espacio para almacenar. Por lo tanto, un nuevo estándar evolucionó llamado un archivo BAM (*.bam). Un archivo BAM almacena los datos de secuencia en forma comprimida, indizada y binaria. Nosotros "descargado" Un conjunto de archivos BAM disponibles públicamente para la ejecución de GATK desde el "dominio público". También descargamos archivos de índice (*.bai), archivos de diccionario (*. dict) y archivos de datos de referencia (*. fasta) del mismo dominio público.

Después de la descarga, el kit de herramientas GATK tiene un archivo JAR y un conjunto de secuencias de comandos de soporte.

- `gatk-package-4.2.0.0-local.jar` ejecutable
- `gatk` archivo de script.

Descargamos los archivos BAM y los correspondientes archivos de índice, diccionario y genoma de referencia para una familia que consistía en archivos padre, madre e hijo *.bam.

Motor Cromwell

Cromwell es un motor de código abierto orientado a flujos de trabajo científicos que permite la gestión del flujo de trabajo. El motor Cromwell puede funcionar en dos "modos", Modo servidor o modo de ejecución de un único flujo de trabajo. El comportamiento del motor Cromwell se puede controlar mediante el "Archivo de configuración del motor Cromwell".

- **Modo servidor.** activado "Tranquilo" Ejecución de flujos de trabajo en motor Cromwell.

- **Modo de ejecución.** el modo de ejecución es más adecuado para ejecutar flujos de trabajo individuales en Cromwell, "ref" Para obtener un conjunto completo de opciones disponibles en el modo de ejecución.

Utilizamos el motor Cromwell para ejecutar los flujos de trabajo y las tuberías a escala. El motor Cromwell utiliza un motor fácil de usar "idioma de descripción del flujo de trabajo" Lenguaje de secuencias de comandos basado en (WDL). Cromwell también admite un segundo estándar de secuencias de comandos de flujo de trabajo denominado Common Workflow Language (CWL). A lo largo de este informe técnico, utilizamos el programa WDL. El WDL fue originalmente desarrollado por el Instituto amplio para oleoductos de análisis de genoma. Los flujos de trabajo de WDL se pueden implementar utilizando varias estrategias, incluidas las siguientes:

- **Encadenamiento lineal.** como su nombre indica, la salida de la tarea#1 se envía a la tarea #2 como entrada.
- **Multi-in/out.** esto es similar al encadenamiento lineal en que cada tarea puede tener múltiples salidas enviadas como entrada a tareas posteriores.
- **Scatter-gather.** esta es una de las estrategias de integración de aplicaciones empresariales (EAI) más potentes disponible, especialmente cuando se utiliza en arquitectura basada en eventos. Cada tarea se ejecuta de forma desacoplada y el resultado de cada tarea se consolida en el resultado final.

Hay tres pasos cuando se utiliza WDL para ejecutar GATK en modo independiente:

1. Validar la sintaxis con `womtool.jar`.

```
[root@genomics1 ~]#  java -jar womtool.jar validate ghplo.wdl
```

2. Generar entradas JSON.

```
[root@genomics1 ~]#  java -jar womtool.jar inputs ghplo.wdl > ghplo.json
```

3. Ejecute el flujo de trabajo con el motor Cromwell y. `Cromwell.jar`.

```
[root@genomics1 ~]#  java -jar cromwell.jar run ghplo.wdl --inputs
ghplo.json
```

El GATK se puede ejecutar utilizando varios métodos; este documento explora tres de estos métodos.

Ejecución de GATK usando el archivo JAR

Veamos una sola versión de la ejecución de la canalización de llamadas usando la variante de haplotipo que llama.

```
[root@genomics1 ~]#  java -Dsamjdk.use_async_io_read_samtools=false \
-Dsamjdk.use_async_io_write_samtools=true \
-Dsamjdk.use_async_io_write_tribble=false \
-Dsamjdk.compression_level=2 \
-jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar \
HaplotypeCaller \
--input /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
--output workshop_1906_2-germline_bams_father.validation.vcf \
--reference /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta
```

En este método de ejecución, utilizamos el archivo JAR de ejecución local GATK, utilizamos un solo comando java para invocar el archivo JAR y pasamos varios parámetros al comando.

1. Este parámetro indica que estamos invocando el `HaplotypeCaller` canalización de llamada variante.
2. `-- input` Especifica el archivo BAM de entrada.
3. `--output` especifica el archivo de salida de variante en formato de llamada variante (*.vcf) ("ref").
4. Con la `--reference` parámetro, estamos pasando un genoma de referencia.

Una vez ejecutada, los detalles de salida se pueden encontrar en la sección "Salida para la ejecución de GATK utilizando el archivo JAR."

Ejecución de GATK usando el script ./gatk

El kit de herramientas de GATK se puede ejecutar usando el `./gatk` guión. Examinemos el siguiente comando:

```
[root@genomics1 execution]# ./gatk \
--java-options "-Xmx4G" \
HaplotypeCaller \
-I /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
-R /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
-O /mnt/genomics/GATK/TEST\ DATA/variants.vcf
```

Pasamos varios parámetros al comando.

- Este parámetro indica que estamos invocando el `HaplotypeCaller` canalización de llamada variante.
- `-I` Especifica el archivo BAM de entrada.
- `-O` especifica el archivo de salida de variante en formato de llamada variante (*.vcf) ("ref").
- Con la `-R` parámetro, estamos pasando un genoma de referencia.

Una vez ejecutada, los detalles de salida se pueden encontrar en la sección

Ejecución del GATK con el motor de Cromwell

Utilizamos el motor Cromwell para gestionar la ejecución de GATK. Examinemos la línea de comandos y sus parámetros.

```
[root@genomics1 genomics]# java -jar cromwell-65.jar \
run /mnt/genomics/GATK/seq/ghplo.wdl  \
--inputs /mnt/genomics/GATK/seq/ghplo.json
```

Aquí, invocamos el comando Java pasando el `-jar` parámetro para indicar que queremos ejecutar un archivo jar, por ejemplo, `Cromwell-65.jar`. Se ha pasado el siguiente parámetro (`run`) Indica que el motor Cromwell está funcionando en modo de funcionamiento, la otra opción posible es modo de servidor. El siguiente parámetro es `*.wdl` Que el modo Run debe utilizar para ejecutar las tuberías. El siguiente parámetro es el conjunto de parámetros de entrada de los flujos de trabajo que se están ejecutando.

Esto es lo que el contenido del `ghplo.wdl` aspecto del archivo:

```
[root@genomics1 seq]# cat ghplo.wdl
workflow helloHaplotypeCaller {
  call haplotypeCaller
}
task haplotypeCaller {
  File GATK
  File RefFasta
  File RefIndex
  File RefDict
  String sampleName
  File inputBAM
  File bamIndex
  command {
    java -jar ${GATK} \
         HaplotypeCaller \
        -R ${RefFasta} \
        -I ${inputBAM} \
        -O ${sampleName}.raw.indels.snps.vcf
  }
  output {
    File rawVCF = "${sampleName}.raw.indels.snps.vcf"
  }
}
[root@genomics1 seq]#
```

Aquí está el archivo JSON correspondiente con las entradas del motor Cromwell.

```
[root@genomics1 seq]# cat ghplo.json
{
"helloHaplotypeCaller.haplotypeCaller.GATK": "/mnt/genomics/GATK/gatk-
4.2.0.0/gatk-package-4.2.0.0-local.jar",
"helloHaplotypeCaller.haplotypeCaller.RefFasta": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta",
"helloHaplotypeCaller.haplotypeCaller.RefIndex": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta.fai",
"helloHaplotypeCaller.haplotypeCaller.RefDict": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.dict",
"helloHaplotypeCaller.haplotypeCaller.sampleName": "fatherbam",
"helloHaplotypeCaller.haplotypeCaller.inputBAM": "/mnt/genomics/GATK/TEST
DATA/bam/workshop_1906_2-germline_bams_father.bam",
"helloHaplotypeCaller.haplotypeCaller.bamIndex": "/mnt/genomics/GATK/TEST
DATA/bam/workshop_1906_2-germline_bams_father.bai"
}
[root@genomics1 seq]#
```

Tenga en cuenta que Cromwell utiliza una base de datos en memoria para la ejecución. Una vez ejecutado, el registro de salida se puede ver en la sección "Salida para la ejecución del GATK utilizando el motor Cromwell."

Para ver un conjunto completo de pasos sobre cómo ejecutar GATK, consulte "Documentación de GATK".

"Siguiente: Salida para la ejecución de GATK usando el archivo JAR."

Salida para la ejecución de GATK utilizando el archivo JAR

"Anterior: Genómica - instalación y ejecución de GATK."

La ejecución de GATK usando el archivo JAR produjo la siguiente salida de muestra.

```
[root@genomics1 execution]# java -Dsamjdk.use_async_io_read_samtools=false
\
-Dsamjdk.use_async_io_write_samtools=true \
-Dsamjdk.use_async_io_write_tribble=false \
-Dsamjdk.compression_level=2 \
-jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar \
HaplotypeCaller \
--input /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
--output workshop_1906_2-germline_bams_father.validation.vcf \
--reference /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
22:52:58.430 INFO  NativeLibraryLoader - Loading libgkl_compression.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_compression.so
```

```
Aug 17, 2021 10:52:58 PM
shaded.cloud_nio.com.google.auth.oauth2.ComputeEngineCredentials
runningOnComputeEngine
INFO: Failed to detect whether we are running on Google Compute Engine.
22:52:58.541 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller - The Genome Analysis Toolkit (GATK)
v4.2.0.0
22:52:58.542 INFO  HaplotypeCaller - For support and documentation go to
https://software.broadinstitute.org/gatk/
22:52:58.542 INFO  HaplotypeCaller - Executing as
root@genomics1.healthylife.fp on Linux v4.18.0-305.3.1.el8_4.x86_64 amd64
22:52:58.542 INFO  HaplotypeCaller - Java runtime: OpenJDK 64-Bit Server
VM v1.8.0_302-b08
22:52:58.542 INFO  HaplotypeCaller - Start Date/Time: August 17, 2021
10:52:58 PM EDT
22:52:58.542 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller - HTSJDK Version: 2.24.0
22:52:58.542 INFO  HaplotypeCaller - Picard Version: 2.25.0
22:52:58.542 INFO  HaplotypeCaller - Built for Spark Version: 2.4.5
22:52:58.542 INFO  HaplotypeCaller - HTSJDK Defaults.COMPRESSION_LEVEL : 2
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_READ_FOR_SAMTOOLS : false
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_SAMTOOLS : true
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_TRIBBLE : false
22:52:58.543 INFO  HaplotypeCaller - Deflater: IntelDeflater
22:52:58.543 INFO  HaplotypeCaller - Inflater: IntelInflater
22:52:58.543 INFO  HaplotypeCaller - GCS max retries/reopens: 20
22:52:58.543 INFO  HaplotypeCaller - Requester pays: disabled
22:52:58.543 INFO  HaplotypeCaller - Initializing engine
22:52:58.804 INFO  HaplotypeCaller - Done initializing engine
22:52:58.809 INFO  HaplotypeCallerEngine - Disabling physical phasing,
which is supported only for reference-model confidence output
22:52:58.820 INFO  NativeLibraryLoader - Loading libgkl_utils.so from
jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_utils.so
22:52:58.821 INFO  NativeLibraryLoader - Loading libgkl_pairhmm_omp.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_pairhmm_omp.so
22:52:58.854 INFO  IntelPairHmm - Using CPU-supported AVX-512 instructions
22:52:58.854 INFO  IntelPairHmm - Flush-to-zero (FTZ) is enabled when
```

```
running PairHMM
22:52:58.854 INFO  IntelPairHmm - Available threads: 16
22:52:58.854 INFO  IntelPairHmm - Requested threads: 4
22:52:58.854 INFO  PairHMM - Using the OpenMP multi-threaded AVX-
accelerated native PairHMM implementation
22:52:58.872 INFO  ProgressMeter - Starting traversal
22:52:58.873 INFO  ProgressMeter -        Current Locus  Elapsed Minutes
Regions Processed   Regions/Minute
22:53:00.733 WARN  InbreedingCoeff - InbreedingCoeff will not be
calculated at position 20:9999900 and possibly subsequent; at least 10
samples must have called genotypes
22:53:08.873 INFO  ProgressMeter -          20:17538652              0.2
58900         353400.0
22:53:17.681 INFO  HaplotypeCaller - 405 read(s) filtered by:
MappingQualityReadFilter
0 read(s) filtered by: MappingQualityAvailableReadFilter
0 read(s) filtered by: MappedReadFilter
0 read(s) filtered by: NotSecondaryAlignmentReadFilter
6628 read(s) filtered by: NotDuplicateReadFilter
0 read(s) filtered by: PassesVendorQualityCheckReadFilter
0 read(s) filtered by: NonZeroReferenceLengthAlignmentReadFilter
0 read(s) filtered by: GoodCigarReadFilter
0 read(s) filtered by: WellformedReadFilter
7033 total reads filtered
22:53:17.681 INFO  ProgressMeter -          20:63024652              0.3
210522         671592.9
22:53:17.681 INFO  ProgressMeter - Traversal complete. Processed 210522
total regions in 0.3 minutes.
22:53:17.687 INFO  VectorLoglessPairHMM - Time spent in setup for JNI call
: 0.010347438
22:53:17.687 INFO  PairHMM - Total compute time in PairHMM
computeLogLikelihoods() : 0.259172573
22:53:17.687 INFO  SmithWatermanAligner - Total compute time in java
Smith-Waterman : 1.27 sec
22:53:17.687 INFO  HaplotypeCaller - Shutting down engine
[August 17, 2021 10:53:17 PM EDT]
org.broadinstitute.hellbender.tools.walkers.haplotypecaller.HaplotypeCalle
r done. Elapsed time: 0.32 minutes.
Runtime.totalMemory()=5561122816
[root@genomics1 execution]#
```

Observe que el archivo de salida se encuentra en la ubicación especificada después de la ejecución.

Salida para la ejecución de GATK usando el script ./gatk

"Anterior: Salida para la ejecución de GATK usando el archivo JAR."

La ejecución de GATK con el útil `./gatk` la secuencia de comandos produjo la siguiente salida de ejemplo.

```
[root@genomics1 gatk-4.2.0.0]# ./gatk --java-options "-Xmx4G" \
HaplotypeCaller \
-I /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
-R /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
-O /mnt/genomics/GATK/TEST\ DATA/variants.vcf
Using GATK jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar
Running:
    java -Dsamjdk.use_async_io_read_samtools=false
-Dsamjdk.use_async_io_write_samtools=true
-Dsamjdk.use_async_io_write_tribble=false -Dsamjdk.compression_level=2
-Xmx4G -jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar
HaplotypeCaller -I /mnt/genomics/GATK/TEST DATA/bam/workshop_1906_2-
germline_bams_father.bam -R /mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta -O /mnt/genomics/GATK/TEST
DATA/variants.vcf
23:29:45.553 INFO  NativeLibraryLoader - Loading libgkl_compression.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_compression.so
Aug 17, 2021 11:29:45 PM
shaded.cloud_nio.com.google.auth.oauth2.ComputeEngineCredentials
runningOnComputeEngine
INFO: Failed to detect whether we are running on Google Compute Engine.
23:29:45.686 INFO  HaplotypeCaller -
------------------------------------------------------------
23:29:45.686 INFO  HaplotypeCaller - The Genome Analysis Toolkit (GATK)
v4.2.0.0
23:29:45.686 INFO  HaplotypeCaller - For support and documentation go to
https://software.broadinstitute.org/gatk/
23:29:45.687 INFO  HaplotypeCaller - Executing as
root@genomics1.healthylife.fp on Linux v4.18.0-305.3.1.el8_4.x86_64 amd64
23:29:45.687 INFO  HaplotypeCaller - Java runtime: OpenJDK 64-Bit Server
VM v11.0.12+7-LTS
23:29:45.687 INFO  HaplotypeCaller - Start Date/Time: August 17, 2021 at
11:29:45 PM EDT
23:29:45.687 INFO  HaplotypeCaller -
------------------------------------------------------------
23:29:45.687 INFO  HaplotypeCaller -
------------------------------------------------------------
23:29:45.687 INFO  HaplotypeCaller - HTSJDK Version: 2.24.0
```

```
23:29:45.687 INFO  HaplotypeCaller - Picard Version: 2.25.0
23:29:45.687 INFO  HaplotypeCaller - Built for Spark Version: 2.4.5
23:29:45.688 INFO  HaplotypeCaller - HTSJDK Defaults.COMPRESSION_LEVEL : 2
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_READ_FOR_SAMTOOLS : false
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_SAMTOOLS : true
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_TRIBBLE : false
23:29:45.688 INFO  HaplotypeCaller - Deflater: IntelDeflater
23:29:45.688 INFO  HaplotypeCaller - Inflater: IntelInflater
23:29:45.688 INFO  HaplotypeCaller - GCS max retries/reopens: 20
23:29:45.688 INFO  HaplotypeCaller - Requester pays: disabled
23:29:45.688 INFO  HaplotypeCaller - Initializing engine
23:29:45.804 INFO  HaplotypeCaller - Done initializing engine
23:29:45.809 INFO  HaplotypeCallerEngine - Disabling physical phasing,
which is supported only for reference-model confidence output
23:29:45.818 INFO  NativeLibraryLoader - Loading libgkl_utils.so from
jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_utils.so
23:29:45.819 INFO  NativeLibraryLoader - Loading libgkl_pairhmm_omp.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_pairhmm_omp.so
23:29:45.852 INFO  IntelPairHmm - Using CPU-supported AVX-512 instructions
23:29:45.852 INFO  IntelPairHmm - Flush-to-zero (FTZ) is enabled when
running PairHMM
23:29:45.852 INFO  IntelPairHmm - Available threads: 16
23:29:45.852 INFO  IntelPairHmm - Requested threads: 4
23:29:45.852 INFO  PairHMM - Using the OpenMP multi-threaded AVX-
accelerated native PairHMM implementation
23:29:45.868 INFO  ProgressMeter - Starting traversal
23:29:45.868 INFO  ProgressMeter -        Current Locus  Elapsed Minutes
Regions Processed   Regions/Minute
23:29:47.772 WARN  InbreedingCoeff - InbreedingCoeff will not be
calculated at position 20:9999900 and possibly subsequent; at least 10
samples must have called genotypes
23:29:55.868 INFO  ProgressMeter -          20:18885652              0.2
63390         380340.0
23:30:04.389 INFO  HaplotypeCaller - 405 read(s) filtered by:
MappingQualityReadFilter
0 read(s) filtered by: MappingQualityAvailableReadFilter
0 read(s) filtered by: MappedReadFilter
0 read(s) filtered by: NotSecondaryAlignmentReadFilter
6628 read(s) filtered by: NotDuplicateReadFilter
0 read(s) filtered by: PassesVendorQualityCheckReadFilter
0 read(s) filtered by: NonZeroReferenceLengthAlignmentReadFilter
```

```
0 read(s) filtered by: GoodCigarReadFilter
0 read(s) filtered by: WellformedReadFilter
7033 total reads filtered
23:30:04.389 INFO  ProgressMeter -          20:63024652              0.3
210522         681999.9
23:30:04.389 INFO  ProgressMeter - Traversal complete. Processed 210522
total regions in 0.3 minutes.
23:30:04.395 INFO  VectorLoglessPairHMM - Time spent in setup for JNI call
: 0.012129203000000002
23:30:04.395 INFO  PairHMM - Total compute time in PairHMM
computeLogLikelihoods() : 0.267345217
23:30:04.395 INFO  SmithWatermanAligner - Total compute time in java
Smith-Waterman : 1.23 sec
23:30:04.395 INFO  HaplotypeCaller - Shutting down engine
[August 17, 2021 at 11:30:04 PM EDT]
org.broadinstitute.hellbender.tools.walkers.haplotypecaller.HaplotypeCalle
r done. Elapsed time: 0.31 minutes.
Runtime.totalMemory()=2111832064
[root@genomics1 gatk-4.2.0.0]#
```

Observe que el archivo de salida se encuentra en la ubicación especificada después de la ejecución.

"Siguiente: Salida para la ejecución de GATK con el motor Cromwell."

Salida para la ejecución del GATK utilizando el motor Cromwell

La ejecución de GATK con el motor Cromwell produjo la siguiente salida de muestra.

```
[root@genomics1 genomics]# java -jar  cromwell-65.jar run
/mnt/genomics/GATK/seq/ghplo.wdl  --inputs
/mnt/genomics/GATK/seq/ghplo.json
[2021-08-18 17:10:50,78] [info] Running with database db.url =
jdbc:hsqldb:mem:856a1f0d-9a0d-42e5-9199-
5e6c1d0f72dd;shutdown=false;hsqldb.tx=mvcc
[2021-08-18 17:10:57,74] [info] Running migration
RenameWorkflowOptionsInMetadata with a read batch size of 100000 and a
write batch size of 100000
[2021-08-18 17:10:57,75] [info] [RenameWorkflowOptionsInMetadata] 100%
[2021-08-18 17:10:57,83] [info] Running with database db.url =
jdbc:hsqldb:mem:6afe0252-2dc9-4e57-8674-
ce63c67aa142;shutdown=false;hsqldb.tx=mvcc
[2021-08-18 17:10:58,17] [info] Slf4jLogger started
[2021-08-18 17:10:58,33] [info] Workflow heartbeat configuration:
{
  "cromwellId" : "cromid-41b7e30",
  "heartbeatInterval" : "2 minutes",
```

```
  "ttl" : "10 minutes",
  "failureShutdownDuration" : "5 minutes",
  "writeBatchSize" : 10000,
  "writeThreshold" : 10000
}
[2021-08-18 17:10:58,38] [info] Metadata summary refreshing every 1
second.
[2021-08-18 17:10:58,38] [info] No metadata archiver defined in config
[2021-08-18 17:10:58,38] [info] No metadata deleter defined in config
[2021-08-18 17:10:58,40] [info] KvWriteActor configured to flush with
batch size 200 and process rate 5 seconds.
[2021-08-18 17:10:58,40] [info] WriteMetadataActor configured to flush
with batch size 200 and process rate 5 seconds.
[2021-08-18 17:10:58,44] [info] CallCacheWriteActor configured to flush
with batch size 100 and process rate 3 seconds.
[2021-08-18 17:10:58,44] [warn] 'docker.hash-lookup.gcr-api-queries-per-
100-seconds' is being deprecated, use 'docker.hash-lookup.gcr.throttle'
instead (see reference.conf)
[2021-08-18 17:10:58,54] [info] JobExecutionTokenDispenser - Distribution
rate: 50 per 1 seconds.
[2021-08-18 17:10:58,58] [info] SingleWorkflowRunnerActor: Version 65
[2021-08-18 17:10:58,58] [info] SingleWorkflowRunnerActor: Submitting
workflow
[2021-08-18 17:10:58,64] [info] Unspecified type (Unspecified version)
workflow 3e246147-b1a9-41dc-8679-319f81b7701e submitted
[2021-08-18 17:10:58,66] [info] SingleWorkflowRunnerActor: Workflow
submitted 3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,66] [info] 1 new workflows fetched by cromid-41b7e30:
3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,67] [info] WorkflowManagerActor: Starting workflow
3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,68] [info] WorkflowManagerActor: Successfully started
WorkflowActor-3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,68] [info] Retrieved 1 workflows from the
WorkflowStoreActor
[2021-08-18 17:10:58,70] [info] WorkflowStoreHeartbeatWriteActor
configured to flush with batch size 10000 and process rate 2 minutes.
[2021-08-18 17:10:58,76] [info] MaterializeWorkflowDescriptorActor
[3e246147]: Parsing workflow as WDL draft-2
[2021-08-18 17:10:59,34] [info] MaterializeWorkflowDescriptorActor
[3e246147]: Call-to-Backend assignments:
helloHaplotypeCaller.haplotypeCaller -> Local
[2021-08-18 17:11:00,54] [info] WorkflowExecutionActor-3e246147-b1a9-41dc-
8679-319f81b7701e [3e246147]: Starting
helloHaplotypeCaller.haplotypeCaller
[2021-08-18 17:11:01,56] [info] Assigned new job execution tokens to the
```

```
following groups: 3e246147: 1
[2021-08-18 17:11:01,70] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: java -jar
/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-41dc-
8679-319f81b7701e/call-haplotypeCaller/inputs/-179397211/gatk-package-
4.2.0.0-local.jar \
     HaplotypeCaller \
    -R /mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-
b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/inputs/604632695/workshop_1906_2-germline_ref_ref.fasta \
    -I /mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-
b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/inputs/604617202/workshop_1906_2-germline_bams_father.bam
\
    -O fatherbam.raw.indels.snps.vcf
[2021-08-18 17:11:01,72] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: executing: /bin/bash
/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-41dc-
8679-319f81b7701e/call-haplotypeCaller/execution/script
[2021-08-18 17:11:03,49] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: job id: 26867
[2021-08-18 17:11:03,53] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: Status change from -
to WaitingForReturnCode
[2021-08-18 17:11:03,54] [info] Not triggering log of token queue status.
Effective log interval = None
[2021-08-18 17:11:23,65] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: Status change from
WaitingForReturnCode to Done
[2021-08-18 17:11:25,04] [info] WorkflowExecutionActor-3e246147-b1a9-41dc-
8679-319f81b7701e [3e246147]: Workflow helloHaplotypeCaller complete.
Final Outputs:
{
  "helloHaplotypeCaller.haplotypeCaller.rawVCF": "/mnt/genomics/cromwell-
executions/helloHaplotypeCaller/3e246147-b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/execution/fatherbam.raw.indels.snps.vcf"
}
[2021-08-18 17:11:28,43] [info] WorkflowManagerActor: Workflow actor for
3e246147-b1a9-41dc-8679-319f81b7701e completed with status 'Succeeded'.
The workflow will be removed from the workflow store.
[2021-08-18 17:11:32,24] [info] SingleWorkflowRunnerActor workflow
finished with status 'Succeeded'.
{
  "outputs": {
    "helloHaplotypeCaller.haplotypeCaller.rawVCF":
"/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-
```

```
41dc-8679-319f81b7701e/call-
haplotypeCaller/execution/fatherbam.raw.indels.snps.vcf"
  },
  "id": "3e246147-b1a9-41dc-8679-319f81b7701e"
}
[2021-08-18 17:11:33,45] [info] Workflow polling stopped
[2021-08-18 17:11:33,46] [info] 0 workflows released by cromid-41b7e30
[2021-08-18 17:11:33,46] [info] Shutting down WorkflowStoreActor - Timeout
= 5 seconds
[2021-08-18 17:11:33,46] [info] Shutting down WorkflowLogCopyRouter -
Timeout = 5 seconds
[2021-08-18 17:11:33,46] [info] Shutting down JobExecutionTokenDispenser -
Timeout = 5 seconds
[2021-08-18 17:11:33,46] [info] Aborting all running workflows.
[2021-08-18 17:11:33,46] [info] JobExecutionTokenDispenser stopped
[2021-08-18 17:11:33,46] [info] WorkflowStoreActor stopped
[2021-08-18 17:11:33,47] [info] WorkflowLogCopyRouter stopped
[2021-08-18 17:11:33,47] [info] Shutting down WorkflowManagerActor -
Timeout = 3600 seconds
[2021-08-18 17:11:33,47] [info] WorkflowManagerActor: All workflows
finished
[2021-08-18 17:11:33,47] [info] WorkflowManagerActor stopped
[2021-08-18 17:11:33,64] [info] Connection pools shut down
[2021-08-18 17:11:33,64] [info] Shutting down SubWorkflowStoreActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down JobStoreActor - Timeout =
1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down CallCacheWriteActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] SubWorkflowStoreActor stopped
[2021-08-18 17:11:33,64] [info] Shutting down ServiceRegistryActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down DockerHashActor - Timeout =
1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down IoProxy - Timeout = 1800
seconds
[2021-08-18 17:11:33,64] [info] CallCacheWriteActor Shutting down: 0
queued messages to process
[2021-08-18 17:11:33,64] [info] JobStoreActor stopped
[2021-08-18 17:11:33,64] [info] CallCacheWriteActor stopped
[2021-08-18 17:11:33,64] [info] KvWriteActor Shutting down: 0 queued
messages to process
[2021-08-18 17:11:33,64] [info] IoProxy stopped
[2021-08-18 17:11:33,64] [info] WriteMetadataActor Shutting down: 0 queued
messages to process
[2021-08-18 17:11:33,65] [info] ServiceRegistryActor stopped
```

```
[2021-08-18 17:11:33,65] [info] DockerHashActor stopped
[2021-08-18 17:11:33,67] [info] Database closed
[2021-08-18 17:11:33,67] [info] Stream materializer shut down
[2021-08-18 17:11:33,67] [info] WDL HTTP import resolver closed
[root@genomics1 genomics]#
```

"Siguiente: Configuración de GPU."

Configuración de GPU

"Anterior: Salida para la ejecución de GATK con el motor Cromwell."

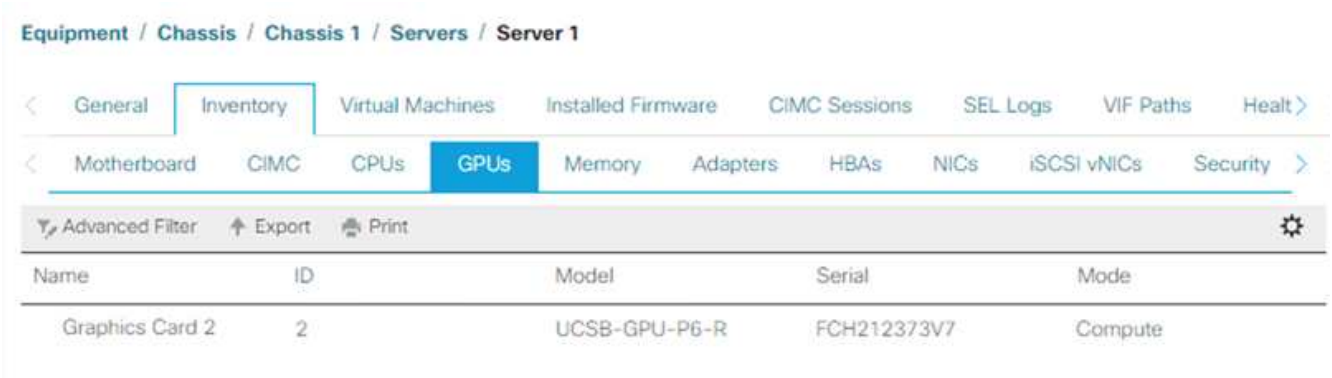
En el momento de su publicación, la herramienta GATK no tiene soporte nativo para la ejecución basada en GPU en las instalaciones. Se proporcionan las siguientes instrucciones y configuración para que los lectores puedan comprender lo sencillo que es utilizar FlexPod con una GPU NVIDIA Tesla P6 montada en la parte posterior utilizando una tarjeta intermedia PCIe para GATK.

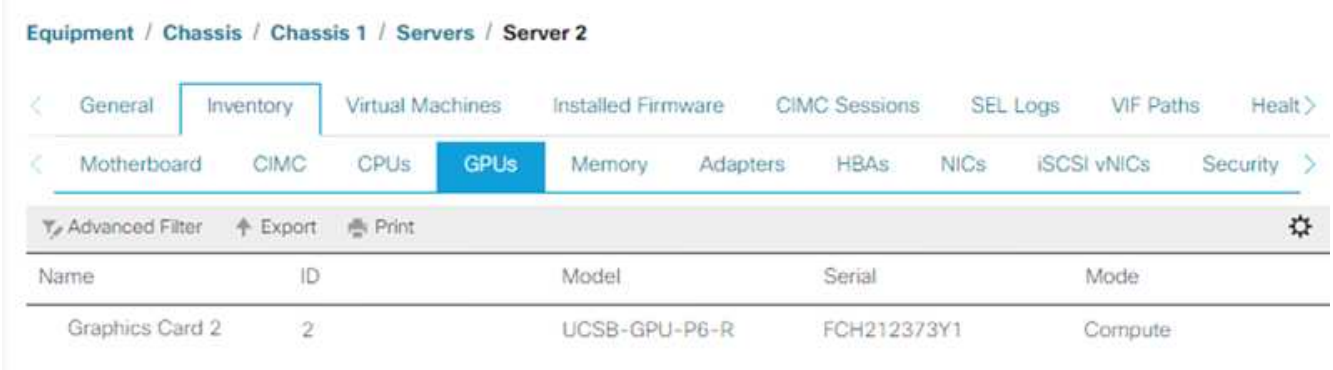
Utilizamos el siguiente diseño validado por Cisco (CVD) como arquitectura de referencia y guía de prácticas recomendadas para configurar el entorno FlexPod de modo que podamos ejecutar aplicaciones que utilizan GPU.

- "Centro de datos FlexPod para IA/ML con Cisco UCS 480 ML para aprendizaje profundo"

Este es un conjunto de puntos clave durante esta configuración:

1. Utilizamos una GPU PCIe NVIDIA Tesla P6 en una ranura intermedia en los servidores UCS B200 M5.





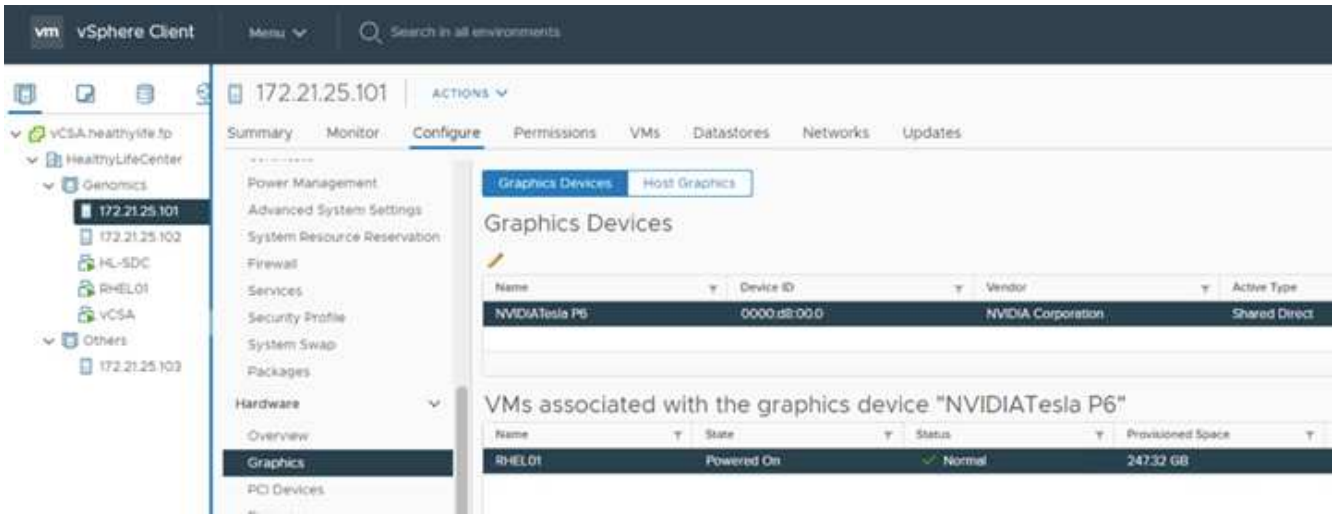
2. Para esta configuración, nos registramos en el portal de partners de NVIDIA y obtuvimos una licencia de evaluación (también conocida como autorización) para poder utilizar las GPU en el modo de computación.
3. Hemos descargado el software vGPU de NVIDIA requerido desde el sitio web para partners de NVIDIA.
4. Hemos descargado el derecho `*.bin` Archivo del sitio web del partner NVIDIA.
5. Instalamos un servidor de licencias NVIDIA vGPU y añadimos los derechos al servidor de licencias mediante `*.bin` Archivo descargado del sitio del partner de NVIDIA.
6. Asegúrese de elegir la versión correcta del software vGPU de NVIDIA para su puesta en marcha en el portal de partners de NVIDIA. Para esta configuración utilizamos la versión 460.73.02 del controlador.
7. Este comando instala el "Administrador vGPU de NVIDIA" En ESXi.

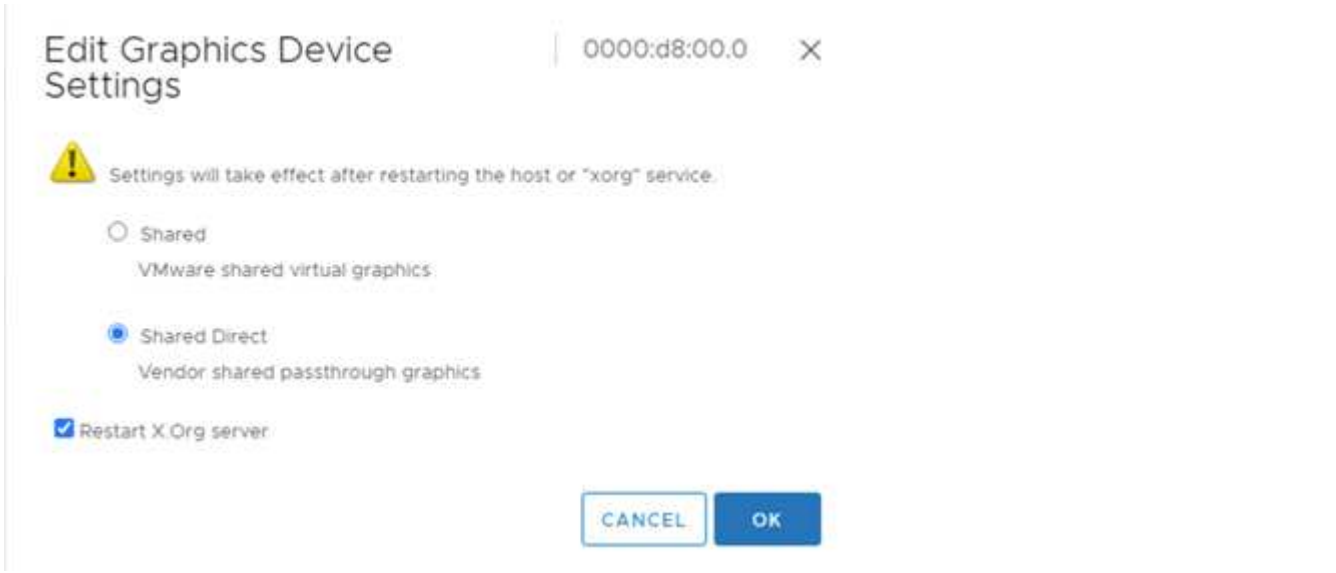
```
[root@localhost:~] esxcli software vib install -v
/vmfs/volumes/infra_datastore_nfs/nvidia/vib/NVIDIA_bootbank_NVIDIA-
VMware_ESXi_7.0_Host_Driver_460.73.02-1OEM.700.0.0.15525992.vib
Installation Result
Message: Operation finished successfully.
Reboot Required: false
VIBs Installed: NVIDIA_bootbank_NVIDIA-
VMware_ESXi_7.0_Host_Driver_460.73.02-1OEM.700.0.0.15525992
VIBs Removed:
VIBs Skipped:
```

8. Después de reiniciar el servidor ESXi, ejecute el siguiente comando para validar la instalación y comprobar el estado de las GPU.

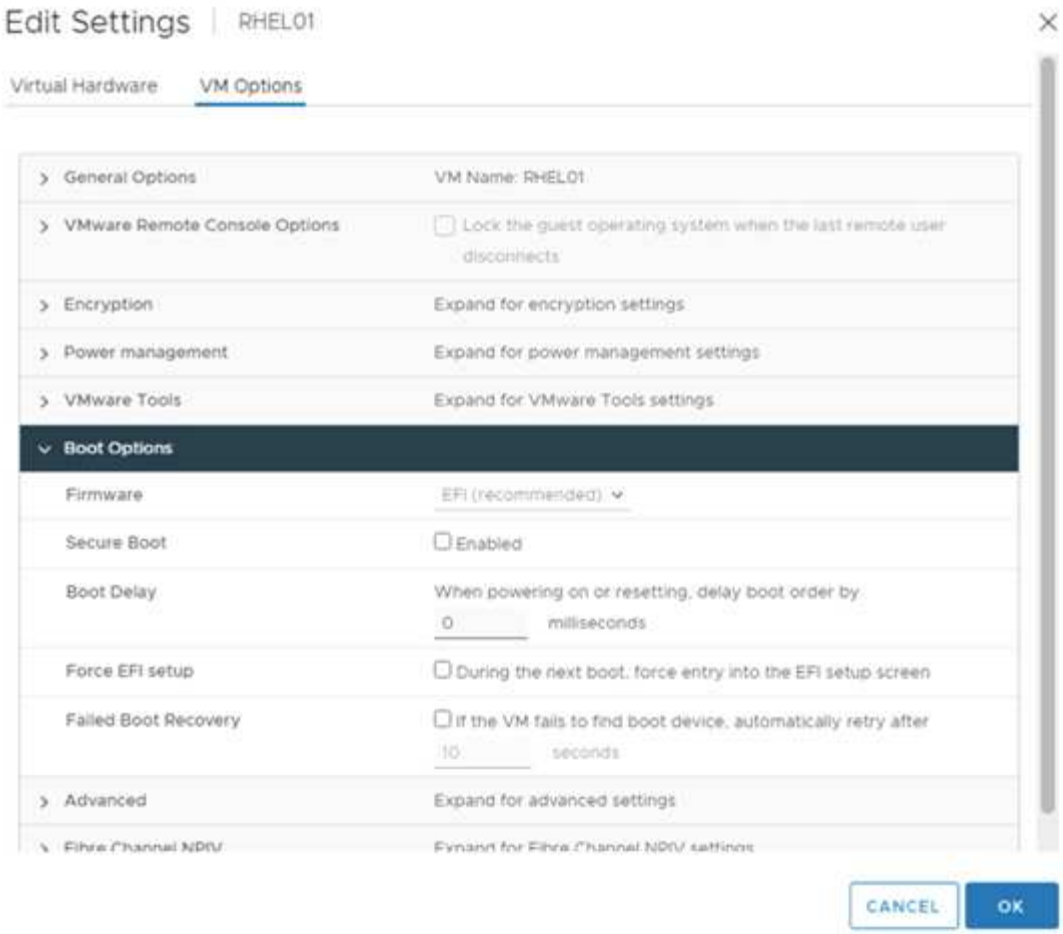
```
[root@localhost:~] nvidia-smi
Wed Aug 18 21:37:19 2021
+-----------------------------------------------------------------------------
------+
| NVIDIA-SMI 460.73.02    Driver Version: 460.73.02    CUDA Version: N/A
|
|-------------------------------+----------------------
+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
Compute M. |
|                               |                      |
MIG M. |
|===============================+======================+===============
======|
|   0  Tesla P6            On   | 00000000:D8:00.0 Off |
0 |
| N/A   35C    P8     9W /  90W |  15208MiB / 15359MiB |      0%
Default |
|                               |                      |
N/A |
+-------------------------------+----------------------
+----------------------+
+-----------------------------------------------------------------------------
------+
| Processes:
|
|  GPU   GI   CI        PID   Type   Process name                  GPU
Memory |
|        ID   ID                                                   Usage
|
|=============================================================================
======|
|    0   N/A  N/A   2812553    C+G   RHEL01
15168MiB |
+-----------------------------------------------------------------------------
------+
[root@localhost:~]
```

9. Con vCenter, "configurar" La configuración del dispositivo gráfico a “Shared Direct”.





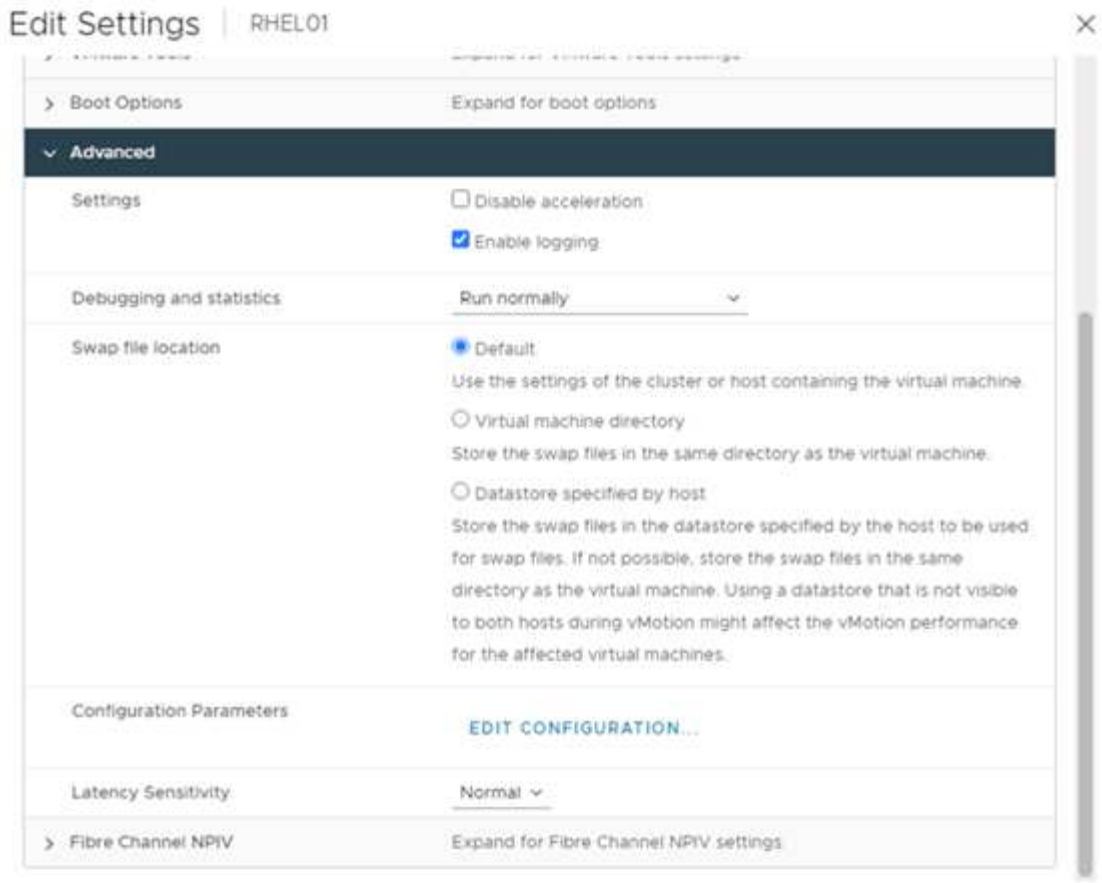
10. Asegúrese de que el arranque seguro está desactivado para el equipo virtual RedHat.
11. Asegúrese de que el firmware de VM Boot Options esté establecido en EFI ("ref").

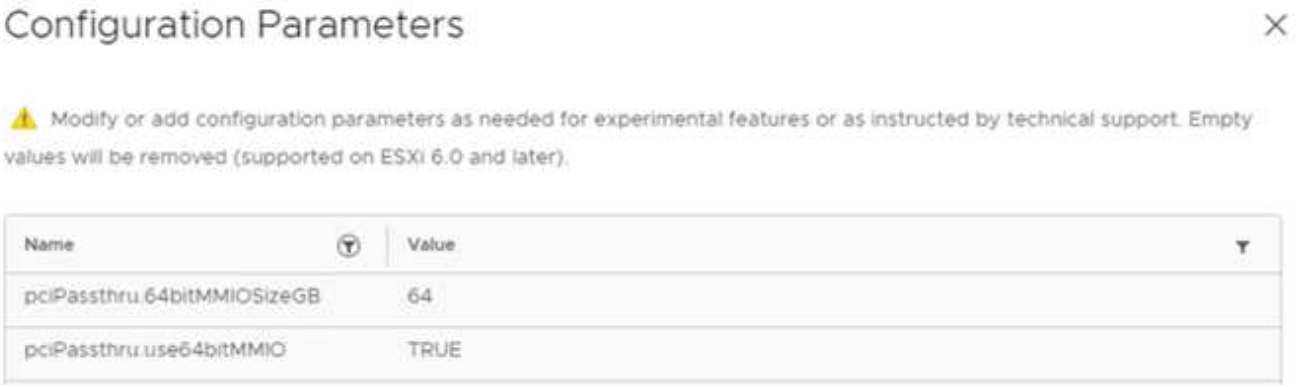


12. Asegúrese de que los siguientes PARÁMETROS se agreguen a la VM Options Advanced Edit Configuration. El valor de `pciPassthru.64bitMMIOSizeGB` El parámetro depende de la memoria de la GPU y del número de GPU asignadas a la máquina virtual. Por ejemplo:

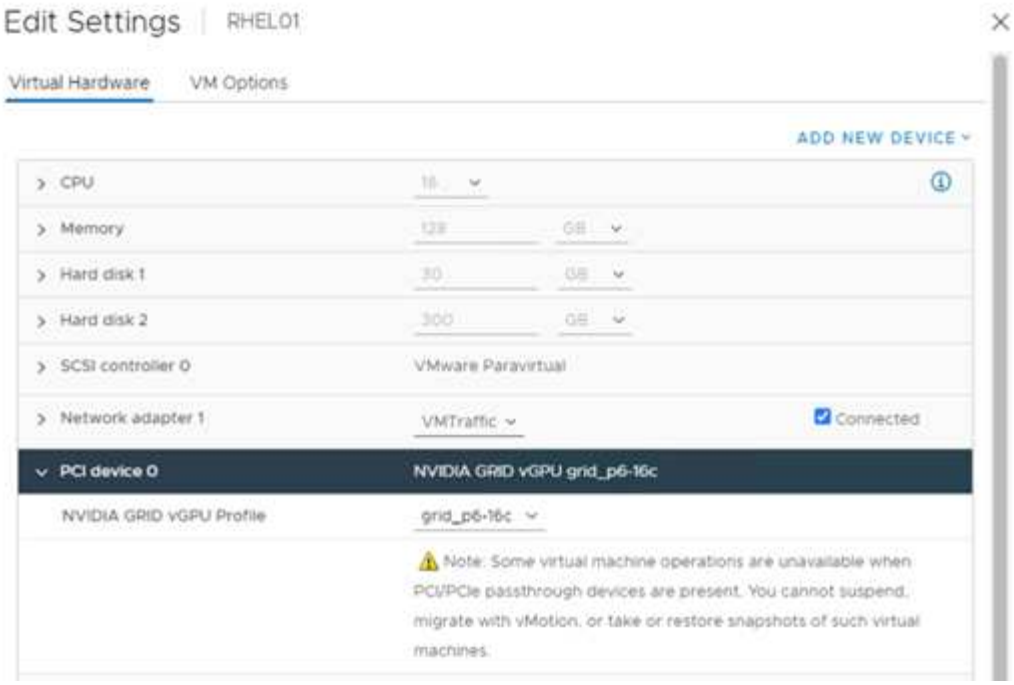
    a. Si se asigna una máquina virtual 4 GPU V100 de 32 GB, este valor debe ser 128.

    b. Si a una máquina virtual se le asignan 4 GPU P6 de 16 GB, este valor debe ser 64.





13. Cuando se añaden vGPU como un nuevo dispositivo PCI a la máquina virtual en vCenter, asegúrese de seleccionar NVIDIA GRID vGPU como tipo de dispositivo PCI.
14. Elija el perfil correcto de GPU que Suite la GPU que se va a usar, la memoria de la GPU y el objetivo de uso: Por ejemplo, los gráficos frente al procesamiento.



15. En el equipo virtual RedHat Linux, los controladores NVIDIA se pueden instalar ejecutando el siguiente comando:

```
[root@genomics1 genomics]#sh NVIDIA-Linux-x86_64-460.73.01-grid.run
```

16. Compruebe que se está reportando el perfil correcto de vGPU ejecutando el siguiente comando:

```
[root@genomics1 genomics]# nvidia-smi –query-gpu=gpu_name
–format=csv,noheader –id=0 | sed -e 's/ /-/g'
GRID-P6-16C
[root@genomics1 genomics]#
```

17. Después de reiniciar, compruebe que se ha informado de la unidad vGPU de NVIDIA correcta junto con las versiones del controlador.

```
[root@genomics1 genomics]# nvidia-smi
Wed Aug 18 20:30:56 2021
+-----------------------------------------------------------------------------
------+
| NVIDIA-SMI 460.73.01    Driver Version: 460.73.01    CUDA Version:
11.2     |
|-------------------------------+----------------------
+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
Compute M. |
|                               |                      |
MIG M. |
|===============================+======================+===============
======|
|   0  GRID P6-16C         On   | 00000000:02:02.0 Off |
N/A |
| N/A   N/A    P8    N/A /  N/A |   2205MiB / 16384MiB |      0%
Default |
|                               |                      |
N/A |
+-------------------------------+----------------------
+----------------------+
+-----------------------------------------------------------------------------
------+
| Processes:
|
|  GPU   GI   CI        PID   Type   Process name                  GPU
Memory |
|        ID   ID                                                   Usage
|
|=============================================================================
======|
|    0   N/A  N/A      8604      G   /usr/libexec/Xorg
13MiB |
+-----------------------------------------------------------------------------
------+
[root@genomics1 genomics]#
```

18. Asegúrese de que la IP del servidor de licencias está configurada en el equipo virtual en el archivo de configuración de grid vGPU.
    a. Copie la plantilla.

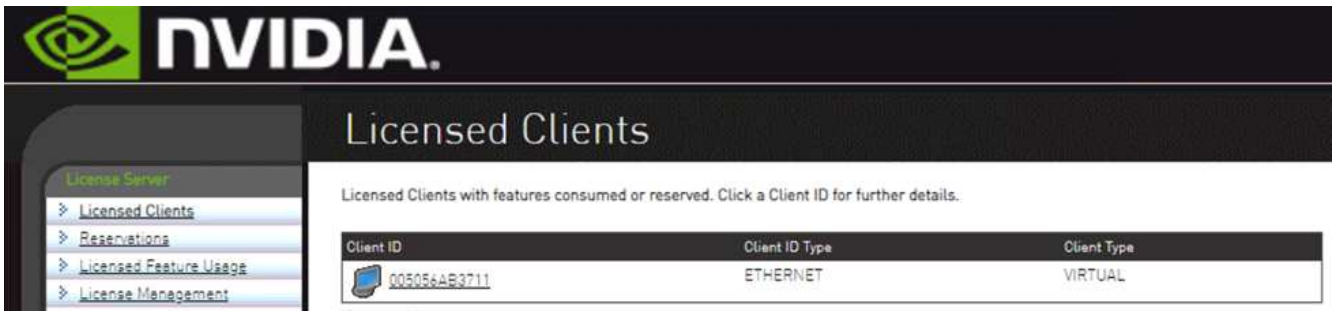
```
[root@genomics1 genomics]# cp /etc/nvidia/gridd.conf.template
/etc/nvidia/gridd.conf
```

b. Edite el archivo `/etc/nvidia/rid.conf`, Agregue la dirección IP del servidor de licencias y establezca el tipo de característica en 1.

```
ServerAddress=192.168.169.10
```

```
FeatureType=1
```

19. Después de reiniciar la máquina virtual, deberá ver una entrada en clientes con licencia en el servidor de licencias como se muestra a continuación.



20. Consulte la sección Configuración de soluciones para obtener más información sobre la descarga del software GATK y Cromwell.
21. Una vez que GATK puede utilizar las GPU en las instalaciones, el lenguaje de descripción del flujo de trabajo `*. wdl` tiene los atributos de tiempo de ejecución como se muestra a continuación.

```
task ValidateBAM {
  input {
    # Command parameters
    File input_bam
    String output_basename
    String? validation_mode
    String gatk_path
    # Runtime parameters
    String docker
    Int machine_mem_gb = 4
    Int addtional_disk_space_gb = 50
  }
  Int disk_size = ceil(size(input_bam, "GB")) + addtional_disk_space_gb
  String output_name = "${output_basename}_${validation_mode}.txt"
  command {
    ${gatk_path} \
      ValidateSamFile \
      --INPUT ${input_bam} \
      --OUTPUT ${output_name} \
      --MODE ${default="SUMMARY" validation_mode}
  }
  runtime {
    gpuCount: 1
    gpuType: "nvidia-tesla-p6"
    docker: docker
    memory: machine_mem_gb + " GB"
    disks: "local-disk " + disk_size + " HDD"
  }
  output {
    File validation_report = "${output_name}"
  }
}
```

"Siguiente: Conclusión."

Conclusión

"Anterior: Configuración de GPU."

Muchas organizaciones sanitarias de todo el mundo se han estandarizado en FlexPod como plataforma común. Con FlexPod, puede implementar capacidades en el sector sanitario con confianza. FlexPod con ONTAP de NetApp viene de serie con la capacidad de implementar un conjunto de protocolos líderes en el sector desde el primer momento. Con independencia del origen de la solicitud de ejecución de la genómica de un paciente dado, la interoperabilidad, la accesibilidad, la disponibilidad y la escalabilidad vienen de

serie con una plataforma FlexPod. Una solución estandarizada con la plataforma FlexPod es que la cultura de la innovación llega a ser contagiosa.

Dónde encontrar información adicional

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

- Centro de datos FlexPod para IA/ML con Cisco UCS 480 ML para aprendizaje profundo

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_480ml_aiml_deployment.pdf"

- FlexPod Datacenter con VMware vSphere 7.0 y ONTAP 9.7 de NetApp

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/fp_vmware_vsphere_7_0_ontap_9_7.html"

- Centro de documentación de ONTAP 9

  "http://docs.netapp.com"

- Ágil y eficiente: Cómo impulsa FlexPod la modernización del centro de datos

  "https://www.flexpod.com/idc-white-paper/"

- IA en la sanidad

  "https://www.netapp.com/us/media/na-369.pdf"

- FlexPod para el sector sanitario facilita su transformación

  "https://flexpod.com/solutions/verticals/healthcare/"

- FlexPod de Cisco y NetApp

  "https://flexpod.com/"

- IA y análisis en el sector sanitario (NetApp)

  "https://www.netapp.com/us/artificial-intelligence/healthcare-ai-analytics/index.aspx"

- IA en el sector sanitario las opciones de infraestructura inteligente aumentan el éxito

  https://www.netapp.com/pdf.html?item=/media/7410-wp-7314.pdf

- Centro de datos FlexPod con ONTAP 9.8, conector de almacenamiento ONTAP para Cisco Intersight y Cisco Intersight Managed Mode.

  https://www.netapp.com/pdf.html?item=/media/25001-tr-4883.pdf

- Centro de datos FlexPod con plataforma OpenStack Red Hat Enterprise Linux

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_openstack_osp6.html"

Historial de versiones

Versión	Fecha	Historial de versiones del documento
Versión 1.0	Noviembre de 2021	Versión inicial.

Guía de tamaños direccionales de FlexPod para MEDITECH

TR-4774: FlexPod para el dimensionamiento direccional de MEDITECH

Brandon Agee, John Duignan, NetApp Mike Brennan, Jon Ebmeir, Cisco

En colaboración con: 

Este informe proporciona directrices para dimensionar FlexPod en un entorno de software de aplicaciones EHR de MEDITECH.

Específico

Los sistemas FlexPod se pueden poner en marcha para alojar servicios MEDITECH EXPANSE, 6.x, 5.x y MAGIC. Los servidores FlexPod que alojan la capa de aplicación de MEDITECH proporcionan una plataforma integrada para una infraestructura fiable de alto rendimiento. La plataforma integrada de FlexPod se pone en marcha rápidamente por parte de partners de canal de FlexPod cualificados y cuenta con el soporte de los centros de asistencia técnica de Cisco y NetApp.

El dimensionamiento se basa en la información contenida en la propuesta de configuración de hardware de MEDITECH y en el documento de tareas de MEDITECH. El objetivo es determinar el tamaño óptimo para los componentes de infraestructura de almacenamiento, red y computación.

La "Descripción general de la carga de trabajo de MEDITECH" La sección describe los tipos de cargas de trabajo de computación y almacenamiento que se pueden encontrar en entornos de MEDITECH.

La "Especificaciones técnicas para arquitecturas pequeñas, medianas y grandes" La sección detalla una lista de materiales de muestra para las diferentes arquitecturas de almacenamiento descritas en la sección. Las configuraciones que se proporcionan son únicamente directrices generales. Configure siempre los sistemas utilizando los adaptadores de tamaño en función de la carga de trabajo y ajuste las configuraciones según corresponda.

Beneficios generales de la solución

Ejecutar un entorno MEDITECH con la base arquitectónica FlexPod puede ayudar a las organizaciones sanitarias a mejorar la productividad y reducir los gastos operativos y de capital. FlexPod proporciona una infraestructura convergente, rigurosamente probada, validada previamente desde la alianza estratégica de Cisco y NetApp. Se ha diseñado y diseñado específicamente para proporcionar un sistema con una alta disponibilidad y un rendimiento predecibles de baja latencia. Este enfoque permite reducir el tiempo de respuesta a los usuarios del sistema EHR de MEDITECH.

La solución FlexPod de Cisco y NetApp cumple los requisitos del sistema MEDITECH con un sistema modular, validado, convergente, virtualizado y de alto rendimiento. plataforma eficiente, escalable y rentable.

FlexPod Datacenter con MEDITECH proporciona diversas ventajas específicas del sector sanitario:

- **Arquitectura modular**. FlexPod satisface las distintas necesidades de la arquitectura modular de MEDITECH con sistemas FlexPod personalizados para cada carga de trabajo específica. Todos los componentes están conectados a través de un tejido de gestión del almacenamiento y de servidor en clúster y utilizan un conjunto de herramientas de gestión cohesivo.
- **Operaciones simplificadas y costes reducidos**. Puede eliminar el gasto y la complejidad de las plataformas heredadas reemplazándolas por un recurso compartido más eficiente y escalable que pueda ayudar a los médicos dondequiera que estén. Esta solución ofrece un mejor uso de los recursos para un mayor retorno de la inversión (ROI).
- **Implantación más rápida de la infraestructura**. El diseño integrado del centro de datos FlexPod con MEDITECH permite a los clientes tener la nueva infraestructura en funcionamiento de forma rápida y sencilla tanto en los centros de datos locales como remotos.
- **Arquitectura de escalabilidad horizontal**. Puede escalar SAN y NAS de terabytes a decenas de petabytes sin tener que reconfigurar las aplicaciones en ejecución.
- **Operaciones no disruptivas**. Puede realizar operaciones de mantenimiento del almacenamiento y de ciclo de vida del hardware, así como actualizaciones de software, sin interrumpir la actividad de la empresa.
- **Multitenancy seguro**. Esta ventaja respalda las necesidades crecientes de servidores virtualizados e infraestructura de almacenamiento compartido, lo que permite un multi-tenancy seguro de información específica de las instalaciones. Esta ventaja es importante si aloja varias instancias de bases de datos y software.
- **Optimización de recursos agrupados**. Esta ventaja puede ayudar a reducir el número de controladoras de almacenamiento y servidores físicos, equilibrar la carga de trabajo, aumentar la utilización y mejorar el rendimiento simultáneamente.
- **Calidad de servicio (QoS).** FlexPod ofrece calidad de servicio (QoS) en toda la pila. Las políticas de almacenamiento de calidad de servicio líderes del sector permiten niveles de servicio diferenciados en un entorno compartido. Estas normativas ofrecen un rendimiento óptimo para las cargas de trabajo y ayudan a aislar y controlar aplicaciones fuera de control.
- **Eficiencia del almacenamiento**. Puede reducir los costes de almacenamiento con la eficiencia del almacenamiento de 7:1 de NetApp.
- **Agilidad**. Las herramientas de automatización, orquestación y gestión de flujos de trabajo líderes del sector que ofrecen los sistemas FlexPod permiten que LA TI tenga mucho más capacidad de respuesta a las solicitudes de empresa. Estas solicitudes pueden abarcar desde el backup y el aprovisionamiento de MEDITECH de más entornos de prueba y entrenamiento, hasta las replicaciones de bases de datos de análisis para las iniciativas de gestión del estado de la población.
- **Productividad**. Puede poner en marcha y escalar rápidamente esta solución para obtener experiencias de usuario final médicas óptimas.
- **Data Fabric**. La arquitectura Data Fabric de NetApp aúna los datos de distintos sitios, sin que los barreras físicas y de todas las aplicaciones. Data Fabric de NetApp se ha creado pensando en empresas basadas en datos en un mundo donde todo gira alrededor de ellos. Los datos se crean y se usan en varias ubicaciones y, a menudo, se comparten con las aplicaciones y las infraestructuras. Data Fabric ofrece una forma de gestionar datos que es coherente y está integrada. Además, ofrece a LA TECNOLOGÍA más control sobre los datos y simplifica la cada vez mayor complejidad TECNOLÓGICA.

Ámbito

Este documento cubre los entornos que usan almacenamiento basado en Cisco UCS y ONTAP de NetApp. Proporciona ejemplos de arquitecturas de referencia para alojar MEDITECH.

No cubre:

- Guía detallada sobre el ajuste de tamaño mediante System Performance Modeler (SPM) de NetApp u otras herramientas de ajuste de tamaño de NetApp.
- Dimensionamiento para cargas de trabajo no productivas.

Destinatarios

Este documento está dirigido a ingenieros de sistemas de NetApp y partners y al personal de Servicios profesionales de NetApp. NetApp asume que el lector tiene un buen conocimiento de los conceptos de configuración de almacenamiento y computación, así como de la familiaridad técnica con los sistemas de almacenamiento de Cisco UCS y NetApp.

Documentos relacionados

Los siguientes informes técnicos y otros documentos son relevantes para este informe técnico y constituyen un conjunto completo de documentos necesarios para el dimensionamiento, el diseño y la implementación de MEDITECH en la infraestructura FlexPod.

- "TR-4753: Guía de puesta en marcha de FlexPod Datacenter para MEDITECH"
- "TR-4190: Directrices de tamaño de NetApp para entornos de MEDITECH"
- "TR-4319: Directrices de puesta en marcha de NetApp para entornos de MEDITECH"

> Se necesitan credenciales de inicio de sesión para Field Portal de NetApp para acceder a algunos de estos informes.

Descripción general de la carga de trabajo de MEDITECH

En esta sección se describen los tipos de cargas de trabajo de computación y almacenamiento que puede encontrar en entornos de MEDITECH.

MEDITECH y cargas de trabajo de backup

Cuando calcule el tamaño de los sistemas de almacenamiento de NetApp para entornos de MEDITECH, debe tener en cuenta la carga de trabajo de producción de MEDITECH y la carga de trabajo de backup.

Host MEDITECH
Un host MEDITECH es un servidor de base de datos. Este host también se conoce como servidor de archivos MEDITECH (para la plataforma 6.x o C/S 5.x) o como máquina MÁGICA (para la plataforma MAGIC). Este documento utiliza el término host de MEDITECH para hacer referencia a un servidor de archivos MEDITECH y a una máquina MÁGICA.

Las siguientes secciones describen las características de I/o y los requisitos de rendimiento de estas dos cargas de trabajo.

Carga de trabajo de MEDITECH

En un entorno MEDITECH, varios servidores que ejecutan el software MEDITECH realizan diversas tareas como un sistema integrado conocido como el sistema MEDITECH. Para obtener más información sobre el sistema MEDITECH, consulte la documentación de MEDITECH:

- Para entornos de MEDITECH de producción, consulte la documentación MEDITECH correspondiente para determinar el número de hosts MEDITECH y la capacidad de almacenamiento que debe incluirse en el dimensionamiento del sistema de almacenamiento de NetApp.
- Para nuevos entornos de MEDITECH, consulte el documento de propuesta de configuración de hardware. Para entornos MEDITECH existentes, consulte el documento de tarea de evaluación del hardware. La tarea de evaluación del hardware está asociada con un ticket de MEDITECH. Los clientes pueden solicitar cualquiera de estos documentos a MEDITECH.

Puede escalar el sistema MEDITECH para proporcionar mayor capacidad y rendimiento añadiendo hosts. Cada host requiere capacidad de almacenamiento para sus archivos de base de datos y aplicaciones. El almacenamiento disponible para cada host MEDITECH también debe admitir la E/S generada por el host. En un entorno MEDITECH, cada host tiene a su disposición un LUN que admita los requisitos de almacenamiento de aplicaciones y bases de datos del host. El tipo de categoría MEDITECH y el tipo de plataforma que usted implementa determinan las características de carga de trabajo de cada host MEDITECH y, por lo tanto, del sistema en su conjunto.

Categorías de MEDITECH

MEDITECH asocia el tamaño de la implementación con un número de categoría comprendido entre 1 y 6. La categoría 1 representa las implementaciones de MEDITECH más pequeñas; la categoría 6 representa la mayor. Entre los ejemplos de la especificación de la aplicación MEDITECH asociada con cada categoría se incluyen métricas como:

- Número de camas de hospital
- Pacientes hospitalizados al año
- Pacientes ambulatorios al año
- Visitas a la sala de emergencias por año
- Exámenes al año
- Recetas para pacientes hospitalizados por día
- Recetas para pacientes ambulatorios por día

Para obtener más información sobre las categorías de MEDITECH, consulte la hoja de referencia de la categoría MEDITECH. Puede obtener esta hoja de MEDITECH a través del cliente o a través del instalador del sistema MEDITECH.

Plataformas MEDITECH

MEDITECH tiene cuatro plataformas:

- EXPANSIÓN
- MEDITECH 6.x
- Cliente/servidor 5.x (C/S 5.x)
- MAGIA

Para las plataformas MEDITECH EXPANSE, 6.x y C/S 5.x, las características de E/S de cada host se definen como 100% aleatorias con un tamaño de solicitud de 4,000. Para la plataforma MEDITECH MAGIC, las características de E/S de cada host se definen como 100% al azar con un tamaño de solicitud de 8,000 o 16,000. De acuerdo con MEDITECH, el tamaño de la solicitud para una implementación DE producción MÁGICA típica es 8,000 o 16,000.

El ratio de lecturas y escrituras varía en función de la plataforma que se haya puesto en marcha. MEDITECH estima la combinación media de lectura y escritura y luego los expresa como porcentajes. MEDITECH también estima el valor de IOPS sostenido medio necesario para cada host MEDITECH en una plataforma MEDITECH particular. En la siguiente tabla se resumen las características de E/S específicas de la plataforma que proporciona MEDITECH.

Categoría de MEDITECH	Plataforma MEDITECH	% De lectura aleatoria promedio	Porcentaje de escritura aleatoria promedio	Promedio de IOPS sostenidas por host de MEDITECH
1	EXPANSIÓN, 6.x.	20	80	750
2-6	EXPANSIÓN	20	80	750
	6.x.	20	80	750
	C/S 5.x	40	60	600
	MAGIA	90	10	400

En un sistema MEDITECH, el nivel medio de IOPS de cada host debe ser igual a los valores de IOPS definidos en la tabla anterior. Para determinar cuál es la configuración de almacenamiento correcta en función de cada plataforma, se utilizan los valores de IOPS especificados en la tabla anterior como parte de la metodología de dimensionamiento descrita en el "Especificaciones técnicas para arquitecturas pequeñas, medianas y grandes" sección.

MEDITECH requiere que la latencia de escritura aleatoria media permanezca por debajo de 1 ms en cada host. Sin embargo, se considera aceptable un aumento temporal de la latencia de escritura de hasta 2 ms durante las tareas de backup y reasignación. MEDITECH también requiere que la latencia media de lectura aleatoria permanezca por debajo de los 7 ms en los hosts de la categoría 1 y por debajo de los 5 ms en los hosts de la categoría 2. Estos requisitos de latencia se aplican a todos los hosts, independientemente de la plataforma de MEDITECH que se esté utilizando.

La siguiente tabla resume las características de I/o que debe tener en cuenta cuando configure el almacenamiento de NetApp para cargas de trabajo de MEDITECH.

Parámetro	Categoría de MEDITECH	EXPANSIÓN	MEDITECH 6.x	C/S 5.x	MAGIA
Tamaño de la solicitud	1-6	4K	4K	4K	8K o 16K
Aleatorio/secuencial		100 % aleatorio	100 % aleatorio	100 % aleatorio	100 % aleatorio
IOPS sostenido promedio	1	750	750	N.A.	N.A.
	2-6	750	750	600	400
Relación de lectura/escritura	1-6	20 % lectura, 80 % escritura	20 % lectura, 80 % escritura	40 % lectura, 60 % escritura	90 % lectura, 10 % escritura
Latencia de escritura		<1 ms	<1 ms	<1 ms	<1 ms
Latencia de escritura máxima temporal	1-6	<2 ms	<2 ms	<2 ms	<2 ms

Parámetro	Categoría de MEDITECH	EXPANSIÓN	MEDITECH 6.x	C/S 5.x	MAGIA
Latencia de lectura	1	<7 ms	<7 ms	N.A.	N.A.
	2-6	<5 ms	<5 ms	<5 ms	<5 ms

Los hosts de MEDITECH de las categorías 3 a 6 tienen las mismas características de E/S que la categoría 2. Para las categorías de MEDITECH 2 a 6, el número de hosts que se implementan en cada categoría difiere.

Debe ajustar el tamaño del sistema de almacenamiento NetApp para satisfacer los requisitos de rendimiento descritos en las secciones anteriores. Además de la carga de trabajo de producción de MEDITECH, el sistema de almacenamiento de NetApp debe ser capaz de mantener estos objetivos de rendimiento de MEDITECH durante las operaciones de backup, como se describe en la siguiente sección.

Descripción de la carga de trabajo de backup

El software de backup certificado por MEDITECH realiza copias de seguridad de la LUN utilizada por cada host MEDITECH en un sistema MEDITECH. Para que los backups estén en un estado coherente con las aplicaciones, el software de backup consulta el sistema MEDITECH y suspende las solicitudes de E/S al disco. Mientras el sistema está en estado inactivo, el software de backup emite un comando al sistema de almacenamiento de NetApp para crear una copia Snapshot de NetApp de los volúmenes que contienen las LUN. El software de copia de seguridad posteriormente le permite al sistema MEDITECH, que permite a las solicitudes de E/S de producción continuar a la base de datos. El software crea un volumen FlexClone de NetApp basado en la copia snapshot. Este volumen lo utiliza el origen de backup mientras las solicitudes de I/o de producción continúan en los volúmenes principales que alojan los LUN.

La carga de trabajo generada por el software de backup proviene de la lectura secuencial de los LUN que residen en los volúmenes FlexClone. La carga de trabajo se define como una carga de trabajo de lectura secuencial del 100 % con un tamaño de solicitud de 64,000. Para la carga de trabajo de producción de MEDITECH, el criterio de rendimiento es mantener las IOPS necesarias y los niveles de latencia de lectura/escritura asociados. No obstante, para la carga de trabajo de backup, la atención se desplaza hasta el rendimiento de los datos general (Mbps) que se genera durante la operación de backup. Los backups de LUN de MEDITECH deben completarse en un período de backup de ocho horas, pero NetApp recomienda que el backup de todas las LUN de MEDITECH se complete en seis horas o menos. El objetivo de completar el backup en menos de seis horas mitiga eventos como un aumento no planificado de la carga de trabajo de MEDITECH, las operaciones en segundo plano de ONTAP de NetApp o el crecimiento de los datos con el tiempo. Cualquiera de estos eventos puede suponer tiempo de backup adicional. Independientemente de la cantidad de datos de aplicaciones almacenados, el software de backup realiza una copia de seguridad completa a nivel de bloque de toda la LUN en cada host de MEDITECH.

Calcule el rendimiento de lectura secuencial necesario para completar el backup en esta ventana en función de los otros factores involucrados:

- La duración deseada de la copia de seguridad
- El número de LUN
- El tamaño de cada LUN para la que se va a realizar el backup

Por ejemplo, en un entorno MEDITECH de 50 hosts en el que el tamaño de LUN de cada host es de 200 GB, la capacidad total de las LUN a la que se debe hacer backup es de 10 TB.

Para realizar un backup de 10 TB de datos en ocho horas, se necesita el siguiente rendimiento:

- = (10 x 10 6)MB (8 x 3,600)s.
- = 347,2 MBps

Sin embargo, para tener en cuenta los eventos no planificados, se selecciona un periodo de backup conservador de 5.5 horas para ofrecer un margen adicional superior a las seis horas recomendadas.

Para realizar un backup de 10 TB de datos en ocho horas, se necesita el siguiente rendimiento:

- = (10 x 10 6)MB (5.5 x 3,600)s.
- = 500 Mbps

A una velocidad de rendimiento de 500 Mbps, el backup se puede completar en un intervalo de 5.5 horas sin problemas dentro de los requisitos de backup de 8 horas.

La tabla siguiente resume las características de I/o de la carga de trabajo de backup que se debe utilizar al configurar el sistema de almacenamiento.

Parámetro	Todas las plataformas
Tamaño de la solicitud	64K
Aleatorio/secuencial	100 % secuencial
Relación de lectura/escritura	100 % lectura
Rendimiento promedio	Depende del número de hosts de MEDITECH y del tamaño de cada LUN: El backup debe completarse en un plazo de 8 horas.
Duración de backup requerida	8 horas

Cisco UCS Reference Architecture para MEDITECH

La arquitectura de MEDITECH en FlexPod se basa en las directrices de MEDITECH, Cisco y NetApp y en la experiencia de los partners al trabajar con clientes de MEDITECH de todos los tamaños. La arquitectura es adaptable y aplica las mejores prácticas para MEDITECH, en función de la estrategia del centro de datos del cliente: Ya sea pequeña o grande, centralizada, distribuida o multi-tenant.

Cuando se implementa MEDITECH, Cisco ha diseñado arquitecturas de referencia Cisco UCS que se alinean directamente con las prácticas recomendadas de MEDITECH. Cisco UCS proporciona una solución estrechamente integrada para ofrecer alto rendimiento, alta disponibilidad, fiabilidad y escalabilidad como respaldo de las prácticas médicas y los sistemas hospitalarios con varias miles de camas.

Especificaciones técnicas para arquitecturas pequeñas, medianas y grandes

En esta sección se describe una lista de ejemplos de materiales para arquitecturas de almacenamiento de diferentes tamaños.

Lista de materiales para arquitecturas pequeñas, medianas y grandes.

El diseño de FlexPod es una infraestructura flexible que abarca muchos componentes y versiones de software diferentes. Uso "TR-4036: Especificaciones técnicas de FlexPod" Como guía para el montaje de una configuración de FlexPod válida. Las configuraciones que aparecen en la siguiente tabla son los requisitos mínimos de FlexPod, y son solo una muestra. La configuración se puede ampliar para cada familia de productos según sea necesario para distintos entornos y casos de uso.

Para este ejercicio de tamaño pequeño corresponde a un entorno MEDITECH de categoría 3, de categoría media a categoría 5 y de categoría grande a categoría 6.

	Pequeño	Mediano	Grande
Plataforma	Un par de alta disponibilidad de sistema de almacenamiento all-flash AFF A220 de NetApp	Un par de alta disponibilidad de AFF A220 de NetApp	Un par de alta disponibilidad del sistema de almacenamiento all-flash AFF A300 de NetApp
Bandejas de discos	9 TB x 3,8 TB	13 TB x 3,8 TB	19 TB x 3,8 TB
Tamaño de la base de datos de MEDITECH	3 TB-12 TB	17 TB	>30 TB
IOPS DE MEDITECH	<22,000 IOPS	>25,000 IOPS	>32,000 IOPS
IOPS totales	22000	27000	35000
Sin formato	34,2 TB	49,4 TB	68,4 TB
Capacidad utilizable	18,53 TIB	27,96 TIB	33,82 TIB
Capacidad efectiva (eficiencia del almacenamiento 2:1)	55,6 TIB	83.89TIB	101,47 TIB

Algunos entornos de cliente pueden tener varias cargas de trabajo de producción de MEDITECH simultáneamente o pueden tener requisitos de IOPS más altos. En estos casos, trabaje con el equipo de cuentas de NetApp para ajustar el tamaño de los sistemas de almacenamiento de acuerdo con las IOPS y la capacidad necesarias. Se debe poder determinar cuál es la plataforma correcta para servir las cargas de trabajo. Por ejemplo, hay clientes que ejecutan con éxito varios entornos de MEDITECH en un par de alta disponibilidad del sistema de almacenamiento all-flash A700 de AFF.

La siguiente tabla muestra el software estándar necesario para las configuraciones de MEDITECH.

De NetApp	Familia de productos	Versión o versión	Detalles
Reducida	ONTAP	Disponibilidad general de ONTAP 9.4 (GA)	
Red	Interconexiones de estructura Cisco UCS	Cisco UCSM 4.x	Versión actual recomendada
	Switches Ethernet Cisco Nexus	7.0(3)I7(6)	Versión actual recomendada
	Cisco FC: Cisco MDS 9132T	8.3(2)	Versión actual recomendada
Hipervisor	Hipervisor	VMware vSphere ESXi 6.7	
	Máquinas virtuales (VM)	Windows 2016	

De NetApp	Familia de productos	Versión o versión	Detalles
Gestión	Sistema de gestión de hipervisores	VMware vCenter Server 6.7 U1 (VCSA)	
	Virtual Storage Console (VSC) de NetApp	VSC 7.0P1	
	SnapCenter de NetApp	SnapCenter 4.0	
	Administrador de Cisco UCS	4.x.	

En la siguiente tabla se muestra un ejemplo de configuración pequeña (categoría 3): Componentes de infraestructura.

Capa	Familia de productos	Cantidad y modelo	Detalles
Informática	Chasis Cisco UCS 5108	1	Admite hasta ocho hojas de media anchura o cuatro de anchura completa. Agregue chasis conforme aumente la necesidad de servidor.
	Módulos de I/o de chasis de Cisco	2 x 2208	8 GB x 10 GB de puertos de enlace ascendente
	Servidores blade Cisco UCS	4 x B200 M5	Cada una con 2 x 14 núcleos, 2,6 GHz o una velocidad de reloj superior y 3.2 GB de BIOS (3#)
	Tarjetas de interfaz virtual Cisco UCS	4 × UCS 1440	Controlador VMware ESXi fnic FC: Controlador 1.6.0.47 VMware ESXi ENIC Ethernet: 1.0.27.0 (consulte la matriz de interoperabilidad:
	2 x interconexiones de estructura Cisco UCS (FI)	2 X UCS 6454 FI	Interconexiones de estructura de cuarta generación que admiten Ethernet de 10/100/100 GB y FC de 25 GB
Red	Switches Ethernet de Cisco	2 Nexus 9336c-FX2	1 GB, 10 GB, 25 GB, 40 GB Y 100 GB
Red de almacenamiento	Red IP Nexus 9k para almacenamiento BLOB		Chasis FI y UCS
	FC: CISCO MDS 9132T		Dos switches Cisco 9132T

Capa	Familia de productos	Cantidad y modelo	Detalles
Reducida	Sistema de almacenamiento all-flash AFF A300 de NetApp	1 par de alta disponibilidad	Clúster de 2 nodos para todas las cargas de trabajo de MEDITECH (File Server, Image Server, SQL Server, VMware, etc.)
	Bandeja de discos DS224C	1 Bandeja de discos DS224C	
	Unidad de estado sólido (SSD)	9 x 3,8 TB	

En la siguiente tabla se muestra una configuración de ejemplo de medio (categoría 5): Componentes de infraestructura

Capa	Familia de productos	Cantidad y modelo	Detalles
Informática	Chasis Cisco UCS 5108	1	Admite hasta ocho hojas de media anchura o cuatro de anchura completa. Agregue chasis conforme aumente la necesidad de servidor.
	Módulos I/o de chasis de Cisco	2 x 2208	8 GB x 10 GB de puertos de enlace ascendente
	Servidores blade Cisco UCS	6 x B200 M5	Con 2 x 16 núcleos, 2,5 GHz/o más de velocidad de reloj y 384 GB de memoria BIOS 3.2 (3#)
	Tarjeta de interfaz virtual (VIC) Cisco UCS	6 × UCS 1440 VIC	Controlador VMware ESXi fnic FC: Controlador 1.6.0.47 VMware ESXi ENIC Ethernet: 1.0.27.0 (consulte la matriz de interoperabilidad:)
	2 x interconexiones de estructura Cisco UCS (FI)	2 X UCS 6454 FI	Interconexiones de estructura de cuarta generación con Ethernet de 10 GB/25 GB/100 GB y FC de 32 GB
Red	Switches Ethernet de Cisco	2 Nexus 9336c-FX2	1 GB, 10 GB, 25 GB, 40 GB Y 100 GB
Red de almacenamiento	Red IP Nexus 9k para almacenamiento BLOB		
	FC: CISCO MDS 9132T		Dos switches Cisco 9132T

Capa	Familia de productos	Cantidad y modelo	Detalles
Reducida	Sistema de almacenamiento all-flash AFF A220 de NetApp	2 par de alta disponibilidad	Clúster de 2 nodos para todas las cargas de trabajo de MEDITECH (File Server, Image Server, SQL Server, VMware, etc.)
	Bandeja de discos DS224C	1 bandeja de discos DS224C	
	SSD	13 x 3,8 TB	

En la siguiente tabla se muestra un ejemplo de configuración grande (categoría 6): Componentes de infraestructura.

Capa	Familia de productos	Cantidad y modelo	Detalles
Informática	Chasis Cisco UCS 5108	1	
	Módulos I/o de chasis de Cisco	2 x 2208	8 puertos de enlace ascendente de 10 GB
	Servidores blade Cisco UCS	8 x B200 M5	Cada uno con 2 x 24 núcleos, 2,7 GHz y 768 GB de BIOS 3.2(3#)
	Tarjeta de interfaz virtual (VIC) Cisco UCS	8 × UCS 1440 VIC	Controlador VMware ESXi fnic FC: Controlador 1.6.0.47 VMware ESXi ENIC Ethernet: 1.0.27.0 (consulte la matriz de interoperabilidad:
	2 interconexiones de estructura Cisco UCS (FI)	2 X UCS 6454 FI	Interconexiones de estructura de cuarta generación con Ethernet de 10 GB/25 GB/100 GB y FC de 32 GB
Red	Switches Ethernet de Cisco	2 Nexus 9336c-FX2	2 Nexus 9332PQ1 de Cisco, 10 GB, 25 GB, 40 GB y 100 GB
Red de almacenamiento	IP Network N9k para almacenamiento BLOB		
	FC: CISCO MDS 9132T		Dos switches Cisco 9132T

Capa	Familia de productos	Cantidad y modelo	Detalles
Reducida	AFF A300	1 par de alta disponibilidad	Clúster de 2 nodos para todas las cargas de trabajo de MEDITECH (File Server, Image Server, SQL Server, VMware, etc.)
	Bandeja de discos DS224C	1 bandejas de discos DS224C	
	SSD	19 x 3,8 TB	

Estas configuraciones proporcionan un punto de partida para calcular el tamaño. Algunos entornos de cliente pueden tener varias cargas de trabajo de MEDITECH de producción y no MEDITECH simultáneamente, o pueden tener requisitos de IOP más altos. Debe colaborar con el equipo de cuentas de NetApp para dimensionar los sistemas de almacenamiento en función de las IOPS, las cargas de trabajo y la capacidad requeridas para determinar la plataforma adecuada para prestar servicio a las cargas de trabajo.

Información adicional

Si quiere obtener más información sobre la información descrita en este documento, consulte los siguientes documentos o sitios web:

- Centro de datos FlexPod con diseño validado por FC Cisco.

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi65u1_n9fc.html"

- Directrices de puesta en marcha de NetApp para entornos MEDITECH.

  "https://fieldportal.netapp.com/content/248456" (Se requiere inicio de sesión de NetApp)

- Estimaciones de tamaño de NetApp para entornos de MEDITECH.

  "www.netapp.com/us/media/tr-4190.pdf"

- Centro de datos FlexPod para la puesta en marcha de EHR de Epic

  "www.netapp.com/us/media/tr-4693.pdf"

- Zona de diseño de FlexPod

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

- FlexPod DC con almacenamiento FC (switches MDS) mediante NetApp AFF, vSphere 6.5U1 y Cisco UCS Manager

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi65u1_n9fc.html"

- Asistencia sanitaria de Cisco

  https://www.cisco.com/c/en/us/solutions/industries/healthcare.html?dtid=osscdc000283

Reconocimientos

Las siguientes personas contribuyeron a la redacción y creación de esta guía.

- Brandon Agee, Ingeniero de Marketing Técnico, NetApp
- John Duignan, Arquitecto de Soluciones - Sanidad, NetApp
- Ketan Mota, Gestor de Productos de NetApp
- Jon Ebmeier, Arquitecto de Soluciones técnicas, Cisco Systems, Inc
- Mike Brennan, Director de producto de Cisco Systems, Inc

Guía de puesta en marcha de FlexPod Datacenter para MEDITECH

TR-4753: Guía de puesta en marcha de FlexPod Datacenter para MEDITECH

Brandon Agee y John Duignan, NetApp Mike Brennan y Jon Ebmeier, Cisco

En colaboración con: 

Beneficios generales de la solución

Al ejecutar un entorno MEDITECH en la base arquitectónica FlexPod, su organización sanitaria puede esperar una mejora en la productividad del personal y una reducción en los gastos operativos y de capital. FlexPod Datacenter para MEDITECH proporciona diversas ventajas específicas del sector sanitario, como:

- **Operaciones simplificadas y costes reducidos.** elimine el gasto y la complejidad de las plataformas heredadas reemplazándolas con un recurso compartido más eficiente y escalable que pueda dar soporte a los médicos dondequiera que estén. Esta solución ofrece un mayor uso de recursos para un mayor retorno de la inversión (ROI).
- **Implementación más rápida de la infraestructura.** tanto si se trata de un centro de datos existente como de una ubicación remota, con el diseño integrado y probado del centro de datos FlexPod, puede tener su nueva infraestructura en funcionamiento en menos tiempo y con menos esfuerzo.
- **Almacenamiento certificado.** el software de gestión de datos ONTAP de NetApp con MEDITECH le proporciona la fiabilidad superior de un proveedor de almacenamiento probado y certificado. MEDITECH no certifica otros componentes de la infraestructura.
- **Arquitectura de escalabilidad horizontal.** Escale SAN y NAS de terabytes (TB) a decenas de petabytes (PB) sin necesidad de reconfigurar las aplicaciones en ejecución.
- **Operaciones no disruptivas.** realice el mantenimiento del almacenamiento, las operaciones del ciclo de vida del hardware y las actualizaciones de FlexPod sin interrumpir el negocio.
- **Multitenancy seguro.** Soporte a las crecientes necesidades de la infraestructura compartida de almacenamiento y servidor virtualizado, permitiendo multi-tenancy seguro de la información específica de la instalación, particularmente si su sistema aloja varias instancias de bases de datos y software.
- **Optimización de recursos agrupados.** Ayuda a reducir el número de servidores físicos y controladores de almacenamiento, las demandas de carga de trabajo de equilibrio y aumentar la utilización a la vez que mejora el rendimiento.

- **Calidad de servicio (QoS).** FlexPod ofrece QoS en toda la pila. Políticas de calidad de servicio, computación y almacenamiento líderes del sector que permiten niveles de servicio diferenciados en un entorno compartido. Estas normativas ofrecen un rendimiento óptimo para las cargas de trabajo y ayudan a aislar y controlar aplicaciones fuera de control.
- **Eficiencia de almacenamiento.** Reduzca los costes de almacenamiento con la "Garantía de eficiencia del almacenamiento 7:1 de NetApp".
- **Agilidad.** con las herramientas de automatización, coordinación y gestión de flujos de trabajo líderes del sector que proporcionan los sistemas FlexPod, su equipo DE TI puede responder mucho más a las solicitudes empresariales. Estas solicitudes pueden abarcar desde el backup y el aprovisionamiento de MEDITECH de más entornos de prueba y entrenamiento, hasta las replicaciones de bases de datos de análisis para las iniciativas de gestión del estado de la población.
- **Mayor productividad.** despliegue y escale rápidamente esta solución para obtener experiencias óptimas de usuario final clínico.
- **Data Fabric de NetApp.** la arquitectura Data Fabric de NetApp aúna los datos de un sitio a otro, más allá de los límites físicos y de las aplicaciones. Data Fabric de NetApp se ha creado pensando en empresas basadas en datos en un mundo donde todo gira alrededor de ellos. Los datos se crean y se usan en varias ubicaciones y, a menudo, es necesario aprovecharlos y compartirlos con otras ubicaciones, aplicaciones e infraestructuras. Necesita una forma de gestionar sus datos que sea coherente y esté integrada. Data Fabric ofrece una forma de gestionar los datos que los controla y simplifica la cada vez mayor complejidad TECNOLÓGICA.

FlexPod

Nuevo enfoque de la infraestructura para MEDITECH EHR

Las organizaciones de proveedores de atención médica como la suya siguen presionadas para maximizar los beneficios de una inversión sustancial en registros médicos electrónicos de MEDITECH (EHR) líderes del sector. Para aplicaciones de misión crítica, cuando los clientes diseñan sus centros de datos para soluciones MEDITECH, suelen identificar los siguientes objetivos por su arquitectura de centro de datos:

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

A medida que los usuarios de MEDITECH transforman sus organizaciones en organizaciones de atención médica responsables y se adaptan a modelos de reembolso ajustados y agrupados, el reto pasa a proporcionar la infraestructura MEDITECH necesaria en un modelo DE prestación DE SERVICIOS DE TI más eficiente y ágil.

Valor de la infraestructura convergente prevalidada

Dado que existe el requisito general de proporcionar un rendimiento del sistema previsible de baja latencia y alta disponibilidad, MEDITECH tiene el requisito más preceptivo en cuanto a los requisitos de hardware de sus clientes.

FlexPod es una infraestructura convergente prevalidada y rigurosamente probada desde la alianza estratégica de Cisco y NetApp. Se ha diseñado y diseñado específicamente para proporcionar un sistema predecible de baja latencia y una alta disponibilidad. Este enfoque da como resultado la conformidad con MEDITECH y, en última instancia, el tiempo de respuesta óptimo para los usuarios del sistema MEDITECH.

La solución FlexPod de Cisco y NetApp cumple los requisitos del sistema MEDITECH con un sistema modular, validado, convergente, virtualizado y de alto rendimiento. plataforma eficiente, escalable y rentable. Proporciona:

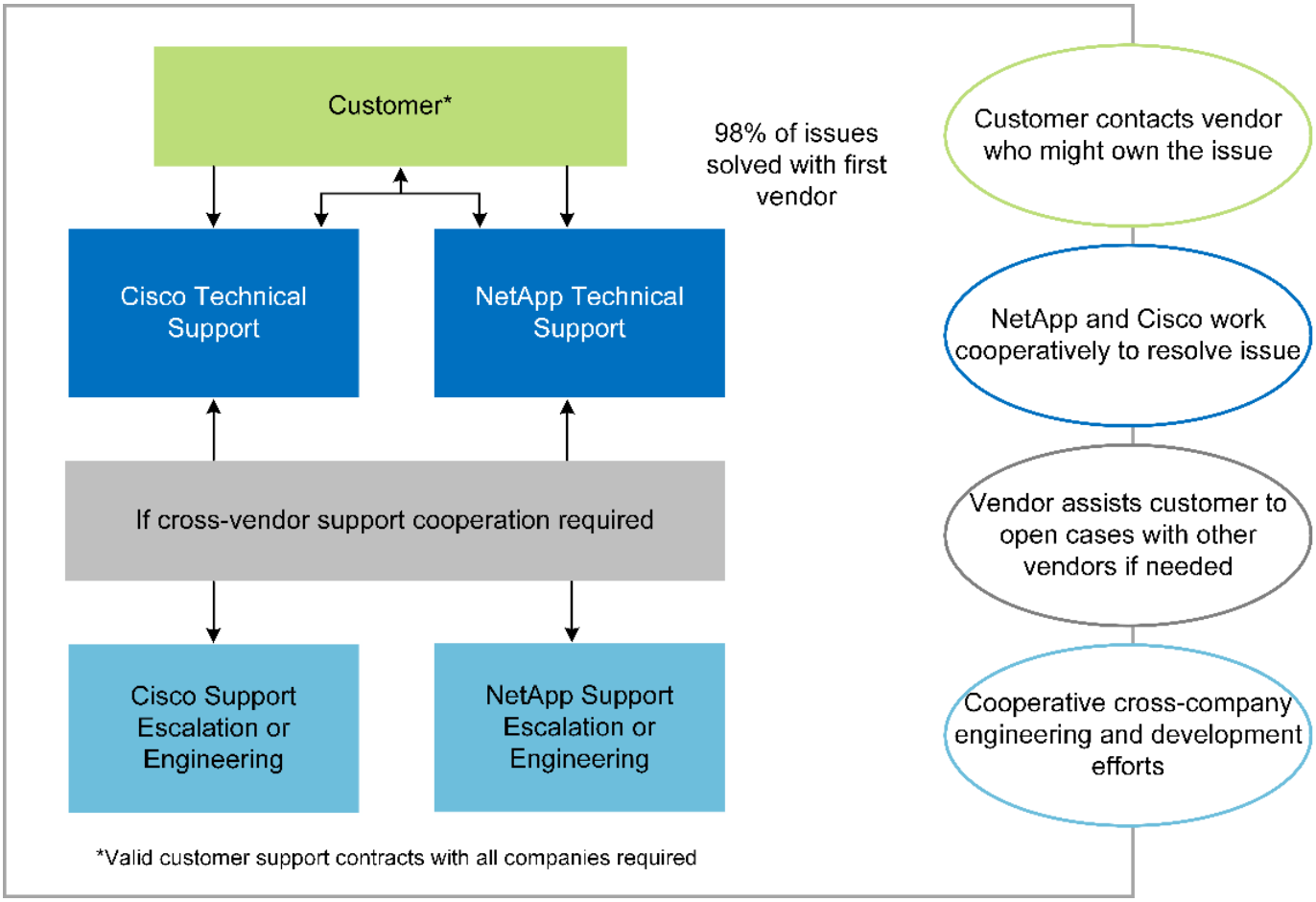
- **Arquitectura modular.** FlexPod satisface las variadas necesidades de la arquitectura modular de MEDITECH con plataformas FlexPod configuradas específicamente para cada carga de trabajo específica. Todos los componentes están conectados a través de un servidor en clúster y un tejido de gestión del almacenamiento y un conjunto de herramientas de gestión cohesivo.
- **La tecnología líder del sector en todos los niveles de la pila convergente.** Cisco, NetApp, VMware y Microsoft Windows están clasificados como número 1 o número 2 por analistas del sector en sus respectivas categorías de servidores, redes, almacenamiento y sistemas operativos.
- **Protección de la inversión con TECNOLOGÍA DE LA INFORMACIÓN flexible y estandarizada.** la arquitectura de referencia de FlexPod anticipa nuevas versiones y actualizaciones de productos, con rigurosas pruebas de interoperabilidad continuas para acomodar tecnologías futuras a medida que estén disponibles.
- **Implementación probada en una amplia gama de entornos.** probado previamente y validado conjuntamente con los hipervisores, sistemas operativos, aplicaciones y software de infraestructura más populares, FlexPod se ha instalado en varias organizaciones de clientes de MEDITECH.

Arquitectura FlexPod y soporte conjunto demostrados

FlexPod es una solución de centro de datos probada que ofrece una infraestructura compartida flexible que se puede escalar fácilmente para respaldar las demandas crecientes de sus cargas de trabajo sin que esto afecte al rendimiento de forma negativa. Al aprovechar la arquitectura de FlexPod, esta solución ofrece todas las ventajas de FlexPod, como:

- **Rendimiento para cumplir con los requisitos de carga de trabajo de MEDITECH.** dependiendo de los requisitos de la propuesta de configuración del hardware de MEDITECH, pueden ponerse en marcha diferentes plataformas ONTAP para satisfacer sus requisitos de E/S y latencia necesarios.
- **Escalabilidad para adaptarse fácilmente al crecimiento de datos clínicos.** ampliar dinámicamente las máquinas virtuales (VM), los servidores y la capacidad de almacenamiento bajo demanda, sin límites tradicionales.
- **Eficiencia mejorada.** reduzca tanto el tiempo de administración como el coste total de propiedad gracias a una infraestructura virtualizada convergente, que es más fácil de gestionar y que almacena los datos de forma más eficiente a la vez que aumenta el rendimiento del software MEDITECH.
- **Reducción del riesgo.** minimice la interrupción del negocio con una plataforma prevalidada que se basa en una arquitectura definida que elimina las conjeturas de la implementación y se adapta a la optimización continua de la carga de trabajo.
- **Soporte conjunto de FlexPod.** NetApp y Cisco han establecido Soporte conjunto, un modelo de soporte sólido, escalable y flexible para cumplir los requisitos de soporte exclusivos de la infraestructura convergente de FlexPod. Este modelo utiliza la experiencia combinada de NetApp y Cisco, así como sus recursos y conocimientos en el campo del soporte técnico, para proporcionar un proceso optimizado para identificar y solucionar su problema de soporte de FlexPod, con independencia de dónde se encuentre el problema. Con el modelo de soporte conjunto de FlexPod, su sistema de FlexPod funciona de forma eficiente y se beneficia de la tecnología más actualizada, y trabaja con un equipo experimentado para ayudarle a resolver problemas de integración.

El soporte conjunto de FlexPod resulta especialmente valioso para las organizaciones sanitarias que ejecutan aplicaciones vitales para el negocio, como MEDITECH, en la infraestructura convergente FlexPod. En la siguiente figura se muestra el modelo de soporte conjunto de FlexPod.



Además de estas ventajas, cada componente de la pila del centro de datos FlexPod con la solución MEDITECH proporciona ventajas específicas a los flujos de trabajo MEDEHR.

Sistema Cisco Unified Computing

Cisco Unified Computing System (Cisco UCS) es un sistema de integración automática que consta de un único dominio de gestión interconectado con una infraestructura de I/o unificada. Por lo que la infraestructura puede proporcionar información crítica al paciente con la máxima disponibilidad, Cisco UCS para entornos MEDITECH ha seguido las recomendaciones y prácticas recomendadas de la infraestructura MEDITECH.

La base de MEDITECH en la arquitectura Cisco UCS es la tecnología Cisco UCS, con sus sistemas integrados de gestión, procesadores Intel Xeon y virtualización de servidores. Estas tecnologías integradas resuelven los retos de los centros de datos y le ayudan a cumplir sus objetivos de diseño de centros de datos de MEDITECH. Cisco UCS unifica la gestión de LAN, SAN y sistemas en un enlace simplificado para servidores en rack, servidores blade y máquinas virtuales. Cisco UCS es una arquitectura de I/o integral que incorpora la estructura unificada de Cisco y la tecnología FEX (tecnología FEX) para conectar todos los componentes de Cisco UCS con una única estructura de red y una única capa de red.

El sistema se puede poner en marcha como una única o varias unidades lógicas que incorporen y escalan entre varios chasis blade, servidores en rack, racks y centros de datos. El sistema implementa una arquitectura radicalmente simplificada que elimina los múltiples dispositivos redundantes que pueblan el chasis de servidor blade tradicional y los servidores en rack. En los sistemas tradicionales, los dispositivos

redundantes como adaptadores Ethernet y FC y los módulos de gestión de chasis dan lugar a capas de complejidad. Cisco UCS está formado por un par redundante de interconexiones de estructura (FIS) de Cisco UCS que proporciona un único punto de gestión y un único punto de control para todo el tráfico de I/O.

Cisco UCS utiliza perfiles de servicio para ayudar a garantizar que los servidores virtuales de la infraestructura Cisco UCS estén configurados correctamente. Los perfiles de servicio están compuestos por políticas de red, almacenamiento e informática que los expertos en la materia crean una vez en cada disciplina. Los perfiles de servicio incluyen información crítica del servidor acerca de la identidad del servidor, como direccionamiento LAN y SAN, configuraciones de E/S, versiones de firmware, orden de arranque, red virtual LAN (VLAN), puerto físico y políticas QoS. Los perfiles de servicio pueden crearse y asociarse de forma dinámica con cualquier servidor físico del sistema en cuestión de minutos, en lugar de horas o días. La asociación de perfiles de servicio con servidores físicos se realiza como una única operación sencilla y permite la migración de identidades entre servidores del entorno sin necesidad de cambios de configuración física. Facilita un aprovisionamiento sencillo y rápido de sustituciones de servidores retirados.

El uso de perfiles de servicio ayuda a garantizar que los servidores estén configurados de forma coherente en toda la empresa. Cuando se emplean varios dominios de gestión de Cisco UCS, Cisco UCS Central puede utilizar perfiles de servicio globales para sincronizar la información de configuración y políticas entre dominios. Si es necesario realizar tareas de mantenimiento en un dominio, la infraestructura virtual se puede migrar a otro dominio. Este enfoque ayuda a garantizar que incluso cuando un único dominio está desconectado, las aplicaciones siguen funcionando con alta disponibilidad.

Para demostrar que cumple con los requisitos de configuración del servidor, Cisco UCS ha sido ampliamente probado con MEDITECH a lo largo de un período de varios años. Cisco UCS es una plataforma de servidor compatible, tal y como se indica en el sitio de soporte del sistema de recursos de productos de MEDITECH.

Redes Cisco

Los switches Cisco Nexus y los directores multicapa Cisco MDS ofrecen conectividad empresarial y consolidación SAN. Las redes de almacenamiento multiprotocolo de Cisco reducen el riesgo empresarial al proporcionar flexibilidad y opciones: FC, Fibre Connection (FICON), FC a través de Ethernet (FCoE), SCSI sobre IP (iSCSI) y FC sobre IP (FCIP).

Los switches Cisco Nexus ofrecen uno de los conjuntos de funciones de red de centro de datos más completos de una única plataforma. Ofrecen un alto rendimiento y densidad tanto para los centros de datos como para los núcleos de campus. También ofrecen un conjunto completo de funciones para la agregación de centros de datos, el fin de la fila y la interconexión de centros de datos en una plataforma modular altamente resiliente.

Cisco UCS integra los recursos de computación con los switches de Cisco Nexus y una estructura de I/o unificada que identifica y gestiona diferentes tipos de tráfico de red. Este tráfico incluye la I/o de almacenamiento, el tráfico de escritorios distribuido, la gestión y el acceso a aplicaciones clínicas y empresariales. Obtendrá:

- **Escalabilidad de la infraestructura.** la virtualización, la energía y refrigeración eficientes, la escala de la nube con automatización, alta densidad y alto rendimiento son compatibles con el crecimiento eficiente del centro de datos.
- **Continuidad operativa.** el diseño integra hardware, características del software NX-OS y gestión para admitir entornos sin tiempos de inactividad.
- **QoS de red e informática.** Cisco ofrece clase de servicio (cos) basada en políticas y QoS en las redes, el almacenamiento y la estructura informática para un rendimiento óptimo de las aplicaciones de misión crítica.
- **Flexibilidad de transporte.** adoptar gradualmente nuevas tecnologías de red con una solución rentable.

Juntos, Cisco UCS, con switches Cisco Nexus y directores multicapa Cisco MDS, proporciona una solución óptima de conectividad San, redes e informática para MEDITECH.

ONTAP de NetApp

El almacenamiento de NetApp que ejecuta el software ONTAP reduce los costes generales de almacenamiento a la vez que proporciona los tiempos de respuesta de lectura y escritura de baja latencia y las IOPS que necesitan las cargas de trabajo de MEDITECH. ONTAP admite tanto configuraciones de almacenamiento all-flash como híbrido para crear una plataforma de almacenamiento óptima que cumpla con los requisitos de MEDITECH. Los sistemas acelerados mediante flash de NetApp han recibido la validación y la certificación de MEDITECH, lo que le proporciona como cliente de MEDITECH el rendimiento y la capacidad de respuesta que son claves de las operaciones de MEDITECH sensibles a la latencia. Al crear varios dominios de fallos en un único clúster, los sistemas de NetApp también pueden aislar la producción de la producción de la producción. Los sistemas de NetApp también reducen los problemas de rendimiento con un nivel de rendimiento mínimo garantizado para las cargas de trabajo con la calidad de servicio de ONTAP.

La arquitectura de escalado horizontal del software ONTAP puede adaptarse con flexibilidad a varias cargas de trabajo de I/O. Para proporcionar el rendimiento necesario y la baja latencia que necesitan las aplicaciones clínicas a la vez que proporciona una arquitectura modular de escalado horizontal, las configuraciones all-flash normalmente se utilizan en arquitecturas ONTAP. Los nodos AFF de NetApp se pueden combinar en el mismo clúster de escalado horizontal con nodos de almacenamiento híbridos (HDD y flash) adecuados para almacenar conjuntos de datos de gran tamaño con un alto rendimiento. Junto con una solución de backup aprobada por MEDITECH, puede clonar, replicar y hacer backups de su entorno MEDITECH desde el costoso almacenamiento de unidades de estado sólido (SSD) a almacenamiento HDD más económico en otros nodos. Este enfoque cumple o supera las directrices de MEDITECH para el clonado basado en SAN y el backup de los pools de producción.

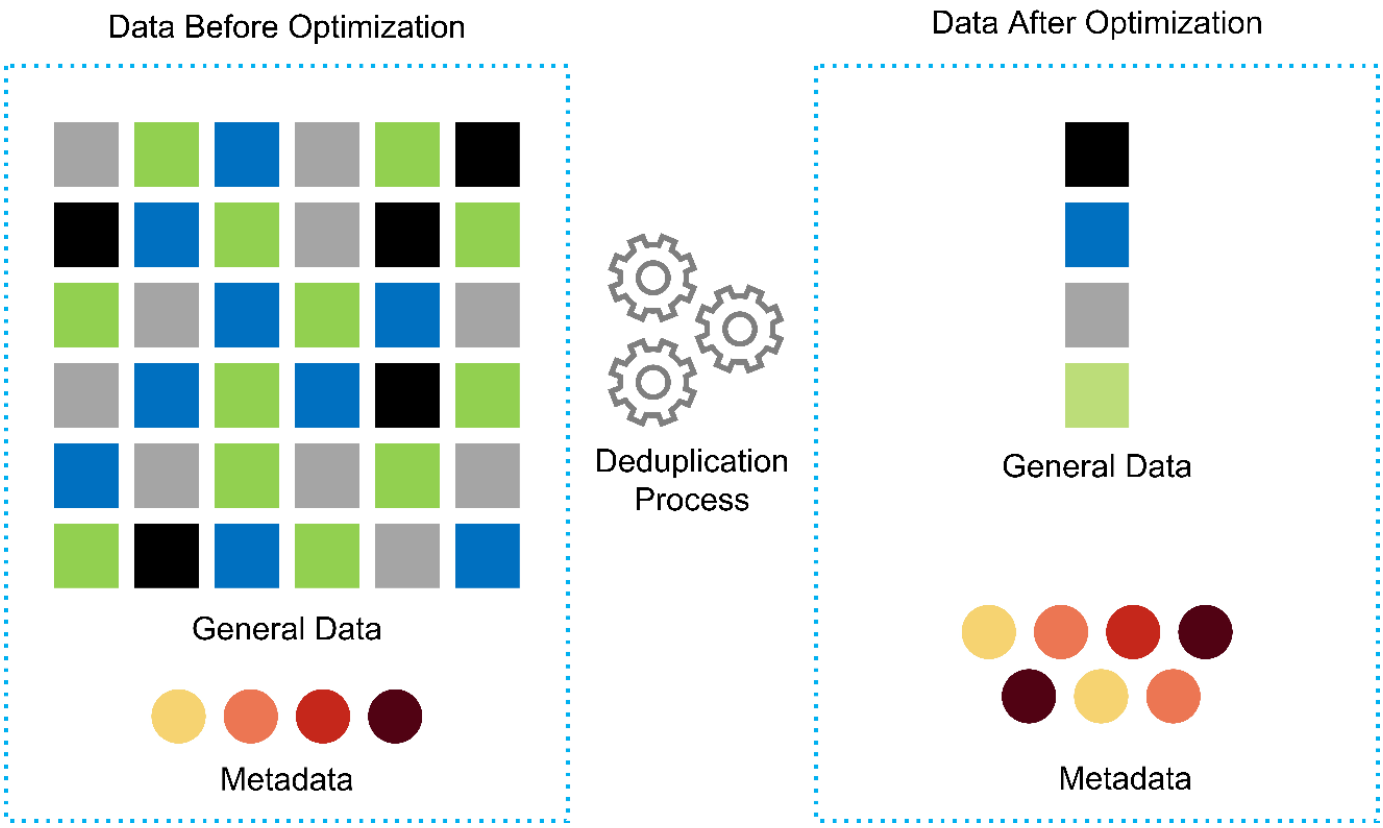
Muchas de las funciones de ONTAP son especialmente útiles en entornos de MEDITECH: Simplificar la gestión, aumentar la disponibilidad y la automatización, y reducir la cantidad total de almacenamiento necesaria. Con estas funciones obtendrá:

- *Rendimiento excepcional *. La solución AFF de NetApp comparte la arquitectura de almacenamiento unificado, el software ONTAP, la interfaz de gestión, los servicios de datos enriquecidos y el conjunto de funciones avanzadas que ofrecen el resto de las familias de productos FAS de NetApp. Esta innovadora combinación de medios all-flash con ONTAP ofrece la baja latencia consistente y las altas IOPS de almacenamiento all-flash con la calidad líder del sector del software ONTAP.
- **Eficiencia del almacenamiento.** reduzca los requisitos de capacidad total con deduplicación, tecnología de replicación de datos FlexClone de NetApp, compresión inline, compactación inline, thin replication, thin provisioning y deduplicación agregada.

  La deduplicación de NetApp proporciona deduplicación a nivel de bloque en un volumen FlexVol de NetApp o un componente de datos. En esencia, la deduplicación elimina los bloques duplicados y solo almacena los bloques únicos en el volumen FlexVol o el componente de datos.

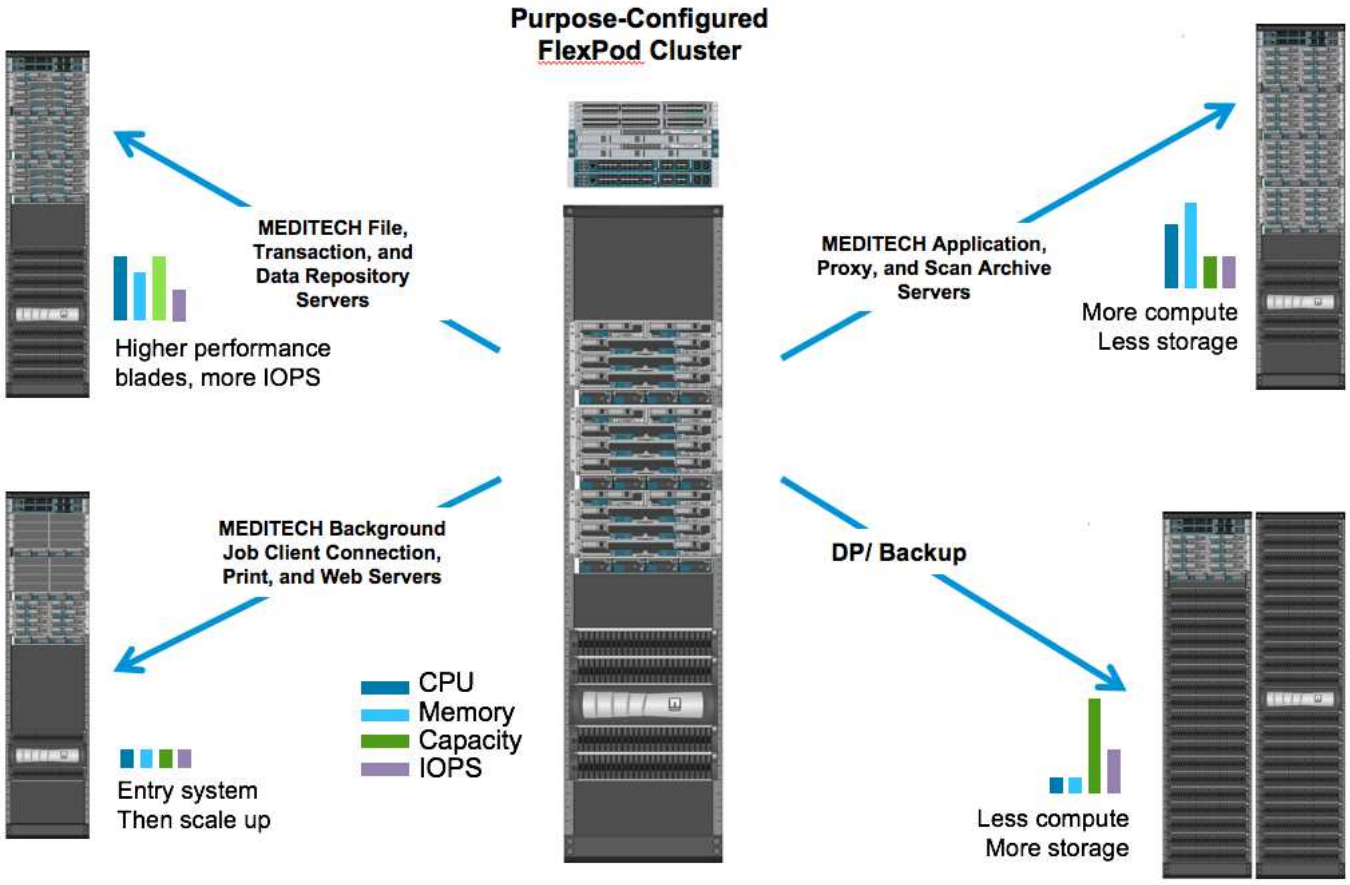
  La deduplicación funciona con un alto grado de granularidad y funciona en el sistema de archivos activo del volumen FlexVol o el componente de datos. Es transparente para las aplicaciones; por lo tanto, puede utilizarlas para deduplicar datos que se originan de cualquier aplicación que utilice el sistema de NetApp. Es posible ejecutar la deduplicación del volumen como un proceso en línea (a partir de ONTAP 8.3.2). También puede ejecutarlo como un proceso en segundo plano que puede configurar para que se ejecute automáticamente, para programar o para que se ejecute manualmente a través de la interfaz de línea de comandos, desde ONTAP System Manager de NetApp o desde Active IQ Unified Manager de NetApp.

  La figura siguiente ilustra cómo funciona la deduplicación de NetApp en el nivel más alto.



- **Clonado con gestión eficiente del espacio.** la funcionalidad FlexClone le permite crear clones casi al instante para admitir la actualización del entorno de copia de seguridad y pruebas. Estos clones consumen más almacenamiento únicamente cuando se realizan cambios.
- **Las tecnologías Snapshot y SnapMirror de NetApp.** ONTAP puede crear copias Snapshot de los números de unidad lógica (LUN) que utiliza el host MEDITECH con el ahorro de espacio. En el caso de puestas en marcha en sitio doble, puede implementar el software SnapMirror para obtener más resiliencia y replicación de datos.
- **Protección de datos integrada.** las funciones completas de protección de datos y recuperación ante desastres le ayudan a proteger los activos de datos críticos y a proporcionar recuperación ante desastres.
- **Operaciones no disruptivas.** puede realizar actualizaciones y mantenimiento sin tener que desconectar los datos.
- **QoS y Adaptive QoS (AQoS).** la calidad de servicio del almacenamiento le permite limitar las posibles cargas de trabajo de intimidación. Y lo que es más importante, la calidad de servicio puede garantizar un rendimiento mínimo para cargas de trabajo cruciales como la producción de MEDITECH. Al limitar la contención, la calidad de servicio de NetApp puede reducir los problemas relacionados con el rendimiento. AQoS funciona con grupos de políticas predefinidos que se pueden aplicar directamente a un volumen. Estos grupos de normativas pueden escalar automáticamente los límites máximos de rendimiento o de espacio en volumen, manteniendo la ratio de IOPS por terabytes y gigabytes a medida que cambie el tamaño del volumen.
- **Data Fabric de NetApp.** Data Fabric de NetApp simplifica e integra la gestión de datos en entornos de cloud y en las instalaciones para acelerar la transformación digital. Proporciona servicios y aplicaciones de gestión de datos consistentes e integrados para ofrecer visibilidad, información, acceso, control, protección y seguridad. NetApp se integra con Amazon Web Services (AWS), Azure, Google Cloud Platform e IBM Cloud, lo que aporta una gran variedad de opciones.

La siguiente figura muestra la arquitectura FlexPod para cargas de trabajo de MEDITECH.



Información general de MEDITECH

Medical Information Technology, Inc., comúnmente conocida como MEDITECH, es una compañía de software con sede en Massachusetts que proporciona sistemas de información a organizaciones sanitarias. MEDITECH proporciona un sistema EHR diseñado para almacenar y organizar los datos más recientes del paciente y proporcionar los datos al personal clínico. Los datos del paciente incluyen, entre otros, datos demográficos; antecedentes médicos; medicamentos; resultados de pruebas de laboratorio; imágenes radiológicos; e información personal como edad, altura y peso.

Supera el alcance de este documento para cubrir la amplia gama de funciones que admite el software MEDITECH. El Apéndice A proporciona más información sobre estos amplios conjuntos de funciones de MEDITECH. Las aplicaciones de MEDITECH requieren varias máquinas virtuales para admitir estas funciones. Para poner en marcha estas aplicaciones, consulte las recomendaciones de MEDITECH.

Para cada puesta en marcha, desde el punto de vista del sistema de almacenamiento, todos los sistemas de software de MEDITECH requieren una base de datos distribuida centrada en el paciente. MEDITECH tiene su propia base de datos propietaria, que utiliza el sistema operativo Windows.

Bridgehead y CommVault son las dos aplicaciones de software de backup certificadas por NetApp y MEDITECH. El alcance de este documento no cubre la implementación de estas aplicaciones de backup.

El objetivo principal de este documento es hacer que la pila FlexPod (servidores y almacenamiento) cumpla los requisitos de rendimiento establecidos para la base de datos de MEDITECH y los requisitos de backup del entorno EHR.

Creado específicamente para cargas de trabajo de MEDITECH específicas

MEDITECH no distribuye el hardware, los hipervisores o los sistemas operativos de servidor, la red o el almacenamiento; sin embargo, tiene requisitos específicos para cada componente de la pila de la infraestructura. Por lo tanto, Cisco y NetApp han trabajado juntos para probar y permitir que FlexPod Datacenter se configure, se ponga en marcha y sea compatible con éxito para cumplir los requisitos del entorno de producción de MEDITECH, tanto de clientes como usted.

Categorías de MEDITECH

MEDITECH asocia el tamaño de la implementación con un número de categoría que oscila entre 1 y 6. La categoría 1 representa las implementaciones de MEDITECH más pequeñas y la categoría 6 representa las implementaciones de MEDITECH más grandes.

Para obtener información sobre las características de I/o y los requisitos de rendimiento de un host MEDITECH en cada categoría, consulte NetApp "TR-4190: Directrices de tamaño de NetApp para entornos de MEDITECH".

Plataforma MEDITECH

La plataforma MEDITECH expanse es la última versión del software EHR de la compañía. Las plataformas MEDITECH anteriores son Client/Server 5.x y MAGIC. En esta sección se describe la plataforma MEDITECH (aplicable a expanse, 6.x, C/S 5.x y MAGIC), en relación con el host MEDITECH y sus requisitos de almacenamiento.

En todas las plataformas MEDITECH anteriores, varios servidores ejecutan el software MEDITECH, realizando diversas tareas. La figura anterior muestra un sistema MEDITECH típico, incluidos los hosts MEDITECH que funcionan como servidores de base de datos de aplicaciones y otros servidores MEDITECH. Entre los ejemplos de otros servidores de MEDITECH se incluyen la aplicación Data Repository, la aplicación Scanning and Archiving y los clientes de trabajos en segundo plano. Para obtener una lista completa de otros servidores de MEDITECH, consulte los documentos “propuesta de configuración de hardware” (para implementaciones nuevas) y “tarea de evaluación de hardware” (para implementaciones existentes). Puede obtener estos documentos de MEDITECH a través del integrador del sistema MEDITECH o de su MEDITECH Technical Account Manager (TAM).

Host MEDITECH

Un host MEDITECH es un servidor de base de datos. Este host también se conoce como servidor de archivos MEDITECH (para la plataforma expanse, 6.x o C/S 5.x) o COMO máquina MÁGICA (para la plataforma MAGIC). Este documento utiliza el término host de MEDITECH para hacer referencia a un servidor de archivos MEDITECH o A una máquina MÁGICA.

Los hosts MEDITECH pueden ser servidores físicos o máquinas virtuales que se ejecuten en el sistema operativo Microsoft Windows Server. Los hosts MEDITECH más comúnmente instalados en el sector, se ponen en marcha como máquinas virtuales Windows que se ejecutan en un servidor VMware ESXi. En el momento en el que se ha redactado este documento, VMware es el único hipervisor que admite MEDITECH. Un host de MEDITECH almacena sus archivos de programa, diccionario y datos en una unidad de Microsoft Windows (por ejemplo, unidad E) en el sistema Windows.

En un entorno virtual, una unidad E de Windows se encuentra en un LUN conectado a la máquina virtual mediante una asignación de dispositivo sin formato (RDM) en modo de compatibilidad física. MEDITECH no admite el uso de archivos de disco de máquina virtual (VMDK) como unidad Windows E en este escenario.

Característica de I/o de la carga de trabajo del host de MEDITECH

La característica de E/S de cada host de MEDITECH y el sistema en su conjunto depende de la plataforma MEDITECH que usted ponga en marcha. Todas las plataformas MEDITECH (expanse, 6.x, C/S 5.x y MAGIC) generan cargas de trabajo 100% aleatorias.

La plataforma de expansión MEDITECH genera la carga de trabajo más exigente porque tiene el mayor porcentaje de operaciones de escritura y de IOPS generales por host, seguido por 6.x, C/S 5.x y las plataformas MÁGICAS.

Para obtener más información acerca de las descripciones de las cargas de trabajo de MEDITECH, consulte "TR-4190: Directrices de tamaño de NetApp para entornos de MEDITECH".

Red de almacenamiento

MEDITECH requiere que el protocolo FC sea utilizado para el tráfico de datos entre el sistema FAS o AFF de NetApp y los hosts MEDITECH de todas las categorías.

Presentación del almacenamiento para un host de MEDITECH

Cada host de MEDITECH utiliza dos unidades Windows:

- **Drive C.** esta unidad almacena el sistema operativo Windows Server y los archivos de la aplicación host MEDITECH.
- **Drive E.** el host MEDITECH almacena sus archivos de programa, diccionario y datos en la unidad E del sistema operativo Windows Server. La unidad E es un LUN asignado desde el sistema FAS o AFF de NetApp mediante el protocolo FC. MEDITECH requiere que se utilice el protocolo FC para que se cumplan los requisitos de IOPS y de latencia de lectura y escritura del host MEDITECH.

Convención de nomenclatura de LUN y volúmenes

MEDITECH requiere que se utilice una convención de nomenclatura específica para todas las LUN.

Antes de cualquier implementación de almacenamiento, verifique la propuesta de configuración de hardware de MEDITECH para confirmar la convención de nomenclatura para las LUN. El proceso de backup de MEDITECH se basa en la convención de nomenclatura de LUN y volúmenes para identificar correctamente las LUN específicas a las que se debe realizar el backup.

Herramientas de gestión completas y funcionalidades de automatización

Cisco UCS con Cisco UCS Manager

Cisco se centra en tres elementos clave para ofrecer una infraestructura de centro de datos superior: Simplificación, seguridad y escalabilidad. El software Cisco UCS Manager, combinado con la modularidad de plataforma, ofrece una plataforma de virtualización de puestos de trabajo simplificada, segura y escalable:

- **Simplificado.** Cisco UCS ofrece un nuevo enfoque radical de la informática estándar del sector y proporciona el núcleo de la infraestructura del centro de datos para todas las cargas de trabajo. Cisco UCS ofrece numerosas funciones y ventajas, como la reducción del número de servidores que necesita y la reducción del número de cables que se utilizan por servidor. Otra función importante es la capacidad de poner en marcha o volver a aprovisionar servidores rápidamente mediante perfiles de servicio de Cisco UCS. Con menos servidores y cables que gestionar y con un provisionamiento optimizado de cargas de trabajo de servidores y aplicaciones, las operaciones se simplifican. La mayor parte de los servidores blade y en rack se pueden aprovisionar en minutos con los perfiles de servicio de Cisco UCS Manager. Los perfiles de servicio de Cisco UCS eliminan las agendas de integración de servidores y eliminan la

deriva en la configuración. Este método acelera el tiempo de productividad de los usuarios finales, mejora la agilidad empresarial y permite asignar recursos TECNOLÓGICOS a otras tareas.

Cisco UCS Manager automatiza muchas operaciones rutinarias y propensas a errores, como la configuración y el aprovisionamiento de infraestructura de acceso a servidores, redes y almacenamiento. Además, los servidores blade Cisco UCS B-Series y los servidores de montaje en rack C-Series con grandes espacios de memoria permiten una alta densidad de usuarios de aplicaciones, lo que ayuda a reducir los requisitos de infraestructura del servidor.

La simplificación conduce a una puesta en marcha de la infraestructura MEDITECH más rápida y satisfactoria.

- **Seguro.** aunque los equipos virtuales son inherentemente más seguros que sus predecesores físicos, introducen nuevos desafíos de seguridad. Los servidores web y de aplicaciones de misión crítica que utilizan una infraestructura común, como los escritorios virtuales, corren ahora un riesgo mayor de sufrir amenazas de seguridad. El tráfico entre máquinas virtuales ahora plantea una importante consideración de seguridad que sus administradores DE TI deben tratar, especialmente en entornos dinámicos en los que las máquinas virtuales, mediante VMware vMotion, se mueven por la infraestructura de servidores.

  Por lo tanto, la virtualización aumenta de forma significativa la necesidad de conocer las políticas y la seguridad a nivel de equipo virtual, sobre todo teniendo en cuenta la naturaleza dinámica y fluida de la movilidad de equipos virtuales en una infraestructura informática ampliada. La facilidad con la que pueden proliferar los nuevos escritorios virtuales amplía la importancia de una red compatible con la virtualización y una infraestructura de seguridad. La infraestructura de centro de datos de Cisco (soluciones de la familia Cisco UCS, Cisco MDS y Cisco Nexus) para la virtualización de escritorios proporciona una seguridad sólida de centros de datos, redes y escritorios, con una seguridad completa desde el escritorio hasta el hipervisor. La seguridad se mejora con la segmentación de puestos de trabajo virtuales, la administración y las políticas para máquinas virtuales y la seguridad de la red en la infraestructura LAN y WAN.

- **Escalable.** el crecimiento de las soluciones de virtualización es casi inevitable, por lo que una solución debe ser capaz de escalar, y de escalar de manera predecible, con ese crecimiento. Las soluciones de virtualización de Cisco admiten una alta densidad de equipos virtuales (equipos virtuales por servidor) y más servidores escalan con un rendimiento casi lineal. La infraestructura de centro de datos de Cisco proporciona una plataforma flexible para crecer y mejora la agilidad empresarial. Los perfiles de servicio de Cisco UCS Manager permiten el aprovisionamiento de hosts bajo demanda y facilitan la puesta en marcha de cientos de hosts al poner en marcha docenas.

  Los servidores Cisco UCS ofrecen un rendimiento y escalado prácticamente lineales. Cisco UCS implementa la tecnología patentada de memoria ampliada de Cisco para ofrecer espacios de memoria grandes con menos sockets (con escalabilidad de hasta 1 TB de memoria con servidores de 2 y 4 sockets). Al usar la tecnología Unified Fabric como elemento básico, el ancho de banda agregado de Cisco UCS Server puede escalarse hasta 80 Gbps por servidor, mientras que el conector de estructura Cisco UCS, enlazado al norte, puede proporcionar 2 TB a velocidad de línea. Esta funcionalidad ayuda a evitar los cuellos de botella de I/o y de memoria en la virtualización de puestos de trabajo. Cisco UCS, gracias a su arquitectura de redes unificada de alto rendimiento y baja latencia basada en Unified Fabric, admite grandes volúmenes de tráfico de escritorios virtuales, incluido el tráfico de comunicaciones y vídeo de alta resolución. Además, ONTAP ayuda a mantener la disponibilidad de datos y un rendimiento óptimo durante los arranques e inicios de sesión masivos como parte de las soluciones de virtualización de FlexPod.

  Los diseños de infraestructuras de centros de datos de Cisco UCS, Cisco MDS y Cisco Nexus proporcionan una plataforma excelente para el crecimiento. Obtiene un escalado transparente de los recursos de servidor, red y almacenamiento para dar soporte a la virtualización de puestos de trabajo, las aplicaciones del centro de datos y el cloud computing.

Servidor VMware vCenter

VMware vCenter Server proporciona una plataforma centralizada para la gestión de entornos MEDITECH, de modo que su organización sanitaria pueda automatizar y proporcionar una infraestructura virtual con total confianza:

- **Implementación sencilla.** ponga en marcha de forma rápida y sencilla vCenter Server con un dispositivo virtual.
- **Control y visibilidad centralizados.** administre toda la infraestructura VMware vSphere desde una única ubicación.
- **Optimización proactiva.** asignar y optimizar los recursos para lograr la máxima eficiencia.
- **Administración.** Utilice potentes complementos y herramientas para simplificar la administración y ampliar el control.

Virtual Storage Console para VMware vSphere

Virtual Storage Console (VSC), API de vSphere para el proveedor de conocimiento del almacenamiento (VASA) y VMware Storage Replication Adapter (SRA) para VMware vSphere de NetApp forman un único dispositivo virtual. La suite de productos incluye SRA y VASA Provider como complementos para vCenter Server, lo que proporciona gestión integral del ciclo de vida de las máquinas virtuales en entornos VMware que usan los sistemas de almacenamiento de NetApp.

El dispositivo virtual para VSC, proveedor VASA y SRA se integra sin problemas con VMware vSphere Web Client y permite utilizar los servicios SSO. En un entorno con varias instancias de VMware vCenter Server, cada instancia de vCenter Server que desea gestionar debe tener su propia instancia registrada de VSC. La página de consola VSC permite comprobar rápidamente el estado general de los almacenes de datos y las máquinas virtuales.

Al implementar el dispositivo virtual para VSC, proveedor VASA y SRA, puede realizar las siguientes tareas:

- **Use VSC para implementar y gestionar almacenamiento y configurar el host ESXi.** puede usar VSC para añadir credenciales, eliminar credenciales, asignar credenciales y configurar permisos para controladoras de almacenamiento en el entorno VMware. Además, puede gestionar servidores ESXi conectados a sistemas de almacenamiento de NetApp. Con un par de clics puede establecer valores de prácticas recomendadas para los tiempos de espera del host, NAS y multivía para todos los hosts. También puede ver detalles del almacenamiento y recopilar información de diagnóstico.
- **Utilice VASA Provider para crear perfiles de capacidad de almacenamiento y para establecer alarmas.** VASA Provider para ONTAP se registra en VSC cuando se activa la extensión VASA Provider. Se pueden crear y utilizar perfiles de funcionalidad del almacenamiento y almacenes de datos virtuales. También se pueden configurar alarmas para que avisen cuando los umbrales de los volúmenes y agregados estén casi llenos. Es posible supervisar el rendimiento de los VMDK y las máquinas virtuales que se crean en almacenes de datos virtuales.
- **Utilice SRA para la recuperación ante desastres.** puede utilizar SRA para configurar sitios protegidos y de recuperación en su entorno para la recuperación ante desastres durante los fallos.

OnCommand Insight y ONTAP de NetApp

OnCommand Insight de NetApp integra la gestión de la infraestructura en la cadena de suministro de servicios de MEDITECH. Este enfoque le proporciona a su organización del sector sanitario un mejor control, automatización y análisis de su infraestructura de almacenamiento, red y computación. Puede optimizar su infraestructura actual para maximizar las ventajas, a la vez que simplifica el proceso de determinar qué comprar y cuándo. Asimismo, se mitigan los riesgos asociados a las complejas migraciones tecnológicas. Como no requiere agentes, su instalación es sencilla y sin interrupciones. OnCommand Insight busca

continuamente dispositivos DE almacenamiento y SAN; asimismo, recopila información detallada para ofrecer una visibilidad total de todo el entorno de almacenamiento. Puede identificar rápidamente activos mal utilizados, mal alineados, infrautilizados o huérfanos, y recuperarlos para abastecer una futura expansión. OnCommand Insight le ayuda a:

- **Optimizar los recursos existentes.** identificar activos mal utilizados, infrautilizados o huérfanos mediante el uso de mejores prácticas establecidas para evitar problemas y satisfacer los niveles de servicio.
- **Tomar mejores decisiones.** los datos en tiempo real ayudan a resolver los problemas de capacidad más rápidamente para planificar con precisión las compras futuras, evitar el gasto excesivo y aplazar los gastos de capital.
- **Acelerar las iniciativas DE TI.** comprender mejor sus entornos virtuales para ayudarle a gestionar los riesgos, minimizar el tiempo de inactividad y acelerar la implementación de la nube.

Diseño

La arquitectura de FlexPod para MEDITECH se basa en las directrices de MEDITECH, Cisco y NetApp, y en la experiencia de los partners al trabajar con clientes de MEDITECH de todos los tamaños. La arquitectura es adaptable y aplica las prácticas recomendadas para MEDITECH, dependiendo de su estrategia de centro de datos, el tamaño de su organización y si su sistema está centralizado, distribuido o multi-tenant.

La arquitectura de almacenamiento correcta se puede determinar en función del tamaño general con las IOPS totales. El rendimiento por sí solo no es el único factor, y puede que decida utilizar un número de nodos mayor en función de los requisitos adicionales del cliente. La ventaja de usar el almacenamiento de NetApp es que puede escalar verticalmente el clúster de forma fácil y sin interrupciones a medida que cambian sus requisitos. También puede quitar nodos del clúster de forma no disruptiva para readaptar equipos o durante las actualizaciones de equipos.

A continuación se muestran algunas de las ventajas de la arquitectura de almacenamiento de ONTAP de NetApp:

- **Escalado vertical y horizontal sencillo y sin interrupciones.** puede actualizar, agregar o eliminar discos y nodos mediante operaciones no disruptivas de ONTAP. Puede comenzar con cuatro nodos y cambiar a seis nodos o actualizar a controladoras más grandes de forma no disruptiva.
- **Eficiencia del almacenamiento.** reduzca sus requisitos de capacidad total con deduplicación, FlexClone de NetApp, compresión inline, compactación inline, thin replication, thin provisioning y deduplicación agregada. La funcionalidad FlexClone le permite crear clones casi al instante para dar cabida a actualizaciones de entornos de backup y pruebas. Estos clones consumen más almacenamiento únicamente cuando se realizan cambios.
- **Servidor de bases de datos redundantes de recuperación ante desastres.** el servidor de bases de datos redundantes de recuperación ante desastres forma parte de su estrategia de continuidad empresarial (utilizado para admitir la funcionalidad de sólo lectura del almacenamiento y potencialmente configurada para ser una instancia de lectura/escritura del almacenamiento). Por lo tanto, la ubicación y el tamaño del tercer sistema de almacenamiento son normalmente los mismos que en el sistema de almacenamiento de base de datos de producción.
- **Consistencia de la base de datos (requiere algo de consideración).** Si utiliza las copias de backup de SnapMirror de NetApp en relación con la continuidad empresarial, consulte "TR-3446: Descripción general de SnapMirror Async y guía de prácticas recomendadas".

Distribución de almacenamiento

Agregados dedicados para los hosts de MEDITECH

El primer paso para cumplir los requisitos de alto rendimiento y alta disponibilidad de MEDITECH es diseñar correctamente la distribución del almacenamiento del entorno MEDITECH para aislar la carga de trabajo de producción del host MEDITECH en un almacenamiento dedicado de alto rendimiento.

Se debe aprovisionar un agregado dedicado en cada controlador de almacenamiento para almacenar los archivos de datos, el diccionario y el programa de los hosts de MEDITECH. Para eliminar la posibilidad de que otras cargas de trabajo utilicen los mismos discos y afecten al rendimiento, no se aprovisiona ningún otro tipo de almacenamiento de estos agregados.

> El almacenamiento que aprovisione para los otros servidores de MEDITECH no debe colocarse en el agregado dedicado para las LUN que utilizan los hosts de MEDITECH. Debería colocar el almacenamiento de otros servidores de MEDITECH en un agregado independiente. Los requisitos de almacenamiento para otros servidores de MEDITECH están disponibles en los documentos “propuesta de configuración de hardware” (para nuevas implementaciones) y “tarea de evaluación de hardware” (para implementaciones existentes). Puede obtener estos documentos de MEDITECH a través del integrador del sistema MEDITECH o de su MEDITECH Technical Account Manager (TAM). Los ingenieros de soluciones de NetApp pueden consultar con el equipo de MEDITECH Independent Software Vendor (ISV) de NetApp para facilitar una configuración de tamaño de almacenamiento adecuada y completa de NetApp.

Distribuya la carga de trabajo del host de MEDITECH de forma uniforme en todas las controladoras de almacenamiento

Los sistemas FAS y AFF de NetApp se ponen en marcha como uno o varios pares de alta disponibilidad. NetApp recomienda que distribuya las cargas de trabajo de MEDITECH y 6.x de forma uniforme en cada controladora de almacenamiento para aplicar los recursos de computación, red y almacenamiento en caché en cada controladora de almacenamiento.

Utilice las siguientes directrices para distribuir las cargas de trabajo de MEDITECH de forma uniforme en cada controladora de almacenamiento:

- Si conoce las IOPS de cada host de MEDITECH, puede propagar las cargas de trabajo MEDITECH expantech y 6.x de manera uniforme en todas las controladoras de almacenamiento confirmando que cada controladora admite un número similar de IOPS de los hosts MEDITECH.
- Si no conoce las IOPS de cada host de MEDITECH, podrá seguir difundiéndose las cargas de trabajo MEDITECH y 6.x a todas las controladoras de almacenamiento. Complete esta tarea confirmando que la capacidad de los agregados de los hosts de MEDITECH se distribuye de forma uniforme entre todas las controladoras de almacenamiento. De esta forma, el número de discos es el mismo en todas las agrupaciones de datos que están dedicadas a los hosts de MEDITECH.
- Utilice tipos de disco similares y grupos RAID idénticos para crear agregados de almacenamiento de ambas controladoras para distribuir las cargas de trabajo por igual. Antes de crear el agregado de almacenamiento, póngase en contacto con un integrador certificado de NetApp.

> Según MEDITECH, dos hosts del sistema MEDITECH generan un IOPS mayor que el resto de los hosts. Los LUN de estos dos hosts se deben colocar en controladoras de almacenamiento independientes. Debe identificar estos dos hosts con la ayuda del equipo de MEDITECH antes de implantar su sistema.

Ubicación del almacenamiento

Almacenamiento de base de datos para hosts de MEDITECH

El almacenamiento de la base de datos para un host de MEDITECH se presenta como dispositivo de bloque (es decir, una LUN) desde el sistema FAS o AFF de NetApp. La LUN suele montarse en el sistema operativo Windows como la unidad E.

Otros almacenamientos

El sistema operativo host de MEDITECH y la aplicación de base de datos suelen generar una cantidad considerable de IOPS en el almacenamiento. El aprovisionamiento de almacenamiento para las máquinas virtuales host de MEDITECH y sus archivos VMDK, si es necesario, se considera independiente del almacenamiento necesario para cumplir los umbrales de rendimiento de MEDITECH.

El almacenamiento que se aprovisiona para los demás servidores de MEDITECH no debe colocarse en el agregado dedicado para las LUN que utilizan los hosts de MEDITECH. Coloque el almacenamiento de otros servidores de MEDITECH en una agrupación independiente.

Configuración de la controladora de almacenamiento

Alta disponibilidad

Para mitigar el efecto del fallo de la controladora y permitir actualizaciones no disruptivas del sistema de almacenamiento, debe configurar su sistema de almacenamiento con controladoras en un par de alta disponibilidad en el modo de alta disponibilidad.

Con la configuración de pares de controladoras de alta disponibilidad, las bandejas de discos deben conectarse a controladoras mediante varias rutas. Esta conexión aumenta la resiliencia del almacenamiento al protegerle contra un fallo de ruta única y mejora la consistencia del rendimiento en caso de fallo de controladora.

Rendimiento del almacenamiento durante la recuperación tras fallos de la controladora de almacenamiento

En el caso de los sistemas de almacenamiento configurados con controladoras de un par de alta disponibilidad, en el improbable caso de que se produzca un fallo en una controladora, la controladora del partner toma el control de las cargas de trabajo y los recursos de almacenamiento de la controladora que ha fallado. Es importante consultar al cliente para determinar los requisitos de rendimiento que se deben cumplir si hay un error en la controladora y ajustar el tamaño del sistema según corresponda.

Toma de control asistida por hardware

NetApp recomienda activar la función de toma de control asistida por hardware en ambas controladoras de almacenamiento.

La toma de control asistida por hardware está diseñada para minimizar el tiempo de recuperación tras fallas de las controladoras de almacenamiento. Permite que el módulo de LAN remota o el módulo del procesador de servicio de un controlador notifique a su compañero acerca de un fallo de controlador más rápidamente de lo que puede haber un disparador de tiempo de espera de latido, reduciendo así el tiempo que tarda en recuperarse tras fallos. La función de toma de control asistida por hardware está habilitada de forma predeterminada para las controladoras de almacenamiento en una configuración de alta disponibilidad.

Para obtener más información sobre la toma de control asistida por hardware, consulte "Centro de documentación de ONTAP 9".

Tipo de disco

Para admitir los requisitos de baja latencia de lectura de las cargas de trabajo de MEDITECH, NetApp recomienda utilizar una SSD de alto rendimiento para las agregados de los sistemas AFF dedicados a los hosts MEDITECH.

AFF de NetApp

NetApp ofrece cabinas AFF de alto rendimiento para abordar las cargas de trabajo de MEDITECH que exigen un alto rendimiento y que tienen patrones de acceso aleatorio a los datos y requisitos de baja latencia. Para las cargas de trabajo de MEDITECH, las cabinas AFF ofrecen ventajas de rendimiento con respecto a los sistemas basados en HDD. La combinación de la tecnología flash y la gestión de datos empresariales ofrece ventajas en tres áreas principales: Rendimiento, disponibilidad y eficiencia del almacenamiento.

Herramientas y servicios de soporte de NetApp

NetApp ofrece un conjunto completo de herramientas de soporte y servicios. La herramienta AutoSupport de NetApp debe estar habilitada y configurada en los sistemas AFF/FAS de NetApp para llamar a casa si se produce un error de hardware o una configuración incorrecta del sistema. Llamar a casa envía alertas al equipo de soporte de NetApp para solucionar cualquier problema de forma puntual. Active IQ de NetApp es una aplicación basada en web que se basa en la información de AutoSupport de sus sistemas de NetApp. Proporciona información predictiva y predictiva con la que mejorar la disponibilidad, la eficiencia y el rendimiento.

Puesta en marcha y configuración

Descripción general

Las directrices sobre almacenamiento de NetApp para la puesta en marcha de FlexPod que se ofrecen en este documento tratan:

- Entornos que usan ONTAP
- Entornos que usan servidores blade y de montaje en rack de Cisco UCS

Este documento no cubre:

- Puesta en marcha detallada del entorno de centro de datos de FlexPod

  Para obtener más información, consulte "Centro de datos FlexPod con diseño validado por FC Cisco" (CVD).

- Descripción general de los entornos de software de MEDITECH, arquitecturas de referencia y directrices de las mejores prácticas de integración.

  Para obtener más información, consulte "TR-4300i: Guía de prácticas recomendadas de sistemas de almacenamiento all-flash y FAS de NetApp para entornos MEDITECH" (Se requiere inicio de sesión de NetApp).

- Requisitos cuantitativos de rendimiento y orientación en la configuración.

  Para obtener más información, consulte "TR-4190: Directrices de tamaño de NetApp para entornos de MEDITECH".

- Uso de las tecnologías SnapMirror de NetApp para cumplir los requisitos de backup y recuperación ante

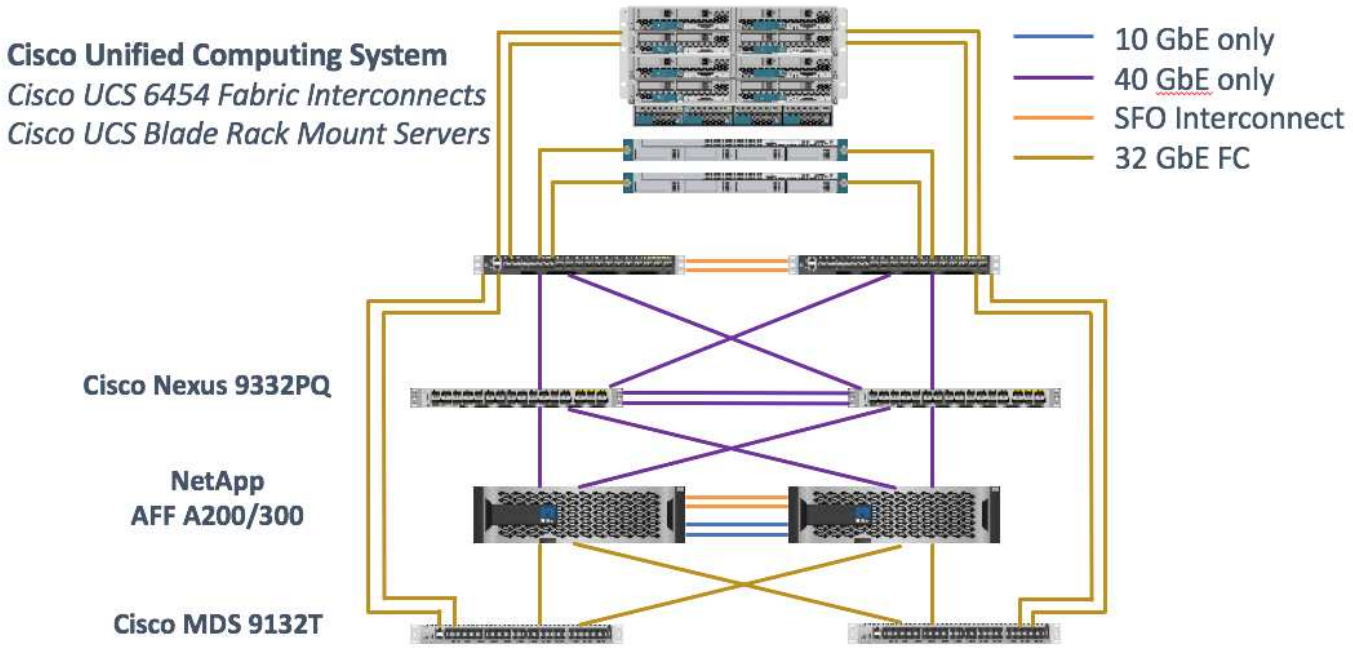
desastres.

- Directrices generales para la implementación del almacenamiento de NetApp.

En esta sección se proporciona un ejemplo de configuración con prácticas recomendadas de implementación de la infraestructura y se enumeran los distintos componentes de hardware y software de la infraestructura y las versiones que puede utilizar.

Diagrama de cableado

La siguiente figura ilustra el diagrama de topología de FC/40 GbE de 32 GB para la implementación de MEDITECH.



Utilice siempre la "Herramienta de matriz de interoperabilidad (IMT)" validar que todas las versiones de software y firmware son compatibles. La tabla de la sección "Módulos y componentes de MEDITECH" la enumera los componentes de hardware y software de la infraestructura que se usaron en la prueba de la solución.

"Siguiente: Configuración de infraestructura base."

Configuración de la infraestructura base

Conectividad de la red

Antes de configurar la infraestructura, deben existir las siguientes conexiones de red:

- La agregación de enlaces que utiliza canales de puertos y canales de puertos virtuales (VPC) se utiliza en todo el proceso, lo que permite un diseño de mayor ancho de banda y alta disponibilidad:
  - VPC se utiliza entre los switches DE Cisco FI y Cisco Nexus.
  - Cada servidor tiene tarjetas de interfaz de red virtuales (vNIC) con conectividad redundante a Unified Fabric. La conmutación por error de NIC se utiliza entre FIS para redundancia.
  - Cada servidor tiene adaptadores de bus de host virtual (vHBA) con conectividad redundante al tejido unificado.

- Cisco UCS FI se configura en modo de host final como se recomienda, proporcionando fijación dinámica de NIC virtuales a switches de enlace ascendente.

Conectividad del almacenamiento

Para poder configurar la infraestructura, deben haberse implementado las siguientes conexiones de almacenamiento:

- Grupos de interfaces de puertos de almacenamiento (grupos de interfaces, VPC)
- Enlace de 10 GB para cambiar N9K-A
- Enlace de 10 GB al interruptor N9K-B
- Gestión en banda (enlace activo-pasivo):
  - Enlace de 1 GB al switch de administración N9K-A
  - Enlace de 1 GB al switch de administración N9K-B
- Conectividad integral de FC de 32 GB mediante switches Cisco MDS; división en zonas de iniciador único configurada
- Arranque SAN FC para lograr equipos informáticos sin estado; los servidores se inician desde las LUN en el volumen de arranque que se aloja en el clúster de almacenamiento de AFF
- Todas las cargas de trabajo de MEDITECH están alojadas en LUN FC, que se distribuyen por los nodos de la controladora de almacenamiento

Software host

Debe instalarse el siguiente software:

- ESXi instalado en los blades de Cisco UCS
- VMware vCenter instalado y configurado (con todos los hosts registrados en vCenter)
- VSC se instaló y se registró en VMware vCenter
- Se configuró el clúster de NetApp

"Siguiente: Configuración de switch y servidor blade Cisco UCS."

Configuración de switch y servidor blade Cisco UCS

El software FlexPod for MEDITECH está diseñado con tolerancia a fallos en todos los niveles. No existe ningún punto único de error en el sistema. Para obtener un rendimiento óptimo, Cisco recomienda el uso de servidores blade de repuesto en caliente.

Este documento proporciona directrices de alto nivel sobre la configuración básica de un entorno FlexPod para el software MEDITECH. En esta sección, presentamos pasos de alto nivel con algunos ejemplos para preparar el elemento de plataforma informática de Cisco UCS de la configuración de FlexPod. Un requisito previo para esta guía es que la configuración de FlexPod se encuentra en rack, encendida y cableada según las instrucciones de la "FlexPod Datacenter con almacenamiento Fibre Channel y VMware vSphere 6.5 Update 1, AFF A-series de NetApp y UCS Manager 3.2 de Cisco"CVD.

Configuración de switches Cisco Nexus

Para esta solución se ha puesto en marcha un par tolerante a fallos de los switches Ethernet de la serie Cisco Nexus 9300. Debe cablear estos switches como se describe en el "Diagrama de cableado" sección. La configuración de Cisco Nexus ayuda a garantizar que los flujos de tráfico Ethernet estén optimizados para la aplicación MEDITECH.

1. Una vez finalizada la instalación y la licencia iniciales, ejecute los siguientes comandos para establecer los parámetros de configuración global en ambos switches:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
port-channel load-balance src-dst l4port
ntp server <global-ntp-server-ip> use-vrf management
ntp master 3
ip route 0.0.0.0/0 <ib-mgmt-vlan-gateway>
copy run start
```

2. Cree las VLAN para la solución en cada switch mediante el modo de configuración global:

```
vlan <ib-mgmt-vlan-id>
name IB-MGMT-VLAN
vlan <native-vlan-id>
name Native-VLAN
vlan <vmotion-vlan-id>
name vMotion-VLAN
vlan <vm-traffic-vlan-id>
name VM-Traffic-VLAN
vlan <infra-nfs-vlan-id>
name Infra-NFS-VLAN
exit
copy run start
```

3. Cree la interfaz de distribución del Protocolo de tiempo de redes (NTP), los canales de puertos, los parámetros del canal de puertos y las descripciones de puertos para la solución de problemas según "FlexPod Datacenter con almacenamiento Fibre Channel y VMware vSphere 6.5 Update 1, AFF A-series de NetApp y UCS Manager 3.2 de Cisco"CVD.

Configuración de Cisco MDS 9132T

Los switches FC de la serie Cisco MDS 9100 proporcionan conectividad FC redundante de 32 GB entre las controladoras AFF A200 o AFF A300 de NetApp y el entramado de computación Cisco UCS. Debe conectar los cables tal como se describe en "Diagrama de cableado" sección.

1. Desde las consolas de cada conmutador MDS, ejecute los siguientes comandos para habilitar las características necesarias para la solución:

```
configure terminal
feature npiv
feature fport-channel-trunk
```

2. Configure puertos individuales, canales de puertos y descripciones de acuerdo con la sección de configuración del switch Cisco MDS de FlexPod de "Centro de datos FlexPod con diseño validado por FC Cisco".
3. Para crear las San virtuales (VSan) necesarias para la solución, realice los pasos siguientes mientras se encuentra en el modo de configuración global:
   a. Para el conmutador MDS Fabric-A, ejecute los siguientes comandos:

```
vsan database
vsan <vsan-a-id>
vsan <vsan-a-id> name Fabric-A
exit
zone smart-zoning enable vsan <vsan-a-id>
vsan database
vsan <vsan-a-id> interface fc1/1
vsan <vsan-a-id> interface fc1/2
vsan <vsan-a-id> interface port-channel110
vsan <vsan-a-id> interface port-channel112
```

   Los números de canal de puerto de las dos últimas líneas del comando se crearon cuando los puertos, canales de puerto y descripciones individuales se aprovisionaron mediante el documento de referencia.

   b. Para el conmutador MDS Fabric-B, ejecute los siguientes comandos:

```
vsan database
vsan <vsan-b-id>
vsan <vsan-b-id> name Fabric-B
exit
zone smart-zoning enable vsan <vsan-b-id>
vsan database
vsan <vsan-b-id> interface fc1/1
vsan <vsan-b-id> interface fc1/2
vsan <vsan-b-id> interface port-channel111
vsan <vsan-b-id> interface port-channel113
```

   Los números de canal de puerto de las dos últimas líneas del comando se crearon cuando los puertos, canales de puerto y descripciones individuales se aprovisionaron mediante el documento de referencia.

4. Para cada switch FC, cree nombres de alias de dispositivo que hagan que la identificación de cada dispositivo sea intuitiva para las operaciones en curso utilizando los detalles del documento de referencia.

5. Finalmente, cree las zonas FC utilizando los nombres de alias de dispositivo que se crearon en el paso 4 para cada switch MDS de la siguiente forma:

   a. Para el conmutador MDS Fabric-A, ejecute los siguientes comandos:

```
configure terminal
zone name VM-Host-Infra-01-A vsan <vsan-a-id>
member device-alias VM-Host-Infra-01-A init
member device-alias Infra-SVM-fcp_lif01a target
member device-alias Infra-SVM-fcp_lif02a target
exit
zone name VM-Host-Infra-02-A vsan <vsan-a-id>
member device-alias VM-Host-Infra-02-A init
member device-alias Infra-SVM-fcp_lif01a target
member device-alias Infra-SVM-fcp_lif02a target
exit
zoneset name Fabric-A vsan <vsan-a-id>
member VM-Host-Infra-01-A
member VM-Host-Infra-02-A
exit
zoneset activate name Fabric-A vsan <vsan-a-id>
exit
show zoneset active vsan <vsan-a-id>
```

   b. Para el conmutador MDS Fabric-B, ejecute los siguientes comandos:

```
configure terminal
zone name VM-Host-Infra-01-B vsan <vsan-b-id>
member device-alias VM-Host-Infra-01-B init
member device-alias Infra-SVM-fcp_lif01b target
member device-alias Infra-SVM-fcp_lif02b target
exit
zone name VM-Host-Infra-02-B vsan <vsan-b-id>
member device-alias VM-Host-Infra-02-B init
member device-alias Infra-SVM-fcp_lif01b target
member device-alias Infra-SVM-fcp_lif02b target
exit
zoneset name Fabric-B vsan <vsan-b-id>
member VM-Host-Infra-01-B
member VM-Host-Infra-02-B
exit
zoneset activate name Fabric-B vsan <vsan-b-id>
exit
show zoneset active vsan <vsan-b-id>
```

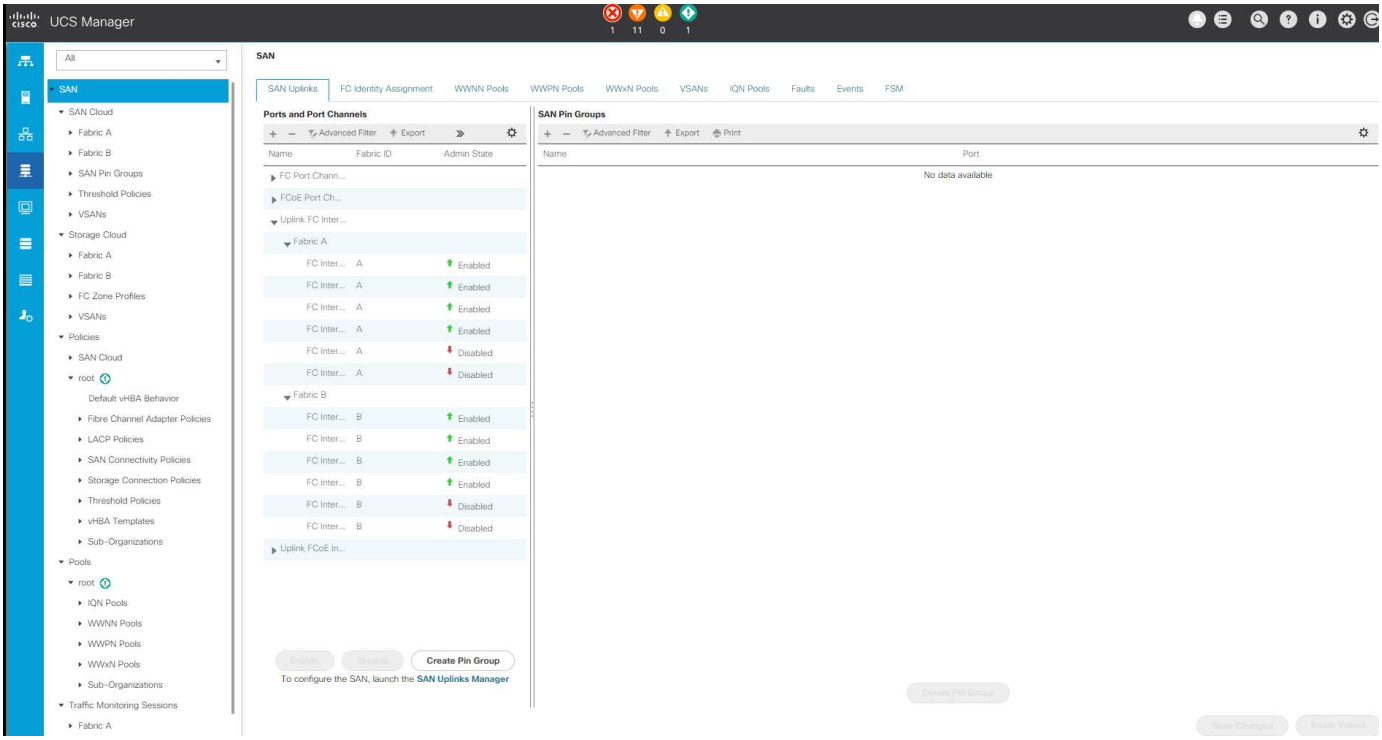
Directrices para la configuración de Cisco UCS

Cisco UCS le permite, como cliente de MEDITECH, aprovechar sus expertos en la materia en redes, almacenamiento y computación para crear políticas y plantillas que adaptan el entorno a sus necesidades específicas. Después de crearse, estas políticas y plantillas pueden combinarse en perfiles de servicio que ofrecen una puesta en marcha coherente, repetible, fiable y rápida de servidores blade y en rack de Cisco.

Cisco UCS proporciona tres métodos para gestionar un sistema Cisco UCS, denominado dominio:

- Interfaz gráfica de usuario HTML5 de Cisco UCS Manager
- CLI de Cisco UCS
- Cisco UCS Central para entornos multidominio

La figura siguiente muestra una captura de pantalla de ejemplo del nodo SAN en Cisco UCS Manager.



En puestas en marcha más grandes, se pueden crear dominios Cisco UCS independientes para obtener una mayor tolerancia a fallos a nivel de componente funcional de MEDITECH.

En diseños con gran tolerancia a fallos con dos o más centros de datos, Cisco UCS Central desempeña un papel fundamental a la hora de establecer políticas globales y perfiles de servicio globales para la coherencia entre los hosts de toda la empresa.

Para configurar la plataforma de computación Cisco UCS, complete los siguientes procedimientos. Realice estos procedimientos después de que se instalen los servidores blade Cisco UCS B200 M5 en el chasis blade Cisco UCS 5108 CA. Además, debe competir con los requisitos de cableado como se describe en "Diagrama de cableado" sección.

1. Actualice el firmware de Cisco UCS Manager a la versión 3.2(2f) o posterior.
2. Configure los informes, las características de llamada a casa de Cisco y los ajustes de NTP para el dominio.
3. Configure el servidor y los puertos de enlace ascendente en cada Fabric Interconnect.

4. Edite la política de detección del chasis.
5. Cree los pools de direcciones para gestión fuera de banda, identificadores únicos universales (UUID), dirección MAC, servidores, nombre de nodo mundial (WWNN) y nombre de puerto WWPN.
6. Cree los canales de puertos de enlace ascendente Ethernet y FC y las VSan.
7. Crear políticas para conectividad SAN, control de red, cualificación de grupos de servidores, control de energía, BIOS de servidores, y el mantenimiento predeterminado.
8. Cree plantillas VNIC y Vhba.
9. Crear directivas de arranque de vMedia y FC.
10. Cree plantillas de perfil de servicio y perfiles de servicio para cada elemento de plataforma de MEDITECH.
11. Asocie los perfiles de servicio con los servidores blade adecuados.

Para obtener los pasos detallados para configurar cada elemento clave de los perfiles de servicio de Cisco UCS para FlexPod, consulte "FlexPod Datacenter con almacenamiento Fibre Channel y VMware vSphere 6.5 Update 1, AFF A-series de NetApp y UCS Manager 3.2 de Cisco"Documento CVD.

"Siguiente: Mejores prácticas de configuración de ESXi."

Prácticas recomendadas de configuración de ESXi

Para la configuración del lado del host ESXi, configure los hosts VMware como si ejecutaría cualquier carga de trabajo de base de datos empresarial:

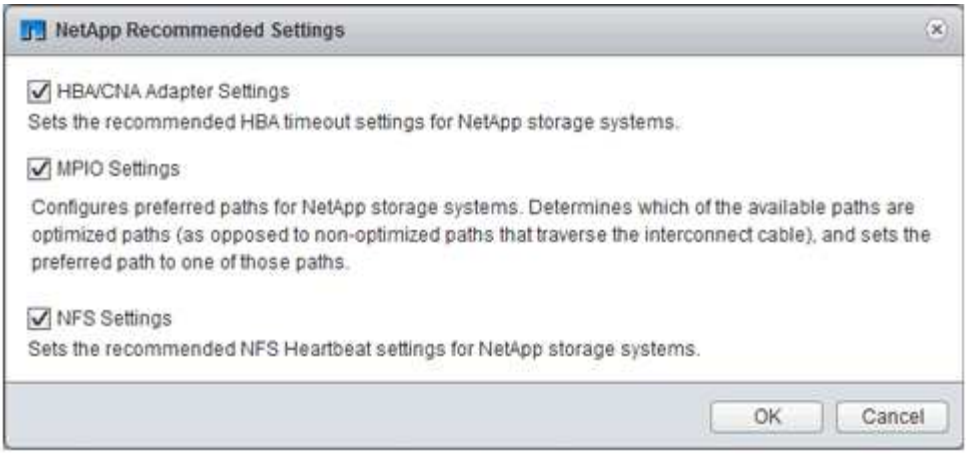
- VSC para VMware vSphere comprueba y configura la configuración de accesos múltiples del host ESXi y de tiempo de espera de HBA que funcionan mejor con los sistemas de almacenamiento de NetApp. Los valores que conjuntos de VSC se basan en rigurosas pruebas internas realizadas por NetApp.
- Para obtener un rendimiento óptimo del almacenamiento, considere la posibilidad de usar hardware de almacenamiento que admita API de VMware vStorage: Integración de cabinas (VAAI). El plugin de NetApp para VAAI es una biblioteca de software que integra las bibliotecas de discos virtuales de VMware que están instaladas en el host ESXi. El paquete VAAI de VMware permite descargar determinadas tareas de los hosts físicos a la cabina de almacenamiento.

  Puede realizar tareas como thin provisioning y la aceleración de hardware en el nivel de cabina para reducir la carga de trabajo en los hosts ESXi. La función de copia de liberación de sobrecarga y reserva de espacio mejoran el rendimiento de las operaciones de VSC. Puede descargar el paquete de instalación del plugin y obtener las instrucciones de instalación del plugin en el sitio de soporte de NetApp.

  VSC establece los tiempos de espera de host ESXi, la configuración de multivía y la configuración de tiempo de espera de HBA y otros valores para obtener un rendimiento óptimo y conmutación por error correcta de las controladoras de almacenamiento de NetApp. Siga estos pasos:

  a. En la página de inicio de VMware vSphere Web Client, seleccione vCenter > hosts.
  b. Haga clic con el botón derecho en un host y seleccione Actions > NetApp VSC > Set Recommended Values.
  c. En el cuadro de diálogo NetApp Recommended Settings, seleccione los valores que mejor se adapten a su sistema.

     Los valores estándar recomendados se establecen de forma predeterminada.



a. Haga clic en Aceptar.

"Siguiente: Configuración de NetApp."

Configuración de NetApp

El sistema de almacenamiento de NetApp que se pone en marcha para entornos de software de MEDITECH utiliza controladoras de almacenamiento en una configuración de parejas de alta disponibilidad. El almacenamiento debe presentarse desde ambas controladoras a los servidores de base de datos de MEDITECH a través del protocolo FC. La configuración presenta almacenamiento de ambas controladoras para equilibrar de forma uniforme la carga de las aplicaciones durante un funcionamiento normal.

Configuración de ONTAP

En esta sección se describe un ejemplo de procedimientos de puesta en marcha y aprovisionamiento que utilizan los comandos de ONTAP relevantes. El énfasis se da en mostrar cómo se aprovisiona el almacenamiento para implementar el diseño del almacenamiento que recomienda NetApp, que utiliza un par de controladoras de alta disponibilidad. Una de las principales ventajas de ONTAP es la capacidad de escalar horizontalmente sin alterar los pares de alta disponibilidad existentes.

Licencias ONTAP

Una vez configuradas las controladoras de almacenamiento, aplique licencias para habilitar las funciones de ONTAP que recomienda NetApp. Las licencias para cargas de trabajo de MEDITECH son FC, CIFS, y Snapshot, SnapRestore, FlexClone, Y SnapMirror.

Para configurar las licencias, abra ONTAP System Manager de NetApp, vaya a Configuration-Licenses y, a continuación, añada las licencias que correspondan.

También puede ejecutar el siguiente comando para añadir licencias utilizando la CLI:

```
license add -license-code <code>
```

Configuración de AutoSupport

La herramienta AutoSupport de NetApp envía información de soporte resumida a NetApp mediante la HTTPS.

Para configurar AutoSupport, ejecute los siguientes comandos de la ONTAP:

