



# Virtualización con VMware

## NetApp Solutions

NetApp  
May 10, 2024

# Tabla de contenidos

- Soluciones de NetApp para la virtualización con VMware de Broadcom ..... 1
  - Base de cloud de VMware ..... 1
  - Introducción a la automatización para ONTAP y vSphere ..... 140
  - Multicloud híbrido de NetApp con soluciones de VMware ..... 153
  - Casos de uso de multicloud híbrido de VMware ..... 153
  - Escritorios virtuales ..... 154
  - Cabina All-Flash SAN de NetApp con VMware vSphere 8 ..... 196
  - Demostraciones y tutoriales ..... 241

# Soluciones de NetApp para la virtualización con VMware de Broadcom

## Base de cloud de VMware

### VMware Cloud Foundation con cabinas SAN all-flash NetApp

Autor: Josh Powell

#### VMware Cloud Foundation con cabinas SAN all-flash NetApp

VMware Cloud Foundation (VCF) es una plataforma integrada de centro de datos definido por software (SDDC) que proporciona una pila completa de infraestructura definida por software para ejecutar aplicaciones empresariales en un entorno de cloud híbrido. Combina funcionalidades de computación, almacenamiento, redes y gestión en una plataforma unificada que ofrece una experiencia operativa consistente en clouds privados y públicos.

Este documento proporciona información sobre las opciones de almacenamiento disponibles para VMware Cloud Foundation mediante la cabina SAN all-flash de NetApp. Las opciones de almacenamiento admitidas se cubren con instrucciones específicas para poner en marcha almacenes de datos iSCSI como almacenamiento complementario para dominios de gestión y tanto almacenes de datos VVol (iSCSI) como NVMe/TCP como almacenes de datos complementarios para dominios de carga de trabajo. También se cubre la protección de datos de máquinas virtuales y almacenes de datos mediante SnapCenter para VMware vSphere.

#### Casos de uso

Casos de uso cubiertos en esta documentación:

- Opciones de almacenamiento para los clientes que buscan entornos uniformes tanto en clouds públicos como privados.
- Solución automatizada para poner en marcha infraestructura virtual para dominios de cargas de trabajo.
- Solución de almacenamiento escalable adaptada para satisfacer las necesidades en constante evolución, incluso cuando no se alinea directamente con los requisitos de recursos informáticos.
- Ponga en marcha el almacenamiento complementario en la gestión y en los dominios de cargas de trabajo de VI mediante ONTAP Tools para VMware vSphere.
- Proteger máquinas virtuales y almacenes de datos con el plugin de SnapCenter para VMware vSphere.

#### Destinatarios

Esta solución está dirigida a las siguientes personas:

- Arquitectos de soluciones que buscan opciones de almacenamiento más flexibles para entornos VMware diseñadas para maximizar el TCO.
- Arquitectos de soluciones que buscan opciones de almacenamiento VCF que ofrezcan opciones de protección de datos y recuperación ante desastres con los principales proveedores de cloud.
- Los administradores de almacenamiento que desean recibir instrucciones específicas sobre cómo configurar VCF con almacenamiento principal y complementario.
- Administradores de almacenamiento que desean instrucciones específicas sobre cómo proteger máquinas virtuales y almacenes de datos que residen en el almacenamiento de ONTAP.

## Visión general de la tecnología

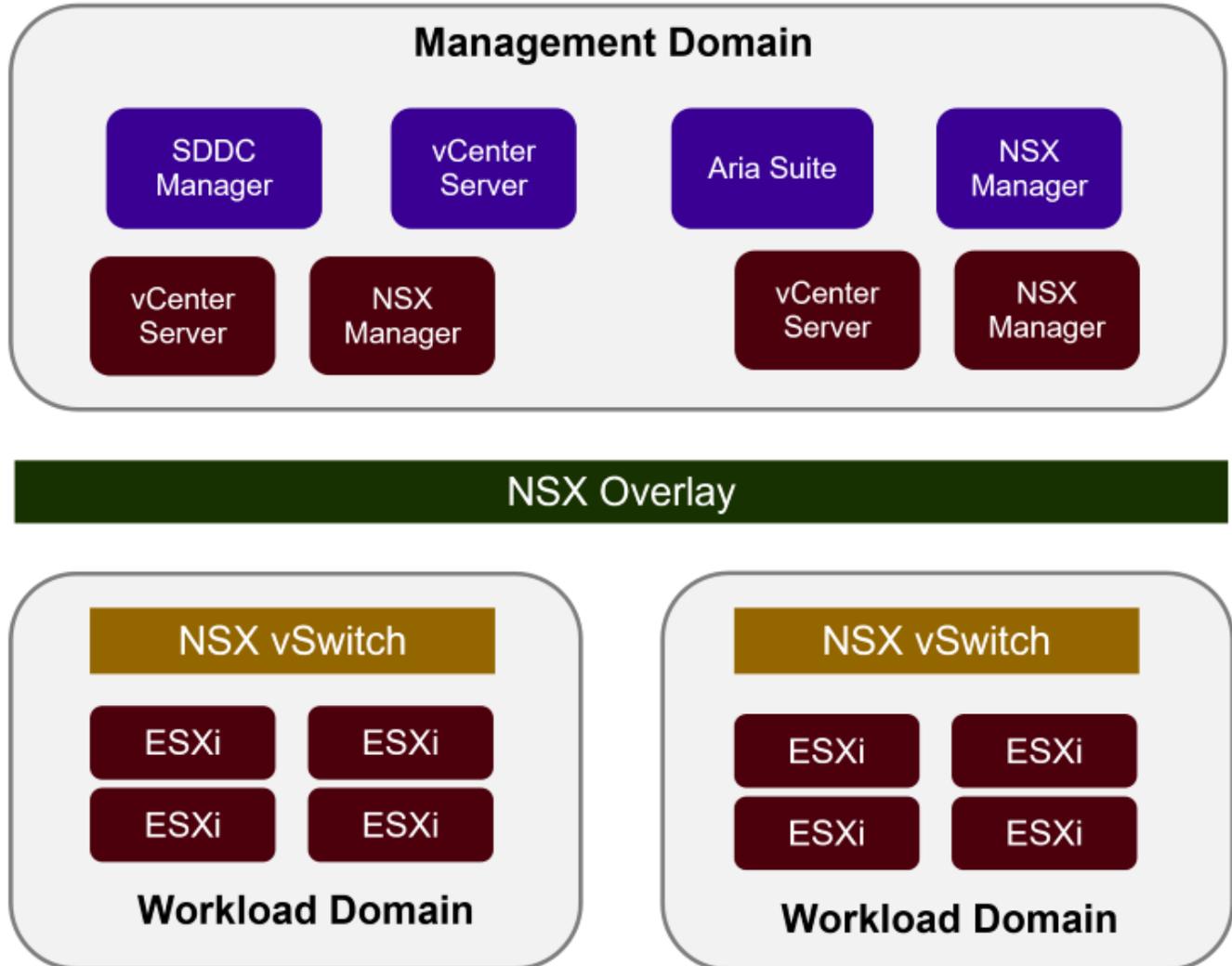
La solución VCF con NetApp ASA consta de los siguientes componentes principales:

### Base de cloud de VMware

VMware Cloud Foundation amplía las ofertas de hipervisores vSphere de VMware combinando componentes clave como SDDC Manager, vSphere, vSAN, NSX y VMware Aria Suite para crear un centro de datos definido por software.

La solución VCF es compatible tanto con cargas de trabajo nativas de Kubernetes como con máquinas virtuales. Los servicios clave como VMware vSphere, VMware vSAN, VMware NSX-T Data Center y VMware Aria Cloud Management son componentes integrales del paquete VCF. Al combinarse, estos servicios establecen una infraestructura definida por software capaz de gestionar con eficiencia la informática, el almacenamiento, las redes, la seguridad y la gestión del cloud.

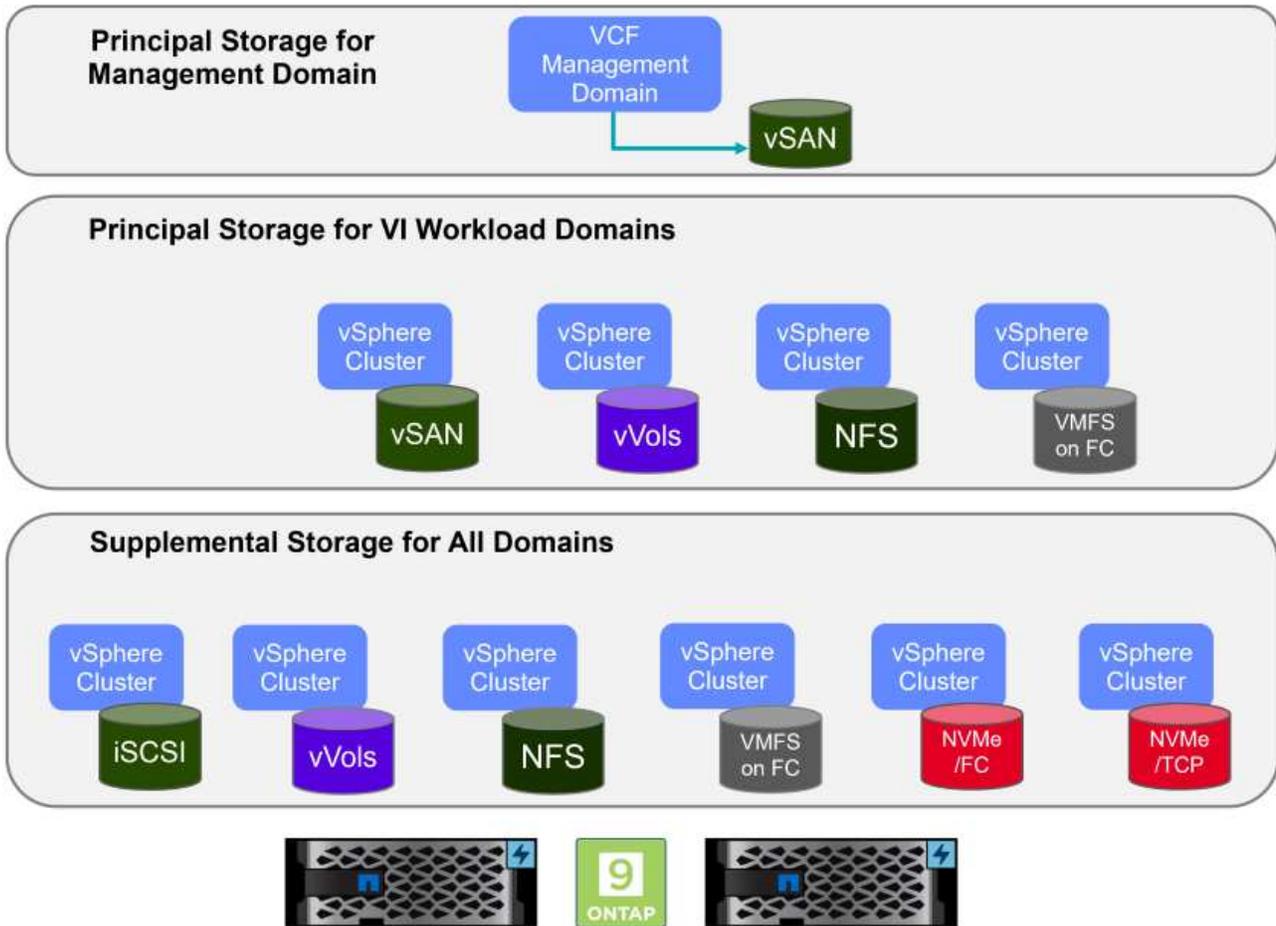
VCF se compone de un único dominio de gestión y hasta 24 dominios de carga de trabajo VI que cada uno representa una unidad de infraestructura lista para aplicaciones. Un dominio de carga de trabajo se compone de uno o más clústeres de vSphere que gestiona una única instancia de vCenter.



Para obtener más información sobre la arquitectura y planificación de VCF, consulte "[Modelos de arquitectura y tipos de dominio de carga de trabajo en VMware Cloud Foundation](#)".

## Opciones de almacenamiento de VCF

VMware divide las opciones de almacenamiento para VCF en almacenamiento **principal** y **suplementario**. El dominio de gestión de VCF debe utilizar vSAN como su almacenamiento principal. Sin embargo, existen muchas opciones de almacenamiento suplementarias para el dominio de gestión y las opciones de almacenamiento principal y suplementario disponibles para los dominios de carga de trabajo VI.



### Almacenamiento principal para dominios de carga de trabajo

El almacenamiento principal se refiere a cualquier tipo de almacenamiento que se puede conectar directamente a un dominio de carga de trabajo de VI durante el proceso de configuración dentro de SDDC Manager. El almacenamiento principal se pone en marcha con el administrador SDDC como parte de la orquestación de la creación de un clúster y es el primer almacén de datos configurado para un dominio de carga de trabajo. Incluye vSAN, vVols (VMFS), NFS y VMFS en Fibre Channel.

### Almacenamiento suplementario para dominios de gestión y carga de trabajo

El almacenamiento complementario es el tipo de almacenamiento que se puede añadir a los dominios de las cargas de trabajo o gestión en cualquier momento una vez que se ha creado el clúster. El almacenamiento complementario representa la gama más amplia de opciones de almacenamiento compatibles, que son compatibles con las cabinas de NetApp ASA. El almacenamiento complementario se puede poner en marcha usando herramientas de ONTAP para VMware vSphere para la mayoría de los tipos de protocolo de almacenamiento.

Recursos de documentación adicionales para VMware Cloud Foundation:

- \* ["Documentación de VMware Cloud Foundation"](#)
- \* ["Tipos de almacenamiento compatibles para VMware Cloud Foundation"](#)
- \* ["Gestión del almacenamiento en VMware Cloud Foundation"](#)

### Cabinas All-Flash SAN NetApp

La cabina all-flash SAN (ASA) de NetApp es una solución de almacenamiento de alto rendimiento diseñada para satisfacer los requisitos más exigentes de los centros de datos modernos. Combina la velocidad y la fiabilidad del almacenamiento flash con las funciones avanzadas de gestión de datos de NetApp para ofrecer un rendimiento, una escalabilidad y una protección de datos excepcionales.

La gama ASA está compuesta por los modelos A-Series y C-Series.

Las cabinas flash all-NVMe NetApp A-Series están diseñadas para cargas de trabajo de alto rendimiento, con una latencia ultrabaja y una alta resiliencia, lo que las convierte en adecuadas para aplicaciones de misión crítica.



Las cabinas flash QLC de C-Series se dirigen a casos de uso de mayor capacidad, y ofrecen la velocidad de la tecnología flash con la economía del flash híbrido.



Para obtener información detallada, consulte ["Página de destino de NetApp ASA"](#).

### Compatibilidad con protocolos de almacenamiento

ASA admite todos los protocolos SAN estándar, incluidos iSCSI, Fibre Channel (FC), Fibre Channel sobre Ethernet (FCoE) y NVMe over Fabrics.

**iSCSI** - NetApp ASA proporciona una sólida compatibilidad con iSCSI, lo que permite el acceso a nivel de bloque a dispositivos de almacenamiento a través de redes IP. Ofrece una integración perfecta con iniciadores

iSCSI, lo que permite aprovisionar y gestionar LUN iSCSI de manera eficaz. Funciones avanzadas de ONTAP, como rutas múltiples, autenticación CHAP y compatibilidad con ALUA.

Para obtener directrices de diseño sobre configuraciones de iSCSI, consulte la ["Documentación de referencia de configuración de SAN"](#).

**Canal de fibra** - NetApp ASA ofrece soporte integral para el canal de fibra (FC), una tecnología de red de alta velocidad comúnmente utilizada en redes de área de almacenamiento (SAN). ONTAP se integra sin problemas con la infraestructura de FC y proporciona un acceso por bloques fiable y eficiente a los dispositivos de almacenamiento. Ofrece funciones como la división en zonas, las rutas múltiples y el inicio de sesión estructural (FLOGI) para optimizar el rendimiento, mejorar la seguridad y garantizar una conectividad perfecta en entornos FC.

Para obtener directrices de diseño sobre configuraciones de Fibre Channel, consulte ["Documentación de referencia de configuración de SAN"](#).

**NVMe over Fabrics** - NetApp ONTAP y ASA admiten NVMe over Fabrics. NVMe/FC permite utilizar dispositivos de almacenamiento NVMe sobre infraestructura Fibre Channel y NVMe/TCP sobre redes IP de almacenamiento.

Para obtener directrices de diseño en NVMe, consulte ["Configuración, compatibilidad y limitaciones de NVMe"](#)

## Tecnología activo-activo

Las cabinas NetApp All-Flash SAN permiten rutas activo-activo que pasan por ambas controladoras, por lo que no es necesario que el sistema operativo host espere a que se produzca un error en una ruta activa antes de activar la ruta alternativa. Esto significa que el host puede utilizar todas las rutas disponibles en todas las controladoras, asegurando que las rutas activas siempre estén presentes sin importar si el sistema está en estado constante o si se debe someter a una operación de conmutación por error de la controladora.

Además, NetApp ASA ofrece una función distintiva que mejora significativamente la velocidad de la conmutación por error de SAN. Cada controladora replica continuamente los metadatos LUN esenciales con su asociado. Como resultado, cada controladora está preparada para asumir las responsabilidades del servicio de datos en caso de un fallo repentino de su compañero. Esta preparación es posible debido a que la controladora ya posee la información necesaria para comenzar a utilizar las unidades que se gestionaron previamente por la controladora con el error.

Con rutas activo-activo, las tomas de control planificadas y sin planificar tienen tiempos de reanudación de I/O de 2-3 segundos.

Para obtener más información, consulte ["TR-4968, cabina All-SAS NetApp: Disponibilidad e integridad de los datos con NetApp ASA"](#).

## Garantías de almacenamiento

NetApp ofrece un conjunto único de garantías de almacenamiento con cabinas SAN All-Flash NetApp. Sus ventajas únicas incluyen:

- **Garantía de eficiencia de almacenamiento:** \* Consiga un alto rendimiento al tiempo que minimiza el costo de almacenamiento con la Garantía de Eficiencia de Almacenamiento. 4:1 para cargas de trabajo SAN.

**Garantía de disponibilidad de datos de 6 Nines (99,9999%):** garantiza la corrección de los tiempos de inactividad no planificados en más de 31,56 segundos al año.

**Garantía de recuperación de ransomware:** Recuperación de datos garantizada en caso de un ataque de ransomware.

Consulte ["Portal de productos de NetApp ASA"](#) si quiere más información.

### **Herramientas de ONTAP de NetApp para VMware vSphere**

Las herramientas de ONTAP para VMware vSphere permiten a los administradores gestionar el almacenamiento de NetApp directamente desde vSphere Client. ONTAP Tools permite poner en marcha y gestionar almacenes de datos, así como aprovisionar almacenes de datos VVOL.

Herramientas ONTAP permite la asignación de almacenes de datos a perfiles de capacidades de almacenamiento que determinan un conjunto de atributos del sistema de almacenamiento. Esto permite la creación de almacenes de datos con atributos específicos como el rendimiento del almacenamiento y la calidad de servicio.

Las herramientas de ONTAP también incluyen un proveedor de API de VMware vSphere para el conocimiento del almacenamiento (VASA)\* para sistemas de almacenamiento de ONTAP, que permite el aprovisionamiento de almacenes de datos de VMware Virtual Volumes (vVols), la creación y el uso de perfiles de capacidades de almacenamiento, la verificación de cumplimiento y la supervisión del rendimiento.

Para obtener más información sobre las herramientas de NetApp ONTAP, consulte la ["Herramientas de ONTAP para documentación de VMware vSphere"](#) página.

### **Plugin de SnapCenter para VMware vSphere**

El plugin de SnapCenter para VMware vSphere (SCV) es una solución de software de NetApp que ofrece una protección de datos completa para entornos VMware vSphere. Está diseñado para simplificar y agilizar el proceso de protección y gestión de máquinas virtuales y almacenes de datos. SCV utiliza almacenamiento Snapshot y replicación a cabinas secundarias para cumplir objetivos de tiempo de recuperación reducidos.

El plugin de SnapCenter para VMware vSphere ofrece las siguientes funcionalidades en una interfaz unificada, integrada con el cliente de vSphere:

**Instantáneas basadas en políticas** - SnapCenter le permite definir políticas para crear y administrar instantáneas consistentes con aplicaciones de máquinas virtuales (VM) en VMware vSphere.

- Automatización \* - La creación y gestión automatizada de instantáneas basadas en políticas definidas ayudan a garantizar una protección de datos consistente y eficiente.

**VM-Level Protection** - La protección granular a nivel de VM permite una gestión y recuperación eficientes de máquinas virtuales individuales.

- Características de eficiencia del almacenamiento \* - La integración con las tecnologías de almacenamiento de NetApp proporciona funciones de eficiencia del almacenamiento como deduplicación y compresión para instantáneas, minimizando los requisitos de almacenamiento.

El complemento de SnapCenter orquesta el modo inactivo de máquinas virtuales junto con los snapshots basados en hardware en las cabinas de almacenamiento de NetApp. La tecnología SnapMirror se utiliza para replicar copias de backups en sistemas de almacenamiento secundarios, incluso en el cloud.

Para obtener más información, consulte ["Documentación del plugin de SnapCenter para VMware vSphere"](#).

La integración de BlueXP habilita estrategias de backup de 3-2-1 que amplían las copias de datos en el almacenamiento de objetos en el cloud.

Para obtener más información sobre estrategias de backup 3-2-1 con BlueXP, visita ["3-2-1 Protección de datos para VMware con complemento SnapCenter y backup y recuperación de datos de BlueXP para máquinas virtuales"](#).

## Descripción general de la solución

Los escenarios presentados en esta documentación mostrarán cómo usar sistemas de almacenamiento de ONTAP como almacenamiento complementario para dominios de cargas de trabajo y gestión. Además, el plugin de SnapCenter para VMware vSphere se utiliza para proteger máquinas virtuales y almacenes de datos.

Escenarios cubiertos en esta documentación:

- **Utilice las herramientas de ONTAP para implementar almacenes de datos iSCSI en un dominio de administración de VCF.** Haga clic en ["aquí"](#) para pasos de despliegue.
- **Utilice las herramientas de ONTAP para implementar almacenes de datos vVols (iSCSI) en un dominio de carga de trabajo VI.** Haga clic en ["aquí"](#) para pasos de despliegue.
- **Configurar almacenes de datos NVMe sobre TCP para su uso en un dominio de carga de trabajo VI.** Haga clic en ["aquí"](#) para pasos de despliegue.
- \* Implementar y utilizar el complemento de SnapCenter para VMware vSphere para proteger y restaurar máquinas virtuales en un dominio de carga de trabajo VI\*. Haga clic en ["aquí"](#) para pasos de despliegue.

## Utilice las herramientas de ONTAP para configurar el almacenamiento complementario para los dominios de gestión de VCF

Autor: Josh Powell

Utilice las herramientas de ONTAP para configurar el almacenamiento complementario para los dominios de gestión de VCF

### Descripción general del escenario

En esta situación, mostraremos cómo poner en funcionamiento y utilizar las herramientas de ONTAP para VMware vSphere (OTV) a fin de configurar un almacén de datos iSCSI para un dominio de gestión de VCF.