```
autosupport modify -node * -state enable
autosupport modify -node * -mail-hosts <mailhost.customer.com>
autosupport modify -node prod1-01 -from prod1-01@customer.com
autosupport modify -node prod1-02 -from prod1-02@customer.com
autosupport modify -node * -to storageadmins@customer.com
autosupport modify -node * -support enable
autosupport modify -node * -transport https
autosupport modify -node * -hostnamesubj true
```

Configuración de toma de control asistida por hardware

En cada nodo, habilite la toma de control asistida por hardware para minimizar el tiempo que se tarda en iniciar una toma de control en el caso poco probable de que se produzca un fallo en una controladora. Para configurar la toma de control asistida por hardware, lleve a cabo los siguientes pasos:

1. Ejecute el siguiente comando de ONTAP a xxx.

   Establezca la opción de dirección de partner en la dirección IP del puerto de administración para `prod1-01`.

   ```
   MEDITECH::> storage failover modify -node prod1-01 -hwassist-partner-ip
   <prod1-02-mgmt-ip>
   ```

2. Ejecute el siguiente comando de ONTAP en xxx:

   Establezca la opción de dirección de partner en la dirección IP del puerto de administración para `cluster1-02`.

   ```
   MEDITECH::> storage failover modify -node prod1-02 -hwassist-partner-ip
   <prod1-01-mgmt-ip>
   ```

3. Ejecute el siguiente comando ONTAP para permitir la toma de control asistida por hardware en ambos `prod1-01` y la `prod1-02` Par de controladoras DE ALTA DISPONIBILIDAD.

   ```
   MEDITECH::> storage failover modify -node prod1-01 -hwassist true
   MEDITECH::> storage failover modify -node prod1-02 -hwassist true
   ```

"Siguiente: Configuración de agregados."

Configuración de agregados

RAID DP de NetApp

NetApp recomienda la tecnología RAID DP de NetApp como tipo de RAID para todos los agregados en un sistema FAS o AFF de NetApp, incluidos los agregados normales Flash Pool de NetApp. La documentación de MEDITECH podría especificar el uso de RAID 10, pero MEDITECH ha aprobado el uso de RAID DP.

Tamaño del grupo RAID y número de grupos RAID

El tamaño de grupo RAID predeterminado es 16. Este tamaño puede ser o no óptimo para los agregados de los hosts MEDITECH en su sitio específico. Para ver el número de discos que NetApp recomienda utilizar en un grupo RAID, consulte "NetApp TR-3838: Guía de configuración del subsistema de almacenamiento".

El tamaño del grupo RAID es importante para la ampliación de almacenamiento, ya que NetApp recomienda añadir discos a un agregado con uno o más grupos de discos iguales al tamaño del grupo RAID. La cantidad de grupos RAID depende del número de discos de datos y del tamaño del grupo RAID. Para determinar el número de discos de datos que necesita, utilice la herramienta de ajuste de tamaño System Performance Modeler (SPM) de NetApp. Después de determinar el número de discos de datos, ajuste el tamaño del grupo RAID para minimizar el número de discos de paridad dentro del intervalo recomendado para el tamaño del grupo RAID por tipo de disco.

Para obtener más información sobre cómo utilizar la herramienta de tamaño SPM para entornos de MEDITECH, consulte "NetApp TR-4190: Estimaciones de tamaño de NetApp para entornos de MEDITECH".

Consideraciones sobre la ampliación del almacenamiento

Cuando expanda agregados con más discos, añada los discos en grupos que sean iguales al tamaño del grupo RAID de agregado. A continuación, se sigue este método para proporcionar consistencia del rendimiento en todo el agregado.

Por ejemplo, para agregar almacenamiento a un agregado que se creó con un tamaño de grupo RAID de 20, la cantidad de discos que NetApp recomienda agregar es uno o más grupos de 20 discos. Así que debería añadir discos 20, 40, 60, etc.

Después de expandir los agregados, puede mejorar el rendimiento ejecutando tareas de reasignación en los volúmenes afectados o agregados para distribuir las franjas de datos existentes en los nuevos discos. Esta acción resulta útil especialmente si el agregado existente estaba casi lleno.

> Debe planificar la reasignación de las programaciones durante las horas de no producción, ya que es una tarea que consume una gran cantidad de CPU y discos.

Para obtener más información sobre el uso de la reasignación después de una expansión agregada, consulte "TR-3929 de NetApp: Guía para reasignar las mejores prácticas".

Copias Snapshot a nivel de agregado

Establezca la reserva de copias Snapshot de NetApp en el nivel del agregado a cero y desactive la programación Snapshot predeterminada del agregado. Elimine cualquier copia Snapshot anterior a nivel de agregado, si es posible.

"Siguiente: Configuración de la máquina virtual de almacenamiento."

Configuración de la máquina virtual de almacenamiento

En esta sección se trata la puesta en marcha en ONTAP 8.3 y versiones posteriores.

Una máquina virtual de almacenamiento (SVM) también se denomina Vserver en la API de ONTAP y en la CLI de ONTAP.

SVM para LUN de host de MEDITECH

Debería crear una SVM dedicada por clúster de almacenamiento de ONTAP para poseer y gestionar los agregados que contengan las LUN para los hosts de MEDITECH.

Configuración de codificación de idioma de SVM

NetApp recomienda establecer la codificación de idioma para todas las SVM. Si no se especifica ninguna configuración de codificación de idioma en el momento de la creación de la SVM, se utiliza la configuración de codificación de idioma predeterminada. La configuración de codificación de idioma predeterminada es C.UTF-8 para ONTAP. Una vez establecida la codificación de idioma, no se puede modificar el idioma de una SVM con Infinite Volume más adelante.

Los volúmenes asociados con la SVM heredan la configuración de codificación de idioma de la SVM, a menos que se especifique explícitamente otra opción cuando se crean los volúmenes. Para que ciertas operaciones funcionen, debe utilizar la configuración de codificación de idioma de forma coherente en todos los volúmenes del sitio. Por ejemplo, SnapMirror requiere que la SVM de origen y destino tenga la misma configuración de codificación de idioma.

"Siguiente: Configuración de volumen."

Configuración de volúmenes

Aprovisionamiento de volúmenes

Los volúmenes de MEDITECH que están dedicados a los hosts MEDITECH pueden tener el aprovisionamiento ligero o grueso.

Copias Snapshot a nivel de volumen predeterminadas

Las copias Snapshot se crean como parte del flujo de trabajo de backup. Cada copia Snapshot se puede utilizar para acceder a los datos almacenados en las LUN de MEDITECH en momentos diferentes. La solución de backup aprobada por MEDITECH crea volúmenes FlexClone aprovisionados mediante thin provisioning en función de estas copias Snapshot, para proporcionar copias puntuales de las LUN de MEDITECH. El entorno MEDITECH está integrado con una solución de software de backup aprobada. Por tanto, NetApp recomienda deshabilitar la programación de la copia Snapshot predeterminada en cada uno de los volúmenes FlexVol de NetApp que componen las LUN de la base de datos de producción de MEDITECH.

Importante: los volúmenes FlexClone comparten espacio en el volumen de datos principal, por lo que es vital que el volumen tenga suficiente espacio para las LUN de datos de MEDITECH y los volúmenes FlexClone que crean los servidores de backup. Los volúmenes FlexClone no ocupan más espacio de la forma en que lo hacen los volúmenes de datos. Sin embargo, si hay grandes eliminaciones en las LUN de MEDITECH en un breve tiempo, es posible que los volúmenes clonados aumenten.

Número de volúmenes por agregado

Para un sistema FAS de NetApp que usa el almacenamiento en caché Flash Pool o Flash Cache de NetApp, NetApp recomienda aprovisionar tres o más volúmenes por agregado dedicados a almacenar los archivos de datos, el diccionario y el programa MEDITECH.

En el caso de sistemas AFF, NetApp recomienda dedicar cuatro o más volúmenes por agregado para

almacenar el programa, el diccionario y los archivos de datos de MEDITECH.

Programa de reasignación de volúmenes

La distribución de datos del almacenamiento será menos óptima con el tiempo, sobre todo cuando las cargas de trabajo que utilizan una gran cantidad de escrituras como las plataformas MEDITECH, 6.x y C/S 5.x. Con el tiempo, esta situación puede aumentar la latencia de lectura secuencial, lo que puede dar como resultado un mayor tiempo para completar el backup. Una distribución o fragmentación de datos incorrectas también pueden afectar a la latencia de escritura. Puede usar la reubicación en el nivel de volumen para optimizar la distribución de datos en el disco para mejorar las latencias de escritura y el acceso de lectura secuencial. La mejora del diseño del almacenamiento ayuda a completar el backup en el plazo de 8 horas asignado.

Mejor práctica
Como mínimo, NetApp recomienda implementar un programa de reasignación de volumen semanal para ejecutar operaciones de reasignación durante el tiempo de inactividad de mantenimiento asignado o durante las horas de menor actividad en un sitio de producción. NetApp recomienda encarecidamente ejecutar la tarea de reasignación en un volumen cada vez por controladora.

Para obtener más información acerca de cómo determinar un programa de reasignación de volumen adecuado para el almacenamiento de su base de datos de producción, consulte la sección 3.12 en "TR-3929 de NetApp: Guía para reasignar las mejores prácticas". Esa sección también le guía sobre cómo crear un programa de reasignación semanal para un sitio ocupado.

"Siguiente: Configuración de LUN."

Configuración de LUN

El número de hosts de MEDITECH en su entorno determina el número de LUN que se crean en los sistemas FAS o AFF de NetApp. La propuesta de configuración de hardware especifica el tamaño de cada LUN.

Aprovisionamiento de LUN

Las LUN de MEDITECH que están dedicadas a los hosts MEDITECH pueden tener el aprovisionamiento ligero o grueso.

Tipo de sistema operativo de LUN

Para alinear correctamente las LUN que se crean, debe configurar correctamente el tipo de sistema operativo para las LUN. Las LUN mal alineadas sufren una sobrecarga de operaciones de escritura innecesaria y es costoso corregir una LUN mal alineada.

El servidor host de MEDITECH normalmente se ejecuta en el entorno virtualizado de Windows Server mediante el hipervisor VMware vSphere. El servidor host también puede ejecutarse en el entorno de Windows Server en un servidor sin sistema operativo. Para determinar el valor correcto del tipo de sistema operativo que se debe establecer, consulte la sección “creación de LUN” de "Comandos de Clustered Data ONTAP 8.3: Referencia de páginas del manual".

Tamaño de LUN

Para determinar el tamaño de LUN de cada host MEDITECH, consulte el documento propuesta de configuración de hardware (nueva implementación) o tarea de evaluación de hardware (implementación existente) de MEDITECH.

Presentación de LUN

MEDITECH requiere que el almacenamiento para los archivos de datos, diccionario y programas se presente a los hosts MEDITECH como LUN mediante el protocolo FC. En el entorno virtual de VMware, las LUN se presentan a los servidores VMware ESXi que alojan los hosts de MEDITECH. A continuación, cada LUN que se presenta al servidor VMware ESXi se asigna a cada equipo virtual host MEDITECH utilizando RDM en el modo de compatibilidad física.

Debe presentar las LUN a los hosts MEDITCH utilizando las convenciones de nomenclatura de LUN adecuadas. Por ejemplo, para facilitar la administración, debe presentar la LUN `MTFS01E` Al host de MEDITECH `mt-host-01`.

Consulte la propuesta de configuración de hardware de MEDITECH cuando consulte con el instalador de MEDITECH y del sistema de copia de seguridad para diseñar una convención de nomenclatura coherente para las LUN que utilizan los hosts MEDITECH.

Un ejemplo de nombre de LUN de MEDITECH es `MTFS05E`, en el que:

- `MTFS` Indica el servidor de archivos MEDITECH (para el host MEDITECH).
- `05` indica el número de host 5.
- `E` Indica la unidad E de Windows.

"Siguiente: Configuración del iGroup."

Configuración del iGroup

Cuando se utiliza FC como protocolo de red de datos, se deben crear dos iGroups en cada controladora de almacenamiento. El primer igroup contiene los WWPN de las tarjetas de interfaz de host FC en los servidores ESXi de VMware que alojan las máquinas virtuales del host de MEDITECH (igroup para MEDITECH).

Debe establecer el tipo de sistema operativo MEDITECH igroup según la configuración del entorno. Por ejemplo:

- Utilice el tipo de sistema operativo del igroup `Windows` Para aplicaciones que se instalan en hardware de servidor con configuración básica en un entorno de Windows Server.
- Utilice el tipo de sistema operativo del igroup `VMware` Para las aplicaciones que se virtualizan mediante el hipervisor VMware vSphere.

> El tipo de sistema operativo de un igroup puede ser diferente del tipo de sistema operativo de una LUN. Por ejemplo, para los hosts MEDITECH virtualizados, debe establecer el tipo de sistema operativo igroup en `VMware`. Para las LUN que utilizan los hosts MEDITECH virtualizados, debe establecer el tipo de sistema operativo en `Windows 2008 or later`. Utilice esta configuración porque el sistema operativo host MEDITECH es Windows Server 2008 R2 64-bit Enterprise Edition.

Para determinar el valor correcto para el tipo de sistema operativo, consulte las secciones “LUN iGroup Create” y “LUN Create” en la "Comandos de Clustered Data ONTAP 8.2: Referencia de páginas del manual".

"Siguiente: Asignaciones de LUN."

Asignaciones de LUN

Las asignaciones de LUN para los hosts de MEDITECH se establecen cuando se crean las LUN.

Módulos y componentes de MEDITECH

La aplicación MEDITECH cubre varios módulos y componentes. En la siguiente tabla se enumeran las funciones que están cubiertas por estos módulos. Para obtener más información sobre la configuración y la implementación de estos módulos, consulte la documentación de MEDITECH.

Función	Tipo
Conectividad	• Servidor web • Servidor de aplicaciones en directo (WI – Web Integration) • Probar el servidor de aplicaciones (WI) • Servidor de autenticación SAML (WI) • Servidor proxy SAML (WI) • Servidor de bases de datos
De almacenamiento	• Servidor de ficheros • Cliente de trabajo en segundo plano • Servidor de conexión • Servidor de transacciones
Análisis y archivado	• Servidor de imágenes
Almacén de datos	• Servidor SQL
Análisis clínicos y empresariales	• Servidor de inteligencia en directo (BCA) • Servidor de inteligencia de prueba (BCA) • Servidor de bases de datos (BCA)

Función	Tipo
Cuidado en el hogar	• Solución para ubicaciones remotas • Conectividad • De almacenamiento • Impresión • Dispositivos de campo • Escaneado • Requisitos del sitio alojado • Configuración del firewall
Soporte técnico	• Cliente de trabajo en segundo plano (CAL: Licencia de acceso de cliente)
Dispositivos de usuario	• Tabletas • Dispositivos fijos
Impresión	• Servidor de impresión en red activo (obligatorio; puede que ya exista) • Probar el servidor de impresión de red (obligatorio; puede que ya exista)
Requisito de terceros	• First Databank (FDB) MedKnowledge Framework v4.3

Reconocimientos

Las siguientes personas contribuyeron a la creación de esta guía.

- Brandon Agee, Ingeniero de Marketing Técnico, NetApp
- Atul Bhalodia, Ingeniero de Marketing Técnico, NetApp
- Ketan Mota, Directora Sénior de producto de NetApp
- John Duignan, Arquitecto de Soluciones — Sanidad, NetApp
- Jon Ebmeier, Cisco
- Mike Brennan, Cisco

Dónde encontrar información adicional

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

Zona de diseño de FlexPod

- "Zona de diseño de FlexPod"

- "Centro de datos de FlexPod con almacenamiento FC (switches MDS) mediante NetApp AFF, vSphere 6.5U1 y Cisco UCS Manager"

Informes técnicos de NetApp

- "TR-3929: Guía para reasignar las mejores prácticas"
- "TR-3987: Complemento para Snap Creator Framework para InterSystems Caché"
- "TR-4300i: Guía de prácticas recomendadas de sistemas de almacenamiento all-flash y FAS de NetApp para entornos MEDITECH"
- "TR-4017: Mejores prácticas para SAN FC"
- "TR-3446: Descripción general de SnapMirror Async y guía de prácticas recomendadas"

Documentación de ONTAP

- "Documentación de productos de NetApp"
- "Documentación de Virtual Storage Console (VSC) para vSphere"
- "Centro de documentación de ONTAP 9":
  - "Guía exprés de FC para ESXi"
- "Documentación de All ONTAP 9.3":
  - "Guía de configuración de software"
  - "Guía completa de discos y agregados"
  - "Guía de administración de SAN"
  - "Guía de configuración de SAN"
  - "Guía exprés de configuración de FC para Windows"
  - "Guía de configuración de AFF optimizado para FC SAN"
  - "Guía de configuración de alta disponibilidad"
  - "Guía de gestión de almacenamiento lógico"
  - "Guía completa de gestión del rendimiento"
  - "Guía completa de configuración de SMB/CIFS"
  - "Referencia de SMB/CIFS"
  - "Guía completa de protección de datos"
  - "Guía de recuperación y backup en cinta de protección de datos"
  - "Guía completa de cifrado de NetApp"
  - "Guía de gestión de redes"
  - "Comandos: Referencia de páginas del manual para ONTAP 9.3"

Guías de Cisco Nexus, MDS, Cisco UCS y Cisco UCS Manager

- "Descripción general de los servidores Cisco UCS"
- "Información general sobre los servidores blade Cisco UCS"
- "Especificaciones técnicas de Cisco UCS B200 M5"

- "Información general de Cisco UCS Manager"
- "Paquete de infraestructura Cisco UCS Manager 3.2 (3a)" (Requiere autorización Cisco.com)
- "Switches de la plataforma Cisco Nexus 9300"
- "Switch FC Cisco MDS 9132T"

FlexPod para exploración médica

TR-4865: FlexPod para imágenes médicas

Jaya Kishore Esanakula y Atul Bhalodia, NetApp

Las imágenes médicas representan el 70% de todos los datos generados por las organizaciones sanitarias. A medida que las modalidades digitales sigan avanzando y surjan nuevas modalidades, la cantidad de datos seguirá aumentando. Por ejemplo, la transición de la patología analógica a la digital aumentará drásticamente el tamaño de las imágenes a un ritmo que desafiará cualquier estrategia de gestión de datos que esté actualmente en vigor.

El COVID-19 ha reformulado claramente la transformación digital; según un informe reciente "informes", El COVID-19 ha acelerado el comercio digital en 5 años. La innovación tecnológica impulsada por los solucionadores de problemas está cambiando fundamentalmente la forma en que hacemos nuestra vida cotidiana. Este cambio impulsado por la tecnología modificará muchos aspectos críticos de nuestra vida, incluida la atención sanitaria.

La asistencia sanitaria está a punto de experimentar un cambio importante en los próximos años. El COVID está acelerando la innovación en sanidad para impulsar el sector en al menos varios años. En el centro de este cambio se encuentra la necesidad de hacer que la atención sanitaria sea más flexible para afrontar las pandemias, ya que sea más asequible, disponible y accesible, sin comprometer la fiabilidad.

En la base de este cambio en la atención médica se encuentra una plataforma bien diseñada. Una de las mediciones clave para medir la plataforma es la facilidad con la que se pueden implementar cambios en la plataforma. La velocidad es la nueva escala y la protección de datos no se puede comprometer. Algunos de los datos más importantes del mundo están siendo creados y consumidos por los sistemas clínicos que dan soporte a los clínicos. NetApp ha puesto los datos cruciales a disposición de la atención al paciente cuando los médicos los necesitan, en las instalaciones, en el cloud o en un entorno híbrido. Los entornos multicloud híbridos son el estado actual de las últimas tecnologías en la arquitectura TECNOLÓGICA.

La asistencia sanitaria como sabemos gira en torno a proveedores (médicos, enfermeras, radiólogos, técnicos de dispositivos médicos, etc.) y pacientes. A medida que acercamos más a los pacientes y los proveedores, convirtiendo la ubicación geográfica en un simple punto de datos, resulta aún más importante que la plataforma subyacente esté disponible cuando los proveedores y los pacientes lo necesiten. La plataforma debe ser eficiente y rentable a largo plazo. En sus esfuerzos por reducir aún más los costos de la atención a los pacientes, "Organizaciones de atención responsable" (Acos) se vería empoderada por una plataforma eficiente.

Cuando se trata de sistemas de información sanitaria utilizados por las organizaciones sanitarias, la cuestión de construir frente a comprar tiende a tener una única respuesta: Compra. Esto podría ser por muchas razones subjetivas. Las decisiones de compra que se toman a lo largo de muchos años pueden crear sistemas de información heterogéneos. Cada sistema tiene un conjunto específico de requisitos para la plataforma en la que se ponen en marcha. El problema más importante es el amplio y diverso conjunto de protocolos de almacenamiento y niveles de rendimiento que requieren los sistemas de información, lo cual

convierte la estandarización de la plataforma y la eficiencia operativa óptima en un reto importante. Las organizaciones sanitarias no pueden centrarse en cuestiones críticas para la misión porque su atención se va reteniendo debido a necesidades operativas triviales, como el gran conjunto de plataformas que requieren un conjunto diversificado de habilidades y, por tanto, la retención de las PYME.

Los retos se pueden clasificar en las siguientes categorías:

- Necesidades de almacenamiento heterogéneas
- Silos departamentales
- Complejidad operativa DE TECNOLOGÍA
- Conectividad del cloud
- Ciberseguridad
- Inteligencia artificial y aprendizaje profundo

Con FlexPod, usted obtiene una plataforma única compatible con FC, FCoE, iSCSI, NFS/pNFS, SMB/CIFS, etc. desde una única plataforma. Las personas, los procesos y la tecnología forman parte del ADN sobre el que se diseñó y se basa FlexPod. La calidad de servicio adaptable de FlexPod ayuda a desglosar los silos departamentales al admitir varios sistemas clínicos críticos para el negocio en la misma plataforma FlexPod subyacente. FlexPod cuenta con la certificación FedRAMP y con la certificación FIPS 140-2-2. Las organizaciones sanitarias, además, deben enfrentarse a oportunidades como la inteligencia artificial y el aprendizaje profundo. FlexPod y NetApp solucionan estos retos y hacen que los datos estén disponibles donde se necesiten, en un entorno local o en un entorno multicloud híbrido en una plataforma estandarizada. Para obtener más información y casos de éxito de clientes de una serie, consulte "Asistencia sanitaria FlexPod".

La información médica típica de exploración y los sistemas PACS tienen el siguiente conjunto de funciones:

- Recepción y registro
- Programación
- Creación de imágenes
- Transcripción
- Gestión
- Intercambio de datos
- Archivo de imágenes
- Visualización de imágenes para captura y lectura de imágenes para técnicos y visualización de imágenes para médicos

En cuanto a la adquisición de imágenes, el sector sanitario está tratando de solucionar los siguientes retos clínicos:

- Adopción más amplia de "procesamiento de lenguaje natural" Asistentes (NLP) por técnicos y médicos para la lectura de imágenes. El departamento de radiología puede beneficiarse del reconocimiento de voz para transcribir informes. NLP puede utilizarse para identificar y anonimizar el registro de un paciente, específicamente las etiquetas DICOM incorporadas en la imagen DICOM. Las capacidades de NLP requieren plataformas de alto rendimiento con tiempos de respuesta de baja latencia para el procesamiento de imágenes. La calidad de servicio de FlexPod no solo ofrece y proporciona rendimiento, sino que también proporciona proyecciones de capacidad maduras para futuras necesidades de crecimiento.
- Adopción más amplia de vías clínicas y protocolos estandarizados por parte de las ACOC y las

organizaciones de salud de la comunidad. Históricamente, las vías clínicas se han utilizado como un conjunto estático de directrices en lugar de un flujo de trabajo integrado que guía las decisiones clínicas. Gracias a los avances en NLP y el procesamiento de imágenes, las etiquetas DICOM de las imágenes se pueden integrar en vías clínicas como hechos para impulsar las decisiones clínicas. Por lo tanto, estos procesos requieren un alto rendimiento, una baja latencia y un alto rendimiento de la plataforma de infraestructura subyacente y de los sistemas de almacenamiento.

- Los modelos DE ML que aprovechan las redes neuronales convolucionales permiten automatizar las capacidades de procesamiento de imágenes en tiempo real y, por lo tanto, requieren una infraestructura que sea compatible con GPU. FlexPod ofrece componentes de computación de CPU y GPU incorporados en el mismo sistema, y las CPU y las GPU se pueden escalar de manera independiente entre sí.
- Si las etiquetas DICOM se utilizan como hechos en los avisos clínicos de mejores prácticas, el sistema debe realizar más lecturas de artefactos DICOM con baja latencia y alto rendimiento.
- Al evaluar las imágenes, la colaboración en tiempo real entre radiólogos en distintas organizaciones requiere el procesamiento de gráficos de alto rendimiento en los dispositivos informáticos del usuario final. NetApp proporciona soluciones VDI líderes del sector específicamente diseñadas y probadas para casos prácticos de gráficos de gama alta. Se puede encontrar más información "aquí".
- La gestión de imágenes y medios a través de las organizaciones sanitarias de ACO puede utilizar una sola plataforma, independientemente del sistema de registro de la imagen, mediante protocolos como Digital Imaging y Communications in Medicine ("DICOM") Y acceso Web a objetos persistentes DICOM ("WADO")
- Intercambio de información sanitaria ("HIE") incluye imágenes incrustadas en mensajes.
- Las modalidades móviles, como los dispositivos de exploración inalámbricos y portátiles (por ejemplo, los escáneres de ultrasonidos de bolsillo conectados a un teléfono), requieren una sólida infraestructura de red con seguridad a nivel DoD, fiabilidad y latencia en el perímetro, el núcleo y en la nube. "Una estructura de datos habilitada por NetApp" ofrezca a las organizaciones esta capacidad a escala.
- Las nuevas modalidades tienen necesidades de almacenamiento exponencial; por ejemplo, la TC y la RM requieren unos pocos cientos de MB para cada modalidad, pero las imágenes de patología digital (incluida la imagen de portaobjetos enteros) pueden tener unos pocos GBS de tamaño. FlexPod está diseñado con "rendimiento, fiabilidad y escalabilidad como rasgos fundamentales".

Una plataforma de sistemas de imágenes médicas bien diseñada es el centro de la innovación. La arquitectura FlexPod ofrece capacidades flexibles de computación y almacenamiento con una eficiencia de almacenamiento líder en el sector.

Beneficios generales de la solución

Al ejecutar un entorno de aplicación de imágenes en una base arquitectónica de FlexPod, el departamento de atención médica puede esperar una mejora de la productividad del personal y una reducción de los gastos operativos y de capital. FlexPod proporciona una solución convergente, prevalidada y rigurosamente probada, diseñada para ofrecer un rendimiento previsible del sistema de baja latencia y alta disponibilidad. Este enfoque da lugar a altos niveles de comodidad y, en última instancia, a tiempos de respuesta óptimos para los usuarios del sistema de imágenes médicas.

Los diferentes componentes del sistema de imágenes pueden requerir el almacenamiento de datos en sistemas de archivos SMB/CIFS, NFS, Ext4 o NTFS. Este requisito implica que la infraestructura debe proporcionar acceso a datos a través de los protocolos NFS, SMB/CIFS y SAN. Un único sistema de almacenamiento de NetApp admite los protocolos NFS, SMB/CIFS y SAN, por lo que elimina la necesidad de recurrir a sistemas de almacenamiento específicos para determinados protocolos.

La infraestructura de FlexPod es una plataforma modular, convergente, virtualizada, escalable (de escalado horizontal y vertical) y rentable. Con la plataforma FlexPod, puede escalar horizontalmente de forma

independiente la computación, la red y el almacenamiento para acelerar la puesta en marcha de las aplicaciones. Además, la arquitectura modular posibilita operaciones no disruptivas incluso durante el escalado horizontal del sistema y las actividades de actualización.

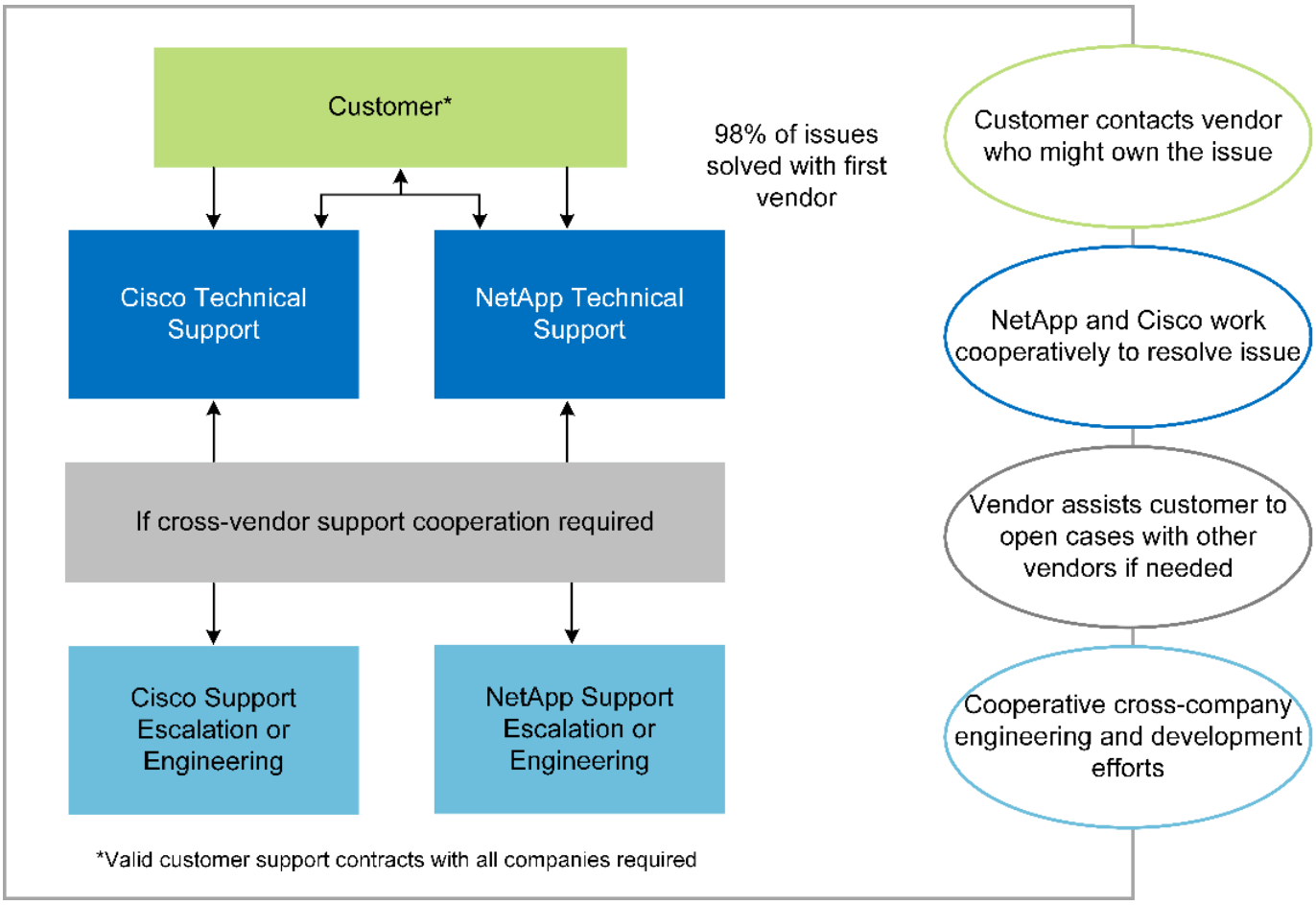
FlexPod ofrece varias ventajas específicas del sector de las imágenes médicas:

- **Rendimiento del sistema de baja latencia.** el tiempo del radiólogo es un recurso de gran valor, y el uso eficiente del tiempo del radiólogo es primordial. Esperar a que se carguen imágenes o vídeos puede contribuir al agotamiento clínico y afectar la eficiencia del médico y la seguridad del paciente.
- **Arquitectura modular.** los componentes de FlexPod están conectados a través de un servidor en cluster, una estructura de administración de almacenamiento y un conjunto de herramientas de administración cohesionado. A medida que las instalaciones de imágenes crezcan año tras año y aumente el número de estudios, será necesario que la infraestructura subyacente se escale de manera acorde. FlexPod puede escalar la computación, el almacenamiento y la red de forma independiente.
- **Implementación más rápida de la infraestructura.** tanto si se encuentra en un centro de datos existente como en una ubicación remota, el diseño integrado y probado del centro de datos FlexPod con imágenes médicas le permite tener la nueva infraestructura en funcionamiento en menos tiempo y con menos esfuerzo.
- **Implementación acelerada de aplicaciones.** Una arquitectura validada previamente reduce el tiempo de integración de la implementación y el riesgo para cualquier carga de trabajo, y la tecnología de NetApp automatiza la implementación de la infraestructura. Tanto si utiliza la solución para la implementación inicial de imágenes médicas, una actualización de hardware o una expansión, puede cambiar más recursos al valor empresarial del proyecto.
- **Operaciones simplificadas y costos más bajos.** puede eliminar el gasto y la complejidad de las plataformas propietarias heredadas reemplazándolas con un recurso compartido más eficiente y escalable que pueda satisfacer las necesidades dinámicas de su carga de trabajo. Esta solución ofrece una mayor utilización de los recursos de la infraestructura para obtener un mayor retorno de la inversión (ROI).
- **Arquitectura de escalabilidad horizontal.** puede escalar SAN y NAS de terabytes a decenas de petabytes sin necesidad de reconfigurar las aplicaciones en ejecución.
- **Operaciones no disruptivas.** puede realizar el mantenimiento del almacenamiento, las operaciones del ciclo de vida del hardware y las actualizaciones de software sin interrumpir su negocio.
- **Multitenancy seguro.** esta ventaja soporta las crecientes necesidades de servidor virtualizado y de infraestructura compartida de almacenamiento, permitiendo multi-tenancy seguro de información específica de instalación, particularmente si usted está alojando múltiples instancias de bases de datos y software.
- **Optimización de recursos agrupados.** esta ventaja puede ayudarle a reducir el número de servidores físicos y controladores de almacenamiento, las demandas de carga de trabajo de equilibrio y aumentar la utilización al tiempo que mejora el rendimiento.
- **Calidad de servicio (QoS).** FlexPod ofrece QoS en toda la pila. Estas políticas de almacenamiento de calidad de servicio líderes del sector permiten niveles de servicio diferenciados en un entorno compartido. Estas normativas ayudan a optimizar el rendimiento de las cargas de trabajo y ayudan a aislar y controlar aplicaciones que no se controlan.
- **Soporte para SLA de nivel de almacenamiento utilizando QoS.** no es necesario implementar diferentes sistemas de almacenamiento para los diferentes niveles de almacenamiento que un entorno de imágenes médicas normalmente requiere. Un único clúster de almacenamiento con múltiples volúmenes FlexVol de NetApp con políticas de calidad de servicio específicas para diferentes niveles puede servir a tal efecto. Con este enfoque, la infraestructura de almacenamiento puede compartirse acomodando de forma dinámica las necesidades cambiantes de un nivel de almacenamiento determinado. AFF de NetApp puede admitir distintos acuerdos de nivel de servicio para niveles de almacenamiento, lo que permite la calidad de servicio en el nivel del volumen FlexVol y, por lo tanto, eliminar la necesidad de disponer de diferentes

sistemas de almacenamiento para distintos niveles de almacenamiento para la aplicación.

- * Eficiencia del almacenamiento.* las imágenes médicas son típicamente pre-comprimidas por la aplicación de imagen a compresión sin pérdidas de jpeg2k que es alrededor de 2.5:1. Sin embargo, se trata de una aplicación de imagen y un proveedor específico. En entornos de aplicaciones de imagen de mayor tamaño (más de 1 PB), es posible ahorrar entre un 5% y un 10% en almacenamiento y reducir los costes de almacenamiento con las funciones de eficiencia del almacenamiento de NetApp. Trabaje con los proveedores de aplicaciones de imágenes y con su experto en la materia de NetApp para descubrir las posibles eficiencias del almacenamiento para su sistema de exploración médica.
- **Agilidad.** con las herramientas de gestión, coordinación y automatización de flujos de trabajo líderes en el sector que ofrecen los sistemas FlexPod, su equipo DE TI puede responder mucho más a las necesidades de la empresa. Estas solicitudes de negocio pueden abarcar desde el backup por imágenes médicas y el aprovisionamiento de entornos de prueba y entrenamiento adicionales hasta replicaciones de bases de datos de análisis para iniciativas de gestión de la salud de la población.
- **Mayor productividad.** puede implementar y ampliar rápidamente esta solución para obtener experiencias óptimas de usuario final clínico.
- **Data Fabric.** su Data Fabric con la tecnología de NetApp aúna los datos de distintos sitios, sin que los barreras físicas y de todas las aplicaciones. Su Data Fabric con la tecnología de NetApp se ha creado pensando en empresas basadas en datos en un mundo donde todo gira alrededor de ellos. Los datos se crean y se usan en varias ubicaciones y, a menudo, hay que aprovecharlos y compartirlos con otras ubicaciones, aplicaciones e infraestructuras. Por lo tanto, usted quiere una forma coherente e integrada de gestionarlo. Esta solución ofrece una manera de gestionar los datos que pone a su equipo DE TECNOLOGÍA en control y que simplifica la complejidad TECNOLÓGICA en aumento.
- **FabricPool.** NetApp ONTAP FabricPool ayuda a reducir los costes de almacenamiento sin comprometer el rendimiento, la eficiencia, la seguridad ni la protección. FabricPool es transparente para las aplicaciones empresariales y aprovecha las eficiencias del cloud al reducir el TCO del almacenamiento sin necesidad de rediseñar la arquitectura de la infraestructura de aplicaciones. FlexPod se puede beneficiar de las funcionalidades de almacenamiento por niveles de FabricPool para hacer un uso más eficiente del almacenamiento flash de ONTAP. Para obtener más información, consulte "FlexPod con FabricPool".
- **Seguridad FlexPod.** La seguridad está en la base misma de FlexPod. En los últimos años, el ransomware se ha convertido en una amenaza importante y creciente. El ransomware es un malware que se basa en la virología criptográfica, el uso de criptografía para crear software malicioso. Este malware puede utilizar cifrado de clave simétrica y asimétrica para bloquear los datos de una víctima y exigir un rescate para proporcionar la clave para descifrar los datos. Para saber cómo FlexPod ayuda a mitigar amenazas como el ransomware, consulte "La solución a Ransomware". Los componentes de la infraestructura de FlexPod también "(FIPS) 140-2" cumplen con el estándar de procesamiento de información federal.
- **Soporte conjunto de FlexPod.** NetApp y Cisco han establecido el soporte conjunto de FlexPod, un modelo de soporte sólido, escalable y flexible para cumplir los requisitos de soporte exclusivos de la infraestructura convergente de FlexPod. Este modelo utiliza la experiencia combinada de NetApp y Cisco, así como sus recursos y conocimientos en el campo del soporte técnico, para proporcionar un proceso optimizado para identificar y solucionar su problema de soporte de FlexPod, con independencia de dónde se encuentre el problema. El modelo de soporte conjunto de FlexPod le ayuda a confirmar que su sistema de FlexPod funciona de forma eficiente y se beneficia de la tecnología más actualizada, al tiempo que proporciona un equipo experimentado para ayudar a resolver problemas de integración.

  El soporte conjunto de FlexPod resulta especialmente valioso si su organización sanitaria ejecuta aplicaciones vitales para el negocio. En la siguiente ilustración, se muestra una descripción general del modelo de soporte conjunto de FlexPod.



Ámbito

Este documento ofrece una descripción general técnica de un sistema Cisco Unified Computing System (Cisco UCS) y la infraestructura FlexPod basada en ONTAP de NetApp para alojar esta solución de imágenes médicas.

Destinatarios

Este documento está dirigido a líderes técnicos del sector sanitario y a ingenieros de soluciones de partners de Cisco y NetApp y personal de servicios profesionales. NetApp asume que el lector tiene un buen conocimiento de los conceptos de configuración de almacenamiento y computación, así como de la familiaridad técnica con el sistema de imágenes médicas, Cisco UCS y los sistemas de almacenamiento de NetApp.

Aplicación de imágenes médicas

Una aplicación de imágenes médicas típica ofrece un conjunto de aplicaciones que juntas forman una solución de imágenes de clase empresarial para pequeñas, medianas y grandes organizaciones sanitarias.

La parte central del conjunto de productos son las siguientes capacidades clínicas:

- Repositorio de imágenes empresariales
- Admite fuentes de imágenes tradicionales como radiología y cardiología. También apoya otras áreas de cuidado como oftalmología, dermatología, colonoscopia, y otros objetos médicos de imágenes como fotos y videos.

- "Sistema de comunicación y archivado de imágenes" (PACS), que es un medio computadorizado de sustituir el papel de la película radiológica convencional
- Archivado comercial neutral (VNA) de los proveedores de imágenes empresariales:
  - Consolidación escalable de documentos DICOM y no DICOM
  - Sistema centralizado de exploración médica
  - Compatibilidad con sincronización de documentos e integridad de datos entre varios (PACSs) en la empresa
  - Documentar la gestión del ciclo de vida por parte de un sistema experto basado en reglas que aprovecha los metadatos de documentos, como:
  - Tipo de modalidad
  - Edad del estudio
  - Antigüedad del paciente (actual y en el momento de la captura de la imagen)
  - Único punto de integración dentro y fuera de la empresa (HIE):
  - Vinculación de documentos que tienen en cuenta el contexto
  - Health Level Seven International (HL7), DICOM y WADO
  - Capacidad de archivado independiente del almacenamiento
- Integración con otros sistemas de información sanitaria que utilizan HL7 y enlaces contextuales:
  - Permite que los EHR implementen enlaces directos a imágenes de pacientes desde gráficos de pacientes, flujos de trabajo de imágenes, etc.
  - Ayuda a integrar el historial de imágenes de cuidados longitudinales de un paciente en EHR.
- Flujos de trabajo del técnico de radiología
- Visores de espacio cero para la empresa para la visualización de imágenes desde cualquier lugar y dispositivo capaz
- Herramientas analíticas que aprovechan datos retrospectivos y en tiempo real:
  - Informes de cumplimiento
  - Informes operativos
  - Informes de control de calidad y garantía de calidad

Tamaño de la organización sanitaria y ajuste de tamaño de la plataforma

Las organizaciones sanitarias pueden clasificarse ampliamente mediante métodos basados en estándares que ayudan a programas como la OCA. Una de estas clasificaciones usa el concepto de red integrada clínica (CIN). Un grupo de hospitales se puede llamar CIN si colaboran y se adhieren a protocolos clínicos y vías probadas estándares para mejorar el valor de la atención y reducir los costos de los pacientes. Los hospitales dentro de un CIN tienen controles y prácticas vigentes a los médicos a bordo que siguen los valores centrales del CIN. Tradicionalmente, las redes integradas de entrega (IDN) se han limitado a hospitales y grupos médicos. Un CIN cruza los límites tradicionales del IDN, y un CIN puede ser todavía parte de un ACO. Siguiendo los principios de una CIN, las organizaciones sanitarias pueden clasificarse en pequeñas, medianas y grandes.

Pequeñas organizaciones sanitarias

Una organización sanitaria es pequeña si incluye solo un hospital con clínicas ambulatorios y un departamento de hospitalización, pero no forma parte de una CIN. Los médicos trabajan como cuidadores y coordinan la atención al paciente durante un proceso de atención. Estas pequeñas organizaciones suelen incluir

instalaciones operadas por médicos. Pueden ofrecer o no atención de emergencia y trauma como atención integrada para el paciente. Por lo general, una organización de atención médica de pequeño tamaño realiza aproximadamente 250,000 estudios de imágenes clínicas al año. Los centros de imágenes se consideran pequeñas organizaciones sanitarias y proporcionan servicios de imágenes. Algunos también ofrecen servicios de dictado radiológico a otras organizaciones.

Organizaciones sanitarias medianas

Una organización sanitaria que se considera de tamaño medio si incluye múltiples sistemas hospitalarios con organizaciones centradas, como los siguientes:

- Clínicas de cuidado de adultos y hospitales de pacientes adultos hospitalizados
- Departamentos de trabajo y entrega
- Clínicas de cuidado de niños y hospitales para niños hospitalizados
- Un centro de tratamiento del cáncer
- Departamentos de emergencia para adultos
- Servicios de urgencias infantiles
- Una oficina de medicina familiar y atención primaria
- Un centro de atención de trauma para adultos
- Un centro de atención de trauma infantil

En una organización sanitaria de tamaño medio, los médicos siguen los principios de una NIC y actúan como una sola unidad. Los hospitales tienen funciones separadas de facturación en hospitales, médicos y farmacias. Los hospitales pueden estar asociados con institutos de investigación académica y realizar estudios y investigaciones clínicas intervencionistas. Una organización sanitaria mediana realiza al año hasta 500,000 estudios de imágenes clínicas.

Grandes organizaciones sanitarias

Se considera que una organización sanitaria es grande si incluye las características de una organización sanitaria de tamaño medio y ofrece las capacidades clínicas de tamaño medio a la comunidad en múltiples ubicaciones geográficas.

Una organización sanitaria de gran tamaño suele realizar las siguientes funciones:

- Cuenta con una oficina central para administrar las funciones generales
- Participa en empresas conjuntas con otros hospitales
- Negocia las tarifas con organizaciones de pagadores anualmente
- Negocia las tarifas de pagadores por estado y región
- Participa en programas de uso significativo (MU)
- Realiza investigación clínica avanzada en cohortes de salud de la población mediante el uso de herramientas de gestión de la salud de la población basadas en estándares (PHM, por sus siglas en inglés)
- Realiza hasta un millón de estudios de imágenes clínicas al año

Algunas grandes organizaciones sanitarias que participan en una CIN también tienen capacidades de lectura de imágenes basadas en IA. Estas organizaciones suelen realizar de uno a dos millones de estudios de imágenes clínicas al año.

Antes de analizar cómo estas organizaciones de diferente tamaño se traducen en un sistema FlexPod de tamaño óptimo, debe comprender los diversos componentes de FlexPod y las diferentes funcionalidades de un sistema FlexPod.

FlexPod

Sistema Cisco Unified Computing

Cisco UCS está formado por un único dominio de gestión interconectado con una infraestructura de I/o unificada. Cisco UCS para entornos de exploración médica se ha alineado con las recomendaciones y prácticas recomendadas de la infraestructura de los sistemas de exploración médica de NetApp para que la infraestructura pueda proporcionar información crítica de los pacientes con la máxima disponibilidad.

La base informática de las exploraciones médicas empresariales es la tecnología Cisco UCS, con sus soluciones integradas de gestión de sistemas, procesadores Intel Xeon y virtualización de servidores. Estas tecnologías integradas resuelven los retos de los centros de datos y le permiten cumplir sus objetivos de diseño de centros de datos con un sistema de imágenes médicas típico. Cisco UCS unifica la gestión de LAN, SAN y sistemas en un enlace simplificado para servidores en rack, servidores blade y máquinas virtuales (VM). Cisco UCS consiste en un par redundante de interconexiones de estructura de Cisco UCS que proporcionan un único punto de gestión y un único punto de control para todo el tráfico de I/O.

Cisco UCS utiliza perfiles de servicio para que los servidores virtuales de la infraestructura Cisco UCS se configuren de manera correcta y coherente. Los perfiles de servicio incluyen información crítica del servidor sobre la identidad del servidor, como direccionamiento LAN y SAN, configuraciones de E/S, versiones de firmware, orden de arranque, red virtual LAN (VLAN), puertos físicos y políticas QoS. Los perfiles de servicio pueden crearse y asociarse de forma dinámica con cualquier servidor físico del sistema en cuestión de minutos, en lugar de horas o días. La asociación de perfiles de servicio con servidores físicos se realiza como una única operación sencilla que permite la migración de identidades entre servidores del entorno sin necesidad de cambios de configuración física. También facilita un aprovisionamiento sencillo y rápido de sustituciones de servidores con fallos.

El uso de perfiles de servicio ayuda a confirmar que los servidores están configurados de forma coherente en toda la empresa. Al utilizar varios dominios de gestión de Cisco UCS, Cisco UCS Central puede utilizar perfiles de servicio globales para sincronizar la información de configuración y políticas entre dominios. Si se debe realizar el mantenimiento en un dominio, la infraestructura virtual se puede migrar a otro dominio. Con este método, incluso cuando un único dominio está sin conexión, las aplicaciones continúan ejecutándose con alta disponibilidad.

Cisco UCS es una solución de última generación para la computación de servidores blade y en rack. El sistema integra una estructura unificada de redes 40 GbE sin pérdidas y de baja latencia con servidores de arquitectura x86 de nivel empresarial. El sistema es una plataforma integrada, escalable y de múltiples chasis en la que todos los recursos participan en un dominio de gestión unificado. Cisco UCS acelera la entrega de nuevos servicios de forma sencilla, fiable y segura mediante el aprovisionamiento y la compatibilidad de migración integrales para sistemas virtualizados y no virtualizados. Cisco UCS proporciona las siguientes funciones:

- Gestión completa
- Simplificación radical
- Altas prestaciones

Cisco UCS consta de los siguientes componentes:

- **Computación.** el sistema se basa en una clase completamente nueva de sistemas informáticos que incorpora servidores blade y montados en rack basados en la familia de productos de procesadores

escalables Intel Xeon.

- **Red.** el sistema está integrado en una estructura de red unificada de 40 Gbps sin pérdidas y de baja latencia. Esta base de redes consolida LAN, San y redes informáticas de alto rendimiento, que son redes independientes en la actualidad. La estructura unificada reduce los costes al disminuir el número de adaptadores de red, switches y cables, además de reducir los requisitos de energía y refrigeración.
- **Virtualización.** el sistema libera todo el potencial de la virtualización al mejorar la escalabilidad, el rendimiento y el control operativo de los entornos virtuales. Las funciones de Cisco de seguridad, aplicación de políticas y diagnóstico se amplían en entornos virtualizados para responder mejor a los cambios empresariales y los requisitos TECNOLÓGICOS.
- **Acceso al almacenamiento.** el sistema proporciona acceso consolidado al almacenamiento SAN y NAS a través de la estructura unificada. También es un sistema ideal para el almacenamiento definido por software. Al combinar las ventajas de un único marco para gestionar tanto los servidores de computación como los de almacenamiento en un único panel, es posible implementar la calidad de servicio si es necesario para inyectar regulación de I/o en el sistema. Además, los administradores de servidores pueden asignar previamente políticas de acceso al almacenamiento a los recursos de almacenamiento, lo que simplifica la conectividad de almacenamiento y la gestión y ayuda a aumentar la productividad. Además del almacenamiento externo, tanto los servidores blade como en rack cuentan con almacenamiento interno al que se puede acceder mediante controladoras RAID de hardware integradas. Al configurar el perfil de almacenamiento y la política de configuración de discos en Cisco UCS Manager, las necesidades de almacenamiento del sistema operativo host y los datos de aplicación se satisfacen mediante grupos RAID definidos por el usuario. El resultado es una alta disponibilidad y un mejor rendimiento.
- **Administración.** el sistema integra de forma exclusiva todos los componentes del sistema para que Cisco UCS Manager pueda administrar toda la solución como una única entidad. Para gestionar todas las operaciones y la configuración del sistema, Cisco UCS Manager cuenta con una interfaz gráfica de usuario intuitiva, una interfaz de línea de comandos y un potente módulo de biblioteca de scripts para Microsoft Windows PowerShell, creados en una API robusta.

Cisco Unified Computing System fusiona las redes y los servidores de la capa de acceso. Este sistema de servidores de última generación de alto rendimiento proporciona a su centro de datos un alto grado de escalabilidad y agilidad de carga de trabajo.

Administrador de Cisco UCS

Cisco UCS Manager proporciona una gestión unificada e integrada para todos los componentes de software y hardware en Cisco UCS. Mediante el uso de tecnología de conexión única, UCS Manager gestiona, controla y administra varios chasis para miles de máquinas virtuales. A través de una interfaz gráfica de usuario intuitiva, una interfaz de línea de comandos o una API XML, los administradores utilizan el software para gestionar todo el Cisco UCS como una única entidad lógica. Cisco UCS Manager reside en un par de interconexiones de estructura Cisco UCS 6300 Series que utilizan la configuración en clúster activo-espera para una alta disponibilidad.

Cisco UCS Manager ofrece una interfaz de gestión integrada y unificada que integra sus servidores, redes y almacenamiento. Cisco UCS Manager realiza detección automática para detectar el inventario, gestionar y aprovisionar componentes del sistema que se añaden o cambian. Ofrece un completo conjunto de API XML para la integración de terceros y expone 9,000 puntos de integración. También facilita el desarrollo personalizado para la automatización, la orquestación y la consecución de nuevos niveles de visibilidad y control del sistema.

Los perfiles de servicios benefician tanto a los entornos virtualizados como a los no virtualizados. Aumentan la movilidad de los servidores no virtualizados, como cuando mueve cargas de trabajo del servidor al servidor o cuando desconecta un servidor para ofrecer servicio o actualización. También puede usar perfiles junto con clústeres de virtualización para lograr que nuevos recursos estén en línea con facilidad y complementar la

movilidad de máquinas virtuales existente.

Para obtener más información sobre Cisco UCS Manager, consulte "Página de producto Cisco UCS Manager".

Diferenciadores de Cisco UCS

Cisco Unified Computing System está revolucionando la forma en que los servidores se gestionan en el centro de datos. Consulte los siguientes diferenciadores únicos de Cisco UCS y Cisco UCS Manager:

- **Administración integrada.** en Cisco UCS, los servidores son administrados por el firmware integrado en las interconexiones de estructura, lo que elimina la necesidad de cualquier dispositivo físico o virtual externo para gestionarlos.
- **Estructura unificada.** en Cisco UCS, desde chasis de servidor blade o servidores en rack hasta interconexiones de estructura, se utiliza un único cable Ethernet para tráfico LAN, SAN y de gestión. Esta I/o convergente reduce el número de cables, SFP y adaptadores que necesita, a su vez, reduce los gastos operativos y de capital relacionados con la solución general.
- **Descubrimiento automático.** simplemente insertando el servidor blade en el chasis o conectando servidores de bastidor a las interconexiones de estructura, el descubrimiento e inventario de recursos informáticos se produce automáticamente sin ninguna intervención de gestión. La combinación de la estructura unificada y la detección automática permite la arquitectura de conexión única de Cisco UCS, donde su capacidad informática se puede ampliar con facilidad a la vez que se mantiene la conectividad externa existente con redes LAN, SAN y de gestión.
- **Clasificación de recursos basada en políticas.** cuando Cisco UCS Manager descubre un recurso informático, se puede clasificar automáticamente a un pool de recursos dado en función de las políticas definidas. Esta funcionalidad es útil en el cloud computing multitenant.
- **Gestión combinada de servidores blade y de bastidor.** Cisco UCS Manager puede administrar servidores blade B-Series y servidores de bastidor C-Series bajo el mismo dominio Cisco UCS. Esta función, junto con la informática sin estado, convierte los recursos informáticos en algo realmente independiente del factor de forma del hardware.
- **Arquitectura de gestión basada en modelos.** la arquitectura y la base de datos de administración de Cisco UCS Manager están basadas en modelos y en datos. La API XML abierta que se proporciona para operar en el modelo de gestión permite una integración sencilla y escalable de Cisco UCS Manager con otros sistemas de gestión.
- * Políticas, pools y plantillas.* el enfoque de gestión en Cisco UCS Manager se basa en la definición de políticas, pools y plantillas en lugar de una configuración en el conjunto. Permite un método sencillo, de acoplamiento flexible, basado en los datos a la hora de gestionar los recursos informáticos, de red y de almacenamiento.
- **Integridad referencial suelta.** en Cisco UCS Manager, un perfil de servicio, un perfil de puerto o políticas pueden hacer referencia a otras directivas o a otros recursos lógicos con integridad referencial suelta. Una directiva a la que se hace referencia no puede existir en el momento de crear la directiva de referencia, pero una directiva a la que se hace referencia puede eliminarse aunque otras directivas se refieran a ella. Esta función permite que distintos expertos en la materia trabajen de forma independiente entre sí. Obtendrá una gran flexibilidad al permitir que distintos expertos de diferentes dominios, como red, almacenamiento, seguridad, servidor y virtualización, trabajen conjuntamente para llevar a cabo una tarea compleja.
- **Resolución de políticas.** en Cisco UCS Manager, puede crear una estructura de árbol de la jerarquía de unidades organizativas que imita a los inquilinos de la vida real y las relaciones organizativas. Puede definir varias directivas, agrupaciones y plantillas en diferentes niveles de la jerarquía de la organización. Una directiva que hace referencia a otra directiva por nombre se resuelve en la jerarquía de la organización con la coincidencia de directiva más cercana. Si no se encuentra ninguna directiva con un nombre específico en la jerarquía de la organización raíz, se busca una directiva especial denominada

"default". Esta práctica de resolución de políticas posibilita API de gestión fáciles de automatizar y proporciona una gran flexibilidad a los propietarios de las distintas organizaciones.

- **Perfiles de servicio e informática sin estado.** un perfil de servicio es una representación lógica de un servidor, llevando sus diferentes identidades y políticas. Puede asignar este servidor lógico a cualquier recurso informático físico, siempre que cumpla con los requisitos de recurso. La informática sin estado permite adquirir un servidor en cuestión de minutos, lo que solía tardar días en los sistemas de gestión de servidores heredados.
- **Soporte multi-tenancy integrado.** la combinación de políticas, pools, plantillas, una integridad referencial suelta, resolución de políticas en la jerarquía de la organización y un enfoque basado en perfiles de servicio para los recursos informáticos hace que Cisco UCS Manager sea inherentemente amigable con los entornos multi-tenant que normalmente se observan en clouds públicos y privados.
- **Memoria ampliada.** el servidor blade Cisco UCS B200 M5 de clase empresarial amplía las capacidades de la cartera de Cisco Unified Computing System en un factor de forma blade de media anchura. Cisco UCS B200 M5 aprovecha la potencia de las CPU de procesador escalable Intel Xeon más recientes con hasta 3 TB de RAM. Esta función hace posible la enorme ratio entre máquinas virtuales y servidores físicos que muchas implementaciones necesitan o permite que determinadas arquitecturas admitan operaciones de memoria grandes, como Big Data.
- **Red compatible con la virtualización.** la tecnología Cisco Virtual Machine Fabric extender (VM-FEX) hace que la capa de red de acceso sea consciente de la virtualización del host. Esta concienciación evita la contaminación de los dominios informáticos y de red con la virtualización cuando una red virtual se gestiona mediante perfiles de puerto definidos por su equipo de administrador de red. VM-FEX también libera la CPU del hipervisor al realizar conmutación en el hardware, lo que permite a la CPU del hipervisor realizar más tareas relacionadas con la virtualización. Para simplificar la gestión del cloud, la tecnología VM-FEX está bien integrada con VMware vCenter, la máquina virtual basada en kernel (KVM) de Linux y Microsoft Hyper-V SR-IOV.
- **QoS simplificada.** aunque FC y Ethernet están convergido en Cisco UCS, la compatibilidad integrada para QoS y Ethernet sin pérdidas la hace perfecta. Al representar todas las clases de sistemas en un panel GUI, la calidad de servicio de la red se simplifica en Cisco UCS Manager.

Cisco Nexus IP y switches MDS

Los switches Cisco Nexus y los directores multicapa Cisco MDS le ofrecen una conectividad empresarial y una consolidación SAN. Las redes de almacenamiento multiprotocolo de Cisco ayudan a reducir el riesgo empresarial al proporcionarle flexibilidad y opciones: FC, Fibre Connection (FICON), FC sobre Ethernet (FCoE), iSCSI y FC sobre IP (FCIP).

Los switches Cisco Nexus ofrecen uno de los conjuntos de funciones de red de centro de datos más completos de una única plataforma. Proporcionan un alto rendimiento y densidad tanto para el centro de datos como para el núcleo del campus. También ofrecen un conjunto completo de funciones para la agregación de centros de datos, el fin de la fila y la interconexión de centros de datos en una plataforma modular altamente resiliente.

Cisco UCS integra los recursos informáticos con los switches de Cisco Nexus y una estructura unificada que identifica y gestiona diferentes tipos de tráfico de red. Este tráfico incluye la I/o de almacenamiento, el tráfico de escritorios distribuido, la gestión y el acceso a aplicaciones clínicas y empresariales. Obtendrá las siguientes capacidades:

- **Escalabilidad de la infraestructura.** la virtualización, la energía y refrigeración eficientes, la escala de la nube con la automatización, la alta densidad y el rendimiento son compatibles con el crecimiento eficiente del centro de datos.
- **Continuidad operativa.** el diseño integra hardware, características de software Cisco NX-OS y administración para admitir entornos sin tiempos de inactividad.

- **Flexibilidad en el transporte.** puede adoptar gradualmente nuevas tecnologías de red con esta solución rentable.

Juntos, Cisco UCS, con switches Cisco Nexus y directores multicapa MDS, proporcionan una solución de conectividad San, conexión a redes e informática para un sistema de exploración médica empresarial.

Almacenamiento all-flash de NetApp

El almacenamiento de NetApp que ejecuta el software ONTAP reduce los costes generales de almacenamiento a la vez que ofrece los tiempos de respuesta de lectura y escritura de baja latencia y las altas IOPS que necesitan las cargas de trabajo del sistema de imágenes médicas. Con el fin de crear un sistema de almacenamiento óptimo que cumpla con los requisitos más habituales del sistema de exploración médica, ONTAP admite configuraciones de almacenamiento all-flash e híbrido. El almacenamiento flash de NetApp ofrece a los clientes de sistemas de imágenes médicas como usted los componentes clave de alto rendimiento y capacidad de respuesta para admitir operaciones de sistemas de imágenes médicas sensibles a la latencia. Mediante la creación de varios dominios de fallos en un único clúster, la tecnología de NetApp también puede aislar sus entornos de producción de entornos que no son de producción. Asimismo, al garantizar que el rendimiento del sistema no se sitúa por debajo de un cierto nivel en las cargas de trabajo con una calidad de servicio mínima de ONTAP, NetApp reduce los problemas de rendimiento del sistema.

La arquitectura de escalado horizontal del software ONTAP puede adaptarse con flexibilidad a sus distintas cargas de trabajo de I/O. Para proporcionar el rendimiento necesario y la baja latencia que necesitan las aplicaciones clínicas y proporcionar una arquitectura modular de escalado horizontal, las configuraciones all-flash normalmente se utilizan en arquitecturas ONTAP. Los nodos AFF de NetApp se pueden combinar en el mismo clúster de escalado horizontal con nodos de almacenamiento híbridos (HDD y flash) para almacenar conjuntos de datos de gran tamaño con un alto rendimiento. Puede clonar, replicar y hacer backup del entorno del sistema de imágenes médicas desde almacenamiento SSD costoso hasta almacenamiento HDD más económico en otros nodos. Con el almacenamiento habilitado para el cloud de NetApp y un Data Fabric que ofrece NetApp, puede realizar backups en el almacenamiento de objetos en las instalaciones o en el cloud.

En el caso de las exploraciones médicas, ONTAP ha sido validada por la mayoría de los sistemas líderes de exploración médica. Esto significa que se ha probado para ofrecer un rendimiento rápido y fiable para las imágenes médicas. Además, las siguientes funciones simplifican la gestión, aumentan la disponibilidad y automatización y reducen la cantidad total de almacenamiento que necesita.

- *Rendimiento excepcional *. La solución AFF de NetApp comparte la misma arquitectura de almacenamiento unificado, software ONTAP, interfaz de gestión, servicios de datos enriquecidos y conjunto de funciones avanzadas como el resto de las familias de productos FAS de NetApp. Esta innovadora combinación de medios all-flash con ONTAP le ofrece la baja latencia constante y una alta tasa de IOPS de almacenamiento all-flash con el software ONTAP líder en el sector.
- **Eficiencia del almacenamiento.** puede reducir los requisitos de capacidad totales utilizando su SME de NetApp para comprender cómo aplicó el sistema de imágenes médicas específico.
- **Clonado con gestión eficiente del espacio.** con la funcionalidad FlexClone, su sistema puede crear clones casi al instante para admitir la actualización del entorno de copia de seguridad y pruebas. Estos clones consumen almacenamiento adicional solo cuando se realizan cambios.
- **Protección de datos integrada.** las funciones completas de protección de datos y recuperación ante desastres le ayudan a proteger sus activos de datos críticos y a proporcionar recuperación ante desastres.
- **Operaciones no disruptivas.** puede realizar actualizaciones y mantenimiento sin tener que desconectar los datos.
- **QoS.** la calidad de servicio del almacenamiento le ayuda a limitar las posibles cargas de trabajo abusivas. Lo que es más importante, la calidad de servicio crea una garantía de rendimiento mínima que garantiza que el rendimiento de su sistema no bajará de un nivel determinado para cargas de trabajo críticas como

el entorno de producción de un sistema de imágenes médicas. Además, al limitar la contención, la calidad de servicio de NetApp también puede reducir los problemas relacionados con el rendimiento.

- **Data Fabric.** para acelerar la transformación digital, su Data Fabric que ofrece NetApp simplifica e integra la gestión de datos en entornos de cloud y en las instalaciones. Proporciona servicios y aplicaciones de gestión de datos consistentes e integrados para ofrecer una visibilidad, información, acceso, control, protección y seguridad. NetApp se integra con grandes clouds públicos, como AWS, Azure, Google Cloud e IBM Cloud le ofrece una amplia variedad de opciones.

Virtualización de host: VMware vSphere

Las arquitecturas de FlexPod se han validado con VMware vSphere 6.x, que es la plataforma de virtualización líder del sector. Se utiliza VMware ESXi 6.x para poner en marcha y ejecutar las máquinas virtuales. VCenter Server Appliance 6.x se utiliza para gestionar los hosts ESXi y las máquinas virtuales. Para formar un clúster VMware ESXi, se utilizan varios hosts ESXi que se ejecutan en blades Cisco UCS B200 M5. El clúster VMware ESXi agrupa los recursos informáticos, de memoria y de red de todos los nodos del clúster y proporciona una plataforma resiliente para las máquinas virtuales que se ejecutan en el clúster. Las funciones de clúster ESXi de VMware, alta disponibilidad de vSphere y Distributed Resource Scheduler (DRS) contribuyen a la tolerancia del clúster vSphere a resistir los fallos y ayudan a distribuir los recursos en los hosts ESXi de VMware.

El complemento de almacenamiento de NetApp y el complemento Cisco UCS se integran con VMware vCenter para conseguir flujos de trabajo operativos que requieren los recursos de computación y almacenamiento.

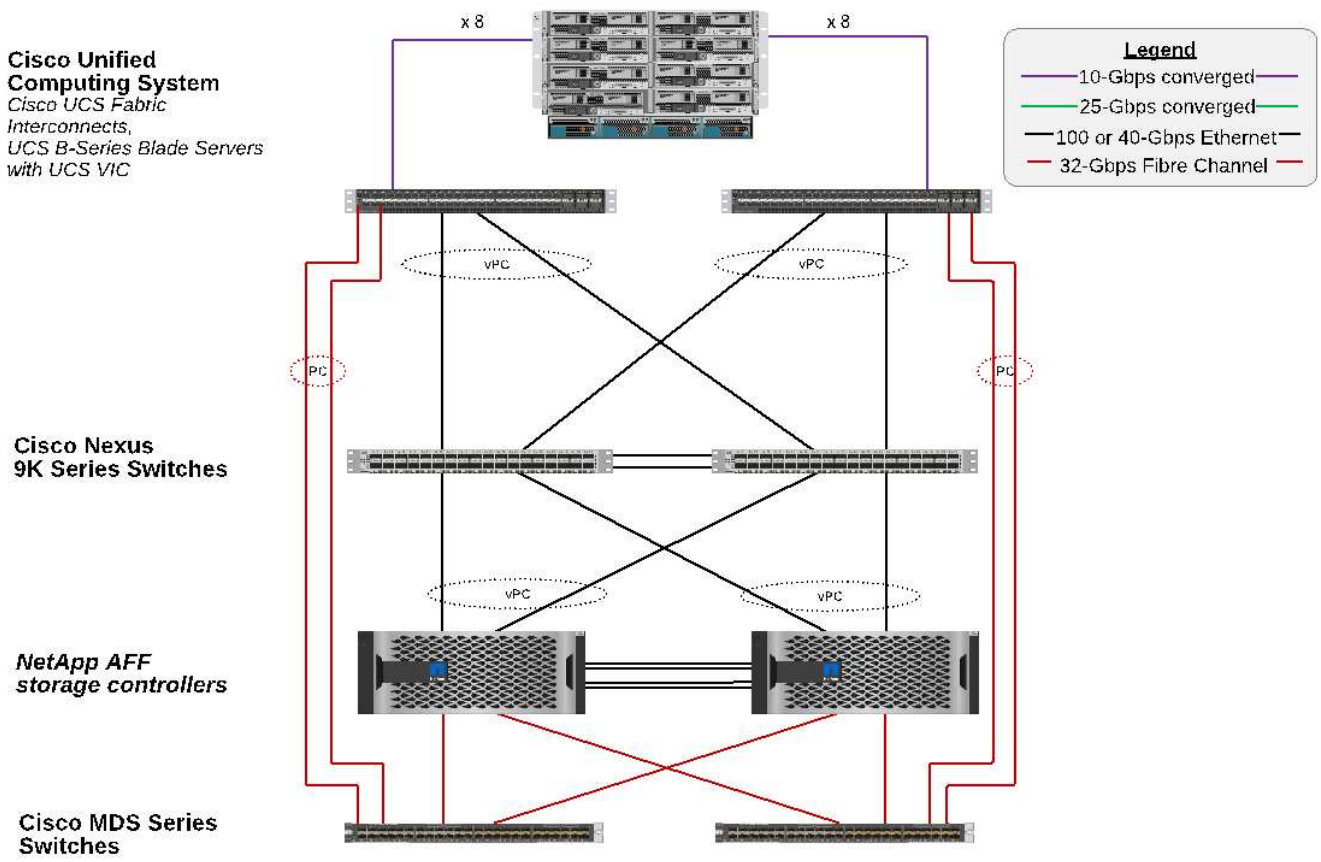
El clúster VMware ESXi y vCenter Server le ofrecen una plataforma centralizada para poner en marcha entornos de imágenes médicas en máquinas virtuales. Su organización de atención médica puede obtener todos los beneficios de una infraestructura virtual líder en el sector con confianza, como los siguientes:

- **Implementación sencilla.** ponga en marcha de forma rápida y sencilla vCenter Server con un dispositivo virtual.
- **Control y visibilidad centralizados.** administre toda la infraestructura de vSphere desde una única ubicación.
- **Optimización proactiva.** asignar, optimizar y migrar recursos para lograr la máxima eficacia.
- **Administración.** Utilice potentes complementos y herramientas para simplificar la administración y ampliar el control.

Arquitectura

La arquitectura de FlexPod está diseñada para proporcionar alta disponibilidad si falla un componente o un enlace en toda su pila de almacenamiento, red e informática. Las múltiples rutas de red para el acceso de los clientes y el acceso al almacenamiento proporcionan un equilibrio de carga y una utilización óptima de los recursos.

La siguiente figura ilustra la topología de Ethernet de 16 GB FC/40 GB (40 GbE) para la implementación de soluciones del sistema de imágenes médicas.



Arquitectura de almacenamiento

Utilice las directrices de arquitectura de almacenamiento de esta sección para configurar la infraestructura de almacenamiento para un sistema de exploración médica empresarial.

Niveles de almacenamiento

Un entorno típico de exploración médica empresarial consta de varios niveles de almacenamiento distintos. Cada nivel tiene requisitos específicos de protocolo de almacenamiento y rendimiento. El almacenamiento de NetApp admite diversas tecnologías de RAID; puede encontrar más información "aquí". A continuación, se explica cómo los sistemas de almacenamiento AFF de NetApp satisfacen las necesidades de los distintos niveles de almacenamiento para el sistema de imagen:

- **Almacenamiento de rendimiento (nivel 1).** este nivel ofrece alto rendimiento y alta redundancia para bases de datos, unidades de SO, almacenes de datos VMware Virtual Machine File System (VMFS), etc. Las operaciones de I/o en bloques se mueven por fibra a una cabina de almacenamiento compartido de SSD, tal y como se configura en ONTAP. La latencia mínima es de 1 ms a 3 ms, con una pico ocasional de 5 ms. Este nivel de almacenamiento se utiliza normalmente para la memoria caché de almacenamiento a corto plazo, normalmente de 6 a 12 meses de almacenamiento de imágenes para un acceso rápido a imágenes DICOM en línea. Este nivel ofrece alto rendimiento y alta redundancia para las cachés de imágenes, la copia de seguridad de la base de datos, etc. Las cabinas all-flash de NetApp proporcionan una latencia de <1 ms a un ancho de banda constante, lo cual es mucho inferior al tiempo de servicio que espera un entorno típico de imagen médica empresarial. ONTAP de NetApp es compatible con RAID-TEC

(RAID de triple paridad para soportar tres errores de disco) y RAID DP (RAID de doble paridad para soportar dos fallos de disco).

- **Almacenamiento de archivo (nivel 2).** este nivel se utiliza para el acceso a archivos típico con un coste optimizado, almacenamiento RAID 5 o RAID 6 para volúmenes más grandes y archivado a largo plazo con un coste/rendimiento más bajo. ONTAP de NetApp es compatible con RAID-TEC (RAID de triple paridad para soportar tres errores de disco) y RAID DP (RAID de doble paridad para soportar dos fallos de disco). FAS de NetApp en FlexPod permite realizar las operaciones de I/o de las aplicaciones de imagen a través de NFS/SMB en una cabina de discos SAS. Los sistemas FAS de NetApp ofrecen una latencia de ~10 ms con un ancho de banda constante, que es mucho menor que los tiempos de servicio esperados para el nivel 2 de almacenamiento en un entorno de sistema de imágenes médicas empresarial.

El archivado basado en cloud en un entorno de cloud híbrido se puede utilizar para archivar en un proveedor de almacenamiento en cloud público mediante S3 o protocolos similares. La tecnología SnapMirror de NetApp permite la replicación de datos de imágenes desde cabinas all-flash o FAS en cabinas de almacenamiento basadas en disco más lentas o en Cloud Volumes ONTAP para AWS, Azure o Google Cloud.

SnapMirror de NetApp ofrece funcionalidades de replicación de datos líderes del sector que ayudan a proteger el sistema de exploraciones médicas con replicación de datos unificada. Simplifique la gestión de la protección de datos en Data Fabric con la replicación entre plataformas: Del flash al disco y al cloud:

- Transporte datos sin problemas y con eficiencia entre sistemas de almacenamiento de NetApp para hacer posible que los backups y recuperación ante desastres se lleven a cabo con el mismo volumen de destino y flujo de I/O.
- Conmutación al nodo de respaldo en cualquier volumen secundario. Recupere desde cualquier copia Snapshot de un momento específico en el almacenamiento secundario.
- Proteja sus cargas de trabajo más importantes con la replicación síncrona con cero pérdida de datos, que ya se encuentra disponible (RPO=0).
- Reduzca el tráfico de red. Reduzca el espacio de almacenamiento con operaciones eficientes.
- Reduzca el tráfico de red teniendo solo que transportar los bloques de datos que cambien.
- Conserve las ventajas de la eficiencia del almacenamiento en el almacenamiento principal durante el transporte, incluidas la deduplicación, la compresión y la compactación.
- Ofrezca otras eficiencias inline adicionales con la compresión de red.

Se puede encontrar más información "aquí" .

La tabla siguiente enumera cada nivel que un sistema de exploraciones médicas típico requiere para una latencia específica y las características de rendimiento.

Nivel de almacenamiento	Requisitos	Recomendación de NetApp
1	Latencia de 1 a 5 ms, rendimiento de 35 a 500 Mbps	AFF con una pareja de alta disponibilidad (ha) de AFF A300 con <1 ms de latencia con dos bandejas de discos puede hacer frente al rendimiento de hasta 1,6 Gbps

Nivel de almacenamiento	Requisitos	Recomendación de NetApp
2	Archivado local	FAS con una latencia de hasta 30 ms
	Archivado en el cloud	Replicación de SnapMirror en Cloud Volumes ONTAP o archivado de backups con el software StorageGRID de NetApp

Conectividad de la red de almacenamiento

Estructura FC

- La estructura FC es para I/o del sistema operativo del host de computación a almacenamiento.
- Dos estructuras FC (Fabric A y Fabric B) están conectadas a Cisco UCS Fabric A y UCS Fabric B, respectivamente.
- Hay una máquina virtual de almacenamiento (SVM) con dos interfaces lógicas de FC (LIF) en cada nodo de controladora. En cada nodo, un LIF está conectado a la estructura A y el otro está conectado a la estructura B.
- La conectividad integral de FC de 16 Gbps se realiza mediante switches Cisco MDS. Se han configurado un único iniciador, varios puertos de destino y una división en zonas.
- El arranque SAN FC se utiliza para crear informática sin estado. Los servidores se arrancan desde las LUN del volumen de arranque que está alojado en el clúster de almacenamiento de AFF.

Red IP para acceso de almacenamiento a través de iSCSI, NFS y SMB/CIFS

- Dos LIF iSCSI se encuentran en la SVM de cada nodo de controladora. En cada nodo, un LIF está conectado al tejido A y el segundo está conectado al tejido B.
- Dos LIF de datos NAS se encuentran en la SVM de cada nodo de controladora. En cada nodo, un LIF está conectado al tejido A y el segundo está conectado al tejido B.
- Grupos de interfaz de puertos de almacenamiento (canal de puerto virtual [VPC]) para un enlace de 10 Gbps para el switch N9k-A y para un enlace de 10 Gbps para el switch N9k-B.
- Carga de trabajo en sistemas de archivos Ext4 o NTFS de un equipo virtual a otro:
  - Protocolo iSCSI por IP.
- Equipos virtuales alojados en almacenes de datos NFS:
  - La actividad de I/o de VM OS se realiza sobre varias rutas Ethernet a través de switches Nexus.

Gestión en banda (enlace activo-pasivo)

- Enlace de 1 Gbps al conmutador de administración N9k-A y enlace de 1 Gbps al conmutador de administración N9k-B.

Backup y recuperación

FlexPod Datacenter se crea en una cabina de almacenamiento gestionada por el software para la gestión de datos ONTAP de NetApp. El software ONTAP ha evolucionado a lo largo de 20 años para ofrecer muchas funciones de gestión de datos para máquinas virtuales, bases de datos de Oracle, archivos compartidos SMB/CIFS y NFS. También proporciona tecnologías de protección como la tecnología Snapshot de NetApp, la tecnología SnapMirror y la tecnología de replicación de datos FlexClone de NetApp. El software SnapCenter

de NetApp cuenta con un servidor y un cliente GUI para utilizar las funciones Snapshot, SnapRestore y FlexClone de ONTAP para VM, recursos compartidos de archivos SMB/CIFS, backup y recuperación de datos de Oracle y NFS.

Utiliza el software SnapCenter de NetApp "patentado" Tecnología Snapshot para crear un backup de toda una máquina virtual o base de datos de Oracle en un volumen de almacenamiento de NetApp de manera instantánea. En comparación con Oracle Recovery Manager (RMAN), las copias Snapshot no requieren una copia de backup completa de referencia, ya que no se almacenan como copias físicas de bloques. Las copias Snapshot se almacenan como punteros a los bloques de almacenamiento tal y como existían en el sistema de archivos ONTAP WAFL cuando se crearon las copias Snapshot. Debido a esta estrecha relación física, las copias Snapshot se mantienen en la misma cabina de almacenamiento que los datos originales. Las copias Snapshot también se pueden crear a nivel de archivo para ofrecer un control más granular para los backups.

La tecnología Snapshot se basa en una técnica de redireccionamiento en escritura. Inicialmente, contiene solo punteros de metadatos y no consume mucho espacio hasta que los primeros cambios de datos cambian a un bloque de almacenamiento. Si un bloque existente está bloqueado por una copia snapshot, el sistema de archivos ONTAP WAFL escribe un bloque nuevo como una copia activa. Este enfoque evita las dobles escrituras que se producen con la técnica de cambio en escritura.

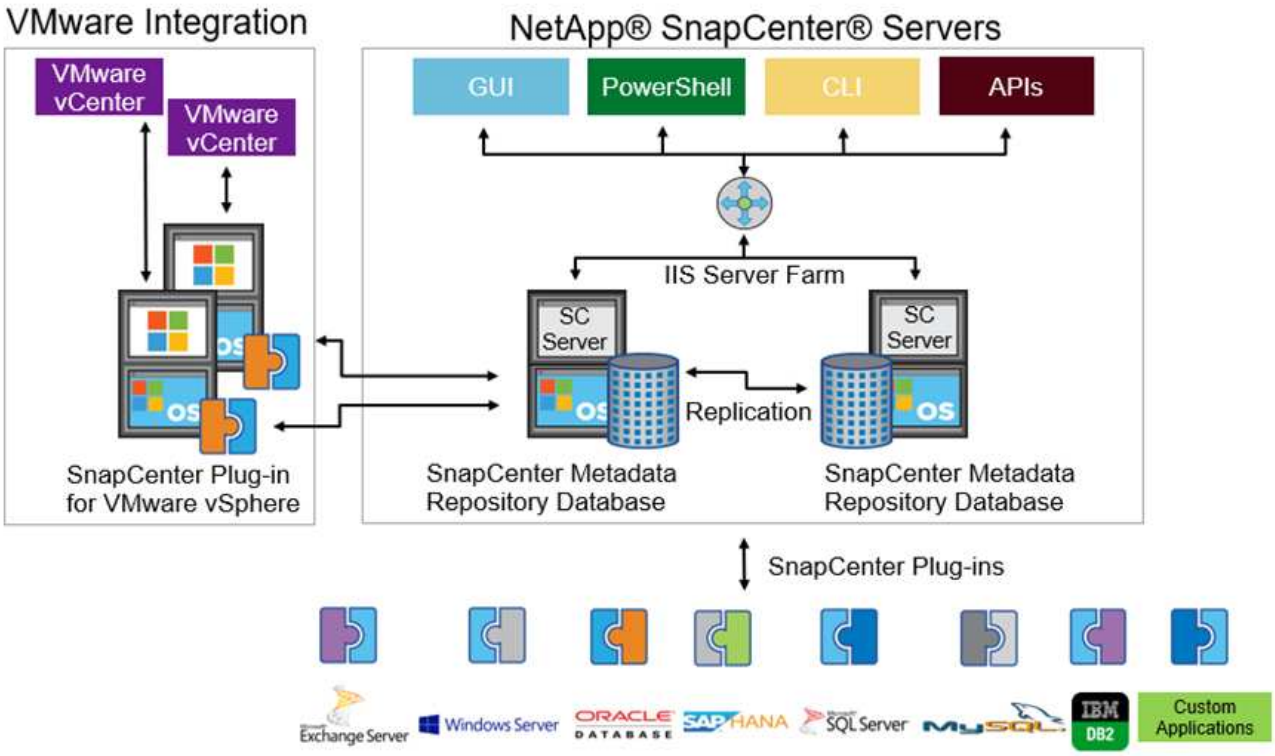
Para el backup de bases de datos de Oracle, las copias Snapshot producen un ahorro de tiempo increíble. Por ejemplo, si se realiza una copia de seguridad que tardaba 26 horas en completarse sólo con RMAN, puede tardar menos de 2 minutos con el software SnapCenter.

Además, como la restauración de datos no copia ningún bloque de datos, sino coloca los punteros en las imágenes de bloque Snapshot coherentes con la aplicación cuando se creó la copia Snapshot, es posible restaurar una copia de backup de Snapshot casi al instante. La clonación de SnapCenter crea una copia independiente de punteros de metadatos a una copia Snapshot existente y monta la nueva copia en un host de destino. Este proceso también es rápido y un almacenamiento eficiente.

La tabla siguiente resume las principales diferencias entre Oracle RMAN y el software SnapCenter de NetApp.

	Backup	**Restaurar**	**Clonar**	**Necesita un backup completo**	**Uso del espacio**	**Copia externa**
RMAN	Lento	Lento	Lento	Sí	Alto	Sí
SnapCenter	Y rápido	Y rápido	Y rápido	No	Bajo	Sí

En la siguiente figura, se presenta la arquitectura SnapCenter.



Miles de empresas de todo el mundo usan las configuraciones de MetroCluster de NetApp para obtener alta disponibilidad (ha), cero pérdida de datos y operaciones no disruptivas tanto en el centro de datos como fuera de él. MetroCluster es una función gratuita del software ONTAP que refleja de forma síncrona los datos y la configuración entre dos clústeres de ONTAP en ubicaciones independientes o dominios de fallo. MetroCluster proporciona almacenamiento disponible de forma continua para las aplicaciones al gestionar automáticamente dos objetivos: Objetivo de punto de recuperación (RPO) cero mediante un mirroring sincrónico de los datos que se escriben en el clúster. El objetivo de tiempo de recuperación (RTO) prácticamente cero mediante la configuración de mirroring y la automatización del acceso a los datos en el segundo sitio MetroCluster ofrece simplicidad con mirroring automático de datos y configuración entre los dos clústeres independientes ubicados en los dos sitios. A medida que se aprovisiona el almacenamiento en un clúster, se replica automáticamente en el segundo clúster del segundo centro. La tecnología SyncMirror de NetApp proporciona una copia completa de todos los datos con un objetivo de punto de recuperación cero. , Por lo tanto, las cargas de trabajo de un sitio pueden cambiar en cualquier momento al sitio opuesto y continuar sirviendo datos sin pérdida de datos. Se puede encontrar más información "aquí".

Redes

Un par de switches Cisco Nexus proporcionan rutas redundantes para el tráfico IP de computación a almacenamiento, y para clientes externos del visor de imágenes del sistema de imágenes médicas:

- La agregación de enlaces que utiliza canales de puertos y VPs se emplea en todas partes, lo que permite un diseño de mayor ancho de banda y alta disponibilidad:
  - VPC se utiliza entre la cabina de almacenamiento de NetApp y los switches de Cisco Nexus.
  - VPC se utiliza entre la interconexión de estructura de Cisco UCS y los switches de Cisco Nexus.
  - Cada servidor dispone de tarjetas de interfaz de red virtual (vNIC) con conectividad redundante a la estructura unificada. La conmutación por error de NIC se utiliza entre las interconexiones de estructura para obtener redundancia.
  - Cada servidor tiene adaptadores de bus de host virtual (vHBA) con conectividad redundante a la

estructura unificada.

- Las interconexiones de estructura Cisco UCS se configuran en modo de host final como se recomienda, lo que permite fijar dinámicamente NIC a switches de enlace ascendente.
- Una red de almacenamiento FC lo proporcionan un par de switches Cisco MDS.

Informática: Cisco Unified Computing System

Dos estructuras de Cisco UCS mediante diferentes interconexiones de estructura proporcionan dos dominios de fallo. Cada estructura está conectada tanto a switches de red IP como a distintos switches de red de FC.

Para ejecutar VMware ESXi, se crean perfiles de servicio idénticos para cada blade de Cisco UCS, tal y como se establecen en las prácticas recomendadas de FlexPod. Cada perfil de servicio debe tener los siguientes componentes:

- Dos NIC (una en cada estructura) para transportar tráfico de clientes o gestión NFS, SMB/CIFS y NFS
- VLAN adicionales necesarias a las NIC virtuales para tráfico de gestión o cliente NFS, SMB/CIFS y NFS
- Dos NIC (una en cada estructura) para transportar tráfico iSCSI
- Dos HBA de FC de almacenamiento (uno en cada estructura) para el tráfico de FC al almacenamiento
- Arranque SAN

Virtualización

El clúster de hosts VMware ESXi ejecuta máquinas virtuales de carga de trabajo. El clúster incluye instancias ESXi que se ejecutan en servidores blade Cisco UCS.

Cada host ESXi incluye los siguientes componentes de red:

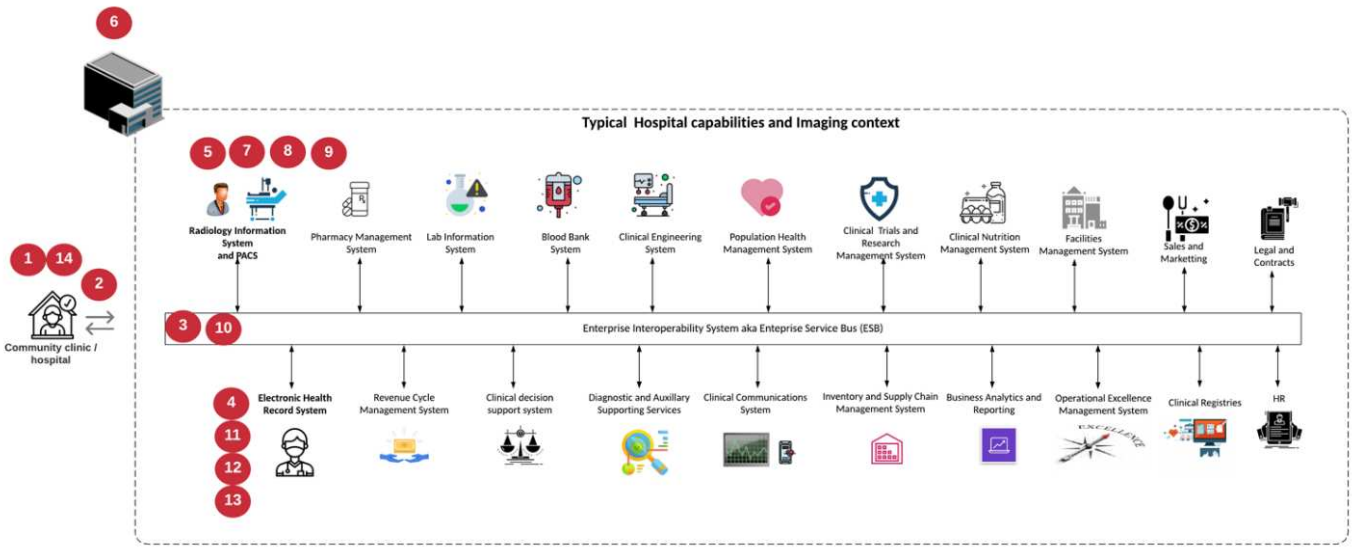
- Arranque SAN mediante FC o iSCSI
- Arranque los LUN en el almacenamiento de NetApp (en un FlexVol dedicado para SO de arranque)
- Dos NIC de gestión (Cisco UCS VNIC) para NFS, SMB/CIFS o tráfico de gestión
- Dos HBA de almacenamiento (Cisco UCS FC Vhba) para el tráfico de FC al almacenamiento
- Switch estándar o switch virtual distribuido (según sea necesario)
- Almacén de datos NFS para máquinas virtuales de carga de trabajo
- Gestión, red de tráfico de clientes y grupos de puertos de red de almacenamiento para máquinas virtuales
- Adaptador de red para la gestión, el tráfico de clientes y el acceso al almacenamiento (NFS, iSCSI o SMB/CIFS) de cada máquina virtual
- DRS de VMware activado
- Multivía nativa habilitada para rutas FC o iSCSI al almacenamiento
- Snapshots de VMware para máquina virtual desactivadas
- SnapCenter de NetApp puesto en marcha para VMware para backups de equipos virtuales

Arquitectura de sistemas de imágenes médicas

En las organizaciones sanitarias, los sistemas de imágenes médicas son aplicaciones cruciales y están bien integrados en los flujos de trabajo clínicos que empiezan desde el registro de los pacientes y finalizan con las actividades relacionadas con la facturación en el ciclo de ingresos.

El siguiente diagrama muestra los diversos sistemas implicados en un hospital grande típico; este diagrama está destinado a proporcionar un contexto arquitectónico a un sistema de imágenes médicas antes de que nos acercamos a los componentes arquitectónicos de un sistema típico de imágenes médicas. Los flujos de trabajo varían ampliamente y son hospitalarios y de uso específico.

La figura siguiente muestra el sistema de imágenes médicas en el contexto de un paciente, una clínica comunitaria y un hospital grande.



1. El paciente visita la clínica comunitaria con síntomas. Durante la consulta, el médico de la comunidad coloca una orden de imagen que se envía al hospital más grande en forma de un mensaje de orden HL7.
2. El sistema EHR del médico de la comunidad envía el mensaje Order/ORD HL7 al hospital de gran tamaño.
3. El sistema de interoperabilidad empresarial (también conocido como bus de servicio empresarial [ESB]) procesa el mensaje de pedido y envía el mensaje de pedido al sistema EHR.
4. EHR procesa el mensaje de pedido. Si no existe un registro de paciente, se crea un nuevo registro de paciente.
5. La EHR envía una solicitud de diagnóstico por imágenes al sistema de imágenes médicas.
6. El paciente llama al gran hospital para una cita con imágenes.
7. La recepción de imágenes y el servicio de registro programa al paciente para una cita con imágenes utilizando información radiológica o un sistema similar.
8. El paciente llega para la cita con imágenes, y las imágenes o el vídeo se crean y envían al PACS.
9. El radiólogo lee las imágenes y anota las imágenes en el PACS utilizando un visor de diagnóstico con gráficos de gama alta/GPU habilitado. Ciertos sistemas de imágenes tienen capacidades de mejora de la eficiencia habilitadas para la inteligencia artificial (IA) en los flujos de trabajo de imágenes.
10. Los resultados del pedido de imágenes se envían al EHR en forma de mensaje ORU HL7 resultados de pedidos a través del ESB.
11. El EHR procesa los resultados del pedido en el registro del paciente, coloca la imagen en miniatura con un vínculo contextual a la imagen DICOM real. Los médicos pueden iniciar el visor de diagnóstico si se necesita una imagen de mayor resolución desde el EHR.
12. El médico revisa la imagen e introduce las notas del médico en el registro del paciente. El médico podría utilizar el sistema de apoyo a la toma de decisiones clínicas para mejorar el proceso de revisión y ayudar en el diagnóstico adecuado para el paciente.

13. A continuación, el sistema EHR envía los resultados de la orden en forma de un mensaje de resultados de la orden al hospital comunitario. En este punto, si el hospital comunitario puede recibir la imagen completa, entonces la imagen se envía a través de WADO o DICOM.
14. El médico de la comunidad completa el diagnóstico y proporciona los siguientes pasos al paciente.

Un sistema típico de imágenes médicas utiliza una arquitectura de N niveles. El componente principal de un sistema de imágenes médicas es un servidor de aplicaciones que aloja varios componentes de la aplicación. Los servidores de aplicaciones típicos están basados en Java Runtime o en C# .Net CLR. La mayoría de las soluciones de imágenes médicas para empresas utilizan un servidor de bases de datos Oracle, MS SQL Server o Sybase como base de datos primaria. Además, algunos sistemas empresariales de exploración médica también utilizan bases de datos para la aceleración de contenidos y el almacenamiento en caché en una región geográfica. Algunos sistemas de imagen médica empresarial también utilizan bases de datos NoSQL como MongoDB, Redis, etc. junto con servidores de integración empresarial para interfaces DICOM y API.

Un sistema típico de imágenes médicas proporciona acceso a imágenes para dos grupos distintos de usuarios: El usuario/radiólogo de diagnóstico, o el médico o el médico que ordenó la adquisición de imágenes.

Los radiólogos suelen utilizar visores de diagnósticos de gama alta habilitados para gráficos que se ejecutan en estaciones de trabajo gráficas e informáticas de gama alta que son físicas o parte de una infraestructura de escritorios virtuales. Si está a punto de iniciar su viaje hacia la infraestructura de puestos de trabajo virtuales, encontrará más información "aquí".

Cuando el huracán Katrina destruyó dos de los principales hospitales docentes de Luisiana, se reunieron los líderes para construir un sistema de registros sanitarios electrónicos resistente que incluía más de 3000 equipos virtuales en un tiempo récord. Se puede encontrar más información sobre la arquitectura de referencia de casos de uso y los paquetes de referencia de FlexPod "aquí".

Los médicos acceden a las imágenes de dos formas principales:

- **Acceso basado en Web.** que suele utilizarse en los sistemas EHR para incorporar las imágenes PACS como enlaces contextuales al registro médico electrónico (EMR) del paciente, y vínculos que se pueden colocar en los flujos de trabajo de imágenes, los flujos de trabajo de procedimientos, los flujos de trabajo de notas de progreso, etc. Los enlaces basados en la Web también se utilizan para proporcionar acceso a imágenes a los pacientes a través de los portales de pacientes. El acceso basado en Web utiliza un patrón tecnológico llamado vínculos contextuales. Los vínculos con contexto pueden ser enlaces estáticos/URI al soporte DICOM directamente o enlaces generados dinámicamente mediante macros personalizadas.
- **Cliente grueso.** algunos sistemas médicos empresariales también le permiten utilizar un enfoque de cliente grueso para ver las imágenes. Puede iniciar un cliente grueso desde el EMR del paciente o como una aplicación independiente.

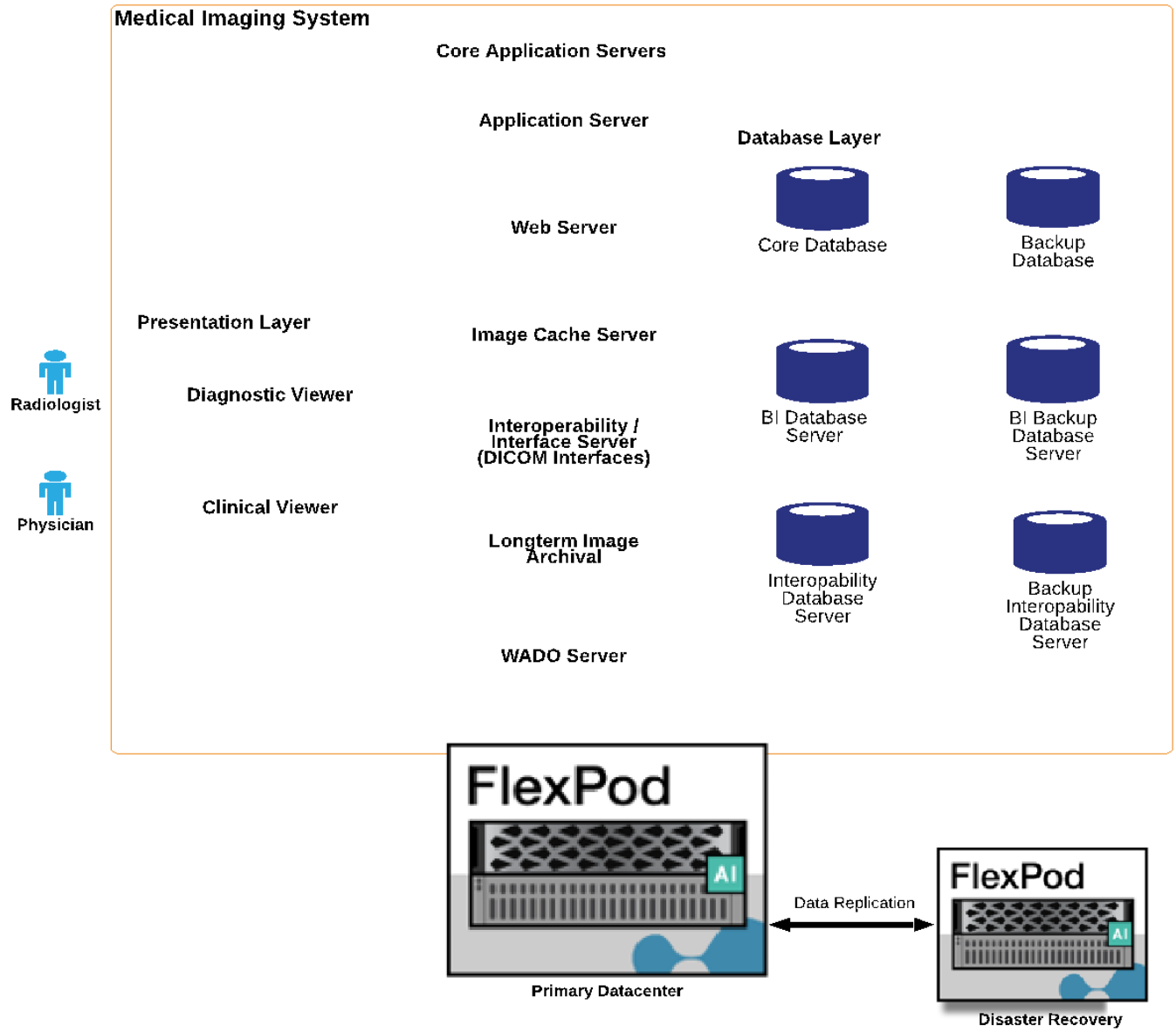
El sistema de imágenes médicas puede proporcionar acceso a imágenes a una comunidad de médicos o a médicos participantes en el CIN. Los sistemas de imágenes médicas típicos incluyen componentes que permiten la interoperabilidad de imágenes con otros sistemas INFORMÁTICOS de salud dentro y fuera de su organización sanitaria. Los médicos de la comunidad pueden acceder a imágenes mediante una aplicación basada en web o utilizar una plataforma de intercambio de imágenes para la interoperabilidad de imágenes. Las plataformas de intercambio de imágenes normalmente utilizan WADO o DICOM como el protocolo de intercambio de imágenes subyacente.

Los sistemas de exploración médica también pueden admitir centros médicos académicos que necesitan sistemas PACS o de exploración para su uso en clases. Para apoyar las actividades académicas, un sistema típico de exploración médica puede tener las capacidades de un sistema PACS en una huella menor o en un entorno de exploración de solo enseñanza. Los sistemas de archivado típicos de proveedores y algunos sistemas de imágenes médicas de clase empresarial ofrecen funciones de morfología de etiquetas de imagen

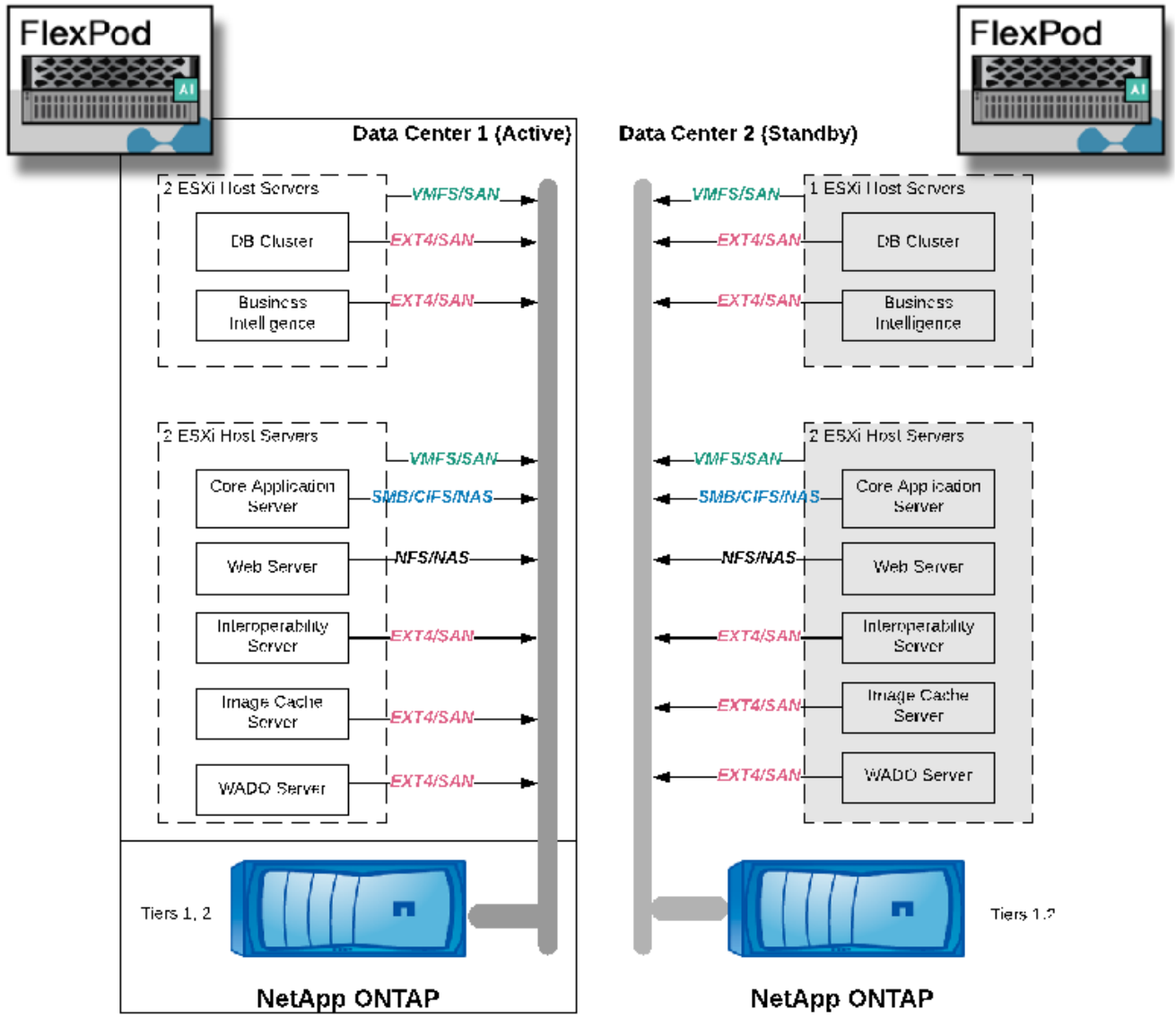
DICOM para anonimizar las imágenes que se utilizan con fines didácticos. Tag morfing permite a las organizaciones sanitarias intercambiar imágenes DICOM entre distintos sistemas de imágenes médicas de distintos proveedores de forma neutral con respecto a los proveedores. Además, TAG morfing permite que los sistemas de imágenes médicas implementen una capacidad de archivado para todas las empresas, neutral con respecto a los proveedores, para las imágenes médicas.

Los sistemas de imágenes médicas están empezando a utilizarse "Funcionalidades de computación basadas en GPU" para mejorar los flujos de trabajo humanos mediante el preprocesamiento de las imágenes y, por lo tanto, la eficiencia. Los sistemas típicos de exploración médica empresarial aprovechan las funcionalidades de eficiencia del almacenamiento de NetApp, líderes del sector. Los sistemas de imágenes médicas empresariales suelen utilizar RMAN para realizar actividades de copia de seguridad, recuperación y restauración. Para mejorar el rendimiento y reducir el tiempo que se tarda en crear backups, la tecnología Snapshot está disponible para las operaciones de backup y la tecnología SnapMirror está disponible para la replicación.

En la siguiente figura se muestran los componentes lógicos de la aplicación en una vista arquitectónica por capas.



La siguiente figura muestra los componentes físicos de la aplicación.



Los componentes lógicos de la aplicación requieren que la infraestructura admita un conjunto diverso de protocolos y sistemas de archivos. El software ONTAP de NetApp admite un conjunto de protocolos y sistemas de archivos líder en el sector.

En la siguiente tabla se enumeran los componentes de la aplicación, el protocolo de almacenamiento y los requisitos del sistema de archivos.

Componente de aplicación	SAN/NAS	Tipo de sistema de archivos	Nivel de almacenamiento	Tipo de replicación
BD de prod del host VMware	local	SAN	VMFS	Nivel 1
Cliente más	BD de prod del host VMware	REP	SAN	VMFS

Componente de aplicación	SAN/NAS	Tipo de sistema de archivos	Nivel de almacenamiento	Tipo de replicación
Nivel 1	Cliente más	Aplicación prod. Host VMware	local	SAN
VMFS	Nivel 1	Cliente más	Aplicación prod. Host VMware	REP
SAN	VMFS	Nivel 1	Cliente más	Servidor de bases de datos principal
SAN	Ext4	Nivel 1	Cliente más	Servidor de bases de datos de respaldo
SAN	Ext4	Nivel 1	Ninguno	Servidor de caché de imágenes
NAS	SMB/CIFS	Nivel 1	Ninguno	Servidor de archivado
NAS	SMB/CIFS	Nivel 2	Cliente más	Servidor web
NAS	SMB/CIFS	Nivel 1	Ninguno	Servidor WADO
SAN	NFS	Nivel 1	Cliente más	Servidor de inteligencia empresarial
SAN	NTFS	Nivel 1	Cliente más	Backup de inteligencia empresarial
SAN	NTFS	Nivel 1	Cliente más	Servidor de interoperabilidad
SAN	Ext4	Nivel 1	Cliente más	Servidor de bases de datos de interoperabilidad

Infraestructura de la solución componentes de hardware y software

En las tablas siguientes se enumeran los componentes de hardware y software, respectivamente, de la infraestructura de FlexPod para el sistema de imágenes médicas.

Capa	Familia de productos	Cantidad y modelo	Detalles
Informática	Chasis Cisco UCS 5108	1 o 2	Según el número de palas necesario para admitir el número de estudios anuales
	Servidores blade Cisco UCS	B200 M5	Número de blades basado en el número de estudios anuales cada uno con 2 x 20 o más núcleos, 2,7 GHz y 128-384 GB de RAM
	Tarjeta de interfaz virtual (VIC) de Cisco UCS	Cisco UCS 1440	Consulte
	2 interconexiones de estructura Cisco UCS	6454 o posterior	–
Red	Switches Cisco Nexus	2 series Cisco Nexus 3000 o 9000	–
Red de almacenamiento	Red IP para el acceso de almacenamiento mediante protocolos SMB/CIFS, NFS o iSCSI	Los mismos switches de red que se han descrito anteriormente	–
	Acceso a almacenamiento mediante FC	2 Cisco MDS 9132T	–
Reducida	Sistema de almacenamiento all-flash AFF A400 de NetApp	1 o más pares de alta disponibilidad	Clúster con dos o más nodos
	Bandeja de discos	1 o más bandejas de discos DS224C o NS224	Totalmente lleno con 24 unidades
	SSD	>24, 1,2 TB o mayor capacidad	–

De NetApp	Familia de productos	Versión o versión	Detalles
Sistema de imágenes médicas empresariales			
	MS SQL u Oracle Database Server	Según lo sugerido por el proveedor del sistema de imágenes médicas	
	Sin bases de datos SQL como MongoDB Server	Según lo sugerido por el proveedor del sistema de imágenes médicas	
	Servidores de aplicaciones	Según lo sugerido por el proveedor del sistema de imágenes médicas	
	Servidor de integración (MS BizTalk, MuleSoft, Rhapsody, Tibco)	Según lo sugerido por el proveedor del sistema de imágenes médicas	
	Equipos virtuales	Linux (64 bits)	
	Equipos virtuales	Windows Server (64 bits)	
Reducida	ONTAP	ONTAP 9.7 o posterior	
Red	Interconexión de estructura Cisco UCS	Cisco UCS Manager 4.1 o posterior	
	Switches Ethernet de Cisco	9.2(3)I7(2) o posterior	
	Cisco FC: Cisco MDS 9132T	8.4(2) o posterior	
Hipervisor	Hipervisor	VMware vSphere ESXi 6.7 U2 o posterior	
Gestión	Sistema de gestión de hipervisores	VMware vCenter Server 6.7 U1 (vcsa) o posterior	
	Virtual Storage Console (VSC) de NetApp	VSC 9.7 o posterior	
	SnapCenter	SnapCenter 4.3 o posterior	

Ajuste del tamaño de la solución

Ajuste de tamaño del almacenamiento

En esta sección se describe el número de estudios y los requisitos de infraestructura correspondientes.

Los requisitos de almacenamiento que se enumeran en la siguiente tabla suponen que los datos existentes tienen un valor de 1 año más un crecimiento previsto para un año de estudio en el sistema primario (nivel 1, 2). Las necesidades de almacenamiento adicionales para el crecimiento previsto para 3 años después de los dos primeros años se enumeran por separado.

	Pequeño	Mediano	Grande
Estudios anuales	<250.000 estudios	Estudios de 250K–500K	500 000–1 millón de estudios
Almacenamiento de nivel 1			
IOPS (promedio)	1,5K–5K	5000 A 15 000	DE 15K A 40K
IOPS (pico)	5000	20 K	65 000
Rendimiento	50–100 Mbps	De 50 a 150 Mbps	100–300 Mbps
Capacidad del centro de datos 1 (1 año de datos antiguos y 1 año de estudio nuevo)	70 TB	140 TB	260 TB
Capacidad del centro de datos 1 (necesidad adicional durante 4 años para un nuevo estudio)	25 TB	45 TB	80 TB
Capacidad del centro de datos 2 (1 año de datos antiguos y 1 año de estudio nuevo)	45 TB	110 TB	165 TB
Capacidad del centro de datos 2 (necesidad adicional durante 4 años para un estudio nuevo)	25 TB	45 TB	80 TB
Almacenamiento en dos niveles			
IOPS (promedio)	1K	2K	3.000
Capacidad del centro de datos 1	320 TB	800 TB	2000 TB

Ajuste de tamaño de computación

En la siguiente tabla se enumeran los requisitos informáticos para sistemas de imágenes médicas pequeños, medianos y grandes.

	Pequeño	Mediano	Grande
Estudios anuales	<250.000 estudios	Estudios de 250K–500K	500 000–1 millón de estudios
Centro de datos 1			
Número de máquinas virtuales	21	27	35
Número total de CPU virtuales (vCPU)	56	124	220
Requisito de memoria total	225 GB	450 GB	900 GB

	Pequeño	Mediano	Grande
Especificaciones de servidores físicos (blades) (presuponga 1 vCPU -=1 núcleo)	4 servidores con 20 núcleos y 192 GB de RAM cada uno	8 servidores con 20 núcleos y 128 GB de RAM cada uno	14 servidores con 20 núcleos y 128 GB de RAM cada uno
Centro de datos 2			
Número de máquinas virtuales	15	17	22
Número total de vCPU	42	72	140
Requisito de memoria total	179 GB	243 GB	513 GB
Especificaciones de servidores físicos (blades) (presuponga 1 vCPU = 1 núcleo)	3 servidores con 20 núcleos y 168 GB de RAM cada uno	6 servidores con 20 núcleos y 128 GB de RAM cada uno	8 servidores con 24 núcleos y 128 GB de RAM cada uno

Ajuste de tamaño de la infraestructura de redes y Cisco UCS

En la siguiente tabla se enumeran los requisitos de la infraestructura de red y Cisco UCS para sistemas de imágenes médicas pequeños, medianos y grandes.

	Pequeño	Mediano	Grande
Centro de datos 1			
El número de puertos del nodo de almacenamiento	2 adaptadores de red convergentes (CNA); 2 FCs	2 CNA; 2 FCF	2 CNA; 2 FCF
Puertos del switch de red de IP (Cisco Nexus 9000)	switch de 48 puertos	switch de 48 puertos	switch de 48 puertos
Switch FC (Cisco MDS)	switch de 32 puertos	switch de 32 puertos	switch de 48 puertos
Número de chasis Cisco UCS	1 x 5108	1 x 5108	2 x 5108
Interconexión de estructura Cisco UCS	2 x 6332	2 x 6332	2 x 6332
Centro de datos 2			
Número de chasis Cisco UCS	1 x 5108	1 x 5108	1 x 5108
Interconexión de estructura Cisco UCS	2 x 6332	2 x 6332	2 x 6332
El número de puertos del nodo de almacenamiento	2 CNA; 2 FCF	2 CNA; 2 FCF	2 CNA; 2 FCF
Puertos del switch de red de IP (Cisco Nexus 9000)	switch de 48 puertos	switch de 48 puertos	switch de 48 puertos
Switch FC (Cisco MDS)	switch de 32 puertos	switch de 32 puertos	switch de 48 puertos

Mejores prácticas

Mejores prácticas de almacenamiento

Alta disponibilidad

El diseño del clúster de almacenamiento de NetApp proporciona alta disponibilidad en todos los niveles:

- Nodos en clúster
- Conectividad del sistema de almacenamiento principal
- RAID TEC que admite tres fallos de disco
- RAID DP, que puede soportar dos errores de disco
- Conectividad física a dos redes físicas desde cada nodo
- Múltiples rutas de datos para los LUN y volúmenes de almacenamiento

Multi-tenancy seguro

Las máquinas virtuales de almacenamiento (SVM) de NetApp proporcionan una estructura de cabina de almacenamiento virtual para separar el dominio de seguridad, las políticas y las redes virtuales. NetApp le recomienda crear SVM independientes para cada organización tenant que aloje los datos en el clúster de almacenamiento de.

Mejores prácticas de almacenamiento de NetApp

Considere las siguientes prácticas recomendadas de almacenamiento de NetApp:

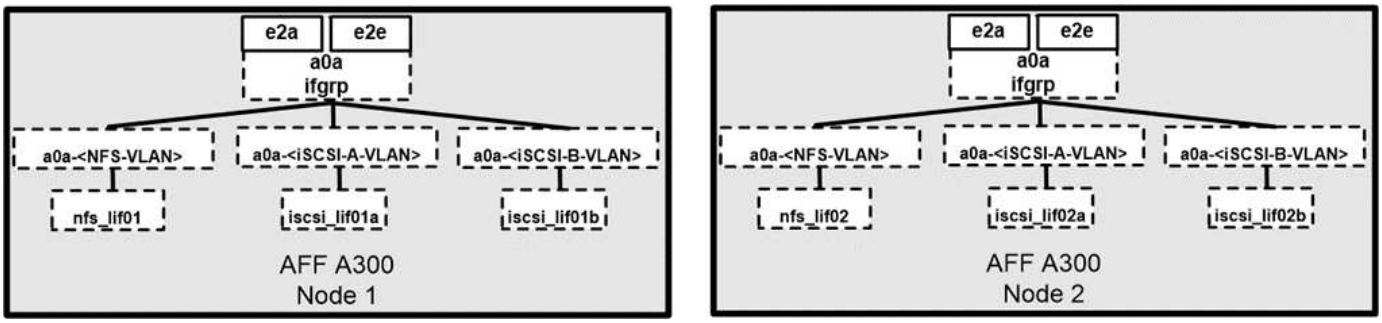
- Siempre habilite la tecnología AutoSupport de NetApp, que envía información de resumen de soporte a NetApp a través de HTTPS.
- Para obtener la máxima disponibilidad y movilidad, asegúrese de que se crea una LIF para cada SVM en cada nodo del clúster de ONTAP de NetApp. El acceso asimétrico de unidad lógica (ALUA, Asymmetric Logical Unit Access) se utiliza para analizar las rutas e identificar las rutas activas optimizadas (directas) frente a las rutas activas no optimizadas. ALUA se utiliza tanto para FC como FCoE e iSCSI.
- No es necesario montar el volumen que solo contiene LUN de forma interna ni es necesaria una ruta de unión.
- Si se utiliza el protocolo de autenticación por desafío mutuo (CHAP) en ESXi para la autenticación de destino, también se debe configurar en ONTAP. Utilice la CLI (`vserver iscsi security create`) O con ONTAP System Manager de NetApp (edite la seguridad del iniciador en almacenamiento > SVM > Configuración de SVM > Protocolos > iSCSI).

Arranque SAN

NetApp recomienda que implemente el arranque SAN para servidores Cisco UCS en la solución de centro de datos FlexPod. Este paso permite proteger el sistema operativo de forma segura mediante el sistema de almacenamiento AFF de NetApp, lo que mejora el rendimiento. El diseño descrito en esta solución utiliza arranque SAN iSCSI.

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 hasta el almacenamiento. Los puertos de almacenamiento de este ejemplo, e2a y e2e, que están conectados a los switches Cisco Nexus, se agrupan para formar un puerto lógico llamado grupo de interfaces (ifgrp) (en este ejemplo, a0a). Las VLAN iSCSI se crean en el igroup y los LIF iSCSI se crean en grupos de puertos iSCSI (en este ejemplo, a0a-<iSCSI-A-VLAN>). El LUN de

arranque iSCSI se expone a los servidores a través del LIF iSCSI mediante grupos de iniciadores. Este enfoque permite que solo el servidor autorizado tenga acceso a la LUN de arranque. Para ver el diseño de los puertos y la LIF, consulte la figura a continuación.



A diferencia de las interfaces de red NAS, las interfaces DE red SAN no están configuradas para realizar la conmutación al nodo de respaldo durante un fallo. En su lugar, si una interfaz de red no está disponible, el host elige una nueva ruta optimizada para una interfaz de red disponible. ALUA, un estándar compatible con NetApp, proporciona información sobre los destinos SCSI, lo que permite a un host identificar la ruta mejor al almacenamiento.

Eficiencia del almacenamiento y thin provisioning

NetApp ha sido el líder del sector en innovación en eficiencia del almacenamiento, como, por ejemplo, la primera deduplicación para cargas de trabajo principales y con la compactación de datos inline, que mejora la compresión y almacena archivos pequeños e I/o de forma eficiente. ONTAP admite deduplicación en línea y en segundo plano, así como compresión en línea y en segundo plano.

Para obtener las ventajas de la deduplicación en un entorno de bloques, se deben aplicar thin provisioning en las LUN. Aunque el administrador de equipos virtuales todavía puede observar la LUN mientras utiliza la capacidad aprovisionada, el ahorro de la deduplicación se devuelve al volumen que se usa para otras necesidades. NetApp recomienda poner en marcha estas LUN en volúmenes de FlexVol que también se aprovisionan mediante thin provisioning con una capacidad que tiene el doble de tamaño que la LUN. Cuando se pone en marcha el LUN de esa manera, el volumen FlexVol actúa simplemente como una cuota. El almacenamiento que consume la LUN se informa en el volumen FlexVol y el agregado que la contiene.

Para obtener el máximo ahorro de la deduplicación, considere la posibilidad de programar la deduplicación en segundo plano. Sin embargo, estos procesos utilizan los recursos del sistema cuando se ejecutan. Por lo tanto, lo ideal es programar los trabajos durante periodos menos activos (como los fines de semana) o ejecutarlos con mayor frecuencia para reducir la cantidad de datos modificados que se van a procesar. La deduplicación automática en segundo plano en los sistemas AFF tiene mucho menos efecto en las actividades de primer plano. La compresión en segundo plano (para sistemas basados en discos duros) también consume recursos, por lo que debe tener en cuenta solo para cargas de trabajo secundarias con requisitos de rendimiento limitados.

Calidad de servicio

Los sistemas que ejecutan el software ONTAP pueden utilizar la función de calidad de servicio del almacenamiento ONTAP para limitar el rendimiento en megabits por segundo (Mbps) y limitar la IOPS de objetos de almacenamiento diferentes como archivos, LUN, volúmenes o SVM completas. La calidad de servicio adaptativa se utiliza para establecer una Suelo de IOPS (calidad de servicio mínima) y un techo (calidad de servicio máxima), que se ajustan de forma dinámica según la capacidad del almacén de datos y el espacio utilizado.

Los límites de rendimiento son útiles para controlar cargas de trabajo desconocidas o de prueba antes de la puesta en marcha para confirmar que no afectan a otras cargas de trabajo. También es posible utilizar estos

límites para limitar una carga de trabajo abusivas después de que se haya identificado. También admite niveles mínimos de servicio basados en IOPS para proporcionar un rendimiento constante para objetos SAN en ONTAP.

Con un almacén de datos NFS, se puede aplicar una política de calidad de servicio a todo el volumen FlexVol o a archivos de disco de máquina virtual (VMDK) individuales en el mismo. Con almacenes de datos VMFS (volúmenes compartidos de clúster [CSV] en Hyper-V) que utilizan LUN de ONTAP, puede aplicar las políticas de calidad de servicio al volumen de FlexVol que contiene las LUN o a las LUN individuales. Sin embargo, como ONTAP no sabe lo que es VMFS, no puede aplicar las políticas de calidad de servicio a archivos VMDK individuales. Cuando se utilizan VMware Virtual Volumes (VVol) con VSC 7.1 o posterior, puede establecer la calidad de servicio máxima en máquinas virtuales individuales usando el perfil de funcionalidad de almacenamiento.

Para asignar una política de calidad de servicio a un LUN, incluidos VMFS o CSV, puede obtener la SVM de ONTAP (que se muestra como `Vserver`), la ruta de LUN y el número de serie en el menú Storage Systems de la página de inicio de VSC. Seleccione el sistema de almacenamiento (SVM) y, a continuación, Related Objects > SAN. Use este enfoque cuando especifique la calidad de servicio mediante una de las herramientas de ONTAP.

Es posible establecer el límite máximo de rendimiento de calidad de servicio en un objeto en Mbps y IOPS. Si utiliza ambos, ONTAP aplica el primer límite al que se alcanza. Una carga de trabajo puede contener varios objetos y una política de calidad de servicio se puede aplicar a una o más cargas de trabajo. Cuando se aplica una política a varias cargas de trabajo, las cargas de trabajo comparten el límite total de la política. No se admiten los objetos anidados (por ejemplo, para un archivo dentro de un volumen, cada uno no puede tener su propia política). Los valores mínimos de calidad de servicio se pueden establecer solo en IOPS.

Distribución de almacenamiento

En esta sección se proporcionan prácticas recomendadas para el diseño de LUN, volúmenes y agregados en el almacenamiento.

LUN de almacenamiento

Para obtener un rendimiento, gestión y backup óptimos, NetApp recomienda las siguientes prácticas recomendadas en el diseño de LUN:

- Crear una LUN independiente para almacenar datos de base de datos y archivos de registro.
- Crear un LUN independiente para cada instancia donde almacenar los backups de registros de la base de datos de Oracle. Las LUN pueden formar parte del mismo volumen.
- Aprovisione las LUN con thin provisioning (deshabilite la opción Space Reservation) para los archivos de base de datos y los archivos de registro.
- Todos los datos de imágenes se alojan en las LUN de FC. Cree estas LUN en volúmenes de FlexVol distribuidos en los agregados propiedad de diferentes nodos de controladora de almacenamiento.

Para colocar las LUN en un volumen de almacenamiento, siga las directrices de la siguiente sección.

Volúmenes de almacenamiento

Para obtener un rendimiento y una gestión óptimos, NetApp recomienda las siguientes prácticas recomendadas en el diseño de volúmenes:

- Aísle bases de datos con consultas con gran volumen de I/o en volúmenes de almacenamiento separados.

- Es posible colocar los archivos de datos en un único LUN o en un volumen, pero se recomiendan varios volúmenes/LUN para lograr un mayor rendimiento.
- El paralelismo de I/o se puede obtener utilizando cualquier sistema de archivos compatible cuando se utilizan varias LUN.
- Coloque archivos de bases de datos y registros de transacciones en volúmenes independientes para aumentar la granularidad de recuperación.
- Considere la posibilidad de usar atributos de volumen como el tamaño automático, la reserva de Snapshot, la calidad de servicio, etc.

Agregados

Los agregados son los contenedores de almacenamiento principales para las configuraciones de almacenamiento de NetApp y contienen uno o varios grupos RAID compuestos tanto por discos de datos como por discos de paridad.

NetApp realizó varias pruebas de caracterización de las cargas de trabajo de I/o usando agregados dedicados y compartidos con archivos de datos y archivos de registro de transacciones separados. Las pruebas muestran que un agregado de gran tamaño con más unidades y grupos RAID (HDD o SSD) optimiza y mejora el rendimiento del almacenamiento y simplifica la gestión por dos motivos:

- Un agregado de gran tamaño pone a disposición de todos los archivos las capacidades de I/o de todas las unidades.
- Un agregado de gran tamaño permite hacer un uso más eficiente del espacio en disco.

Para una recuperación ante desastres efectiva, NetApp recomienda colocar la réplica asíncrona en un agregado que forma parte de un clúster de almacenamiento independiente del sitio de recuperación ante desastres y utilizar la tecnología SnapMirror para replicar contenido.

Para obtener un rendimiento óptimo del almacenamiento, NetApp recomienda tener disponible al menos un 10 % de espacio libre en un agregado.

Las directrices sobre la distribución de agregados de almacenamiento para sistemas AFF A300 (con dos bandejas de discos con 24 unidades) incluyen:

- Mantenga dos unidades de repuesto.
- Utilice la partición avanzada de discos para crear tres particiones en cada unidad: Raíz y datos.
- Use un total de 20 particiones de datos y dos particiones de paridad para cada agregado.

Mejores prácticas para backups

SnapCenter de NetApp se usa para backups de máquinas virtuales y bases de datos. NetApp recomienda las siguientes prácticas recomendadas de backup:

- Cuando se ponga en marcha SnapCenter para crear copias Snapshot para backups, desactive la programación Snapshot para la FlexVol que aloja máquinas virtuales y datos de aplicaciones.
- Cree una FlexVol dedicada para las LUN de arranque del host.
- Utilice una sola política de backup o similar para máquinas virtuales que tengan el mismo fin.
- Utilice una política de backup similar o una única por tipo de carga de trabajo; por ejemplo, utilice una política similar para todas las cargas de trabajo de base de datos. Utilice distintas políticas para bases de datos, servidores web, puestos de trabajo virtuales de usuario final, etc.

- Habilitar la verificación del backup en SnapCenter.
- Configurar el archivado de las copias Snapshot de backup en la solución de backup SnapVault de NetApp.
- Configurar la retención de los backups en el almacenamiento principal según la programación de archivado.

Mejores prácticas de infraestructura

Mejores prácticas en red

NetApp recomienda las siguientes prácticas recomendadas de red:

- Asegúrese de que su sistema incluye NIC físicas redundantes para el tráfico de producción y almacenamiento.
- Hay VLAN independientes para el tráfico iSCSI, NFS y SMB/CIFS entre recursos informáticos y de almacenamiento.
- Asegúrese de que el sistema incluye una VLAN dedicada para el acceso de los clientes al sistema de imágenes médicas.

Encontrará prácticas recomendadas adicionales para la conexión a redes en las guías de diseño y puesta en marcha de infraestructuras de FlexPod.

Prácticas recomendadas de computación

NetApp recomienda las siguientes prácticas recomendadas de computación:

- Asegúrese de que cada vCPU especificado es compatible con un núcleo físico.

Mejores prácticas de virtualización

NetApp recomienda las siguientes prácticas recomendadas de virtualización:

- Utilice VMware vSphere 6 o posterior.
- Establezca la capa de SO y BIOS del servidor host ESXi en Custom Controlled–High Performance.
- Crear backups durante las horas de menor actividad.

Mejores prácticas del sistema de imágenes médicas

Consulte las siguientes prácticas recomendadas y algunos requisitos de un sistema típico de imágenes médicas:

- No comprometa en exceso la memoria virtual.
- Asegúrese de que el número total de vCPU es igual al número de CPU físicas.
- Si tiene un entorno grande, se requieren VLAN dedicadas.
- Configuración de los equipos virtuales de base de datos con clústeres de alta disponibilidad dedicados.
- Asegúrese de que los VMDK de SO de la máquina virtual están alojados en un almacenamiento de nivel 1 rápido.
- Trabajar con el proveedor del sistema de imágenes médicas para identificar el mejor enfoque a la hora de preparar plantillas de equipos virtuales para una rápida implementación y mantenimiento.
- Las redes de gestión, almacenamiento y producción requieren la segregación de LAN para la base de

datos con VLAN aisladas para VMware vMotion.

- Utilice la tecnología de replicación basada en cabina de almacenamiento de NetApp llamada "SnapMirror" en lugar de replicación basada en vSphere.
- Use tecnologías de backup que aprovechen las API de VMware; los plazos de respaldo deben estar fuera del horario normal de producción.

Conclusión

Al ejecutar un entorno de imágenes médicas en FlexPod, su organización de atención médica puede esperar una mejora en la productividad del personal y una reducción en los gastos de capital y operativos. FlexPod proporciona una infraestructura convergente prevalidada y rigurosamente probada desde la alianza estratégica de Cisco y NetApp. Se ha diseñado y diseñado específicamente para proporcionar un sistema predecible de baja latencia y una alta disponibilidad. Este enfoque resulta en una experiencia de usuario superior y un tiempo de respuesta óptimo para los usuarios del sistema de imágenes médicas.

Los diferentes componentes de un sistema de imágenes médicas requieren almacenamiento de datos en sistemas de archivos SMB/CIFS, NFS, Ext4 y NTFS. Por lo tanto, su infraestructura debe proporcionar acceso a datos mediante protocolos NFS, SMB/CIFS y SAN. Los sistemas de almacenamiento de NetApp admiten estos protocolos desde una única cabina de almacenamiento.

Alta disponibilidad, eficiencia del almacenamiento, backups rápidos y programados basados en copias Snapshot, operaciones de restauración rápidas, replicación de datos para recuperación ante desastres y las funcionalidades de infraestructura de almacenamiento de FlexPod proporcionan un sistema de almacenamiento y gestión de datos líder en el sector.

Información adicional

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

- Guía de diseño de FlexPod Datacenter para IA/ML con Cisco UCS 480 ML para aprendizaje profundo

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_c480m5l_aiml_design.html"

- Infraestructura de centro de datos de FlexPod con VMware vSphere 6.7 U1, Cisco UCS de cuarta generación y NetApp AFF A-Series

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

- Breve descripción de la solución: Backup de bases de datos de Oracle en centros de datos FlexPod con SnapCenter

  "https://www.netapp.com/us/media/sb-3999.pdf"

- Centro de datos FlexPod con bases de datos RAC de Oracle en Cisco UCS y AFF A-Series de NetApp

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_orc12cr2_affaseries.ht

ml"

- Centro de datos FlexPod con Oracle RAC en Oracle Linux

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_orcrac_12c_bm.html"

- FlexPod para Microsoft SQL Server

  "https://flexpod.com/solutions/use-cases/microsoft-sql-server/"

- FlexPod de Cisco y NetApp

  "https://flexpod.com/"

- "Soluciones de NetApp para MongoDB" Breve descripción de la solución (se requiere inicio de sesión de NetApp)

  "https://fieldportal.netapp.com/content/734702"

- TR-4700: Complemento de SnapCenter para base de datos de Oracle

  "https://www.netapp.com/us/media/tr-4700.pdf"

- Documentación de productos de NetApp

  "https://www.netapp.com/us/documentation/index.aspx"

- FlexPod para soluciones de infraestructura de puestos de trabajo virtuales (VDI)

  "https://flexpod.com/solutions/use-cases/virtual-desktop-infrastructure/"

Infraestructura de puestos de trabajo virtuales

FlexPod Datacenter con Citrix Virtual Apps & Desktops 1912 LTSR y VMware vSphere 7 para un máximo de 6000 puestos

Jeff Nichols, Cisco Suresh Thoppay y NetApp Dre Jackson, NetApp

Este documento constituye la arquitectura y el diseño de una infraestructura de puestos de trabajo virtuales para hasta 6000 usuarios informáticos de usuario final. La solución se virtualiza en servidores blade Cisco UCS B200 M5 de quinta generación, arrancando VMware vSphere 7,01 Update 1 a través de FC SAN desde la cabina de almacenamiento A400 de AFF. Los puestos de trabajo virtuales utilizan Citrix Provisioning Server 1912 LTSR y Citrix RDS/Citrix Virtual Apps & Desktops 1912 LTSR, con una combinación de puestos de trabajo compartidos alojados en RDS (6000), puestos de trabajo virtuales Windows 10 alojados en pools y/o no persistentes (5000). Y escritorios virtuales Windows 10 alojados constantemente aprovisionados con Citrix Machine Creation Services (5000) para dar cabida a la población de usuarios. Cuando sea necesario, el documento proporciona recomendaciones de prácticas recomendadas y directrices sobre tamaño para las puestas en marcha de esta solución para los clientes.

"Centro de datos FlexPod con Citrix Virtual Apps Desktops 1912 LTSR y VMware vSphere 7 para un máximo de 6000 puestos"

FlexPod Datacenter con VMware Horizon View 7,10, VMware vSphere 6,7 U2, Cisco UCS Manager 4,0 y NetApp ONTAP 9,6 para un máximo de 6700 puestos

Vadim Lebedev, Cisco Suresh Thoppay, NetApp

Este documento ofrece una arquitectura de referencia y guía de diseño para una carga de trabajo de escritorio de 5000 puestos a 6000 puestos, un entorno informático de usuario final en el centro de datos FlexPod con Cisco UCS y AFF A300 de NetApp y el software de gestión de datos ONTAP de NetApp. La solución incluye sesiones RDS basadas en servidor de VMware Horizon Windows Server 2019, escritorios virtuales virtuales de Microsoft Windows 10 con clon completo persistente de VMware Horizon y puestos de trabajo virtuales de Microsoft Windows 10 con clonado instantáneo y sin persistencia en VMware vSphere 6.7U2

"FlexPod Datacenter con VMware Horizon View 7,10, VMware vSphere 6,7 U2, Cisco UCS Manager 4,0 y NetApp ONTAP 9,6 para un máximo de 6700 puestos"

Visualización de gráficos 3D con Citrix y NVIDIA - Documento técnico

En este documento se describe el rendimiento de Citrix XenDesktop en Citrix XenServer

con tarjetas NVIDIA Tesla P4, P6 y P40 en servidores Cisco UCS C240 M5 y B200 M5 con SPECviewperf 13.

"Visualización de gráficos 3D con Citrix y NVIDIA - Documento técnico"

FlexPod Datacenter con Citrix XenDesktop/XenApp 7,15 y VMware vSphere 6,5 Update 1 para 6000 puestos

Vadim Lebedev, Cisco Chris Rodriguez, NetApp

Este documento proporciona una arquitectura de referencia para un diseño de aplicaciones y puestos de trabajo virtuales utilizando Citrix XenApp/XenDesktop 7,15 integrado en Cisco UCS con un almacenamiento All Flash FAS (AFF) A300 de NetApp y la plataforma de hipervisor VMware vSphere ESXi 6,5.

El panorama de la virtualización de puestos de trabajo y aplicaciones cambia constantemente. Los nuevos servidores blade M5 de alto rendimiento Cisco UCS y la estructura unificada Cisco UCS, combinados como parte de la infraestructura contrastada de FlexPod y el almacenamiento AFF de última generación, dan como resultado una plataforma más compacta, más potente, más fiable y más eficiente.

"FlexPod Datacenter con Citrix XenDesktop/XenApp 7,15 y VMware vSphere 6,5 Update 1 para 6000 puestos"

FlexPod Datacenter con VMware Horizon View 7,3 y VMware vSphere 6,5 Update 1 con Cisco UCS Manager 3,2 para 5000 puestos

Ramesh Guduru, Cisco David Arnette, NetApp

Este documento proporciona una arquitectura de referencia, una guía de diseño y una puesta en marcha para un entorno informático de usuario final de hasta 5000 puestos para cargas de trabajo mixtas en el centro de datos de FlexPod con Cisco UCS y almacenamiento All Flash FAS (AFF) A300 de NetApp. La solución incluye sesiones alojadas de Remote Desktop Server basadas en servidor de VMware Horizon, escritorios virtuales persistentes de Microsoft Windows 10 de VMware Horizon y puestos de trabajo virtuales virtuales de clonado instantáneo de Microsoft Windows 10 no persistentes de VMware Horizon en VMware vSphere 6,5.

"FlexPod Datacenter con VMware Horizon View 7,3 y VMware vSphere 6,5 Update 1 con Cisco UCS Manager 3,2 para 5000 puestos"

FlexPod Datacenter con VMware Horizon View 7,10, VMware vSphere 6,7 U2, Cisco UCS Manager 4,0 y NetApp ONTAP 9,6 para un máximo de 6700 puestos

Vadim Lebedev, Cisco Suresh Thoppay, NetApp

Este documento constituye una guía de diseño y arquitectura de referencia para un

entorno informático de usuario final de 5000 puestos a 6000 puestos en el centro de datos FlexPod con Cisco UCS y AFF A300 de NetApp, así como el software de gestión de datos ONTAP de NetApp. La solución incluye sesiones RDS basadas en servidor de VMware Horizon Windows Server 2019, puestos de trabajo virtuales persistentes y con clonado completo de Microsoft Windows 10, y puestos de trabajo virtuales de Microsoft Windows 10 con clonado instantáneo y sin persistencia de VMware Horizon en VMware vSphere 6,7 U2.

"FlexPod Datacenter con VMware Horizon View 7,10, VMware vSphere 6,7 U2, Cisco UCS Manager 4,0 y NetApp ONTAP 9,6 para un máximo de 6700 puestos"

Aplicaciones modernas

Centro de datos FlexPod para IA y ML combinados con Cisco UCS 480 ML para aprendizaje profundo: Diseño

Haseeb Niazi, Cisco Arvind Ramakrishnan, NetApp

Este documento proporciona detalles de diseño sobre la integración de la plataforma Cisco UCS C480 ML M5 en la solución de centro de datos FlexPod para ofrecer un enfoque unificado para proporcionar funcionalidades de IA y AA en la infraestructura convergente. Al ofrecer a los clientes la capacidad de gestionar servidores que combinan capacidades de IA y ML con las herramientas que utilizan para administrar sistemas FlexPod tradicionales, la sobrecarga administrativa, así como el coste de poner en marcha una plataforma de aprendizaje profundo se reduce considerablemente. El diseño presentado en este CVD también incluye otras plataformas Cisco UCS, como un servidor C220 M5 con dos GPU T4 de NVIDIA y un servidor C240 M5 equipado con dos tarjetas PCIe NVIDIA V100 32GB como opciones adicionales para cargas de trabajo simultáneas de IA y ML.

"Centro de datos FlexPod para IA y ML combinados con Cisco UCS 480 ML para aprendizaje profundo: Diseño"

Ponga en marcha el complemento Trident CSI de NetApp en Cisco Container Platform con FlexPod

Este documento proporciona procedimientos paso a paso para poner en marcha el complemento Trident Container Storage Interface (CSI) de NetApp en un clúster de inquilinos de Kubernetes de la plataforma de contenedores de Cisco en una solución FlexPod.

"Ponga en marcha el complemento Trident CSI de NetApp en Cisco Container Platform con FlexPod"

FlexPod Datacenter para OpenShift Container Platform 4: Puesta en marcha

Haseeb Niazi, Cisco Alan Cowles, NetApp

Red Hat OpenShift es una plataforma de contenedores de Kubernetes preparada para la empresa que permite gestionar implementaciones de nube híbrida y multinube. Red Hat OpenShift Container Platform incluye todo lo necesario para la nube híbrida, contenedores empresariales y desarrollo e implementaciones de Kubernetes. Incluye un sistema operativo Linux de clase empresarial, tiempo de ejecución de contenedores, redes, supervisión, registro de contenedores, soluciones de autenticación y autorización.

La combinación de Red Hat OpenShift con la solución FlexPod Datacenter puede simplificar la

implementación y la gestión de la infraestructura de contenedores. Los clientes pueden beneficiarse de la eficiencia mejorada, una mejor protección de datos, un riesgo menor y la flexibilidad necesaria para escalar esta pila de infraestructura de clase empresarial de alta disponibilidad para adaptarse a nuevos requisitos del negocio. El enfoque de solución convergente prevalidada ayuda a las organizaciones a lograr la velocidad, flexibilidad y escalado necesarias para todas sus iniciativas de modernización de aplicaciones y transformación digital.

"FlexPod Datacenter para OpenShift Container Platform 4: Puesta en marcha"

FlexPod Datacenter con Docker Enterprise Edition para la gestión de contenedores

Muhammad Afzal, Cisco John George, Cisco Amit Borulkar, NetApp Uday Shetty y Docker

Docker es la plataforma de contenedores de software líder en el mundo para que los desarrolladores y las operaciones TECNOLÓGICAS creen, distribuyan y ejecuten aplicaciones distribuidas en cualquier lugar. Con la arquitectura de microservicios que da forma a la próxima generación de TI, las empresas con grandes inversiones en aplicaciones monolíticas están encontrando formas de adoptar Docker como estrategia para modernizar sus arquitecturas de aplicaciones y mantener a la organización competitiva y rentable. La creación de contenedores proporciona la agilidad, el control y la portabilidad que los desarrolladores y las operaciones de TI necesitan para crear e implementar aplicaciones en cualquier infraestructura. La plataforma Docker permite que las aplicaciones distribuidas se compongan fácilmente en un contenedor de aplicaciones ligero que puede cambiar de forma dinámica pero sin interrupciones. Esta funcionalidad hace que las aplicaciones se transporten entre entornos de desarrollo, prueba y producción que se ejecutan en máquinas físicas o virtuales de forma local, en centros de datos y a través de las redes de distintos proveedores de servicios cloud.

"FlexPod Datacenter con Docker Enterprise Edition para la gestión de contenedores"

FlexPod Datacenter para OpenShift Container Platform 4: Diseño

Haseeb Niazi, Cisco Alan Cowles, NetApp

Cisco y NetApp se han asociado para ofrecer una serie de soluciones FlexPod que permiten crear plataformas estratégicas de centros de datos. La solución FlexPod proporciona una arquitectura integrada que incorpora prácticas recomendadas para informática, almacenamiento y diseño de red, lo que minimiza los riesgos de LA TECNOLOGÍA mediante la validación de la arquitectura integrada para garantizar la compatibilidad entre varios componentes. La solución también soluciona los problemas DE TI al proporcionar indicaciones de diseño documentadas, directrices para la puesta en marcha y soporte que se puede utilizar en varias etapas (planificación, diseño e implementación) de una implementación.

"FlexPod Datacenter para OpenShift Container Platform 4: Diseño"

Visualización de gráficos 3D con VMware y NVIDIA en Cisco UCS: Whitepaper

Este documento describe el rendimiento del hipervisor ESXi de VMware y VMware Horizon con la solución NVIDIA Tesla P4, P6 y P40 en servidores en rack Cisco UCS C240 M5 y servidores blade B200 M5.

"Visualización de gráficos 3D con VMware y NVIDIA en Cisco UCS: Whitepaper"

Visualización de gráficos 3D con Citrix y NVIDIA - Documento técnico

En este documento se describe el rendimiento de Citrix XenDesktop en Citrix XenServer con tarjetas NVIDIA Tesla P4, P6 y P40 en servidores Cisco UCS C240 M5 y B200 M5 con SPECviewperf 13.

"Visualización de gráficos 3D con Citrix y NVIDIA - Documento técnico"

FlexPod Express

Guía de diseño de FlexPod Express con Cisco UCS C-Series y la serie AFF C190 de NetApp

Diseño de la arquitectura NVA-1139: FlexPod Express con Cisco UCS C-Series y AFF C190 Series de NetApp

Savita Kumari, NetApp

En colaboración con: 

Las tendencias en el sector señalan una gran transformación de los centros de datos hacia una infraestructura compartida y cloud computing. Además, las organizaciones buscan una solución sencilla y eficaz para oficinas remotas y sucursales que utilicen la tecnología con la que están familiarizados en su centro de datos.

FlexPod Express es una arquitectura de centro de datos prediseñada con las mejores prácticas que se basa en Cisco Unified Computing System (Cisco UCS), la familia de switches Cisco Nexus y los sistemas AFF de NetApp. Los componentes de FlexPod Express se asemejan a los homólogos de FlexPod Datacenter, lo que permite sinergias de gestión en un entorno completo de infraestructura TECNOLÓGICA a una escala menor. FlexPod Datacenter y FlexPod Express son plataformas óptimas para virtualización y para sistemas operativos con configuración básica y cargas de trabajo empresariales.

"Siguiente: Resumen del programa."

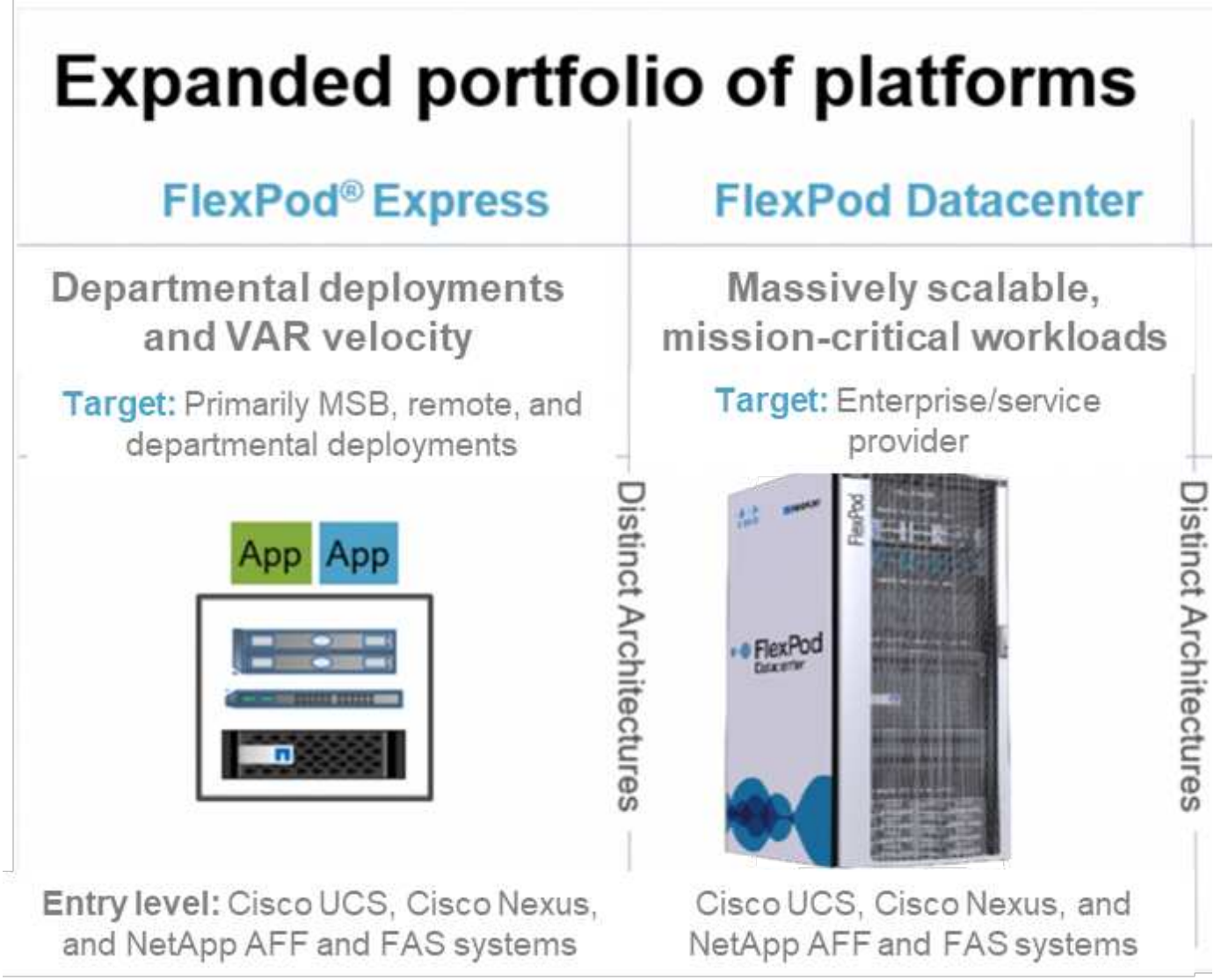
Resumen del programa

Cartera de infraestructura convergente de FlexPod

Las arquitecturas de referencia de FlexPod se proporcionan como diseños validados por Cisco (CVD) o como arquitecturas verificadas de NetApp (NVA). Se permiten las desviaciones basadas en los requisitos del cliente de un CVD o NVA determinado si dichas variaciones no dan como resultado la puesta en marcha de configuraciones no compatibles.

Como se muestra en la siguiente figura, la cartera de FlexPod incluye las siguientes soluciones: FlexPod Express y FlexPod Datacenter.

- **FlexPod Express** es una solución de gama básica con tecnologías de Cisco y NetApp.
- **FlexPod Datacenter** proporciona una base multiuso óptima para diversas cargas de trabajo y aplicaciones.



Programa Arquitectura validada por NetApp

El programa Arquitectura verificada de NetApp ofrece a los clientes una arquitectura verificada para soluciones NetApp. Una solución NVA tiene las siguientes cualidades:

- Ha sido probada a conciencia
- Tiene naturaleza prescriptiva
- Minimiza los riesgos de implementación
- Acelera el plazo de comercialización esta guía detalla el diseño de FlexPod Express con VMware vSphere.

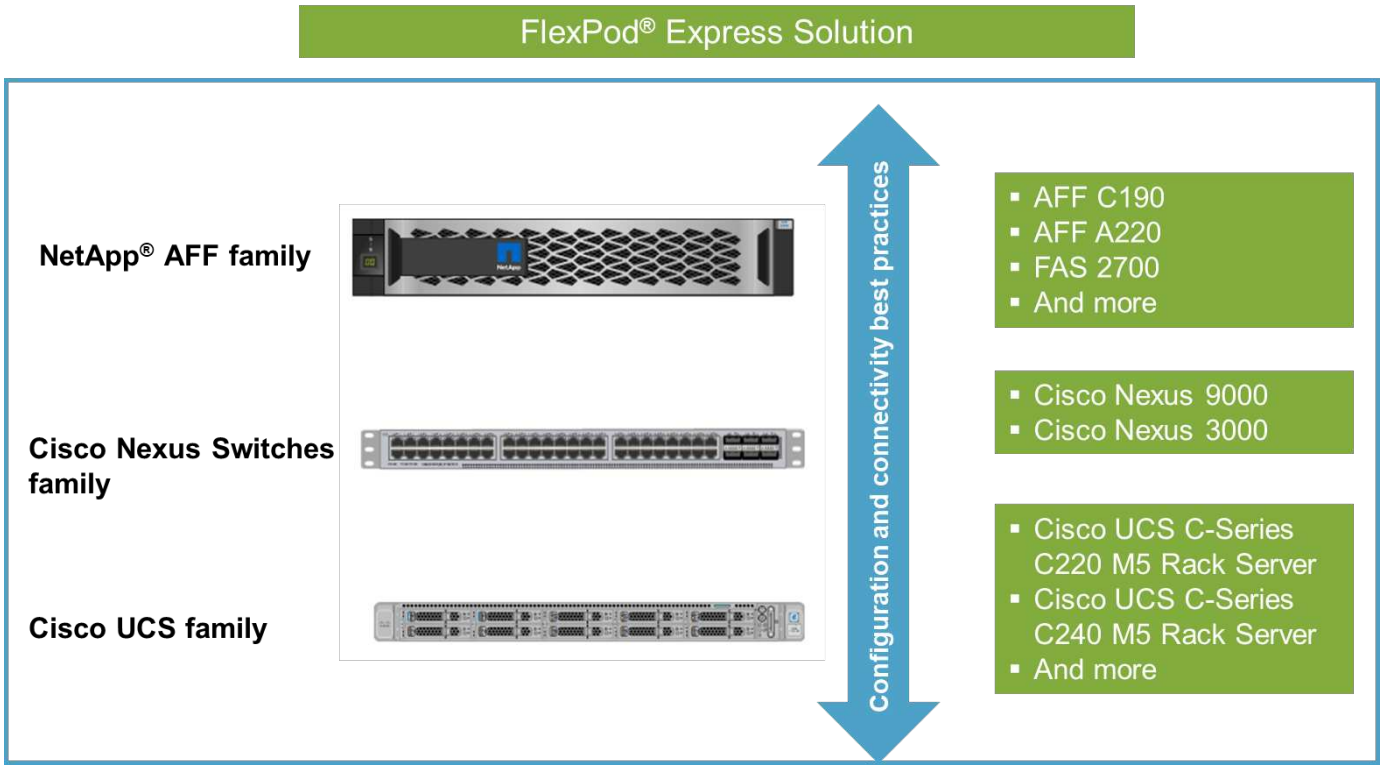
Además, este diseño aprovecha el nuevo sistema AFF C190, que ejecuta el software ONTAP 9.6 de NetApp, los conmutadores Cisco Nexus 31108 y los servidores Cisco UCS C220 M5 como nodos de hipervisor.

Descripción general de la solución

FlexPod Express está diseñado para ejecutar cargas de trabajo de virtualización mixtas. Está pensado para oficinas remotas, sucursales y para pequeñas y medianas empresas. También es perfecto para empresas más grandes que deseen implementar una solución dedicada para un fin específico. Esta nueva solución para FlexPod Express añade nuevas tecnologías, como ONTAP 9.6 de NetApp, el sistema AFF C190 de NetApp y

VMware vSphere 6.7U2.

La siguiente figura muestra los componentes de hardware incluidos en la solución FlexPod Express.

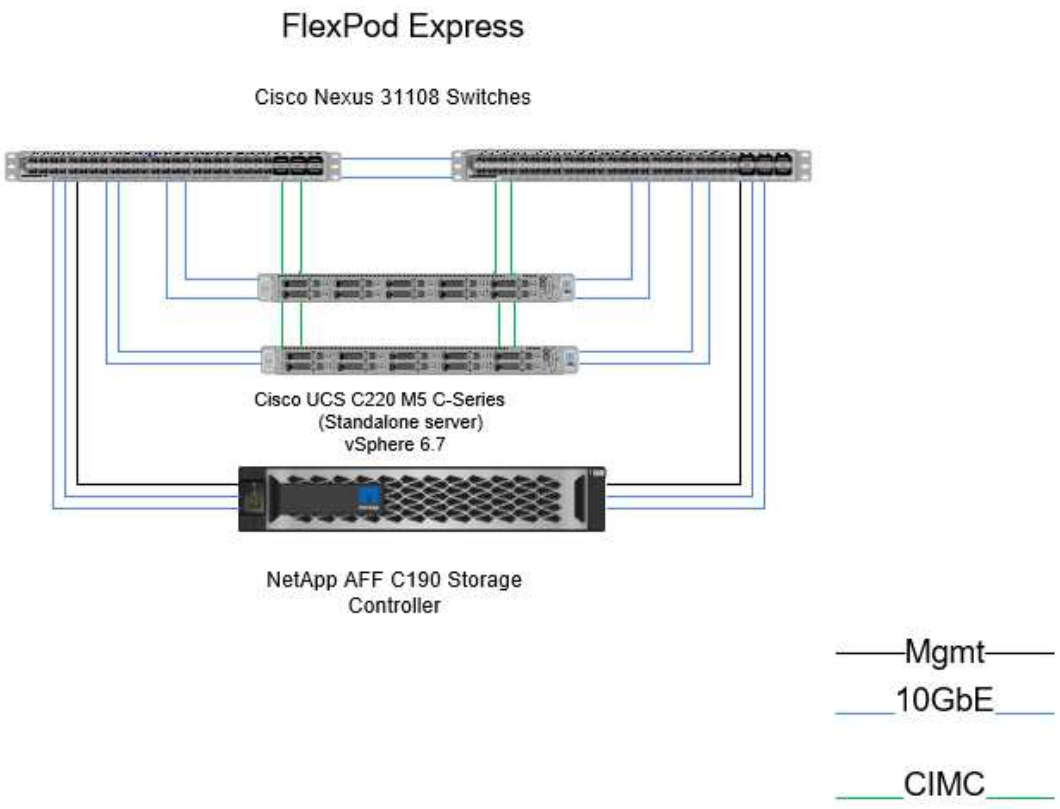


Público objetivo

Este documento está dirigido a usuarios que desean aprovechar una infraestructura creada para proporcionar eficiencia TECNOLÓGICA y posibilitar la innovación EN tecnología. El público de este documento incluye, sin limitarse a ellos, ingenieros de ventas, consultores de campo, personal de servicios profesionales, gestores DE TECNOLOGÍA, ingenieros de partners y clientes.

Tecnología de soluciones

Esta solución aprovecha las últimas tecnologías de NetApp, Cisco y VMware. Incluye el nuevo sistema AFF C190 de NetApp, que ejecuta el software ONTAP 9.6, los switches Cisco Nexus 31108 duales y los servidores de montaje en rack Cisco UCS C220 M5 que ejecutan VMware vSphere 6.7U2. Esta solución validada, como se muestra en la siguiente figura, utiliza tecnología Ethernet de 10 GB (10 GbE). También se ofrece orientación sobre cómo escalar agregando dos nodos de hipervisor a la vez para que la arquitectura FlexPod Express pueda adaptarse a las cambiantes necesidades empresariales de una organización.



"Siguiente: Requisitos tecnológicos."

Requisitos tecnológicos

FlexPod Express requiere una combinación de componentes de hardware y software que depende de la velocidad del hipervisor y de la red seleccionados. Además, FlexPod Express puede establecer los componentes de hardware necesarios para añadir nodos de hipervisor en unidades de dos.

Requisitos de hardware

Independientemente del hipervisor elegido, todas las configuraciones exprés de FlexPod utilizan el mismo hardware. Por lo tanto, aunque cambien los requisitos del negocio, puede utilizar un hipervisor diferente en el mismo hardware de FlexPod Express.

En la siguiente tabla se enumeran los componentes de hardware necesarios para esta configuración exprés de FlexPod e implantar esta solución. Los componentes de hardware que se usan en cualquier implementación de la solución pueden variar en función de las necesidades del cliente.

Hardware subyacente	Cantidad
Clúster de 2 nodos C190 de AFF	1
Servidor Cisco UCS C220 M5	2
Switch Cisco Nexus 31108	2

Hardware subyacente	Cantidad
Tarjeta de interfaz virtual (VIC) Cisco UCS 1457 para el servidor de montaje en rack Cisco UCS C220 M5	2

Requisitos de software

En la siguiente tabla se enumeran los componentes de software necesarios para implementar las arquitecturas de la solución FlexPod Express.

De NetApp	Versión	Detalles
Controladora de gestión integrada de Cisco (CIMC)	4.0.4	Para servidores en rack C220 M5
Cisco NX-OS	7.0(3)I7(6)	Para los switches Cisco Nexus 31108
ONTAP de NetApp	9.6	Para controladoras AFF C190 de NetApp

En la siguiente tabla se muestra el software necesario para todas las implementaciones de VMware vSphere en FlexPod Express.

De NetApp	Versión
Dispositivo VMware vCenter Server	6.7U2
VMware vSphere ESXi	6.7U2
Complemento VAAI de NetApp para ESXi	1.1.2
Consola de almacenamiento virtual de NetApp	9.6

"Siguiente: Opciones de diseño."

Opciones de diseño

Las tecnologías enumeradas en esta sección se han elegido durante la fase de diseño de la arquitectura. Cada tecnología cumple un propósito específico en la solución de infraestructura Express de FlexPod.

Serie AFF C190 de NetApp con ONTAP 9.6

Esta solución aprovecha dos de los productos más recientes de NetApp: El sistema AFF C190 de NetApp y el software ONTAP 9.6.

Sistema C190 de AFF

El grupo objetivo son los clientes que quieren modernizar su infraestructura TECNOLÓGICA con tecnología all-flash a un precio asequible. El sistema AFF C190 incluye el nuevo ONTAP 9.6 y las licencias de paquetes flash, lo que significa que las siguientes funciones están integradas:

- CIFS, NFS, iSCSI y FCP
- Software de replicación de datos SnapMirror de NetApp, software de backup SnapVault de NetApp,

software de recuperación de datos SnapRestore de NetApp, suite de productos de software de gestión del almacenamiento SnapManager de NetApp y software SnapCenter de NetApp

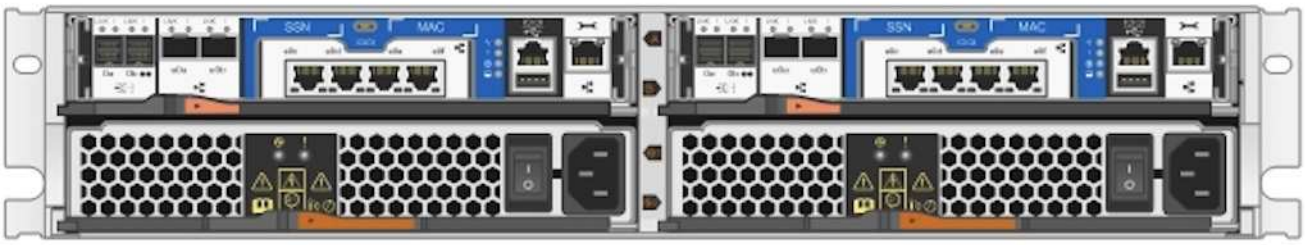
- Tecnología FlexVol
- Deduplicación, compresión y compactación
- Aprovisionamiento ligero
- Calidad de servicio del almacenamiento
- Tecnología RAID DP de NetApp
- Tecnología Snapshot de NetApp
- FabricPool

Las siguientes figuras muestran las dos opciones para la conectividad de host.

La siguiente figura ilustra los puertos UTA 2 donde se puede insertar el módulo SFP+.



En la siguiente figura se muestran los puertos 10GBASE-T para la conexión a través de cables Ethernet RJ-45 convencionales.



Para la opción de puerto 10GBASE-T, debe tener un switch de enlace ascendente basado en 10GBASE-T.

El sistema C190 de AFF se ofrece exclusivamente con SSD de 960 GB. Puede elegir entre cuatro fases de expansión:

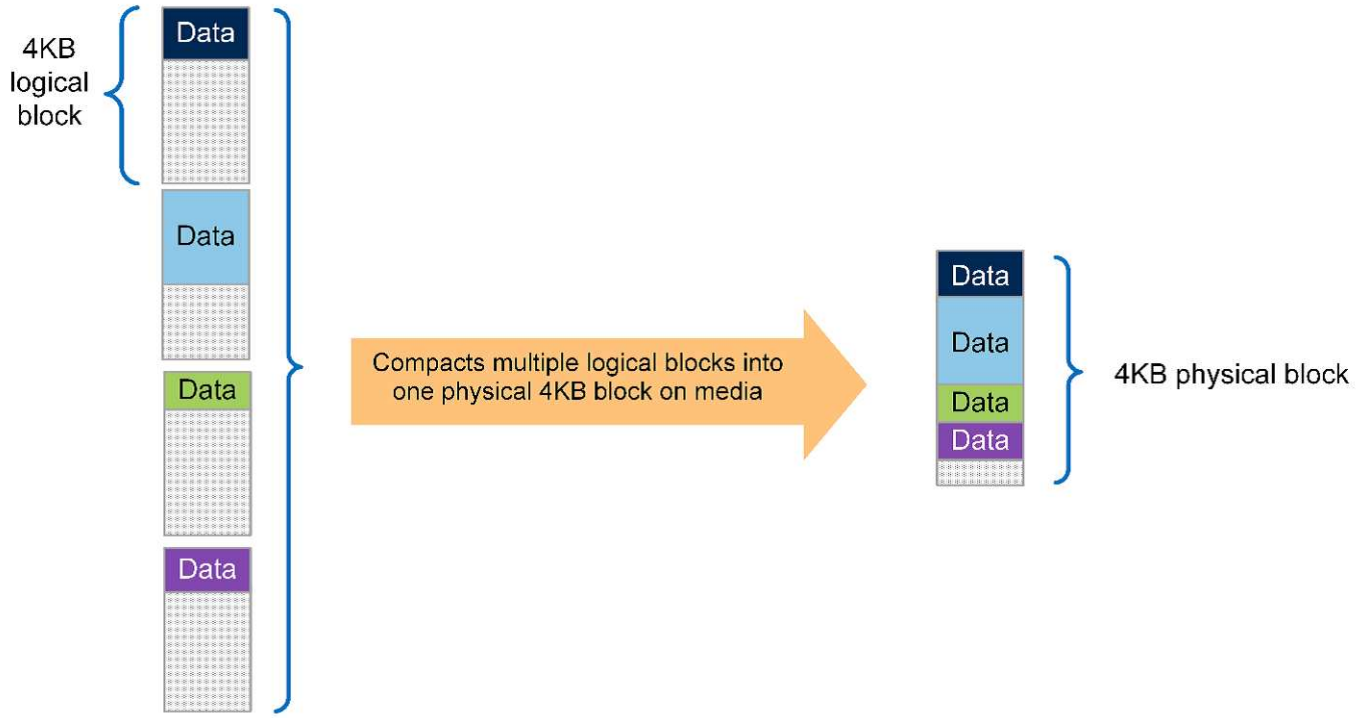
- 8x 960 GB
- 12x 960 GB
- 18x 960 GB
- 24x 960 GB

Para obtener toda la información sobre el sistema de hardware C190 de AFF, consulte "Página de la cabina all-flash C190 de AFF de NetApp".

Software ONTAP 9.6

Los sistemas AFF C190 de NetApp utilizan el nuevo software de gestión de datos ONTAP 9.6. ONTAP 9.6 es el software de gestión de datos empresariales líder del sector. Combina nuevos niveles de simplicidad y flexibilidad con potentes funcionalidades de gestión de datos, eficiencias de almacenamiento e integración del cloud líder.

ONTAP 9.6 cuenta con varias funciones que resultan adecuadas para la solución FlexPod Express. Lo más importante es el compromiso de NetApp con la eficiencia del almacenamiento, que puede ser una de las funciones más importantes para implementaciones pequeñas. Las características distintivas de la eficiencia del almacenamiento de NetApp, como la deduplicación, la compresión, la compactación y el thin provisioning, están disponibles en ONTAP 9.6. El sistema WAFL de NetApp siempre escribe bloques de 4 KB; por tanto, la compactación combina varios bloques en un bloque de 4 KB cuando los bloques no utilizan el espacio asignado de 4 KB. La siguiente figura ilustra este proceso.



ONTAP 9.6 ahora admite un tamaño de bloque de 512 bytes opcional para volúmenes NVMe. Esta funcionalidad funciona bien con el sistema de archivos de máquina virtual (VMFS) de VMware, que utiliza de forma nativa un bloque de 512 bytes. Puede permanecer con el tamaño predeterminado de 4K o, opcionalmente, establecer el tamaño de bloque de 512 bytes.

Entre otras mejoras de las funciones de ONTAP 9.6 se incluyen:

- **Cifrado de agregados de NetApp (NAE).** NAE asigna claves a nivel de agregado, con lo que se cifran todos los volúmenes del agregado. Esta función permite cifrar y deduplicar los volúmenes en el nivel de agregado.
- **Mejora de volumen de ONTAP FlexGroup de NetApp**. En ONTAP 9.6, se puede cambiar fácilmente el nombre de un volumen de FlexGroup. No es necesario crear un nuevo volumen al que migrar los datos. El tamaño del volumen también se puede reducir mediante System Manager o CLI de ONTAP.
- **Mejora de FabricPool.** ONTAP 9.6 añadió compatibilidad adicional para almacenes de objetos como niveles de nube. También se añadió compatibilidad con Google Cloud y Alibaba Cloud Object Storage Service (OSS). FabricPool admite varios almacenes de objetos, incluidos AWS S3, Azure Blob, el almacenamiento de objetos IBM Cloud y el software de almacenamiento basado en objetos StorageGRID

de NetApp.

- **Mejora de SnapMirror.** en ONTAP 9.6, una nueva relación de replicación de volúmenes se cifra de forma predeterminada antes de salir de la matriz de origen y se descifra en el destino de SnapMirror.

Serie Nexus 3000 de Cisco

El Cisco Nexus 31108PC-V es un switch de superior rack (Tor) basado en 10 Gbps SFP+ con 48 puertos SFP+ y 6 puertos QSFP28. Cada puerto SFP+ puede funcionar en 100 Mbps, 10 Gbps y cada puerto QSFP28 puede funcionar en modo nativo de 100 Gbps o 40 Gbps o en modo 4x 10 Gbps, lo que ofrece opciones flexibles de migración. Este conmutador es un verdadero conmutador sin PHY optimizado para una baja latencia y bajo consumo de energía.

La especificación Cisco Nexus 31108PC-V incluye los siguientes componentes:

- Capacidad de conmutación de 2,16 Tbps y velocidad de reenvío de hasta 1,2 Tbps para 31108PC-V.
- 48 puertos SFP admiten 1 y 10 Gigabit Ethernet (10GbE); los seis puertos QSFP28 admiten 4 x 10 GbE o 40 GbE cada uno o 100 GbE

La siguiente figura muestra el switch Cisco Nexus 31108PC-V.



Para obtener más información sobre los switches Cisco Nexus 31108PC-V, consulte "Hoja de datos de los conmutadores Cisco Nexus 3172PQ, 3172TQ, 3172PQ-32T, 3172PQ-XL y 3172TQ-XL".

Cisco UCS C-Series

Se eligió el servidor en rack Cisco UCS C-Series para FlexPod Express porque sus numerosas opciones de configuración permiten adaptarse a requisitos específicos en una puesta en marcha de FlexPod Express.

Los servidores de montaje en rack Cisco UCS C-Series ofrecen informática unificada en un factor de forma estándar del sector para reducir el TCO y aumentar la agilidad.

Los servidores de montaje en rack Cisco UCS C-Series ofrecen las siguientes ventajas:

- Un punto de entrada independiente del factor de forma en Cisco UCS
- Puesta en marcha de aplicaciones simplificada y rápida
- Ampliación de las innovaciones y ventajas de la informática unificada a los servidores en rack
- Mayor elección para el cliente gracias a sus ventajas únicas en un paquete de rack conocido



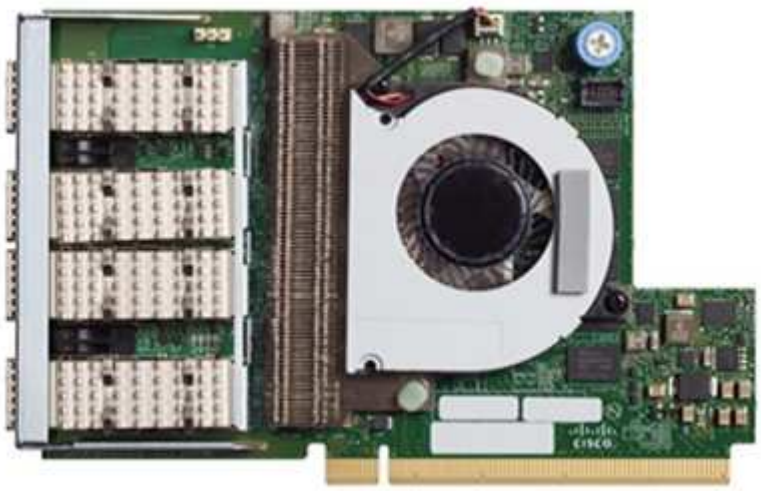
El servidor de montaje en rack Cisco UCS C220 M5, mostrado en la figura anterior, se encuentra entre la

infraestructura empresarial y los servidores de aplicaciones más versátiles y generales del sector. Se trata de un servidor en rack de dos sockets de alta densidad que ofrece un rendimiento y una eficiencia líderes en el sector para una amplia gama de cargas de trabajo, incluidas aplicaciones de virtualización, colaboración y con configuración básica. Los servidores en rack Cisco UCS C-Series se pueden implementar como servidores independientes o como parte de Cisco UCS para aprovechar las innovaciones informáticas unificadas basadas en estándares de Cisco que ayudan a reducir el coste total de propiedad de los clientes y a aumentar la agilidad empresarial.

Para obtener más información sobre los servidores C220 M5, consulte "Hoja de datos del servidor en rack Cisco UCS C220 M5".

Conectividad Cisco UCS VIC 1457 para servidores C220 M5

El adaptador Cisco UCS VIC 1457 mostrado en la siguiente figura es una LAN modular de factor de forma pequeño y conectable (SFP28) de cuatro puertos en la tarjeta madre (mLOM) diseñada para la generación M5 de servidores Cisco UCS C-Series. La tarjeta admite Ethernet o FCoE de 10 Gbps. La tarjeta puede presentar interfaces compatibles con los estándares PCIe al host y pueden configurarse dinámicamente como NIC o HBA.



Para obtener toda la información sobre el adaptador Cisco UCS VIC 1457, consulte "Especificaciones técnicas de la serie 1400 de tarjeta de interfaz virtual Cisco UCS".

VMware vSphere 6.7U2

VMware vSphere 6.7U2 es una de las opciones de hipervisor para utilizar con FlexPod Express. VMware vSphere permite a las organizaciones reducir su huella de potencia y refrigeración a la vez que confirman que la capacidad de computación adquirida se ha aprovechado al máximo. Además, VMware vSphere permite la protección contra fallos de hardware (alta disponibilidad de VMware o ha de VMware) y el equilibrio de carga de recursos informáticos en un clúster de hosts vSphere (planificador de recursos distribuidos de VMware en modo de mantenimiento o DRS-MM de VMware).

Dado que reinicia únicamente el kernel, VMware vSphere 6.7U2 permite a los clientes efectuar un arranque rápido, cargando vSphere ESXi sin reiniciar el hardware. El cliente vSphere 6.7U2 vSphere (cliente basado en HTML5) tiene algunas mejoras nuevas como Developer Center con Code Capture y API Explore. Con Code Capture, puede registrar sus acciones en vSphere Client para proporcionar una salida de código simple y utilizable. VSphere 6.7U2 también contiene nuevas funciones como DRS en modo de mantenimiento (DRS-MM).

VMware vSphere 6.7U2 ofrece las siguientes funciones:

- VMware utiliza el modelo de puesta en marcha externo de VMware Platform Services Controller (PSC).

> A partir de la siguiente versión principal de vSphere, PSC externo no será una opción disponible.

- Nueva compatibilidad de protocolos para realizar backups y restaurar un dispositivo de vCenter Server. Introducción de NFS y SMB como opciones de protocolo admitidas, hasta un total de 7 (HTTP, HTTPS, FTP, FTPS, SCP, NFS y SMB) al configurar una instancia de vCenter Server para operaciones de backup o restauración basadas en archivos.
- Nuevo funcionalmente al utilizar la biblioteca de contenido. La sincronización de una plantilla de máquina virtual nativa entre bibliotecas de contenido ahora está disponible cuando vCenter Server está configurado para el modo vinculado mejorado.
- Actualice a la "Página de complementos de cliente".
- VMware vSphere Update Manager también añade mejoras al cliente vSphere. Puede realizar el cumplimiento de la comprobación de asociación y solucionar acciones desde una sola pantalla.

Para obtener más información sobre VMware vSphere 6.7 U2, consulte "Página del blog de VMware vSphere".

Para obtener más información sobre las actualizaciones de VMware vCenter Server 6.7 U2, consulte "Notas de la versión".

> Aunque esta solución se validó con vSphere 6.7U2, admite cualquier versión de vSphere calificada con los otros componentes del "Herramienta de matriz de interoperabilidad de NetApp (IMT)". NetApp recomienda poner en marcha la siguiente versión de vSphere para sus correcciones y funciones mejoradas.

Arquitectura de arranque

Entre las opciones admitidas para la arquitectura de arranque Express de FlexPod se incluyen las siguientes:

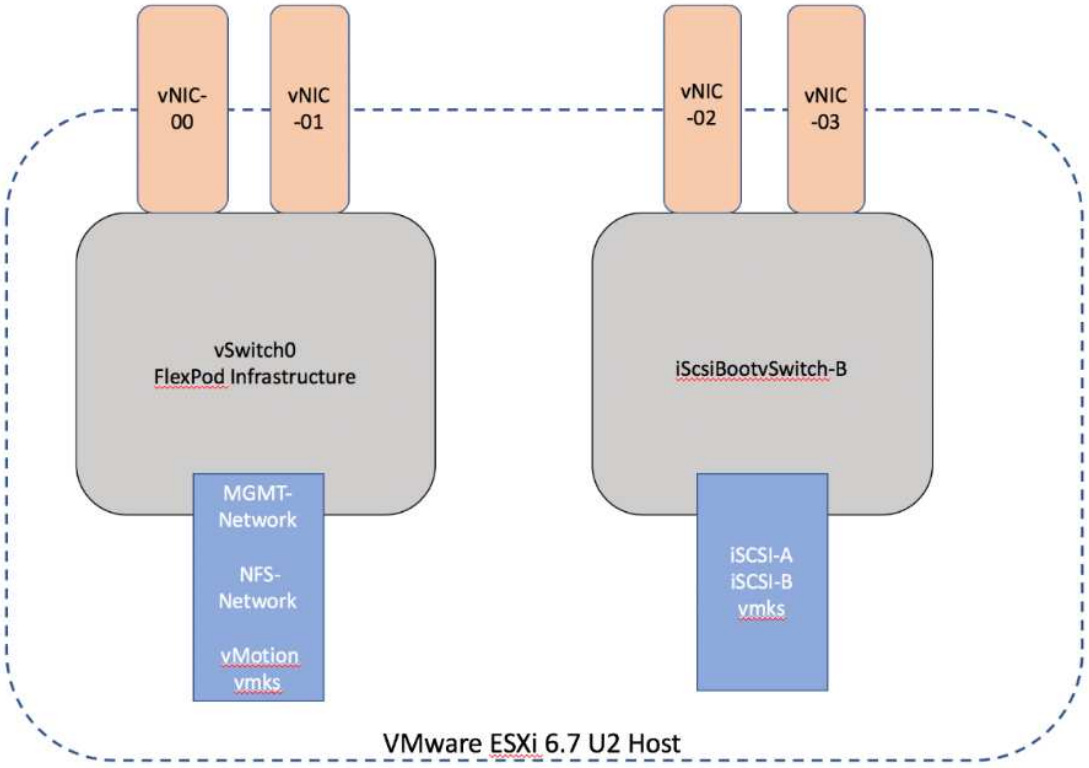
- LUN SAN iSCSI
- Tarjeta SD Cisco FlexFlash
- Disco local

El centro de datos FlexPod se arranca desde LUN de iSCSI; por tanto, la administración de la solución se mejora mediante el uso también del arranque iSCSI para FlexPod Express.

Distribución de la tarjeta de interfaz de red virtual del host ESXi

Cisco UCS VIC 1457 tiene cuatro puertos físicos. Esta validación de solución incluye estos cuatro puertos físicos en el uso del host ESXi. Si tiene un número menor o mayor de NIC, puede tener diferentes números VMNIC.

En una implementación de arranque iSCSI, el arranque iSCSI requiere tarjetas de interfaz de red virtual (vNIC) independientes para el arranque iSCSI. Estos vNIC utilizan la VLAN iSCSI de la estructura adecuada como VLAN nativa y están conectados a los vSwitch de arranque iSCSI, como se muestra en la siguiente figura.



"Siguiente: Conclusión."

Conclusión

El diseño validado FlexPod Express es una solución sencilla y efectiva que utiliza componentes líderes en el sector. Al escalar y proporcionar opciones para la plataforma del hipervisor, FlexPod Express se puede adaptar a las necesidades específicas del negocio. FlexPod Express se ha diseñado para pequeñas y medianas empresas, oficinas remotas y sucursales, y otras empresas que requieren soluciones dedicadas.

"Siguiente: Dónde encontrar información adicional."

Dónde encontrar información adicional

Para obtener más información sobre la información descrita en este documento, consulte los siguientes documentos y sitios web:

- Centro de documentación de los sistemas AFF y FAS

  "https://docs.netapp.com/platstor/index.jsp"

- Recursos de documentación de AFF

  "https://www.netapp.com/us/documentation/all-flash-fas.aspx"

- Guía de puesta en marcha de FlexPod Express con VMware vSphere 6.7 y AFF C190 de NetApp (en curso)

- Documentación de NetApp

  "https://docs.netapp.com"

Guía de puesta en marcha de FlexPod Express con Cisco UCS C-Series y la serie AFF C190 de NetApp

NVA-1142-PUESTA en MARCHA: FlexPod Express con Cisco UCS C-Series y AFF C190 Series de NetApp: Puesta en marcha NVA

Savita Kumari, NetApp

Las tendencias del sector indican que se está produciendo una gran transformación de los centros de datos hacia la infraestructura compartida y el cloud computing. Además, las organizaciones buscan una solución sencilla y eficaz para oficinas remotas y sucursales que utilicen la tecnología con la que estén familiarizados en su centro de datos.

FlexPod® Express es una arquitectura de centro de datos diseñada previamente y basada en el Cisco Unified Computing System (Cisco UCS), la familia de switches Cisco Nexus y las tecnologías de almacenamiento de NetApp®. Los componentes de un sistema FlexPod Express se asemejan a los del centro de datos FlexPod, lo que permite sinergias de gestión en todo el entorno de infraestructura DE TI a una escala menor. FlexPod Datacenter y FlexPod Express son plataformas óptimas para virtualización y para sistemas operativos con configuración básica y cargas de trabajo empresariales.

El centro de datos de FlexPod y FlexPod Express proporcionan una configuración básica y cuentan con la flexibilidad necesaria para ajustar su tamaño y optimizarse con el objetivo de acomodar distintos casos de uso y requisitos. Los clientes existentes de FlexPod Datacenter pueden gestionar su sistema FlexPod Express con las herramientas a las que están acostumbrados. Los nuevos clientes de FlexPod Express pueden realizar fácilmente la transición a la gestión del centro de datos FlexPod a medida que crece su entorno.

FlexPod Express es una base de infraestructura óptima para oficinas remotas y sucursales y para pequeñas y medianas empresas. También es una solución óptima para los clientes que desean proporcionar infraestructura para cargas de trabajo dedicadas.

FlexPod Express proporciona una infraestructura fácil de gestionar que es adecuada para casi cualquier carga de trabajo.

Descripción general de la solución

Esta solución FlexPod Express forma parte del programa de infraestructura convergente de FlexPod.

Programa de infraestructura convergente FlexPod

Las arquitecturas de referencia FlexPod se proporcionan como diseños validados por Cisco (CVD) o como arquitecturas verificadas por NetApp (NVA). Se permiten las desviaciones basadas en los requisitos de los clientes de un CVD o NVA determinado si estas variaciones no crean una configuración incompatible.

El programa FlexPod incluye dos soluciones: FlexPod Express y FlexPod Datacenter.

- **FlexPod Express.** ofrece a los clientes una solución de gama básica con tecnologías de Cisco y NetApp.
- **FlexPod Datacenter.** proporciona una base multiuso óptima para diversas cargas de trabajo y aplicaciones.



Programa Arquitectura validada por NetApp

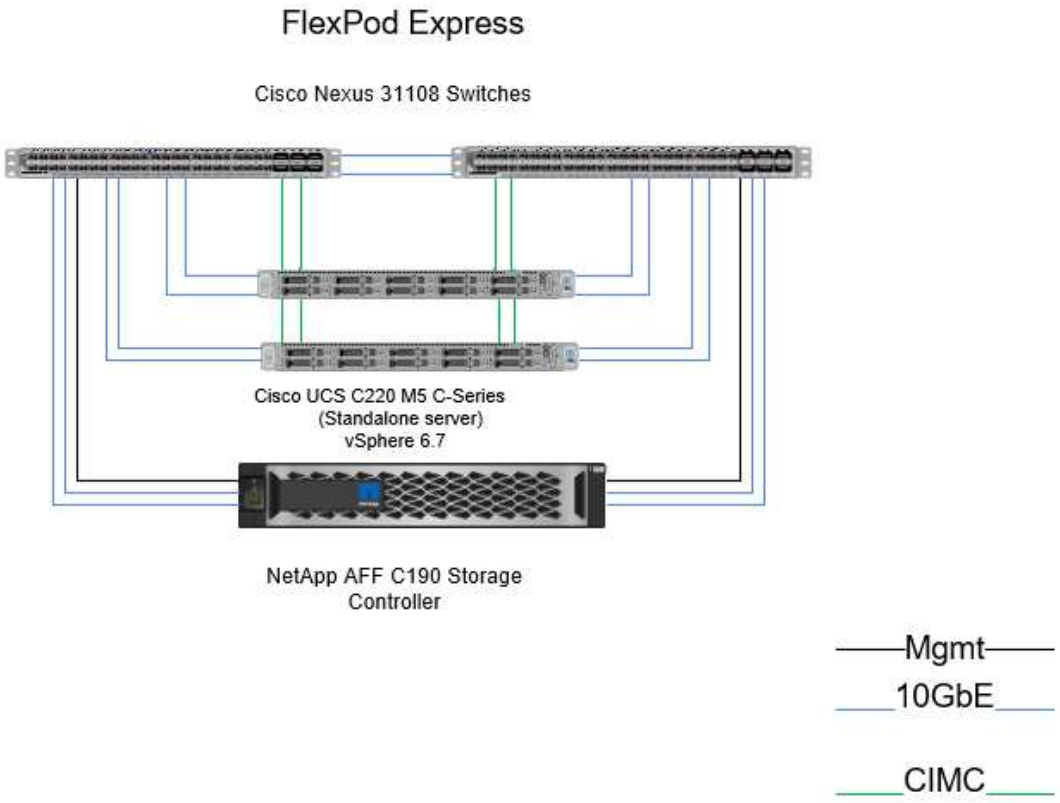
El programa Arquitectura verificada de NetApp ofrece a los clientes una arquitectura verificada para soluciones NetApp. Una arquitectura verificada de NetApp ofrece una arquitectura de solución de NetApp con las siguientes cualidades:

- Completamente probado
- Naturaleza prescriptiva
- Riesgos mínimos en la implementación
- Plazos de comercialización reducidos

Esta guía detalla el diseño de FlexPod Express con VMware vSphere. Además, este diseño utiliza el nuevo sistema AFF C190 (que ejecuta ONTAP® 9.6 de NetApp), los servidores Cisco Nexus 31108 y Cisco UCS C-Series C220 M5 como nodos de hipervisor.

Tecnología de soluciones

Esta solución aprovecha las últimas tecnologías de NetApp, Cisco y VMware. Esta solución incluye el nuevo sistema AFF C190 de NetApp con ONTAP 9.6, switches Cisco Nexus 31108 duales y servidores de rack Cisco UCS C220 M5 con VMware vSphere 6.7U2. Esta solución validada usa tecnología 10 GbE. También se ofrece orientación sobre cómo escalar la capacidad de computación mediante la adición de dos nodos de hipervisor a la vez para que la arquitectura FlexPod Express pueda adaptarse a las cambiantes necesidades empresariales de una organización.



Para utilizar los cuatro puertos físicos de 10 GbE del VIC 1457 de manera eficiente, crear dos enlaces adicionales desde cada servidor hasta los switches de bastidor superior.

Resumen de casos de uso

La solución FlexPod Express puede aplicarse a varios casos prácticos, incluidos los siguientes:

- Oficinas remotas o filiales
- Pequeñas y medianas empresas
- Entornos que requieren una solución dedicada y rentable

FlexPod Express está indicado para cargas de trabajo virtualizadas y mixtas. Aunque esta solución se validó con vSphere 6.7U2, es compatible con cualquier versión de vSphere cualificada con el resto de componentes de la herramienta de matriz de interoperabilidad de NetApp. NetApp recomienda implementar vSphere 6.7U2 debido a sus correcciones y funciones mejoradas, como:

- Nueva compatibilidad de protocolos para backup y restauración de un dispositivo servidor vCenter, incluidos HTTP, HTTPS, FTP, FTPS, SCP, NFS Y SMB.
- Nuevo funcionalmente al utilizar la biblioteca de contenido. La sincronización de plantillas de equipos virtuales nativas entre bibliotecas de contenido ahora está disponible cuando vCenter Server está configurado para el modo vinculado mejorado.
- Una página actualizada del complemento de cliente.
- Se han añadido mejoras en vSphere Update Manager (VUM) y el cliente de vSphere. Ahora puede realizar las acciones de adjuntar, comprobar y solucionar, todas desde una sola pantalla.

Para obtener más información sobre este tema, consulte "Página vSphere 6.7U2" y la "Notas de la versión de vCenter Server 6.7U2".

Requisitos tecnológicos

Un sistema FlexPod Express requiere una combinación de componentes de hardware y software. FlexPod Express también describe los componentes de hardware necesarios para añadir nodos de hipervisor al sistema en unidades de dos.

Requisitos de hardware

Independientemente del hipervisor elegido, todas las configuraciones exprés de FlexPod utilizan el mismo hardware. Por lo tanto, aunque cambien los requisitos del negocio, puede utilizar un hipervisor diferente en el mismo hardware de FlexPod Express.

En la siguiente tabla se enumeran los componentes de hardware necesarios para la configuración e implementación de FlexPod Express. Los componentes de hardware que se usan en cualquier implementación de la solución pueden variar en función de las necesidades del cliente.

Hardware subyacente	Cantidad
Clúster de dos nodos C190 de AFF	1
Servidor Cisco C220 M5	2
Switch Cisco Nexus 31108PC-V	2
Tarjeta de interfaz virtual (VIC) Cisco UCS 1457 para el servidor de montaje en rack Cisco UCS C220 M5	2

Esta tabla enumera el hardware necesario además de la configuración base para implementar 10 GbE.

Hardware subyacente	Cantidad
Servidor Cisco UCS C220 M5	2
Cisco VIC 1457	2

Requisitos de software

En la siguiente tabla se enumeran los componentes de software necesarios para implementar las arquitecturas de las soluciones Express de FlexPod.

De NetApp	Versión	Detalles
Controladora de gestión integrada de Cisco (CIMC)	4.0.4	Para los servidores en rack Cisco UCS C220 M5
Controlador nenic de Cisco	1.0.0.29	Para tarjetas de interfaz VIC 1457
Cisco NX-OS	7.0(3)I7(6)	Para switches Cisco Nexus 31108PC-V.
ONTAP de NetApp	9.6	Para controladoras C190 de AFF

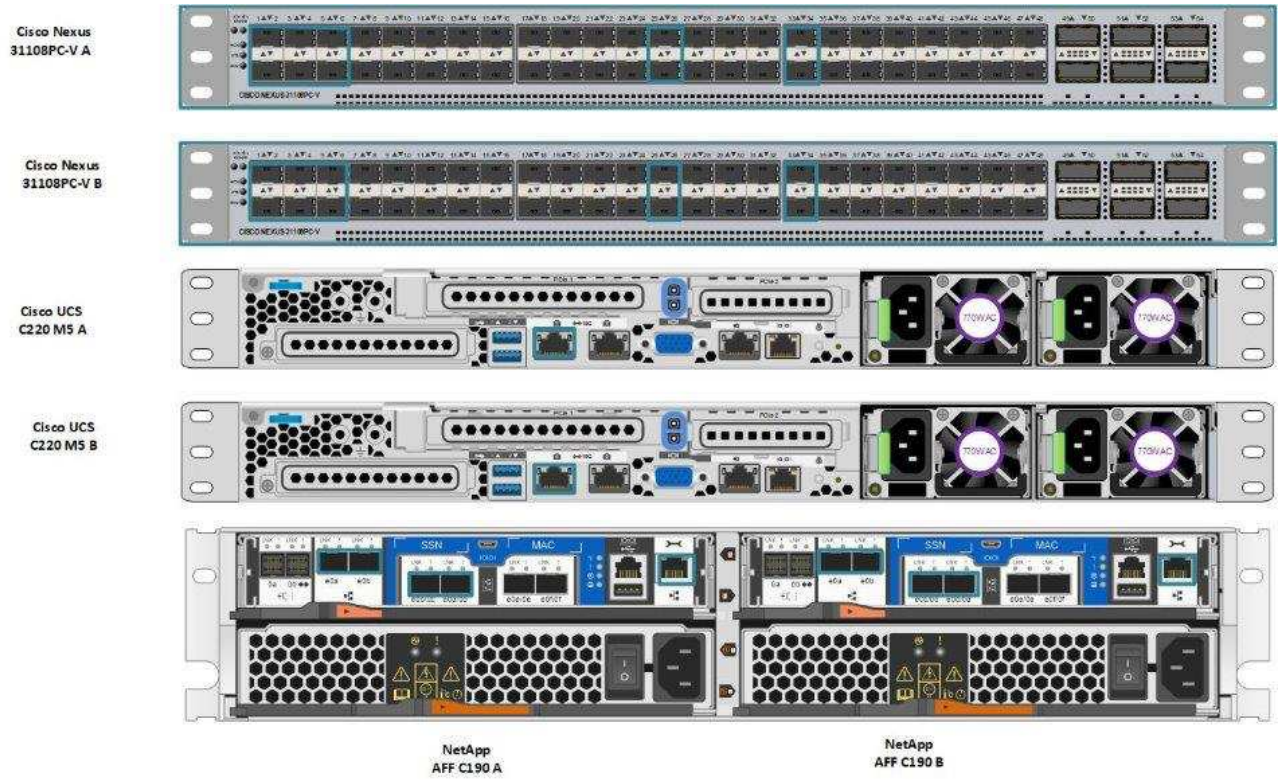
En esta tabla, se enumera el software necesario para todas las implementaciones de VMware vSphere en FlexPod Express.

De NetApp	Versión
Dispositivo VMware vCenter Server	6.7U2
Hipervisor ESXi de VMware vSphere	6.7U2
Complemento VAAI de NetApp para ESXi	1.1.2
VSC de NetApp	9.6

Información sobre el cableado exprés de FlexPod

Esta validación de referencia se cablea como se muestra en las siguientes figuras y tablas.

En esta figura, se muestra el cableado de validación de referencia.



En la siguiente tabla se muestra la información de cableado del switch Cisco Nexus 31108PC-V-A.

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Switch Cisco Nexus 31108PC-V A	Eth1/1	La controladora De almacenamiento C190 de AFF de NetApp	e0c
	Eth1/2	Controladora de almacenamiento AFF C190 de NetApp B.	e0c
	Eth1/3	El servidor A independiente Cisco UCS C220 C-Series	MLOM0
	Eth1/4	Servidor B independiente Cisco UCS C220 C-Series	MLOM0
	Eth1/5	El servidor A independiente Cisco UCS C220 C-Series	MLOM1
	Eth1/6	Servidor B independiente Cisco UCS C220 C-Series	MLOM1
	Eth1/25	Switch Cisco Nexus 31108PC-V B	Eth1/25
	Eth1/26	Switch Cisco Nexus 31108PC-V B	Eth1/26
	Eth1/33	La controladora De almacenamiento C190 de AFF de NetApp	E0M
	Eth1/34	El servidor A independiente Cisco UCS C220 C-Series	CIMC (FEX135/1/25)

Esta tabla enumera la información de cableado del switch Cisco Nexus 31108PC-V- B.

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Switch Cisco Nexus 31108PC-V B	Eth1/1	La controladora De almacenamiento C190 de AFF de NetApp	e0d
	Eth1/2	Controladora de almacenamiento AFF C190 de NetApp B.	e0d
	Eth1/3	El servidor A independiente Cisco UCS C220 C-Series	MLOM2
	Eth1/4	Servidor B independiente Cisco UCS C220 C-Series	MLOM2
	Eth1/5	El servidor A independiente Cisco UCS C220 C-Series	MLOM3
	Eth1/6	Servidor B independiente Cisco UCS C220 C-Series	MLOM3
	Eth1/25	Switch Cisco Nexus 31108 a	Eth1/25
	Eth1/26	Switch Cisco Nexus 31108 a	Eth1/26
	Eth1/33	Controladora de almacenamiento AFF C190 de NetApp B.	E0M
	Eth1/34	Servidor B independiente Cisco UCS C220 C-Series	CIMC (FEX135/1/26)

Esta tabla enumera la información de cableado de la controladora de almacenamiento AFF C190 de NetApp

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
La controladora De almacenamiento C190 de AFF de NetApp	e0a	Controladora de almacenamiento AFF C190 de NetApp B.	e0a
	e0b	Controladora de almacenamiento AFF C190 de NetApp B.	e0b
	e0c	Switch Cisco Nexus 31108PC-V A	Eth1/1
	e0d	Switch Cisco Nexus 31108PC-V B	Eth1/1
	E0M	Switch Cisco Nexus 31108PC-V A	Eth1/33

Esta tabla enumera la información de cableado de la controladora de almacenamiento AFF C190 de NetApp B.

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Controladora de almacenamiento AFF C190 de NetApp B.	e0a	La controladora De almacenamiento C190 de AFF de NetApp	e0a
	e0b	La controladora De almacenamiento C190 de AFF de NetApp	e0b
	e0c	Switch Cisco Nexus 31108PC-V A	Eth1/2
	e0d	Switch Cisco Nexus 31108PC-V B	Eth1/2
	E0M	Switch Cisco Nexus 31108PC-V B	Eth1/33

Procedimientos de implantación

Descripción general

Este documento proporciona detalles para configurar un sistema FlexPod Express completamente redundante y de alta disponibilidad. Para reflejar esta redundancia, los componentes que se configuran en cada paso se denominan componente A o componente B. Por ejemplo, la controladora A y la controladora B identifican las dos controladoras de almacenamiento de NetApp que se aprovisionan en este documento. El switch A y el switch B identifican un par de switches Cisco Nexus.

Además, en este documento se describen los pasos para aprovisionar varios hosts de Cisco UCS, que se identifican secuencialmente como servidor A, servidor B, etc.

Para indicar que debe incluir la información pertinente a su entorno en un paso, `<<text>>` aparece como parte de la estructura de comandos. Consulte el siguiente ejemplo de `vlan create` comando:

```
Controller01> network port vlan create –node <<var_nodeA>> -vlan-name
<<var_vlan-name>>
```

Este documento permite configurar completamente el entorno de FlexPod Express. En este proceso, varios pasos requieren que inserte convenciones de nomenclatura específicas del cliente, direcciones IP y esquemas de red de área local virtual (VLAN). En la siguiente tabla se describen las VLAN necesarias para la implementación, tal y como se describe en esta guía. Esta tabla se puede completar en función de las variables específicas del sitio y se puede utilizar para implementar los pasos de configuración del documento.

Si se utilizan VLAN de gestión fuera de banda y en banda independientes, debe crear una ruta de capa- 3 entre ellas. Para esta validación, se utilizó una VLAN de gestión común.

Nombre de la VLAN	Propósito de VLAN	ID DE VLAN	
VLAN de gestión	VLAN para interfaces de gestión	3437	VSwitch0
VLAN NFS	VLAN para tráfico NFS	3438	VSwitch0
VLAN de VMware vMotion	VLAN designada para mover máquinas virtuales (VM) de un host físico a otro	3441	VSwitch0
VLAN de tráfico de la máquina virtual	VLAN para tráfico de aplicaciones de equipos virtuales	3442	VSwitch0
ISCSI-A-VLAN	VLAN para tráfico iSCSI en la estructura A	3439	IScsiBootvSwitch
ISCSI-B-VLAN	VLAN para tráfico iSCSI en la estructura B	3440	IScsiBootvSwitch
VLAN nativa	VLAN a la que se asignan tramas no etiquetadas	2	

Los números VLAN son necesarios en toda la configuración de FlexPod Express. Las VLAN se denominan `<<var_xxxx_vlan>>`, donde `xxxx` Es la finalidad de la VLAN (como iSCSI-A).

En esta validación se han creado dos vSwitch.

En la siguiente tabla se enumeran los vSwitch de la solución.

Nombre de vSwitch	Adaptadores activos	Puertos	MTU	Balanceo de carga
VSwitch0	Vmnic2, vmnic4	predeterminado (120)	9000	Ruta basada en hash IP
IScsiBootvSwitch	Vmnic3, vmnic5	predeterminado (120)	9000	Ruta basada en el identificador de puerto virtual de origen.

El método hash IP del equilibrio de carga requiere la configuración adecuada para el conmutador físico subyacente mediante SRC-DST-IP EtherChannel con un puerto-canal estático (modo activado). En caso de que se produzca una conectividad intermitente debido a una posible configuración incorrecta del switch, cierre temporalmente uno de los dos puertos de enlace ascendente asociados en el switch de Cisco para restaurar la comunicación con el puerto vmkernel de gestión de ESXi mientras se solucionan los problemas de la configuración del canal de puertos.

La siguiente tabla enumera las máquinas virtuales de VMware que se crean.

Descripción de la máquina virtual	Nombre de host
Servidor VMware vCenter	FlexPod-VCSA

Descripción de la máquina virtual	Nombre de host
Consola de almacenamiento virtual	FlexPod VSC

Ponga en marcha Cisco Nexus 31108PC-V

En esta sección se detalla la configuración del switch Cisco Nexus 331108PC-V utilizada en un entorno FlexPod Express.

Configuración inicial del switch Cisco Nexus 31108PC-V.

Los siguientes procedimientos describen cómo configurar los switches Cisco Nexus para su uso en un entorno FlexPod Express básico.

> En este procedimiento se asume que está utilizando un Cisco Nexus 31108PC-V con el software NX-OS versión 7.0(3)I7(6).

1. Tras el arranque y la conexión iniciales al puerto de la consola del switch, se inicia automáticamente la configuración de Cisco NX-OS. Esta configuración inicial trata los valores básicos, como el nombre del switch, la configuración de la interfaz mgmt0 y la configuración de Secure Shell (SSH).
2. La red de gestión del sistema FlexPod Express se puede configurar de varias maneras. Las interfaces mgmt0 de los conmutadores 31108PC-V se pueden conectar a una red de administración existente, o bien las interfaces mgmt0 de los conmutadores 31108PC-V se pueden conectar en una configuración posterior. Sin embargo, este enlace no se puede utilizar para el acceso de gestión externo, como tráfico SSH.

   > En esta guía de puesta en marcha, los switches Cisco Nexus 31108PC-V de FlexPod Express están conectados a una red de gestión existente.

3. Para configurar los switches Cisco Nexus 31108PC-V, encienda el switch y siga las indicaciones que aparecen en pantalla, como se muestra aquí para la configuración inicial de ambos switches, sustituyendo los valores adecuados para la información específica del conmutador.

```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
  Create another login account (yes/no) [n]: n
  Configure read-only SNMP community string (yes/no) [n]: n
  Configure read-write SNMP community string (yes/no) [n]: n
  Enter the switch name : 31108PC-V-B
  Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
    Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
    Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
  Configure the default gateway? (yes/no) [y]: y
    IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
  Configure advanced IP options? (yes/no) [n]: n
  Enable the telnet service? (yes/no) [n]: n
  Enable the ssh service? (yes/no) [y]: y
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
    Number of rsa key bits <1024-2048> [1024]: <enter>
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 address : <<var_ntp_ip>>
  Configure default interface layer (L3/L2) [L2]: <enter>
  Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]: <enter>
```

4. A continuación, verá un resumen de la configuración y se le preguntará si desea editarla. Si la configuración es correcta, introduzca `n`.

```
Would you like to edit the configuration? (y
es/no) [n]: n
```

5. A continuación, se le preguntará si desea utilizar esta configuración y guardarla. Si es así, introduzca `y`.

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Repita este procedimiento para el switch Cisco Nexus B.

Habilite las funciones avanzadas

Determinadas características avanzadas deben estar habilitadas en Cisco NX-OS para proporcionar opciones de configuración adicionales. Para activar las funciones adecuadas en los switches a y B de Cisco Nexus, entre en el modo de configuración mediante el comando (config t) y ejecute los siguientes comandos:

```
feature interface-vlan
feature lacp
feature vpc
```

> El hash de equilibrio de carga del canal de puerto predeterminado utiliza las direcciones IP de origen y destino para determinar el algoritmo de equilibrio de carga en las interfaces del canal de puerto. Puede lograr una mejor distribución entre los miembros del canal de puerto proporcionando más entradas al algoritmo hash más allá de las direcciones IP de origen y destino. Por el mismo motivo, NetApp recomienda encarecidamente añadir los puertos TCP de origen y destino al algoritmo hash.

En el modo de configuración (config t), introduzca los siguientes comandos para establecer la configuración global del equilibrio de carga del canal de puertos en el switch A y el switch B de Cisco Nexus:

```
port-channel load-balance src-dst ip-l4port
```

Configurar árbol de expansión global

La plataforma Cisco Nexus utiliza una nueva función de protección llamada garantía de puente. La garantía de puente ayuda a proteger contra un enlace unidireccional u otro error de software con un dispositivo que continúa redirectando el tráfico de datos cuando ya no ejecuta el algoritmo de árbol expansivo. Los puertos se pueden colocar en uno de varios estados, incluyendo la red o el borde, dependiendo de la plataforma.

NetApp recomienda establecer la garantía de puente para que todos los puertos se consideren puertos de red de forma predeterminada. Este ajuste obliga al administrador de red a revisar la configuración de cada puerto. También revela los errores de configuración más comunes, como puertos de borde no identificados o un vecino que no tiene activada la función de garantía de puente. Además, es más seguro tener el bloque de árbol expansivo muchos puertos en lugar de muy pocos, lo que permite que el estado de puerto predeterminado mejore la estabilidad general de la red.

Preste especial atención al estado de árbol de expansión al agregar servidores, almacenamiento y switches ascendentes, especialmente si no admiten la garantía de puente. En estos casos, es posible que deba cambiar el tipo de puerto para que los puertos estén activos.

El protector de unidad de datos de protocolo puente (BPDU) está habilitado de forma predeterminada en puertos periféricos como otra capa de protección. Para evitar bucles en la red, esta característica cierra el puerto si se ven BPDU de otro switch en esta interfaz.

En el modo de configuración (config t), ejecute los siguientes comandos para configurar las opciones predeterminadas de árbol de expansión, incluidos el tipo de puerto predeterminado y el protector BPDU, en el conmutador A Cisco Nexus y el conmutador B:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
ntp server <<var_ntp_ip>> use-vrf management
ntp master 3
```

Defina las VLAN

Antes de configurar puertos individuales con VLAN diferentes, se deben definir las VLAN de capa 2 en el switch. También se recomienda nombrar las VLAN para que la solución de problemas sea sencilla en el futuro.

En el modo de configuración (config t), ejecute los siguientes comandos para definir y describir las VLAN de capa 2 en el switch A de Cisco Nexus y el switch B:

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

Configurar el acceso y las descripciones de los puertos de gestión

Como es el caso con la asignación de nombres a las VLAN de capa 2, las descripciones de configuración de todas las interfaces pueden ayudar tanto al aprovisionamiento como a la resolución de problemas.

Desde el modo de configuración (config t) de cada uno de los switches, introduzca las siguientes descripciones de puertos para la configuración grande de FlexPod Express:

Switch Cisco Nexus a

```
int eth1/1
  description AFF C190-A e0c
int eth1/2
  description AFF C190-B e0c
int eth1/3
  description UCS-Server-A: MLOM port 0 vSwitch0
int eth1/4
  description UCS-Server-B: MLOM port 0 vSwitch0
int eth1/5
  description UCS-Server-A: MLOM port 1 iScsiBootvSwitch
int eth1/6
  description UCS-Server-B: MLOM port 1 iScsiBootvSwitch
int eth1/25
  description vPC peer-link 31108PC-V-B 1/25
int eth1/26
  description vPC peer-link 31108PC-V-B 1/26
int eth1/33
  description AFF C190-A e0M
int eth1/34
  description UCS Server A: CIMC
```

Switch Cisco Nexus B

```
int eth1/1
  description AFF C190-A e0d
int eth1/2
  description AFF C190-B e0d
int eth1/3
  description UCS-Server-A: MLOM port 2 vSwitch0
int eth1/4
description UCS-Server-B: MLOM port 2 vSwitch0
int eth1/5
  description UCS-Server-A: MLOM port 3 iScsiBootvSwitch
int eth1/6
  description UCS-Server-B: MLOM port 3 iScsiBootvSwitch
int eth1/25
  description vPC peer-link 31108PC-V-A 1/25
int eth1/26
  description vPC peer-link 31108PC-V-A 1/26
int eth1/33
  description AFF C190-B e0M
int eth1/34
  description UCS Server B: CIMC
```

Configurar las interfaces de gestión de almacenamiento y servidores

Las interfaces de gestión para el servidor y el almacenamiento suelen utilizar una sola VLAN. Por lo tanto, configure los puertos de la interfaz de gestión como puertos de acceso. Defina la VLAN de administración para cada switch y cambie el tipo de puerto de árbol expansivo a EDGE.

En el modo de configuración (config t), introduzca los siguientes comandos para configurar los ajustes del puerto para las interfaces de gestión tanto de los servidores como del almacenamiento:

Switch Cisco Nexus a

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Switch Cisco Nexus B

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Realizar la configuración global del canal de puerto virtual

Un canal de puerto virtual (VPC) permite que los enlaces que están conectados físicamente a dos switches de Cisco Nexus diferentes aparezcan como un único canal de puerto a un tercer dispositivo. El tercer dispositivo puede ser un conmutador, un servidor o cualquier otro dispositivo de red. Un VPC puede proporcionar una multivía de nivel 2, que le permite crear redundancia aumentando el ancho de banda, habilitando varias rutas paralelas entre los nodos y el tráfico de equilibrio de carga donde haya rutas alternativas.

Un VPC proporciona las siguientes ventajas:

- Permitir que un único dispositivo utilice un canal de puerto a través de dos dispositivos de subida
- Eliminar puertos bloqueados con protocolo de árbol expansivo
- Proporciona una topología sin bucles
- Utilizando todo el ancho de banda disponible de enlace ascendente
- Proporcionar convergencia rápida si el enlace o un dispositivo falla
- Resiliencia a nivel de enlace
- Contribuir a proporcionar una alta disponibilidad

La función VPC requiere alguna configuración inicial entre los dos switches de Cisco Nexus para que funcionen correctamente. Si utiliza la configuración de Mgmt0 de fondo a fondo, utilice las direcciones

definidas en las interfaces y compruebe que se pueden comunicar mediante el `ping <<switch_A/B_mgmt0_ip_addr>>vrf` comando de gestión.

En el modo de configuración (config t), ejecute los siguientes comandos para configurar la configuración global de VPC para ambos switches:

Switch Cisco Nexus a

```
vpc domain 1
 role priority 10
  peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf
management
peer-switch
peer-gateway
auto-recovery
delay restore 150
ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
  no shut
exit
copy run start
```

Switch Cisco Nexus B

```
vpc domain 1
  peer-switch
  role priority 20
  peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  delay-restore 150
   ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
no shut
exit
copy run start
```

Configure los canales del puerto de almacenamiento

Las controladoras de almacenamiento de NetApp permiten una conexión activa-activa a la red mediante el protocolo de control de agregación de enlaces (LACP). El uso de LACP es preferido porque añade negociación y registro entre los switches. Debido a que la red está configurada para VPC, este enfoque permite disponer de conexiones activo-activo del almacenamiento para separar los switches físicos. Cada controladora tiene dos enlaces a cada uno de los switches. Sin embargo, los cuatro enlaces forman parte del mismo VPC y grupo de interfaces (ifgrp).

En el modo de configuración (config t), ejecute los siguientes comandos en cada uno de los switches para configurar las interfaces individuales y la configuración de canal de puerto resultante para los puertos conectados a la controladora AFF de NetApp.

1. Ejecute los siguientes comandos en el switch A y en el switch B a para configurar los canales de puertos de la controladora De almacenamiento A:

```
int eth1/1
  channel-group 11 mode active
int Po11
  description vPC to Controller-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<mgmt_vlan_id>>,<<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 11
  no shut
```

2. Ejecute los siguientes comandos en el switch A y en el switch B a para configurar los canales de puertos de la controladora de almacenamiento B:

```
int eth1/2
  channel-group 12 mode active
int Po12
  description vPC to Controller-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<mgmt_vlan_id>>,
<<iSCSI_A_vlan_id>>, <<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 12
  no shut
exit
copy run start
```

Configure las conexiones del servidor

Los servidores Cisco UCS tienen una tarjeta de interfaz virtual de cuatro puertos, VIC1457, que se utiliza para el tráfico de datos y el arranque del sistema operativo ESXi mediante iSCSI. Estas interfaces se configuran para que se conmutan al nodo de respaldo entre sí, lo que proporciona redundancia adicional más allá de un solo enlace. Al distribuir estos enlaces a través de varios switches, el servidor puede sobrevivir incluso a un fallo completo del switch.

Desde el modo de configuración (config t), ejecute los siguientes comandos para configurar los ajustes de puerto para las interfaces conectadas a cada servidor.

Switch Cisco Nexus A: Configuración de Cisco UCS Server-A y Cisco UCS Server-B.

```
int eth1/5
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_A_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

Cisco Nexus Switch B: Configuración de Cisco UCS Server-A y Cisco UCS Server-B.

```
int eth1/6
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_B_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

Configure los canales del puerto del servidor

Ejecute los siguientes comandos en el switch A y el switch B para configurar los canales de puertos para el servidor A:

```
int eth1/3
  channel-group 13 mode active
int Po13
  description vPC to Server-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_id>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 13
  no shut
```

Ejecute los siguientes comandos en el switch A y el switch B para configurar los canales de puerto para el servidor B:

```
int eth1/4
  channel-group 14 mode active
int Po14
  description vPC to Server-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_id>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 14
  no shut
```

Se utilizó una MTU de 9000 en esta validación de solución. Sin embargo, puede configurar un valor diferente para el MTU apropiado para los requisitos de sus aplicaciones. Es importante establecer el mismo valor de MTU en la solución de FlexPod. Una configuración de MTU incorrecta entre componentes provoca que se descartan los paquetes y estos paquetes deberán transmitirse de nuevo, lo que afecta al rendimiento general de la solución.

Para escalar la solución añadiendo servidores Cisco UCS adicionales, ejecute los comandos anteriores con los puertos del switch a los que se han conectado los servidores recién añadidos en los switches A y B.

Enlace ascendente a una infraestructura de red existente

En función de la infraestructura de red disponible, se pueden utilizar varios métodos y funciones para elevar el entorno FlexPod. Si existe un entorno Cisco Nexus existente, NetApp recomienda utilizar PCs para elevar los

switches Cisco Nexus 31108 incluidos en el entorno FlexPod a la infraestructura. Los enlaces ascendentes pueden ser enlaces de subida de 10 GbE para una solución de infraestructura de 10 GbE o 1 GbE para una solución de infraestructura de 1 GbE si fuera necesario. Los procedimientos descritos anteriormente se pueden utilizar para crear un VPC de enlace ascendente al entorno existente. Asegúrese de ejecutar Copy START para guardar la configuración en cada switch una vez completada la configuración.

"Siguiente: Procedimiento de implementación del almacenamiento de NetApp (parte 1)."

Procedimiento de instalación de almacenamiento NetApp (parte 1)

En esta sección se describe el procedimiento de implementación del almacenamiento AFF de NetApp.

Instalación de la controladora de almacenamiento de NetApp C190 Series de AFF

Hardware Universe de NetApp

La aplicación NetApp Hardware Universe (HWU) proporciona componentes de hardware y software compatibles con cualquier versión específica de ONTAP. Proporciona información de configuración para todos los dispositivos de almacenamiento de NetApp compatibles actualmente con el software ONTAP. También se proporciona una tabla de compatibilidades de componentes.

Confirme que los componentes de hardware y software que desea utilizar son compatibles con la versión de ONTAP que tiene previsto instalar:

Acceda a "HWU" aplicación para ver las guías de configuración del sistema. Haga clic en la pestaña controladoras para ver la compatibilidad entre distintas versiones del software ONTAP y los dispositivos de almacenamiento de NetApp con las especificaciones que desea.

Como alternativa, para comparar componentes por dispositivo de almacenamiento, haga clic en Comparar sistemas de almacenamiento.

Requisitos previos de la controladora AFF serie 190
Para planificar la ubicación física de los sistemas de almacenamiento, consulte Hardware Universe de NetApp. Consulte las siguientes secciones: • Requisitos eléctricos • Cables de alimentación compatibles • Puertos y cables integrados

Controladoras de almacenamiento

Siga los procedimientos de instalación física de las controladoras en AFF "C190" Documentación.

ONTAP 9.6 de NetApp

Hoja de datos de configuración

Antes de ejecutar la secuencia de comandos de instalación, rellene la hoja de datos de configuración del manual del producto. La hoja de datos de configuración está disponible en la Guía de configuración de software de ONTAP 9.6.

Este sistema se establece en una configuración de clúster de dos nodos sin switch.

La siguiente tabla contiene información sobre la instalación y la configuración de ONTAP 9.6.

Detalles del clúster	Valor de detalles de clúster
Nodo del clúster: Dirección IP	<<var_nodeA_mgmt_ip>>
Máscara de red Del nodo a del clúster	<<var_nodeA_mgmt_mask>>
Nodo del clúster: Puerta de enlace	<<var_nodeA_mgmt_gateway>>
Nombre del nodo a del clúster	<<var_nodeA>>
Dirección IP del nodo B del clúster	<<var_nodeB_mgmt_ip>>
Máscara de red del nodo B del clúster	<<var_nodeB_mgmt_mask>>
Puerta de enlace del nodo B del clúster	<<var_nodeB_mgmt_gateway>>
Nombre del nodo B del clúster	<<var_nodeB>>
Dirección URL de ONTAP 9.6	<<var_url_boot_software>>
El nombre del clúster	<<var_clustername>>
Dirección IP de gestión del clúster	<<var_clustermgmt_ip>>
Puerta de enlace del clúster B.	<<var_clustermgmt_gateway>>
Máscara de red del clúster B.	<<var_clustermgmt_mask>>
Nombre de dominio	<<var_domain_name>>
IP del servidor DNS (puede introducir más de uno)	<var_dns_server_ip
La IP del servidor NTP (es posible introducir más de uno)	<<var_ntp_server_ip>>

Configure el nodo a

Para configurar el nodo A, complete los siguientes pasos:

1. Conéctese al puerto de la consola del sistema de almacenamiento. Tiene que ver un cargador-a del símbolo del sistema. Sin embargo, si el sistema de almacenamiento está en un bucle de reinicio, pulse Ctrl-C para salir del bucle de autoarranque cuando vea este mensaje:

   ```
   Starting AUTOBOOT press Ctrl-C to abort…
   ```

   Permita que el sistema arranque.

   ```
   autoboot
   ```

2. Pulse Ctrl-C para acceder al menú Inicio.

Si ONTAP 9.6 no es la versión del software que se está arrancando, continúe con los pasos siguientes para instalar el software nuevo. Si ONTAP 9.6 es la versión que se va a arrancar, seleccione la opción 8 e y para reiniciar el nodo. A continuación, continúe con el paso 14.

3. Para instalar software nuevo, seleccione la opción 7.
4. Introduzca y para realizar una actualización.
5. Seleccione e0M para el puerto de red que desee usar para la descarga.
6. Introduzca y para reiniciar ahora.
7. Introduzca la dirección IP, la máscara de red y la puerta de enlace predeterminada para e0M en sus respectivos lugares.

```
<<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
```

8. Especifique la dirección URL donde se puede encontrar el software.

Este servidor web debe ser pingable.

```
<<var_url_boot_software>>
```

9. Pulse Intro para el nombre de usuario, indicando que no hay nombre de usuario.
10. Introduzca y para establecer el software recién instalado como valor predeterminado que se utilizará para los siguientes reinicios.
11. Introduzca y para reiniciar el nodo.

Al instalar el software nuevo, el sistema podría realizar actualizaciones de firmware en el BIOS y las tarjetas adaptadoras, lo que provoca reinicios y posibles interrupciones en el cargador. Si se producen estas acciones, el sistema podría desviarse de este procedimiento.

12. Pulse Ctrl-C para acceder al menú Inicio.
13. Seleccione la opción 4 para Configuración limpia y inicializar todos los discos.
14. Introduzca y para poner a cero discos, restablezca la configuración e instale un nuevo sistema de archivos.
15. Introduzca y para borrar todos los datos de los discos.

La inicialización y creación del agregado raíz puede tardar 90 minutos o más en completarse, según el número y el tipo de discos conectados. Una vez finalizada la inicialización, el sistema de almacenamiento se reinicia. Tenga en cuenta que los SSD tardan mucho menos tiempo en inicializarse. Puede continuar con la configuración del nodo B mientras los discos del nodo A se están poniendo a cero.

Mientras el nodo A se está inicializando, empiece a configurar el nodo B.

Configure el nodo B

Para configurar el nodo B, complete los siguientes pasos:

1. Conéctese al puerto de la consola del sistema de almacenamiento. Tiene que ver un cargador-a del símbolo del sistema. Sin embargo, si el sistema de almacenamiento está en un bucle de reinicio, pulse Ctrl-C para salir del bucle de autoarranque cuando vea este mensaje:

```
Starting AUTOBOOT press Ctrl-C to abort…
```

2. Pulse Ctrl-C para acceder al menú Inicio.

```
autoboot
```

3. Pulse Ctrl-C cuando se le solicite.

> Si ONTAP 9.6 no es la versión del software que se está arrancando, continúe con los pasos siguientes para instalar el software nuevo. Si ONTAP 9.6 es la versión que se va a arrancar, seleccione la opción 8 e y para reiniciar el nodo. A continuación, continúe con el paso 14.

4. Para instalar software nuevo, seleccione la opción 7.A.
5. Introduzca y para realizar una actualización.
6. Seleccione e0M para el puerto de red que desee usar para la descarga.
7. Introduzca y para reiniciar ahora.
8. Introduzca la dirección IP, la máscara de red y la puerta de enlace predeterminada para e0M en sus respectivos lugares.

```
<<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
```

9. Especifique la dirección URL donde se puede encontrar el software.

> Este servidor web debe ser pingable.

```
<<var_url_boot_software>>
```

10. Pulse Intro para el nombre de usuario, indicando que no hay nombre de usuario.
11. Introduzca y para establecer el software recién instalado como valor predeterminado que se utilizará para los siguientes reinicios.
12. Introduzca y para reiniciar el nodo.

Al instalar el software nuevo, el sistema podría realizar actualizaciones de firmware en el BIOS y las tarjetas adaptadoras, lo que provoca reinicios y posibles interrupciones en el cargador. Si se producen estas acciones, el sistema podría desviarse de este procedimiento.

13. Pulse Ctrl-C para acceder al menú Inicio.
14. Seleccione la opción 4 para Configuración limpia y inicializar todos los discos.
15. Introduzca y para poner a cero discos, restablezca la configuración e instale un nuevo sistema de archivos.
16. Introduzca y para borrar todos los datos de los discos.

La inicialización y creación del agregado raíz puede tardar 90 minutos o más en completarse, según el número y el tipo de discos conectados. Una vez finalizada la inicialización, el sistema de almacenamiento se reinicia. Tenga en cuenta que los SSD tardan mucho menos tiempo en inicializarse.

Continuación de la configuración del nodo a y de la configuración del clúster

Desde un programa de puertos de consola conectado al puerto de la consola De la controladora De almacenamiento A (nodo A), ejecute el script de configuración del nodo. Este script se muestra cuando ONTAP 9.6 arranca en el nodo por primera vez.

El procedimiento de configuración del nodo y de los clústeres ha cambiado ligeramente en ONTAP 9.6. El asistente de configuración de clúster se utiliza ahora para configurar el primer nodo de un clúster y el Administrador del sistema ONTAP de NetApp (anteriormente, OnCommand® System Manager) se utiliza para configurar el clúster.

1. Siga las instrucciones para configurar el nodo A.

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

2. Vaya a la dirección IP de la interfaz de gestión del nodo.

> La configuración del clúster también se puede realizar mediante la CLI. Este documento describe la configuración del clúster mediante la configuración guiada de System Manager.

3. Haga clic en Guided Setup para configurar el clúster.
4. Introduzca `<<var_clustername>>` del nombre del clúster y. `<<var_nodeA>>` y.. `<<var_nodeB>>` para cada uno de los nodos que va a configurar. Introduzca la contraseña que desea usar para el sistema de almacenamiento. Seleccione Switchless Cluster para el tipo de clúster. Introduzca la licencia base del clúster.
5. También es posible introducir licencias de funciones para Cluster, NFS e iSCSI.
6. Ve un mensaje de estado que indica que el clúster se está creando. Este mensaje de estado cambia por varios Estados. Este proceso tarda varios minutos.
7. Configure la red.

a. Anule la selección de la opción intervalo de direcciones IP.

b. Introduzca `<<var_clustermgmt_ip>>` En el campo Cluster Management IP Address, `<<var_clustermgmt_mask>>` En el campo máscara de red, y. `<<var_clustermgmt_gateway>>` En el campo Puerta de enlace. Utilice el… Selector en el campo Port para seleccionar e0M del nodo A.

c. La IP de gestión de nodos para el nodo A ya se ha rellenado. Introduzca `<<var_nodeA_mgmt_ip>>` Para el nodo B.

d. Introduzca `<<var_domain_name>>` En el campo DNS Domain Name. Introduzca `<<var_dns_server_ip>>` En el campo DNS Server IP Address.

> Puede introducir varias direcciones IP del servidor DNS.

e. Introduzca `10.63.172.162` En el campo servidor NTP primario.

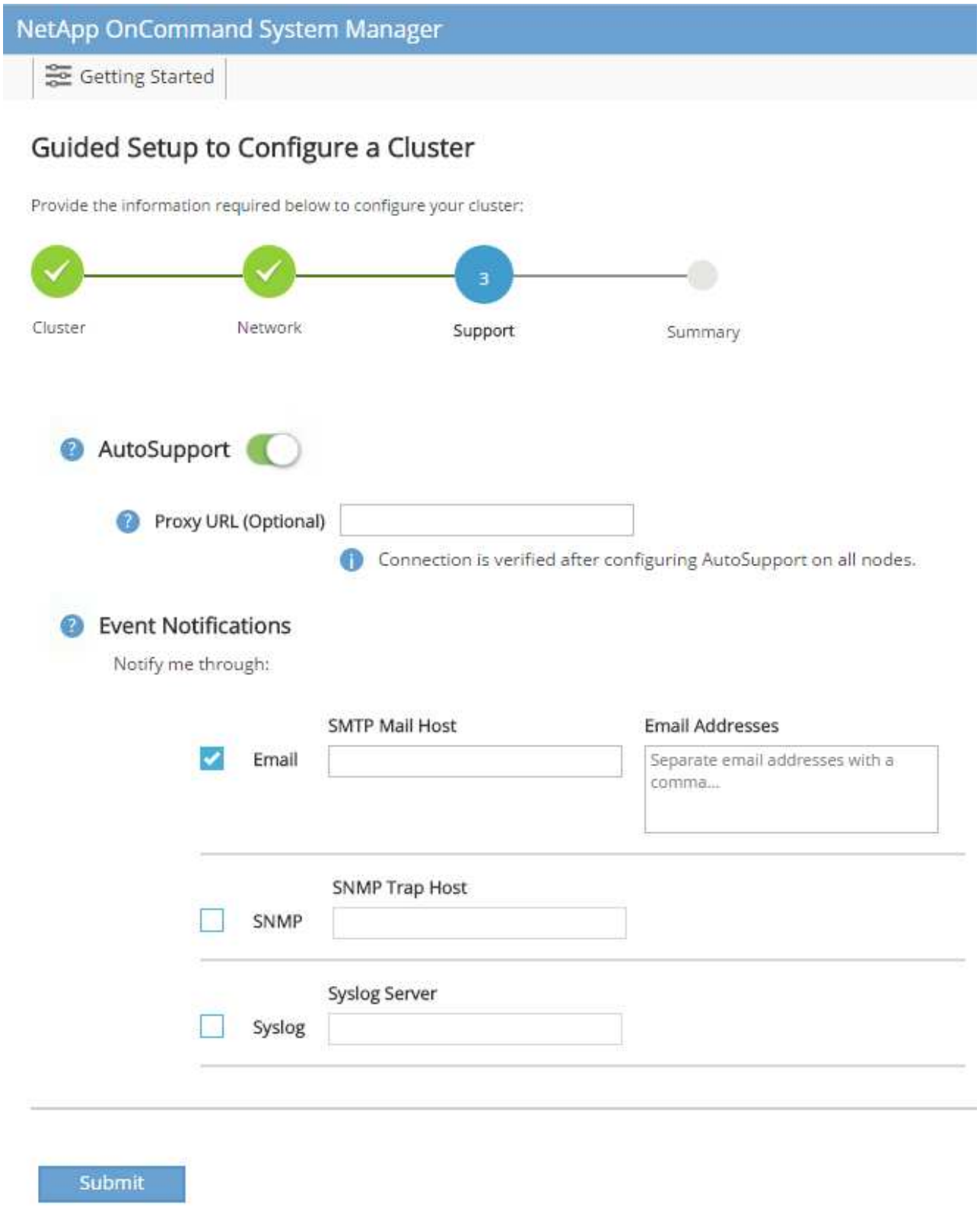
> También puede introducir un servidor NTP alternativo. La dirección IP `10.63.172.162` de `<<var_ntp_server_ip>>` Es el IP de gestión de Nexus.

8. Configure la información de soporte.

a. Si el entorno requiere un proxy para acceder a AutoSupport, introduzca la URL en Proxy URL.

b. Introduzca el host de correo SMTP y la dirección de correo electrónico para las notificaciones de eventos.

> Debe, como mínimo, configurar el método de notificación de eventos antes de continuar. Puede seleccionar cualquiera de los métodos.



Una vez que el sistema indica que ha finalizado la configuración del clúster, haga clic en Manage your Cluster para configurar el almacenamiento.

Continuación de la configuración del clúster de almacenamiento

Después de configurar los nodos de almacenamiento y el clúster base, puede continuar con la configuración del clúster de almacenamiento.

Ponga a cero todos los discos de repuesto

Para poner a cero todos los discos de repuesto del clúster, ejecute el siguiente comando:

```
disk zerospares
```

Configure la personalidad de los puertos UTA2 integrados

1. Compruebe el modo actual y el tipo actual de los puertos ejecutando el `ucadmin show` comando.

```
AFF C190::> ucadmin show
                      Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFF C190_A     0c       cna       target     -        -          online
AFF C190_A     0d       cna       target     -        -          online
AFF C190_A     0e       cna       target     -        -          online
AFF C190_A     0f       cna       target     -        -          online
AFF C190_B     0c       cna       target     -        -          online
AFF C190_B     0d       cna       target     -        -          online
AFF C190_B     0e       cna       target     -        -          online
AFF C190_B     0f       cna       target     -        -          online
8 entries were displayed.
```

2. Compruebe que el modo actual de los puertos que se están utilizando es cna y que el tipo actual está establecido como objetivo. De lo contrario, cambie la personalidad de puerto mediante el siguiente comando:

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

> Los puertos deben estar desconectados para que se ejecute el comando anterior. Para desconectar un puerto, ejecute el siguiente comando:

```
network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down
```

Si ha cambiado la personalidad del puerto, debe reiniciar cada nodo para que el cambio se aplique.

Cambie el nombre de las interfaces lógicas de gestión

Para cambiar el nombre de las interfaces lógicas de gestión (LIF), realice los pasos siguientes:

1. Muestra los nombres de las LIF de gestión actuales.

```
network interface show -vserver <<clustername>>
```

2. Cambie el nombre de la LIF de gestión del clúster.

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_cluster_mgmt_lif_1 -newname cluster_mgmt
```

3. Cambie el nombre del LIF de gestión del nodo B.

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_node_mgmt_lif_AFF C190_B_1 -newname AFF C190-02_mgmt1
```

Configure la reversión automática en la gestión del clúster

Configure el parámetro de reversión automática en la interfaz de gestión del clúster.

```
network interface modify -vserver <<clustername>> -lif cluster_mgmt -auto-
revert true
```

Configure la interfaz de red del procesador de servicios

Para asignar una dirección IPv4 estática al procesador de servicios en cada nodo, ejecute los siguientes comandos:

```
system service-processor network modify -node <<var_nodeA>> -address
-family IPv4 -enable true -dhcp none -ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify -node <<var_nodeB>> -address
-family IPv4 -enable true -dhcp none -ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

Las direcciones IP de Service Processor deben estar en la misma subred que las direcciones IP de gestión de nodos.

Activar la recuperación tras fallos de almacenamiento en ONTAP

Para confirmar que la conmutación por error del almacenamiento está habilitada, ejecute los siguientes comandos de una pareja de conmutación por error:

1. Comprobar el estado de recuperación tras fallos del almacenamiento.

```
storage failover show
```

> Ambas <<var_nodeA>> y.. <<var_nodeB>> debe poder realizar una toma de control. Vaya al paso 3 si los nodos pueden realizar una toma de control.

2. Habilite la conmutación al nodo de respaldo en uno de los dos nodos.

```
storage failover modify -node <<var_nodeA>> -enabled true
```

> Habilitar la conmutación al nodo de respaldo en un solo nodo permite que se produzca en ambos nodos.

3. Compruebe el estado de alta disponibilidad del clúster de dos nodos.

> Este paso no es aplicable para clústeres con más de dos nodos.

```
cluster ha show
```

4. Vaya al paso 6 si está configurada la alta disponibilidad. Si se ha configurado la alta disponibilidad, verá el siguiente mensaje al emitir el comando:

```
High Availability Configured: true
```

5. Habilite el modo de alta disponibilidad solo para el clúster de dos nodos.

> No ejecute este comando para clústeres con más de dos nodos debido a que provoca problemas con la conmutación al nodo de respaldo.

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. Compruebe que la asistencia de hardware está correctamente configurada y, si es necesario, modifique la dirección IP del partner.

```
storage failover hwassist show
```

El mensaje `Keep Alive Status: Error:` indica que una de las controladoras no recibió alertas de hwassist keep alive de su compañero, lo que indica que la asistencia de hardware no está configurada. Ejecute los siguientes comandos para configurar hardware Assist.

```
storage failover modify –hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify –hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

Cree un dominio de retransmisión MTU de trama gigante en ONTAP

Para crear un dominio de retransmisión de datos con un valor MTU de 9000, ejecute los siguientes comandos:

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

Quite los puertos de datos del dominio de retransmisión predeterminado

Los puertos de datos de 10 GbE se utilizan para el tráfico iSCSI/NFS y estos puertos deben eliminarse del dominio predeterminado. Los puertos e0e y e0f no se utilizan y deben eliminarse del dominio predeterminado.

Para quitar puertos del dominio de retransmisión, ejecute el siguiente comando:

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

Deshabilite el control de flujo en los puertos UTA2

Se recomienda utilizar las mejores prácticas de NetApp para deshabilitar el control de flujo en todos los puertos UTA2 conectados a dispositivos externos. Para desactivar el control de flujo, ejecute el siguiente comando:

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
```

Configure el grupo de interfaces LACP en ONTAP

Este tipo de grupo de interfaces requiere dos o más interfaces Ethernet y un switch compatible con LACP. asegúrese de que está configurado según los pasos de esta guía en la sección 5.1.

Desde el símbolo del sistema del clúster, complete los siguientes pasos:

```
ifgrp create -node <<var_nodeA>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0d
ifgrp create -node << var_nodeB>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0d
```

Configure las tramas gigantes en ONTAP

Para configurar un puerto de red ONTAP para que utilice tramas gigantes (normalmente con una MTU de 9,000 bytes), ejecute los siguientes comandos desde el shell del clúster:

```
AFF C190::> network port modify -node node_A -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
AFF C190::> network port modify -node node_B -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
```

Crear VLAN en ONTAP

Para crear VLAN en ONTAP, complete los siguientes pasos:

1. Cree puertos VLAN NFS y añádalos al dominio de retransmisión de datos.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_nfs_vlan_id>>
broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
<<var_nodeA>>:a0a-<<var_nfs_vlan_id>>, <<var_nodeB>>:a0a-
<<var_nfs_vlan_id>>
```

2. Cree puertos VLAN iSCSI y añádalos al dominio de retransmisión de datos.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_A_id>>,<<var_nodeB>>:a0a-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_B_id>>,<<var_nodeB>>:a0a-
<<var_iscsi_vlan_B_id>>
```

3. Cree puertos MGMT-VLAN.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<mgmt_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<mgmt_vlan_id>>
```

Crear agregados de datos en ONTAP

Durante el proceso de configuración de ONTAP, se crea un agregado que contiene el volumen raíz. Para crear agregados adicionales, determine el nombre del agregado, el nodo en el que se creará y el número de discos que contiene.

Para crear agregados, ejecute los siguientes comandos:

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

Conserve al menos un disco (seleccione el disco más grande) en la configuración como un repuesto. Una práctica recomendada es tener al menos un repuesto para cada tipo y tamaño de disco.

Empiece con cinco discos; puede añadir discos a un agregado cuando necesite almacenamiento adicional.

No se puede crear el agregado hasta que se complete el establecimiento en cero del disco. Ejecute el `aggr show` comando para mostrar el estado de creación del agregado. No continúe hasta que aggr1_NODEA esté en línea.

Configurar la zona horaria en ONTAP

Para configurar la sincronización horaria y establecer la zona horaria en el clúster, ejecute el siguiente comando:

```
timezone <<var_timezone>>
```

Por ejemplo, en el este de Estados Unidos, la zona horaria es América/Nueva York. Cuando haya comenzado a escribir el nombre de la zona horaria, pulse la tecla TAB para ver las opciones disponibles.

Configurar SNMP en ONTAP

Para configurar SNMP, realice los siguientes pasos:

1. Configure la información básica de SNMP, como la ubicación y el contacto. Cuando se sondean, esta información es visible como `sysLocation` y.. `sysContact` Variables en SNMP.

   ```
   snmp contact <<var_snmp_contact>>
   snmp location "<<var_snmp_location>>"
   snmp init 1
   options snmp.enable on
   ```

2. Configure las capturas SNMP para que se envíen a hosts remotos.

   ```
   snmp traphost add <<var_snmp_server_fqdn>>
   ```

Configure SNMPv1 en ONTAP

Para configurar SNMPv1, establezca la contraseña de texto sin formato secreta compartida denominada comunidad.

```
snmp community add ro <<var_snmp_community>>
```

Utilice la `snmp community delete all` comando con precaución. Si se utilizan cadenas de comunidad para otros productos de supervisión, este comando las quita.

Configure SNMPv3 en ONTAP

SNMPv3 requiere que defina y configure un usuario para la autenticación. Para configurar SNMPv3, lleve a cabo los siguientes pasos:

1. Ejecute el `security snmpusers` Comando para ver el ID del motor.
2. Cree un usuario llamado `snmpv3user`.

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. Introduzca el ID de motor de la entidad autorizada y seleccione md5 como protocolo de autenticación.
4. Escriba una contraseña de longitud mínima de ocho caracteres para el protocolo de autenticación cuando se le solicite.
5. Seleccione des como protocolo de privacidad.
6. Escriba una contraseña de longitud mínima de ocho caracteres para el protocolo de privacidad cuando se le solicite.

Configure HTTPS de AutoSupport en ONTAP

La herramienta AutoSupport de NetApp envía información de resumen de soporte a NetApp mediante HTTPS. Para configurar AutoSupport, ejecute el siguiente comando:

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

Cree una máquina virtual de almacenamiento

Para crear una máquina virtual de almacenamiento (SVM) de infraestructura, complete los siguientes pasos:

1. Ejecute el `vserver create` comando.

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume-security-style unix
```

2. Añada el agregado de datos a la lista de agregados de infra-SVM para VSC de NetApp.

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. Elimine los protocolos de almacenamiento que no se utilicen de la SVM, con lo que dejará NFS e iSCSI.

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. Habilite y ejecute el protocolo NFS en la SVM de infra-SVM.

```
nfs create -vserver Infra-SVM -udp disabled
```

5. Encienda la `SVM vstorage` Parámetro para el plugin VAAI para NFS de NetApp. A continuación, compruebe que NFS se ha configurado.

```
vserver nfs modify –vserver Infra-SVM –vstorage enabled
vserver nfs show
```

Los comandos están precedidos por `vserver` En la línea de comandos, debido a que las SVM se denominaban previamente vServers.

Configure NFSv3 en ONTAP

En la siguiente tabla, se enumera la información necesaria para completar esta configuración.

Detalles	Valor de detalle
Host ESXi dirección IP de NFS	<<var_esxi_hostA_nfs_ip>>
Dirección IP de NFS del host ESXi B	<<var_esxi_hostB_nfs_ip>>

Para configurar NFS en la SVM, ejecute los siguientes comandos:

1. Cree una regla para cada host ESXi en la política de exportación predeterminada.
2. Asigne una regla para cada host ESXi que se cree. Cada host tiene su propio índice de reglas. El primer host ESXi tiene el índice de regla 1, el segundo host ESXi tiene el índice de regla 2, etc.

```
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 1 –protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 2 –protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule show
```

3. Asigne la política de exportación al volumen raíz de la SVM de infraestructura.

```
volume modify –vserver Infra-SVM –volume rootvol –policy default
```

VSC de NetApp gestiona automáticamente las políticas de exportación si decide instalarlas después de configurar vSphere. Si no lo instala, debe crear reglas de políticas de exportación cuando se añadan servidores C-Series de Cisco UCS adicionales.

Cree el servicio iSCSI en ONTAP

Para crear el servicio iSCSI en la SVM, ejecute el comando siguiente. Este comando también inicia el servicio iSCSI y establece el IQN de iSCSI para la SVM. Comprobar que iSCSI se ha configurado.

```
iscsi create -vserver Infra-SVM
iscsi show
```

Crear reflejo de uso compartido de carga del volumen raíz de la SVM en ONTAP

Para crear un reflejo de uso compartido de carga del volumen raíz de la SVM en ONTAP, complete los pasos siguientes:

1. Cree un volumen para que sea el reflejo de uso compartido de carga del volumen raíz de la SVM de infraestructura en cada nodo.

```
volume create –vserver Infra_Vserver –volume rootvol_m01 –aggregate
aggr1_nodeA –size 1GB –type DP
volume create –vserver Infra_Vserver –volume rootvol_m02 –aggregate
aggr1_nodeB –size 1GB –type DP
```

2. Crear una programación de tareas para actualizar las relaciones de mirroring del volumen raíz cada 15 minutos.

```
job schedule interval create -name 15min -minutes 15
```

3. Cree las relaciones de mirroring.

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

4. Inicialice la relación de mirroring y compruebe que se haya creado.

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol
snapmirror show
```

Configure el acceso HTTPS en ONTAP

Para configurar el acceso seguro a la controladora de almacenamiento, lleve a cabo los siguientes pasos:

1. Aumente el nivel de privilegio para acceder a los comandos de certificado.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. En general, ya se encuentra en funcionamiento un certificado autofirmado. Verifique el certificado ejecutando el siguiente comando:

```
security certificate show
```

3. Para cada SVM que se muestra, el nombre común de certificado debe coincidir con el FQDN de DNS de la SVM. Los cuatro certificados predeterminados deben eliminarse y sustituirse por certificados autofirmados o certificados de una entidad de certificación.

> La práctica recomendada es eliminar certificados caducados antes de crear certificados. Ejecute el `security certificate delete` comando para eliminar certificados caducados. En el siguiente comando, use LA TABULACIÓN automática para seleccionar y eliminar cada certificado predeterminado.

```
security certificate delete [TAB] …
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM -type server -serial 552429A6
```

4. Para generar e instalar certificados autofirmados, ejecute los siguientes comandos como comandos de una sola vez. Generar un certificado de servidor para la SVM de infraestructura y la SVM de clúster. De nuevo, utilice LA TABULACIÓN automática como ayuda para completar estos comandos.

```
security certificate create [TAB] …
Example: security certificate create -common-name infra-svm.netapp.com
-type server -size 2048 -country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email-addr
"abc@netapp.com" -expire-days 3650 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. Para obtener los valores de los parámetros requeridos en el siguiente paso, ejecute el comando Security certificate show.
6. Habilite cada certificado que se acaba de crear mediante el `-server-enabled true` y.. `-client-enabled false` parámetros. De nuevo, utilice LA TABULACIÓN automática.

```
security ssl modify [TAB] …
Example: security ssl modify -vserver Infra-SVM -server-enabled true
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common
-name infra-svm.netapp.com
```

7. Configure y habilite el acceso SSL y HTTPS y deshabilite el acceso HTTP.

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http
-vserver <<var_clustername>>
```

Es normal que algunos de estos comandos devuelvan un mensaje de error indicando que la entrada no existe.

8. Vuelva al nivel de privilegio de administrador y cree la configuración para permitir que la SVM esté disponible en la web.

```
set –privilege admin
vserver services web modify –name spi –vserver * -enabled true
```

Cree un volumen de FlexVol de NetApp en ONTAP

Para crear un volumen FlexVol® de NetApp, introduzca el nombre del volumen, el tamaño y el agregado en el que existe. Crear dos volúmenes de almacenes de datos de VMware y un volumen de arranque del servidor.

```
volume create -vserver Infra-SVM -volume infra_datastore -aggregate
aggr1_nodeB -size 500GB -state online -policy default -junction-path
/infra_datastore -space-guarantee none -percent-snapshot-space 0
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -junction-path /infra_swap
-space-guarantee none -percent-snapshot-space 0 -snapshot-policy none
-efficiency-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

Crear LUN en ONTAP

Para crear dos LUN de arranque, ejecute los siguientes comandos:

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware -space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware -space-reserve disabled
```

Cuando se añade un servidor Cisco UCS C-Series adicional, debe crear una LUN de arranque adicional.

Creación de LIF iSCSI en ONTAP

En la siguiente tabla, se enumera la información necesaria para completar esta configuración.

Detalles	Valor de detalle
Nodo de almacenamiento a iSCSI LIF01A	<<var_nodeA_iscsi_lif01a_ip>>
Nodo de almacenamiento: Una máscara de red LIF01A de iSCSI	<<var_nodeA_iscsi_lif01a_mask>>
Nodo de almacenamiento a iSCSI LIF01B	<<var_nodeA_iscsi_lif01b_ip>>
Nodo de almacenamiento a máscara de red LIF01B de iSCSI	<<var_nodeA_iscsi_lif01b_mask>>
Nodo de almacenamiento B iSCSI LIF01A	<<var_nodeB_iscsi_lif01a_ip>>
Máscara de red del nodo de almacenamiento B iSCSI LIF01A	<<var_nodeB_iscsi_lif01a_mask>>
ISCSI LIF01B del nodo de almacenamiento	<<var_nodeB_iscsi_lif01b_ip>>
Máscara de red LIF01B de nodo de almacenamiento B.	<<var_nodeB_iscsi_lif01b_mask>>

Creación de cuatro LIF iSCSI, dos en cada nodo.

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface show
```

Creación de LIF NFS en ONTAP

En la siguiente tabla, se enumera la información necesaria para completar esta configuración.

Detalles	Valor de detalle
Nodo de almacenamiento: LIF NFS 01 IP	<<var_nodeA_nfs_lif_01_ip>>
Nodo de almacenamiento máscara de red a LIF 01 de NFS	<<var_nodeA_nfs_lif_01_mask>>
Nodo de almacenamiento B LIF NFS 02 IP	<<var_nodeB_nfs_lif_02_ip>>
Máscara de red del nodo de almacenamiento B LIF NFS 02	<<var_nodeB_nfs_lif_02_mask>>

Cree una LIF NFS.

```
network interface create -vserver Infra-SVM -lif nfs_lif01 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_ip>> -netmask <<
var_nodeA_nfs_lif_01_mask>> -status-admin up –failover-policy broadcast-
domain-wide –firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> –address <<var_nodeB_nfs_lif_02_ip>> -netmask <<
var_nodeB_nfs_lif_02_mask>> -status-admin up –failover-policy broadcast-
domain-wide –firewall-policy data –auto-revert true
network interface show
```

Añadir un administrador de SVM de infraestructura

En la siguiente tabla, se enumera la información necesaria para añadir un administrador de SVM.

Detalles	Valor de detalle
IP de Vsmgmt	<<var_svm_mgmt_ip>>
Máscara de red Vsmgmt	<<var_svm_mgmt_mask>>
Puerta de enlace predeterminada de Vsmgmt	<<var_svm_mgmt_gateway>>

Para añadir la interfaz lógica de administración de SVM y el administrador de SVM de la infraestructura a la red de gestión, realice los siguientes pasos:

1. Ejecute el siguiente comando:

```
network interface create –vserver Infra-SVM –lif vsmgmt –role data
–data-protocol none –home-node <<var_nodeB>> -home-port  e0M –address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> -status-admin up
–failover-policy broadcast-domain-wide –firewall-policy mgmt –auto-
revert true
```

> La IP de administración de SVM aquí debe estar en la misma subred que la IP de administración del clúster de almacenamiento.

2. Cree una ruta predeterminada para permitir que la interfaz de gestión de SVM llegue al mundo exterior.

```
network route create –vserver Infra-SVM -destination 0.0.0.0/0 –gateway
<<var_svm_mgmt_gateway>>
network route show
```

3. Establezca una contraseña para el usuario de SVM vsadmin y desbloquee el usuario.

```
security login password –username vsadmin –vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock –username vsadmin –vserver Infra-SVM
```

"A continuación, ponga en marcha el servidor en rack C-Series de Cisco UCS."

Poner en marcha el servidor de montaje en rack Cisco UCS C-Series

En esta sección, se proporciona un procedimiento detallado para configurar un servidor de rack independiente Cisco UCS C-Series para su uso en la configuración exprés de FlexPod.

Realice la configuración inicial del servidor independiente Cisco UCS C-Series para CIMC

Complete estos pasos para la configuración inicial de la interfaz de CIMC para servidores independientes Cisco UCS C-Series.

En la siguiente tabla se enumera la información necesaria para configurar CIMC para cada servidor independiente Cisco UCS C-Series.

Detalles	Valor de detalle
Dirección IP de CIMC	<<cimc_ip>>
Máscara de subred CIMC	\<<cimc_netmask
Puerta de enlace predeterminada CIMC	<<cimc_gateway>>

La versión de CIMC utilizada en esta validación es CIMC 4.0.(4).

Todos los servidores

1. Conecte la mochila del teclado, vídeo y ratón (KVM) de Cisco (suministrada con el servidor) al puerto KVM de la parte frontal del servidor. Conecte un monitor VGA y un teclado USB a los puertos de mochila KVM adecuados.

   Encienda el servidor y pulse F8 cuando se le solicite que introduzca la configuración de CIMC.



2. En la utilidad de configuración de CIMC, defina las siguientes opciones:
   a. Modo de tarjeta de interfaz de red (NIC):

      Específico `[X]`

   b. IP (básico):

      IPV4: `[X]`

      DHCP habilitado: `[ ]`

      IP DE CIMC: `<<cimc_ip>>`

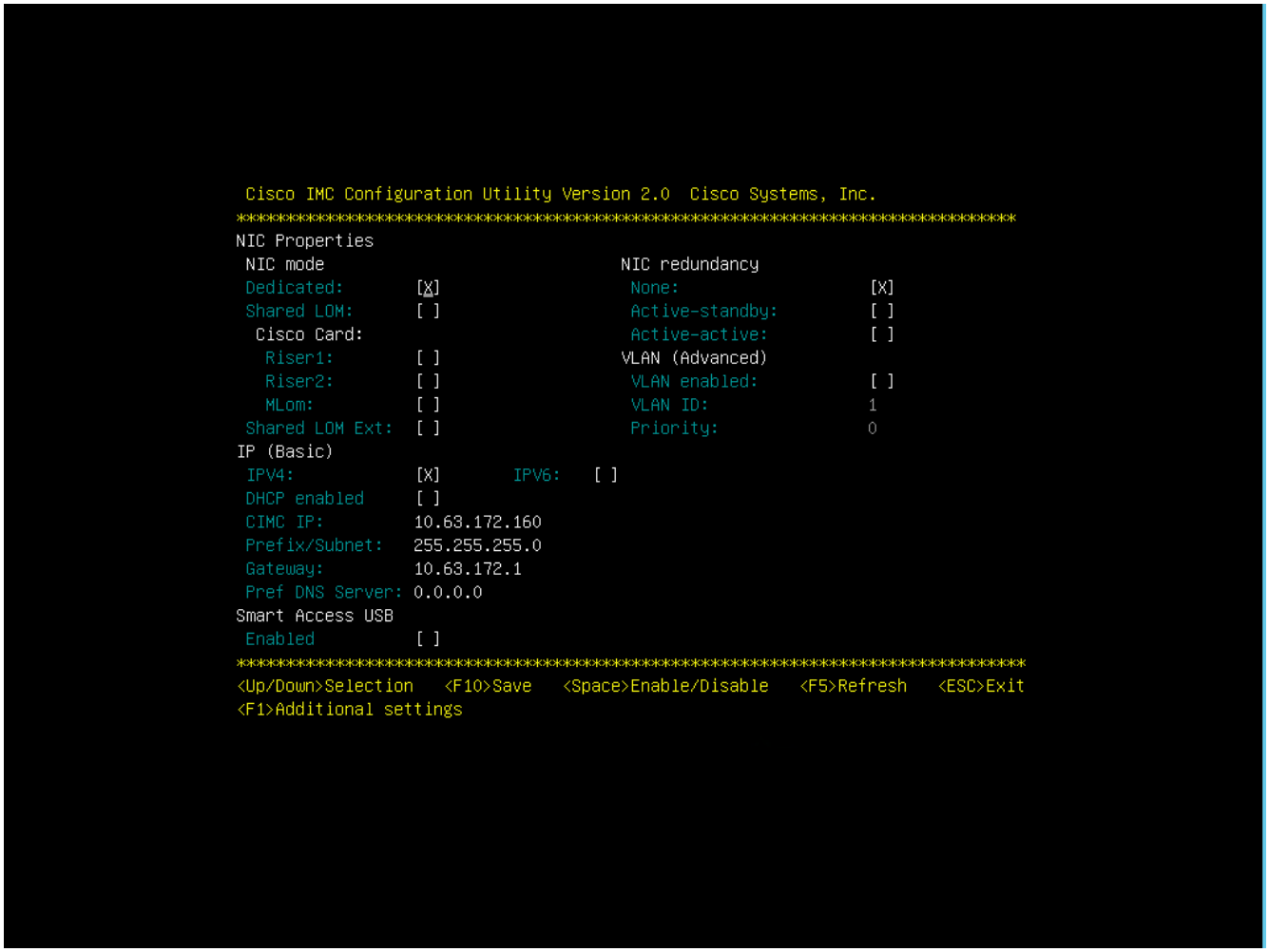
      Prefijo/subred: `<<cimc_netmask>>`

      Puerta de enlace: `<<cimc_gateway>>`

   c. VLAN (Advanced): Deje borrado para deshabilitar el etiquetado VLAN.

      Redundancia NIC

      Ninguna: `[X]`



3. Pulse F1 para ver los ajustes adicionales:
   a. Propiedades comunes:

      Nombre de host: `<<esxi_host_name>>`

      DNS dinámico: `[ ]`

      Valores predeterminados de fábrica: Dejar borrado.

   b. Usuario predeterminado (básico):

      Contraseña predeterminada: `<<admin_password>>`

      Vuelva a introducir la contraseña: `<<admin_password>>`

      Propiedades del puerto: Utilice los valores predeterminados.

   Perfiles de puerto: Dejar borrado.
4. Pulse F10 para guardar la configuración de la interfaz CIMC.
5. Una vez guardada la configuración, pulse Esc para salir.

Configurar arranque iSCSI de servidores Cisco UCS C-Series

En esta configuración de FlexPod Express, la VIC1457 se utiliza para el arranque iSCSI.

La tabla siguiente enumera la información necesaria para configurar el arranque iSCSI.

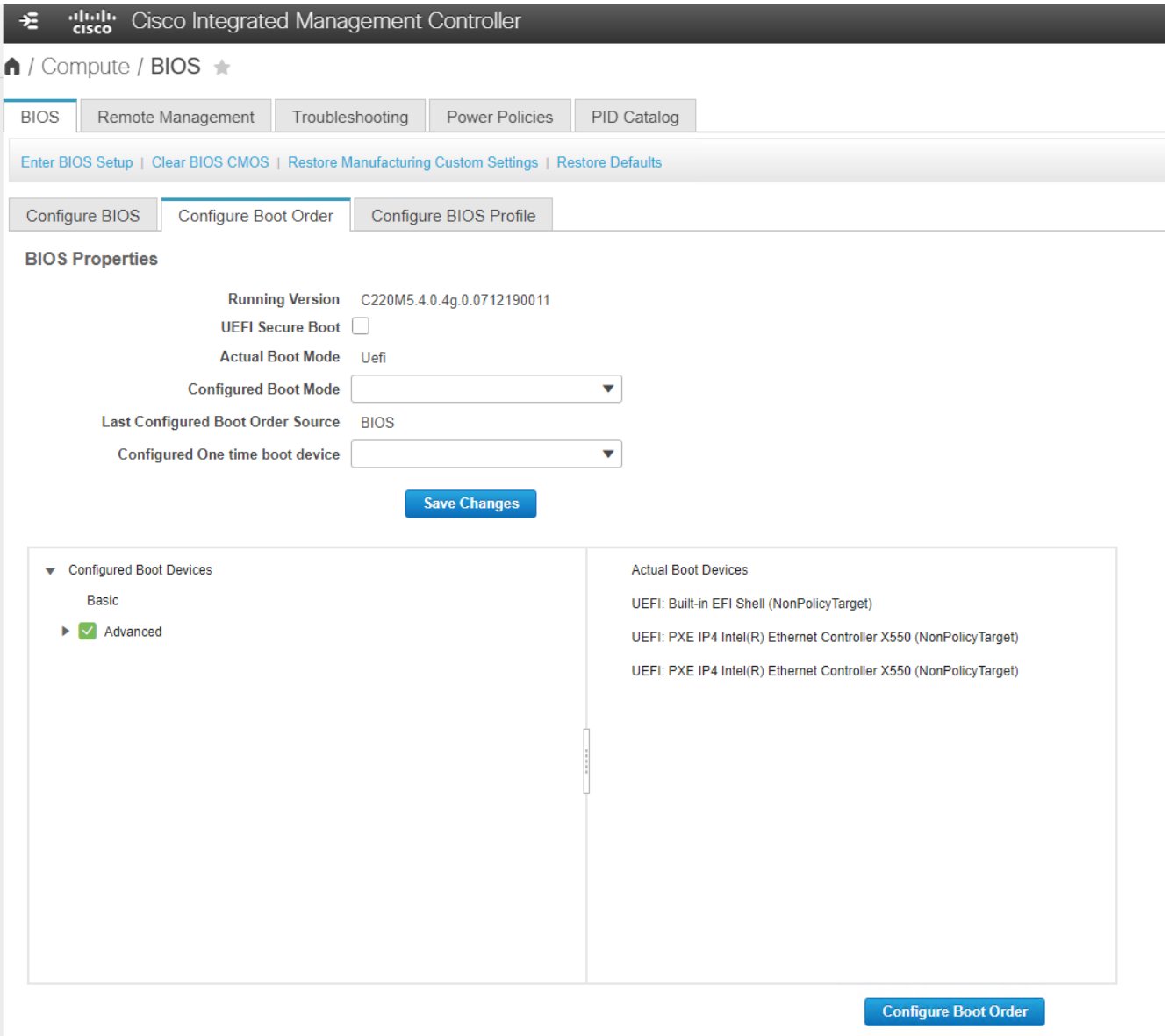
Un font en cursiva indica variables que son únicas para cada host ESXi.

Detalles	Valor de detalle
Nombre Del iniciador del host ESXi	<<var_ucs_initiator_name_A>>
Host ESXi iSCSI-A IP	<<var_esxi_host_iscsiA_ip>>
Máscara de red iSCSI-A del host ESXi	<<var_esxi_host_iscsiA_mask>>
ISCSI del host ESXi: Puerta de enlace predeterminada	<<var_esxi_host_iscsiA_gateway>>
Nombre B del iniciador del host ESXi	<<var_ucs_initiator_name_B>>
Host ESXi iSCSI-B IP	<<var_esxi_host_iscsiB_ip>>
Máscara de red iSCSI-B del host ESXi	<<var_esxi_host_iscsiB_mask>>
Puerta de enlace iSCSI-B del host ESXi	<<var_esxi_host_iscsiB_gateway>>
Dirección IP iscsi_lif01a	<<var_iscsi_lif01a>>
Dirección IP iscsi_lif02a	<<var_iscsi_lif02a>>
Dirección IP iscsi_lif01b	<<var_iscsi_lif01b>>
Dirección IP iscsi_lif02b	<<var_iscsi_lif02b>>
IQN de infr_SVM	<<var_SVM_IQN>>

Configuración del orden de arranque

Para establecer la configuración del orden de arranque, lleve a cabo los siguientes pasos:

1. En la ventana del navegador de la interfaz CIMC, haga clic en la ficha Compute (computación) y seleccione BIOS.
2. Haga clic en Configurar orden de arranque y, a continuación, en Aceptar.



3. Configure los siguientes dispositivos haciendo clic en el dispositivo en Agregar dispositivo de arranque y yendo a la ficha Opciones avanzadas:

   a. Agregar medios virtuales:

      NOMBRE: KVM-CD-DVD

      SUBTIPO: DVD KVM ASIGNADO

      Estado: Habilitado

      Orden: 1

   b. Agregar arranque iSCSI:

      Nombre: ISCSI-a

      Estado: Habilitado

      Orden: 2

Ranura: MLOM

Puerto: 1

c. Haga clic en Add iSCSI Boot:

Nombre: ISCSI-B

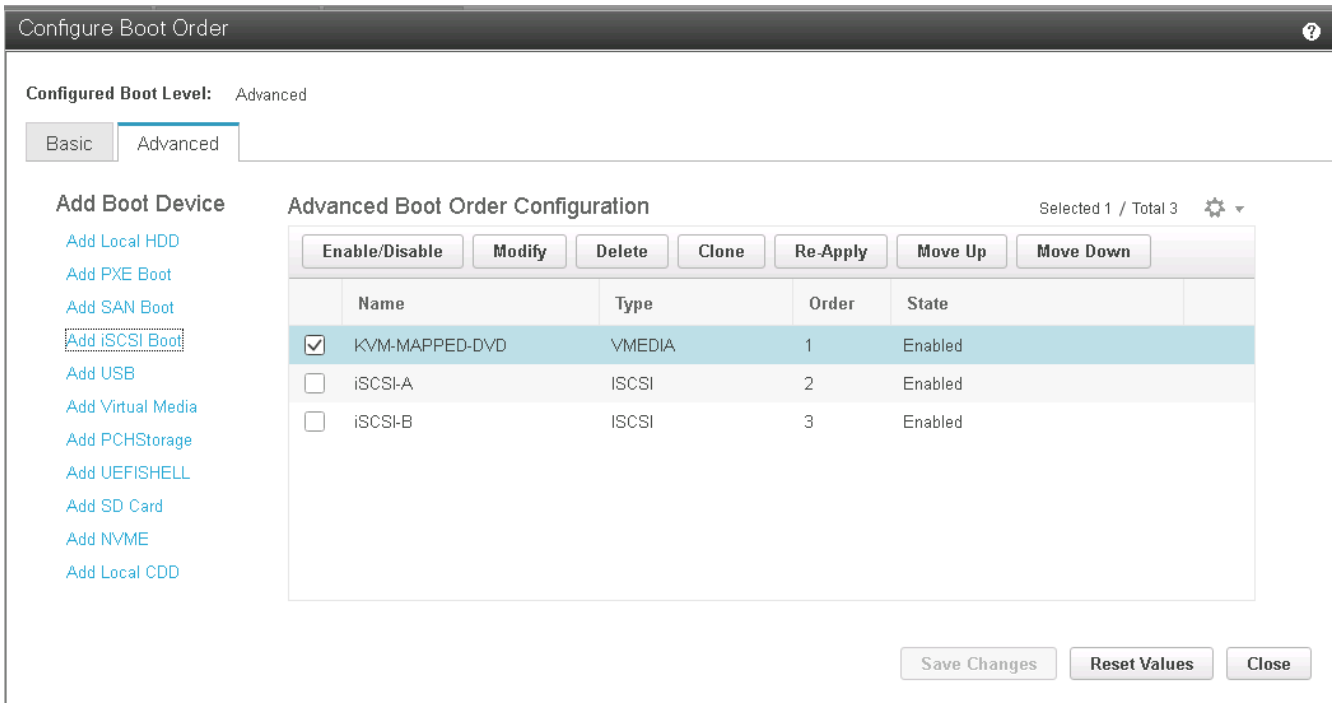
Estado: Habilitado

Pedido: 3

Ranura: MLOM

Puerto: 3

4. Haga clic en Agregar dispositivo.
5. Haga clic en Save Changes y, a continuación, en Close.

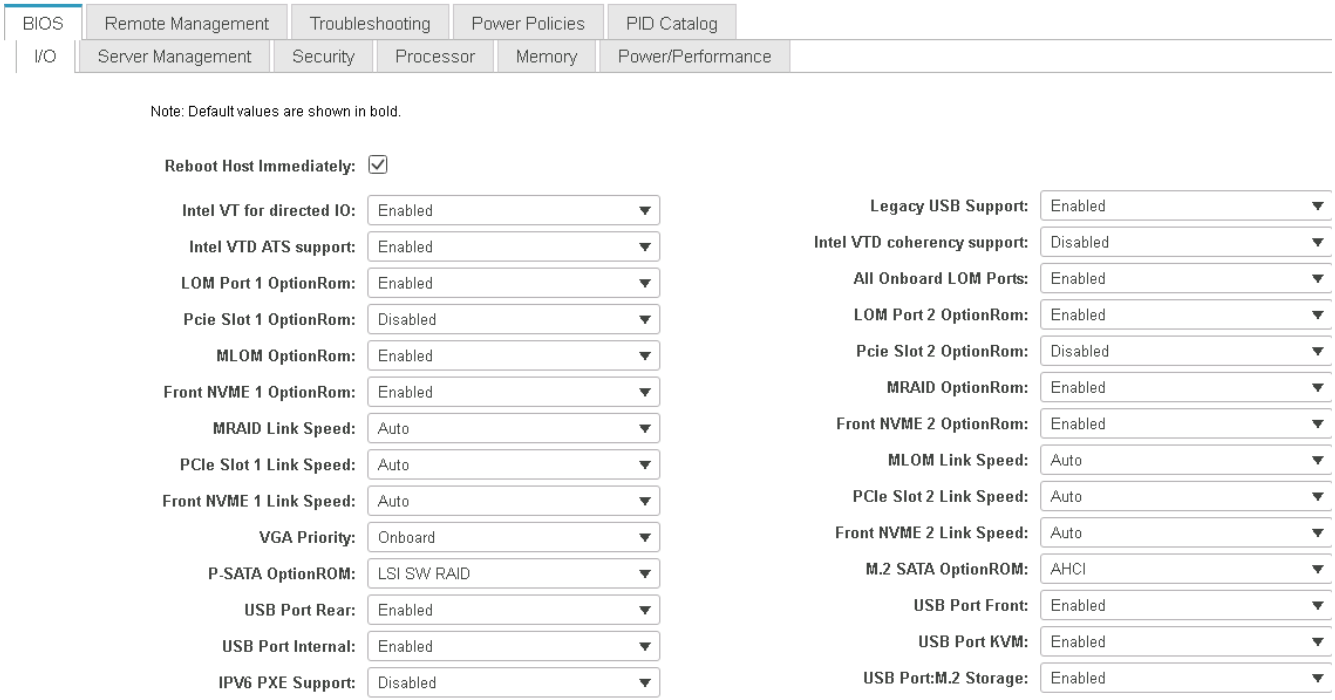


6. Reinicie el servidor para arrancar con el nuevo orden de inicio.

Desactivar la controladora RAID (si existe)

Siga estos pasos si el servidor C-Series contiene una controladora RAID. No se necesita una controladora RAID en el arranque desde la configuración SAN. De manera opcional, también puede quitar físicamente la controladora RAID del servidor.

1. En la pestaña Compute, haga clic en BIOS en el panel de navegación izquierdo de CIMC.
2. Seleccione Configurar BIOS.
3. Desplácese hacia abajo hasta la ranura PCIe:ROM de opción HBA.
4. Si el valor no está desactivado, configúrelo en Desactivado.

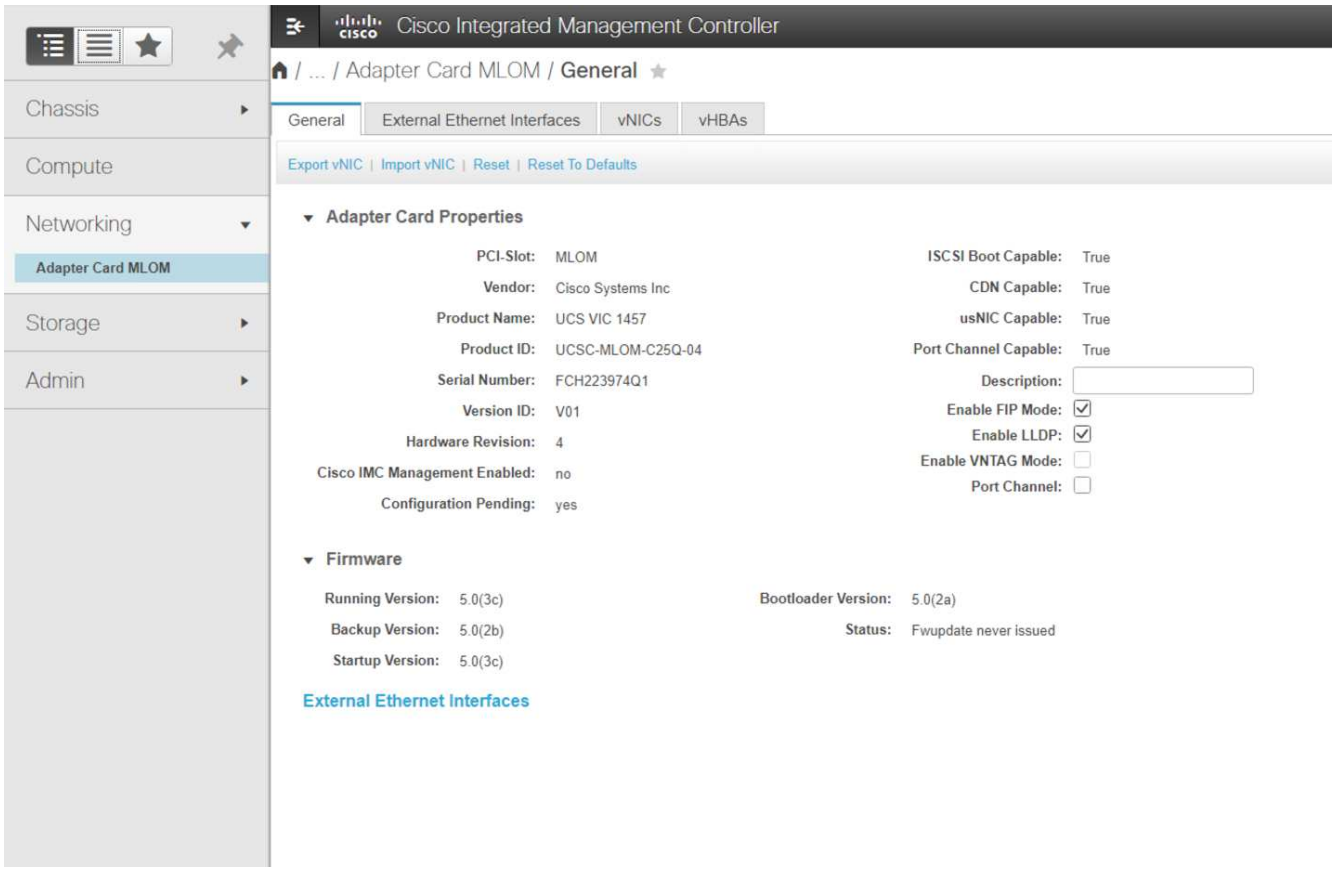


Configurar Cisco VIC1457 para el arranque iSCSI

Los pasos de configuración siguientes son para el VIC 1457 de Cisco para arranque iSCSI.

> La canalización de puertos predeterminada entre los puertos 0, 1, 2 y 3 se debe desactivar antes de poder configurar los cuatro puertos individuales. Si la canalización del puerto no está desactivada, sólo aparecen dos puertos para el VIC 1457. Realice los siguientes pasos para activar el canal de puerto en el CIMC:

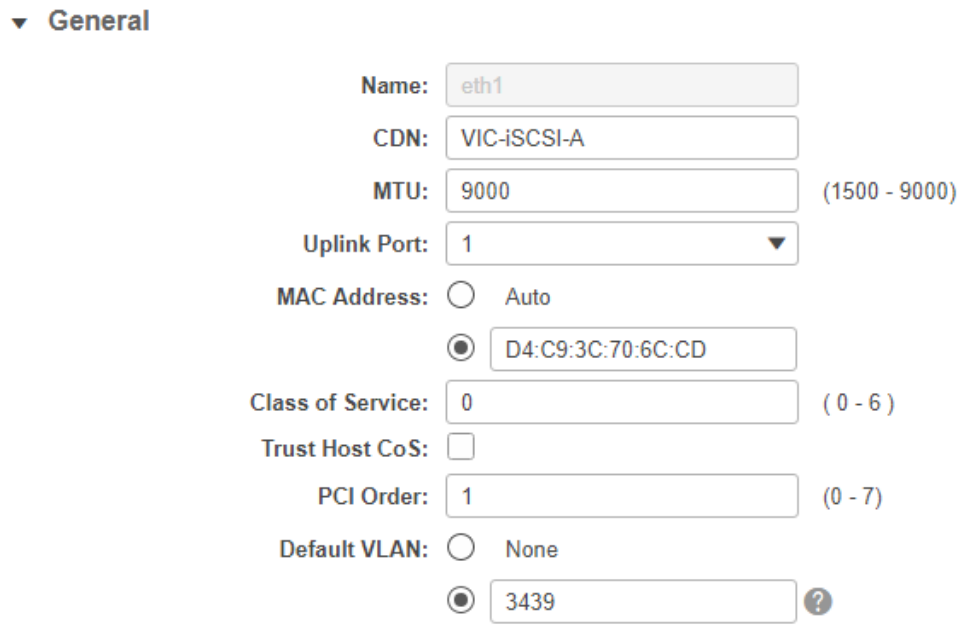
1. En la ficha redes, haga clic en la tarjeta adaptadora MLOM.
2. En la ficha General, desactive el canal de puerto.
3. Guarde los cambios y reinicie el CIMC.



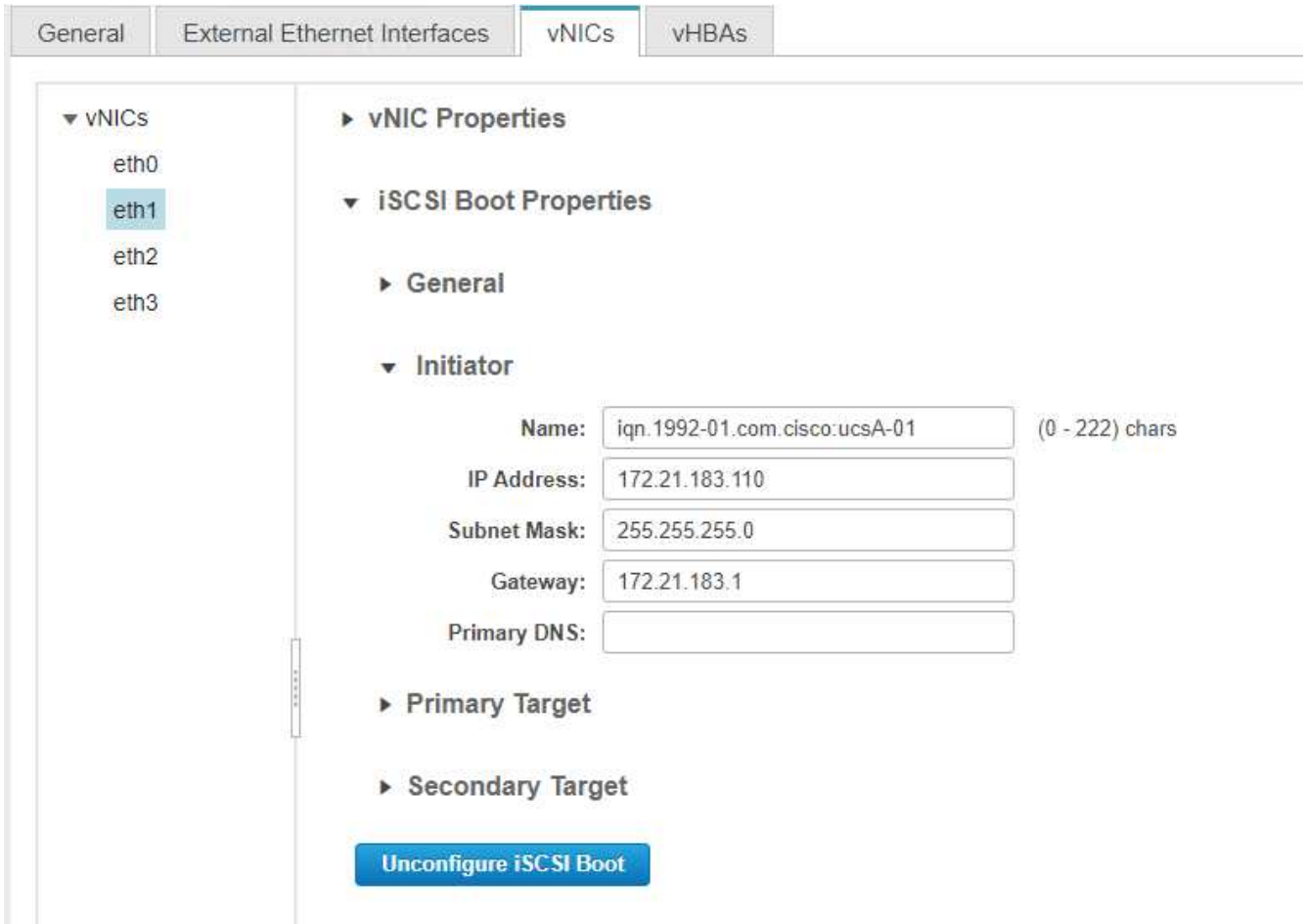
Cree NIC iSCSI

Para crear VNIC iSCSI, lleve a cabo los siguientes pasos:

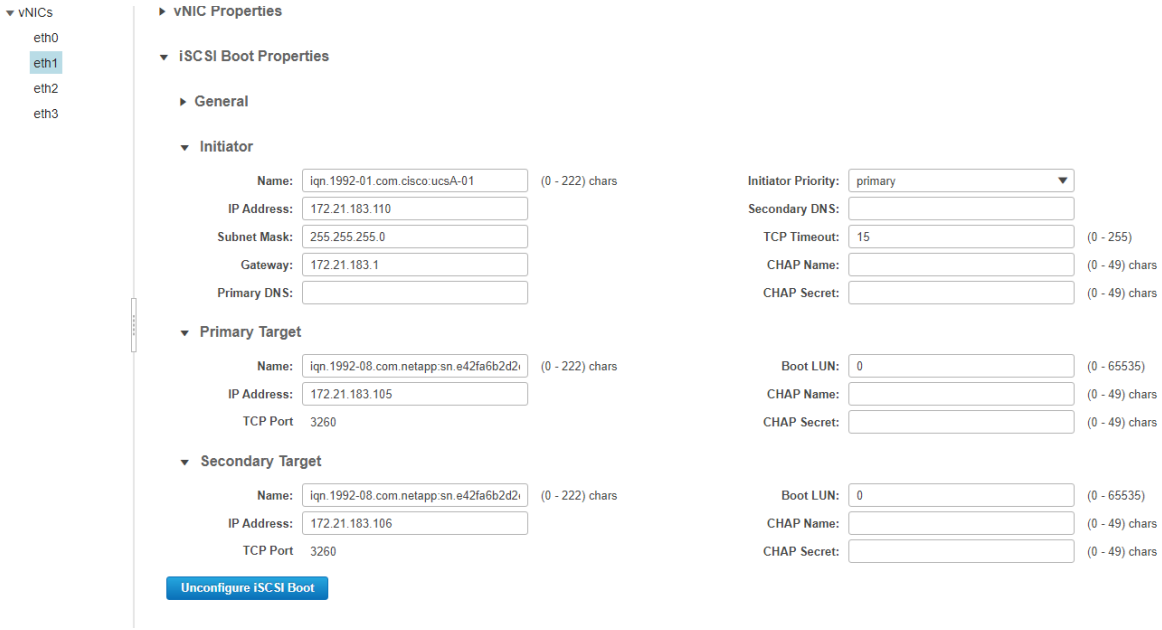
1. En la ficha redes, haga clic en adaptador de tarjeta MLOM.
2. Haga clic en Agregar VNIC para crear un VNIC.
3. En la sección Agregar VNIC, introduzca los siguientes ajustes:
   - Nombre: Eth1
   - Nombre de CDN: ISCSI-VNIC-A
   - MTU: 9000
   - VLAN predeterminada: `<<var_iscsi_vlan_a>>`
   - Modo VLAN: TRONCO
   - Activar inicio PXE: Comprobación
4. Haga clic en Agregar VNIC y, a continuación, en Aceptar.
5. Repita el proceso para agregar un segundo VNIC:
   - Asigne un nombre al VNIC eth3.
   - Nombre de CDN: ISCSI-VNIC-B
   - Introduzca `<<var_iscsi_vlan_b>>` Como VLAN.
   - Establezca el puerto de enlace ascendente en 3.



6. Seleccione el eth1 de VNIC a la izquierda.



7. En Propiedades de arranque iSCSI, introduzca los detalles del iniciador:
   - Nombre: `<<var_ucsa_initiator_name_a>>`
   - Dirección IP: `<<var_esxi_hostA_iscsiA_ip>>`
   - Máscara de subred: `<<var_esxi_hostA_iscsiA_mask>>`
   - Puerta de enlace: `<<var_esxi_hostA_iscsiA_gateway>>`



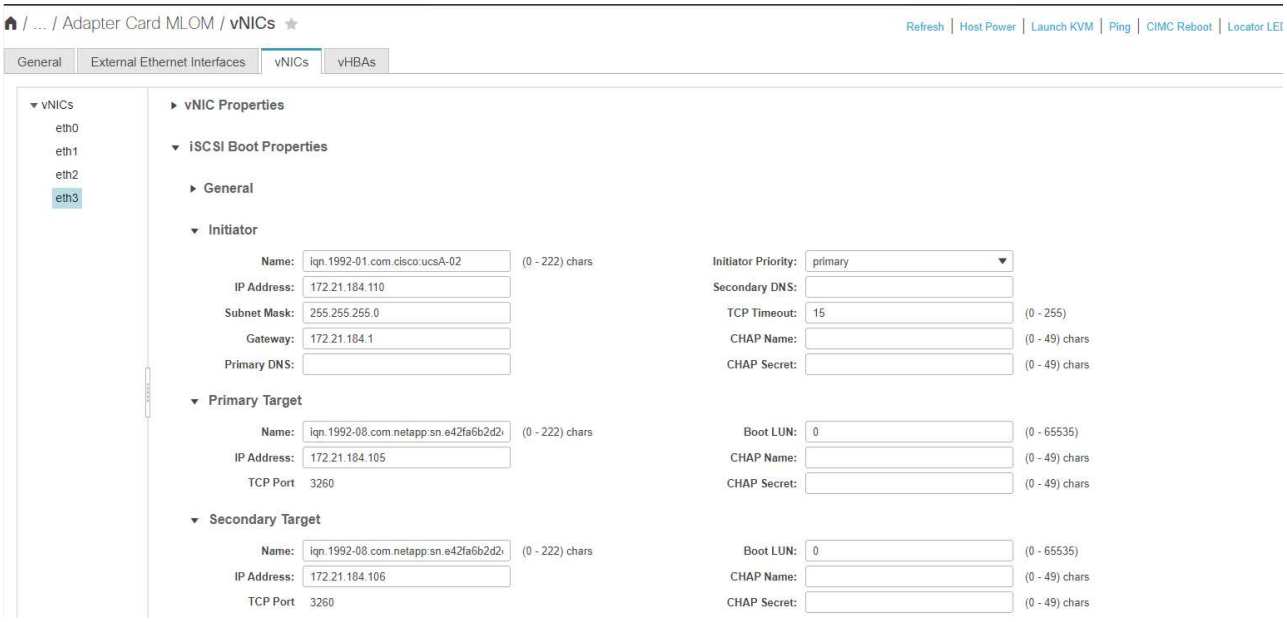
8. Introduzca los detalles del destino principal:
   - Nombre: Número IQN de infra-SVM
   - Dirección IP: Dirección IP de iscsi_lif01a
   - LUN de arranque: 0
9. Introduzca los detalles del destino secundario:
   - Nombre: Número IQN de infra-SVM
   - Dirección IP: Dirección IP de iscsi_lif02a
   - LUN de arranque:0

> Puede obtener el número IQN de almacenamiento ejecutando el `vserver iscsi show` comando.

> Asegúrese de registrar los nombres IQN de cada VNIC. Se necesitan para un paso más adelante. Además, los nombres IQN para los iniciadores deben ser únicos para cada servidor y para el VNIC de iSCSI.

10. Haga clic en Save Changes.
11. Seleccione VNIC eth3 y haga clic en el botón de inicio iSCSI que se encuentra en la parte superior de la sección interfaces de Ethernet del host.
12. Repita el proceso para configurar eth3.

13. Introduzca los detalles del iniciador:
    - Nombre: `<<var_ucsa_initiator_name_b>>`
    - Dirección IP: `<<var_esxi_hostb_iscsib_ip>>`
    - Máscara de subred: `<<var_esxi_hostb_iscsib_mask>>`
    - Puerta de enlace: `<<var_esxi_hostb_iscsib_gateway>>`



14. Introduzca los detalles del destino principal:
    - Nombre: Número IQN de infra-SVM
    - Dirección IP: Dirección IP de iscsi_lif01b
    - LUN de arranque: 0
15. Introduzca los detalles del destino secundario:
    - Nombre: Número IQN de infra-SVM
    - Dirección IP: Dirección IP de iscsi_lif02b
    - LUN de arranque: 0

> Puede obtener el número de IQN de almacenamiento mediante el `vserver iscsi show` comando.

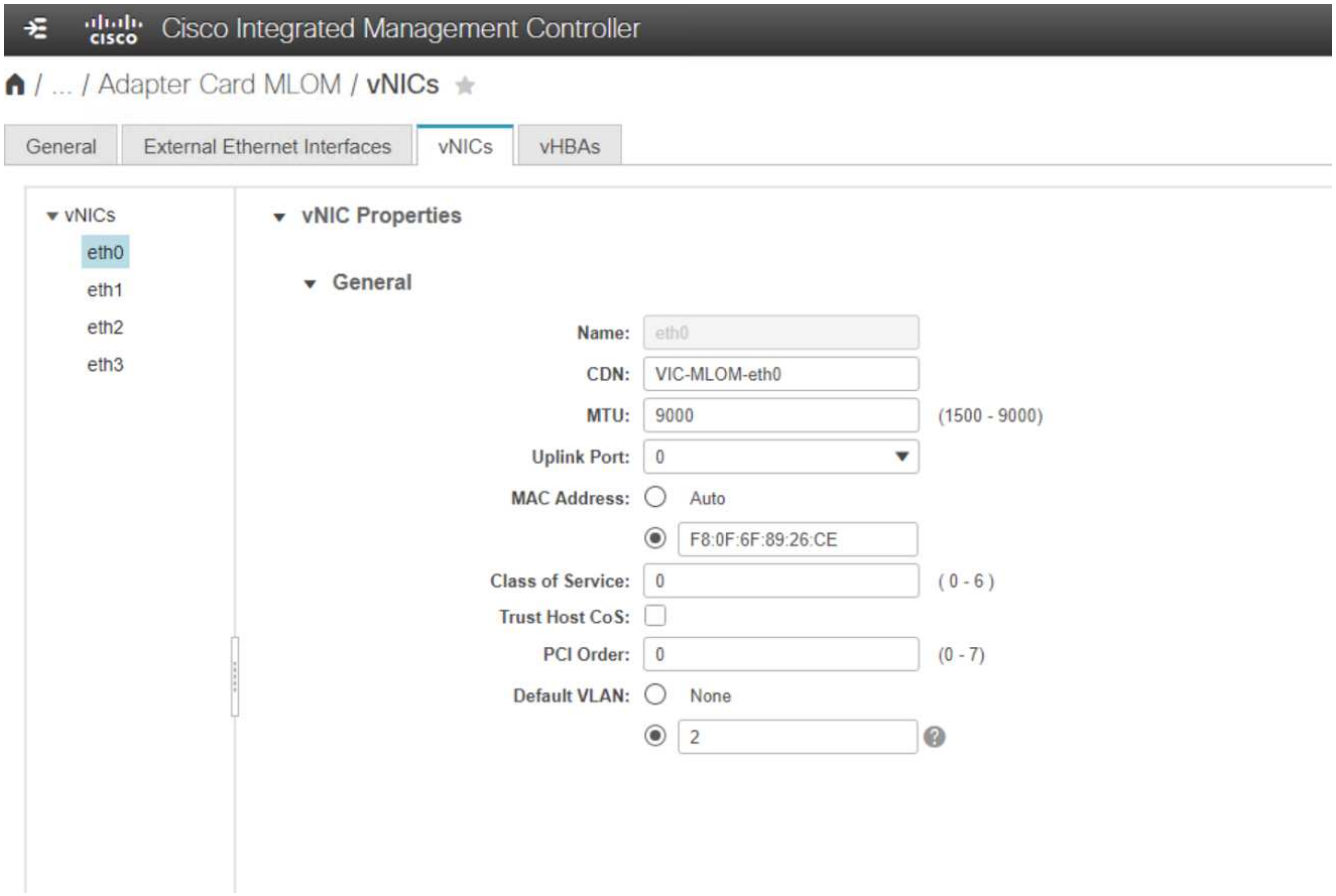
> Asegúrese de registrar los nombres IQN de cada VNIC. Se necesitan para un paso más adelante.

16. Haga clic en Save Changes.
17. Repita este proceso para configurar el arranque iSCSI para el servidor Cisco UCS B.

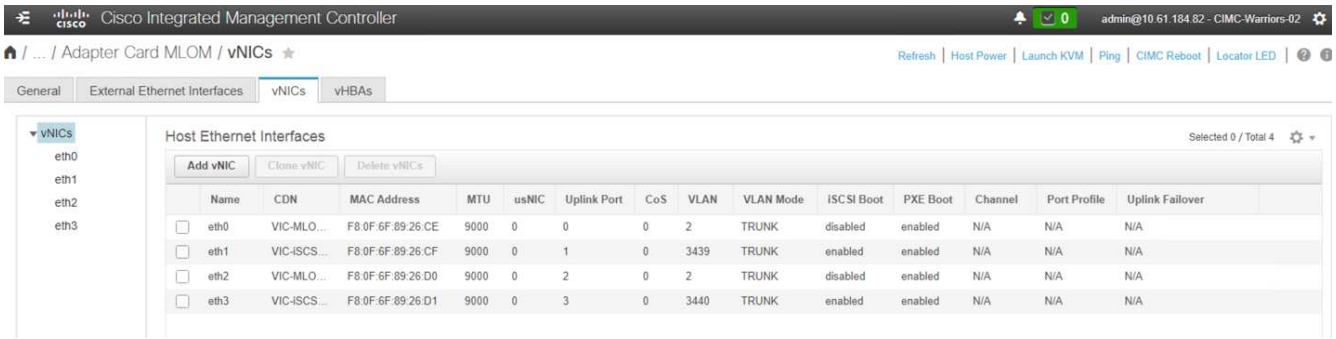
Configure las NIC virtuales para ESXi

Para configurar VNIC para ESXi, realice los siguientes pasos:

1. En la ventana del navegador de la interfaz CIMC, haga clic en Inventario y, a continuación, en Adaptadores Cisco VIC en el panel derecho.
2. En redes > Tarjeta adaptadora MLOM, seleccione la ficha vNIC y, a continuación, seleccione las vNIC debajo.
3. Seleccione eth0 y haga clic en Propiedades.
4. Establezca la MTU en 9000. Haga clic en Save Changes.
5. Establezca la VLAN como VLAN nativa 2.



6. Repita los pasos 3 y 4 en eth1, verificando que el puerto de enlace ascendente se establece en 1 para eth1.



Este procedimiento debe repetirse para cada nodo de servidor Cisco UCS inicial y cada nodo de servidor Cisco UCS adicional agregado al entorno.

"Siguiente: Procedimiento de implementación del almacenamiento AFF de NetApp (parte 2)."

Procedimiento de puesta en marcha del almacenamiento AFF de NetApp (parte 2)

Configurar el almacenamiento DE arranque SAN de ONTAP

Cree iGroups iSCSI

Para este paso, se necesitan los IQN de iniciadores iSCSI desde la configuración del servidor.

Para crear iGroups, ejecute los siguientes comandos desde la conexión SSH del nodo de gestión del clúster. Para ver los tres iGroups creados en este paso, ejecute el `igroup show` comando.

```
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-A –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_a_iSCSI-
A_vNIC_IQN>>,<<var_vm_host_infra_a_iSCSI-B_vNIC_IQN>>
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-B –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_b_iSCSI-
A_vNIC_IQN>>,<<var_vm_host_infra_b_iSCSI-B_vNIC_IQN>>
```

Este paso se debe completar cuando se añaden servidores Cisco UCS C-Series adicionales.

Asigne LUN de arranque a iGroups

```
To map boot LUNs to igroups, run the following commands from the cluster
management SSH connection:
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra-A –igroup
VM-Host-Infra-A –lun-id 0
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra-B –igroup
VM-Host-Infra-B –lun-id 0
```

Este paso se debe completar cuando se añaden servidores Cisco UCS C-Series adicionales.

"Siguiente: Procedimiento de puesta en marcha de VMware vSphere 6.7U2."

Procedimiento de puesta en marcha de VMware vSphere 6.7U2

En esta sección, se proporcionan los procedimientos detallados para la instalación de VMware ESXi 6.7U2 en una configuración FlexPod Express. Los procedimientos de implementación siguientes se personalizan para incluir las variables de entorno descritas en secciones anteriores.

Existen varios métodos para instalar VMware ESXi en dicho entorno. Este procedimiento utiliza la consola KVM virtual y las funciones de medios virtuales de la interfaz CIMC para servidores Cisco UCS C-Series para asignar medios de instalación remotos a cada servidor individual.

Este procedimiento se debe completar para el servidor Cisco UCS A y el servidor Cisco UCS B.

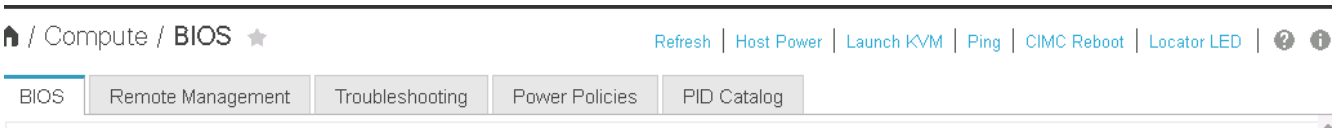
Este procedimiento debe completarse para los nodos adicionales que se añadan al clúster.

Inicie sesión en la interfaz de CIMC para servidores independientes de Cisco UCS C-Series

Los siguientes pasos detallan el método para iniciar sesión en la interfaz de CIMC para servidores independientes Cisco UCS C-Series. Debe iniciar sesión en la interfaz de CIMC para ejecutar el KVM virtual, que permite al administrador iniciar la instalación del sistema operativo a través de medios remotos.

Todos los hosts

1. Desplácese hasta un explorador web e introduzca la dirección IP para la interfaz de CIMC para Cisco UCS C-Series. Este paso inicia la aplicación GUI de CIMC.
2. Inicie sesión en la interfaz de usuario de CIMC con el nombre de usuario y las credenciales de administrador.
3. En el menú principal, seleccione la ficha servidor.
4. Haga clic en Iniciar la consola KVM.



5. En la consola KVM virtual, seleccione la ficha Medios virtuales.
6. Selecciona Mapa CD/DVD.

Es posible que primero tenga que hacer clic en Activar dispositivos virtuales. Seleccione Aceptar esta sesión si se le solicita.

7. Desplácese hasta el archivo de imagen ISO del instalador VMware ESXi 6.7U2 y haga clic en Open. Haga clic en asignar dispositivo.
8. Seleccione el menú de encendido y elija sistema de ciclo de encendido (arranque en frío). Haga clic en Yes.

Instale VMware ESXi

Los siguientes pasos describen cómo instalar VMware ESXi en cada host.

Descargue LA imagen personalizada de Cisco DE ESXI 6.7U2

1. Desplácese hasta la "Página de descarga de VMware vSphere" Para ISO personalizados.
2. Haga clic en Go to Downloads junto a la imagen personalizada de Cisco para el CD de instalación de ESXi 6.7U2.
3. Descargue la imagen personalizada de Cisco para el CD de instalación de ESXi 6.7U2 (ISO).
4. Cuando el sistema arranca, la máquina detecta la presencia del medio de instalación de VMware ESXi.
5. Seleccione el instalador de VMware ESXi en el menú que aparece. El instalador se carga, lo que puede tardar varios minutos.

6. Cuando el instalador haya terminado de cargarse, pulse Intro para continuar con la instalación.
7. Después de leer el contrato de licencia del usuario final, acepte y continúe con la instalación pulsando F11.
8. Seleccione el LUN de NetApp que se configuró anteriormente como disco de instalación para ESXi y pulse Intro para continuar con la instalación.



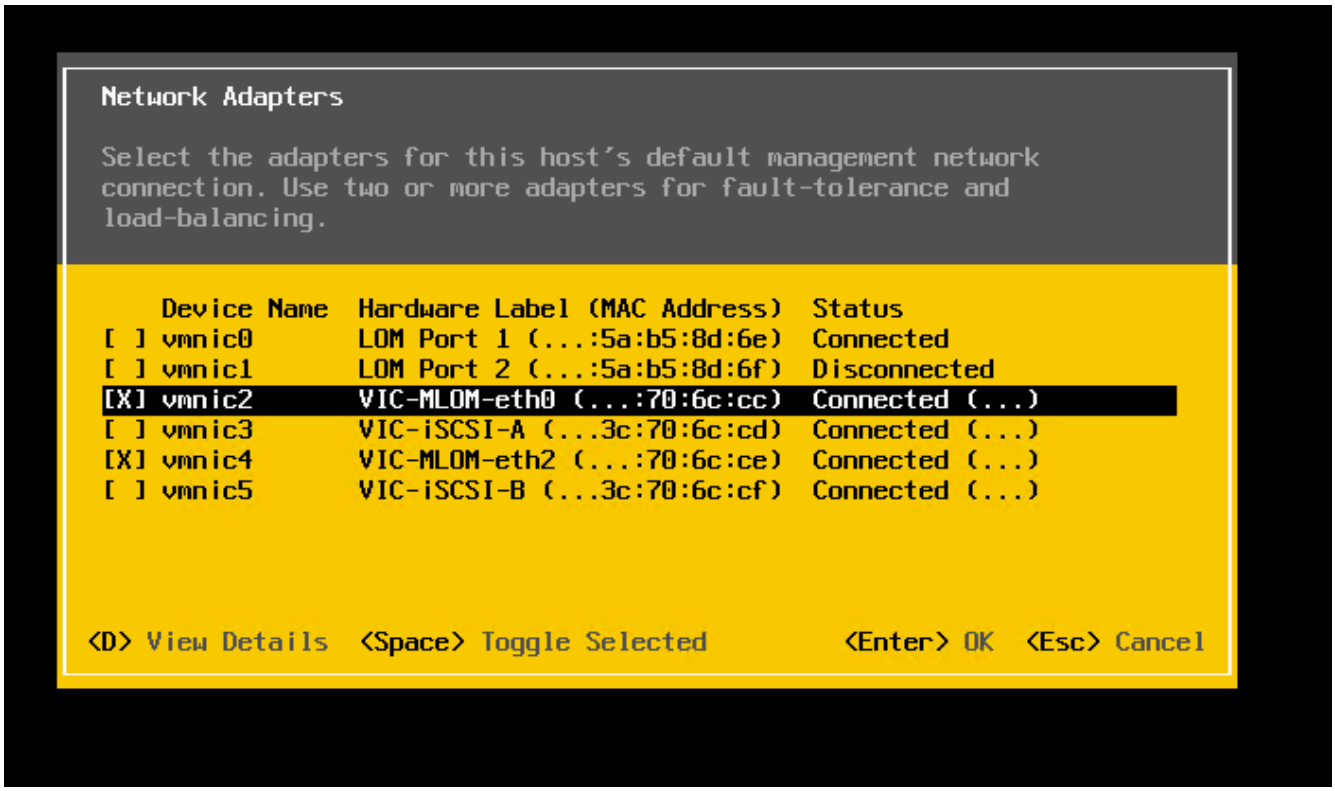
9. Seleccione la distribución de teclado adecuada y pulse Intro.
10. Introduzca y confirme la contraseña de root y pulse Intro.
11. El instalador le advierte que las particiones existentes se han eliminado en el volumen. Continúe con la instalación pulsando F11. El servidor se reinicia después de la instalación de ESXi.

Configure la red de gestión del host VMware ESXi

Los siguientes pasos describen cómo añadir la red de gestión de cada host VMware ESXi.

Todos los hosts

1. Una vez que el servidor haya terminado de reiniciarse, introduzca la opción de personalizar el sistema pulsando F2.
2. Inicie sesión con root como nombre de inicio de sesión y la contraseña raíz que se introdujo anteriormente durante el proceso de instalación.
3. Seleccione la opción Configure Management Network.
4. Seleccione Adaptadores de red y pulse Intro.
5. Seleccione los puertos deseados para vSwitch0. Pulse Intro.
6. Seleccione los puertos que corresponden a eth0 y eth1 en CIMC.



7. Seleccione VLAN (opcional) y presione Enter.
8. Introduzca el identificador de VLAN `<<mgmt_vlan_id>>`. Pulse Intro.
9. En el menú Configurar red de gestión, seleccione Configuración de IPv4 para configurar la dirección IP de la interfaz de gestión. Pulse Intro.
10. Utilice las teclas de flecha para resaltar establecer dirección IPv4 estática y utilice la barra espaciadora para seleccionar esta opción.
11. Introduzca la dirección IP para gestionar el host VMware ESXi `<<esxi_host_mgmt_ip>>`.
12. Introduzca la máscara de subred para el host VMware ESXi `<<esxi_host_mgmt_netmask>>`.
13. Introduzca la puerta de enlace predeterminada para el host VMware ESXi `<<esxi_host_mgmt_gateway>>`.
14. Pulse Intro para aceptar los cambios en la configuración de IP.
15. Acceda al menú de configuración de IPv6.
16. Utilice la barra de espacio para desactivar IPv6 deseleccionando la opción Habilitar IPv6 (reiniciar requerido). Pulse Intro.
17. Abra el menú para configurar los ajustes de DNS.
18. Dado que la dirección IP se asigna manualmente, la información DNS también debe introducirse manualmente.
19. Introduzca la dirección IP del servidor DNS primario `<<nameserver_ip>>`.
20. (Opcional) Introduzca la dirección IP del servidor DNS secundario.
21. Introduzca el FQDN para el nombre de host VMware ESXi: `<<esxi_host_fqdn>>`.
22. Pulse Intro para aceptar los cambios en la configuración de DNS.
23. Salga del submenú Configurar red de administración pulsando Esc.

24. Pulse y para confirmar los cambios y reiniciar el servidor.
25. Seleccione Troubleshooting Options y, a continuación, habilite ESXi Shell y SSH.

> Estas opciones de solución de problemas se pueden desactivar después de la validación de acuerdo con la política de seguridad del cliente.

26. Pulse Esc dos veces para volver a la pantalla principal de la consola.
27. Haga clic en Alt-F1 en el menú desplegable macros de CIMC > macros estáticas > Alt-F en la parte superior de la pantalla.
28. Inicie sesión con las credenciales adecuadas para el host ESXi.
29. En el símbolo del sistema de, introduzca la siguiente lista de comandos esxcli para habilitar la conectividad de red de forma secuencial.

```
esxcli network vswitch standard policy failover set -v vSwitch0 -a
vmnic2,vmnic4 -l iphash
```

Configure el host ESXi

Utilice la información de la siguiente tabla para configurar cada host ESXi.

Detalles	Valor de detalle
Nombre de host ESXi	<<esxi_host_fqdn>>
La IP de gestión del host ESXi	<<esxi_host_mgmt_ip>>
Máscara de gestión de host ESXi	<<esxi_host_mgmt_netmask>>
Pasarela de gestión de host ESXi	<<esxi_host_mgmt_gateway>>
IP NFS del host ESXi	<<esxi_host_NFS_ip>>
Máscara de NFS del host ESXi	<<esxi_host_NFS_netmask>>
Puerta de enlace NFS del host ESXi	<<esxi_host_NFS_gateway>>
Host ESXi IP de vMotion	<<esxi_host_vMotion_ip>>
Máscara de vMotion del host ESXi	<<esxi_host_vMotion_netmask>>
Puerta de enlace vMotion del host ESXi	<<esxi_host_vMotion_gateway>>
Host ESXi iSCSI-A IP	<<esxi_host_iSCSI-A_ip>>
Máscara iSCSI-A del host ESXi	<<esxi_host_iSCSI-A_netmask>>
Puerta de enlace iSCSI-A del host ESXi	<<esxi_host_iSCSI-A_gateway>>
Host ESXi iSCSI-B IP	<<esxi_host_iSCSI-B_ip>>
Máscara iSCSI-B del host ESXi	<<esxi_host_iSCSI-B_netmask>>
Puerta de enlace iSCSI-B del host ESXi	<<esxi_host_SCSI-B_gateway>>

Inicie sesión en el host ESXi

Para iniciar sesión en el host ESXi, complete los siguientes pasos:

1. Abra la dirección IP de administración del host en un explorador Web.
2. Inicie sesión en el host ESXi con la cuenta raíz y la contraseña que especificó durante el proceso de instalación.
3. Lea la declaración sobre el Programa de mejora de la experiencia del cliente de VMware. Después de seleccionar la respuesta correcta, haga clic en Aceptar.

Configurar el arranque iSCSI

Para configurar el arranque iSCSI, lleve a cabo los siguientes pasos:

1. Seleccione Networking a la izquierda.
2. A la derecha, seleccione la ficha Switches virtuales.



3. Haga clic en iScsiBootvSwitch.
4. Seleccione Editar configuración.
5. Cambie la MTU a 9000 y haga clic en Save.
6. Cambie el nombre del puerto iSCSIBootPG a iSCSIBootPG-A.

> En esta configuración, se utilizan vmnic3 y vmnic5 para arranque iSCSI. Si tiene NIC adicionales en el host ESXi, puede tener distintos números vmnic. Para confirmar qué NIC se utilizan para el arranque iSCSI, haga coincidir las direcciones MAC de las NIC iSCSI de CIMC con los vmnics de ESXi.

7. En el panel central, seleccione la ficha NIC de VMkernel.
8. Seleccione Agregar NIC de VMkernel.
   a. Especifique un nuevo nombre de grupo de puertos de iScsiBootPG-B.

b. Seleccione iScsiBootvSwitch para el switch virtual.

c. Introduzca `<<iscsib_vlan_id>>` Para el ID de VLAN.

d. Cambie el MTU a 9000.

e. Expanda Configuración IPv4.

f. Seleccione Configuración estática.

g. Introduzca `<<var_hosta_iscsib_ip>>` Para Dirección.

h. Introduzca `<<var_hosta_iscsib_mask>>` Para Máscara de subred.

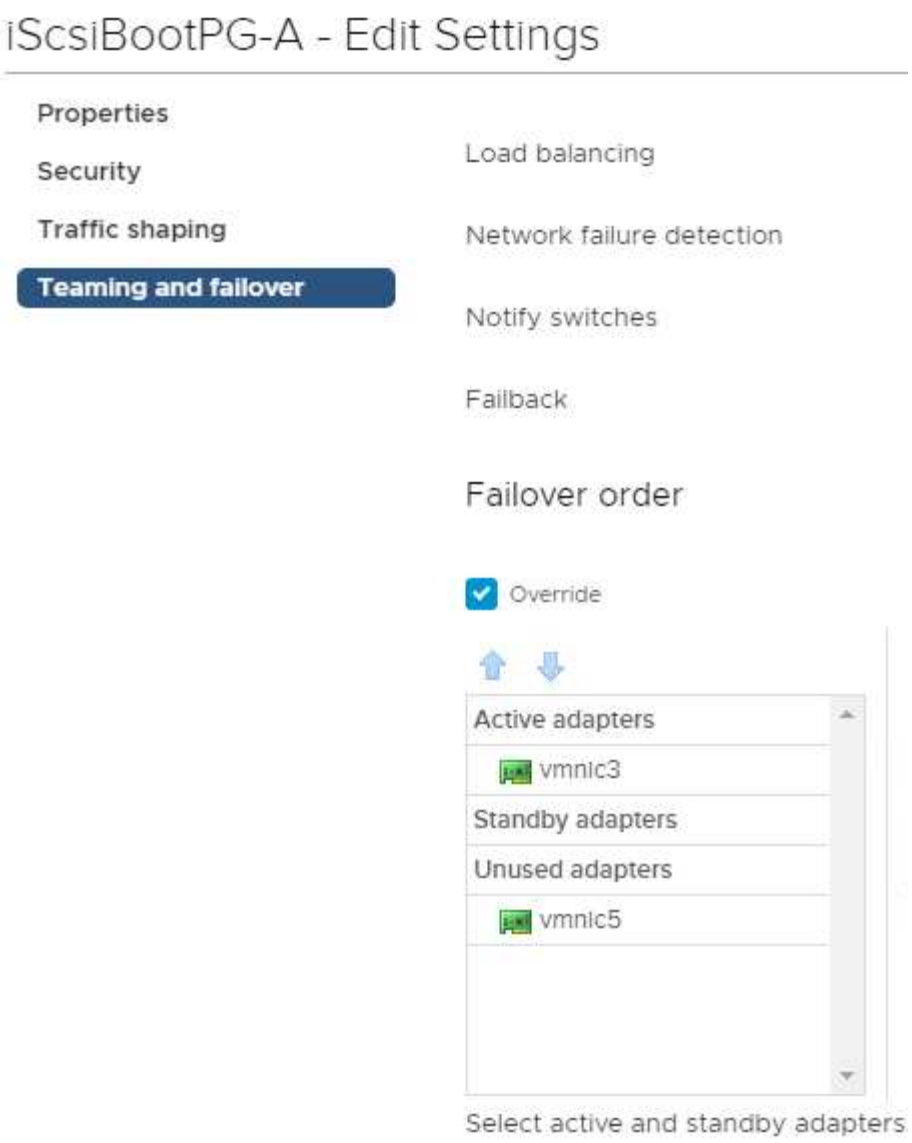
i. Haga clic en Crear.

Establezca la MTU en 9000 en iSCsiBootPG-A.

9. Para configurar la conmutación por error, lleve a cabo los siguientes pasos:

a. Haga clic en Edit Settings on iSCSIBootPG-A > Tiering and Failover > Failover Order > vmnic3. Vmnic3 debe estar activo y vmnic5 no se debe utilizar.

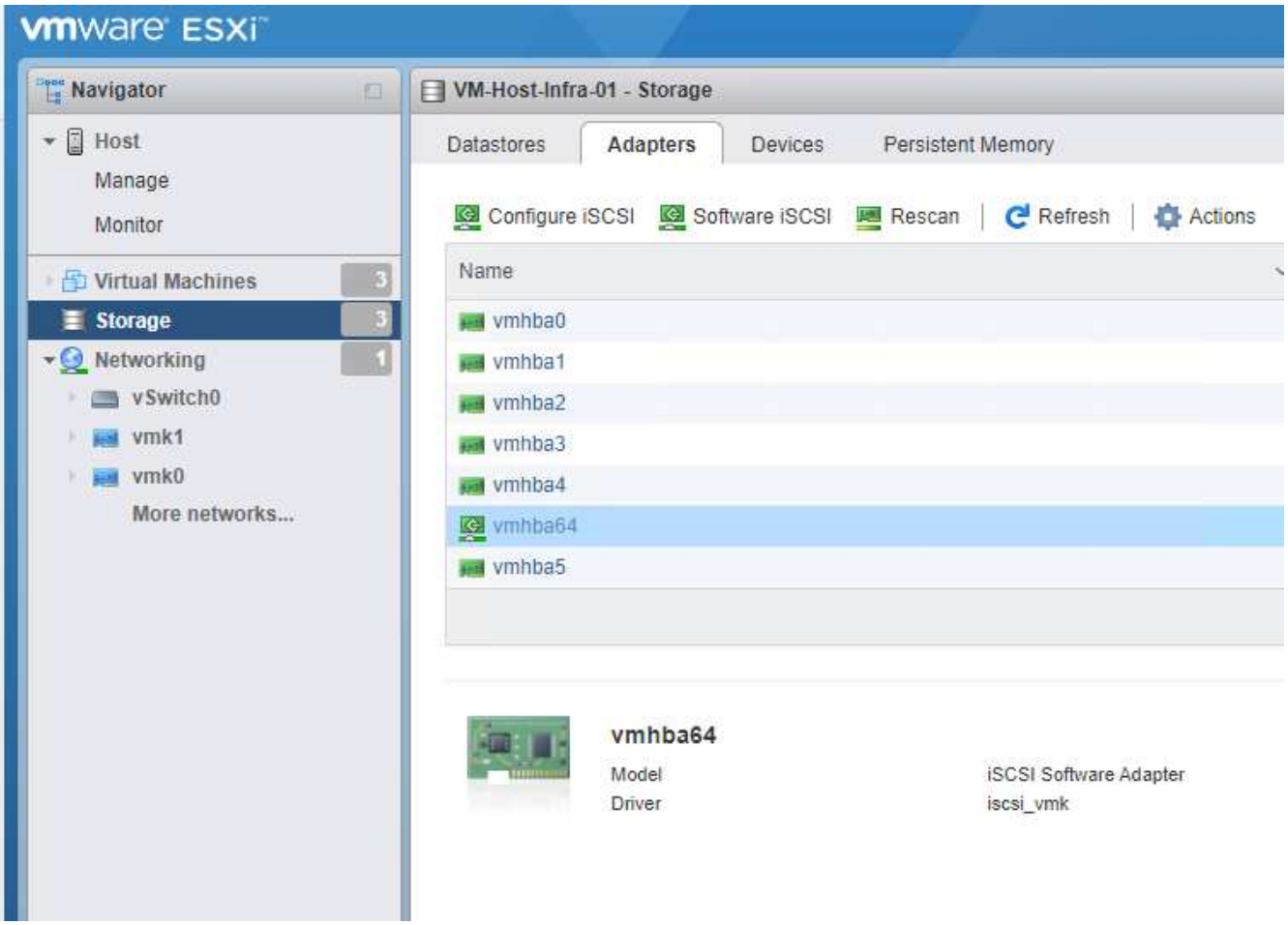
b. Haga clic en Editar configuración en iSCSIBootPG-B > equipos y failover > Orden de conmutación por error > vmnic5. Vmnic5 debe estar activo y vmnic3 no se debe utilizar.



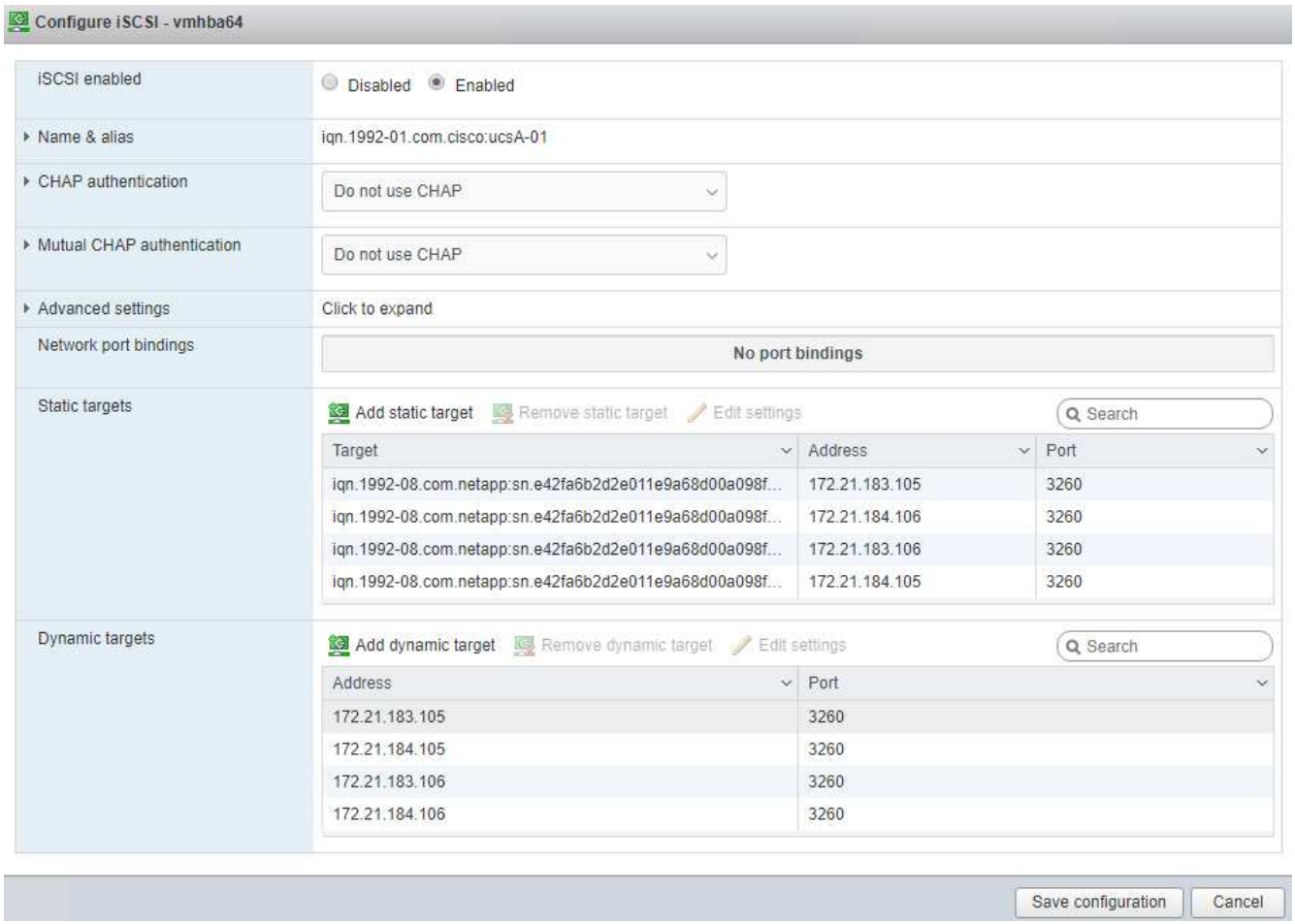
Configuración de accesos múltiples iSCSI

Para configurar la multivía iSCSI en los hosts ESXi, complete los pasos siguientes:

1. Seleccione Storage en el panel de navegación de la izquierda. Haga clic en Adaptadores.
2. Seleccione el adaptador de software iSCSI y haga clic en Configurar iSCSI.



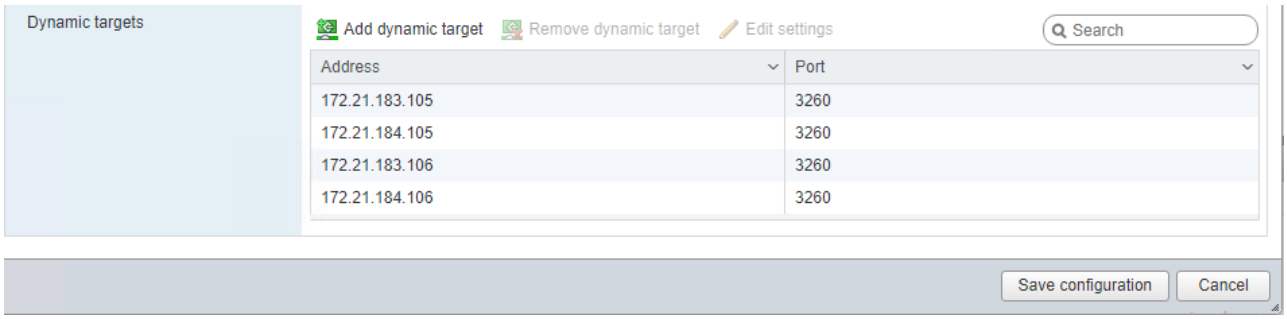
3. En Destinos dinámicos, haga clic en Agregar destino dinámico.



4. Introduzca la dirección IP `iscsi_lif01a`.

   a. Repita el proceso con las direcciones IP `iscsi_lif01b`, `iscsi_lif02a`, y. `iscsi_lif02b`.

   b. Haga clic en Save Configuration.



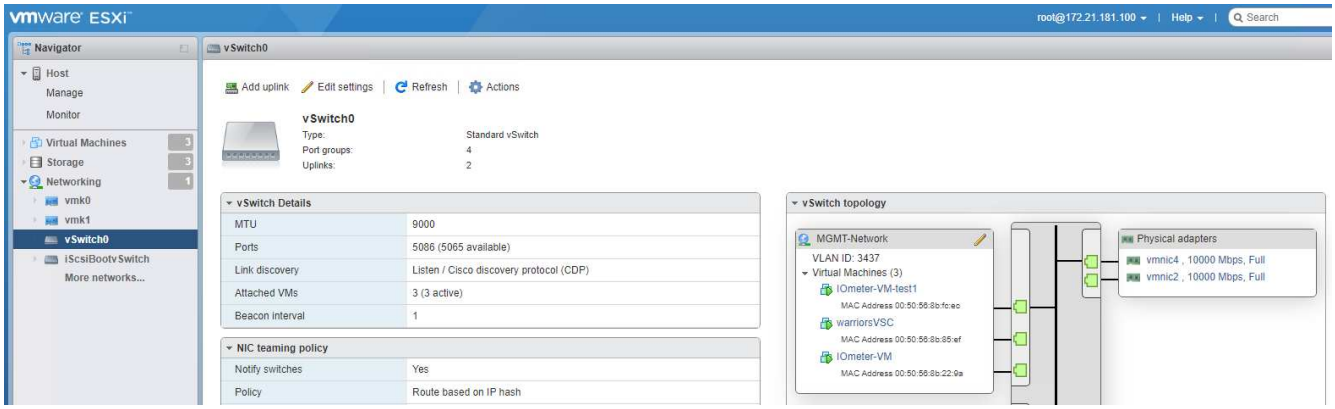
Puede encontrar las direcciones IP de LIF de iSCSI ejecutando el comando network interface show en el clúster de NetApp o mirando en la pestaña Network interfaces en System Manager.

Configure el host ESXi

Para configurar el arranque ESXi, complete los pasos siguientes:

1. En el panel de navegación de la izquierda, seleccione Networking.

2. Seleccione vSwitch0.



3. Seleccione Editar configuración.
4. Cambie el MTU a 9000.
5. Expanda NIC Teaming y verifique que tanto vmnic2 como vmnic4 estén configurados en activo y que NIC Teaming y Failover se establezcan en Route basado en IP Hash.

> El método hash IP del equilibrio de carga requiere que el conmutador físico subyacente se configure correctamente mediante SRC-DST-IP EtherChannel con un canal de puerto estático (modo activado). Es posible que experimente una conectividad intermitente debido a una posible configuración incorrecta del switch. En ese caso, apague temporalmente uno de los dos puertos de enlace ascendente asociados del switch Cisco para restaurar la comunicación con el puerto vmkernel de gestión de ESXi, a la vez que solucione problemas de la configuración del canal de puertos.

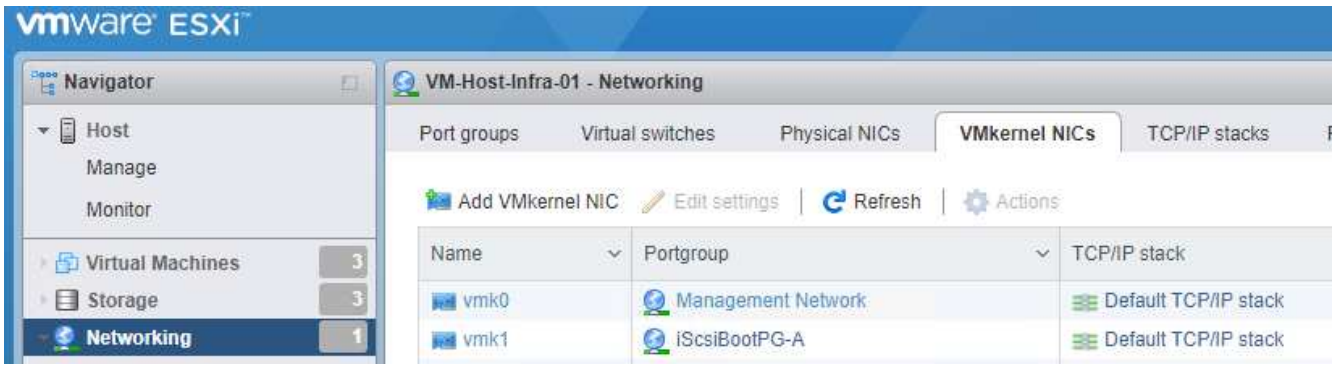
Configure los grupos de puertos y las NIC de VMkernel

Para configurar los grupos de puertos y las NIC de VMkernel, lleve a cabo los siguientes pasos:

1. En el panel de navegación de la izquierda, seleccione Networking.
2. Haga clic con el botón derecho en la pestaña grupos de puertos.

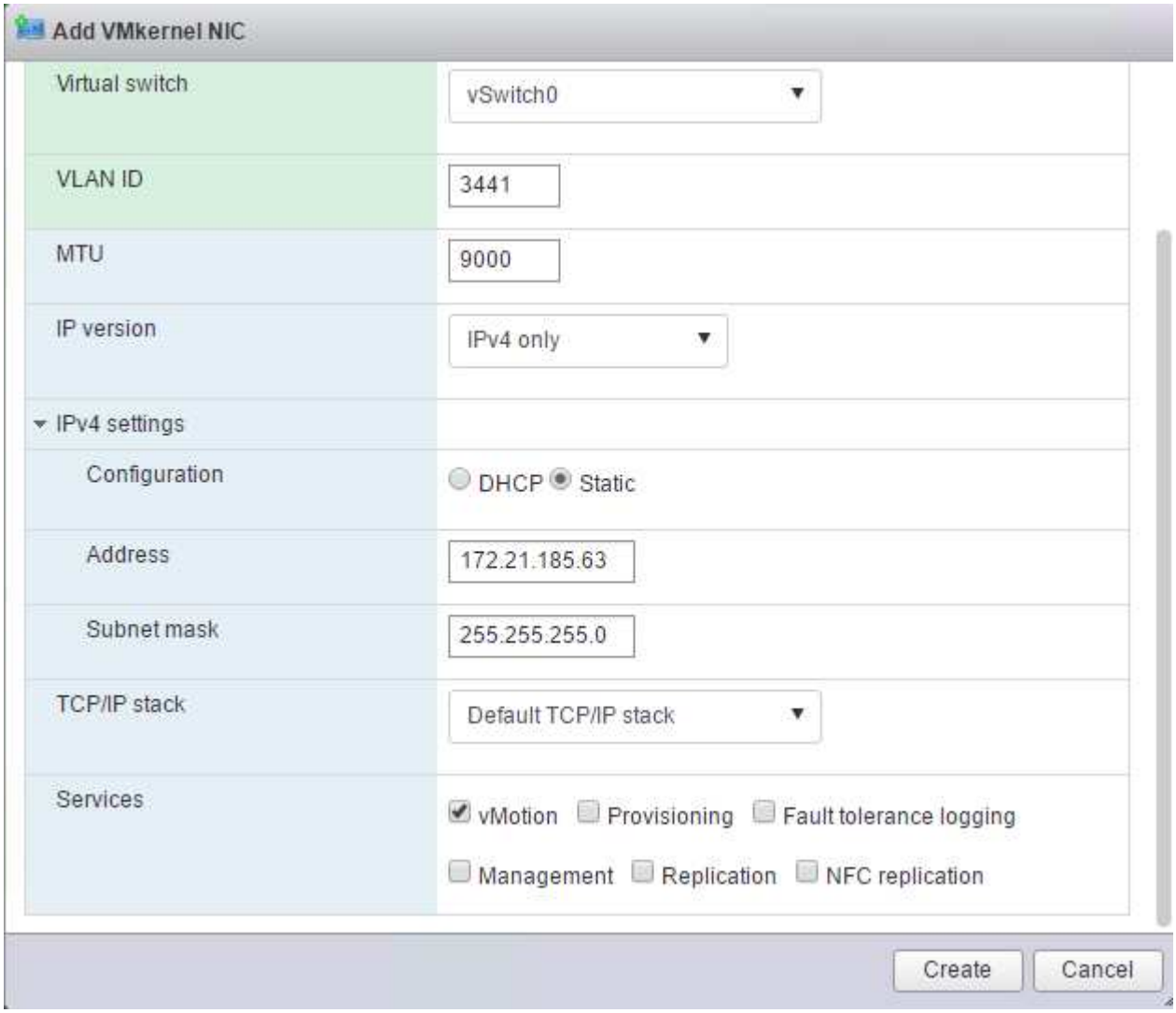


3. Haga clic con el botón derecho en VM Network y seleccione Edit. Cambie el ID de VLAN a. `<<var_vm_traffic_vlan>>`.
4. Haga clic en Agregar grupo de puertos.
   a. Asigne el nombre MGMT-Network al grupo de puertos.
   b. Introduzca `<<mgmt_vlan>>` Para el ID de VLAN.
   c. Asegúrese de que vSwitch0 esté seleccionado.
   d. Haga clic en Guardar.
5. Haga clic en la ficha NIC de VMkernel.



6. Seleccione Agregar NIC de VMkernel.
   a. Seleccione Nuevo grupo de puertos.
   b. Asigne un nombre al grupo de puertos NFS-Network.
   c. Introduzca `<<nfs_vlan_id>>` Para el ID de VLAN.
   d. Cambie el MTU a 9000.
   e. Expanda Configuración IPv4.
   f. Seleccione Configuración estática.
   g. Introduzca `<<var_hosta_nfs_ip>>` Para Dirección.
   h. Introduzca `<<var_hosta_nfs_mask>>` Para Máscara de subred.
   i. Haga clic en Crear.
7. Repita este proceso para crear el puerto VMkernel de vMotion.
8. Seleccione Agregar NIC de VMkernel.
   a. Seleccione Nuevo grupo de puertos.
   b. Asigne un nombre al grupo de puertos vMotion.
   c. Introduzca `<<vmotion_vlan_id>>` Para el ID de VLAN.
   d. Cambie el MTU a 9000.
   e. Expanda Configuración IPv4.
   f. Seleccione Configuración estática.
   g. Introduzca `<<var_hosta_vmotion_ip>>` Para Dirección.
   h. Introduzca `<<var_hosta_vmotion_mask>>` Para Máscara de subred.

i. Asegúrese de que la casilla de comprobación vMotion esté seleccionada después de IPv4 Settings.

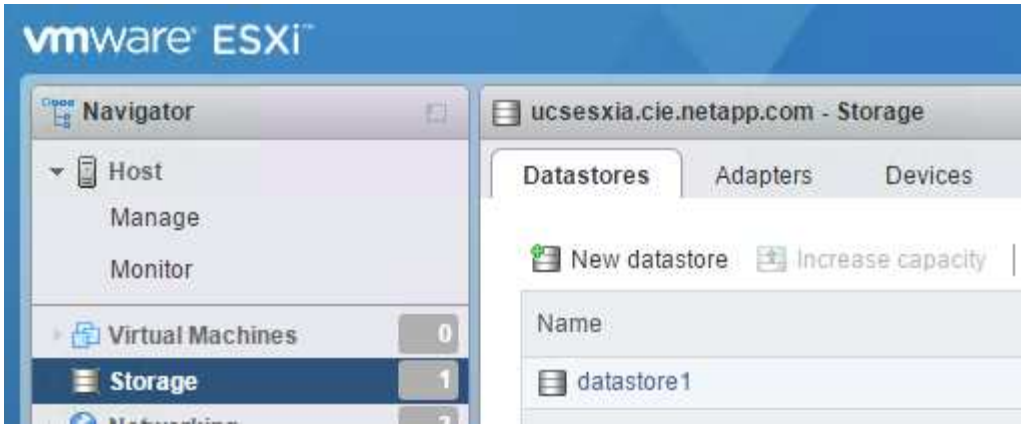


Hay muchas formas de configurar redes ESXi, por ejemplo, mediante el switch distribuido de VMware vSphere si la licencia lo permite. FlexPod Express admite configuraciones de red alternativas si se requieren para satisfacer los requisitos del negocio.

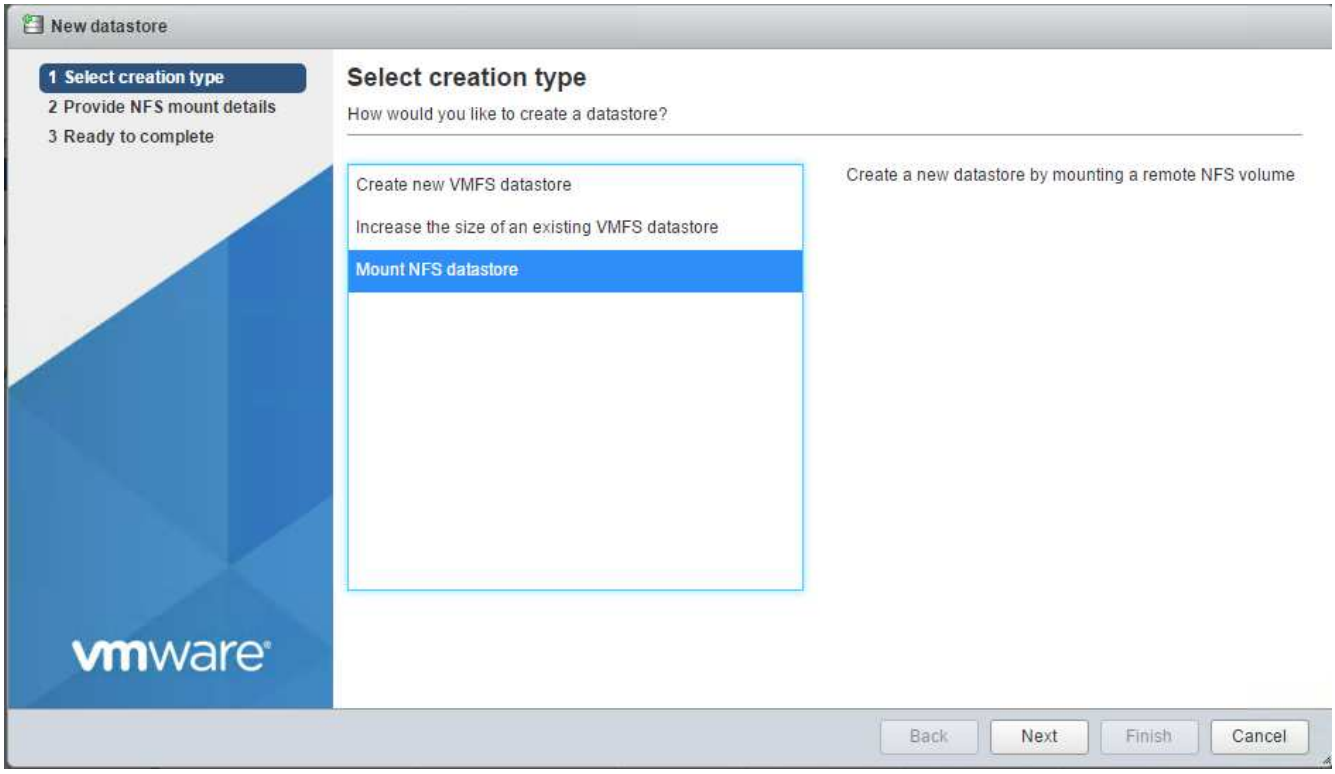
Monte los primeros almacenes de datos

Los primeros almacenes de datos que se van a montar son el `infra_datastore` Almacén de datos para las máquinas virtuales y para `infra_swap` Almacén de datos para archivos de intercambio de equipos virtuales.

1. Haga clic en Storage en el panel de navegación de la izquierda y después haga clic en New Datastore.



2. Seleccione Mount NFS Datastore.



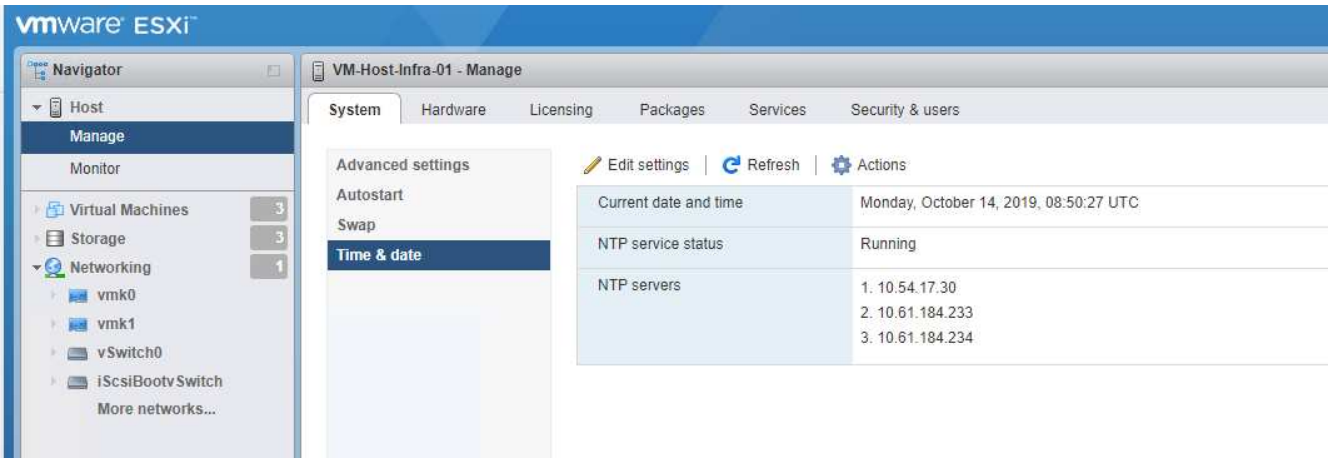
3. Introduzca la siguiente información en la página Provide NFS Mount Details:
   - Nombre: `infra_datastore`
   - Servidor NFS: `<<var_nodea_nfs_lif>>`
   - Compartir: `/infra_datastore`
   - Asegúrese de que la opción NFS 3 esté seleccionada.
4. Haga clic en Finalizar. Puede ver que la tarea se está completando en el panel tareas recientes.
5. Repita este proceso para montar el `infra_swap` almacén de datos:
   - Nombre: `infra_swap`
   - Servidor NFS: `<<var_nodea_nfs_lif>>`
   - Compartir: `/infra_swap`

- Asegúrese de que la opción NFS 3 esté seleccionada.

Configure NTP

Para configurar NTP para un host ESXi, complete los siguientes pasos:

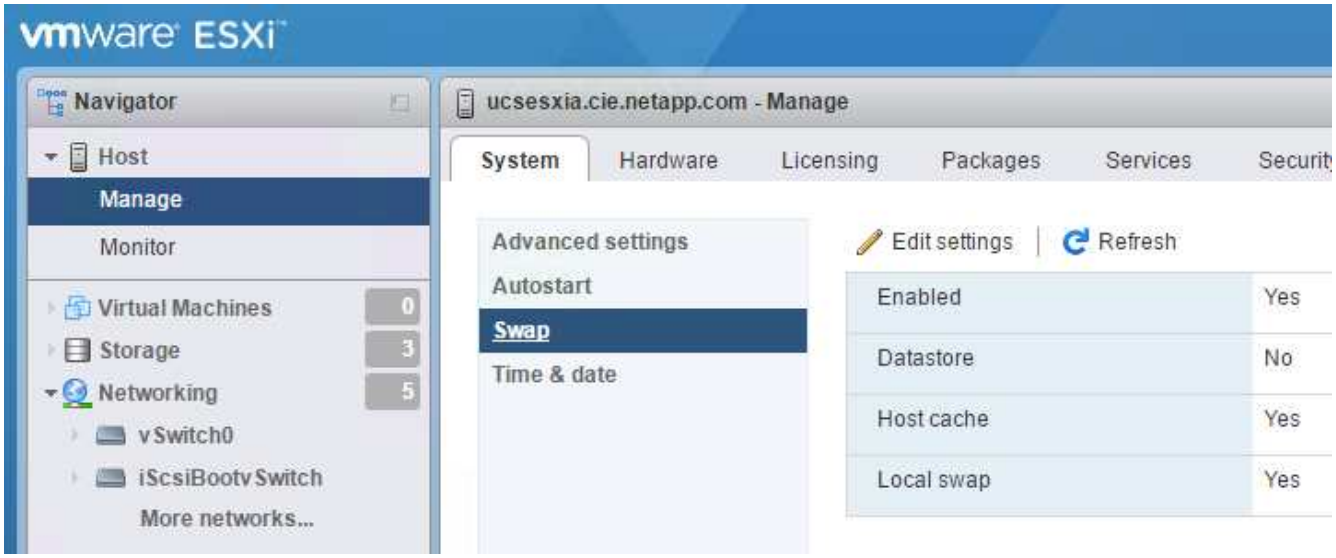
1. Haga clic en Administrar en el panel de navegación de la izquierda. Seleccione sistema en el panel derecho y, a continuación, haga clic en Hora y fecha.
2. Seleccione Use Network Time Protocol (Habilitar cliente NTP).
3. Seleccione Start and Stop with Host como política de inicio del servicio NTP.
4. Introduzca `<<var_ntp>>` Como servidor NTP. Puede establecer varios servidores NTP.
5. Haga clic en Guardar.



Mueva la ubicación del archivo de intercambio de la máquina virtual

Estos pasos proporcionan detalles para mover la ubicación del archivo de intercambio de la máquina virtual.

1. Haga clic en Administrar en el panel de navegación de la izquierda. Seleccione sistema en el panel derecho y, a continuación, haga clic en intercambiar.



2. Haga clic en Editar configuración. Seleccione `infra_swap` En las opciones del Datastore.



3. Haga clic en Guardar.

"Siguiente: Procedimiento de instalación de VMware vCenter Server 6.7U2."

Procedimiento de instalación de VMware vCenter Server 6.7U2

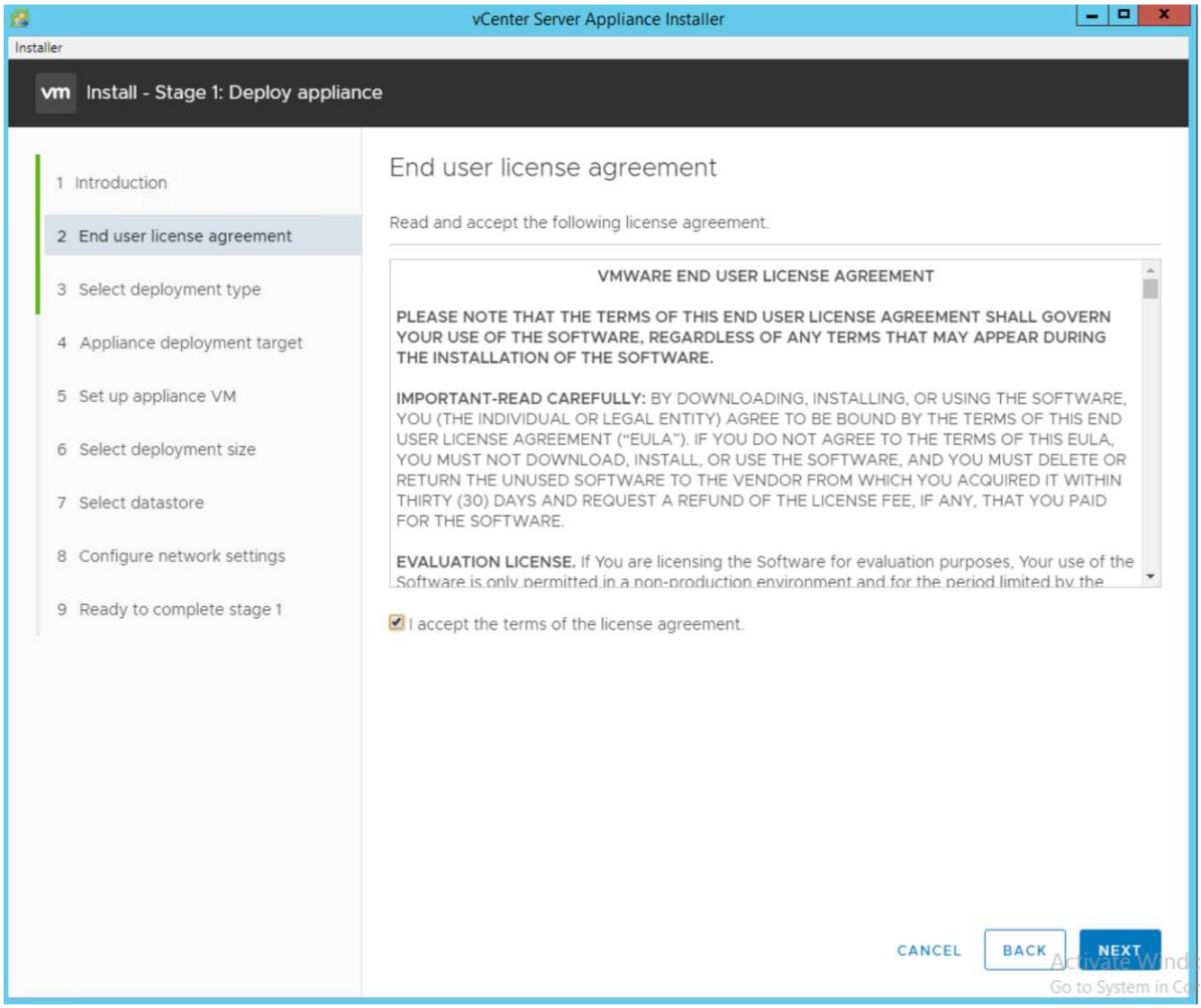
En esta sección, se proporcionan los procedimientos detallados para instalar VMware vCenter Server 6.7 en una configuración exprés de FlexPod.

FlexPod Express utiliza el dispositivo de VMware vCenter Server (VCSA).

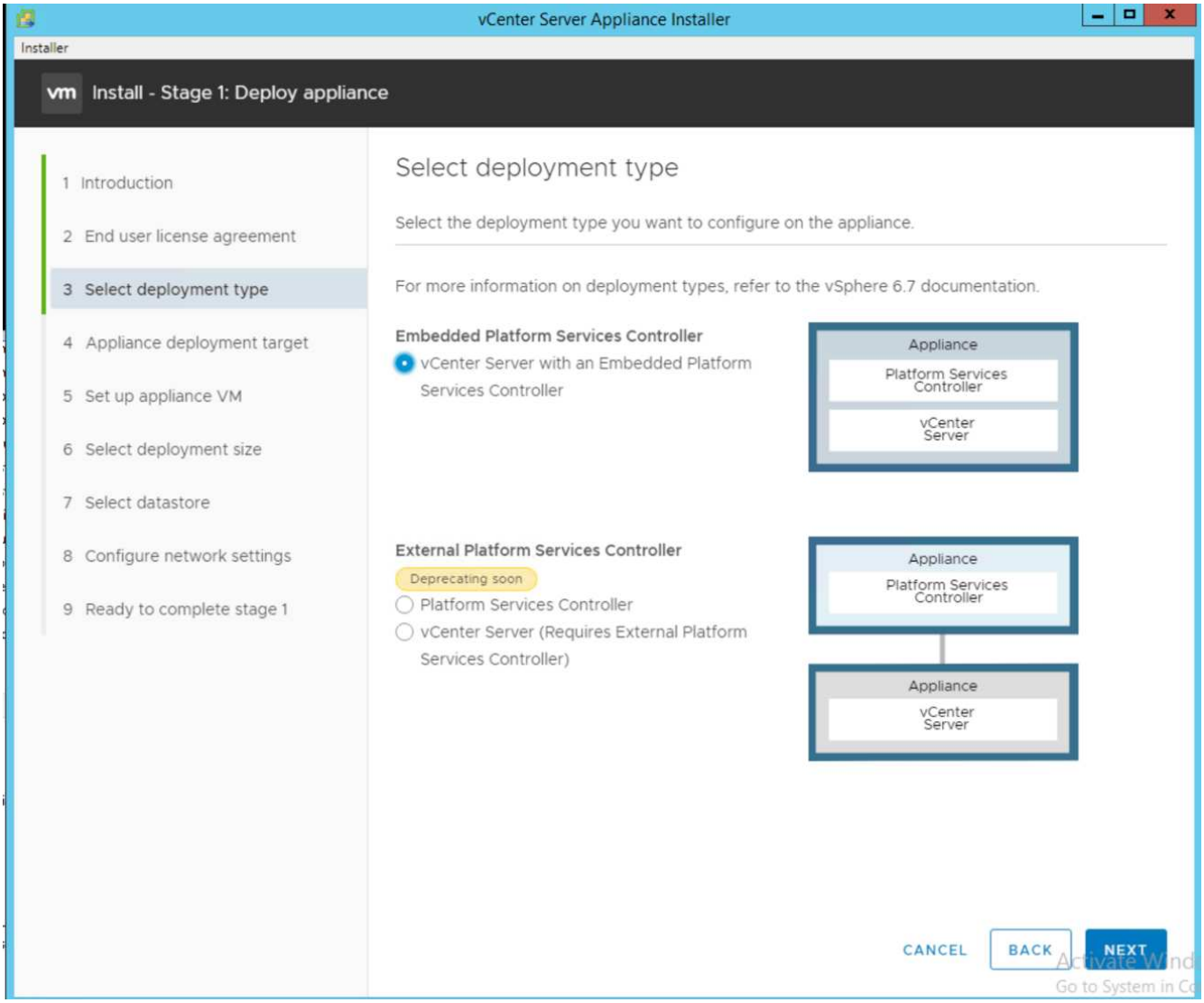
Descargue el dispositivo de VMware vCenter Server

Para descargar el dispositivo de VMware vCenter Server (VCSA), siga los pasos siguientes:

1. Descargue el VCSA. Acceda al enlace de descarga haciendo clic en el icono Get vCenter Server cuando gestione el host ESXi.
2. Descargue el VCSA desde el sitio de VMware.
3. Aunque se admite la instalación de Microsoft Windows vCenter Server, VMware recomienda VCSA para las nuevas implementaciones.
4. Monte la imagen ISO.
5. Vaya al directorio vcsa- ui-installer > win32. Haga doble clic `installer.exe`.
6. Haga clic en instalar.
7. Haga clic en Siguiente en la página Introducción.

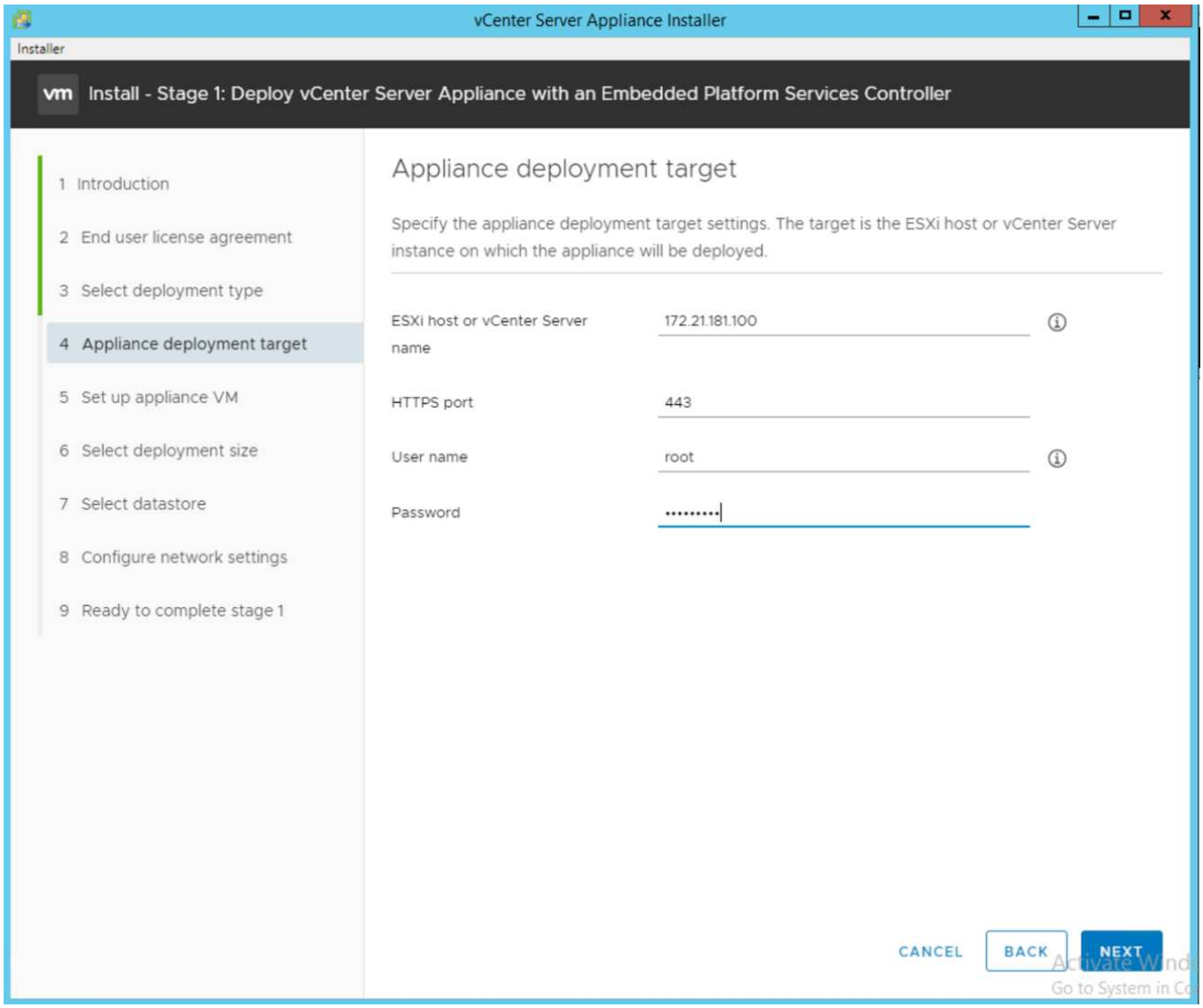


8. Seleccione Embedded Platform Services Controller (controladora de servicios de plataforma integrada) como tipo de implementación.

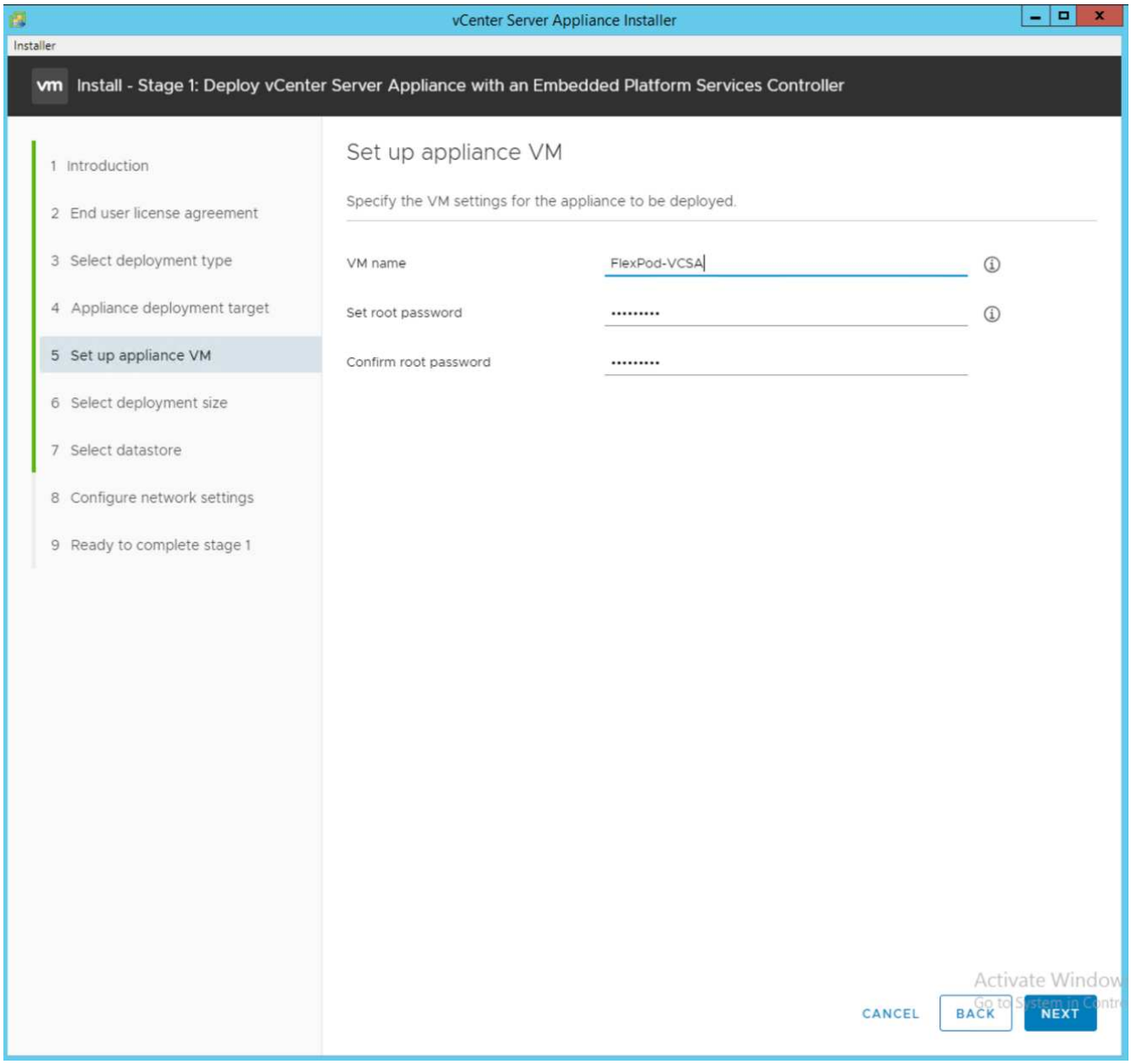


Si es necesario, también admite la puesta en marcha de la controladora de servicios de plataforma externa como parte de la solución FlexPod Express.

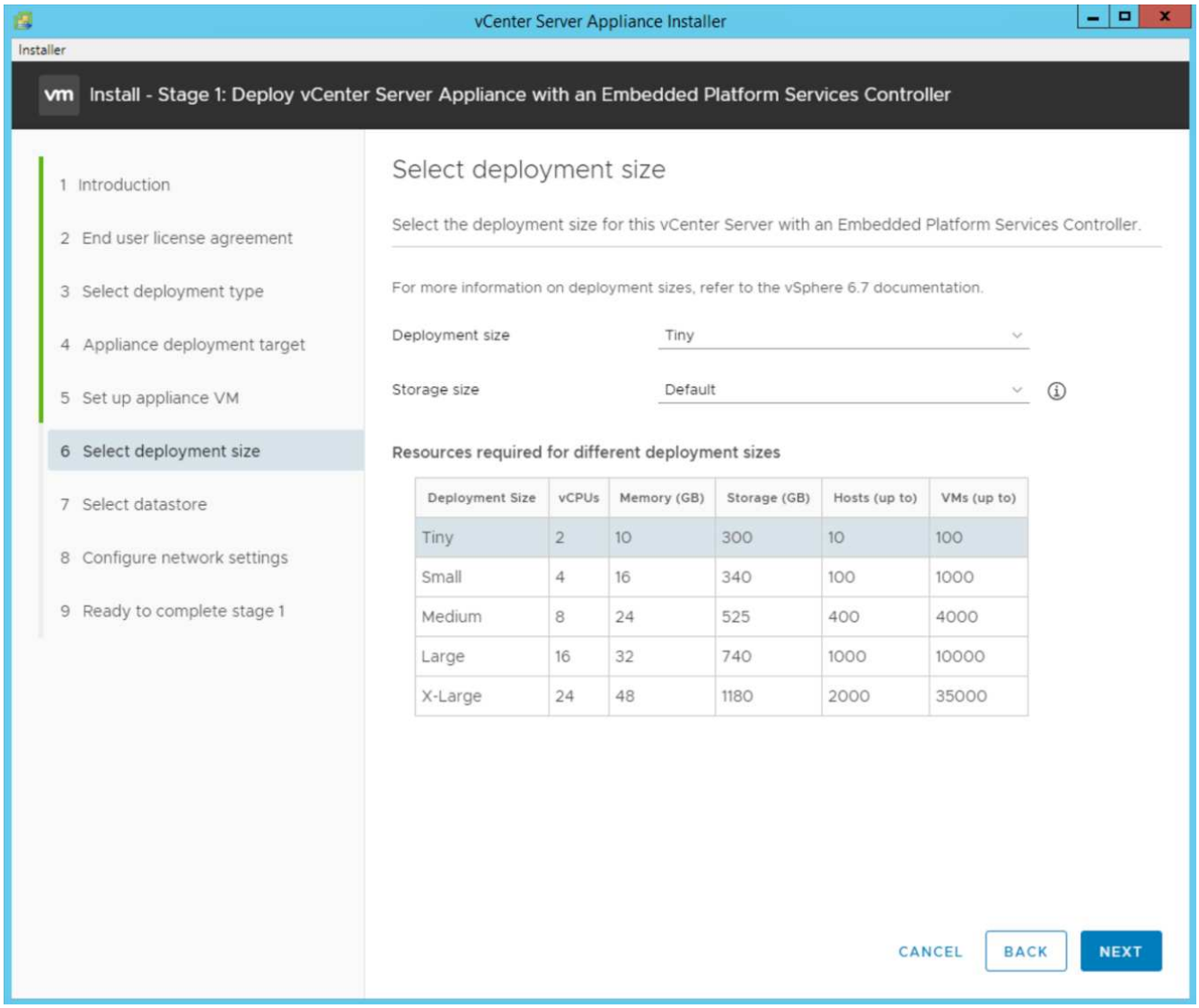
9. En Appliance Deployment Target, introduzca la dirección IP de un host ESXi que haya implementado, el nombre de usuario raíz y la contraseña raíz.



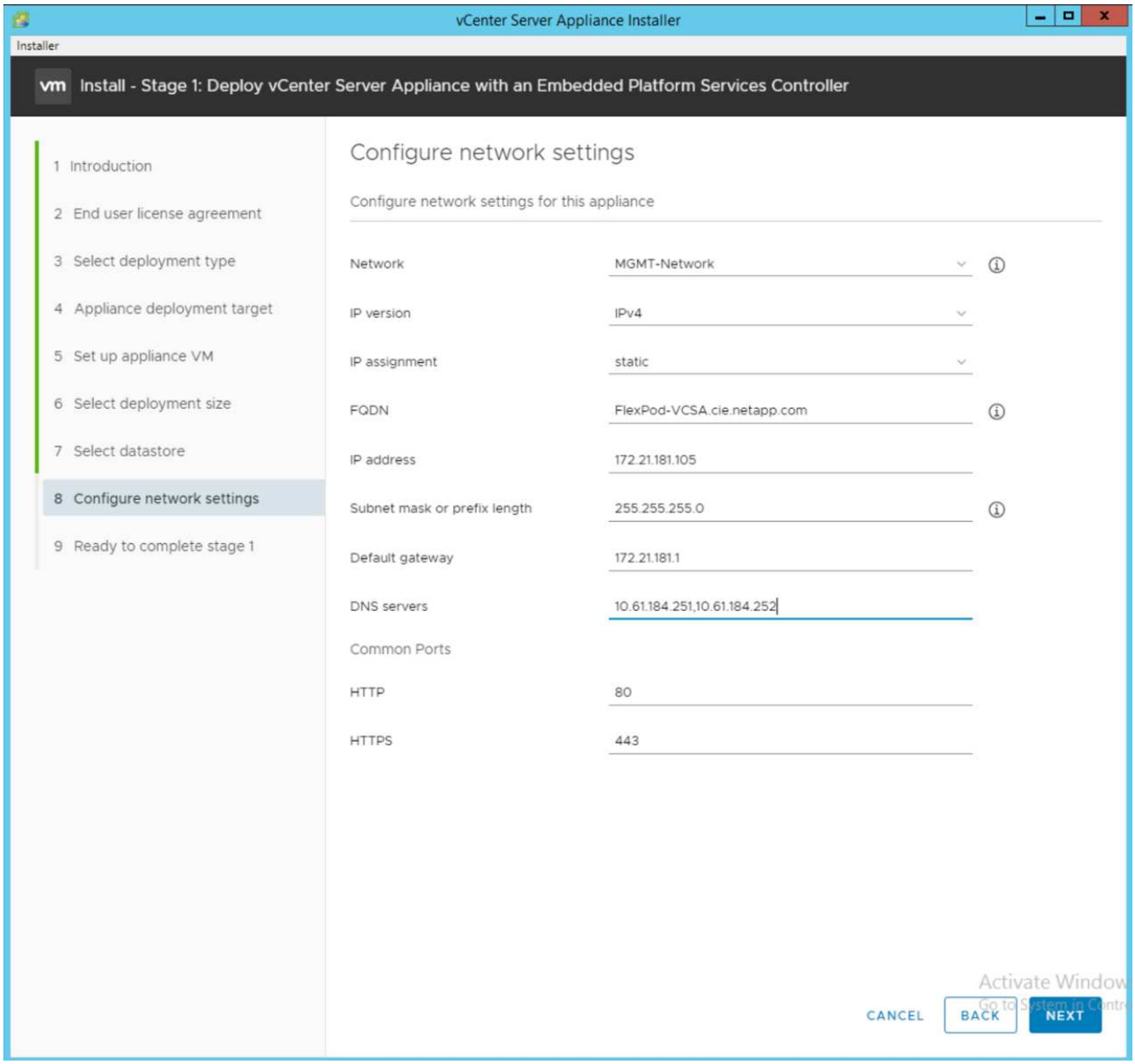
10. Para establecer el equipo virtual, introduzca VCSA como nombre de equipo virtual y la contraseña raíz que desea utilizar para el VCSA.



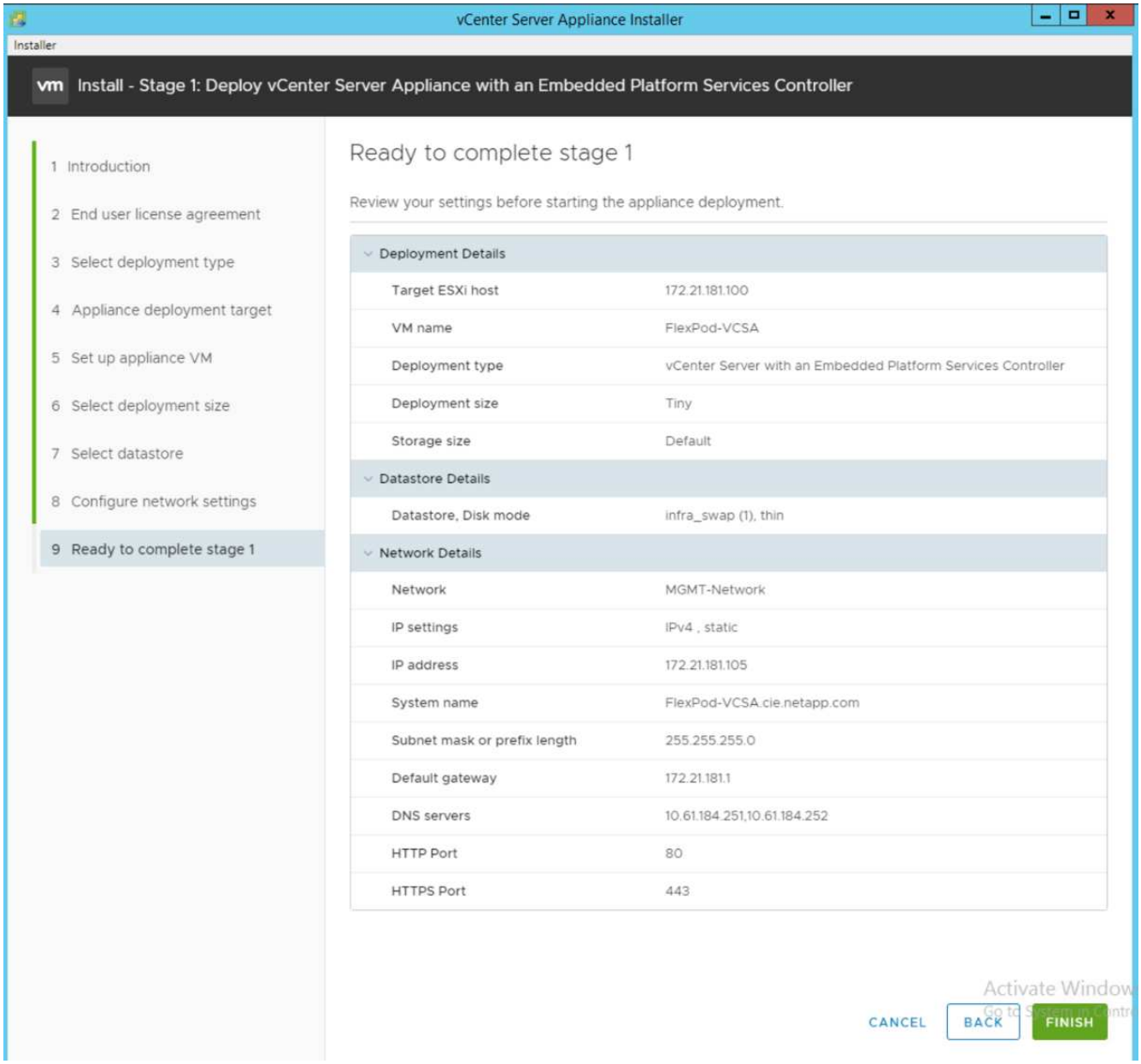
11. Seleccione el tamaño de puesta en marcha que mejor se adapte a su entorno. Haga clic en Siguiente.



12. Seleccione la `infra_datastore` almacén de datos. Haga clic en Siguiente.
13. Introduzca la siguiente información en la página Configure network settings y haga clic en Next.
    a. Seleccione MGMT-Network para Red.
    b. Introduzca el FQDN o IP que se va a utilizar para la VCSA.
    c. Introduzca la dirección IP que se utilizará.
    d. Introduzca la máscara de subred que desea utilizar.
    e. Introduzca la pasarela predeterminada.
    f. Introduzca el servidor DNS.
14. En la página Ready to Complete Stage 1, compruebe que los ajustes introducidos son correctos. Haga clic en Finalizar.

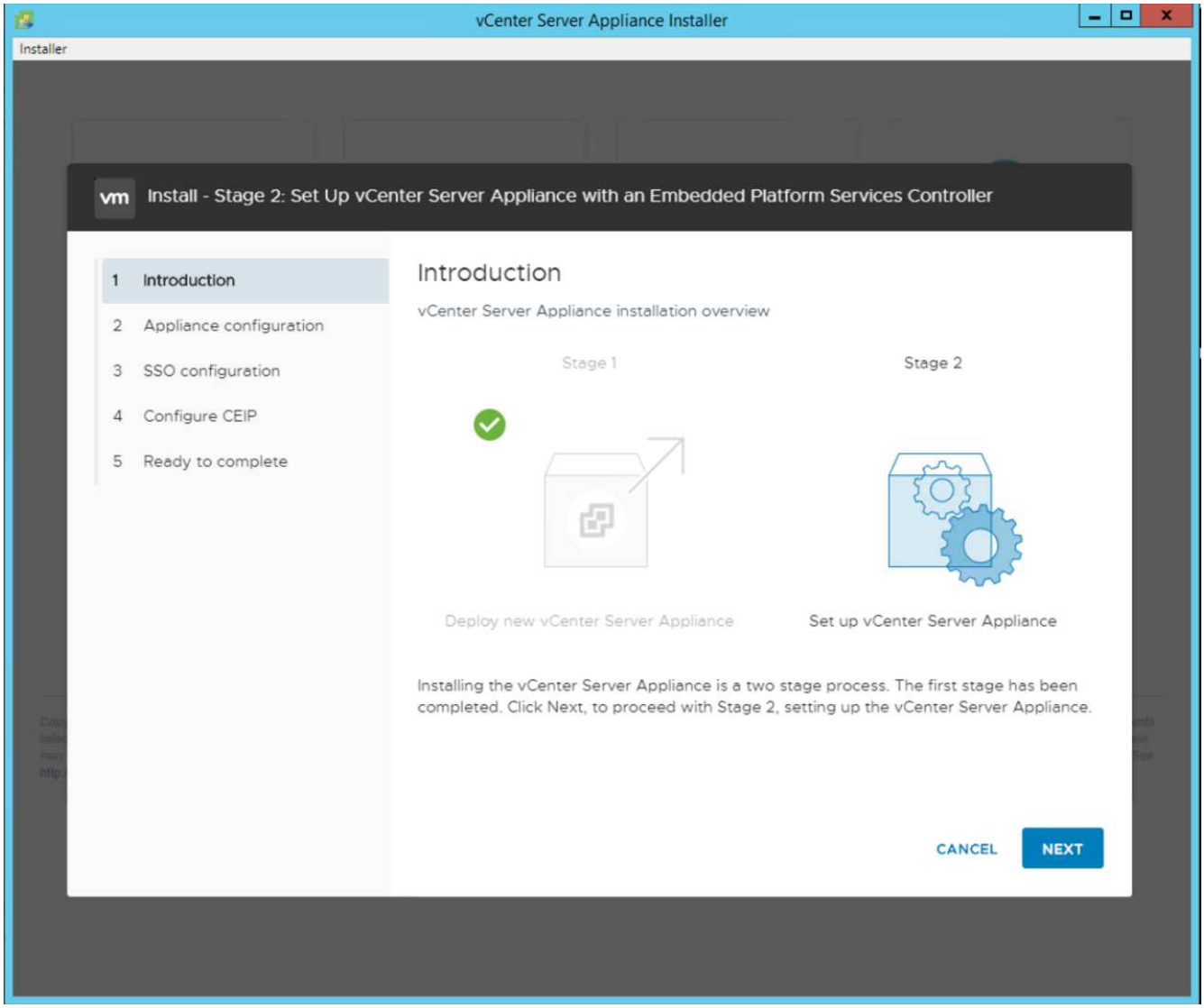


15. Revise la configuración en la etapa 1 antes de iniciar la implementación del dispositivo.

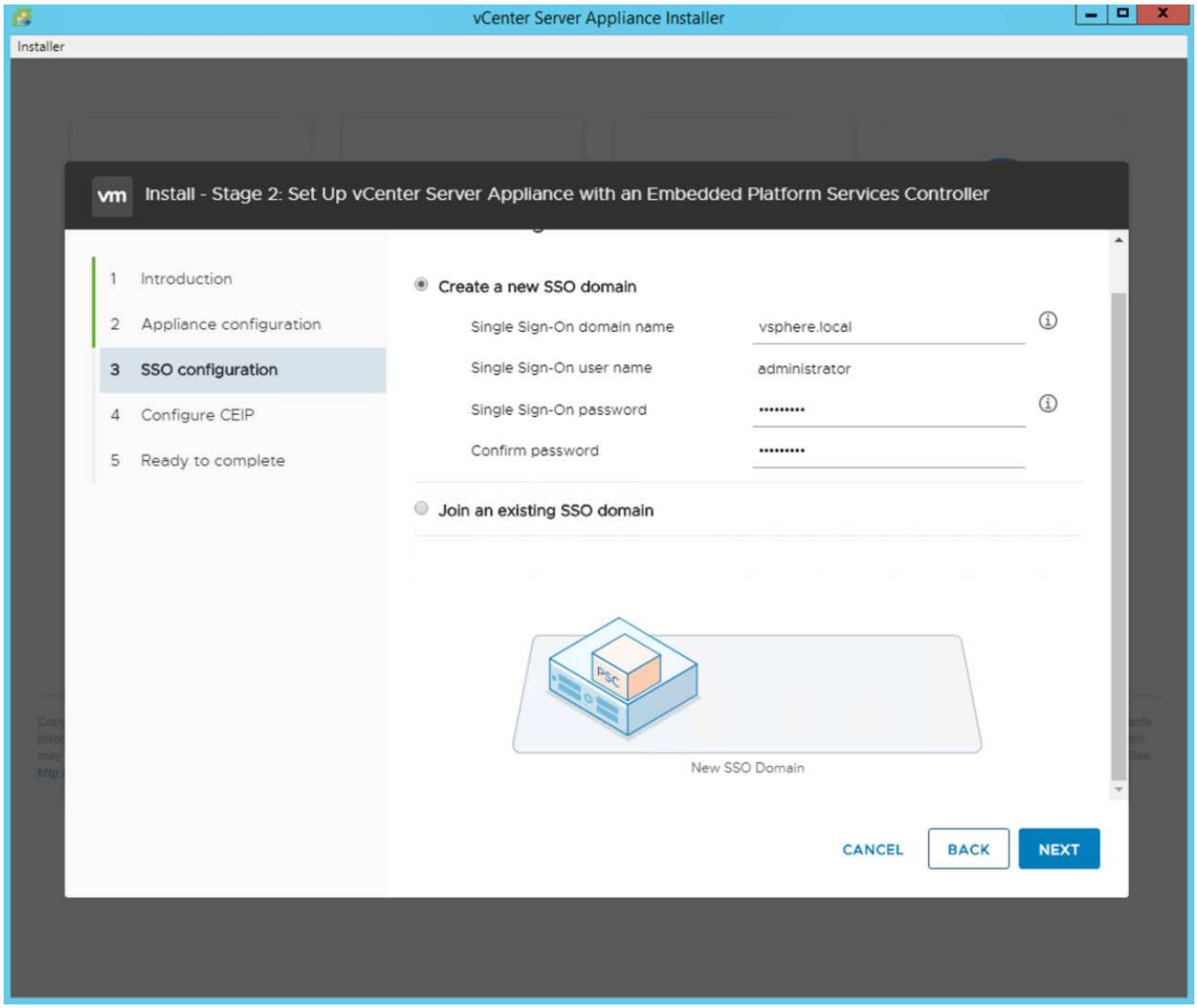


La VCSA se instala ahora. Este proceso tarda varios minutos.

16. Una vez completada la fase 1, aparece un mensaje que indica que se ha completado. Haga clic en continuar para iniciar la configuración de la fase 2.
17. En la página Introducción de fase 2, haga clic en Siguiente.

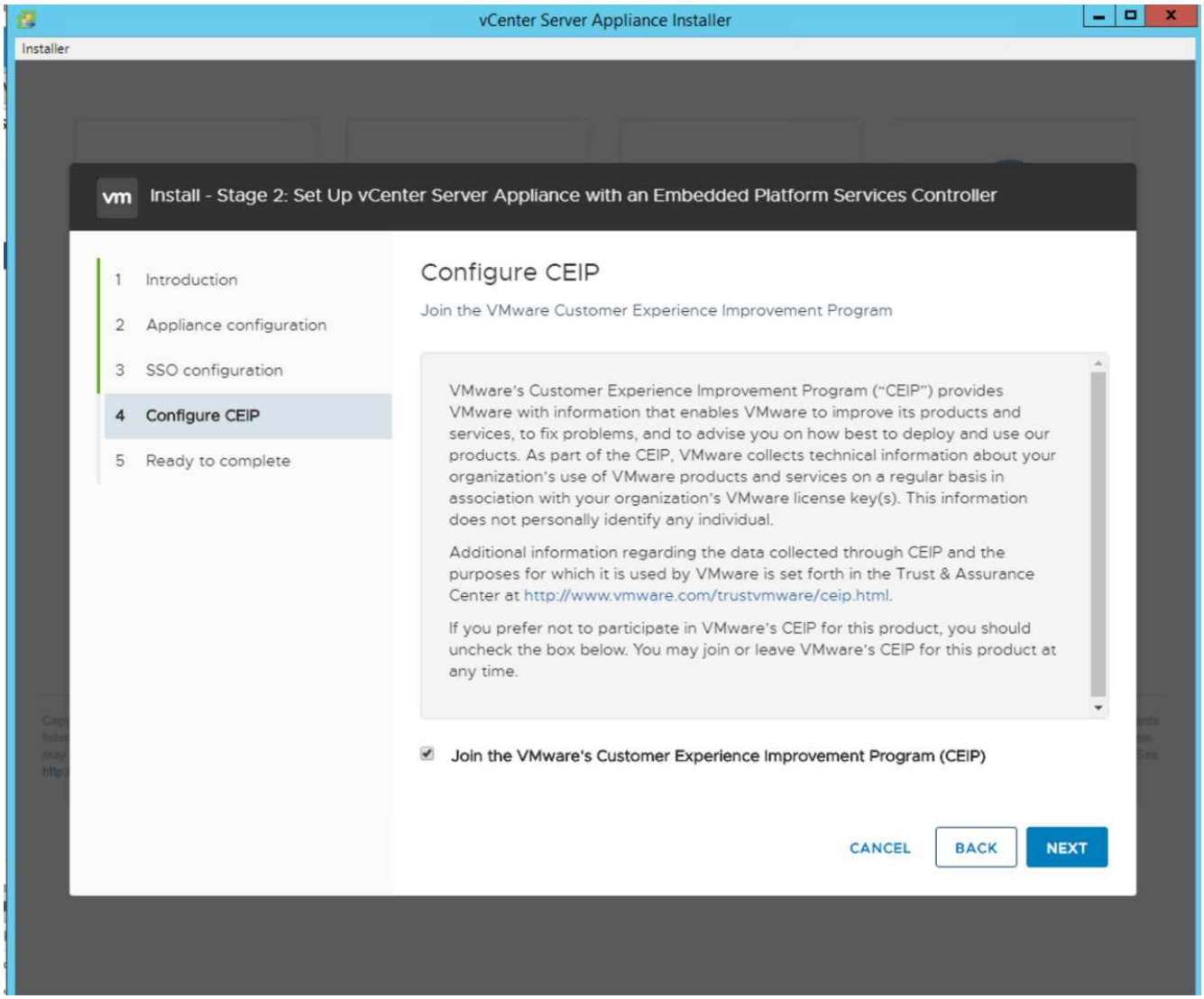


18. Introduzca `<<var_ntp_id>>` Para la dirección del servidor NTP. Puede introducir varias direcciones IP de NTP.
19. Si tiene pensado utilizar la alta disponibilidad (ha) de vCenter Server, asegúrese de que el acceso SSH esté habilitado.
20. Configure el nombre de dominio, la contraseña y el nombre del sitio de SSO. Haga clic en Siguiente.

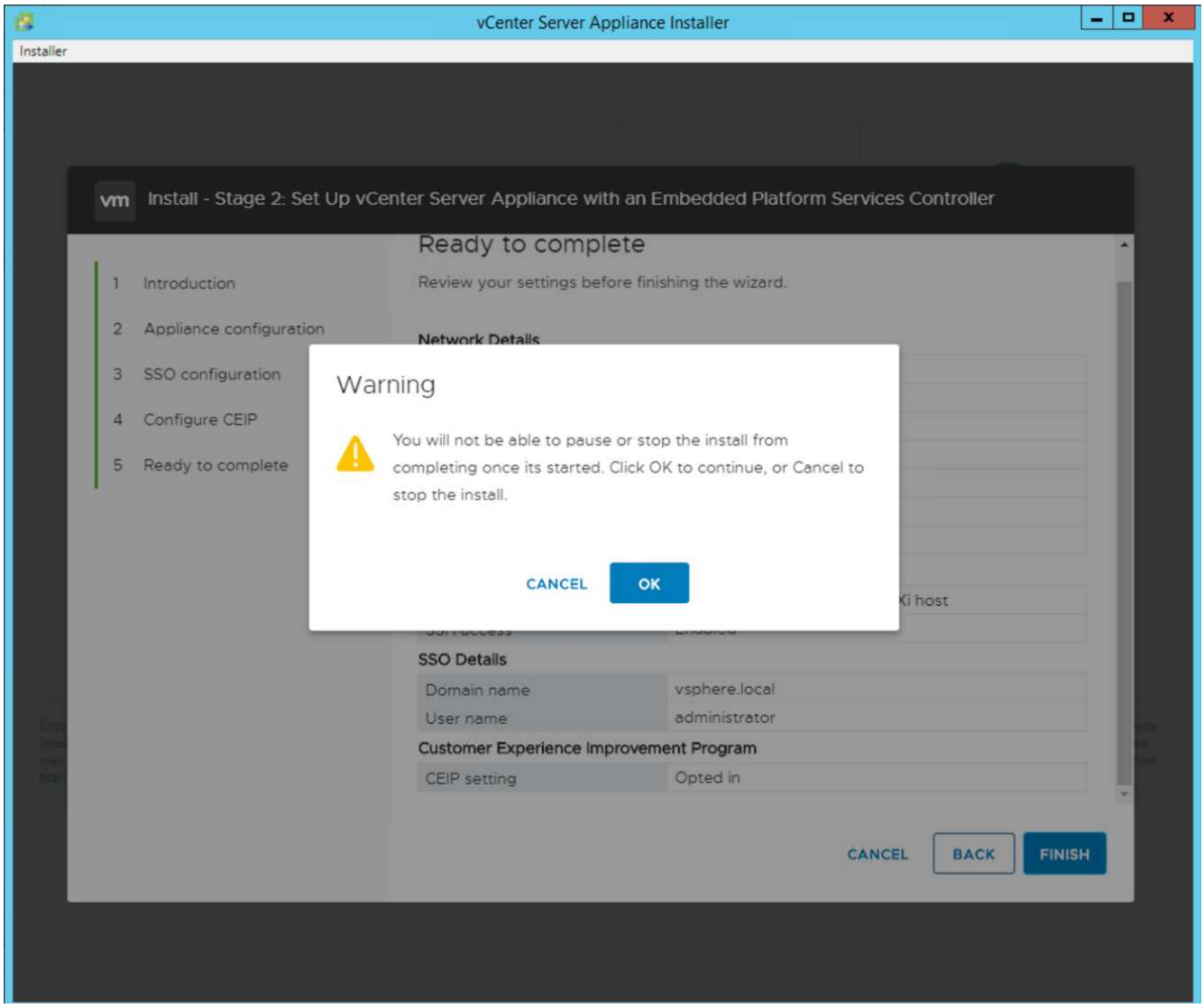


Registre estos valores para su referencia, especialmente si se desvía de la `vsphere.local` nombre de dominio.

21. Únase al programa de experiencia del cliente de VMware si lo desea. Haga clic en Siguiente.



22. Vea el resumen de la configuración. Haga clic en Finalizar o utilice el botón Atrás para editar la configuración.
23. Aparece un mensaje que indica que no podrá detener o detener la instalación una vez iniciada. Haga clic en OK para continuar.



La configuración del dispositivo continúa. Esto tarda varios minutos.

Aparece un mensaje que indica que la configuración se ha realizado correctamente.

24. Los enlaces que el instalador proporciona para acceder a vCenter Server pueden hacer clic.

"Siguiente: Configuración de clustering de VMware vCenter Server 6.7U2 y vSphere."

Configuración de clustering de VMware vCenter Server 6.7U2 y vSphere

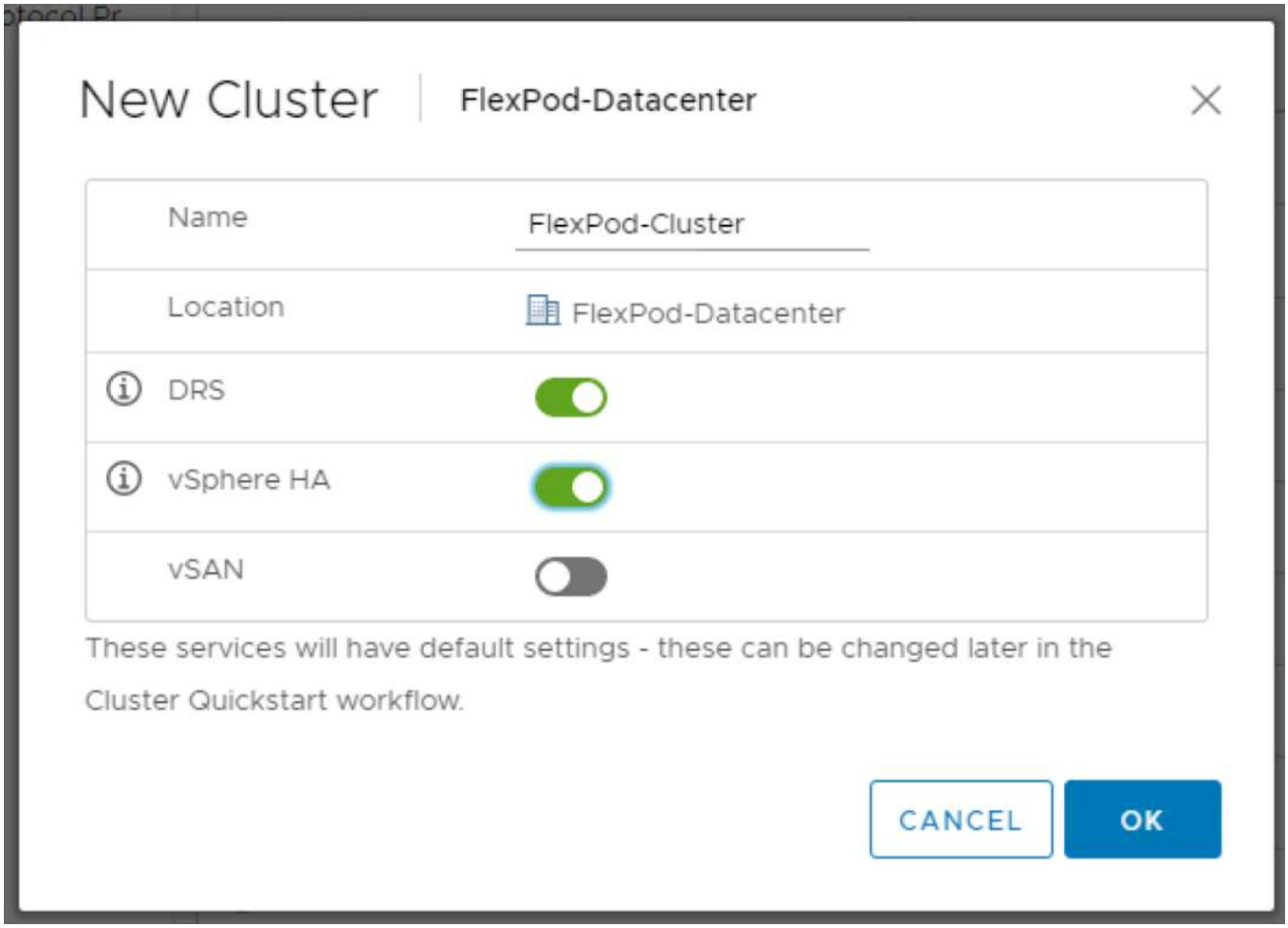
Para configurar la agrupación en clústeres de VMware vCenter Server 6.7 y vSphere, complete los pasos siguientes:

1. Vaya a. `https://<<FQDN or IP of vCenter>>/vsphere-client/`.
2. Haga clic en Launch vSphere Client.
3. Inicie sesión con el nombre de usuario mailto:administrator@vspehre.loc/ tl[Administrator]@vsphere.local y la contraseña SSO que introdujo durante el proceso de configuración de VCSA.
4. Haga clic con el botón derecho en el nombre de vCenter y seleccione New Datacenter.
5. Introduzca un nombre para el centro de datos y haga clic en Aceptar.

Cree un clúster de vSphere

Para crear un clúster de vSphere, complete los siguientes pasos:

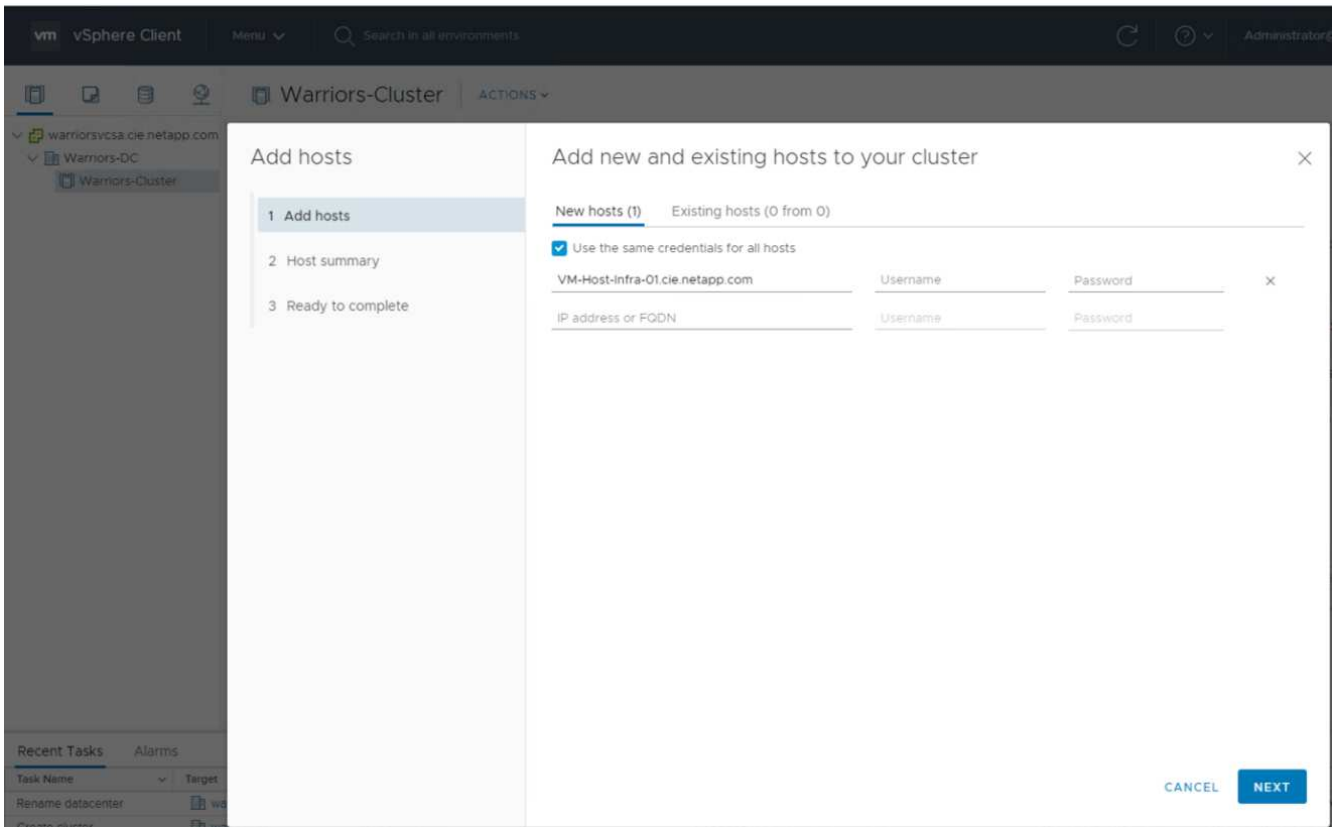
1. Haga clic con el botón derecho en el centro de datos recién creado y seleccione New Cluster.
2. Escriba un nombre para el clúster.
3. Active la recuperación ante desastres y vSphere ha seleccionando las casillas de verificación.
4. Haga clic en Aceptar.



Añada los hosts ESXi al clúster

Para añadir los hosts ESXi al clúster, complete los siguientes pasos:

1. Haga clic con el botón derecho en el clúster y seleccione Add Host.



2. Para añadir un host ESXi al clúster, complete los siguientes pasos:
   a. Introduzca la dirección IP o el FQDN del host. Haga clic en Siguiente.
   b. Introduzca el nombre de usuario raíz y la contraseña. Haga clic en Siguiente.
   c. Haga clic en Sí para reemplazar el certificado del host por un certificado firmado por el servidor de certificados VMware.
   d. Haga clic en Siguiente en la página Resumen de host.
   e. Haga clic en el icono verde + para añadir una licencia al host de vSphere.
3. Este paso se puede completar más adelante si se desea.
   a. Haga clic en Siguiente para desactivar el modo de bloqueo.
   b. Haga clic en Next en la página de ubicación de la máquina virtual.
   c. Revise la página Listo para completar. Utilice el botón Atrás para realizar cualquier cambio o seleccione Finalizar.
4. Repita los pasos 1 y 2 para el host Cisco UCS B.

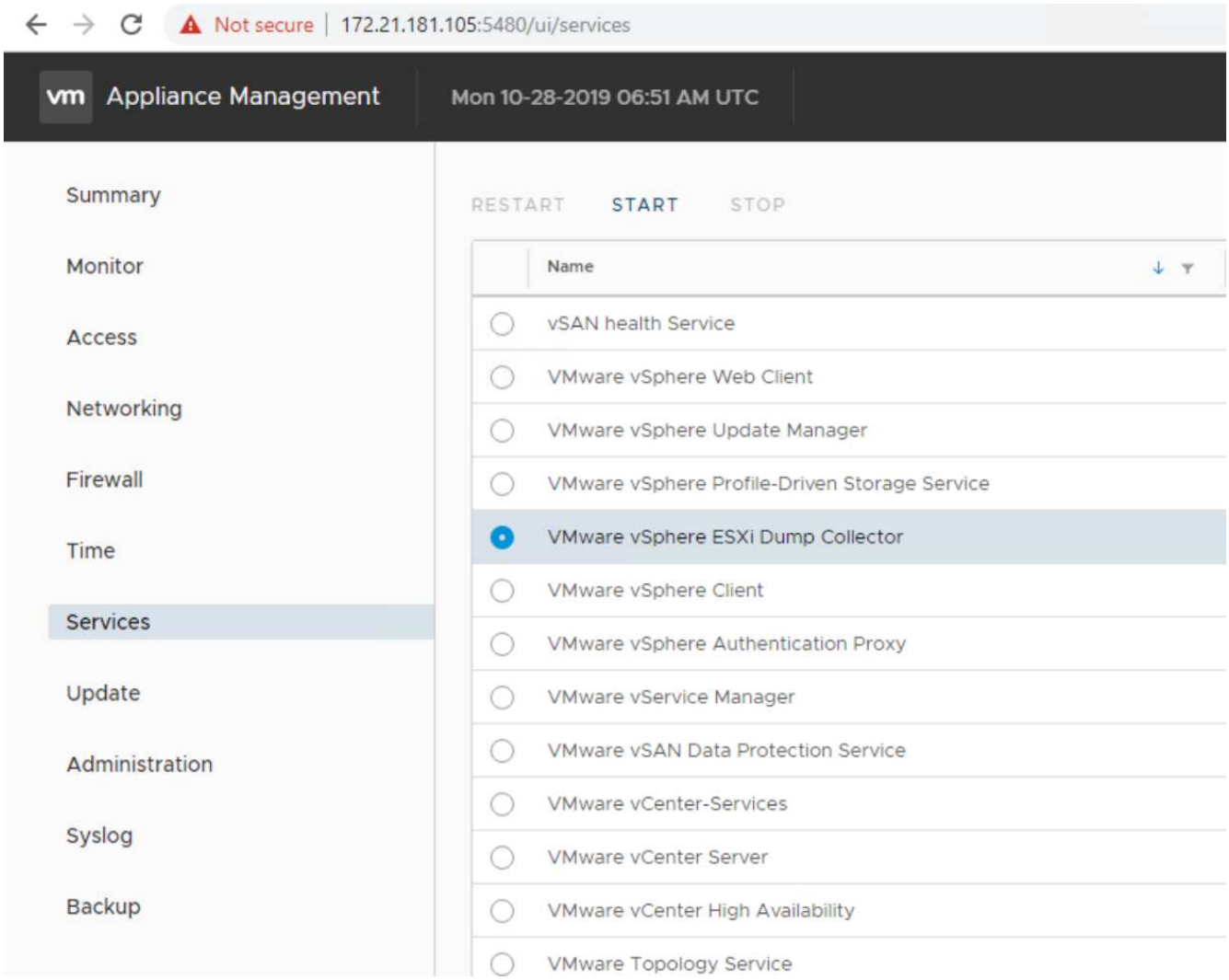
> Debe completar este proceso para los hosts adicionales que se agreguen a la configuración exprés de FlexPod.

Configure coredump en hosts ESXi

Para configurar coredump en hosts ESXi, complete los siguientes pasos:

1. Inicie sesión en https:// "VCenter" IP:5480/, escriba root para el nombre de usuario e introduzca la contraseña de root.

2. Haga clic en Services y seleccione VMware vSphere ESXI Dump collector.
3. Inicie el servicio de recopilador DE volcado DE ESXI de VMware vSphere.



4. Utilice SSH, conéctese al host ESXi de IP de gestión, introduzca root para el nombre de usuario e introduzca la contraseña raíz.
5. Ejecute los siguientes comandos:

```
esxcli system coredump network set -i ip_address_of_core_dump_collector
-v vmk0 -o 6500
esxcli system coredump network set --enable=true
esxcli system coredump network check
```

6. El mensaje `Verified the configured netdump server is running` aparece después de introducir el comando final.