Este escenario cubre los siguientes pasos de alto nivel:

- Cree una máquina virtual de almacenamiento (SVM) con interfaces lógicas (LIF) para el tráfico de iSCSI.
- Cree grupos de puertos distribuidos para las redes iSCSI en el dominio de gestión de VCF.
- Cree adaptadores vmkernel para iSCSI en los hosts ESXi para el dominio de gestión de VCF.
- Implemente las herramientas de ONTAP en el dominio de gestión de VCF.
- Cree un nuevo almacén de datos VMFS en el dominio de gestión de VCF.

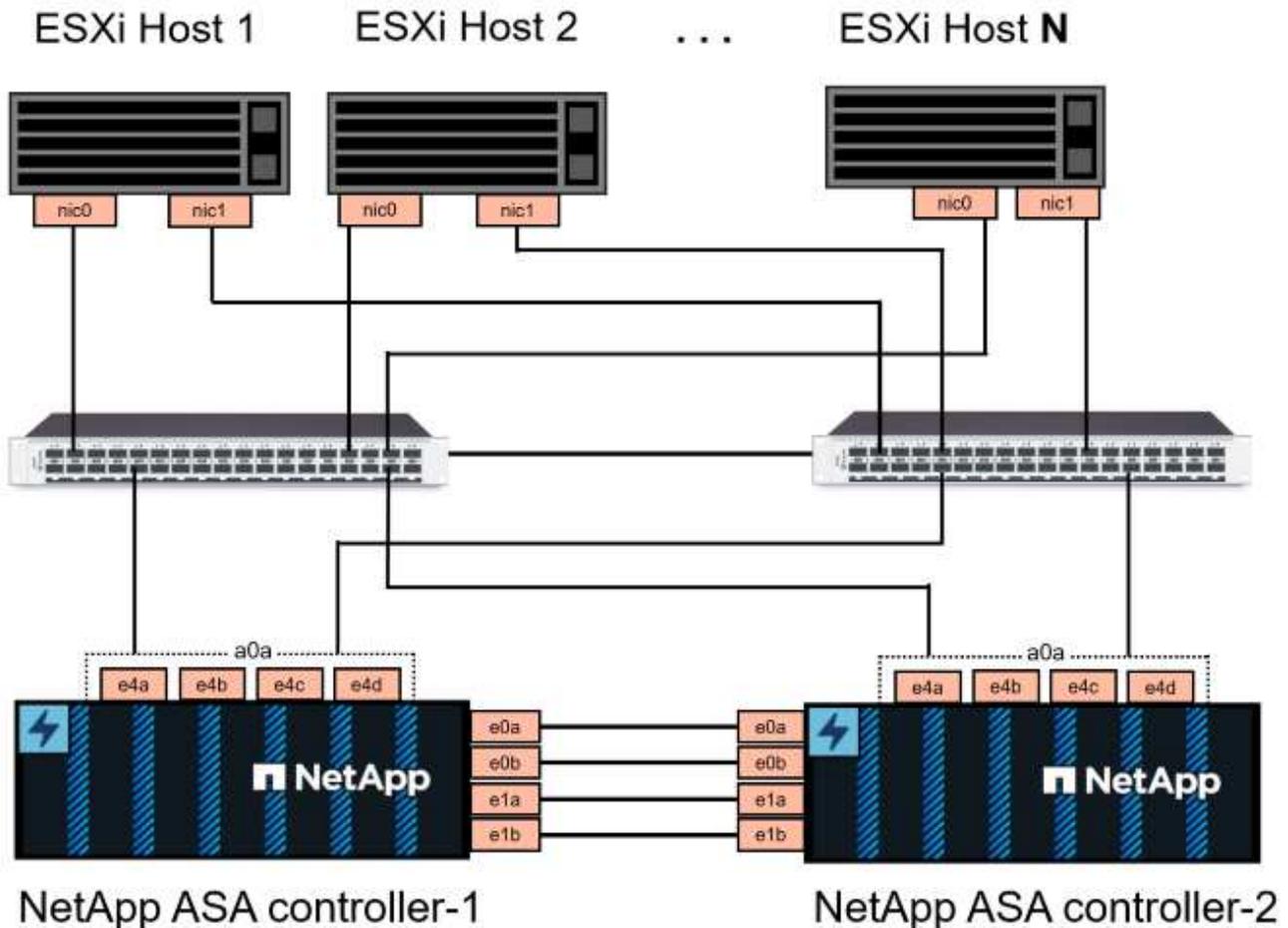
### Requisitos previos

Este escenario requiere los siguientes componentes y configuraciones:

- Un sistema de almacenamiento de ONTAP ASA con puertos de datos físicos en switches ethernet dedicados al tráfico de almacenamiento.

- La puesta en marcha del dominio de gestión de VCF está completa y se puede acceder al cliente vSphere.

NetApp recomienda diseños de red completamente redundantes para iSCSI. En el siguiente diagrama se muestra un ejemplo de una configuración redundante, que proporciona tolerancia a fallos para los sistemas de almacenamiento, los switches, los adaptadores de red y los sistemas host. Consulte NetApp ["Referencia para la configuración DE SAN"](#) para obtener más información.



Para la multivía y la conmutación al respaldo en varias rutas, NetApp recomienda tener un mínimo de dos LIF por nodo de almacenamiento en redes ethernet independientes para todas las SVM en configuraciones de iSCSI.

Esta documentación muestra el proceso de crear una SVM nueva y especificar la información de dirección IP para crear varias LIF para el tráfico de iSCSI. Para agregar LIF nuevos a una SVM existente, consulte ["Crear una LIF \(interfaz de red\)"](#).

Para obtener información adicional sobre el uso de almacenes de datos VMFS iSCSI con VMware, consulte ["Almacén de datos VMFS de vSphere: Entorno de administración del almacenamiento iSCSI con ONTAP"](#).



En situaciones en las que se configuran varios adaptadores VMkernel en la misma red IP, se recomienda utilizar el enlace de puerto iSCSI de software en los hosts ESXi para garantizar el equilibrio de carga entre los adaptadores. Consulte el artículo de la base de conocimientos ["Consideraciones sobre el uso de la vinculación de puertos iSCSI de software en ESX/ESXi \(2038869\)"](#).

## **Pasos de despliegue**

Para implementar las herramientas de ONTAP y utilizarlo para crear un almacén de datos VMFS en el dominio de gestión de VCF, lleve a cabo los siguientes pasos:

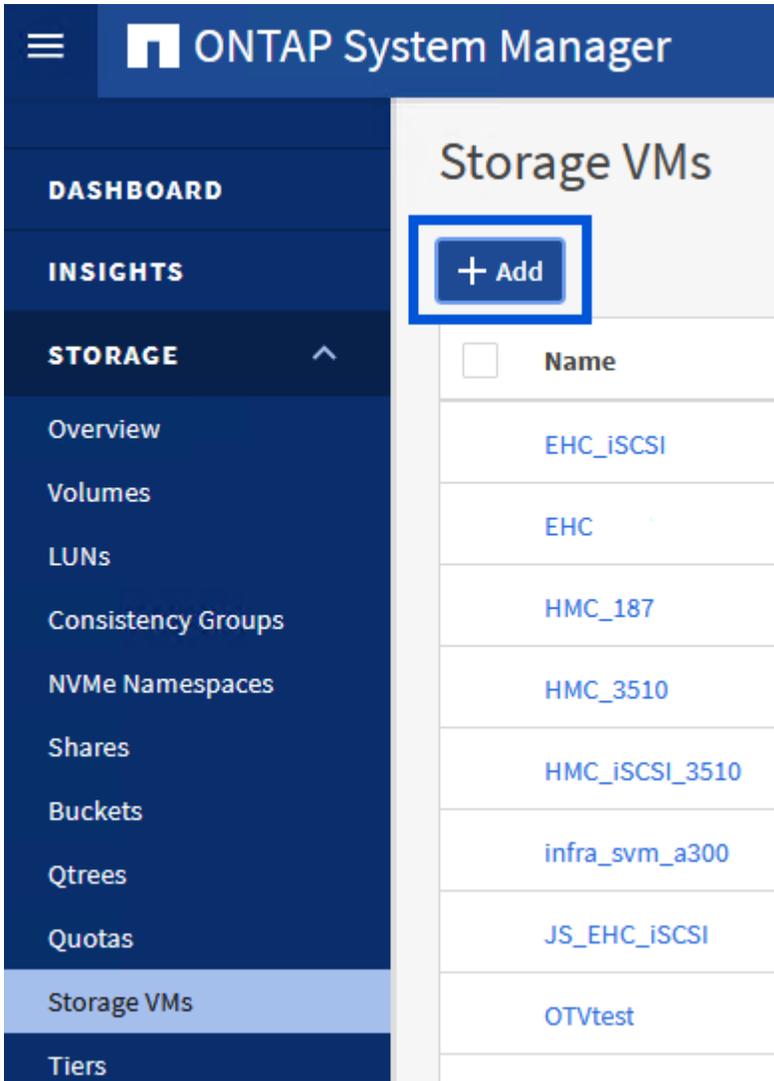
### **Crear SVM y LIF en el sistema de almacenamiento ONTAP**

El siguiente paso se lleva a cabo en ONTAP System Manager.

## Crear la máquina virtual de almacenamiento y las LIF

Complete los siguientes pasos para crear una SVM junto con varios LIF para el tráfico de iSCSI.

1. Desde el Administrador del sistema de ONTAP navegue hasta **VM de almacenamiento** en el menú de la izquierda y haga clic en **+ Agregar** para comenzar.



2. En el asistente de **Add Storage VM**, proporcione un **Name** para la SVM, seleccione **IP Space** y, a continuación, en **Access Protocol**, haga clic en la pestaña **\*iSCSI** y marque la casilla **Enable iSCSI**.

## Add Storage VM



STORAGE VM NAME

SVM\_ISCSI

IPSPACE

Default

### Access Protocol

SMB/CIFS, NFS, S3

iSCSI

FC

NVMe

Enable iSCSI

3. En la sección **Interfaz de red**, rellena la **Dirección IP**, **Máscara de subred** y **Dominio de difusión y puerto** para la primera LIF. En el caso de LIF posteriores, la casilla de verificación puede estar activada para utilizar una configuración común en todas las LIF restantes o utilizar una configuración independiente.



Para la multivía y la conmutación al respaldo en varias rutas, NetApp recomienda tener un mínimo de dos LIF por nodo de almacenamiento en redes Ethernet independientes para todas las SVM en configuraciones de iSCSI.

## NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS

172.21.118.179

SUBNET MASK

24

GATEWAY

Add optional gateway

BROADCAST DOMAIN AND PORT

NFS\_iSCSI

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

IP ADDRESS

172.21.119.179

PORT

a0a-3375

ntaphci-a300-02

IP ADDRESS

172.21.118.180

PORT

a0a-3374

IP ADDRESS

172.21.119.180

PORT

a0a-3375

4. Elija si desea activar la cuenta de administración de Storage VM (para entornos multi-tenancy) y haga clic en **Guardar** para crear la SVM.

## Storage VM Administration

Manage administrator account

Save

Cancel

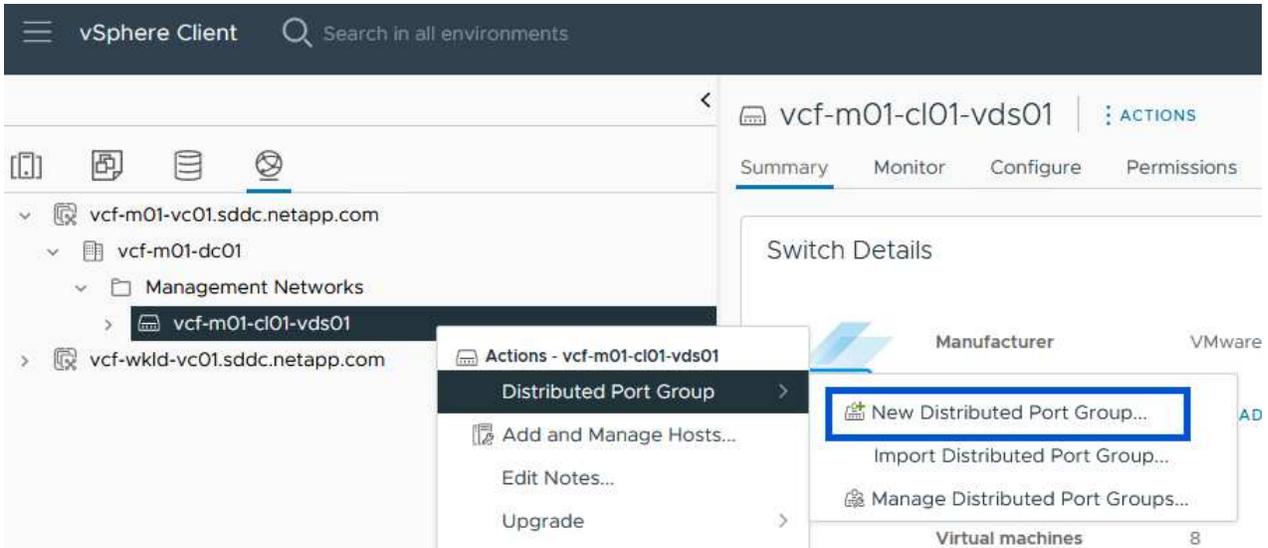
## Configure las redes para iSCSI en hosts ESXi

Los siguientes pasos se realizan en el clúster de dominio de gestión de VCF mediante el cliente vSphere.

## Crear grupos de puertos distribuidos para el tráfico de iSCSI

Complete lo siguiente para crear un nuevo grupo de puertos distribuidos para cada red iSCSI:

1. Desde el cliente vSphere para el clúster de dominio de gestión, vaya a **Inventory > Networking**. Navegue hasta el conmutador distribuido existente y elija la acción para crear **Nuevo grupo de puertos distribuidos...**



2. En el asistente de **New Distributed Port Group**, introduzca un nombre para el nuevo grupo de puertos y haga clic en **Next** para continuar.
3. En la página **Configure settings**, complete todos los ajustes. Si se utilizan VLAN, asegúrese de proporcionar el identificador de VLAN correcto. Haga clic en **Siguiente** para continuar.

## New Distributed Port Group

- 1 Name and location
- 2 Configure settings
- 3 Ready to complete

## Configure settings

Set general properties of the new port group.

Port binding	Static binding
Port allocation	Elastic ⓘ
Number of ports	8
Network resource pool	(default)
VLAN	
VLAN type	VLAN
VLAN ID	3374
Advanced	
<input type="checkbox"/> Customize default policies configuration	

CANCEL BACK NEXT

4. En la página **Listo para completar**, revise los cambios y haga clic en **Finalizar** para crear el nuevo grupo de puertos distribuidos.
5. Repita este proceso para crear un grupo de puertos distribuidos para la segunda red iSCSI que se esté utilizando y asegúrese de que ha introducido el **VLAN ID** correcto.
6. Una vez que ambos grupos de puertos han sido creados, navegue al primer grupo de puertos y seleccione la acción para **Editar configuración**....

The screenshot shows the vSphere Client interface. The top navigation bar includes the vSphere Client logo and a search bar. The main content area is divided into a left-hand navigation pane and a right-hand details pane. The left pane shows a tree view of the environment, with the path **vcf-m01-cl01-vds01-pg-iscsi-a** selected. A context menu is open over this selection, with the **Edit Settings...** option highlighted. The right pane displays the **Distributed Port Group Details** for the selected port group, showing the following configuration:

Port binding	Static binding
Port allocation	Elastic
VLAN ID	3374
Distributed switch	<a href="#">vcf-m01-cl01-vds01</a>
Network protocol profile	--
Network resource pool	--
Hosts	4

7. En la página **Distributed Port Group - Edit Settings**, navega a **Teaming and failover** en el menú de la izquierda y haz clic en **uplink2** para moverlo hacia abajo a **Uplinks sin usar**.

Distributed Port Group - Edit Settings | vcf-m01-cl01-vds01-pg-iscsi-a ×

General	<b>Load balancing</b>	Route based on originating virtual por ▾
Advanced	<b>Network failure detection</b>	Link status only ▾
VLAN	<b>Notify switches</b>	Yes ▾
Security	<b>Failback</b>	Yes ▾
Traffic shaping		
<b>Teaming and failover</b>		
Monitoring		
Miscellaneous		

**Failover order** ⓘ

MOVE UP MOVE DOWN

**Active uplinks**

- uplink1

**Standby uplinks**

**Unused uplinks**

- uplink2

CANCEL OK

8. Repita este paso para el segundo grupo de puertos iSCSI. Sin embargo, esta vez mueva **uplink1** hacia abajo a **Uplinks sin usar**.

# Distributed Port Group - Edit Settings | vcf-m01-cl01-vds01-pg-iscsi-b

General

Advanced

VLAN

Security

Traffic shaping

**Teaming and failover**

Monitoring

Miscellaneous

**Load balancing**

Route based on originating virtual por 

**Network failure detection**

Link status only 

**Notify switches**

Yes 

**Failback**

Yes 

Failover order 

MOVE UP MOVE DOWN

**Active uplinks**

 uplink2

**Standby uplinks**

**Unused uplinks**

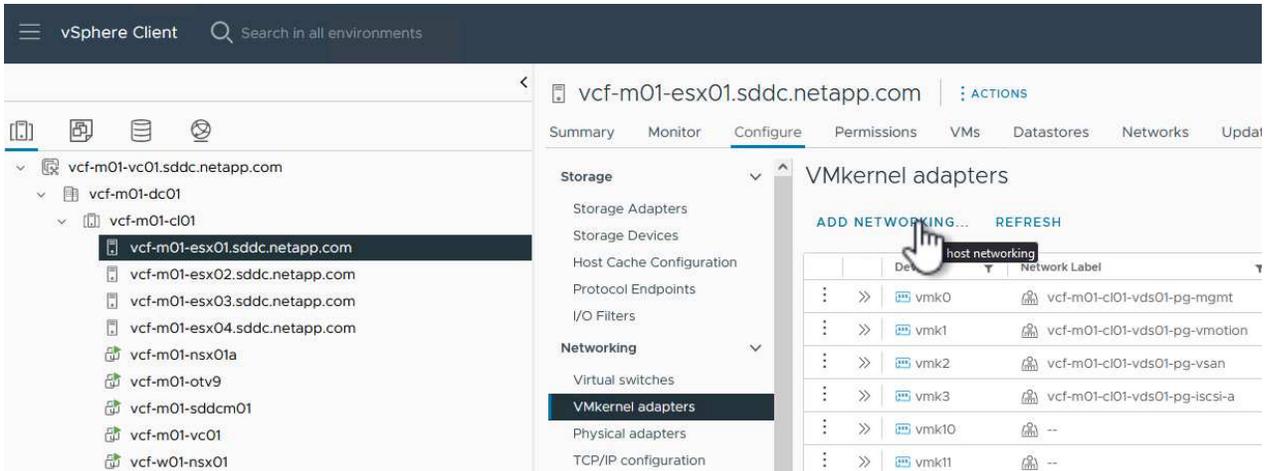
 uplink1



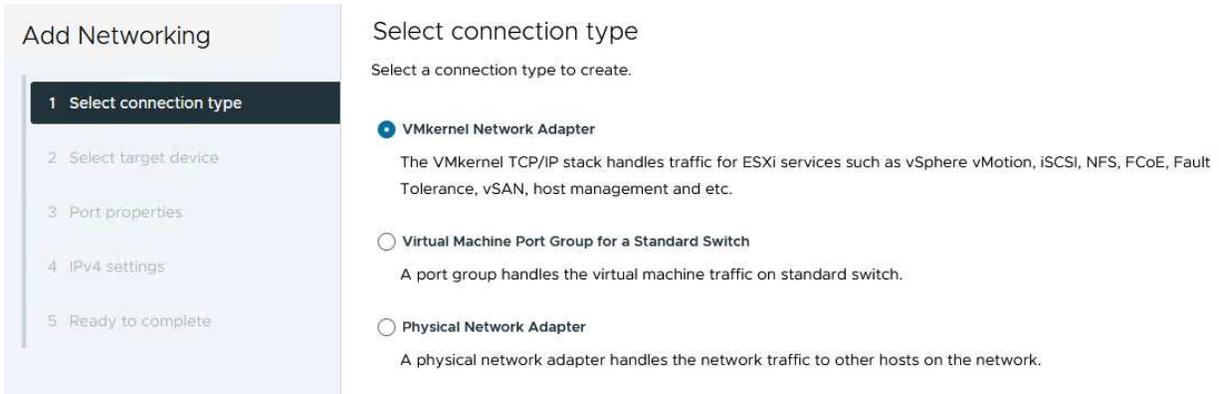
## Crear adaptadores de VMkernel en cada host ESXi

Repita este proceso en cada host ESXi del dominio de gestión.

1. En el cliente de vSphere, desplácese hasta uno de los hosts ESXi en el inventario de dominio de gestión. En la pestaña **Configure**, seleccione **VMkernel adapter** y haga clic en **Add Networking...** para comenzar.



2. En la ventana **Seleccionar tipo de conexión**, elija **Adaptador de red VMkernel** y haga clic en **Siguiente** para continuar.



3. En la página **Seleccionar dispositivo de destino**, elija uno de los grupos de puertos distribuidos para iSCSI que se crearon anteriormente.

## Add Networking

- 1 Select connection type
- 2 Select target device**
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

## Select target device

Select a target device for the new connection.

- Select an existing network
- Select an existing standard switch
- New standard switch

Quick Filter

Enter value

	Name	NSX Port Group ID	Distributed Switch
<input type="radio"/>	SDDC-DPortGroup-VM-Mgmt	--	vcf-m01-ci01-vds01
<input checked="" type="radio"/>	vcf-m01-ci01-vds01-pg-iscsi-a	--	vcf-m01-ci01-vds01
<input type="radio"/>	vcf-m01-ci01-vds01-pg-iscsi-b	--	vcf-m01-ci01-vds01
<input type="radio"/>	vcf-m01-ci01-vds01-pg-mgmt	--	vcf-m01-ci01-vds01
<input type="radio"/>	vcf-m01-ci01-vds01-pg-vmotion	--	vcf-m01-ci01-vds01
<input type="radio"/>	vcf-m01-ci01-vds01-pg-vsan	--	vcf-m01-ci01-vds01

Manage Columns 6 items

CANCEL

BACK

NEXT

4. En la página **Propiedades del puerto**, mantenga los valores predeterminados y haga clic en **Siguiente** para continuar.

## Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties**
- 4 IPv4 settings
- 5 Ready to complete

## Port properties

Specify VMkernel port settings.

**Network label** vcf-m01-ci01-vds01-pg-iscsi-a (vcf-m01-ci01-vds01)

**MTU** Get MTU from switch 9000

**TCP/IP stack** Default

### Available services

**Enabled services**

- vMotion
- Provisioning
- Fault Tolerance logging
- Management
- vSphere Replication
- vSphere Replication NFC
- vSAN
- vSAN Witness
- vSphere Backup NFC
- NVMe over TCP
- NVMe over RDMA

5. En la página **IPv4 settings**, rellena la **IP address**, **Subnet mask** y proporciona una nueva dirección IP de Gateway (solo si es necesario). Haga clic en **Siguiente** para continuar.

### Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

### IPv4 settings

Specify VMkernel IPv4 settings.

Obtain IPv4 settings automatically  
 Use static IPv4 settings

**IPv4 address**

**Subnet mask**

**Default gateway**  Override default gateway for this adapter

**DNS server addresses**

6. Revise sus selecciones en la página **Listo para completar** y haga clic en **Finalizar** para crear el adaptador VMkernel.

### Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

### Ready to complete

Review your selections before finishing the wizard

- ▼ Select target device

Distributed port group vcf-m01-cl01-vds01-pg-iscsi-a

Distributed switch vcf-m01-cl01-vds01
- ▼ Port properties

New port group vcf-m01-cl01-vds01-pg-iscsi-a (vcf-m01-cl01-vds01)

MTU 9000

vMotion Disabled

Provisioning Disabled

Fault Tolerance logging Disabled

Management Disabled

vSphere Replication Disabled

vSphere Replication NFC Disabled

vSAN Disabled

vSAN Witness Disabled

vSphere Backup NFC Disabled

NVMe over TCP Disabled

NVMe over RDMA Disabled
- ▼ IPv4 settings

IPv4 address 172.21.118.114 (static)

Subnet mask 255.255.255.0

CANCEL
BACK
FINISH

7. Repita este proceso para crear un adaptador de VMkernel para la segunda red iSCSI.

## **Pon en marcha y utiliza herramientas de ONTAP para configurar el almacenamiento**

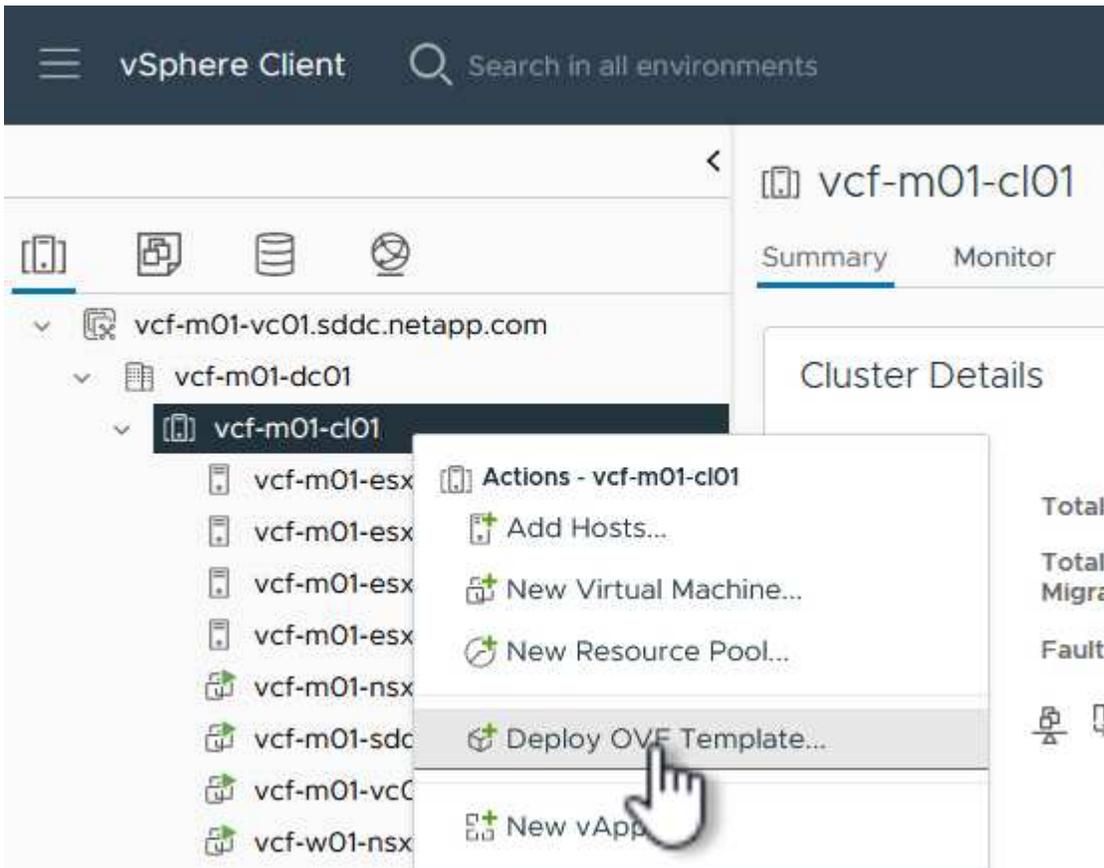
Los siguientes pasos se realizan en el clúster de dominio de gestión de VCF mediante el cliente vSphere e implican la puesta en marcha de OTV, la creación de un almacén de datos iSCSI de VMFS y la migración de equipos virtuales de gestión al nuevo almacén de datos.

## Ponga en marcha herramientas de ONTAP para VMware vSphere

Las herramientas de ONTAP para VMware vSphere (OTV) se ponen en marcha como dispositivo de máquina virtual y proporcionan una interfaz de usuario integrada de vCenter para gestionar el almacenamiento de ONTAP.

Complete lo siguiente para poner en marcha herramientas de ONTAP para VMware vSphere:

1. Obtenga la imagen OVA de las herramientas de ONTAP de la "[Sitio de soporte de NetApp](#)" y descárguelo a una carpeta local.
2. Inicie sesión en el dispositivo vCenter para el dominio de gestión de VCF.
3. Desde la interfaz del dispositivo vCenter, haga clic con el botón derecho en el clúster de administración y seleccione **Implementar plantilla OVF...**



4. En el asistente de **Desplegar plantilla OVF** haga clic en el botón de opción **Archivo local** y seleccione el archivo OVA de herramientas ONTAP descargado en el paso anterior.

## Deploy OVF Template

### 1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

## Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

5. En los pasos 2 a 5 del asistente, seleccione un nombre y una carpeta para la máquina virtual, seleccione el recurso de computación, revise los detalles y acepte el acuerdo de licencia.
6. Para la ubicación de almacenamiento de los archivos de configuración y disco, seleccione el almacén de datos vSAN del clúster de dominio de gestión de VCF.

## Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

**6 Select storage**

7 Select networks

8 Customize template

9 Ready to complete

## Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine [?](#)

Select virtual disk format As defined in the VM storage policy

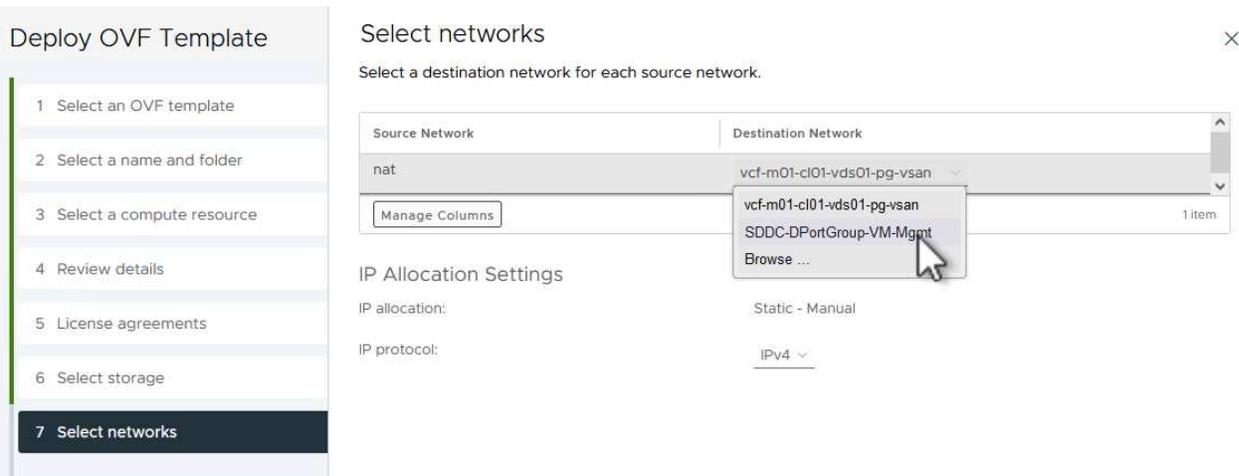
VM Storage Policy Datastore Default

Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	vcf-m01-c01-ds-vsant01	--	999.97 GB	7.17 TB	225.72 GB	v
<input type="radio"/>	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v

Manage Columns Items per page 10 5 items

7. En la página Seleccionar red, seleccione la red que se utiliza para el tráfico de gestión.



8. En la página Personalizar plantilla, rellene toda la información necesaria:

- Contraseña que se utilizará para el acceso administrativo a OTV.
- Dirección IP del servidor NTP.
- Contraseña de la cuenta de mantenimiento de OTV.
- Contraseña de OTV Derby DB.
- No marque la casilla para **Enable VMware Cloud Foundation (VCF)**. El modo VCF no es necesario para implementar almacenamiento complementario.
- El FQDN o la dirección IP del dispositivo de vCenter y proporciona credenciales para vCenter.
- Proporcione los campos de propiedades de red necesarios.

Haga clic en **Siguiente** para continuar.

## Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template**
- 9 Ready to complete

## Customize template

Customize the deployment properties of this software solution.

❗ 2 properties have invalid values ✕

▼ System Configuration 4 settings

**Application User Password (\*)** Password to assign to the administrator account. For security reasons, it is recommended to use a password that is of eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character.

Password

Confirm Password

---

**NTP Servers** A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used.

---

**Maintenance User Password (\*)** Password to assign to maint user account.

Password

Confirm Password

## Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template**
- 9 Ready to complete

## Customize template

▼ Configure vCenter or Enable VCF 5 settings

**Enable VMware Cloud Foundation (VCF)** vCenter server and user details are ignored when VCF is enabled.

---

**vCenter Server Address (\*)** Specify the IP address/hostname of an existing vCenter to register to.

---

**Port (\*)** Specify the HTTPS port of an existing vCenter to register to.

---

**Username (\*)** Specify the username of an existing vCenter to register to.

---

**Password (\*)** Specify the password of an existing vCenter to register to.

Password

Confirm Password

---

▼ Network Properties 8 settings

**Host Name** Specify the hostname for the appliance. (Leave blank if DHCP is desired)

---

**IP Address** Specify the IP address for the appliance. (Leave blank if DHCP is

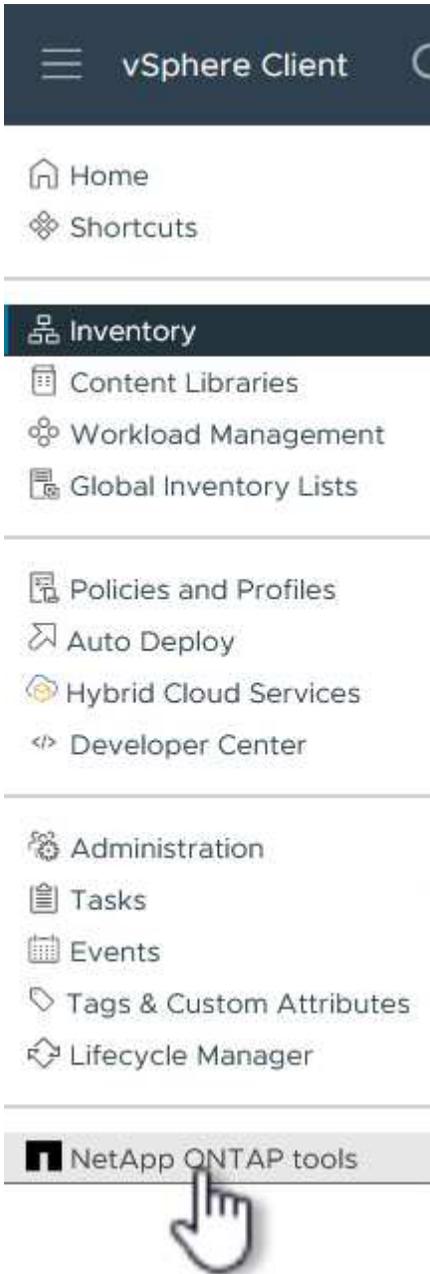
CANCELBACKNEXT

9. Revise toda la información en la página Listo para completar y haga clic en Finalizar para comenzar a desplegar el dispositivo OTV.

## Configure un almacén de datos iSCSI de VMFS en el dominio de gestión mediante OTV

Realice lo siguiente para utilizar OTV para configurar un almacén de datos iSCSI de VMFS como almacenamiento complementario en el dominio de gestión:

1. En el cliente de vSphere, vaya al menú principal y seleccione \* Herramientas de NetApp ONTAP \*.



2. Una vez en **Herramientas de ONTAP**, desde la página de inicio (o desde **Sistemas de almacenamiento**), haga clic en **Agregar** para agregar un nuevo sistema de almacenamiento.

vSphere Client Search in all environments

NetApp ONTAP tools INSTANCE 172.21.166.139:8443

**Overview**

- Storage Systems
- Storage capability profile
- Storage Mapping
- Settings
- Reports
  - Datastore Report
  - Virtual Machine Report
  - vVols Datastore Report
  - vVols Virtual Machine Report
  - Log Integrity Report

### ONTAP tools for VMware vSphere

Getting Started Traditional Dashboard vVols Dashboard

ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware environments using NetApp storage systems.

**Add Storage System**

Add storage systems to ONTAP tools for VMware vSphere.



**Provision Datastore**

Create traditional or vVols datastores.



**Next Steps**

 [View Dashboard](#)  
View and monitor the datastores in ONTAP tools for VMware vSphere.

 [Settings](#)  
Configure administrative settings such as credentials, alarm thresholds.

[What's new?](#)  
September 4, 2023

- Qualified and supported with ONTAP 9.13.1
- Supports and interoperates with VMware vSphere 8.x releases
- Includes newer enhanced SCPs that efficiently map workloads to the newer All SAN Array platforms through policy based management

**Resources**

- [ONTAP tools for VMware vSphere Documentation Resources](#)
- [RBAC User Creator for Data ONTAP](#)
- [ONTAP tools for VMware vSphere REST API Documentation](#)

3. Proporcione la dirección IP y las credenciales del sistema de almacenamiento de ONTAP y haga clic en **Agregar**.

## Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server	vcf-m01-vc01.sddc.netapp.com
Name or IP address:	172.16.9.25
Username:	admin
Password:	●●●●●●●●
Port:	443
Advanced options	>

CANCEL

SAVE & ADD MORE

ADD



4. Haga clic en **Sí** para autorizar el certificado de clúster y agregar el sistema de almacenamiento.

## Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server

vcf-m01-vc01.sddc.netapp.com

### Authorize Cluster Certificate

Host 172.16.9.25 has identified itself with a self-signed certificate.

[Show certificate](#)

Do you want to trust this certificate?

NO

YES



CANCEL

SAVE & ADD MORE

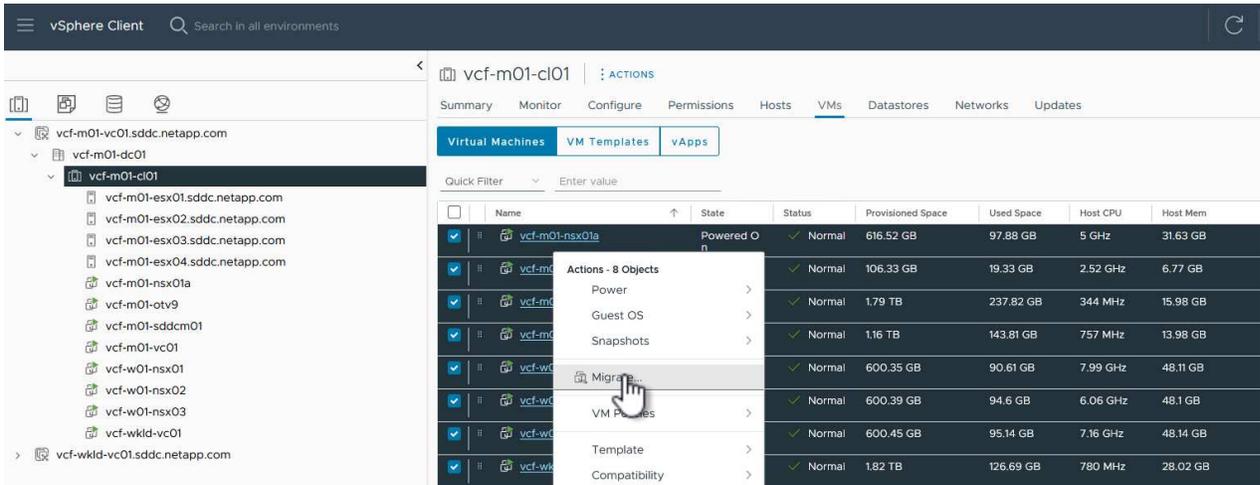
ADD

## Migrar VM de gestión's a almacén de datos iSCSI

En los casos en los que se prefiera utilizar almacenamiento ONTAP para proteger vMotion del equipo virtual de gestión VCF se puede utilizar para migrar los equipos virtuales al almacén de datos iSCSI recién creado.

Complete los siguientes pasos para migrar los equipos virtuales de gestión de VCF al almacén de datos iSCSI.

1. Desde vSphere Client, navegue hasta el clúster de dominio de administración y haga clic en la pestaña **VMs**.
2. Seleccione las máquinas virtuales que se migrarán al almacén de datos iSCSI, haga clic con el botón derecho y seleccione **Migrate...**



3. En el asistente de **Máquinas virtuales - Migrar**, seleccione **Cambiar solo almacenamiento** como tipo de migración y haga clic en **Siguiente** para continuar.



### Select a migration type

Change the virtual machines' compute resource, storage, or both.

- Change compute resource only  
Migrate the virtual machines to another host or cluster.
- Change storage only  
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.
- Change both compute resource and storage  
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.
- Cross vCenter Server export  
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

4. En la página **Seleccionar almacenamiento**, seleccione el almacén de datos iSCSI y seleccione **Siguiente** para continuar.

## 8 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

### Select storage

Select the destination storage for the virtual machine migration.

**BATCH CONFIGURE** CONFIGURE PER DISK

Select virtual disk format Same format as source

VM Storage Policy Datastore Default

Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free
mgmt_01_iscsi	--	3 TB	1.46 GB	3 TB
vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.28 TB	52.38 GB

Manage Columns Items per page 10 2 items

#### Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. Revise las selecciones y haga clic en **Finish** para iniciar la migración.

6. El estado de reubicación se puede ver desde el panel **Tareas recientes**.

Task Name	Target	Status	Details
Relocate virtual machine	<a href="#">vcf-w01-nsx03</a>	38%	Migrating Virtual Machine active state
Relocate virtual machine	<a href="#">vcf-wkld-vc01</a>	42%	Migrating Virtual Machine active state
Relocate virtual machine	<a href="#">vcf-m01-otv9</a>	36%	Migrating Virtual Machine active state
Relocate virtual machine	<a href="#">vcf-m01-nsx01a</a>	49%	Migrating Virtual Machine active state
Relocate virtual machine	<a href="#">vcf-w01-nsx02</a>	47%	Migrating Virtual Machine active state
Relocate virtual machine	<a href="#">vcf-m01-sddcm01</a>	39%	Migrating Virtual Machine active state
Relocate virtual machine	<a href="#">vcf-w01-nsx01</a>	42%	Migrating Virtual Machine active state
Relocate virtual machine	<a href="#">vcf-m01-vc01</a>	44%	Migrating Virtual Machine active state

## Información adicional

Para obtener información acerca de la configuración de los sistemas de almacenamiento ONTAP, consulte la ["Documentación de ONTAP 9"](#) centro.

Para obtener información sobre la configuración de VCF, consulte ["Documentación de VMware Cloud Foundation"](#).

## Demostración en vídeo de esta solución

[Almacenes de datos iSCSI como almacenamiento complementario para dominios de gestión de VCF](#)

## Utilice las herramientas de ONTAP para configurar el almacenamiento complementario (vVols) para los dominios de carga de trabajo de VCF

Autor: Josh Powell

Utilice las herramientas de ONTAP para configurar el almacenamiento complementario (vVols) para los dominios de carga de trabajo de VCF

## Descripción general del escenario

En este escenario, mostraremos cómo implementar y usar Herramientas de ONTAP para VMware vSphere (OTV) para configurar un almacén de datos **vVols** para un dominio de carga de trabajo VCF.

**iSCSI** se utiliza como protocolo de almacenamiento para el almacén de datos vVols.

Este escenario cubre los siguientes pasos de alto nivel:

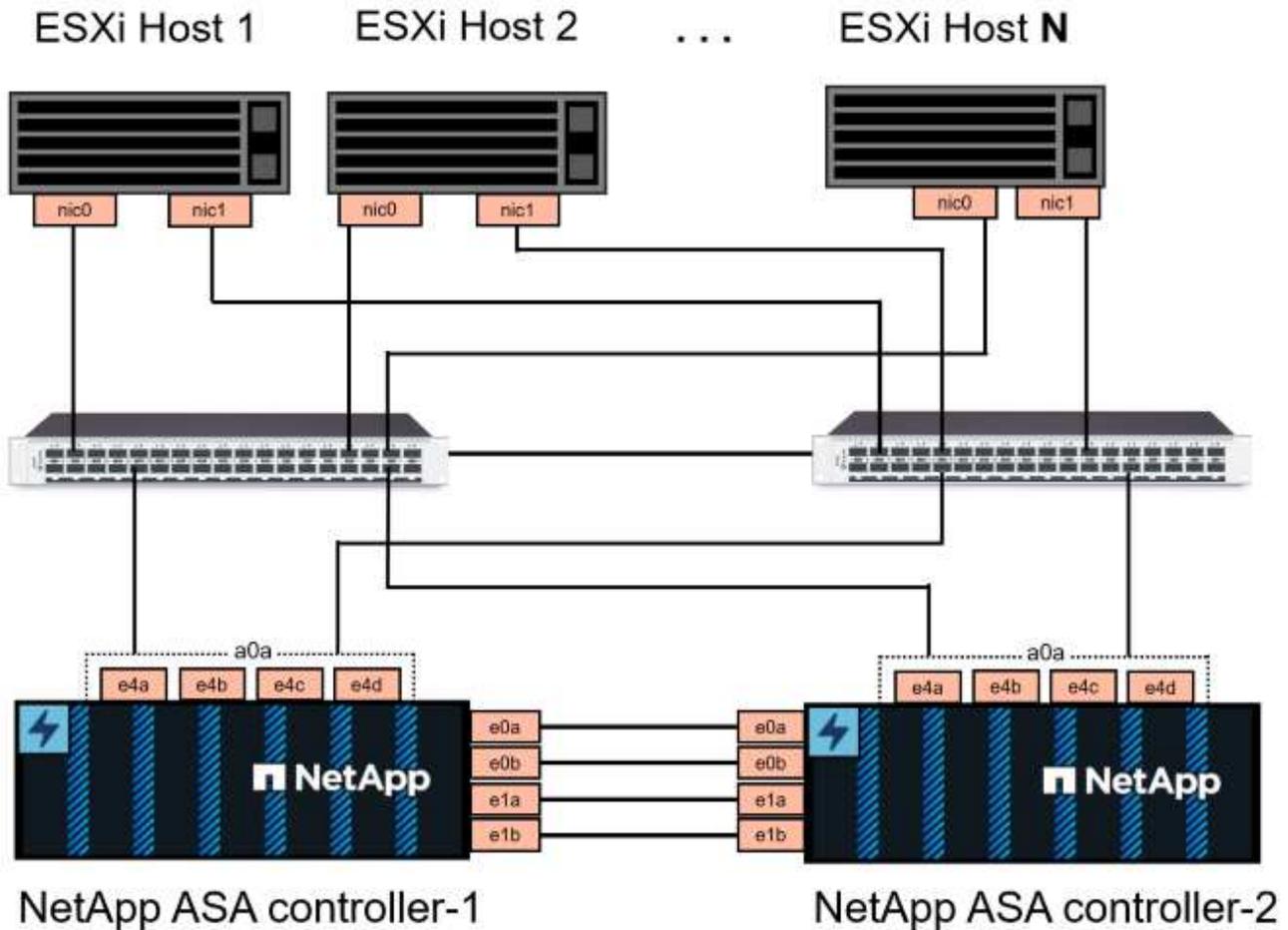
- Cree una máquina virtual de almacenamiento (SVM) con interfaces lógicas (LIF) para el tráfico de iSCSI.
- Cree grupos de puertos distribuidos para redes iSCSI en el dominio de carga de trabajo de VI.
- Cree adaptadores vmkernel para iSCSI en los hosts ESXi para el dominio de carga de trabajo VI.
- Implemente las herramientas de ONTAP en el dominio de la carga de trabajo de VI.
- Cree un nuevo almacén de datos vVols en el dominio de carga de trabajo de VI.