```
root@VM-Host-Infra-01:~] esxcli system coredump network set -i 172.21.181.105 -
 vmk0 -o 6500
root@VM-Host-Infra-01:~]
root@VM-Host-Infra-01:~] esxcli system coredump network set --enable=true
root@VM-Host-Infra-01:~] esxcli system coredump network check
erified the configured netdump server is running
```

Este proceso debe completarse para cualquier host adicional que se añada a FlexPod Express.

`ip_address_of_core_dump_collector` En esta validación está la IP de vCenter.

"Siguiente: Procedimientos de puesta en marcha de Virtual Storage Console 9,6 de NetApp."

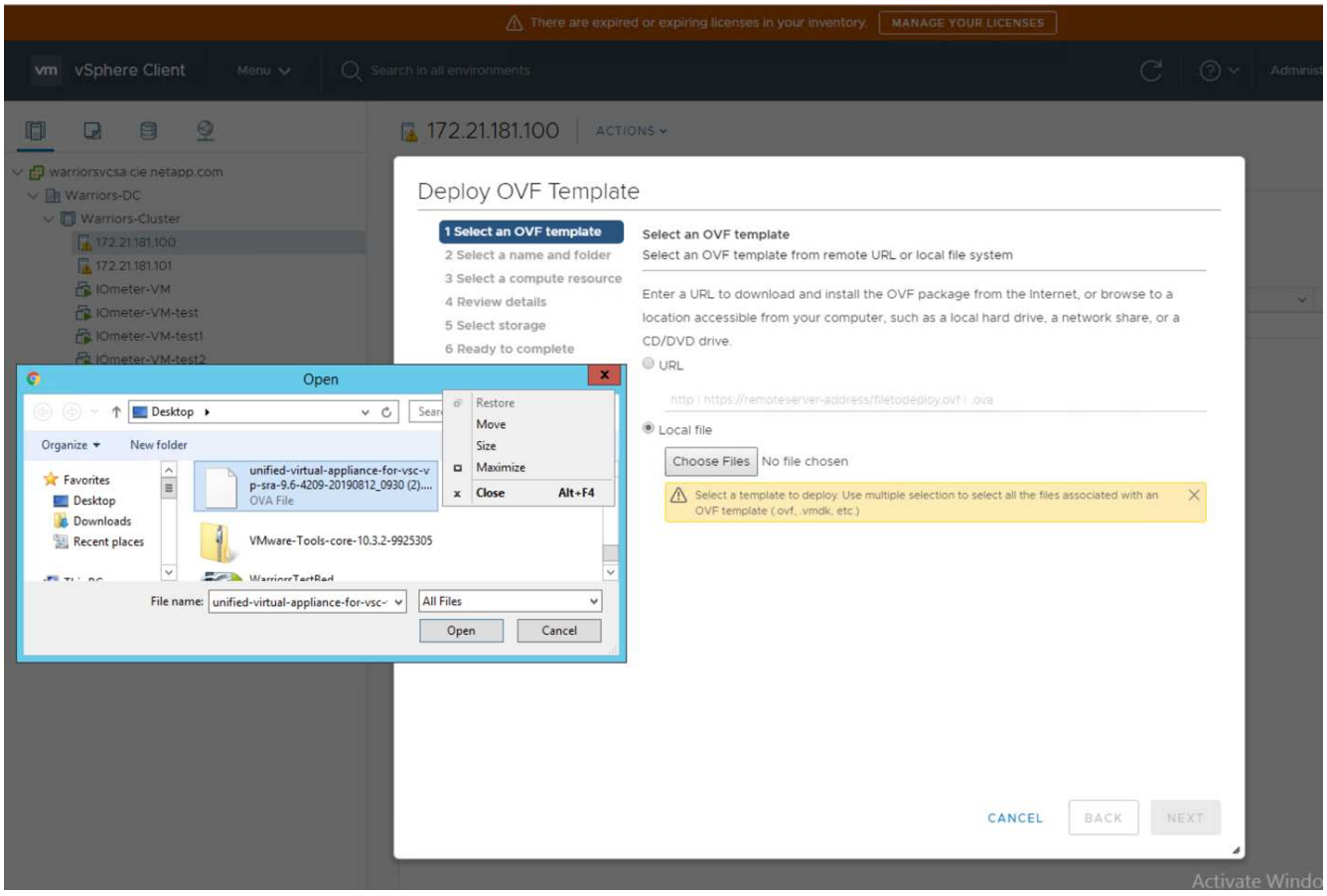
Procedimientos de puesta en marcha de Virtual Storage Console 9.6 de NetApp

En esta sección se describen los procedimientos de puesta en marcha de Virtual Storage Console (VSC) de NetApp.

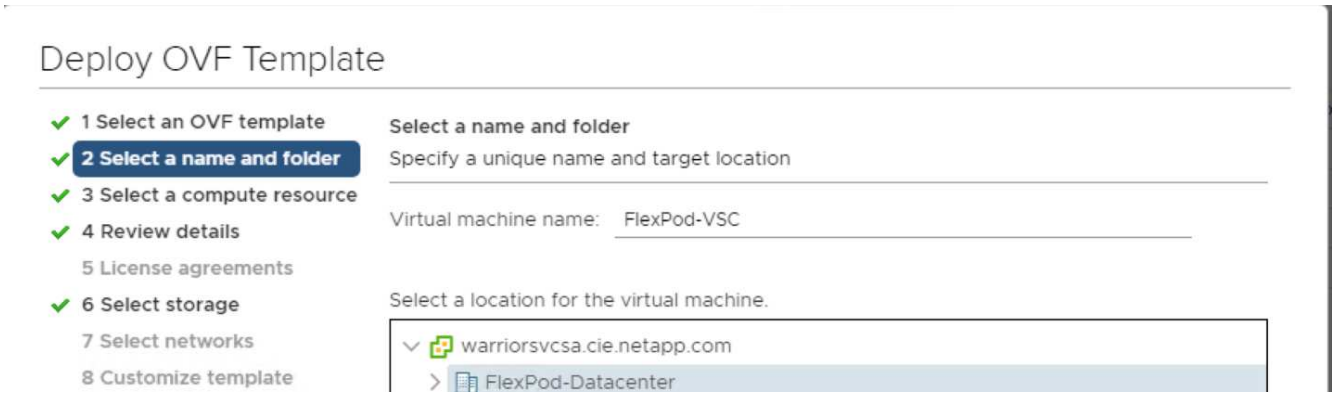
Instalar Virtual Storage Console 9.6

Para instalar el software VSC 9.6 mediante una implementación de formato de virtualización abierta (OVF), siga estos pasos:

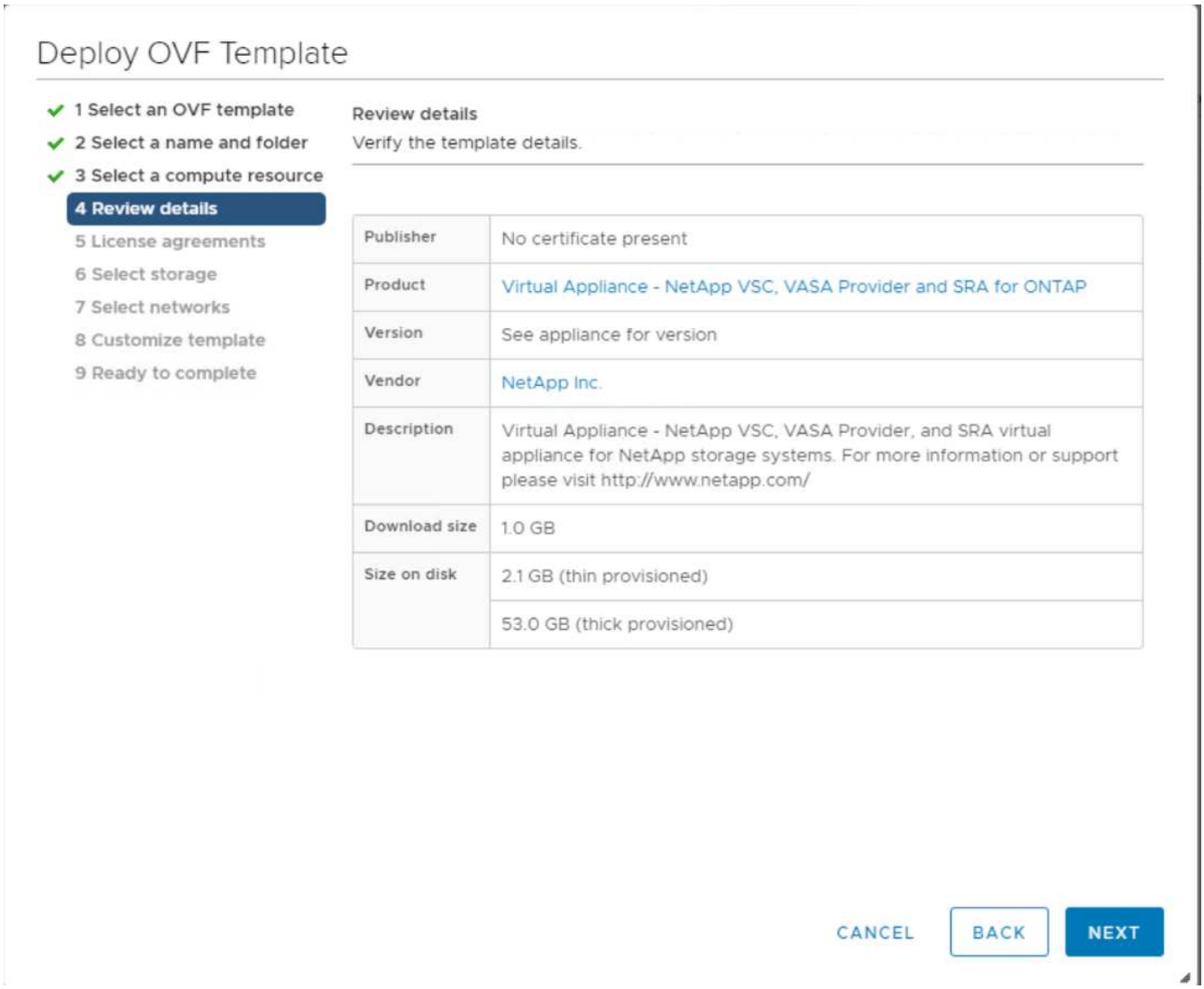
1. Vaya a vSphere Web Client > Host Cluster > Deploy OVF Template.
2. Desplácese hasta el archivo OVF de VSC descargado del sitio de soporte de NetApp.



3. Introduzca el nombre de la máquina virtual y seleccione el centro de datos o la carpeta en la que desea implementar. Haga clic en Siguiente.

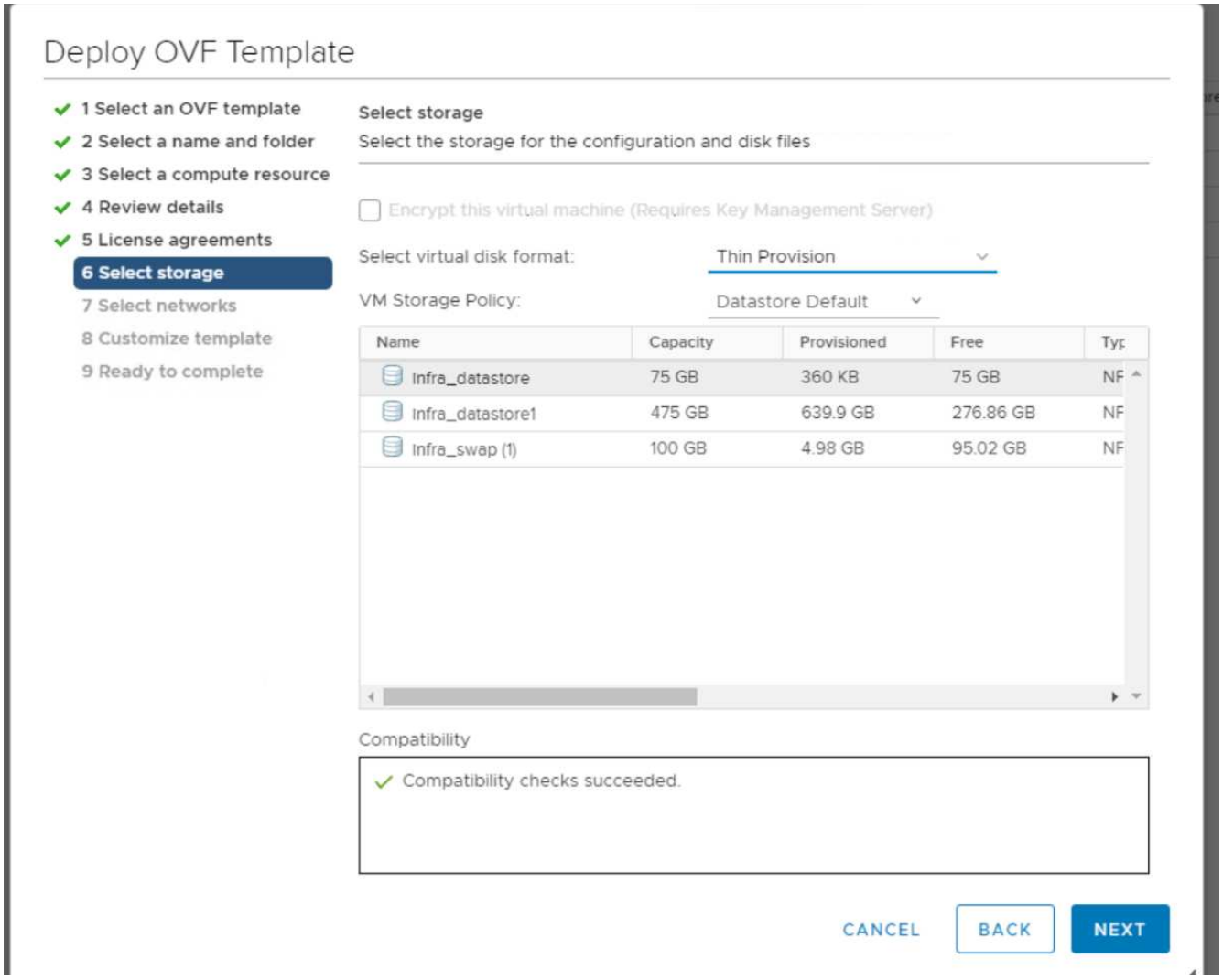


4. Seleccione el clúster FlexPod-Cluster ESXi y haga clic en Next.
5. Revise los detalles y haga clic en Next.

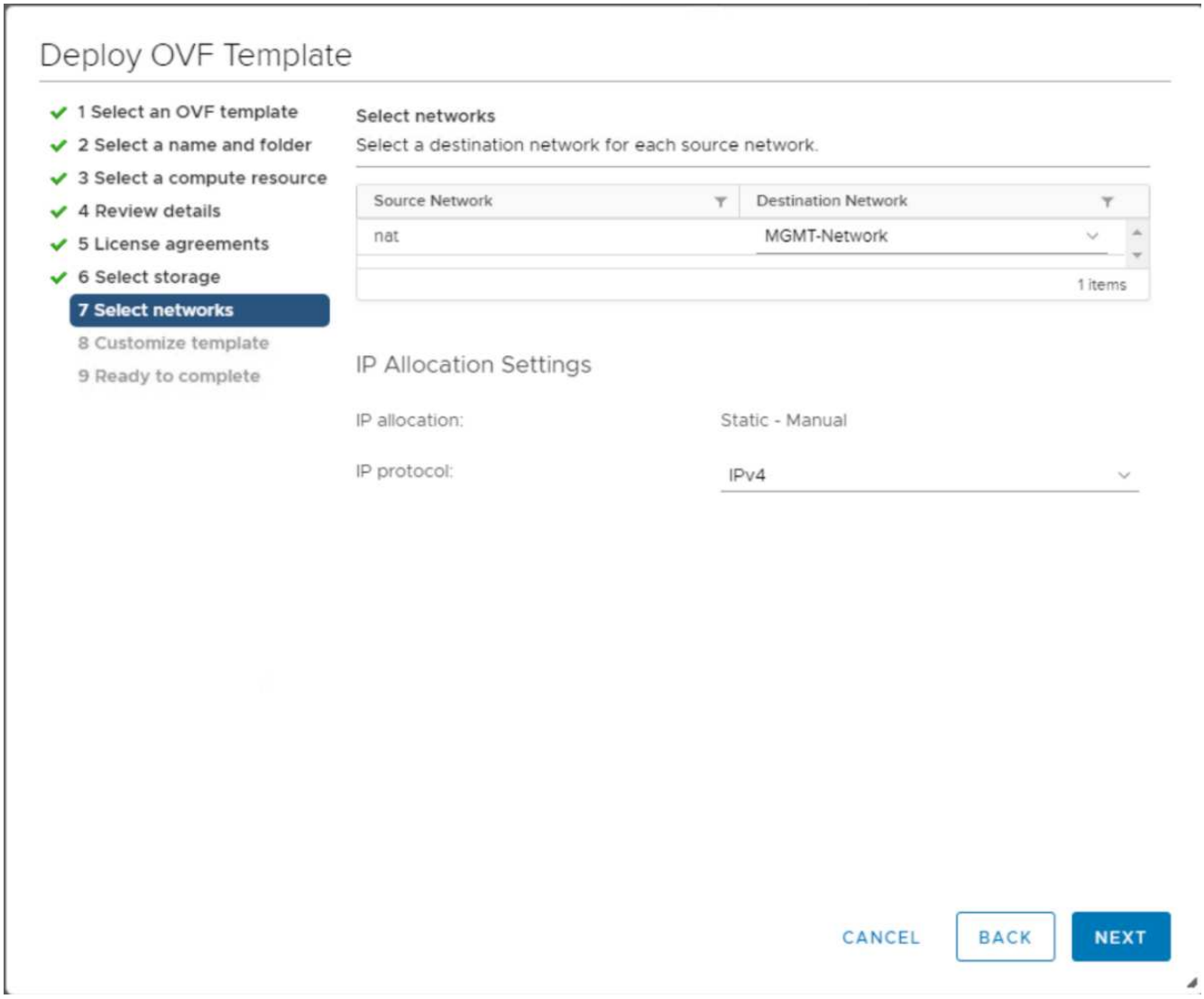


6. Haga clic en Aceptar para aceptar la licencia y haga clic en Siguiente.
7. Seleccione el formato de disco virtual de thin provisioning y uno de los almacenes de datos NFS. Haga clic

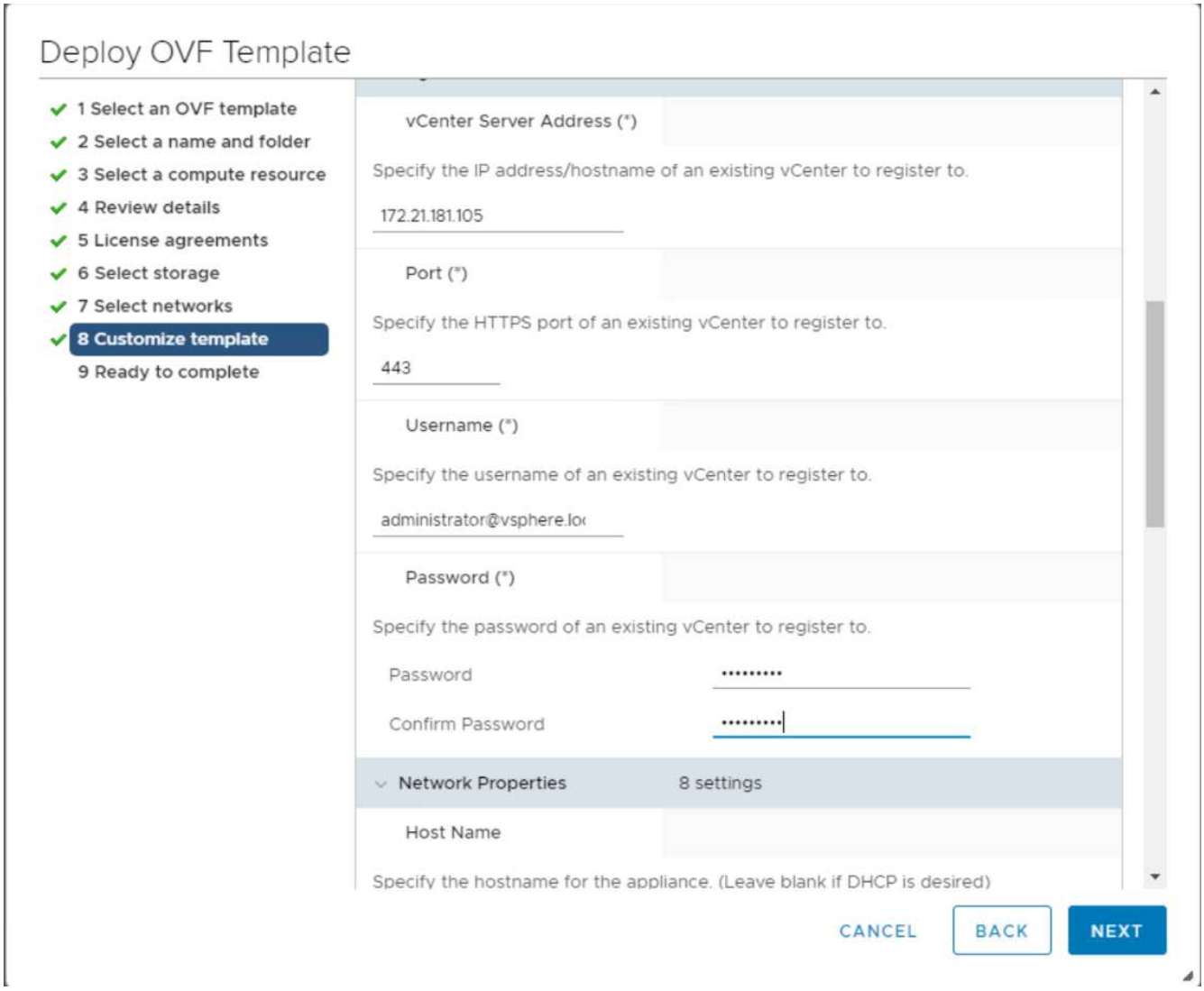
en Siguiente.



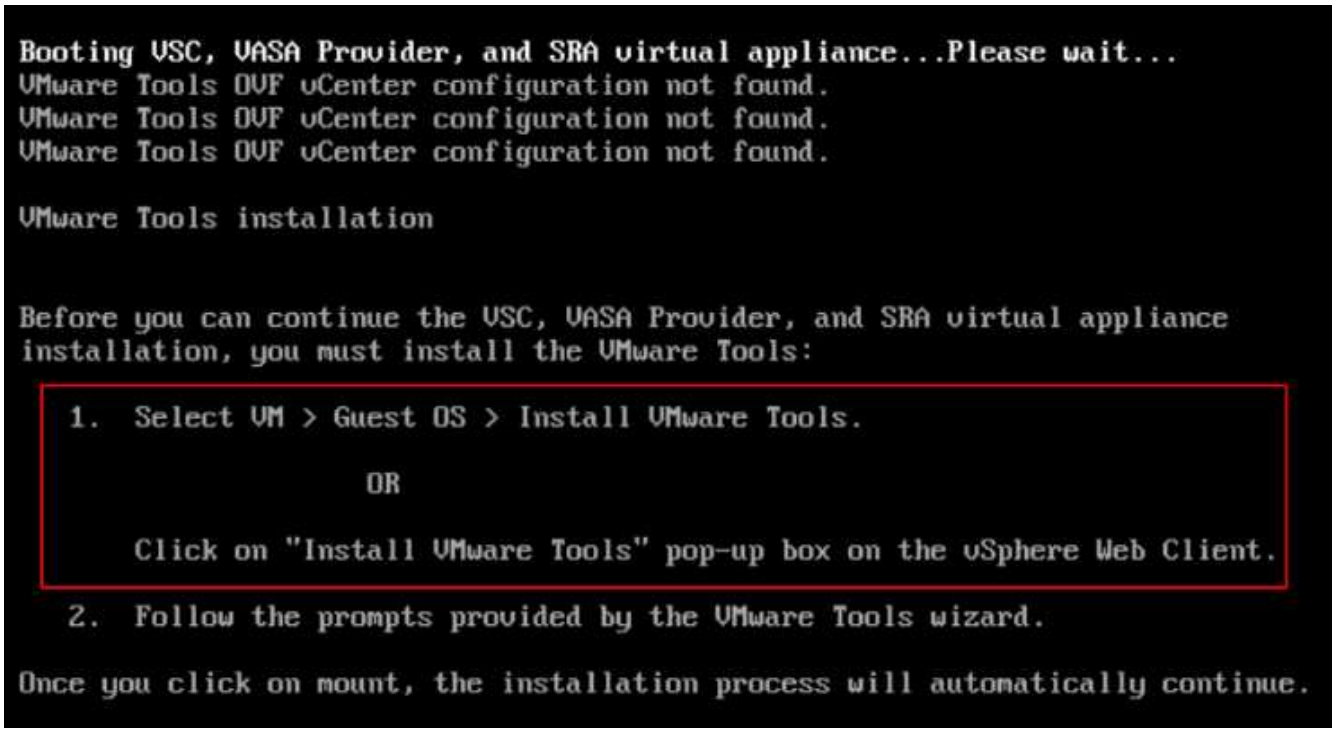
8. En Seleccionar redes, elija una red de destino y haga clic en Siguiente.



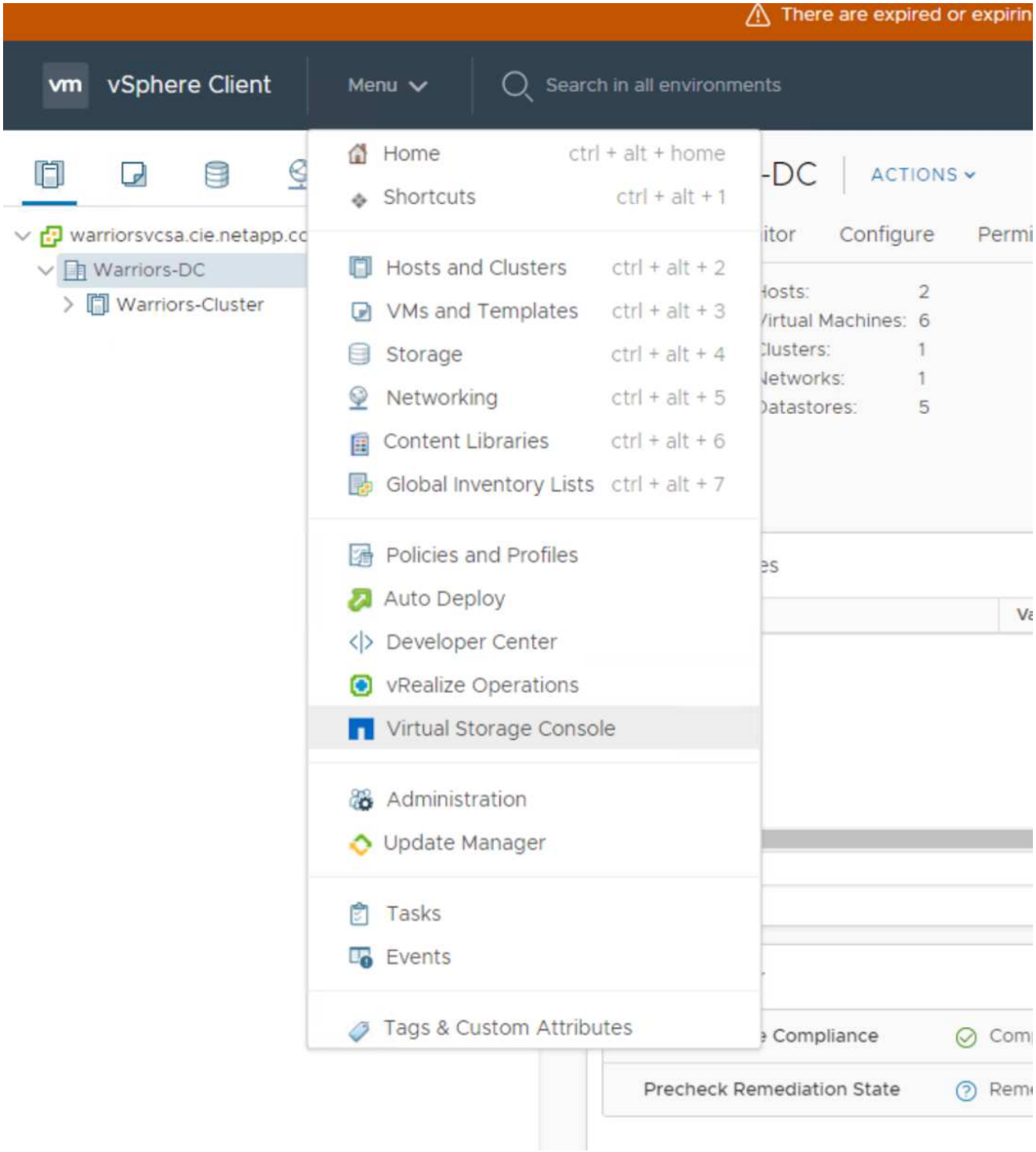
9. En Customize Template, introduzca la contraseña del administrador de VSC, el nombre o la dirección IP de vCenter y otros detalles de la configuración, y haga clic en Next.



10. Revise los detalles de la configuración introducidos y haga clic en Finish para completar la puesta en marcha de la máquina virtual de NetApp-VSC.
11. Encienda la máquina virtual de NetApp-VSC y abra la consola de equipos virtuales.
12. Durante el proceso de arranque de máquinas virtuales NetApp-VSC, verá un aviso para instalar las herramientas de VMware. En vCenter, seleccione NetApp-VSC VM > SO invitado > instalar VMware Tools.



13. La información de registro de vCenter y la configuración de la red se proporcionó durante la personalización de la plantilla OVF. Por lo tanto, una vez que se ejecuta la máquina virtual de NetApp-VSC, VSC, las API de vSphere para el reconocimiento del almacenamiento (VASA) y el adaptador de replicación de almacenamiento (SRA) de VMware se registran en vCenter.
14. Cierre la sesión en vCenter Client y vuelva a iniciarla. En el menú Inicio, confirme que VSC de NetApp está instalado.



Descargue e instale el complemento VAAI para NFS de NetApp

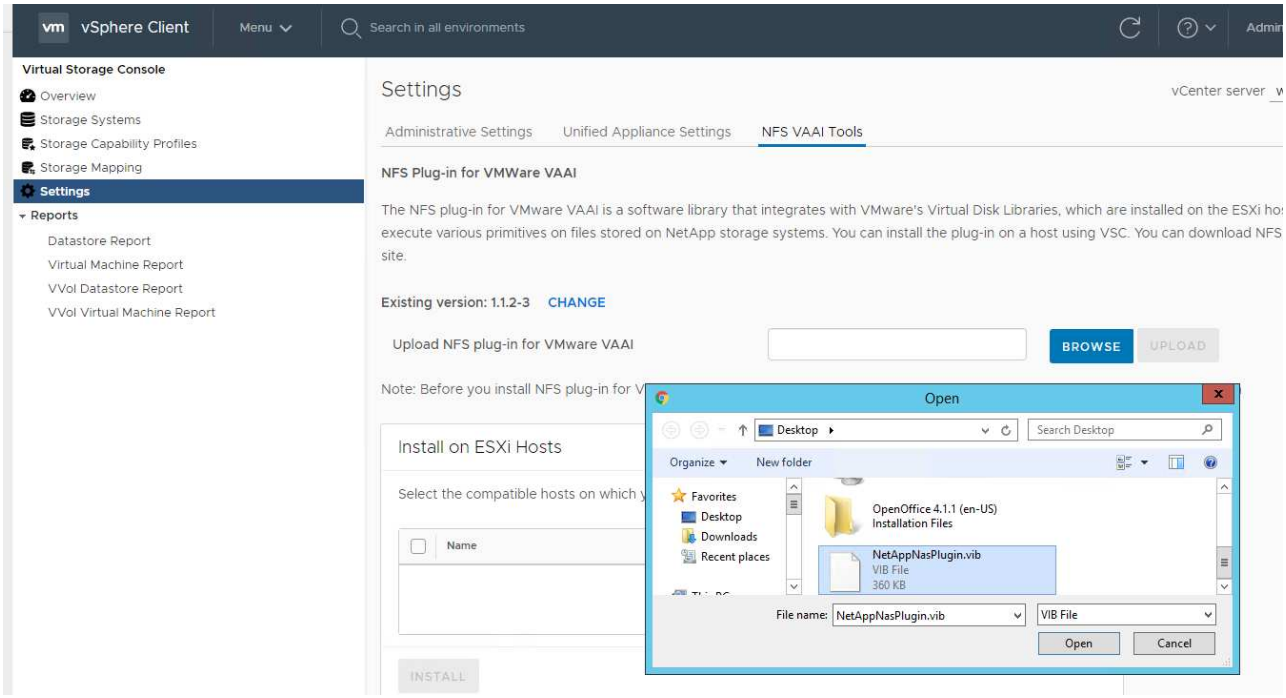
Para descargar e instalar el complemento VAAI para NFS de NetApp, complete los siguientes pasos:

1. Descargue el complemento NFS de NetApp 1.1.2 para VMware `.vib` Archivo desde la página de descarga del complemento NFS y guárdelo en el equipo local o en el host de administración.
2. Descargue el plugin de NetApp NFS para VMware VAAI:
   a. Vaya a la "página de descarga del software".

b. Desplácese hacia abajo y haga clic en NetApp NFS Plug-in for VMware VAAI.

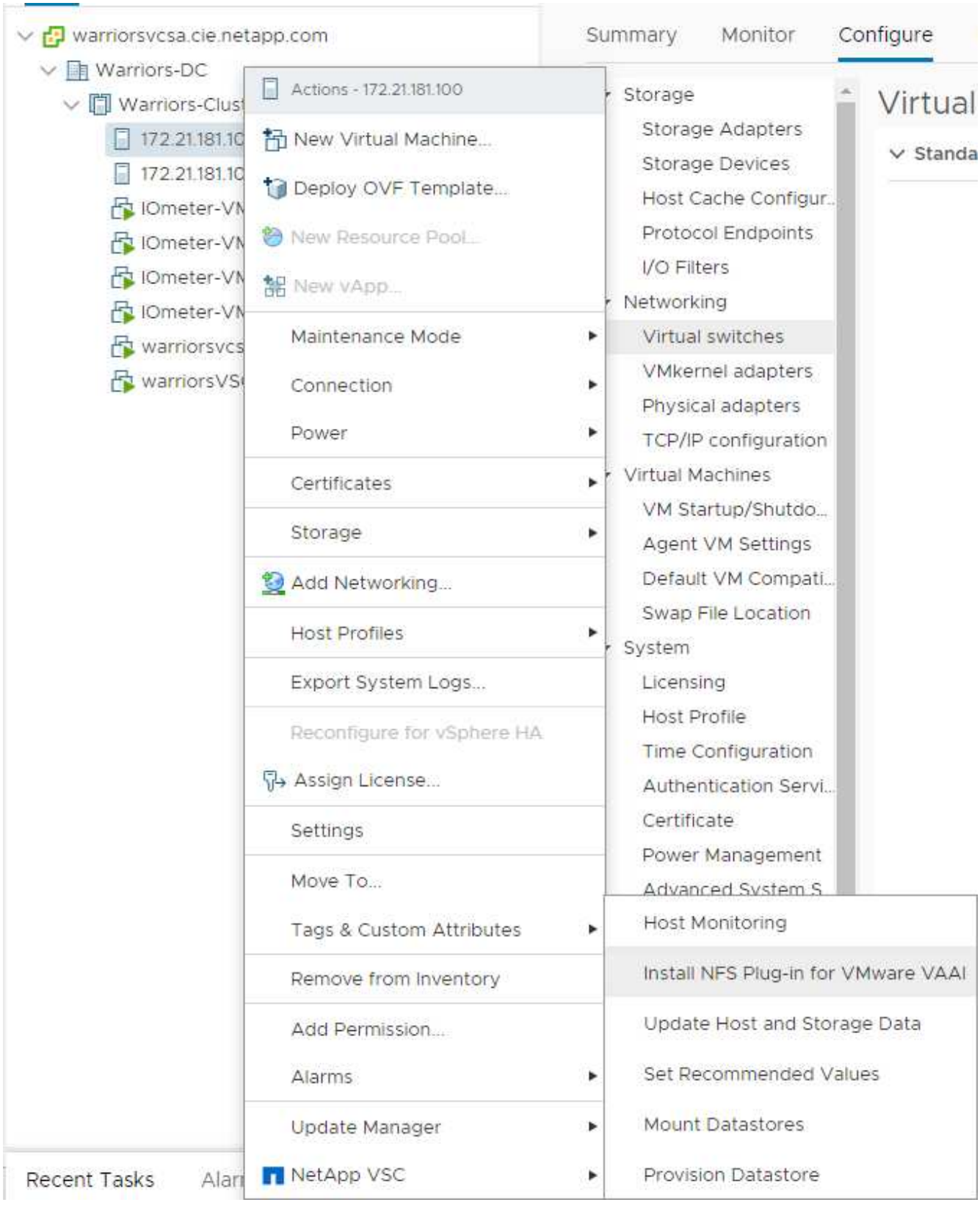
c. En la pantalla de inicio del cliente web de vSphere, seleccione Virtual Storage Console.

d. En Virtual Storage Console > Configuración > NFS VAAI Tools, cargue el plugin de NFS seleccionando Select File y desplácese hasta la ubicación donde se almacena el plugin descargado.



3. Haga clic en Upload para transferir el plugin a vCenter.

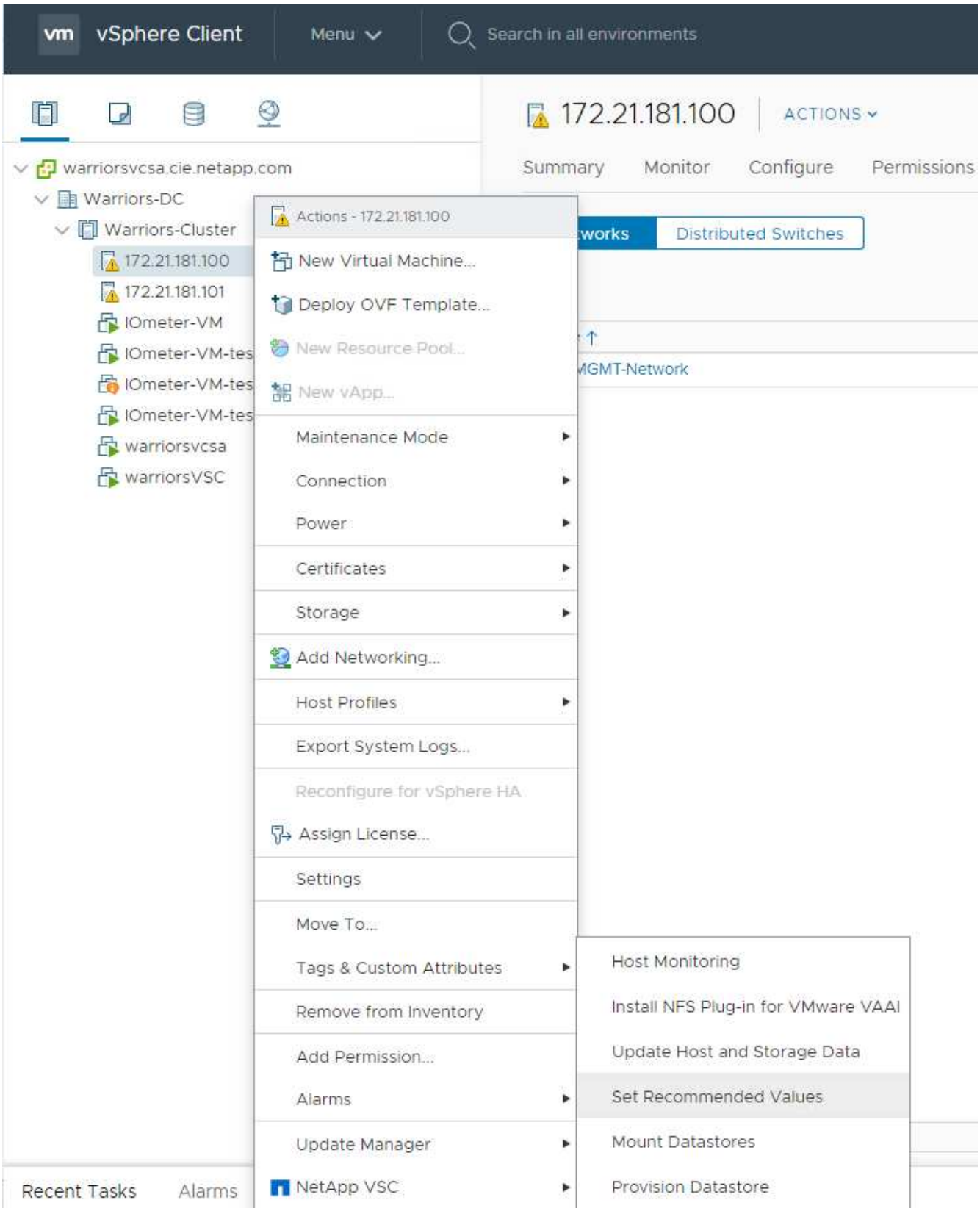
4. Seleccione el host y, a continuación, seleccione NetApp VSC > Install NFS Plug-in for VMware VAAI.



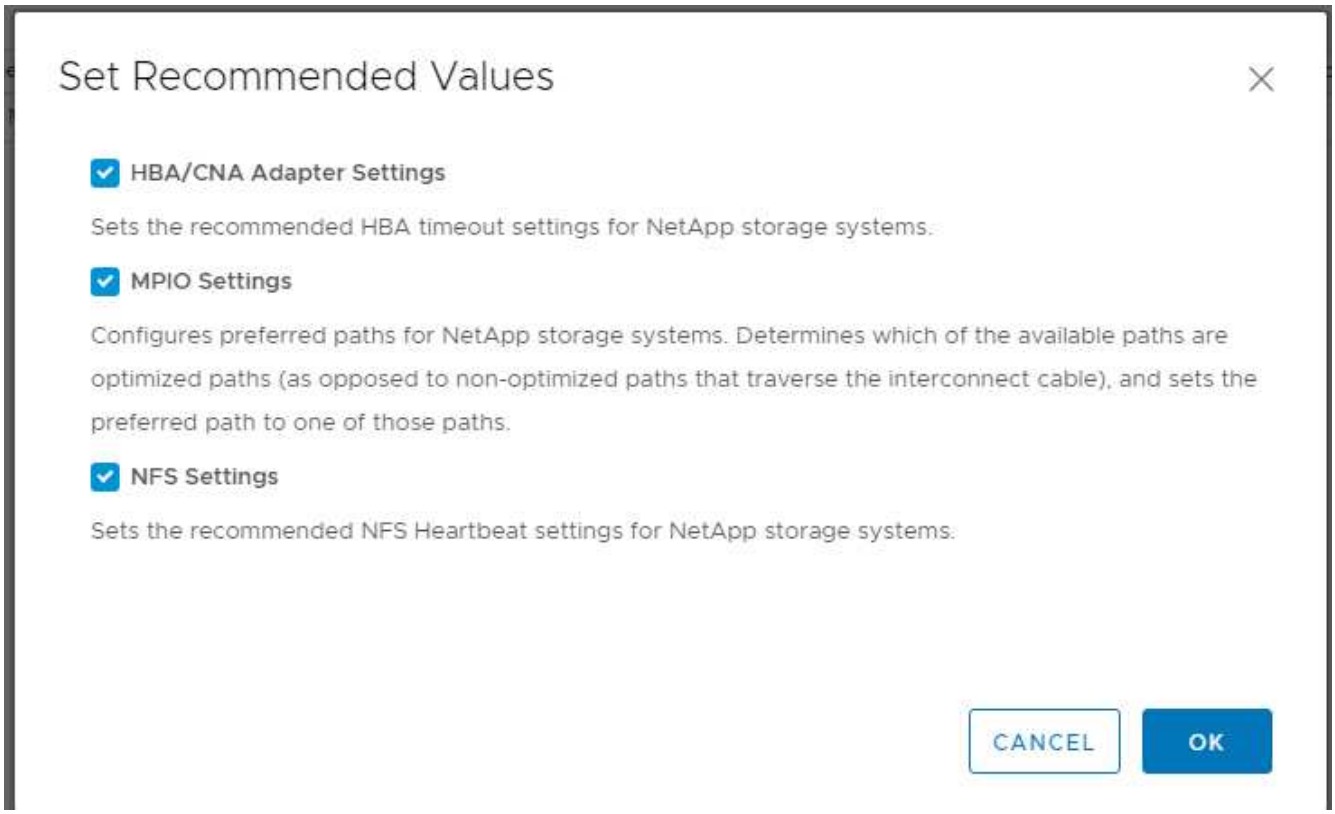
Use la configuración de almacenamiento óptima para los hosts ESXi

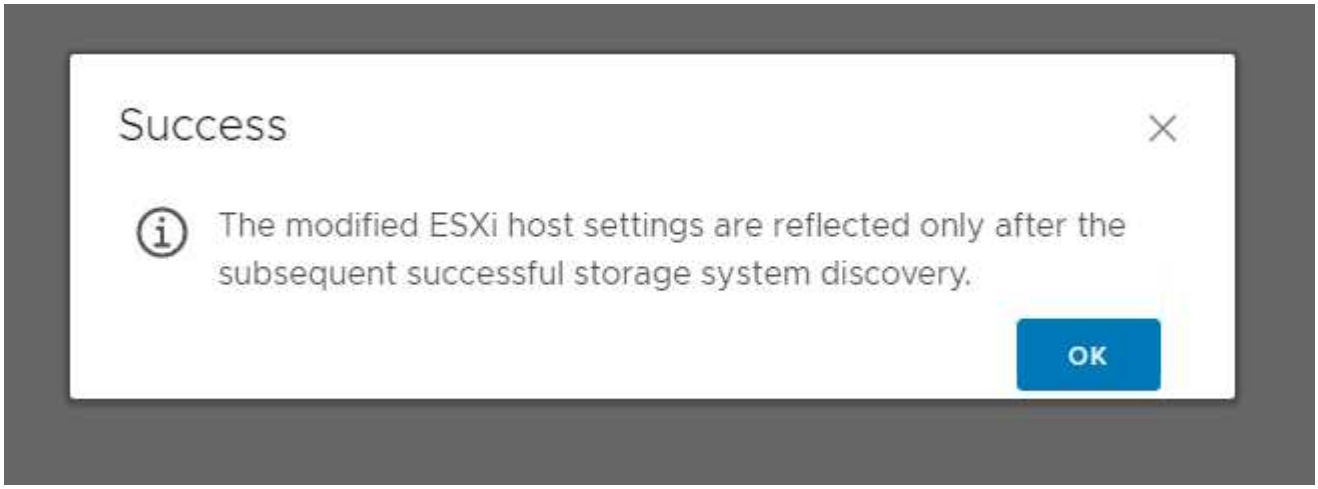
VSC permite configurar de forma automatizada ajustes relacionados con el almacenamiento para todos los hosts ESXi conectados a controladoras de almacenamiento de NetApp. Para utilizar esta configuración, lleve a cabo los siguientes pasos:

1. En la pantalla Inicio, seleccione vCenter > hosts and Clusters. Para cada host ESXi, haga clic con el botón derecho y seleccione NetApp VSC > Set Recommended Values.



2. Compruebe la configuración que desea aplicar a los hosts de vSphere seleccionados. Haga clic en Aceptar para aplicar la configuración.





3. Reinicie el host ESXI después de aplicar esta configuración.

Conclusión

FlexPod Express proporciona una solución sencilla y efectiva, ya que proporciona un diseño validado que utiliza componentes líderes del sector. Al escalar mediante la adición de componentes, FlexPod Express puede adaptarse a las necesidades específicas del negocio. FlexPod Express se diseñó para pequeñas y medianas empresas, oficinas remotas y otras empresas que requieren soluciones dedicadas.

Reconocimientos

Los autores quieren reconocer a John George por su apoyo y contribución a este diseño.

Dónde encontrar información adicional

Para obtener más información sobre la información descrita en este documento, consulte los siguientes documentos y/o sitios web:

Documentación de productos de NetApp

http://docs. "netapp".com

Guía exprés de FlexPod

Diseño de la arquitectura NVA-1139: FlexPod Express con Cisco UCS C-Series y AFF C190 Series de NetApp

"https://www.netapp.com/us/media/nva-1139-design.pdf"

Historial de versiones

Versión	Fecha	Historial de versiones del documento
Versión 1.0	Noviembre de 2019	Versión inicial.

Guía de diseño de FlexPod Express con Cisco UCS C-Series y AFF A220 Series

Diseño NVA-1125: FlexPod Express con Cisco UCS C-Series y AFF A220 Series

Savita Kumari, NetApp en colaboración con:

Las tendencias en el sector señalan una gran transformación de los centros de datos hacia una infraestructura compartida y cloud computing. Además, las organizaciones buscan una solución sencilla y eficaz para oficinas remotas y sucursales que aprovechen la tecnología con la que están familiarizados en su centro de datos.

FlexPod Express es una arquitectura de centro de datos prediseñada con las mejores prácticas que se basa en Cisco Unified Computing System (Cisco UCS), la familia de switches Cisco Nexus y AFF de NetApp. Los componentes de FlexPod Express se asemejan a los centros de datos FlexPod, lo que permite sinergias de gestión en un entorno completo de infraestructura TECNOLÓGICA a una escala menor. FlexPod Datacenter y FlexPod Express son plataformas óptimas para virtualización y para sistemas operativos con configuración básica y cargas de trabajo empresariales.

"Siguiente: Resumen del programa."

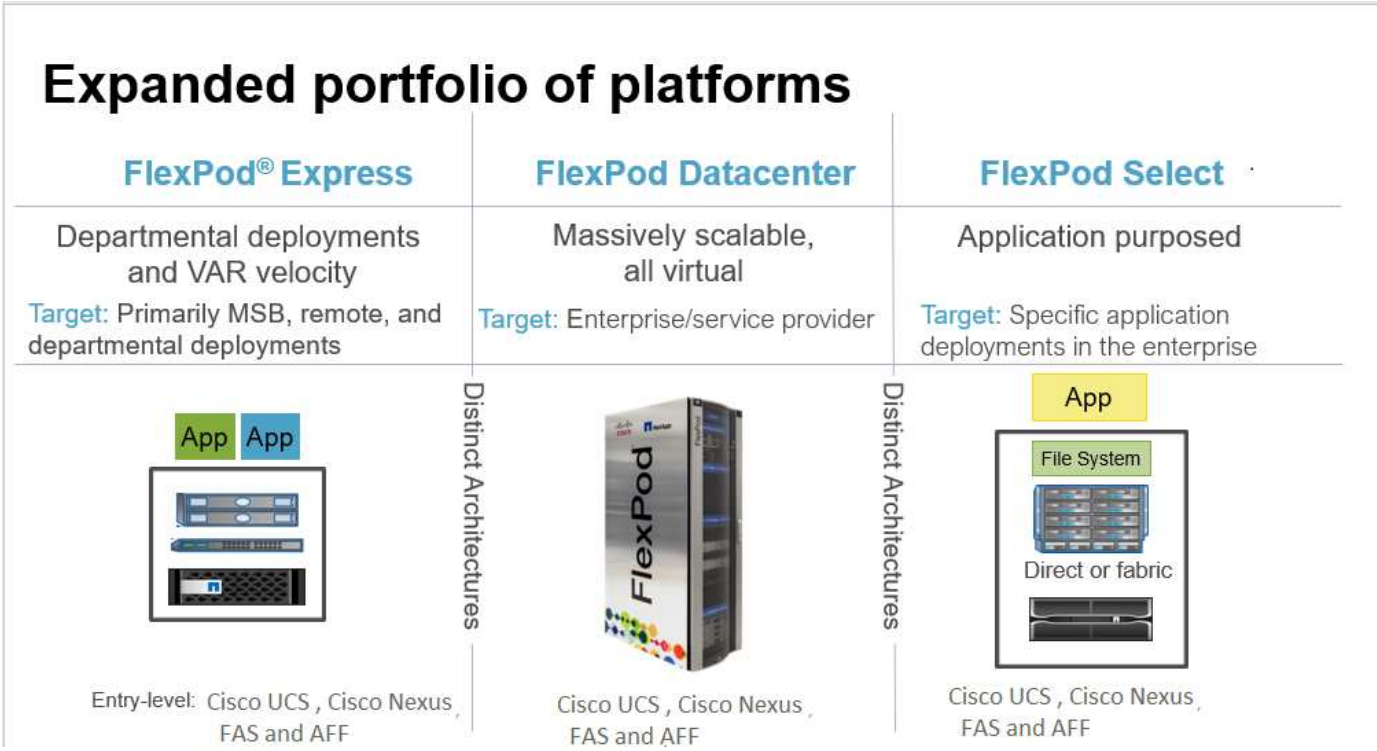
Resumen del programa

Cartera de infraestructuras convergentes FlexPod

Las arquitecturas de referencia de FlexPod se proporcionan como diseños validados por Cisco (CVD) o como arquitecturas verificadas de NetApp (NVA). Se permiten las desviaciones basadas en los requisitos del cliente de un CVD o NVA determinado si las variaciones no dan como resultado la puesta en marcha de configuraciones no compatibles.

Como se muestra en la siguiente figura, la cartera de FlexPod incluye tres soluciones: FlexPod Express, FlexPod Datacenter y FlexPod Select:

- **FlexPod Express.** ofrece una solución de gama básica que consiste en tecnologías de Cisco y NetApp.
- **FlexPod Datacenter.** proporciona una base multiuso óptima para diversas cargas de trabajo y aplicaciones.
- **FlexPod Select.** incorpora los mejores aspectos del centro de datos FlexPod y adapta la infraestructura a una aplicación determinada.



Programa Arquitectura validada por NetApp

El programa NVA ofrece a los clientes una arquitectura verificada para las soluciones NetApp. Una arquitectura validada de NetApp implica que la solución de NetApp tiene las siguientes cualidades:

- Ha sido probada a conciencia
- Tiene naturaleza prescriptiva
- Minimiza los riesgos de implementación
- Reduce el plazo de comercialización

Esta guía detalla el diseño de FlexPod Express con VMware vSphere. Además, este diseño aprovecha el nuevo sistema AFF A220, que ejecuta el software ONTAP 9.4 de NetApp, los switches Cisco Nexus 3172P y los servidores Cisco UCS C220 M5 como nodos de hipervisor.

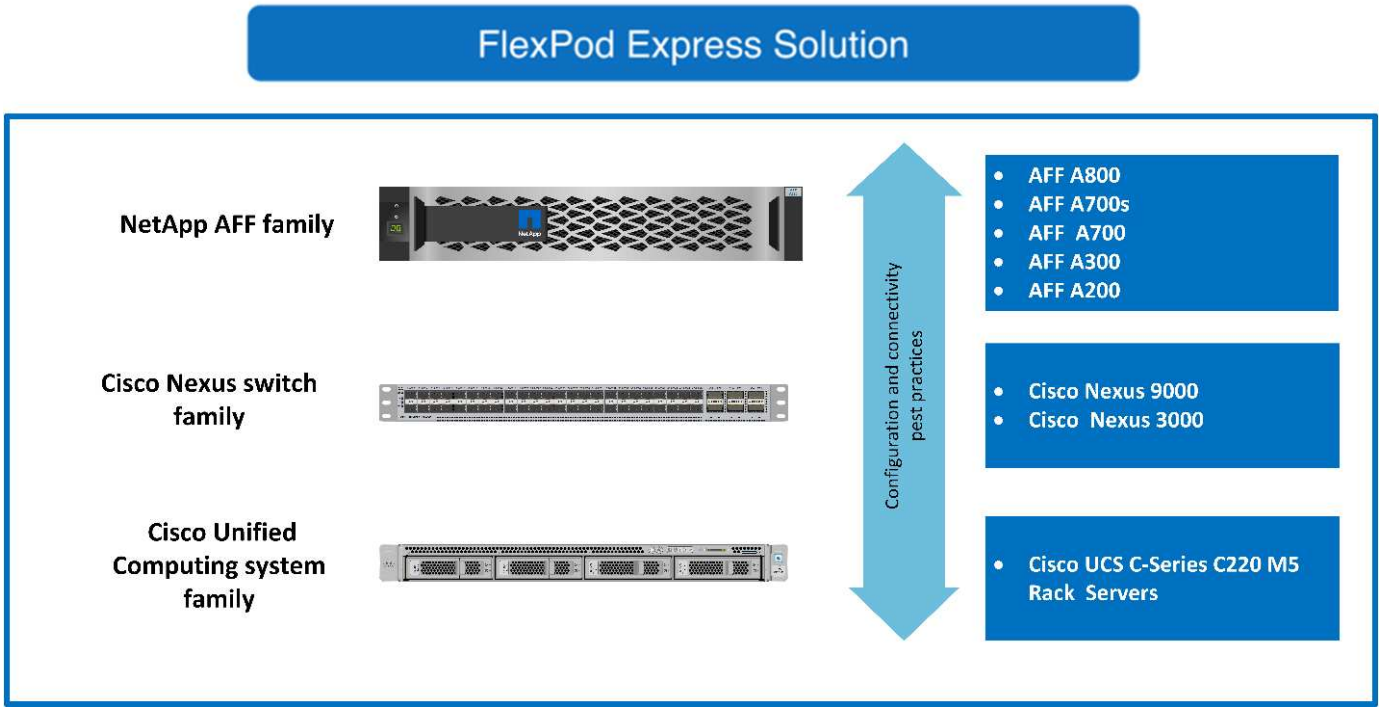
Aunque este documento está validado para AFF A220, esta solución también admite FAS2700.

"Siguiente: Descripción general de la solución."

Descripción general de la solución

FlexPod Express está diseñado para ejecutar cargas de trabajo de virtualización mixtas. Está pensado para oficinas remotas, sucursales y para pequeñas y medianas empresas. También es perfecto para empresas grandes que deseen implementar una solución dedicada para un propósito. Esta nueva solución para FlexPod Express añade nuevas tecnologías como ONTAP 9.4, AFF A220 de NetApp y VMware vSphere 6.7.

La siguiente figura muestra los componentes de hardware incluidos en la solución FlexPod Express.

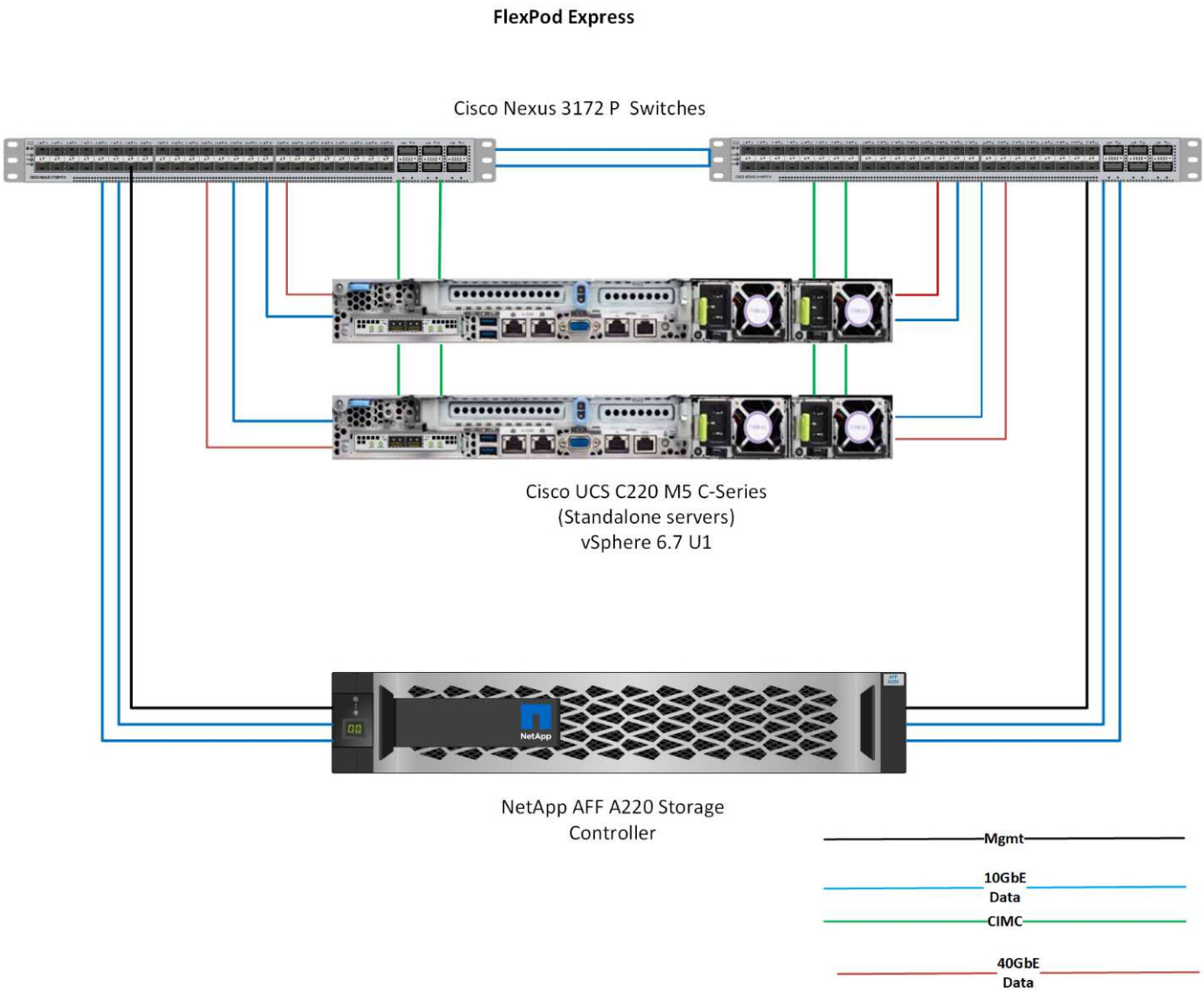


Público objetivo

Este documento está dirigido a los clientes que desean aprovechar una infraestructura creada para proporcionar eficiencia TECNOLÓGICA y permitir la innovación EN TECNOLOGÍA. El público de este documento incluye, sin limitarse a ellos, ingenieros de ventas, consultores de campo, personal de servicios profesionales, gestores DE TECNOLOGÍA, ingenieros de partners y clientes.

Tecnología de soluciones

Esta solución aprovecha las últimas tecnologías de NetApp, Cisco y VMware. Esta solución incluye el nuevo sistema AFF A220 de NetApp, que ejecuta el software ONTAP 9.4, switches Cisco Nexus 3172P duales y servidores de rack Cisco UCS C220 M5 que ejecutan VMware vSphere 6.7. Esta solución validada usa tecnología Ethernet de 10 GB (10GbE). En la siguiente figura se muestra una descripción general. También se ofrece orientación sobre cómo escalar agregando dos nodos de hipervisor a la vez para que la arquitectura FlexPod Express pueda adaptarse a las cambiantes necesidades empresariales de una organización.



40 GbE no está validado, pero es una infraestructura compatible.

"Siguiente: Requisitos tecnológicos."

Requisitos tecnológicos

FlexPod Express requiere una combinación de componentes de hardware y software que depende de la velocidad del hipervisor y de la red seleccionados. Además, FlexPod Express puede establecer los componentes de hardware necesarios para añadir nodos de hipervisor en unidades de dos.

Requisitos de hardware

Independientemente del hipervisor elegido, todas las configuraciones exprés de FlexPod utilizan el mismo hardware. Por lo tanto, aunque cambien los requisitos del negocio, cualquiera de los hipervisores puede ejecutarse en el mismo hardware de FlexPod Express.

La siguiente tabla enumera los componentes de hardware necesarios para todas las configuraciones exprés

de FlexPod e implementar la solución. Los componentes de hardware que se usan en cualquier implementación particular de la solución pueden variar en función de las necesidades del cliente.

Hardware subyacente	Cantidad
Clúster de dos nodos AFF A220	1
Servidor Cisco UCS C220 M5	2
Switch Cisco Nexus 3172P	2
Tarjeta de interfaz virtual (VIC) Cisco UCS 1387 para el servidor en rack Cisco UCS C220 M5	2
Adaptador Cisco CVR-QSFP-SFP10G	4

Requisitos de software

En las siguientes tablas, se enumeran los componentes de software necesarios para implementar las arquitecturas de la solución FlexPod Express.

La siguiente tabla enumera los requisitos de software para la implementación básica de FlexPod Express.

De NetApp	Versión	Detalles
Controladora de gestión integrada de Cisco (CIMC)	3.1.3	Para servidores en rack C220 M5
Cisco NX-OS	nxos.7.0.3.I7.5.bin	Para switches Cisco Nexus 3172P
ONTAP de NetApp	9.4	Para controladoras AFF A220

En la siguiente tabla se muestra el software necesario para todas las implementaciones de VMware vSphere en FlexPod Express.

De NetApp	Versión
Dispositivo VMware vCenter Server	6.7
VMware vSphere ESXi	6.7
Complemento VAAI de NetApp para ESXi	1.1.2

"Siguiente: Opciones de diseño."

Opciones de diseño

Se han elegido las siguientes tecnologías durante el proceso de creación de este diseño. Cada tecnología cumple un propósito específico en la solución de infraestructura Express de FlexPod.

Serie AFF A220 de NetApp con ONTAP 9.4

Esta solución aprovecha dos de los productos más recientes de NetApp: El software AFF A220 y ONTAP 9.4 de NetApp.

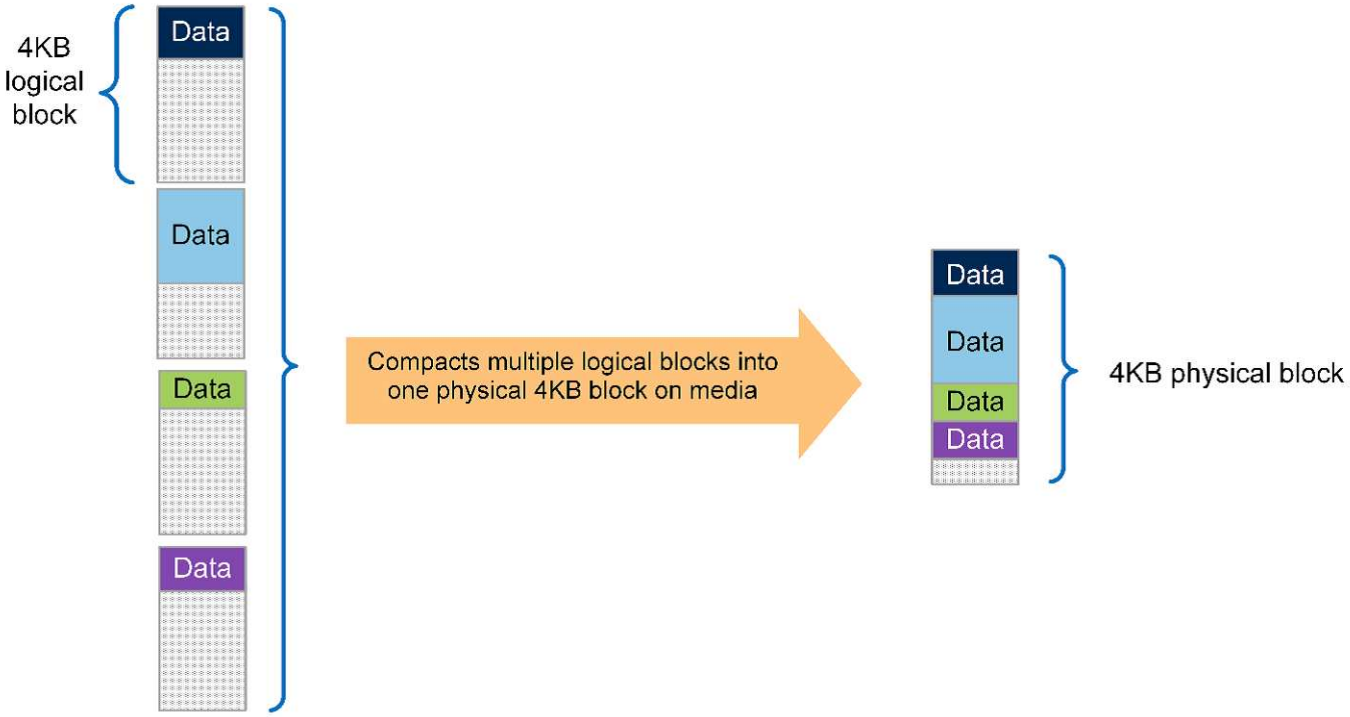
Sistema AFF A220

Si desea obtener más información sobre el sistema de hardware AFF A220, consulte "Página de inicio De AFF a-Series".

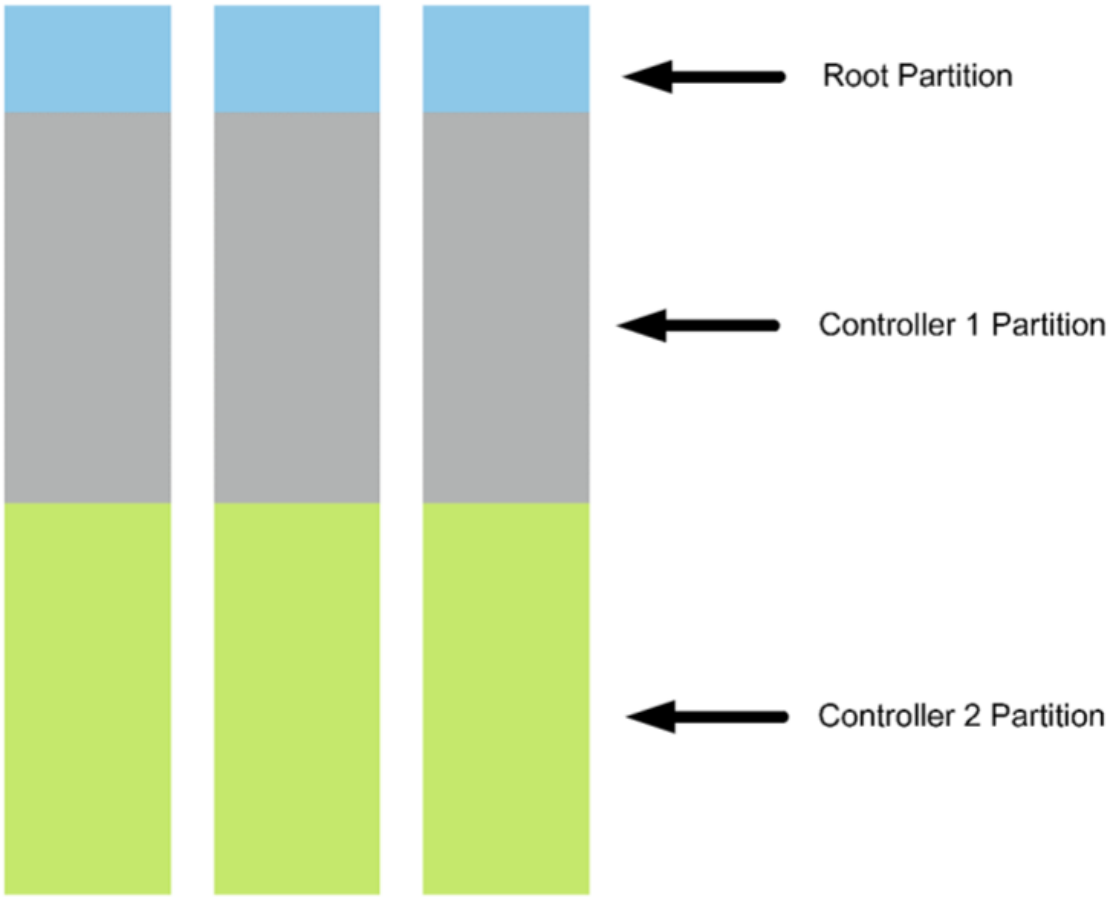
Software ONTAP 9.4

Los sistemas AFF A220 de NetApp utilizan el nuevo software ONTAP 9.4. ONTAP 9.4 es el software de gestión de datos empresariales líder del sector. Combina nuevos niveles de simplicidad y flexibilidad con potentes funcionalidades de gestión de datos, eficiencias de almacenamiento e integración del cloud líder.

ONTAP 9.4 cuenta con varias funciones que resultan adecuadas para la solución FlexPod Express. Lo más importante es el compromiso de NetApp con la eficiencia del almacenamiento, que puede ser una de las funciones más importantes para implementaciones pequeñas. Las características distintivas de la eficiencia del almacenamiento de NetApp, como la deduplicación, la compresión y el thin provisioning, están disponibles en ONTAP 9.4, además de compactación. Como el sistema WAFL de NetApp siempre escribe bloques de 4 KB, la compactación combina varios bloques en un bloque de 4 KB cuando los bloques no utilizan el espacio asignado de 4 KB. La siguiente figura ilustra este proceso.



Además, el sistema AFF A220 puede aprovechar la partición de datos raíz. Esta partición permite dividir el agregado raíz y dos agregados de datos en los discos del sistema. Por lo tanto, ambas controladoras en un clúster de AFF A220 de dos nodos pueden aprovechar el rendimiento de todos los discos del agregado. Consulte la figura siguiente.



Estas son solo algunas de sus funciones clave que complementan la solución FlexPod Express. Para obtener más información sobre las características y funciones adicionales de ONTAP 9.4, consulte la "Especificaciones técnicas del software de gestión de datos ONTAP 9". Consulte también NetApp "Centro de documentación de ONTAP 9" , que se ha actualizado para incluir ONTAP 9.4.

Serie Nexus 3000 de Cisco

El Cisco Nexus 3172P es un switch sólido y rentable que ofrece conmutación de 1/10/40/100Gbps. El switch Cisco Nexus 3172PQ, parte de la familia Unified Fabric, es un switch compacto de 1 unidad de rack (1RU) para las puestas en marcha de centros de datos en la parte superior del rack. (Ver la figura siguiente). Ofrece hasta setenta puertos de 1/10 GbE en 1RU o cuarenta y ocho puertos de 1/10 GbE más seis puertos de 40 GbE en 1RU. Además, para obtener la máxima flexibilidad de la capa física, también admite 1/10/40 Gbps.

Dado que todos los distintos modelos de la serie Cisco Nexus ejecutan el mismo sistema operativo subyacente, NX-OS, son compatibles con múltiples modelos Cisco Nexus en las soluciones FlexPod Express y FlexPod Datacenter.

Las especificaciones de rendimiento incluyen:

- Rendimiento del tráfico de velocidad de línea (ambas capas 2 y 3) en todos los puertos
- Unidades de transmisión máxima configurables (MTU) de hasta 9216 bytes (tramas gigantes)



Para obtener más información sobre los switches Cisco Nexus 3172, consulte "Hoja de datos de los conmutadores Cisco Nexus 3172PQ, 3172TQ, 3172TQ-32T, 3172PQ-XL y 3172TQ-XL".

Cisco UCS C-Series

Se eligió el servidor en rack Cisco UCS C-Series para FlexPod Express porque sus numerosas opciones de configuración permiten adaptarse a requisitos específicos en una puesta en marcha de FlexPod Express.

Los servidores de montaje en rack Cisco UCS C-Series ofrecen informática unificada en un factor de forma estándar del sector para reducir el TCO y aumentar la agilidad.

Los servidores de montaje en rack Cisco UCS C-Series ofrecen las siguientes ventajas:

- Un punto de entrada independiente del factor de forma en Cisco UCS
- Puesta en marcha de aplicaciones simplificada y rápida
- Ampliación de las innovaciones y ventajas de la informática unificada a los servidores en rack
- Mayor elección para el cliente gracias a sus ventajas únicas en un paquete de rack conocido



El servidor de montaje en rack Cisco UCS C220 M5 (en la figura anterior) se encuentra entre la infraestructura empresarial para uso general más versátil y los servidores de aplicaciones del sector. Se trata de un servidor en rack de dos sockets de alta densidad que ofrece un rendimiento y una eficiencia líderes en el sector para una amplia gama de cargas de trabajo, incluidas aplicaciones de virtualización, colaboración y con configuración básica. Los servidores en rack Cisco UCS serie C se pueden implementar como servidores independientes o como parte de Cisco UCS para aprovechar las innovaciones informáticas unificadas basadas en estándares de Cisco que ayudan a reducir el coste total de propiedad de los clientes y a aumentar la agilidad empresarial.

Para obtener más información sobre los servidores C220 M5, consulte "Hoja de datos del servidor en rack Cisco UCS C220 M5".

Opciones de conectividad para los servidores en rack C220 M5

Las opciones de conectividad para los servidores C220 M5 rack son las siguientes:

- **Cisco UCS VIC 1387**

  El Cisco UCS VIC 1387 (en la siguiente figura) ofrece dos puertos mejorados QSFP+ 40 GbE y FC sobre Ethernet (FCoE) en un factor de forma modular-LAN en la placa base (mLOM). La ranura mLOM se puede

utilizar para instalar un Cisco VIC sin consumir una ranura Peripheral Component Interconnect Express (PCIe), lo que proporciona una mayor capacidad de ampliación de E/S.



Para obtener más información acerca del adaptador Cisco UCS VIC 1387, consulte "Tarjeta de interfaz virtual 1387 de Cisco UCS" hoja de datos.

- **ADAPTADOR CVR-QSFP-SFP10G**

  El módulo QSA de Cisco convierte un puerto QSFP en un puerto SFP o SFP+. Con este adaptador, los clientes tienen la flexibilidad de usar cualquier módulo o cable SFP+ o SFP para conectarse a un puerto de menor velocidad en el otro extremo de la red. Esta flexibilidad permite una transición rentable a 40 GbE al optimizar el uso de plataformas QSFP de 40 GbE de alta densidad. Este adaptador es compatible con todos los cables ópticos SFP+ y con diversos módulos SFP de 1 GbE. Dado que este proyecto se ha validado utilizando conectividad 10 GbE y puesto que VIC 1387 utilizado es 40 GbE, se utiliza para la conversión el adaptador CVR-QSFP-SFP10G (en la siguiente figura).



VMware vSphere 6.7

VMware vSphere 6.7 es una opción de hipervisor para utilizar con FlexPod Express. VMware vSphere permite a las organizaciones reducir su huella de potencia y refrigeración a la vez que confirman que la capacidad de computación adquirida se ha aprovechado al máximo. Además, VMware vSphere permite la protección contra fallos de hardware (alta disponibilidad de VMware o ha de VMware) y el equilibrio de carga de recursos

informáticos en un clúster de hosts vSphere (Distributed Resource Scheduler de VMware o DRS de VMware).

Debido a que solo reinicia el kernel, VMware vSphere 6.7 permite a los clientes “arrancar rápidamente” donde cargan vSphere ESXi sin reiniciar el hardware. Esta función sólo está disponible con plataformas y controladores que se encuentran en la lista blanca de Quick Boot. VSphere 6.7 amplía las funcionalidades de vSphere Client, que puede realizar aproximadamente un 90% de lo que puede hacer vSphere Web Client.

En vSphere 6.7, VMware ha ampliado esta funcionalidad para permitir a los clientes establecer Enhanced vMotion Compatibility (EVC) por máquina virtual (VM) en lugar de hacerlo por host. En vSphere 6.7, VMware también ha expuesto las API que pueden utilizarse para crear clones instantáneos.

A continuación se muestran algunas de las funciones de vSphere 6.7 U1:

- VSphere Client basado en web HTML5 con todas las funciones
- VMotion para máquinas virtuales GRID vGPU de NVIDIA. Compatibilidad con Intel FPGA.
- VCenter Server reúnen la herramienta para pasar de PSC externo a PCS interno.
- Mejoras para VSAN (actualizaciones de HCI).
- Biblioteca de contenido mejorada.

Para obtener más información sobre vSphere 6.7 U1, consulte "Novedades de vCenter Server 6.7 Update 1". A pesar de que esta solución se validó con vSphere 6.7, es compatible con cualquier versión de vSphere que esté cualificada con los demás componentes de la herramienta de matriz de interoperabilidad de NetApp. NetApp recomienda implementar vSphere 6.7U1 para sus correcciones y funciones mejoradas.

Arquitectura de arranque

A continuación, se muestran las opciones compatibles de la arquitectura de arranque exprés de FlexPod:

- LUN SAN iSCSI
- Tarjeta SD Cisco FlexFlash
- Disco local

Dado que FlexPod Datacenter se arranca desde LUN de iSCSI, la capacidad de gestión de la solución se mejora mediante el uso del arranque iSCSI para FlexPod Express.

"Siguiente: Verificación de la solución."

Verificación de la solución

Cisco y NetApp diseñaron y crearon FlexPod Express para servir como una plataforma de infraestructura de primer nivel para sus clientes. Al ser diseñado con componentes líderes en el sector, los clientes pueden confiar en FlexPod Express como base de su infraestructura. De acuerdo con los principios fundamentales de la cartera de FlexPod, la arquitectura de FlexPod Express ha sido probada a conciencia por arquitectos e ingenieros de centros de datos de Cisco y NetApp. Desde la redundancia y la disponibilidad a cada funcionalidad individual, se valida toda la arquitectura FlexPod Express para infundir confianza en los clientes y fomentar la confianza en el proceso de diseño.

VMware vSphere 6.7 se verificó en los componentes de la infraestructura de FlexPod Express. Esta validación

incluye opciones de conectividad de enlace ascendente 10 GbE para el hipervisor.

"Siguiente: Conclusión."

Conclusión

FlexPod Express ofrece una solución sencilla y efectiva, ya que proporciona un diseño validado que utiliza componentes líderes en el sector. Al escalar y proporcionar opciones para la plataforma de hipervisor, FlexPod Express se puede adaptar a las necesidades específicas del negocio. FlexPod Express se ha diseñado teniendo en cuenta a las pequeñas y medianas empresas, las oficinas remotas y sucursales, y otras empresas que requieren soluciones dedicadas.

"Siguiente: Dónde encontrar información adicional."

Dónde encontrar información adicional

Si quiere obtener más información sobre la información descrita en este documento, consulte los siguientes documentos y sitios web:

- Documentación de NetApp

  "https://docs.netapp.com"

- Guía de puesta en marcha de FlexPod Express con VMware vSphere 6.7 y AFF A220 de NetApp

  "https://www.netapp.com/us/media/nva-1123-deploy.pdf"

Guía de puesta en marcha de FlexPod Express con Cisco UCS C-Series y AFF A220 Series

NVA-1123-PUESTA en MARCHA: FlexPod Express con VMware vSphere 6.7 y la guía de puesta en marcha de AFF A220 de NetApp

Savita Kumari, NetApp

En colaboración con: 

Las tendencias en el sector señalan una gran transformación de los centros de datos hacia una infraestructura compartida y cloud computing. Además, las organizaciones buscan una solución sencilla y eficaz para oficinas remotas y sucursales que aprovechen la tecnología con la que ya están familiarizados en su centro de datos.

FlexPod Express es una arquitectura de centro de datos prediseñada con las mejores prácticas que se basa en el Cisco Unified Computing System (Cisco UCS), la familia de switches Cisco Nexus y las tecnologías de almacenamiento de NetApp. Los componentes de un sistema FlexPod Express se asemejan a los del centro

de datos FlexPod, lo que permite sinergias de gestión en todo el entorno de infraestructura DE TI a una escala menor. FlexPod Datacenter y FlexPod Express son plataformas óptimas para virtualización y para sistemas operativos con configuración básica y cargas de trabajo empresariales.

El centro de datos de FlexPod y FlexPod Express proporcionan una configuración básica y cuentan con la flexibilidad necesaria para ajustar su tamaño y optimizarse con el objetivo de acomodar distintos casos de uso y requisitos. Los clientes existentes de FlexPod Datacenter pueden gestionar su sistema FlexPod Express con las herramientas a las que están acostumbrados. Los nuevos clientes de FlexPod Express pueden adaptarse fácilmente a la gestión del centro de datos FlexPod cuando crezca su entorno.

FlexPod Express es una base de infraestructura óptima para oficinas remotas y sucursales y para pequeñas y medianas empresas. También es una solución óptima para los clientes que desean proporcionar infraestructura para cargas de trabajo dedicadas.

FlexPod Express proporciona una infraestructura fácil de gestionar que es adecuada para casi cualquier carga de trabajo.

Descripción general de la solución

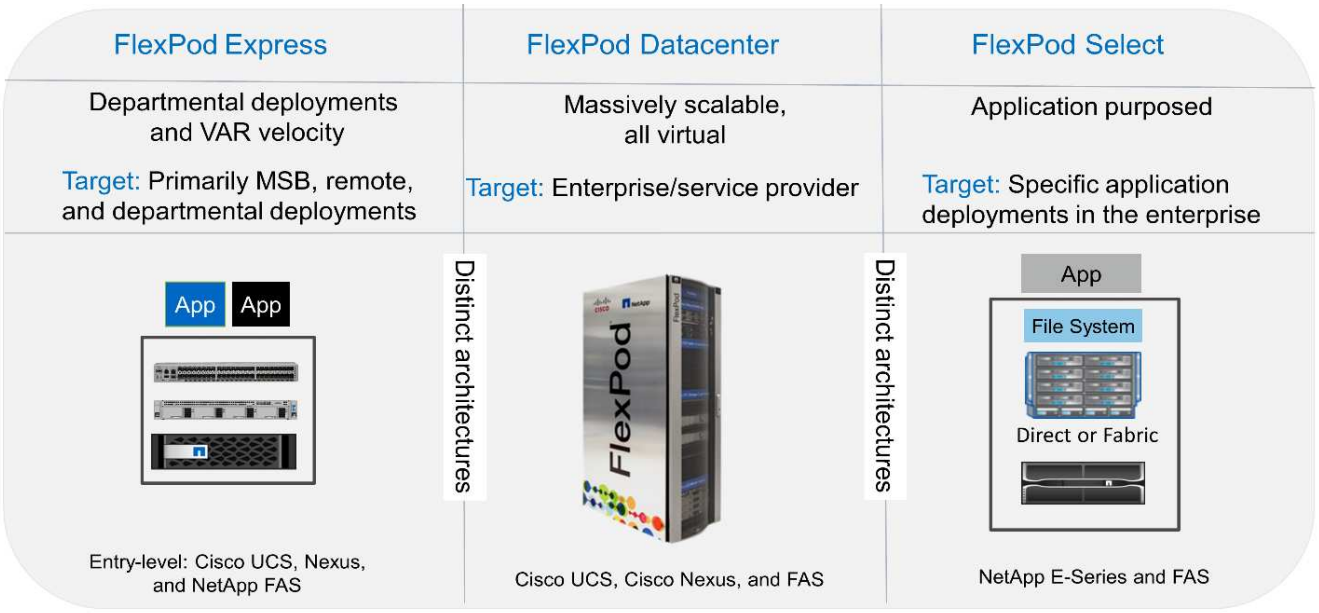
Esta solución FlexPod Express forma parte del programa de infraestructura convergente de FlexPod.

Programa de infraestructura convergente FlexPod

Las arquitecturas de referencia FlexPod se proporcionan como diseños validados por Cisco (CVD) o como arquitecturas verificadas por NetApp (NVA). Se permiten las desviaciones basadas en los requisitos de los clientes de un CVD o NVA determinado si estas variaciones no crean una configuración incompatible.

Como se muestra en la siguiente figura, el programa FlexPod incluye tres soluciones: FlexPod Express, FlexPod Datacenter y FlexPod Select:

- **FlexPod Express.** ofrece a los clientes una solución de gama básica con tecnologías de Cisco y NetApp.
- **FlexPod Datacenter.** proporciona una base multiuso óptima para diversas cargas de trabajo y aplicaciones.
- **FlexPod Select.** incorpora los mejores aspectos del centro de datos FlexPod y adapta la infraestructura a una aplicación determinada.



Programa Arquitectura validada por NetApp

El programa Arquitectura verificada de NetApp ofrece a los clientes una arquitectura verificada para soluciones NetApp. Una arquitectura verificada de NetApp ofrece una arquitectura de solución de NetApp con las siguientes cualidades:

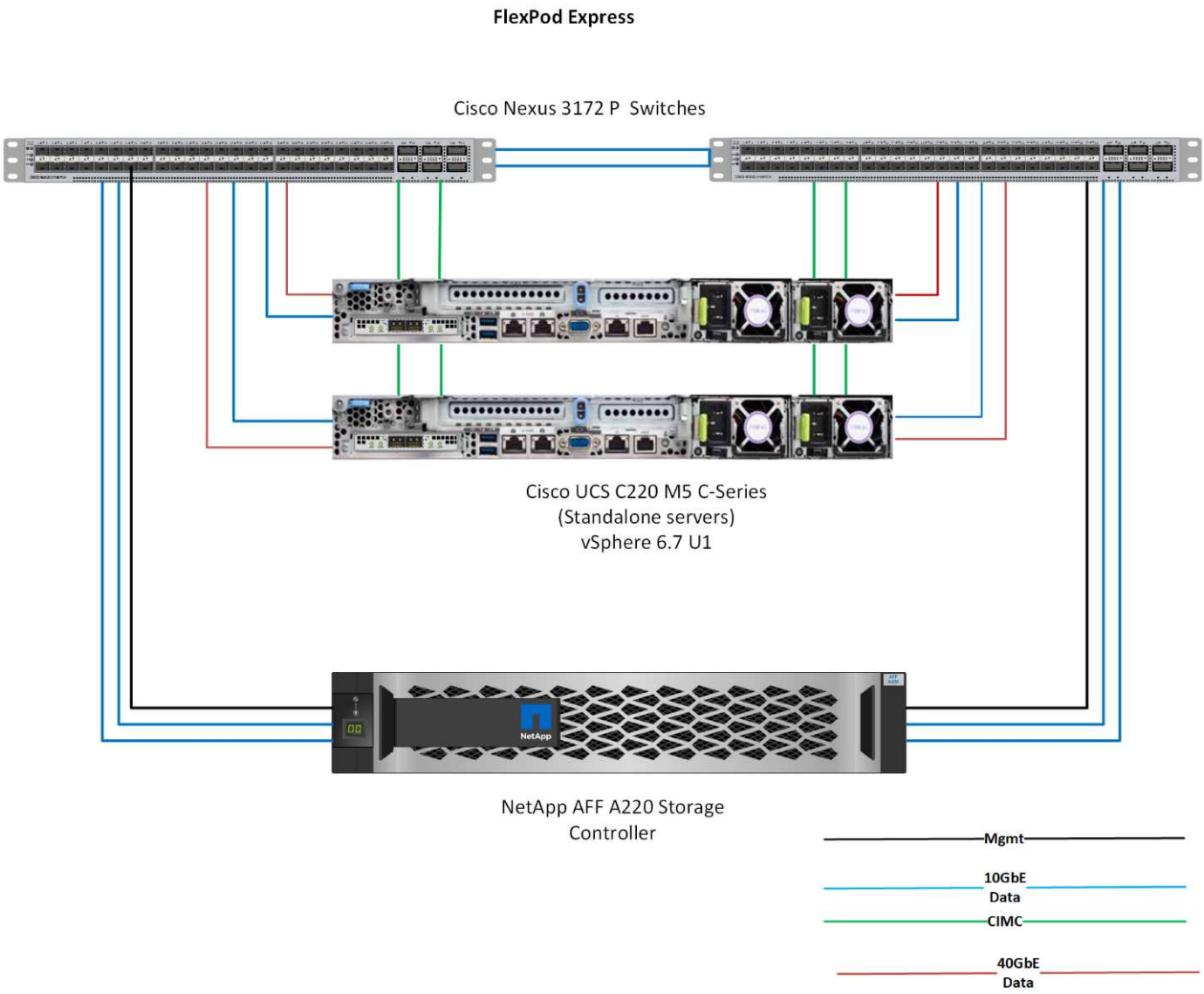
- Ha sido probada a conciencia
- Tiene naturaleza prescriptiva
- Minimiza los riesgos de implementación
- Reduce el plazo de comercialización

Esta guía detalla el diseño de FlexPod Express con VMware vSphere. Además, este diseño usa el nuevo sistema AFF A220, que ejecuta ONTAP 9.4 de NetApp, los servidores Cisco Nexus 3172P y Cisco UCS C-Series C220 M5 como nodos de hipervisor.

Tecnología de soluciones

Esta solución aprovecha las últimas tecnologías de NetApp, Cisco y VMware. Esta solución incluye el nuevo sistema AFF A220 de NetApp que ejecuta ONTAP 9.4, los conmutadores Cisco Nexus 3172P duales y los servidores de montaje en rack Cisco UCS C220 M5 que ejecutan VMware vSphere 6.7. Esta solución validada usa tecnología 10 GbE. También se ofrece orientación sobre cómo escalar la capacidad de computación mediante la adición de dos nodos de hipervisor a la vez para que la arquitectura FlexPod Express pueda adaptarse a las cambiantes necesidades empresariales de una organización.

La figura siguiente muestra FlexPod Express con arquitectura 10 GbE de VMware vSphere.



Esta validación utiliza conectividad de 10 GbE y un Cisco UCS VIC 1387, que es 40 GbE. Para lograr conectividad de 10 GbE, se utiliza el adaptador CVR-QSFP-SFP10G.

Resumen de casos de uso

La solución FlexPod Express puede aplicarse a varios casos prácticos, incluidos los siguientes:

- Oficinas remotas o sucursales
- Pequeñas y medianas empresas
- Entornos que requieren una solución dedicada y rentable

FlexPod Express está indicado para cargas de trabajo virtualizadas y mixtas.

A pesar de que esta solución se validó con vSphere 6.7, es compatible con cualquier versión de vSphere que esté cualificada con los demás componentes de la herramienta de matriz de interoperabilidad de NetApp. NetApp recomienda implementar vSphere 6.7U1 para sus correcciones y funciones mejoradas.

A continuación se muestran algunas de las características de vSphere 6.7 U1:

- Cliente vSphere basado en web HTML5 con todas las funciones
- VMotion para máquinas virtuales GRID vGPU de NVIDIA. Compatibilidad con Intel FPGA
- VCenter Server reúnen la herramienta para pasar de PSC externo a PCS interno
- Mejoras para VSAN (actualizaciones de HCI)
- Biblioteca de contenido mejorada

Para obtener más información sobre vSphere 6.7 U1, consulte "Novedades de vCenter Server 6.7 Update 1".

Requisitos tecnológicos

Un sistema FlexPod Express requiere una combinación de componentes de hardware y software. FlexPod Express también describe los componentes de hardware necesarios para añadir nodos de hipervisor al sistema en unidades de dos.

Requisitos de hardware

Independientemente del hipervisor elegido, todas las configuraciones exprés de FlexPod utilizan el mismo hardware. Por lo tanto, aunque cambien los requisitos del negocio, cualquiera de los hipervisores puede ejecutarse en el mismo hardware de FlexPod Express.

En la siguiente tabla se enumeran los componentes de hardware necesarios para todas las configuraciones exprés de FlexPod.

Hardware subyacente	Cantidad
Par de alta disponibilidad AFF A220	1
Servidor Cisco C220 M5	2
Switch Cisco Nexus 3172P	2
Tarjeta de interfaz virtual (VIC) Cisco UCS 1387 para el servidor C220 M5	2
ADAPTADOR CVR-QSFP-SFP10G	4

En la siguiente tabla se enumera el hardware necesario además de la configuración base para la implementación de 10 GbE.

Hardware subyacente	Cantidad
Servidor Cisco UCS C220 M5	2
Cisco VIC 1387	2
ADAPTADOR CVR-QSFP-SFP10G	4

Requisitos de software

En la siguiente tabla se enumeran los componentes de software necesarios para implementar las arquitecturas de las soluciones FlexPod Express.

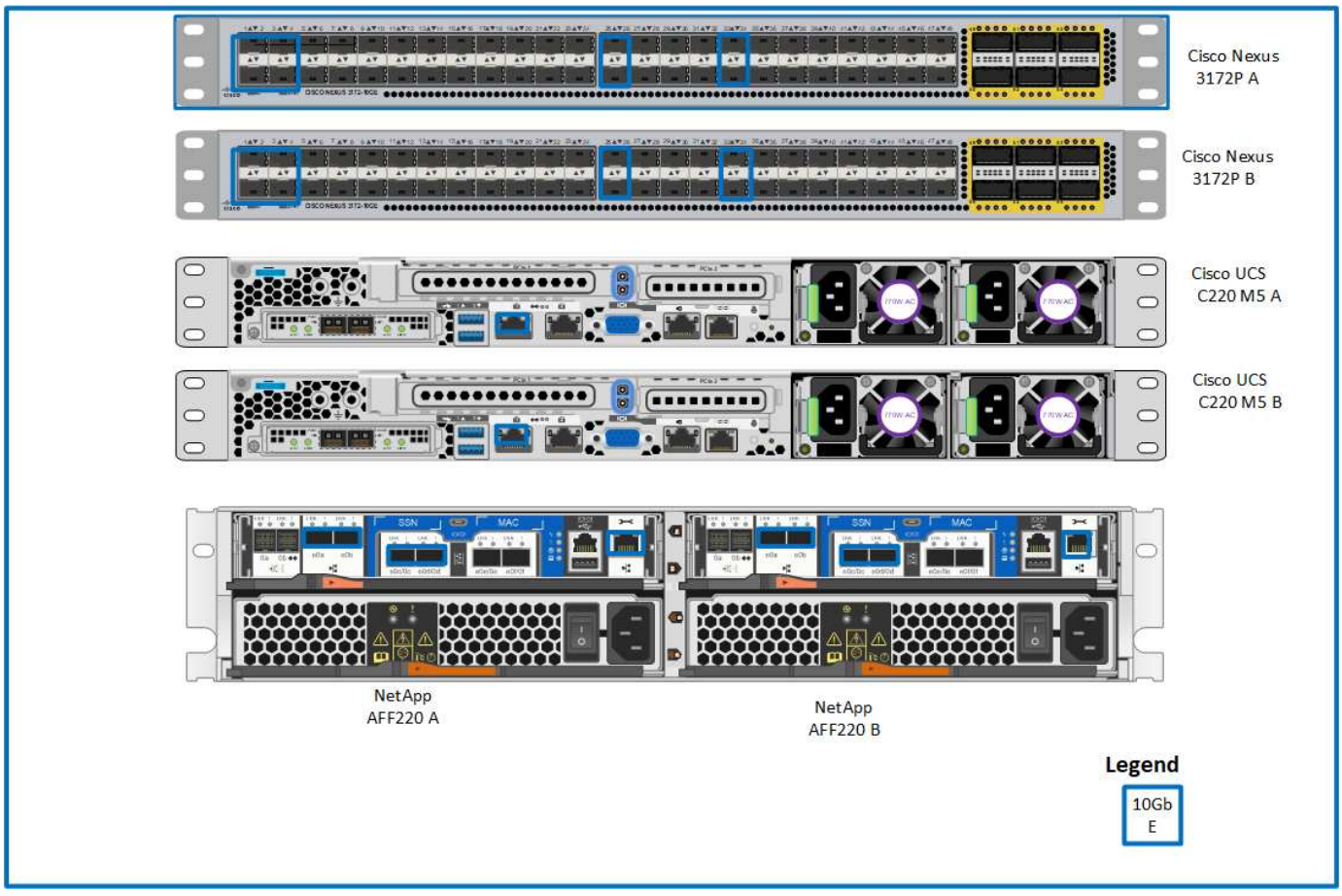
De NetApp	Versión	Detalles
Controladora de gestión integrada de Cisco (CIMC)	3.1 (3g)	Para los servidores en rack Cisco UCS C220 M5
Controlador nenic de Cisco	1.0.25.0	Para tarjetas de interfaz VIC 1387
Cisco NX-OS	nxos.7.0.3.I7.5.bin	Para switches Cisco Nexus 3172P
ONTAP de NetApp	9.4	Para controladoras AFF A220

En la siguiente tabla se enumera el software requerido para todas las implementaciones de VMware vSphere en FlexPod Express.

De NetApp	Versión
Dispositivo VMware vCenter Server	6.7
Hipervisor ESXi de VMware vSphere	6.7
Complemento VAAI de NetApp para ESXi	1.1.2

Información sobre el cableado exprés de FlexPod

La siguiente figura muestra el cableado de validación de referencia.



En la siguiente tabla se muestra información sobre el cableado del switch Cisco Nexus 3172P A.

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Switch Cisco Nexus 3172P A	Eth1/1	Controladora De almacenamiento A AFF A220 de NetApp	e0c
	Eth1/2	Controladora de almacenamiento B de AFF A220 de NetApp	e0c
	Eth1/3	El servidor A independiente Cisco UCS C220 C-Series	MLOM1 con adaptador CVR-QSFP-SFP10G
	Eth1/4	Servidor B independiente Cisco UCS C220 C-Series	MLOM1 con adaptador CVR-QSFP-SFP10G
	Eth1/25	Switch Cisco Nexus 3172P B	Eth1/25
	Eth1/26	Switch Cisco Nexus 3172P B	Eth1/26
	Eth1/33	Controladora De almacenamiento A AFF A220 de NetApp	E0M
	Eth1/34	El servidor A independiente Cisco UCS C220 C-Series	CIMC

En la siguiente tabla se muestra información sobre el cableado del switch Cisco Nexus 3172P B.

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Switch Cisco Nexus 3172P B	Eth1/1	Controladora De almacenamiento A AFF A220 de NetApp	e0d
	Eth1/2	Controladora de almacenamiento B de AFF A220 de NetApp	e0d
	Eth1/3	El servidor A independiente Cisco UCS C220 C-Series	MLOM2 con adaptador CVR-QSFP-SFP10G
	Eth1/4	Servidor B independiente Cisco UCS C220 C-Series	MLOM2 con adaptador CVR-QSFP-SFP10G
	Eth1/25	Switch Cisco Nexus 3172P A	Eth1/25
	Eth1/26	Switch Cisco Nexus 3172P A	Eth1/26
	Eth1/33	Controladora de almacenamiento B de AFF A220 de NetApp	E0M

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
	Eth1/34	Servidor B independiente Cisco UCS C220 C-Series	CIMC

La siguiente tabla muestra la información de cableado de la controladora de almacenamiento AFF A220 A. de NetApp

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Controladora De almacenamiento A AFF A220 de NetApp	e0a	Controladora de almacenamiento B de AFF A220 de NetApp	e0a
	e0b	Controladora de almacenamiento B de AFF A220 de NetApp	e0b
	e0c	Switch Cisco Nexus 3172P A	Eth1/1
	e0d	Switch Cisco Nexus 3172P B	Eth1/1
	E0M	Switch Cisco Nexus 3172P A	Eth1/33

La siguiente tabla muestra información de cableado para la controladora de almacenamiento B de AFF A220 de NetApp

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Controladora de almacenamiento B de AFF A220 de NetApp	e0a	Controladora De almacenamiento A AFF A220 de NetApp	e0a
	e0b	Controladora De almacenamiento A AFF A220 de NetApp	e0b
	e0c	Switch Cisco Nexus 3172P A	Eth1/2
	e0d	Switch Cisco Nexus 3172P B	Eth1/2
	E0M	Switch Cisco Nexus 3172P B	Eth1/33

Procedimientos de implantación

Este documento proporciona detalles para configurar un sistema FlexPod Express completamente redundante y de alta disponibilidad. Para reflejar esta redundancia, los componentes que se configuran en cada paso se denominan componente A o componente B. Por ejemplo, la controladora A y la controladora B identifican las dos controladoras de almacenamiento de NetApp que se aprovisionan en este documento. El

switch A y el switch B identifican un par de switches Cisco Nexus.

Además, en este documento se describen los pasos para aprovisionar varios hosts de Cisco UCS, que se identifican secuencialmente como servidor A, servidor B, etc.

Para indicar que debe incluir la información pertinente a su entorno en un paso, `<<text>>` aparece como parte de la estructura de comandos. Consulte el siguiente ejemplo de `vlan create` comando:

```
Controller01>vlan create vif0 <<mgmt_vlan_id>>
```

Este documento permite configurar completamente el entorno de FlexPod Express. En este proceso, varios pasos requieren que inserte convenciones de nomenclatura específicas del cliente, direcciones IP y esquemas de red de área local virtual (VLAN). En la siguiente tabla se describen las VLAN necesarias para la implementación, tal y como se explica en esta guía. Esta tabla se puede completar en función de las variables específicas del sitio y se puede utilizar para implementar los pasos de configuración del documento.

Si se utilizan VLAN de gestión fuera de banda y en banda independientes, debe crear una ruta de capa- 3 entre ellas. Para esta validación, se utilizó una VLAN de gestión común.

Un nombre	Propósito de VLAN	ID utilizado en la validación de este documento
VLAN de gestión	VLAN para interfaces de gestión	3437
VLAN nativa	VLAN a la que se asignan tramas no etiquetadas	2
VLAN NFS	VLAN para tráfico NFS	3438
VLAN de VMware vMotion	VLAN designada para mover máquinas virtuales de un host físico a otro	3441
VLAN de tráfico de equipos virtuales	VLAN para tráfico de aplicaciones de equipos virtuales	3442
ISCSI-A-VLAN	VLAN para tráfico iSCSI en la estructura A	3439
ISCSI-B-VLAN	VLAN para tráfico iSCSI en la estructura B	3440

Los números VLAN son necesarios en toda la configuración de FlexPod Express. Las VLAN se denominan `<<var_xxxx_vlan>>`, donde `xxxx` Es la finalidad de la VLAN (como iSCSI-A).

La siguiente tabla enumera las máquinas virtuales de VMware creadas.

Descripción de la máquina virtual	Nombre de host
Servidor VMware vCenter	

Procedimiento de puesta en marcha de Cisco Nexus 3172P

En la siguiente sección se detalla la configuración del switch Cisco Nexus 3172P

utilizada en un entorno de FlexPod Express.

Configuración inicial del switch Cisco Nexus 3172P

Los siguientes procedimientos describen cómo configurar los switches Cisco Nexus para su uso en un entorno FlexPod Express básico.

> Este procedimiento supone que está utilizando un Cisco Nexus 3172P con la versión 7.0(3)I7(5) del software NX-OS.

1. Tras el arranque y la conexión iniciales al puerto de la consola del switch, se inicia automáticamente la configuración de Cisco NX-OS. Esta configuración inicial trata los valores básicos, como el nombre del switch, la configuración de la interfaz mgmt0 y la configuración de Secure Shell (SSH).
2. La red de gestión del sistema FlexPod Express se puede configurar de varias maneras. Las interfaces mgmt0 de los conmutadores 3172P se pueden conectar a una red de gestión existente, o las interfaces mgmt0 de los conmutadores 3172P se pueden conectar en una configuración posterior. Sin embargo, este enlace no se puede utilizar para el acceso de gestión externo, como tráfico SSH.

   En esta guía de implementación, los switches FlexPod Express Cisco Nexus 3172P están conectados a una red de gestión existente.
3. Para configurar los switches Cisco Nexus 3172P, encienda el switch y siga las instrucciones en pantalla, como se muestra aquí para la configuración inicial de ambos conmutadores, sustituyendo los valores adecuados para la información específica del conmutador.

```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
  Create another login account (yes/no) [n]: n
  Configure read-only SNMP community string (yes/no) [n]: n
  Configure read-write SNMP community string (yes/no) [n]: n
  Enter the switch name : 3172P-B
  Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
    Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
    Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
  Configure the default gateway? (yes/no) [y]: y
    IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
  Configure advanced IP options? (yes/no) [n]: n
  Enable the telnet service? (yes/no) [n]: n
  Enable the ssh service? (yes/no) [y]: y
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
    Number of rsa key bits <1024-2048> [1024]:  <enter>
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 address : <<var_ntp_ip>>
  Configure default interface layer (L3/L2) [L2]: <enter>
  Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:  <enter>
```

4. A continuación, verá un resumen de la configuración y se le preguntará si desea editarla. Si la configuración es correcta, introduzca `n`.

```
Would you like to edit the configuration? (yes/no) [n]: n
```

5. A continuación, se le preguntará si desea utilizar esta configuración y guardarla. Si es así, introduzca `y`.

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Repita este procedimiento para el switch Cisco Nexus B.

Habilite funciones avanzadas

Determinadas características avanzadas deben estar habilitadas en Cisco NX-OS para proporcionar opciones de configuración adicionales.

> La `interface-vlan` la función sólo es obligatoria si se utiliza el back-to-back `mgmt0` opción descrita en este documento. Esta función permite asignar una dirección IP a la interfaz VLAN (interfaz virtual de switch), que habilita la comunicación de gestión en banda al switch (como a través de SSH).

1. Para habilitar las funciones adecuadas en los switches a y B de Cisco Nexus, escriba el modo de configuración mediante el comando `(config t)` y ejecute los siguientes comandos:

   ```
   feature interface-vlan
   feature lacp
   feature vpc
   ```

   El hash de equilibrio de carga del canal de puerto predeterminado utiliza las direcciones IP de origen y destino para determinar el algoritmo de equilibrio de carga en las interfaces del canal de puerto. Puede lograr una mejor distribución entre los miembros del canal de puerto proporcionando más entradas al algoritmo hash más allá de las direcciones IP de origen y destino. Por el mismo motivo, NetApp recomienda encarecidamente añadir los puertos TCP de origen y destino al algoritmo hash.

2. Desde el modo de configuración (`config t`), introduzca los siguientes comandos para establecer la configuración de equilibrio de carga del canal de puerto global en los conmutadores A y B de Cisco Nexus:

   ```
   port-channel load-balance src-dst ip-l4port
   ```

Realizar la configuración de árbol de expansión global

La plataforma Cisco Nexus utiliza una nueva función de protección llamada garantía de puente. La garantía de puente ayuda a proteger contra un enlace unidireccional u otro error de software con un dispositivo que continúa redirectando el tráfico de datos cuando ya no ejecuta el algoritmo de árbol expansivo. Los puertos se pueden colocar en uno de varios estados, incluyendo la red o el borde, dependiendo de la plataforma.

NetApp recomienda establecer la garantía de puente para que todos los puertos se consideren puertos de red de forma predeterminada. Este ajuste obliga al administrador de red a revisar la configuración de cada puerto. También revela los errores de configuración más comunes, como puertos de borde no identificados o un vecino que no tiene activada la función de garantía de puente. Además, es más seguro tener el bloque de árbol expansivo muchos puertos en lugar de muy pocos, lo que permite que el estado de puerto predeterminado mejore la estabilidad general de la red.

Preste especial atención al estado de árbol de expansión al agregar servidores, almacenamiento y switches ascendentes, especialmente si no admiten la garantía de puente. En estos casos, es posible que deba cambiar el tipo de puerto para que los puertos estén activos.

El protector de unidad de datos de protocolo puente (BPDU) está habilitado de forma predeterminada en puertos periféricos como otra capa de protección. Para evitar bucles en la red, esta característica cierra el puerto si se ven BPDU de otro switch en esta interfaz.

Desde el modo de configuración (`config t`), ejecute los siguientes comandos para configurar las opciones de árbol de expansión predeterminadas, incluidos el tipo de puerto predeterminado y el protector BPDU, en el conmutador A de Cisco Nexus y el conmutador B:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
```

Defina las VLAN

Antes de configurar puertos individuales con VLAN diferentes, se deben definir las VLAN de capa 2 en el switch. También se recomienda nombrar las VLAN para que la solución de problemas sea sencilla en el futuro.

Desde el modo de configuración (`config t`), ejecute los siguientes comandos para definir y describir las VLAN de capa 2 en el switch A y el switch B de Cisco Nexus:

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

Configurar el acceso y las descripciones de los puertos de gestión

Al igual que en la asignación de nombres a las VLAN de capa 2, las descripciones de configuración de todas las interfaces pueden ayudar tanto al aprovisionamiento como a la solución de problemas.

Desde el modo de configuración (`config t`) En cada uno de los conmutadores, introduzca las siguientes descripciones de puerto para la configuración grande de FlexPod Express:

Switch Cisco Nexus a

```
int eth1/1
  description AFF A220-A e0c
int eth1/2
  description AFF A220-B e0c
int eth1/3
  description UCS-Server-A: MLOM port 0
int eth1/4
  description UCS-Server-B: MLOM port 0
int eth1/25
  description vPC peer-link 3172P-B 1/25
int eth1/26
  description vPC peer-link 3172P-B 1/26
int eth1/33
  description AFF A220-A e0M
int eth1/34
  description UCS Server A: CIMC
```

Switch Cisco Nexus B

```
int eth1/1
  description AFF A220-A e0d
int eth1/2
  description AFF A220-B e0d
int eth1/3
  description UCS-Server-A: MLOM port 1
int eth1/4
  description UCS-Server-B: MLOM port 1
int eth1/25
  description vPC peer-link 3172P-A 1/25
int eth1/26
  description vPC peer-link 3172P-A 1/26
int eth1/33
  description AFF A220-B e0M
int eth1/34
  description UCS Server B: CIMC
```

Configurar las interfaces de gestión de almacenamiento y servidores

Las interfaces de gestión para el servidor y el almacenamiento suelen utilizar una sola VLAN. Por lo tanto, configure los puertos de la interfaz de gestión como puertos de acceso. Defina la VLAN de administración para cada switch y cambie el tipo de puerto de árbol expansivo a EDGE.

Desde el modo de configuración (`config t`), introduzca los siguientes comandos para configurar los ajustes del puerto para las interfaces de gestión tanto de los servidores como del almacenamiento:

Switch Cisco Nexus a

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Switch Cisco Nexus B

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Llevar a cabo la configuración global del canal de puertos virtuales

Un canal de puerto virtual (VPC) permite que los enlaces que están conectados físicamente a dos switches de Cisco Nexus diferentes aparezcan como un único canal de puerto a un tercer dispositivo. El tercer dispositivo puede ser un conmutador, un servidor o cualquier otro dispositivo de red. Un VPC puede proporcionar una multivía de nivel 2, que le permite crear redundancia aumentando el ancho de banda, permitiendo múltiples rutas paralelas entre los nodos y tráfico de equilibrio de carga donde haya rutas alternativas.

Un VPC proporciona las siguientes ventajas:

- Permitir que un único dispositivo utilice un canal de puerto a través de dos dispositivos de subida
- Eliminar puertos bloqueados del protocolo de árbol expansivo
- Proporciona una topología sin bucles
- Utilizando todo el ancho de banda disponible de enlace ascendente
- Proporcionar convergencia rápida si el enlace o un dispositivo falla
- Resiliencia a nivel de enlace
- Contribuir a proporcionar una alta disponibilidad

La función VPC requiere alguna configuración inicial entre los dos switches de Cisco Nexus para que funcionen correctamente. Si utiliza la configuración de mgmt0 de fondo, utilice las direcciones definidas en las interfaces y compruebe que se pueden comunicar mediante ping `[switch_A/B_mgmt0_ip_addr]vrf` comando de gestión.

Desde el modo de configuración (`config t`), ejecute los siguientes comandos para configurar la configuración global de VPC para ambos switches:

Switch Cisco Nexus a

```
vpc domain 1
 role priority 10
  peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
  no shut
exit
copy run start
```

Switch Cisco Nexus B

```
vpc domain 1
  peer-switch
  role priority 20
  peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
int eth1/25- 26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
no shut
exit
copy run start
```

Configure los canales del puerto de almacenamiento

Las controladoras de almacenamiento de NetApp permiten una conexión activa-activa a la red mediante el protocolo de control de agregación de enlaces (LACP). El uso de LACP es preferido porque añade negociación y registro entre los switches. Debido a que la red está configurada para VPC, este enfoque permite disponer de conexiones activo-activo del almacenamiento para separar los switches físicos. Cada controladora tiene dos enlaces a cada uno de los switches. Sin embargo, los cuatro vínculos forman parte del mismo VPC y grupo de interfaces (IFGRP).

Desde el modo de configuración (`config t`), ejecute los siguientes comandos en cada uno de los switches para configurar las interfaces individuales y la configuración resultante del canal de puerto para los puertos conectados a la controladora AFF de NetApp.

1. Ejecute los siguientes comandos en el switch A y en el switch B a para configurar los canales de puertos de la controladora De almacenamiento A:

```
int eth1/1
  channel-group 11 mode active
int Po11
  description vPC to Controller-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<mgmt_vlan_id>>,<<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 11
  no shut
```

2. Ejecute los siguientes comandos en el switch A y en el switch B a para configurar los canales de puertos para la controladora de almacenamiento B.

```
int eth1/2
  channel-group 12 mode active
int Po12
  description vPC to Controller-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<mgmt_vlan_id>>,
<<iSCSI_A_vlan_id>>, <<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 12
  no shut
exit
copy run start
```



En esta validación de soluciones se utilizó una MTU de 9000. Sin embargo, en función de los requisitos de la aplicación, puede configurar un valor de MTU adecuado. Es importante establecer el mismo valor de MTU en la solución de FlexPod. Las configuraciones de MTU incorrectas entre componentes provocan la caída de paquetes y de estos paquetes.

Configurar las conexiones del servidor

Los servidores Cisco UCS tienen una tarjeta de interfaz virtual de dos puertos VIC1387, que se utiliza para el tráfico de datos y el arranque del sistema operativo ESXi mediante iSCSI. Estas interfaces se configuran para que se conmutan al nodo de respaldo entre sí, lo que proporciona redundancia adicional más allá de un solo enlace. Al distribuir estos enlaces a través de varios switches, el servidor puede sobrevivir incluso a un fallo

completo del switch.

Desde el modo de configuración (`config t`), ejecute los siguientes comandos para configurar los valores de puerto para las interfaces conectadas a cada servidor.

Switch Cisco Nexus A: Configuración de Cisco UCS Server-A y Cisco UCS Server-B.

```
int eth1/3-4
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_A_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu9216
  no shut
exit
copy run start
```

Cisco Nexus Switch B: Configuración de Cisco UCS Server-A y Cisco UCS Server-B.

```
int eth1/3-4
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_B_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

En esta validación de soluciones se utilizó una MTU de 9000. Sin embargo, en función de los requisitos de la aplicación, puede configurar un valor de MTU adecuado. Es importante establecer el mismo valor de MTU en la solución de FlexPod. Las configuraciones de MTU incorrectas entre componentes dejarán de tener paquetes y estos paquetes deberán transmitirse de nuevo. Esto afectará al rendimiento general de la solución.

Para escalar la solución añadiendo servidores Cisco UCS adicionales, ejecute los comandos anteriores con los puertos del switch a los que se han conectado los servidores recién añadidos en los switches A y B.

Enlace ascendente a la infraestructura de red existente

En función de la infraestructura de red disponible, se pueden utilizar varios métodos y funciones para elevar el entorno FlexPod. Si hay un entorno Cisco Nexus existente presente, NetApp recomienda el uso de VPC para elevar los switches Cisco Nexus 3172P incluidos en el entorno FlexPod a la infraestructura. Los enlaces ascendentes pueden ser enlaces de subida de 10 GbE para una solución de infraestructura de 10 GbE o 1

GbE para una solución de infraestructura de 1 GbE si fuera necesario. Los procedimientos descritos anteriormente se pueden utilizar para crear un VPC de enlace ascendente al entorno existente. Asegúrese de ejecutar Copy RUN START para guardar la configuración en cada switch una vez completada la configuración.

"Siguiente: Procedimiento de instalación de almacenamiento de NetApp (parte 1)"

Procedimiento de instalación de almacenamiento NetApp (parte 1)

En esta sección se describe el procedimiento de implementación del almacenamiento AFF de NetApp.

Instalación de la controladora de almacenamiento de NetApp serie AFF2xx

Hardware Universe de NetApp

La aplicación NetApp Hardware Universe (HWU) proporciona componentes de hardware y software compatibles con cualquier versión específica de ONTAP. Proporciona información de configuración para todos los dispositivos de almacenamiento de NetApp compatibles actualmente con el software ONTAP. También se proporciona una tabla de compatibilidades de componentes.

Confirme que los componentes de hardware y software que desea utilizar son compatibles con la versión de ONTAP que tiene previsto instalar:

1. Acceda a "HWU" aplicación para ver las guías de configuración del sistema. Haga clic en la pestaña controladoras para ver la compatibilidad entre distintas versiones del software ONTAP y los dispositivos de almacenamiento de NetApp con las especificaciones que desea.
2. Como alternativa, para comparar componentes por dispositivo de almacenamiento, haga clic en Comparar sistemas de almacenamiento.

Requisitos previos de la controladora de la serie AFF2XX
Para planificar la ubicación física de los sistemas de almacenamiento, consulte Hardware Universe de NetApp. Consulte las siguientes secciones: Requisitos eléctricos, cables de alimentación admitidos y puertos y cables integrados.

Controladoras de almacenamiento

Siga los procedimientos de instalación física de los controladores de la "Documentación de AFF A220".

ONTAP 9.4 de NetApp

Hoja de datos de configuración

Antes de ejecutar la secuencia de comandos de instalación, rellene la hoja de datos de configuración del manual del producto. La hoja de datos de configuración está disponible en la "Guía de configuración de software de ONTAP 9.4".

Este sistema se establece en una configuración de clúster de dos nodos sin switch.

La siguiente tabla muestra información sobre la instalación y la configuración de ONTAP 9.4.

Detalles del clúster	Valor de detalles de clúster
Nodo del clúster: Dirección IP	<<var_nodeA_mgmt_ip>>
Máscara de red Del nodo a del clúster	<<var_nodeA_mgmt_mask>>
Nodo del clúster: Puerta de enlace	<<var_nodeA_mgmt_gateway>>
Nombre del nodo a del clúster	<<var_nodeA>>
Dirección IP del nodo B del clúster	<<var_nodeB_mgmt_ip>>
Máscara de red del nodo B del clúster	<<var_nodeB_mgmt_mask>>
Puerta de enlace del nodo B del clúster	<<var_nodeB_mgmt_gateway>>
Nombre del nodo B del clúster	<<var_nodeB>>
Dirección URL de ONTAP 9.4	<<var_url_boot_software>>
El nombre del clúster	<<var_clustername>>
Dirección IP de gestión del clúster	<<var_clustermgmt_ip>>
Puerta de enlace del clúster B.	<<var_clustermgmt_gateway>>
Máscara de red del clúster B.	<<var_clustermgmt_mask>>
Nombre de dominio	<<var_domain_name>>
IP del servidor DNS (puede introducir más de uno)	<<var_dns_server_ip>>
La IP del servidor NTP (es posible introducir más de uno)	<<var_ntp_server_ip>>

Configure el nodo a

Para configurar el nodo A, complete los siguientes pasos:

1. Conéctese al puerto de la consola del sistema de almacenamiento. Tiene que ver un cargador-a del símbolo del sistema. Sin embargo, si el sistema de almacenamiento está en un bucle de reinicio, pulse Ctrl-C para salir del bucle de autoarranque cuando vea este mensaje:

   ```
   Starting AUTOBOOT press Ctrl-C to abort…
   ```

2. Permita que el sistema arranque.

   ```
   autoboot
   ```

3. Pulse Ctrl-C para acceder al menú Inicio.

   Si ONTAP 9.4 no es la versión del software que se está arrancando, continúe con los pasos siguientes para instalar el software nuevo. Si ONTAP 9.4 es la versión que se va a arrancar, seleccione la opción 8 e y para reiniciar el nodo. A continuación, continúe con el paso 14.

4. Para instalar software nuevo, seleccione opción `7`.

5. Introduzca `y` para realizar una actualización.
6. Seleccione `e0M` para el puerto de red que desea usar para la descarga.
7. Introduzca `y` para reiniciar ahora.
8. Introduzca la dirección IP, la máscara de red y la puerta de enlace predeterminada para e0M en sus respectivos lugares.

```
<<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
```

9. Especifique la dirección URL donde se puede encontrar el software.

   Este servidor web debe ser pingable.

```
<<var_url_boot_software>>
```

10. Pulse Intro para el nombre de usuario, indicando que no hay nombre de usuario.
11. Introduzca `y` para establecer el software recién instalado como el predeterminado que se utilizará para los siguientes reinicios.
12. Introduzca `y` para reiniciar el nodo.

    Al instalar el software nuevo, el sistema podría realizar actualizaciones de firmware en el BIOS y las tarjetas adaptadoras, lo que provoca reinicios y posibles interrupciones en el cargador. Si se producen estas acciones, el sistema podría desviarse de este procedimiento.

13. Pulse Ctrl-C para acceder al menú Inicio.
14. Seleccione opción `4` Para una configuración limpia y inicializar todos los discos.
15. Introduzca `y` para poner a cero discos, restablezca la configuración e instale un nuevo sistema de archivos.
16. Introduzca `y` para borrar todos los datos de los discos.

    La inicialización y creación del agregado raíz puede tardar 90 minutos o más en completarse, según el número y el tipo de discos conectados. Una vez finalizada la inicialización, el sistema de almacenamiento se reinicia. Tenga en cuenta que los SSD tardan mucho menos tiempo en inicializarse. Puede continuar con la configuración del nodo B mientras los discos del nodo A se están poniendo a cero.

17. Mientras el nodo A se está inicializando, empiece a configurar el nodo B.

Configure el nodo B

Para configurar el nodo B, complete los siguientes pasos:

1. Conéctese al puerto de la consola del sistema de almacenamiento. Tiene que ver un cargador-a del símbolo del sistema. Sin embargo, si el sistema de almacenamiento está en un bucle de reinicio, pulse Ctrl-C para salir del bucle de autoarranque cuando vea este mensaje:

```
Starting AUTOBOOT press Ctrl-C to abort…
```

2. Pulse Ctrl-C para acceder al menú Inicio.

```
autoboot
```

3. Pulse Ctrl-C cuando se le solicite.

   Si ONTAP 9.4 no es la versión del software que se está arrancando, continúe con los pasos siguientes para instalar el software nuevo. Si ONTAP 9.4 es la versión que se va a arrancar, seleccione la opción 8 e y para reiniciar el nodo. A continuación, continúe con el paso 14.

4. Para instalar software nuevo, seleccione la opción 7.
5. Introduzca `y` para realizar una actualización.
6. Seleccione `e0M` para el puerto de red que desea usar para la descarga.
7. Introduzca `y` para reiniciar ahora.
8. Introduzca la dirección IP, la máscara de red y la puerta de enlace predeterminada para e0M en sus respectivos lugares.

```
<<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
```

9. Especifique la dirección URL donde se puede encontrar el software.

   Este servidor web debe ser pingable.

```
<<var_url_boot_software>>
```

10. Pulse Intro para el nombre de usuario, indicando que no hay nombre de usuario.
11. Introduzca `y` para establecer el software recién instalado como el predeterminado que se utilizará para los siguientes reinicios.
12. Introduzca `y` para reiniciar el nodo.

    Al instalar el software nuevo, el sistema podría realizar actualizaciones de firmware en el BIOS y las tarjetas adaptadoras, lo que provoca reinicios y posibles interrupciones en el cargador. Si se producen estas acciones, el sistema podría desviarse de este procedimiento.

13. Pulse Ctrl-C para acceder al menú Inicio.
14. Seleccione la opción 4 para Configuración limpia y inicializar todos los discos.
15. Introduzca `y` para poner a cero discos, restablezca la configuración e instale un nuevo sistema de archivos.
16. Introduzca `y` para borrar todos los datos de los discos.

La inicialización y creación del agregado raíz puede tardar 90 minutos o más en completarse, según el número y el tipo de discos conectados. Una vez finalizada la inicialización, el sistema de almacenamiento se reinicia. Tenga en cuenta que los SSD tardan mucho menos tiempo en inicializarse.

Continuación de la configuración del nodo A y de la configuración del clúster

Desde un programa de puertos de consola conectado al puerto de la consola De la controladora De almacenamiento A (nodo A), ejecute el script de configuración del nodo. Este script se muestra cuando ONTAP 9.4 arranca en el nodo por primera vez.

> El procedimiento de configuración del nodo y de los clústeres ha cambiado ligeramente en ONTAP 9.4. El asistente de configuración de clúster ahora se utiliza para configurar el primer nodo de un clúster, y System Manager se utiliza para configurar el clúster.

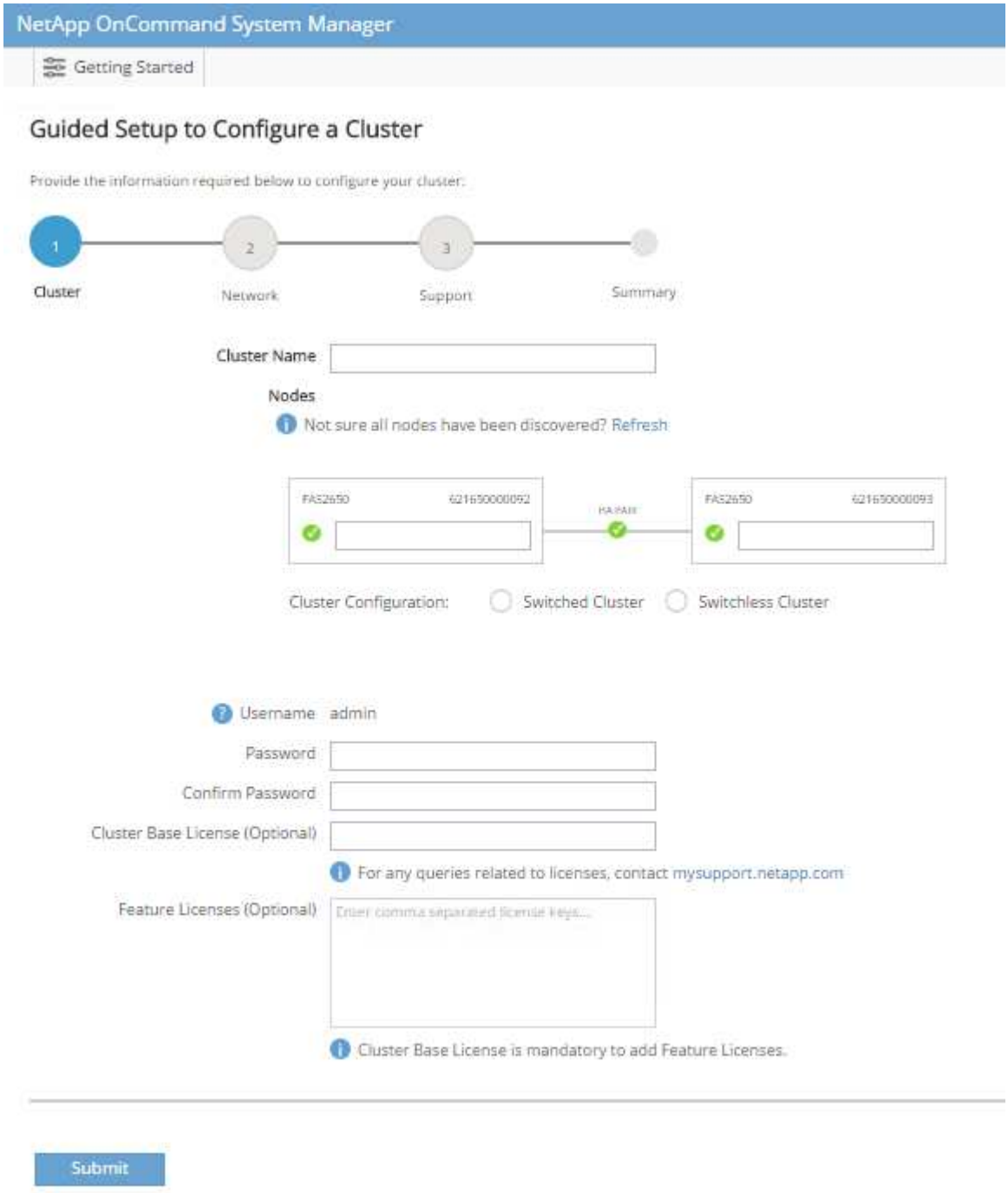
1. Siga las instrucciones para configurar el nodo A.

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

2. Vaya a la dirección IP de la interfaz de gestión del nodo.

La configuración del clúster también se puede realizar mediante la CLI. Este documento describe la configuración del clúster mediante la configuración guiada de System Manager de NetApp.

3. Haga clic en Guided Setup para configurar el clúster.
4. Introduzca `<<var_clustername>>` del nombre del clúster y. `<<var_nodeA>>` y.. `<<var_nodeB>>` para cada uno de los nodos que va a configurar. Introduzca la contraseña que desea usar para el sistema de almacenamiento. Seleccione Switchless Cluster para el tipo de clúster. Introduzca la licencia base del clúster.



5. También es posible introducir licencias de funciones para Cluster, NFS e iSCSI.
6. Ve un mensaje de estado que indica que el clúster se está creando. Este mensaje de estado cambia por varios Estados. Este proceso tarda varios minutos.

7. Configure la red.
   a. Anule la selección de la opción intervalo de direcciones IP.
   b. Introduzca `<<var_clustermgmt_ip>>` En el campo Cluster Management IP Address, `<<var_clustermgmt_mask>>` En el campo máscara de red, y. `<<var_clustermgmt_gateway>>` En el campo Puerta de enlace. Utilice el… Selector en el campo Port para seleccionar e0M del nodo A.
   c. La IP de gestión de nodos para el nodo A ya se ha rellenado. Introduzca `<<var_nodeA_mgmt_ip>>` Para el nodo B.
   d. Introduzca `<<var_domain_name>>` En el campo DNS Domain Name. Introduzca `<<var_dns_server_ip>>` En el campo DNS Server IP Address.

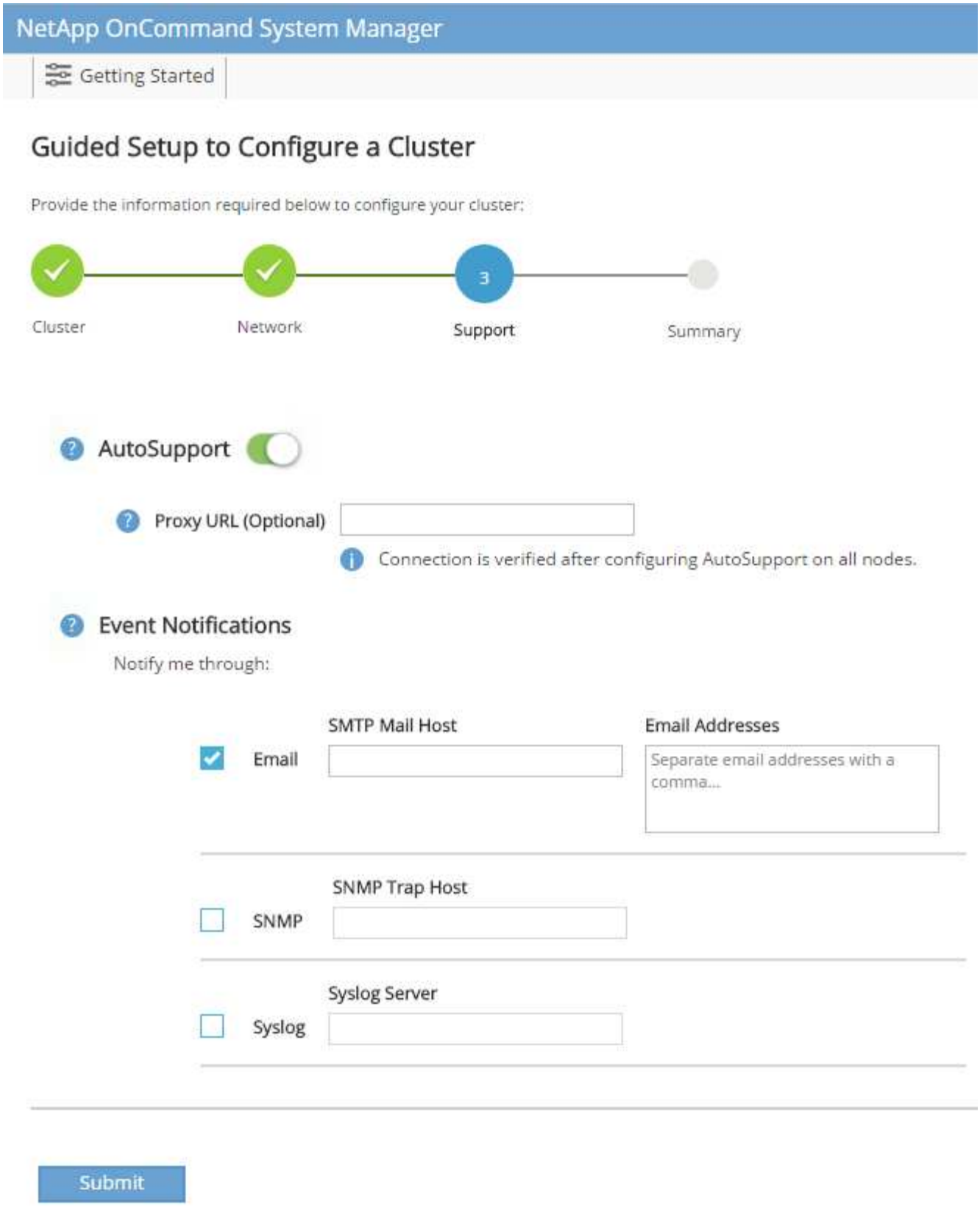
      Puede introducir varias direcciones IP del servidor DNS.

   e. Introduzca `<<var_ntp_server_ip>>` En el campo servidor NTP primario.

      También puede introducir un servidor NTP alternativo.

8. Configure la información de soporte.
   a. Si el entorno requiere un proxy para acceder a AutoSupport, introduzca la URL en Proxy URL.
   b. Introduzca el host de correo SMTP y la dirección de correo electrónico para las notificaciones de eventos.

      Debe, como mínimo, configurar el método de notificación de eventos antes de continuar. Puede seleccionar cualquiera de los métodos.



9. Cuando indique que ha finalizado la configuración del clúster, haga clic en Manage your Cluster para configurar el almacenamiento.

Continuación de la configuración del clúster de almacenamiento

Después de configurar los nodos de almacenamiento y el clúster base, puede continuar con la configuración del clúster de almacenamiento.

Ponga a cero todos los discos de repuesto

Para poner a cero todos los discos de repuesto del clúster, ejecute el siguiente comando:

```
disk zerospares
```

Configure la personalidad de los puertos UTA2 integrados

1. Verifique el modo actual y el tipo actual de puertos ejecutando el `ucadmin show` comando.

```
AFF A220::> ucadmin show
                      Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFF A220_A     0c       fc       target     -        -          online
AFF A220_A     0d       fc       target     -        -          online
AFF A220_A     0e       fc       target     -        -          online
AFF A220_A     0f       fc       target     -        -          online
AFF A220_B     0c       fc       target     -        -          online
AFF A220_B     0d       fc       target     -        -          online
AFF A220_B     0e       fc       target     -        -          online
AFF A220_B     0f       fc       target     -        -          online
8 entries were displayed.
```

2. Compruebe que el modo actual de los puertos que se están utilizando es `cna` y que el tipo actual está establecido en `target`. De lo contrario, cambie la personalidad de puerto mediante el siguiente comando:

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

Los puertos deben estar desconectados para que se ejecute el comando anterior. Para desconectar un puerto, ejecute el siguiente comando:

```
`network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down`
```

Si ha cambiado la personalidad del puerto, debe reiniciar cada nodo para que el cambio se aplique.

Cambiar el nombre de las interfaces lógicas de gestión (LIF)

Para cambiar el nombre de las LIF de administración, realice los pasos siguientes:

1. Muestra los nombres de las LIF de gestión actuales.

```
network interface show –vserver <<clustername>>
```

2. Cambie el nombre de la LIF de gestión del clúster.

```
network interface rename –vserver <<clustername>> –lif
cluster_setup_cluster_mgmt_lif_1 –newname cluster_mgmt
```

3. Cambie el nombre del LIF de gestión del nodo B.

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_node_mgmt_lif_AFF A220_B_1 -newname AFF A220-02_mgmt1
```

Configure la reversión automática en la gestión del clúster

Ajuste la `auto-revert` parámetro en la interfaz de gestión del clúster.

```
network interface modify –vserver <<clustername>> -lif cluster_mgmt –auto-
revert true
```

Configure la interfaz de red del procesador de servicio

Para asignar una dirección IPv4 estática al procesador de servicios en cada nodo, ejecute los siguientes comandos:

```
system service-processor network modify –node <<var_nodeA>> -address
-family IPv4 –enable true –dhcp none –ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify –node <<var_nodeB>> -address
-family IPv4 –enable true –dhcp none –ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

Las direcciones IP de Service Processor deben estar en la misma subred que las direcciones IP de gestión de nodos.

Activar la recuperación tras fallos de almacenamiento en ONTAP

Para confirmar que la conmutación por error del almacenamiento está habilitada, ejecute los siguientes

comandos de una pareja de conmutación por error:

1. Comprobar el estado de recuperación tras fallos del almacenamiento.

```
storage failover show
```

   Ambas <<var_nodeA>> y.. <<var_nodeB>> debe poder realizar una toma de control. Vaya al paso 3 si los nodos pueden realizar una toma de control.

2. Habilite la conmutación al nodo de respaldo en uno de los dos nodos.

```
storage failover modify -node <<var_nodeA>> -enabled true
```

   Habilitar la conmutación al nodo de respaldo en un solo nodo permite que se produzca en ambos nodos.

3. Compruebe el estado de alta disponibilidad del clúster de dos nodos.

   Este paso no es aplicable para clústeres con más de dos nodos.

```
cluster ha show
```

4. Vaya al paso 6 si está configurada la alta disponibilidad. Si se ha configurado la alta disponibilidad, verá el siguiente mensaje al emitir el comando:

```
High Availability Configured: true
```

5. Habilite el modo de alta disponibilidad solo para el clúster de dos nodos.

   No ejecute este comando para clústeres con más de dos nodos debido a que provoca problemas con la conmutación al nodo de respaldo.

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. Compruebe que la asistencia de hardware está correctamente configurada y, si es necesario, modifique la dirección IP del partner.

```
storage failover hwassist show
```

   El mensaje `Keep Alive Status : Error: did not receive hwassist keep alive alerts from partner` indica que la asistencia de hardware no está configurada. Ejecute los siguientes comandos para configurar hardware Assist.

```
storage failover modify –hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify –hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

Cree un dominio de retransmisión MTU para tramas gigantes en ONTAP

Para crear un dominio de retransmisión de datos con un valor MTU de 9000, ejecute los siguientes comandos:

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

Quite los puertos de datos del dominio de retransmisión predeterminado

Los puertos de datos de 10 GbE se utilizan para el tráfico iSCSI/NFS y estos puertos deben eliminarse del dominio predeterminado. Los puertos e0e y e0f no se utilizan y deben eliminarse del dominio predeterminado.

Para quitar puertos del dominio de retransmisión, ejecute el siguiente comando:

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

Deshabilite el control de flujo en los puertos UTA2

Se recomienda utilizar las mejores prácticas de NetApp para deshabilitar el control de flujo en todos los puertos UTA2 conectados a dispositivos externos. Para desactivar el control de flujo, ejecute el siguiente comando:

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
```

Configure LACP con IFGRP en ONTAP

Este tipo de grupo de interfaces requiere dos o más interfaces Ethernet y un switch compatible con LACP. Asegúrese de que el interruptor está configurado correctamente.

Desde el símbolo del sistema del clúster, complete los siguientes pasos.

```
ifgrp create -node <<var_nodeA>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0d
ifgrp create -node << var_nodeB>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0d
```

Configurar tramas gigantes en ONTAP de NetApp

Para configurar un puerto de red ONTAP para que utilice tramas gigantes (que normalmente tienen una MTU de 9,000 bytes), ejecute los siguientes comandos desde el shell del clúster:

```
AFF A220::> network port modify -node node_A -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
```

Crear VLAN en ONTAP

Para crear VLAN en ONTAP, complete los siguientes pasos:

1. Cree puertos VLAN NFS y añádalos al dominio de retransmisión de datos.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_nfs_vlan_id>>
broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
<<var_nodeA>>:a0a-<<var_nfs_vlan_id>>, <<var_nodeB>>:a0a-
<<var_nfs_vlan_id>>
```

2. Cree puertos VLAN iSCSI y añádalos al dominio de retransmisión de datos.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_A_id>>, <<var_nodeB>>:a0a-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_B_id>>, <<var_nodeB>>:a0a-
<<var_iscsi_vlan_B_id>>
```

3. Cree puertos MGMT-VLAN.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<mgmt_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<mgmt_vlan_id>>
```

Crear agregados en ONTAP

Durante el proceso de configuración de ONTAP, se crea un agregado que contiene el volumen raíz. Para crear agregados adicionales, determine el nombre del agregado, el nodo en el que se creará y el número de discos que contiene.

Para crear agregados, ejecute los siguientes comandos:

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

Conserve al menos un disco (seleccione el disco más grande) en la configuración como un repuesto. Una práctica recomendada es tener al menos un repuesto para cada tipo y tamaño de disco.

Empiece con cinco discos; puede añadir discos a un agregado cuando necesite almacenamiento adicional.

No se puede crear el agregado hasta que se complete el establecimiento en cero del disco. Ejecute el `aggr show` comando para mostrar el estado de creación del agregado. No continúe hasta `aggr1`_`nodeA` está en línea.

Configurar la zona horaria en ONTAP

Para configurar la sincronización horaria y establecer la zona horaria en el clúster, ejecute el siguiente comando:

```
timezone <<var_timezone>>
```

Por ejemplo, en el este de los Estados Unidos, la zona horaria es `America/New York`. Cuando haya comenzado a escribir el nombre de la zona horaria, pulse la tecla TAB para ver las opciones disponibles.

Configurar SNMP en ONTAP

Para configurar SNMP, realice los siguientes pasos:

1. Configure la información básica de SNMP, como la ubicación y el contacto. Cuando se sondean, esta información es visible como `sysLocation` y.. `sysContact` Variables en SNMP.

```
snmp contact <<var_snmp_contact>>
snmp location "<<var_snmp_location>>"
snmp init 1
options snmp.enable on
```

2. Configure las capturas SNMP para que se envíen a hosts remotos.

```
snmp traphost add <<var_snmp_server_fqdn>>
```

Configure SNMPv1 en ONTAP

Para configurar SNMPv1, establezca la contraseña de texto sin formato secreta compartida denominada comunidad.

```
snmp community add ro <<var_snmp_community>>
```

Utilice la `snmp community delete all` comando con precaución. Si se utilizan cadenas de comunidad para otros productos de supervisión, este comando las quita.

Configure SNMPv3 en ONTAP

SNMPv3 requiere que defina y configure un usuario para la autenticación. Para configurar SNMPv3, lleve a cabo los siguientes pasos:

1. Ejecute el `security snmpusers` Comando para ver el ID del motor.
2. Cree un usuario llamado `snmpv3user`.

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. Introduzca el ID del motor de la entidad autoritativa y seleccione `md5` como protocolo de autenticación.
4. Escriba una contraseña de longitud mínima de ocho caracteres para el protocolo de autenticación cuando se le solicite.
5. Seleccione `des` como protocolo de privacidad.
6. Escriba una contraseña de longitud mínima de ocho caracteres para el protocolo de privacidad cuando se le solicite.

Configure HTTPS de AutoSupport en ONTAP

La herramienta AutoSupport de NetApp envía información de resumen de soporte a NetApp mediante HTTPS. Para configurar AutoSupport, ejecute el siguiente comando:

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

Cree una máquina virtual de almacenamiento

Para crear una máquina virtual de almacenamiento (SVM) de infraestructura, complete los siguientes pasos:

1. Ejecute el `vserver create` comando.

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume-security-style unix
```

2. Añada el agregado de datos a la lista de agregados de infra-SVM para VSC de NetApp.

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. Elimine los protocolos de almacenamiento que no se utilicen de la SVM, con lo que dejará NFS e iSCSI.

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. Habilite y ejecute el protocolo NFS en la SVM de infra-SVM.

```
`nfs create -vserver Infra-SVM -udp disabled`
```

5. Encienda la `SVM vstorage` Parámetro para el plugin VAAI para NFS de NetApp. A continuación,

compruebe que NFS se ha configurado.

```
`vserver nfs modify –vserver Infra-SVM –vstorage enabled`
`vserver nfs show `
```

Los comandos están precedidos por `vserver` en la línea de comandos porque las máquinas virtuales de almacenamiento se denominaban servidores anteriormente.

Configure NFSv3 en ONTAP

En la siguiente tabla, se enumera la información necesaria para completar esta configuración.

Detalles	Valor de detalle
Host ESXi dirección IP de NFS	<<var_esxi_hostA_nfs_ip>>
Dirección IP de NFS del host ESXi B	<<var_esxi_hostB_nfs_ip>>

Para configurar NFS en la SVM, ejecute los siguientes comandos:

1. Cree una regla para cada host ESXi en la política de exportación predeterminada.
2. Asigne una regla para cada host ESXi que se cree. Cada host tiene su propio índice de reglas. El primer host ESXi tiene el índice de regla 1, el segundo host ESXi tiene el índice de regla 2, etc.

```
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 1 –protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 2 –protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule show
```

3. Asigne la política de exportación al volumen raíz de la SVM de infraestructura.

```
volume modify –vserver Infra-SVM –volume rootvol –policy default
```

VSC de NetApp gestiona automáticamente las políticas de exportación si decide instalarlas después de configurar vSphere. Si no lo instala, debe crear reglas de políticas de exportación cuando se añadan servidores C-Series de Cisco UCS adicionales.

Cree el servicio iSCSI en ONTAP

Para crear el servicio iSCSI, complete el paso siguiente:

1. Cree el servicio iSCSI en la SVM. Este comando también inicia el servicio iSCSI y establece el IQN de iSCSI para la SVM. Comprobar que iSCSI se ha configurado.

```
iscsi create -vserver Infra-SVM
iscsi show
```

Crear reflejo de uso compartido de carga del volumen raíz de la SVM en ONTAP

1. Cree un volumen para que sea el reflejo de carga compartida del volumen raíz de la SVM de infraestructura en cada nodo.

```
volume create –vserver Infra_Vserver –volume rootvol_m01 –aggregate
aggr1_nodeA –size 1GB –type DP
volume create –vserver Infra_Vserver –volume rootvol_m02 –aggregate
aggr1_nodeB –size 1GB –type DP
```

2. Crear una programación de tareas para actualizar las relaciones de mirroring del volumen raíz cada 15 minutos.

```
job schedule interval create -name 15min -minutes 15
```

3. Cree las relaciones de mirroring.

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

4. Inicialice la relación de mirroring y compruebe que se haya creado.

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol
snapmirror show
```

Configure el acceso HTTPS en ONTAP

Para configurar el acceso seguro a la controladora de almacenamiento, lleve a cabo los siguientes pasos:

1. Aumente el nivel de privilegio para acceder a los comandos de certificado.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. En general, ya se encuentra en funcionamiento un certificado autofirmado. Verifique el certificado ejecutando el siguiente comando:

```
security certificate show
```

3. Para cada SVM que se muestra, el nombre común de certificado debe coincidir con el FQDN de DNS de la SVM. Los cuatro certificados predeterminados deben eliminarse y sustituirse por certificados autofirmados o certificados de una entidad de certificación.

   La práctica recomendada es eliminar certificados caducados antes de crear certificados. Ejecute el `security certificate delete` comando para eliminar certificados caducados. En el siguiente comando, use LA TABULACIÓN automática para seleccionar y eliminar cada certificado predeterminado.

```
security certificate delete [TAB] …
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM -type server -serial 552429A6
```

4. Para generar e instalar certificados autofirmados, ejecute los siguientes comandos como comandos de una sola vez. Generar un certificado de servidor para la SVM de infraestructura y la SVM de clúster. De nuevo, utilice LA TABULACIÓN automática como ayuda para completar estos comandos.

```
security certificate create [TAB] …
Example: security certificate create -common-name infra-svm. netapp.com
-type  server -size 2048 -country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email-addr
"abc@netapp.com" -expire-days 365 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. Para obtener los valores de los parámetros necesarios en el paso siguiente, ejecute el `security certificate show` comando.
6. Habilite cada certificado que se acaba de crear mediante el `-server-enabled true` y.. `-client-enabled false` parámetros. De nuevo, utilice LA TABULACIÓN automática.

```
security ssl modify [TAB] …
Example: security ssl modify -vserver Infra-SVM -server-enabled true
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common
-name infra-svm.netapp.com
```

7. Configure y habilite el acceso SSL y HTTPS y deshabilite el acceso HTTP.

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be
         interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http
-vserver <<var_clustername>>
```

Es normal que algunos de estos comandos devuelvan un mensaje de error indicando que la entrada no existe.

8. Vuelva al nivel de privilegio de administrador y cree la configuración para permitir que la SVM esté disponible en la web.

```
set –privilege admin
vserver services web modify –name spi|ontapi|compat –vserver * -enabled
true
```

Cree un volumen de FlexVol de NetApp en ONTAP

Para crear un volumen de FlexVol de NetApp, introduzca el nombre, el tamaño y el agregado del volumen en el que existe. Crear dos volúmenes de almacenes de datos de VMware y un volumen de arranque del servidor.

```
volume create -vserver Infra-SVM -volume infra_datastore_1 -aggregate
aggr1_nodeA -size 500GB -state online -policy default -junction-path
/infra_datastore_1 -space-guarantee none -percent-snapshot-space 0
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -junction-path /infra_swap
-space-guarantee none -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

Habilite la deduplicación en ONTAP

Para activar la deduplicación en volúmenes adecuados, ejecute los siguientes comandos:

```
volume efficiency on –vserver Infra-SVM -volume infra_datastore_1
volume efficiency on –vserver Infra-SVM -volume esxi_boot
```

Crear LUN en ONTAP

Para crear dos LUN de arranque, ejecute los siguientes comandos:

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware -space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware -space-reserve disabled
```

Cuando se añade un servidor Cisco UCS C-Series adicional, se debe crear un LUN de arranque adicional.

Creación de LIF iSCSI en ONTAP

En la siguiente tabla, se enumera la información necesaria para completar esta configuración.

Detalles	Valor de detalle
Nodo de almacenamiento a iSCSI LIF01A	<<var_nodeA_iscsi_lif01a_ip>>
Nodo de almacenamiento: Una máscara de red LIF01A de iSCSI	<<var_nodeA_iscsi_lif01a_mask>>
Nodo de almacenamiento a iSCSI LIF01B	<<var_nodeA_iscsi_lif01b_ip>>
Nodo de almacenamiento a máscara de red LIF01B de iSCSI	<<var_nodeA_iscsi_lif01b_mask>>
Nodo de almacenamiento B iSCSI LIF01A	<<var_nodeB_iscsi_lif01a_ip>>
Máscara de red del nodo de almacenamiento B iSCSI LIF01A	<<var_nodeB_iscsi_lif01a_mask>>
ISCSI LIF01B del nodo de almacenamiento	<<var_nodeB_iscsi_lif01b_ip>>
Máscara de red LIF01B de nodo de almacenamiento B.	<<var_nodeB_iscsi_lif01b_mask>>

1. Creación de cuatro LIF iSCSI, dos en cada nodo.

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface show
```

Creación de LIF NFS en ONTAP

En la siguiente tabla, se enumera la información necesaria para completar esta configuración.

Detalles	Valor de detalle
Nodo de almacenamiento: LIF NFS 01 IP	<<var_nodeA_nfs_lif_01_ip>>
Nodo de almacenamiento máscara de red a LIF 01 de NFS	<<var_nodeA_nfs_lif_01_mask>>
Nodo de almacenamiento B LIF NFS 02 IP	<<var_nodeB_nfs_lif_02_ip>>
Máscara de red del nodo de almacenamiento B LIF NFS 02	<<var_nodeB_nfs_lif_02_mask>>

1. Cree una LIF NFS.