## Requisitos previos

Este escenario requiere los siguientes componentes y configuraciones:

- Un sistema de almacenamiento de ONTAP ASA con puertos de datos físicos en switches ethernet dedicados al tráfico de almacenamiento.
- La puesta en marcha del dominio de gestión de VCF está completa y se puede acceder al cliente vSphere.
- Se ha desplegado anteriormente un dominio de carga de trabajo de VI.

NetApp recomienda diseños de red completamente redundantes para iSCSI. En el siguiente diagrama se muestra un ejemplo de una configuración redundante, que proporciona tolerancia a fallos para los sistemas de almacenamiento, los switches, los adaptadores de red y los sistemas host. Consulte NetApp ["Referencia para la configuración DE SAN"](#) para obtener más información.



Para la multivía y la conmutación al respaldo en varias rutas, NetApp recomienda tener un mínimo de dos LIF por nodo de almacenamiento en redes ethernet independientes para todas las SVM en configuraciones de iSCSI.

Esta documentación muestra el proceso de crear una SVM nueva y especificar la información de dirección IP para crear varias LIF para el tráfico de iSCSI. Para agregar LIF nuevos a una SVM existente, consulte ["Crear una LIF \(interfaz de red\)"](#).



En situaciones en las que se configuran varios adaptadores VMkernel en la misma red IP, se recomienda utilizar el enlace de puerto iSCSI de software en los hosts ESXi para garantizar el equilibrio de carga entre los adaptadores. Consulte el artículo de la base de conocimientos ["Consideraciones sobre el uso de la vinculación de puertos iSCSI de software en ESX/ESXi \(2038869\)"](#).

Para obtener información adicional sobre el uso de almacenes de datos VMFS iSCSI con VMware, consulte ["Almacén de datos VMFS de vSphere: Entorno de administración del almacenamiento iSCSI con ONTAP"](#).

### Pasos de despliegue

Para desplegar las herramientas de ONTAP y utilizarlo para crear un almacén de datos vVols en el dominio de administración de VCF, lleve a cabo los siguientes pasos:

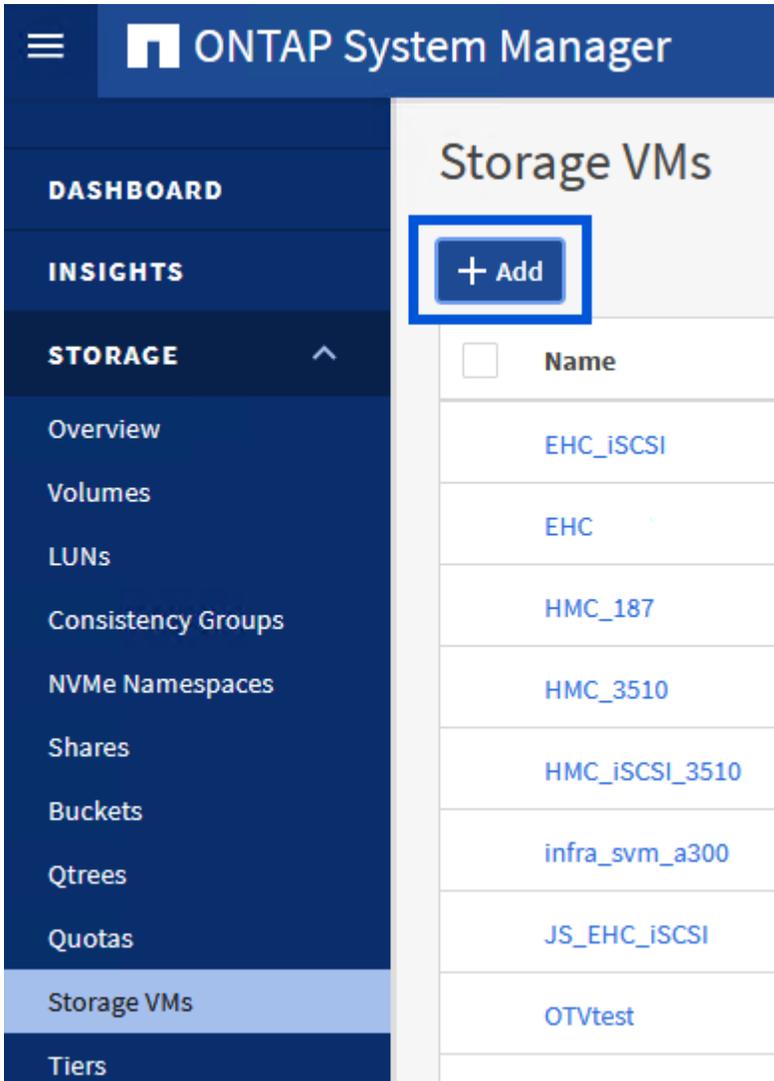
## **Crear SVM y LIF en el sistema de almacenamiento ONTAP**

El siguiente paso se lleva a cabo en ONTAP System Manager.

## Crear la máquina virtual de almacenamiento y las LIF

Complete los siguientes pasos para crear una SVM junto con varios LIF para el tráfico de iSCSI.

1. Desde el Administrador del sistema de ONTAP navegue hasta **VM de almacenamiento** en el menú de la izquierda y haga clic en **+ Agregar** para comenzar.



2. En el asistente de **Add Storage VM**, proporcione un **Name** para la SVM, seleccione **IP Space** y, a continuación, en **Access Protocol**, haga clic en la pestaña **iSCSI** y marque la casilla **Enable iSCSI**.

## Add Storage VM



STORAGE VM NAME

SVM\_ISCSI

IPSPACE

Default



### Access Protocol

SMB/CIFS, NFS, S3

iSCSI

FC

NVMe

Enable iSCSI

3. En la sección **Interfaz de red**, rellena la **Dirección IP**, **Máscara de subred** y **Dominio de difusión y puerto** para la primera LIF. En el caso de LIF posteriores, la casilla de verificación puede estar activada para utilizar una configuración común en todas las LIF restantes o utilizar una configuración independiente.



Para la multivía y la conmutación al respaldo en varias rutas, NetApp recomienda tener un mínimo de dos LIF por nodo de almacenamiento en redes Ethernet independientes para todas las SVM en configuraciones de iSCSI.

## NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS

172.21.118.179

SUBNET MASK

24

GATEWAY

Add optional gateway

BROADCAST DOMAIN AND PORT

NFS\_iSCSI

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

IP ADDRESS

172.21.119.179

PORT

a0a-3375

ntaphci-a300-02

IP ADDRESS

172.21.118.180

PORT

a0a-3374

IP ADDRESS

172.21.119.180

PORT

a0a-3375

4. Elija si desea activar la cuenta de administración de Storage VM (para entornos multi-tenancy) y haga clic en **Guardar** para crear la SVM.

## Storage VM Administration

Manage administrator account

Save

Cancel

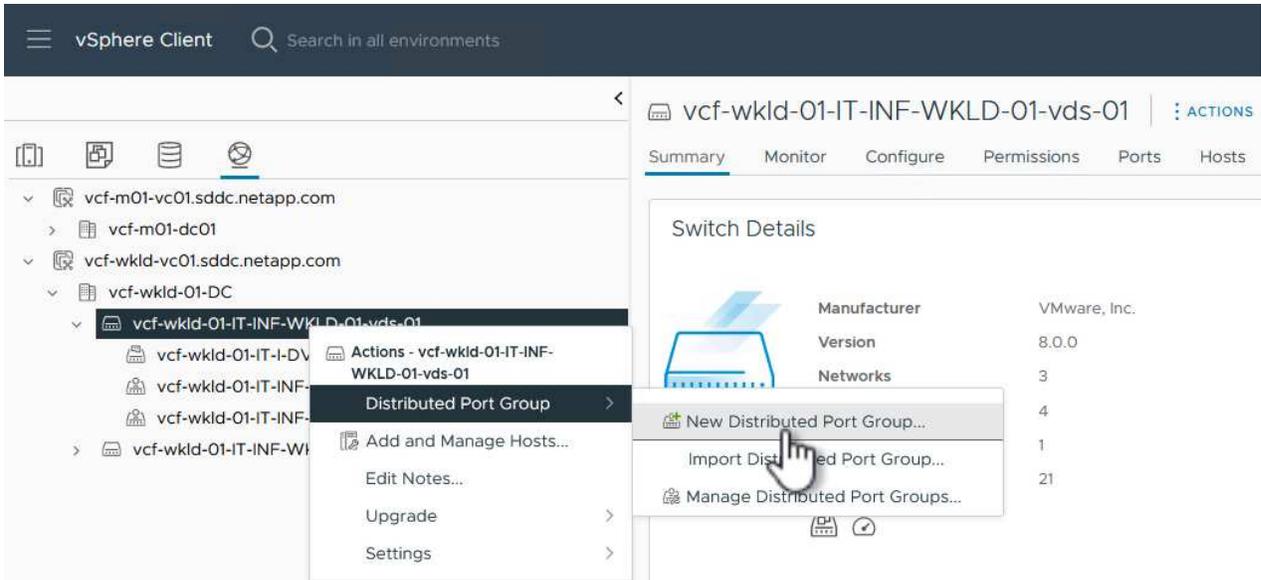
## Configure las redes para iSCSI en hosts ESXi

Los siguientes pasos se llevan a cabo en el clúster de dominio de carga de trabajo VI con el cliente vSphere. En este caso, se utiliza vCenter Single Sign-On para que el cliente vSphere sea común en los dominios de carga de trabajo y gestión.

## Crear grupos de puertos distribuidos para el tráfico de iSCSI

Complete lo siguiente para crear un nuevo grupo de puertos distribuidos para cada red iSCSI:

1. En el cliente vSphere , desplácese hasta **Inventory > Networking** para el dominio de la carga de trabajo. Navegue hasta el conmutador distribuido existente y elija la acción para crear **Nuevo grupo de puertos distribuidos...**



2. En el asistente de **New Distributed Port Group**, introduzca un nombre para el nuevo grupo de puertos y haga clic en **Next** para continuar.
3. En la página **Configure settings**, complete todos los ajustes. Si se utilizan VLAN, asegúrese de proporcionar el identificador de VLAN correcto. Haga clic en **Siguiente** para continuar.

## New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

### Configure settings

Set general properties of the new port group.

Port binding	Static binding
Port allocation	Elastic ⓘ
Number of ports	8
Network resource pool	(default)
VLAN	
VLAN type	VLAN
VLAN ID	3374
Advanced	
<input type="checkbox"/> Customize default policies configuration	

CANCEL

BACK

NEXT

4. En la página **Listo para completar**, revise los cambios y haga clic en **Finalizar** para crear el nuevo grupo de puertos distribuidos.
5. Repita este proceso para crear un grupo de puertos distribuidos para la segunda red iSCSI que se esté utilizando y asegúrese de que ha introducido el **VLAN ID** correcto.
6. Una vez que ambos grupos de puertos han sido creados, navegue al primer grupo de puertos y seleccione la acción para **Editar configuración...**

The screenshot shows the vSphere Client interface. On the left, a tree view displays the environment structure, with the path **vcf-wkld-01-iscsi-a** selected. A context menu is open over this selection, showing options like **Actions - vcf-wkld-01-iscsi-a** and **Edit Settings...**. On the right, the **Distributed Port Group Details** panel is visible, showing the following configuration:

Port binding	Static binding
Port allocation	Elastic
VLAN ID	3374
Distributed switch	<a href="#">vcf-wkld-01-IT-INF-WKLD-01-vds-01</a>
Network protocol profile	--

7. En la página **Distributed Port Group - Edit Settings**, navega a **Teaming and failover** en el menú de la izquierda y haz clic en **uplink2** para moverlo hacia abajo a **Uplinks sin usar**.

Distributed Port Group - Edit Settings | vcf-wkld-01-iscsi-a

General | Load balancing | Route based on originating virtual por

Advanced | Network failure detection | Link status only

VLAN | Notify switches | Yes

Security | Failback | Yes

Traffic shaping

**Teaming and failover**

Monitoring

Miscellaneous

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink1

Standby uplinks

Unused uplinks

uplink2

CANCEL OK

8. Repita este paso para el segundo grupo de puertos iSCSI. Sin embargo, esta vez mueva **uplink1** hacia abajo a **Uplinks sin usar**.

Distributed Port Group - Edit Settings | vcf-wkld-01-iscsi-b

General | Load balancing | Route based on originating virtual por

Advanced | Network failure detection | Link status only

VLAN | Notify switches | Yes

Security | Failback | Yes

Traffic shaping

**Teaming and failover**

Monitoring

Miscellaneous

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink2

Standby uplinks

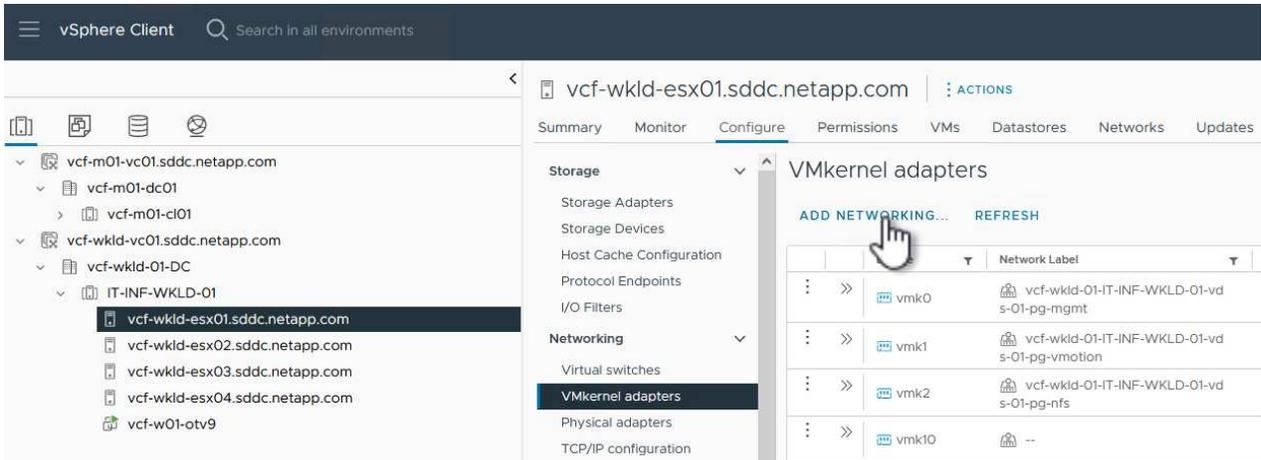
Unused uplinks

uplink1

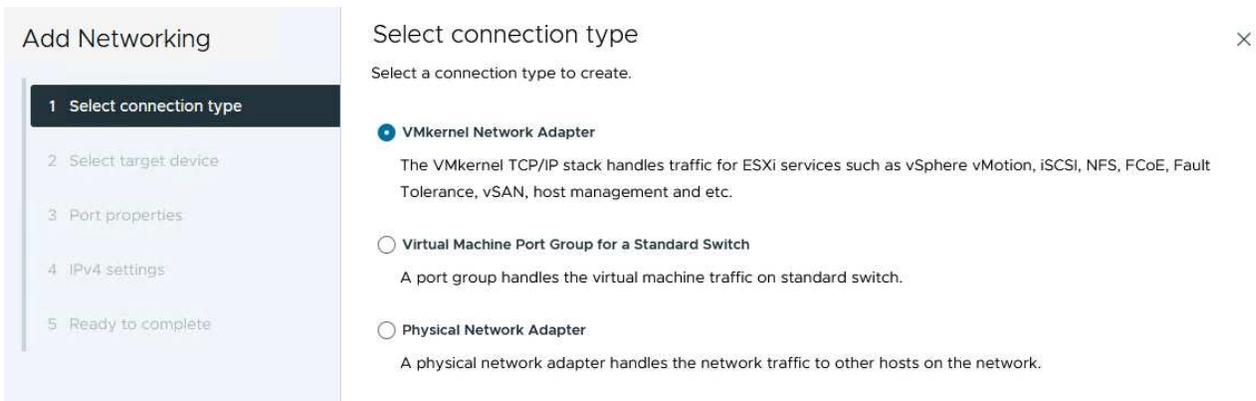
## Crear adaptadores de VMkernel en cada host ESXi

Repita este proceso en cada host ESXi del dominio de la carga de trabajo.

1. En el cliente de vSphere, desplácese hasta uno de los hosts ESXi en el inventario de dominio de la carga de trabajo. En la pestaña **Configure**, seleccione **VMkernel adapter** y haga clic en **Add Networking...** para comenzar.



2. En la ventana **Seleccionar tipo de conexión**, elija **Adaptador de red VMkernel** y haga clic en **Siguiente** para continuar.



3. En la página **Seleccionar dispositivo de destino**, elija uno de los grupos de puertos distribuidos para iSCSI que se crearon anteriormente.

## Add Networking

- 1 Select connection type
- 2 Select target device**
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

## Select target device

Select a target device for the new connection.

- Select an existing network
- Select an existing standard switch
- New standard switch

### Quick Filter

Enter value

	Name	NSX Port Group ID	Distributed Switch
<input checked="" type="radio"/>	 vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	 vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	 vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	 vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
<input type="radio"/>	 vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

Manage Columns 5 items

CANCEL

BACK

NEXT

4. En la página **Propiedades del puerto**, mantenga los valores predeterminados y haga clic en **Siguiente** para continuar.

## Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties**
- 4 IPv4 settings
- 5 Ready to complete

## Port properties

Specify VMkernel port settings.

**Network label**

**MTU**

**TCP/IP stack**

### Available services

#### Enabled services

- vMotion
- Provisioning
- Fault Tolerance logging
- Management
- vSphere Replication
- vSphere Replication NFC
- vSAN
- vSAN Witness
- vSphere Backup NFC
- NVMe over TCP
- NVMe over RDMA

5. En la página **IPv4 settings**, rellena la **IP address**, **Subnet mask** y proporciona una nueva dirección IP de Gateway (solo si es necesario). Haga clic en **Siguiente** para continuar.

### Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

### IPv4 settings

Specify VMkernel IPv4 settings.

Obtain IPv4 settings automatically  
 Use static IPv4 settings

**IPv4 address**

**Subnet mask**

**Default gateway**  Override default gateway for this adapter

**DNS server addresses**

6. Revise sus selecciones en la página **Listo para completar** y haga clic en **Finalizar** para crear el adaptador VMkernel.

### Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

### Ready to complete

Review your selections before finishing the wizard

- ▼ **Select target device**

Distributed port group vcf-wkld-01-iscsi-a

Distributed switch vcf-wkld-01-IT-INF-WKLD-01-vds-01
- ▼ **Port properties**

New port group vcf-wkld-01-iscsi-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)

MTU 9000

vMotion Disabled

Provisioning Disabled

Fault Tolerance logging Disabled

Management Disabled

vSphere Replication Disabled

vSphere Replication NFC Disabled

vSAN Disabled

vSAN Witness Disabled

vSphere Backup NFC Disabled

NVMe over TCP Disabled

NVMe over RDMA Disabled
- ▼ **IPv4 settings**

IPv4 address 172.21.118.127 (static)

Subnet mask 255.255.255.0

CANCEL
BACK
FINISH

7. Repita este proceso para crear un adaptador de VMkernel para la segunda red iSCSI.

## **Pon en marcha y utiliza herramientas de ONTAP para configurar el almacenamiento**

Los siguientes pasos se realizan en el clúster de dominio de gestión de VCF mediante el cliente vSphere e implican la puesta en marcha de OTV, la creación de un almacén de datos iSCSI vVols y la migración de equipos virtuales de gestión al nuevo almacén de datos.

Para dominios de carga de trabajo VI, OTV se instala en el clúster de gestión de VCF, pero se registra en el vCenter asociado al dominio de carga de trabajo VI.