```
network interface create -vserver Infra-SVM -lif nfs_lif01 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_ip>> -netmask <<
var_nodeA_nfs_lif_01_mask>> -status-admin up –failover-policy broadcast-
domain-wide –firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> –address <<var_nodeB_nfs_lif_02_ip>> -netmask <<
var_nodeB_nfs_lif_02_mask>> -status-admin up –failover-policy broadcast-
domain-wide –firewall-policy data –auto-revert true
network interface show
```

Añada el administrador de SVM de infraestructura

En la siguiente tabla, se enumera la información necesaria para completar esta configuración.

Detalles	Valor de detalle
IP de Vsmgmt	<<var_svm_mgmt_ip>>
Máscara de red Vsmgmt	<<var_svm_mgmt_mask>>
Puerta de enlace predeterminada de Vsmgmt	<<var_svm_mgmt_gateway>>

Para añadir la interfaz lógica de administración de SVM y el administrador de SVM de la infraestructura a la red de gestión, realice los siguientes pasos:

1. Ejecute el siguiente comando:

```
network interface create –vserver Infra-SVM –lif vsmgmt –role data
–data-protocol none –home-node <<var_nodeB>> -home-port  e0M –address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> -status-admin up
–failover-policy broadcast-domain-wide –firewall-policy mgmt –auto-
revert true
```

> La IP de administración de SVM aquí debe estar en la misma subred que la IP de administración del clúster de almacenamiento.

2. Cree una ruta predeterminada para permitir que la interfaz de gestión de SVM llegue al mundo exterior.

```
network route create –vserver Infra-SVM -destination 0.0.0.0/0 –gateway
<<var_svm_mgmt_gateway>>
network route show
```

3. Establezca una contraseña para el usuario de SVM vsadmin y desbloquee el usuario.

```
security login password –username vsadmin –vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock –username vsadmin –vserver Infra-SVM
```

"Siguiente: Procedimiento de puesta en marcha de servidores en rack Cisco UCS C-Series"

Procedimiento para la puesta en marcha de servidores en rack Cisco UCS C-Series

En la siguiente sección, se proporciona un procedimiento detallado para configurar un servidor de montaje en rack independiente Cisco UCS C-Series para su uso en la configuración de FlexPod Express.

Realice la configuración inicial del servidor independiente Cisco UCS C-Series para Cisco Integrated Management Server

Complete estos pasos para la configuración inicial de la interfaz de CIMC para servidores independientes Cisco UCS C-Series.

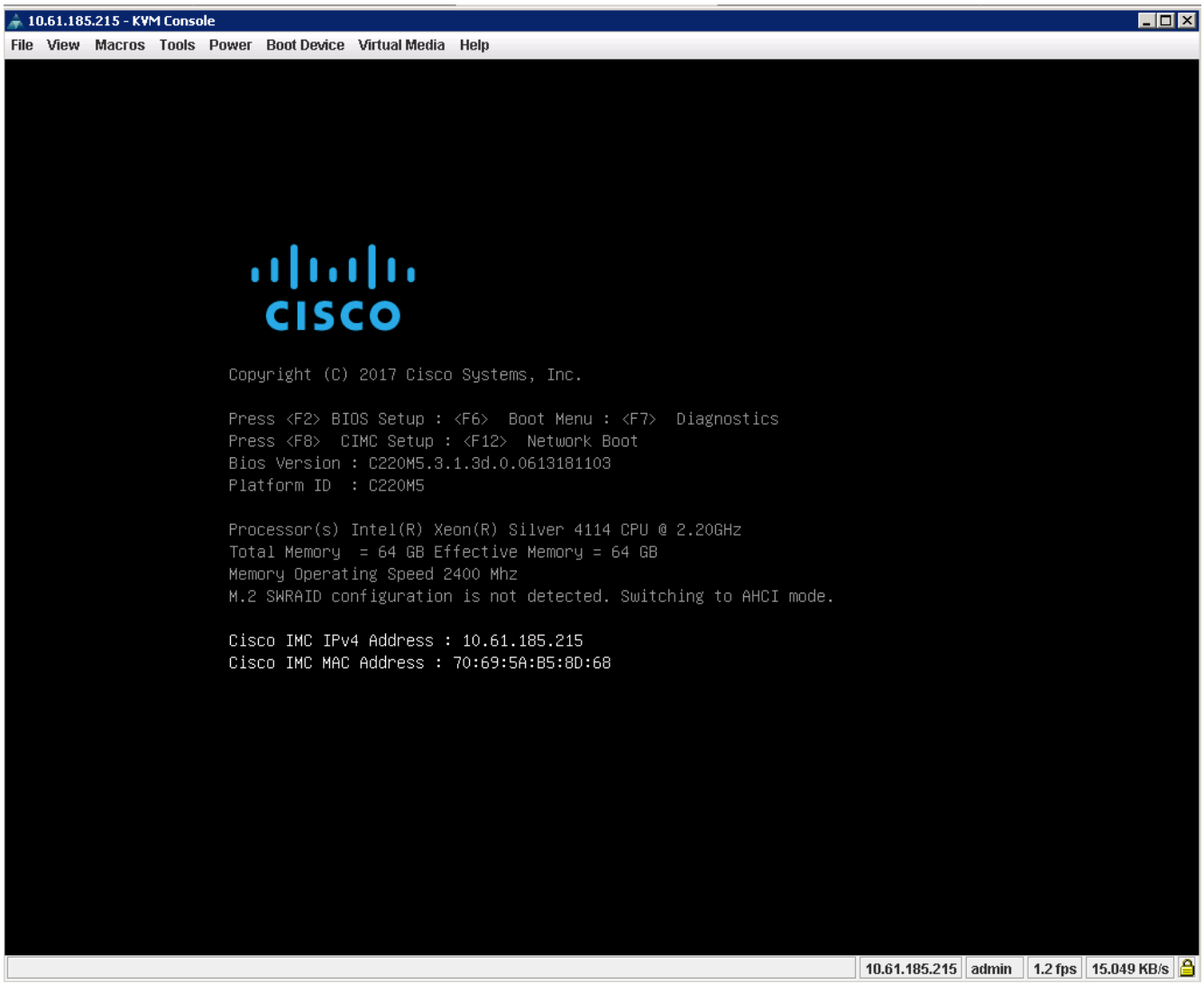
En la siguiente tabla se enumera la información necesaria para configurar CIMC para cada servidor independiente Cisco UCS C-Series.

Detalles	Valor de detalle
Dirección IP de CIMC	<<cimc_ip>>
Máscara de subred CIMC	<<cimc_netmask>>
Puerta de enlace predeterminada CIMC	<<cimc_gateway>>

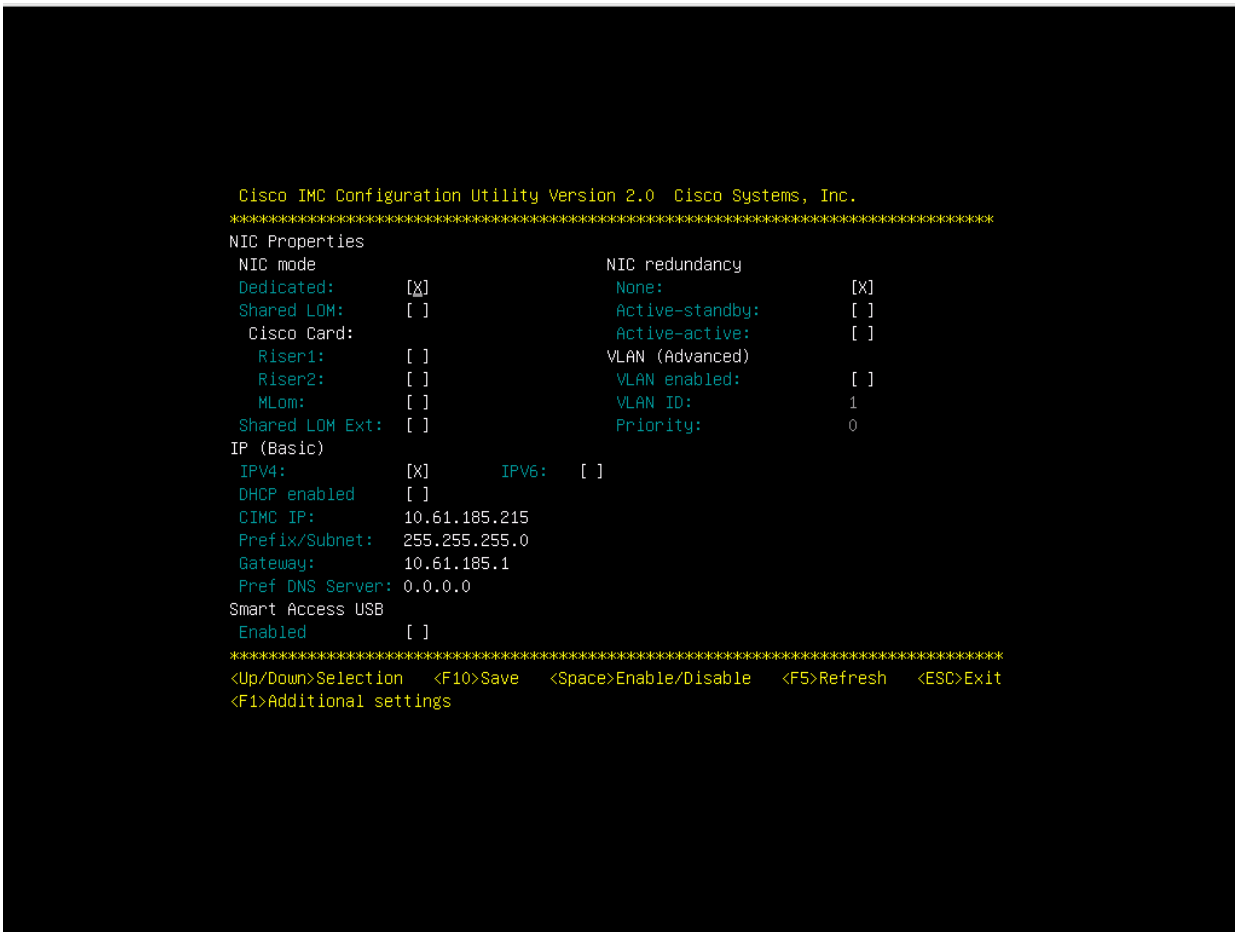
La versión de CIMC utilizada en esta validación es CIMC 3.1.3(g).

Todos los servidores

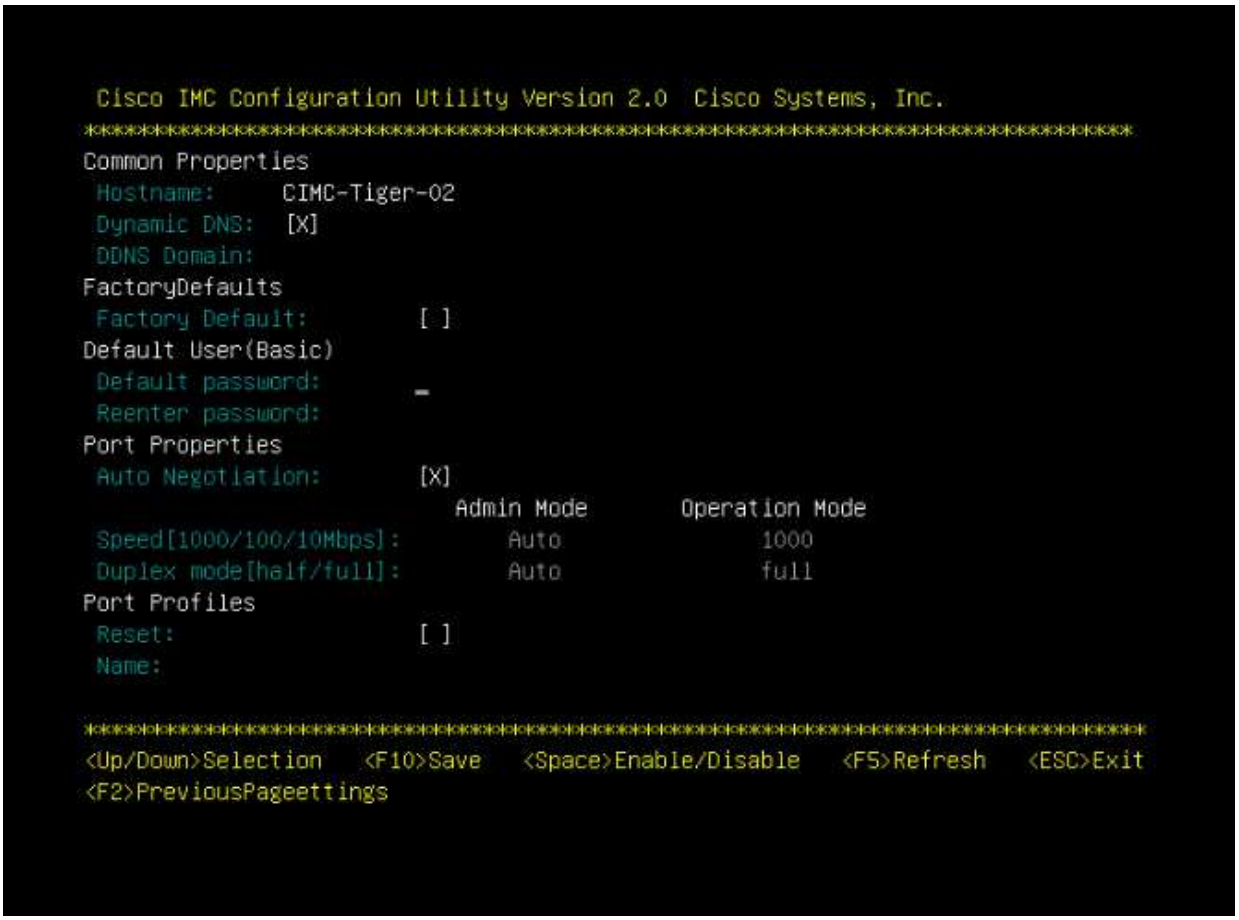
1. Conecte la mochila del teclado, vídeo y ratón (KVM) de Cisco (suministrada con el servidor) al puerto KVM de la parte frontal del servidor. Conecte un monitor VGA y un teclado USB a los puertos de mochila KVM adecuados.
2. Encienda el servidor y pulse F8 cuando se le solicite que introduzca la configuración de CIMC.



3. En la utilidad de configuración de CIMC, defina las siguientes opciones:
   - Modo de tarjeta de interfaz de red (NIC):
     - Dedicado [X]
   - IP (básico):
     - IPV4: [X]
     - DHCP habilitado: [ ]
     - IP de CIMC: <<cimc_ip>>
     - Prefijo/subred: <<cimc_netmask>>
     - Puerta de enlace: <<cimc_gateway>>
   - VLAN (Advanced): Deje borrado para deshabilitar el etiquetado VLAN.
     - Redundancia NIC
     - Ninguna: [X]



4. Pulse F1 para ver los ajustes adicionales.
   - Propiedades comunes:
     - Nombre del host: <<esxi_host_name>>
     - DNS dinámico: [ ]
     - Valores predeterminados de fábrica: Dejar borrado.
   - Usuario predeterminado (básico):
     - Contraseña predeterminada: <<admin_password>>
     - Vuelva a introducir la contraseña: <<admin_password>>
     - Propiedades del puerto: Utilice los valores predeterminados.
     - Perfiles de puerto: Dejar borrado.



5. Pulse F10 para guardar la configuración de la interfaz CIMC.
6. Una vez guardada la configuración, pulse Esc para salir.

Configurar arranque iSCSI de los servidores Cisco UCS C-Series

En esta configuración de FlexPod Express, la VIC1387 se utiliza para el arranque iSCSI.

La tabla siguiente enumera la información necesaria para configurar el arranque iSCSI.

La fuente en cursiva indica las variables que son únicas de cada host ESXi.

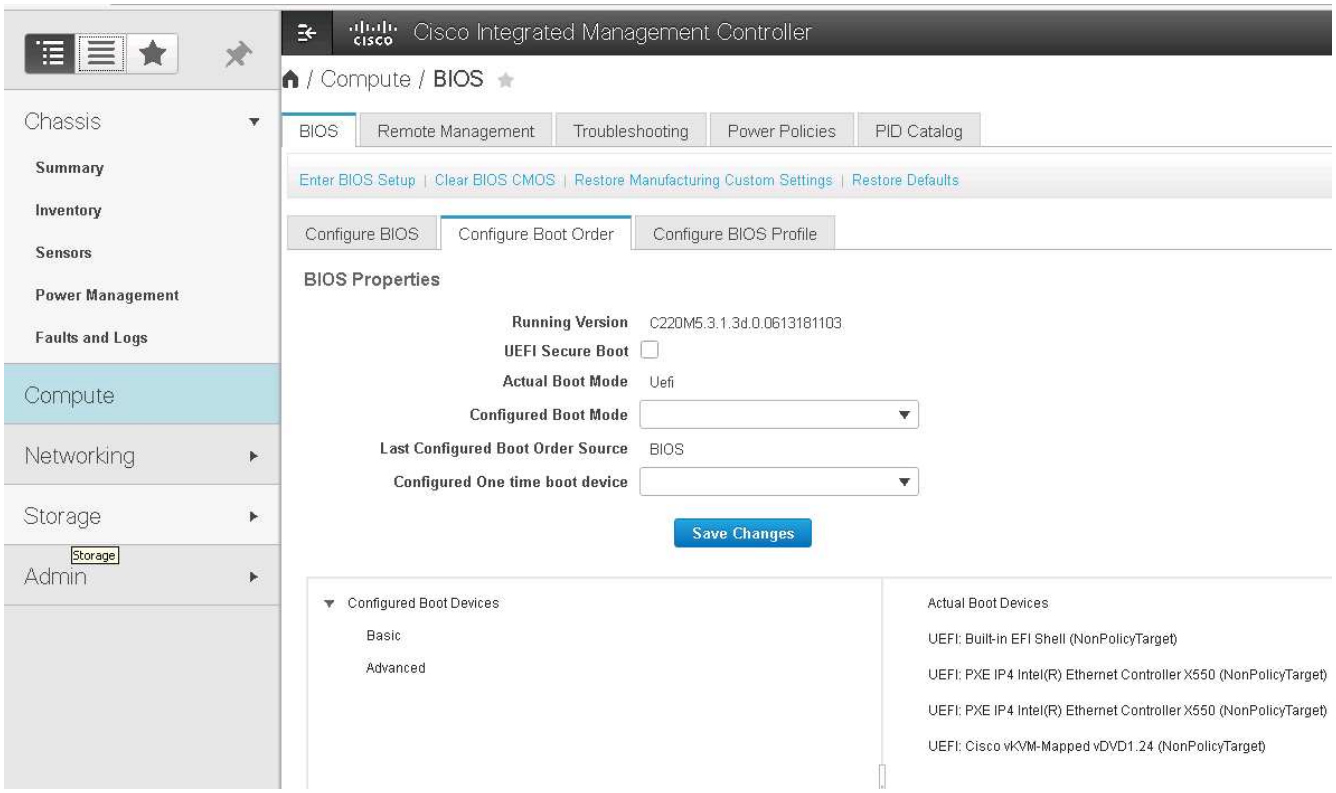
Detalles	Valor de detalle
Nombre Del iniciador del host ESXi	<<var_ucs_initiator_name_A>>
Host ESXi iSCSI-A IP	<<var_esxi_host_iscsiA_ip>>
Máscara de red iSCSI-A del host ESXi	<<var_esxi_host_iscsiA_mask>>
ISCSI del host ESXi: Puerta de enlace predeterminada	<<var_esxi_host_iscsiA_gateway>>
Nombre B del iniciador del host ESXi	<<var_ucs_initiator_name_B>>
Host ESXi iSCSI-B IP	<<var_esxi_host_iscsiB_ip>>
Máscara de red iSCSI-B del host ESXi	<<var_esxi_host_iscsiB_mask>>
Puerta de enlace iSCSI-B del host ESXi	<<var_esxi_host_iscsiB_gateway>>

Detalles	Valor de detalle
Dirección IP iscsi_lif01a	
Dirección IP iscsi_lif02a	
Dirección IP iscsi_lif01b	
Dirección IP iscsi_lif02b	
IQN de infr_SVM	

Configuración del orden de arranque

Para establecer la configuración del orden de arranque, lleve a cabo los siguientes pasos:

1. En la ventana del explorador de la interfaz CIMC, haga clic en la ficha servidor y seleccione BIOS.
2. Haga clic en Configurar orden de arranque y, a continuación, en Aceptar.



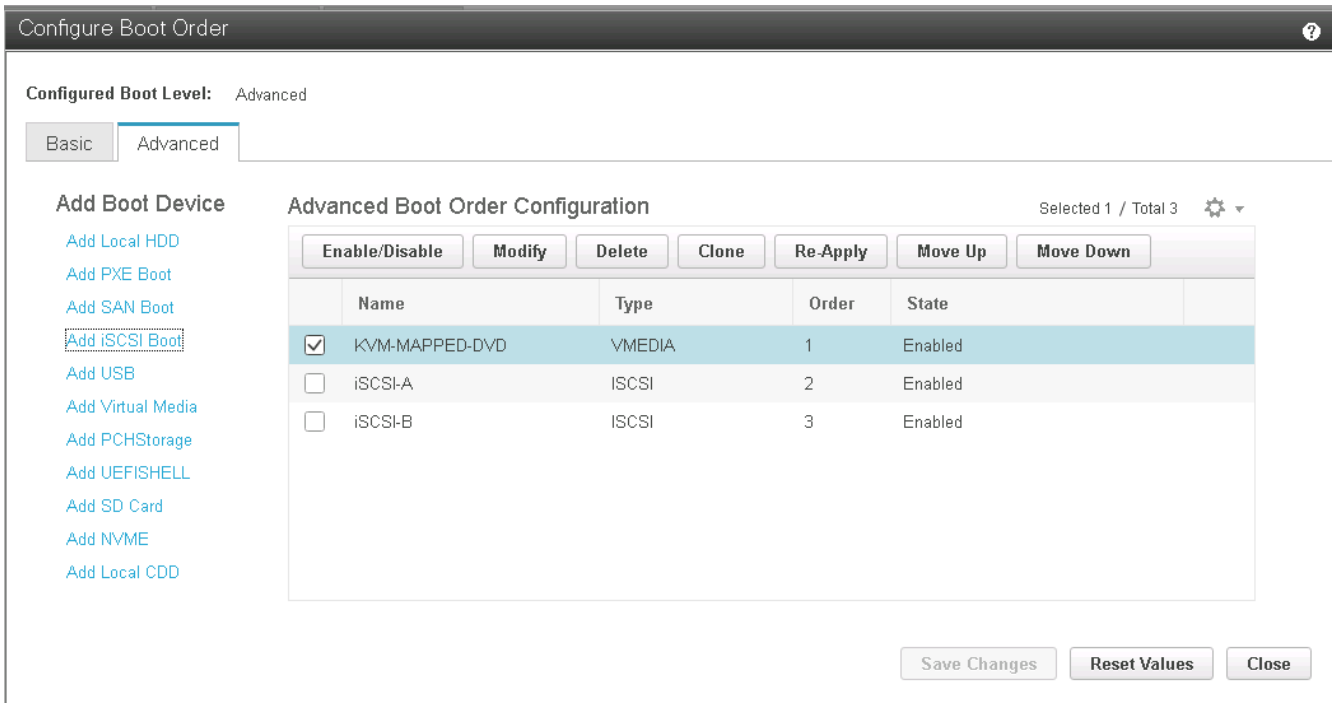
3. Para configurar los siguientes dispositivos, haga clic en el dispositivo en Agregar dispositivo de arranque y vaya a la ficha Opciones avanzadas.
   - Agregar medios virtuales
     - NOMBRE: KVM-CD-DVD
     - SUBTIPO: DVD KVM ASIGNADO
     - Estado: Habilitado
     - Orden: 1
   - Agregar arranque iSCSI.
     - Nombre: ISCSI-a

- Estado: Habilitado
- Orden: 2
- Ranura: MLOM
- Puerto: 0

◦ Haga clic en Add iSCSI Boot.

- Nombre: ISCSI-B
- Estado: Habilitado
- Pedido: 3
- Ranura: MLOM
- Puerto: 1

4. Haga clic en Agregar dispositivo.
5. Haga clic en Save Changes y, a continuación, en Close.

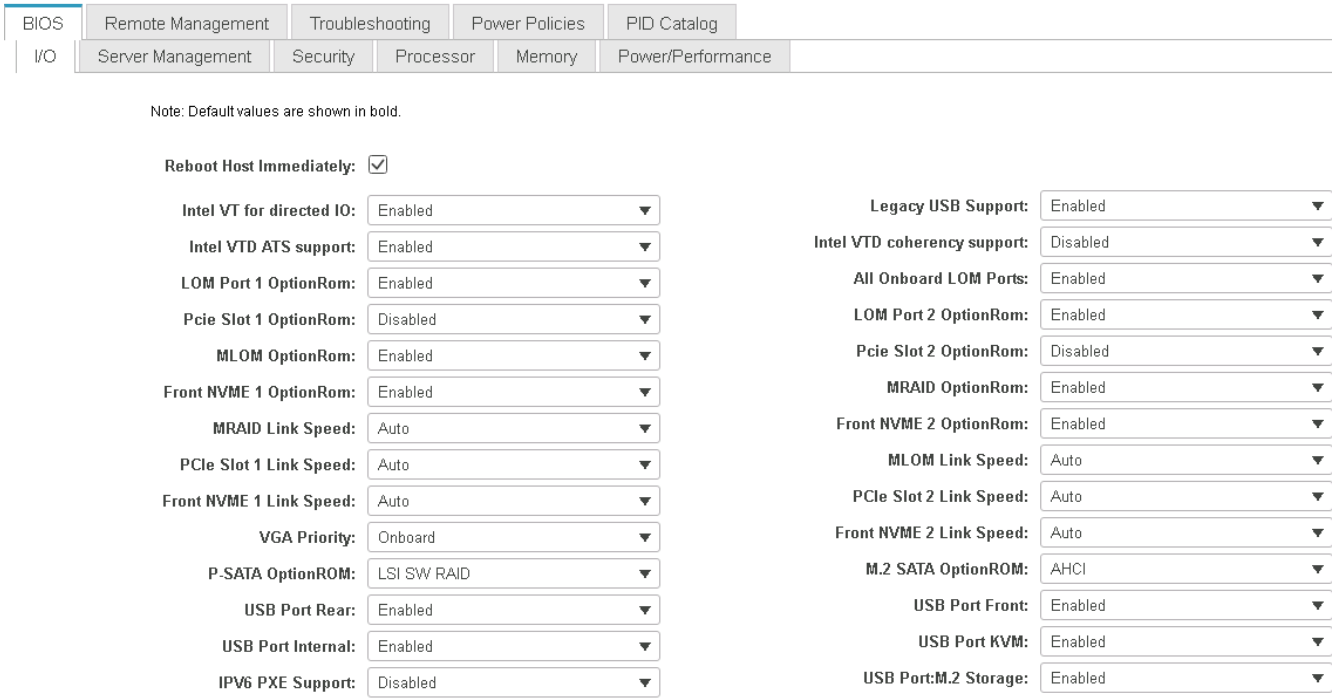


6. Reinicie el servidor para arrancar con el nuevo orden de inicio.

Desactivar la controladora RAID (si existe)

Siga estos pasos si el servidor C-Series contiene una controladora RAID. No se necesita una controladora RAID en el arranque desde la configuración SAN. De manera opcional, también puede quitar físicamente la controladora RAID del servidor.

1. Haga clic en BIOS en el panel de navegación izquierdo de CIMC.
2. Seleccione Configurar BIOS.
3. Desplácese hacia abajo hasta la ranura PCIe:ROM de opción HBA.
4. Si el valor no está desactivado, configúrelo en Desactivado.



Configure Cisco VIC1387 para el arranque iSCSI

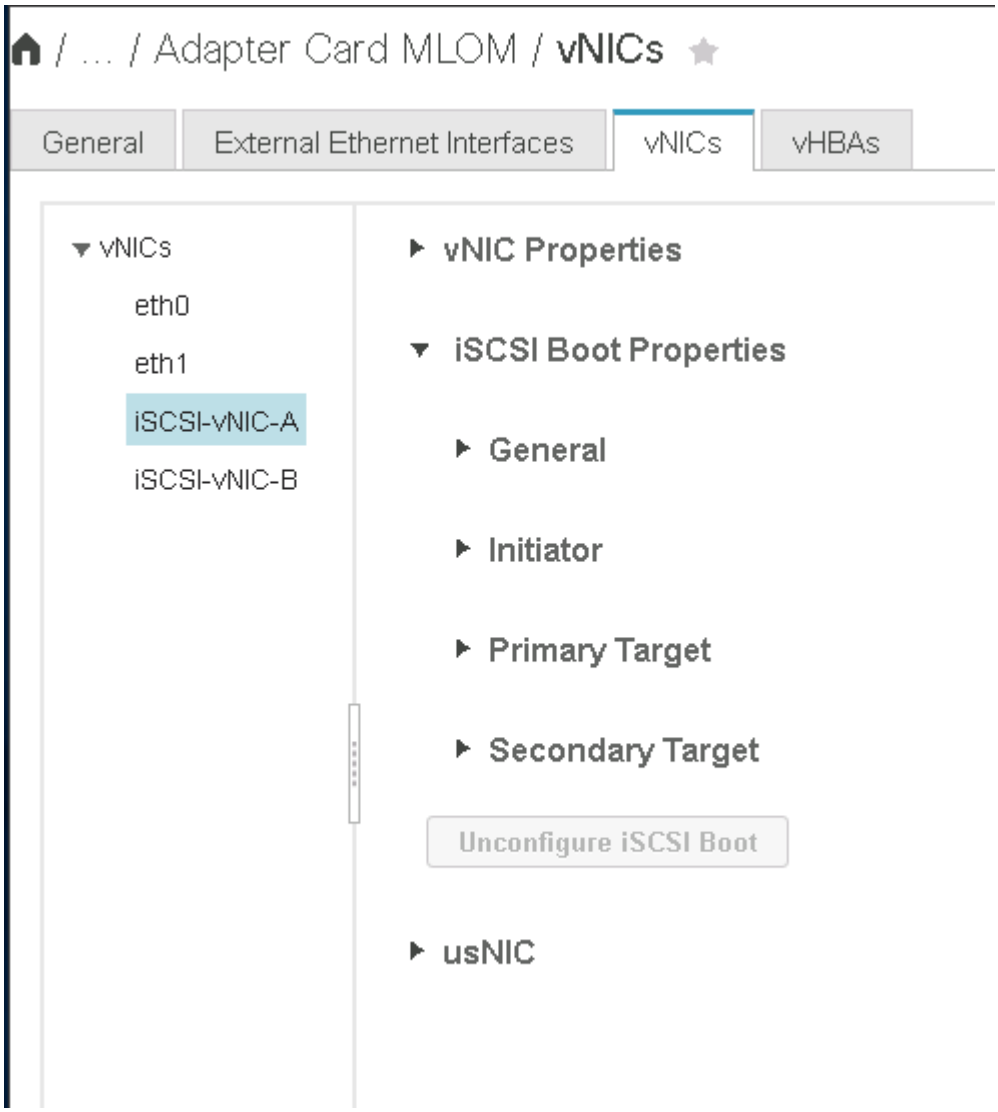
Los pasos de configuración siguientes son para el VIC 1387 de Cisco para arranque iSCSI.

Cree NIC iSCSI

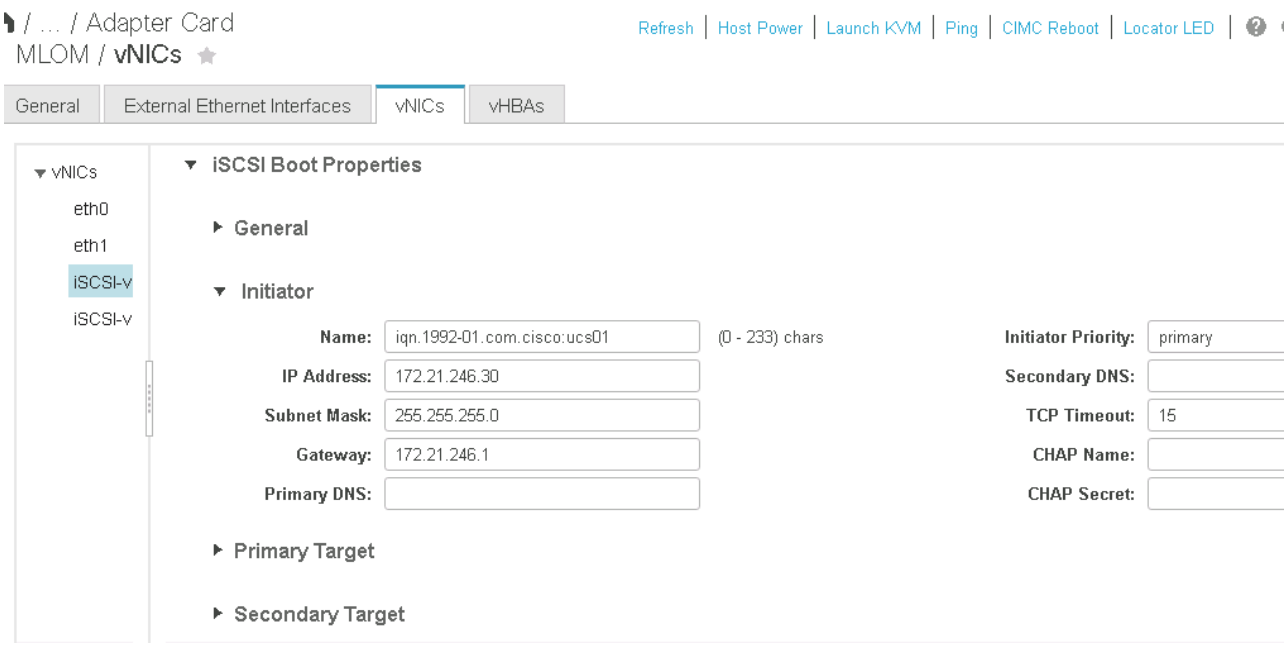
1. Haga clic en Agregar para crear un VNIC.
2. En la sección Agregar VNIC, introduzca los siguientes ajustes:
   - Nombre: ISCSI-VNIC-A
   - MTU: 9000
   - VLAN predeterminada: `<<var_iscsi_vlan_a>>`
   - Modo VLAN: TRONCO
   - Activar inicio PXE: Comprobación



3. Haga clic en Agregar VNIC y, a continuación, en Aceptar.
4. Repita el proceso para agregar un segundo VNIC.
   a. Nombre el VNIC `iSCSI-vNIC-B`.
   b. Introduzca `<<var_iscsi_vlan_b>>` Como VLAN.
   c. Establezca el puerto de enlace ascendente en `1`.
5. Seleccione el VNIC `iSCSI-vNIC-A` a la izquierda.



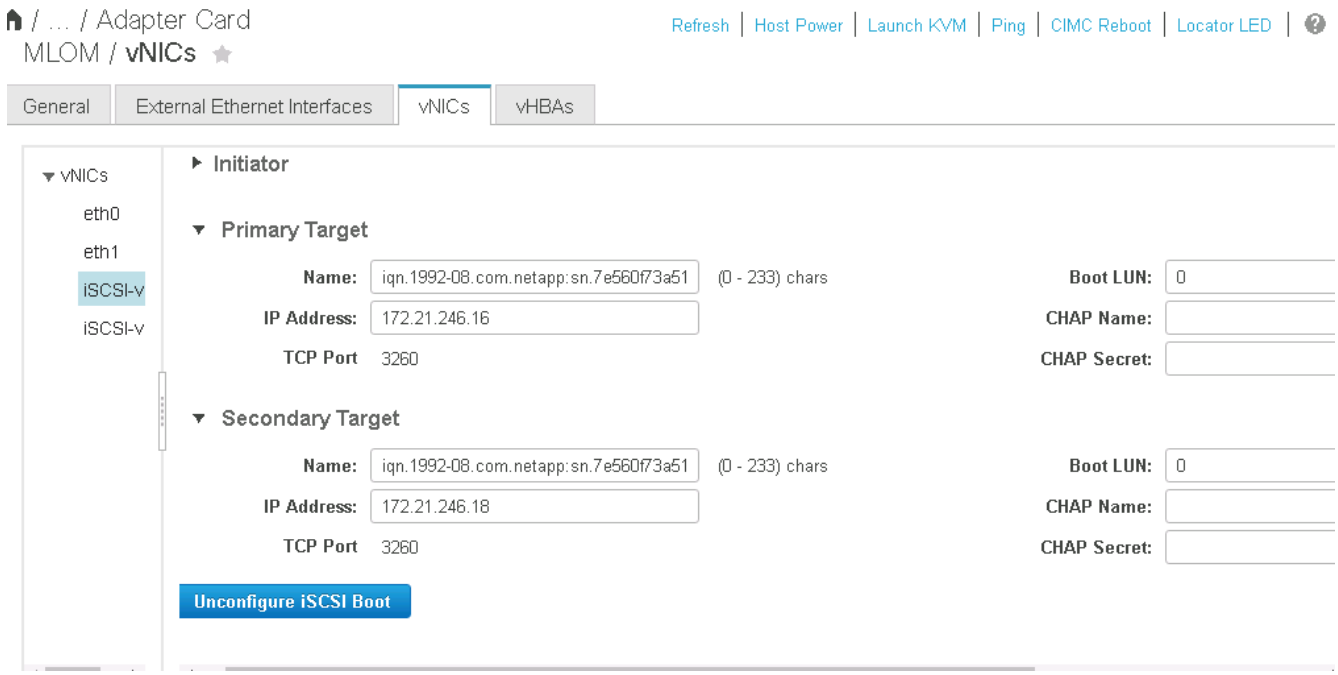
6. En Propiedades de arranque iSCSI, introduzca los detalles del iniciador:
   - Nombre: <<var_ucsa_initiator_name_a>>
   - Dirección IP: <<var_esxi_hostA_iscsiA_ip>>
   - Máscara de subred: <<var_esxi_hostA_iscsiA_mask>>
   - Puerta de enlace: <<var_esxi_hostA_iscsiA_gateway>>



7. Introduzca los detalles del destino principal.
   - Nombre: Número IQN de infra-SVM
   - Dirección IP: Dirección IP de `iscsi_lif01a`
   - LUN de arranque: 0
8. Introduzca los detalles del destino secundario.
   - Nombre: Número IQN de infra-SVM
   - Dirección IP: Dirección IP de `iscsi_lif02a`
   - LUN de arranque: 0

   Puede obtener el número IQN de almacenamiento ejecutando el `vserver iscsi show` comando.

   > Asegúrese de registrar los nombres IQN de cada VNIC. Se necesitan para un paso más adelante.



9. Haga clic en Configurar iSCSI.
10. Seleccione el VNIC `iSCSI-vNIC- B` Y haga clic en el botón de arranque iSCSI que se encuentra en la parte superior de la sección interfaces de Ethernet del host.
11. Repita el proceso para configurar `iSCSI-vNIC-B`.
12. Introduzca los detalles del iniciador.
    - Nombre: `<<var_ucsa_initiator_name_b>>`
    - Dirección IP: `<<var_esxi_hostb_iscsib_ip>>`
    - Máscara de subred: `<<var_esxi_hostb_iscsib_mask>>`
    - Puerta de enlace: `<<var_esxi_hostb_iscsib_gateway>>`
13. Introduzca los detalles del destino principal.
    - Nombre: Número IQN de infra-SVM
    - Dirección IP: Dirección IP de `iscsi_lif01b`
    - LUN de arranque: 0
14. Introduzca los detalles del destino secundario.
    - Nombre: Número IQN de infra-SVM
    - Dirección IP: Dirección IP de `iscsi_lif02b`
    - LUN de arranque: 0

    Puede obtener el número de IQN de almacenamiento mediante el `vserver iscsi show` comando.

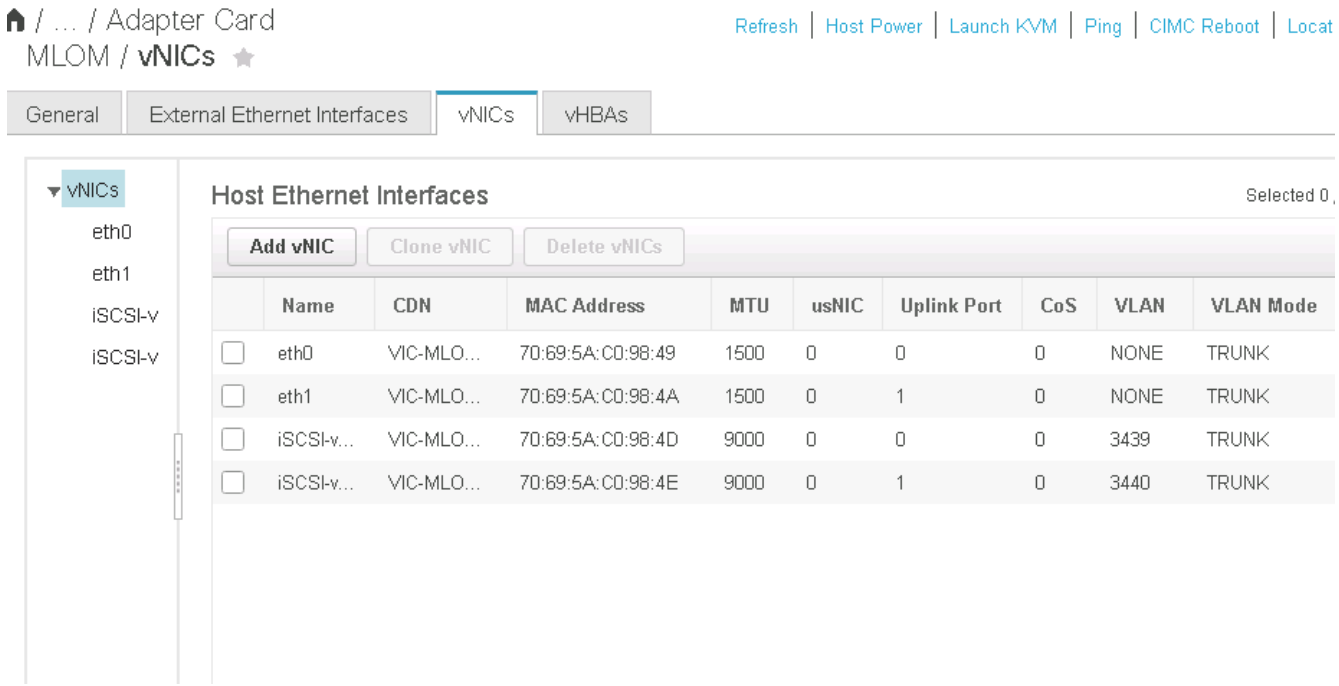
    Asegúrese de registrar los nombres IQN de cada VNIC. Se necesitan para un paso más adelante.

15. Haga clic en Configurar ISCSI.

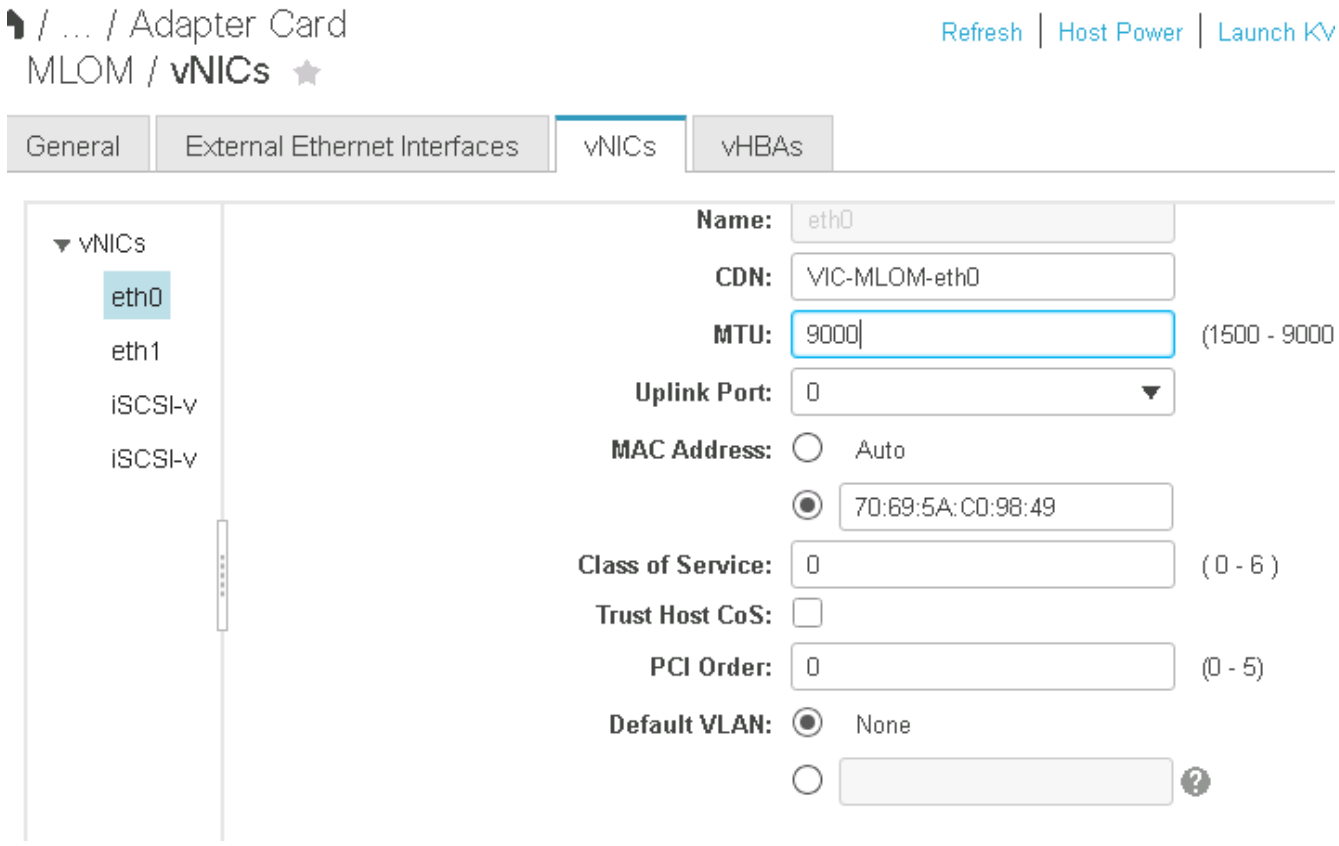
16. Repita este proceso para configurar el arranque iSCSI para el servidor Cisco UCS B.

Configure las NIC virtuales para ESXi

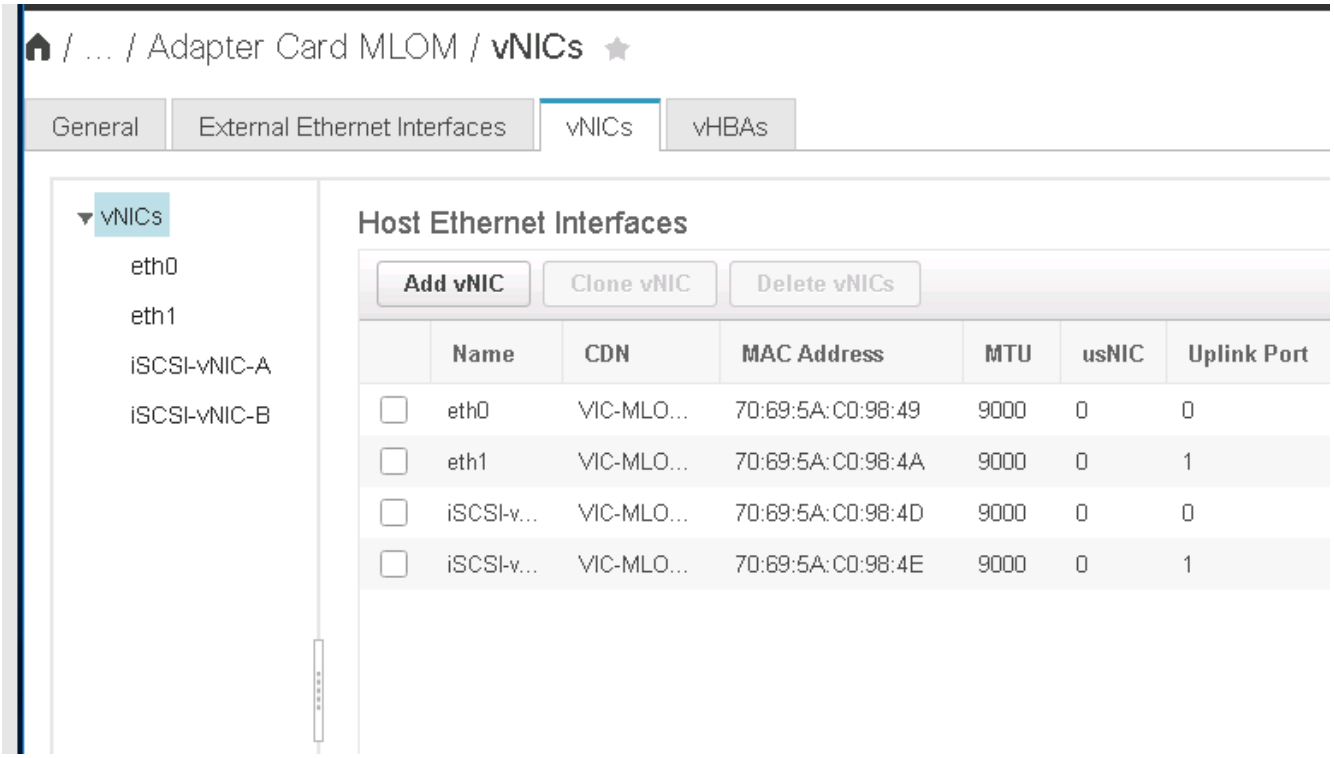
1. En la ventana del navegador de la interfaz CIMC, haga clic en Inventario y, a continuación, en Adaptadores Cisco VIC en el panel derecho.
2. En Tarjetas de adaptador, seleccione Cisco UCS VIC 1387 y, a continuación, seleccione las NIC de abajo.



3. Seleccione eth0 y haga clic en Propiedades.
4. Establezca la MTU en 9000. Haga clic en Save Changes.



5. Repita los pasos 3 y 4 en eth1, comprobando que el puerto de enlace ascendente está configurado en `1` en eth1.



Este procedimiento se debe repetir para cada nodo inicial de Cisco UCS Server y cada nodo adicional de Cisco UCS Server que se agregue al entorno.

"Siguiente: Procedimiento de implementación de almacenamiento AFF de NetApp (parte 2)"

Procedimiento de instalación de almacenamiento AFF de NetApp (parte 2)

Configuración del almacenamiento DE arranque SAN de ONTAP

Cree iGroups iSCSI

Para crear iGroups, complete el paso siguiente:

Para este paso, se necesitan los IQN de iniciadores iSCSI desde la configuración del servidor.

1. Desde la conexión SSH del nodo de gestión del clúster, ejecute los siguientes comandos. Para ver los tres iGroups creados en este paso, ejecute el comando igroup show.

```
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-A –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_a_iSCSI-A_vNIC_IQN>>,
<<var_vm_host_infra_a_iSCSI-B_vNIC_IQN>>
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-B –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_b_iSCSI-A_vNIC_IQN>>,
<<var_vm_host_infra_b_iSCSI-B_vNIC_IQN>>
```

Este paso se debe completar cuando se añaden servidores Cisco UCS C- Series adicionales.

Asigne LUN de arranque a iGroups

Para asignar LUN de arranque a iGroups, ejecute los siguientes comandos desde la conexión SSH de administración del clúster:

```
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra- A –igroup
VM-Host-Infra- A –lun-id 0
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra- B –igroup
VM-Host-Infra- B –lun-id 0
```

Este paso se debe completar cuando se añaden servidores Cisco UCS C-Series adicionales.

"Siguiente: Procedimiento de puesta en marcha de VMware vSphere 6.7."

Procedimiento de puesta en marcha de VMware vSphere 6.7

En esta sección, se proporcionan los procedimientos detallados para la instalación de VMware ESXi 6.7 en una configuración exprés de FlexPod. Los procedimientos de implementación siguientes se personalizan para incluir las variables de entorno descritas en secciones anteriores.

Existen varios métodos para instalar VMware ESXi en dicho entorno. Este procedimiento utiliza la consola

KVM virtual y las funciones de medios virtuales de la interfaz CIMC para servidores Cisco UCS C-Series para asignar medios de instalación remotos a cada servidor individual.

Este procedimiento se debe completar para el servidor Cisco UCS A y el servidor Cisco UCS B.

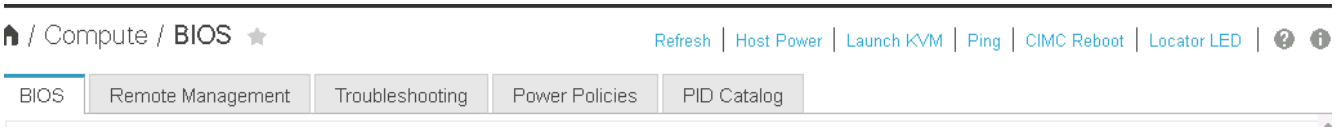
Este procedimiento debe completarse para los nodos adicionales que se añadan al clúster.

Inicie sesión en la interfaz de CIMC para servidores independientes de Cisco UCS C-Series

Los siguientes pasos detallan el método para iniciar sesión en la interfaz de CIMC para servidores independientes Cisco UCS C-Series. Debe iniciar sesión en la interfaz de CIMC para ejecutar el KVM virtual, que permite al administrador iniciar la instalación del sistema operativo a través de medios remotos.

Todos los hosts

1. Desplácese hasta un explorador web e introduzca la dirección IP para la interfaz de CIMC para Cisco UCS C-Series. Este paso inicia la aplicación GUI de CIMC.
2. Inicie sesión en la interfaz de usuario de CIMC con el nombre de usuario y las credenciales de administrador.
3. En el menú principal, seleccione la ficha servidor.
4. Haga clic en Iniciar la consola KVM.



5. En la consola KVM virtual, seleccione la ficha Medios virtuales.
6. Selecciona Mapa CD/DVD.

Es posible que primero tenga que hacer clic en Activar dispositivos virtuales. Seleccione Aceptar esta sesión si se le solicita.

7. Desplácese hasta el archivo de imagen ISO del instalador VMware ESXi 6.7 y haga clic en Open. Haga clic en asignar dispositivo.
8. Seleccione el menú de encendido y elija sistema de ciclo de encendido (arranque en frío). Haga clic en Yes.

Instale VMware ESXi

Los siguientes pasos describen cómo instalar VMware ESXi en cada host.

Descargue LA imagen personalizada de ESXI 6.7 Cisco

1. Desplácese hasta la "Página de descarga de VMware vSphere" Para ISO personalizados.
2. Haga clic en Ir a Descargas junto al CD de instalación de la imagen personalizada de Cisco para ESXi 6.7 GA.
3. Descargue la imagen personalizada de Cisco para el CD de instalación de ESXi 6.7 GA (ISO).

Todos los hosts

1. Cuando el sistema arranca, la máquina detecta la presencia del medio de instalación de VMware ESXi.
2. Seleccione el instalador de VMware ESXi en el menú que aparece.

   El instalador se carga. Esto tarda varios minutos.

3. Cuando el instalador haya terminado de cargarse, pulse Intro para continuar con la instalación.
4. Después de leer el contrato de licencia del usuario final, acepte y continúe con la instalación pulsando F11.
5. Seleccione el LUN de NetApp que se configuró anteriormente como disco de instalación para ESXi y pulse Intro para continuar con la instalación.



6. Seleccione la distribución de teclado adecuada y pulse Intro.
7. Introduzca y confirme la contraseña de root y pulse Intro.
8. El instalador le advierte que las particiones existentes se han eliminado en el volumen. Continúe con la instalación pulsando F11. El servidor se reinicia después de la instalación de ESXi.

Configure la red de gestión del host VMware ESXi

Los siguientes pasos describen cómo añadir la red de gestión de cada host VMware ESXi.

Todos los hosts

1. Una vez que el servidor haya terminado de reiniciarse, introduzca la opción de personalizar el sistema pulsando F2.
2. Inicie sesión con root como nombre de inicio de sesión y la contraseña raíz que se introdujo anteriormente durante el proceso de instalación.
3. Seleccione la opción Configure Management Network.
4. Seleccione Adaptadores de red y pulse Intro.
5. Seleccione los puertos deseados para vSwitch0. Pulse Intro.

   Seleccione los puertos que corresponden a eth0 y eth1 en CIMC.



6. Seleccione VLAN (opcional) y presione Enter.
7. Introduzca el identificador de VLAN `<<mgmt_vlan_id>>`. Pulse Intro.
8. En el menú Configurar red de gestión, seleccione Configuración de IPv4 para configurar la dirección IP de la interfaz de gestión. Pulse Intro.
9. Utilice las teclas de flecha para resaltar establecer dirección IPv4 estática y utilice la barra espaciadora para seleccionar esta opción.
10. Introduzca la dirección IP para gestionar el host VMware ESXi `<<esxi_host_mgmt_ip>>`.
11. Introduzca la máscara de subred para el host VMware ESXi `<<esxi_host_mgmt_netmask>>.`
12. Introduzca la puerta de enlace predeterminada para el host VMware ESXi `<<esxi_host_mgmt_gateway>>`.
13. Pulse Intro para aceptar los cambios en la configuración de IP.
14. Acceda al menú de configuración de IPv6.
15. Utilice la barra de espacio para desactivar IPv6 deseleccionando la opción Habilitar IPv6 (reiniciar requerido). Pulse Intro.
16. Abra el menú para configurar los ajustes de DNS.
17. Dado que la dirección IP se asigna manualmente, la información DNS también debe introducirse manualmente.
18. Introduzca la dirección IP del servidor DNS primario[nameserver_ip].
19. (Opcional) Introduzca la dirección IP del servidor DNS secundario.
20. Introduzca el FQDN para el nombre de host VMware ESXi:[esxi_host_fqdn].
21. Pulse Intro para aceptar los cambios en la configuración de DNS.
22. Salga del submenú Configurar red de administración pulsando Esc.
23. Pulse y para confirmar los cambios y reiniciar el servidor.
24. Cierre la sesión de la consola de VMware pulsando Esc.

Configure el host ESXi

Necesita la información de la siguiente tabla para configurar cada host ESXi.

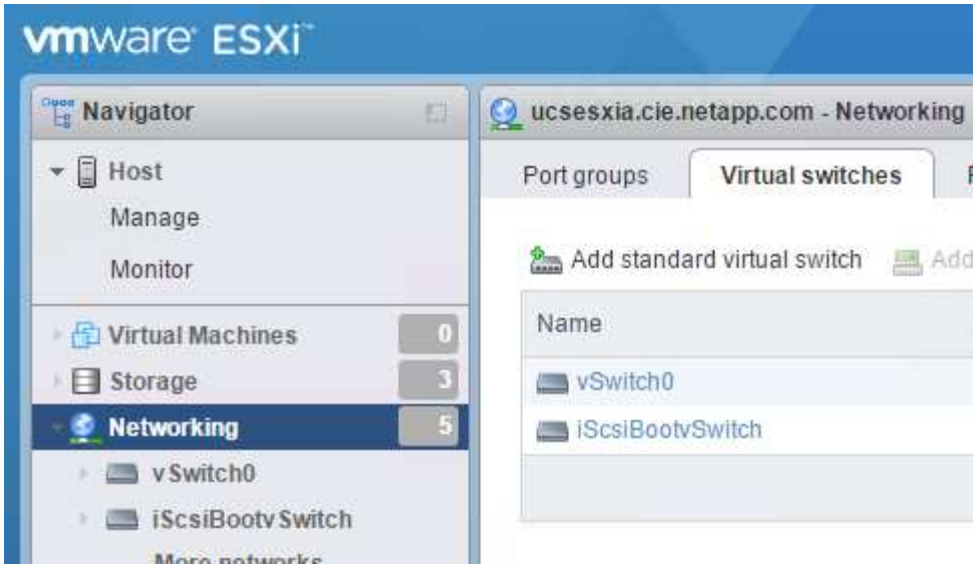
Detalles	Valor
Nombre de host ESXi	
La IP de gestión del host ESXi	
Máscara de gestión de host ESXi	
Pasarela de gestión de host ESXi	
IP NFS del host ESXi	
Máscara de NFS del host ESXi	
Puerta de enlace NFS del host ESXi	
Host ESXi IP de vMotion	
Máscara de vMotion del host ESXi	
Puerta de enlace vMotion del host ESXi	
Host ESXi iSCSI-A IP	
Máscara iSCSI-A del host ESXi	
Puerta de enlace iSCSI-A del host ESXi	
Host ESXi iSCSI-B IP	
Máscara iSCSI-B del host ESXi	
Puerta de enlace iSCSI-B del host ESXi	

Inicie sesión en el host ESXi

1. Abra la dirección IP de administración del host en un explorador Web.
2. Inicie sesión en el host ESXi con la cuenta raíz y la contraseña que especificó durante el proceso de instalación.
3. Lea la declaración sobre el Programa de mejora de la experiencia del cliente de VMware. Después de seleccionar la respuesta correcta, haga clic en Aceptar.

Configurar el arranque iSCSI

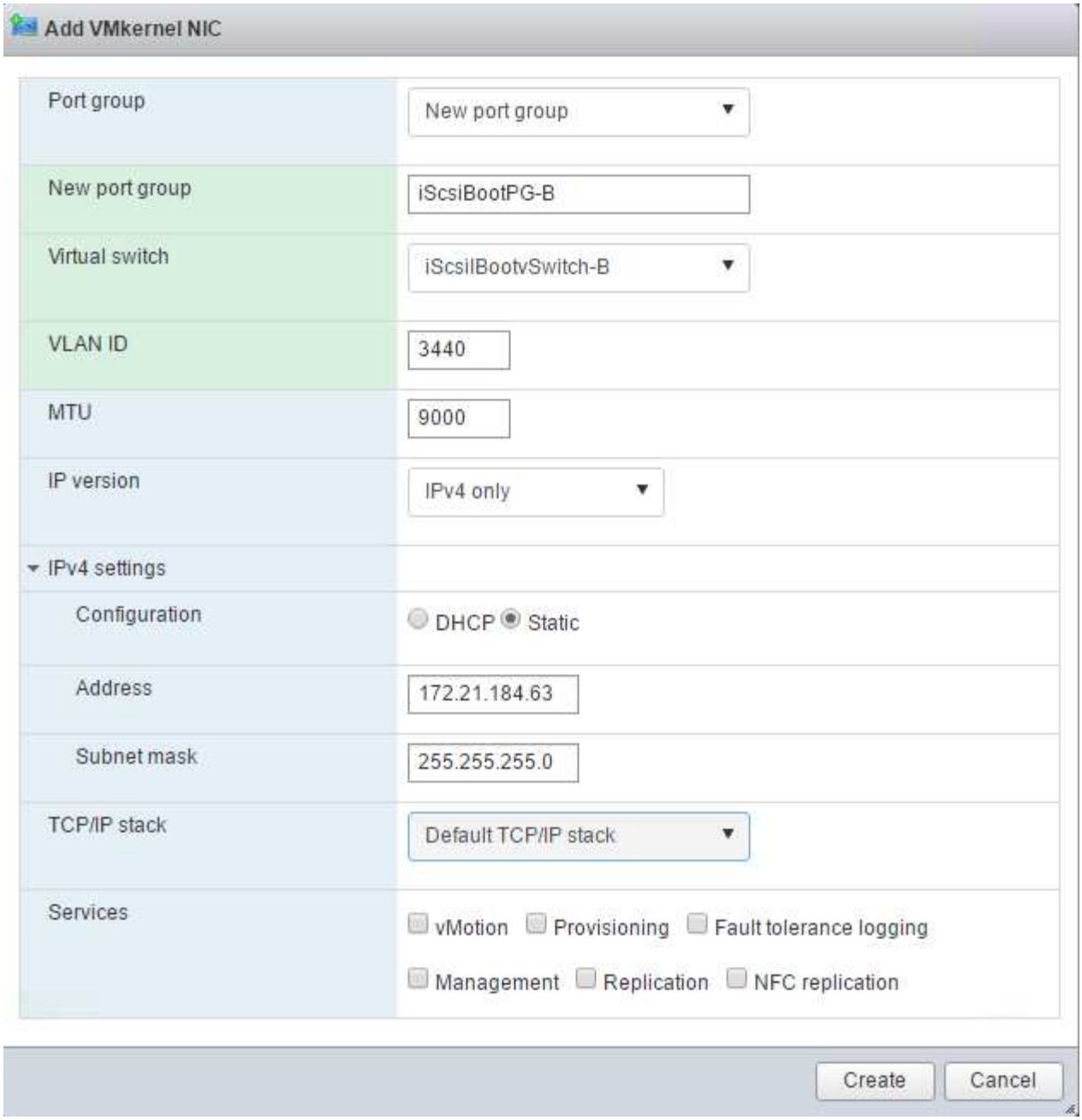
1. Seleccione Networking a la izquierda.
2. A la derecha, seleccione la ficha Switches virtuales.



3. Haga clic en iScsiBootvSwitch.
4. Seleccione Editar configuración.
5. Cambie la MTU a 9000 y haga clic en Save.
6. Haga clic en redes en el panel de navegación de la izquierda para volver a la ficha Switches virtuales.
7. Haga clic en Agregar conmutador virtual estándar.
8. Escriba el nombre `iScsiBootvSwitch-B` Para el nombre de vSwitch.
   - Establezca la MTU en 9000.
   - Seleccione vmnic3 en las opciones de Uplink 1.
   - Haga clic en Añadir.

> En esta configuración, se utilizan Vmnic2 y vmnic3 para el arranque iSCSI. Si tiene NIC adicionales en el host ESXi, puede tener distintos números vmnic. Para confirmar qué NIC se utilizan para el arranque iSCSI, haga coincidir las direcciones MAC de las NIC iSCSI de CIMC con los vmnics de ESXi.

9. En el panel central, seleccione la ficha NIC de VMkernel.
10. Seleccione Agregar NIC de VMkernel.
    - Especifique un nuevo nombre de grupo de puertos de `iScsiBootPG-B`.
    - Seleccione iScsiBootvSwitch-B para el conmutador virtual.
    - Introduzca `<<iscsib_vlan_id>>` Para el ID de VLAN.
    - Cambie el MTU a 9000.
    - Expanda Configuración IPv4.
    - Seleccione Configuración estática.
    - Introduzca `<<var_hosta_iscsib_ip>>` Para Dirección.
    - Introduzca `<<var_hosta_iscsib_mask>>` Para Máscara de subred.
    - Haga clic en Crear.

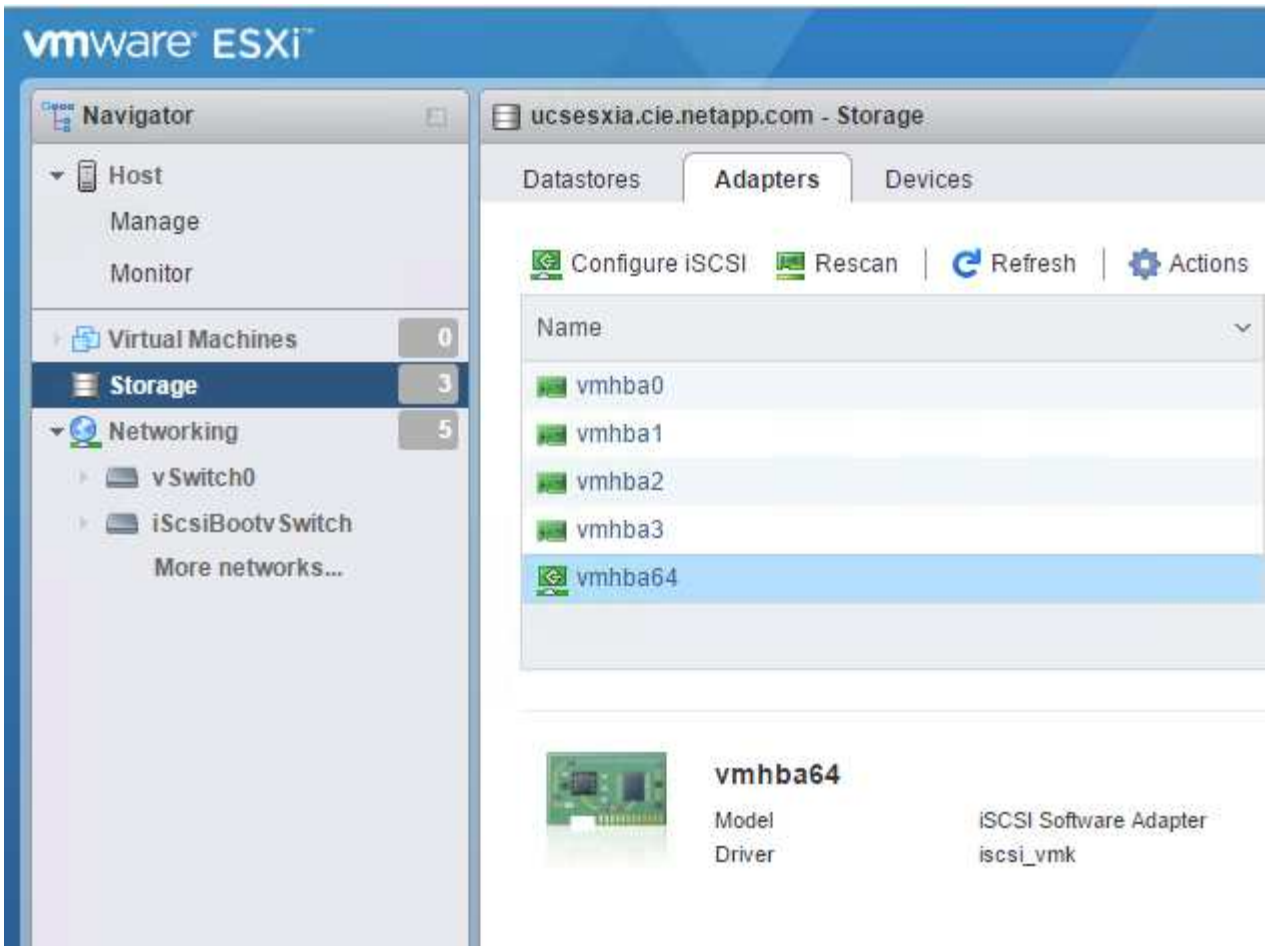


Establezca la MTU en 9000 on `iScsiBootPG- A`.

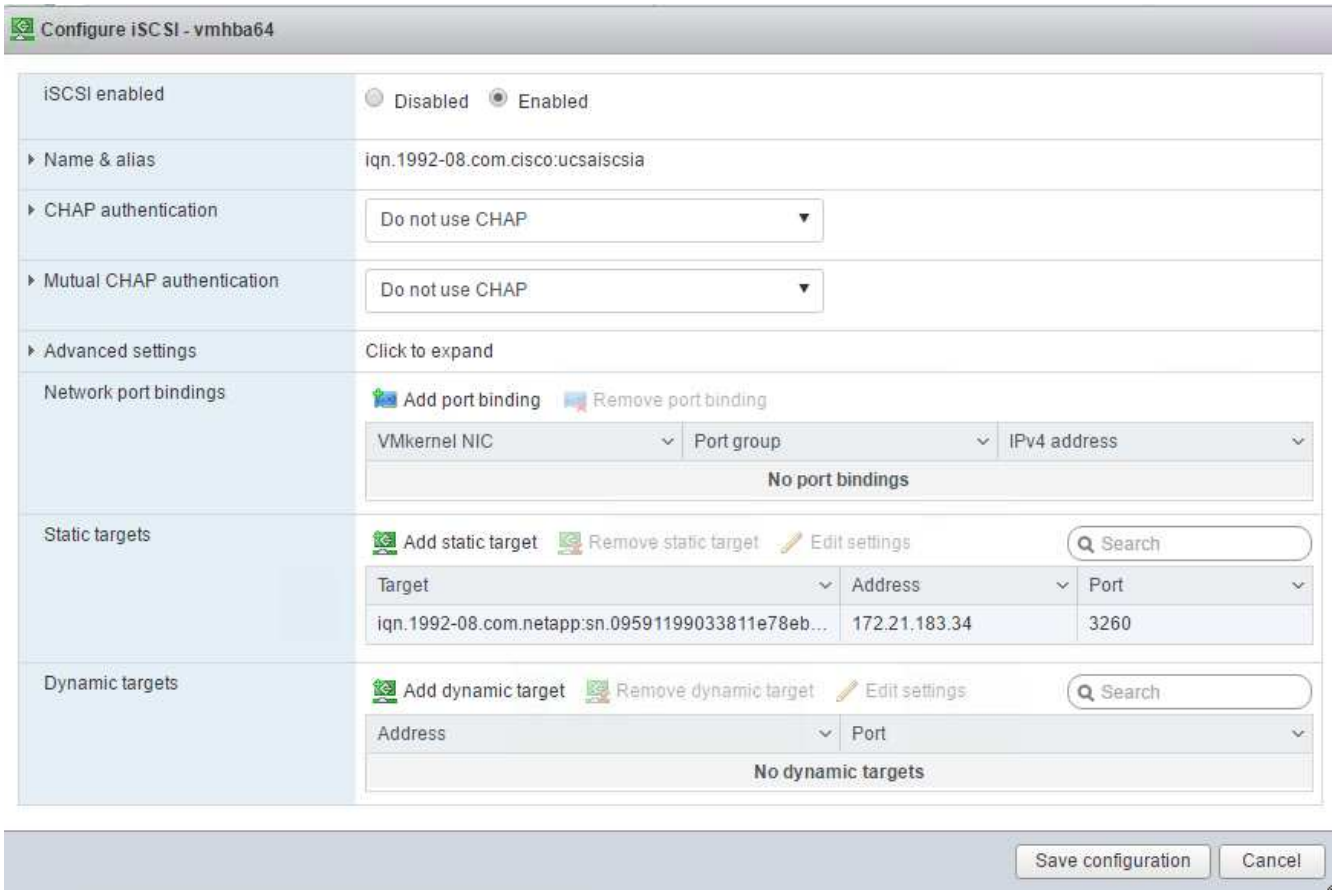
Configuración de accesos múltiples iSCSI

Para configurar la multivía iSCSI en los hosts ESXi, complete los pasos siguientes:

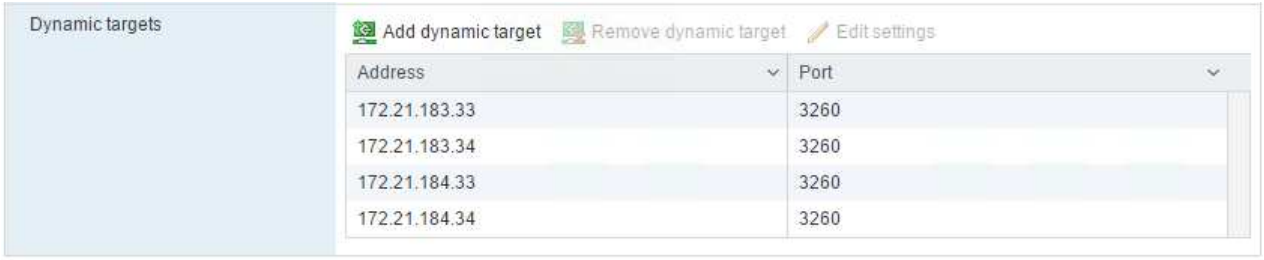
1. Seleccione Storage en el panel de navegación de la izquierda. Haga clic en Adaptadores.
2. Seleccione el adaptador de software iSCSI y haga clic en Configurar iSCSI.



3. En Destinos dinámicos, haga clic en Agregar destino dinámico.



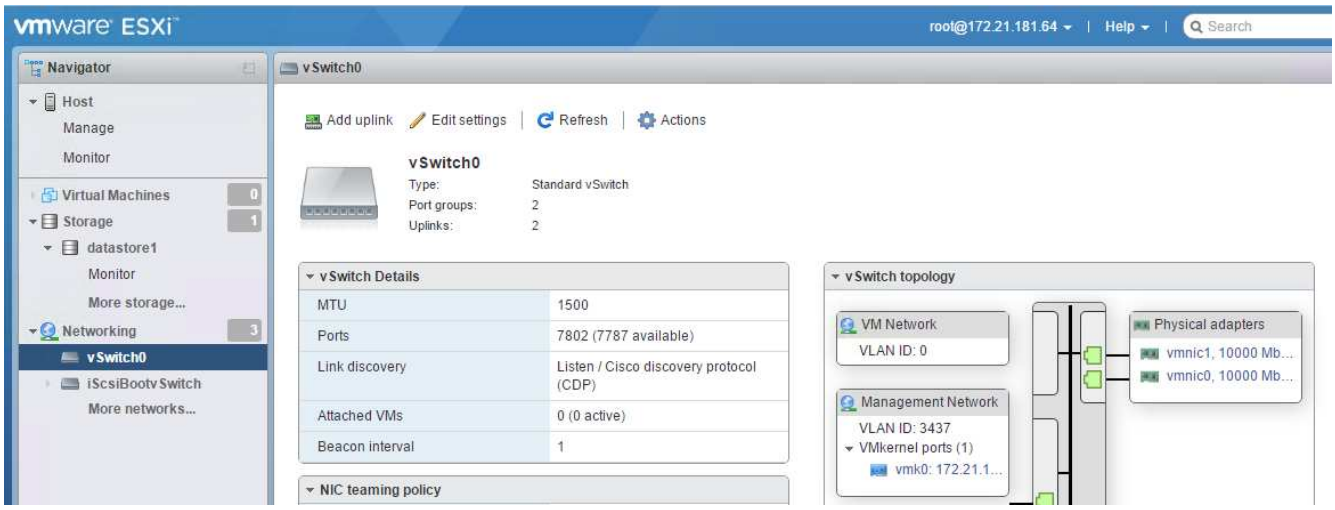
4. Introduzca la dirección IP `iscsi_lif01a`.
   - Repita el proceso con las direcciones IP `iscsi_lif01b`, `iscsi_lif02a`, y. `iscsi_lif02b`.
   - Haga clic en Save Configuration.



Para encontrar las direcciones IP de LIF iSCSI, ejecute el comando "network interface show "en el clúster de NetApp o consulte la pestaña Network interfaces en OnCommand System Manager.

Configure el host ESXi

1. En el panel de navegación de la izquierda, seleccione Networking.
2. Seleccione vSwitch0.



3. Seleccione Editar configuración.
4. Cambie el MTU a 9000.
5. Expanda NIC Teaming y verifique que tanto vmnic0 como vmnic1 estén definidos en activo.

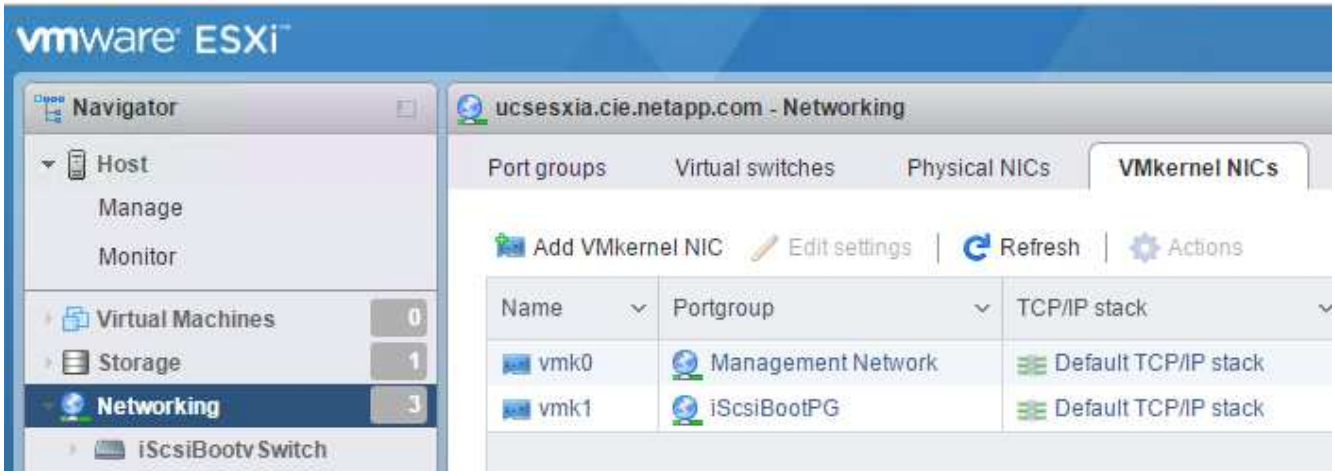
Configurar grupos de puertos y NIC de VMkernel

1. En el panel de navegación de la izquierda, seleccione Networking.
2. Haga clic con el botón derecho en la pestaña grupos de puertos.

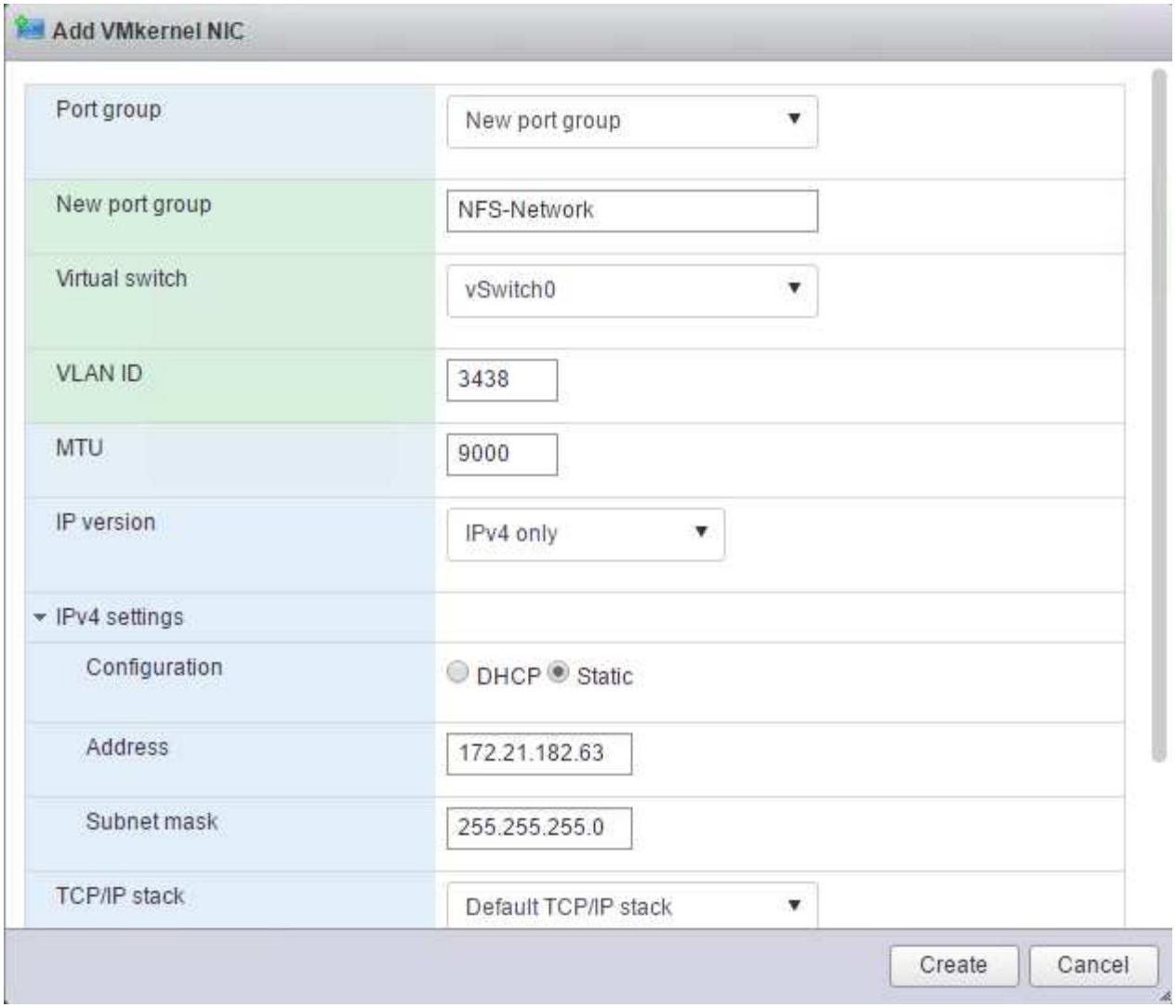


3. Haga clic con el botón derecho en VM Network y seleccione Edit. Cambie el ID de VLAN a. `<<var_vm_traffic_vlan>>`.
4. Haga clic en Agregar grupo de puertos.
   - Asigne un nombre al grupo de puertos `MGMT-Network`.
   - Introduzca `<<mgmt_vlan>>` Para el ID de VLAN.
   - Asegúrese de que vSwitch0 esté seleccionado.
   - Haga clic en Añadir.

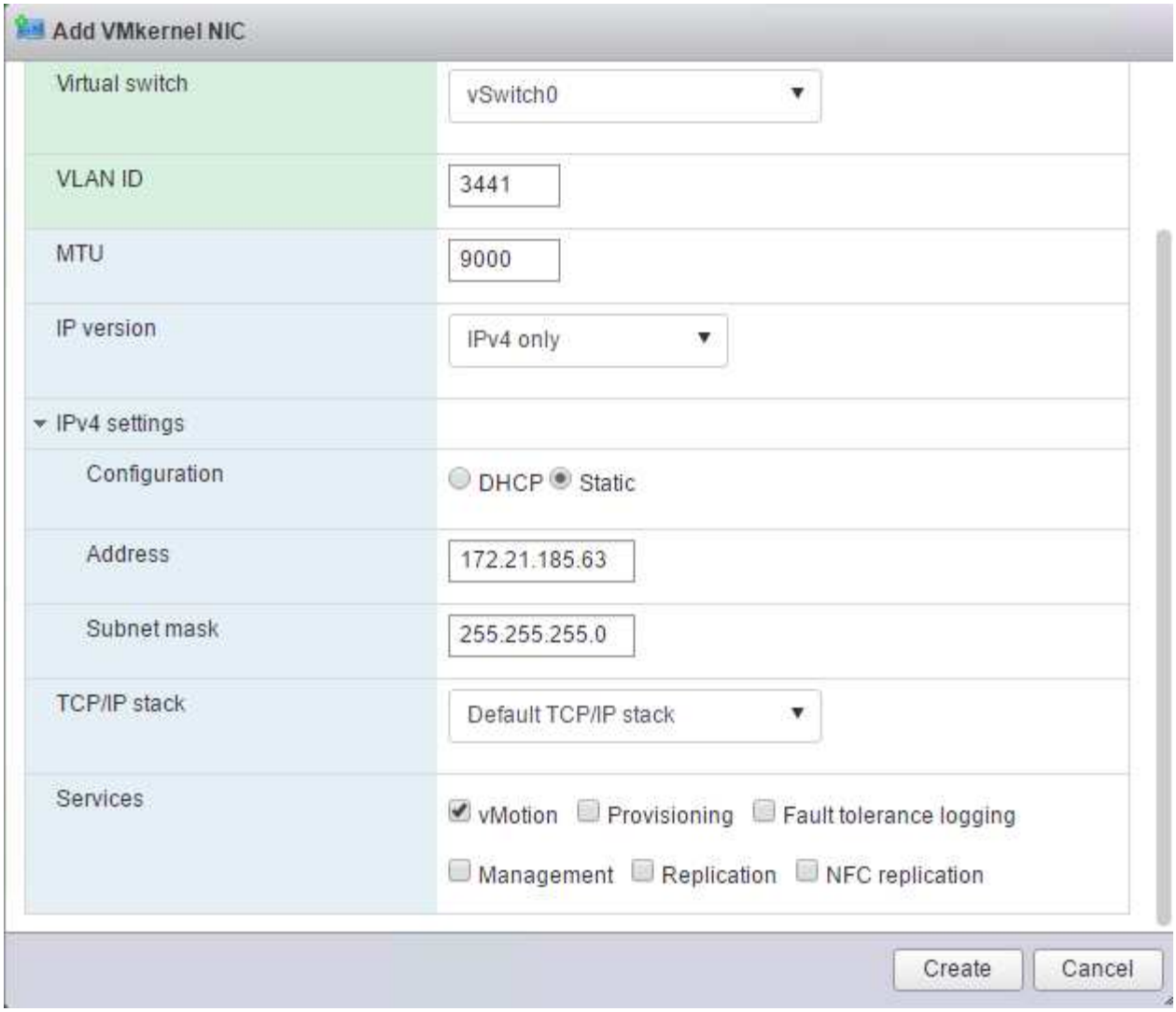
5. Haga clic en la ficha NIC de VMkernel.



6. Seleccione Agregar NIC de VMkernel.
   - Seleccione Nuevo grupo de puertos.
   - Asigne un nombre al grupo de puertos `NFS-Network`.
   - Introduzca `<<nfs_vlan_id>>` Para el ID de VLAN.
   - Cambie el MTU a 9000.
   - Expanda Configuración IPv4.
   - Seleccione Configuración estática.
   - Introduzca `<<var_hosta_nfs_ip>>` Para Dirección.
   - Introduzca `<<var_hosta_nfs_mask>>` Para Máscara de subred.
   - Haga clic en Crear.



7. Repita este proceso para crear el puerto VMkernel de vMotion.
8. Seleccione Agregar NIC de VMkernel.
    a. Seleccione Nuevo grupo de puertos.
    b. Asigne un nombre al grupo de puertos vMotion.
    c. Introduzca `<<vmotion_vlan_id>>` Para el ID de VLAN.
    d. Cambie el MTU a 9000.
    e. Expanda Configuración IPv4.
    f. Seleccione Configuración estática.
    g. Introduzca `<<var_hosta_vmotion_ip>>` Para Dirección.
    h. Introduzca `<<var_hosta_vmotion_mask>>` Para Máscara de subred.
    i. Asegúrese de que la casilla de comprobación vMotion esté seleccionada después de IPv4 Settings.

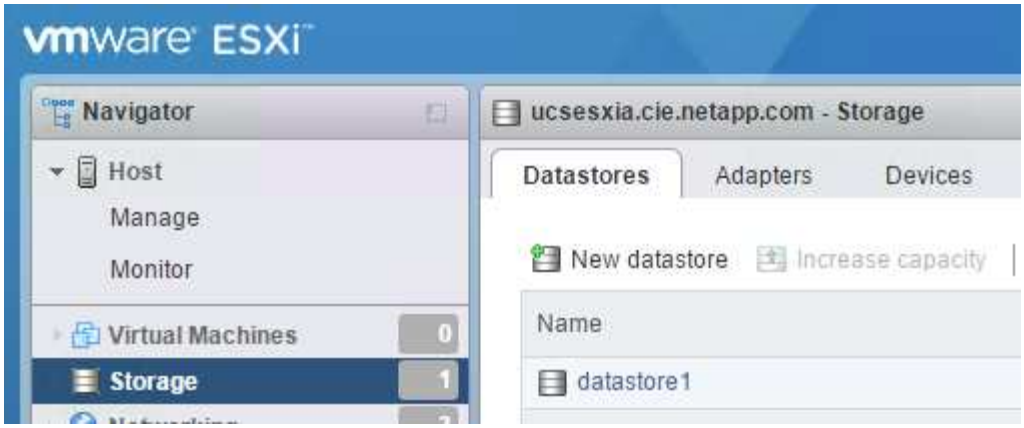


Hay muchas formas de configurar redes ESXi, por ejemplo, mediante el switch distribuido de VMware vSphere si la licencia lo permite. FlexPod Express admite configuraciones de red alternativas si se requieren para satisfacer los requisitos del negocio.

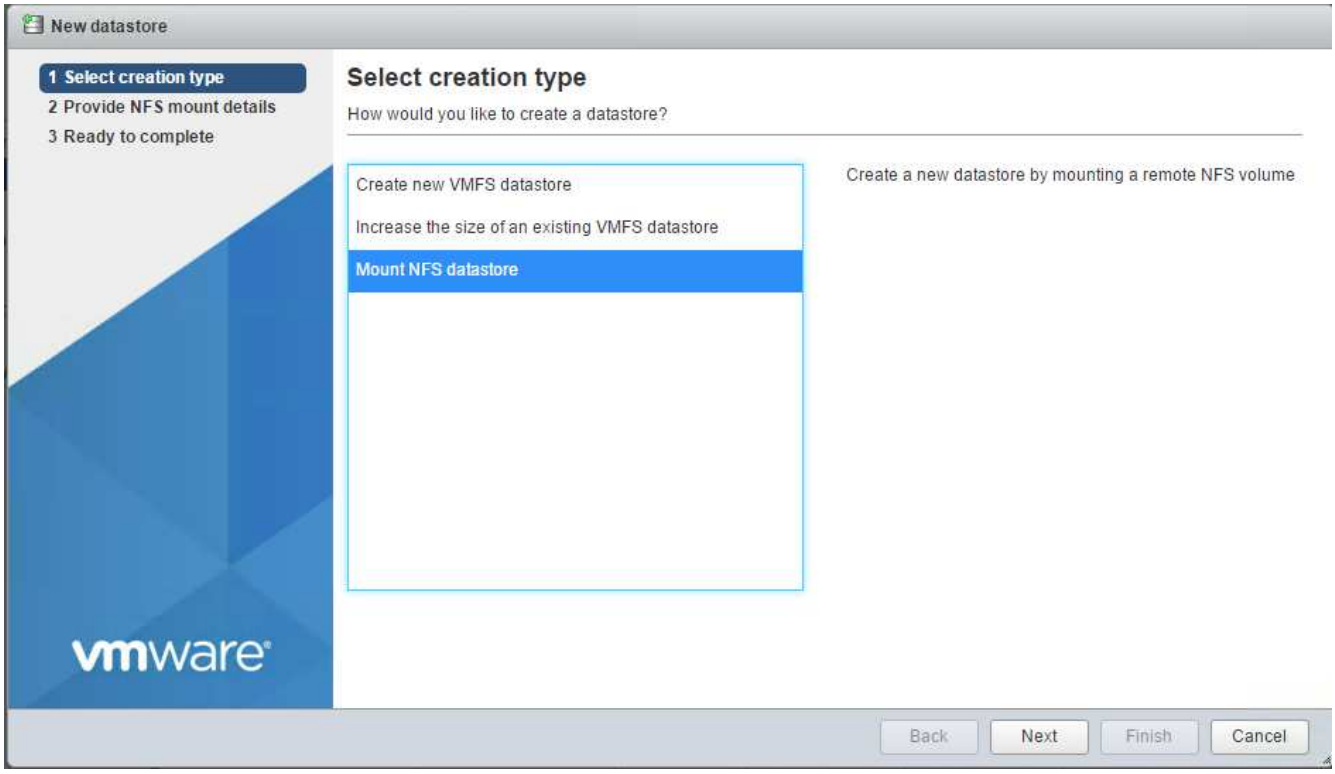
Montaje de los primeros almacenes de datos

Los primeros almacenes de datos que se van a montar son el almacén de datos de infra_datastore_1 para máquinas virtuales y el almacén de datos de infra_swap para archivos de intercambio de máquinas virtuales.

1. Haga clic en Storage en el panel de navegación de la izquierda y después haga clic en New Datastore.



2. Seleccione Mount NFS Datastore.



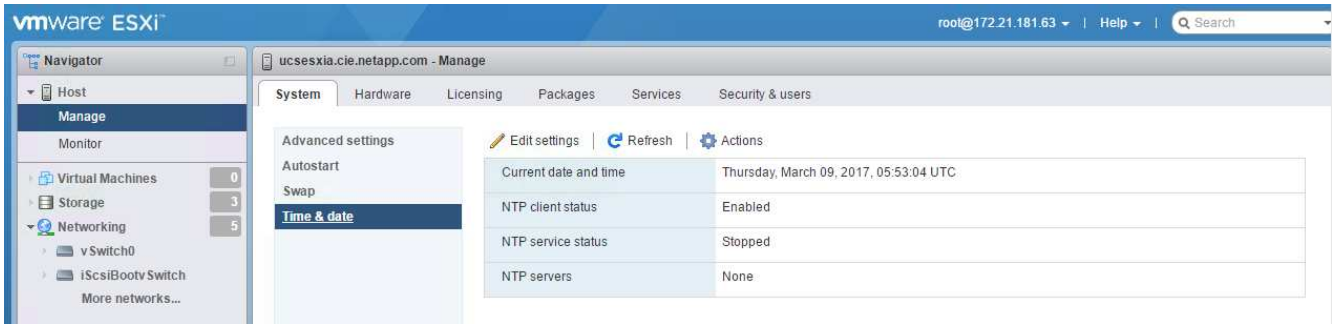
3. A continuación, introduzca la siguiente información en la página Provide NFS Mount Details:
   - Nombre: `infra_datastore_1`
   - Servidor NFS: `<<var_nodea_nfs_lif>>`
   - Compartir: /Infra_datastore_1
   - Asegúrese de que la opción NFS 3 esté seleccionada.
4. Haga clic en Finalizar. Puede ver que la tarea se está completando en el panel tareas recientes.
5. Repita este proceso para montar el almacén de datos infra_swap:
   - Nombre: `infra_swap`
   - Servidor NFS: `<<var_nodea_nfs_lif>>`
   - Compartir: `/infra_swap`

- Asegúrese de que la opción NFS 3 esté seleccionada.

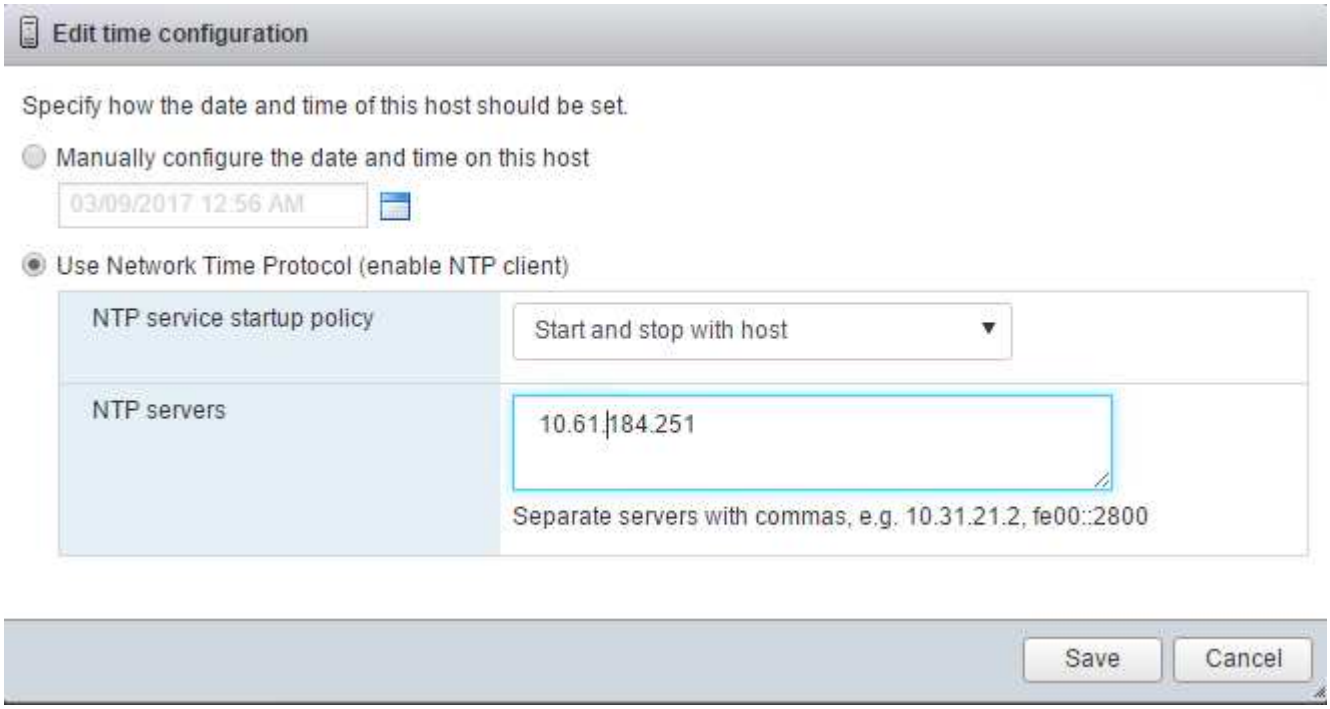
Configure NTP

Para configurar NTP para un host ESXi, complete los siguientes pasos:

1. Haga clic en Administrar en el panel de navegación de la izquierda. Seleccione sistema en el panel derecho y, a continuación, haga clic en Hora y fecha.



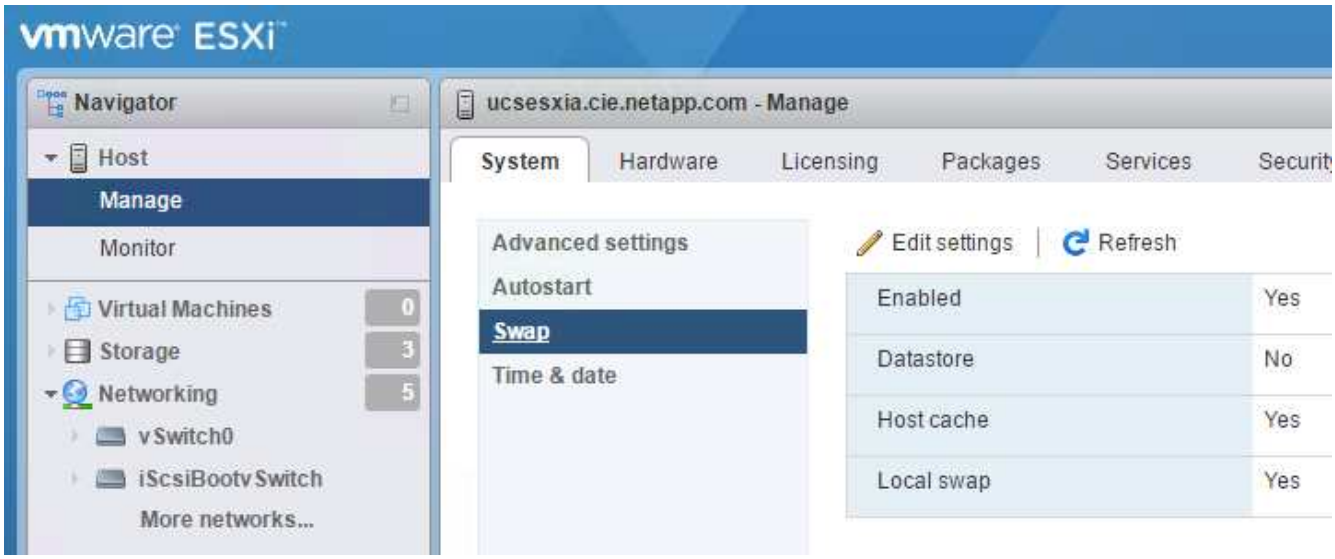
2. Seleccione Use Network Time Protocol (Habilitar cliente NTP).
3. Seleccione Start and Stop with Host como política de inicio del servicio NTP.
4. Introduzca `<<var_ntp>>` Como servidor NTP. Puede establecer varios servidores NTP.
5. Haga clic en Guardar.



Mueva la ubicación del archivo de intercambio de la máquina virtual

Estos pasos proporcionan detalles para mover la ubicación del archivo de intercambio de la máquina virtual.

1. Haga clic en Administrar en el panel de navegación de la izquierda. Seleccione sistema en el panel derecho y, a continuación, haga clic en intercambiar.



2. Haga clic en Editar configuración. Seleccione infra_swap desde las opciones de Datastore.



3. Haga clic en Guardar.

Instale el plugin de NetApp NFS 1.0.20 para VMware VAAI

Para instalar el complemento NFS de NetApp 1.0.20 para VMware VAAI, complete los pasos siguientes.

1. Introduzca los siguientes comandos para verificar que VAAI está habilitado:

```
esxcfg-advcfg -g /DataMover/HardwareAcceleratedMove
esxcfg-advcfg -g /DataMover/HardwareAcceleratedInit
```

   Si VAAI está habilitada, estos comandos generan el siguiente resultado:

```
~ #  esxcfg-advcfg -g /DataMover/HardwareAcceleratedMove
Value of HardwareAcceleratedMove is 1
~ # esxcfg-advcfg -g /DataMover/HardwareAcceleratedInit
Value of HardwareAcceleratedInit is 1
```

2. Si VAAI no está habilitada, introduzca los siguientes comandos para habilitar VAAI:

```
esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedInit
esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedMove
```

Estos comandos generan el siguiente resultado:

```
~ # esxcfg-advcfg -s 1 /Data Mover/HardwareAcceleratedInit
Value of HardwareAcceleratedInit is 1
~ #  esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedMove
Value of HardwareAcceleratedMove is 1
```

3. Descargue el plugin de NetApp NFS para VMware VAAI:
   a. Vaya a la "página de descarga del software".
   b. Desplácese hacia abajo y haga clic en NetApp NFS Plug-in for VMware VAAI.
   c. Seleccione la plataforma ESXi.
   d. Descargue el paquete sin conexión (.zip) o el paquete en línea (.vib) del plugin más reciente.
4. Instale el plugin en el host ESXi mediante la CLI ESX.
5. Reinicie el host ESXI.

```
[root@vm-host-infra-04:~] ls /vmfs/volumes/datastore1/NetAppNasPlugin.vib
/vmfs/volumes/datastore1/NetAppNasPlugin.vib
[root@vm-host-infra-04:~] esxcli software vib install -v /vmfs/volumes/datastore1/NetAppNasPlugin.vib
Installation Result
   Message: The update completed successfully, but the system needs to be rebooted for the changes to be effective.
   Reboot Required: true
   VIBs Installed: NetApp_bootbank_NetAppNasPlugin_1.1.2-3
   VIBs Removed:
   VIBs Skipped:
[root@vm-host-infra-04:~]
```

"Siguiente: Instale VMware vCenter Server 6.7"

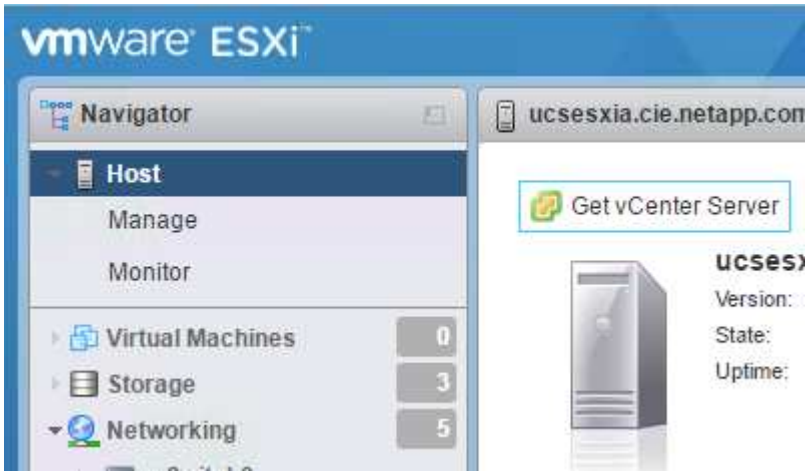
Instale VMware vCenter Server 6.7

En esta sección, se proporcionan los procedimientos detallados para instalar VMware vCenter Server 6.7 en una configuración exprés de FlexPod.

FlexPod Express utiliza el dispositivo de VMware vCenter Server (VCSA).

Descargue el dispositivo VMware vCenter Server

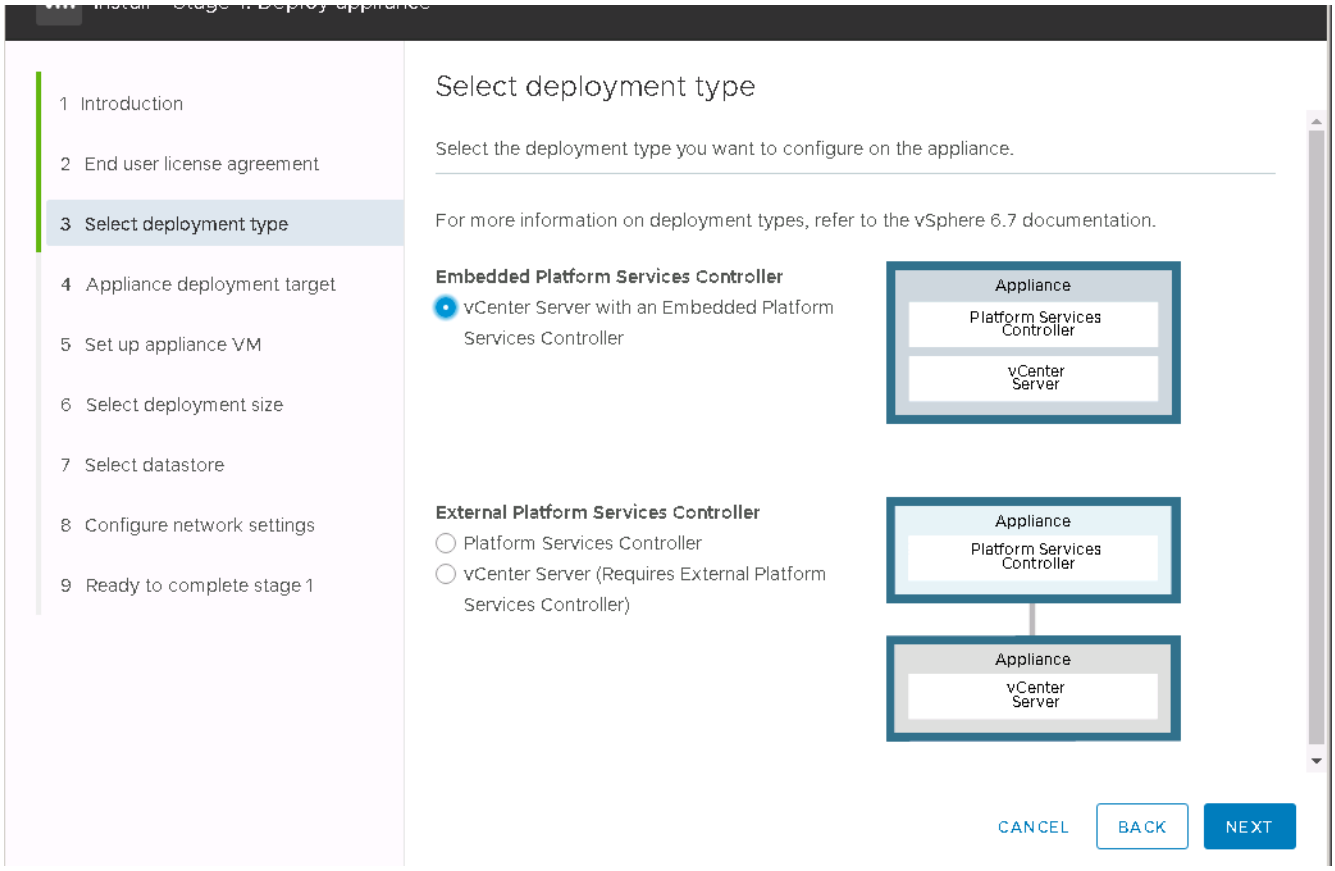
1. Descargue el VCSA. Acceda al enlace de descarga haciendo clic en el icono Get vCenter Server cuando gestione el host ESXi.



2. Descargue el VCSA desde el sitio de VMware.

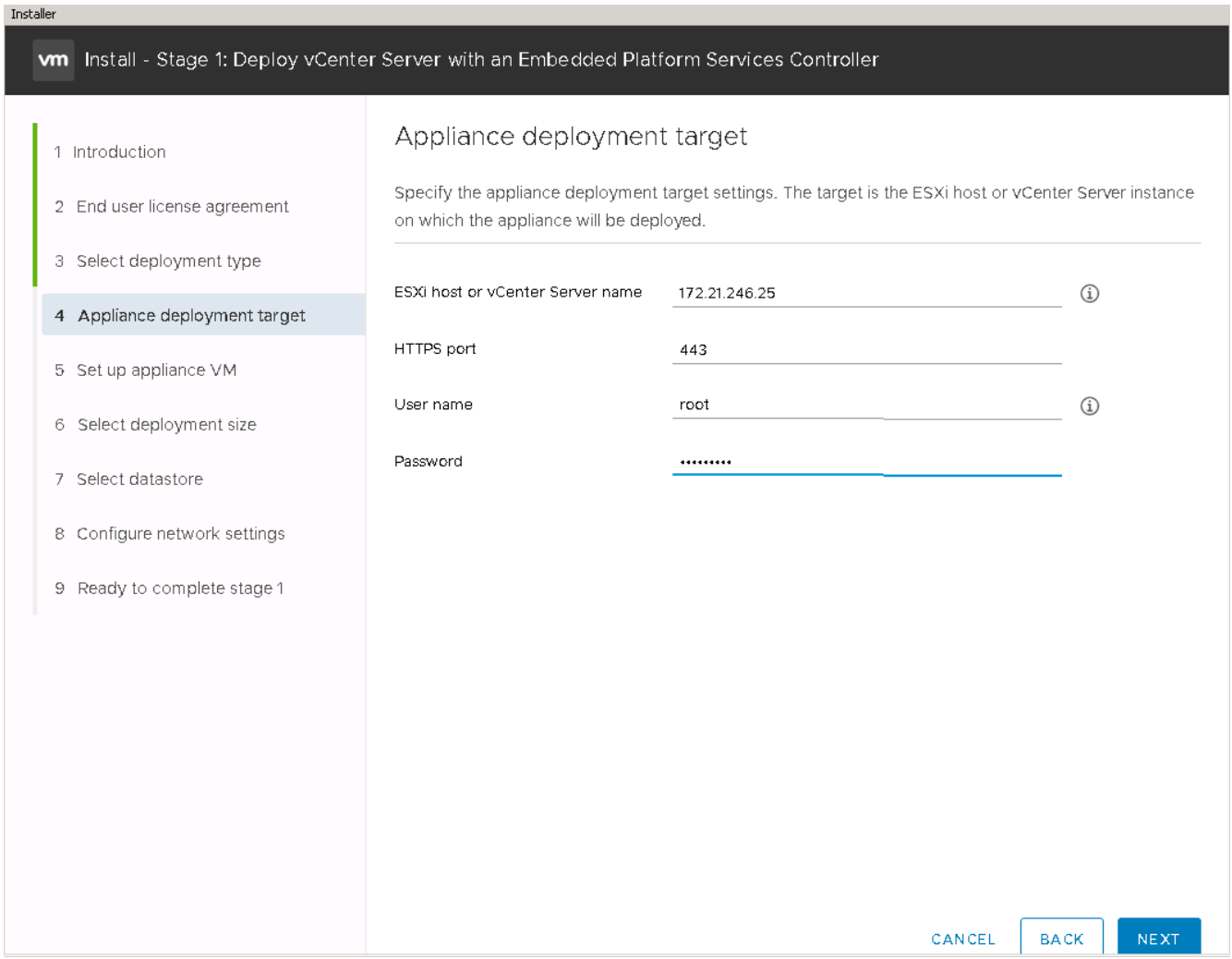
> Aunque se admite la instalación de Microsoft Windows vCenter Server, VMware recomienda VCSA para las nuevas implementaciones.

3. Monte la imagen ISO.
4. Desplácese al directorio vcsa-ui-installer> win32. Haga doble clic en Installer.exe.
5. Haga clic en instalar.
6. Haga clic en Siguiente en la página Introducción.
7. Acepte el acuerdo de licencia para el usuario final.
8. Seleccione Embedded Platform Services Controller (controladora de servicios de plataforma integrada) como tipo de implementación.

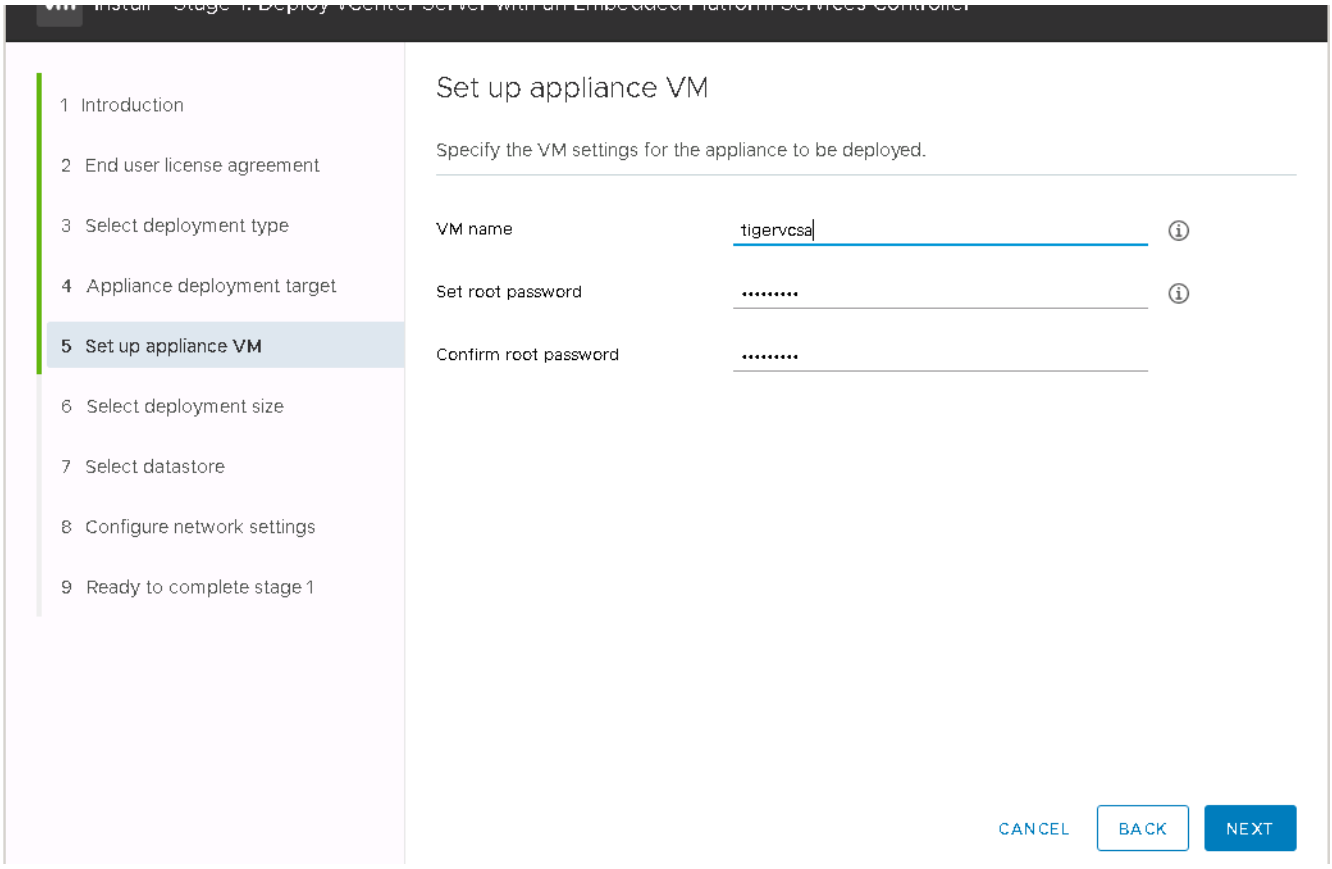


Si es necesario, también admite la puesta en marcha de la controladora de servicios de plataforma externa como parte de la solución FlexPod Express.

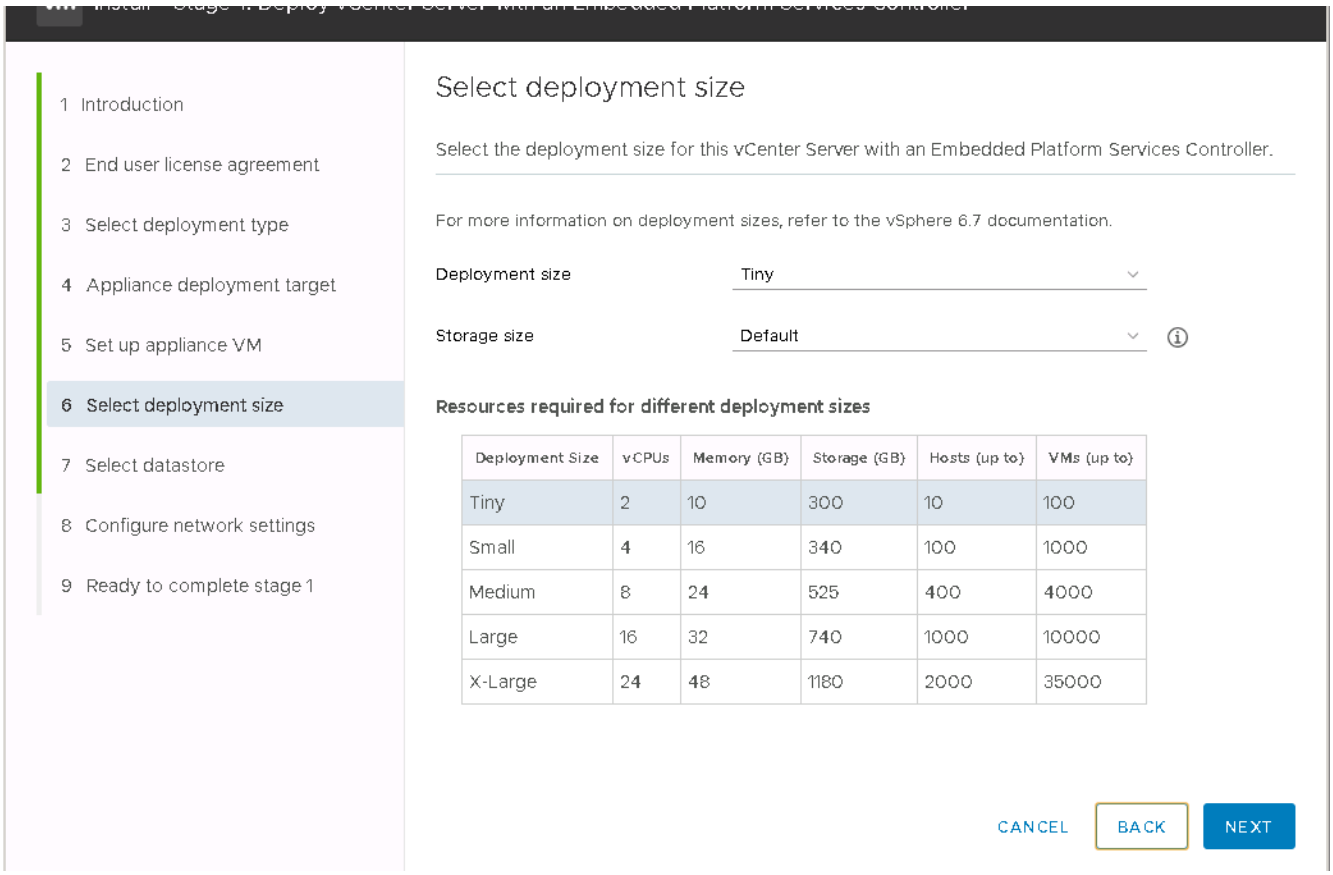
9. En Appliance Deployment Target, introduzca la dirección IP de un host ESXi implementado, así como el nombre de usuario raíz y la contraseña raíz.



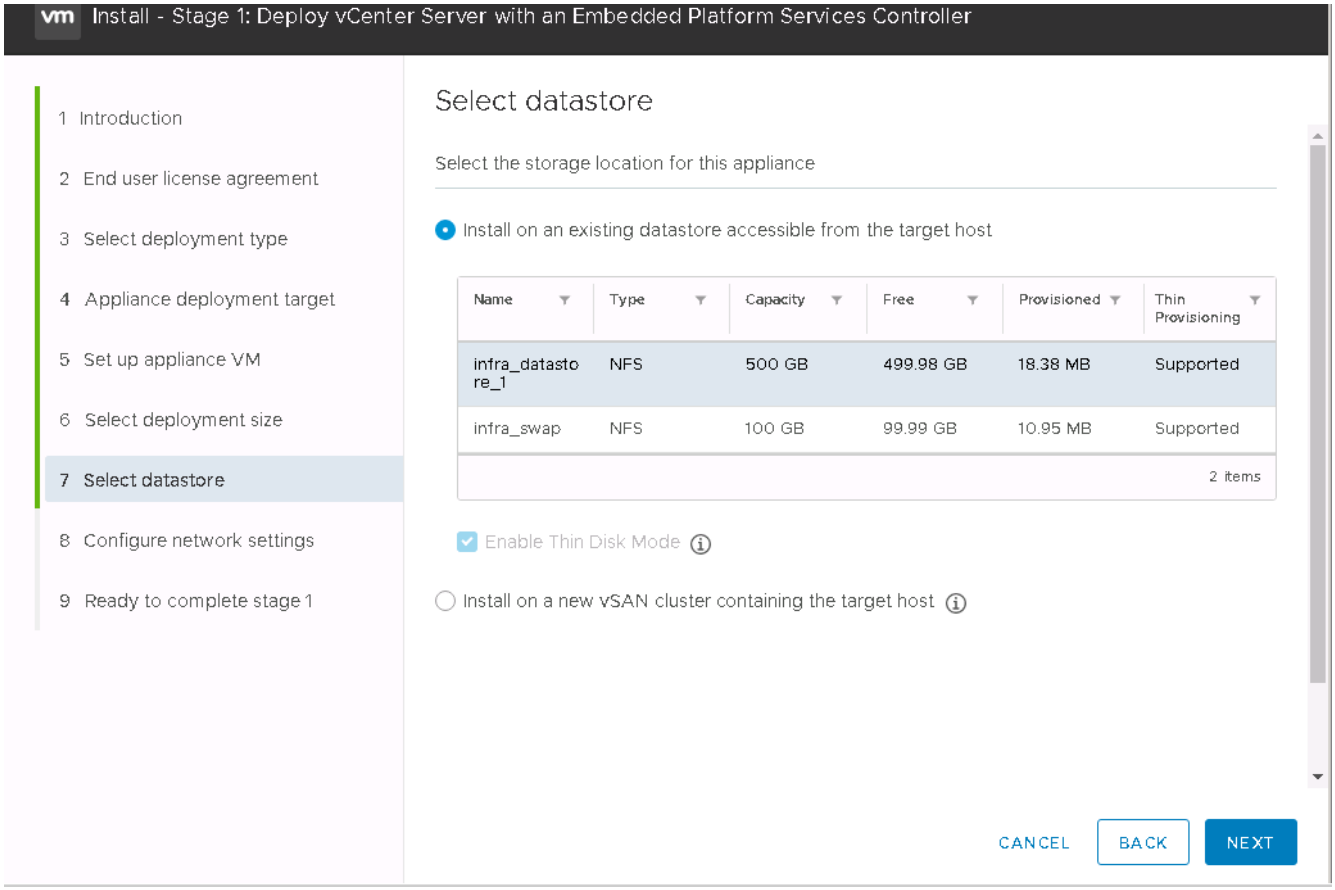
10. Introduzca para establecer la máquina virtual del dispositivo `VCSA` Como el nombre del equipo virtual y la contraseña raíz que desea utilizar para el VCSA.



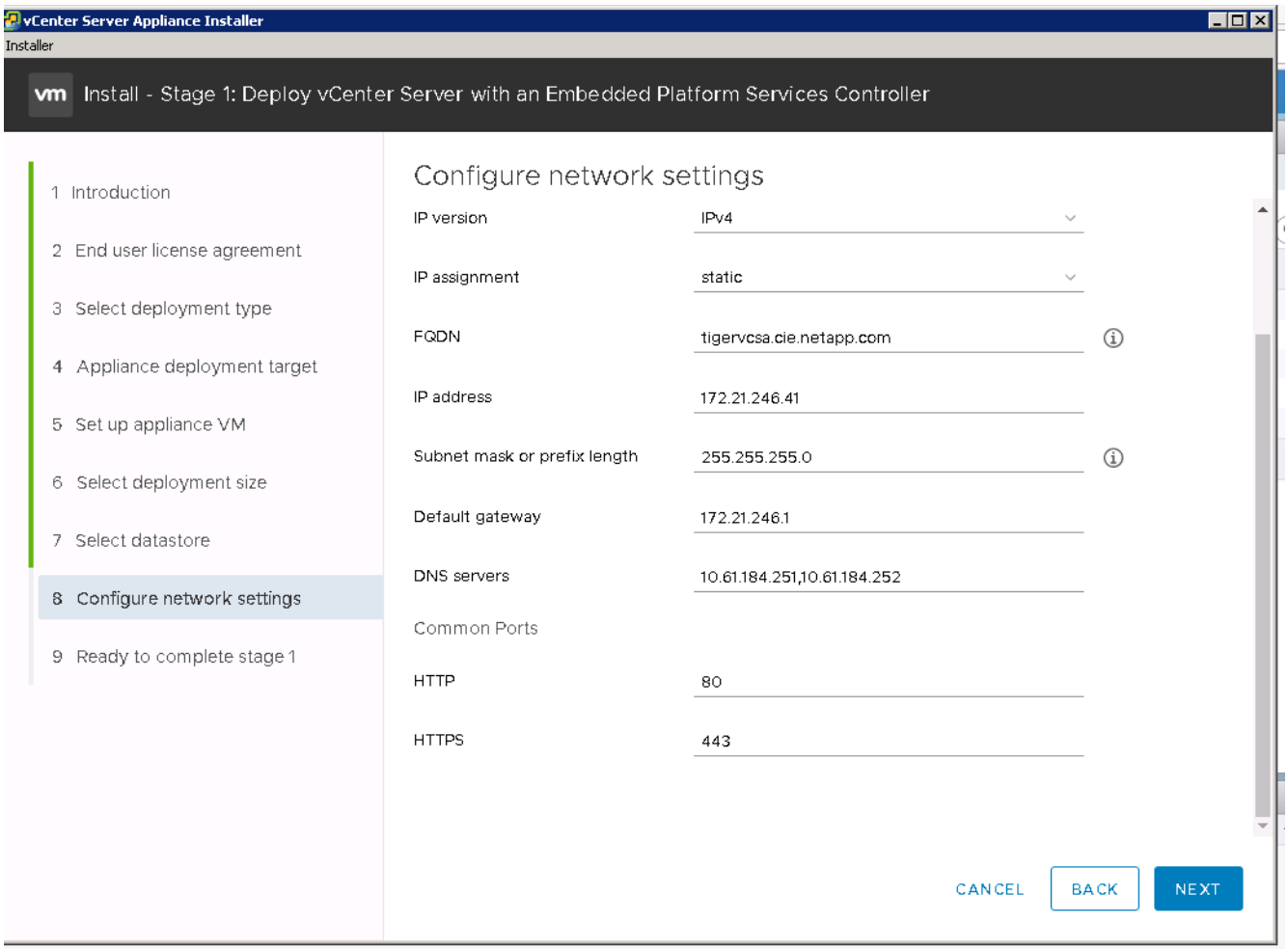
11. Seleccione el tamaño de puesta en marcha que mejor se adapte a su entorno. Haga clic en Siguiente.



12. Seleccione el almacén de datos de infra_datastore_1. Haga clic en Siguiente.

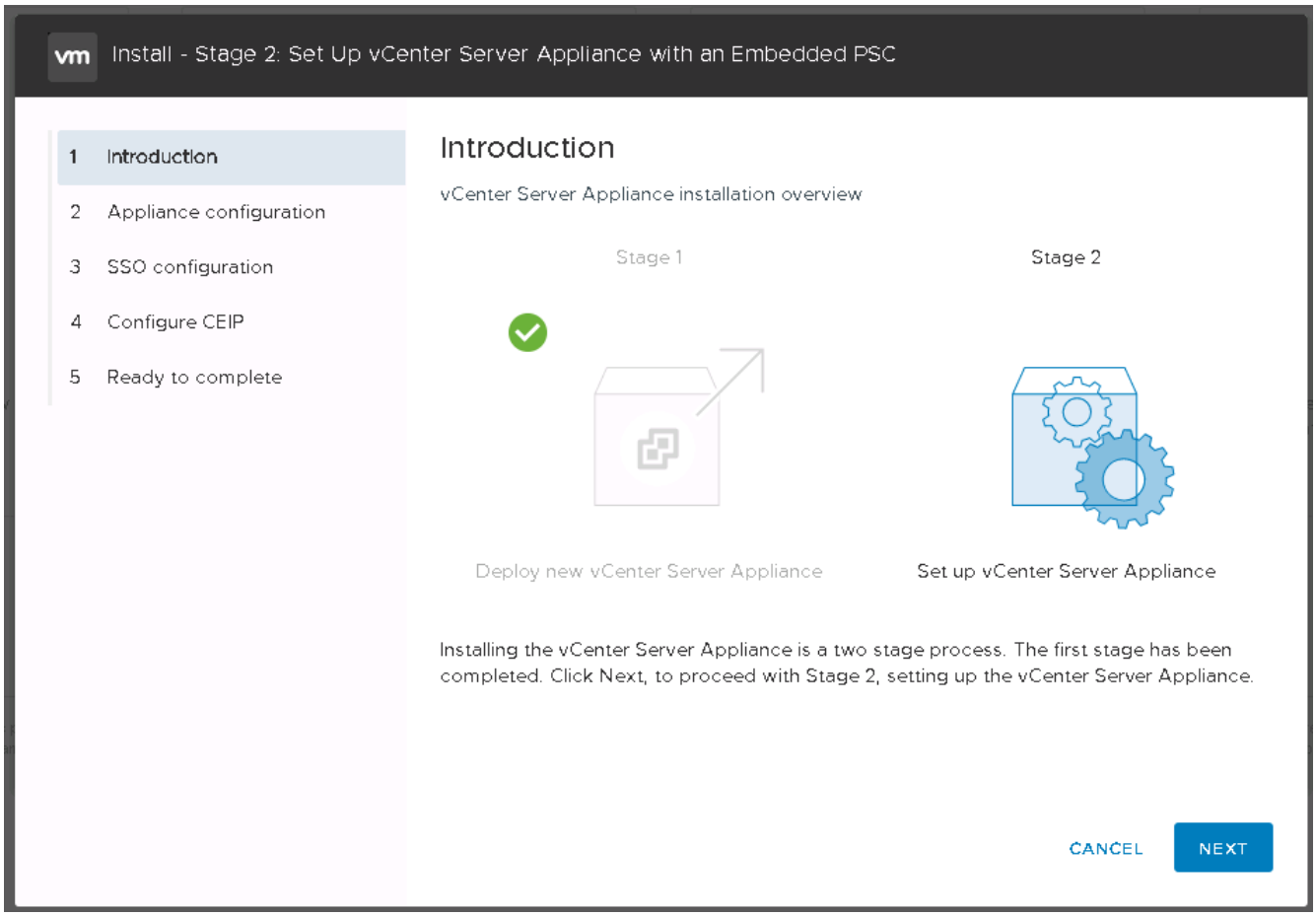


13. Introduzca la siguiente información en la página Configure network settings y haga clic en Next.
    a. Seleccione MGMT-Network para Red.
    b. Introduzca el FQDN o IP que se va a utilizar para la VCSA.
    c. Introduzca la dirección IP que se utilizará.
    d. Introduzca la máscara de subred que desea utilizar.
    e. Introduzca la pasarela predeterminada.
    f. Introduzca el servidor DNS.
14. En la página Ready to Complete Stage 1, compruebe que los ajustes introducidos son correctos. Haga clic en Finalizar.



La VCSA se instala ahora. Este proceso tarda varios minutos.

15. Una vez completada la fase 1, aparece un mensaje que indica que se ha completado. Haga clic en continuar para iniciar la configuración de la fase 2.
16. En la página Introducción de fase 2, haga clic en Siguiente.



17. Introduzca `<<var_ntp_id>>` Para la dirección del servidor NTP. Puede introducir varias direcciones IP de NTP.

    Si tiene pensado utilizar la alta disponibilidad (ha) de vCenter Server, asegúrese de que el acceso SSH esté habilitado.

18. Configure el nombre de dominio, la contraseña y el nombre del sitio de SSO. Haga clic en Siguiente.

    Registre estos valores para la referencia, especialmente si se desvía del nombre de dominio vsphere.local.

19. Únase al programa de experiencia del cliente de VMware si lo desea. Haga clic en Siguiente.
20. Vea el resumen de la configuración. Haga clic en Finalizar o utilice el botón Atrás para editar la configuración.
21. Aparece un mensaje que indica que no podrá detener o detener la instalación una vez iniciada. Haga clic en OK para continuar.

    La configuración del dispositivo continúa. Esto tarda varios minutos.

    Aparece un mensaje que indica que la configuración se ha realizado correctamente.

    Los enlaces que el instalador proporciona para acceder a vCenter Server pueden hacer clic.

"Siguiente: Configure VMware vCenter Server 6.7 y vSphere agrupando en clústeres."

Configure VMware vCenter Server 6.7 y el clustering de vSphere

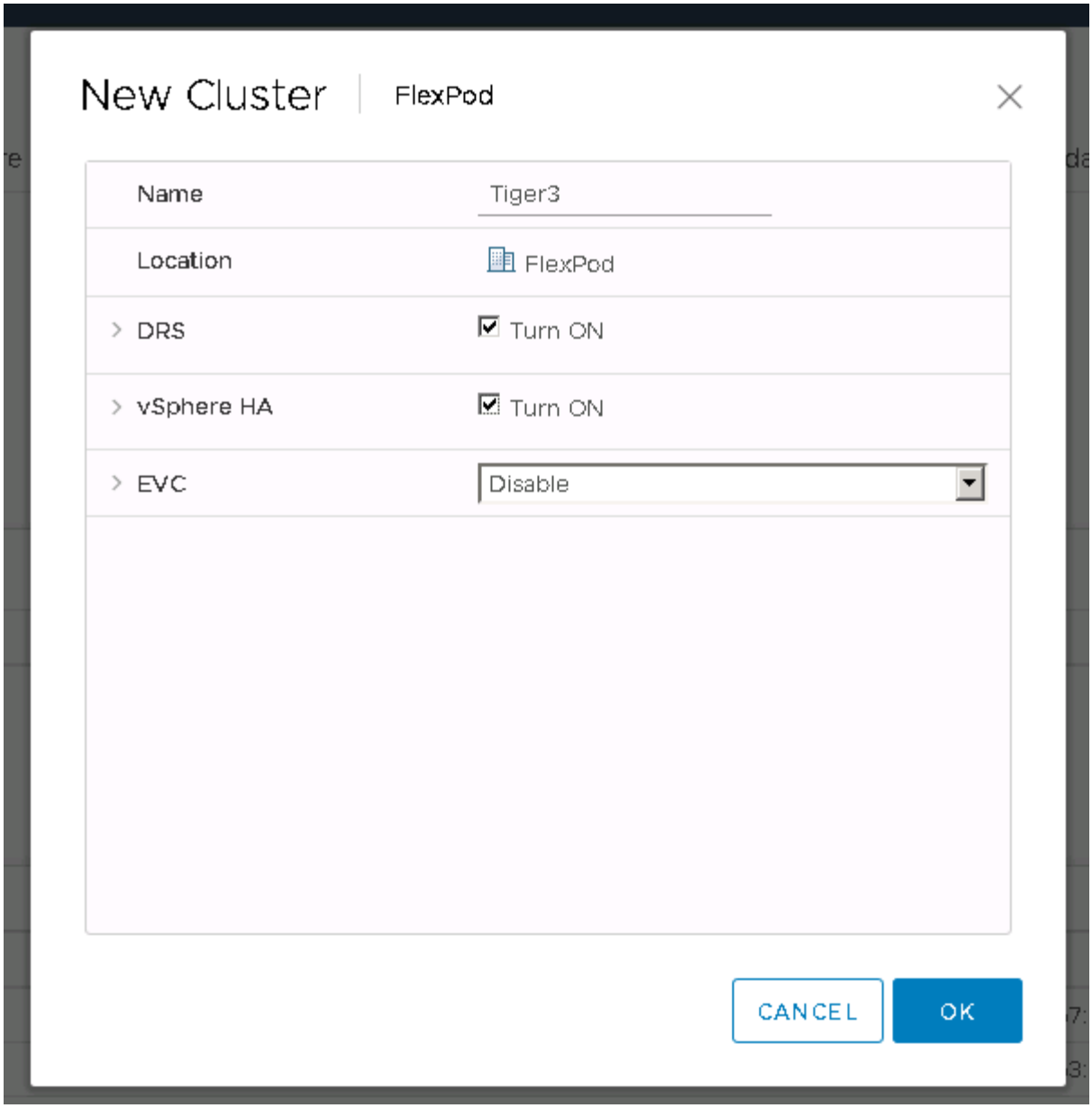
Para configurar la agrupación en clústeres de VMware vCenter Server 6.7 y vSphere, complete los pasos siguientes:

1. Desplácese hasta https://<<FQDN or IP of vCenter>>/vsphere-client/.
2. Haga clic en Launch vSphere Client.
3. Inicie sesión con el nombre de usuario mailto:administrator@vspehre.loc/ loc/[administrator@vsphere.loc/] y la contraseña SSO que introdujo durante el proceso de configuración de VCSA.
4. Haga clic con el botón derecho en el nombre de vCenter y seleccione New Datacenter.
5. Introduzca un nombre para el centro de datos y haga clic en Aceptar.

Cree un clúster de vSphere

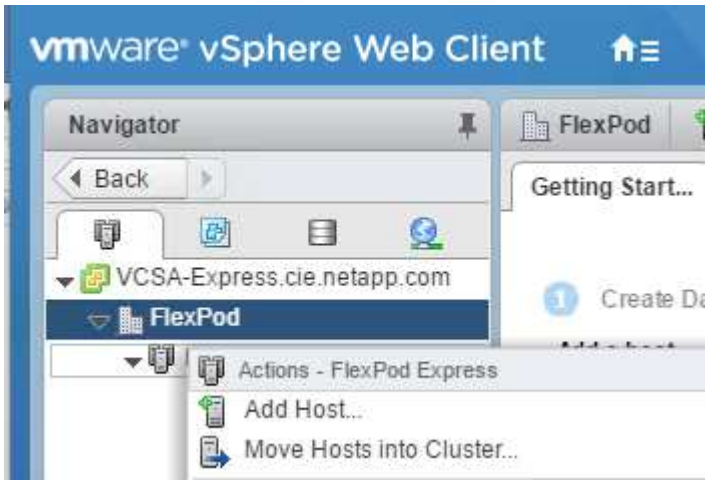
Complete los siguientes pasos para crear un clúster de vSphere:

1. Haga clic con el botón derecho en el centro de datos recién creado y seleccione New Cluster.
2. Escriba un nombre para el clúster.
3. Active la recuperación ante desastres y vSphere ha seleccionando las casillas de verificación.
4. Haga clic en Aceptar.



Añada hosts ESXi al clúster

1. Haga clic con el botón derecho en el clúster y seleccione Add Host.



2. Para añadir un host ESXi al clúster, complete los siguientes pasos:
   a. Introduzca la dirección IP o el FQDN del host. Haga clic en Siguiente.
   b. Introduzca el nombre de usuario raíz y la contraseña. Haga clic en Siguiente.
   c. Haga clic en Sí para reemplazar el certificado del host por un certificado firmado por el servidor de certificados VMware.
   d. Haga clic en Siguiente en la página Resumen de host.
   e. Haga clic en el icono verde + para añadir una licencia al host de vSphere.

      Este paso se puede completar más adelante si se desea.

   f. Haga clic en Siguiente para desactivar el modo de bloqueo.
   g. Haga clic en Next en la página de ubicación de la máquina virtual.
   h. Revise la página Listo para completar. Utilice el botón Atrás para realizar cualquier cambio o seleccione Finalizar.
3. Repita los pasos 1 y 2 para el host Cisco UCS B. Debe completar este proceso para los hosts adicionales que se agreguen a la configuración exprés de FlexPod.

Configure coredump en hosts ESXi

1. Utilice SSH, conéctese al host ESXi de IP de gestión, introduzca root para el nombre de usuario e introduzca la contraseña raíz.
2. Ejecute los siguientes comandos:

```
esxcli system coredump network set -i ip_address_of_core_dump_collector
-v vmk0 -o 6500
esxcli system coredump network set --enable=true
esxcli system coredump network check
```

3. El mensaje `Verified the configured netdump server is running` aparece después de introducir el comando final.

Este proceso debe completarse para cualquier host adicional que se añada a FlexPod Express.

Conclusión

FlexPod Express proporciona una solución sencilla y efectiva, ya que proporciona un diseño validado que utiliza componentes líderes del sector. Al escalar agregando componentes adicionales, FlexPod Express puede adaptarse según las necesidades específicas del negocio. FlexPod Express se diseñó teniendo en cuenta a las pequeñas y medianas empresas, oficinas remotas y otras empresas que precisan soluciones dedicadas.

Dónde encontrar información adicional

Para obtener más información sobre la información descrita en este documento, consulte

los siguientes documentos y/o sitios web:

- Documentación de productos de NetApp

  "http://docs.netapp.com"

- Guía de diseño de FlexPod Express con VMware vSphere 6.7 y AFF A220 de NetApp

  "https://www.netapp.com/us/media/nva-1125-design.pdf"

FlexPod Express con VMware vSphere 6.7U1 y NetApp AFF A220 con almacenamiento basado en IP directamente incluido

NVA-1131-DEPLOY: FlexPod Express con VMware vSphere 6.7U1 y NetApp AFF A220 con almacenamiento basado en IP directamente incluido

Sree Lakshmi Lanka, NetApp

Las tendencias en el sector señalan una gran transformación de los centros de datos hacia una infraestructura compartida y cloud computing. Además, las organizaciones buscan una solución sencilla y eficaz para oficinas remotas y sucursales que aprovechen la tecnología con la que ya están familiarizados en su centro de datos.

FlexPod Express es una arquitectura prediseñada de prácticas recomendadas que se basa en el Cisco Unified Computing System (Cisco UCS), la familia de switches Cisco Nexus y las tecnologías de almacenamiento de NetApp. Los componentes de un sistema FlexPod Express se asemejan a los del centro de datos FlexPod, lo que permite sinergias de gestión en todo el entorno de infraestructura DE TI a una escala menor. FlexPod Datacenter y FlexPod Express son plataformas óptimas para virtualización y sistemas operativos con configuración básica y cargas de trabajo empresariales.

El centro de datos FlexPod y FlexPod Express proporcionan una configuración básica y disponen de la versatilidad necesaria para ajustar el tamaño y optimizarse con el objetivo de acomodar distintos casos de uso y requisitos. Los clientes existentes de FlexPod Datacenter pueden gestionar su sistema FlexPod Express con las herramientas a las que están acostumbrados. Los nuevos clientes de FlexPod Express pueden adaptarse fácilmente a la gestión del centro de datos FlexPod cuando crezca su entorno.

FlexPod Express es una base de infraestructura óptima para oficinas remotas y sucursales (robo) y para pequeñas y medianas empresas. También es una solución óptima para los clientes que desean proporcionar infraestructura para cargas de trabajo dedicadas.

FlexPod Express proporciona una infraestructura fácil de gestionar que es adecuada para casi cualquier carga de trabajo.

Descripción general de la solución

Esta solución FlexPod Express forma parte del programa de infraestructura convergente de FlexPod.

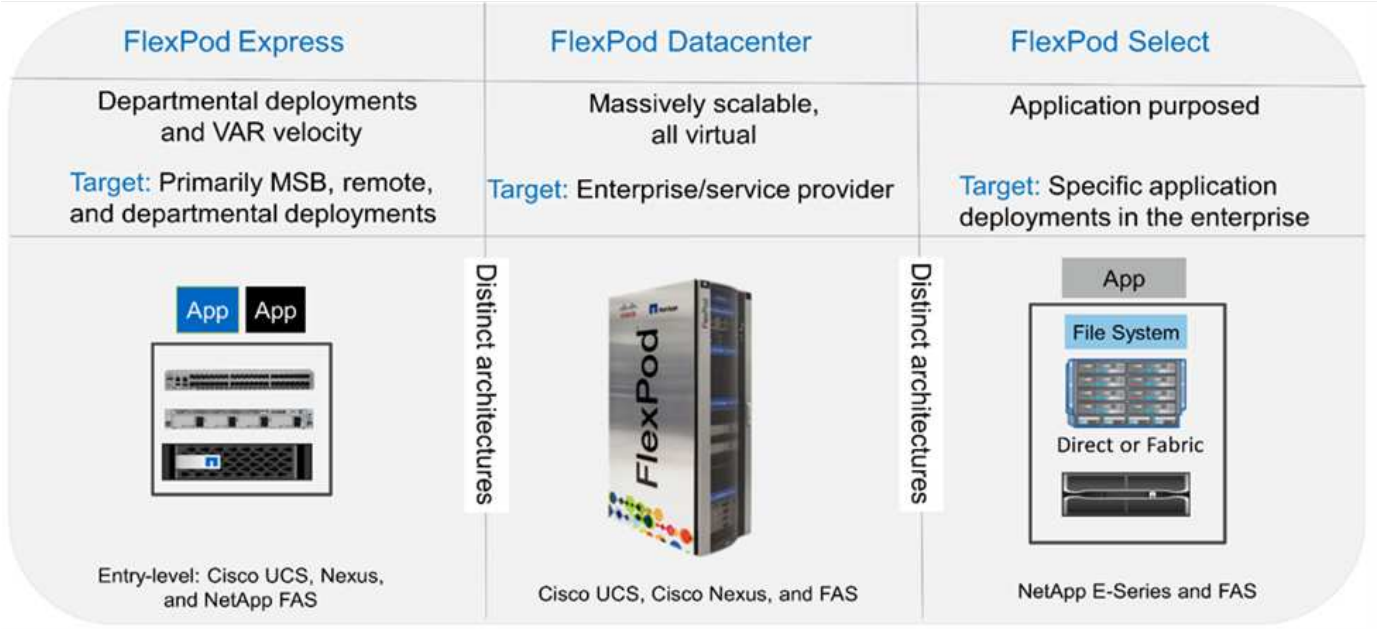
Programa de infraestructura convergente FlexPod

Las arquitecturas de referencia FlexPod se proporcionan como diseños validados por Cisco (CVD) o como arquitecturas verificadas por NetApp (NVA). Se permiten las desviaciones basadas en los requisitos de los clientes de un CVD o NVA determinado si estas variaciones no crean una configuración incompatible.

Como se muestra en la siguiente figura, el programa FlexPod incluye tres soluciones: FlexPod Express, FlexPod Datacenter y FlexPod Select:

- **FlexPod Express** ofrece a los clientes una solución de gama básica con tecnologías de Cisco y NetApp.
- **FlexPod Datacenter** proporciona una base multiuso óptima para diversas cargas de trabajo y aplicaciones.
- **FlexPod Select** incorpora los mejores aspectos del centro de datos FlexPod y adapta la infraestructura a una aplicación determinada.

En la siguiente figura se muestran los componentes técnicos de la solución.



Programa Arquitectura validada por NetApp

El programa NVA ofrece a los clientes una arquitectura verificada para las soluciones NetApp. NVA proporciona una arquitectura de solución de NetApp con las siguientes cualidades:

- Ha sido probada a conciencia
- Tiene naturaleza prescriptiva
- Minimiza los riesgos de implementación
- Reduce el plazo de comercialización

En esta guía se detalla el diseño de FlexPod Express con almacenamiento de NetApp de conexión directa. Las secciones siguientes enumeran los componentes utilizados para el diseño de esta solución.

Componentes de hardware

- AFF A220 de NetApp
- Cisco UCS Mini
- CISCO UCS B200 M5
- Cisco UCS VIC 1440/1480.
- Switches Cisco Nexus serie 3000

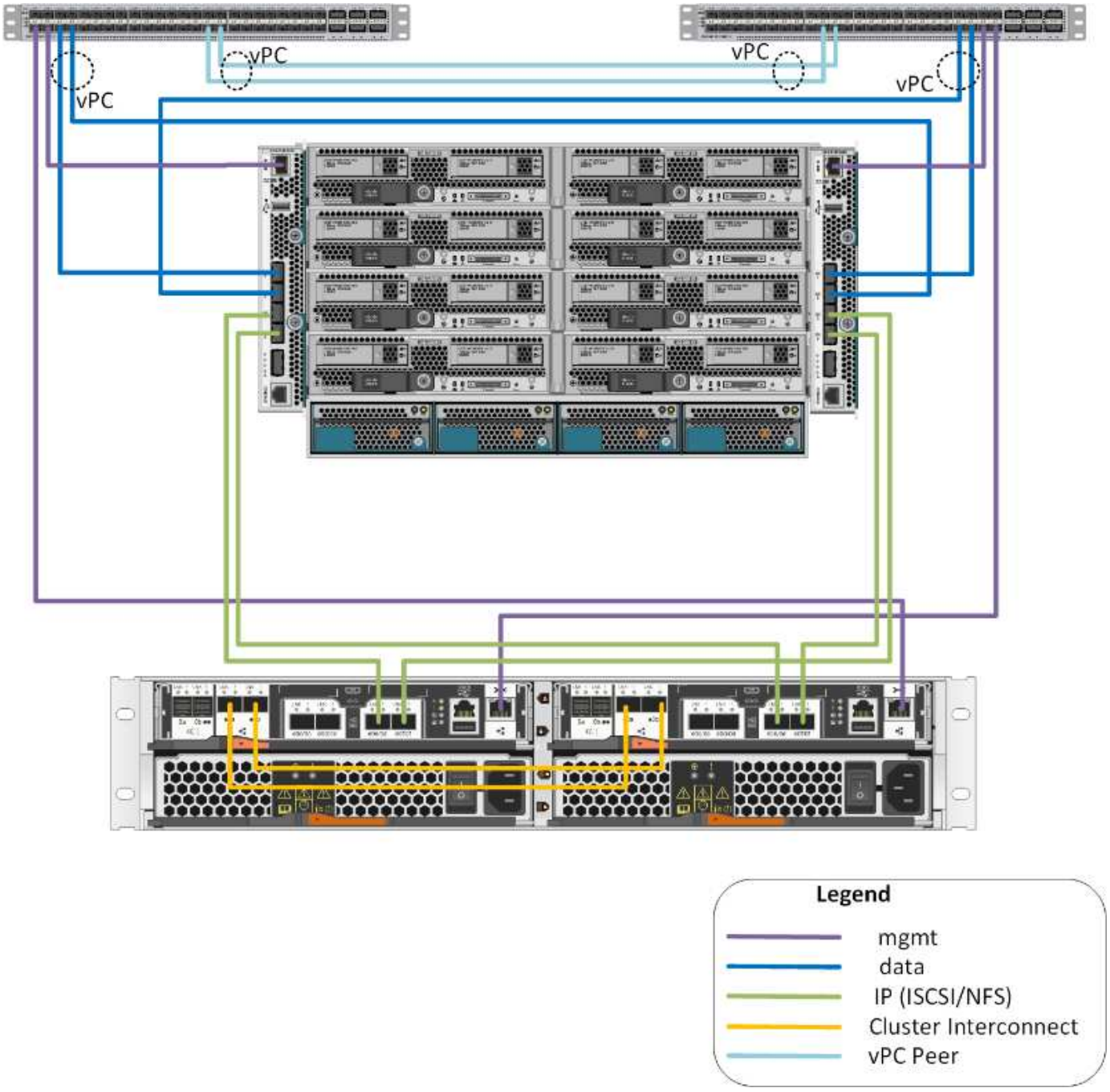
Componentes de software

- ONTAP 9 de NetApp. 5
- VMware vSphere 6.7U1
- Cisco UCS Manager 4.0(1b)
- Firmware Cisco NXOS 7.0(3)I6(1)

Tecnología de soluciones

Esta solución aprovecha las últimas tecnologías de NetApp, Cisco y VMware. Incluye el nuevo AFF A220 de NetApp que ejecute ONTAP 9.5, los conmutadores Cisco Nexus 31108PCV duales y los servidores Cisco UCS B200 M5 que ejecutan VMware vSphere 6.7U1. Esta solución validada usa almacenamiento IP de Direct Connect con tecnología 10GbE.

La siguiente figura muestra FlexPod Express con VMware vSphere 6.7U1, una arquitectura Direct Connect basada en IP.



Resumen de casos de uso

La solución FlexPod Express puede aplicarse a varios casos prácticos, incluidos los siguientes:

- ROBOS
- Pequeñas y medianas empresas
- Entornos que requieren una solución dedicada y rentable

FlexPod Express está indicado para cargas de trabajo virtualizadas y mixtas.

Requisitos tecnológicos

Un sistema FlexPod Express requiere una combinación de componentes de hardware y

software. FlexPod Express también describe los componentes de hardware necesarios para añadir nodos de hipervisor al sistema en unidades de dos.

Requisitos de hardware

Independientemente del hipervisor elegido, todas las configuraciones exprés de FlexPod utilizan el mismo hardware. Por lo tanto, aunque cambien los requisitos del negocio, cualquiera de los hipervisores puede ejecutarse en el mismo hardware de FlexPod Express.

En la siguiente tabla se enumeran los componentes de hardware necesarios para todas las configuraciones exprés de FlexPod.

Hardware subyacente	Cantidad
Par de alta disponibilidad AFF A220	1
Servidor Cisco UCS B200 M5	2
Switch Cisco Nexus 31108PCV	2
Tarjeta de interfaz virtual (VIC) Cisco UCS 1440 para el servidor Cisco UCS B200 M5	2
Cisco UCS Mini con dos interconexiones de estructura UCS-FI-M-6324 integradas	1

Requisitos de software

En la siguiente tabla se enumeran los componentes de software necesarios para implementar las arquitecturas de las soluciones Express de FlexPod.

De NetApp	Versión	Detalles
Administrador de Cisco UCS	4.0(1b)	Para Cisco UCS Fabric Interconnect FI-6324UP
Software blade Cisco	4.0(1b)	Para servidores Cisco UCS B200 M5
Controlador nenic de Cisco	1.0.25.0	Para tarjetas de interfaz Cisco VIC 1440
Cisco NX-OS	7.0(3)I6(1)	Para switches Cisco Nexus 31108PCV
ONTAP de NetApp	9.5	Para controladoras AFF A220

En la siguiente tabla se muestra el software necesario para todas las implementaciones de VMware vSphere en FlexPod Express.

De NetApp	Versión
Dispositivo VMware vCenter Server	6.7U1
Hipervisor ESXi de VMware vSphere	6.7U1

Información de cableado exprés de FlexPod

El cableado de validación de referencia se documenta en las siguientes tablas.

La tabla siguiente enumera información de cableado para el switch Cisco Nexus 31108PCV A.

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Switch Cisco Nexus 31108PCV A	Eth1/1	Controladora De almacenamiento A AFF A220 de NetApp	E0M
	Eth1/2	Cisco UCS-mini FI-A.	mgmt0
	Eth1/3	Cisco UCS-mini FI-A.	Eth1/1
	ETH 1/4	Cisco UCS-mini FI-B	Eth1/1
	ETH 1/13	CISCO NX 31108PCV B	ETH 1/13
	ETH 1/14	CISCO NX 31108PCV B	ETH 1/14

En la siguiente tabla se muestra la información de cableado del switch Cisco Nexus 31108PCV B.

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Switch Cisco Nexus 31108PCV B	Eth1/1	Controladora de almacenamiento B de AFF A220 de NetApp	E0M
	Eth1/2	Cisco UCS-mini FI-B	mgmt0
	Eth1/3	Cisco UCS-mini FI-A.	Eth1/2
	ETH 1/4	Cisco UCS-mini FI-B	Eth1/2
	ETH 1/13	CISCO NX 31108PCV A	ETH 1/13
	ETH 1/14	CISCO NX 31108PCV A	ETH 1/14

En la siguiente tabla se muestra información de cableado para la controladora de almacenamiento AFF A220 A. de NetApp

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Controladora De almacenamiento A AFF A220 de NetApp	e0a	Controladora de almacenamiento B de AFF A220 de NetApp	e0a
	e0b	Controladora de almacenamiento B de AFF A220 de NetApp	e0b
	e0e	Cisco UCS-mini FI-A.	Eth1/3
	e0f	Cisco UCS-mini FI-B	Eth1/3
	E0M	CISCO NX 31108PCV A	Eth1/1

La siguiente tabla enumera información de cableado para la controladora de almacenamiento AFF A220 B.

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Controladora de almacenamiento B de AFF A220 de NetApp	e0a	Controladora de almacenamiento B de AFF A220 de NetApp	e0a
	e0b	Controladora de almacenamiento B de AFF A220 de NetApp	e0b
	e0e	Cisco UCS-mini FI-A.	Eth1/4
	e0f	Cisco UCS-mini FI-B	Eth1/4
	E0M	CISCO NX 31108PCV B	Eth1/1

La siguiente tabla enumera la información de cableado para Cisco UCS Fabric Interconnect A.

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Interconexión de estructura Cisco UCS a	Eth1/1	CISCO NX 31108PCV A	Eth1/3
	Eth1/2	CISCO NX 31108PCV B	Eth1/3
	Eth1/3	Controladora De almacenamiento A AFF A220 de NetApp	e0e
	Eth1/4	Controladora de almacenamiento B de AFF A220 de NetApp	e0e
	mgmt0	CISCO NX 31108PCV A	Eth1/2

La siguiente tabla enumera información de cableado para Cisco UCS Fabric Interconnect B.

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Interconexión de estructura B de Cisco UCS	Eth1/1	CISCO NX 31108PCV A	Eth1/4
	Eth1/2	CISCO NX 31108PCV B	Eth1/4
	Eth1/3	Controladora De almacenamiento A AFF A220 de NetApp	e0f
	Eth1/4	Controladora de almacenamiento B de AFF A220 de NetApp	e0f
	mgmt0	CISCO NX 31108PCV B	Eth1/2

Procedimientos de implantación

Este documento proporciona detalles para configurar un sistema FlexPod Express completamente redundante y de alta disponibilidad. Para reflejar esta redundancia, los componentes que se configuran en cada paso se denominan componente A o componente B. Por ejemplo, la controladora A y la controladora B identifican las dos

controladoras de almacenamiento de NetApp que se aprovisionan en este documento. El switch A y el switch B identifican un par de switches Cisco Nexus. La interconexión de estructura A y la interconexión de estructura B son las dos interconexiones de estructura Nexus integradas.

Además, en este documento se describen los pasos para aprovisionar varios hosts de Cisco UCS, que se identifican secuencialmente como servidor A, servidor B, etc.

Para indicar que debe incluir la información pertinente a su entorno en un paso, `<<text>>` aparece como parte de la estructura de comandos. Consulte el siguiente ejemplo de `vlan create` comando:

```
Controller01>vlan create vif0 <<mgmt_vlan_id>>
```

Este documento permite configurar completamente el entorno de FlexPod Express. En este proceso, varios pasos requieren que inserte convenciones de nomenclatura específicas del cliente, direcciones IP y esquemas de red de área local virtual (VLAN). En la siguiente tabla se describen las VLAN necesarias para la implementación, tal y como se explica en esta guía. Esta tabla se puede completar en función de las variables específicas del sitio y se puede utilizar para implementar los pasos de configuración del documento.



Si utiliza VLAN de gestión fuera de banda y en banda independientes, debe crear una ruta de capa 3 entre ellas. Para esta validación, se utilizó una VLAN de gestión común.

Nombre de la VLAN	Propósito de VLAN	ID utilizado para validar este documento
VLAN de gestión	VLAN para interfaces de gestión	18
VLAN nativa	VLAN a la que se asignan tramas no etiquetadas	2
VLAN NFS	VLAN para tráfico NFS	104
VLAN de VMware vMotion	VLAN designada para mover máquinas virtuales (VM) de un host físico a otro	103
VLAN de tráfico de la máquina virtual	VLAN para tráfico de aplicaciones de equipos virtuales	102
ISCSI-A-VLAN	VLAN para tráfico iSCSI en la estructura A	124
ISCSI-B-VLAN	VLAN para tráfico iSCSI en la estructura B	125

Los números VLAN son necesarios en toda la configuración de FlexPod Express. Las VLAN se denominan `<<var_xxxx_vlan>>`, donde `xxxx` Es la finalidad de la VLAN (como iSCSI-A).

La siguiente tabla enumera las máquinas virtuales de VMware creadas.

Descripción de VM	Nombre de host
Servidor VMware vCenter	Seahawks-vcsa.cie.netapp.com

Procedimiento de puesta en marcha de Cisco Nexus 31108PCV

En esta sección se detalla la configuración del switch Cisco Nexus 31308PCV utilizada en un entorno FlexPod Express.

Configuración inicial del switch Cisco Nexus 31108PCV

Este procedimiento describe cómo configurar los switches Cisco Nexus para su uso en un entorno FlexPod Express básico.

> En este procedimiento se asume que está utilizando un Cisco Nexus 31108PCV con la versión de software NX-OS 7.0(3)I6(1).

1. Tras el arranque y la conexión iniciales al puerto de la consola del switch, se inicia automáticamente la configuración de Cisco NX-OS. Esta configuración inicial trata los valores básicos, como el nombre del switch, la configuración de la interfaz mgmt0 y la configuración de Secure Shell (SSH).
2. La red de gestión del sistema FlexPod Express se puede configurar de varias maneras. Las interfaces mgmt0 de los conmutadores 31108PCV se pueden conectar a una red de administración existente, o las interfaces mgmt0 de los conmutadores 31108PCV se pueden conectar en una configuración posterior. Sin embargo, este enlace no se puede utilizar para el acceso de gestión externo, como tráfico SSH.

   En esta guía de puesta en marcha, los switches Cisco Nexus 31108PCV de FlexPod Express están conectados a una red de gestión existente.
3. Para configurar los switches Cisco Nexus 31108PCV, encienda el switch y siga las indicaciones que aparecen en pantalla, como se muestra aquí para la configuración inicial de ambos switches, sustituyendo los valores adecuados para la información específica del switch.

   ```
   This setup utility will guide you through the basic configuration of the
   system. Setup configures only enough connectivity for management of the
   system.
   ```

```
*Note: setup is mainly used for configuring the system initially, when
no configuration is present. So setup always assumes system defaults and
not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip
the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
Create another login account (yes/no) [n]: n
Configure read-only SNMP community string (yes/no) [n]: n
Configure read-write SNMP community string (yes/no) [n]: n
Enter the switch name : 31108PCV-A
Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
Configure the default gateway? (yes/no) [y]: y
IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
Configure advanced IP options? (yes/no) [n]: n
Enable the telnet service? (yes/no) [n]: n
Enable the ssh service? (yes/no) [y]: y
Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
Number of rsa key bits <1024-2048> [1024]: <enter>
Configure the ntp server? (yes/no) [n]: y
NTP server IPv4 address : <<var_ntp_ip>>
Configure default interface layer (L3/L2) [L2]: <enter>
Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
Configure CoPP system profile (strict/moderate/lenient/dense) [strict]:
<enter>
```

4. Se muestra un resumen de la configuración y se le pregunta si desea editar la configuración. Si la configuración es correcta, introduzca `n`.

```
Would you like to edit the configuration? (yes/no) [n]: no
```

5. A continuación, se le preguntará si desea utilizar esta configuración y guardarla. Si es así, introduzca `y`.

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Repita los pasos del 1 al 5 para el switch Cisco Nexus B.

Habilite funciones avanzadas

Determinadas características avanzadas deben estar habilitadas en Cisco NX-OS para proporcionar opciones

de configuración adicionales.

1. Para habilitar las funciones adecuadas en los switches a y B de Cisco Nexus, escriba el modo de configuración mediante el comando `(config t)` y ejecute los siguientes comandos:

```
feature interface-vlan
feature lacp
feature vpc
```

> El hash de equilibrio de carga del canal de puerto predeterminado utiliza las direcciones IP de origen y destino para determinar el algoritmo de equilibrio de carga en las interfaces del canal de puerto. Puede lograr una mejor distribución entre los miembros del canal de puerto proporcionando más entradas al algoritmo hash más allá de las direcciones IP de origen y destino. Por el mismo motivo, NetApp recomienda encarecidamente añadir los puertos TCP de origen y destino al algoritmo hash.

2. Desde el modo de configuración `(config t)`, Ejecute los siguientes comandos para establecer la configuración de equilibrio de carga del canal de puertos global en los conmutadores A y B de Cisco Nexus:

```
port-channel load-balance src-dst ip-l4port
```

Realizar la configuración de árbol de expansión global

La plataforma Cisco Nexus utiliza una nueva función de protección llamada garantía de puente. La garantía de puente ayuda a proteger contra un enlace unidireccional u otro error de software con un dispositivo que continúa redirectando el tráfico de datos cuando ya no ejecuta el algoritmo de árbol expansivo. Los puertos se pueden colocar en uno de varios estados, incluyendo la red o el borde, dependiendo de la plataforma.

NetApp recomienda establecer la garantía de puente para que todos los puertos se consideren puertos de red de forma predeterminada. Este ajuste obliga al administrador de red a revisar la configuración de cada puerto. También revela los errores de configuración más comunes, como puertos de borde no identificados o un vecino que no tiene activada la función de garantía de puente. Además, es más seguro tener el bloque de árbol expansivo muchos puertos en lugar de muy pocos, lo que permite que el estado de puerto predeterminado mejore la estabilidad general de la red.

Preste especial atención al estado de árbol de expansión al agregar servidores, almacenamiento y switches ascendentes, especialmente si no admiten la garantía de puente. En estos casos, es posible que deba cambiar el tipo de puerto para que los puertos estén activos.

El protector de unidad de datos de protocolo puente (BPDU) está habilitado de forma predeterminada en puertos periféricos como otra capa de protección. Para evitar bucles en la red, esta característica cierra el puerto si se ven BPDU de otro switch en esta interfaz.

Desde el modo de configuración (`config t`), ejecute los siguientes comandos para configurar las opciones de árbol expansivo predeterminadas, incluidos el tipo de puerto predeterminado y el protector BPDU, en el conmutador A de Cisco Nexus y el conmutador B:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
```

Defina las VLAN

Antes de configurar puertos individuales con VLAN diferentes, se deben definir las VLAN de capa 2 en el switch. También se recomienda nombrar las VLAN para que la solución de problemas sea sencilla en el futuro.

Desde el modo de configuración (`config t`), ejecute los siguientes comandos para definir y describir las VLAN de capa 2 en el switch A y el switch B de Cisco Nexus:

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

Configurar el acceso y las descripciones de los puertos de gestión

Como es el caso, la asignación de nombres a las VLAN de capa 2, las descripciones de configuración de todas las interfaces pueden ayudar tanto al aprovisionamiento como a la solución de problemas.

Desde el modo de configuración (`config t`) En cada uno de los conmutadores, introduzca las siguientes descripciones de puerto para la configuración grande de FlexPod Express:

Switch Cisco Nexus a

```
int eth1/1
  description AFF A220-A e0M
int eth1/2
  description Cisco UCS FI-A mgmt0
int eth1/3
  description Cisco UCS FI-A eth1/1
int eth1/4
  description Cisco UCS FI-B eth1/1
int eth1/13
  description vPC peer-link 31108PVC-B 1/13
int eth1/14
  description vPC peer-link 31108PVC-B 1/14
```

Switch Cisco Nexus B

```
int eth1/1
  description AFF A220-B e0M
int eth1/2
  description Cisco UCS FI-B mgmt0
int eth1/3
  description Cisco UCS FI-A eth1/2
int eth1/4
  description Cisco UCS FI-B eth1/2
int eth1/13
  description vPC peer-link 31108PVC-B 1/13
int eth1/14
  description vPC peer-link 31108PVC-B 1/14
```

Configurar las interfaces de gestión de almacenamiento y servidores

Las interfaces de gestión para el servidor y el almacenamiento suelen utilizar una sola VLAN. Por lo tanto, configure los puertos de la interfaz de gestión como puertos de acceso. Defina la VLAN de administración para cada switch y cambie el tipo de puerto de árbol expansivo a EDGE.

Desde el modo de configuración (`config t`), ejecute los siguientes comandos para configurar los ajustes de puerto para las interfaces de administración tanto de los servidores como del almacenamiento:

Switch Cisco Nexus a

```
int eth1/1-2
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Switch Cisco Nexus B

```
int eth1/1-2
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Añada la interfaz de distribución de NTP

Switch Cisco Nexus a

Desde el modo de configuración global, ejecute los siguientes comandos.

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch-a-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exitntp peer <switch-b-ntp-ip> use-vrf default
```

Switch Cisco Nexus B

Desde el modo de configuración global, ejecute los siguientes comandos.

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch- b-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exitntp peer <switch-a-ntp-ip> use-vrf default
```

Llevar a cabo la configuración global del canal de puertos virtuales

Un canal de puerto virtual (VPC) permite que los enlaces que están conectados físicamente a dos switches de Cisco Nexus diferentes aparezcan como un único canal de puerto a un tercer dispositivo. El tercer dispositivo puede ser un conmutador, un servidor o cualquier otro dispositivo de red. Un VPC puede proporcionar una multivía de nivel 2, que le permite crear redundancia aumentando el ancho de banda, permitiendo múltiples rutas paralelas entre los nodos y tráfico de equilibrio de carga donde haya rutas alternativas.

Un VPC proporciona las siguientes ventajas:

- Permitir que un único dispositivo utilice un canal de puerto a través de dos dispositivos de subida
- Eliminar puertos bloqueados del protocolo de árbol expansivo
- Proporciona una topología sin bucles
- Utilizando todo el ancho de banda disponible de enlace ascendente
- Proporcionar convergencia rápida si el enlace o un dispositivo falla
- Resiliencia a nivel de enlace
- Contribuir a proporcionar una alta disponibilidad

La función VPC requiere alguna configuración inicial entre los dos switches de Cisco Nexus para que funcionen correctamente. Si utiliza la configuración de mgmt0 de fondo, utilice las direcciones definidas en las interfaces y compruebe que se pueden comunicar mediante ping `<<switch_A/B_mgmt0_ip_addr>>vrf` comando de gestión.

Desde el modo de configuración (`config t`), ejecute los siguientes comandos para configurar la configuración global de VPC para ambos switches:

Switch Cisco Nexus a

```
vpc domain 1
 role priority 10
peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
  int eth1/13-14
  channel-group 10 mode active
int Po10description vPC peer-link
switchport
switchport mode trunkswitchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>> spanning-tree port type network
vpc peer-link
no shut
exit
int Po13
description vPC ucs-FI-A
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 13
no shut
exit
int eth1/3
  channel-group 13 mode active
int Po14
description vPC ucs-FI-B
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 14
no shut
exit
int eth1/4
  channel-group 14 mode active
copy run start
```

Switch Cisco Nexus B

```
vpc domain 1
peer-switch
role priority 20
peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
  int eth1/13-14
  channel-group 10 mode active
int Po10
description vPC peer-link
switchport
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>> spanning-tree port type network
vpc peer-link
no shut
exit
int Po13
description vPC ucs-FI-A
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 13
no shut
exit
int eth1/3
  channel-group 13 mode active
int Po14
description vPC ucs-FI-B
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 14
no shut
exit
int eth1/4
```

```
  channel-group 14 mode active
copy run start
```

En esta validación de solución se utilizó una unidad de transmisión máxima (MTU) de 9000. Sin embargo, en función de los requisitos de la aplicación, puede configurar un valor de MTU adecuado. Es importante establecer el mismo valor de MTU en la solución de FlexPod. Las configuraciones de MTU incorrectas entre componentes provocan la eliminación de paquetes.

Enlace ascendente a la infraestructura de red existente

En función de la infraestructura de red disponible, se pueden utilizar varios métodos y funciones para elevar el entorno FlexPod. Si existe un entorno Cisco Nexus existente, NetApp recomienda utilizar VPC para conectar los switches Cisco Nexus 31108PVC incluidos en el entorno FlexPod a la infraestructura. Los enlaces ascendentes pueden ser enlaces de subida de 10 GbE para una solución de infraestructura de 10 GbE o 1 GbE para una solución de infraestructura de 1 GbE si fuera necesario. Los procedimientos descritos anteriormente se pueden utilizar para crear un VPC de enlace ascendente al entorno existente. Asegúrese de ejecutar Copy RUN START para guardar la configuración en cada switch una vez completada la configuración.

Procedimiento de instalación de almacenamiento NetApp (parte 1)

En esta sección se describe el procedimiento de implementación del almacenamiento AFF de NetApp.

Instalación de la controladora de almacenamiento de NetApp serie AFF2xx

Hardware Universe de NetApp

La "Hardware Universe de NetApp" (HWU) proporciona componentes de hardware y software compatibles con cualquier versión específica de ONTAP. Proporciona información de configuración para todos los dispositivos de almacenamiento de NetApp compatibles actualmente con el software ONTAP. También se proporciona una tabla de compatibilidades de componentes.

Confirme que los componentes de hardware y software que desea utilizar son compatibles con la versión de ONTAP que tiene previsto instalar:

1. Acceda a "HWU" aplicación para ver las guías de configuración del sistema. Seleccione la pestaña Comparar sistemas de almacenamiento para ver la compatibilidad entre diferentes versiones del software ONTAP y los dispositivos de almacenamiento de NetApp con las especificaciones que desea.
2. Como alternativa, para comparar componentes por dispositivo de almacenamiento, haga clic en Comparar sistemas de almacenamiento.

Requisitos previos de la controladora de la serie AFF2XX
Para planificar la ubicación física de los sistemas de almacenamiento, consulte las siguientes secciones: Requisitos eléctricos cables de alimentación compatibles puertos y cables integrados

Controladoras de almacenamiento

Siga los procedimientos de instalación física de los controladores de la "Documentación de AFF A220".

ONTAP 9.5 de NetApp

Hoja de datos de configuración

Antes de ejecutar la secuencia de comandos de instalación, rellene la hoja de datos de configuración del manual del producto. La hoja de datos de configuración está disponible en la "Guía de configuración de software de ONTAP 9.5" (disponible en la "Centro de documentación de ONTAP 9"). La siguiente tabla muestra información sobre la instalación y la configuración de ONTAP 9.5.

Este sistema se establece en una configuración de clúster de dos nodos sin switch.

Detalles del clúster	Valor de detalles del clúster
Nodo del clúster: Dirección IP	<<var_nodeA_mgmt_ip>>
Máscara de red Del nodo a del clúster	<<var_nodeA_mgmt_mask>>
Nodo del clúster: Puerta de enlace	<<var_nodeA_mgmt_gateway>>
Nombre del nodo a del clúster	<<var_nodeA>>
Dirección IP del nodo B del clúster	<<var_nodeB_mgmt_ip>>
Máscara de red del nodo B del clúster	<<var_nodeB_mgmt_mask>>
Puerta de enlace del nodo B del clúster	<<var_nodeB_mgmt_gateway>>
Nombre del nodo B del clúster	<<var_nodeB>>
Dirección URL de ONTAP 9.5	<<var_url_boot_software>>
El nombre del clúster	<<var_clustername>>
Dirección IP de gestión del clúster	<<var_clustermgmt_ip>>
Puerta de enlace del clúster B.	<<var_clustermgmt_gateway>>
Máscara de red del clúster B.	<<var_clustermgmt_mask>>
Nombre de dominio	<<var_domain_name>>
IP del servidor DNS (puede introducir más de uno)	<<var_dns_server_ip>>
SERVIDOR NTP: UNA IP	<< switch-a-ntp-ip >>
IP DEL SERVIDOR NTP B.	<< switch-b-ntp-ip >>

Configure el nodo A

Para configurar el nodo A, complete los siguientes pasos:

1. Conéctese al puerto de la consola del sistema de almacenamiento. Tiene que ver un cargador-a del símbolo del sistema. Sin embargo, si el sistema de almacenamiento está en un bucle de reinicio, pulse Ctrl- C para salir del bucle de autoarranque cuando vea este mensaje:

```
Starting AUTOBOOT press Ctrl-C to abort...
```

2. Permita que el sistema arranque.

```
autoboot
```

3. Pulse Ctrl- C para acceder al menú Inicio.

   Si es ONTAP 9. 5 no es la versión del software que se está arrancando, continúe con los pasos siguientes para instalar el software nuevo. Si es ONTAP 9. 5 es la versión que se va a arrancar, seleccione la opción 8 e y para reiniciar el nodo. A continuación, continúe con el paso 14.

4. Para instalar software nuevo, seleccione opción `7`.
5. Introduzca `y` para realizar una actualización.
6. Seleccione `e0M` para el puerto de red que desea usar para la descarga.
7. Introduzca `y` para reiniciar ahora.
8. Introduzca la dirección IP, la máscara de red y la puerta de enlace predeterminada para e0M en sus respectivos lugares.

   ```
   <<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
   ```

9. Especifique la dirección URL donde se puede encontrar el software.

   Este servidor web debe ser pingable.

10. Pulse Intro para el nombre de usuario, indicando que no hay nombre de usuario.
11. Introduzca `y` para establecer el software recién instalado como el predeterminado que se utilizará para los siguientes reinicios.
12. Introduzca `y` para reiniciar el nodo.

    Al instalar el software nuevo, el sistema podría realizar actualizaciones de firmware en el BIOS y las tarjetas adaptadoras, lo que provoca reinicios y posibles interrupciones en el cargador. Si se producen estas acciones, el sistema podría desviarse de este procedimiento.

13. Pulse Ctrl- C para acceder al menú Inicio.
14. Seleccione opción `4` Para una configuración limpia y inicializar todos los discos.
15. Introduzca `y` para poner a cero discos, restablezca la configuración e instale un nuevo sistema de archivos.
16. Introduzca `y` para borrar todos los datos de los discos.

    La inicialización y creación del agregado raíz puede tardar 90 minutos o más en completarse, según el número y el tipo de discos conectados. Una vez finalizada la inicialización, el sistema de almacenamiento se reinicia. Tenga en cuenta que los SSD tardan mucho menos tiempo en inicializarse. Puede continuar con la configuración del nodo B mientras los discos del nodo A se están poniendo a cero.

17. Mientras el nodo A se está inicializando, empiece a configurar el nodo B.

Configure el nodo B

Para configurar el nodo B, complete los siguientes pasos:

1. Conéctese al puerto de la consola del sistema de almacenamiento. Tiene que ver un cargador-a del símbolo del sistema. Sin embargo, si el sistema de almacenamiento está en un bucle de reinicio, pulse Ctrl-C para salir del bucle de autoarranque cuando vea este mensaje:

   ```
   Starting AUTOBOOT press Ctrl-C to abort...
   ```

2. Pulse Ctrl-C para acceder al menú Inicio.

   ```
   autoboot
   ```

3. Pulse Ctrl-C cuando se le solicite.

   Si es ONTAP 9. 5 no es la versión del software que se está arrancando, continúe con los pasos siguientes para instalar el software nuevo. Si ONTAP 9.4 es la versión que se va a arrancar, seleccione la opción 8 e y para reiniciar el nodo. A continuación, continúe con el paso 14.

4. Para instalar software nuevo, seleccione la opción 7.
5. Introduzca `y` para realizar una actualización.
6. Seleccione `e0M` para el puerto de red que desea usar para la descarga.
7. Introduzca `y` para reiniciar ahora.
8. Introduzca la dirección IP, la máscara de red y la puerta de enlace predeterminada para e0M en sus respectivos lugares.

   ```
   <<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
   ```

9. Especifique la dirección URL donde se puede encontrar el software.

   Este servidor web debe ser pingable.