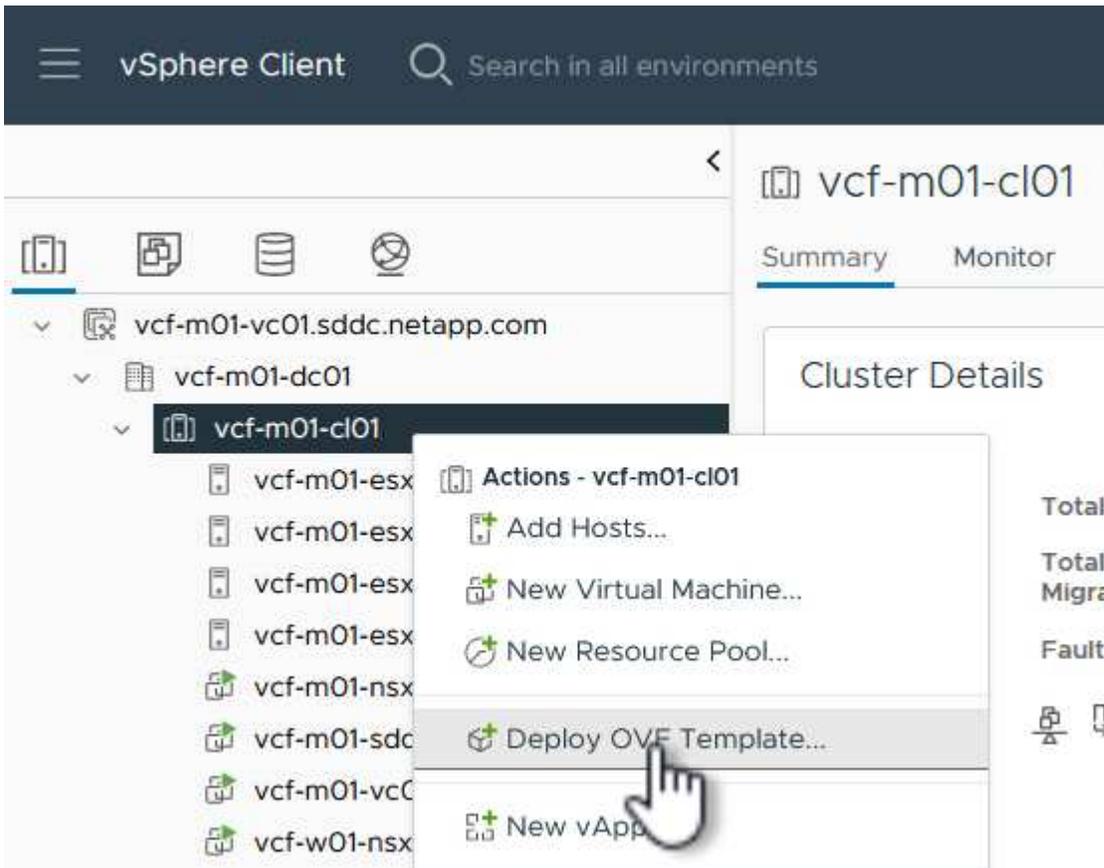
Para obtener información adicional sobre la puesta en marcha y el uso de las herramientas de ONTAP en un entorno múltiple de vCenter, consulte ["Requisitos para registrar herramientas de ONTAP en varios entornos de vCenter Server"](#).

## Ponga en marcha herramientas de ONTAP para VMware vSphere

Las herramientas de ONTAP para VMware vSphere (OTV) se ponen en marcha como dispositivo de máquina virtual y proporcionan una interfaz de usuario integrada de vCenter para gestionar el almacenamiento de ONTAP.

Complete lo siguiente para poner en marcha herramientas de ONTAP para VMware vSphere:

1. Obtenga la imagen OVA de las herramientas de ONTAP de la "[Sitio de soporte de NetApp](#)" y descárguelo a una carpeta local.
2. Inicie sesión en el dispositivo vCenter para el dominio de gestión de VCF.
3. Desde la interfaz del dispositivo vCenter, haga clic con el botón derecho en el clúster de administración y seleccione **Implementar plantilla OVF...**



4. En el asistente de **Desplegar plantilla OVF** haga clic en el botón de opción **Archivo local** y seleccione el archivo OVA de herramientas ONTAP descargado en el paso anterior.

## Deploy OVF Template

### 1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

## Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

5. En los pasos 2 a 5 del asistente, seleccione un nombre y una carpeta para la máquina virtual, seleccione el recurso de computación, revise los detalles y acepte el acuerdo de licencia.
6. Para la ubicación de almacenamiento de los archivos de configuración y disco, seleccione el almacén de datos vSAN del clúster de dominio de gestión de VCF.

## Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

## Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine [?](#)

Select virtual disk format As defined in the VM storage policy

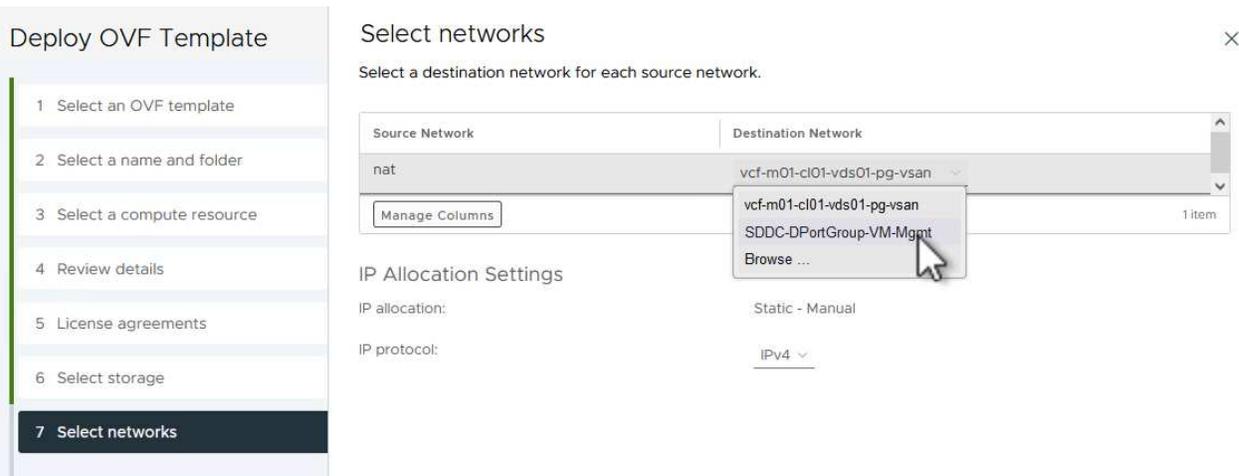
VM Storage Policy Datastore Default

Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	T
<input checked="" type="radio"/>	vcf-m01-c01-ds-vsant01	--	999.97 GB	7.17 TB	225.72 GB	v
<input type="radio"/>	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v

Manage Columns Items per page 10 5 items

7. En la página Seleccionar red, seleccione la red que se utiliza para el tráfico de gestión.



8. En la página Personalizar plantilla, rellene toda la información necesaria:

- Contraseña que se utilizará para el acceso administrativo a OTV.
- Dirección IP del servidor NTP.
- Contraseña de la cuenta de mantenimiento de OTV.
- Contraseña de OTV Derby DB.
- No marque la casilla para **Enable VMware Cloud Foundation (VCF)**. El modo VCF no es necesario para implementar almacenamiento complementario.
- FQDN o dirección IP del dispositivo vCenter para el **VI Workload Domain**
- Credenciales para el dispositivo vCenter del **VI Workload Domain**
- Proporcione los campos de propiedades de red necesarios.

Haga clic en **Siguiente** para continuar.

## Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template**
- 9 Ready to complete

## Customize template

Customize the deployment properties of this software solution.

❗ 2 properties have invalid values ✕

System Configuration		4 settings
<b>Application User Password (*)</b>	Password to assign to the administrator account. For security reasons, it is recommended to use a password that is of eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character.	
	Password	..... <span>👁</span>
	Confirm Password	..... <span>👁</span>
<b>NTP Servers</b>	A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used. 172.21.166.1	
<b>Maintenance User Password (*)</b>	Password to assign to maint user account.	
	Password	..... <span>👁</span>
	Confirm Password	..... <span>👁</span>

## Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template**
- 9 Ready to complete

## Customize template

❗ 2 properties have invalid values ✕

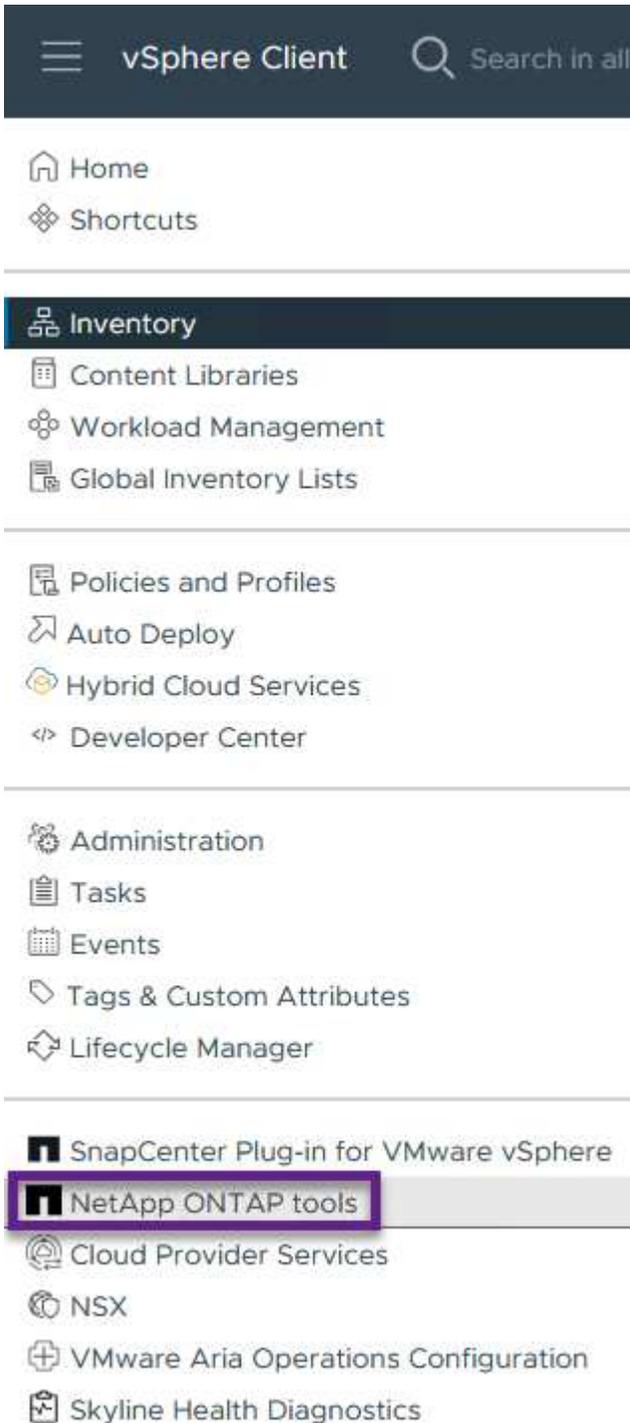
Configure vCenter or Enable vCenter		3 settings
<b>Enable VMware Cloud Foundation (VCF)</b>	vCenter server and user details are ignored when VCF is enabled. <input type="checkbox"/>	
<b>vCenter Server Address (*)</b>	Specify the IP address/hostname of an existing vCenter to register to. cf-wkld-vc01.sddc.netapp.com	
<b>Port (*)</b>	Specify the HTTPS port of an existing vCenter to register to. 443	
<b>Username (*)</b>	Specify the username of an existing vCenter to register to. administrator@vsphere.local	
<b>Password (*)</b>	Specify the password of an existing vCenter to register to.	
	Password	..... <span>👁</span>
	Confirm Password	..... <span>👁</span>
Network Properties		8 settings
<b>Host Name</b>	Specify the hostname for the appliance. (Leave blank if DHCP is desired) vcf-w01-otv9	
<b>IP Address</b>	Specify the IP address for the appliance. (Leave blank if DHCP is desired)	

CANCEL BACK NEXT

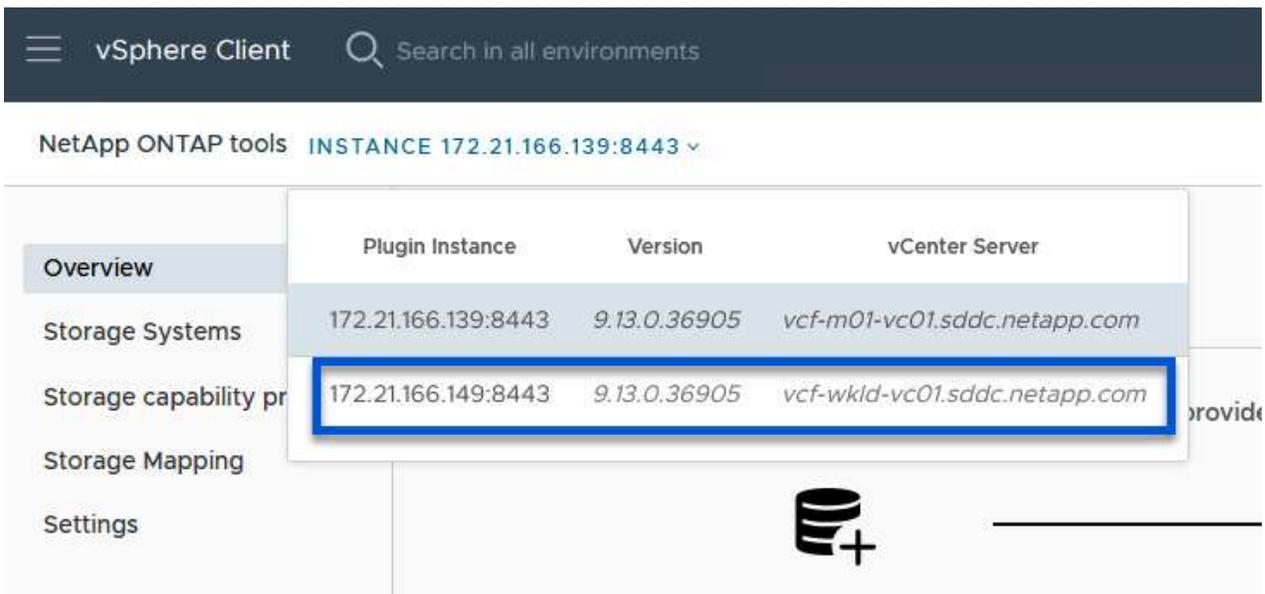
9. Revise toda la información en la página Listo para completar y haga clic en Finalizar para comenzar a desplegar el dispositivo OTV.

## Agregar un sistema de almacenamiento a las herramientas de ONTAP.

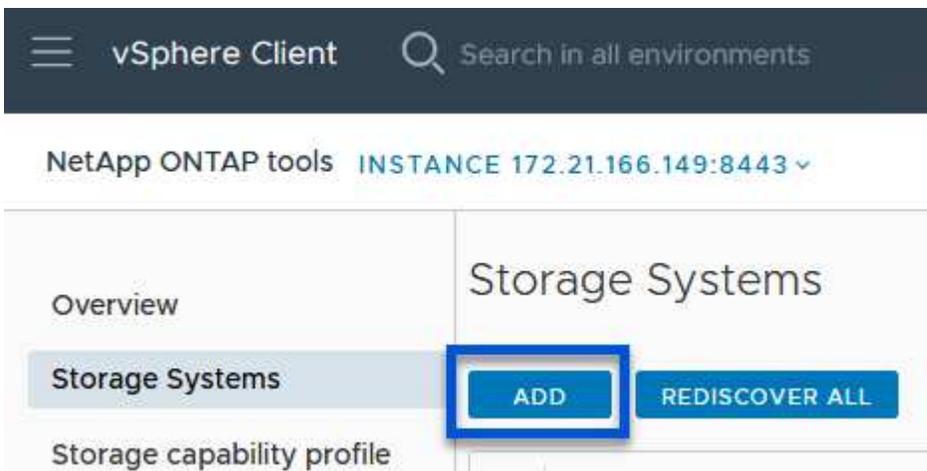
1. Acceda a herramientas de NetApp ONTAP seleccionándolo en el menú principal del vSphere Client.



2. En el menú desplegable **INSTANCE** de la interfaz de la herramienta ONTAP, seleccione la instancia OTV asociada al dominio de carga de trabajo que se va a gestionar.



3. En Herramientas de ONTAP seleccione **Sistemas de almacenamiento** en el menú de la izquierda y luego presione **Añadir**.



4. Rellene la dirección IP, las credenciales del sistema de almacenamiento y el número de puerto. Haga clic en **Add** para iniciar el proceso de descubrimiento.



VVol requiere credenciales del clúster de ONTAP en lugar de credenciales de SVM. Para obtener más información, consulte ["Añadir sistemas de almacenamiento"](#) En la documentación de Herramientas de ONTAP.

## Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server	<input type="text" value="vcf-m01-vc01.sddc.netapp.com"/> ▾
Name or IP address:	<input type="text" value="172.16.9.25"/>
Username:	<input type="text" value="admin"/>
Password:	<input type="password" value="••••••••"/>
Port:	<input type="text" value="443"/>

Advanced options 

ONTAP Cluster Certificate:  Automatically fetch  Manually upload

CANCEL

SAVE & ADD MORE

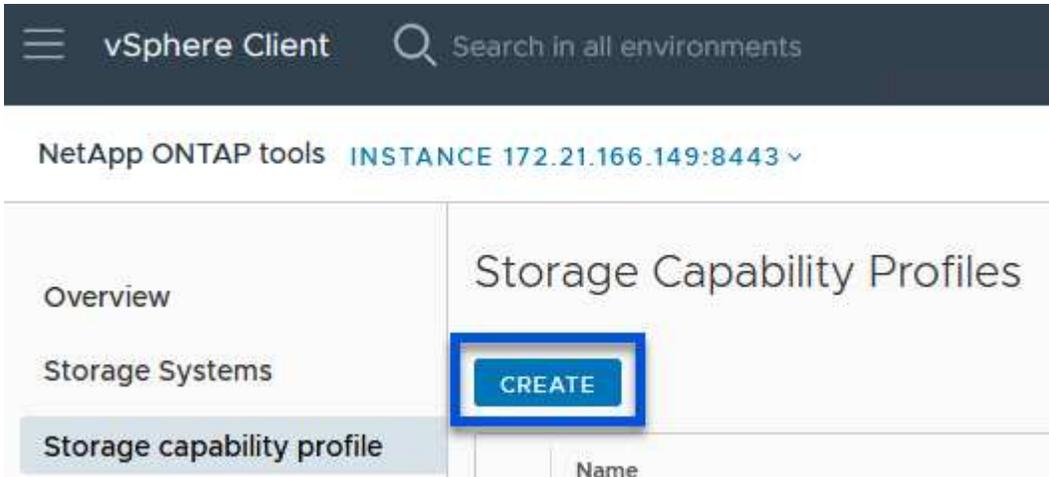
ADD

## Crear un perfil de capacidad de almacenamiento en las herramientas de ONTAP

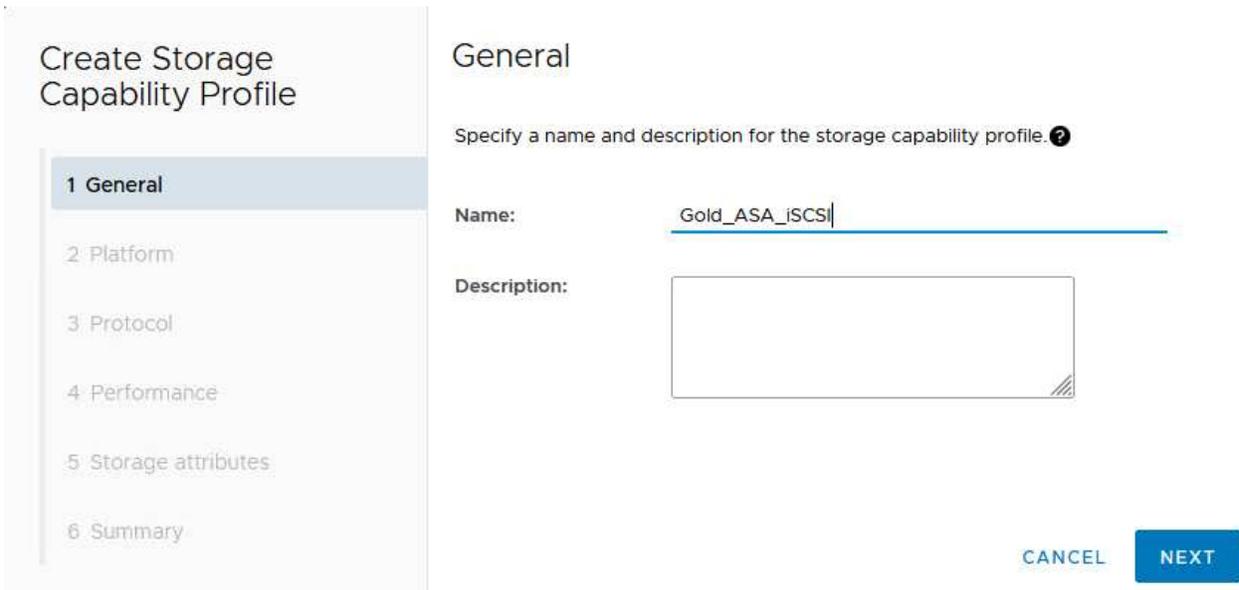
Los perfiles de funcionalidad de almacenamiento describen las funciones de una cabina de almacenamiento o un sistema de almacenamiento. Incluyen definiciones de calidad de servicio y se utilizan para seleccionar sistemas de almacenamiento que cumplan con los parámetros definidos en el perfil. Se puede utilizar uno de los perfiles proporcionados o se pueden crear otros nuevos.

Para crear un perfil de funcionalidad del almacenamiento en las herramientas de ONTAP, complete los siguientes pasos:

1. En Herramientas de ONTAP seleccione **Perfil de capacidad de almacenamiento** en el menú de la izquierda y luego presione **Crear**.



2. En el asistente de **Crear perfil de capacidad de almacenamiento**, proporcione un nombre y una descripción del perfil y haga clic en **Siguiente**.



3. Seleccione el tipo de plataforma y especifique que el sistema de almacenamiento debe ser una cabina SAN All-Flash establecida en **asimétrica** en false.

## Create Storage Capability Profile

- 1 General
- 2 Platform**
- 3 Protocol
- 4 Performance
- 5 Storage attributes
- 6 Summary

### Platform

Platform: Performance

Asymmetric:

CANCEL

BACK

NEXT

4. A continuación, seleccione la opción de protocolo o \* cualquiera \* para permitir todos los protocolos posibles. Haga clic en **Siguiente** para continuar.

## Create Storage Capability Profile

- 1 General
- 2 Platform
- 3 Protocol**
- 4 Performance
- 5 Storage attributes
- 6 Summary

### Protocol

Protocol: Any

- Any
- FCP
- iSCSI
- NVMe/FC

CANCEL

BACK

NEXT

5. La página **PERFORMANCE** permite establecer la calidad del servicio en forma de IOPS mínima y máxima permitida.

## Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

## Performance

None ⓘ

QoS policy group ⓘ

Min IOPS:

\_\_\_\_\_

Max IOPS:

6000

Unlimited

CANCEL

BACK

NEXT

6. Complete la página **atributos de almacenamiento** seleccionando eficiencia de almacenamiento, reserva de espacio, cifrado y cualquier política de organización en niveles según sea necesario.

## Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

## Storage attributes

Deduplication:

Yes

Compression:

Yes

Space reserve:

Thin

Encryption:

No

Tiering policy (FabricPool):

None

CANCEL

BACK

NEXT

7. Por último, revise el resumen y haga clic en Finalizar para crear el perfil.

## Create Storage Capability Profile

- 1 General
- 2 Platform
- 3 Protocol
- 4 Performance
- 5 Storage attributes
- 6 Summary**

## Summary

Name:	ASA_Gold_iSCSI
Description:	N/A
Platform:	Performance
Asymmetric:	No
Protocol:	Any
Max IOPS:	6000 IOPS
Space reserve:	Thin
Deduplication:	Yes
Compression:	Yes
Encryption:	Yes
Tiering policy (FabricPool):	None

CANCEL

BACK

FINISH



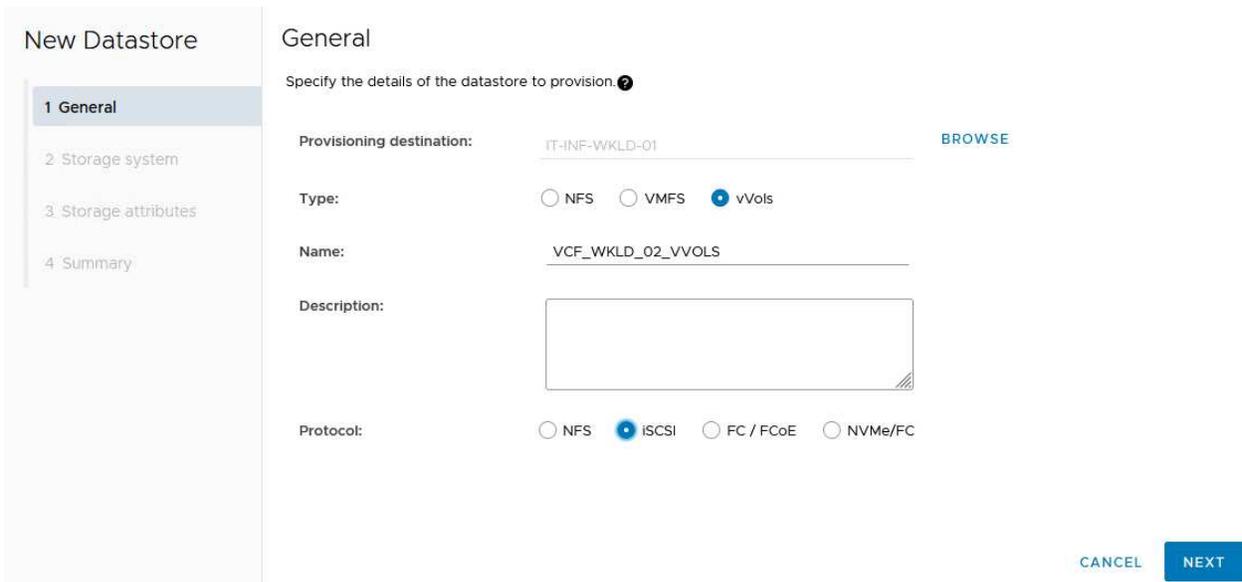
## Cree un almacén de datos vVols en Herramientas de ONTAP

Para crear un almacén de datos vVols en Herramientas de ONTAP, lleve a cabo los siguientes pasos:

1. En Herramientas de ONTAP seleccione **Descripción general** y en la pestaña **Introducción** haga clic en **Provisión** para iniciar el asistente.



2. En la página **General** del asistente New Datastore, seleccione el centro de datos de vSphere o el destino del clúster. Seleccione **vVols** como tipo de almacén de datos, rellene un nombre para el almacén de datos y seleccione **iSCSI** como protocolo. Haga clic en **Siguiente** para continuar.



3. En la página **Sistema de almacenamiento**, seleccione el perfil de capacidad de almacenamiento, el sistema de almacenamiento y SVM. Haga clic en **Siguiente** para continuar.

## New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

### Storage system

Specify the storage capability profiles and the storage system you want to use.

Storage capability profiles:

- AFF\_Encrypted\_Min50\_ASA\_A
- FAS\_Default
- FAS\_Max20
- Custom profiles
- ASA\_Gold\_iSCSI

Storage system: ntaphci-a300e9u25 (172.16.9.25)

Storage VM: VCF\_iSCSI

CANCEL BACK NEXT

4. En la página **Atributos de almacenamiento**, seleccione crear un nuevo volumen para el almacén de datos y completar los atributos de almacenamiento del volumen que se va a crear. Haga clic en **Agregar** para crear el volumen y luego en **Siguiente** para continuar.

## New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

### Storage attributes

Specify the storage details for provisioning the datastore.

Volumes:  Create new volumes  Select volumes

Create new volumes

Name	Size	Storage Capability Profile	Aggregate
 FlexVol volumes are not added.			

Name	Size(GB) ⓘ	Storage capability profile	Aggregates	Space reserve
f_wkld_02_vvols	3000	ASA_Gold_iSCSI	EHCaggr02 - (27053.3 GE)	Thin

CANCEL BACK NEXT

5. Por último, revise el resumen y haga clic en **Finish** para iniciar el proceso de creación del almacén de datos de VVol.

### New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

### Summary

**Datstore type:** vVols  
**Protocol:** iSCSI  
**Storage capability profile:** ASA\_Gold\_iSCSI

**Storage system details**  
**Storage system:** ntaphcl-a300e9u25  
**SVM:** VCF\_iSCSI

**Storage attributes**

New FlexVol Name	New FlexVol Size	Aggregate	Storage Capability Profile
vcf_wkld_02_vvols	3000 GB	EHCAggr02	ASA_Gold_iSCSI

Click 'Finish' to provision this datastore.

CANCEL BACK FINISH

## Información adicional

Para obtener información acerca de la configuración de los sistemas de almacenamiento ONTAP, consulte la ["Documentación de ONTAP 9"](#) centro.

Para obtener información sobre la configuración de VCF, consulte ["Documentación de VMware Cloud Foundation"](#).

## Configurar el almacenamiento complementario NVMe/TCP para dominios de carga de trabajo de VCF

Autor: Josh Powell

### Configurar el almacenamiento complementario NVMe/TCP para dominios de carga de trabajo de VCF

#### Descripción general del escenario

En esta situación, mostraremos cómo configurar el almacenamiento complementario NVMe/TCP para un dominio de carga de trabajo de VCF.

Este escenario cubre los siguientes pasos de alto nivel:

- Cree una máquina virtual de almacenamiento (SVM) con interfaces lógicas (LIF) para el tráfico NVMe/TCP.
- Cree grupos de puertos distribuidos para redes iSCSI en el dominio de carga de trabajo de VI.
- Cree adaptadores vmkernel para iSCSI en los hosts ESXi para el dominio de carga de trabajo VI.
- Añada adaptadores NVMe/TCP en los hosts ESXi.
- Implemente un almacén de datos NVMe/TCP.

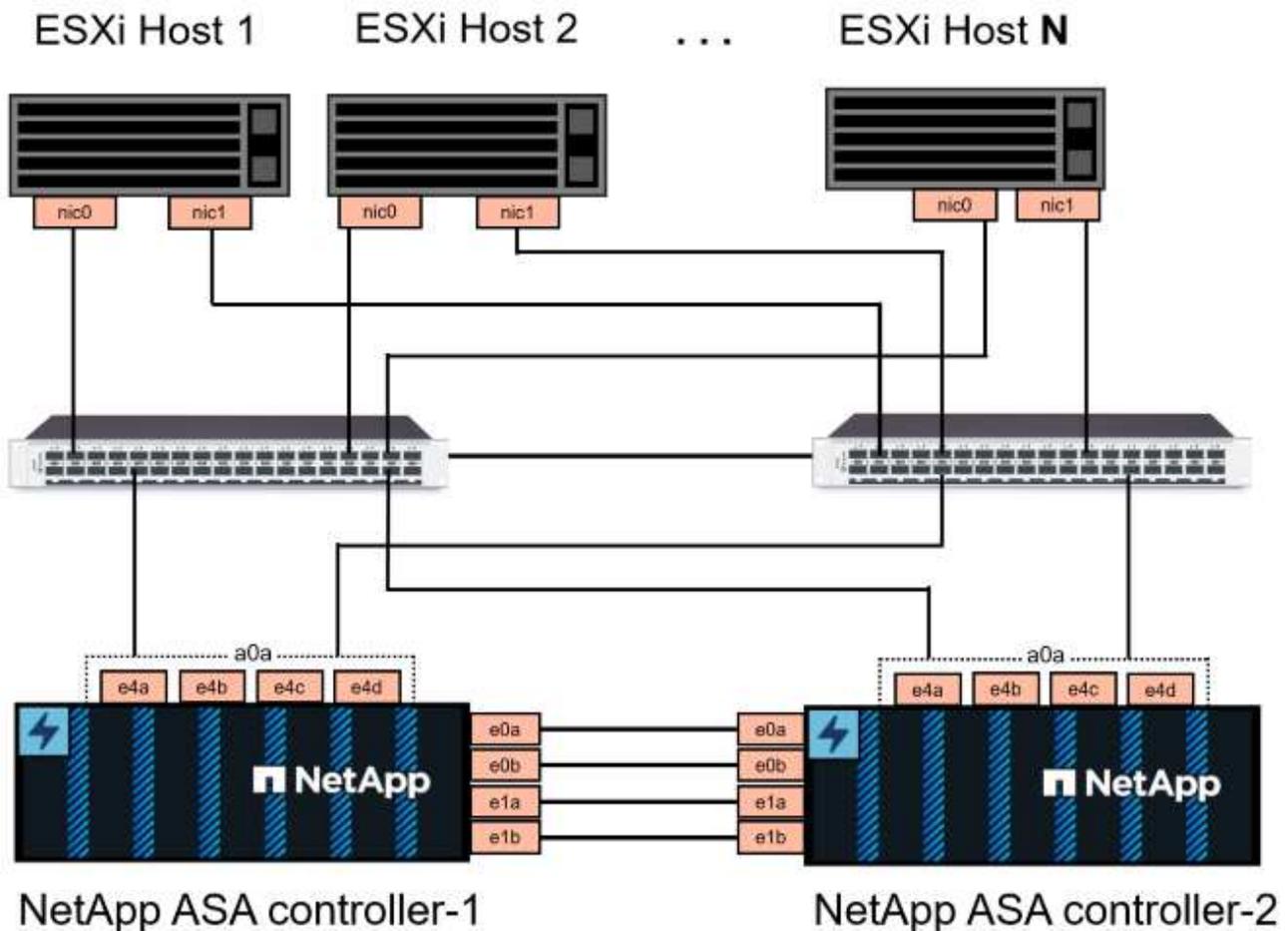
#### Requisitos previos

Este escenario requiere los siguientes componentes y configuraciones:

- Un sistema de almacenamiento de ONTAP ASA con puertos de datos físicos en switches ethernet dedicados al tráfico de almacenamiento.

- La puesta en marcha del dominio de gestión de VCF está completa y se puede acceder al cliente vSphere.
- Se ha desplegado anteriormente un dominio de carga de trabajo de VI.

NetApp recomienda diseños de red totalmente redundantes para NVMe/TCP. En el siguiente diagrama se muestra un ejemplo de una configuración redundante, que proporciona tolerancia a fallos para los sistemas de almacenamiento, los switches, los adaptadores de red y los sistemas host. Consulte NetApp ["Referencia para la configuración DE SAN"](#) para obtener más información.



Para la multivía y la conmutación al nodo de respaldo en varias rutas, NetApp recomienda tener un mínimo de dos LIF por nodo de almacenamiento en redes ethernet independientes para todas las SVM en las configuraciones de NVMe/TCP.

Esta documentación muestra el proceso de crear una SVM nueva y especificar la información de dirección IP para crear varias LIF para el tráfico NVMe/TCP. Para agregar LIF nuevos a una SVM existente, consulte ["Crear una LIF \(interfaz de red\)"](#).

Si quiere más información sobre las consideraciones de diseño de NVMe para sistemas de almacenamiento ONTAP, consulte ["Configuración, compatibilidad y limitaciones de NVMe"](#).

## Pasos de despliegue

Para crear un almacén de datos VMFS en un dominio de carga de trabajo de VCF con NVMe/TCP, complete los siguientes pasos.

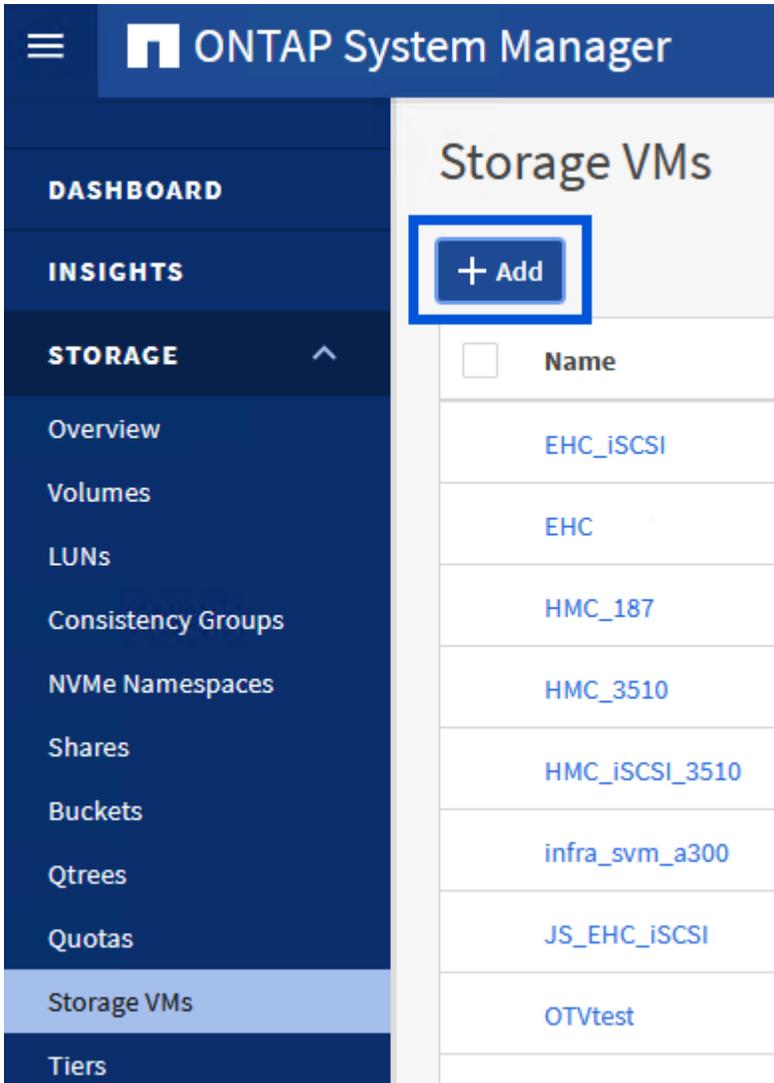
## **Crear SVM, LIF y espacio de nombres de NVMe en el sistema de almacenamiento ONTAP**

El siguiente paso se lleva a cabo en ONTAP System Manager.

## Crear la máquina virtual de almacenamiento y las LIF

Complete los siguientes pasos para crear una SVM junto con varias LIF para el tráfico NVMe/TCP.

1. Desde el Administrador del sistema de ONTAP navegue hasta **VM de almacenamiento** en el menú de la izquierda y haga clic en **+ Agregar** para comenzar.



2. En el asistente de **Add Storage VM**, proporcione un **Name** para la SVM, seleccione **IP Space** y, a continuación, en **Access Protocol**, haga clic en la pestaña **NVMe** y marque la casilla **Enable NVMe/TCP**.

## Add Storage VM



STORAGE VM NAME

VCF\_NVMe

IPSPACE

Default

### Access Protocol

SMB/CIFS, NFS, S3

iSCSI

FC

NVMe

Enable NVMe/FC

Enable NVMe/TCP

3. En la sección **Interfaz de red**, rellena la **Dirección IP**, **Máscara de subred** y **Dominio de difusión y puerto** para la primera LIF. En el caso de las LIF posteriores, la casilla de verificación puede estar activada para utilizar una configuración común en todas las LIF restantes, o utilizar una configuración independiente.



Para la multivía y la conmutación al nodo de respaldo en varias rutas, NetApp recomienda tener un mínimo de dos LIF por nodo de almacenamiento en redes Ethernet independientes para todas las SVM en las configuraciones de NVMe/TCP.

## NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS

172.21.118.189

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN AND PORT 

NFS\_iSCSI 

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

IP ADDRESS

172.21.119.189

PORT

a0a-3375 

ntaphci-a300-02

IP ADDRESS

172.21.118.190

PORT

a0a-3374 

IP ADDRESS

172.21.119.190

PORT

a0a-3375 

## Storage VM Administration

Manage administrator account

**Save**

Cancel

4. Elija si desea activar la cuenta de administración de Storage VM (para entornos multi-tenancy) y haga clic en **Guardar** para crear la SVM.

## Storage VM Administration

Manage administrator account

Save

Cancel

## Cree el espacio de nombres de NVMe

Los espacios de nombres de NVMe son análogos a las LUN para iSCSI o FC. Se debe crear el espacio de nombres de NVMe antes de que se pueda implementar un almacén de datos VMFS desde vSphere Client. Para crear el espacio de nombres NVMe, primero se debe obtener el nombre completo de NVMe (NQN) desde cada host ESXi del clúster. ONTAP utiliza el NQN para proporcionar control de acceso al espacio de nombres.

Complete los siguientes pasos para crear un espacio de nombres NVMe:

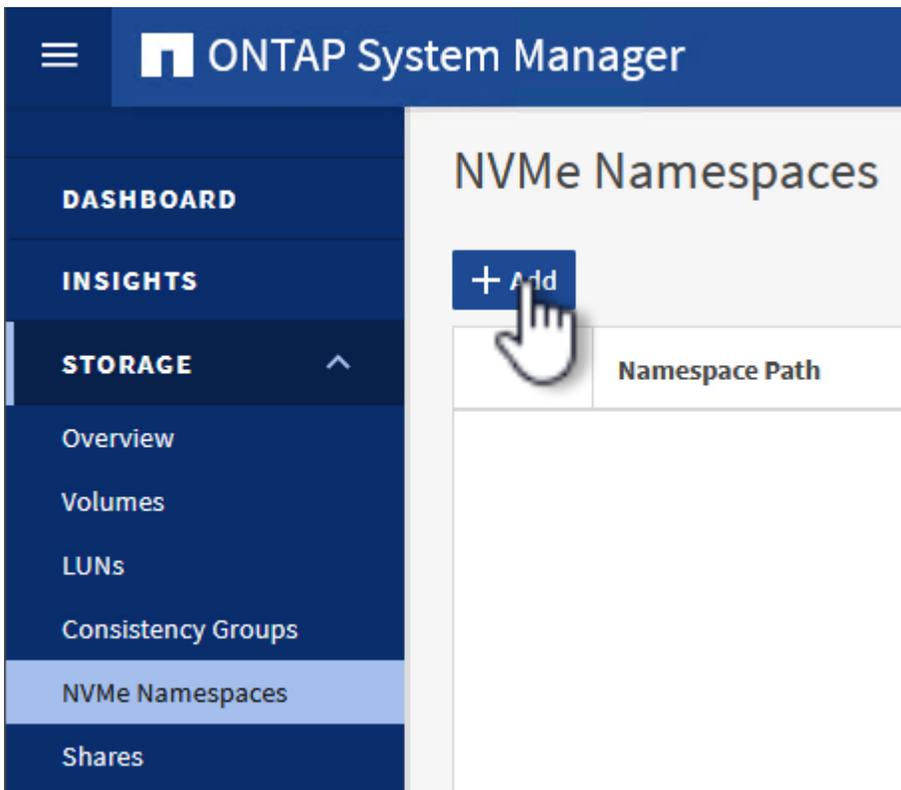
1. Abra una sesión SSH con un host ESXi del clúster para obtener el NQN. Utilice el siguiente comando de la CLI:

```
esxcli nvme info get
```

Debería aparecer una salida similar a la siguiente:

```
Host NQN: nqn.2014-08.com.netapp.sddc:nvme:vcf-wkld-esx01
```

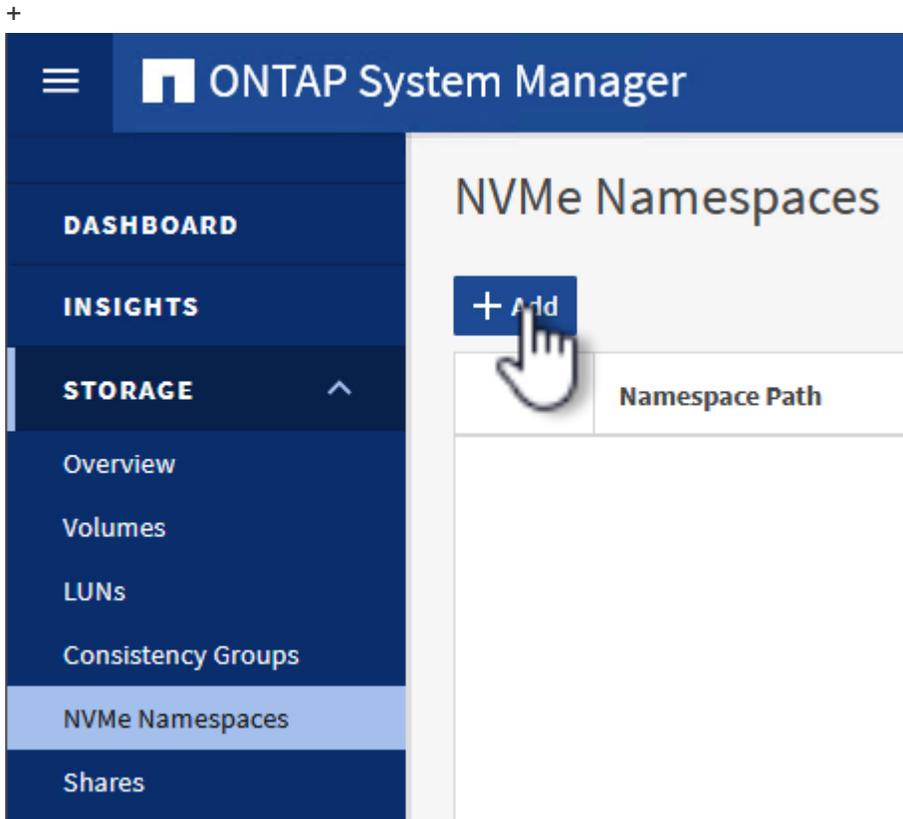
2. Registre el NQN de cada host ESXi del clúster
3. Desde el Administrador del sistema de ONTAP, navegue hasta **Espacios de nombres de NVMe** en el menú de la izquierda y haga clic en **+ Agregar** para comenzar.



4. En la página **Add NVMe Namespace**, rellene un prefijo de nombre, el número de espacios de

nombres que se van a crear, el tamaño del espacio de nombres y el sistema operativo host que accederá al espacio de nombres. En la sección **Host NQN** cree una lista separada por comas de los NQN previamente recopilados de los hosts ESXi que accederán a los espacios de nombres.

Haga clic en **Más opciones** para configurar elementos adicionales como la política de protección de instantáneas. Por último, haga clic en **Save** para crear el espacio de nombres NVMe.