   ```
   <<var_url_boot_software>>
   ```

10. Pulse Intro para el nombre de usuario, indicando que no hay nombre de usuario
11. Introduzca `y` para establecer el software recién instalado como el predeterminado que se utilizará para los siguientes reinicios.
12. Introduzca `y` para reiniciar el nodo.

    Al instalar el software nuevo, el sistema podría realizar actualizaciones de firmware en el BIOS y las tarjetas adaptadoras, lo que provoca reinicios y posibles interrupciones en el cargador. Si se producen estas acciones, el sistema podría desviarse de este procedimiento.

13. Pulse Ctrl-C para acceder al menú Inicio.
14. Seleccione la opción 4 para Configuración limpia y inicializar todos los discos.
15. Introduzca `y` para poner a cero discos, restablezca la configuración e instale un nuevo sistema de archivos.
16. Introduzca `y` para borrar todos los datos de los discos.

    La inicialización y creación del agregado raíz puede tardar 90 minutos o más en completarse, según el número y el tipo de discos conectados. Una vez finalizada la inicialización, el sistema de almacenamiento se reinicia. Tenga en cuenta que los SSD tardan mucho menos tiempo en inicializarse.

Continuación de la configuración Del nodo a y de la configuración del clúster

Desde un programa de puertos de consola conectado al puerto de la consola De la controladora De almacenamiento A (nodo A), ejecute el script de configuración del nodo. Este script se muestra cuando ONTAP 9.5 arranca en el nodo por primera vez.

El procedimiento de configuración del nodo y de los clústeres ha cambiado ligeramente en ONTAP 9.5. El asistente de configuración de clúster ahora se utiliza para configurar el primer nodo de un clúster, y System Manager se utiliza para configurar el clúster.

1. Siga las instrucciones para configurar el nodo A.

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

2. Vaya a la dirección IP de la interfaz de gestión del nodo.

> La configuración del clúster también se puede realizar mediante la CLI. Este documento describe la configuración del clúster mediante la configuración guiada de System Manager de NetApp.

3. Haga clic en Guided Setup para configurar el clúster.
4. Introduzca `<<var_clustername>>` del nombre del clúster y. `<<var_nodeA>>` y.. `<<var_nodeB>>` para cada uno de los nodos que va a configurar. Introduzca la contraseña que desea usar para el sistema de almacenamiento. Seleccione Switchless Cluster para el tipo de clúster. Introduzca la licencia base del clúster.
5. También es posible introducir licencias de funciones para Cluster, NFS e iSCSI.
6. Ve un mensaje de estado que indica que el clúster se está creando. Este mensaje de estado cambia por varios Estados. Este proceso tarda varios minutos.
7. Configure la red.
   a. Anule la selección de la opción intervalo de direcciones IP.

b. Introduzca <<var_clustermgmt_ip>> En el campo Cluster Management IP Address, <<var_clustermgmt_mask>> En el campo máscara de red, y. <<var_clustermgmt_gateway>> En el campo Puerta de enlace. Use el … Selector en el campo Port para seleccionar e0M del nodo A.

c. La IP de gestión de nodos para el nodo A ya se ha rellenado. Introduzca <<var_nodeA_mgmt_ip>> Para el nodo B.

d. Introduzca <<var_domain_name>> En el campo DNS Domain Name. Introduzca <<var_dns_server_ip>> En el campo DNS Server IP Address.

   Puede introducir varias direcciones IP del servidor DNS.

e. Introduzca <<switch-a-ntp-ip>> En el campo servidor NTP primario.

   También puede introducir un servidor NTP alternativo como <<switch- b-ntp-ip>>.

8. Configure la información de soporte.
   a. Si el entorno requiere un proxy para acceder a AutoSupport, introduzca la URL en Proxy URL.
   b. Introduzca el host de correo SMTP y la dirección de correo electrónico para las notificaciones de eventos.

      Debe, como mínimo, configurar el método de notificación de eventos antes de continuar. Puede seleccionar cualquiera de los métodos.

9. Cuando indique que ha finalizado la configuración del clúster, haga clic en Manage your Cluster para configurar el almacenamiento.

Continuación de la configuración del clúster de almacenamiento

Después de configurar los nodos de almacenamiento y el clúster base, puede continuar con la configuración del clúster de almacenamiento.

Ponga a cero todos los discos de repuesto

Para poner a cero todos los discos de repuesto del clúster, ejecute el siguiente comando:

```
disk zerospares
```

Configure la personalidad de los puertos UTA2 integrados

1. Verifique el modo actual y el tipo actual de puertos ejecutando el `ucadmin show` comando.

```
AFFA220-Clus::> ucadmin show
                     Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFFA220-Clus-01
              0c       cna      target     -        -          offline
AFFA220-Clus-01
              0d       cna      target     -        -          offline
AFFA220-Clus-01
              0e       cna      target     -        -          offline
AFFA220-Clus-01
              0f       cna      target     -        -          offline
AFFA220-Clus-02
              0c       cna      target     -        -          offline
AFFA220-Clus-02
              0d       cna      target     -        -          offline
AFFA220-Clus-02
              0e       cna      target     -        -          offline
AFFA220-Clus-02
              0f       cna      target     -        -          offline
8 entries were displayed.
```

2. Compruebe que el modo actual de los puertos que se están utilizando es `cna` y que el tipo actual está establecido en `target`. De lo contrario, cambie la personalidad de puerto ejecutando el siguiente comando:

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

Los puertos deben estar desconectados para que se ejecute el comando anterior. Para desconectar un puerto, ejecute el siguiente comando:

```
network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down
```

Si ha cambiado la personalidad del puerto, debe reiniciar cada nodo para que el cambio se aplique.

Habilite el protocolo de detección de Cisco

Para habilitar el protocolo de detección de Cisco (CDP) en las controladoras de almacenamiento de NetApp, ejecute el siguiente comando:

```
node run -node * options cdpd.enable on
```

Habilite el protocolo de detección de capa de enlace en todos los puertos Ethernet

Habilite el intercambio de información cercana del protocolo de detección de capa de enlace (LLDP) entre los switches de red y almacenamiento ejecutando el siguiente comando. Este comando habilita LLDP en todos los puertos de todos los nodos del clúster.

```
node run * options lldp.enable on
```

Cambie el nombre de las interfaces lógicas de gestión

Para cambiar el nombre de las interfaces lógicas de gestión (LIF), realice los pasos siguientes:

1. Muestra los nombres de las LIF de gestión actuales.

   ```
   network interface show –vserver <<clustername>>
   ```

2. Cambie el nombre de la LIF de gestión del clúster.

   ```
   network interface rename –vserver <<clustername>> –lif
   cluster_setup_cluster_mgmt_lif_1 –newname cluster_mgmt
   ```

3. Cambie el nombre del LIF de gestión del nodo B.

   ```
   network interface rename -vserver <<clustername>> -lif
   cluster_setup_node_mgmt_lif_AFF A220_A_1 - newname AFF A220-01_mgmt1
   ```

Configure la reversión automática en la gestión del clúster

Ajuste la `auto-revert` parámetro en la interfaz de gestión del clúster.

```
network interface modify –vserver <<clustername>> -lif cluster_mgmt –auto-
revert true
```

Configure la interfaz de red del procesador de servicio

Para asignar una dirección IPv4 estática al procesador de servicios en cada nodo, ejecute los siguientes comandos:

```
system service-processor network modify -node <<var_nodeA>> -address
-family IPv4 -enable true - dhcp none -ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify -node <<var_nodeB>> -address
-family IPv4 -enable true - dhcp none -ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

Las direcciones IP de Service Processor deben estar en la misma subred que las direcciones IP de gestión de nodos.

Activar la recuperación tras fallos de almacenamiento en ONTAP

Para confirmar que la conmutación por error del almacenamiento está habilitada, ejecute los siguientes comandos de una pareja de conmutación por error:

1. Comprobar el estado de recuperación tras fallos del almacenamiento.

   ```
   storage failover show
   ```

   Ambas `<<var_nodeA>>` y.. `<<var_nodeB>>` debe poder realizar una toma de control. Vaya al paso 3 si los nodos pueden realizar una toma de control.

2. Habilite la conmutación al nodo de respaldo en uno de los dos nodos.

   ```
   storage failover modify -node <<var_nodeA>> -enabled true
   ```

3. Compruebe el estado de alta disponibilidad del clúster de dos nodos.

   Este paso no es aplicable para clústeres con más de dos nodos.

   ```
   cluster ha show
   ```

4. Vaya al paso 6 si está configurada la alta disponibilidad. Si se ha configurado la alta disponibilidad, verá el siguiente mensaje al emitir el comando:

   ```
   High Availability Configured: true
   ```

5. Habilite el modo de alta disponibilidad solo para el clúster de dos nodos.

   No ejecute este comando para clústeres con más de dos nodos debido a que provoca problemas con la conmutación al nodo de respaldo.

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. Compruebe que la asistencia de hardware está correctamente configurada y, si es necesario, modifique la dirección IP del partner.

```
storage failover hwassist show
```

El mensaje `Keep Alive Status : Error: did not receive hwassist keep alive alerts from partner` indica que la asistencia de hardware no está configurada. Ejecute los siguientes comandos para configurar hardware Assist.

```
storage failover modify –hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify –hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

Cree un dominio de retransmisión MTU para tramas gigantes en ONTAP

Para crear un dominio de retransmisión de datos con un valor MTU de 9000, ejecute los siguientes comandos:

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

Quite los puertos de datos del dominio de retransmisión predeterminado

Los puertos de datos de 10 GbE se utilizan para el tráfico iSCSI/NFS y estos puertos deben eliminarse del dominio predeterminado. Los puertos e0e y e0f no se utilizan y deben eliminarse del dominio predeterminado.

Para quitar puertos del dominio de retransmisión, ejecute el siguiente comando:

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

Deshabilite el control de flujo en los puertos UTA2

Se recomienda utilizar las mejores prácticas de NetApp para deshabilitar el control de flujo en todos los puertos UTA2 conectados a dispositivos externos. Para desactivar el control de flujo, ejecute los siguientes comandos:

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
```



La conexión mínima directa de Cisco UCS a ONTAP no es compatible con LACP.

Configurar tramas gigantes en ONTAP de NetApp

Para configurar un puerto de red ONTAP para que utilice tramas gigantes (que normalmente tienen una MTU de 9,000 bytes), ejecute los siguientes comandos desde el shell del clúster:

```
AFF A220::> network port modify -node node_A -port e0e -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port e0e -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_A -port e0f -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port e0f -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
```

Crear VLAN en ONTAP

Para crear VLAN en ONTAP, complete los siguientes pasos:

1. Cree puertos VLAN NFS y añádalos al dominio de retransmisión de datos.

```
network port vlan create –node <<var_nodeA>> -vlan-name e0e-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeA>> -vlan-name e0f-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0e-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0f-
<<var_nfs_vlan_id>>
broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
<<var_nodeA>>: e0e- <<var_nfs_vlan_id>>, <<var_nodeB>>: e0e-
<<var_nfs_vlan_id>> , <<var_nodeA>>:e0f- <<var_nfs_vlan_id>>,
<<var_nodeB>>:e0f-<<var_nfs_vlan_id>>
```

2. Cree puertos VLAN iSCSI y añádalos al dominio de retransmisión de datos.

```
network port vlan create –node <<var_nodeA>> -vlan-name e0e-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeA>> -vlan-name e0f-
<<var_iscsi_vlan_B_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0e-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0f-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>: e0e- <<var_iscsi_vlan_A_id>>,<<var_nodeB>>: e0e-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>: e0f- <<var_iscsi_vlan_B_id>>,<<var_nodeB>>: e0f-
<<var_iscsi_vlan_B_id>>
```

3. Cree puertos MGMT-VLAN.

```
network port vlan create –node <<var_nodeA>> -vlan-name e0m-
<<mgmt_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0m-
<<mgmt_vlan_id>>
```

Crear agregados en ONTAP

Durante el proceso de configuración de ONTAP, se crea un agregado que contiene el volumen raíz. Para crear agregados adicionales, determine el nombre del agregado, el nodo en el que se creará y el número de discos que contiene.

Para crear agregados, ejecute los siguientes comandos:

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

Conserve al menos un disco (seleccione el disco más grande) en la configuración como un repuesto. Una práctica recomendada es tener al menos un repuesto para cada tipo y tamaño de disco.

Empiece con cinco discos; puede añadir discos a un agregado cuando necesite almacenamiento adicional.

No se puede crear el agregado hasta que se complete el establecimiento en cero del disco. Ejecute el `aggr show` comando para mostrar el estado de creación del agregado. No continúe hasta `aggr1_nodeA` está en línea.

Configurar la zona horaria en ONTAP

Para configurar la sincronización horaria y establecer la zona horaria en el clúster, ejecute el siguiente comando:

```
timezone <<var_timezone>>
```

Por ejemplo, en el este de los Estados Unidos, la zona horaria es `America/New_York`. Cuando haya comenzado a escribir el nombre de la zona horaria, pulse la tecla TAB para ver las opciones disponibles.

Configurar SNMP en ONTAP

Para configurar SNMP, realice los siguientes pasos:

1. Configure la información básica de SNMP, como la ubicación y el contacto. Cuando se sondean, esta información es visible como `sysLocation` y.. `sysContact` Variables en SNMP.

```
snmp contact <<var_snmp_contact>>
snmp location "<<var_snmp_location>>"
snmp init 1
options snmp.enable on
```

2. Configure las capturas SNMP para que se envíen a hosts remotos.

```
snmp traphost add <<var_snmp_server_fqdn>>
```

Configure SNMPv1 en ONTAP

Para configurar SNMPv1, establezca la contraseña de texto sin formato secreta compartida denominada comunidad.

```
snmp community add ro <<var_snmp_community>>
```

Utilice la `snmp community delete all` comando con precaución. Si se utilizan cadenas de comunidad para otros productos de supervisión, este comando las quita.

Configure SNMPv3 en ONTAP

SNMPv3 requiere que defina y configure un usuario para la autenticación. Para configurar SNMPv3, lleve a cabo los siguientes pasos:

1. Ejecute el `security snmpusers` Comando para ver el ID del motor.
2. Cree un usuario llamado `snmpv3user`.

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. Introduzca el ID del motor de la entidad autoritativa y seleccione `md5` como protocolo de autenticación.
4. Escriba una contraseña de longitud mínima de ocho caracteres para el protocolo de autenticación cuando se le solicite.
5. Seleccione `des` como protocolo de privacidad.
6. Escriba una contraseña de longitud mínima de ocho caracteres para el protocolo de privacidad cuando se le solicite.

Configure HTTPS de AutoSupport en ONTAP

La herramienta AutoSupport de NetApp envía información de resumen de soporte a NetApp mediante HTTPS. Para configurar AutoSupport, ejecute el siguiente comando:

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

Cree una máquina virtual de almacenamiento

Para crear una máquina virtual de almacenamiento (SVM) de infraestructura, complete los siguientes pasos:

1. Ejecute el `vserver create` comando.

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume- security-style unix
```

2. Añada el agregado de datos a la lista de agregados de infra-SVM para VSC de NetApp.

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. Elimine los protocolos de almacenamiento que no se utilicen de la SVM, con lo que dejará NFS e iSCSI.

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. Habilite y ejecute el protocolo NFS en la SVM de infra-SVM.

```
nfs create -vserver Infra-SVM -udp disabled
```

5. Encienda la `SVM vstorage` Parámetro para el plugin VAAI para NFS de NetApp. A continuación,

compruebe que NFS se ha configurado.

```
vserver nfs modify –vserver Infra-SVM –vstorage enabled
vserver nfs show
```

Los comandos están precedidos por `vserver` En la línea de comandos porque las SVM se denominaban servidores anteriormente

Configure NFSv3 en ONTAP

En la siguiente tabla se muestra la información necesaria para completar esta configuración.

Detalles	Valor de detalle
Host ESXi dirección IP de NFS	<<var_esxi_hostA_nfs_ip>>
Dirección IP de NFS del host ESXi B	<<var_esxi_hostB_nfs_ip>>

Para configurar NFS en la SVM, ejecute los siguientes comandos:

1. Cree una regla para cada host ESXi en la política de exportación predeterminada.
2. Asigne una regla para cada host ESXi que se cree. Cada host tiene su propio índice de reglas. El primer host ESXi tiene el índice de regla 1, el segundo host ESXi tiene el índice de regla 2, etc.

```
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 1 –protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid falsevserver export-
policy rule create –vserver Infra-SVM -policyname default –ruleindex 2
–protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>> -rorule sys –rwrule
sys -superuser sys –allow-suid false
vserver export-policy rule show
```

3. Asigne la política de exportación al volumen raíz de la SVM de infraestructura.

```
volume modify –vserver Infra-SVM –volume rootvol –policy default
```

VSC de NetApp gestiona automáticamente las políticas de exportación si decide instalarlas después de configurar vSphere. Si no lo instala, debe crear reglas de políticas de exportación cuando se añadan servidores Cisco UCS B-Series adicionales.

Cree el servicio iSCSI en ONTAP

Para crear el servicio iSCSI, complete el paso siguiente:

1. Cree el servicio iSCSI en la SVM. Este comando también inicia el servicio iSCSI y establece el nombre completo de iSCSI (IQN) para la SVM. Comprobar que iSCSI se ha configurado.

```
iscsi create -vserver Infra-SVM
iscsi show
```

Crear reflejo de uso compartido de carga del volumen raíz de la SVM en ONTAP

Para crear un reflejo de uso compartido de carga del volumen raíz de la SVM en ONTAP, complete los pasos siguientes:

1. Cree un volumen para que sea el reflejo de uso compartido de carga del volumen raíz de la SVM de infraestructura en cada nodo.

```
volume create –vserver Infra_Vserver –volume rootvol_m01 –aggregate
aggr1_nodeA –size 1GB –type DPvolume create –vserver Infra_Vserver
–volume rootvol_m02 –aggregate aggr1_nodeB –size 1GB –type DP
```

2. Crear una programación de tareas para actualizar las relaciones de mirroring del volumen raíz cada 15 minutos.

```
job schedule interval create -name 15min -minutes 15
```

3. Cree las relaciones de mirroring.

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

4. Inicialice la relación de mirroring y compruebe que se haya creado.

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol snapmirror
show
```

Configure el acceso HTTPS en ONTAP

Para configurar el acceso seguro a la controladora de almacenamiento, lleve a cabo los siguientes pasos:

1. Aumente el nivel de privilegio para acceder a los comandos de certificado.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. En general, ya se encuentra en funcionamiento un certificado autofirmado. Verifique el certificado ejecutando el siguiente comando:

```
security certificate show
```

3. Para cada SVM que se muestra, el nombre común del certificado debe coincidir con el nombre de dominio completo (FQDN) de DNS de la SVM. Los cuatro certificados predeterminados deben eliminarse y sustituirse por certificados autofirmados o certificados de una entidad de certificación.

   La práctica recomendada es eliminar certificados caducados antes de crear certificados. Ejecute el `security certificate delete` comando para eliminar certificados caducados. En el siguiente comando, use LA TABULACIÓN automática para seleccionar y eliminar cada certificado predeterminado.

```
security certificate delete [TAB] ...
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM - type server -serial 552429A6
```

4. Para generar e instalar certificados autofirmados, ejecute los siguientes comandos como comandos de una sola vez. Generar un certificado de servidor para la SVM de infraestructura y la SVM de clúster. De nuevo, utilice LA TABULACIÓN automática como ayuda para completar estos comandos.

```
security certificate create [TAB] ...
Example: security certificate create -common-name infra-svm.netapp.com
-type server -size 2048 - country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email- addr
"abc@netapp.com" -expire-days 365 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. Para obtener los valores de los parámetros necesarios en el paso siguiente, ejecute el `security certificate show` comando.
6. Habilite cada certificado que se acaba de crear mediante el `-server-enabled true` y.. `-client-enabled false` parámetros. De nuevo, utilice LA TABULACIÓN automática.

```
security ssl modify [TAB] ...
Example: security ssl modify -vserver Infra-SVM -server-enabled true
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common
-name infra-svm.netapp.com
```

7. Configure y habilite el acceso SSL y HTTPS y deshabilite el acceso HTTP.

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
System services firewall policy delete -policy mgmt -service http
-vserver <<var_clustername>>
```

Es normal que algunos de estos comandos devuelvan un mensaje de error indicando que la entrada no existe.

8. Vuelva al nivel de privilegio de administrador y cree la configuración para permitir que la SVM esté disponible en la web.

```
set –privilege admin
vserver services web modify –name spi|ontapi|compat –vserver * -enabled
true
```

Cree un volumen de FlexVol de NetApp en ONTAP

Para crear un volumen FlexVol® de NetApp, introduzca el nombre del volumen, el tamaño y el agregado en el que existe. Crear dos volúmenes de almacenes de datos de VMware y un volumen de arranque del servidor.

```
volume create -vserver Infra-SVM -volume infra_datastore_1 -aggregate
aggr1_nodeA -size 500GB - state online -policy default -junction-path
/infra_datastore_1 -space-guarantee none -percent- snapshot-space 0
volume create -vserver Infra-SVM -volume infra_datastore_2 -aggregate
aggr1_nodeB -size 500GB - state online -policy default -junction-path
/infra_datastore_2 -space-guarantee none -percent- snapshot-space 0
```

```
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -juntion-path /infra_swap -space
-guarantee none -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

Habilite la deduplicación en ONTAP

Para activar la deduplicación en los volúmenes adecuados una vez al día, ejecute los siguientes comandos:

```
volume efficiency modify –vserver Infra-SVM –volume esxi_boot –schedule
sun-sat@0
volume efficiency modify –vserver Infra-SVM –volume infra_datastore_1
–schedule sun-sat@0
volume efficiency modify –vserver Infra-SVM –volume infra_datastore_2
–schedule sun-sat@0
```

Crear LUN en ONTAP

Para crear dos números de unidad lógica de arranque (LUN), ejecute los siguientes comandos:

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware - space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware - space-reserve disabled
```

Cuando se añade un servidor Cisco UCS C-Series adicional, se debe crear un LUN de arranque adicional.

Creación de LIF iSCSI en ONTAP

En la siguiente tabla se muestra la información necesaria para completar esta configuración.

Detalles	Valor de detalle
Nodo de almacenamiento a iSCSI LIF01A	<<var_nodeA_iscsi_lif01a_ip>>
Nodo de almacenamiento: Una máscara de red LIF01A de iSCSI	<<var_nodeA_iscsi_lif01a_mask>>
Nodo de almacenamiento a iSCSI LIF01B	<<var_nodeA_iscsi_lif01b_ip>>
Nodo de almacenamiento a máscara de red LIF01B de iSCSI	<<var_nodeA_iscsi_lif01b_mask>>
Nodo de almacenamiento B iSCSI LIF01A	<<var_nodeB_iscsi_lif01a_ip>>
Máscara de red del nodo de almacenamiento B iSCSI LIF01A	<<var_nodeB_iscsi_lif01a_mask>>
ISCSI LIF01B del nodo de almacenamiento	<<var_nodeB_iscsi_lif01b_ip>>
Máscara de red LIF01B de nodo de almacenamiento B.	<<var_nodeB_iscsi_lif01b_mask>>

1. Creación de cuatro LIF iSCSI, dos en cada nodo.

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi - home-node <<var_nodeA>> -home-port e0e-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi - home-node <<var_nodeA>> -home-port e0f-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi - home-node <<var_nodeB>> -home-port e0e-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi - home-node <<var_nodeB>> -home-port e0f-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface show
```

Creación de LIF NFS en ONTAP

En la siguiente tabla, se enumera la información necesaria para completar esta configuración.

Detalles	Valor de detalle
Nodo de almacenamiento: LIF NFS 01 a IP	<<var_nodeA_nfs_lif_01_a_ip>>
Nodo de almacenamiento A LIF NFS 01 una máscara de red	<<var_nodeA_nfs_lif_01_a_mask>>
Nodo de almacenamiento A LIF NFS 01 b IP	<<var_nodeA_nfs_lif_01_b_ip>>
Nodo de almacenamiento a máscara de red LIF 01 b de LIF	<<var_nodeA_nfs_lif_01_b_mask>>
Nodo de almacenamiento B LIF NFS 02 a IP	<<var_nodeB_nfs_lif_02_a_ip>>
Nodo de almacenamiento B LIF NFS 02 a máscara de red	<<var_nodeB_nfs_lif_02_a_mask>>
Nodo de almacenamiento B LIF NFS 02 b IP	<<var_nodeB_nfs_lif_02_b_ip>>
Nodo de almacenamiento B LIF NFS 02 b máscara de red	<<var_nodeB_nfs_lif_02_b_mask>>

1. Cree una LIF NFS.

```
network interface create -vserver Infra-SVM -lif nfs_lif01_a -role data
-data-protocol nfs -home- node <<var_nodeA>> -home-port e0e-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_a_ip>> - netmask <<
var_nodeA_nfs_lif_01_a_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif01_b -role data
-data-protocol nfs -home- node <<var_nodeA>> -home-port e0f-
<<var_nfs_vlan_id>> –address <<var_nodeA_nfs_lif_01_b_ip>> - netmask <<
var_nodeA_nfs_lif_01_b_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02_a -role data
-data-protocol nfs -home- node <<var_nodeB>> -home-port e0e-
<<var_nfs_vlan_id>> –address <<var_nodeB_nfs_lif_02_a_ip>> - netmask <<
var_nodeB_nfs_lif_02_a_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02_b -role data
-data-protocol nfs -home- node <<var_nodeB>> -home-port e0f-
<<var_nfs_vlan_id>> –address <<var_nodeB_nfs_lif_02_b_ip>> - netmask <<
var_nodeB_nfs_lif_02_b_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface show
```

Añada el administrador de SVM de infraestructura

En la siguiente tabla, se enumera la información necesaria para completar esta configuración.

Detalles	Valor de detalle
IP de Vsmgmt	<<var_svm_mgmt_ip>>
Máscara de red Vsmgmt	<<var_svm_mgmt_mask>>
Puerta de enlace predeterminada de Vsmgmt	<<var_svm_mgmt_gateway>>

Para añadir la LIF de administrador de SVM de infraestructura y de administración de SVM a la red de gestión, realice los siguientes pasos:

1. Ejecute el siguiente comando:

```
network interface create –vserver Infra-SVM –lif vsmgmt –role data
–data-protocol none –home-node <<var_nodeB>> -home-port e0M –address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> - status-admin up
–failover-policy broadcast-domain-wide –firewall-policy mgmt –auto-
revert true
```

La IP de administración de SVM aquí debe estar en la misma subred que la IP de administración del clúster de almacenamiento.

2. Cree una ruta predeterminada para permitir que la interfaz de gestión de SVM llegue al mundo exterior.

```
network route create –vserver Infra-SVM -destination 0.0.0.0/0 –gateway
<<var_svm_mgmt_gateway>> network route show
```

3. Establezca una contraseña para la SVM `vsadmin` usuario y desbloquear el usuario.

```
security login password –username vsadmin –vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock –username vsadmin –vserver
```

Configuración de servidor Cisco UCS

Base de Cisco UCS de FlexPod

Realice la configuración inicial de la interconexión de estructura Cisco UCS 6324 para entornos FlexPod.

En esta sección se proporcionan procedimientos detallados para configurar Cisco UCS para su uso en un entorno FlexPod robo mediante Cisco UCS Manager.

Cisco UCS Fabric Interconnect 6324 A

Cisco UCS utiliza servidores y redes de capa de acceso. Este sistema de servidores de última generación de alto rendimiento proporciona un centro de datos con un alto grado de escalabilidad y agilidad de las cargas de trabajo.

Cisco UCS Manager 4.0(1b) es compatible con la interconexión de estructura 6324 que integra la interconexión de estructura en el chasis Cisco UCS y proporciona una solución integrada para un entorno de puesta en marcha más pequeño. Cisco UCS Mini simplifica la gestión del sistema y ahorra costes en puestas en marcha a baja escala.

Los componentes de hardware y software son compatibles con la estructura unificada de Cisco, que ejecuta varios tipos de tráfico de centros de datos a través de un único adaptador de red convergente.

Configuración inicial del sistema

La primera vez que accede a una interconexión de estructura en un dominio de Cisco UCS, el asistente de configuración le solicita la siguiente información necesaria para configurar el sistema:

- Método de instalación (GUI o CLI)
- Modo de configuración (restauración a partir de una copia de seguridad completa del sistema o la configuración inicial)
- Tipo de configuración del sistema (configuración en clúster o independiente)
- Nombre del sistema

- Contraseña de administrador
- La dirección IPv4 del puerto de gestión y la máscara de subred, o el prefijo y la dirección IPv6
- Dirección IPv4 o IPv6 de la pasarela predeterminada
- Dirección IPv4 o IPv6 del servidor DNS
- Nombre de dominio predeterminado

La siguiente tabla enumera la información necesaria para completar la configuración inicial de Cisco UCS en Fabric Interconnect A

Detalles	**Detalle/valor**
Nombre del sistema	<<var_ucs_clustername>>
Contraseña de administrador	<<var_password>>
Dirección IP de administración: Interconexión de estructura A	<<var_ucsa_mgmt_ip>>
Máscara de red de gestión: Interconexión de estructura A	<<var_ucsa_mgmt_mask>>
Puerta de enlace predeterminada: Interconexión de estructura A	<<var_ucsa_mgmt_gateway>>
Dirección IP del clúster	<<var_ucs_cluster_ip>>
Dirección IP del servidor DNS	<<var_nameserver_ip>>
Nombre de dominio	<<var_domain_name>>

Para configurar Cisco UCS para su uso en un entorno FlexPod, complete los pasos siguientes:

1. Conéctese al puerto de la consola de la primera interconexión de estructura a Cisco UCS 6324

```
Enter the configuration method. (console/gui) ? console

  Enter the setup mode; setup newly or restore from backup.
(setup/restore) ? setup

  You have chosen to setup a new Fabric interconnect. Continue? (y/n): y

  Enforce strong password? (y/n) [y]: Enter

  Enter the password for "admin":<<var_password>>
  Confirm the password for "admin":<<var_password>>

  Is this Fabric interconnect part of a cluster(select 'no' for
standalone)? (yes/no) [n]: yes

  Enter the switch fabric (A/B) []: A

  Enter the system name: <<var_ucs_clustername>>

  Physical Switch Mgmt0 IP address : <<var_ucsa_mgmt_ip>>

  Physical Switch Mgmt0 IPv4 netmask : <<var_ucsa_mgmt_mask>>

  IPv4 address of the default gateway : <<var_ucsa_mgmt_gateway>>

  Cluster IPv4 address : <<var_ucs_cluster_ip>>

  Configure the DNS Server IP address? (yes/no) [n]: y

       DNS IP address : <<var_nameserver_ip>>

  Configure the default domain name? (yes/no) [n]: y
Default domain name: <<var_domain_name>>

  Join centralized management environment (UCS Central)? (yes/no) [n]:
no

 NOTE: Cluster IP will be configured only after both Fabric
Interconnects are initialized. UCSM will be functional only after peer
FI is configured in clustering mode.

  Apply and save the configuration (select 'no' if you want to re-
enter)? (yes/no): yes
  Applying configuration. Please wait.

  Configuration file - Ok
```

2. Revise la configuración que se muestra en la consola. Si son correctos, responda `yes` para aplicar y guardar la configuración.
3. Espere a que se muestre la solicitud de inicio de sesión para comprobar que la configuración se ha guardado.

La siguiente tabla enumera la información necesaria para completar la configuración inicial de Cisco UCS en Fabric Interconnect B.

Detalles	**Detalle/valor**
Nombre del sistema	<<var_ucs_clustername>>
Contraseña de administrador	<<var_password>>
Dirección IP de administración B	<<var_ucsb_mgmt_ip>>
Netmask-FI B de gestión	<<var_ucsb_mgmt_mask>>
Gateway-FI B predeterminada	<<var_ucsb_mgmt_gateway>>
Dirección IP del clúster	<<var_ucs_cluster_ip>>
Dirección IP del servidor DNS	<<var_nameserver_ip>>
Nombre de dominio	<<var_domain_name>>

1. Conéctese al puerto de la consola del segundo Cisco UCS 6324 Fabric Interconnect B.

```
 Enter the configuration method. (console/gui) ? console

  Installer has detected the presence of a peer Fabric interconnect.
This Fabric interconnect will be added to the cluster. Continue (y/n) ?
y

  Enter the admin password of the peer Fabric
interconnect:<<var_password>>
    Connecting to peer Fabric interconnect... done
    Retrieving config from peer Fabric interconnect... done
    Peer Fabric interconnect Mgmt0 IPv4 Address: <<var_ucsb_mgmt_ip>>
    Peer Fabric interconnect Mgmt0 IPv4 Netmask: <<var_ucsb_mgmt_mask>>
    Cluster IPv4 address: <<var_ucs_cluster_address>>

    Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric
Interconnect Mgmt0 IPv4 Address

  Physical Switch Mgmt0 IP address : <<var_ucsb_mgmt_ip>>


  Apply and save the configuration (select 'no' if you want to re-
enter)? (yes/no): yes
  Applying configuration. Please wait.

  Configuration file - Ok
```

2. Espere a que la solicitud de inicio de sesión confirme que la configuración se ha guardado.

Inicie sesión en Cisco UCS Manager

Para iniciar sesión en el entorno de Cisco Unified Computing System (UCS), complete los siguientes pasos:

1. Abra un explorador web y desplácese hasta la dirección del clúster de Cisco UCS Fabric Interconnect.

   Puede que tenga que esperar al menos 5 minutos tras configurar la segunda interconexión de estructura para que aparezca Cisco UCS Manager.

2. Haga clic en el enlace Iniciar UCS Manager para iniciar Cisco UCS Manager.
3. Acepte los certificados de seguridad necesarios.
4. Cuando se lo pida, introduzca admin como nombre de usuario e introduzca la contraseña de administrador.
5. Haga clic en Login para iniciar sesión en Cisco UCS Manager.

Software Cisco UCS Manager, versión 4.0(1b)

En este documento se asume el uso del software Cisco UCS Manager, versión 4.0(1b). Para actualizar el software Cisco UCS Manager y el software Cisco UCS 6324 Fabric Interconnect, consulte "Guías de instalación y actualización de Cisco UCS Manager."

Configure Cisco UCS Call Home

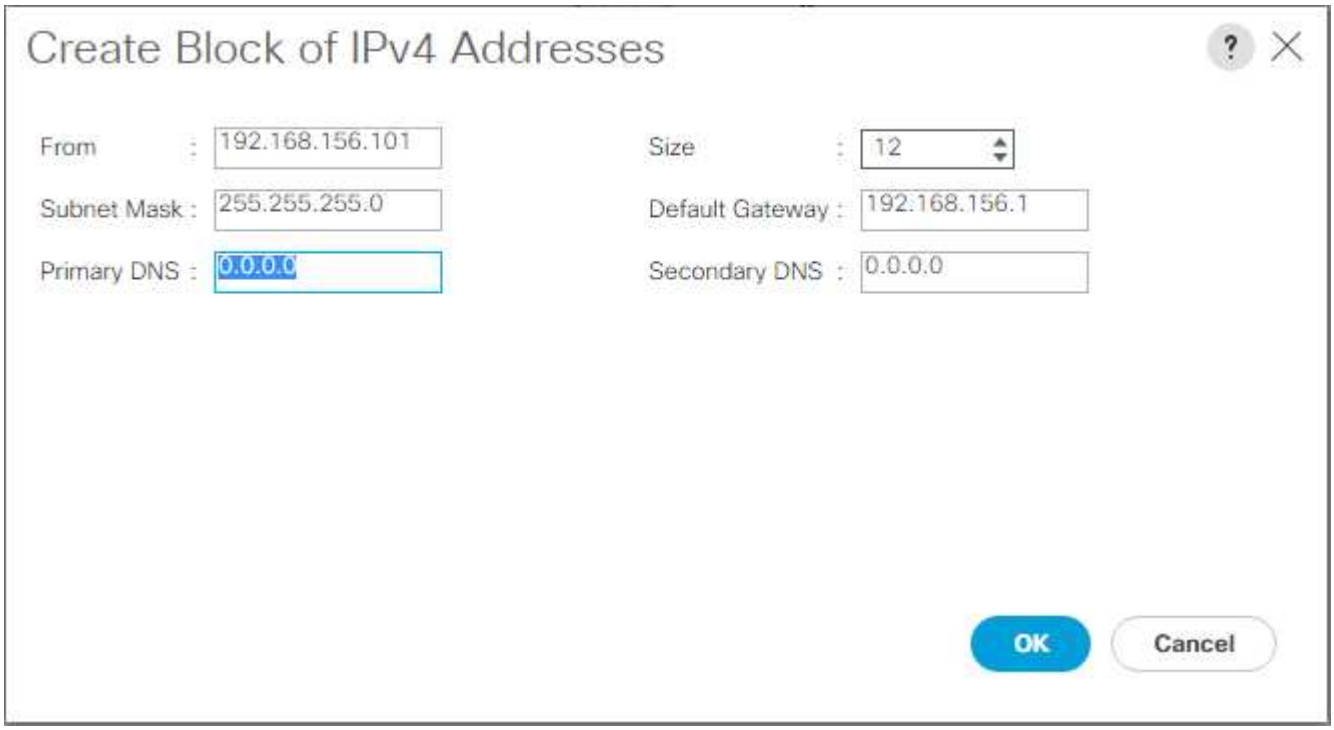
Cisco recomienda encarecidamente que configure Call Home en Cisco UCS Manager. La configuración de Call Home acelera la resolución de los casos de soporte. Para configurar Call Home, lleve a cabo los siguientes pasos:

1. En Cisco UCS Manager, haga clic en Admin a la izquierda.
2. Seleccione All > Communication Management > Call Home.
3. Cambie el estado a Activado.
4. Rellene todos los campos según sus preferencias de administración y haga clic en Guardar cambios y en Aceptar para completar la configuración de Call Home.

Agregue bloque de direcciones IP para el acceso al teclado, vídeo y ratón

Para crear un bloque de direcciones IP para el acceso de teclado, vídeo y ratón en banda en el entorno Cisco UCS, lleve a cabo los siguientes pasos:

1. En Cisco UCS Manager, haga clic en LAN a la izquierda.
2. Expanda Pools > raíz > grupos IP.
3. Haga clic con el botón derecho del ratón en IP Pool ext-mgmt y seleccione Crear bloque de direcciones IPv4.
4. Introduzca la dirección IP de inicio del bloque, el número de direcciones IP necesarias y la información de máscara de subred y puerta de enlace.



5. Haga clic en OK para crear el bloque.
6. Haga clic en Aceptar en el mensaje de confirmación.

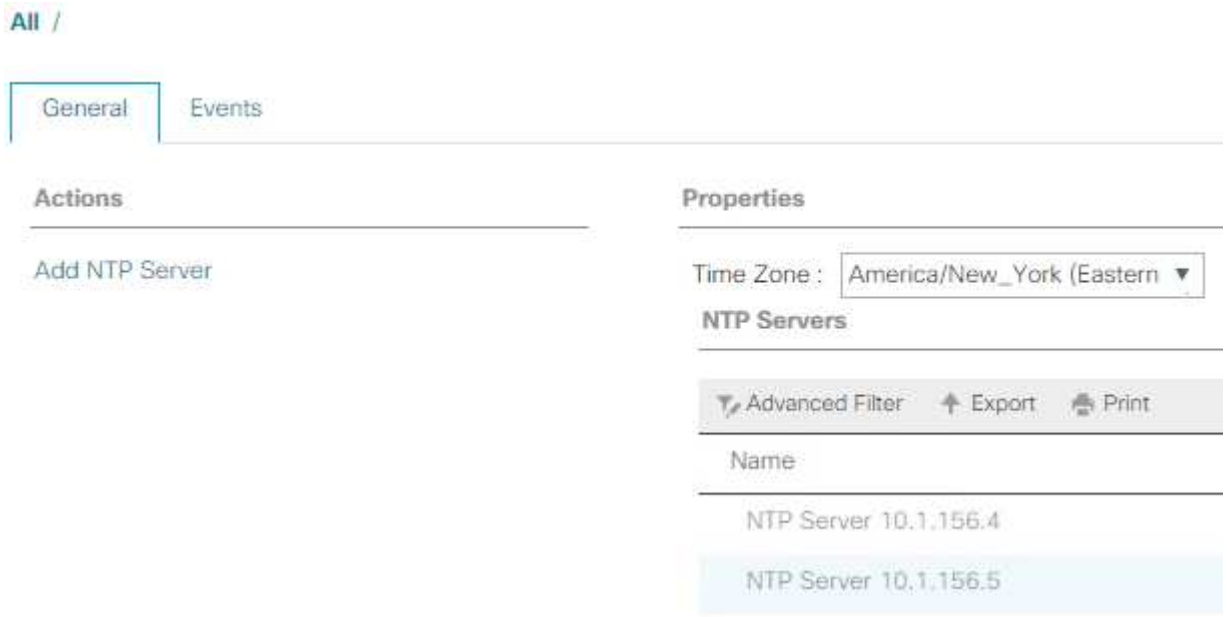
Sincronice Cisco UCS con NTP

Para sincronizar el entorno Cisco UCS con los servidores NTP en los switches Nexus, realice los siguientes pasos:

1. En Cisco UCS Manager, haga clic en Admin a la izquierda.
2. Expanda todo > Administración de zonas horarias.
3. Seleccione Time Zone.
4. En el panel Propiedades, seleccione la zona horaria adecuada en el menú Zona horaria.
5. Haga clic en Save Changes y haga clic en OK.
6. Haga clic en Add NTP Server.
7. Introduzca `<switch-a-ntp-ip> or <Nexus-A-mgmt-IP>` Y haga clic en Aceptar. Haga clic en Aceptar.



8. Haga clic en Add NTP Server.
9. Introduzca `<switch-b-ntp-ip> or <Nexus-B-mgmt-IP>` Y haga clic en Aceptar. Haga clic en Aceptar en la confirmación.



Edite la política de detección del chasis

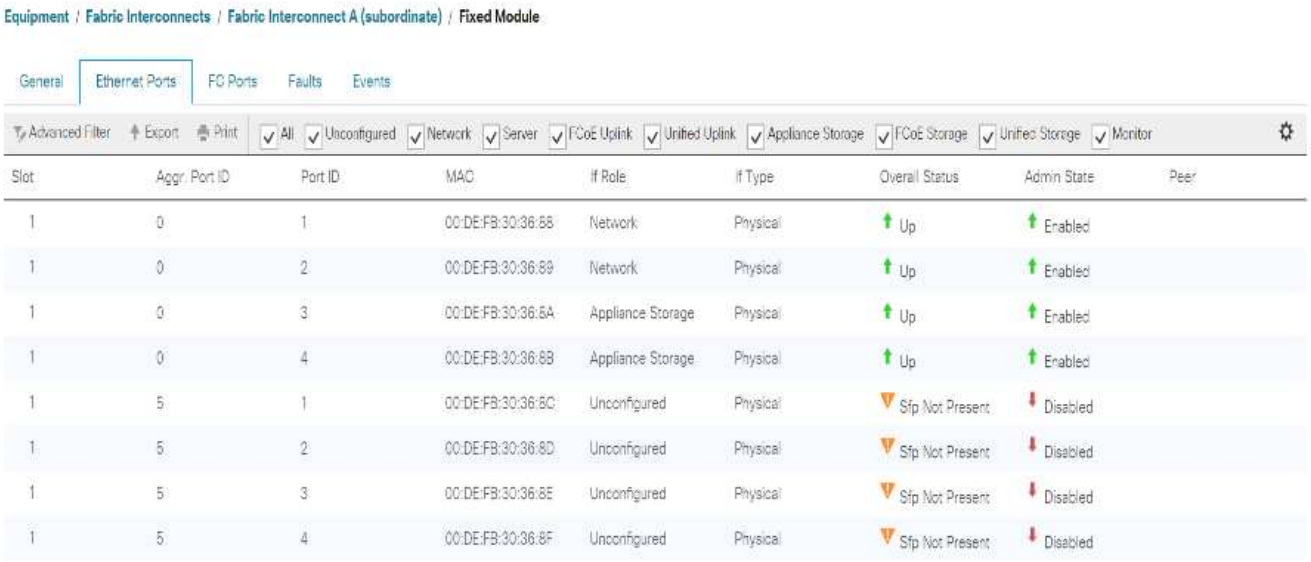
La configuración de la política de detección simplifica la adición de chasis Cisco UCS B-Series y de extensores de estructura adicionales para ampliar la conectividad de Cisco UCS C-Series. Para modificar la política de detección del chasis, complete los siguientes pasos:

1. En Cisco UCS Manager, haga clic en Equipment a la izquierda y seleccione Equipment en la segunda lista.
2. En el panel derecho, seleccione la ficha Directivas.
3. En Directivas globales, establezca la directiva de descubrimiento chasis/FEX para que coincida con el número mínimo de puertos de enlace ascendente conectados entre el chasis o los extensores de estructura (FEXes) y las interconexiones de estructura.
4. Establezca la preferencia de agrupación de enlaces en Canal de puertos. Si el entorno que se está configurando contiene una gran cantidad de tráfico de multidifusión, establezca el valor hash de hardware de multidifusión en Activado.
5. Haga clic en Save Changes.
6. Haga clic en Aceptar.

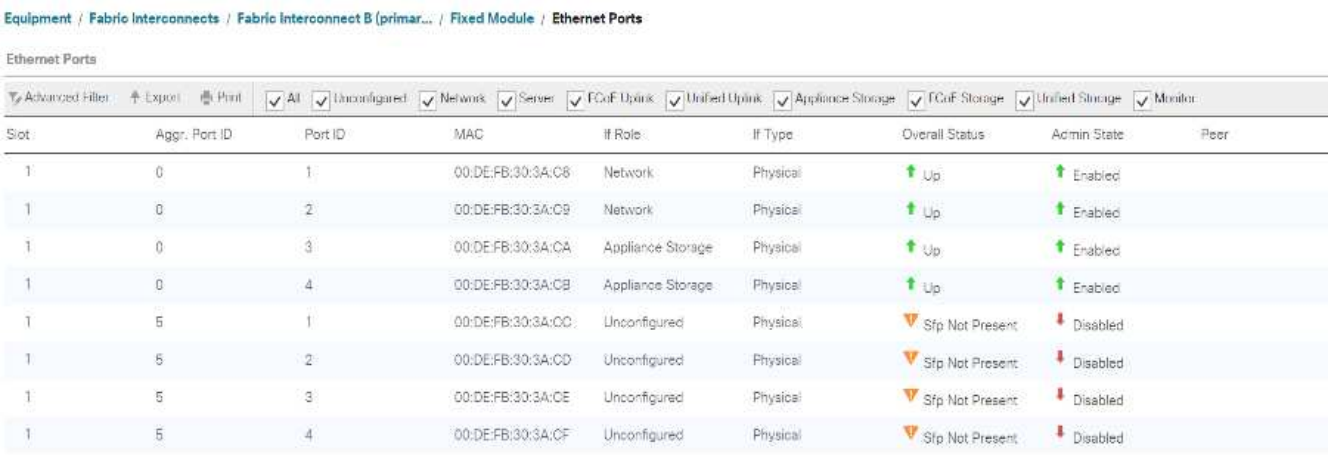
Habilite puertos de servidor, enlace ascendente y almacenamiento

Para habilitar los puertos de servidor y enlace ascendente, lleve a cabo los siguientes pasos:

1. En Cisco UCS Manager, en el panel de navegación, seleccione la pestaña equipos.
2. Expanda Equipo > interconexiones de estructura > interconexión de estructura A > módulo fijo.
3. Expanda puertos Ethernet.
4. Seleccione los puertos 1 y 2 conectados a los switches Cisco Nexus 31108, haga clic con el botón derecho del ratón y seleccione Configurar como puerto de enlace ascendente.
5. Haga clic en Sí para confirmar los puertos de enlace ascendente y haga clic en Aceptar.
6. Seleccione los puertos 3 y 4 que están conectados a las controladoras de almacenamiento de NetApp, haga clic con el botón derecho y seleccione Configurar como puerto de dispositivo.
7. Haga clic en Yes para confirmar los puertos del dispositivo.
8. En la ventana Configurar como puerto de dispositivo, haga clic en Aceptar.
9. Haga clic en OK para confirmar.
10. En el panel izquierdo, seleccione módulo fijo en interconexión de estructura A.
11. En la pestaña puertos Ethernet, confirme que los puertos se han configurado correctamente en la columna If Role. Si se han configurado servidores C-Series de puertos en el puerto de escalabilidad, haga clic en él para verificar la conectividad de los puertos.



12. Expanda Equipo > interconexiones de estructura > interconexión de estructura B > módulo fijo.
13. Expanda puertos Ethernet.
14. Seleccione los puertos Ethernet 1 y 2 conectados a los switches Cisco Nexus 31108, haga clic con el botón derecho del ratón y seleccione Configurar como puerto de enlace ascendente.
15. Haga clic en Sí para confirmar los puertos de enlace ascendente y haga clic en Aceptar.
16. Seleccione los puertos 3 y 4 que están conectados a las controladoras de almacenamiento de NetApp, haga clic con el botón derecho y seleccione Configurar como puerto de dispositivo.
17. Haga clic en Yes para confirmar los puertos del dispositivo.
18. En la ventana Configurar como puerto de dispositivo, haga clic en Aceptar.
19. Haga clic en OK para confirmar.
20. En el panel izquierdo, seleccione módulo fijo en interconexión de estructura B.
21. En la pestaña puertos Ethernet, confirme que los puertos se han configurado correctamente en la columna If Role. Si se han configurado servidores C-Series de puertos en el puerto de escalabilidad, haga clic en él para verificar la conectividad de los puertos.



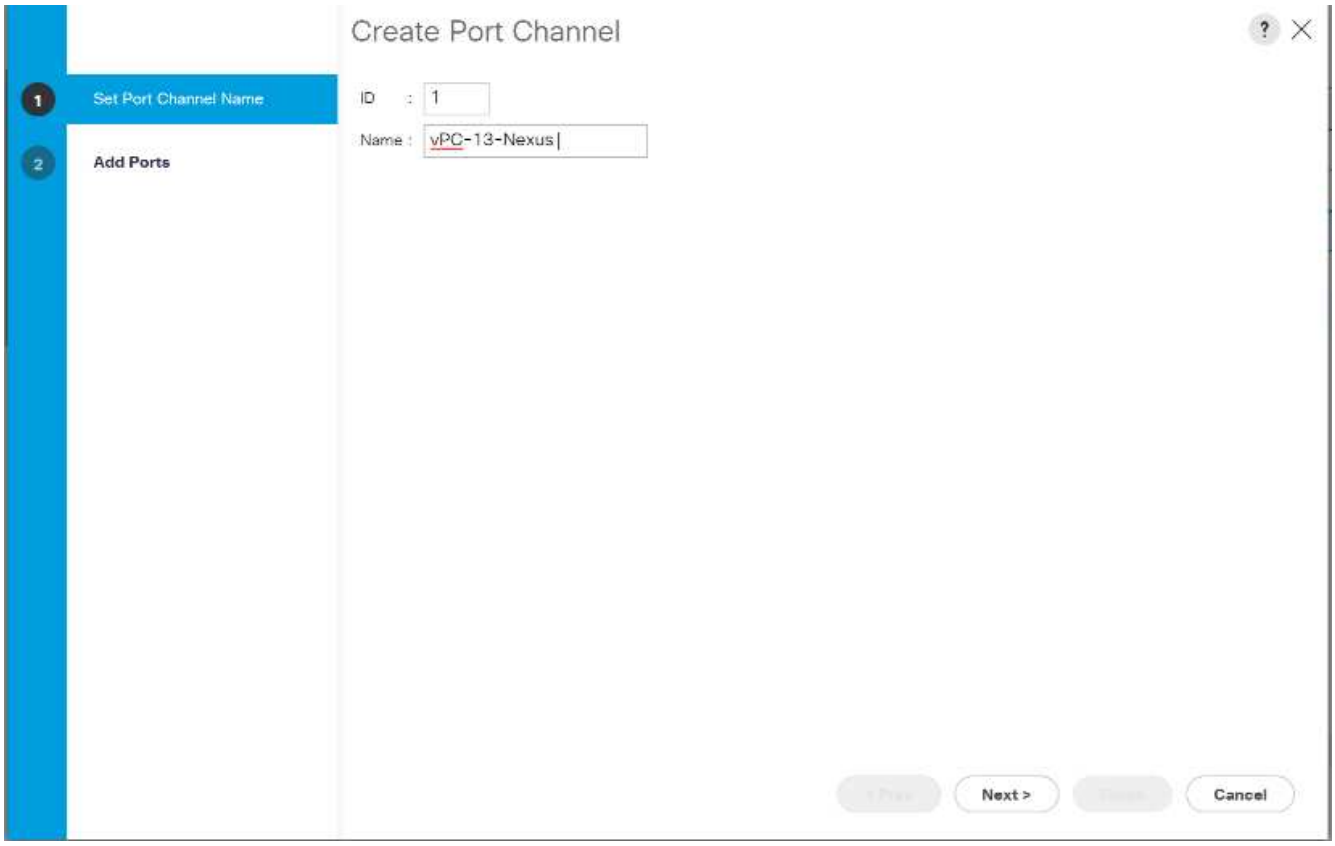
Cree canales de puertos de enlace ascendente con switches Cisco Nexus 31108

Para configurar los canales de puerto necesarios en el entorno Cisco UCS, complete los siguientes pasos:

1. En Cisco UCS Manager, seleccione la pestaña LAN en el panel de navegación.

> En este procedimiento se crean dos canales de puerto: Uno desde la estructura a hasta los switches Cisco Nexus 31108 y uno desde la estructura B a los dos switches Cisco Nexus 31108. Si está utilizando interruptores estándar, modifique este procedimiento en consecuencia. Si utiliza 1 switch Gigabit Ethernet (1 GbE) y SFP GLC-T en las interconexiones de estructura, las velocidades de interfaz de los puertos Ethernet 1/1 y 1/2 en las interconexiones de estructura deben configurarse en 1 Gbps.

2. En LAN > LAN Cloud, expanda el árbol de Fabric A.
3. Haga clic con el botón derecho del ratón en Canales de puerto.
4. Seleccione Crear canal de puerto.
5. Introduzca 13 como el ID único del canal del puerto.
6. Introduzca VPC-13-Nexus como nombre del canal de puerto.
7. Haga clic en Siguiente.



8. Seleccione los siguientes puertos para añadir al canal de puerto:
   a. ID de ranura 1 y puerto 1
   b. ID de ranura 1 y puerto 2
9. Haga clic en >> para agregar los puertos al canal de puerto.
10. Haga clic en Finish para crear el canal del puerto. Haga clic en Aceptar.

11. En Canales de puerto, seleccione el canal de puerto recién creado.

    El canal del puerto debe tener un estado general de subida.

12. En el panel de navegación, en LAN > LAN Cloud, expanda el árbol de la estructura B.
13. Haga clic con el botón derecho del ratón en Canales de puerto.
14. Seleccione Crear canal de puerto.
15. Introduzca 14 como el ID único del canal del puerto.
16. Introduzca VPC-14-Nexus como nombre del canal de puerto. Haga clic en Siguiente.
17. Seleccione los siguientes puertos para añadir al canal de puerto:
    a. ID de ranura 1 y puerto 1
    b. ID de ranura 1 y puerto 2
18. Haga clic en >> para agregar los puertos al canal de puerto.
19. Haga clic en Finish para crear el canal del puerto. Haga clic en Aceptar.
20. En Canales de puerto, seleccione el puerto-canal recién creado.
21. El canal del puerto debe tener un estado general de subida.

Crear una organización (opcional)

Las organizaciones se utilizan para organizar los recursos y restringir el acceso a varios grupos dentro de la organización DE TI, con lo que permiten el multi-tenancy de los recursos informáticos.

> Aunque este documento no asume el uso de las organizaciones, este procedimiento proporciona instrucciones para crear una.

Para configurar una organización en el entorno Cisco UCS, complete los pasos siguientes:

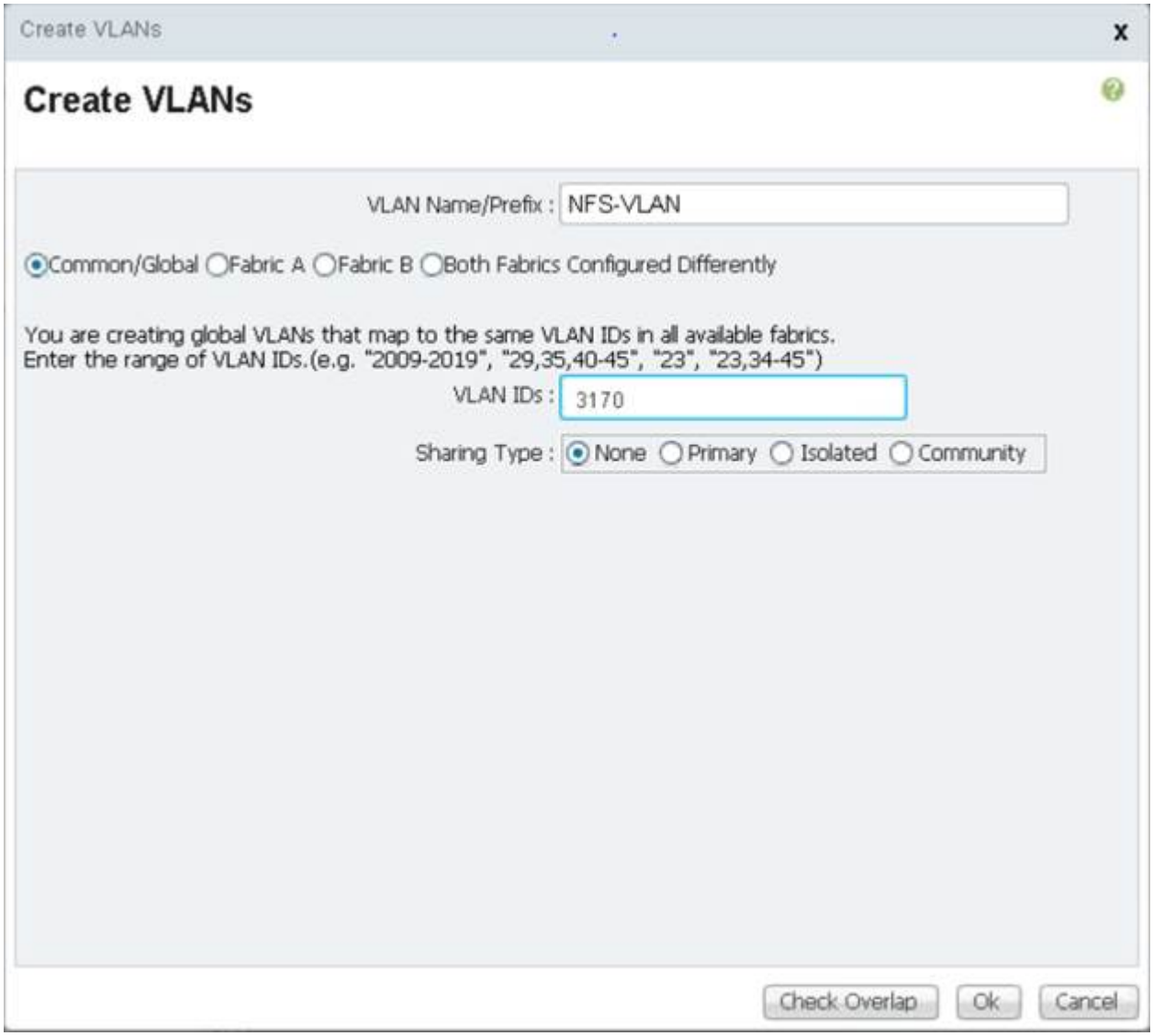
1. En Cisco UCS Manager, en el menú Nuevo de la barra de herramientas, en la parte superior de la ventana, seleccione Crear organización.
2. Escriba un nombre para la organización.
3. Opcional: Introduzca una descripción para la organización. Haga clic en Aceptar.
4. Haga clic en Aceptar en el mensaje de confirmación.

Configure los puertos del dispositivo de almacenamiento y las VLAN de almacenamiento

Para configurar los puertos del dispositivo de almacenamiento y las VLAN de almacenamiento, siga estos pasos:

1. En Cisco UCS Manager, seleccione la pestaña LAN.
2. Amplíe el cloud de dispositivos.
3. Haga clic con el botón derecho en Appliances Cloud.
4. Seleccione Create VLAN.
5. Introduzca NFS-VLAN como el nombre de la VLAN de Infrastructure NFS.
6. Deje común/Global seleccionado.
7. Introduzca `<<var_nfs_vlan_id>>` Para el ID de VLAN.

8. Tipo de uso compartido de baja establecido en Ninguno.

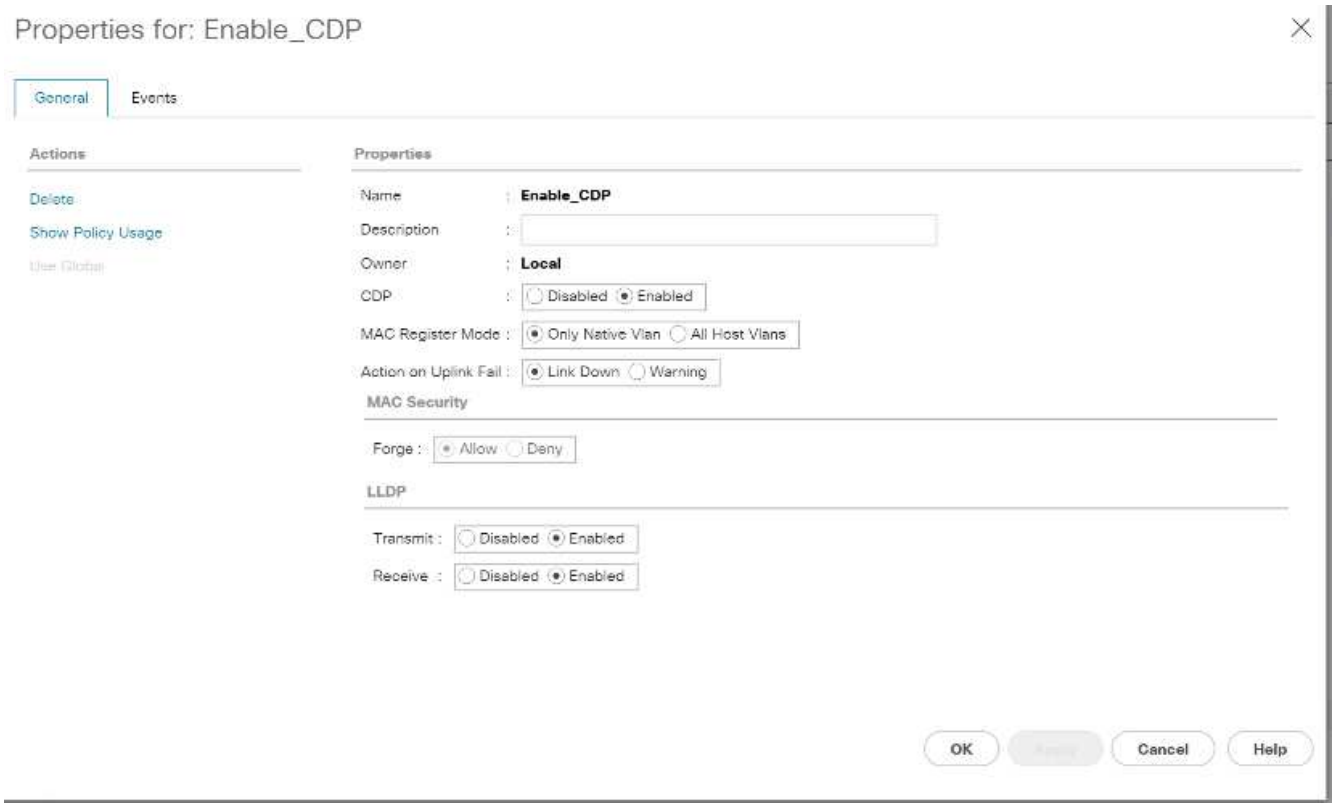


9. Haga clic en OK y, a continuación, vuelva a hacer clic en OK para crear la VLAN.
10. Haga clic con el botón derecho en Appliances Cloud.
11. Seleccione Create VLAN.
12. Introduzca iSCSI-A-VLAN como nombre para la infraestructura iSCSI Fabric A VLAN.
13. Deje común/Global seleccionado.
14. Introduzca `<<var_iscsi-a_vlan_id>>` Para el ID de VLAN.
15. Haga clic en OK y, a continuación, vuelva a hacer clic en OK para crear la VLAN.
16. Haga clic con el botón derecho en Appliances Cloud.
17. Seleccione Create VLAN.
18. Introduzca iSCSI-B-VLAN como nombre para la VLAN de infraestructura iSCSI Fabric B.
19. Deje común/Global seleccionado.
20. Introduzca `<<var_iscsi-b_vlan_id>>` Para el ID de VLAN.
21. Haga clic en OK y, a continuación, vuelva a hacer clic en OK para crear la VLAN.

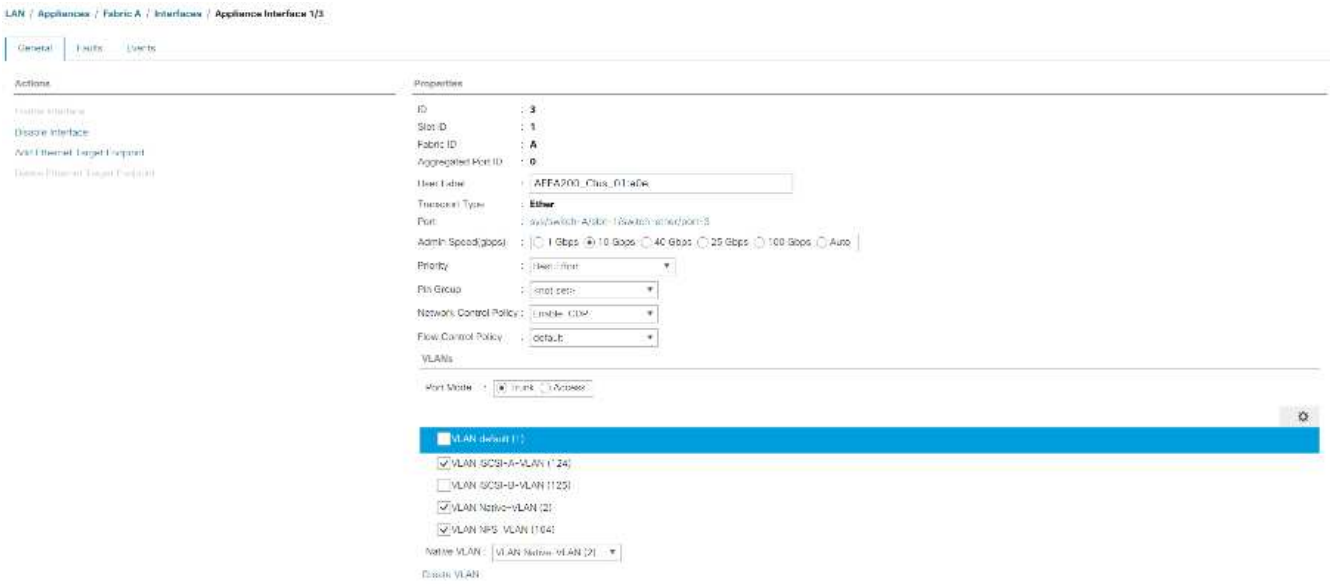
22. Haga clic con el botón derecho en Appliances Cloud.
23. Seleccione Create VLAN.
24. Introduzca Native-VLAN como nombre de la VLAN nativa.
25. Deje común/Global seleccionado.
26. Introduzca `<<var_native_vlan_id>>` Para el ID de VLAN.
27. Haga clic en OK y, a continuación, vuelva a hacer clic en OK para crear la VLAN.



28. En el panel de navegación, en LAN > Directivas, expanda dispositivos y haga clic con el botón derecho del ratón en Directivas de control de red.
29. Seleccione Crear Directiva de control de red.
30. Asigne un nombre a la política `Enable_CDP_LLPD` Y seleccione habilitado junto a CDP.
31. Habilite las funciones de transmisión y recepción para LLDP.



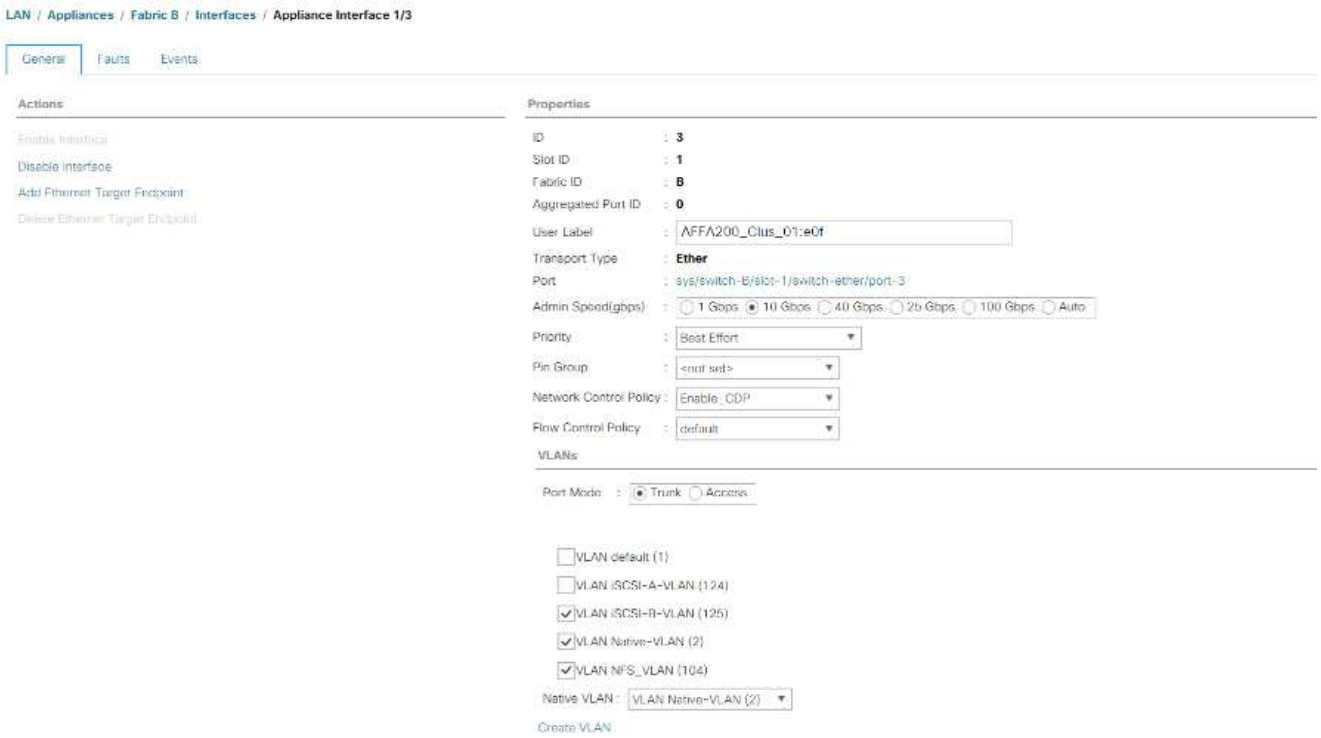
32. Haga clic en Aceptar y, a continuación, vuelva a hacer clic en Aceptar para crear la directiva.
33. En el panel de navegación, en LAN > Appliances Cloud, expanda el árbol de Fabric A.
34. Amplíe las interfaces.
35. Seleccione interfaz de dispositivo 1/3.
36. En el campo etiqueta de usuario, incluya información que indique el puerto de la controladora de almacenamiento; por ejemplo `<storage_controller_01_name>:e0e`. Haga clic en Save Changes y OK.
37. Seleccione Enable_CDP Network Control Policy y seleccione Save Changes (Guardar cambios) y OK (Aceptar).
38. En VLAN, seleccione iSCSI-A-VLAN, NFS VLAN y la VLAN nativa. Establezca la VLAN nativa como VLAN nativa. Borre la selección de VLAN predeterminada.
39. Haga clic en Save Changes y OK.



40. Seleccione Appliance Interface 1/4 en Fabric A.
41. En el campo etiqueta de usuario, incluya información que indique el puerto de la controladora de almacenamiento; por ejemplo `<storage_controller_02_name>:e0e`. Haga clic en Save Changes y OK.
42. Seleccione Enable_CDP Network Control Policy y seleccione Save Changes (Guardar cambios) y OK (Aceptar).
43. En VLAN, seleccione iSCSI-A-VLAN, NFS VLAN y la VLAN nativa.
44. Establezca la VLAN nativa como VLAN nativa.
45. Borre la selección de VLAN predeterminada.
46. Haga clic en Save Changes y OK.
47. En el panel de navegación, en LAN > Appliances Cloud, expanda el árbol de Fabric B.
48. Amplíe las interfaces.
49. Seleccione interfaz de dispositivo 1/3.
50. En el campo etiqueta de usuario, incluya información que indique el puerto de la controladora de

almacenamiento; por ejemplo `<storage_controller_01_name>:e0f`. Haga clic en Save Changes y OK.

51. Seleccione Enable_CDP Network Control Policy y seleccione Save Changes (Guardar cambios) y OK (Aceptar).
52. En VLAN, seleccione iSCSI-B-VLAN, NFS VLAN y la VLAN nativa. Establezca la VLAN nativa como VLAN nativa. Anule la selección de la VLAN predeterminada.



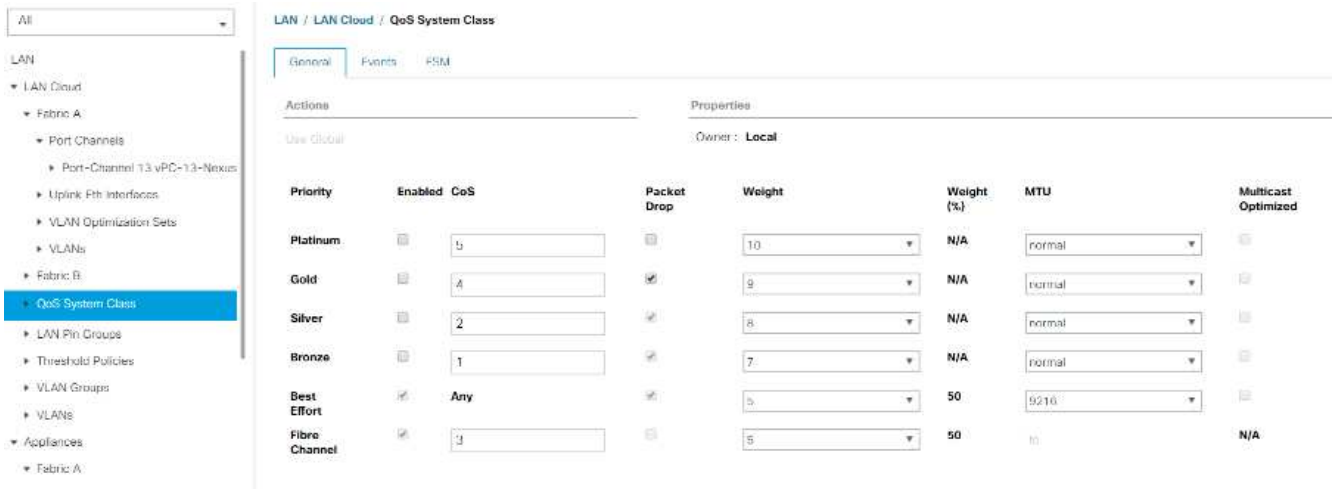
53. Haga clic en Save Changes y OK.
54. Seleccione interfaz de dispositivo 1/4 en Fabric B.
55. En el campo etiqueta de usuario, incluya información que indique el puerto de la controladora de almacenamiento; por ejemplo `<storage_controller_02_name>:e0f`. Haga clic en Save Changes y OK.
56. Seleccione Enable_CDP Network Control Policy y seleccione Save Changes (Guardar cambios) y OK (Aceptar).
57. En VLAN, seleccione iSCSI-B-VLAN, NFS VLAN y la VLAN nativa. Establezca la VLAN nativa como VLAN nativa. Anule la selección de la VLAN predeterminada.
58. Haga clic en Save Changes y OK.

Establezca las tramas gigantes en la estructura de Cisco UCS

Para configurar tramas gigantes y permitir la calidad de servicio en la estructura Cisco UCS, realice los siguientes pasos:

1. En Cisco UCS Manager, en el panel de navegación, haga clic en la pestaña LAN.
2. Seleccione LAN > LAN Cloud > QoS System Class.
3. En el panel derecho, haga clic en la ficha General .

4. En la fila esfuerzo, introduzca 9216 en el cuadro situado bajo la columna MTU.



5. Haga clic en Save Changes.
6. Haga clic en Aceptar.

Reconozca el chasis de Cisco UCS

Para reconocer todos los chasis Cisco UCS, lleve a cabo los siguientes pasos:

1. En Cisco UCS Manager, seleccione la pestaña Equipo y, a continuación, expanda la pestaña equipos de la derecha.
2. Expanda Equipo > chasis.
3. En acciones para el chasis 1, seleccione reconocer chasis.
4. Haga clic en Aceptar y, a continuación, en Aceptar para completar el reconocimiento del chasis.
5. Haga clic en Cerrar para cerrar la ventana Propiedades.

Cargar imágenes de firmware de Cisco UCS 4.0(1b)

Para actualizar el software Cisco UCS Manager y el software Cisco UCS Fabric Interconnect a la versión 4.0(1b), consulte "Guías de instalación y actualización de Cisco UCS Manager".

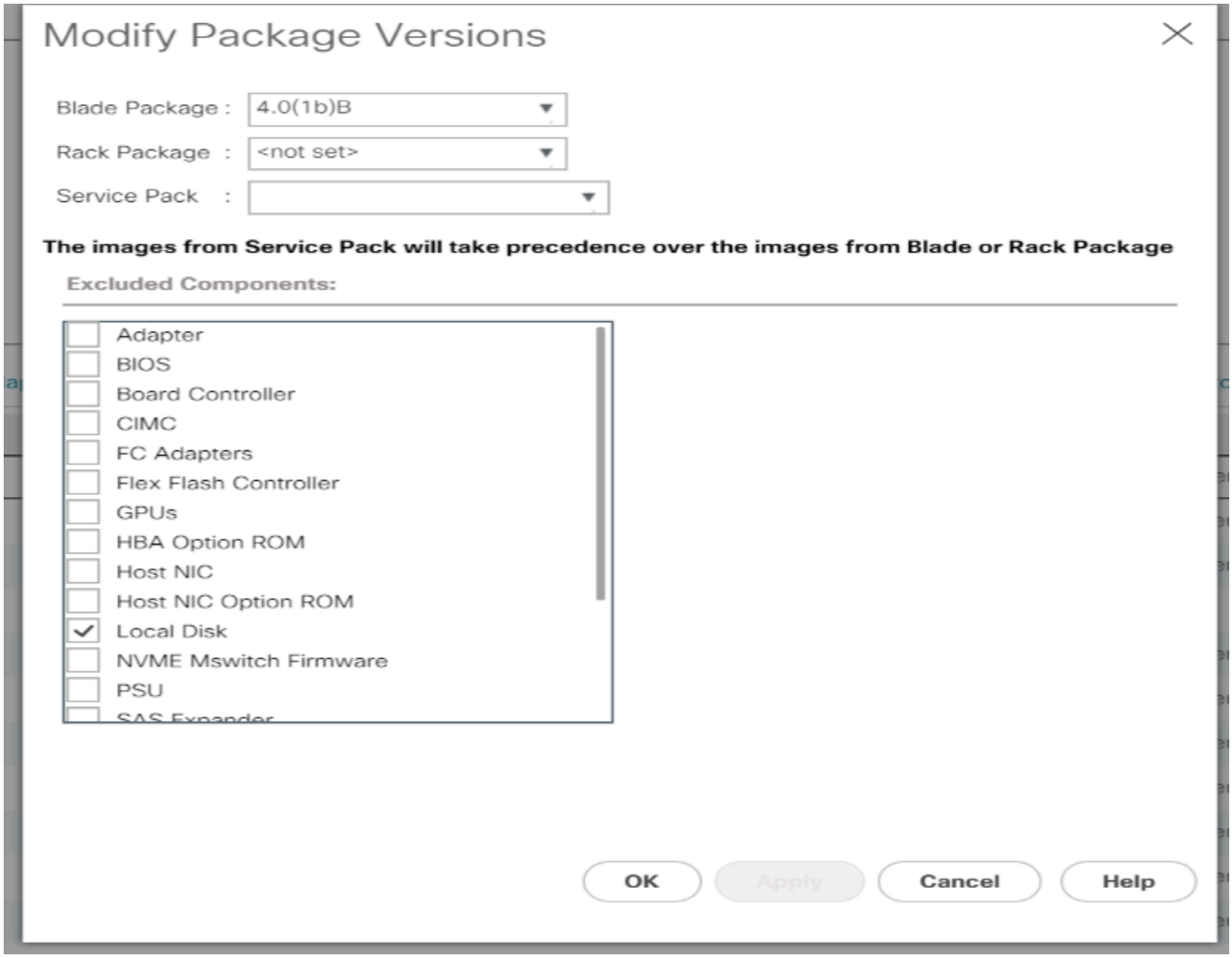
Cree un paquete de firmware del host

Las directivas de administración de firmware permiten al administrador seleccionar los paquetes correspondientes para una configuración de servidor determinada. Estas políticas suelen incluir paquetes para adaptadores, BIOS, controlador de placa, adaptadores de FC, ROM de opción del adaptador de bus de host (HBA) y propiedades de la controladora de almacenamiento.

Para crear una política de gestión de firmware para una configuración de servidor determinada en el entorno de Cisco UCS, lleve a cabo los pasos siguientes:

1. En Cisco UCS Manager, haga clic en Servers (servidores) a la izquierda.
2. Seleccione Policies > root.
3. Expanda Paquetes de firmware del host.
4. Seleccione predeterminado.

5. En el panel acciones, seleccione Modificar versiones de paquete.
6. Seleccione la versión 4.0(1b) para los dos paquetes blade.



7. Haga clic en OK y, a continuación, en OK de nuevo para modificar el paquete de firmware del host.

Crear pools de direcciones MAC

Para configurar los pools de direcciones MAC necesarios para el entorno Cisco UCS, realice los siguientes pasos:

1. En Cisco UCS Manager, haga clic en LAN a la izquierda.
2. Seleccione Pools > raíz.

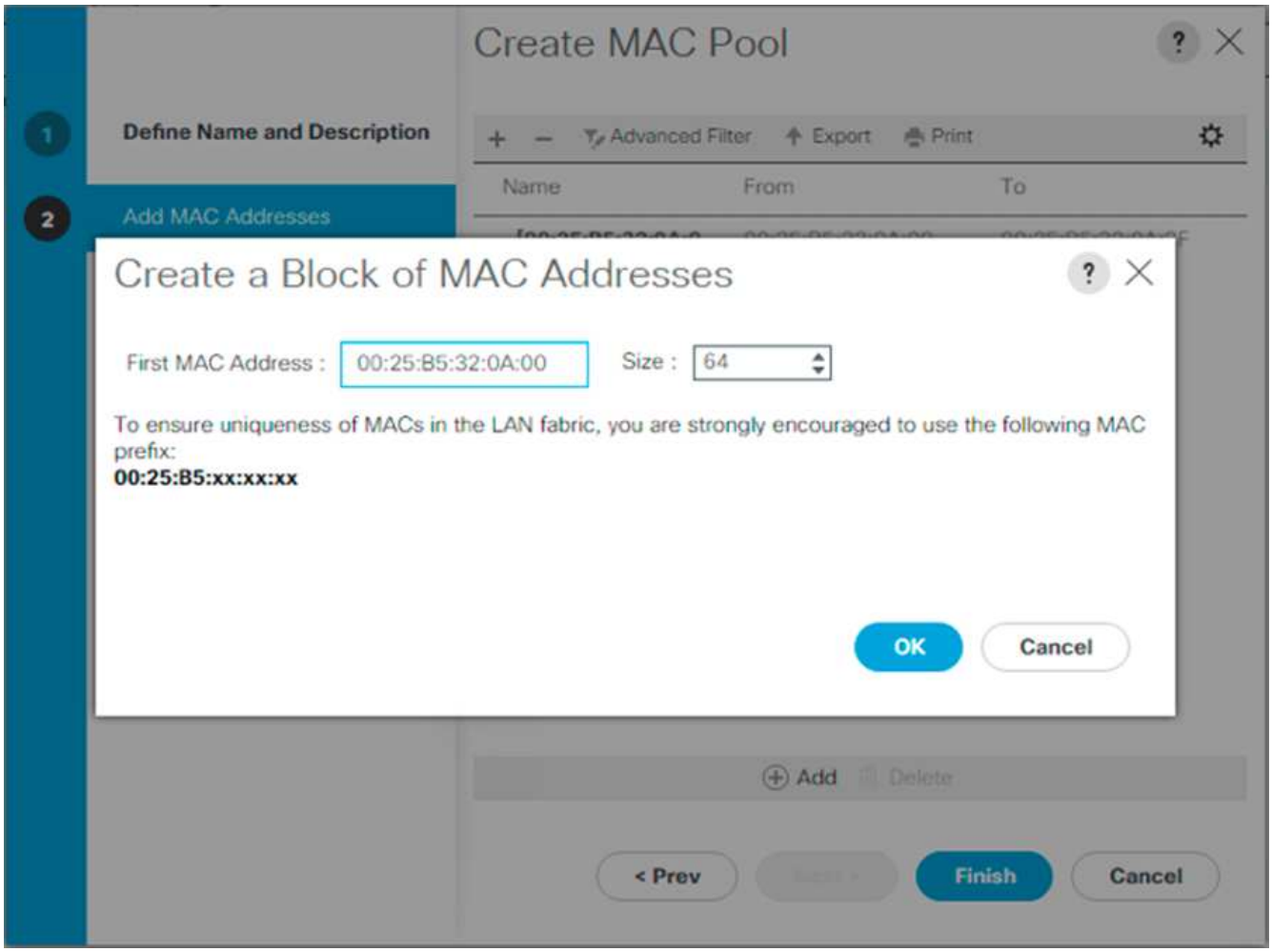
   En este procedimiento, se crean dos grupos de direcciones MAC, uno para cada estructura de conmutación.

3. Haga clic con el botón derecho del ratón en grupos MAC de la organización raíz.
4. Seleccione Crear pool MAC para crear el pool de direcciones MAC.
5. Introduzca MAC-Pool-A como nombre del pool MAC.
6. Opcional: Introduzca una descripción para el grupo MAC.
7. Seleccione secuencial como opción para Orden de asignación. Haga clic en Siguiente.

8. Haga clic en Añadir.
9. Especifique una dirección MAC inicial.

> Para la solución FlexPod, se recomienda colocar 0A en el octeto siguiente al último de la dirección MAC inicial para identificar todas las direcciones MAC como direcciones de la estructura A. En nuestro ejemplo, hemos seguido el ejemplo de incrustar también la información de número de dominio de Cisco UCS, que nos proporciona 00:25:B5:32:0A:00 como primera dirección MAC.

10. Especifique un tamaño para el grupo de direcciones MAC que sea suficiente para admitir los recursos de servidor o blade disponibles. Haga clic en Aceptar.



11. Haga clic en Finalizar.
12. En el mensaje de confirmación, haga clic en Aceptar.
13. Haga clic con el botón derecho del ratón en grupos MAC de la organización raíz.
14. Seleccione Crear pool MAC para crear el pool de direcciones MAC.
15. Introduzca MAC-Pool-B como nombre del pool MAC.
16. Opcional: Introduzca una descripción para el grupo MAC.
17. Seleccione secuencial como opción para Orden de asignación. Haga clic en Siguiente.
18. Haga clic en Añadir.

19. Especifique una dirección MAC inicial.

> Para la solución FlexPod, se recomienda colocar 0B en el siguiente al último octeto de la dirección MAC inicial para identificar todas las direcciones MAC de este grupo como direcciones de la estructura B. Una vez más, hemos seguido adelante en nuestro ejemplo de incrustar también la información de número de dominio de Cisco UCS, que nos proporciona 00:25:B5:32:0B:00 como nuestra primera dirección MAC.

20. Especifique un tamaño para el grupo de direcciones MAC que sea suficiente para admitir los recursos de servidor o blade disponibles. Haga clic en Aceptar.
21. Haga clic en Finalizar.
22. En el mensaje de confirmación, haga clic en Aceptar.

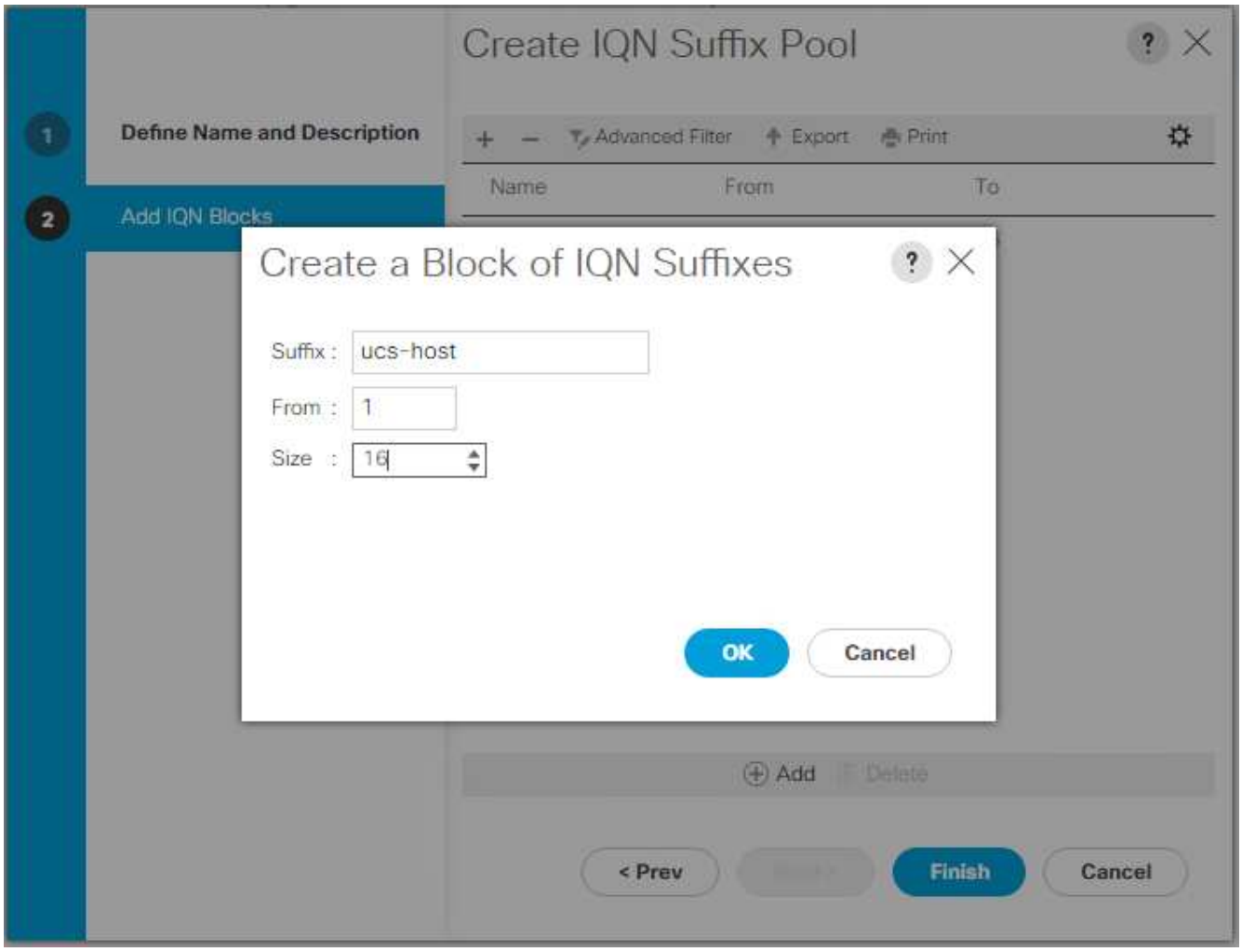
Cree un pool IQN de iSCSI

Para configurar los pools IQN necesarios para el entorno Cisco UCS, complete los siguientes pasos:

1. En Cisco UCS Manager, haga clic en SAN a la izquierda.
2. Seleccione Pools > raíz.
3. Haga clic con el botón derecho en IQN Pools.
4. Seleccione Create IQN Suffix Pool para crear el pool IQN.
5. Introduzca IQN-Pool para el nombre del pool IQN.
6. Opcional: Introduzca una descripción para el pool de IQN.
7. Introduzca `iqn.1992-08.com.cisco` como prefijo.
8. Seleccione secuencial para orden de asignación. Haga clic en Siguiente.
9. Haga clic en Añadir.
10. Introduzca `ucs-host` como sufijo.

> Si se utilizan varios dominios de Cisco UCS, es posible que deba utilizar un sufijo IQN más específico.

11. Introduzca 1 en el campo de.
12. Especifique el tamaño del bloque de IQN suficiente para admitir los recursos del servidor disponibles. Haga clic en Aceptar.



13. Haga clic en Finalizar.

Cree pools de direcciones IP del iniciador de iSCSI

Para configurar el arranque iSCSI de los pools IP necesarios para el entorno Cisco UCS, realice los pasos siguientes:

1. En Cisco UCS Manager, haga clic en LAN a la izquierda.
2. Seleccione Pools > raíz.
3. Haga clic con el botón derecho en IP Pools.
4. Seleccione Crear Pool IP.
5. Introduzca iSCSI-IP-Pool-A como nombre del pool IP.
6. Opcional: Introduzca una descripción para el grupo IP.
7. Seleccione secuencial para la orden de asignación. Haga clic en Siguiente.
8. Haga clic en Agregar para agregar un bloque de dirección IP.
9. En el campo from, introduzca el principio del rango que se asignará como direcciones IP de iSCSI.
10. Establezca el tamaño en direcciones suficientes para acomodar los servidores. Haga clic en Aceptar.
11. Haga clic en Siguiente.
12. Haga clic en Finalizar.

13. Haga clic con el botón derecho en IP Pools.
14. Seleccione Crear Pool IP.
15. Introduzca iSCSI-IP-Pool-B como nombre del pool IP.
16. Opcional: Introduzca una descripción para el grupo IP.
17. Seleccione secuencial para la orden de asignación. Haga clic en Siguiente.
18. Haga clic en Agregar para agregar un bloque de dirección IP.
19. En el campo from, introduzca el principio del rango que se asignará como direcciones IP de iSCSI.
20. Establezca el tamaño en direcciones suficientes para acomodar los servidores. Haga clic en Aceptar.
21. Haga clic en Siguiente.
22. Haga clic en Finalizar.

Cree un pool de sufijos UUID

Para configurar el pool de sufijos de identificador único universal (UUID) necesario para el entorno de Cisco UCS, complete los siguientes pasos:

1. En Cisco UCS Manager, haga clic en Servers (servidores) a la izquierda.
2. Seleccione Pools > raíz.
3. Haga clic con el botón derecho en grupos de sufijo de UUID.
4. Seleccione Crear pool de sufijo de UUID.
5. Introduzca UUID-Pool como el nombre del pool de sufijos de UUID.
6. Opcional: Introduzca una descripción para el pool de sufijos UUID.
7. Mantenga el prefijo en la opción derivada.
8. Seleccione secuencial para la orden de asignación.
9. Haga clic en Siguiente.
10. Haga clic en Add para añadir un bloque de UUID.
11. Mantenga el campo de en el valor predeterminado.
12. Especifique un tamaño para el bloque UUID que sea suficiente para admitir los recursos blade o de servidor disponibles. Haga clic en Aceptar.
13. Haga clic en Finalizar.
14. Haga clic en Aceptar.

Cree un pool de servidores

Para configurar el pool de servidores necesario para el entorno Cisco UCS, lleve a cabo los pasos siguientes:

> Considere la posibilidad de crear pools de servidores únicos para lograr la granularidad necesaria en su entorno.

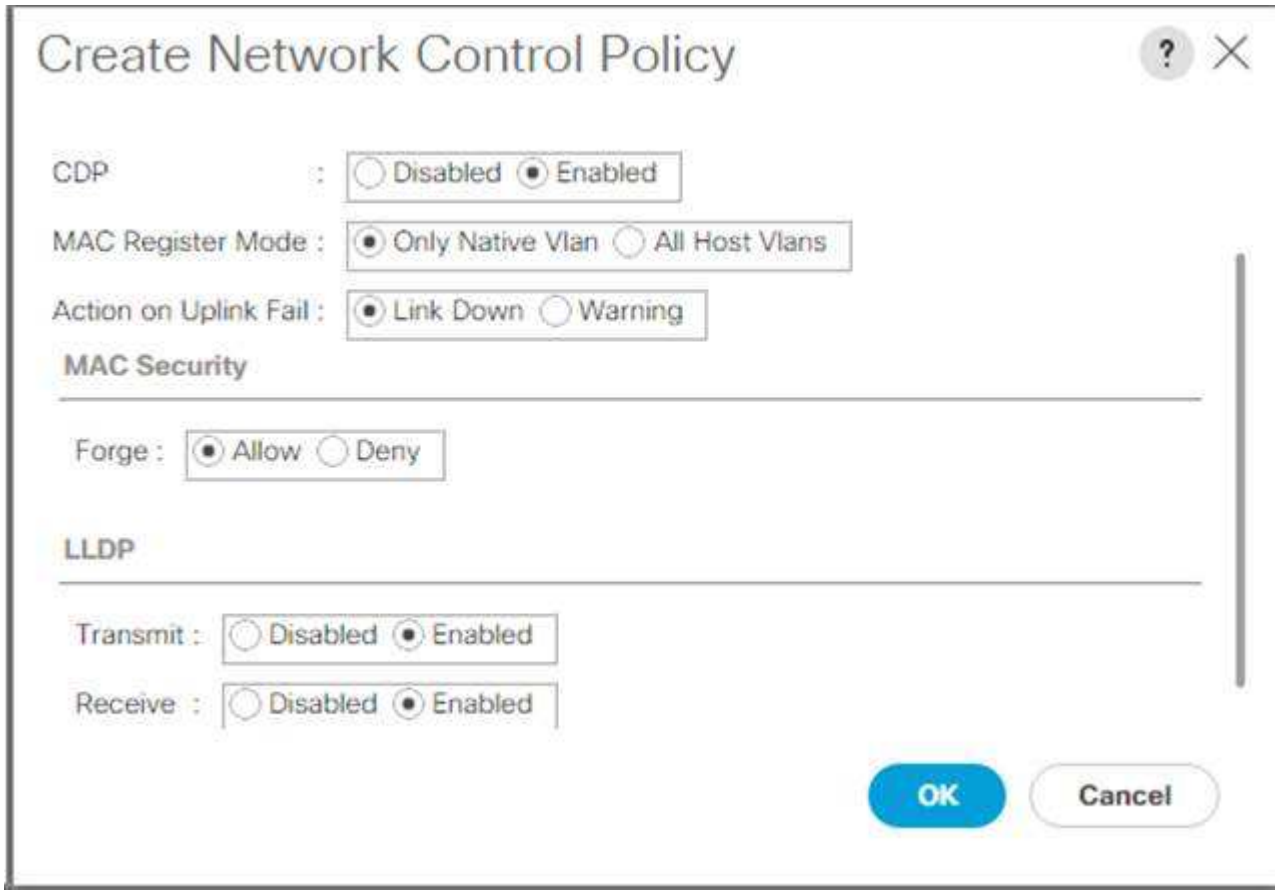
1. En Cisco UCS Manager, haga clic en Servers (servidores) a la izquierda.
2. Seleccione Pools > raíz.
3. Haga clic con el botón derecho en grupos de servidores.

4. Seleccione Crear Pool de servidores.
5. Escriba "Infra-Pool" como nombre del pool de servidores.
6. Opcional: Introduzca una descripción para el pool de servidores. Haga clic en Siguiente.
7. Seleccione dos (o más) servidores que se utilizarán para el clúster de gestión de VMware y haga clic en >> para añadirlos al pool "servidor de infra-Pool".
8. Haga clic en Finalizar.
9. Haga clic en Aceptar.

Cree una política de control de red para el protocolo de descubrimiento de Cisco y el protocolo de detección de la capa de enlace

Para crear una política de control de red para el protocolo de descubrimiento de Cisco (CDP) y el protocolo de detección de capas de vínculo (LLDP), lleve a cabo los siguientes pasos:

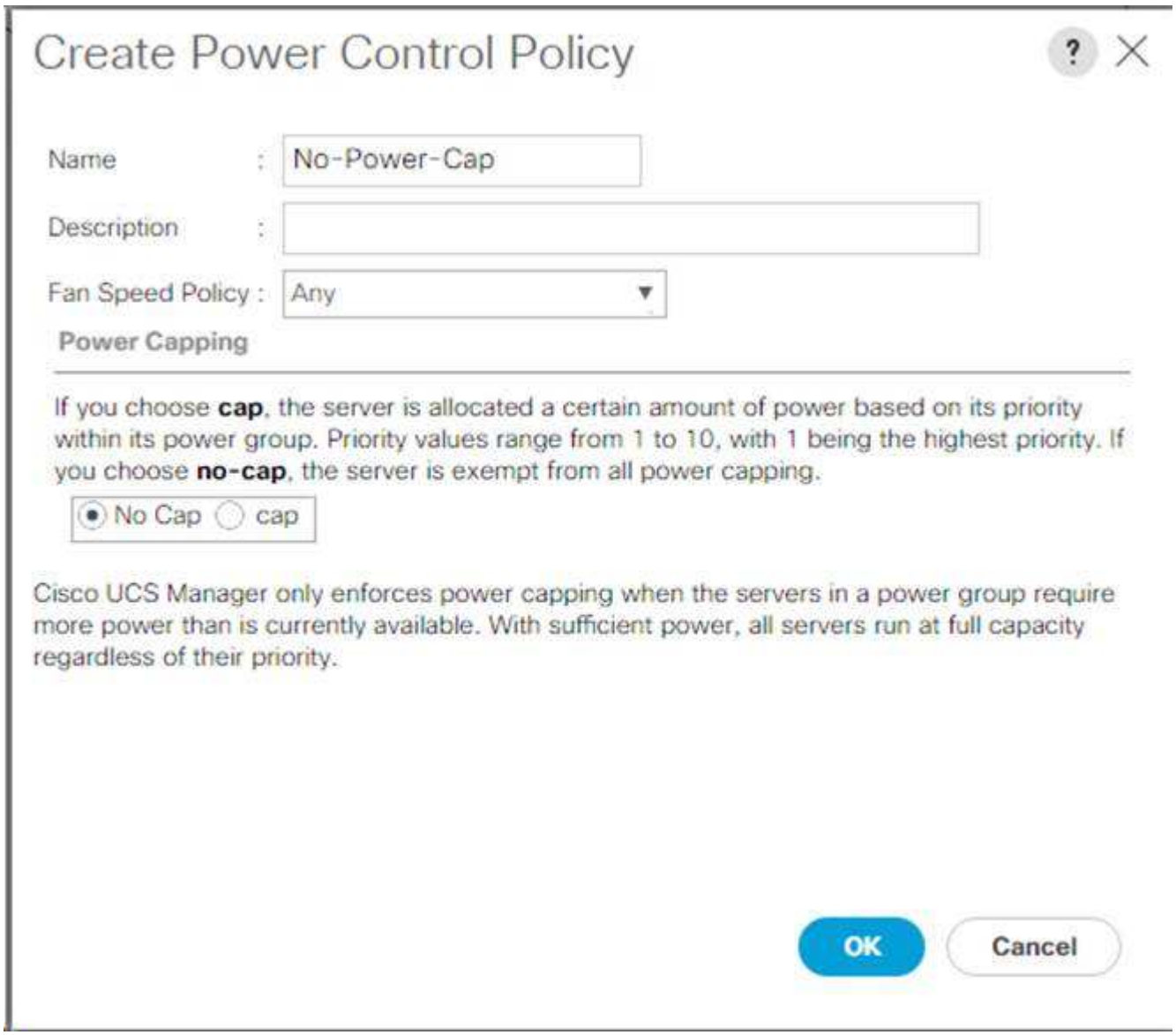
1. En Cisco UCS Manager, haga clic en LAN a la izquierda.
2. Seleccione Policies > root.
3. Haga clic con el botón derecho en Directivas de control de red.
4. Seleccione Crear Directiva de control de red.
5. Introduzca el nombre de la política Enable-CDP-LLDP.
6. Para CDP, seleccione la opción Enabled.
7. Para LLDP, desplácese hacia abajo y seleccione Enabled tanto para transmisión como para recepción.
8. Haga clic en Aceptar para crear la directiva de control de red. Haga clic en Aceptar.



Crear política de control de potencia

Para crear una política de control de alimentación para el entorno Cisco UCS, lleve a cabo los pasos siguientes:

1. En Cisco UCS Manager, haga clic en la pestaña servidores de la izquierda.
2. Seleccione Policies > root.
3. Haga clic con el botón derecho del ratón en Directivas de control de energía.
4. Seleccione Crear política de control de alimentación.
5. Introduzca sin tapa de alimentación como nombre de la política de control de alimentación.
6. Cambie la configuración de la tapa de alimentación a sin tapa.
7. Haga clic en Aceptar para crear la política de control de alimentación. Haga clic en Aceptar.

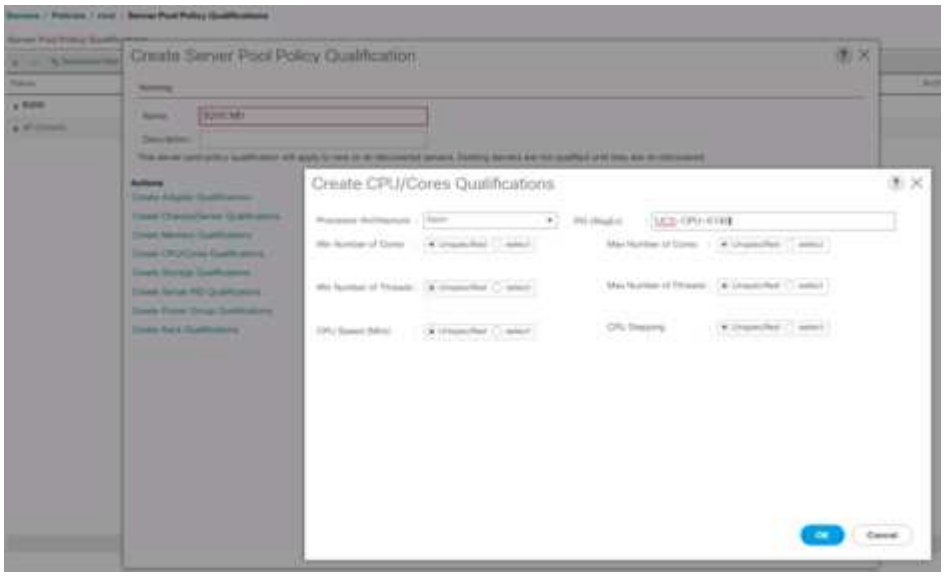


Crear política de calificación de pool de servidores (opcional)

Para crear una política de cualificación de pool de servidores opcional para el entorno Cisco UCS, realice los pasos siguientes:

Este ejemplo crea una política para los servidores Cisco UCS B-Series con los procesadores Intel E2660 v4 Xeon Broadwell.

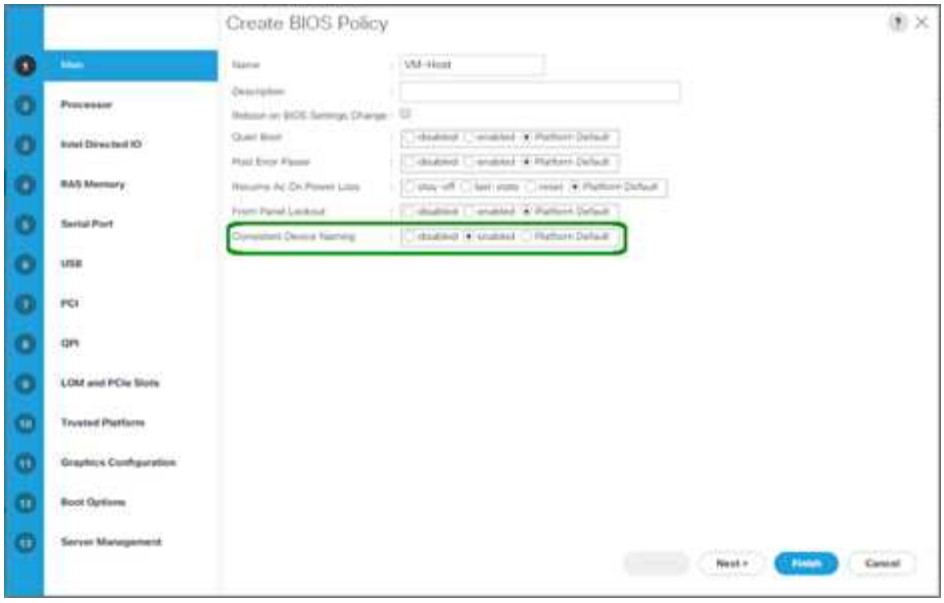
1. En Cisco UCS Manager, haga clic en Servers (servidores) a la izquierda.
2. Seleccione Policies > root.
3. Seleccione requisitos de directiva de pool de servidores.
4. Seleccione Crear calificación de directiva de grupo de servidores o Agregar.
5. Asigne un nombre a la política Intel.
6. Seleccione Crear CPU/calificaciones de núcleos.
7. Seleccione Xeon en el procesador/arquitectura.
8. Introduzca `<UCS-CPU- PID>` Como el ID de proceso (PID).
9. Haga clic en Aceptar para crear la calificación CPU/Core.
10. Haga clic en Aceptar para crear la directiva y, a continuación, haga clic en Aceptar para confirmar la directiva.



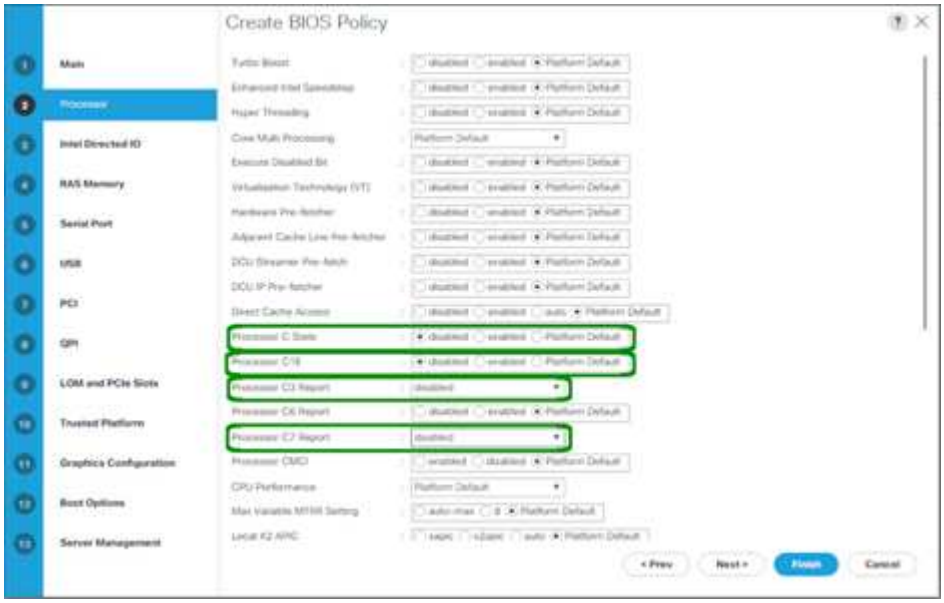
Crear directiva de BIOS del servidor

Para crear una política de BIOS de servidor para el entorno Cisco UCS, complete los pasos siguientes:

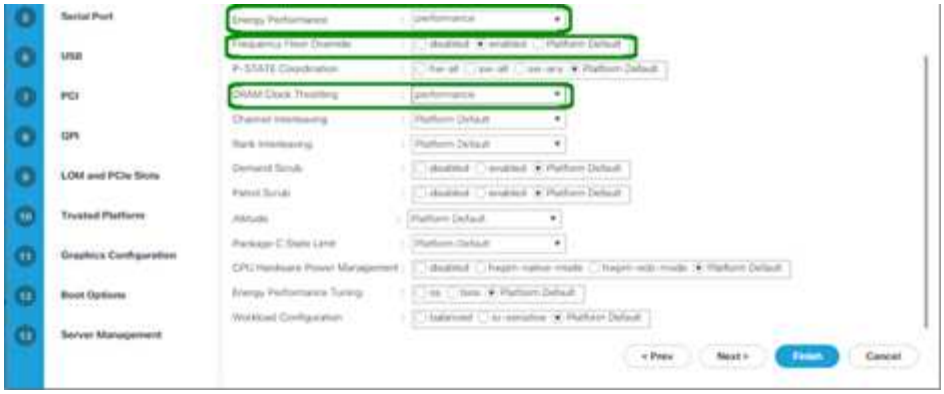
1. En Cisco UCS Manager, haga clic en Servers (servidores) a la izquierda.
2. Seleccione Policies > root.
3. Haga clic con el botón derecho del ratón en Directivas de BIOS.
4. Seleccione Crear directiva de BIOS.
5. Escriba VM-Host como nombre de la política del BIOS.
6. Cambie la configuración de arranque silencioso a Desactivado.
7. Cambie la asignación de nombres de dispositivos coherente a Activado.



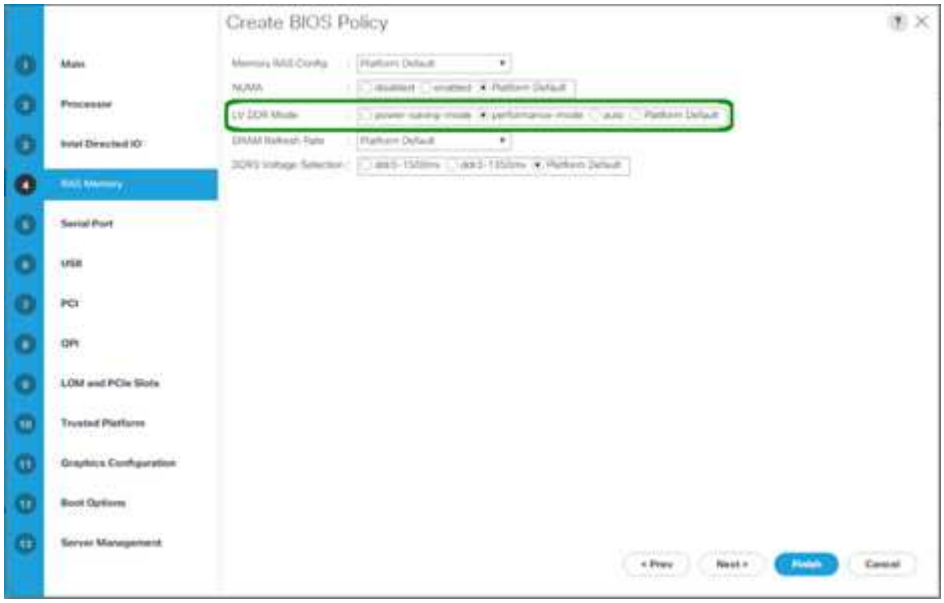
8. Seleccione la ficha procesador y configure los siguientes parámetros:
   - Estado del procesador C: Desactivado
   - Procesador C1E: Desactivado
   - Informe C3 del procesador: Desactivado
   - Informe del procesador C7: Desactivado



9. Desplácese hasta las opciones restantes del procesador y configure los siguientes parámetros:
   - Rendimiento energético: Rendimiento
   - Sustitución de suelo de frecuencia: Activada
   - Regulación del reloj DRAM: Rendimiento



10. Haga clic en memoria RAS y establezca los siguientes parámetros:
    - Modo DDR LV: Modo de rendimiento

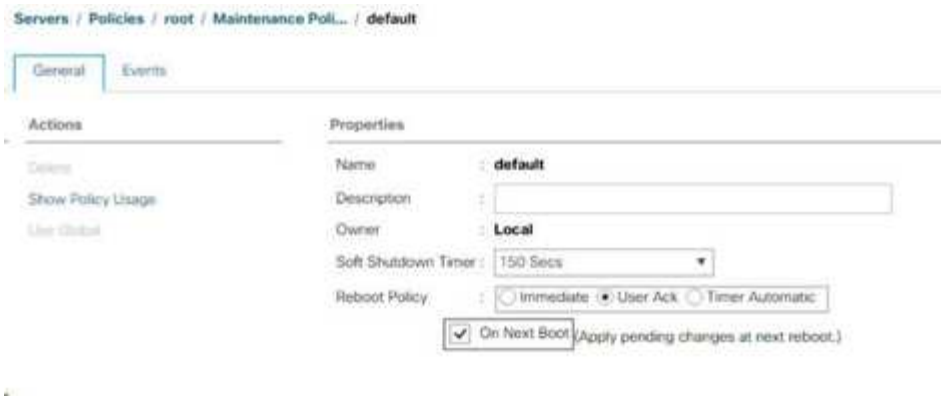


11. Haga clic en Finalizar para crear la directiva de BIOS.
12. Haga clic en Aceptar.

Actualice la directiva de mantenimiento predeterminada

Para actualizar la directiva de mantenimiento predeterminada, lleve a cabo los siguientes pasos:

1. En Cisco UCS Manager, haga clic en Servers (servidores) a la izquierda.
2. Seleccione Policies > root.
3. Seleccione Directivas de mantenimiento > predeterminado.
4. Cambie la directiva de reinicio a Ack de usuario.
5. Seleccione en Siguiente arranque para delegar las ventanas de mantenimiento a los administradores del servidor.



6. Haga clic en Save Changes.
7. Haga clic en Aceptar para aceptar el cambio.

Cree plantillas VNIC

Para crear varias plantillas de tarjeta de interfaz de red virtual (VNIC) para el entorno de Cisco UCS, complete los procedimientos descritos en esta sección.

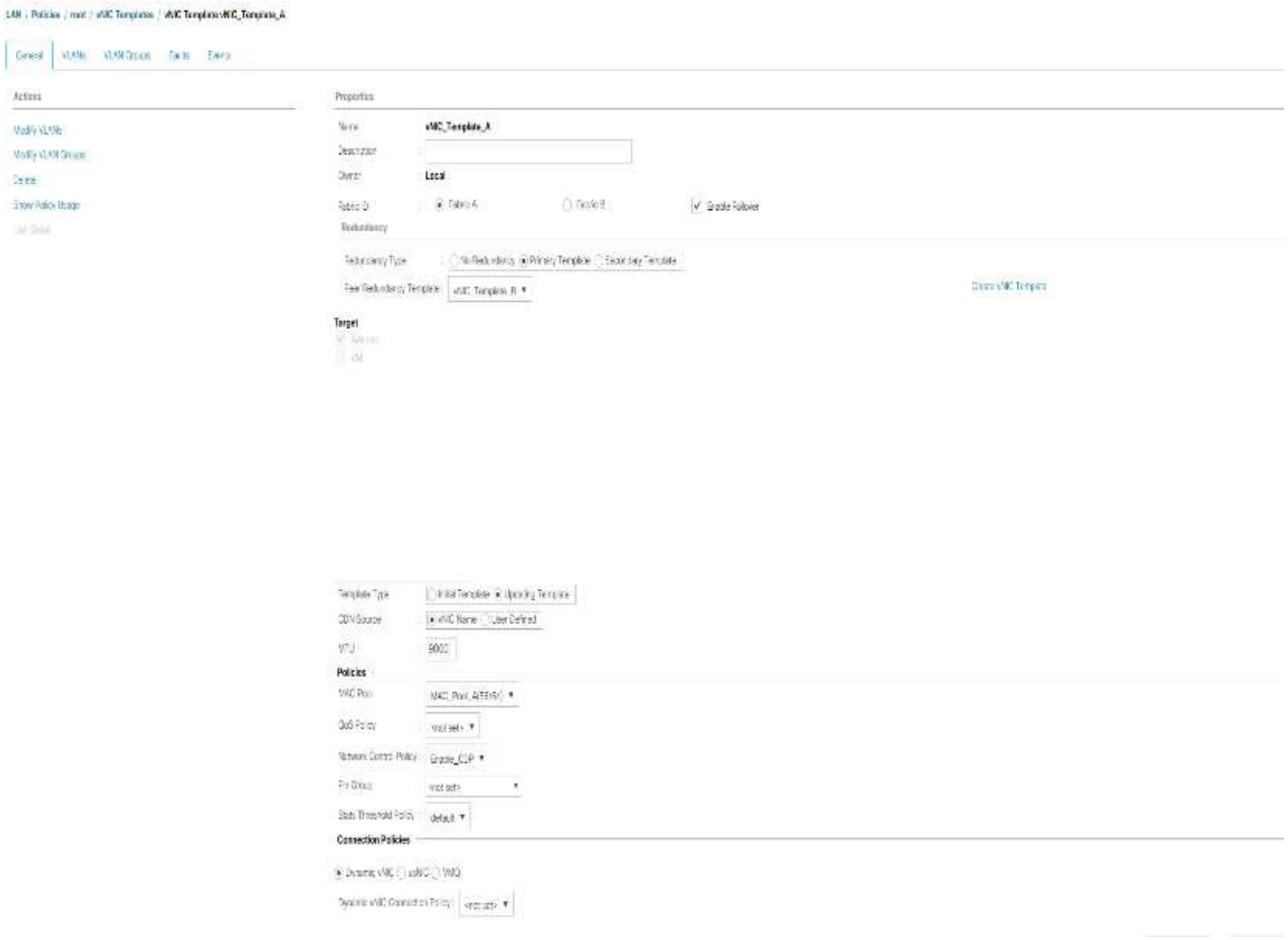
Se crea un total de cuatro plantillas VNIC.

Crear NIC virtuales de infraestructura

Para crear una infraestructura VNIC, lleve a cabo los siguientes pasos:

1. En Cisco UCS Manager, haga clic en LAN a la izquierda.
2. Seleccione Policies > root.
3. Haga clic con el botón derecho del ratón en Plantillas VNIC.
4. Seleccione Crear plantilla VNIC.
5. Introduzca `Site-XX-vNIC_A` Como nombre de plantilla VNIC.
6. Seleccione Actualizar plantilla como el Tipo de plantilla.
7. Para Fabric ID, seleccione Fabric A.
8. Asegúrese de que la opción Activar conmutación por error no esté seleccionada.
9. Seleccione plantilla principal para Tipo de redundancia.
10. Deje la plantilla de redundancia del mismo nivel establecida en `<not set>`.
11. En destino, asegúrese de que sólo está seleccionada la opción adaptador.
12. Configurado `Native-VLAN` Como la VLAN nativa.
13. Seleccione Nombre VNIC para el origen CDN.
14. Para MTU, introduzca 9000.
15. En VLAN permitidas, seleccione `Native-VLAN, Site-XX-IB-MGMT, Site-XX-NFS, Site-XX-VM-Traffic`, Y Site-XX-vMotion. Utilice la tecla Ctrl para realizar esta selección múltiple.
16. Haga clic en Select. Estas VLAN ahora deben aparecer en las VLAN seleccionadas.
17. En la lista MAC Pool, seleccione `MAC_Pool_A`.

18. En la lista Directiva de control de red, seleccione Pool-A.
19. En la lista Network Control Policy, seleccione Enable-CDP-LLDP.
20. Haga clic en Aceptar para crear la plantilla VNIC.
21. Haga clic en Aceptar.

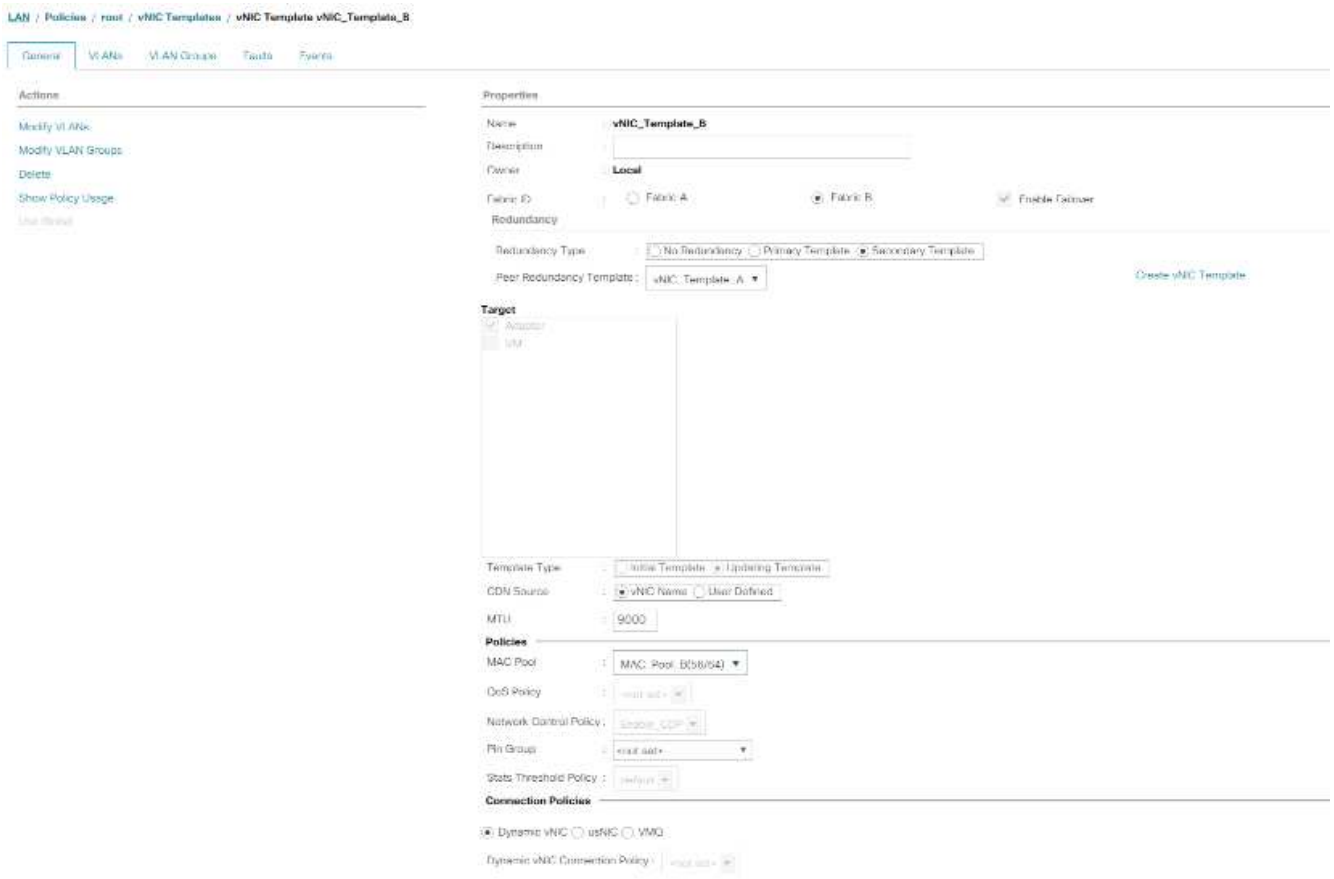


Para crear la plantilla de redundancia secundaria infra-B, lleve a cabo los siguientes pasos:

1. En Cisco UCS Manager, haga clic en LAN a la izquierda.
2. Seleccione Policies > root.
3. Haga clic con el botón derecho del ratón en Plantillas VNIC.
4. Seleccione Crear plantilla VNIC.
5. Introduzca "site-XX-VNIC_B 'como nombre de plantilla VNIC.
6. Seleccione Actualizar plantilla como el Tipo de plantilla.
7. Para Fabric ID, seleccione Fabric B.
8. Seleccione la opción Habilitar conmutación por error.

La selección de la opción de recuperación tras fallos es un paso crítico para mejorar el tiempo de recuperación tras fallos de enlaces, ya que la gestión se lleva a cabo a nivel de hardware y la protección frente a cualquier posible fallo de NIC que no detecte el switch virtual.

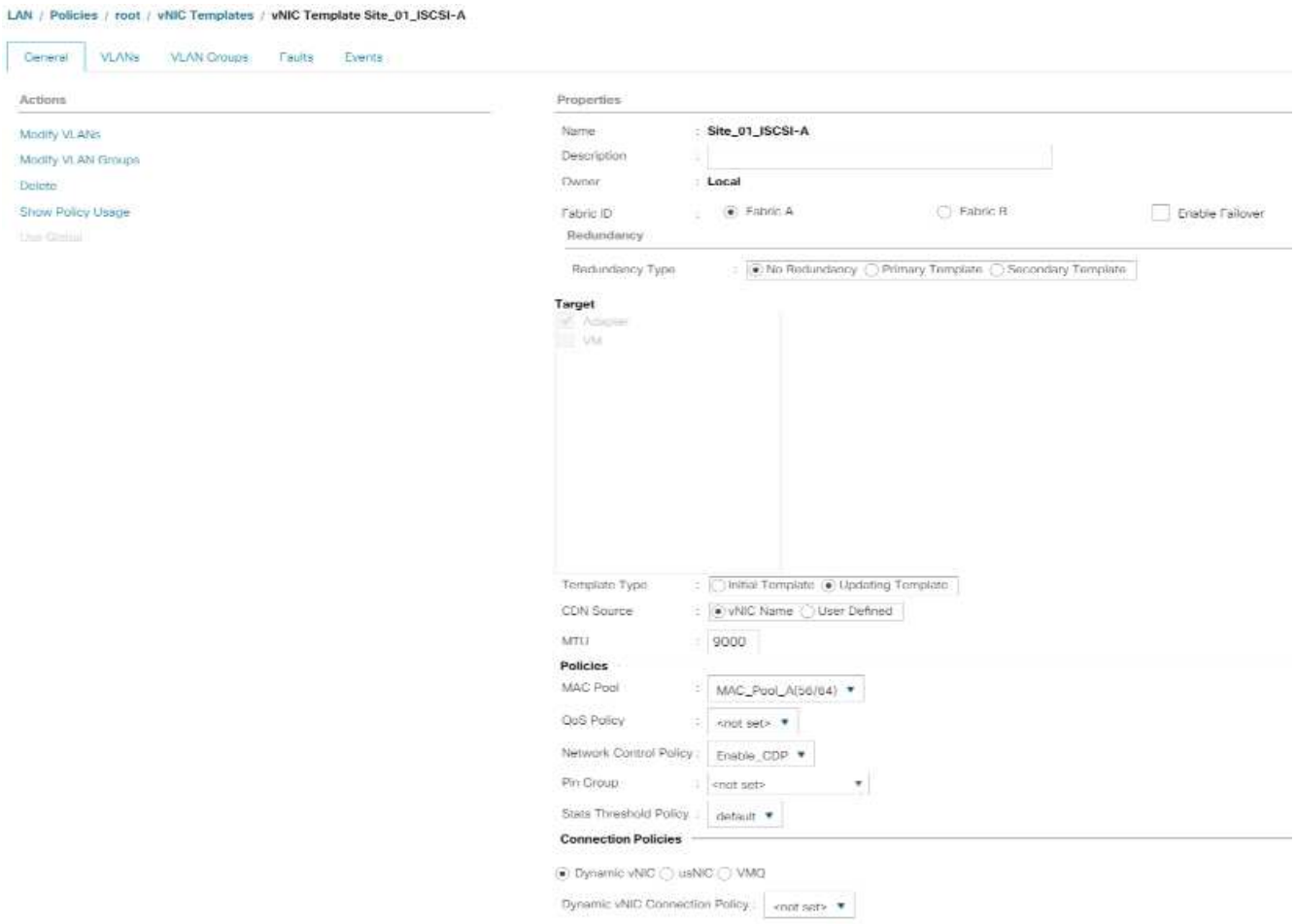
9. Seleccione plantilla principal para Tipo de redundancia.
10. Deje la plantilla de redundancia del mismo nivel establecida en `vNIC_Template_A`.
11. En destino, asegúrese de que sólo está seleccionada la opción adaptador.
12. Configurado `Native-VLAN` Como la VLAN nativa.
13. Seleccione Nombre VNIC para el origen CDN.
14. Para MTU, introduzca `9000`.
15. En VLAN permitidas, seleccione `Native-VLAN, Site-XX-IB-MGMT, Site-XX-NFS, Site-XX-VM-Traffic`, Y Site-XX-vMotion. Utilice la tecla Ctrl para realizar esta selección múltiple.
16. Haga clic en Select. Estas VLAN ahora deben aparecer en las VLAN seleccionadas.
17. En la lista MAC Pool, seleccione `MAC_Pool_B`.
18. En la lista Directiva de control de red, seleccione Pool-B.
19. En la lista Network Control Policy, seleccione Enable-CDP-LLDP.
20. Haga clic en Aceptar para crear la plantilla VNIC.
21. Haga clic en Aceptar.



Cree NIC iSCSI

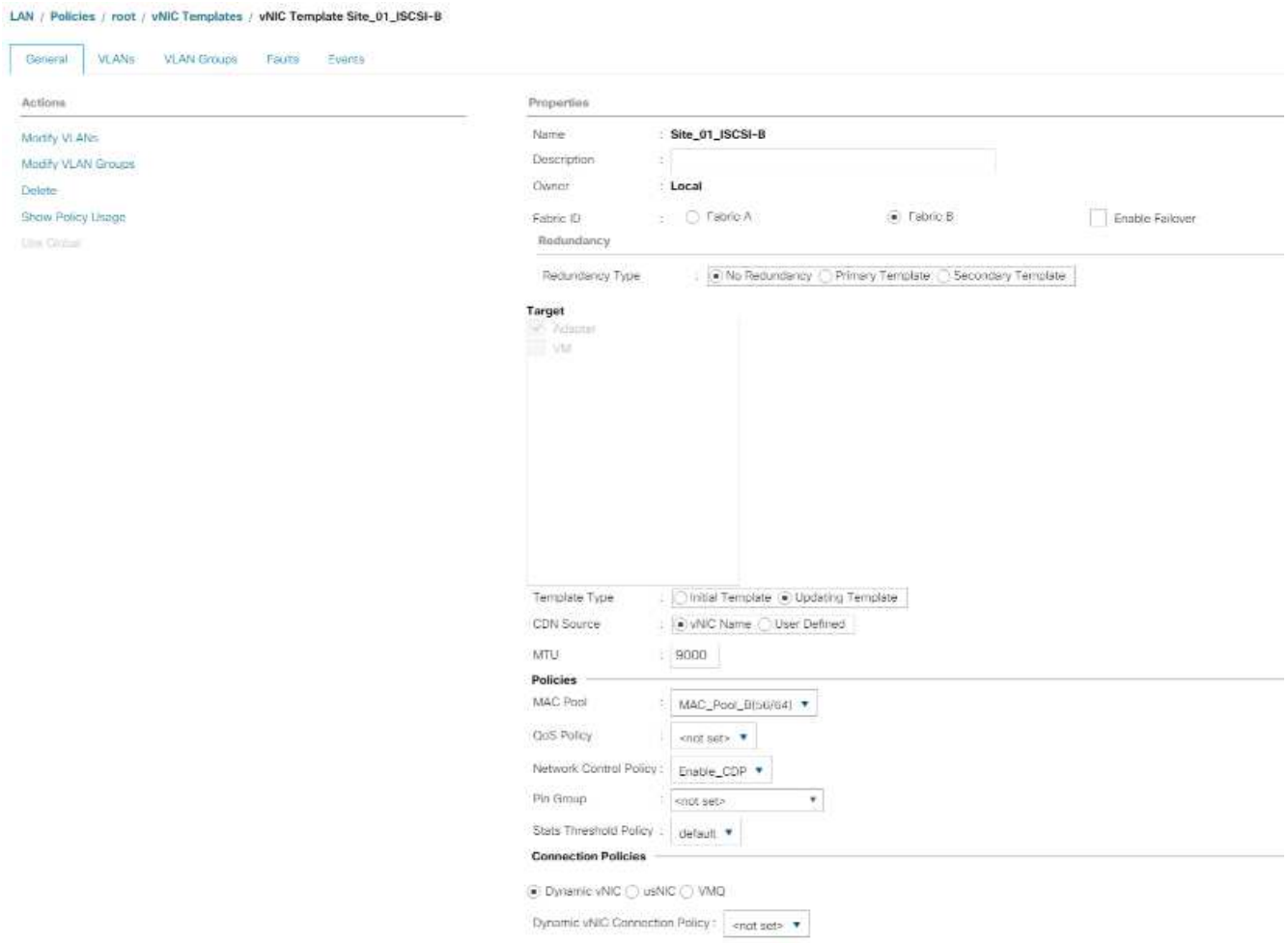
Para crear NIC iSCSI, lleve a cabo los siguientes pasos:

1. Seleccione LAN a la izquierda.
2. Seleccione Policies > root.
3. Haga clic con el botón derecho del ratón en Plantillas VNIC.
4. Seleccione Crear plantilla VNIC.
5. Introduzca `Site- 01-iSCSI_A` Como nombre de plantilla VNIC.
6. Seleccione Fabric A. No seleccione la opción Activar conmutación por error.
7. Deje el tipo de redundancia establecido en sin redundancia.
8. En destino, asegúrese de que sólo está seleccionada la opción adaptador.
9. Seleccione Actualizar plantilla para Tipo de plantilla.
10. En VLAN, seleccione Only Site- 01-iSCSI_A_VLAN.
11. Seleccione Site- 01-iSCSI_A_VLAN como VLAN nativa.
12. Deje el nombre VNIC establecido para el origen CDN.
13. En MTU, introduzca 9000.
14. En la lista MAC Pool, seleccione MAC-Pool-A.
15. En la lista Network Control Policy, seleccione Enable-CDP-LLDP.
16. Haga clic en Aceptar para completar la creación de la plantilla VNIC.
17. Haga clic en Aceptar.



18. Seleccione LAN a la izquierda.
19. Seleccione Policies > root.
20. Haga clic con el botón derecho del ratón en Plantillas VNIC.
21. Seleccione Crear plantilla VNIC.
22. Introduzca `Site- 01-iSCSI_B` Como nombre de plantilla VNIC.
23. Seleccione Fabric B. No seleccione la opción Activar conmutación por error.
24. Deje el tipo de redundancia establecido en sin redundancia.
25. En destino, asegúrese de que sólo está seleccionada la opción adaptador.
26. Seleccione Actualizar plantilla para Tipo de plantilla.
27. En VLAN, seleccione solo `Site- 01-iSCSI_B_VLAN`.
28. Seleccione `Site- 01-iSCSI_B_VLAN` Como la VLAN nativa.
29. Deje el nombre VNIC establecido para el origen CDN.
30. En MTU, introduzca 9000.
31. En la lista Pool MAC, seleccione `MAC-Pool-B`.
32. En la lista Directiva de control de red, seleccione `Enable-CDP-LLDP`.
33. Haga clic en Aceptar para completar la creación de la plantilla VNIC.

34. Haga clic en Aceptar.



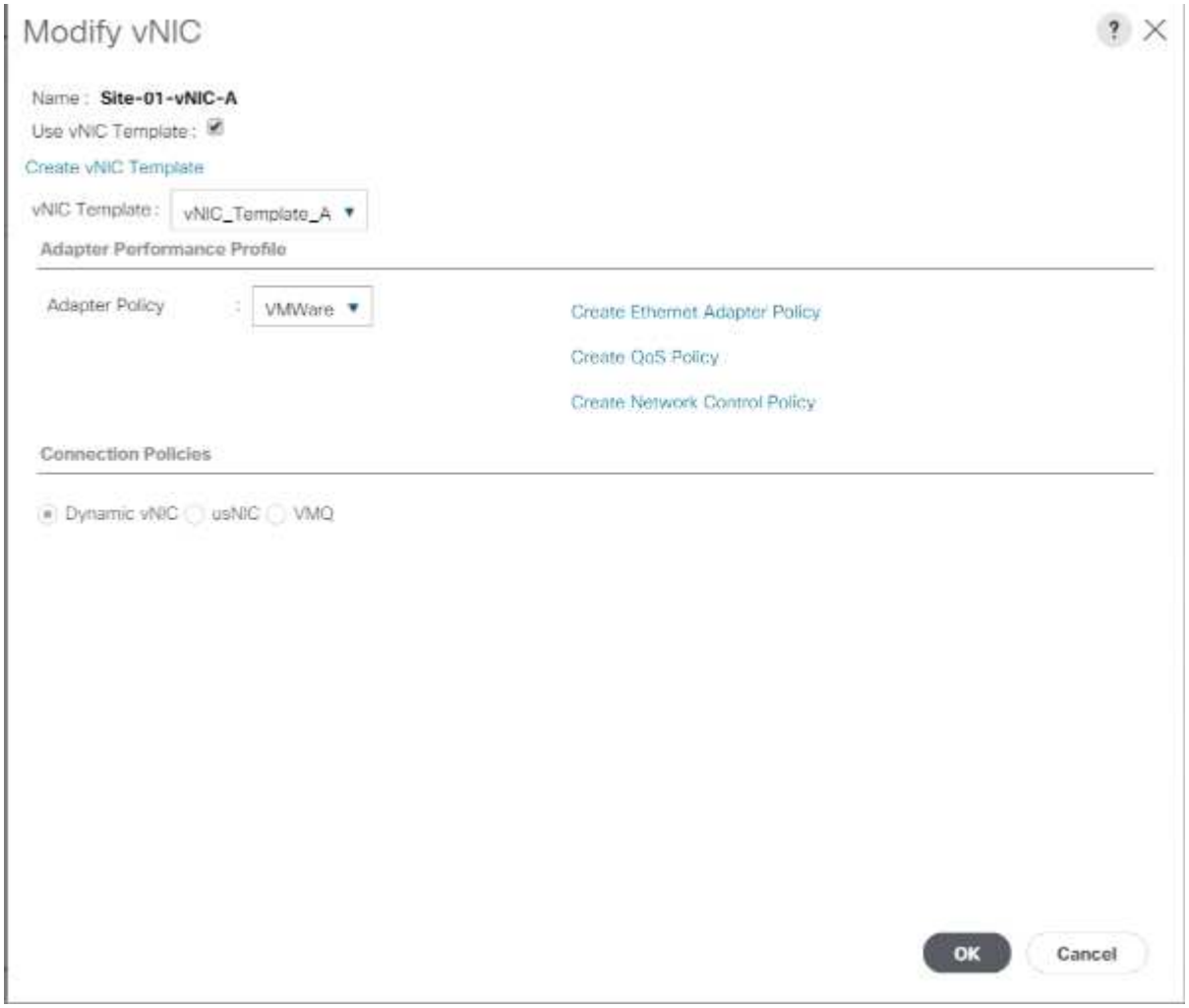
Cree una política de conectividad LAN para el arranque iSCSI

Este procedimiento se aplica a un entorno de Cisco UCS en el que hay dos LIF iSCSI en el nodo de clúster 1 (`iscsi_lif01a` y.. `iscsi_lif01b`) Y dos LIF iSCSI están en el nodo de cluster 2 (`iscsi_lif02a` y.. `iscsi_lif02b`). Asimismo, se supone que los LIF A están conectados al tejido A (Cisco UCS 6324 A) y que los LIF B están conectados al tejido B (Cisco UCS 6324 B).

Para configurar la directiva de conectividad LAN de la infraestructura necesaria, lleve a cabo los siguientes pasos:

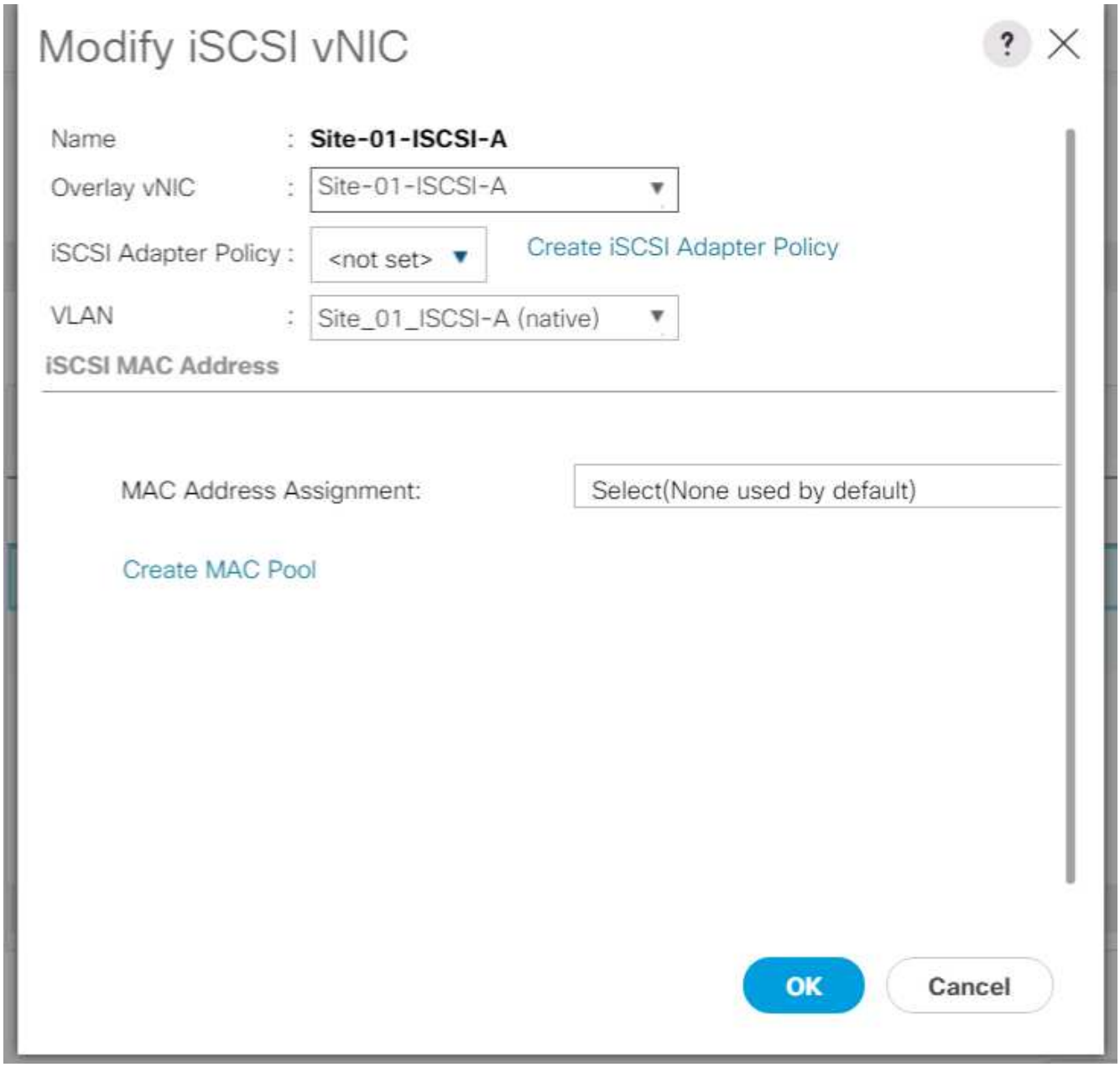
1. En Cisco UCS Manager, haga clic en LAN a la izquierda.
2. Seleccione LAN > Directivas > raíz.
3. Haga clic con el botón derecho del ratón en Directivas de conectividad LAN.
4. Seleccione Crear directiva de conectividad LAN.
5. Introduzca `Site-XX-Fabric-A` como nombre de la política.
6. Haga clic en la opción Agregar superior para agregar un VNIC.
7. En el cuadro de diálogo Crear VNIC, introduzca `Site-01-vNIC-A` Como nombre del VNIC.

8. Seleccione la opción usar plantilla VNIC.
9. En la lista plantilla VNIC, seleccione `vNIC_Template_A`.
10. En la lista desplegable Adapter Policy, seleccione VMware.
11. Haga clic en Aceptar para agregar este VNIC a la directiva.

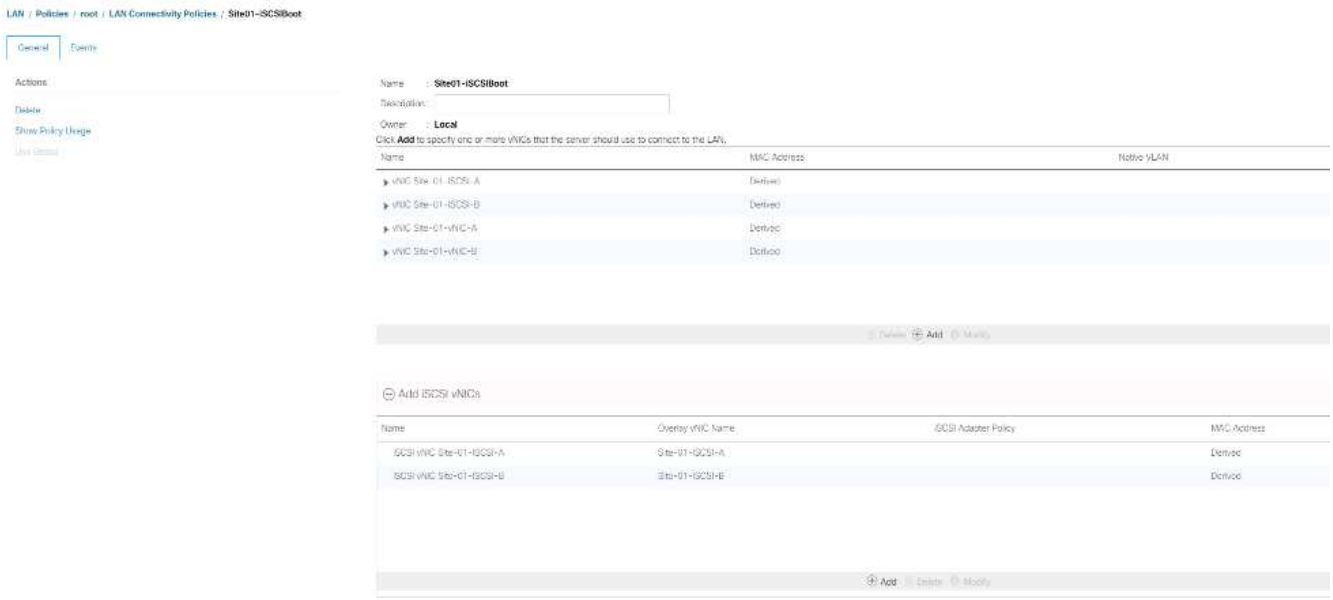


12. Haga clic en la opción Agregar superior para agregar un VNIC.
13. En el cuadro de diálogo Crear VNIC, introduzca `Site-01-vNIC-B` Como nombre del VNIC.
14. Seleccione la opción usar plantilla VNIC.
15. En la lista plantilla VNIC, seleccione `vNIC_Template_B`.
16. En la lista desplegable Adapter Policy, seleccione VMware.
17. Haga clic en Aceptar para agregar este VNIC a la directiva.
18. Haga clic en la opción Agregar superior para agregar un VNIC.
19. En el cuadro de diálogo Crear VNIC, introduzca `Site-01- iSCSI-A` Como nombre del VNIC.
20. Seleccione la opción usar plantilla VNIC.
21. En la lista plantilla VNIC, seleccione `Site-01-iSCSI-A`.
22. En la lista desplegable Adapter Policy, seleccione VMware.

23. Haga clic en Aceptar para agregar este VNIC a la directiva.
24. Haga clic en la opción Agregar superior para agregar un VNIC.
25. En el cuadro de diálogo Crear VNIC, introduzca `Site-01-iSCSI-B` Como nombre del VNIC.
26. Seleccione la opción usar plantilla VNIC.
27. En la lista plantilla VNIC, seleccione `Site-01-iSCSI-B`.
28. En la lista desplegable Adapter Policy, seleccione VMware.
29. Haga clic en Aceptar para agregar este VNIC a la directiva.
30. Expanda la opción Agregar NIC iSCSI.
31. Haga clic en la opción Agregar inferior del espacio Agregar vNIC iSCSI para agregar el VNIC iSCSI.
32. En el cuadro de diálogo Create iSCSI VNIC, introduzca `Site-01-iSCSI-A` Como nombre del VNIC.
33. Seleccione Overlay VNIC AS `Site-01-iSCSI-A`.
34. Deje la opción iSCSI Adapter Policy (Política del adaptador iSCSI) en no configurado.
35. Seleccione la VLAN como `Site-01-iSCSI-Site-A` (nativo).
36. Seleccione Ninguno (utilizado de forma predeterminada) como asignación de dirección MAC.
37. Haga clic en Aceptar para agregar el VNIC iSCSI a la directiva.



38. Haga clic en la opción Agregar inferior del espacio Agregar vNIC iSCSI para agregar el VNIC iSCSI.
39. En el cuadro de diálogo Create iSCSI VNIC, introduzca `Site-01-iSCSI-B` Como nombre del VNIC.
40. Seleccione Overlay VNIC como Site-01-iSCSI-B.
41. Deje la opción iSCSI Adapter Policy (Política del adaptador iSCSI) en no configurado.
42. Seleccione la VLAN como `Site-01-iSCSI-Site-B` (nativo).
43. Seleccione Ninguno (utilizado de forma predeterminada) como asignación de direcciones MAC.
44. Haga clic en Aceptar para agregar el VNIC iSCSI a la directiva.
45. Haga clic en Save Changes.



Cree la política vMedia para el arranque de instalación de VMware ESXi 6.7U1

En los pasos de configuración de Data ONTAP de NetApp es necesario un servidor web HTTP, que se utiliza para alojar Data ONTAP de NetApp y software VMware. La política de vMedia creada aquí asigna VMware ESXi 6. 7U1 ISO al servidor Cisco UCS para arrancar la instalación ESXi. Para crear esta directiva, lleve a cabo los siguientes pasos:

1. En Cisco UCS Manager, seleccione Servers a la izquierda.
2. Seleccione Policies > root.
3. Seleccione vMedia Policies.
4. Haga clic en Agregar para crear una nueva directiva de vMedia.
5. Asigne un nombre a la política ESXi-6.7U1-HTTP.
6. Introduzca Mounts ISO para ESXi 6.7U1 en el campo Description.
7. Seleccione Sí si Reintentar en caso de fallo de montaje.
8. Haga clic en Añadir.
9. Asigne el nombre Mount ESXi-6.7U1-HTTP.
10. Seleccione el tipo de dispositivo CDD.
11. Seleccione el protocolo HTTP.
12. Introduzca la dirección IP del servidor web.

> Las IP del servidor DNS no se han introducido anteriormente en la IP del KVM, por lo tanto, es necesario introducir la IP del servidor web en lugar del nombre de host.

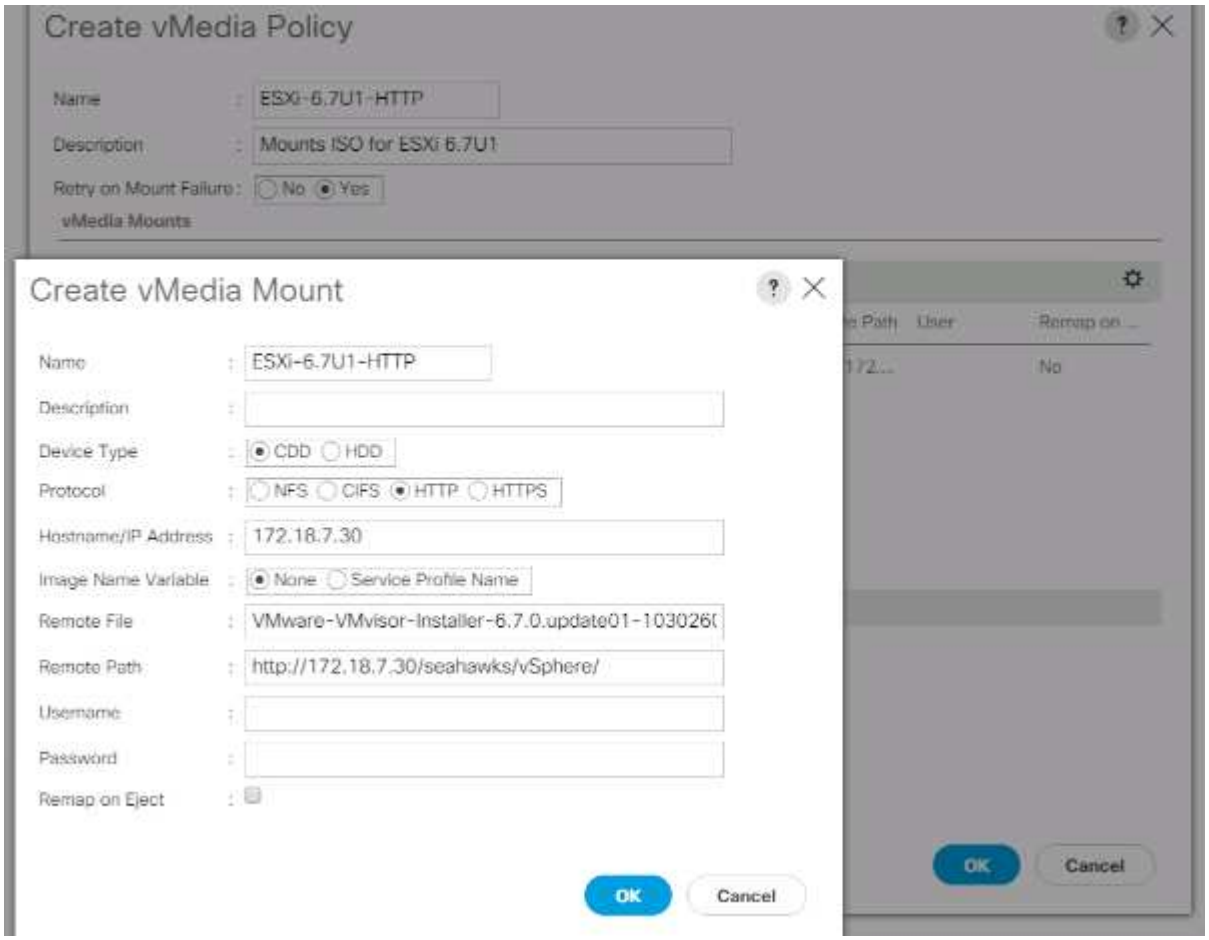
13. Introduzca `VMware-VMvisor-Installer-6.7.0.update01-10302608.x86_64.iso` Como nombre de archivo remoto.

    Este VMware ESXi 6.7U1 ISO se puede descargar desde "Descargas de VMware".

14. Introduzca la ruta del servidor web al archivo ISO en el campo Remote Path.

15. Haga clic en Aceptar para crear el montaje vMedia.
16. Haga clic en Aceptar y, a continuación, vuelva a Aceptar para completar la creación de la política de vMedia.

    Para cualquier servidor nuevo añadido al entorno Cisco UCS, se puede utilizar la plantilla de perfil de servicio vMedia para instalar el host ESXi. En el primer arranque, el host arranca en el instalador de ESXi desde que el disco montado en SAN está vacío. Una vez instalado ESXi, no se hace referencia a vMedia mientras se pueda acceder al disco de arranque.



Crear política de arranque iSCSI

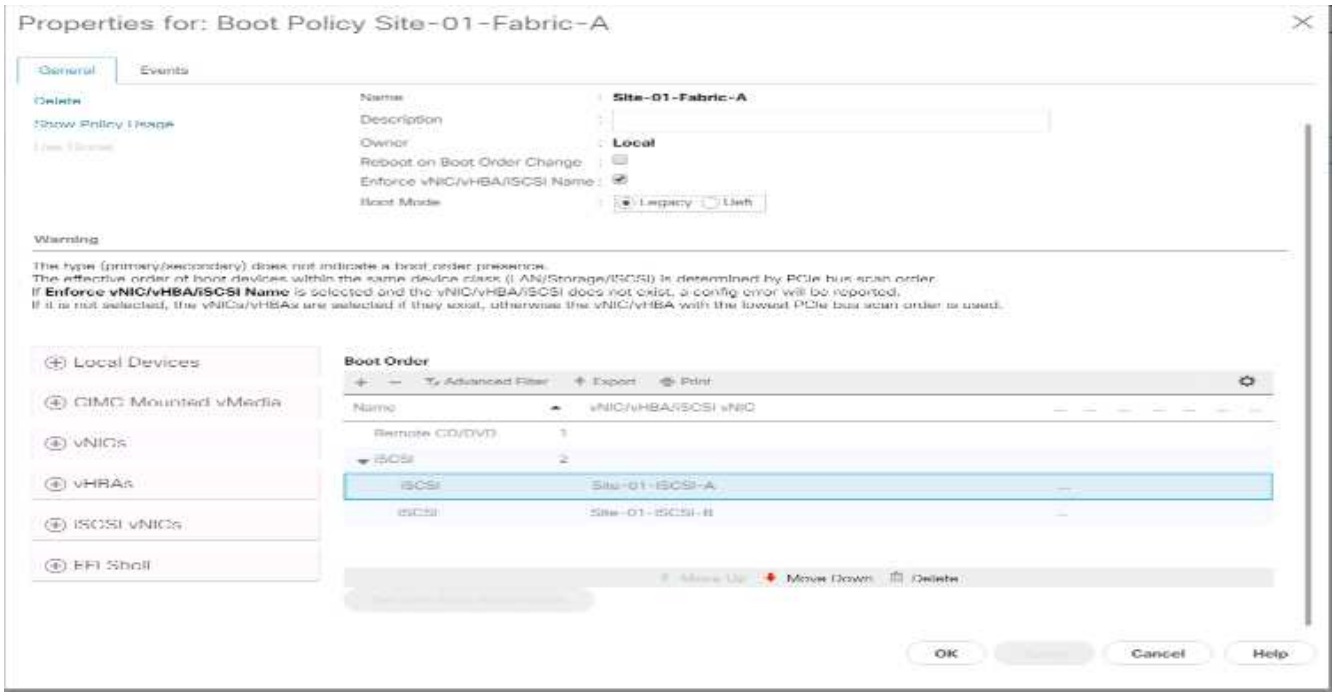
El procedimiento de esta sección se aplica a un entorno Cisco UCS en el que hay dos interfaces lógicas iSCSI (LIF) en el nodo de clúster 1 (`iscsi_lif01a` y.. `iscsi_lif01b`) Y dos LIF iSCSI están en el nodo de cluster 2 (`iscsi_lif02a` y.. `iscsi_lif02b`). Además, se supone que las LIF A están conectadas a la estructura A (Cisco UCS Fabric Interconnect A) y que los LIF B están conectados a la estructura B (Cisco UCS Fabric Interconnect B).

> Hay una política de arranque configurada en este procedimiento. La directiva configura el destino principal que se va a utilizar `iscsi_lif01a`.

Para crear una política de arranque para el entorno Cisco UCS, complete los pasos siguientes:

1. En Cisco UCS Manager, haga clic en Servers (servidores) a la izquierda.
2. Seleccione Policies > root.

3. Haga clic con el botón derecho del ratón en Directivas de arranque.
4. Seleccione Crear directiva de arranque.
5. Introduzca `Site-01-Fabric-A` como nombre de la directiva de arranque.
6. Opcional: Introduzca una descripción para la directiva de arranque.
7. Mantenga desactivada la opción Reiniciar en orden de arranque.
8. El modo de arranque es heredado.
9. Expanda el menú desplegable dispositivos locales y seleccione Agregar CD/DVD remoto.
10. Expanda el menú desplegable NIC iSCSI y seleccione Agregar inicio iSCSI.
11. En el cuadro de diálogo Add iSCSI Boot, introduzca `Site-01-iSCSI-A`. Haga clic en Aceptar.
12. Seleccione Add iSCSI Boot.
13. En el cuadro de diálogo Add iSCSI Boot, introduzca `Site-01-iSCSI-B`. Haga clic en Aceptar.
14. Haga clic en OK para crear la directiva.



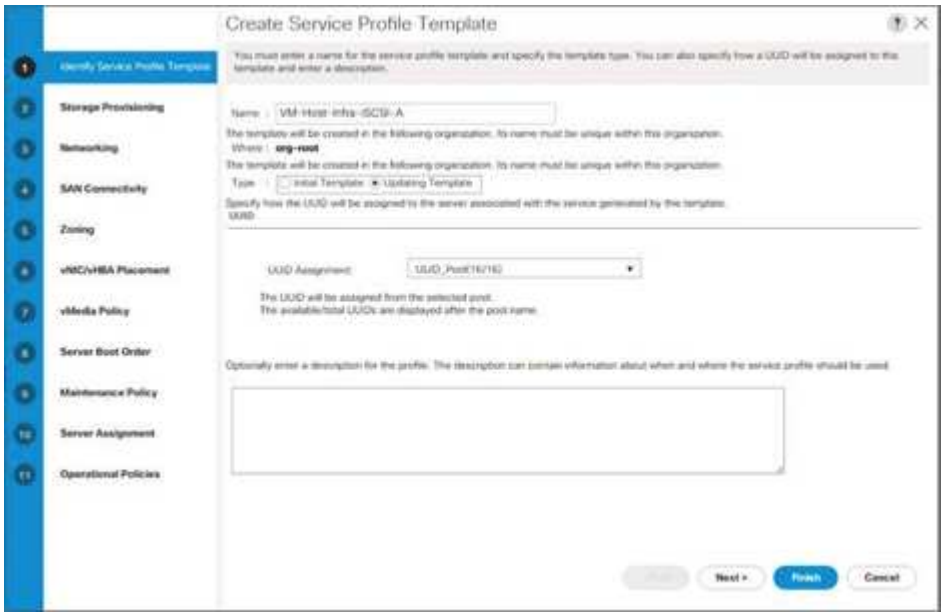
Crear plantilla de perfil de servicio

En este procedimiento, se crea una plantilla de perfil de servicio para los hosts ESXi de infraestructura para el arranque de Fabric A.

Para crear la plantilla de perfil de servicio, lleve a cabo los siguientes pasos:

1. En Cisco UCS Manager, haga clic en Servers (servidores) a la izquierda.
2. Seleccione Plantillas de perfil de servicio > raíz.
3. Haga clic con el botón derecho del ratón en root.
4. Seleccione Crear plantilla de perfil de servicio para abrir el asistente Crear plantilla de perfil de servicio.
5. Introduzca `VM-Host-Infra-iSCSI-A` como nombre de la plantilla de perfil de servicio. Esta plantilla de perfil de servicio está configurada para arrancar desde el nodo de almacenamiento 1 en la estructura A.

6. Seleccione la opción Actualizar plantilla.
7. En UUID, seleccione `UUID_Pool` Como pool de UUID. Haga clic en Siguiente.



Configure el aprovisionamiento del almacenamiento

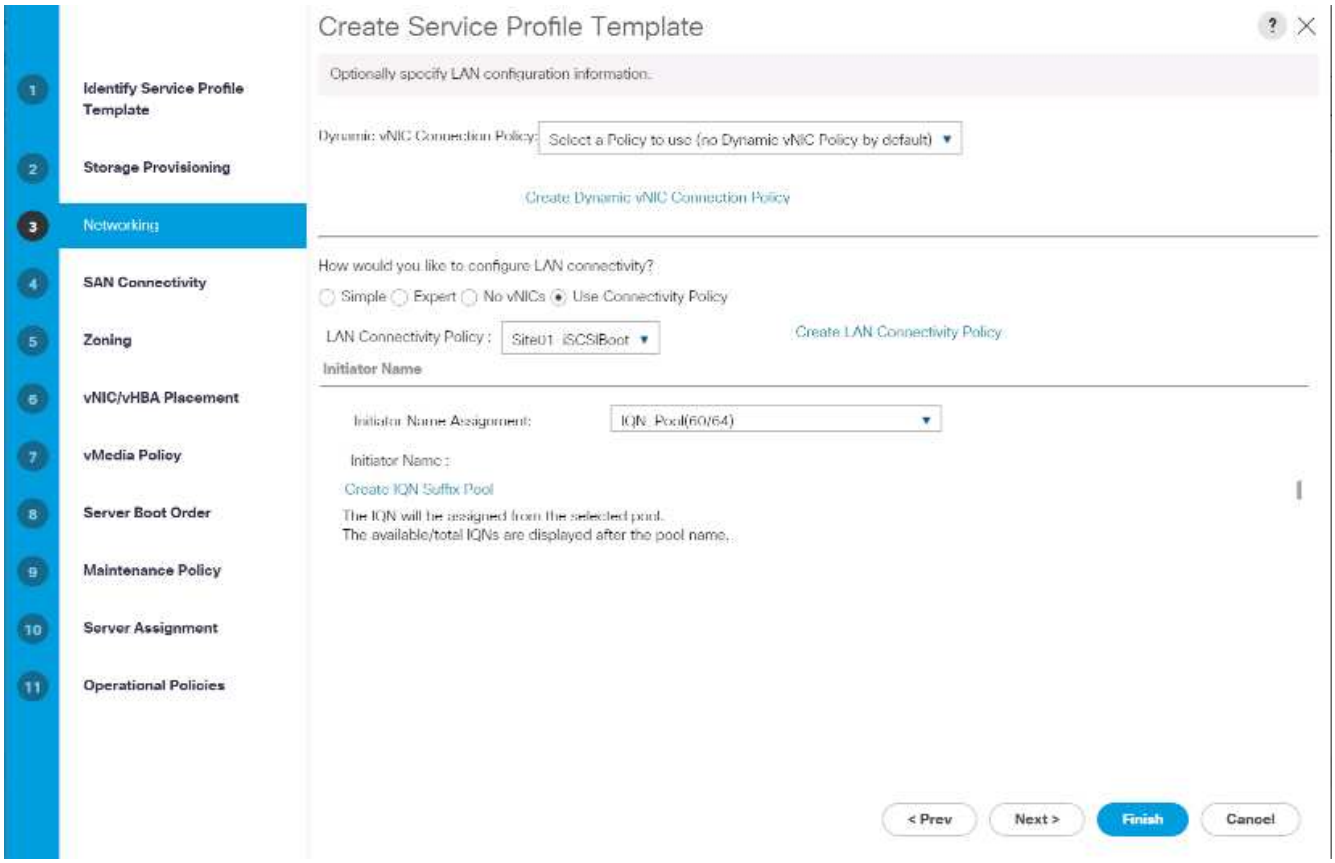
Para configurar el aprovisionamiento de almacenamiento, complete los siguientes pasos:

1. Si tiene servidores sin discos físicos, haga clic en Directiva de configuración de disco local y seleccione la Directiva de almacenamiento local de arranque DE SAN. De lo contrario, seleccione la Política de almacenamiento local predeterminada.
2. Haga clic en Siguiente.

Configuración de las opciones de red

Para configurar las opciones de red, lleve a cabo los siguientes pasos:

1. Mantenga la configuración predeterminada de la directiva de conexión dinámica de VNIC.
2. Seleccione la opción usar directiva de conectividad para configurar la conectividad LAN.
3. Seleccione iSCSI-Boot en el menú desplegable LAN Connectivity Policy.
4. Seleccione `IQN_Pool` En asignación de nombre de iniciador. Haga clic en Siguiente.



Configurar la conectividad SAN

Para configurar la conectividad SAN, siga estos pasos:

1. En el caso de vHBA, seleccione no para el ¿Cómo desea configurar la conectividad DE SAN? opción.
2. Haga clic en Siguiente.

Configurar la división en zonas

Para configurar la división en zonas, haga clic en Next.

Configurar la colocación de VNIC/HBA

Para configurar la colocación de VNIC/HBA, lleve a cabo los siguientes pasos:

1. En la lista desplegable Seleccionar ubicación, deje la política de colocación como permitir que el sistema realice la colocación.
2. Haga clic en Siguiente.

Configure la directiva vMedia

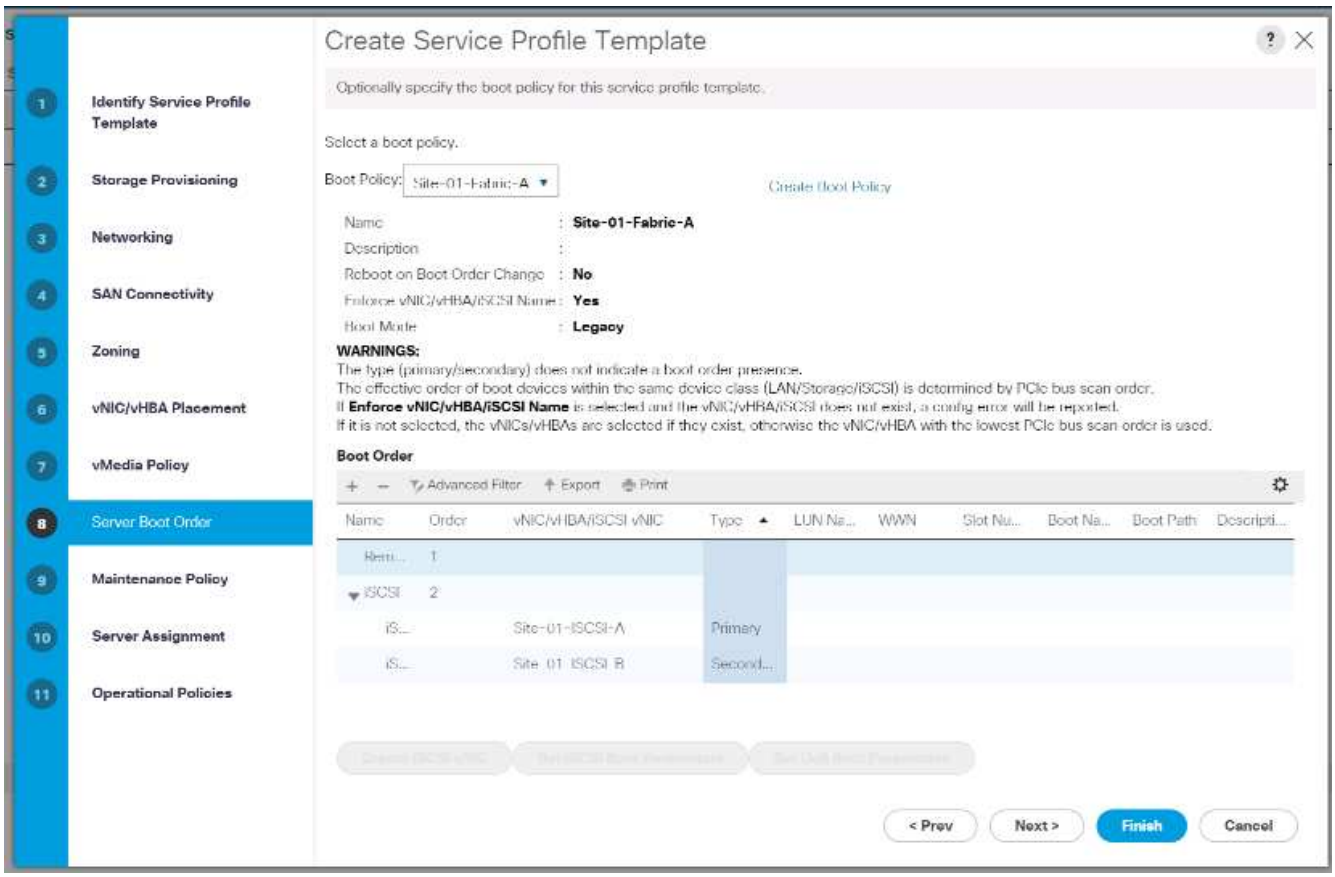
Para configurar la directiva vMedia, realice los siguientes pasos:

1. No seleccione una política de vMedia.
2. Haga clic en Siguiente.

Configurar el orden de arranque del servidor

Para configurar el orden de arranque del servidor, lleve a cabo los siguientes pasos:

1. Seleccione `Boot-Fabric-A` Para Directiva de inicio.



2. En el orden Boor, seleccione `Site-01- iSCSI-A`.
3. Haga clic en Set iSCSI Boot Parameters.
4. En el cuadro de diálogo definir parámetros de arranque iSCSI, deje la opción Perfil de autenticación en sin establecer a menos que haya creado de forma independiente uno adecuado para su entorno.
5. Deje el cuadro de diálogo asignación de nombre de iniciador no establecido para utilizar el nombre de iniciador de perfil de servicio único definido en los pasos anteriores.
6. Configurado `iSCSI_IP_Pool_A` Como directiva de dirección IP del iniciador.
7. Seleccione la opción iSCSI Static Target Interface (interfaz de destino estática iSCSI).
8. Haga clic en Añadir.
9. Introduzca el nombre del destino iSCSI. Para obtener el nombre de destino iSCSI de infra-SVM, inicie sesión en la interfaz de gestión de clústeres de almacenamiento y ejecute el `iscsi show` comando.

```
bb04-aff300::> iscsi show
            Target                          Target                          Status
Vserver     Name                            Alias                           Admin
----------- ------------------------------- ------------------------------- ------
Infra-SVM   iqn.1992-08.com.netapp:sn.b5acab9ef1c811e68d9d00a098a9fec2:vs.3
                                            Infra-SVM                       up
```

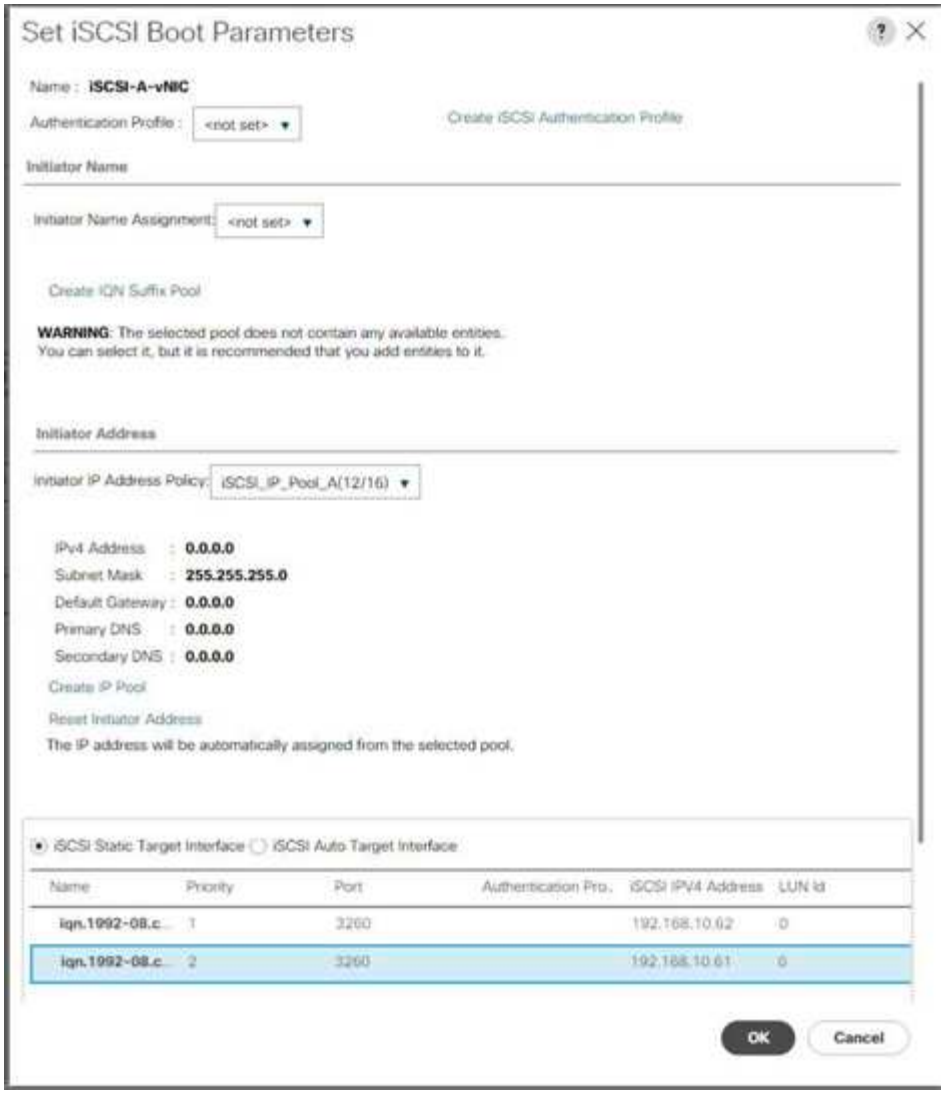
10. Introduzca la dirección IP de `iscsi_lif_02a` Para el campo Dirección IPv4.



11. Haga clic en OK para añadir el destino estático iSCSI.
12. Haga clic en Añadir.
13. Introduzca el nombre del destino iSCSI.
14. Introduzca la dirección IP de `iscsi_lif_01a` Para el campo Dirección IPv4.



15. Haga clic en OK para añadir el destino estático iSCSI.



Las IP de destino se colocaron con el nodo de almacenamiento 02 IP primero y el nodo de almacenamiento 01 IP segundo. Se asume que la LUN de arranque está en el nodo 01. El host arranca mediante la ruta al nodo 01 si se utiliza el orden de este procedimiento.