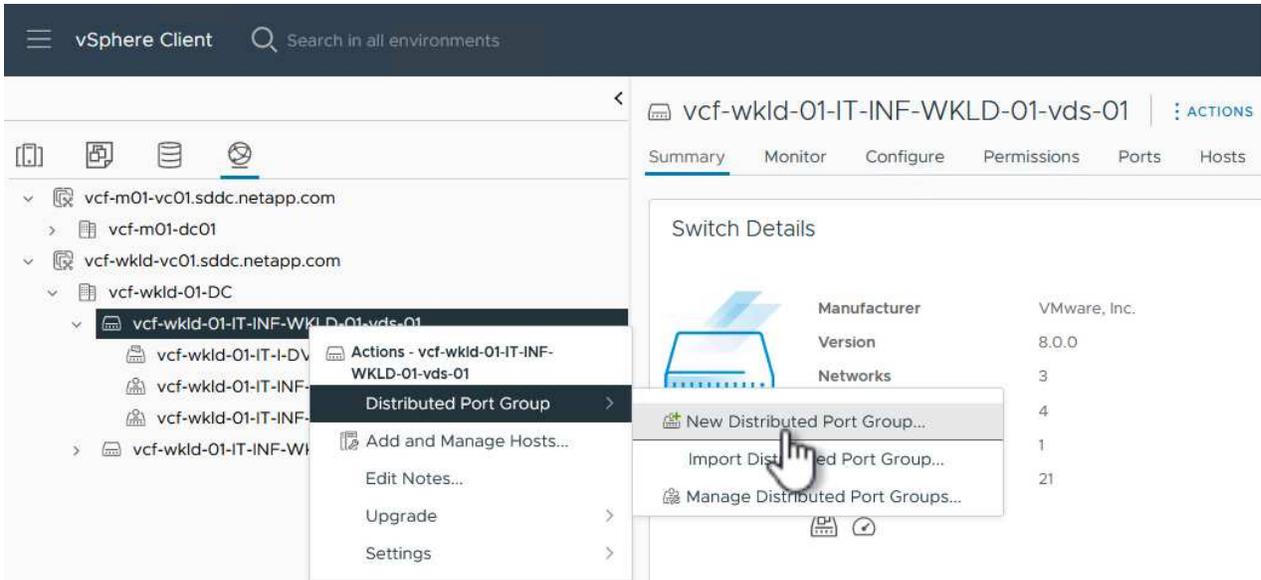
### Configure los adaptadores de red y de software NVMe en hosts ESXi

Los siguientes pasos se realizan en el clúster de dominio de cargas de trabajo de VI utilizando el cliente de vSphere. En este caso, se utiliza vCenter Single Sign-On para que el cliente vSphere sea común a los dominios de carga de trabajo y de gestión.

## Cree grupos de puertos distribuidos para el tráfico de NVMe/TCP

Complete lo siguiente para crear un nuevo grupo de puertos distribuidos para cada red NVMe/TCP:

1. En el cliente vSphere , desplácese hasta **Inventory > Networking** para el dominio de la carga de trabajo. Navegue hasta el conmutador distribuido existente y elija la acción para crear **Nuevo grupo de puertos distribuidos...**



2. En el asistente de **New Distributed Port Group**, introduzca un nombre para el nuevo grupo de puertos y haga clic en **Next** para continuar.
3. En la página **Configure settings**, complete todos los ajustes. Si se utilizan VLAN, asegúrese de proporcionar el identificador de VLAN correcto. Haga clic en **Siguiente** para continuar.

## New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

### Configure settings

Set general properties of the new port group.

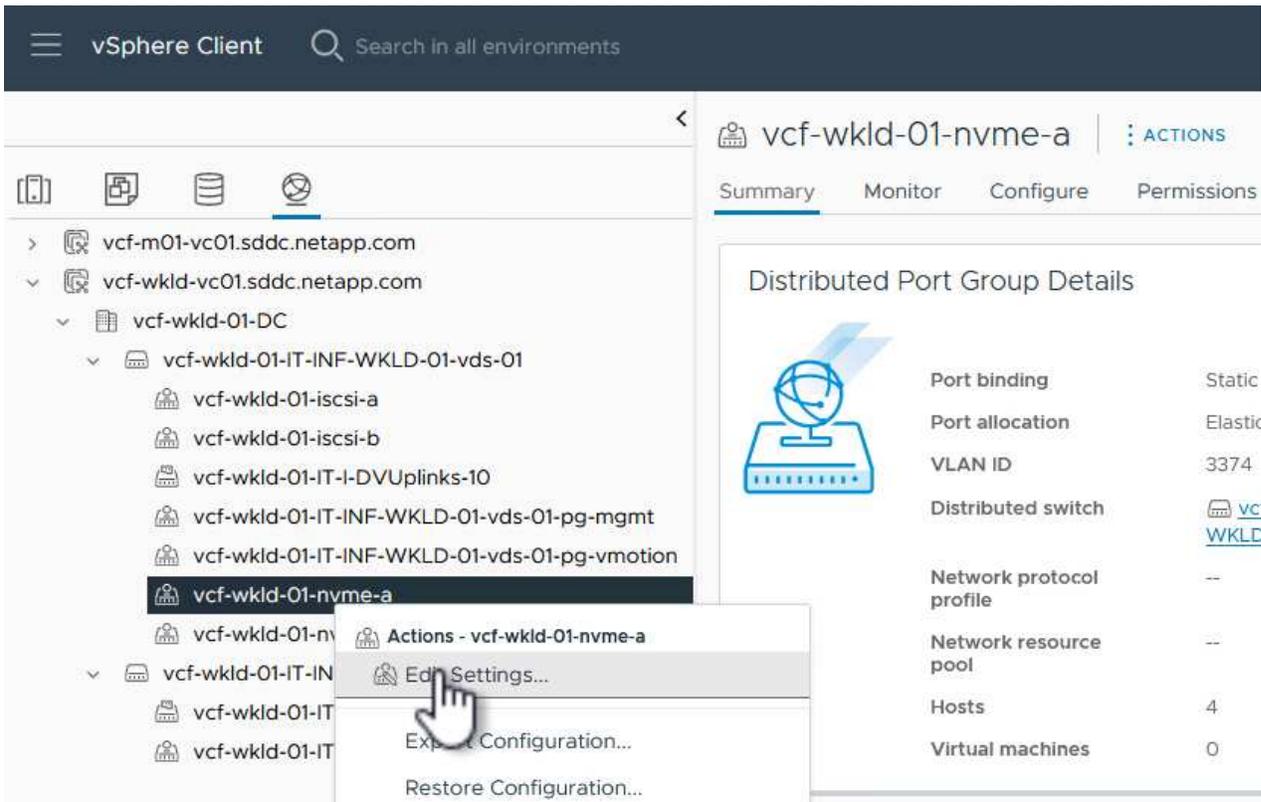
Port binding	Static binding
Port allocation	Elastic ⓘ
Number of ports	8
Network resource pool	(default)
VLAN	
VLAN type	VLAN
VLAN ID	3374
Advanced	
<input type="checkbox"/> Customize default policies configuration	

CANCEL

BACK

**NEXT**

4. En la página **Listo para completar**, revise los cambios y haga clic en **Finalizar** para crear el nuevo grupo de puertos distribuidos.
5. Repita este proceso para crear un grupo de puertos distribuidos para la segunda red NVMe/TCP que se esté utilizando y asegúrese de que ha introducido el **VLAN ID** correcto.
6. Una vez que ambos grupos de puertos han sido creados, navegue al primer grupo de puertos y seleccione la acción para **Editar configuración....**



- En la página **Distributed Port Group - Edit Settings**, navega a **Teaming and failover** en el menú de la izquierda y haz clic en **uplink2** para moverlo hacia abajo a **Uplinks sin usar**.

## Distributed Port Group - Edit Settings | vcf-wkld-01-nvme-a

General

Advanced

VLAN

Security

Traffic shaping

**Teaming and failover**

Monitoring

Miscellaneous

**Load balancing** Route based on originating virtual port

**Network failure detection** Link status only

**Notify switches** Yes

**Failback** Yes

**Failover order** ⓘ

MOVE UP MOVE DOWN

**Active uplinks**

uplink1

**Standby uplinks**

**Unused uplinks**

uplink2

- Repita este paso para el segundo grupo de puertos NVMe/TCP. Sin embargo, esta vez mueva

**uplink1** hacia abajo a **Uplinks sin usar**.

## Distributed Port Group - Edit Settings | vcf-wkld-01-nvme-b

General

Advanced

VLAN

Security

Traffic shaping

**Teaming and fallover**

Monitoring

Miscellaneous

**Load balancing**

Route based on originating virtual por

**Network failure detection**

Link status only

**Notify switches**

Yes

**Failback**

Yes

Failover order 

[MOVE UP](#) [MOVE DOWN](#)

**Active uplinks**

uplink2

**Standby uplinks**

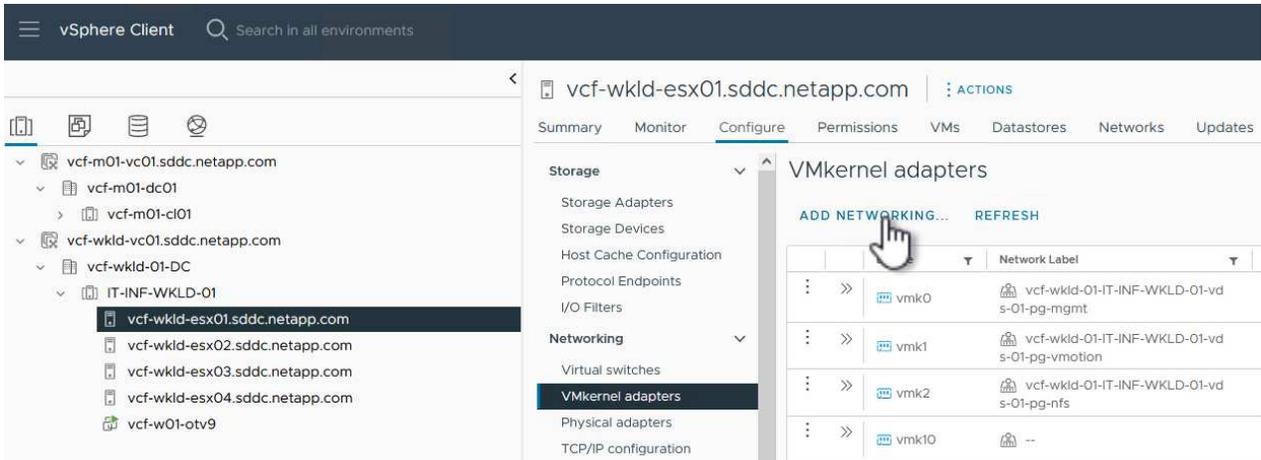
**Unused uplinks**

uplink1

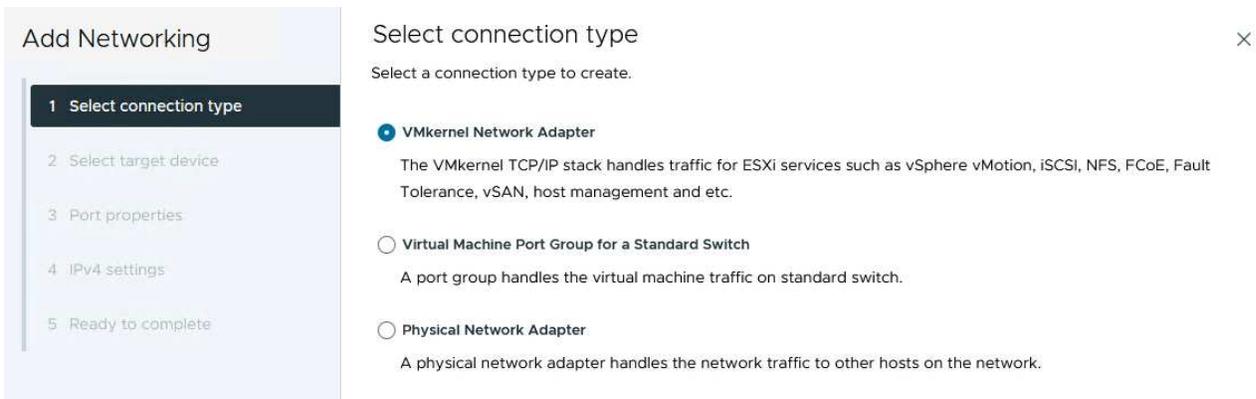
## Crear adaptadores de VMkernel en cada host ESXi

Repita este proceso en cada host ESXi del dominio de la carga de trabajo.

1. En el cliente de vSphere, desplácese hasta uno de los hosts ESXi en el inventario de dominio de la carga de trabajo. En la pestaña **Configure**, seleccione **VMkernel adapter** y haga clic en **Add Networking...** para comenzar.



2. En la ventana **Seleccionar tipo de conexión**, elija **Adaptador de red VMkernel** y haga clic en **Siguiente** para continuar.



3. En la página **Seleccionar dispositivo de destino**, elija uno de los grupos de puertos distribuidos para iSCSI que se crearon anteriormente.

## Add Networking

- 1 Select connection type
- 2 Select target device**
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

## Select target device



Select a target device for the new connection.

- Select an existing network
- Select an existing standard switch
- New standard switch

Quick Filter

Enter value

	Name	NSX Port Group ID	Distributed Switch
<input type="radio"/>	vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input checked="" type="radio"/>	vcf-wkld-01-nvme-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-nvme-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

Manage Columns 7 Items

CANCEL

BACK

NEXT



Packages

4. En la página **Propiedades del puerto** haga clic en la casilla **NVMe sobre TCP** y haga clic en **Siguiente** para continuar.

### Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

### Port properties

Specify VMkernel port settings.

**Network label**

**MTU**

**TCP/IP stack**

**Available services**

**Enabled services**

<input checked="" type="checkbox"/> vMotion	<input type="checkbox"/> vSphere Replication NFC	<input type="checkbox"/> NVMe over RDMA
<input type="checkbox"/> Provisioning	<input type="checkbox"/> vSAN	
<input type="checkbox"/> Fault Tolerance logging	<input type="checkbox"/> vSAN Witness	
<input type="checkbox"/> Management	<input type="checkbox"/> vSphere Backup NFC	
<input type="checkbox"/> vSphere Replication	<input checked="" type="checkbox"/> NVMe over TCP	

CANCEL BACK NEXT

5. En la página **IPv4 settings**, rellena la **IP address**, **Subnet mask** y proporciona una nueva dirección IP de Gateway (solo si es necesario). Haga clic en **Siguiente** para continuar.

### Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

### IPv4 settings

Specify VMkernel IPv4 settings.

Obtain IPv4 settings automatically

Use static IPv4 settings

**IPv4 address**

**Subnet mask**

**Default gateway**  Override default gateway for this adapter

**DNS server addresses**

6. Revise sus selecciones en la página **Listo para completar** y haga clic en **Finalizar** para crear el adaptador VMkernel.

## Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

## Ready to complete

Review your selections before finishing the wizard

### ▼ Select target device

Distributed port group	vcf-wkld-01-nvme-a
Distributed switch	vcf-wkld-01-IT-INF-WKLD-01-vds-01

### ▼ Port properties

New port group	vcf-wkld-01-nvme-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)
MTU	9000
vMotion	Disabled
Provisioning	Disabled
Fault Tolerance logging	Disabled
Management	Disabled
vSphere Replication	Disabled
vSphere Replication NFC	Disabled
vSAN	Disabled
vSAN Witness	Disabled
vSphere Backup NFC	Disabled
NVMe over TCP	Enabled
NVMe over RDMA	Disabled

### ▼ IPv4 settings

IPv4 address	172.21.118.191 (static)
Subnet mask	255.255.255.0

CANCEL

BACK

FINISH

Packages

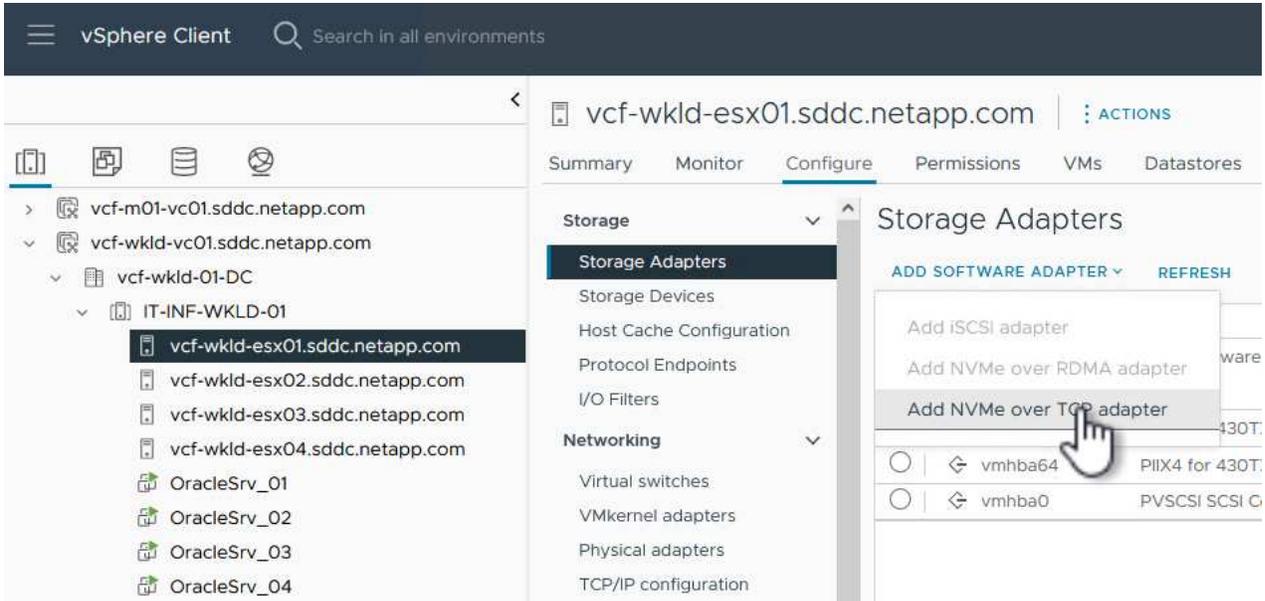
7. Repita este proceso para crear un adaptador de VMkernel para la segunda red iSCSI.

## Añada el adaptador NVMe over TCP

Cada host ESXi en el clúster de dominio de carga de trabajo debe tener un adaptador de software NVMe over TCP instalado para cada red NVMe/TCP establecida dedicada al tráfico de almacenamiento.

Para instalar los adaptadores NVMe over TCP y detectar las controladoras NVMe, complete los pasos siguientes:

1. En el cliente de vSphere, desplácese hasta uno de los hosts ESXi del clúster de dominio de la carga de trabajo. En la pestaña **Configurar**, haga clic en **Adaptadores de almacenamiento** en el menú y, a continuación, en el menú desplegable **Agregar adaptador de software**, seleccione **Agregar adaptador NVMe sobre TCP**.



2. En la ventana **Add Software NVMe over TCP adapter**, accede al menú desplegable **Physical Network Adapter** y selecciona el adaptador de red físico correcto en el que habilitar el adaptador NVMe.

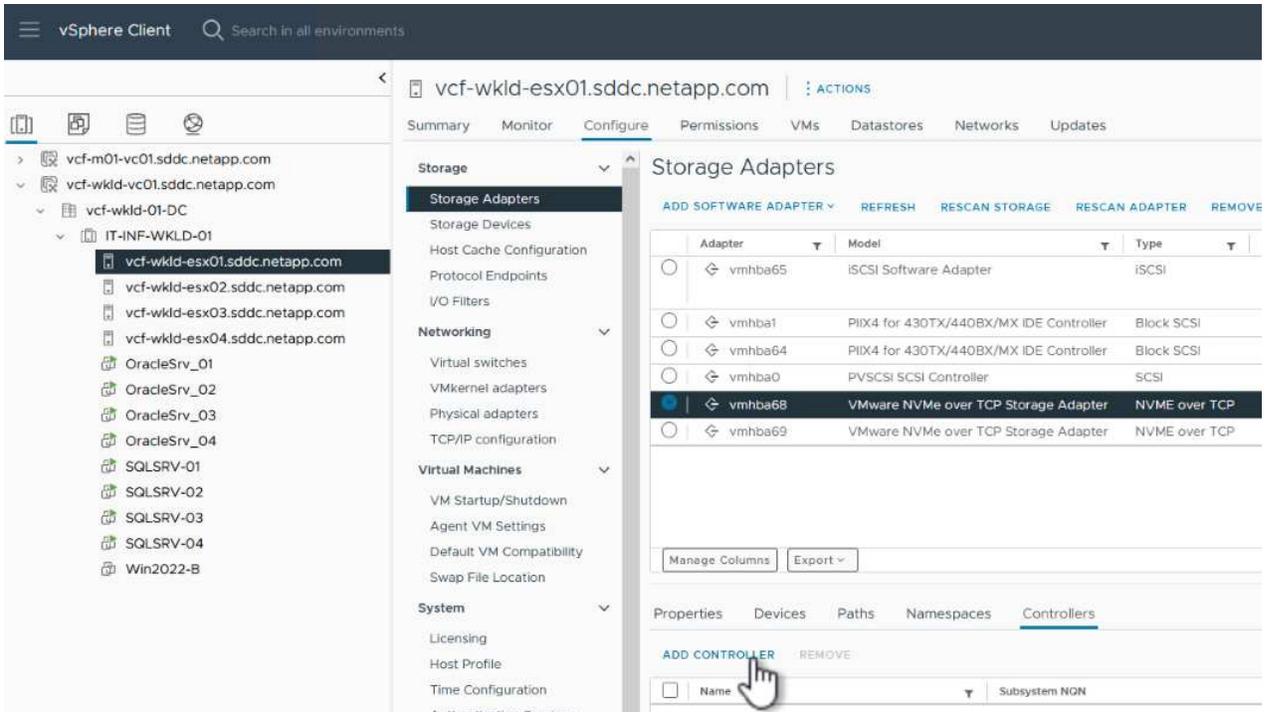
Add Software NVMe over TCP adapter | vcf-wkld-esx01.sddc.netapp.com

Enable software NVMe adapter on the selected physical network adapter.

Physical Network Adapter



3. Repita este proceso para la segunda red asignada al tráfico NVMe over TCP, asignando el adaptador físico correcto.
4. Seleccione uno de los adaptadores NVMe over TCP recién instalados y, en la pestaña **Controladores**, seleccione **Agregar controlador**.



5. En la ventana **Agregar controlador**, seleccione la pestaña **Automáticamente** y complete los siguientes pasos.
  - Rellene direcciones IP para una de las interfaces lógicas de SVM en la misma red que el adaptador físico asignado a este adaptador de NVMe over TCP.
  - Haga clic en el botón **Discover Controllers**.
  - En la lista de controladoras detectadas, haga clic en la casilla de comprobación de las dos controladoras con direcciones de red alineadas con este adaptador NVMe over TCP.
  - Haga clic en el botón **OK** para agregar los controladores seleccionados.

## Add controller | vmhba68



Automatically

Manually

Host NQN

nqn.2014-08.com.netapp.sddc:nvme:vcf-wkld-...

COPY

IP



172.21.118.189

Enter IPv4 / IPv6 address

Central discovery controller

Port Number

Range more from 0

Digest parameter

Header digest

Data digest

DISCOVER CONTROLLERS



Select which controller to connect

<input type="checkbox"/>	Id	Subsystem NQN	Transport Type	IP	Port Number
<input checked="" type="checkbox"/>	65535	nqn.1992-08.com.netapp:sn.64df3069fb6411eea55100a098b46a21:subsystem.VCF_WKLD_04_NVMe_VCF_WKLD_04_NVMe	nvm	172.21.118.189	4420
<input checked="" type="checkbox"/>	65535	nqn.1992-08.com.netapp:sn.64df3069fb6411eea55100a098b46a21:subsystem.VCF	nvm	172.21.118.190	4420

Manage Columns 4 items



OK

- Después de unos segundos, es recomendable que aparezca el espacio de nombres de NVMe en la pestaña Devices.