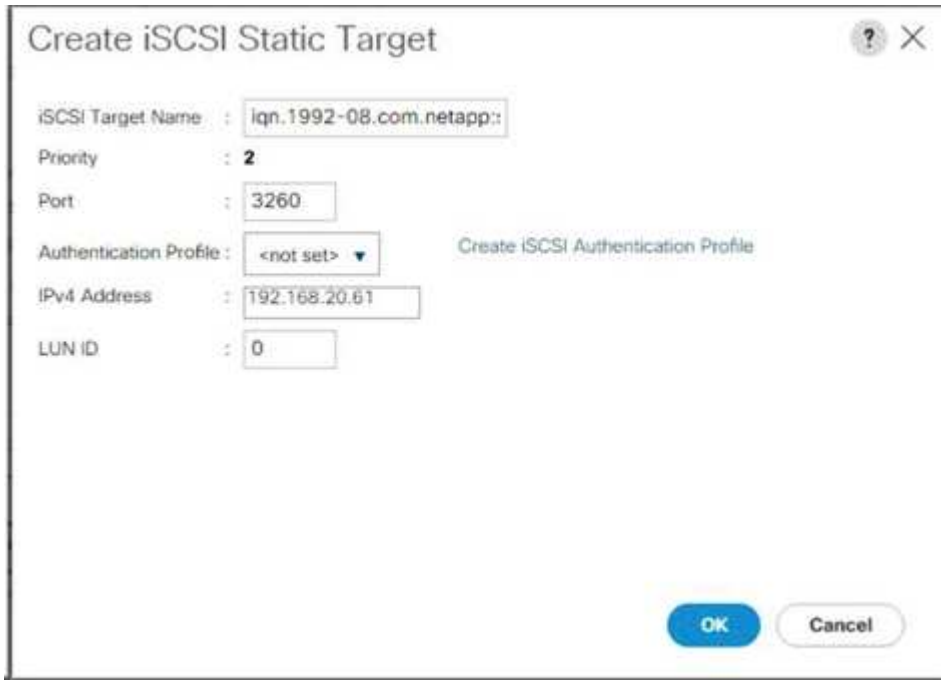
16. En el orden de arranque, seleccione iSCSI-B-VNIC.
17. Haga clic en Set iSCSI Boot Parameters.
18. En el cuadro de diálogo definir parámetros de arranque iSCSI, deje la opción Perfil de autenticación como no establecido a menos que haya creado de forma independiente uno adecuado para su entorno.
19. Deje el cuadro de diálogo asignación de nombre de iniciador no establecido para utilizar el nombre de iniciador de perfil de servicio único definido en los pasos anteriores.
20. Configurado `iSCSI_IP_Pool_B` Como política de dirección IP del iniciador.
21. Seleccione la opción iSCSI Static Target Interface (interfaz de destino estático iSCSI).
22. Haga clic en Añadir.
23. Introduzca el nombre del destino iSCSI. Para obtener el nombre de destino iSCSI de infra-SVM, inicie sesión en la interfaz de gestión de clústeres de almacenamiento y ejecute el `iscsi show` comando.

```
bb04-aff300::> iscsi show
          Target                          Target                         Status
Vserver   Name                            Alias                          Admin
--------- ------------------------------- ------------------------------ ------
Infra-SVM iqn.1992-08.com.netapp:sn.b5acab9ef1c811e68d9d00a098a9fec2:vs.3
                                          Infra-SVM                      up
```

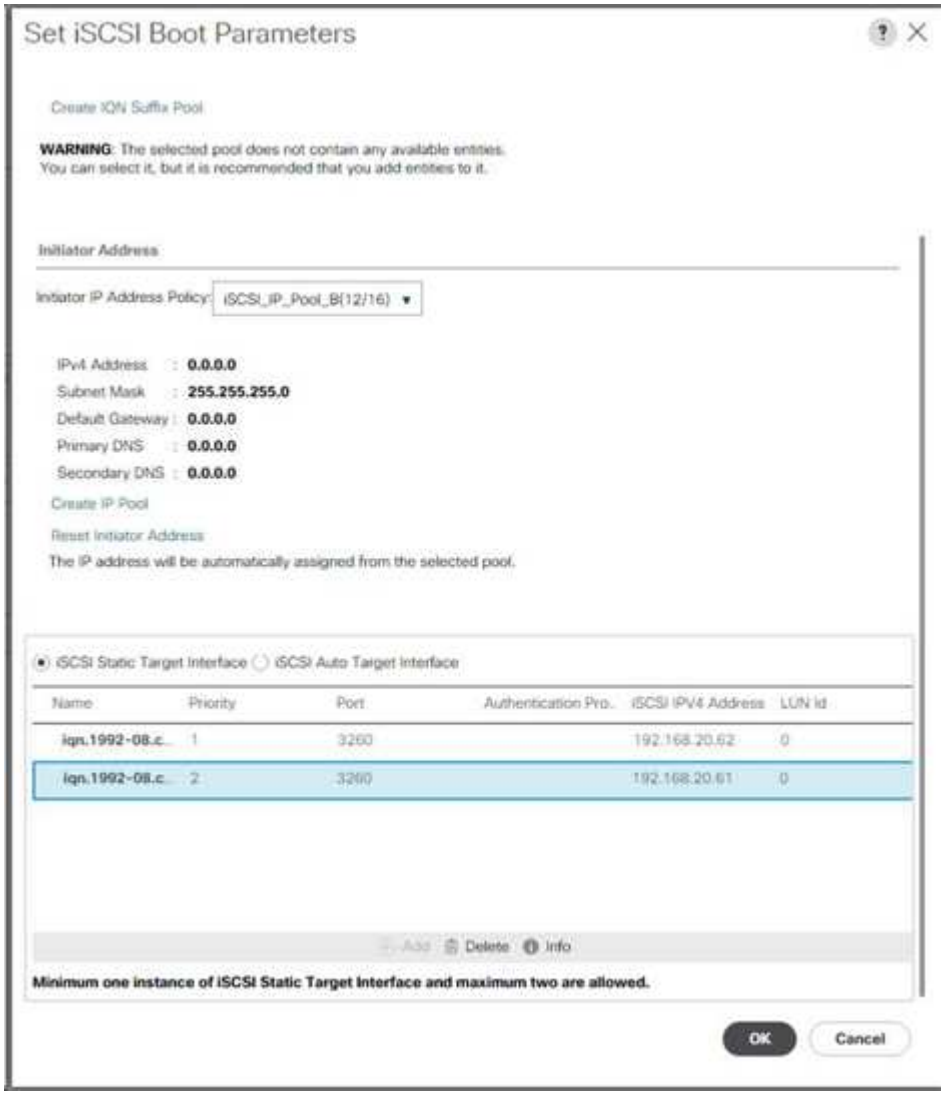
24. Introduzca la dirección IP de `iscsi_lif_02b` Para el campo Dirección IPv4.



25. Haga clic en OK para añadir el destino estático iSCSI.
26. Haga clic en Añadir.
27. Introduzca el nombre del destino iSCSI.
28. Introduzca la dirección IP de `iscsi_lif_01b` Para el campo Dirección IPv4.



29. Haga clic en OK para añadir el destino estático iSCSI.

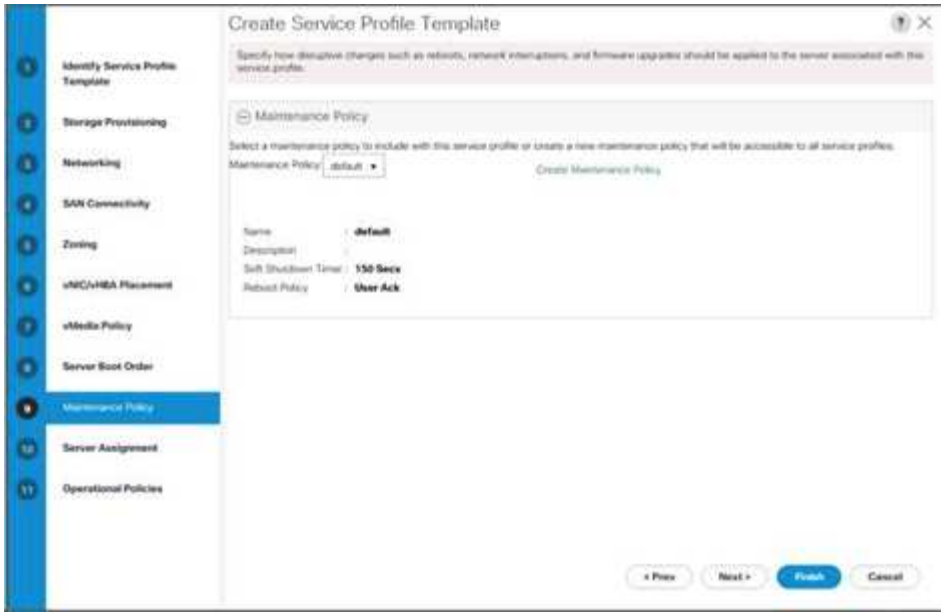


30. Haga clic en Siguiente.

Configure la directiva de mantenimiento

Para configurar la directiva de mantenimiento, lleve a cabo los siguientes pasos:

1. Cambie la directiva de mantenimiento a predeterminada.

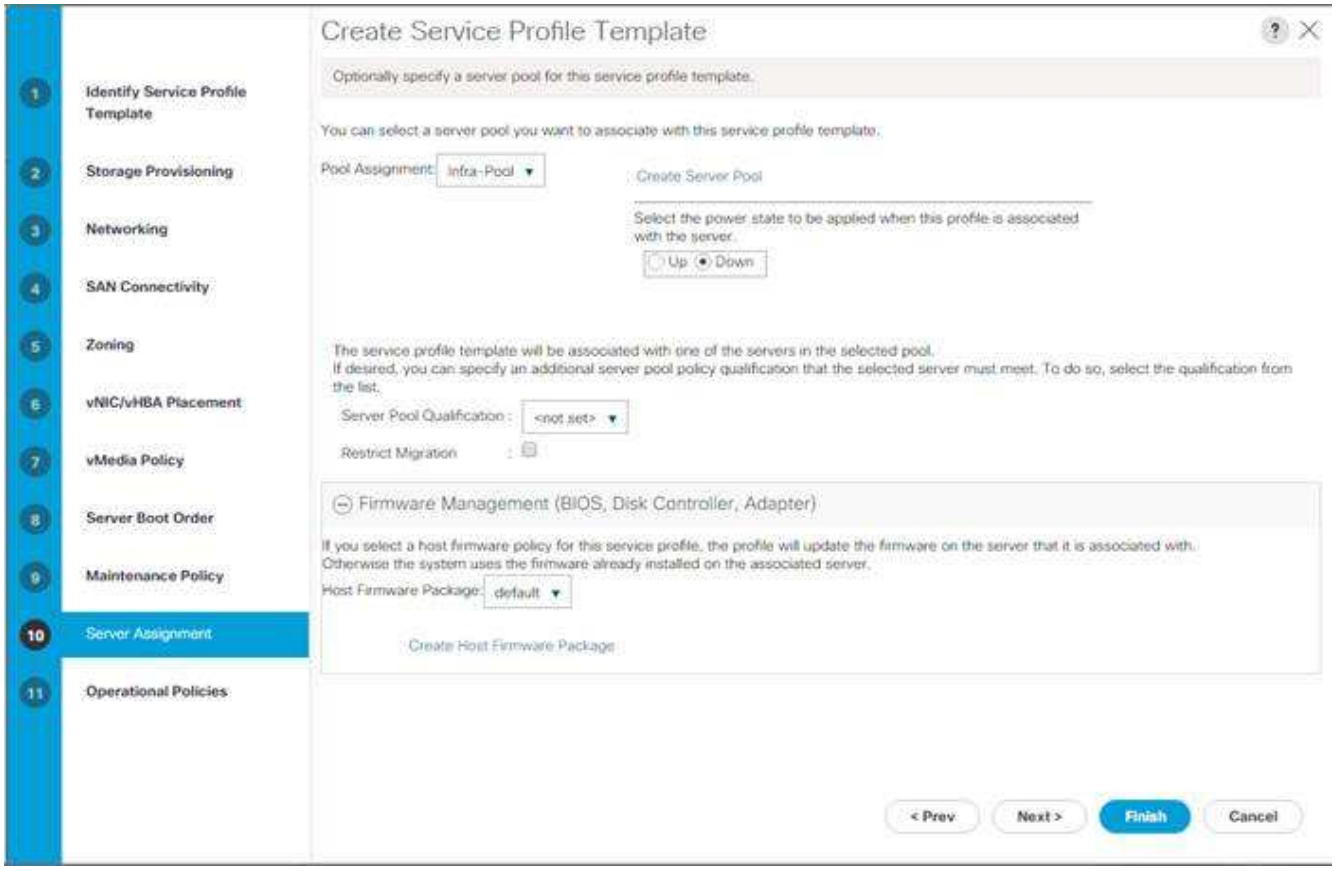


2. Haga clic en Siguiente.

Configurar la asignación de servidores

Para configurar la asignación del servidor, lleve a cabo los siguientes pasos:

1. En la lista asignación de grupos, seleccione Infra-Pool.
2. Seleccione Down como estado de alimentación que se va a aplicar cuando el perfil esté asociado al servidor.
3. Expanda Administración de firmware en la parte inferior de la página y seleccione la directiva predeterminada.

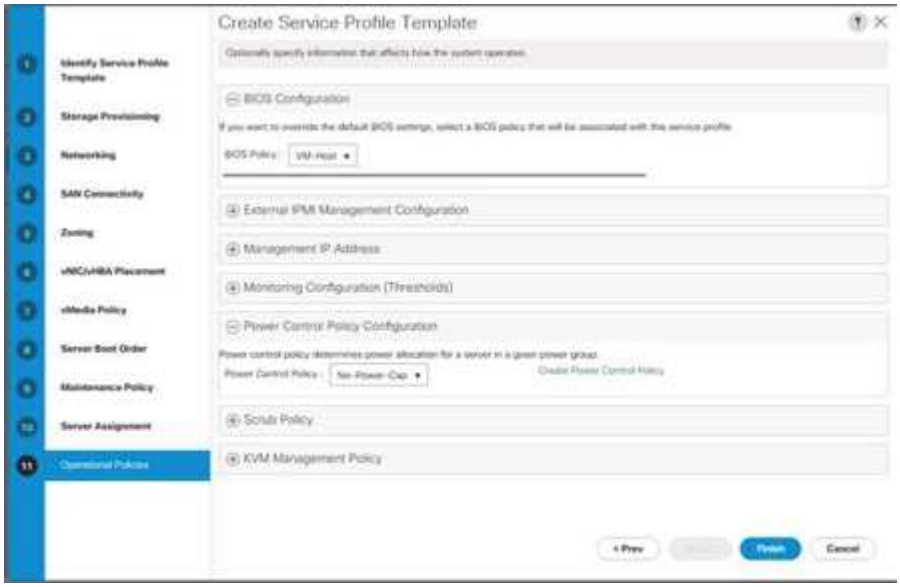


4. Haga clic en Siguiente.

Configure las políticas operativas

Para configurar las directivas operativas, realice los siguientes pasos:

1. En la lista desplegable BIOS Policy, seleccione VM-Host.
2. Expanda Configuración de la política de control de alimentación y seleccione sin límite de alimentación en la lista desplegable Política de control de alimentación.



3. Haga clic en Finalizar para crear la plantilla de perfil de servicio.
4. Haga clic en Aceptar en el mensaje de confirmación.

Crear una plantilla de perfil de servicio habilitada para vMedia

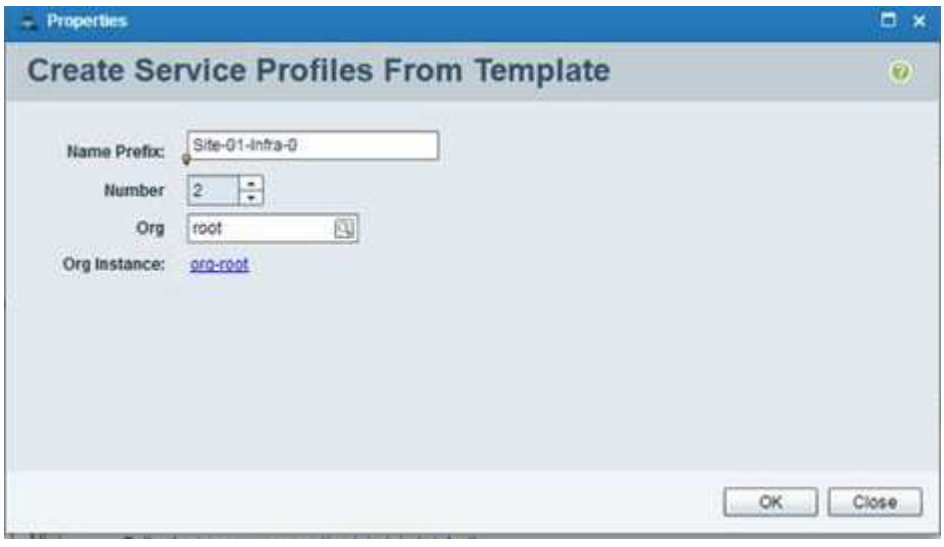
Para crear una plantilla de perfil de servicio con vMedia activado, lleve a cabo los siguientes pasos:

1. Conéctese a UCS Manager y haga clic en servidores a la izquierda.
2. Seleccione Plantillas de perfil de servicio > raíz > plantilla de servicio VM-Host-Infra-iSCSI-A.
3. Haga clic con el botón derecho en VM-Host-Infra-iSCSI-A y seleccione Create a Clone.
4. Asigne un nombre al clon `VM-Host-Infra-iSCSI-A-vM`.
5. Seleccione la VM-Host-infra-iSCSI-A-VM recién creada y seleccione la ficha vMedia Policy a la derecha.
6. Haga clic en Modificar la directiva de vMedia.
7. Seleccione ESXi-6. 7U1-HTTP vMedia Policy y haga clic en Aceptar.
8. Haga clic en OK para confirmar.

Crear perfiles de servicio

Para crear perfiles de servicio a partir de la plantilla de perfil de servicio, lleve a cabo los siguientes pasos:

1. Conéctese a Cisco UCS Manager y haga clic en servidores a la izquierda.
2. Expanda servidores > Plantillas de perfil de servicio > raíz > <name> de plantilla de servicio.
3. En acciones, haga clic en Crear perfil de servicio desde plantilla y compita los siguientes pasos:
   a. Introduzca `Site- 01-Infra-0` como prefijo de nombre.
   b. Introduzca `2` como el número de instancias que se van a crear.
   c. Seleccione root como org.
   d. Haga clic en Aceptar para crear los perfiles de servicio.



4. Haga clic en Aceptar en el mensaje de confirmación.
5. Compruebe que los perfiles de servicio `Site-01-Infra-01` y.. `Site-01-Infra-02` se han creado.

Los perfiles de servicio se asocian automáticamente con los servidores de sus pools de servidores asignados.

Parte de configuración del almacenamiento 2: Arranque de las LUN y los iGroups

Configuración del almacenamiento de arranque de ONTAP

Cree iGroups

Para crear grupos iniciadores (iGroups), complete los pasos siguientes:

1. Ejecute los siguientes comandos desde la conexión SSH del nodo de gestión del clúster:

```
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-01 –protocol
iscsi –ostype vmware –initiator <vm-host-infra-01-iqn>
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-02 –protocol
iscsi –ostype vmware –initiator <vm-host-infra-02-iqn>
igroup create –vserver Infra-SVM –igroup MGMT-Hosts –protocol iscsi
–ostype vmware –initiator <vm-host-infra-01-iqn>, <vm-host-infra-02-iqn>
```

Utilice los valores enumerados en la tabla 1 y la tabla 2 para obtener la información de IQN.

2. Para ver los tres iGroups recién creados, ejecute el `igroup show` comando.

Asigne LUN de arranque a iGroups

Para asignar LUN de arranque a iGroups, complete el paso siguiente:

1. Desde la conexión SSH de administración del clúster de almacenamiento, ejecute los siguientes comandos:

```
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra- A
–igroup VM-Host-Infra-01 –lun-id 0lun map –vserver Infra-SVM –volume
esxi_boot –lun VM-Host-Infra- B –igroup VM-Host-Infra-02 –lun-id 0
```

Procedimiento de implementación de VMware vSphere 6.7U1

En esta sección, se proporcionan los procedimientos detallados para la instalación de VMware ESXi 6.7U1 en una configuración FlexPod Express. Una vez finalizados los procedimientos, se aprovisionan dos hosts ESXi arrancados.

Existen varios métodos para instalar ESXi en un entorno VMware. Estos procedimientos se centran en cómo utilizar la consola KVM incorporada y las funciones de medios virtuales de Cisco UCS Manager para asignar medios de instalación remotos a servidores individuales y conectarse a sus LUN de arranque.

Descargue la imagen personalizada de Cisco para ESXi 6.7U1

Si no se ha descargado la imagen personalizada de VMware ESXi, complete los siguientes pasos para completar la descarga:

1. Haga clic en el siguiente enlace: VMware vSphere Hypervisor (ESXi) 6.7U1.
2. Necesita un ID de usuario y una contraseña en "vmware.com" para descargar este software.
3. Descargue el `.iso` archivo.

Administrador de Cisco UCS

Cisco UCS IP KVM permite al administrador iniciar la instalación del sistema operativo a través de medios remotos. Es necesario iniciar sesión en el entorno Cisco UCS para ejecutar el KVM de IP.

Para iniciar sesión en el entorno de Cisco UCS, complete los siguientes pasos:

1. Abra un explorador web e introduzca la dirección IP para la dirección del clúster de Cisco UCS. Este paso inicia la aplicación Cisco UCS Manager.
2. Haga clic en el enlace Iniciar UCS Manager en HTML para iniciar la GUI de HTML 5 UCS Manager.
3. Si se le solicita que acepte los certificados de seguridad, acepte según sea necesario.
4. Cuando se le solicite, introduzca `admin` como nombre de usuario e introduzca la contraseña administrativa.
5. Para iniciar sesión en Cisco UCS Manager, haga clic en Iniciar sesión.
6. En el menú principal, haga clic en servidores a la izquierda.
7. Seleccione servidores > Perfiles de servicios > raíz > `VM-Host-Infra-01`.
8. Haga clic con el botón derecho del ratón `VM-Host-Infra-01` Y seleccione KVM Console.
9. Siga las indicaciones para iniciar la consola KVM basada en Java.
10. Seleccione servidores > Perfiles de servicios > raíz > `VM-Host-Infra-02`.
11. Haga clic con el botón derecho del ratón `VM-Host-Infra-02`. Y seleccione KVM Console.
12. Siga las indicaciones para iniciar la consola KVM basada en Java.

Configure la instalación de VMware ESXi

ESXi aloja VM-Host-infra-01 y VM-Host- infra-02

Para preparar el servidor para la instalación del sistema operativo, complete los siguientes pasos en cada host ESXi:

1. En la ventana KVM, haga clic en Medios virtuales.
2. Haga clic en Activar dispositivos virtuales.
3. Si se le solicita que acepte una sesión KVM sin cifrar, acepte según sea necesario.
4. Haga clic en Medios virtuales y seleccione Mapa CD/DVD.
5. Desplácese hasta el archivo de imagen ISO del instalador ESXi y haga clic en Open.
6. Haga clic en asignar dispositivo.
7. Haga clic en la ficha KVM para supervisar el inicio del servidor.

Instalar ESXi

ESXi aloja VM-Host-Infra-01 y VM-Host-Infra-02

Para instalar VMware ESXi en el LUN de inicio iSCSI de los hosts, realice los pasos siguientes en cada host:

1. Inicie el servidor seleccionando Boot Server (servidor de inicio) y haciendo clic en OK (Aceptar). A continuación, vuelva a hacer clic en Aceptar.
2. En el reinicio, la máquina detecta la presencia de los medios de instalación de ESXi. Seleccione el instalador de ESXi en el menú de arranque que aparece.
3. Cuando el instalador haya terminado de cargarse, presione Entrar para continuar con la instalación.
4. Leer y aceptar el contrato de licencia para usuario final (CLUF). Pulse F11 para aceptar y continuar.
5. Seleccione el LUN que se configuró anteriormente como disco de instalación para ESXi y pulse Intro para continuar con la instalación.
6. Seleccione la distribución de teclado adecuada y pulse Intro.
7. Introduzca y confirme la contraseña de root y pulse Intro.
8. El instalador emite una advertencia de que el disco seleccionado se volverá a particionar. Pulse F11 para continuar con la instalación.
9. Una vez finalizada la instalación, seleccione la pestaña Virtual Media y borre la Marca P junto al medio de instalación de ESXi. Haga clic en Yes.

> ⓘ Debe anular la asignación de la imagen de instalación de ESXi para asegurarse de que el servidor se reinicie en ESXi y no en el instalador.

10. Una vez finalizada la instalación, pulse Intro para reiniciar el servidor.
11. En Cisco UCS Manager, enlace el perfil de servicio actual a la plantilla de perfil de servicio que no es vMedia para evitar el montaje de la instalación de ESXi iso a través de HTTP.

Configure las redes de gestión para los hosts ESXi

Es necesario añadir una red de gestión para cada host VMware para gestionar el host. Para añadir una red de gestión para los hosts VMware, complete los siguientes pasos en cada host ESXi:

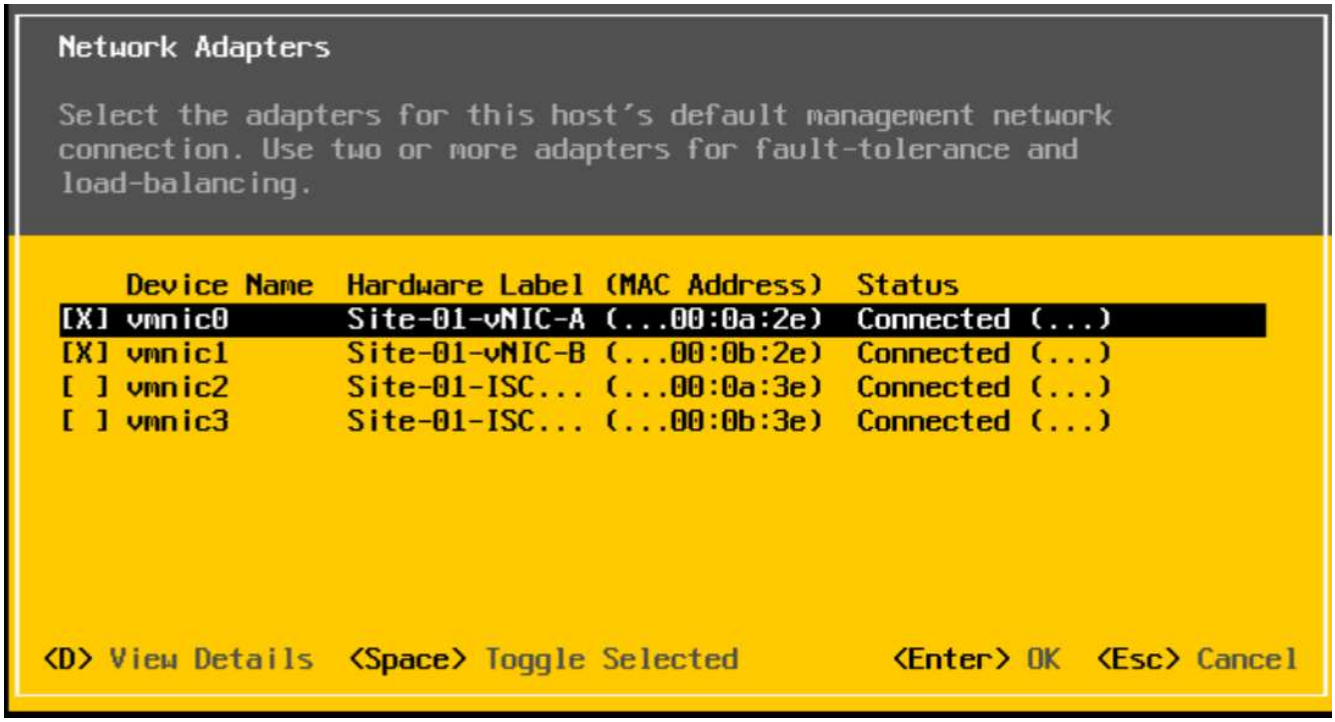
ESXi Host VM-Host-Infra-01 y VM-Host-Infra-02

Para configurar cada host ESXi con acceso a la red de gestión, complete los pasos siguientes:

1. Cuando el servidor haya terminado de reiniciarse, pulse F2 para personalizar el sistema.
2. Inicie sesión como `root`, Introduzca la contraseña correspondiente y pulse Intro para iniciar sesión.
3. Seleccione Opciones de solución de problemas y pulse Intro.
4. Seleccione Enable ESXi Shell y pulse Enter.
5. Seleccione Habilitar SSH y pulse Intro.
6. Pulse Esc para salir del menú Opciones de solución de problemas.
7. Seleccione la opción Configure Management Network y pulse Intro.
8. Seleccione Adaptadores de red y pulse Intro.
9. Compruebe que los números del campo etiqueta de hardware coinciden con los números del campo

Nombre del dispositivo.

10. Pulse Intro.



11. Seleccione la opción VLAN (opcional) y pulse Intro.
12. Introduzca el `<ib-mgmt-vlan-id>` Y pulse Intro.
13. Seleccione IPv4 Configuration y presione Enter.
14. Seleccione la opción establecer la dirección IPv4 estática y la configuración de red mediante la barra espaciadora.
15. Introduzca la dirección IP para gestionar el primer host ESXi.
16. Introduzca la máscara de subred para el primer host ESXi.
17. Introduzca la puerta de enlace predeterminada para el primer host ESXi.
18. Pulse Intro para aceptar los cambios en la configuración de IP.
19. Seleccione la opción DNS Configuration y presione Enter.

> Dado que la dirección IP se asigna manualmente, la información DNS también debe introducirse manualmente.

20. Introduzca la dirección IP del servidor DNS primario.
21. Optional: Introduzca la dirección IP del servidor DNS secundario.
22. Introduzca el FQDN para el primer host ESXi.
23. Pulse Intro para aceptar los cambios en la configuración de DNS.
24. Pulse Esc para salir del menú Configurar red de gestión.
25. Seleccione Test Management Network (Red de administración de pruebas) para comprobar que la red de gestión está configurada correctamente y pulse Intro.
26. Pulse Intro para ejecutar la prueba, pulse Intro de nuevo una vez que haya finalizado la prueba, revise el

entorno si hay un fallo.

27. Seleccione de nuevo Configurar red de administración y pulse Intro.
28. Seleccione la opción IPv6 Configuration y presione Enter.
29. Mediante la barra espaciadora, seleccione Disable IPv6 (Reiniciar requerido) y pulse Intro.
30. Pulse Esc para salir del submenú Configurar red de administración.
31. Pulse y para confirmar los cambios y reiniciar el host ESXi.

Restablecer la dirección MAC del puerto de VMkernel de host VMware ESXi vmk0 (opcional)

ESXi Host VM-Host-Infra-01 y VM-Host-Infra-02

De forma predeterminada, la dirección MAC del puerto de VMkernel de gestión vmk0 es la misma que la dirección MAC del puerto Ethernet en el que se coloca. Si el LUN de arranque del host ESXi se reasigna a un servidor diferente con direcciones MAC diferentes, se producirá un conflicto de dirección MAC porque vmk0 conserva la dirección MAC asignada a menos que se restablezca la configuración del sistema ESXi. Para restablecer la dirección MAC de vmk0 a una dirección MAC asignada por VMware aleatoria, complete los siguientes pasos:

1. En la pantalla principal del menú de la consola ESXi, pulse Ctrl-Alt-F1 para acceder a la interfaz de línea de comandos de VMware Console. En el KVM UCSM, Ctrl-Alt-F1 aparece en la lista de macros estáticas.
2. Inicie sesión como root.
3. Tipo `esxcfg-vmknic –l` para obtener una lista detallada de la interfaz vmk0. Vmk0 debe formar parte del grupo de puertos de la red de gestión. Anote la dirección IP y la máscara de red de vmk0.
4. Para eliminar vmk0, introduzca el siguiente comando:

```
esxcfg-vmknic –d “Management Network”
```

5. Para volver a añadir vmk0 con una dirección MAC aleatoria, introduzca el siguiente comando:

```
esxcfg-vmknic –a –i <vmk0-ip> -n <vmk0-netmask> “Management Network””.
```

6. Verifique que vmk0 se ha añadido de nuevo con una dirección MAC aleatoria

```
esxcfg-vmknic –l
```

7. Tipo `exit` para cerrar la sesión en la interfaz de línea de comandos.
8. Pulse Ctrl-Alt-F2 para volver a la interfaz de menús de la consola ESXi.

Inicie sesión en hosts VMware ESXi con el cliente host de VMware

Host ESXi VM-host-Infra-01

Para iniciar sesión en el host ESXi de VM-Host-Infra-01 con el cliente host de VMware, complete los siguientes pasos:

1. Abra un explorador Web en la estación de trabajo de gestión y desplácese hasta `VM-Host-Infra-01` Dirección IP de administración.
2. Haga clic en Open the VMware Host Client.
3. Introduzca `root` para el nombre de usuario.
4. Introduzca la contraseña de raíz.
5. Haga clic en Iniciar sesión para conectarse.
6. Repita este proceso para iniciar sesión en `VM-Host-Infra-02` en una pestaña o ventana del navegador por separado.

Instalación de controladores de VMware para la tarjeta de interfaz virtual (VIC) de Cisco

Descargue y extraiga el paquete sin conexión del controlador VIC de VMware a la estación de trabajo de gestión:

- Controlador Nenic versión 1.0.25.0

ESXi aloja VM-Host-Infra-01 y VM-Host-Infra-02

Para instalar los controladores VIC de VMware en el host de ESXi VM-Host-Infra-01 y VM-Host-Infra-02, lleve a cabo los siguientes pasos:

1. En cada cliente host, seleccione almacenamiento.
2. Haga clic con el botón derecho del ratón en datastor1 y seleccione examinar.
3. En el explorador Datastore, haga clic en Upload.
4. Desplácese hasta la ubicación guardada de los controladores VIC descargados y seleccione VMW-ESX-6.7.0-nenic-1.0.25.0-offline_Bundle-11271332.zip.
5. En el explorador Datastore, haga clic en Upload.
6. Haga clic en Abrir para cargar el archivo en datos1.
7. Asegúrese de que el archivo se haya cargado en ambos hosts ESXi.
8. Coloque cada host en modo de mantenimiento si no lo está ya.
9. Conéctese a cada host ESXi a través de ssh desde una conexión de shell o un terminal de putty.
10. Inicie sesión como root con la contraseña root.
11. Ejecute los siguientes comandos en cada host:

```
esxcli software vib update -d /vmfs/volumes/datastore1/VMW-ESX-6.7.0-
nenic-1.0.25.0-offline_bundle-11271332.zip
reboot
```

12. Inicie sesión en el cliente host en cada host una vez que se haya completado el reinicio y salga del modo de mantenimiento.

Configure los puertos de VMkernel y el conmutador virtual

ESXi Host VM-Host-Infra-01 y VM-Host-Infra-02

Para configurar los puertos de VMkernel y los switches virtuales en los hosts ESXi, complete los pasos siguientes:

1. En Host Client, seleccione Networking en la izquierda.
2. En el panel central, seleccione la ficha conmutadores virtuales.
3. Seleccione vSwitch0.
4. Seleccione Editar configuración.
5. Cambie el MTU a 9000.
6. Amplíe NIC Teaming.
7. En la sección Orden de conmutación por error, seleccione vmnic1 y haga clic en Marcar activo.
8. Verifique que vmnic1 ahora tenga el estado Active.
9. Haga clic en Guardar.
10. Seleccione Networking a la izquierda.
11. En el panel central, seleccione la ficha conmutadores virtuales.
12. Seleccione iScsiBootvSwitch.
13. Seleccione Editar configuración.
14. Cambie el MTU a 9000
15. Haga clic en Guardar.
16. Seleccione la ficha NIC de VMkernel.
17. Seleccione vmk1 iScsiBootPG.
18. Seleccione Editar configuración.
19. Cambie el MTU a 9000.
20. Expanda Configuración de IPv4 y cambie la dirección IP a una dirección fuera de UCS iSCSI-IP-Pool-A.

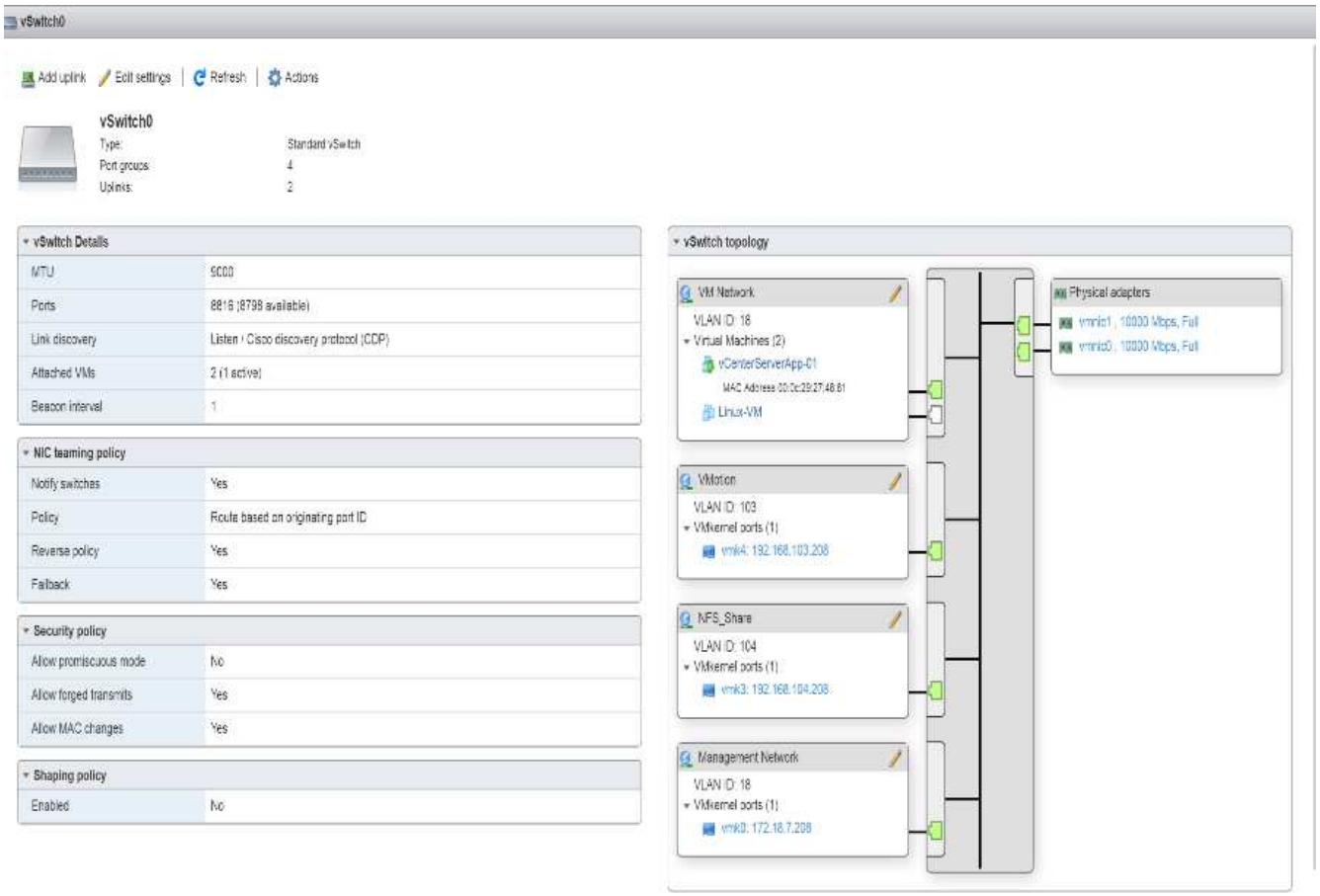
> Para evitar conflictos de direcciones IP si las direcciones IP Pool de Cisco UCS se deben volver a asignar, se recomienda utilizar direcciones IP diferentes en la misma subred para los puertos de VMkernel de iSCSI.

21. Haga clic en Guardar.
22. Seleccione la ficha switches virtuales.
23. Seleccione el conmutador virtual estándar Add.
24. Escriba un nombre de `iScsciBootvSwitch-B` Para el nombre de vSwitch.
25. Establezca la MTU en 9000.
26. Seleccione vmnic3 en el menú desplegable Uplink 1.
27. Haga clic en Añadir.
28. En el panel central, seleccione la ficha NIC de VMkernel.
29. Seleccione Agregar NIC de VMkernel
30. Especifique un nombre de grupo de puertos nuevo de iScsiBootPG-B.
31. Seleccione iScciBootvSwitch-B para el conmutador virtual.
32. Establezca la MTU en 9000. No introduzca un ID de VLAN.

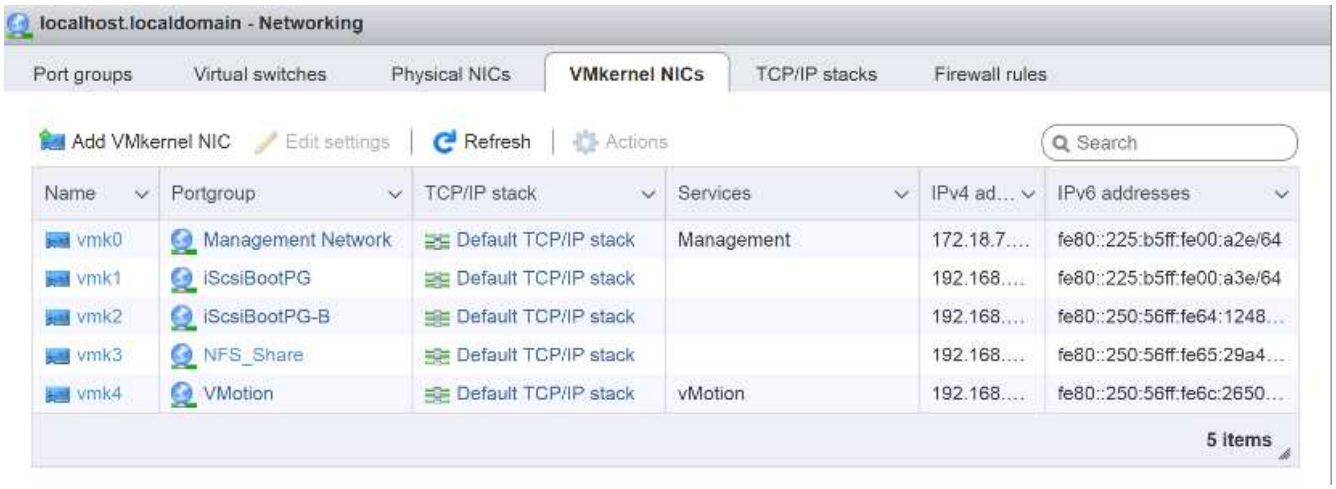
33. Seleccione Static (estático) para la configuración IPv4 y expanda la opción para proporcionar la dirección y la máscara de subred dentro de la configuración.

> Para evitar conflictos de direcciones IP, si las direcciones IP Pool de Cisco UCS se deben volver a asignar, se recomienda utilizar direcciones IP diferentes en la misma subred para los puertos VMkernel de iSCSI.

34. Haga clic en Crear.
35. A la izquierda, seleccione Networking (redes) y, a continuación, seleccione la ficha Port groups (grupos de puertos).
36. En el panel central, haga clic con el botón derecho del ratón en VM Network y seleccione Remove.
37. Haga clic en Quitar para completar la eliminación del grupo de puertos.
38. En el panel central, seleccione Agregar grupo de puertos.
39. Asigne el nombre al grupo de puertos Management Network e introduzca `<ib-mgmt-vlan-id>` En el campo VLAN ID, y asegúrese de que esté seleccionado Virtual Switch vSwitch0.
40. Haga clic en Agregar para finalizar las ediciones de la red IB-MGMT.
41. En la parte superior, seleccione la ficha NIC de VMkernel.
42. Haga clic en Add VMkernel NIC.
43. Para el grupo de puertos nuevo, introduzca VMotion.
44. En el conmutador virtual, seleccione vSwitch0 seleccionado.
45. Introduzca `<vmotion-vlan-id>` Para el ID de VLAN.
46. Cambie el MTU a 9000.
47. Seleccione Configuración IPv4 estática y expanda Configuración de IPv4.
48. Introduzca la dirección IP y la máscara de red del host ESXi.
49. Seleccione la pila vMotion TCP/IP.
50. Seleccione vMotion en Services.
51. Haga clic en Crear.
52. Haga clic en Add VMkernel NIC.
53. Para New Port group, introduzca NFS_Share.
54. En el conmutador virtual, seleccione vSwitch0 seleccionado.
55. Introduzca `<infra-nfs-vlan-id>` Para el ID de VLAN
56. Cambie el MTU a 9000.
57. Seleccione Configuración IPv4 estática y expanda Configuración de IPv4.
58. Introduzca la dirección IP y la máscara de red de NFS de la infraestructura del host ESXi.
59. No seleccione ninguno de los Servicios.
60. Haga clic en Crear.
61. Seleccione la pestaña Switches virtuales y seleccione vSwitch0. Las propiedades de los NIC de VMkernel vSwitch0 deberían ser similares al ejemplo siguiente:



62. Seleccione la ficha NIC de VMkernel para confirmar los adaptadores virtuales configurados. Los adaptadores enumerados deben ser similares al ejemplo siguiente:



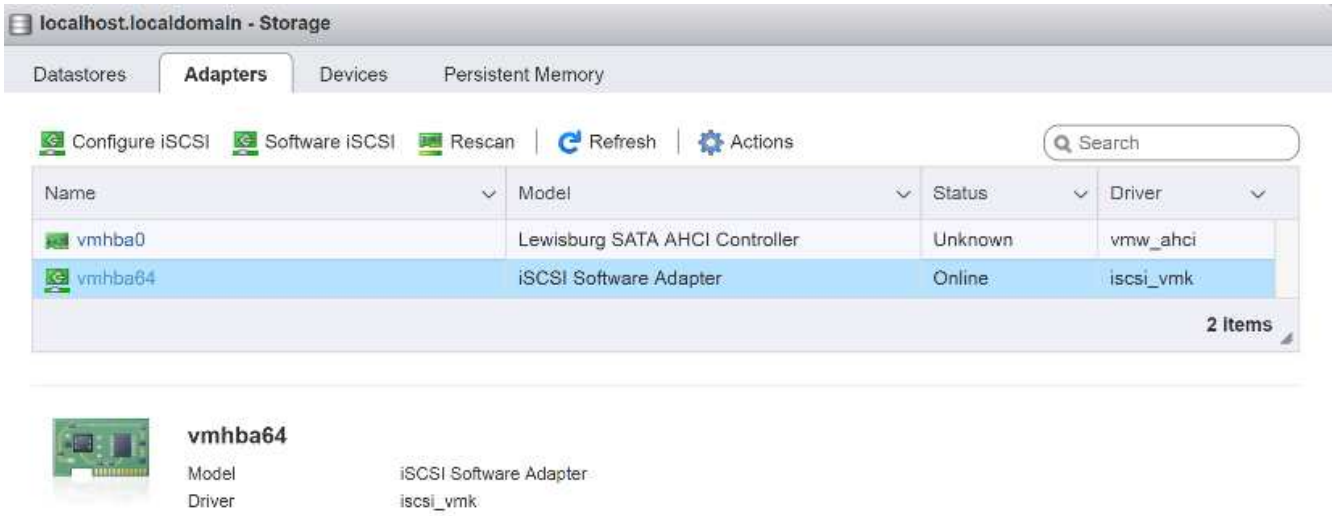
Configure la multivía iSCSI

ESXi aloja VM-Host-Infra-01 y VM-Host-Infra-02

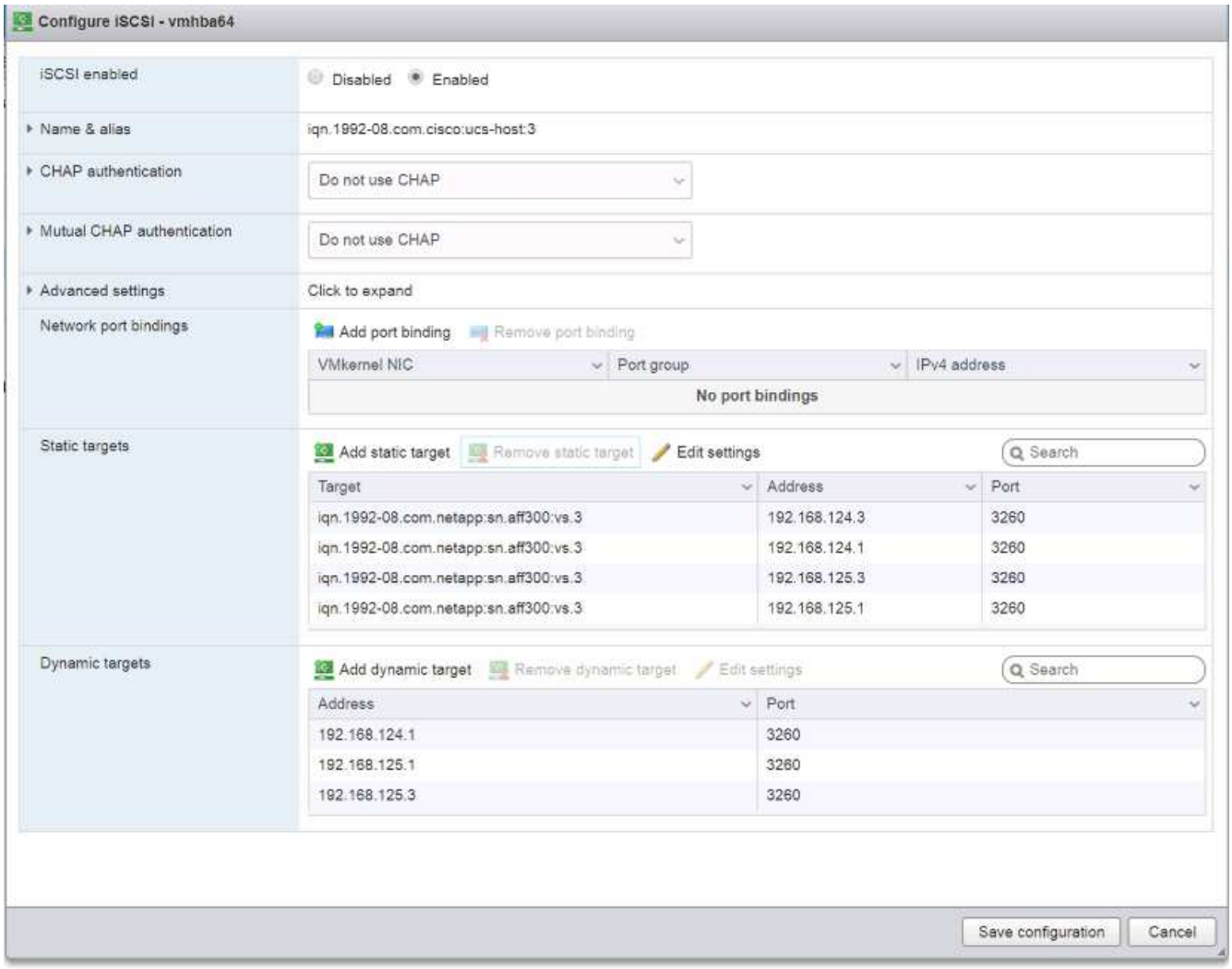
Para configurar la función multivía de iSCSI en el host ESXi VM-Host-Infra-01 y VM-Host-Infra-02, complete los siguientes pasos:

1. En cada cliente host, seleccione almacenamiento a la izquierda.

2. En el panel central, haga clic en Adaptadores.
3. Seleccione el adaptador de software iSCSI y haga clic en Configurar iSCSI.



4. En Destinos dinámicos, haga clic en Agregar destino dinámico.
5. Introduzca la dirección IP de `iSCSI_lif01a`.
6. Repita esto para introducir estas direcciones IP: `iscsi_lif01b`, `iscsi_lif02a`, y. `iscsi_lif02b`.
7. Haga clic en Save Configuration.



Para obtener todo el `iscsi_lif` Las direcciones IP, inicie sesión en la interfaz de gestión del clúster de almacenamiento de NetApp y ejecute el `network interface show` comando.

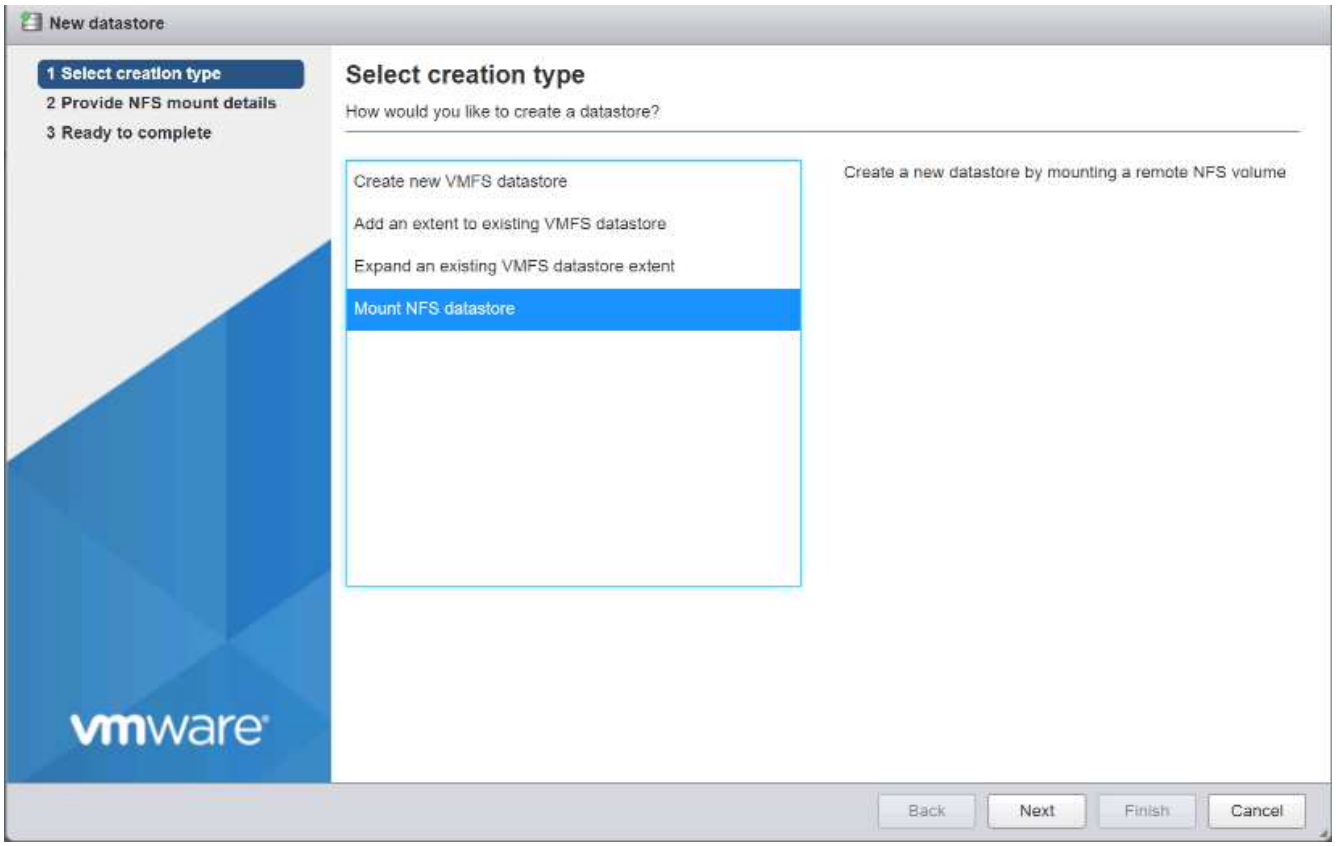
> El host vuelve a buscar automáticamente el adaptador de almacenamiento y los destinos se agregan a los destinos estáticos.

Montar los almacenes de datos necesarios

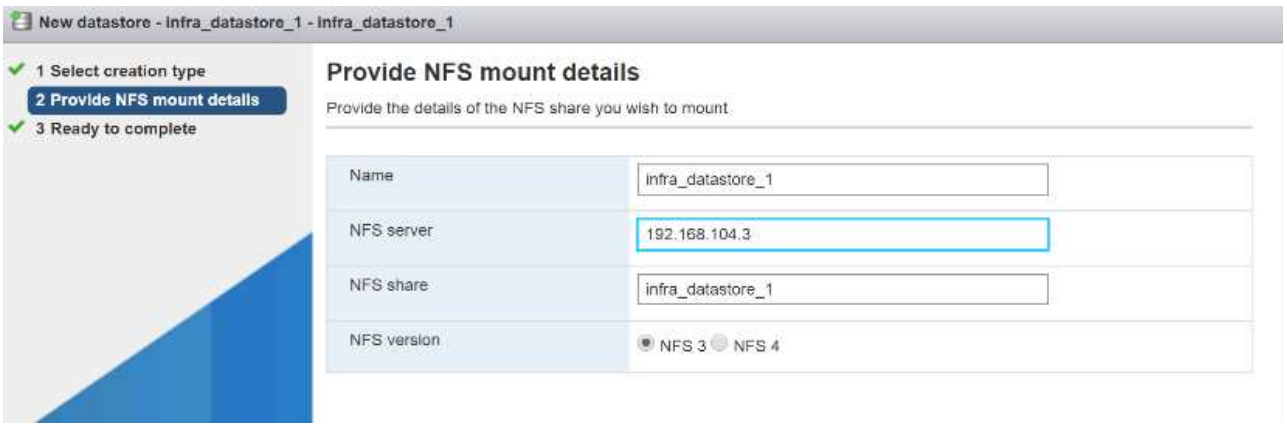
ESXi aloja VM-Host-Infra-01 y VM-Host-Infra-02

Para montar los almacenes de datos necesarios, complete los siguientes pasos en cada host ESXi:

1. En Host Client, seleccione Storage a la izquierda.
2. En el panel central, seleccione datastores.
3. En el panel central, seleccione New Datastore para añadir un almacén de datos nuevo.
4. En el cuadro de diálogo New datastore, seleccione Mount NFS datastore y haga clic en Next.



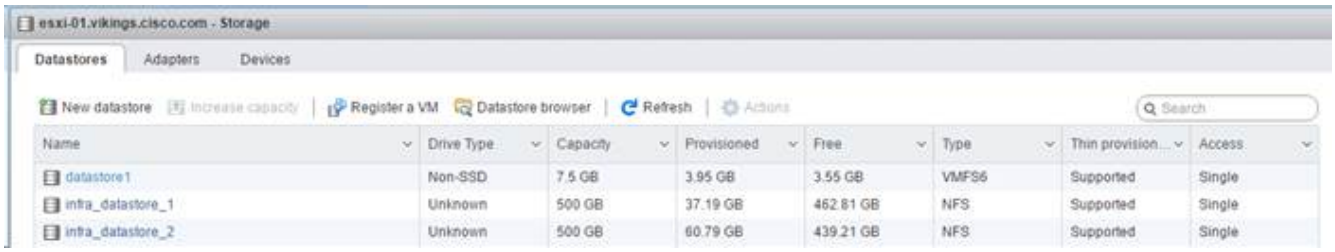
5. En la página Provide NFS Mount Details, complete los siguientes pasos:
   a. Introduzca `infra_datastore_1` para el nombre del almacén de datos.
   b. Introduzca la dirección IP para el `nfs_lif01_a` LIF para el servidor NFS.
   c. Introduzca `/infra_datastore_1` Para el recurso compartido NFS.
   d. Deje la versión de NFS configurada en NFS 3.
   e. Haga clic en Siguiente.



6. Haga clic en Finalizar. El almacén de datos ahora debe aparecer en la lista de almacenes de datos.
7. En el panel central, seleccione New Datastore para añadir un almacén de datos nuevo.
8. En el cuadro de diálogo New Datastore, seleccione Mount NFS Datastore y haga clic en Next.
9. En la página Provide NFS Mount Details, complete los siguientes pasos:

a. Introduzca `infra_datastore_2` para el nombre del almacén de datos.
b. Introduzca la dirección IP para el `nfs_lif02_a` LIF para el servidor NFS.
c. Introduzca `/infra_datastore_2` Para el recurso compartido NFS.
d. Deje la versión de NFS configurada en NFS 3.
e. Haga clic en Siguiente.

10. Haga clic en Finalizar. El almacén de datos ahora debe aparecer en la lista de almacenes de datos.



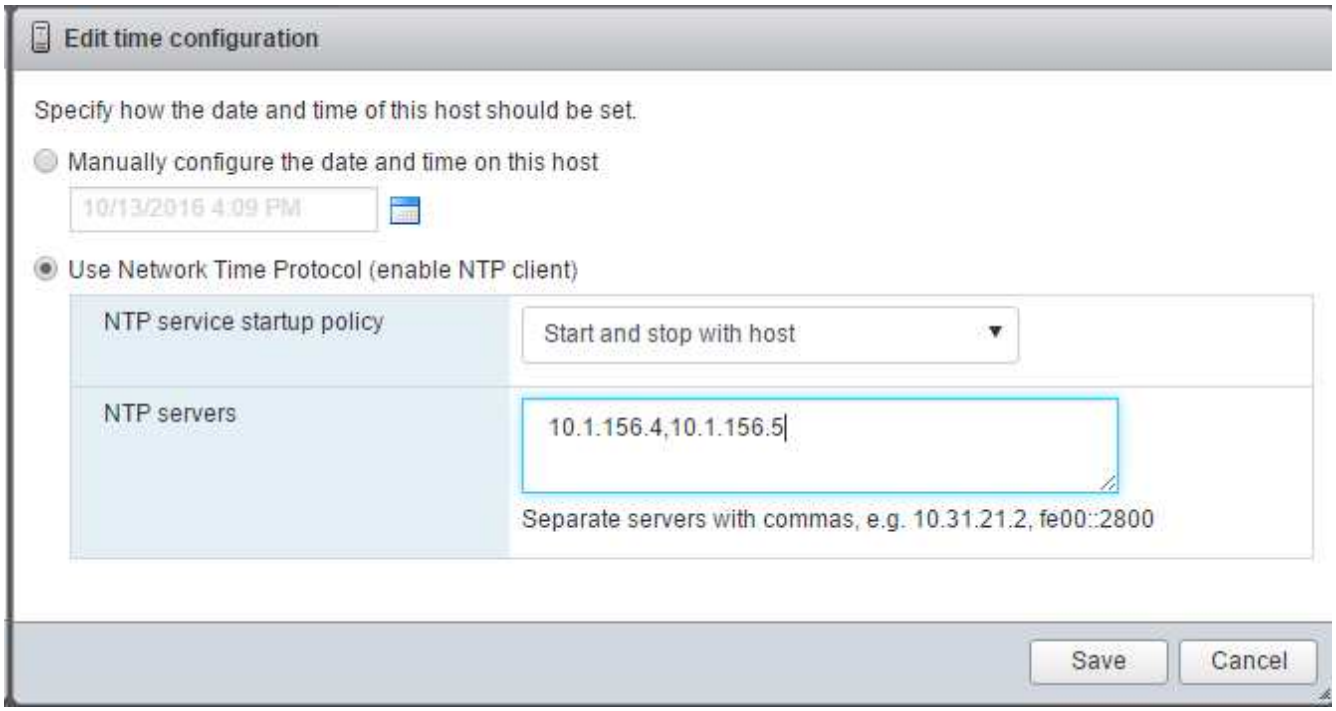
11. Montar ambos almacenes de datos en ambos hosts ESXi.

Configure NTP en hosts ESXi

ESXi aloja VM-Host-Infra-01 y VM-Host-Infra-02

Para configurar NTP en los hosts ESXi, complete los siguientes pasos en cada host:

1. En Host Client, seleccione Manage a la izquierda.
2. En el panel central, seleccione la ficha Hora y fecha.
3. Haga clic en Editar configuración.
4. Asegúrese de que esté seleccionada la opción Use Network Time Protocol (habilitar cliente NTP).
5. Use el menú desplegable para seleccionar Inicio y Detener con Host.
6. Introduzca las dos direcciones NTP del switch Nexus en el cuadro servidores NTP separados por una coma.



7. Haga clic en Guardar para guardar los cambios de configuración.
8. Seleccione Actions > NTP service > Start.
9. Compruebe que el servicio NTP está en ejecución y que el reloj está ahora ajustado aproximadamente a la hora correcta

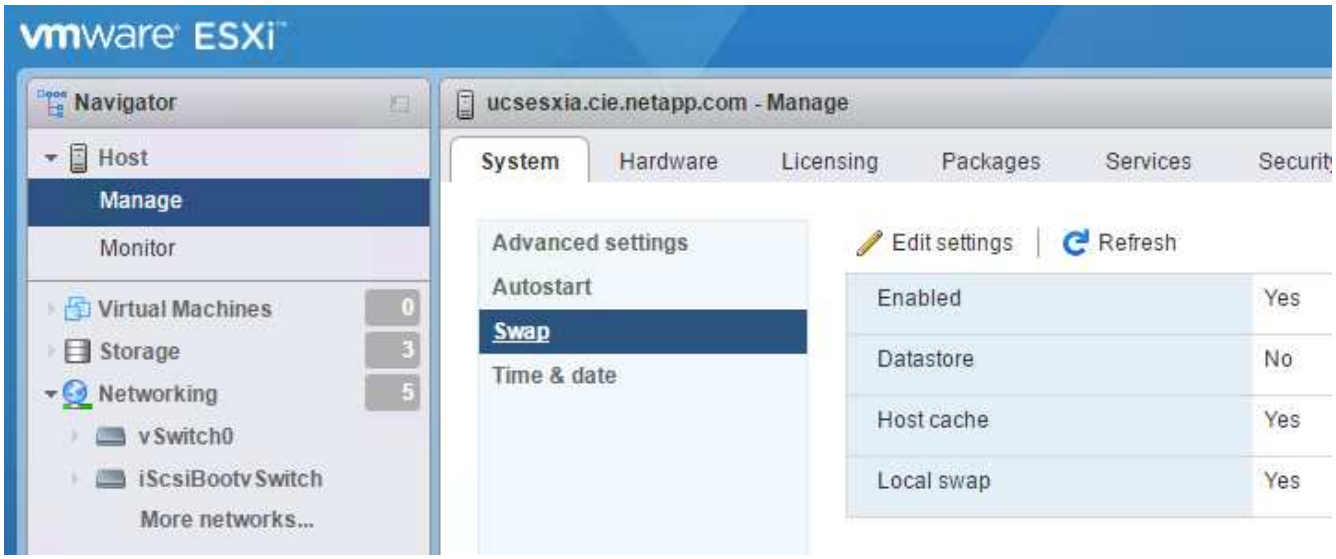
El tiempo del servidor NTP puede variar ligeramente respecto del tiempo del host.

Configurar el intercambio del host ESXi

ESXi aloja VM-Host-Infra-01 y VM-Host-Infra-02

Para configurar el intercambio del host en los hosts ESXi, siga estos pasos en cada host:

1. Haga clic en Administrar en el panel de navegación de la izquierda. Seleccione sistema en el panel derecho y haga clic en intercambiar.



2. Haga clic en Editar configuración. Seleccione `infra_swap` En las opciones del Datastore.



3. Haga clic en Guardar.

Instale el plugin de NetApp NFS 1.1.2 para VMware VAAI

Para instalar el complemento NFS de NetApp 1. 1.2 para VMware VAAI, realice los siguientes pasos.

1. Descargue el plugin de NetApp NFS para VMware VAAI:
   a. Vaya a la "Página de descarga del software NetApp".
   b. Desplácese hacia abajo y haga clic en NetApp NFS Plug-in for VMware VAAI.
   c. Seleccione la plataforma ESXi.
   d. Descargue el paquete sin conexión (.zip) o el paquete en línea (.vib) del plugin más reciente.
2. El complemento NFS de NetApp para VAAI de VMware está pendiente para la cualificación de IMT con ONTAP 9.5; los detalles de interoperabilidad se publicarán en el próximamente en el IMT de NetApp.
3. Instale el plugin en el host ESXi mediante la CLI ESX.
4. Reinicie el host ESXI.

Instale VMware vCenter Server 6.7

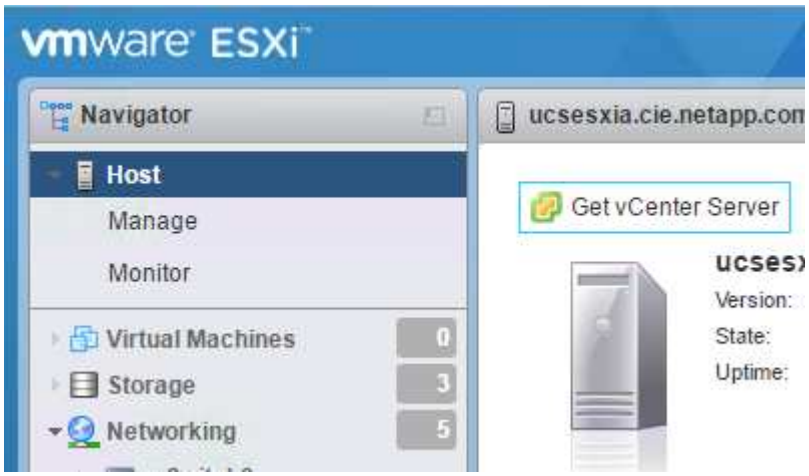
En esta sección, se proporcionan los procedimientos detallados para instalar VMware vCenter Server 6.7 en una configuración exprés de FlexPod.

FlexPod Express utiliza el dispositivo de VMware vCenter Server (VCSA).

Instale el dispositivo VMware vCenter Server

Para instalar VCSA, lleve a cabo los siguientes pasos:

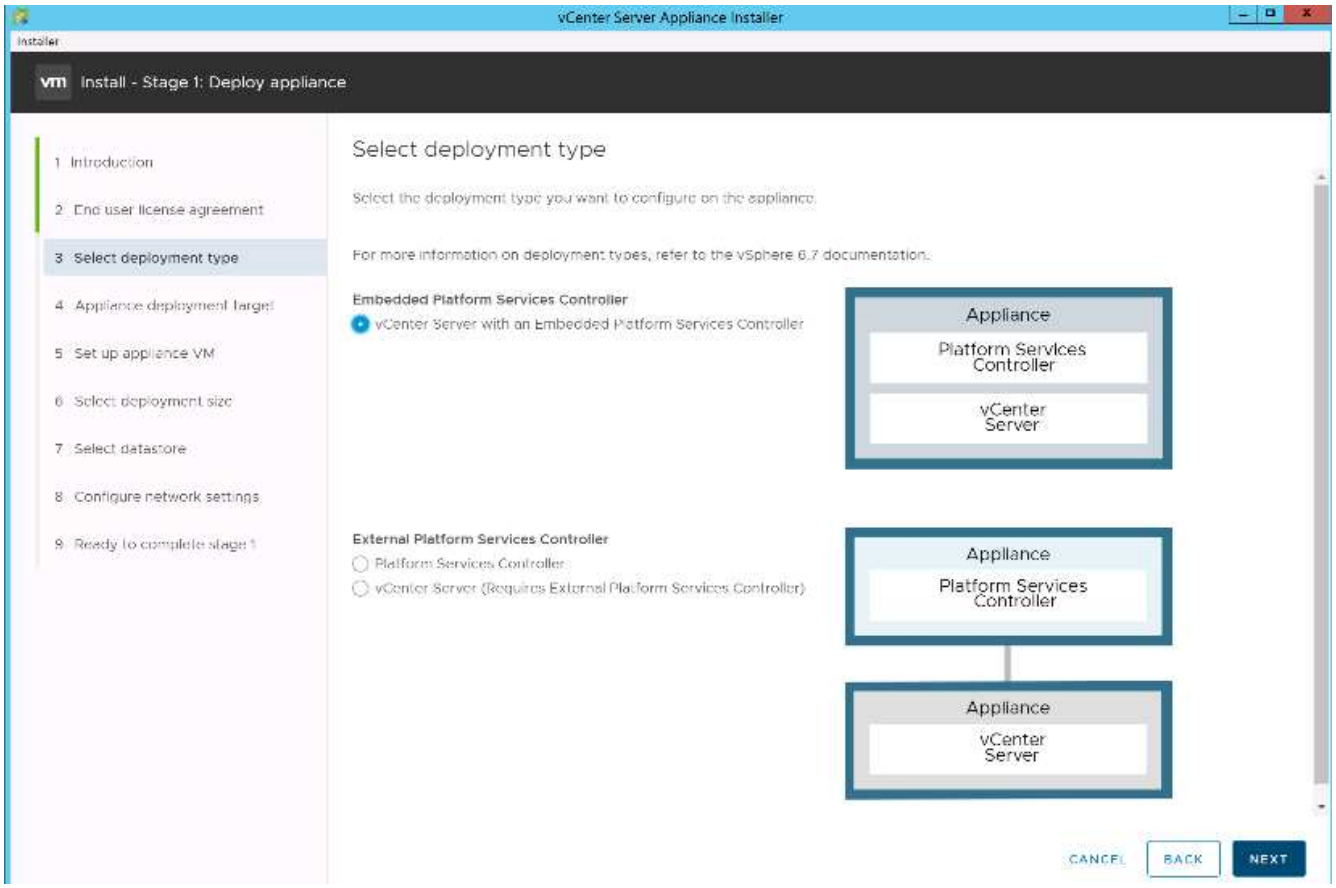
1. Descargue el VCSA. Acceda al enlace de descarga haciendo clic en el icono Get vCenter Server cuando gestione el host ESXi.



2. Descargue el VCSA desde el sitio de VMware.

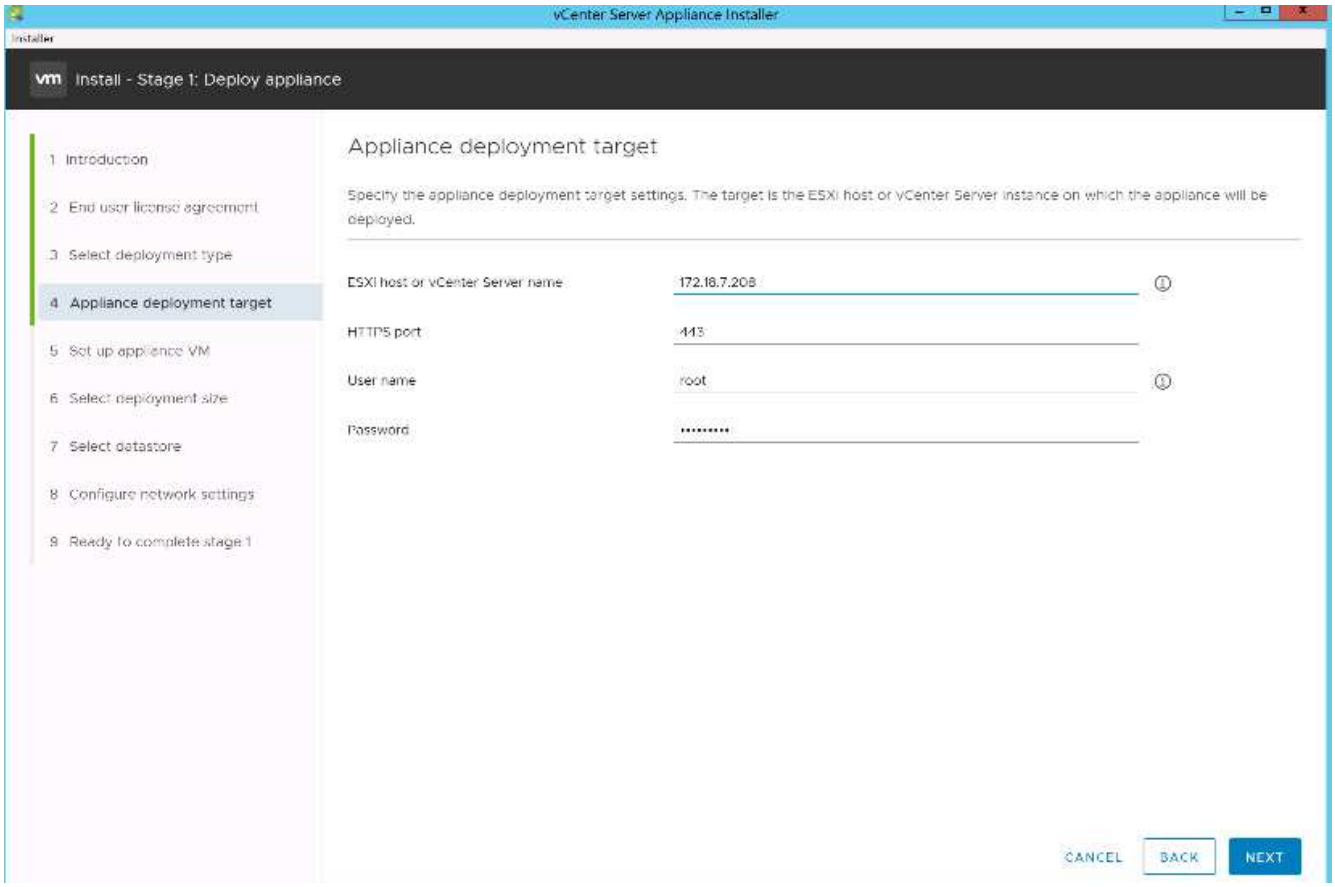
Aunque se admite la instalación de Microsoft Windows vCenter Server, VMware recomienda VCSA para las nuevas implementaciones.

3. Monte la imagen ISO.
4. Desplácese hasta la `vcsa-ui-installer` > `win32` directorio. Haga doble clic `installer.exe`.
5. Haga clic en instalar.
6. Haga clic en Siguiente en la página Introducción.
7. Acepte el contrato de licencia para usuario final.
8. Seleccione Embedded Platform Services Controller (controladora de servicios de plataforma integrada) como tipo de implementación.

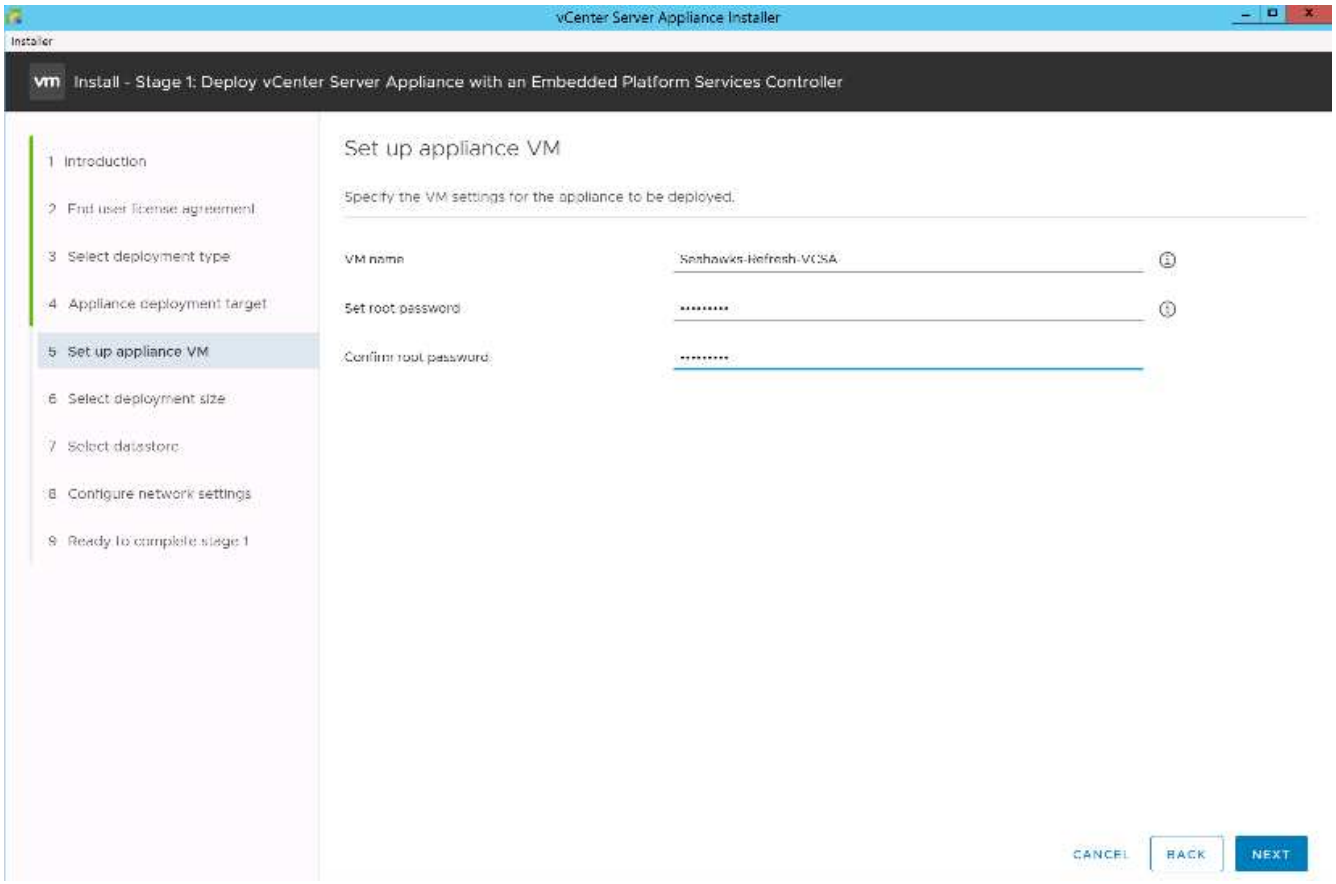


Si es necesario, también admite la puesta en marcha de la controladora de servicios de plataforma externa como parte de la solución FlexPod Express.

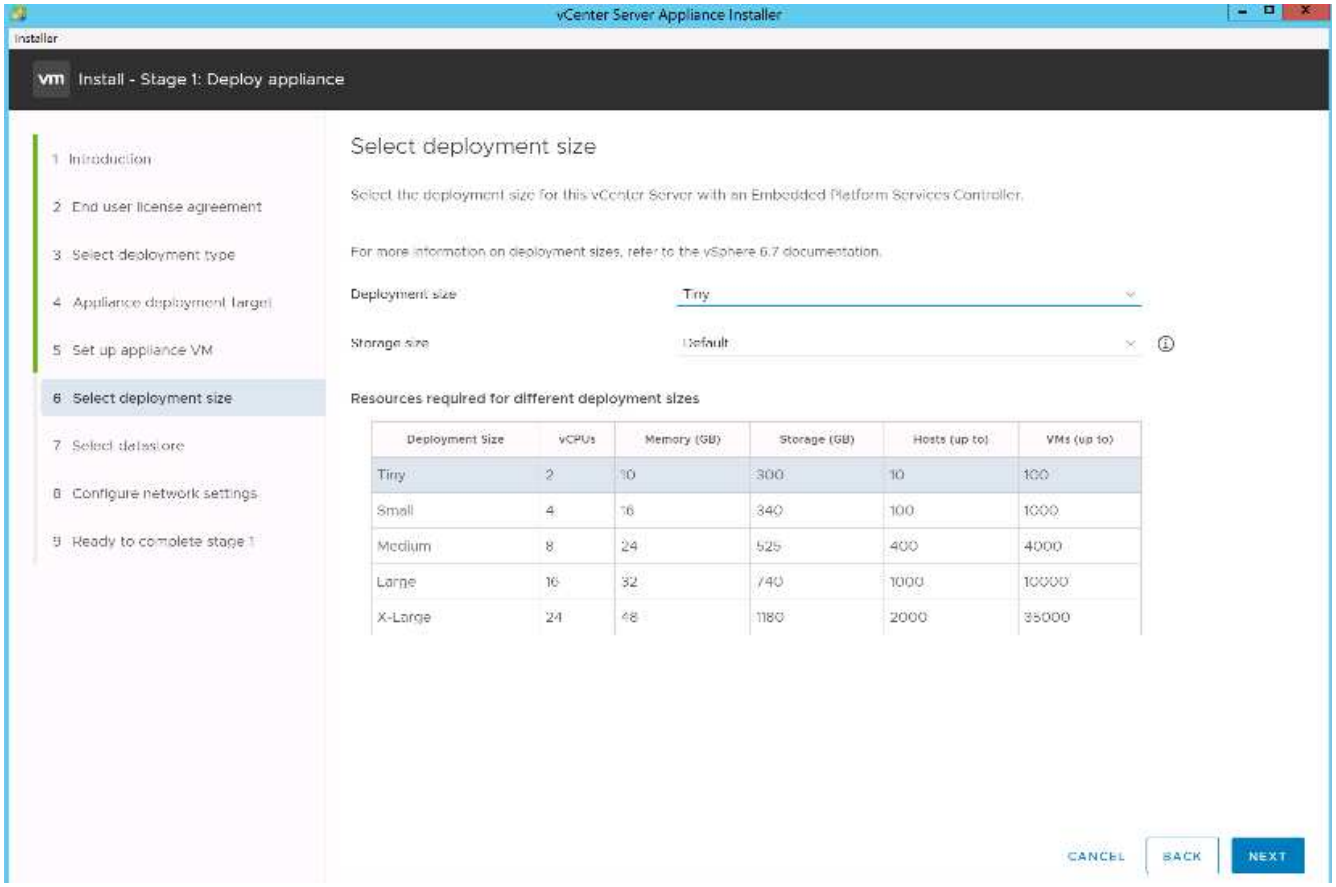
9. En la página Appliance Deployment Target, introduzca la dirección IP de un host ESXi que haya implementado, el nombre de usuario raíz y la contraseña raíz. Haga clic en Siguiente.



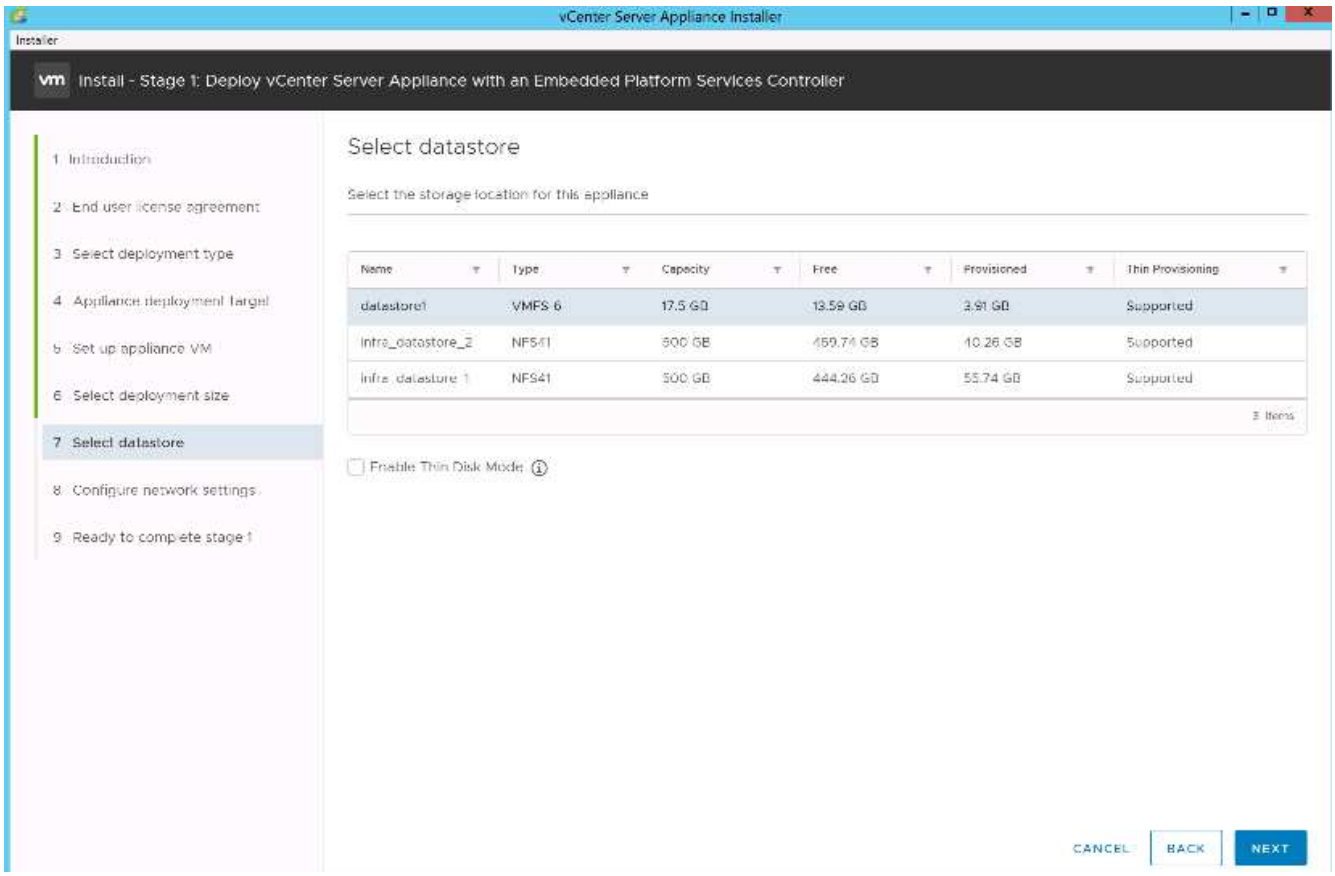
10. Para establecer el equipo virtual, introduzca VCSA como nombre de equipo virtual y la contraseña de raíz que desea utilizar para el VCSA. Haga clic en Siguiente.



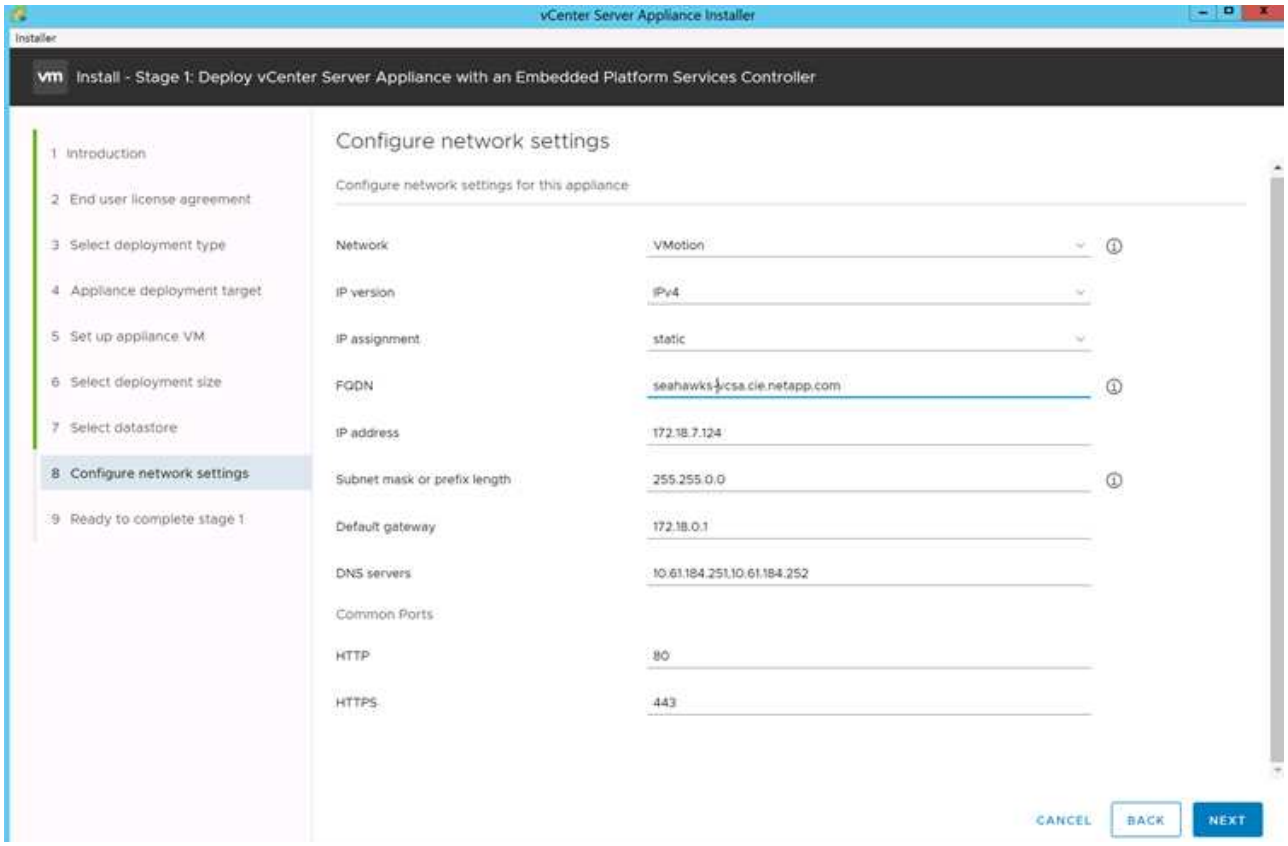
11. Seleccione el tamaño de puesta en marcha que mejor se adapte a su entorno. Haga clic en Siguiente.



12. Seleccione la `infra_datastore_1` almacén de datos. Haga clic en Siguiente.



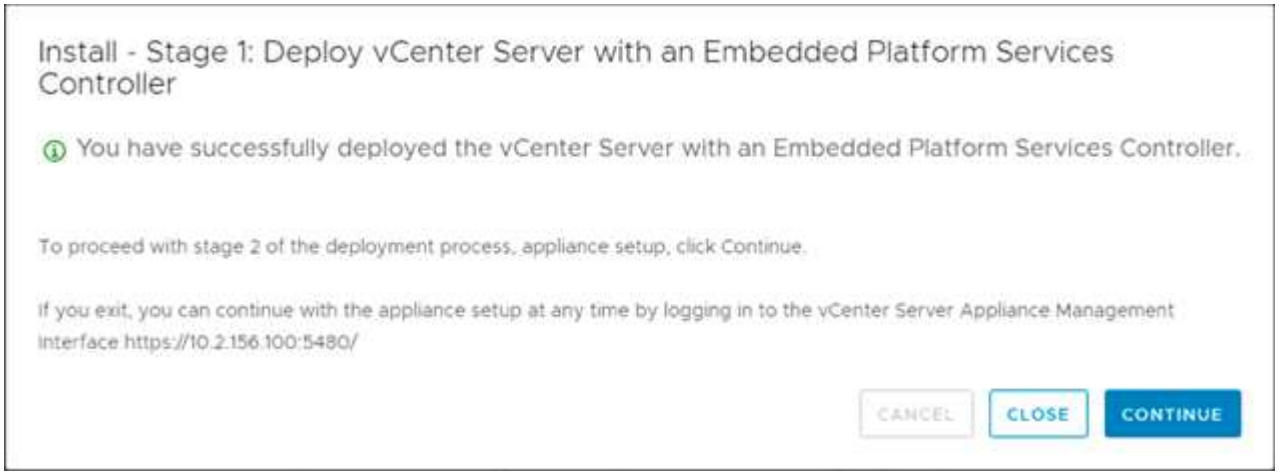
13. Introduzca la siguiente información en la página Configure Network Settings y haga clic en Next.
    a. Seleccione MGMT-Network como su red.
    b. Introduzca el FQDN o IP que se va a utilizar para la VCSA.
    c. Introduzca la dirección IP que se utilizará.
    d. Introduzca la máscara de subred que desea utilizar.
    e. Introduzca la pasarela predeterminada.
    f. Introduzca el servidor DNS.



14. En la página Ready to Complete Stage 1, compruebe que los ajustes introducidos son correctos. Haga clic en Finalizar.

    La VCSA se instala ahora. Este proceso tarda varios minutos.

15. Una vez completada la fase 1, aparece un mensaje que indica que se ha completado. Haga clic en continuar para iniciar la configuración de la fase 2.



16. En la página Introducción de fase 2, haga clic en Siguiente.
17. Introduzca `<<var_ntp_id>>` Para la dirección del servidor NTP. Puede introducir varias direcciones IP de NTP.

    Si planea utilizar la alta disponibilidad de vCenter Server, asegúrese de que el acceso SSH esté habilitado.

18. Configure el nombre de dominio, la contraseña y el nombre del sitio de SSO. Haga clic en Siguiente.

    Registre estos valores para su referencia, especialmente si se desvía de la `vsphere.local` nombre de dominio.

19. Únase al programa de experiencia del cliente de VMware si lo desea. Haga clic en Siguiente.
20. Vea el resumen de la configuración. Haga clic en Finalizar o utilice el botón Atrás para editar la configuración.
21. Aparece un mensaje que indica que no puede pausar o detener la instalación para que se complete después de que se haya iniciado. Haga clic en OK para continuar.

    La configuración del dispositivo continúa. Esto tarda varios minutos.

    Aparece un mensaje que indica que la configuración se ha realizado correctamente.

    Los enlaces que el instalador proporciona para acceder a vCenter Server pueden hacer clic.

Configure VMware vCenter Server 6.7 y el clustering de vSphere

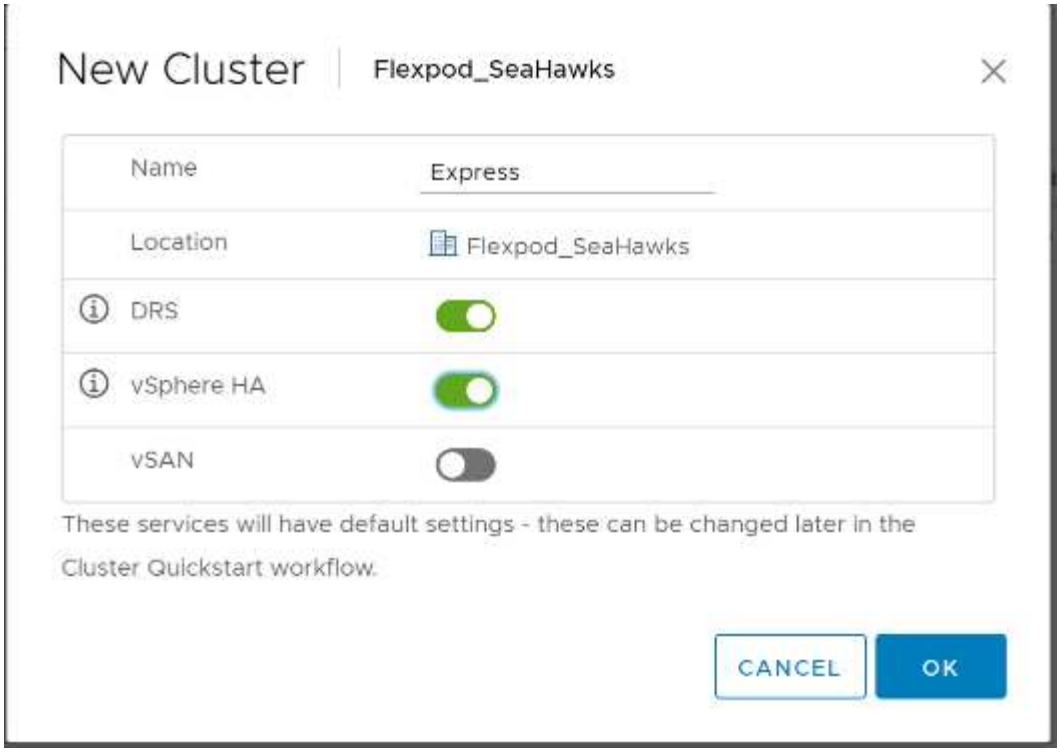
Para configurar la agrupación en clústeres de VMware vCenter Server 6.7 y vSphere, complete los pasos siguientes:

1. Desplácese hasta https://<<FQDN or IP of vCenter>>/vsphere-client/.
2. Haga clic en Launch vSphere Client.
3. Inicie sesión con el nombre de usuario administrator@vsphere.loc/ y la contraseña SSO que introdujo durante el proceso de configuración de VCSA.
4. Haga clic con el botón derecho en el nombre de vCenter y seleccione New Datacenter.
5. Introduzca un nombre para el centro de datos y haga clic en Aceptar.

Crear clúster vSphere.

Para crear un clúster de vSphere, complete los siguientes pasos:

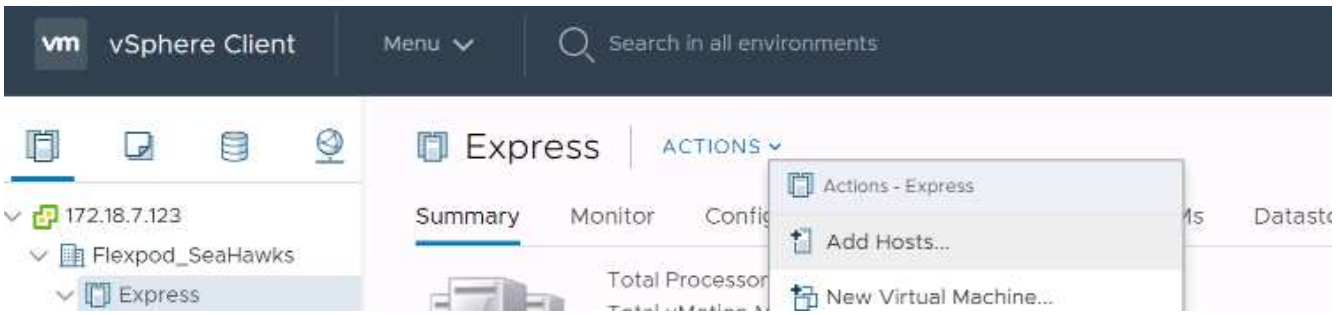
1. Haga clic con el botón derecho en el centro de datos recién creado y seleccione New Cluster.
2. Escriba un nombre para el clúster.
3. Seleccione y habilite las opciones de DRS y vSphere ha.
4. Haga clic en Aceptar.



Agregue hosts ESXi al Cluster

Para añadir hosts ESXi al clúster, complete los siguientes pasos:

1. Seleccione Add Host en el menú Actions del clúster.



2. Para añadir un host ESXi al clúster, complete los siguientes pasos:
   a. Introduzca la dirección IP o el FQDN del host. Haga clic en Siguiente.
   b. Introduzca el nombre de usuario raíz y la contraseña. Haga clic en Siguiente.
   c. Haga clic en Sí para reemplazar el certificado del host por un certificado firmado por el servidor de certificados VMware.
   d. Haga clic en Siguiente en la página Resumen de host.
   e. Haga clic en el icono verde + para añadir una licencia al host de vSphere.

      Este paso se puede completar más adelante si se desea.

   f. Haga clic en Siguiente para desactivar el modo de bloqueo.
   g. Haga clic en Next en la página de ubicación de la máquina virtual.

h. Revise la página Listo para completar. Utilice el botón Atrás para realizar cualquier cambio o seleccione Finalizar.

3. Repita los pasos 1 y 2 para el host Cisco UCS B.

   Debe completar este proceso para los hosts adicionales que se agreguen a la configuración exprés de FlexPod.

Configure coredump en hosts ESXi

Configuración de colector ESXi para hosts arrancados con iSCSI

Los hosts ESXi que se inician con iSCSI mediante el iniciador del software iSCSI de VMware se deben configurar para hacer volcados de memoria al colector ESXi que forma parte de vCenter. Dump Collector no está habilitado de forma predeterminada en vCenter Appliance. Este procedimiento se debe ejecutar al final de la sección de puesta en marcha de vCenter. Para configurar ESXi Dump Collector, siga estos pasos:

1. Inicie sesión en vSphere Web Client como administrator@vsphere.local y seleccione Home.
2. En el panel central, haga clic en Configuración del sistema.
3. En el panel izquierdo, seleccione Servicios.
4. En Services, haga clic en VMware vSphere ESXi Dump Collector.
5. En el panel central, haga clic en el icono verde de inicio para iniciar el servicio.
6. En el menú acciones, haga clic en Editar tipo de inicio.
7. Seleccione automático.
8. Haga clic en Aceptar.
9. Conéctese a cada host ESXi usando ssh como raíz.
10. Ejecute los siguientes comandos:

```
esxcli system coredump network set –v vmk0 –j <vcenter-ip>
esxcli system coredump network set –e true
esxcli system coredump network check
```

El mensaje `Verified the configured netdump server is running` aparece después de ejecutar el comando final.



Este proceso debe completarse para cualquier host adicional que se añada a FlexPod Express.

Conclusión

FlexPod Express proporciona una solución sencilla y efectiva, ya que proporciona un diseño validado que utiliza componentes líderes del sector. Al escalar agregando componentes adicionales, FlexPod Express puede adaptarse según las necesidades específicas del negocio. FlexPod Express se diseñó teniendo en cuenta a las pequeñas y medianas empresas, oficinas remotas y otras empresas que precisan soluciones dedicadas.

Información adicional

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

- Arquitectura validada de NetApp: 1130 FlexPod Express con VMware vSphere 6.7U1 y NetApp AFF A220 con IP directamente vinculada=basado en Diseño NVA de almacenamiento

  "https://www.netapp.com/us/media/nva-1130-design.pdf"

- Centro de documentación para sistemas AFF y FAS

  "http://docs.netapp.com/platstor/index.jsp"

- Centro de documentación de ONTAP 9

  "http://docs.netapp.com/ontap-9/index.jsp"

- Documentación de productos de NetApp

  "https://docs.netapp.com"

FlexPod Express para VMware vSphere 7,0 con Cisco UCS Mini y NetApp AFF/FAS - NVA - Deployment

Jyh-shing Chen, NetApp

La solución FlexPod Express para VMware vSphere 7,0 con Cisco UCS Mini y la solución AFF/FAS de NetApp aprovecha Cisco UCS Mini con servidores blade B200 M5, interconexiones de estructura en chasis Cisco UCS 6324, switches Cisco Nexus 31108PC-V u otros switches conformes a la normativa y el par de alta disponibilidad de controladoras de la serie FAS2700, AFF A220, C190 o el par de alta disponibilidad de controladoras de la serie, Que ejecuta el software para la gestión de datos ONTAP 9,7 de NetApp. Este documento de puesta en marcha de Arquitectura verificada de NetApp (NVA) contiene los pasos detallados necesarios para configurar los componentes de la infraestructura y para implementar VMware vSphere 7,0 y las herramientas asociadas para crear una infraestructura virtual basada en FlexPod Express de alta fiabilidad y alta disponibilidad.

"FlexPod Express para VMware vSphere 7,0 con Cisco UCS Mini y NetApp AFF/FAS - NVA - Deployment"

FlexPod y Seguridad

FlexPod, la solución a ransomware

TR-4802: FlexPod, la solución para ransomware

Arvind Ramakrishnan, NetApp

En colaboración con: 

Para comprender el ransomware, es necesario en primer lugar comprender algunos puntos clave sobre la criptografía. Los métodos criptográficos permiten el cifrado de datos con una clave secreta compartida (cifrado de clave simétrica) o un par de claves (cifrado de claves asimétrico). Una de estas claves es una clave pública ampliamente disponible y la otra es una clave privada no revelada.

El ransomware es un tipo de malware basado en la criptovirología, que es el uso de criptografía para crear software malicioso. Este malware puede utilizar tanto el cifrado simétrico como el cifrado de claves asimétricas para bloquear los datos de una víctima y exigir un rescate para proporcionar la clave para descifrar los datos de la víctima.

¿Cómo funciona el ransomware?

Los siguientes pasos describen cómo el ransomware utiliza la criptografía para cifrar los datos de la víctima sin ningún ámbito para su descifrado o recuperación por parte de la víctima:

1. El atacante genera un par de claves como en el cifrado de claves asimétricas. La clave pública generada se coloca dentro del malware y el malware se libera.
2. Después de que el malware haya entrado en el equipo o sistema de la víctima, genera una clave simétrica aleatoria utilizando un generador de números pseudoorandom (PRNG) o cualquier otro algoritmo viable de generación de números aleatorios.
3. El malware utiliza esta clave simétrica para cifrar los datos de la víctima. Finalmente, cifra la clave simétrica mediante el uso de la clave pública del atacante que se incrustó en el malware. El resultado de este paso es un cifrado asimétrico de la clave simétrica cifrada y el texto cifrado simétrico de los datos de la víctima.
4. El malware borra los datos de la víctima y la clave simétrica que se utilizó para cifrar los datos, sin así dejar margen para la recuperación.
5. La víctima se muestra ahora el texto cifrado asimétrico de la clave simétrica y un valor de rescate que debe pagarse para obtener la clave simétrica que se utilizó para cifrar los datos.
6. La víctima paga el rescate y comparte el cifrado asimétrico con el atacante. El atacante descifra el cifrado con su clave privada, lo que da como resultado la clave simétrica.
7. El atacante comparte esta clave simétrica con la víctima, que se puede utilizar para descifrar todos los datos y, por tanto, recuperarse del ataque.

Retos

Individuos y organizaciones se enfrentan a los siguientes retos cuando son atacados por ransomware:

- El desafío más importante es que se cobra un costo inmediato en la productividad de la organización o del individuo. Toma tiempo para volver a un estado de normalidad, porque todos los archivos importantes deben ser recuperados, y los sistemas deben ser asegurados.
- Podría llevar a una filtración de datos que contenga información confidencial y confidencial de clientes o clientes, y provocar una situación de crisis que una organización querría evitar claramente.
- Existe una gran posibilidad de que los datos entren en las manos equivocadas o se eliminen por completo, lo que conduce a un punto de retorno nulo que podría ser desastroso para las organizaciones y los individuos.
- Después de pagar el rescate, no hay garantía de que el atacante proporcionará la clave para restaurar los datos.
- No hay garantías de que el atacante se abstenga de transmitir los datos delicados a pesar de pagar el rescate.
- En las grandes empresas, identificar la laguna que llevó a un ataque de ransomware es una tarea tediosa, y asegurar todos los sistemas implica un gran esfuerzo.

¿Quién está en riesgo?

Cualquiera puede ser atacado por ransomware, incluidos individuos y organizaciones grandes. Las organizaciones que no aplican medidas y prácticas de seguridad bien definidas son aún más vulnerables a esos ataques. El efecto del ataque en una organización grande puede ser varias veces mayor de lo que un individuo podría soportar.

El ransomware representa aproximadamente el 28 % de todos los ataques de malware. En otras palabras, más de uno de cada cuatro incidentes de malware es un ataque de ransomware. El ransomware puede propagarse automática e indiscriminadamente a través de Internet y, cuando hay un lapso de seguridad, puede entrar en los sistemas de la víctima y continuar extendiéndose a otros sistemas conectados. Los atacantes tienden a dirigirse a personas u organizaciones que realizan un gran uso compartido de archivos, tienen una gran cantidad de datos confidenciales y críticos o a mantener una protección inadecuada frente a ataques.

Los atacantes tienden a centrarse en los siguientes objetivos potenciales:

- Universidades y comunidades estudiantiles
- Oficinas y organismos gubernamentales
- Hospitales
- De Estados Unidos

Esta no es una lista exhaustiva de objetivos. Usted no puede considerarse seguro de los ataques si se encuentra fuera de una de estas categorías.

¿Cómo se introduce el ransomware en un sistema o se distribuye?

Existen varias formas en las que el ransomware puede entrar en un sistema o propagarse a otros sistemas. En el mundo actual, casi todos los sistemas están conectados entre sí a través de Internet, LAN, WAN, etc. La cantidad de datos que se generan e intercambian entre estos sistemas no hace más que aumentar.

Algunos de los métodos más comunes mediante los que se puede distribuir el ransomware incluyen métodos

que utilizamos diariamente para compartir o acceder a los datos:

- Correo electrónico
- Redes P2P
- Descargas de archivos
- Redes sociales
- Dispositivos móviles
- Conectarse a redes públicas no seguras
- Acceso a direcciones URL Web

Consecuencias de la pérdida de datos

Las consecuencias o los efectos de la pérdida de datos pueden ser más amplios de lo que las organizaciones podrían anticipar. Los efectos pueden variar en función de la duración del tiempo de inactividad o del período de tiempo durante el cual una organización no tiene acceso a sus datos. Cuanto más dure el ataque, mayor será el efecto sobre los ingresos, la Marca y la reputación de la organización. Una organización también puede enfrentarse a problemas legales y a una fuerte disminución de la productividad.

A medida que estas cuestiones continúan persistiéndose con el tiempo, comienzan a magnificar y podrían terminar cambiando la cultura de una organización, dependiendo de cómo responda al ataque. En el mundo actual, la información se propaga rápidamente y las noticias negativas sobre una organización podrían causar un daño permanente a su reputación. Una organización podría enfrentarse a enormes sanciones por pérdida de datos, lo que podría desembocar en el cierre de un negocio.

Efectos financieros

Según un informe reciente "Informe de McAfee", Los costos globales incurridos por el crimen cibernético son aproximadamente 600 mil millones de dólares, lo que representa aproximadamente el 0.8% del PIB global. Cuando esta cantidad se compara con la creciente economía mundial de internet de 4.2 billones de dólares, equivale a un impuesto del 14% sobre el crecimiento.

El ransomware asume una parte importante de este coste financiero. En 2018, los costos incurridos debido a los ataques de ransomware fueron aproximadamente de $8 mil millones—una cantidad que se prevé que alcanzará los $11.5 mil millones en 2019.

¿Cuál es la solución?

La recuperación a partir de un ataque de ransomware con un tiempo de inactividad mínimo solo es posible gracias a la implementación de un plan de recuperación ante desastres proactivo. Tener la capacidad para recuperarse de un ataque es bueno, pero evitar un ataque es ideal.

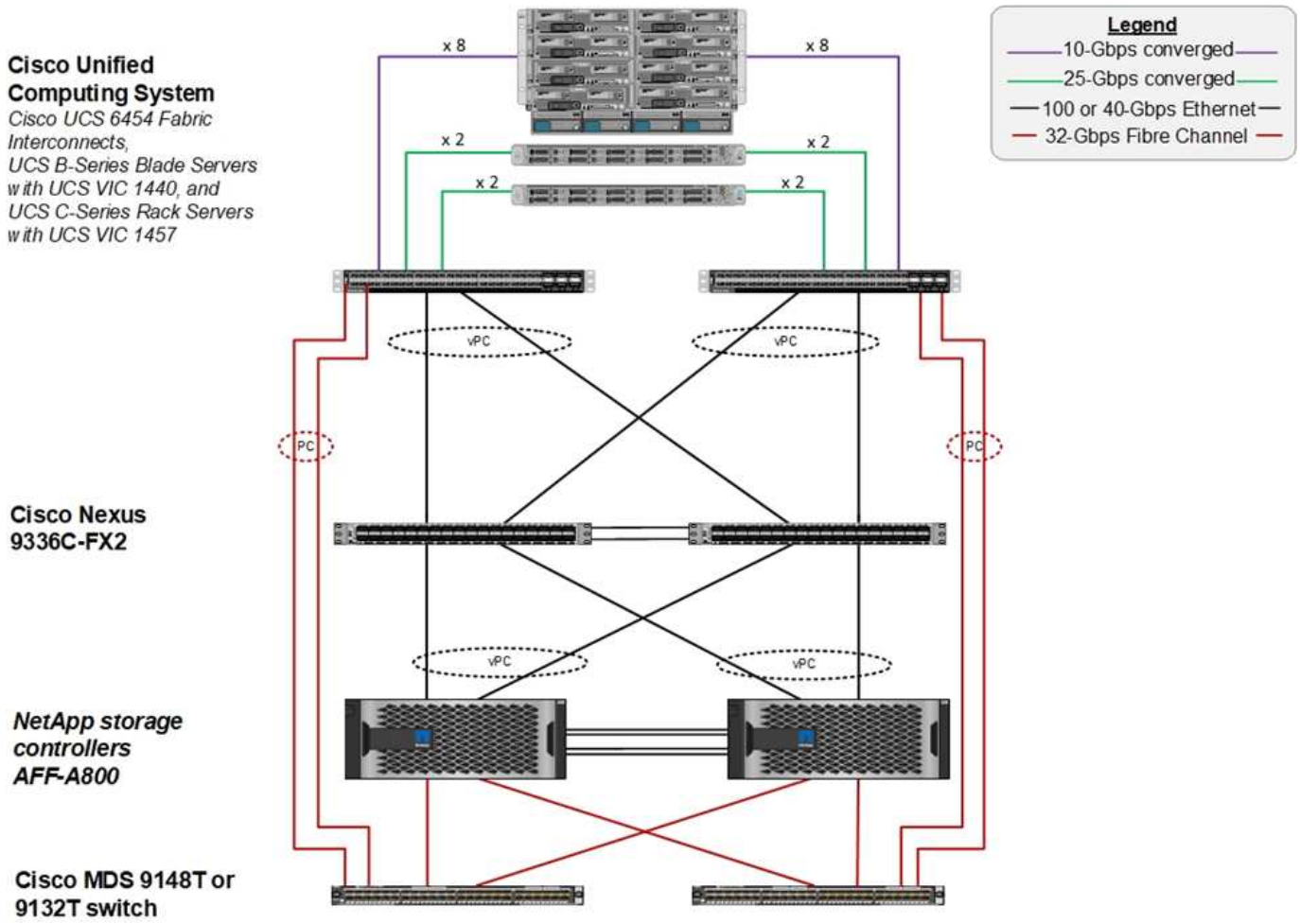
Aunque hay varios frentes que se deben revisar y reparar para evitar un ataque, el componente central que permite prevenir o recuperar de un ataque es el centro de datos.

El diseño del centro de datos y las funciones que proporciona para proteger los puntos finales de red, informática y almacenamiento tienen un papel fundamental a la hora de crear un entorno seguro para las operaciones cotidianas. Este documento muestra cómo las funciones de una infraestructura de cloud híbrido de FlexPod pueden ayudar a lograr una recuperación de datos rápida en caso de ataque, y también pueden ayudar a evitar ataques.

Información general de FlexPod

FlexPod es una arquitectura prediseñada, integrada y validada que combina servidores Cisco Unified Computing System (Cisco UCS), la familia de switches Cisco Nexus, switches estructurales Cisco MDS y cabinas de almacenamiento de NetApp en una sola arquitectura flexible. Las soluciones FlexPod están diseñadas para ofrecer alta disponibilidad sin puntos únicos de error, a la vez que mantienen la rentabilidad y la flexibilidad del diseño necesarias para acomodar una amplia variedad de cargas de trabajo. Un diseño de FlexPod puede admitir diferentes hipervisores y servidores con configuración básica, y también puede dimensionarse y optimizarse según los requisitos de carga de trabajo de los clientes.

La siguiente figura muestra la arquitectura de FlexPod y destaca claramente la alta disponibilidad en todas las capas de la pila. Los componentes de la infraestructura de almacenamiento, red y computación se configuran de forma que las operaciones se pueden conmutar al respaldo instantáneamente al partner superviviente en caso de que uno de los componentes falle.



Una ventaja importante para un sistema FlexPod es que está diseñado, integrado y validado para varias cargas de trabajo. Se publican guías detalladas de diseño e instalación para cada validación de soluciones. Estos documentos incluyen las prácticas recomendadas que debe emplear para que las cargas de trabajo se ejecuten sin problemas en FlexPod. Estas soluciones se han creado con los mejores productos de informática, red y almacenamiento de su clase y con una gran cantidad de funciones centradas en la seguridad y el endurecimiento de toda la infraestructura.

"El índice de inteligencia de amenazas X-Force de IBM" estados, “error humano responsable de dos tercios de los registros comprometidos, incluido un aumento histórico del 424% en infraestructura de nube mal configurada”.

Con un sistema FlexPod, puede evitar una configuración incorrecta de su infraestructura mediante los libros de estrategia de Ansible que realizan una configuración integral de la infraestructura de acuerdo con las mejores prácticas descritas en los diseños validados por Cisco (CVD) y las arquitecturas verificadas de NetApp (NVA).

Medidas de protección contra ransomware

En esta sección se describen las funciones clave del software de gestión de datos ONTAP de NetApp y las herramientas para Cisco UCS y Cisco Nexus que puede usar para proteger y recuperar datos de forma efectiva de ataques de ransomware.

Almacenamiento: ONTAP de NetApp

El software ONTAP ofrece muchas funciones útiles para la protección de datos, la mayoría de las cuales son gratuitas para los clientes que tienen un sistema ONTAP. Puede utilizar las siguientes funciones en todo momento para proteger los datos de los ataques:

- **Tecnología Snapshot de NetApp.** una copia snapshot es una imagen de solo lectura de un volumen que captura el estado de un sistema de archivos en un momento dado. Estas copias ayudan a proteger los datos sin afectar el rendimiento del sistema y, al mismo tiempo, no ocupan mucho espacio de almacenamiento. NetApp recomienda crear un programa para la creación de copias Snapshot. Usted también debe mantener un largo período de retención porque algunos malware pueden permanecer inactivos y luego reactivar semanas o meses después de una infección. En caso de ataque, es posible revertir el volumen utilizando una copia snapshot que se había realizado antes de la infección.
- **Tecnología SnapRestore de NetApp.** el software de recuperación de datos SnapRestore es extremadamente útil para la recuperación de datos dañados o para revertir únicamente el contenido del archivo. SnapRestore no revierte los atributos de un volumen; es mucho más rápido de lo que puede conseguir un administrador al copiar los archivos de la copia snapshot al sistema de archivos activo. La velocidad a la que se pueden recuperar los datos resulta útil cuando se deben recuperar muchos archivos lo antes posible. En caso de ataque, este eficiente proceso de recuperación ayuda a que el negocio vuelva a estar online rápidamente.
- **La tecnología SnapCenter de NetApp.** el software SnapCenter utiliza funciones de backup y replicación basadas en almacenamiento de NetApp para proporcionar una protección de datos coherente con las aplicaciones. Este software se integra con aplicaciones empresariales y proporciona flujos de trabajo específicos para aplicaciones y bases de datos para satisfacer las necesidades de los administradores de aplicaciones, bases de datos e infraestructuras virtuales. SnapCenter proporciona una plataforma empresarial fácil de usar para coordinar y administrar de un modo seguro la protección de datos en aplicaciones, bases de datos y sistemas de archivos. Su capacidad de proporcionar protección de datos coherente con las aplicaciones es fundamental durante la recuperación de datos, ya que facilita la restauración de las aplicaciones a un estado coherente con mayor rapidez.
- **La tecnología SnapLock de NetApp.** SnapLock proporciona un volumen para finalidades especiales en el que los archivos se pueden almacenar y poner en un estado en el que no se pueden borrar ni sobrescribir. Los datos de producción del usuario que se encuentran en un volumen FlexVol se pueden duplicar o realizar copias vault en un volumen SnapLock mediante la tecnología SnapMirror o SnapVault de NetApp, respectivamente. Los archivos del volumen de SnapLock, el volumen en sí y su agregado de alojamiento no se pueden eliminar hasta que finalice el período de retención.
- **Tecnología FPolicy de NetApp.** Utilice el software FPolicy para evitar ataques al desactivar las operaciones en archivos con extensiones específicas. Es posible activar un evento de FPolicy para

operaciones de archivos específicas. El evento está ligado a una política, que llama al motor que necesita utilizar. Puede configurar una política con un conjunto de extensiones de archivo que potencialmente puedan contener ransomware. Cuando un archivo con una extensión no permitida intenta realizar una operación no autorizada, FPolicy impide que esa operación se ejecute.

Red: Cisco Nexus

El software Cisco NX OS admite la función NetFlow que permite una detección mejorada de anomalías y seguridad de la red. NetFlow captura los metadatos de cada conversación de la red, las partes implicadas en la comunicación, el protocolo utilizado y la duración de la transacción. Una vez agregada y analizado la información, puede proporcionar una visión del comportamiento normal.

Los datos recopilados también permiten la identificación de patrones de actividad cuestionables, como el malware que se propaga a través de la red, lo que de otra manera puede pasar desapercibida.

NetFlow utiliza flujos para proporcionar estadísticas para la supervisión de la red. Un flujo es un flujo unidireccional de paquetes que llega a una interfaz de origen (o VLAN) y tiene los mismos valores para las claves. Una clave es un valor identificado para un campo dentro del paquete. Puede crear un flujo utilizando un registro de flujo para definir las claves únicas para su flujo. Puede exportar los datos que NetFlow recopila para sus flujos utilizando un exportador de flujo a un colector NetFlow remoto, como Cisco StealtWatch. StealtWatch utiliza esta información para la supervisión continua de la red y proporciona información forense de respuesta a incidentes y detección de amenazas en tiempo real si se produce un brote de ransomware.

Computación: Cisco UCS

Cisco UCS es el extremo de computación en una arquitectura de FlexPod. Puede usar varios productos de Cisco que pueden ayudar a proteger esta capa de la pila en el nivel del sistema operativo.

Puede implementar los siguientes productos clave en la capa informática o de aplicación:

- **Cisco Advanced Malware Protection (AMP) para endpoints.** compatible con los sistemas operativos Microsoft Windows y Linux, esta solución integra capacidades de prevención, detección y respuesta. Este software de seguridad evita infracciones, bloquea el malware en el punto de entrada y supervisa y analiza continuamente la actividad de los archivos y procesos para detectar, contener y resolver rápidamente amenazas que puedan evadir las defensas de primera línea.

  El componente de Protección de actividad maliciosa (MAP) de AMP supervisa continuamente todas las actividades de los extremos y proporciona detección en tiempo de ejecución y bloqueo del comportamiento anormal de un programa en ejecución en el punto final. Por ejemplo, cuando el comportamiento del punto final indica ransomware, los procesos ofensor se terminan, lo que impide el cifrado del punto final y detiene el ataque.

- **Cisco Advanced Malware Protection for Email Security.** los correos electrónicos se han convertido en el vehículo principal para propagar malware y llevar a cabo ciberataques. En promedio, aproximadamente 100 mil millones de correos electrónicos se intercambian en un solo día, lo que proporciona a los atacantes un excelente vector de penetración en los sistemas de los usuarios. Por lo tanto, es absolutamente esencial defender contra esta línea de ataque.

  AMP analiza correos electrónicos para amenazas tales como exploits de día cero y malware sigiloso ocultos en archivos adjuntos maliciosos. También utiliza la inteligencia de URL líder en el sector para combatir enlaces maliciosos. Proporciona a los usuarios protección avanzada contra el phishing espear, el ransomware y otros ataques sofisticados.

- **Sistema de prevención de intrusiones de próxima generación (NGIPS).** Cisco Firepower NGIPS se puede implementar como un dispositivo físico en el centro de datos o como un dispositivo virtual en

VMware (NGIPSv para VMware). Este sistema altamente eficaz de prevención de intrusiones proporciona un rendimiento fiable y un costo total de propiedad bajo. La protección contra amenazas se puede ampliar con licencias de suscripción opcionales para proporcionar funciones de AMP, visibilidad y control de aplicaciones y filtrado de URL. La virtualización de NGIPS inspecciona el tráfico entre equipos virtuales (VM) y facilita la implementación y gestión de soluciones de NGIPS en sitios con recursos limitados, lo que aumenta la protección tanto para activos físicos como virtuales.

Proteja y recupere datos en FlexPod

En esta sección se describe cómo se pueden recuperar los datos de un usuario final en caso de un ataque y cómo se pueden prevenir los ataques mediante un sistema FlexPod.

Resumen de banco

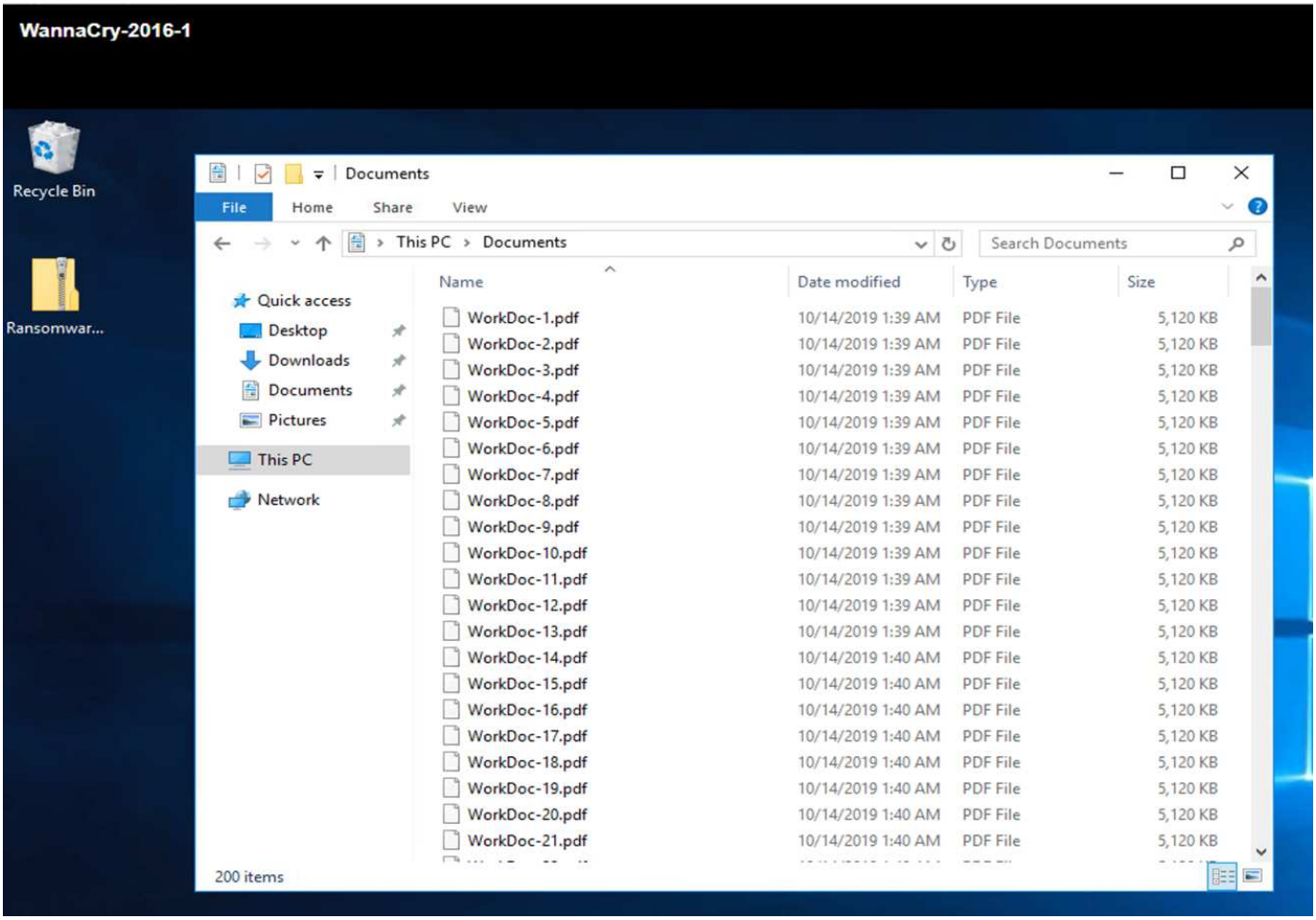
Para presentar la detección, la corrección y la prevención de FlexPod, se creó un banco de pruebas basado en las directrices especificadas en el último CVD de plataforma disponible en el momento en el que se escribió este documento: "FlexPod Datacenter con VMware vSphere 6.7 U1, Cisco UCS de cuarta generación y NetApp AFF A-Series CVD".

Se puso en marcha un equipo virtual con Windows 2016, que proporcionaba un recurso compartido CIFS del software ONTAP de NetApp, en la infraestructura de VMware vSphere. A continuación, se configuró FPolicy de NetApp en el recurso compartido de CIFS para evitar la ejecución de archivos con ciertos tipos de extensiones. El software SnapCenter de NetApp también se puso en marcha para gestionar las copias Snapshot de los equipos virtuales de la infraestructura para proporcionar copias Snapshot coherentes con las aplicaciones.

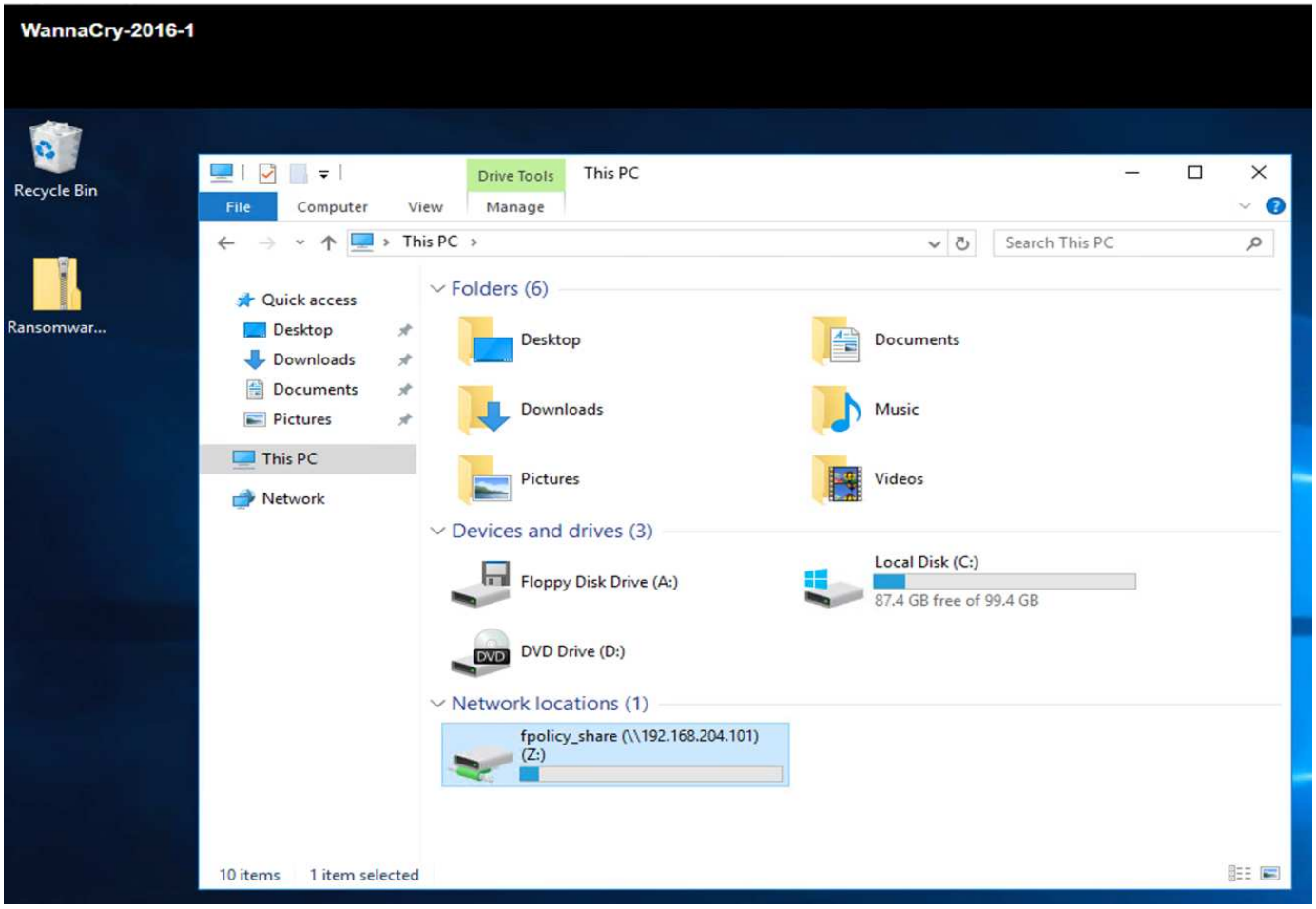
Estado del equipo virtual y sus archivos antes de un ataque

En esta sección se muestra el estado de los archivos antes de un ataque a la máquina virtual y al recurso compartido CIFS que se le ha asignado.

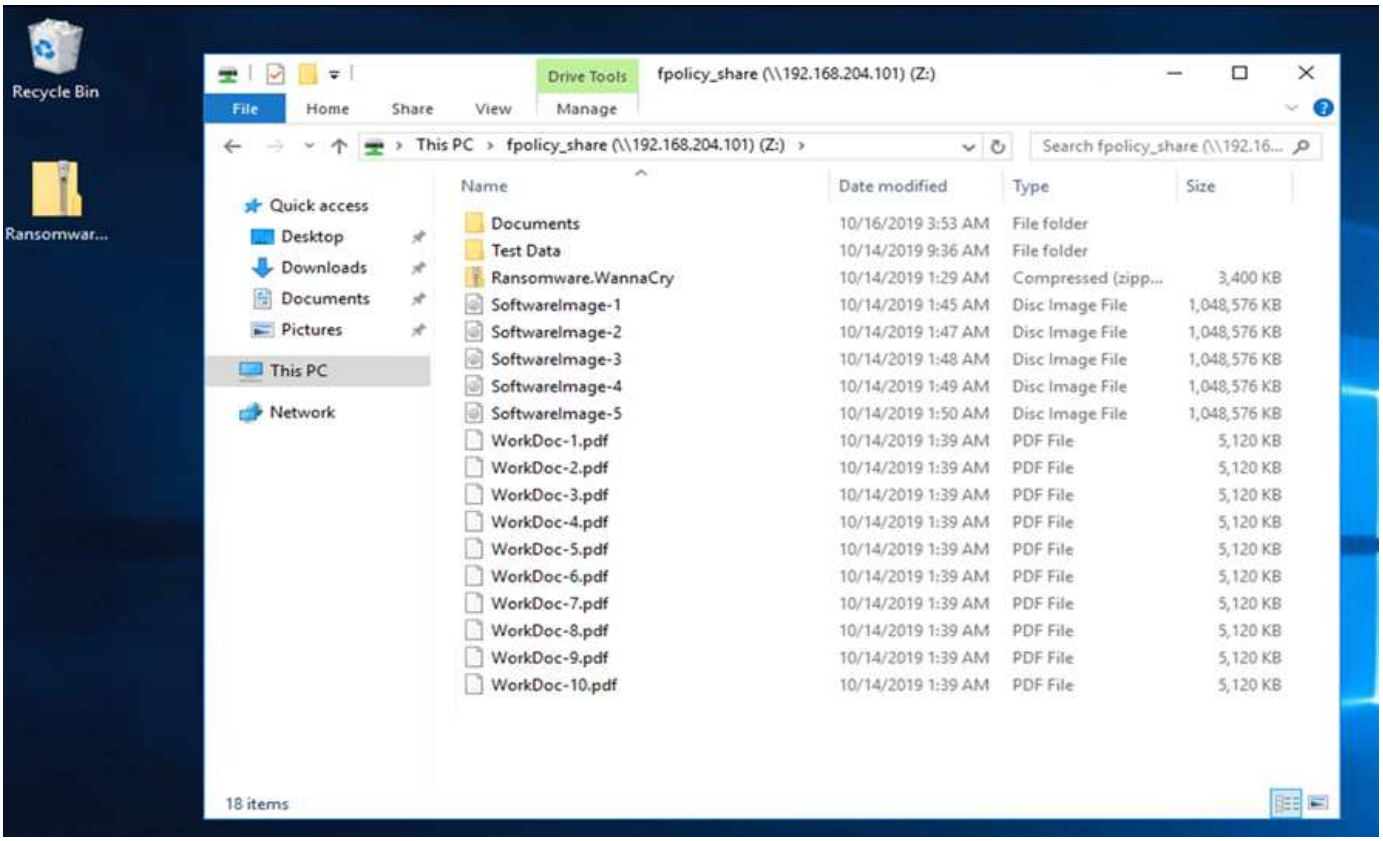
La carpeta Documentos del equipo virtual tenía un conjunto de archivos PDF que todavía no han sido cifrados por el malware WannaCry.



La siguiente captura de pantalla muestra el recurso compartido de CIFS asignado a la máquina virtual.



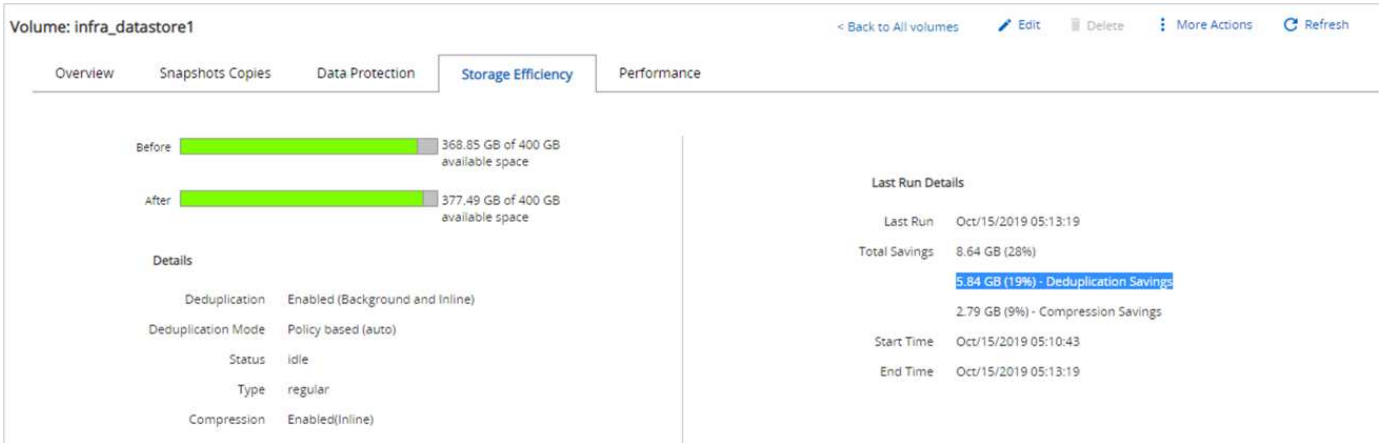
La siguiente captura de pantalla muestra los archivos del recurso compartido CIFS `fpolicy_share` Que todavía no han sido cifrados por el malware WannaCry.



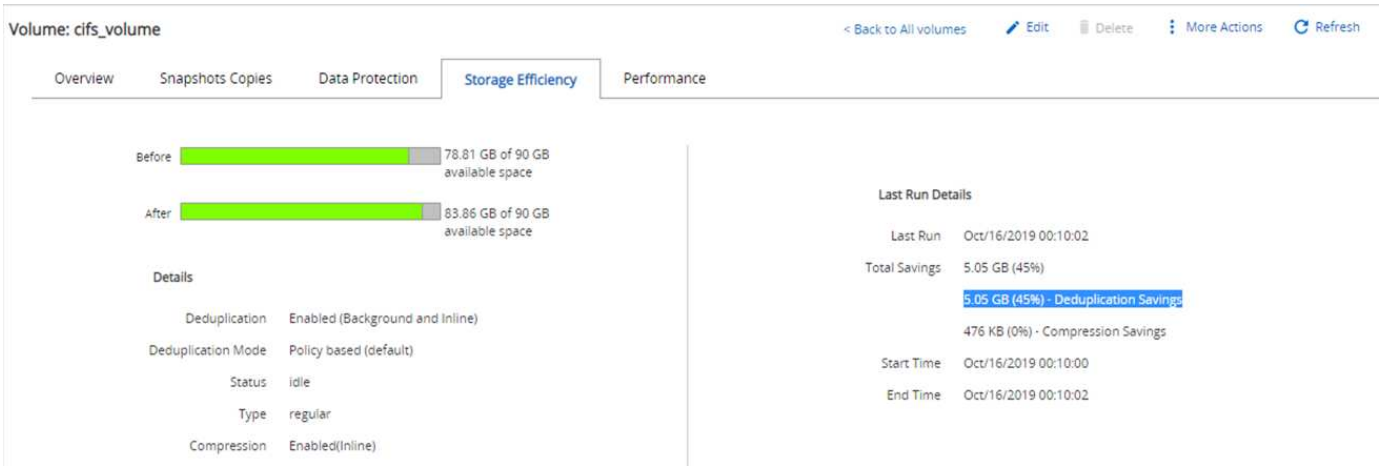
Información sobre deduplicación y copias snapshot antes de un ataque

Los detalles de la eficiencia del almacenamiento y el tamaño de la copia Snapshot antes de un ataque se indican y se utilizan como referencia durante la fase de detección.

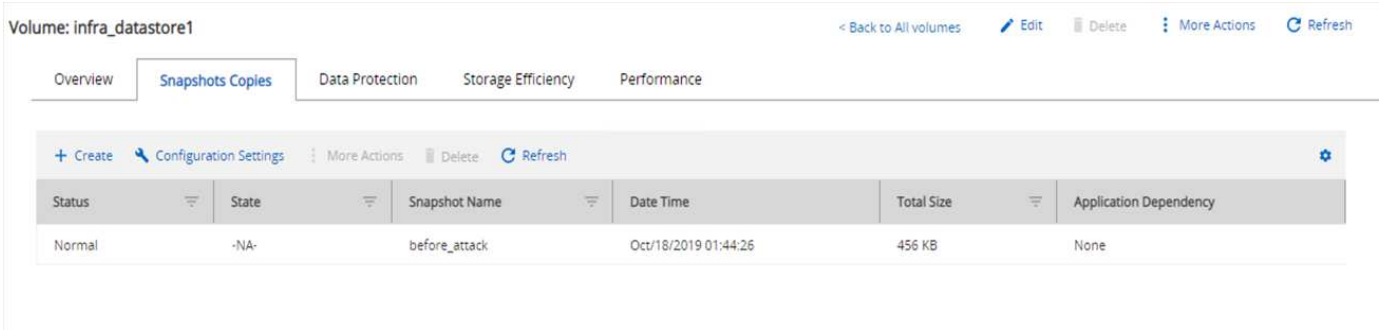
Se obtuvo un ahorro del 19% en el almacenamiento, gracias a la deduplicación en el volumen que alojaba el equipo virtual.



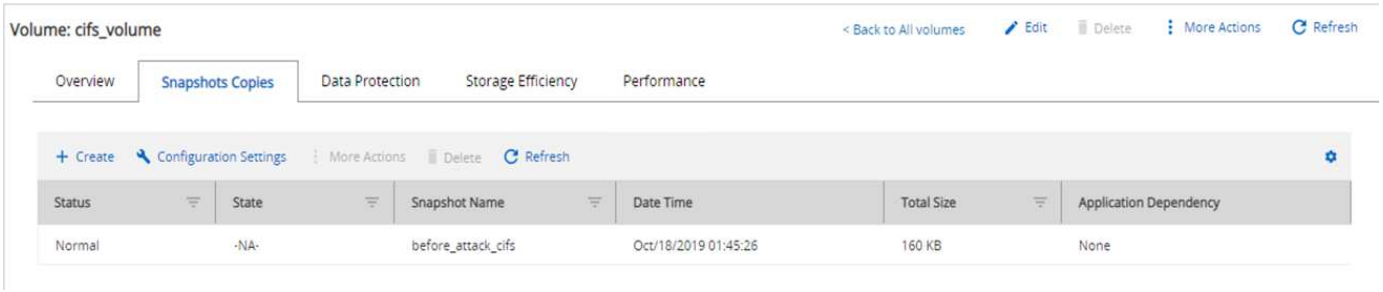
Se obtuvo un ahorro del 45% gracias a la deduplicación en la unidad CIFS `fpolicy_share`.



Se observó un tamaño de copia snapshot de 456 KB para el volumen donde se alojaba el equipo virtual.



Se observó un tamaño de copia Snapshot de 160 KB para el recurso compartido de CIFS `fpolicy_share`.



Infección de WannaCry en VM y recursos compartidos de CIFS

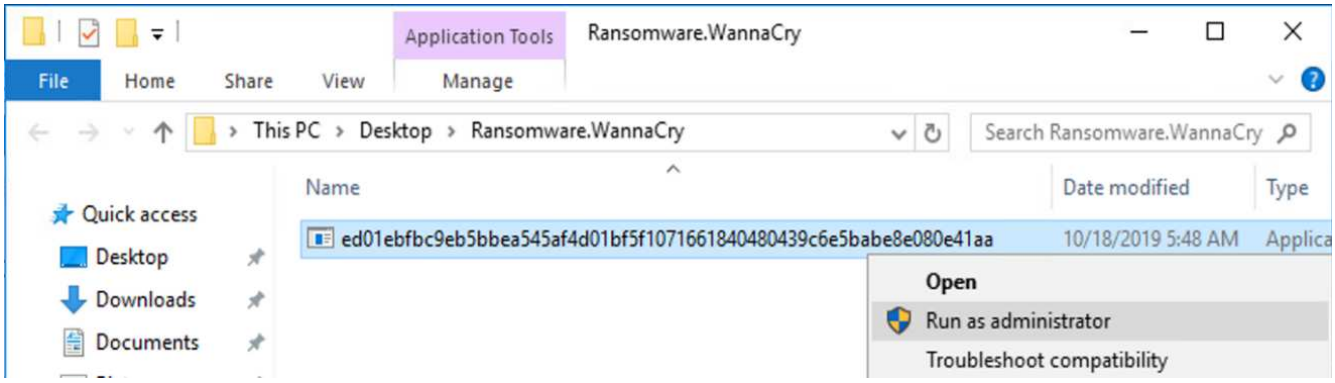
En esta sección, mostramos cómo se introdujo el malware de WannaCry en el entorno de FlexPod y los posteriores cambios en el sistema que se observaron.

Los pasos siguientes muestran cómo se introdujo el binario de malware WannaCry en el equipo virtual:

1. Se extrajo el malware protegido.



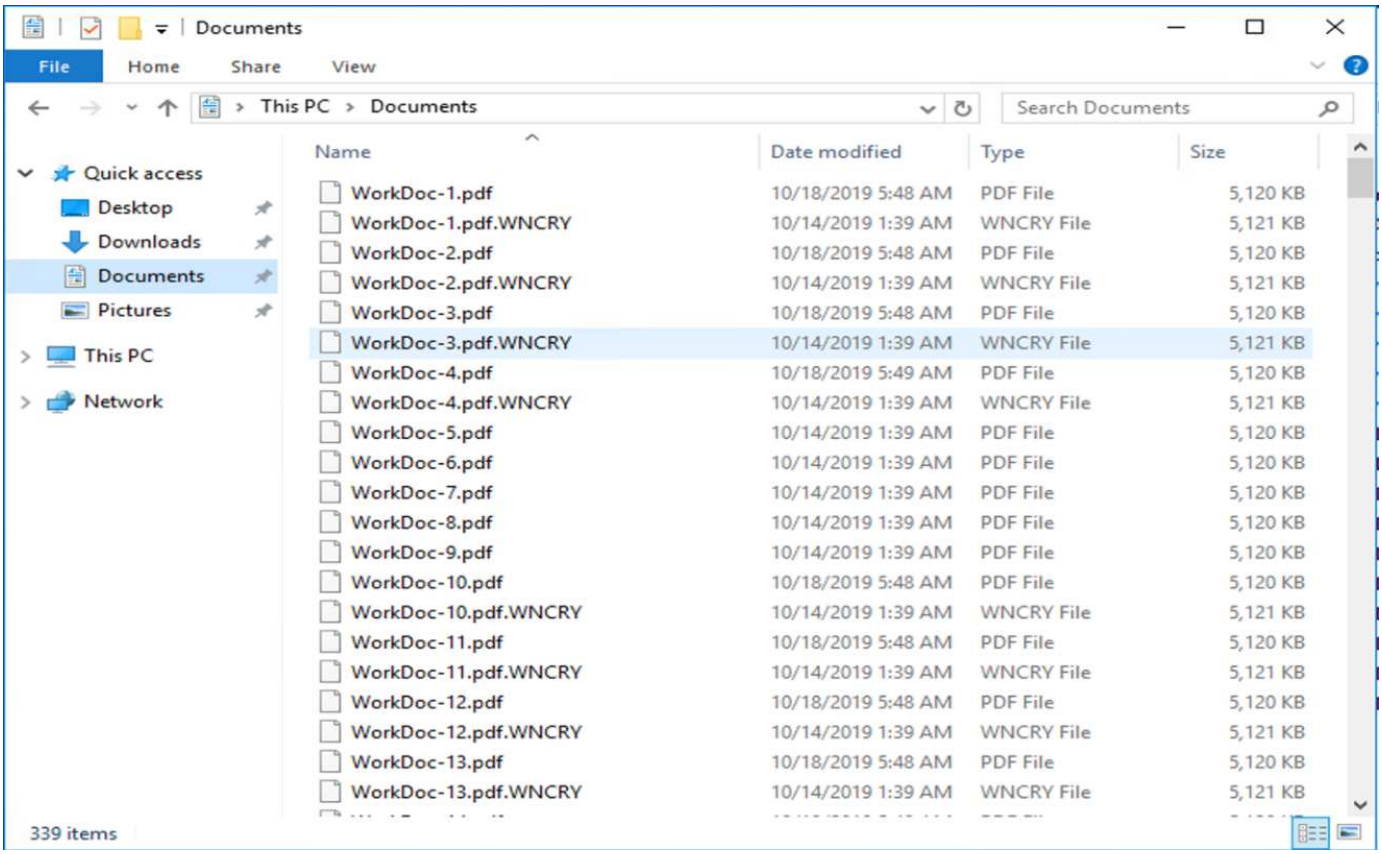
2. Se ejecutó el binario.



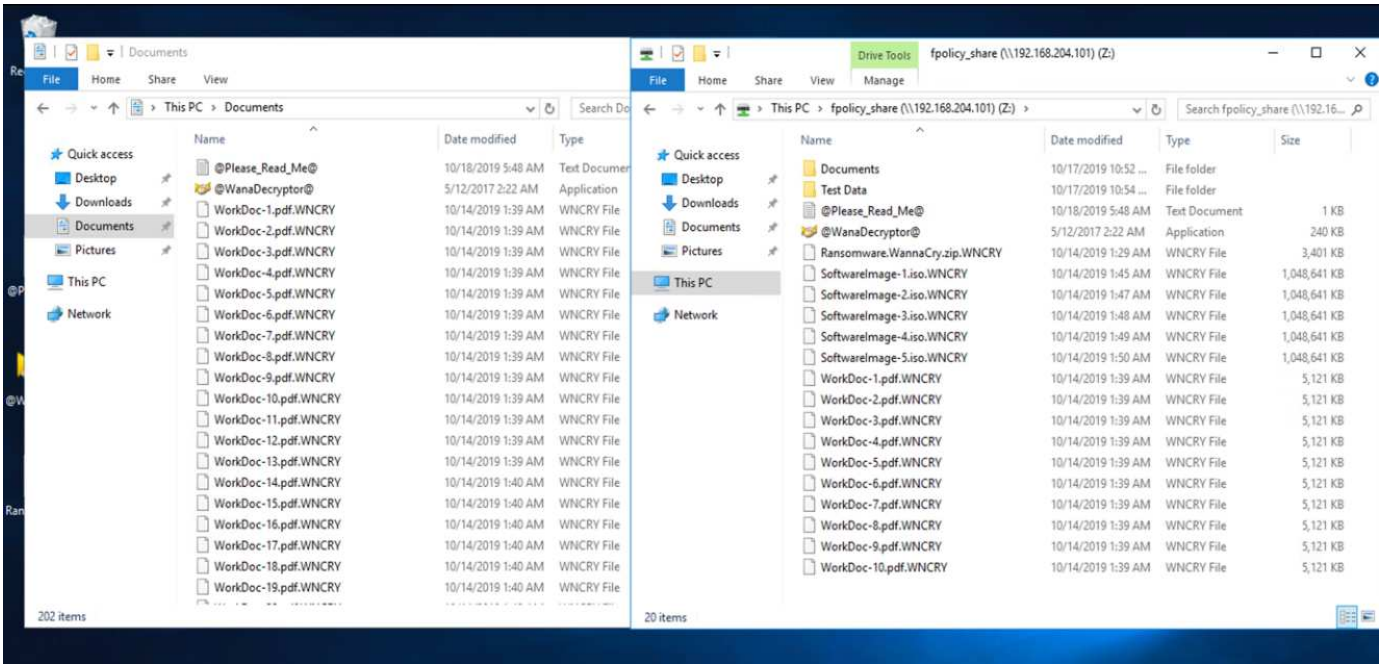
Caso 1: WannaCry cifra el sistema de archivos dentro del equipo virtual y el recurso compartido CIFS asignado

El sistema de archivos local y el recurso compartido CIFS asignado fueron cifrados por el malware WannaCry.

El malware comienza a cifrar archivos con extensiones WNCRY.



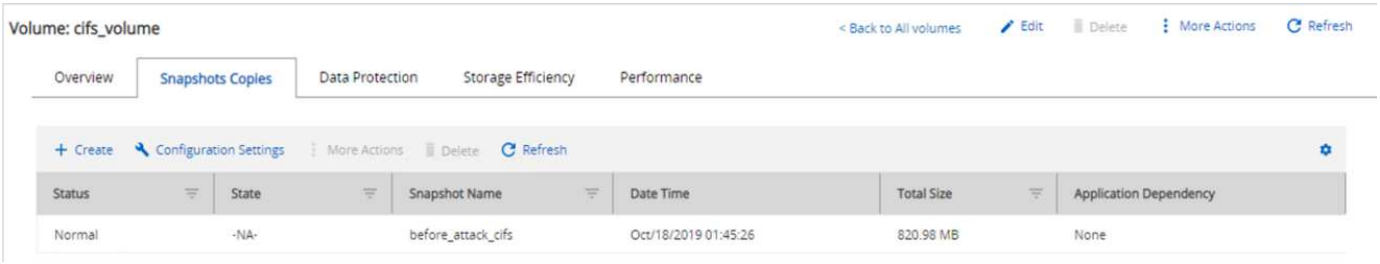
El malware cifra todos los archivos del equipo virtual local y del recurso compartido asignado.



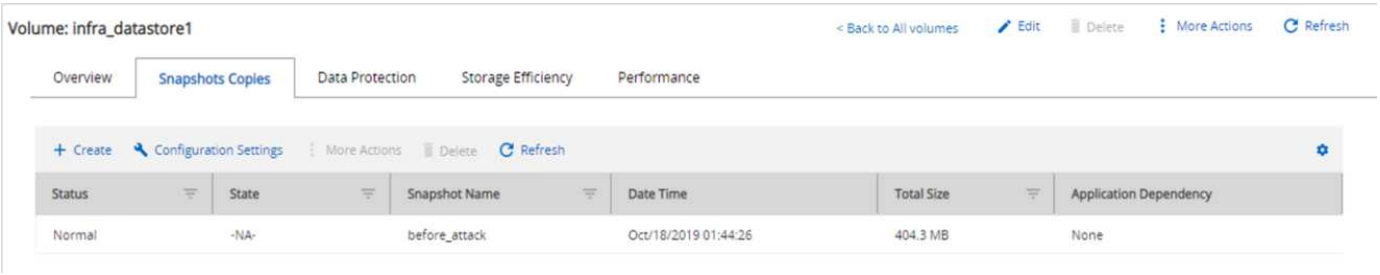
Detección

Desde el momento en que el malware comenzó a cifrar los archivos, se activó un aumento exponencial del tamaño de las copias snapshot y una reducción exponencial del porcentaje de eficiencia del almacenamiento.

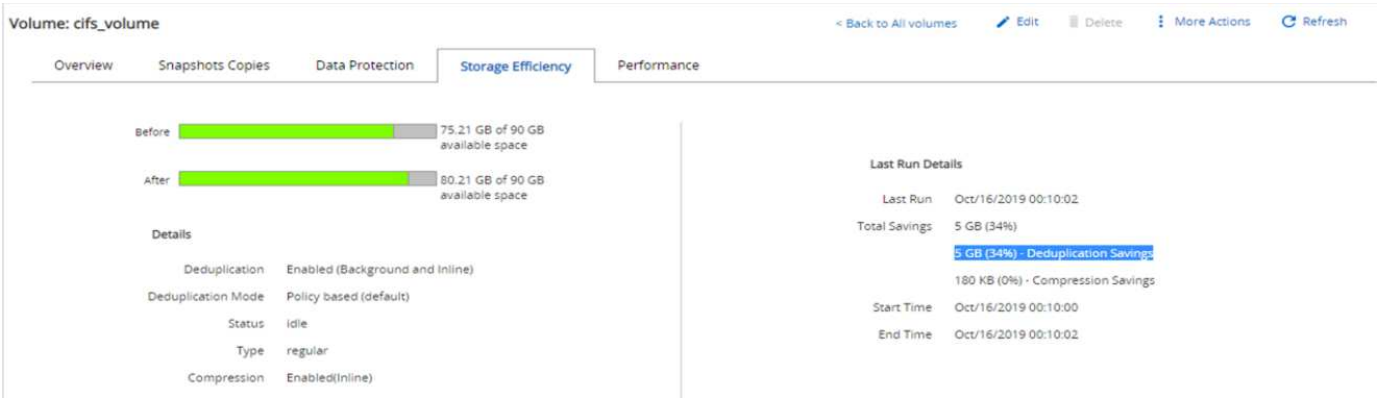
Se detectó un aumento espectacular del tamaño de snapshot a 820,98 MB para el volumen que aloja la unidad CIFS durante el ataque.



Hemos detectado un aumento en el tamaño de la copia snapshot a 404,3 MB para el volumen donde se aloja la máquina virtual.



La eficiencia de almacenamiento para el volumen que aloja la unidad CIFS se redujo a un 34 %.



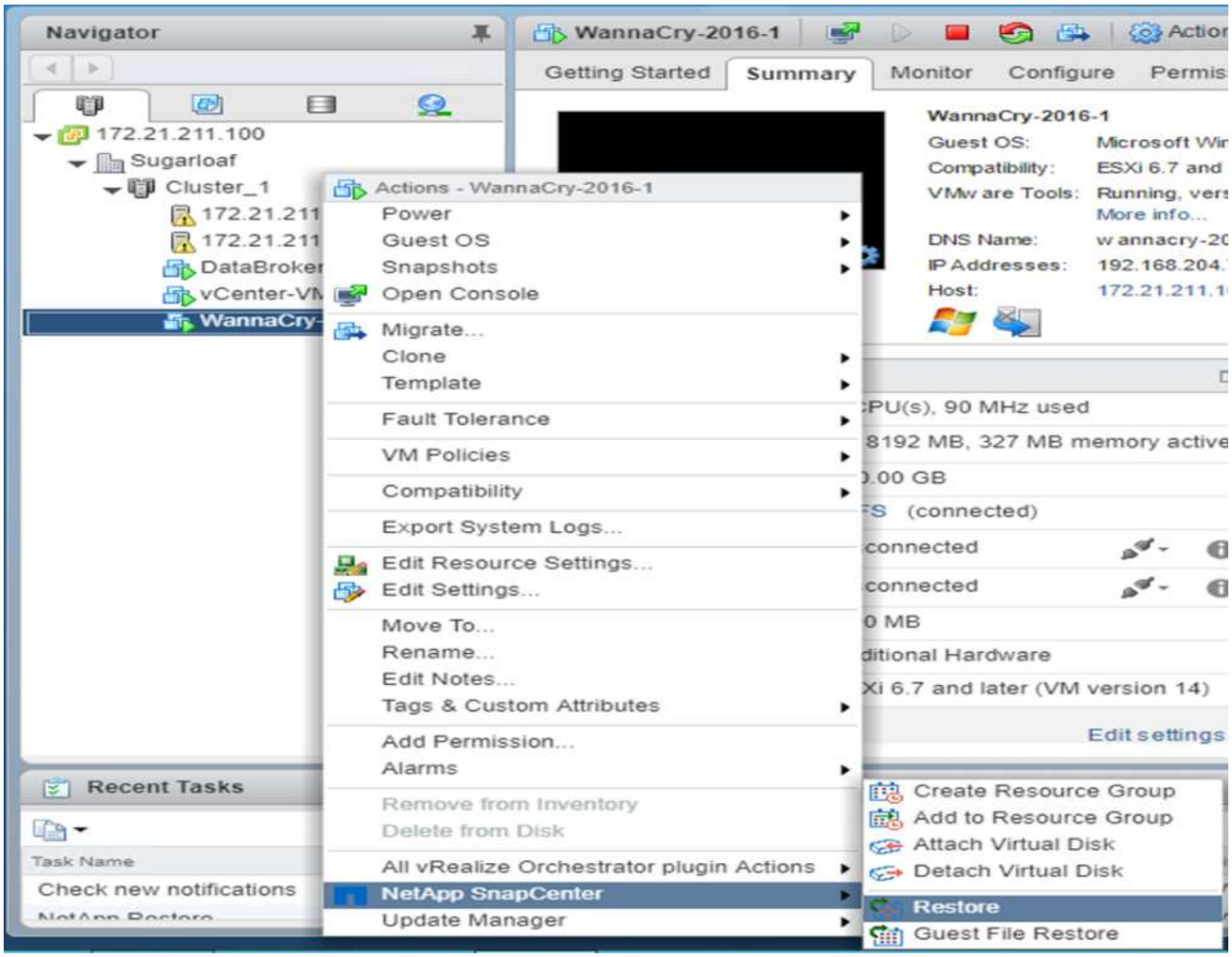
Reparación

Restaurar el equipo virtual y el recurso compartido CIFS asignado mediante una copia Snapshot limpia creada antes del ataque

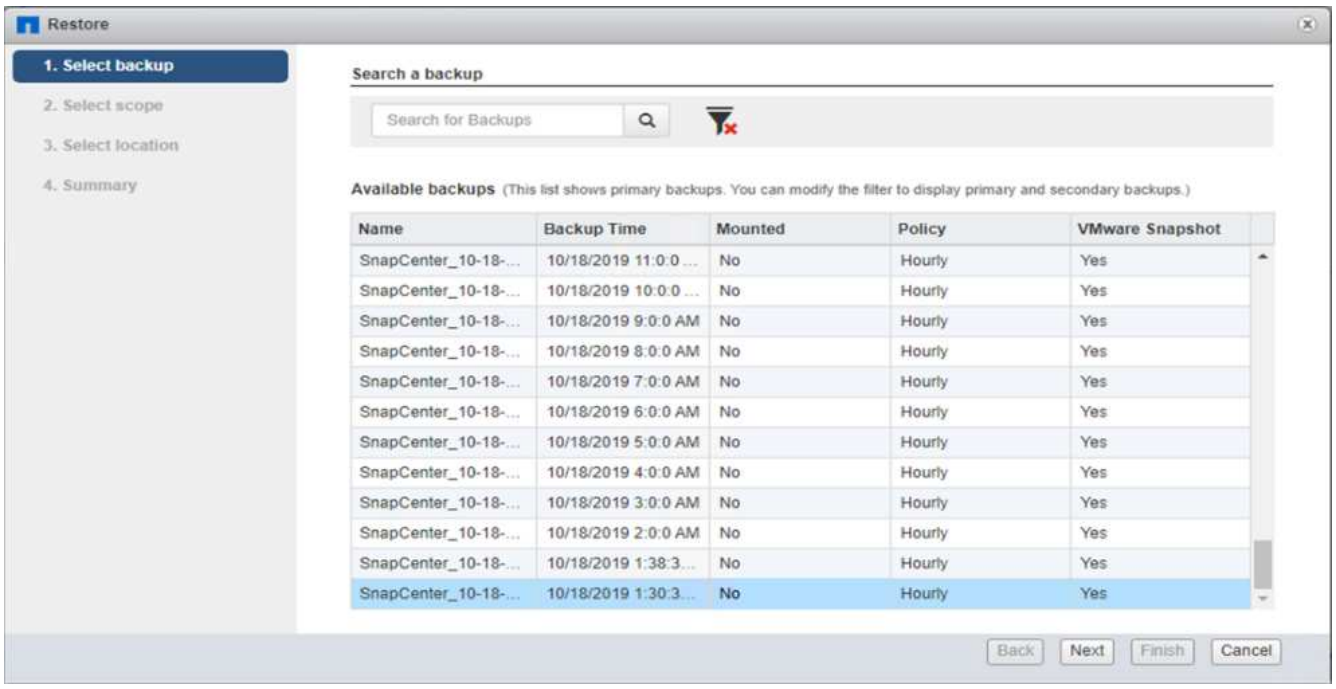
Restaurar VM

Para restaurar el equipo virtual, complete los siguientes pasos:

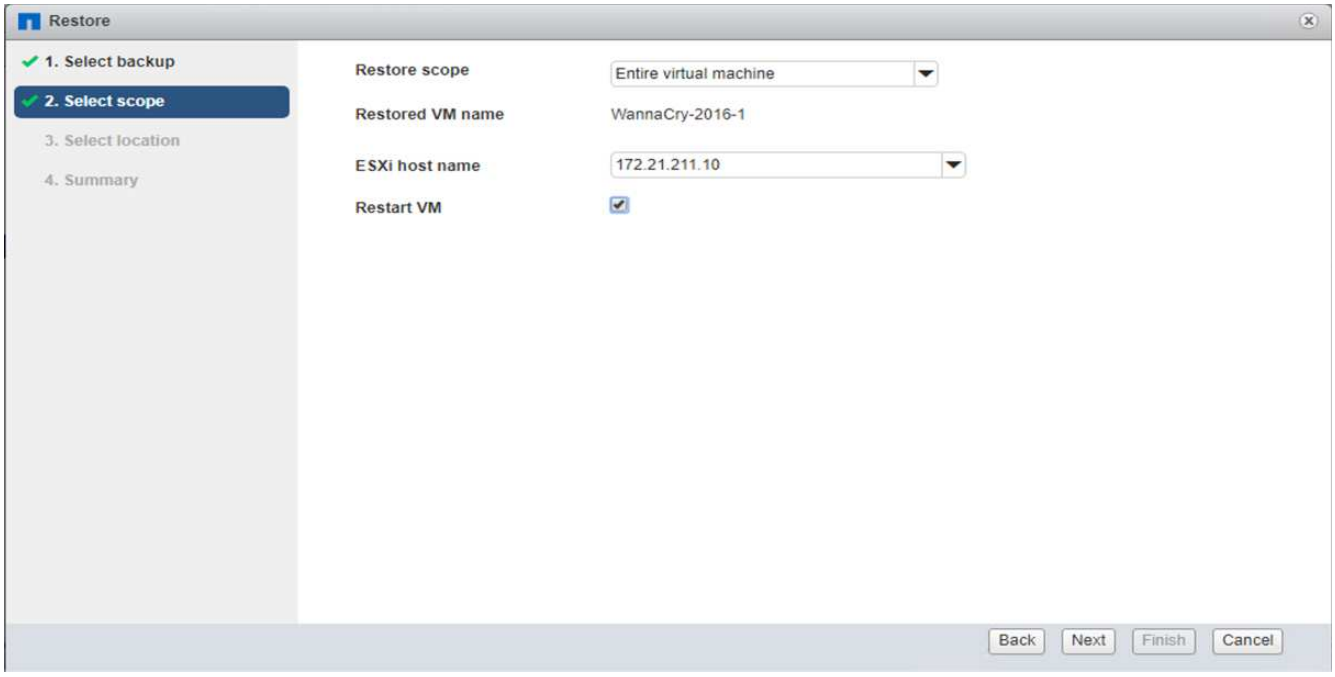
1. Use la copia Snapshot que creó con SnapCenter para restaurar la máquina virtual.



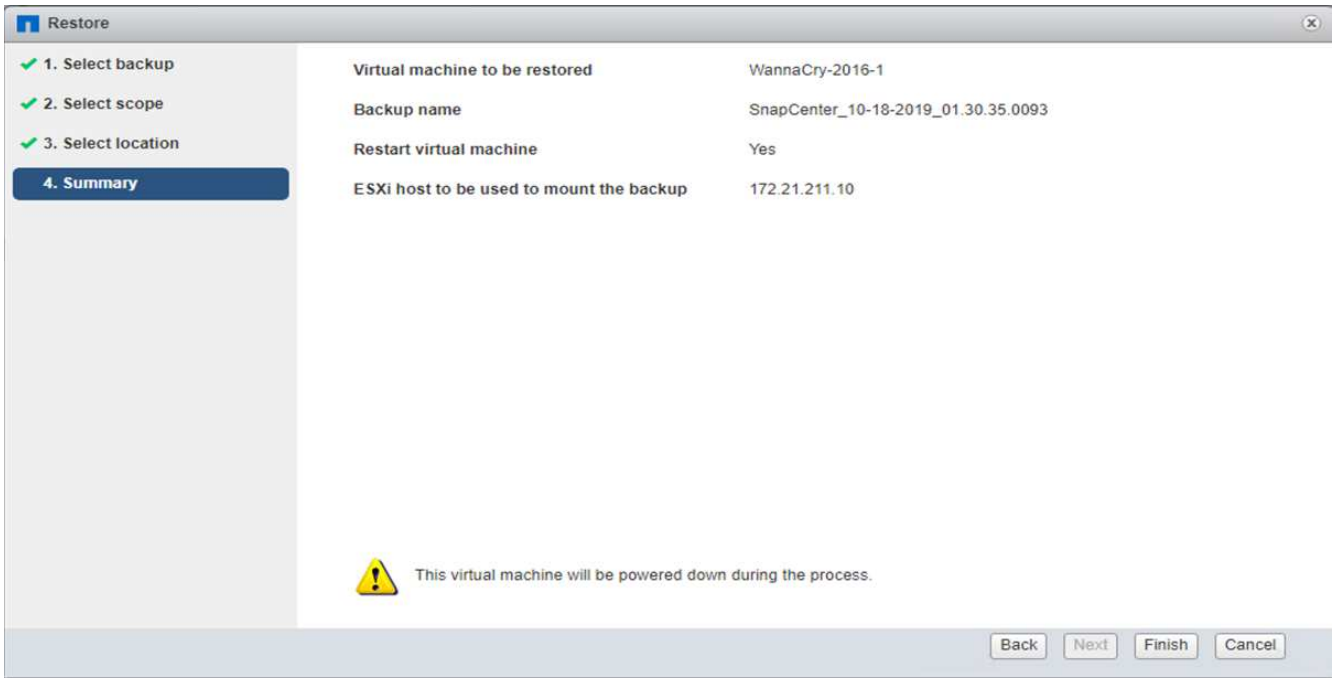
2. Seleccione la copia de Snapshot coherente con VMware que desee restaurar.



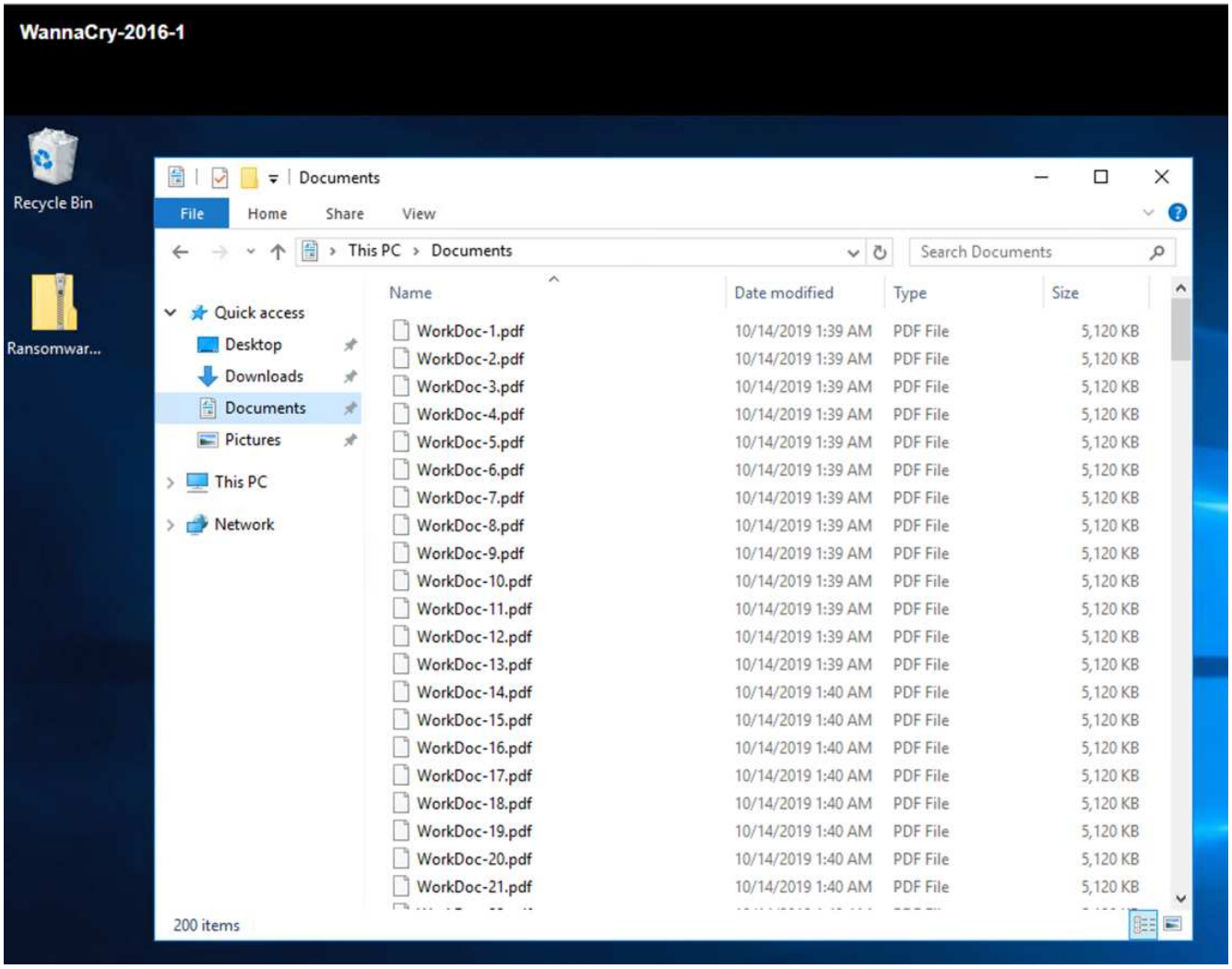
3. Toda la máquina virtual se restaura y se reinicia.



4. Haga clic en Finalizar para iniciar el proceso de restauración.



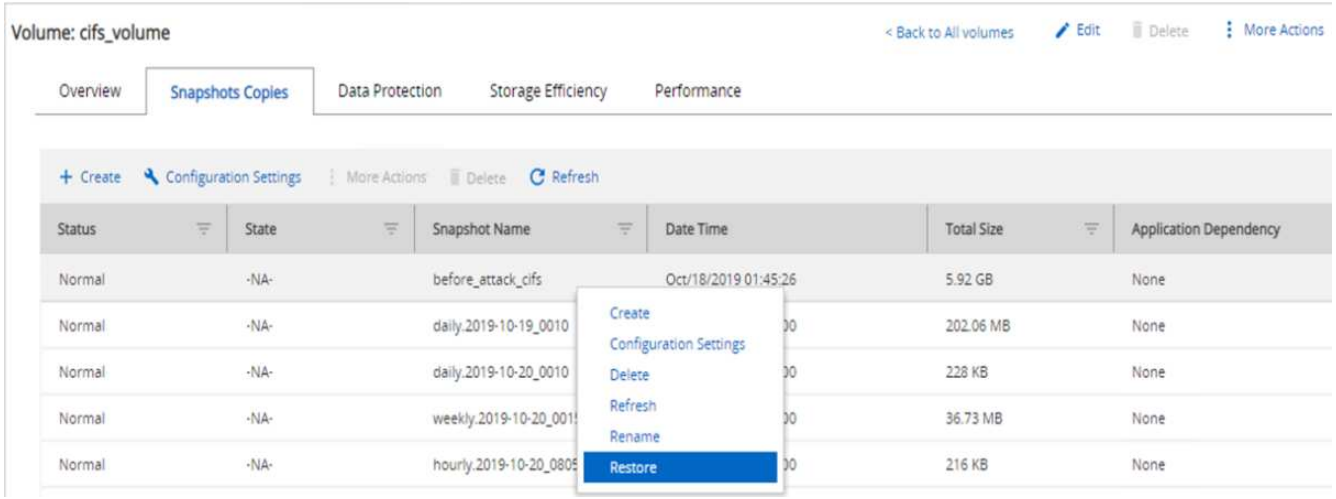
5. Se restauran el equipo virtual y sus archivos.



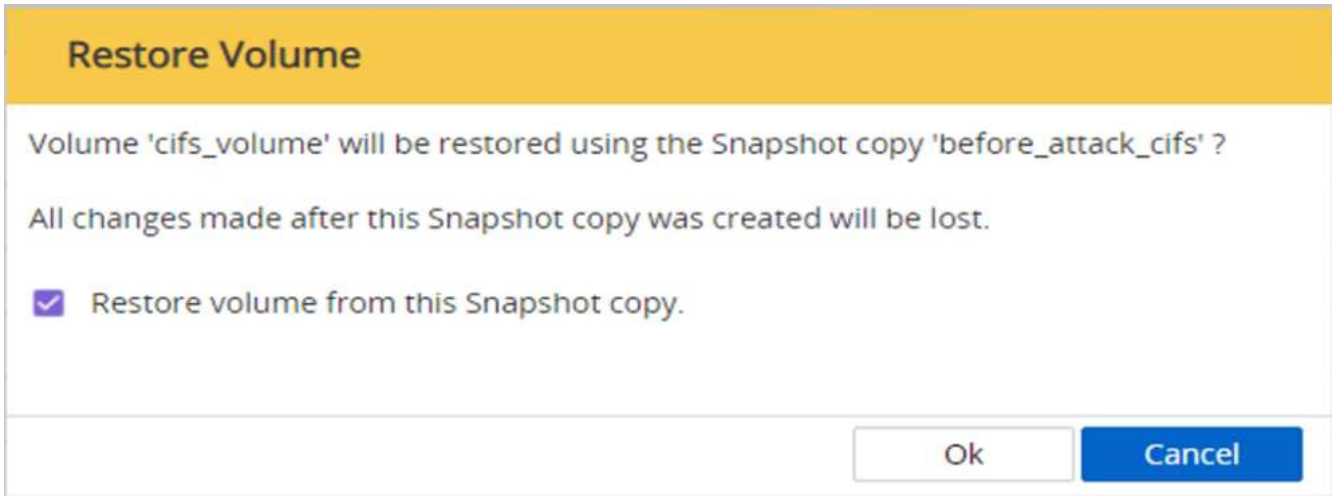
Restaurar recurso compartido CIFS

Para restaurar el recurso compartido CIFS, realice los siguientes pasos:

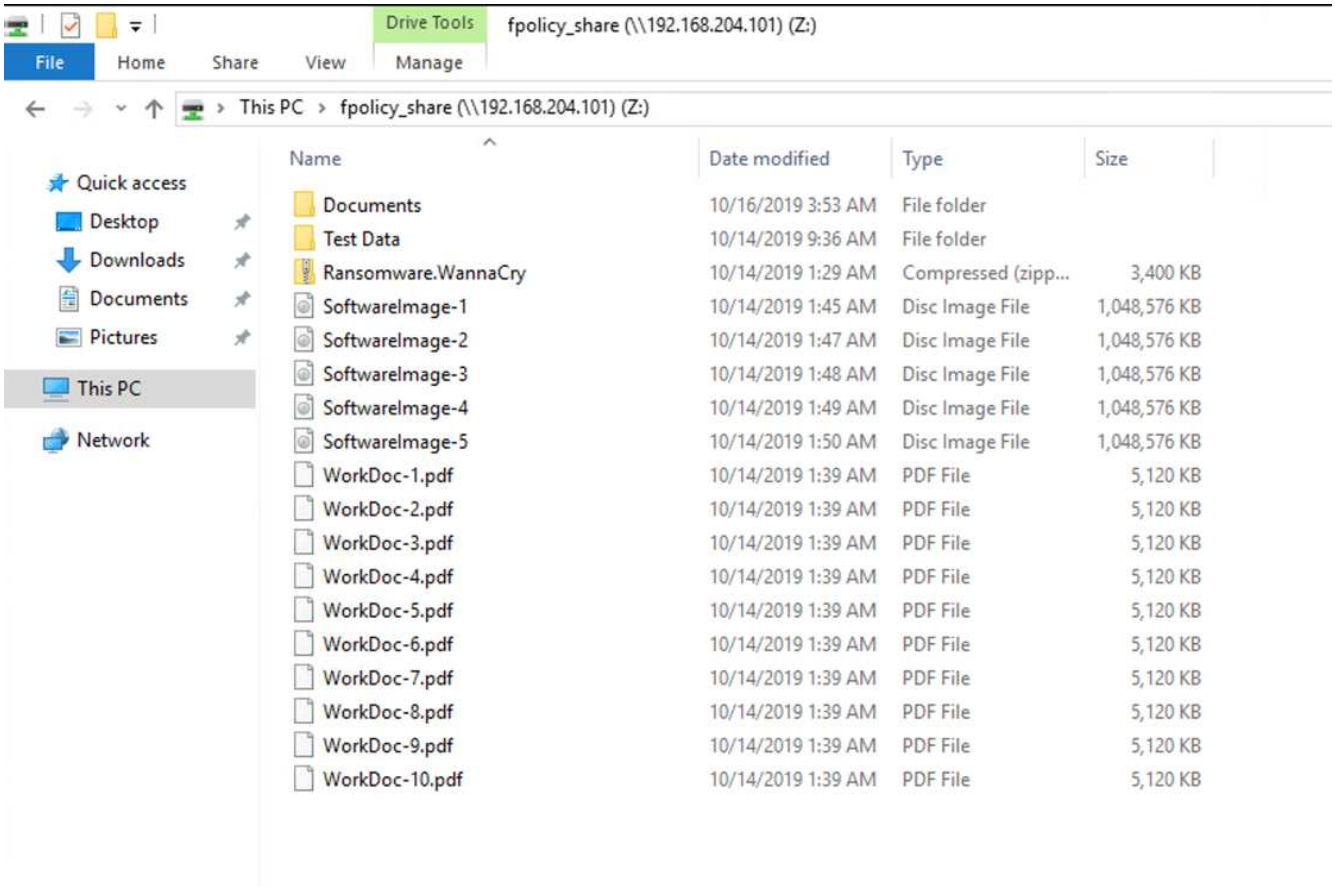
1. Utilice la copia snapshot del volumen que haya tomado antes del ataque para restaurar el recurso compartido.



2. Haga clic en OK para iniciar la operación de restauración.



3. Vea el recurso compartido CIFS después de la restauración.



Caso 2: WannaCry cifra el sistema de archivos dentro del equipo virtual e intenta cifrar el recurso compartido CIFS asignado que está protegido mediante FPolicy

Prevención

Configurar FPolicy

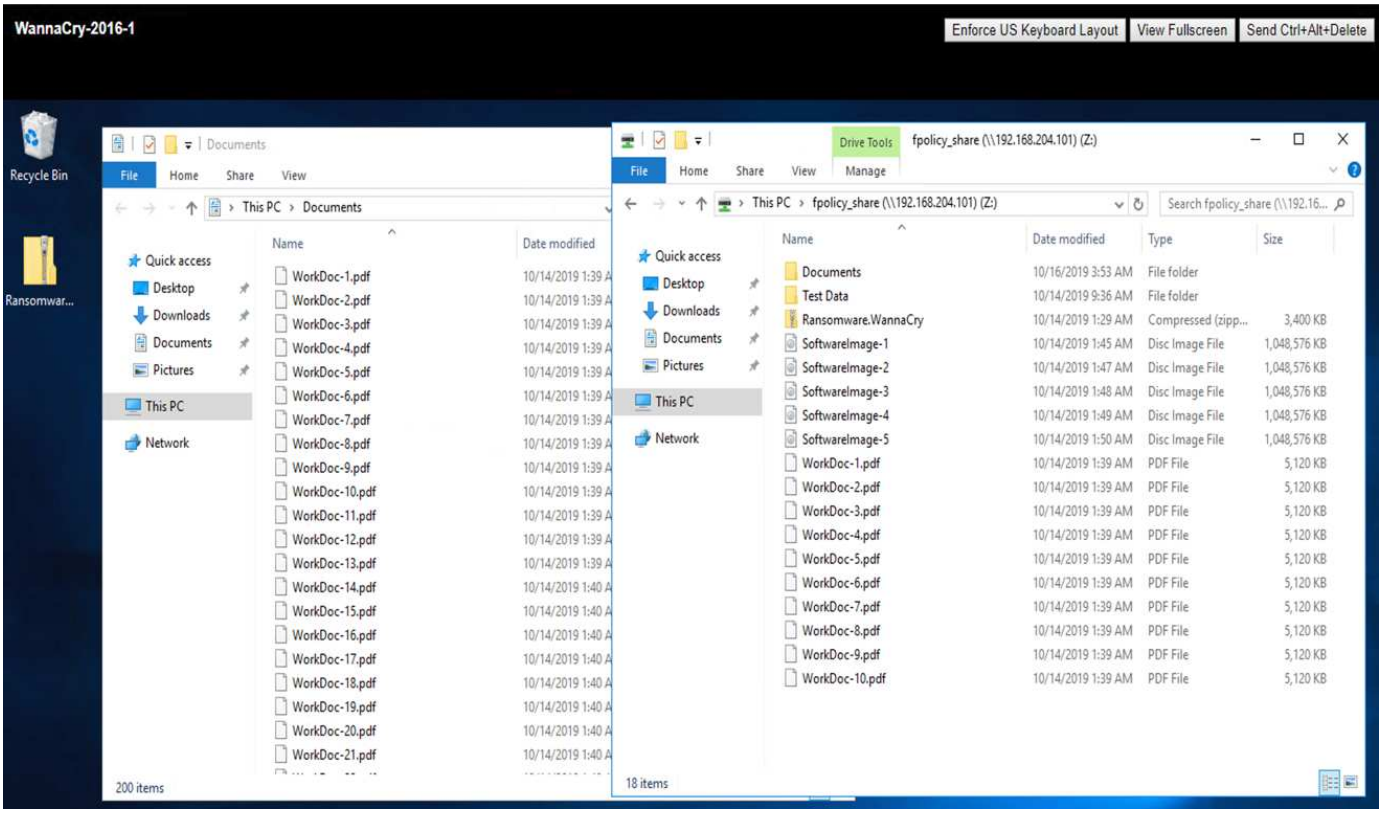
Para configurar FPolicy en el recurso compartido de CIFS, ejecute los siguientes comandos en el clúster de

ONTAP:

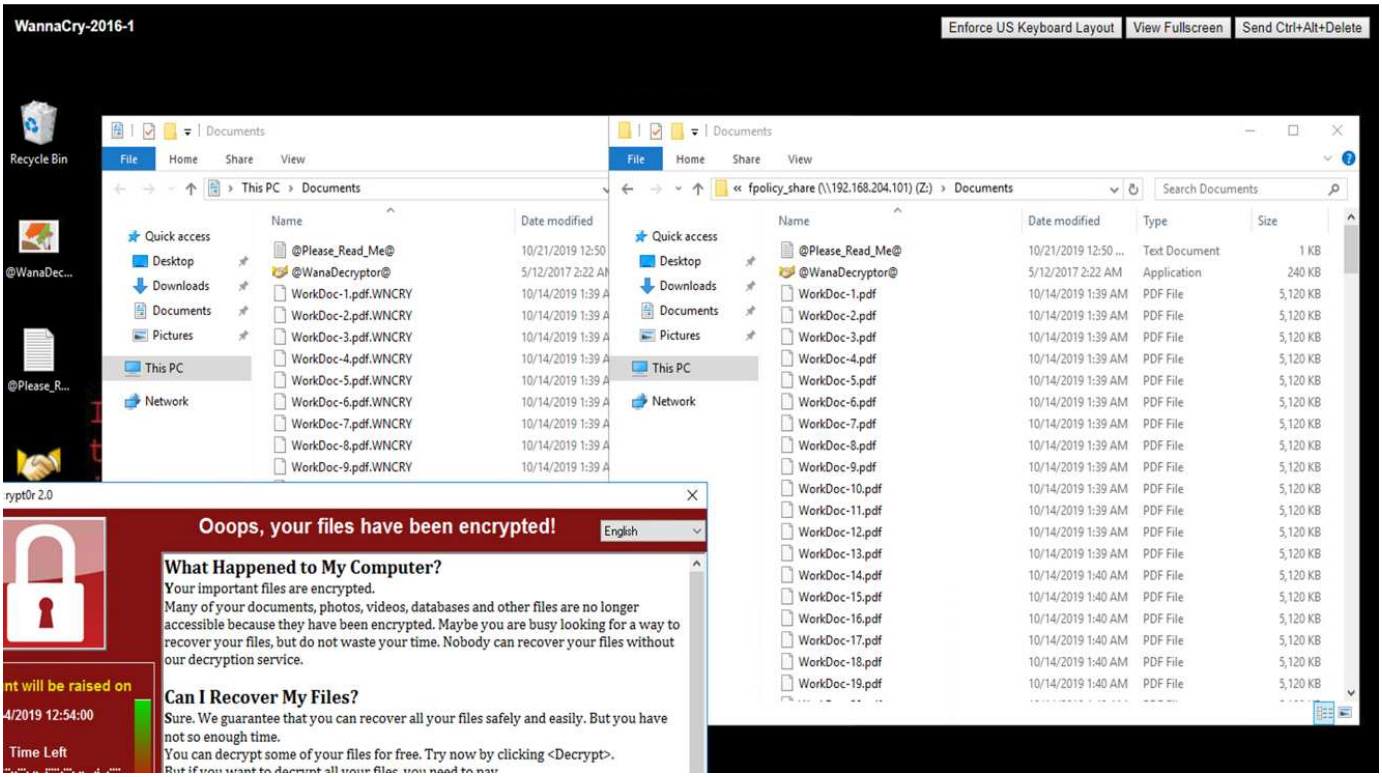
```
vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create -vserver infra_svm -policy-name
Ransomware_policy -shares-to-include fpolicy_share -file-extensions-to
-include WNCRY,Locky,ad4c
vserver fpolicy enable -vserver infra_svm -policy-name Ransomware_policy
-sequence-number 1
```

Con esta directiva, los archivos con extensiones WNCRY, Locky y ad4c no pueden realizar las operaciones de archivo crear, cambiar el nombre, escribir o abrir.

Ver el estado de los archivos antes del ataque: Están sin cifrar y en un sistema limpio.



Los archivos del equipo virtual están cifrados. El malware WannaCry intenta cifrar los archivos en el recurso compartido de CIFS, pero FPolicy evita que afecten a los archivos.



Continuar las operaciones de negocios sin pagar el rescate

Las funcionalidades de NetApp descritas en este documento le ayudan a restaurar los datos en cuestión de minutos después de un ataque y a evitar ataques en primer lugar, de tal modo que pueda continuar con sus operaciones empresariales sin impedimentos.

Es posible establecer una programación de copias Snapshot para cumplir el objetivo de punto de recuperación (RPO) deseado. Las operaciones de restauración basadas en copias de Snapshot son muy rápidas; por lo tanto, se puede lograr un objetivo de tiempo de recuperación (RTO) muy bajo.

Por encima de todo, usted no tiene que pagar cualquier rescate como resultado de un ataque, y usted puede rápidamente volver a las operaciones regulares.

Conclusión

El ransomware es un producto de la delincuencia organizada, y los atacantes no operan con la ética. Pueden abstenerse de proporcionar la clave para el descifrado incluso después de recibir el rescate. La víctima no solo pierde sus datos, sino también una cantidad importante de dinero, y se enfrenta a las consecuencias asociadas con la pérdida de datos de producción.

Según a "Artículo de Forbes", sólo el 19% de las víctimas de ransomware obtienen sus datos después de pagar el rescate. Por lo tanto, los autores recomiendan no pagar un rescate en caso de un ataque porque hacerlo refuerza la fe del atacante en su modelo de negocios.

Las operaciones de backup y restauración de datos juegan un papel importante de la recuperación de ransomware. Por lo tanto, deben incluirse como parte integral de la planificación empresarial. La implementación de estas operaciones se debe presupuestar para que no exista ningún compromiso en las funcionalidades de recuperación en caso de ataque.

La clave está en seleccionar el partner tecnológico correcto en este viaje. FlexPod proporciona la mayoría de las funcionalidades necesarias de forma nativa sin coste adicional en un sistema FAS all-flash.

Reconocimientos

El autor desea agradecer a las siguientes personas su apoyo en la creación de este documento:

- Jorge Gómez Navarrete, NetApp
- Ganesh Kamath, NetApp

Información adicional

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

- Software Snapshot de NetApp

  "https://www.netapp.com/us/products/platform-os/snapshot.aspx"

- Gestión de backups de SnapCenter

  "https://www.netapp.com/us/products/backup-recovery/snapcenter-backup-management.aspx"

- Cumplimiento de normativas para datos de SnapLock

  "https://www.netapp.com/us/products/backup-recovery/snaplock-compliance.aspx"

- Documentación de productos de NetApp

  "https://www.netapp.com/us/documentation/index.aspx"

- Cisco Advanced Malware Protection (AMP)

  "https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html"

- Cisco StealtWatch

  "https://www.cisco.com/c/en_in/products/security/stealthwatch/index.html"

Solución FlexPod para el sector sanitario conforme a la seguridad FIPS 140-2-2

TR-4892: Solución FlexPod para el sector sanitario conforme a la seguridad FIPS 140-2-2

JayaKishore Esanakula, NetApp John McAbel, Cisco

La Ley de Tecnología de la Información sanitaria para la Salud Económica y Clínica (HITECH) requiere el cifrado validado de la Norma Federal de procesamiento de Información (FIPS) 140-2 de la Información médica protegida electrónica (ePHI). Las

aplicaciones y el software de tecnología de la información sanitaria (HIT) deben cumplir los requisitos de FIPS 140-2 para obtener la certificación del Programa de interoperabilidad de promoción (anteriormente, significativo programa de incentivos para uso). Los proveedores y hospitales elegibles deben usar UN GOLPE conforme a FIPS 140-2 (nivel 1) para recibir los incentivos de Medicare y Medicaid y para evitar las sanciones de reembolso del Centro para Medicare y Medicaid (CMS). Los algoritmos de cifrado certificados FIPS 140-2-2, cumplen los requisitos técnicos de protección "Regla de seguridad" De la Ley de Portabilidad y responsabilidad de la Información de Salud (HIPAA).

FIPS 140-2 es un territorio estadounidense estándar gubernamental que establece los requisitos de seguridad de los módulos criptográficos en hardware, software y firmware que protegen la información confidencial. El cumplimiento del estándar es obligatorio para su uso por parte de EE. UU también se utilizan a menudo en sectores regulados como los servicios financieros y la asistencia sanitaria. Este informe técnico ayuda al lector a comprender la norma de seguridad FIPS 140-2 de alto nivel. También ayuda a la audiencia a comprender las diversas amenazas a las que se enfrentan las organizaciones sanitarias. Por último, el informe técnico nos ayuda a comprender cómo puede ayudarle un sistema FlexPod conforme a FIPS 140-2 a proteger los activos sanitarios cuando se implementa en una infraestructura convergente de FlexPod.

Ámbito

Este documento es una descripción general técnica de un sistema Cisco Unified Computing System (Cisco UCS), Cisco Nexus, Cisco MDS y la infraestructura FlexPod basada en ONTAP de NetApp para alojar una o más aplicaciones o soluciones DE TI para el sector sanitario que requieren cumplimiento de normativas de seguridad FIPS 140-2-2.

Destinatarios

Este documento está dirigido a líderes técnicos del sector sanitario y a ingenieros de soluciones de partners de Cisco y NetApp y personal de servicios profesionales. NetApp asume que el lector tiene un buen conocimiento de los conceptos de configuración de la computación y el almacenamiento, así como una familiaridad técnica con las amenazas para la salud, la seguridad sanitaria, los sistemas TECNOLÓGICOS para el sector sanitario, Cisco UCS y los sistemas de almacenamiento de NetApp.

"Siguiente: Amenazas de ciberseguridad en sanidad."

Amenazas de ciberseguridad en sanidad

"Anterior: Introducción."

En cada uno de los problemas se presenta una nueva oportunidad, un ejemplo de esta oportunidad dado por la pandemia del COVID. Según a "informes" Por el Programa de ciberseguridad del Departamento de Salud y Servicios Humanos (HHS), la respuesta del COVID ha dado lugar a un mayor número de ataques de ransomware. Había 6,000 nuevos dominios de Internet registrados apenas en la tercera semana de marzo de 2020. Más del 50% de los dominios hospedados de malware. Los ataques de ransomware fueron responsables de casi el 50 % de todas las infracciones de datos en la atención sanitaria en 2020, lo que afectó a más de 630 organizaciones sanitarias y a aproximadamente 29 millones de registros sanitarios. Diecinueve leakers/sitios duplicaron la extorsión. Con un 24.5%, el sector sanitario registró el mayor número de

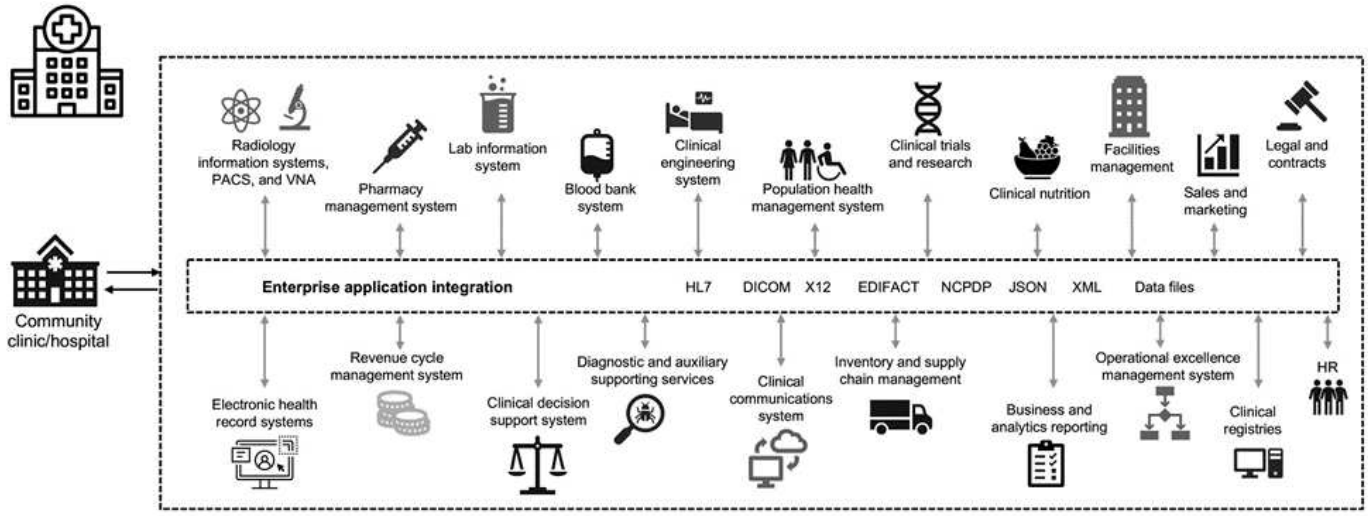
infracciones de datos en 2020.

Agentes malintencionados intentaron violar la seguridad y privacidad de la información médica protegida (PHI) vendiendo la información o amenazando con destruirla o exponerla. Con frecuencia se realizan intentos de difusión en masa y objetivo para obtener acceso no autorizado a ePHI. Aproximadamente el 75% de los registros de pacientes expuestos en el segundo semestre de 2020 se debieron a socios comerciales comprometidos.

La siguiente lista de organizaciones de atención médica fue dirigida por los agentes maliciosos:

- Los sistemas hospitalarios
- Laboratorios de ciencias de la vida
- Laboratorios de investigación
- Instalaciones de rehabilitación
- Hospitales y clínicas comunitarias

La diversidad de aplicaciones que constituyen una organización sanitaria es innegable y cada vez más compleja. Las oficinas de seguridad de la información se enfrentan al reto de proporcionar gobierno a la gran variedad de sistemas Y activos TECNOLÓGICOS. La figura siguiente muestra las capacidades clínicas de un sistema hospitalario típico.



Los datos del paciente se encuentran en el centro de esta imagen. La pérdida de datos de pacientes y el estigma asociado con condiciones médicas sensibles es muy real. Otras cuestiones sensibles incluyen el riesgo de exclusión social, chantaje, perfilado, vulnerabilidad a la comercialización dirigida, explotación y posible responsabilidad financiera hacia los pagadores sobre la información médica más allá de los privilegios del pagador.

Las amenazas a la salud son multidimensionales en la naturaleza y en el impacto. Los gobiernos de todo el mundo han promulgado diversas disposiciones para asegurar la ePHI. Los efectos perjudiciales y la naturaleza en evolución de las amenazas a la atención sanitaria hacen que a las organizaciones sanitarias les resulte difícil defender todas las amenazas.

A continuación se presenta una lista de amenazas comunes identificadas en la atención sanitaria:

- Ataques de ransomware
- Pérdida o robo de equipo o datos con información confidencial

- Ataques de phishing
- Ataques contra dispositivos médicos conectados que pueden afectar la seguridad del paciente
- Ataques de phishing por correo electrónico
- Pérdida o robo de equipo o datos
- Protocolo de puesto de trabajo remoto sacrifica
- Vulnerabilidad del software

Las organizaciones sanitarias trabajan en un entorno legal y regulatorio que es tan complicado como sus ecosistemas digitales. Este entorno incluye, entre otros, lo siguiente:

- Oficina del Coordinador Nacional (para Tecnología sanitaria) normas de interoperabilidad de Tecnología Electrónica de la Información de Salud con certificación ONC
- Acceso a Medicare y Ley de reautorización del Programa de Seguro médico para niños (MACRA)/uso significativo
- Múltiples obligaciones bajo la Administración de Alimentos y medicamentos (FDA)
- Los procesos de acreditación de la Comisión conjunta
- Requisitos de HIPAA
- Requisitos DE HITECH
- Normas de riesgo mínimas aceptables para los pagadores
- Normas de privacidad y seguridad del Estado
- Requisitos de la Ley Federal de modernización de la Seguridad de la Información tal como están incorporados a contratos federales y subvenciones de investigación a través de agencias como los Institutos nacionales de la Salud
- Estándar de seguridad de datos del sector de tarjetas de pago (PCI-DSS)
- Requisitos de la Administración de Servicios de abuso de sustancias y Salud Mental (SAMHSA)
- La ley Gramm-Leach-Bliley relativa al procesamiento financiero
- La Ley Stark en su relación con la prestación de servicios a organizaciones afiliadas
- Ley de Derechos educativos y Privacidad de la Familia (FERPA) para instituciones que participan en la educación superior
- Información genética Ley de no discriminación (GINA)
- El nuevo Reglamento general de protección de datos (GDPR) en la Unión Europea

Los estándares de la arquitectura de seguridad están evolucionando rápidamente para impedir que los actores malintencionados afecten a los sistemas de información sanitaria. Uno de estos estándares es FIPS 140-2, definido por el Instituto Nacional de estándares y Tecnología (NIST). La publicación FIPS 140-2 detalla el territorio de EE. UU requisitos gubernamentales de un módulo criptográfico. Los requisitos de seguridad cubren las áreas relacionadas con un diseño seguro y la implementación de un módulo criptográfico y se pueden aplicar para GOLPEAR. Los límites criptográficos bien definidos permiten una gestión de la seguridad más sencilla al tiempo que se mantienen al día con los módulos criptográficos. Estos límites ayudan a prevenir módulos criptográfico débiles que pueden ser explotados fácilmente por actores malintencionados. También pueden ayudar a prevenir errores humanos al gestionar módulos criptográficos estándar.

NIST junto con el establecimiento de seguridad de comunicaciones (CSE) han establecido el programa de validación de módulos criptográficos (CMVP) para certificar módulos criptográficos para niveles de validación FIPS 140-2-2. Mediante el uso de un módulo certificado FIPS 140-2-2, las organizaciones federales deben

proteger tanto los datos confidenciales como los valiosos mientras están en movimiento. Debido a su éxito en la protección de información sensible o valiosa, muchos sistemas de atención médica han decidido cifrar la ePHI mediante el uso de módulos criptográficos FIPS 140-2 más allá del nivel mínimo de seguridad legalmente requerido.

El aprovechamiento e implementación de las funcionalidades de FIPS 140-2 de FlexPod solo lleva horas (no días). Cumplir con FIPS está al alcance de la mayoría de las organizaciones sanitarias, independientemente del tamaño. Con límites criptográficos claramente definidos y pasos de implementación sencillos y bien documentados, una arquitectura de FlexPod conforme a FIPS 140-2 puede establecer una base de seguridad sólida para la infraestructura y permitir mejoras sencillas que incrementen aún más la protección frente a amenazas de seguridad.

"Siguiente: Descripción general de FIPS 140-2."

Información general de FIPS 140-2

"Anterior: Amenazas de ciberseguridad en sanidad."

"FIPS 140-2" especifica los requisitos de seguridad de un módulo criptográfico utilizado en un sistema de seguridad que protege la información confidencial en los sistemas informáticos y de telecomunicaciones. Un módulo criptográfico debe ser un conjunto de hardware, software, firmware o una combinación. FIPS se aplica a los algoritmos criptográficos, la generación de claves y los gestores de claves contenidos en un ámbito criptográfico. Es importante entender que FIPS 140-2 se aplica específicamente al módulo criptográfico, no al producto, la arquitectura, los datos o el ecosistema. El módulo criptográfico, que se define en los términos clave más adelante en este documento, es el componente específico (ya sea hardware, software o firmware) que implementa funciones de seguridad aprobadas. Además, FIPS 140-2 especifica cuatro niveles. Los algoritmos criptográficos aprobados son comunes a todos los niveles. Algunos de los elementos clave y requisitos de cada nivel de seguridad son:

- **Nivel de seguridad 1**
  - Especifica los requisitos básicos de seguridad de un módulo criptográfico (se requiere al menos un algoritmo aprobado o una función de seguridad).
  - No se requieren mecanismos de seguridad física especificados para el nivel 1 más allá de los requisitos básicos para los componentes de nivel de producción.
- **Nivel de seguridad 2**
  - Mejora los mecanismos de seguridad física al añadir el requisito de prueba de manipulación mediante el uso de soluciones a prueba de manipulación como revestimientos o sellos, bloqueos de cubiertas extraíbles o puertas de los módulos criptográficos.
  - Requiere, como mínimo, el control de acceso basado en funciones (RBAC) en el que el módulo criptográfico autentica la autorización de un operador o administrador para asumir una función específica y realizar un conjunto de funciones correspondiente.
- **Nivel de seguridad 3**
  - Se basa en los requisitos de seguridad a prueba de manipulaciones del nivel 2 e intenta evitar un mayor acceso a los parámetros de seguridad críticos (CSP) del módulo criptográfico.
  - Los mecanismos de seguridad física necesarios en el nivel 3 tienen la intención de tener una alta probabilidad de detectar y responder a los intentos de acceso físico, o cualquier uso o modificación del

módulo criptográfico. Los ejemplos pueden incluir carcasas fuertes, detección de manipulación y circuitos de respuesta que se ceros a todos los CSPs de texto sin formato cuando se abre una cubierta extraíble en el módulo criptográfico.

  - Requiere mecanismos de autenticación basados en identidades para mejorar la seguridad de los mecanismos RBAC especificados en el nivel 2. Un módulo criptográfico autentica la identidad de un operador y verifica que el operador está autorizado a utilizar una función y realizar las funciones de la función.

- **Nivel de seguridad 4**
  - El nivel más alto de seguridad en FIPS 140-2.
  - El nivel más útil para operaciones en entornos físicamente sin protección.
  - En este nivel, los mecanismos de seguridad física tienen por objeto proporcionar una protección completa alrededor del módulo criptográfico, con la responsabilidad de detectar y responder a cualquier intento no autorizado de acceso físico.
  - La penetración o exposición del módulo criptográfico debe tener una alta probabilidad de detección y dar como resultado la zeroización inmediata de todos los CSPs no seguros o de texto sin formato.

"Siguiente: Plano de control frente al plano de datos."

Plano de control frente al plano de datos

"Anterior: Descripción general de FIPS 140-2."

Al implementar una estrategia FIPS 140-2-2, es importante comprender qué se está protegiendo. Esto se puede dividir fácilmente en dos áreas: Plano de control y plano de datos. Un plano de control se refiere a los aspectos que afectan al control y al funcionamiento de los componentes del sistema FlexPod; por ejemplo, acceso administrativo a las controladoras de almacenamiento de NetApp, los switches Cisco Nexus y los servidores Cisco UCS. La protección en esta capa se proporciona limitando los protocolos y los cyphers criptográficos que los administradores pueden utilizar para conectar a dispositivos y realizar cambios. Un plano de datos hace referencia a la información real, como la PHI, dentro del sistema FlexPod. Esto se protege mediante el cifrado de datos en reposo y de nuevo en FIPS, lo que garantiza que los módulos criptográficos en uso cumplen los estándares.

"Siguiente: Computación Cisco UCS de FlexPod y FIPS 140-2."

Computación Cisco UCS de FlexPod y FIPS 140-2

"Anterior: Plano de control frente al plano de datos."

La arquitectura de FlexPod se puede diseñar con un servidor Cisco UCS compatible con FIPS 140-2-2. De acuerdo con la U. S. El servidor Cisco UCS puede funcionar en modo de cumplimiento de normativas FIPS 140-2 nivel 1. Si desea obtener una lista completa de los componentes de Cisco conformes con FIPS, consulte "Página FIPS 140 de Cisco". Cisco UCS Manager está validado según FIPS 140-2.

Cisco UCS y Fabric Interconnect

Cisco UCS Manager se pone en marcha y se ejecuta desde las interconexiones de estructura de Cisco (FIS).

Para obtener más información sobre Cisco UCS y cómo habilitar FIPS, consulte "Documentación de Cisco UCS Manager".

Para habilitar el modo FIPS en la interconexión de estructura Cisco en cada estructura A y B, ejecute los siguientes comandos:

```
fp-health-fabric-A# connect local-mgmt
fp-health-fabric-A(local-mgmt)# enable fips-mode
FIPS mode is enabled
```

> Para sustituir UNA FI de un clúster en Cisco UCS Manager versión 3.2(3) por UNA FI en una versión anterior a Cisco UCS Manager versión 3.2(3), deshabilite el modo FIPS (disable `fips-mode`) En LA RED EXISTENTE antes de agregar LA RED FI de repuesto al clúster. Después de formar el clúster, como parte del arranque de Cisco UCS Manager, se habilita el modo FIPS automáticamente.

Cisco ofrece los siguientes productos clave que se pueden implementar en la capa informática o de aplicación:

- **Cisco Advanced Malware Protection (AMP) para endpoints.** compatible con los sistemas operativos Microsoft Windows y Linux, esta solución integra capacidades de prevención, detección y respuesta. Este software de seguridad evita infracciones, bloquea el malware en el punto de entrada y supervisa y analiza continuamente la actividad de los archivos y procesos para detectar, contener y resolver rápidamente amenazas que puedan evadir las defensas de primera línea. El componente de Protección de actividad maliciosa (MAP) de AMP supervisa continuamente todas las actividades de los extremos y proporciona detección en tiempo de ejecución y bloqueo del comportamiento anormal de un programa en ejecución en el punto final. Por ejemplo, cuando el comportamiento del punto final indica ransomware, los procesos ofensor se terminan, lo que impide el cifrado del punto final y detiene el ataque.
- **AMP para seguridad de correo electrónico.** los correos electrónicos se han convertido en el vehículo principal para difundir malware y llevar a cabo ciberataques. En promedio, aproximadamente 100 mil millones de correos electrónicos se intercambian en un solo día, lo que proporciona a los atacantes un excelente vector de penetración en los sistemas de los usuarios. Por lo tanto, es absolutamente esencial defender contra esta línea de ataque. AMP analiza correos electrónicos para amenazas tales como exploits de día cero y malware sigiloso ocultos en archivos adjuntos maliciosos. También utiliza la inteligencia de URL líder en el sector para combatir enlaces maliciosos. Proporciona a los usuarios protección avanzada contra el phishing espear, el ransomware y otros ataques sofisticados.
- **Sistema de prevención de intrusiones de próxima generación (NGIPS).** Cisco Firepower NGIPS se puede implementar como un dispositivo físico en el centro de datos o como un dispositivo virtual en VMware (NGIPSv para VMware). Este sistema altamente eficaz de prevención de intrusiones proporciona un rendimiento fiable y un costo total de propiedad bajo. La protección contra amenazas se puede ampliar con licencias de suscripción opcionales para proporcionar funciones de AMP, visibilidad y control de aplicaciones y filtrado de URL. La virtualización de NGIPS inspecciona el tráfico entre equipos virtuales (VM) y facilita la implementación y gestión de soluciones de NGIPS en sitios con recursos limitados, lo que aumenta la protección tanto para activos físicos como virtuales.

"Siguiente: Redes Cisco de FlexPod y FIPS 140-2."

Redes Cisco de FlexPod y FIPS 140-2

"Anterior: Computación Cisco UCS de FlexPod y FIPS 140-2."

MDS de Cisco

Plataforma Cisco MDS 9000 con software 8.4.x. "Conforme a FIPS 140-2-2". Cisco MDS implementa módulos criptográficos y los siguientes servicios para SNMPv3 y SSH.

- Establecimiento de sesiones en apoyo de cada servicio
- Todos los algoritmos criptográficos subyacentes admiten las funciones de derivación de cada clave de servicios
- Hash para cada servicio
- Cifrado simétrico para cada servicio

Antes de activar el modo FIPS, complete las siguientes tareas en el conmutador MDS:

1. Convierta las contraseñas en un mínimo de ocho caracteres.
2. Desactivar Telnet. Los usuarios deben iniciar sesión solo con SSH.
3. Desactive la autenticación remota mediante RADIUS/TACACS+. Sólo se pueden autenticar los usuarios locales del conmutador.
4. Deshabilite SNMP v1 y v2. Cualquier cuenta de usuario existente en el conmutador que se haya configurado para SNMPv3 debe configurarse sólo con SHA para autenticación y AES/3DES para privacidad.
5. Desactive VRRP.
6. Elimine todas las directivas IKE que tengan MD5 para autenticación o DES para cifrado. Modifique las directivas para que utilicen SHA para la autenticación y 3DES/AES para el cifrado.
7. Elimine todos los teclados RSA1 del servidor SSH.

Para activar el modo FIPS y mostrar el estado FIPS en el conmutador MDS, lleve a cabo los pasos siguientes:

1. Muestra el estado de FIPS.

```
MDSSwitch# show fips status
FIPS mode is disabled
MDSSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. Configure la clave SSH de 2048 bits.

```
MDSSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
MDSSwitch(config)# no ssh key
MDSSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
MDSSwitch(config)# ssh key
dsa   rsa
MDSSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. Habilite el modo FIPS.

```
MDSSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
```

4. Muestra el estado de FIPS.

```
MDSSwitch(config)# show fips status
FIPS mode is enabled
MDSSwitch(config)# feature ssh
MDSSwitch(config)# show feature | grep ssh
sshServer            1        enabled
```

5. Guarde la configuración en la configuración en ejecución.

```
MDSSwitch(config)# copy ru st
[##################################################] 100%
exitCopy complete.
MDSSwitch(config)# exit
```

6. Reinicie el conmutador MDS

```
MDSSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

7. Muestra el estado de FIPS.

```
Switch(config)# fips mode enable
Switch(config)# show fips status
```

Para obtener más información, consulte "Habilitar el modo FIPS".

Cisco Nexus

Los switches de la serie Cisco Nexus 9000 (versión 9.3) son "Conforme a FIPS 140-2-2". Cisco Nexus implementa módulos criptográficos y los siguientes servicios para SNMPv3 y SSH.

- Establecimiento de sesiones en apoyo de cada servicio
- Todos los algoritmos criptográficos subyacentes admiten las funciones de derivación de cada clave de servicios
- Hash para cada servicio
- Cifrado simétrico para cada servicio

Antes de habilitar el modo FIPS, complete las siguientes tareas en el switch Cisco Nexus:

1. Desactivar Telnet. Los usuarios deben iniciar sesión solo con Secure Shell (SSH).
2. Desactive SNMPv1 y v2. Cualquier cuenta de usuario existente en el dispositivo que se haya configurado para SNMPv3 debe configurarse sólo con SHA para autenticación y AES/3DES para privacidad.
3. Elimine todos los pares de claves RSA1 del servidor SSH.
4. Habilite la comprobación de integridad de mensajes (MIC) HMAC-SHA1 para que se utilice durante la negociación del protocolo de asociación de seguridad (SAP) de Cisco TrustSec. Para ello, introduzca el algoritmo hash de SAP `HMAC-SHA-1` desde el `cts-manual` o. `cts-dot1x` modo.

Para activar el modo FIPS en el switch Nexus, realice los pasos siguientes:

1. Configure una clave SSH de 2048 bits.

```
NexusSwitch# show fips status
FIPS mode is disabled
NexusSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. Configure la clave SSH de 2048 bits.

```
NexusSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
NexusSwitch(config)# no ssh key
NexusSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
NexusSwitch(config)# ssh key
dsa   rsa
NexusSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. Habilite el modo FIPS.

```
NexusSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
Show fips status
NexusSwitch(config)# show fips status
FIPS mode is enabled
NexusSwitch(config)# feature ssh
NexusSwitch(config)# show feature | grep ssh
sshServer            1        enabled
Save configuration to the running configuration
NexusSwitch(config)# copy ru st
[########################################] 100%
exitCopy complete.
NexusSwitch(config)# exit
```

4. Reinicie el switch Nexus.

```
NexusSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

5. Muestra el estado de FIPS.

```
NexusSwitch(config)# fips mode enable
NexusSwitch(config)# show fips status
```

Además, el software Cisco NX OS admite la función NetFlow que permite una detección mejorada de anomalías y seguridad de la red. NetFlow captura los metadatos de cada conversación de la red, las partes implicadas en la comunicación, el protocolo utilizado y la duración de la transacción. Una vez agregada y analizado la información, puede proporcionar una visión del comportamiento normal. Los datos recopilados también permiten la identificación de patrones de actividad cuestionables, como el malware que se propaga a través de la red, lo que de otra manera puede pasar desapercibida. NetFlow utiliza flujos para proporcionar estadísticas para la supervisión de la red. Un flujo es un flujo unidireccional de paquetes que llega a una interfaz de origen (o VLAN) y tiene los mismos valores para las claves. Una clave es un valor identificado para un campo dentro del paquete. Puede crear un flujo utilizando un registro de flujo para definir las claves únicas para su flujo. Puede exportar los datos que NetFlow recopila para sus flujos utilizando un exportador de flujo a un colector NetFlow remoto, como Cisco StealtWatch. StealtWatch utiliza esta información para la supervisión continua de la red y proporciona información forense de respuesta a incidentes y detección de amenazas en tiempo real si se produce un brote de ransomware.

"Siguiente: Almacenamiento ONTAP de FlexPod y FIPS 140-2."

Almacenamiento ONTAP de FlexPod y FIPS 140-2

"Anterior: Redes Cisco de FlexPod y FIPS 140-2."

NetApp ofrece una amplia gama de hardware, software y servicios que pueden incluir varios componentes de los módulos criptográficos validados bajo el estándar. Por lo tanto, NetApp utiliza diferentes enfoques para el cumplimiento de normativas FIPS 140-2 para el plano de control y el plano de datos:

- NetApp incluye módulos criptográficos que han logrado una validación de nivel 1 para cifrado de datos en tránsito y de datos en reposo.
- NetApp adquiere módulos de hardware y software que han sido validados por FIPS 140-2-2 por los proveedores de dichos componentes. Por ejemplo, la solución de cifrado del almacenamiento de NetApp aprovecha las unidades validadas con el nivel 2 de FIPS.
- Los productos de NetApp pueden utilizar un módulo validado de manera que se cumpla con la norma aunque el producto o la función no estén dentro del límite de la validación. Por ejemplo, el cifrado de volúmenes de NetApp (NVE) cumple con FIPS 140-2-2. Aunque no se valida por separado, aprovecha el módulo criptográfico de NetApp, que se valida en el nivel 1. Para comprender cuáles son las características específicas del cumplimiento de su versión de ONTAP, póngase en contacto con su SME de FlexPod.

Los módulos criptográficos de NetApp están validados con FIPS 140-2 nivel 1

- El módulo de seguridad criptográfica de NetApp (NCSM) tiene la validación FIPS 140-2 nivel 1.

Las unidades de autocifrado de NetApp cuentan con la validación FIPS 140-2 nivel 2

NetApp adquiere unidades de autocifrado (SED) 140-2 que han sido validadas por el fabricante del equipo original (OEM); los clientes que buscan estas unidades deben especificarlas al realizar el pedido. Las unidades se validan en el nivel 2. Los siguientes productos de NetApp pueden aprovechar SED validados:

- Sistemas de almacenamiento A-Series y FAS de AFF
- Sistemas de almacenamiento E-Series y EF-Series

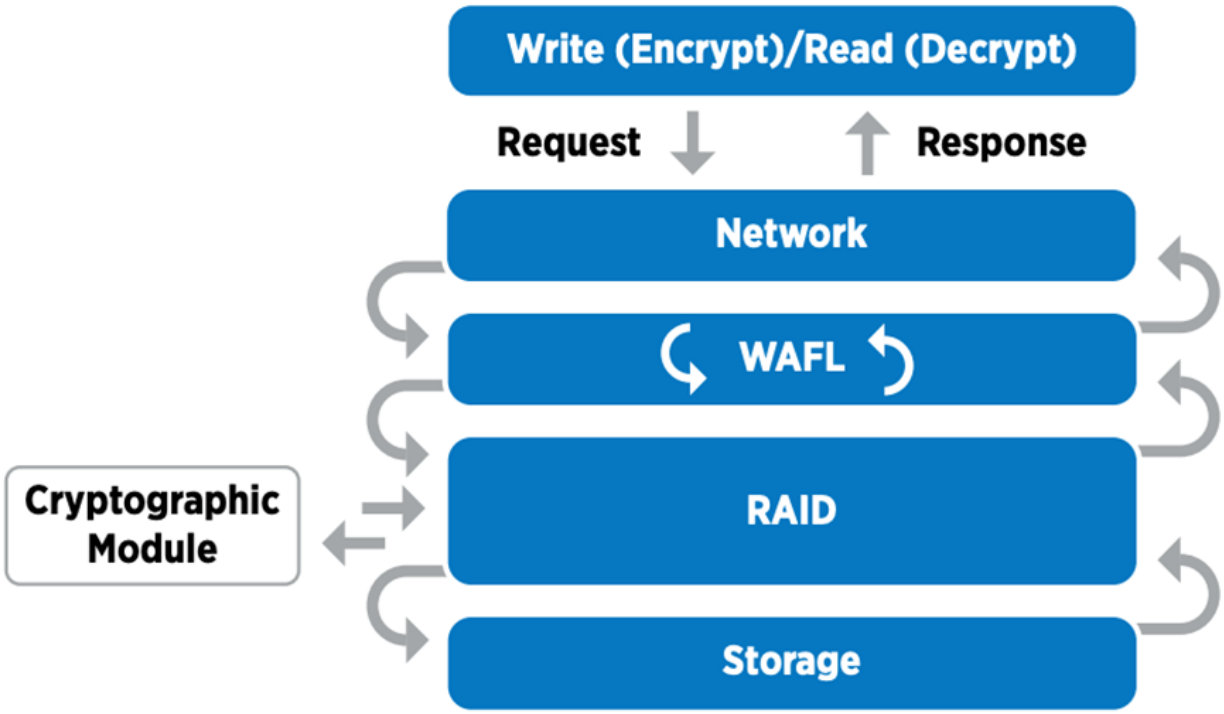
Cifrado de agregados de NetApp y cifrado de volúmenes de NetApp

Las tecnologías NVE y NetApp Aggregate Encryption (NAE) permiten el cifrado de datos a nivel de volumen y agregado respectivamente, lo que convierte la solución en independiente de la unidad física.

NVE es una solución de cifrado de datos en reposo basada en software disponible a partir de ONTAP 9.1. Desde ONTAP 9.2 es compatible con FIPS 140-2-2. NVE permite a ONTAP cifrar los datos por cada volumen para obtener granularidad. NAE, disponible con ONTAP 9.6, es una consecuencia del crecimiento de NVE; permite a ONTAP cifrar datos en cada volumen y los volúmenes pueden compartir claves en el agregado. Tanto NVE como NAE utilizan el cifrado AES de 256 bits. Los datos también se pueden almacenar en disco sin SED. NVE y NAE le permiten utilizar las funciones de eficiencia del almacenamiento incluso cuando el cifrado está habilitado. Un cifrado de solo capa de aplicaciones vence a todas las ventajas de la eficiencia del almacenamiento. Con NVE y NAE se mantienen las eficiencias del almacenamiento porque los datos entran desde la red a través de WAFL de NetApp hasta la capa RAID, que determina si los datos deben ser cifrados. Con el fin de mejorar la eficiencia del almacenamiento, puede utilizar la deduplicación de agregados con NAE. Los volúmenes NVE y NAE pueden coexistir en el mismo agregado NAE. Los agregados NAE no admiten volúmenes no cifrados.

Aquí está cómo funciona el proceso: Cuando se cifran los datos, se envían al módulo criptográfico que está

validado FIPS 140-2 nivel 1. El módulo criptográfico cifra los datos y los envía de nuevo a la capa RAID. A continuación, los datos cifrados se envían al disco. Por lo tanto, con la combinación de NVE y NAE, los datos ya se cifran en el camino al disco. Las lecturas siguen la ruta inversa. En otras palabras, los datos salen del disco cifrado, se envían a RAID, se descifran por el módulo criptográfico y, a continuación, se envían por el resto de la pila, como se muestra en la siguiente figura.



NVE utiliza un módulo criptográfico de software validado por FIPS 140-2 nivel 1.

Para obtener más información sobre NVE, consulte la "Especificaciones técnicas de NVE".

NVE protege los datos en el cloud. Cloud Volumes ONTAP y Azure NetApp Files pueden proporcionar cifrado de datos en reposo conforme a la normativa FIPS 140-2-2.

A partir de ONTAP 9.7, los agregados y los volúmenes recién creados se cifran de forma predeterminada cuando tiene la licencia de NVE y la gestión de claves incorporada o externa. A partir de ONTAP 9.6, se puede utilizar el cifrado a nivel de agregado para asignar claves al agregado que contiene para los volúmenes que se van a cifrar. Los volúmenes que se crean en el agregado están cifrados de manera predeterminada. Puede anular el valor predeterminado al cifrar el volumen.

Comandos de la CLI de NAE de ONTAP

Antes de ejecutar los siguientes comandos de la CLI, asegúrese de que el clúster tenga la licencia de NVE requerida.

Para crear un agregado y cifrarlo, ejecute el siguiente comando (cuando se ejecuta en ONTAP 9.6 y una CLI de clúster posterior):

```
fp-health::> storage aggregate create -aggregate aggregatename -encrypt
-with-aggr-key true
```

Para convertir un agregado que no sea NAE en un agregado de NAE, ejecute el siguiente comando (cuando se ejecute en ONTAP 9.6 y versiones posteriores de CLI de clústeres):

```
fp-health::> storage aggregate modify -aggregate aggregatename  -node
svmname -encrypt-with-aggr-key true
```

Para convertir un agregado de NAE en un agregado que no sea NAE, ejecute el siguiente comando (cuando se ejecute en ONTAP 9.6 y versiones posteriores de CLI de clústeres):

```
fp-health::> storage aggregate modify -aggregate aggregatename -node
svmname -encrypt-with-aggr-key false
```

Comandos de la CLI de NVE de ONTAP

A partir de ONTAP 9.6, se puede utilizar el cifrado a nivel de agregado para asignar claves al agregado que contiene para los volúmenes que se van a cifrar. Los volúmenes que se crean en el agregado están cifrados de manera predeterminada.

Para crear un volumen en un agregado que NAE esté habilitado, ejecute el siguiente comando (cuando se ejecute en ONTAP 9.6 y versiones posteriores de CLI de clústeres):

```
fp-health::> volume create -vserver svmname -volume volumename -aggregate
aggregatename -encrypt true
```

Para habilitar el cifrado de un volumen existente “en posición” sin mover un volumen, ejecute el siguiente comando (cuando se ejecute en ONTAP 9.6 y versiones posteriores de CLI de clústeres):

```
fp-health::> volume encryption conversion start -vserver svmname -volume
volumename
```

Para verificar que los volúmenes estén habilitados para el cifrado, ejecute el siguiente comando de la CLI:

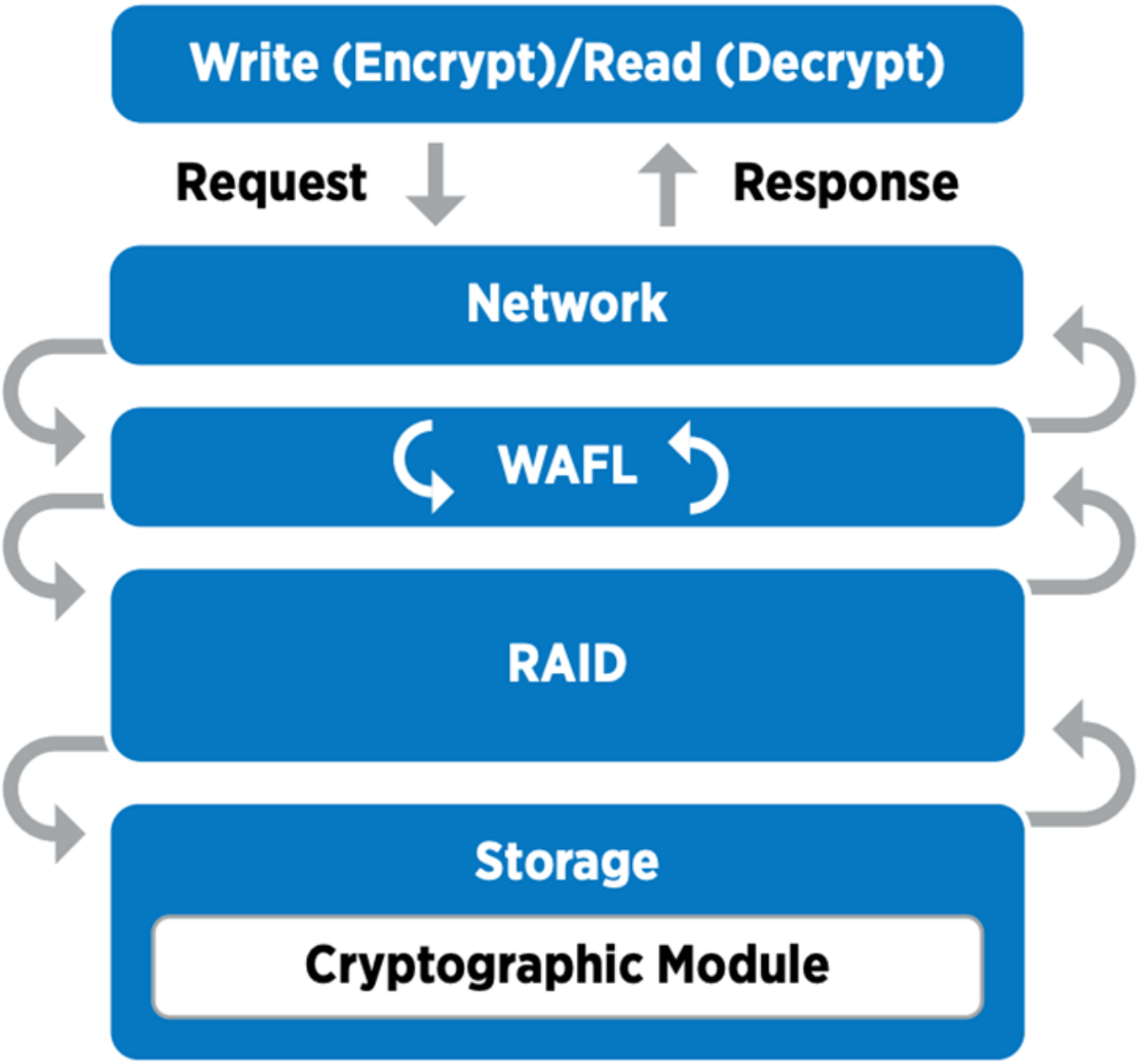
```
fp-health::> volume show -is-encrypted true
```

NSE

NSe utiliza SED para realizar el cifrado de datos a través de un mecanismo acelerado por hardware.

NSe está configurado para utilizar unidades de autocifrado FIPS 140-2 de nivel 2 para facilitar el cumplimiento de normativas y el retorno de reserva al permitir la protección de los datos en reposo mediante el cifrado de

disco transparente AES de 256 bits. Las unidades realizan todas las operaciones de cifrado de datos internamente, como se muestra en la siguiente figura, incluida la generación de claves de cifrado. Para evitar el acceso no autorizado a los datos, el sistema de almacenamiento debe autenticarse con la unidad mediante una clave de autenticación que se establezca la primera vez que se utilice la unidad.



NSe utiliza el cifrado de hardware en cada unidad, que se valida con FIPS 140-2 nivel 2.

Para obtener más información sobre NSE, consulte la "Especificaciones técnicas de NSE".

Gestión de claves

El estándar FIPS 140-2 se aplica al módulo criptográfico según lo definido por el límite, como se muestra en la siguiente figura.

2.1.1 Cryptographic Boundary

The logical cryptographic boundary of the CryptoMod module is the cryptomod_fips.ko component of ONTAP OS kernel. The logical boundary is depicted in the block diagram below. The Approved DRBG is used to supply the module's cryptographic keys. The physical boundary for the module is the enclosure of the NetApp controller.

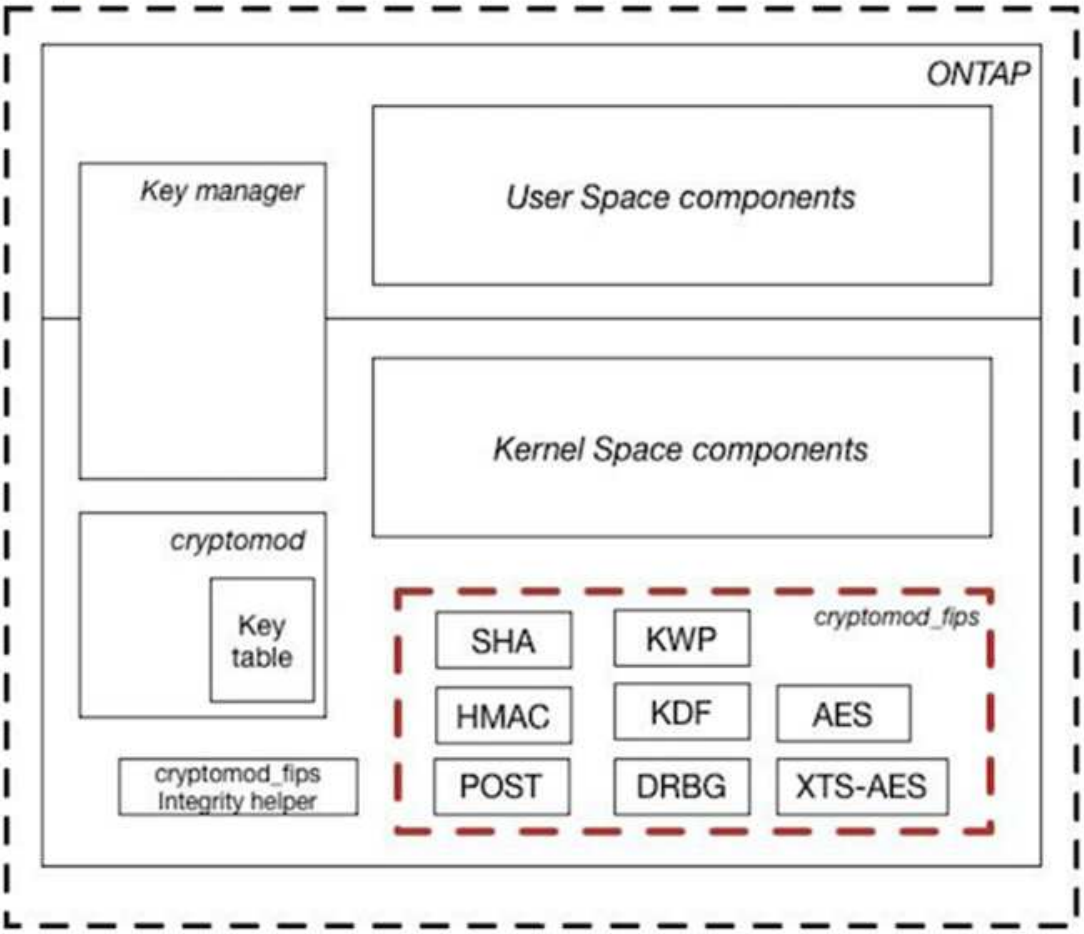


Figure 1 - Block Diagram

Key Manager realiza un seguimiento de todas las claves de cifrado utilizadas por ONTAP. NSe SED utiliza el gestor de claves para establecer las claves de autenticación de NSE SED. Cuando se utiliza el gestor de claves, la solución combinada NVE y NAE está compuesta por un módulo criptográfico de software, claves de cifrado y un gestor de claves. Para cada volumen, NVE utiliza una clave de cifrado de datos XTS-AES 256 única que almacena el gestor de claves. La clave utilizada para un volumen de datos es única para el volumen de datos de ese clúster y se genera cuando se crea el volumen cifrado. De forma similar, un volumen NAE utiliza claves de cifrado de datos XTS-AES 256 exclusivas por agregado, que también almacena el gestor de claves. Las claves NAE se generan cuando se crea el agregado cifrado. ONTAP no pregenera claves, las reutiliza o las muestra en texto sin formato; el administrador de claves las almacena y protege.

Compatibilidad con gestor de claves externo

A partir de ONTAP 9.3, los gestores de claves externos son compatibles con las soluciones NVE y NSE. El estándar FIPS 140-2 se aplica al módulo criptográfico utilizado en la implementación del proveedor específico. Con mayor frecuencia, los clientes de FlexPod y ONTAP utilizan una de las siguientes opciones validadas (según el "Matriz de interoperabilidad de NetApp") gestores de claves:

- Gemalto o SafeNet EN

- Vormétrico (Thales)
- SKLM DE IBM
- Utimaco (anteriormente Microfocus, HPE)

Se realiza un backup de la clave de autenticación SED de NSE y NVMe en un gestor de claves externo mediante el protocolo de interoperabilidad de gestión de claves (KMIP) DE OASIS estándar del sector. Solo el sistema de almacenamiento, la unidad y el administrador de claves tienen acceso a la clave y no es posible desbloquear la unidad si se mueve fuera del dominio de seguridad, para evitar la fuga de datos. El gestor de claves externo también almacena claves de cifrado de volúmenes NVE y claves de cifrado de agregados de NAE. Si el controlador y los discos se mueven y ya no tienen acceso al gestor de claves externo, no se podrá acceder a los volúmenes NVE y NAE ni se podrán descifrar.

El siguiente comando de ejemplo añade dos servidores de gestión de claves a la lista de servidores usados por el administrador de claves externo para almacenar máquinas virtuales (SVM) `svmname1`.

```
fp-health::> security key-manager external add-servers -vserver svmname1
-key-servers 10.0.0.20:15690, 10.0.0.21:15691
```

Cuando se utiliza un centro de datos de FlexPod en una situación de multi-tenancy, ONTAP permite a los usuarios al proporcionar separación de tenancy por motivos de seguridad en el nivel de SVM.

Para verificar la lista de gestores de claves externos, ejecute el siguiente comando de la CLI:

```
fp-health::> security key-manager external show
```

Combine el cifrado para obtener el doble cifrado (defensa por capas).

Si necesita segregar el acceso a los datos y asegurarse de que los datos estén protegidos todo el tiempo, NSE SED puede combinarse con cifrado a nivel de red o estructura. NSe SED actúa como una backstop si un administrador se olvida de configurar o configurar incorrectamente el cifrado de nivel superior. Para dos capas distintas de cifrado, puede combinar NSE SED con NVE y NAE.

Plano de control ONTAP de NetApp modo FIPS para todo el clúster

El software de gestión de datos ONTAP de NetApp tiene una configuración de modo FIPS que instancia un nivel de seguridad añadido para el cliente. Este modo FIPS sólo se aplica al plano de control. Cuando se habilita el modo FIPS, de acuerdo con los elementos clave de FIPS 140-2, se deshabilitan Transport Layer Security v1 (TLSv1) y SSLv3, y sólo se mantienen habilitadas TLS v1.1 y TLS v1.2.

> El panel de control de todo el clúster ONTAP del modo FIPS es compatible con FIPS 140-2 de nivel 1. El modo FIPS de todo el clúster utiliza un módulo criptográfico basado en software proporcionado por NCSM.

El modo de cumplimiento de normativas FIPS 140-2 para el plano de control de todo el clúster protege todas las interfaces de control de ONTAP. De forma predeterminada, el modo solo FIPS 140-2 está deshabilitado; sin embargo, puede habilitar este modo mediante la configuración del `is- fips-enabled` parámetro a. `true` para la `security config modify` comando.

Para habilitar el modo FIPS en el clúster ONTAP, ejecute el siguiente comando:

```
fp-health::> security config modify -interface SSL -is-fips-enabled true
```

Cuando el modo SSL FIPS está habilitado, la comunicación SSL de ONTAP con el cliente o los componentes de servidor externos a ONTAP utilizará la criptografía de quejas FIPS para SSL.

Para ver el estado FIPS del clúster completo, ejecute los siguientes comandos:

```
fp-health::> set advanced
fp-health::*> security config modify -interface SSL -is-fips-enabled true
```

"Siguiente: Ventajas de la solución de la infraestructura convergente de FlexPod."

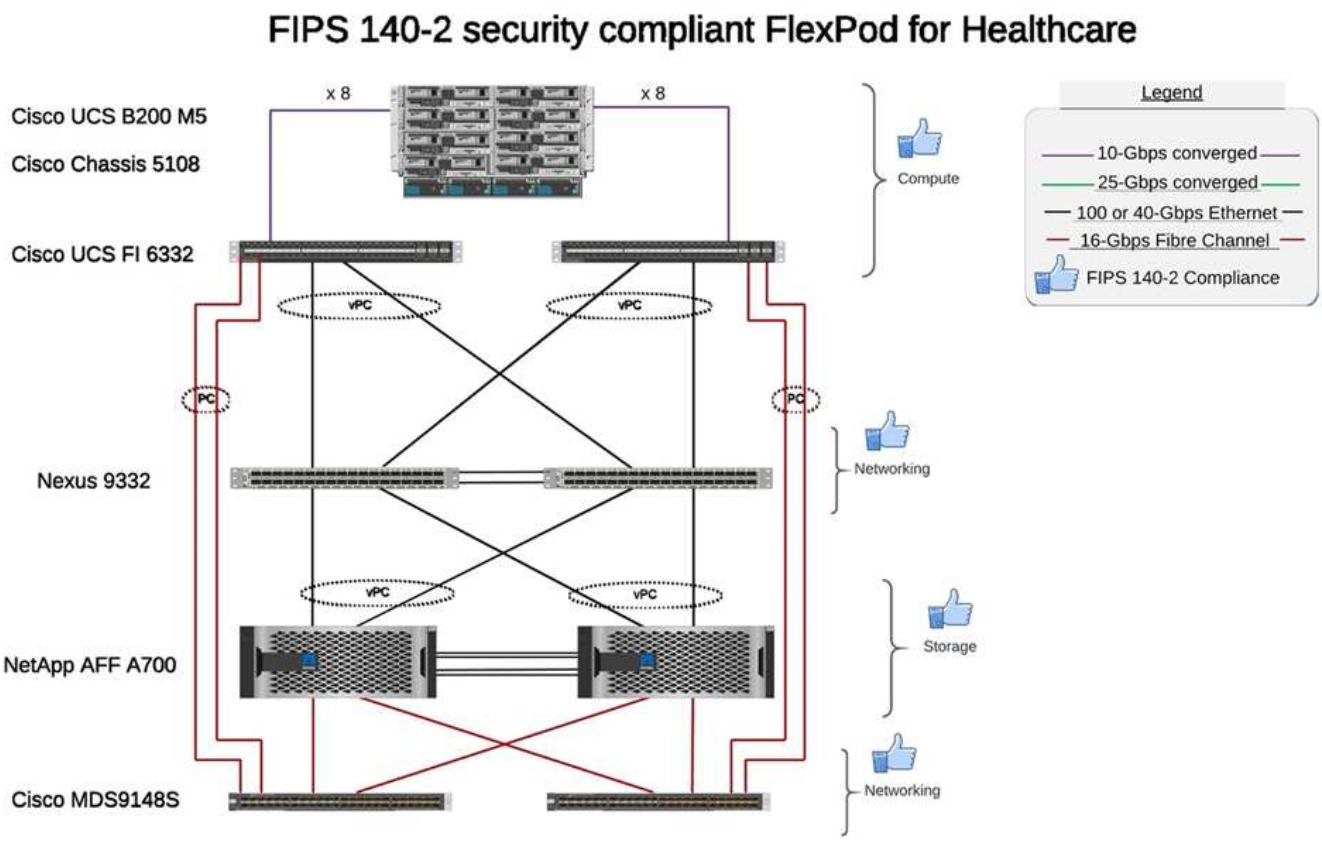
Ventajas para las soluciones de la infraestructura convergente de FlexPod

"Anterior: Almacenamiento ONTAP de FlexPod y FIPS 140-2."

Las organizaciones sanitarias cuentan con varios sistemas de misión crítica. Dos de los sistemas más críticos son los sistemas de historiales médicos electrónicos (EHR) y los sistemas de exploración médica. Para realizar una demostración de la configuración de FIPS en un sistema FlexPod, utilizamos un sistema EHR de código abierto y un sistema de archivado y comunicación de imágenes (PACS) de código abierto para la configuración de laboratorio y la validación de cargas de trabajo en el sistema FlexPod. Para obtener una lista completa de las funcionalidades de EHR, los componentes de las aplicaciones lógicas de EHR y las ventajas que se obtienen con la implantación en un sistema FlexPod, consulte "TR-4881: FlexPod para sistemas de registros sanitarios electrónicos". Para obtener una lista completa de las capacidades del sistema de imágenes médicas, los componentes de la aplicación lógica y cómo se benefician los sistemas de imágenes médicas cuando se implementan en FlexPod, consulte "TR-4865: FlexPod para imágenes médicas".

Durante la configuración de FIPS y la validación de cargas de trabajo, hemos ejercido características de carga de trabajo que eran representativas de una organización sanitaria típica. Por ejemplo, hemos ejercido un sistema EHR de código abierto para incluir un acceso realista a los datos del paciente y escenarios de cambio. Además, se realizaron cargas de trabajo de imágenes médicas que incluyeron imágenes digitales y comunicaciones en objetos médicos (DICOM) en un `*. dcm` formato de archivo. Los objetos DICOM con metadatos se almacenaban en el almacenamiento de archivos y bloques. Además, implementamos funciones multivía desde un servidor Red Hat Enterprise Linux (RHEL) virtualizado. Almacenamos objetos DICOM en un NFS, montamos LUN mediante iSCSI y montan LUN mediante FC. Durante la configuración y validación FIPS, observamos que la infraestructura convergente FlexPod superó nuestras expectativas y tuvo un rendimiento fluido.

La siguiente figura muestra el sistema FlexPod utilizado para la configuración y validación FIPS. Aprovechamos la "FlexPod Datacenter con VMware vSphere 7.0 y NetApp ONTAP 9.7 Cisco Validated Design (CVD)" durante el proceso de configuración.



Infraestructura de la solución componentes de hardware y software

En las dos figuras siguientes se enumeran los componentes de hardware y software respectivamente, que se usan durante las pruebas FIPS que se habilitan en una FlexPod. Las recomendaciones en estas tablas son ejemplos. Debe trabajar con el SME de NetApp para garantizar que los componentes se corresponden con su organización. Además, asegúrese de que los componentes y las versiones sean compatibles con el "Herramienta de matriz de interoperabilidad de NetApp" (IMT) y. "Lista de compatibilidad de hardware (HCL) de Cisco".

Capa	Familia de productos	Cantidad y modelo	Detalles
Informática	Chasis Cisco UCS 5108	1 o 2	
	Servidores blade Cisco UCS	3 B200 M5	Cada uno con 2 20 núcleos o más, 2,7 GHz y 128 GB de RAM
	Tarjeta de interfaz virtual (VIC) de Cisco UCS	Cisco UCS 1440	Consulte
	2 interconexiones de estructura Cisco UCS	6332	-
Red	Switches Cisco Nexus	2 switches Cisco Nexus 9332	-

Capa	Familia de productos	Cantidad y modelo	Detalles
Red de almacenamiento	Red IP para el acceso de almacenamiento mediante protocolos SMB/CIFS, NFS o iSCSI	Los mismos switches de red que se han descrito anteriormente	-
	Acceso a almacenamiento mediante FC	2 Cisco MDS 9148S	-
Reducida	Sistema de almacenamiento all-flash AFF A700 de NetApp	Clúster 1	Clúster con dos nodos
	Bandeja de discos	Una bandeja de discos DS224C o NS224	Totalmente lleno con 24 unidades
	SSD	>24, 1,2 TB o mayor capacidad	-

De NetApp	Familia de productos	Versión o versión	Detalles
Varios	Linux	RHEL 7.X	-
	Windows	Windows Server 2012 R2 (64 bits)	-
	ONTAP de NetApp	ONTAP 9.7 o posterior	-
	Interconexión de estructura Cisco UCS	Cisco UCS Manager 4.1 o posterior	-
	Switches de las series Cisco Ethernet 3000 o 9000	Para la serie 9000, 7.0(3)I7(7) o posterior para la serie 3000, 9.2(4) o posterior	-
	Cisco FC: Cisco MDS 9132T	8.4(1a) o posterior	-
	Hipervisor	VMware vSphere ESXi 6.7 U2 o posterior	-
Reducida	Sistema de gestión de hipervisores	VMware vCenter Server 6.7 U3 (vcsa) o posterior	-
Red	Virtual Storage Console (VSC) de NetApp	VSC 9.7 o posterior	-
	SnapCenter de NetApp	SnapCenter 4.3 o posterior	-
	Administrador de Cisco UCS	4.1(1c) o posterior	
Hipervisor	ESXi		
Gestión	Sistema de gestión de hipervisores VMware vCenter Server 6.7 U3 (vcsa) o posterior		

De NetApp	Familia de productos	Versión o versión	Detalles
	Virtual Storage Console (VSC) de NetApp	VSC 9.7 o posterior	
	SnapCenter de NetApp	SnapCenter 4.3 o posterior	
	Administrador de Cisco UCS	4.1(1c) o posterior	

"Siguiente: Consideraciones adicionales sobre seguridad de FlexPod."

Otras consideraciones de seguridad de FlexPod

"Anterior: Ventajas de la solución de la infraestructura convergente de FlexPod."

La infraestructura FlexPod es una plataforma modular, convergente, opcionalmente virtualizada, escalable (escalado horizontal y vertical) y rentable. Con la plataforma FlexPod, puede escalar horizontalmente de forma independiente la computación, la red y el almacenamiento para acelerar la puesta en marcha de las aplicaciones. Además, la arquitectura modular posibilita operaciones no disruptivas incluso durante las actividades de escalado horizontal y actualización del sistema.

Los diferentes componentes de un sistema HIT requieren que los datos se almacenen en sistemas de archivos SMB/CIFS, NFS, Ext4 y NTFS. Este requisito implica que la infraestructura debe proporcionar acceso a datos a través de los protocolos NFS, CIFS y SAN. Un único sistema de almacenamiento de NetApp es compatible con todos estos protocolos, lo que elimina la necesidad de utilizar sistemas de almacenamiento específicos de protocolos existentes. Además, un único sistema de almacenamiento de NetApp es compatible CON múltiples CARGAS de trabajo DE HIT, como EHR, PACS o VNA, genómica, VDI, etc. con niveles de rendimiento garantizados y configurables.

CUANDO se implementa en un sistema FlexPod, HIT ofrece varias ventajas específicas para el sector sanitario. La siguiente lista es una descripción de alto nivel de estas ventajas:

- **Seguridad FlexPod**. La seguridad es la base misma de un sistema FlexPod. En los últimos años, el ransomware se ha convertido en una amenaza. El ransomware es un tipo de malware basado en la criptovirología, el uso de criptografía para crear software malicioso. Este malware puede utilizar cifrado de clave simétrica y asimétrica para bloquear los datos de una víctima y exigir un rescate para proporcionar la clave para descifrar los datos. Para obtener más información sobre cómo la solución de FlexPod ayuda a mitigar amenazas como el ransomware, consulte "TR-4802: La solución para el ransomware". Los componentes de la infraestructura de FlexPod también "Conforme a FIPS 140-2"son .
- * Cisco Intersight.* Cisco Intersight es una plataforma innovadora basada en la nube y de gestión como servicio que proporciona un único panel para la gestión y orquestación de FlexPod en toda la pila. La plataforma InterSight utiliza módulos criptográficos compatibles con la seguridad FIPS 140-2. La arquitectura de gestión fuera de banda de la plataforma lo hace fuera del alcance de algunos estándares o auditorías como HIPAA. Nunca se envía al portal Intersight ningún tipo de información de salud identificable de la red.
- **La tecnología FPolicy de NetApp.** FPolicy de NetApp (una evolución de la política de archivos de nombres) es un marco de notificaciones de acceso a archivos para supervisar y gestionar el acceso a archivos a través de los protocolos NFS o SMB/CIFS. Esta tecnología forma parte del software de gestión de datos ONTAP desde hace más de una década, lo cual resulta útil para detectar ransomware. Este motor Zero Trust proporciona medidas de seguridad adicionales más allá de los permisos en las listas de

control de acceso (ACL). FPolicy tiene dos modos de funcionamiento: Nativo y externo:

  - El modo nativo proporciona tanto la lista negra como la lista blanca de extensiones de archivo.
  - El modo externo tiene las mismas funcionalidades que el modo nativo, pero también se integra con un servidor FPolicy que se ejecuta externamente al sistema ONTAP así como un sistema SIEM (información de seguridad y gestión de eventos). Para obtener más información sobre cómo combatir el ransomware, consulte la "Lucha contra el ransomware: Parte tres – FPolicy de ONTAP, otra potente herramienta nativa (también conocida como gratuita)" blog.

- **Datos en reposo**. ONTAP 9 y versiones posteriores tienen tres soluciones de cifrado de datos en reposo conformes con la normativa FIPS 140-2:
  - NSe es una solución de hardware que utiliza unidades de autocifrado.
  - NVE es una solución de software que permite el cifrado de cualquier volumen de datos en cualquier tipo de unidad donde se habilita con una clave única para cada volumen.
  - NAE es una solución de software que permite el cifrado de cualquier volumen de datos en cualquier tipo de unidad en la que se habilita con claves únicas para cada agregado.

> A partir de ONTAP 9.7, NAE y NVE están habilitados por defecto si el paquete de licencia NetApp NVE con el nombre ve está en su lugar.

- **Datos en vuelo**. A partir de ONTAP 9.8, IPsec (el protocolo de seguridad de Internet) proporciona compatibilidad con cifrado de extremo a extremo para todo el tráfico de IP entre un cliente y una SVM de ONTAP. El cifrado de datos IPSec para todo el tráfico IP incluye protocolos NFS, iSCSI y SMB/CIFS. IPSec proporciona la única opción de cifrado en vuelo para el tráfico iSCSI.
- **Cifrado de datos integral en una estructura de datos multicloud híbrida**. Los clientes que usan tecnologías de cifrado de datos en reposo como NSE, NVE y el cifrado de paridad de clúster (CPE) para el tráfico de replicación de datos pueden ahora usar el cifrado integral entre el cliente y el almacenamiento en su estructura de datos multicloud híbrido mediante la actualización a ONTAP 9.8 o una versión posterior y mediante IPsec. A partir de ONTAP 9, puede habilitar el modo de cumplimiento normativo FIPS 140-2 para las interfaces en el plano de control de todo el clúster. De manera predeterminada, se deshabilita el modo FIPS 140-2-only. A partir de ONTAP 9.6, CPE proporciona compatibilidad del cifrado TLS 1.2 AES-256 GCM para las funciones de replicación de datos de ONTAP como las tecnologías SnapMirror, NetApp SnapVault y NetApp FlexCache. El cifrado se configura mediante una clave precompartida (PSK) entre dos pares de clústeres.
- **Multitenancy seguro**. Admite el aumento de las necesidades de la infraestructura compartida de servidores virtualizados y almacenamiento, lo que permite una multi-tenancy seguro de información específica del centro, en particular cuando se alojan varias instancias de bases de datos y software.

"Siguiente: Conclusión."

Conclusión

"Anterior: Consideraciones adicionales sobre seguridad de FlexPod."

Al ejecutar su aplicación de atención médica en una plataforma FlexPod, su organización de atención médica estará mejor protegida por una plataforma habilitada para FIPS 140-2. FlexPod ofrece protección con varias capas en cada componente único: Informática, redes y almacenamiento. Las funcionalidades de protección de datos de FlexPod protegen los datos en reposo o en movimiento y conservan los backups seguros y listos cuando sea necesario.

Evite errores humanos aprovechando los diseños prevalidados de FlexPod recientemente probados e infraestructuras convergentes de la alianza estratégica de Cisco y NetApp. Un sistema FlexPod ha diseñado y diseñado para proporcionar un rendimiento del sistema previsible y de baja latencia, y una alta disponibilidad con un impacto mínimo, incluso si se habilita FIPS 140-2 en las capas de computación, redes y almacenamiento. Este enfoque da como resultado una experiencia de usuario superior y un tiempo de respuesta óptimo para los usuarios del sistema HIT.

"Siguiente: Reconocimientos, historial de versiones y dónde encontrar información adicional."

Agradecimientos, historial de versiones y dónde encontrar información adicional

"Anterior: Conclusión."

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

- Guía de configuración de seguridad de la familia Cisco MDS 9000 NX-OS

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8_x/config/security/cisco_mds9000_security_config_guide_8x/configuring_fips.html#task_1188151

- Guía de configuración de seguridad de NX-OS con Cisco Nexus serie 9000, versión 9.3(x)

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/security/configuration/guide/b-cisco-nexus-9000-nx-os-security-configuration-guide-93x/m-configuring-fips.html

- Publicación 140-2 de NetApp y del estándar de procesamiento de información federal (FIPS)

  https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- FIPS 140-2

  https://fieldportal.netapp.com/content/902303

- Guía de fortalecimiento de NetApp ONTAP 9

  https://www.netapp.com/pdf.html?item=/media/10674-tr4569pdf.pdf

- Guía completa de cifrado de NetApp

  https://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.pow-nve%2Fhome.html

- Especificaciones técnicas de NVE y NAE

  https://www.netapp.com/pdf.html?item=/media/17070-ds-3899.pdf

- Especificaciones técnicas de NSE

  https://www.netapp.com/pdf.html?item=/media/7563-ds-3213-en.pdf

- Centro de documentación de ONTAP 9

  http://docs.netapp.com

- Publicación 140-2 de NetApp y del estándar de procesamiento de información federal (FIPS)

https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- Cumplimiento de normativas Cisco y FIPS 140-2-2

  https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html

- Módulo de seguridad de criptografía de NetApp

  https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2648.pdf

- Prácticas de ciberseguridad para medianas y grandes organizaciones sanitarias

  https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf

- Programa de validación de módulos de criptografía y Cisco (CMVP)

  https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search?SearchMode=Basic&Vendor=cisco&CertificateStatus=Active&ValidationYear=0

- Cifrado del almacenamiento de NetApp, unidades de autocifrado NVMe, cifrado de volúmenes de NetApp y cifrado agregado de NetApp

  https://www.netapp.com/pdf.html?item=/media/17073-ds-3898.pdf

- Cifrado de volúmenes de NetApp y cifrado de agregados de NetApp

  https://www.netapp.com/pdf.html?item=/media/17070-ds-3899.pdf

- Cifrado del almacenamiento de NetApp

  https://www.netapp.com/pdf.html?item=/media/7563-ds-3213-en.pdf

- FlexPod para sistemas de registros médicos electrónicos

  https://www.netapp.com/pdf.html?item=/media/22199-tr-4881.pdf

- Datos ahora: Mejora de rendimiento en entornos EHR de Epic con la tecnología flash conectada al cloud

  https://www.netapp.com/media/10809-cloud-connected-flash-wp.pdf

- Centro de datos FlexPod para infraestructura EHR de Epic

  https://www.netapp.com/pdf.html?item=/media/17061-ds-3683.pdf

- Guía de puesta en marcha del centro de datos FlexPod para EHR de Epic

  https://www.netapp.com/media/10658-tr-4693.pdf

- Infraestructura de centro de datos FlexPod para el software MEDITECH

  https://www.netapp.com/media/8552-flexpod-for-meditech-software.pdf

- El estándar FlexPod se extiende al software MEDITECH

https://blog.netapp.com/the-flexpod-standard-extends-to-meditech-software/

- Guía de tamaños direccionales de FlexPod para MEDITECH

  https://www.netapp.com/pdf.html?item=/media/12429-tr4774.pdf

- FlexPod para imágenes médicas

  https://www.netapp.com/media/19793-tr-4865.pdf

- IA en la sanidad

  https://www.netapp.com/pdf.html?item=/media/7393-na-369pdf.pdf

- FlexPod para el sector sanitario facilita su transformación

  https://flexpod.com/solutions/verticals/healthcare/

- FlexPod de Cisco y NetApp

  https://flexpod.com/

Reconocimientos

- Abhinav Singh, Ingeniero Técnico de Marketing de NetApp
- Brian o'Mahony, arquitecto de soluciones Healthcare (Epic), NetApp
- Brian Pruitt, director de desarrollo comercial de NetApp
- Arvind Ramakrishnan, arquitecto sénior de soluciones de NetApp
- Michael Hommer, Director técnico de FlexPod Global Field, NetApp

Historial de versiones

Versión	Fecha	Historial de versiones del documento
Versión 1.0	Abril de 2021	Versión inicial

Cisco Intersight con el almacenamiento ONTAP de NetApp

Guía de inicio rápido de Cisco Intersight con el almacenamiento de NetApp

En colaboración con: 

Introducción

NetApp y Cisco se han asociado para proporcionar Cisco Intersight, una visión única del ecosistema de FlexPod. Esta integración simplificada crea una plataforma de gestión unificada para todos los componentes de la infraestructura de FlexPod y la solución de FlexPod. Cisco Intersight le permite supervisar el almacenamiento de NetApp, la informática de Cisco y el inventario de VMware. También permite orquestar o automatizar flujos de trabajo para cumplir con las tareas de almacenamiento y virtualización en tándem.

Información relacionada

Para obtener más información, consulte los siguientes documentos y sitios web:

"TR 4883: Centro de datos de FlexPod con ONTAP 9.8, el conector de almacenamiento de ONTAP para Cisco Intersight y el modo gestionado de Cisco Intersight"

"Centro de ayuda de Cisco Intersight"

"Introducción a Cisco Intersight Descripción general"

"Guía de instalación y actualización de Intersight Appliance"

Lo nuevo

En esta sección se enumeran las nuevas funciones y funcionalidades disponibles para Cisco Intersight con el almacenamiento ONTAP de NetApp.

A enero de 2024

- Orquestación de almacenamiento de NetApp mediante flujos de trabajo de referencia que ahora están disponibles para su descarga en GitHub mediante la "Repositorio de flujo de trabajo Intersight de FlexPod". Para obtener más información sobre los nuevos flujos de trabajo de referencia en GitHub, consulte "Caso de uso 2: Orquestación del almacenamiento de NetApp mediante flujos de trabajo de referencia".

Noviembre de 2023

- Se agregó la página NVMe Namespaces en la sección Inventario de la interfaz de usuario.

Agosto de 2023

Es necesario actualizar a NetApp Active IQ Unified Manager 9,13GA para garantizar la compatibilidad y completa funcionalidad con la última versión.

- Se ha mejorado la tarea de Nueva LUN inteligente de NetApp para indicar claramente la disponibilidad de las opciones de selección para crear un iGroup nuevo o seleccionar un iGroup existente. Cuando ahora los usuarios seleccionan la casilla para crear un iGroup nuevo, el parámetro para elegir un iGroup existente ya no está disponible. Si los usuarios deseleccionan el cuadro para crear un nuevo iGroup, el parámetro de iGroup existente queda disponible.
- Se han mejorado las tareas de asignación de nueva LUN de NetApp y eliminación de asignación de LUN de NetApp. Se ha actualizado la nueva relación entre la LUN y el iGroup. El inventario de interfaz de usuario se actualiza de inmediato tanto para la LUN como para el iGroup tras la ejecución de la tarea.
- La página Comprobaciones ahora carga correctamente los usuarios que inician sesión por primera vez y ya no necesita refrescarse.

Julio de 2023

Es necesario actualizar a NetApp Active IQ Unified Manager 9,13GA para garantizar la compatibilidad y completa funcionalidad con la última versión.

- Nombres actualizados para las tareas de almacenamiento de NetApp. Consulte Caso de uso 3 Flujos de trabajo personalizados utilizando un formulario sin diseñador para obtener la lista completa de tareas renombradas.
- La dirección IP de la interfaz NFS se agregó como resultado de la nueva tarea de volumen inteligente NAS de NetApp.
- Se agregó una comprobación de que el transporte ASUP es HTTPS a la pestaña Comprobaciones.
- El tipo de nivel correcto para todos los niveles ahora se muestra correctamente en la interfaz de usuario de Niveles.
- Todas las licencias compatibles ahora se muestran correctamente en la página Licencias.
- El valor preciso para los recursos compartidos CIFS sin o sin un directorio inicial ahora aparece en la página Recursos compartidos.
- Ahora el ordenación y el filtrado están habilitados para la columna Asignada en la página LUN.
- La ordenación y el filtrado ahora han habilitado la columna Autenticación Activada en la página Servidores NTP.
- Se han añadido nuevas comprobaciones y las siguientes categorías correspondientes a la ficha Comprobaciones.
  - Seguridad
  - Anti-ransomware
  - Disponibilidad
  - Otros
- En la vista de detalle Inventario, el informe ahora se utiliza en lugar de la capacidad utilizada física.

Junio de 2023

Se requiere una actualización a NetApp Active IQ Unified Manager 9.13RC1 para garantizar la compatibilidad y la funcionalidad completa con la última versión.

- Nombres actualizados para las tareas de almacenamiento de NetApp. Consulte "Caso de uso 3 flujos de trabajo personalizados utilizando un formulario sin diseñador" para obtener la lista completa de tareas renombradas.

Abril de 2023

- Agregadas políticas de protección (SnapMirror) y políticas de Snapshot en la página Políticas de la sección Inventario de la interfaz de usuario.
- Se ha agregado la página Clientes NFS en la sección Inventario de la interfaz de usuario.
- Se ha agregado la columna Protected en la página Storage VMs en la sección Inventory de la interfaz de usuario.
- Se ha modificado la forma en que se informa y se muestra la información de Reducción de datos.
- Se han agregado pestañas Nivel Local y Nivel de Nube en la página Niveles de la sección Inventario de la interfaz de usuario.
- La columna Nodo ahora se muestra después de la columna Nombre en la página Puertos dentro de la sección Inventario de la interfaz de usuario.

Enero de 2023

Se requiere una actualización a Active IQ Unified Manager 9.12 GA de NetApp para garantizar la compatibilidad y todas las funciones con la última versión. Para obtener una lista de problemas conocidos relacionados con esta versión, consulte Problemas conocidos.

- Las comprobaciones de interoperabilidad de Intersight pueden distinguir entre los modos de firmware de UCSM e IMM cuando se realizan comprobaciones de compatibilidad.
- Las relaciones de protección no se mostrarán en Intersight para ONTAP 9.7. Este problema se solucionó en ONTAP 9.8RC1.

Agosto de 2022

Se requiere una actualización a Active IQ Unified Manager 9.11 GA de NetApp para garantizar la compatibilidad y todas las funciones con la última versión. Para obtener una lista de problemas conocidos relacionados con esta versión, consulte Problemas conocidos.

- Se ha actualizado el cálculo de la capacidad disponible del clúster para que coincida con System Manager
- Se ha actualizado la página General del clúster para ocultar el resumen de las métricas de rendimiento hasta que se rellenan los datos de rendimiento
- Se ha solucionado el problema de la interfaz de usuario de la página General del clúster que ocasionalmente provocó la bloqueo de la página
- Se han agregado recursos compartidos de CIFS, servicios CIFS, qtrees y políticas de SnapMirror de SVM para realizar un inventario de back-end.
- Se han añadido los recursos compartidos y Qtrees al menú de navegación de la interfaz de usuario en la

sección Logical Inventory

- Se añadieron recursos compartidos como pestaña de una máquina virtual de almacenamiento seleccionada
- Se ha agregado información del servicio CIFS en la pestaña Storage VM General si la máquina virtual de almacenamiento está habilitada para CIFS
- Se ha añadido una página de comprobaciones del clúster que permite a los usuarios validar la configuración de los sistemas de almacenamiento de NetApp que cumple las prácticas recomendadas

Julio de 2022

- Imágenes mejoradas para la proporción de reducción de datos en clúster que ahora está disponible en el widget Capacity
- Se ha añadido la pestaña FC interfaces a la página Network interfaces
- La creación de un nuevo volumen con la tarea genérica “Nuevo volumen de almacenamiento” ahora establece la garantía de espacio de volumen en ninguno y el porcentaje de reserva de instantáneas en 0%
- El campo de comentario de la tarea Editar política de snapshot ahora es opcional y ya no es obligatorio
- Se ha mejorado la coherencia de la orquestación y el inventario de IU
- La información sobre capacidad de Intersight bajo capacidad del clúster ahora es coherente con System Manager
- Se ha agregado la casilla de verificación en la tarea New Storage Virtual Machine para mostrar todos los parámetros al crear una nueva interfaz de administración con el fin de mejorar la facilidad de uso
- Los protocolos movidos por debajo de Client Match, ahora son coherentes con System Manager
- La página general de la política de exportación ahora muestra los protocolos de acceso
- ahora se ha registrado de forma condicional el eliminación del igroup
- Se han añadido los parámetros “Failover Policy” y "autorevert" para NAS en New Storage NAS Data Interface y New Storage iSCSI Data Interface
- La tarea revertir para nuevo volumen inteligente NAS de almacenamiento ahora elimina la política de exportación si no hay otros volúmenes asociados
- Se han realizado mejoras para las tareas de Smart Volume y Smart LUN

Abril de 2022

Para garantizar la compatibilidad y completar la funcionalidad con futuras versiones, se recomienda actualizar el Active IQ Unified Manager de NetApp a la versión 9.10P1.

- Se ha agregado el dominio de difusión a la página Detalles del puerto Ethernet
- Se cambió el término “agregado” a “nivel” para el agregado y SVM dentro de la interfaz de usuario
- Se ha cambiado el término "Estado del clúster" a "Estado de la cabina".
- El filtro MTU funciona ahora con <,>,=,⇐,>= caracteres
- Se ha agregado la página de interfaz de red al inventario del clúster
- Se ha agregado AutoSupport al inventario de clústeres
- Añadido `cdpd.enable` opción a nodo
- Se ha agregado un objeto para el vecino de CDP

- Se han agregado tareas de almacenamiento de flujos de trabajo de NetApp en Cisco Intersight. Consulte "Caso de uso 3 flujos de trabajo personalizados utilizando un formulario sin diseñador" Para obtener una lista completa de tareas de almacenamiento de NetApp.

Enero de 2022

- Se han añadido alarmas de intervisión basadas en eventos para Active IQ Unified Manager 9.10 de NetApp o posterior.

> Para garantizar la compatibilidad y todas las funcionalidades con futuras versiones, se recomienda actualizar el sistema Active IQ Unified Manager de NetApp a la versión 9.10.

- Establezca explícitamente cada protocolo habilitado (true o false) para el equipo virtual de almacenamiento
- El estado clusterHealthStatus correlacionado está bien-con-suprimido a OK
- La columna Estado cambiado su nombre a la columna Estado del clúster en la página de lista Cluster
- Muestra “no accesible” la cabina de almacenamiento si el clúster está inactivo o no se puede acceder a él de otro modo
- Cambie el nombre de la columna Estado a la columna Estado de la cabina en la página Cluster General
- SVM ahora tiene una pestaña "Volumes" que muestra todos los volúmenes para la SVM
- El volumen tiene una sección de capacidad Snapshot
- Ahora las licencias se muestran correctamente

Octubre de 2021

- Lista actualizada de tareas de almacenamiento de NetApp disponibles en Cisco Intersight. Consulte "Caso de uso 3 flujos de trabajo personalizados utilizando un formulario sin diseñador" Para obtener una lista completa de tareas de almacenamiento de NetApp.
- Se ha agregado la columna Estado en la página de lista Cluster.
- Ahora hay detalles ampliados disponibles en la página General de un clúster seleccionado.
- Ahora se puede acceder a la tabla NTP Server a través del panel de navegación.
- Se ha agregado una nueva ficha Sensores que contiene la página General de la máquina virtual de almacenamiento.
- El resumen de grupos de agregación de vínculos y VLAN ya está disponible en la página General de puertos.
- Columna total Data Capacity añadida en la tabla Volume total Capacity.
- Las columnas de latencia, IOPS y rendimiento se añaden en las tablas Average Volume Statistics, Average LUN Statistics, Average Aggregate Statistics, Average Storage VM Statistics y Average Node Statistics

> Las métricas de rendimiento anteriores solo están disponibles para cabinas de almacenamiento supervisadas con Active IQ Unified Manager 9.9 de NetApp o versiones posteriores.

Problemas conocidos

- Si utiliza una versión de AIUM 9.11 o anterior, se producirá una discrepancia entre los valores mostrados en la página Lista de almacenamiento y el gráfico de barras de capacidad de la página General de almacenamiento. Para resolver este problema, actualice a AIQUM 9.12 o superior para garantizar la precisión de los valores de capacidad mostrados.
- Si utiliza AIUM 9.11 o anterior, las comprobaciones realizadas por la pestaña "Interoperability" de la página "Integrated Systems" no podrán distinguir con precisión los componentes de Cisco de IMM y UCSM. Para resolver este problema, actualice a AIQUM 9.12 para asegurarse de que todos los componentes están correctamente identificados.
- Para garantizar que los datos de inventario de almacenamiento Intersight no se vean afectados durante el proceso de recopilación de datos, deben eliminarse de Active IQ Unified Manager todos los clústeres de ONTAP no admitidos (es decir, versiones inferiores a ONTAP 9.7P1).
- Todos los destinos reclamados requieren una versión mínima de AIUM de 9.11 para que las consultas de interoperabilidad del sistema integrado de FlexPod se completen correctamente.
- La página Comprobaciones de Inventario de Almacenamiento no se rellenará si el cluster ONTAP se agrega a AIQUM mediante un FQDN. Los usuarios deben agregar clústeres de ONTAP a AIQUM mediante una dirección IP.

Requisitos

Compruebe que cumple los requisitos de hardware, software y licencias para la integración del almacenamiento de NetApp ONTAP con Cisco Intersight.

Requisitos de hardware y software

Estos son los componentes mínimos de hardware y software necesarios para implementar la solución. Los componentes que se usan en cualquier implementación particular de la solución pueden variar en función de las necesidades del cliente.

Componente	Detalles de los requisitos
ONTAP de NetApp	ONTAP 9.7P1 y posterior
Active IQ Unified Manager de NetApp	Se requiere la última versión de NetApp Active IQ Unified Manager (actualmente 9.14RC1)
Cabina de almacenamiento NetApp	Cabinas de almacenamiento All ONTAP ASA, AFF y FAS compatibles con ONTAP 9.7P1 y versiones posteriores
Hipervisor de virtualización	VSphere 7,0 y versiones posteriores

Consulte "Sistemas compatibles con Cisco Intersight" Para ver los requisitos mínimos de los componentes de computación de Cisco UCS y la versión UCSM.

Requisitos para la licencia de Cisco Intersight

Cisco Intersight ofrece servicios como el servicio de infraestructura y el servicio Cloud Orchestrator para gestionar, automatizar y optimizar el almacenamiento físico (almacenamiento de NetApp). Puede utilizar estos servicios para gestionar el servidor Cisco UCS y el sistema Cisco HyperFlex. El servicio Infrastructure Service y Cloud Orchestrator utilizan un modelo de licencias basado en suscripción con varios niveles. Puede

seleccionar el nivel de volumen de Cisco UCS Server necesario para el período de suscripción seleccionado.

Modelo de licencia

Se ha simplificado el modelo de licencias de Cisco Intersight Infrastructure Services y ahora ofrece los siguientes dos niveles:

- **Cisco Intersight Infrastructure Services Essentials** - El nivel de licencia Essentials ofrece gestión de servidores, incluida la funcionalidad de monitoreo de estado global, inventario, soporte proactivo a través de la integración de Cisco TAC, autenticación multifactor, además de proporcionar acceso a SDK y API.
- * Cisco Intersight Infrastructure Services Advantage* - El nivel de licencia Advantage ofrece una gestión avanzada de servidores con visibilidad extendida, integración de ecosistemas, automatización de Cisco y hardware y software de terceros, además de proporcionar soluciones multidominio.

Para obtener más información acerca de las funciones cubiertas por los distintos niveles de licencia, vaya a. "Licencia de servicios de infraestructura".

Antes de empezar

Para supervisar y orquestar el almacenamiento de NetApp desde Cisco Intersight, necesita tener instalado Active IQ Unified Manager de NetApp y Cisco Intersight Virtual Appliance en el entorno vCenter.

Instale o actualice Active IQ Unified Manager de NetApp

Instale o actualice a Active IQ Unified Manager (se requiere la última versión, actualmente 9.14RC1) si no lo ha hecho. Para obtener instrucciones, vaya a "Documentación de Active IQ Unified Manager de NetApp".

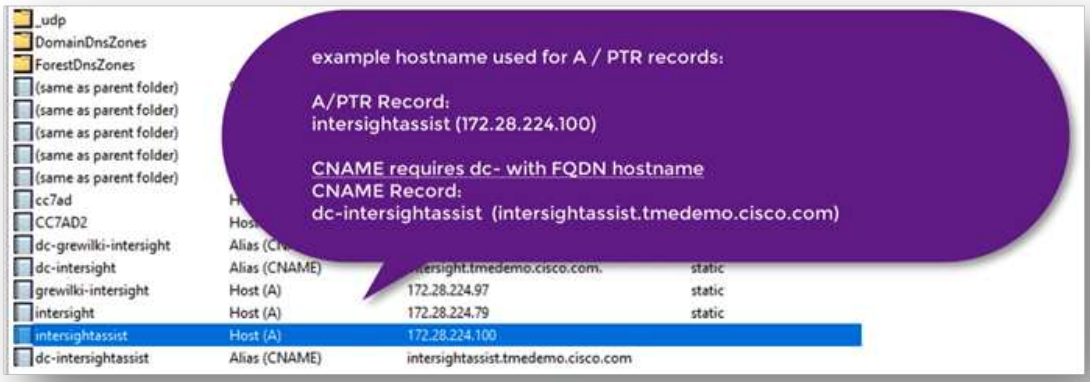
Instale el dispositivo virtual Cisco Intersight Assist

Asegúrese de cumplir con la "Requisitos de la red, el sistema y las licencias de dispositivos virtuales Cisco Intersight".

- Pasos*

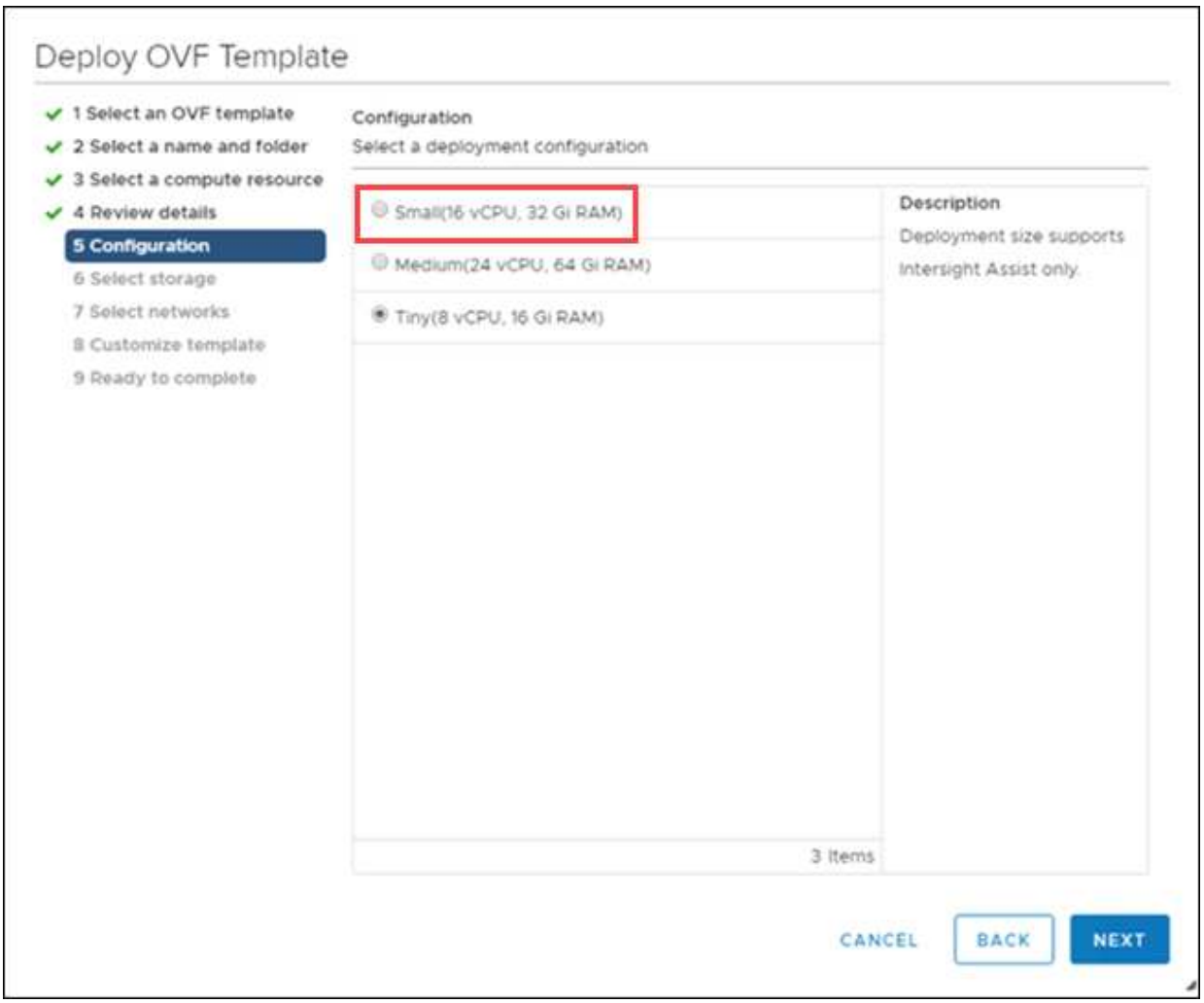
1. Cree una cuenta de Cisco Intersight. Visite "https://intersight.com/" Para crear su cuenta de Intersight. Debe tener un ID de Cisco válido para crear una cuenta de Cisco Intersight.
2. Descargue el dispositivo virtual de Intersight en "software.cisco.com". Para obtener más información, vaya a la "Guía de instalación y actualización de Intersight Appliance".
3. Implemente el OVA. Se requiere DNS y NTP para implementar el OVA.

    a. Configurar DNS con registros de alias A/PTR y CNAME antes de implementar el OVA. Vea el ejemplo siguiente.



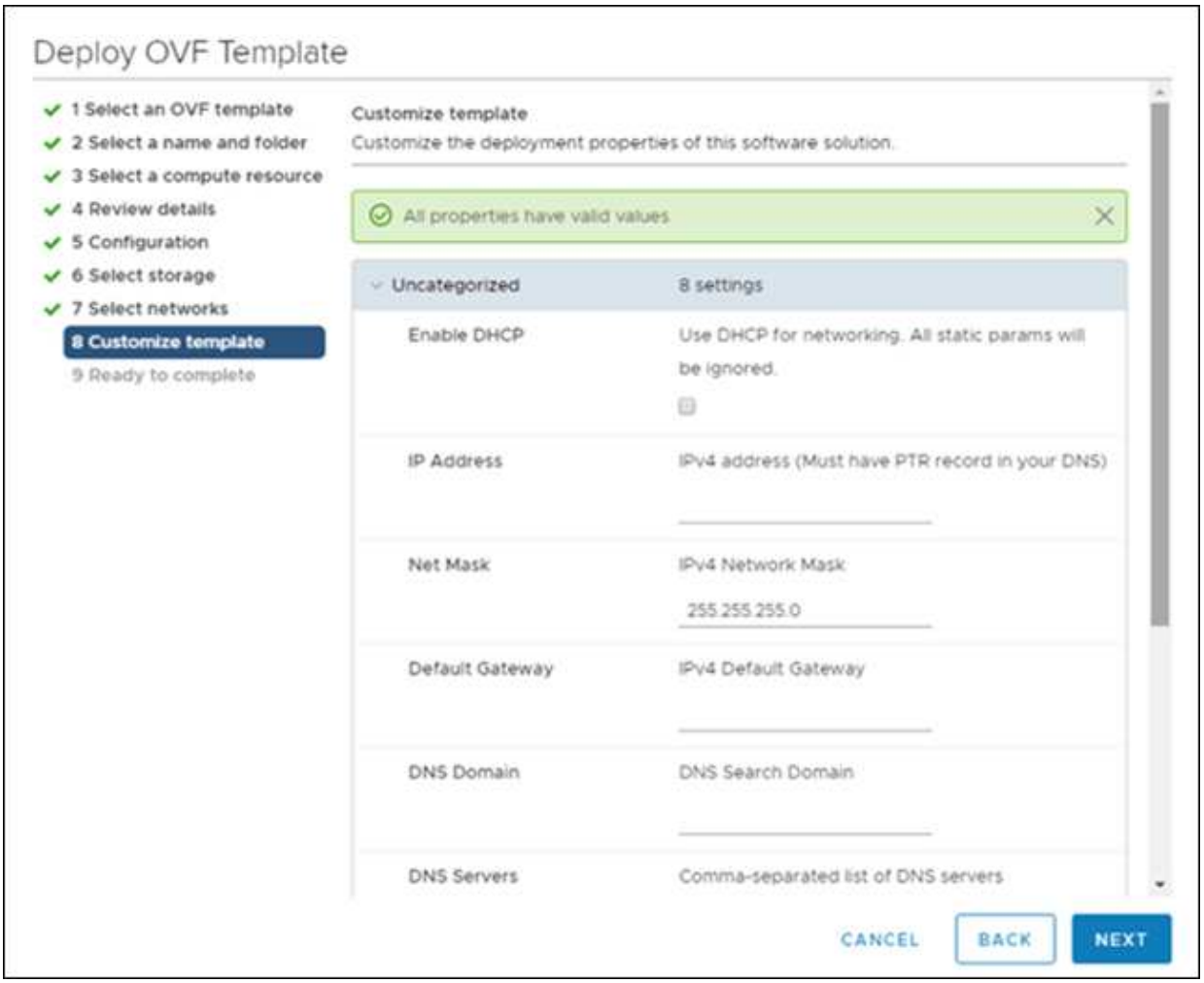
b. Elija el tamaño de configuración adecuado (pequeño, pequeño o mediano) en función de los requisitos de puesta en marcha de OVA para Intersight Virtual Appliance.

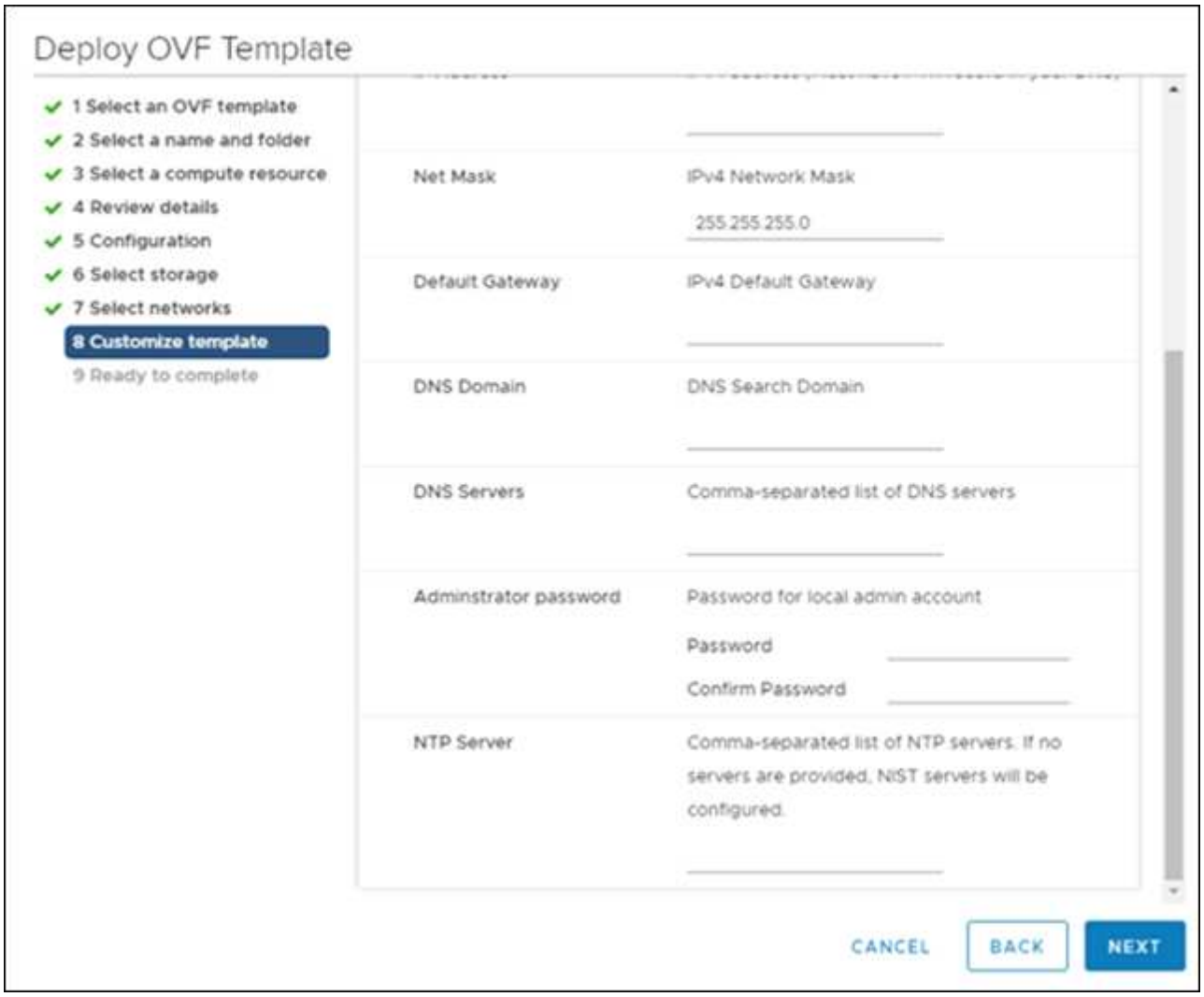
SUGERENCIA: para un clúster ONTAP de dos nodos con un gran número de objetos de almacenamiento, NetApp recomienda utilizar la opción pequeña (16 vCPU, 32 Gi RAM).



c. En la página **Personalizar plantilla**, personalice las propiedades de implementación de la plantilla OVF. La contraseña de administrador se utiliza para los usuarios locales: Admin(

webUI/cli/ssh).





a. Haga clic en **Siguiente**.

4. Después de la implementación del dispositivo Intersight Assist.

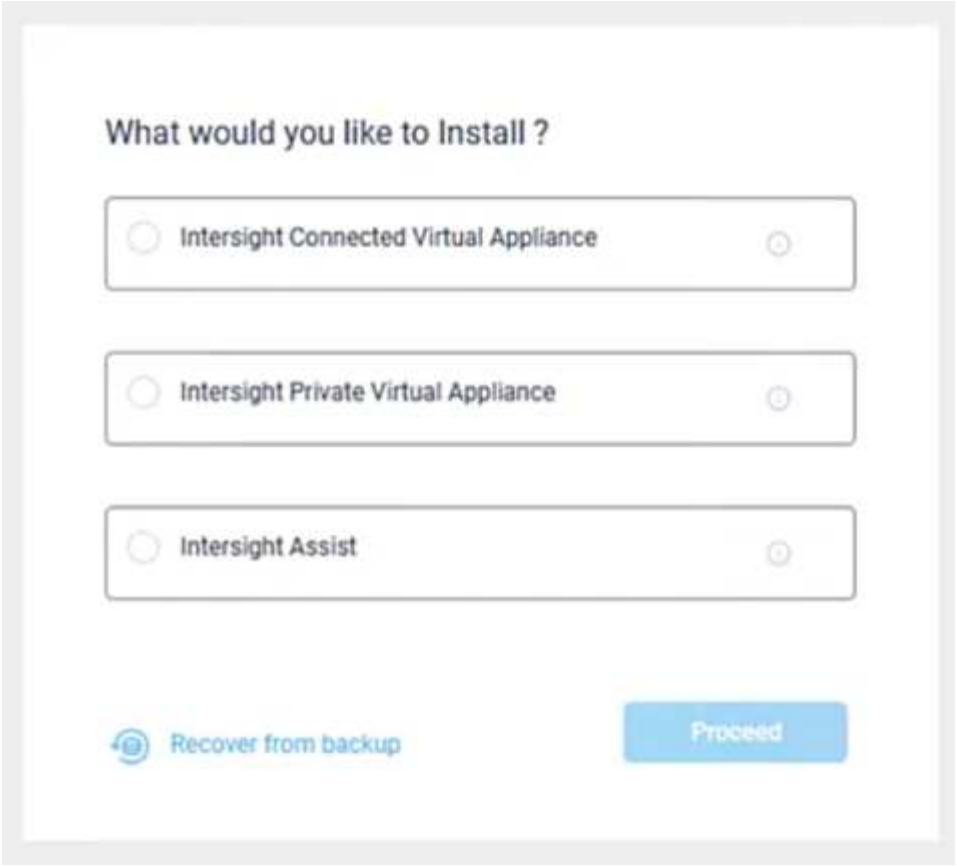
   a. Vaya a. https://FQDN-of-your-appliance para completar la configuración posterior a la instalación del dispositivo.

      El proceso de instalación se inicia automáticamente. La instalación puede tardar hasta una hora dependiendo del ancho de banda hasta Intersight.com. También puede tardar varios segundos en que el sitio seguro esté operativo una vez que se encienda el equipo virtual.

   b. Durante el proceso posterior a la implementación, seleccione la siguiente opción:

      - **Asistencia de Intersight.** esta implementación permite que el modelo SaaS se conecte a Cisco Intersight.

      > Al seleccionar Intersight Assist, anote el ID del dispositivo y el código de reclamación antes de continuar.



a. Haga clic en **proseguir**.

b. Seleccione **asistencia a la vista** y complete los siguientes pasos:

   i. Acceda a su cuenta de SaaS Intersight en "https://intersight.com".

   ii. Haga clic en **Targets**, **Cisco Intersight Assist** y a continuación **Iniciar**.

   iii. Solicite el dispositivo **Cisco Intersight Assist** copiando y pegando el identificador de dispositivo y el código de reclamación desde el dispositivo virtual Intersight Assist recién implementado.



   iv. Vuelva al dispositivo **Cisco Intersight Assist** y haga clic en **continuar.** puede que necesite actualizar el explorador.

Se inicia el proceso de descarga e instalación. Los binarios se transfieren de Intersight Cloud a su dispositivo en las instalaciones. El tiempo de finalización varía en función del ancho de banda que tenga con Intersight Cloud.

Configure el servidor proxy de mensajería unificada de AIQ para el servicio IMT

Si utiliza un servidor proxy con AIQ para Cisco Intersight con el almacenamiento ONTAP de NetApp, debe configurar la configuración a través de la interfaz de línea de comandos (CLI) para utilizar el servicio de la herramienta de matriz de interoperabilidad (IMT). El servicio IMT está disponible en la pestaña **Interoperability** de la página **sistemas integrados**. Debe usar el shell de Diag de máquina virtual (OVA) de Active IQ Unified Manager para configurar la configuración del servidor proxy de AIQ.

Para obtener información sobre cómo acceder al shell AIQ UM Diag, consulte "Cómo acceder al shell de DIAG de máquina virtual Active IQ Unified Manager (OVA)"

- Pasos*

1. Inicie sesión en el terminal de mensajería unificada de AIQ y ejecute el siguiente comando para iniciar sesión en um.

```
um cli login -u <um maintenance user name>
```

ejemplo

```
um cli login -u admin
```

2. Ajuste la `imt_proxy_host` y.. `imt_proxy_port` ejecutando los siguientes comandos.

El proxy de IMT es una configuración independiente de las configuraciones de proxy de AutoSupport (ASUP).

```
um option set imt.https.proxy.host=<IMT_PROXY_HOST>
um option set imt.https.proxy.port=<IMT_PROXY_PORT>
```

ejemplo

```
um option set imt.https.proxy.host=example-proxy.cls.eng.com
um option set imt.https.proxy.port=8200
```

+

Las configuraciones del servidor proxy IMT no admiten la autenticación.

1. Consulte los detalles del proxy IMT para verificar el `proxy_host` y.. `proxy_port` los ajustes a través del comando siguiente.

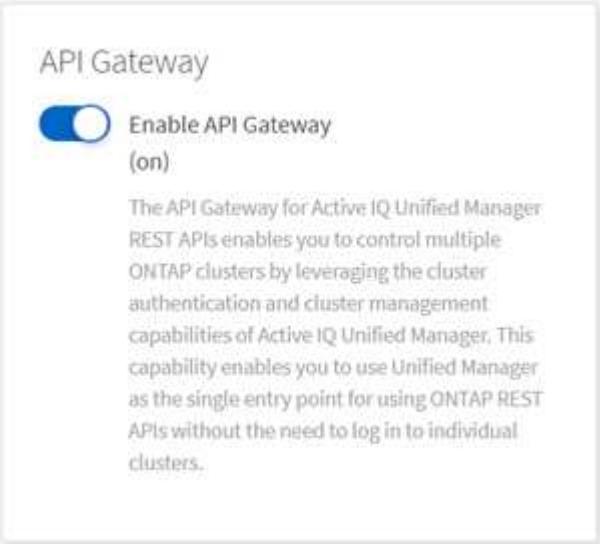
```
um option list |grep imt
```

Objetivos de reclamaciones

Una vez instalado Cisco Intersight Assist, puede solicitar los dispositivos de almacenamiento y virtualización de NetApp. Vuelva a la página **Intersight Targets** y añada sus destinos de Active IQ Unified Manager de vCenter y NetApp.

Asegúrese de que la puerta de enlace API de Active IQ Unified Manager (AIQ) de NetApp esté habilitada.

En NetApp IQ Unified Manager, vaya a **Configuración > General > Configuración de funciones**.



El siguiente ejemplo muestra el destino de mensajería unificada de NetApp AIQ para Cisco Intersight.

Cuando se solicita el destino de mensajería unificada de NetApp AIQ, todos los clústeres que gestiona Active IQ Unified Manager se añaden automáticamente a Intersight.

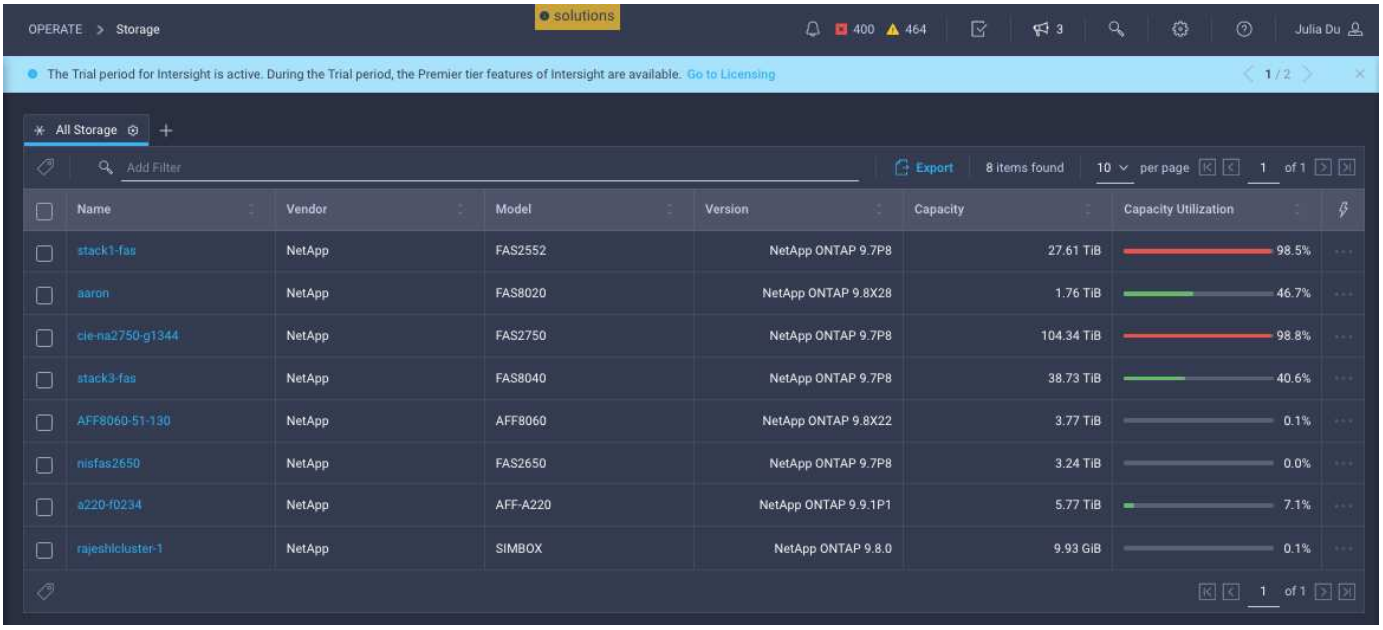


Supervise el almacenamiento de NetApp de Cisco Intersight

Después de reclamar los destinos, los widgets de almacenamiento de NetApp, el inventario de almacenamiento y las pestañas de virtualización quedan disponibles si dispone de una licencia de nivel Advantage. Hay pestañas de orquestación disponibles si tiene una licencia de nivel Premier.

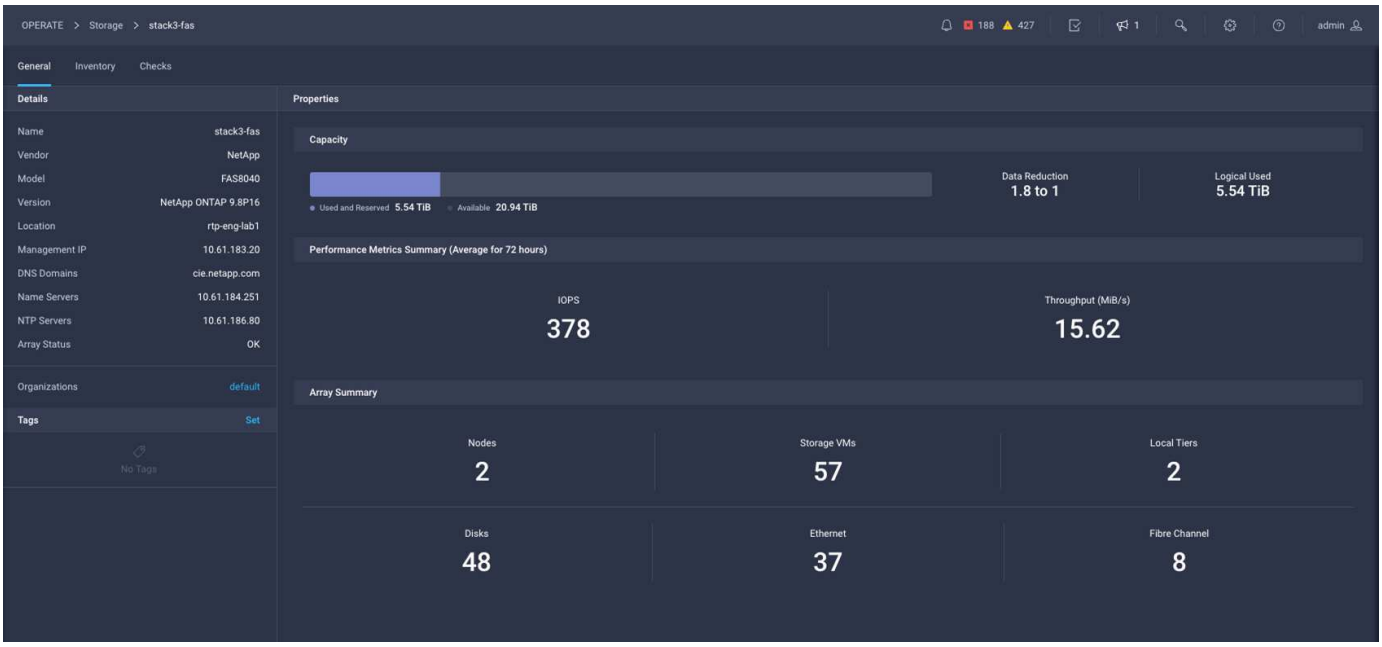
Información general del inventario de almacenamiento

La siguiente captura de pantalla muestra la pantalla **operar > almacenamiento**.



La siguiente captura de pantalla muestra la descripción general del clúster de almacenamiento.

La siguiente información de resumen de las métricas de rendimiento solo se muestra si la cabina de almacenamiento se supervisa mediante Active IQ Unified Manager 9.9 de NetApp o versiones posteriores.



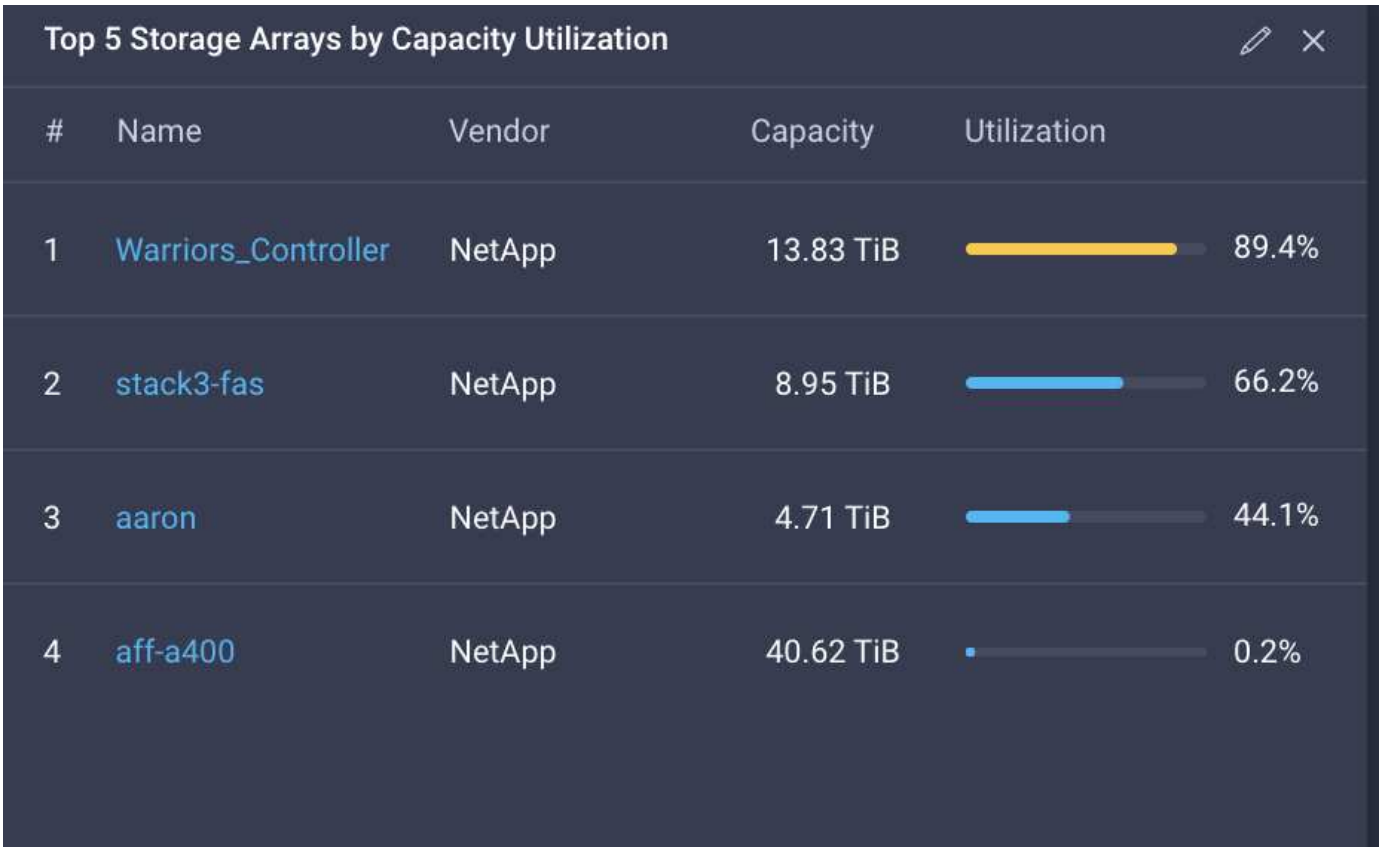
Widgets de almacenamiento

Para ver los widgets de almacenamiento, vaya a **Supervisión > Paneles > Ver widgets de almacenamiento de NetApp**.

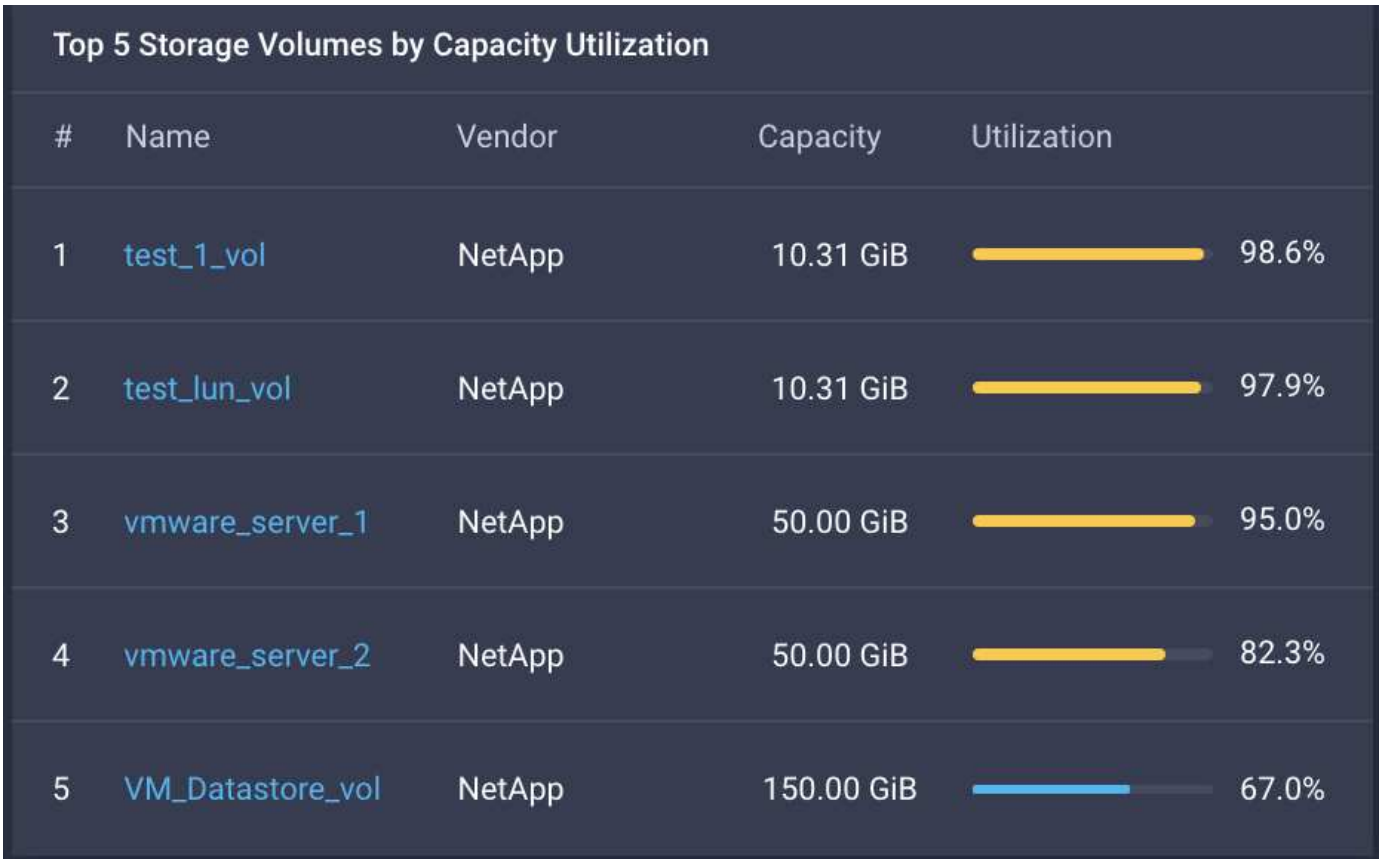
- La siguiente captura de pantalla muestra el widget Storage Version Summary.



- Esta captura de pantalla muestra el widget 5 principales cabinas de almacenamiento por aprovechamiento de la capacidad.



- Esta captura de pantalla muestra el widget 5 principales volúmenes de almacenamiento por utilización de la capacidad.



Casos de uso

Estos son algunos ejemplos de casos de uso para la supervisión y la orquestación del almacenamiento de NetApp de Cisco Intersight.

Caso de uso 1: Supervisión del inventario y los widgets de almacenamiento de NetApp

Si el entorno de almacenamiento de NetApp está disponible en Cisco Interview, puede supervisar los objetos de almacenamiento de NetApp de forma detallada desde el inventario de almacenamiento y obtener una descripción general de los widgets de almacenamiento.

1. Implemente el OVA de Intersight Assist (tarea OnPrem en el entorno de vCenter).
2. Añada dispositivos de mensajería unificada AIQ de NetApp en Intersight Assist.
3. Vaya a **Storage** y desplácese por el inventario de almacenamiento de NetApp.
4. Añada **Widgets** para almacenamiento de NetApp a su **Panel de monitores**.

Caso de uso 2: Orquestación de almacenamiento de NetApp mediante flujos de trabajo de referencia

Cuando los entornos de almacenamiento de NetApp y vCenter están disponibles en Cisco Intersight, puede utilizar los flujos de trabajo de referencia integrales disponibles en GitHub a través del "Repositorio de flujo de trabajo Intersight de FlexPod".

Los flujos de trabajo de referencia incluyen tareas de almacenamiento y virtualización. El archivo README del repositorio proporciona los requisitos previos necesarios para ejecutar flujos de trabajo, enlaces a recursos útiles (incluida la documentación sobre cómo importar un flujo de trabajo) y enlaces de documentación para cada flujo de trabajo de referencia.

Cada flujo de trabajo tiene una carpeta en el repositorio que contiene dos archivos:

- El archivo JSON para descargar e importar a Intersight,
- Archivo de documentación que proporciona una vista de las tareas del flujo de trabajo, entradas del flujo de trabajo y un ejemplo de ejecución del flujo de trabajo.

Realice lo siguiente para importar y utilizar un flujo de trabajo de referencia:

1. Implemente el OVA de Intersight Assist (tarea OnPrem en el entorno de vCenter).
2. Añada dispositivos de mensajería unificada AIQ de NetApp en Intersight Assist.
3. Añada el destino de vCenter a Intersight mediante Intersight Assist.
4. Descargue el archivo JSON para obtener un flujo de trabajo de referencia del repositorio de FlexPod-Intersight-Workflow.
5. Importe el flujo de trabajo a Intersight y, a continuación, ejecute el flujo de trabajo.

La siguiente es una lista de flujos de trabajo disponibles en el repositorio de GitHub FlexPod-Intersight-Workflow:

- Agregue iniciadores al iGroup de NetApp
- Nueva política de exportación para volúmenes de NetApp

- Nuevo almacén de datos NAS con el volumen inteligente de NetApp
- Nueva interfaz de datos de FC NetApp
- Nuevo iGroup de NetApp
- Nueva interfaz de datos de iSCSI de NetApp
- Nueva interfaz de datos NAS de NetApp
- Nuevo equipo virtual de almacenamiento de NetApp
- Nuevo almacén de datos de VMFS mediante la Smart LUN de NetApp
- Quite los iniciadores del iGroup de NetApp
- Elimine el almacén de datos NAS con el volumen inteligente de NetApp
- Eliminar Política de exportación de NetApp
- Quite el iGroup de NetApp
- Elimine el almacén de datos de VMFS mediante la Smart LUN de NetApp
- Actualice el almacén de datos NAS con el volumen inteligente de NetApp
- Actualice el almacén de datos de VMFS mediante la Smart LUN de NetApp

Caso de uso 3: Flujos de trabajo personalizados utilizando un formulario sin diseñador

Cuando haya disponibles los entornos de almacenamiento de NetApp y vCenter en Cisco Intersight, puede crear flujos de trabajo personalizados mediante las tareas de virtualización y almacenamiento de NetApp.

1. Implemente el OVA de Intersight Assist (tarea OnPrem en el entorno de vCenter)
2. Añada dispositivos de mensajería unificada AIQ de NetApp en Intersight Assist.
3. Añada un destino de vCenter a Intersight mediante Intersight Assist.
4. Desplácese hasta la ficha **orquestación** de Intersight.
5. Seleccione **Crear flujo de trabajo**.
6. Añada tareas de almacenamiento y virtualización a sus flujos de trabajo.

   Estas son las tareas de almacenamiento de NetApp que están disponibles en Cisco Intersight:

   - Añadir ACL a recurso compartido CIFS de NetApp
   - Agregar coincidencia de cliente a regla de política de exportación de NetApp
   - Añada una política de exportación a volumen NetApp
   - Agregue iniciadores al iGroup de NetApp
   - Agregar regla a la política de exportación de NetApp
   - Agregue programación a la política de snapshot de NetApp
   - Confirme el estado de la licencia de NetApp
   - Confirme el estado del protocolo FCP de la máquina virtual de almacenamiento NetApp
   - Editar agregados de NetApp para la máquina virtual de almacenamiento
   - Editar Política de SnapMirror asíncrono de NetApp
   - Editar permiso de ACL de uso compartido de CIFS de NetApp

- Editar regla de política de exportación de NetApp
- Editar política de snapshot de NetApp
- Editar la programación de política de snapshots de NetApp
- Editar el estilo de seguridad del volumen NetApp
- Editar la política de snapshots de volumen NetApp
- Habilite los servicios CIFS de NetApp
- Expanda NetApp LUN
- Nueva Política de SnapMirror asíncrono de NetApp
- Nuevo servidor CIFS de NetApp
- Nuevo recurso compartido CIFS de NetApp
- Busque Mapa de LUN de iGroup de NetApp
- Busque LUN de NetApp por ID
- Busque Volumen NetApp por ID
- Nueva política de exportación de NetApp
- Nueva interfaz de datos de FC NetApp
- Nuevo iGroup de NetApp
- Nueva interfaz de datos de iSCSI de NetApp
- Nuevos reflejos de uso compartido de carga de NetApp para el volumen raíz de SVM
- Nuevo LUN de NetApp
- Nuevo mapa de LUN de NetApp
- Nueva interfaz de datos NAS de NetApp
- Nuevo volumen inteligente NAS de NetApp
- Nuevo Smart LUN de NetApp
- Nueva relación de SnapMirror de NetApp para volumen
- Nueva política de copias Snapshot de NetApp
- Nuevo equipo virtual de almacenamiento de NetApp
- Nuevo volumen NetApp
- Nueva snapshot de volúmenes de NetApp
- Registrar DNS para la máquina virtual de almacenamiento de NetApp
- Eliminar ACL del recurso compartido CIFS de NetApp
- Eliminar coincidencia de cliente de regla de política de exportación de NetApp
- Quite la política de exportación de volúmenes NetApp
- Quite el iniciador del iGroup de NetApp
- Quite el servidor CIFS de NetApp
- Eliminar el recurso compartido CIFS de NetApp
- Eliminar Política de exportación de NetApp
- Quite la interfaz de datos de FC de NetApp

- Quite el iGroup de NetApp
- Elimine la interfaz IP de NetApp
- Elimine los reflejos de uso compartido de carga de NetApp para el volumen raíz de SVM
- Quite la LUN de NetApp
- Quite Mapa de LUN de NetApp
- Elimine el volumen inteligente del NAS de NetApp
- Eliminar NetApp Smart LUN
- Quite la relación de SnapMirror de NetApp para volumen
- Quitar la política de SnapMirror de NetApp
- Eliminar la política de snapshot de NetApp
- Quitar la máquina virtual de almacenamiento de NetApp
- Quite el volumen NetApp
- Quite una snapshot de volumen NetApp
- Eliminar regla de la política de exportación de NetApp
- Quitar programación de la política de snapshots de NetApp
- Cambie el nombre de NetApp Volume Snapshot
- Actualice los reflejos de uso compartido de carga de NetApp para el volumen raíz de SVM
- Actualice la capacidad del volumen NetApp

De almacenamiento

NVMe integral para FlexPod con Cisco UCSM, VMware vSphere 7.0 y ONTAP 9 de NetApp

TR-4914: NVMe integral para FlexPod con Cisco UCSM, VMware vSphere 7.0 y ONTAP 9 de NetApp

Chris Schmitt y Kamini Singh, NetApp

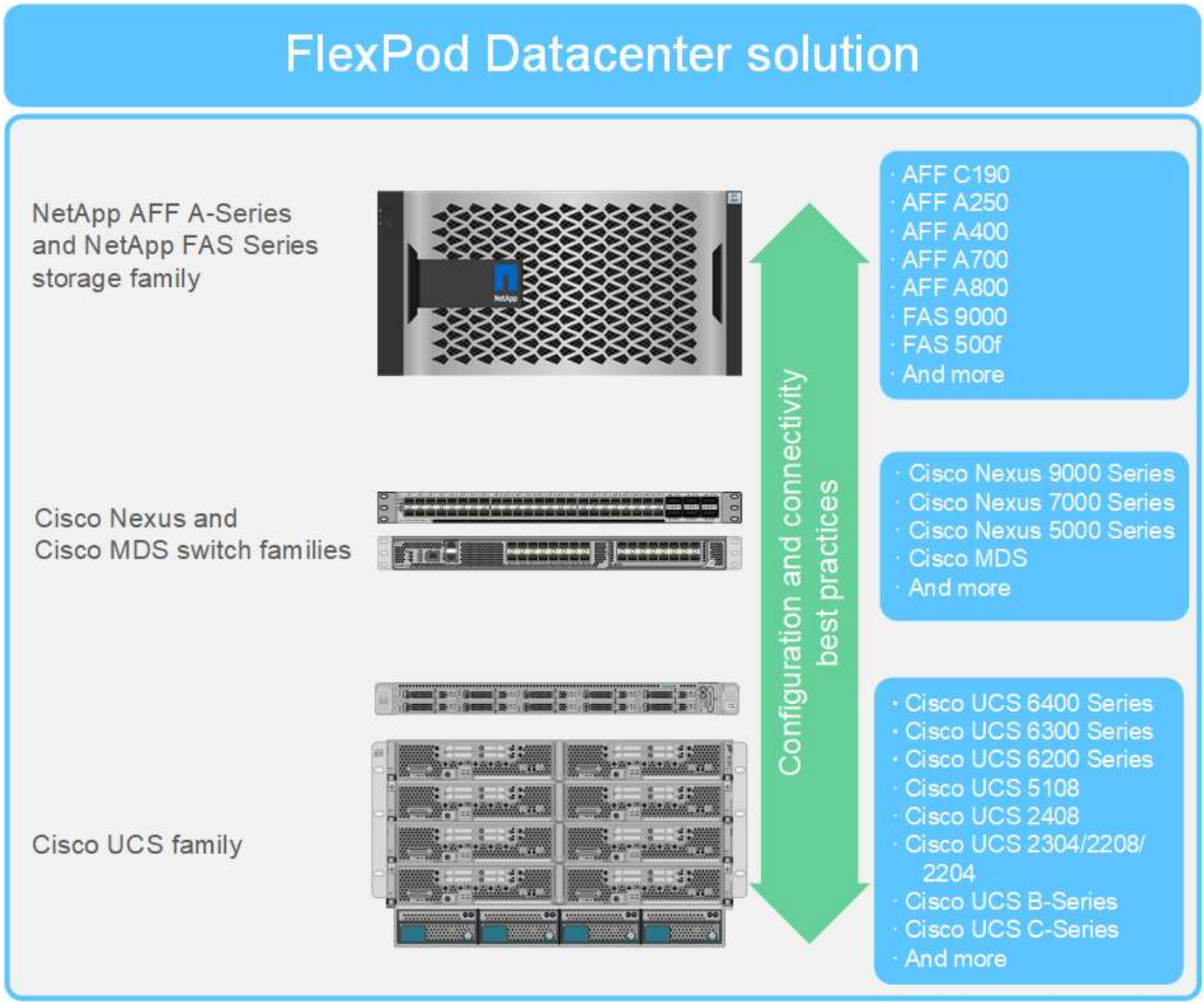
En colaboración con: 

El estándar de almacenamiento de datos NVMe, una tecnología central emergente, está transformando el acceso y el transporte al almacenamiento de datos empresariales ofreciendo un ancho de banda muy elevado y un acceso al almacenamiento de latencia muy baja para las tecnologías de memoria actuales y futuras. NVMe sustituye el conjunto de comandos SCSI por el conjunto de comandos NVMe.

NVMe se diseñó para funcionar con unidades flash no volátiles, CPU de varios núcleos y gigabytes de memoria. También aprovecha los importantes avances en informática desde la década de 1970, permitiendo conjuntos de comandos optimizados que analizan y manipulan datos de manera más eficiente. Una arquitectura NVMe integral también permite que los administradores de centros de datos se replanteen el grado en que pueden extender sus entornos virtualizados y en contenedores, y la cantidad de escalabilidad que admiten sus bases de datos orientadas a transacciones.

FlexPod es una arquitectura de centro de datos de mejores prácticas que incluye Unified Computing System (Cisco UCS), switches Cisco Nexus, switches Cisco MDS y sistemas AFF de NetApp. Estos componentes están conectados y configurados según las mejores prácticas de Cisco y NetApp, a fin de proporcionar una plataforma excelente para ejecutar diversas cargas de trabajo empresariales con total confianza. FlexPod se puede escalar verticalmente para obtener un rendimiento y una capacidad mayores (añadir recursos informáticos, de red o de almacenamiento de forma individual según sea necesario), o bien se puede escalar horizontalmente para los entornos que requieren múltiples puestas en marcha consistentes (por ejemplo, la implementación de pilas FlexPod adicionales).

La siguiente figura presenta las familias de componentes de FlexPod.



FlexPod es la plataforma perfecta para introducir FC-NVMe. Puede admitirá la adición de los servidores de montaje en rack Cisco UCS VIC 1400 y Port Expander en los servidores Cisco UCS B200 M5 o M6 existentes o Cisco UCS C-Series M5 o M6, así como actualizaciones de software sencillas y no disruptivas del sistema Cisco UCS, los switches Cisco MDS de 32 Gbps, Y las cabinas de almacenamiento AFF de NetApp. Una vez implementados el hardware y el software admitidos, la configuración de FC-NVMe es similar a la de FCP.

NetApp ONTAP 9.5 y versiones posteriores ofrecen una solución FC-NVMe completa. Gracias a una actualización del software de ONTAP no disruptiva para las cabinas AFF A300, AFF A400, AFF A700, AFF A700s y AFF A800, estos dispositivos son compatibles con una pila de almacenamiento NVMe integral. Por lo tanto, los servidores con adaptadores de bus de host (HBA) de sexta generación y compatibilidad con controladores NVMe pueden comunicarse con estas cabinas mediante NVMe nativo.

Objetivo

Esta solución proporciona un resumen general del rendimiento de FC-NVMe con VMware vSphere 7 en FlexPod. Se verificó que la solución traspase correctamente el tráfico FC-NVMe, y se capturaron las metricas de rendimiento para FC-NVMe con distintos tamaños de bloques de datos.

Ventajas de la solución

NVMe integral para FlexPod ofrece un valor excepcional a los clientes gracias a las siguientes ventajas soluciones:

- NVMe se basa en PCIe, un protocolo de hardware de alta velocidad y ancho de banda elevado que es sustancialmente más rápido que los estándares anteriores, como SCSI, SAS y SATA. Conectividad de latencia ultrabaja y de alto ancho de banda entre el servidor Cisco UCS y la cabina de almacenamiento de NetApp para la mayoría de las aplicaciones más exigentes.
- Una solución FC-NVMe no tiene pérdidas y puede gestionar los requisitos de escalabilidad de las aplicaciones de nueva generación. Entre estas nuevas tecnologías se incluyen la inteligencia artificial (IA), el aprendizaje automático (ML), el aprendizaje profundo (DL), los análisis en tiempo real y otras aplicaciones cruciales para la misión.
- Reduce el coste DE LA TECNOLOGÍA al utilizar de forma eficiente todos los recursos de la pila.
- Reduce drásticamente los tiempos de respuesta y aumenta el rendimiento de la aplicación, lo que se corresponde con un IOPS y un rendimiento mejorados con una latencia reducida. La solución ofrece un rendimiento ~60 % mayor y reduce la latencia en ~50 % para las cargas de trabajo existentes.
- FC-NVMe es un protocolo optimizado con excelentes funcionalidades de cola, especialmente en situaciones en las que hay más operaciones de I/o por segundo (IOPS; es decir, más transacciones) y actividades paralelas.
- Ofrece actualizaciones de software no disruptivas a los componentes de FlexPod como Cisco UCS, Cisco MDS y las cabinas de almacenamiento AFF de NetApp. No requiere ninguna modificación en las aplicaciones.

"Siguiente: Método de pruebas."

Método de prueba

"Anterior: Introducción."

Esta sección proporciona un resumen a grandes rasgos de las pruebas de validación FC-NVMe en FlexPod. Incluye tanto el entorno de pruebas/configuración como el plan de pruebas adoptado para realizar las pruebas de la carga de trabajo con respecto a FC-NVMe para FlexPod con VMware vSphere 7.

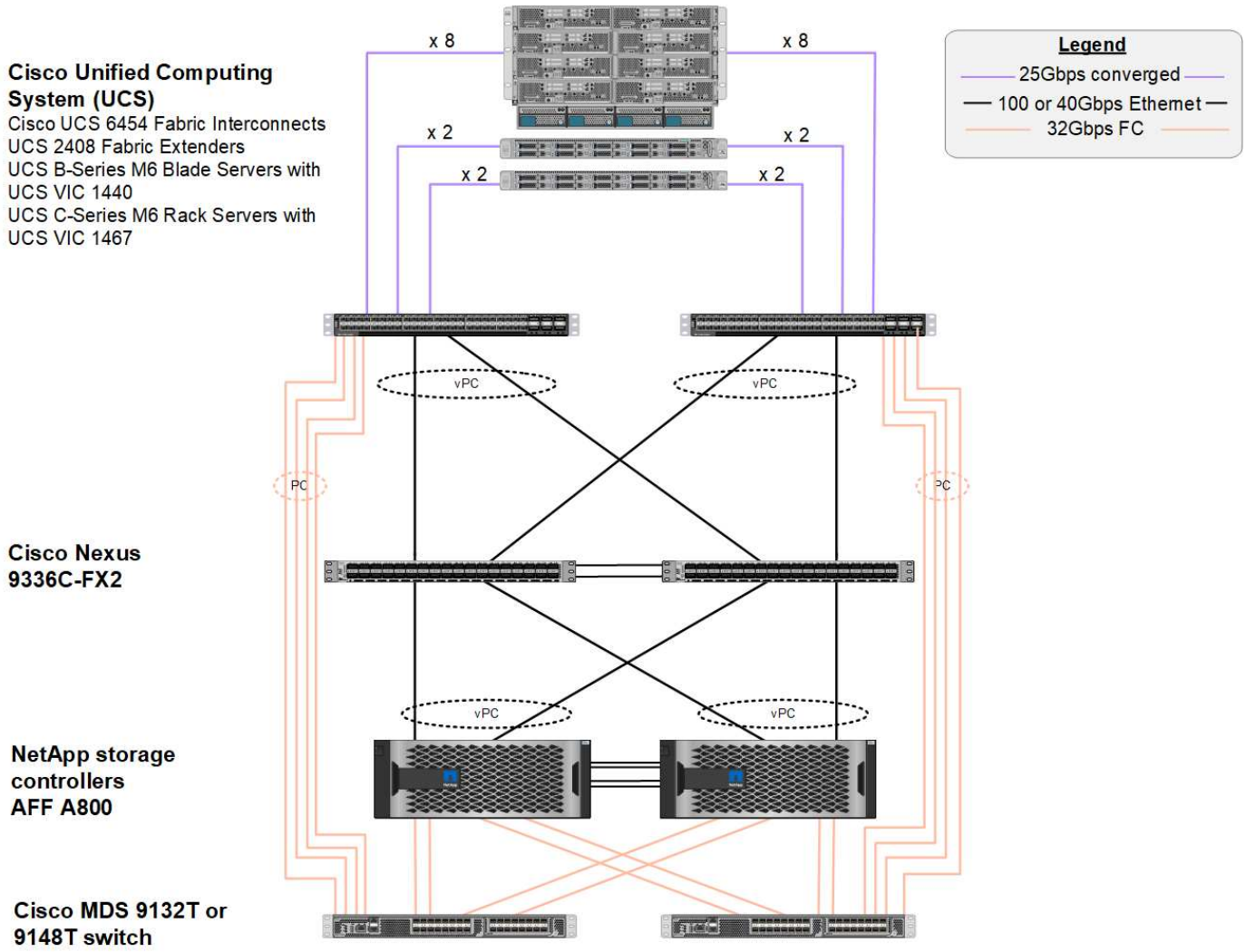
Entorno de pruebas

Los switches de la serie Cisco Nexus 9000 admiten dos modos de funcionamiento:

- Modo independiente NX-OS, con software Cisco NX-OS
- El modo de estructura ACI, con la plataforma Cisco Application Centric Infrastructure (Cisco ACI)

En el modo independiente, el switch funciona como un switch Cisco Nexus normal, con mayor densidad de puertos, baja latencia y conectividad de 40 GbE y 100 GbE.

FlexPod con NX-OS está diseñado para ser totalmente redundante en las capas informática, red y almacenamiento. No existe ningún punto único de error desde el punto de vista de un dispositivo o de una ruta de tráfico. La siguiente ilustración muestra la conexión de los distintos elementos del diseño de FlexPod más reciente utilizado en esta validación de FC-NVMe.



Desde la perspectiva DE SAN FC, este diseño utiliza las interconexiones de estructura Cisco UCS 6454 de cuarta generación más recientes y la plataforma Cisco UCS VICS 1400 con expansor de puertos en los servidores. Los servidores blade Cisco UCS B200 M6 en el chasis Cisco UCS utilizan el Cisco UCS VIC 1440 con expansión de puertos conectado al IOM de Cisco UCS 2408 Fabric extender y cada adaptador de bus de host virtual (Vhba) Fibre Channel sobre Ethernet (FCoE) tiene una velocidad de 40 Gbps. Los servidores en rack Cisco UCS C220 M5 gestionados por Cisco UCS utilizan Cisco UCS VIC 1457 con dos interfaces de 25 Gbps para cada interconexión de estructura. Cada Vhba FCoE C220 M5 tiene una velocidad de 50 Gbps.

Las interconexiones de estructura se conectan a través de canales de puertos SAN de 32 Gbps con los switches FC Cisco MDS 9148T o 9132T de última generación. La conectividad entre los switches Cisco MDS y el clúster de almacenamiento AFF A800 de NetApp también es FC de 32 Gbps. Esta configuración admite FC de 32 Gbps, para el protocolo Fibre Channel (FCP) y almacenamiento FC-NVMe entre el clúster de almacenamiento y Cisco UCS. Para esta validación, se utilizan cuatro conexiones FC a cada controladora de almacenamiento. En cada controladora de almacenamiento, los cuatro puertos FC se utilizan tanto para los protocolos FCP como FC-NVMe.

La conectividad entre los switches Cisco Nexus y el clúster de almacenamiento A800 de AFF de NetApp de última generación también es de 100 Gbps con canales de puertos en las controladoras de almacenamiento y los equipos virtuales de los switches. Las controladoras de almacenamiento AFF A800 de NetApp están equipadas con discos NVMe en el bus Peripheral Connect Interface Express (PCIe) de alta velocidad.

La implementación de FlexPod utilizada en esta validación se basa en "FlexPod Datacenter con Cisco UCS 4.2(1) en el modo gestionado de UCS, VMware vSphere 7.0U2 y NetApp ONTAP 9.9".

Hardware y software validados

En la siguiente tabla se enumeran las versiones de hardware y software que se utilizan durante el proceso de validación de la solución. Tenga en cuenta que Cisco y NetApp presentan matrices de interoperabilidad que deben hacerse referencia para determinar la compatibilidad con cualquier implantación específica de FlexPod. Para más información, consulte los siguientes recursos:

- "Herramienta de matriz de interoperabilidad de NetApp"
- "Herramienta de interoperabilidad de hardware y software Cisco UCS"

Capa	Dispositivo	Imagen	Comentarios
Informática	• Dos interconexiones de estructura Cisco UCS 6454 • Un chasis blade Cisco UCS 5108 con dos módulos I/o Cisco UCS 2408 • Cuatro blades Cisco UCS B200 M6, cada uno con un adaptador Cisco UCS VIC 1440 y una tarjeta de expansión de puerto	Versión 4.2(1f)	Incluye Cisco UCS Manager, Cisco UCS VIC 1440 y módulo de ampliación de puertos
CPU	Dos CPU Intel Xeon Gold 6330 a 2.0 GHz, con 42 MB de caché de capa 3 y 28 núcleos por CPU	–	–
Memoria	1024 GB (16 DIMM de 64 GB funcionando a 3200 MHz)	–	–
Red	Dos switches Cisco Nexus 9336C-FX2 en el modo independiente de NX-OS	Versión 9.3(8)	–
Red de almacenamiento	Dos switches FC de 32 puertos Cisco MDS 9132T de 32 Gbps	Versión 8.4 (2c)	Admite análisis SAN FC-NVMe
Reducida	Dos controladoras de almacenamiento AFF A800 de NetApp con 24 unidades SSD NVMe de 1,8 TB	ONTAP 9.9.1P1 de NetApp	–
De NetApp	Administrador de Cisco UCS	Versión 4.2(1f)	–
	VSphere de VMware	7.0U2	–
	VMware ESXi	7.0.2	–

Capa	Dispositivo	Imagen	Comentarios
	Controlador de NIC de Fibre Channel nativo de VMware ESXi (NFNIC)	5.0.0.12	Admite FC-NVMe en VMware
	Controlador NIC Ethernet nativo VMware ESXi (NNIC)	1.0.35.0	–
Herramienta de prueba	FIO	3.19	–

Plan de pruebas

Desarrollamos un plan de pruebas de rendimiento para validar NVMe en FlexPod con una carga de trabajo sintética. Esta carga de trabajo nos permitió ejecutar lecturas y escrituras aleatorias de 8 KB, así como lecturas y escrituras de 64 KB. Utilizamos hosts ESXi de VMware para ejecutar nuestros casos de prueba con el almacenamiento A800 de AFF.

Utilizamos fio, una herramienta de I/o sintética de código abierto que puede utilizarse para medir el rendimiento y generar nuestra carga de trabajo sintética.

Para completar nuestra prueba de rendimiento, realizamos diversos pasos de configuración tanto en el almacenamiento como en los servidores. A continuación se muestran los pasos detallados para la implementación:

1. Por lo que respecta al almacenamiento, creamos cuatro máquinas virtuales de almacenamiento (SVM, antes denominadas Vserver), ocho volúmenes por SVM y un espacio de nombres por volumen. Creamos volúmenes de 1 TB y espacios de nombres de 960 GB. Creamos cuatro LIF por SVM, así como un subsistema por SVM. Los LIF de SVM se distribuyeron de forma equitativa entre los ocho puertos FC disponibles del clúster.
2. En lo que respecta al servidor, creamos una única máquina virtual (VM) en cada uno de nuestros hosts ESXi, con un total de cuatro equipos virtuales. Instalamos FIO en nuestros servidores para ejecutar las cargas de trabajo sintéticas.
3. Después de configurar el almacenamiento y las máquinas virtuales, pudimos conectarse a los espacios de nombres de almacenamiento desde los hosts ESXi. Esto nos permitió crear almacenes de datos basados en nuestro espacio de nombres y, a continuación, crear discos de máquina virtual (VMDK) basados en dichos almacenes de datos.

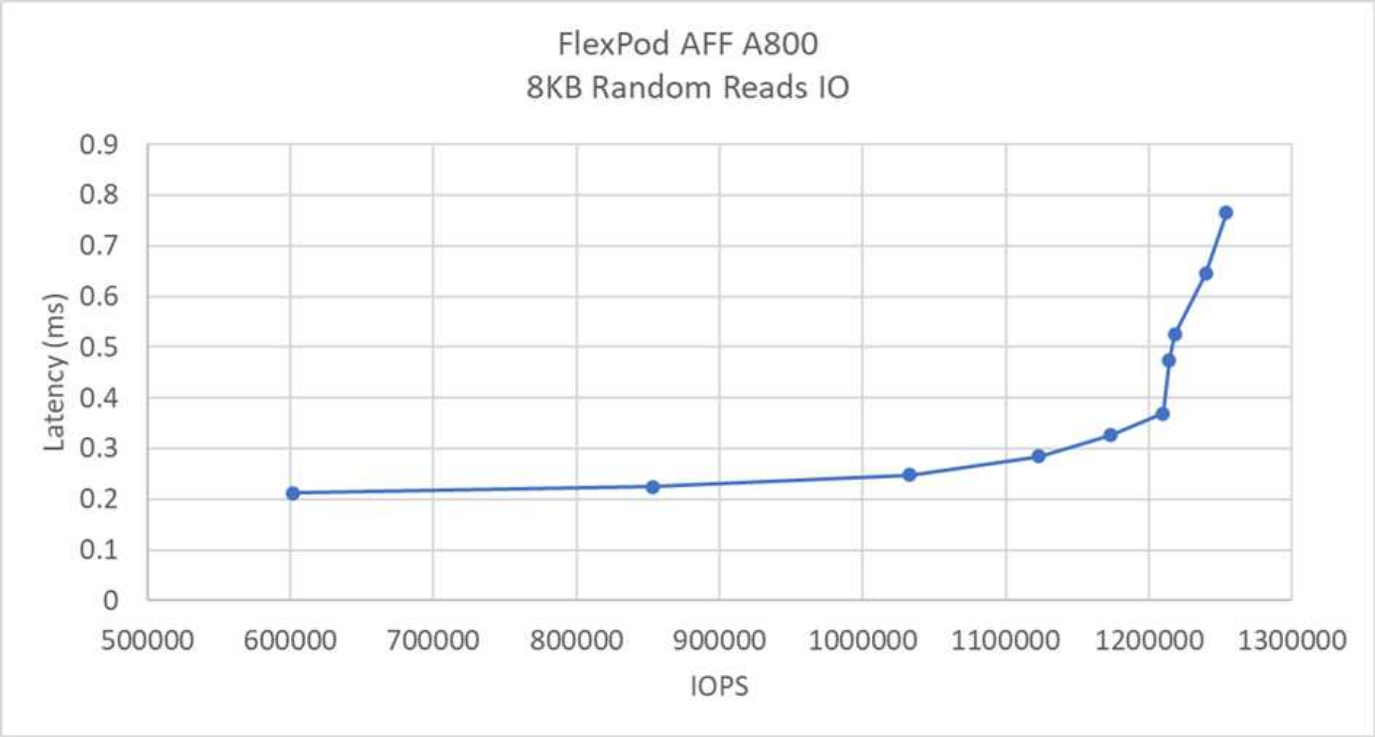
"Siguiente: Resultados de las pruebas."

Resultados de la prueba

"Anterior: Método de pruebas."

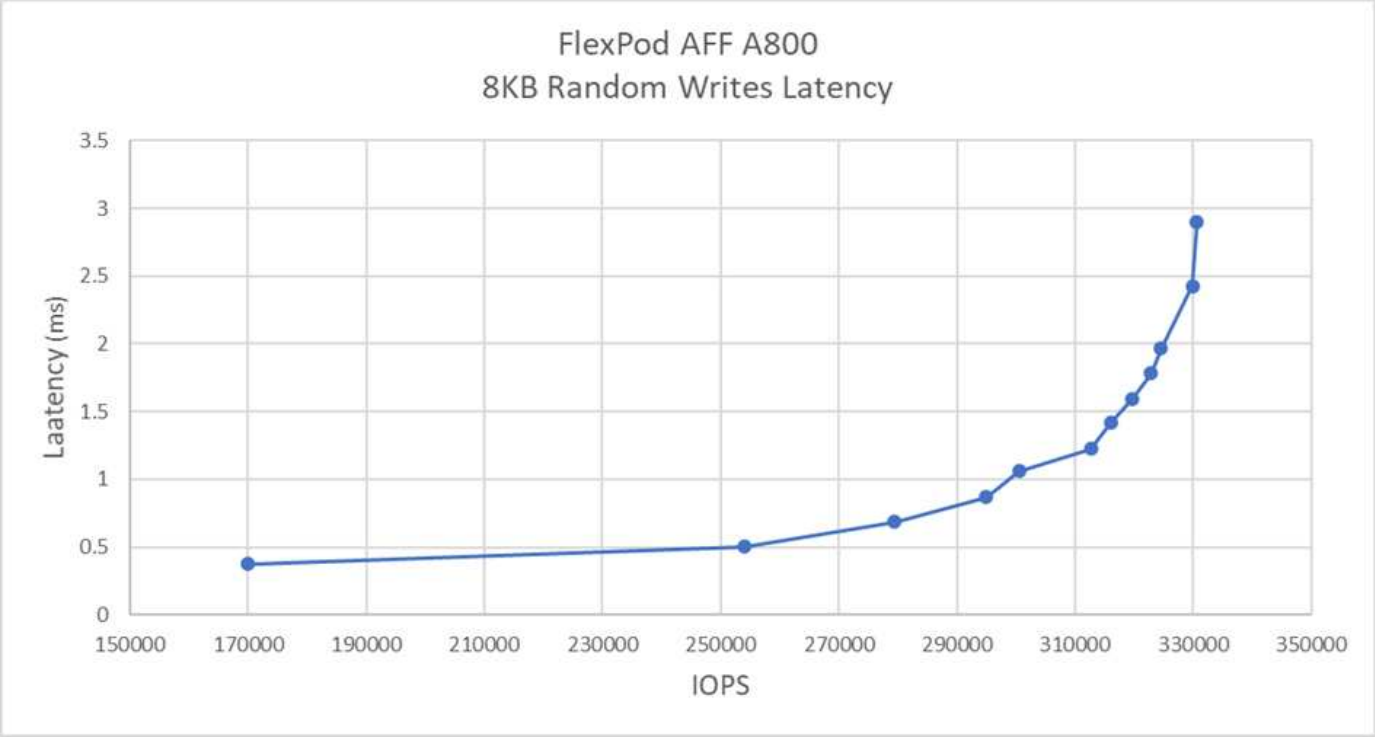
Las pruebas consistieron en ejecutar las cargas de trabajo de fio para medir el rendimiento de FC-NVMe en términos de IOPS y latencia.

En el siguiente gráfico se muestran nuestros resultados cuando se ejecuta una carga de trabajo de lectura aleatoria del 100 % utilizando bloques de 8 KB.



En nuestras pruebas, descubrimos que el sistema logró más de 1,2 millones de IOPS a la vez que mantuvo un nivel de latencia inferior a 0,35 ms en el lado del servidor.

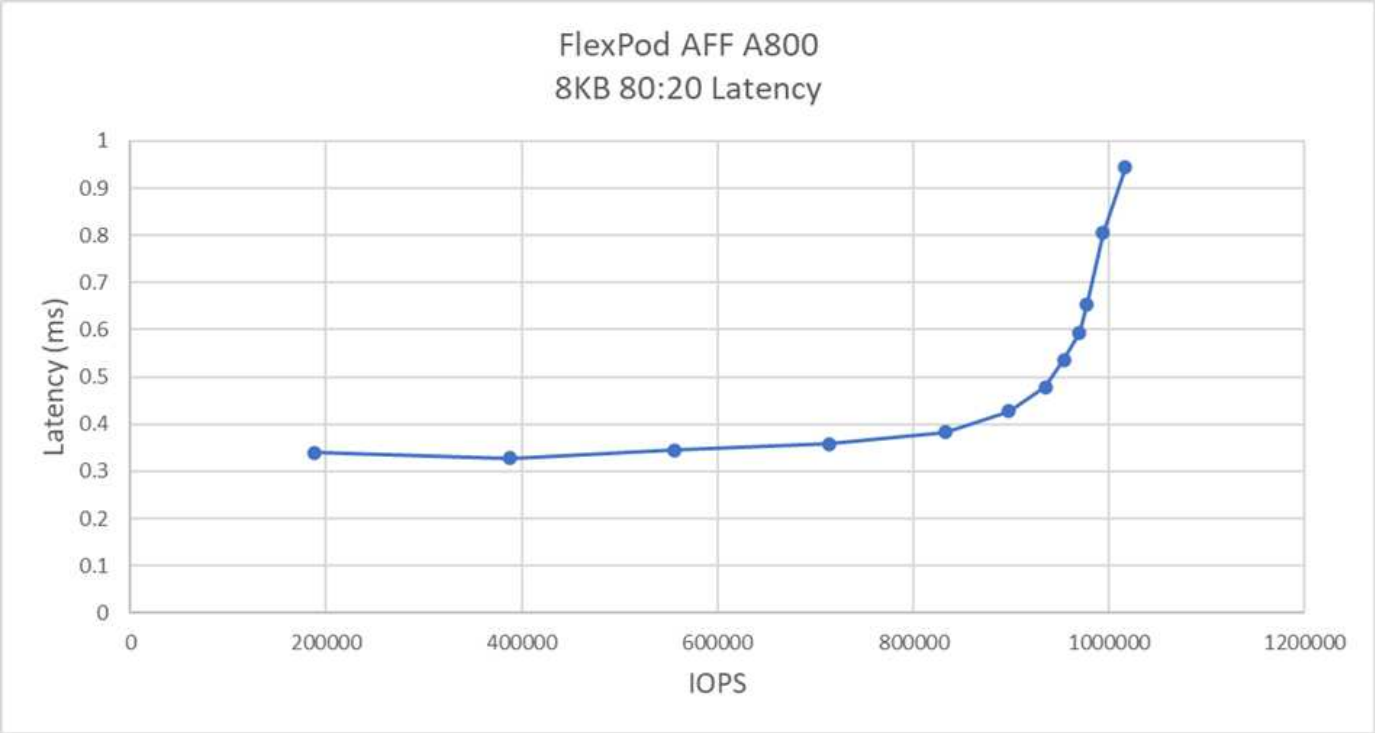
En el siguiente gráfico se muestran nuestros hallazgos al ejecutar una carga de trabajo de escritura aleatoria del 100 % utilizando tamaños de bloque de 8 KB.



En nuestras pruebas, descubrimos que el sistema alcanzó cerca de 300 000 IOPS, a la vez que mantiene solo menos de 1 ms de latencia en el lado del servidor.

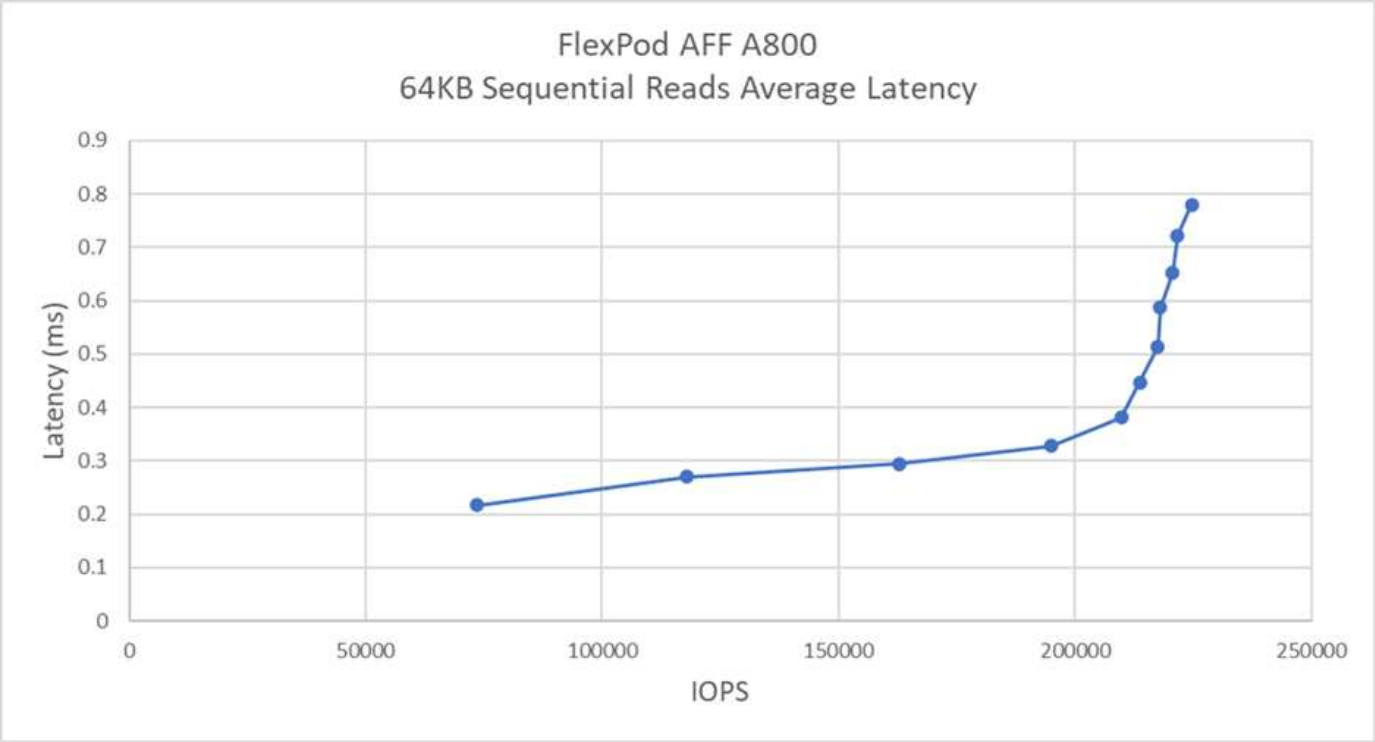
Para un tamaño de bloque de 8 KB con un 80 % de lecturas aleatorias y un 20 % de escrituras, hemos

observado los siguientes resultados:



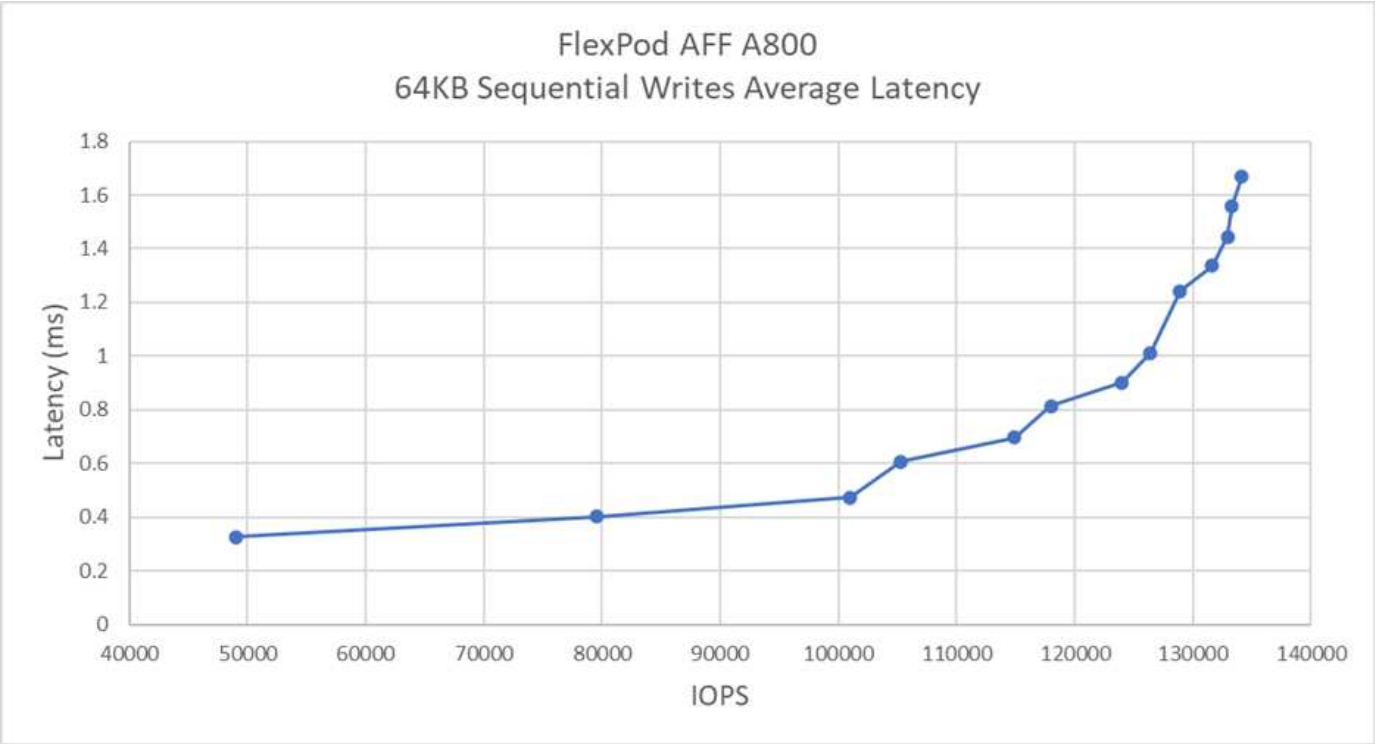
En nuestras pruebas, descubrimos que el sistema alcanzó más de 1 millón de IOPS, a la vez que mantiene solo menos de 1 ms de latencia en el lado del servidor.

Para un tamaño de bloque de 64 KB y un 100 % de lecturas secuenciales, observamos los siguientes resultados:



En nuestras pruebas, descubrimos que el sistema alcanzó alrededor de 250 000 IOPS, a la vez que mantiene una latencia de servidor inferior a 1 ms.

Para un tamaño de bloque de 64 KB y un 100 % de escrituras secuenciales, observamos los siguientes resultados:



En nuestras pruebas, descubrimos que el sistema alcanzó alrededor de 120 000 IOPS, a la vez que mantiene una latencia por debajo de 1 ms en el lado del servidor.

"Siguiente: Conclusión."

Conclusión

"Anterior: Resultados de la prueba."

El rendimiento observado para esta solución fue de 14 Gbps y 220 000 IOPS en una carga de trabajo de lectura secuencial por debajo de 1 ms de latencia. En el caso de cargas de trabajo de lectura aleatoria, alcanzamos un rendimiento de 9,5 Gbps y 1,25 MILLONES de IOPS. La capacidad de FlexPod para ofrecer este rendimiento con FC-NVMe puede satisfacer las necesidades de cualquier aplicación de misión crítica.

El centro de datos de FlexPod con VMware vSphere 7.0 U2 es la base de infraestructura compartida óptima para poner en marcha FC-NVMe para diversas cargas de trabajo DE TI, con lo que se ofrece acceso al almacenamiento de alto rendimiento para aplicaciones que lo requieran. A medida que FC-NVMe evoluciona para incluir alta disponibilidad, multivía y compatibilidad con sistemas operativos adicionales, FlexPod se adapta perfectamente a la plataforma preferida, lo que proporciona la escalabilidad y fiabilidad necesarias para respaldar estas funcionalidades.

Con FlexPod, Cisco y NetApp han creado una plataforma flexible y escalable para múltiples casos de uso y aplicaciones. Con FC-NVMe, FlexPod añade otra función para ayudar a las organizaciones a admitir de forma eficiente y eficaz aplicaciones vitales para el negocio que se ejecutan simultáneamente desde la misma infraestructura compartida. La flexibilidad y la escalabilidad de FlexPod también permiten a los clientes comenzar con una infraestructura del tamaño adecuado que puede crecer con los requisitos cambiantes del negocio y adaptarse a ellos.

Información adicional

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

- Sistema de computación unificada de Cisco (UCS)

  "http://www.cisco.com/en/US/products/ps10265/index.html"

- Especificaciones técnicas de las interconexiones de estructura Cisco UCS serie 6400

  "https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/datasheet-c78-741116.html"

- Chasis de servidor blade Cisco UCS serie 5100

  "http://www.cisco.com/en/US/products/ps10279/index.html"

- Servidores blade Cisco UCS serie B

  "http://www.cisco.com/en/US/partner/products/ps10280/index.html"

- Servidores en rack Cisco UCS serie C

  "http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-c-series-rack-servers/index.html"

- Adaptadores de Cisco Unified Computing System

  "http://www.cisco.com/en/US/products/ps10277/prod_module_series_home.html"

- Administrador de Cisco UCS

  "http://www.cisco.com/en/US/products/ps10281/index.html"

- Switches Cisco Nexus serie 9000

  "http://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/index.html"

- Switches de estructura multicapa Cisco MDS 9000

  "http://www.cisco.com/c/en/us/products/storage-networking/mds-9000-series-multilayer-switches/index.html"

- Cisco MDS 9132T conmutador Fibre Channel de 32 puertos y 32 Gbps

  "https://www.cisco.com/c/en/us/products/collateral/storage-networking/mds-9100-series-multilayer-fabric-switches/datasheet-c78-739613.html"

- ONTAP 9 de NetApp

  "http://www.netapp.com/us/products/platform-os/ontap/index.aspx"

- AFF A-Series de NetApp

  "http://www.netapp.com/us/products/storage-systems/all-flash-array/aff-a-series.aspx"

- VSphere de VMware

"https://www.vmware.com/products/vsphere"

- Servidor VMware vCenter

  "http://www.vmware.com/products/vcenter-server/overview.html"

- Prácticas recomendadas para SAN modernas

  "https://www.netapp.com/us/media/tr-4080.pdf"

- Presentamos NVMe integral para FlexPod

  "https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/whitepaper-c11-741907.html"

Matrices de interoperabilidad

- Herramienta de matriz de interoperabilidad de NetApp

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

- Matriz de compatibilidad de hardware de Cisco UCS

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

- Guía de compatibilidad de VMware

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

Reconocimientos

Los autores del proyecto agradecen a John George de Cisco y Scott Lane y Bobby Oommen de NetApp la asistencia y el asesoramiento ofrecidos durante la ejecución de este proyecto.

Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

Derechos de autor

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

"https://www.netapp.com/company/legal/trademarks/"

Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidad

"https://www.netapp.com/company/legal/privacy-policy/"

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.