## Storage Adapters

ADD SOFTWARE ADAPTER ▾ REFRESH RESCAN STORAGE RESCAN ADAPTER REMOVE

Adapter	Model	Type	Status	Identifier	Targets	Devices	Paths
vmhba65	iSCSI Software Adapter	iSCSI	Online	iscsi_vmk(iqn.1998-01.com.vmware:vcf-wkld-esx01.sddc.net app.com:794177624:65)	4	2	8
vmhba1	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	1	1	1
vmhba64	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	0	0	0
vmhba0	PVSCSI SCSI Controller	SCSI	Unknown	--	3	3	3
vmhba68	VMware NVMe over TCP Storage Adapter	NVME over TCP	Online	--	1	1	1
vmhba69	VMware NVMe over TCP Storage Adapter	NVME over TCP	Online	--	0	0	0

Manage Columns Export ▾ 6 items

Properties **Devices** Paths Namespaces Controllers

REFRESH ATTACH DETACH RENAME

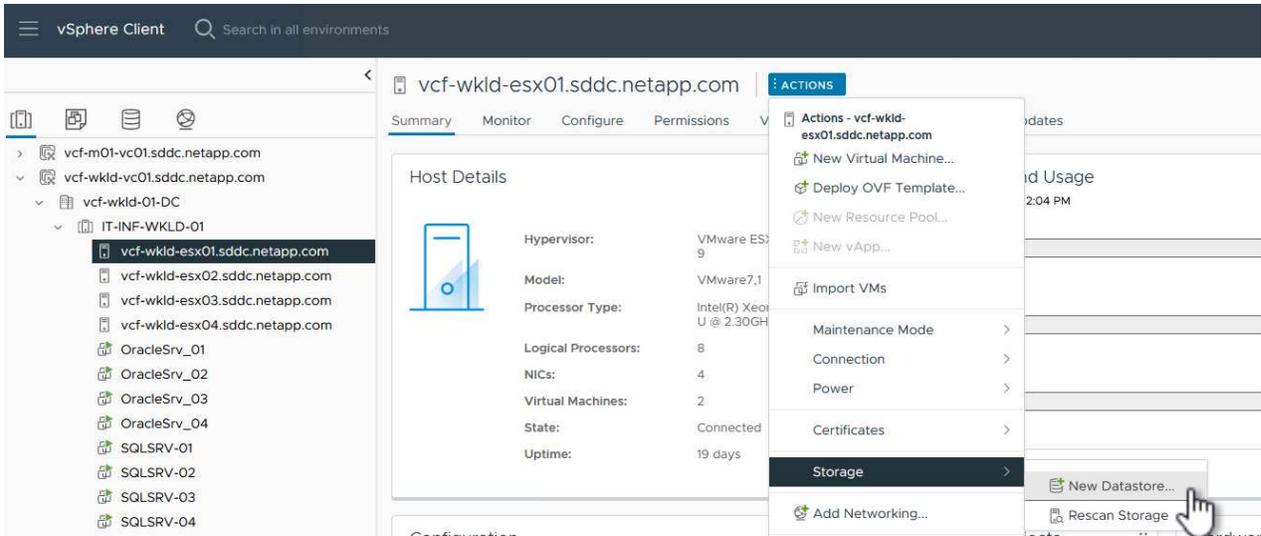
Name	LUN	Type	Capacity	Datastore	Operational State	Hardware Acceleration	Drive Type	Transport
NVMe TCP Disk (uuid.929a6a9045764784 9146e09d6e55b076)	0	disk	3.00 TB	Not Consumed	Attached	Supported	Flash	TCPTRA RT

7. Repita este procedimiento para crear un adaptador NVMe over TCP para la segunda red establecida para el tráfico NVMe/TCP.

## Ponga en marcha un almacén de datos de NVMe sobre TCP

Para crear un almacén de datos VMFS en el espacio de nombres de NVMe, complete los siguientes pasos:

1. En el cliente de vSphere, desplácese hasta uno de los hosts ESXi del clúster de dominio de la carga de trabajo. En el menú **Acciones**, selecciona **Almacenamiento > Nuevo Datastore...**



2. En el asistente **New Datastore**, seleccione **VMFS** como tipo. Haga clic en **Siguiente** para continuar.
3. En la página **Nombre y selección de dispositivos**, proporcione un nombre para el almacén de datos y seleccione el espacio de nombres NVMe de la lista de dispositivos disponibles.

## New Datastore

1 Type

2 Name and device selection

3 VMFS version

4 Partition configuration

5 Ready to complete

## Name and device selection

×

Specify datastore name and a disk/LUN for provisioning the datastore.

Name VCF\_WKLD\_04\_NVMe

	Name	LUN	Capacity	Hardware Acceleration	Drive Type	Sector Format	Cl V S
<input checked="" type="radio"/>	NVMe TCP Disk (uuid.929a6a90457647849146e09d6e55b076)	0	3.00 TB	Supported	Flash	512e	N
<input type="radio"/>	Local VMware Disk (naa.6000c29f83dcf1e42d230340deb66036)	0	4.00 GB	Not supported	Flash	512n	N
<input type="radio"/>	Local VMware Disk (naa.6000c291464644a835bc23d384813ac0)	0	75.00 GB	Not supported	Flash	512n	N

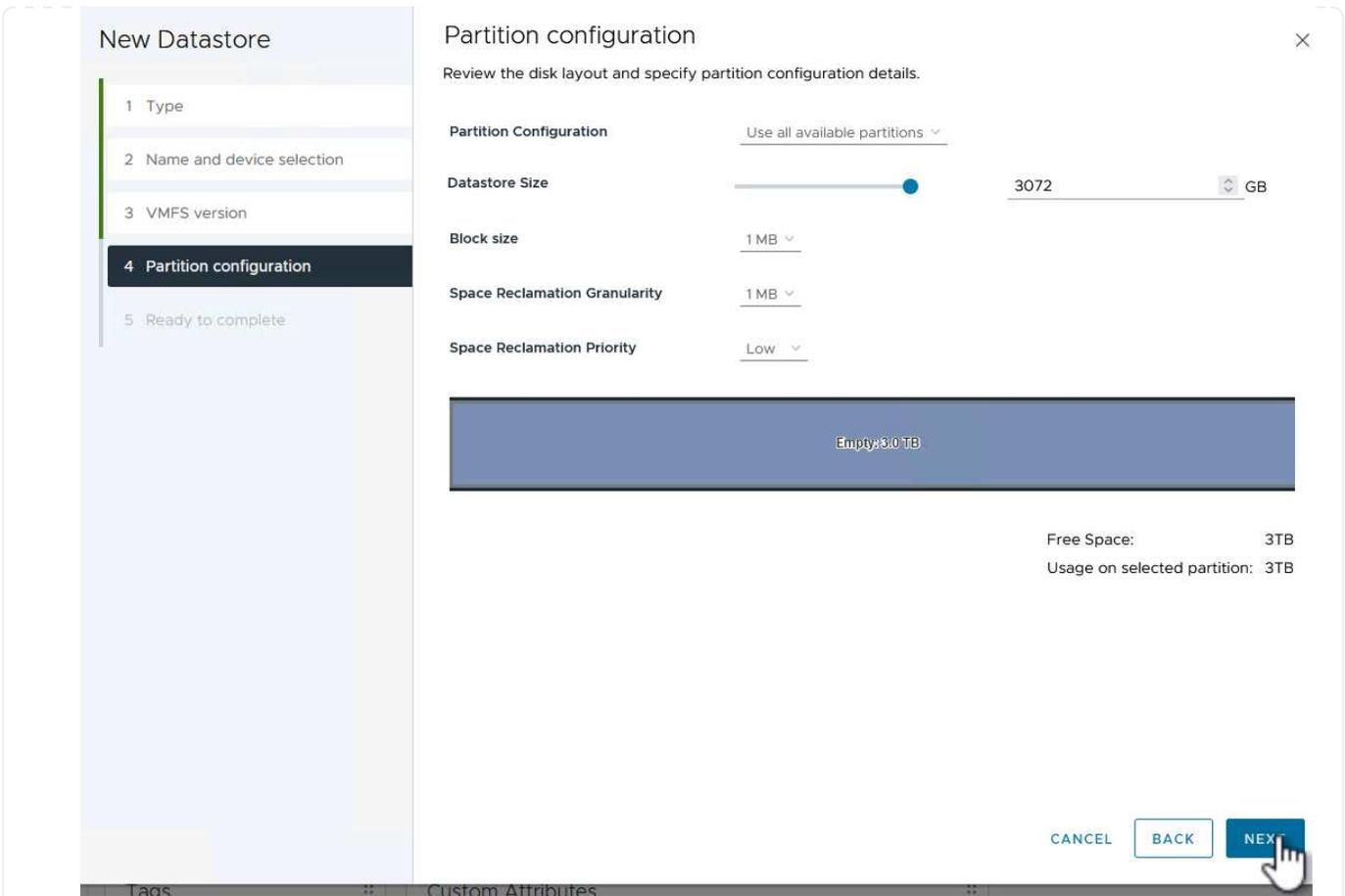
Manage Columns Export 3 items

CANCEL

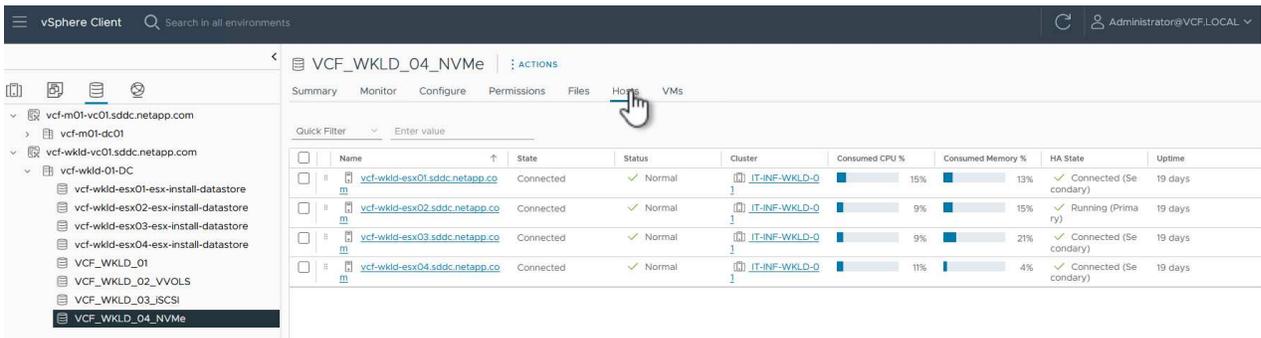
BACK

NEXT

4. En la página **VMFS version** seleccione la versión de VMFS para el almacén de datos.
5. En la página **Configuración de partición**, realice los cambios deseados en el esquema de partición predeterminado. Haga clic en **Siguiente** para continuar.



6. En la página **Listo para completar**, revise el resumen y haga clic en **Finalizar** para crear el almacén de datos.
7. Navegue hasta el nuevo almacén de datos en el inventario y haga clic en la pestaña **hosts**. Si se configuró correctamente, todos los hosts ESXi del clúster deben aparecer en la lista y tener acceso al nuevo almacén de datos.



## Información adicional

Para obtener información acerca de la configuración de los sistemas de almacenamiento ONTAP, consulte la ["Documentación de ONTAP 9"](#) centro.

Para obtener información sobre la configuración de VCF, consulte ["Documentación de VMware Cloud Foundation"](#).

## **Utilice el complemento de SnapCenter para VMware vSphere para proteger las máquinas virtuales en los dominios de carga de trabajo de VCF**

Autor: Josh Powell

Utilice el complemento de SnapCenter para VMware vSphere para proteger las máquinas virtuales en los dominios de carga de trabajo de VCF

### **Descripción general del escenario**

En este escenario, mostraremos cómo poner en marcha y utilizar el complemento de SnapCenter para VMware vSphere (SCV) para realizar backups y restaurar máquinas virtuales y almacenes de datos en un dominio de carga de trabajo de VCF. SCV utiliza la tecnología Snapshot de ONTAP para realizar copias de backup rápidas y eficientes de los volúmenes de almacenamiento de ONTAP que alojan almacenes de datos de vSphere. La tecnología SnapMirror y SnapVault se usa para crear backups secundarios en un sistema de almacenamiento independiente y con políticas de retención que imiten el volumen original o pueden ser independientes del volumen original para su retención a largo plazo.

**ISCSI** se utiliza como protocolo de almacenamiento para el almacén de datos VMFS en esta solución.

Este escenario cubre los siguientes pasos de alto nivel:

- Ponga en marcha el plugin de SnapCenter para VMware vSphere (SCV) en el dominio de la carga de trabajo de VI.
- Añada sistemas de almacenamiento a SCV.
- Cree políticas de backup en SCV.
- Cree grupos de recursos en SCV.
- Utilice SCV para realizar backup de almacenes de datos o máquinas virtuales específicas.
- Utilice SCV para restaurar las máquinas virtuales a una ubicación alternativa del clúster.
- Utilice SCV para restaurar archivos en un sistema de archivos Windows.

### **Requisitos previos**

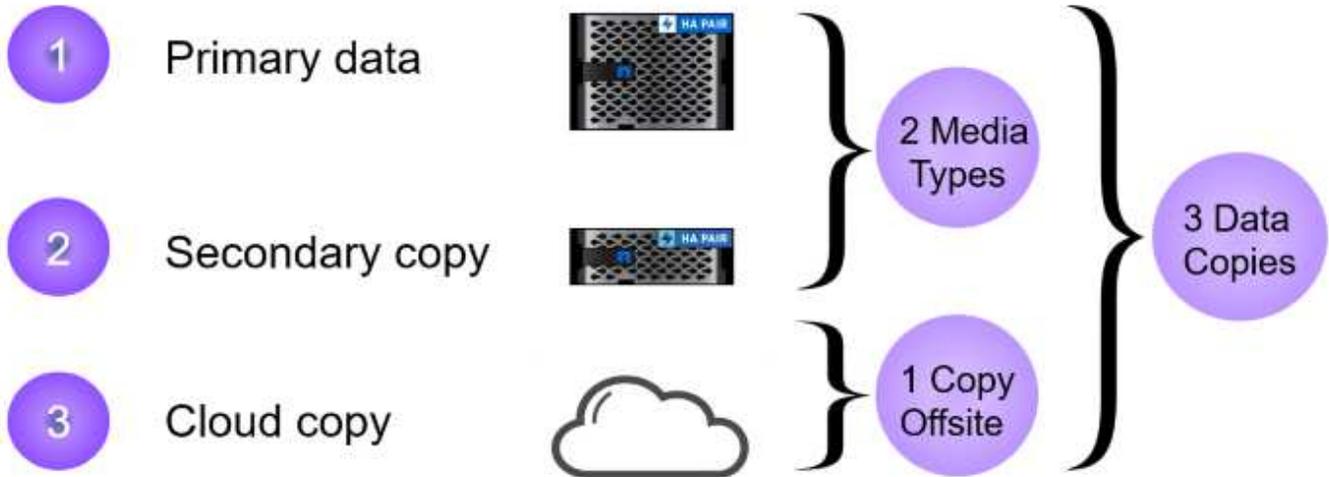
Este escenario requiere los siguientes componentes y configuraciones:

- Un sistema de almacenamiento de ONTAP ASA con almacenes de datos VMFS iSCSI asignados al clúster de dominio de cargas de trabajo.
- Un sistema de almacenamiento secundario de ONTAP configurado para recibir backups secundarios mediante SnapMirror.
- La puesta en marcha del dominio de gestión de VCF está completa y se puede acceder al cliente vSphere.
- Se ha desplegado anteriormente un dominio de carga de trabajo de VI.
- Hay máquinas virtuales en la SCV del clúster designada para proteger.

Para obtener información sobre la configuración de almacenes de datos VMFS iSCSI como almacenamiento complementario, consulte ["ISCSI como almacenamiento complementario para Dominios de Gestión"](#) en esta documentación. El proceso para utilizar OTV para desplegar almacenes de datos es idéntico para los dominios de gestión y carga de trabajo.



Además de replicar los backups realizados con SCV en el almacenamiento secundario, se pueden hacer copias de los datos externos en el almacenamiento de objetos en uno de los tres (3) proveedores de cloud líderes que utilicen el backup y recuperación de datos de NetApp BlueXP para máquinas virtuales. Para obtener más información, consulte la solución "[3-2-1 Protección de datos para VMware con complemento SnapCenter y backup y recuperación de datos de BlueXP para máquinas virtuales](#)".



### Pasos de despliegue

Para implementar el plugin de SnapCenter y utilizarlo para crear backups, y restaurar máquinas virtuales y almacenes de datos, complete los siguientes pasos:

### Implemente y utilice SCV para proteger los datos en un dominio de carga de trabajo de VI

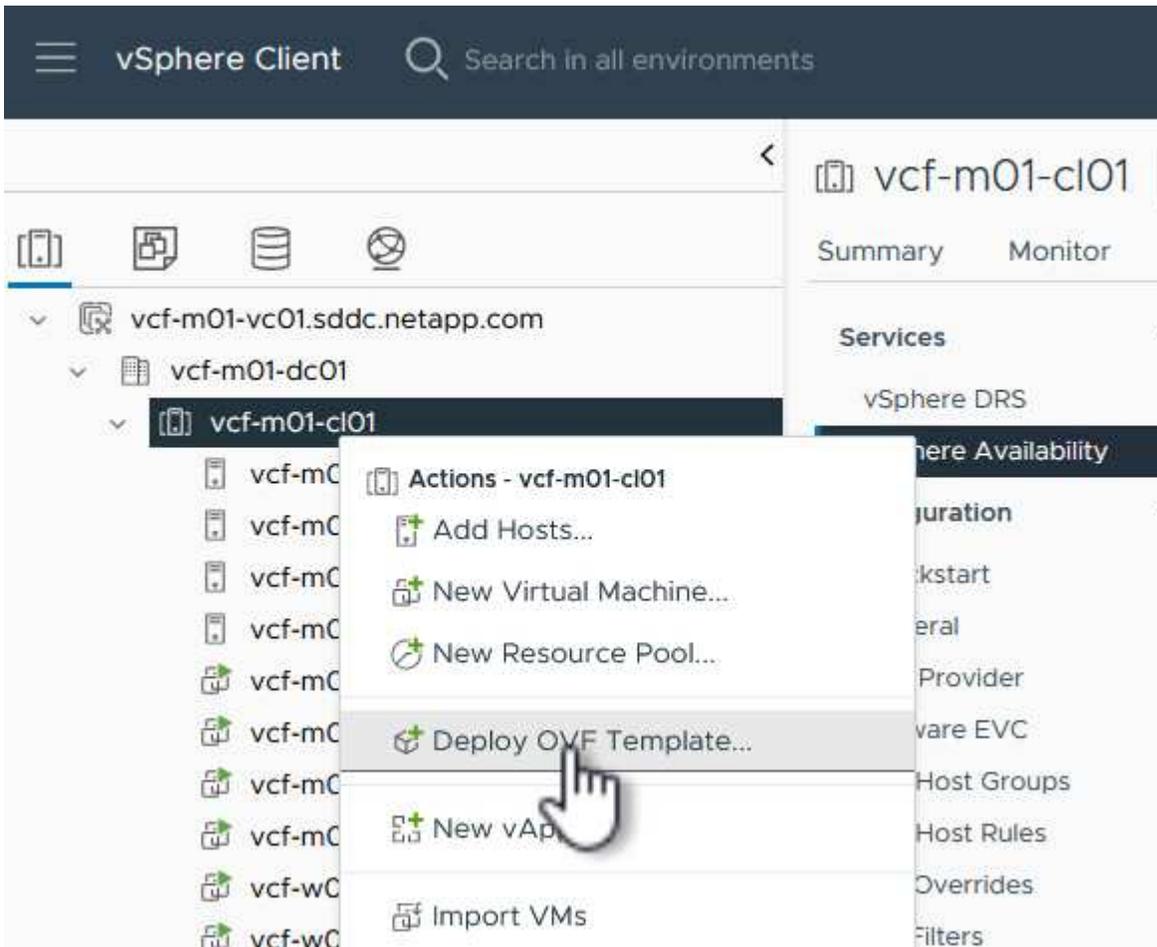
Complete los siguientes pasos para poner en marcha, configurar y utilizar SCV para proteger los datos en un dominio de carga de trabajo de VI:

## Ponga en marcha el complemento SnapCenter para VMware vSphere

El plugin de SnapCenter se aloja en el dominio de gestión de VCF, pero se registra en el para el dominio de carga de trabajo de VI para vCenter. Se requiere una instancia de SCV para cada instancia de vCenter y, tenga en cuenta que un dominio de carga de trabajo puede incluir varios clústeres gestionados por una única instancia de vCenter.

Complete los siguientes pasos desde el cliente de vCenter para poner en marcha SCV en el dominio de cargas de trabajo de VI:

1. Descargue el archivo OVA para la implementación de SCV desde el área de descarga del sitio de soporte de NetApp "[AQUÍ](#)".
2. Desde el dominio de gestión vCenter Client, seleccione **Desplegar plantilla OVF...**



3. En el asistente **Implementar plantilla OVF**, haga clic en el botón de opción **Archivo local** y, a continuación, seleccione cargar la plantilla OVF descargada anteriormente. Haga clic en **Siguiente** para continuar.

## Deploy OVF Template

### 1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

## Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

http | https://remoteserver-address/filetoinstall.ovf | .ova

Local file

UPLOAD FILES

scv-5.OP2-240310\_1514.ova

4. En la página **Seleccionar nombre y carpeta**, proporcione un nombre para la VM del broker de datos SCV y una carpeta en el dominio de administración. Haga clic en **Siguiente** para continuar.
5. En la página **Select a compute resource**, seleccione el cluster de dominio de administración o el host ESXi específico dentro del cluster para instalar la VM.
6. Revise la información relativa a la plantilla OVF en la página **Detalles de revisión** y acepte los términos de licencia en la página **Acuerdos de licencia**.
7. En la página **Seleccionar almacenamiento**, elija el almacén de datos en el que se instalará la VM y seleccione el **formato de disco virtual** y **Política de almacenamiento de VM**. En esta solución, la máquina virtual se instalará en un almacén de datos VMFS iSCSI ubicado en un sistema de almacenamiento de ONTAP, como se ha puesto en marcha previamente en una sección separada de este documento. Haga clic en **Siguiente** para continuar.

## Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

## Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine ⓘ

Select virtual disk format Thin Provision ▾

VM Storage Policy Datastore Default ▾

Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/> mgmt_01_iscsi	--	3 TB	3.71 TB	2.5 TB	▼
<input type="radio"/> vcf-m01-cl01-ds-vsant01	--	999.97 GB	49.16 GB	957.54 GB	▼
<input type="radio"/> vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/> vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/> vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/> vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼

Manage Columns Items per page 10 6 items

### Compatibility

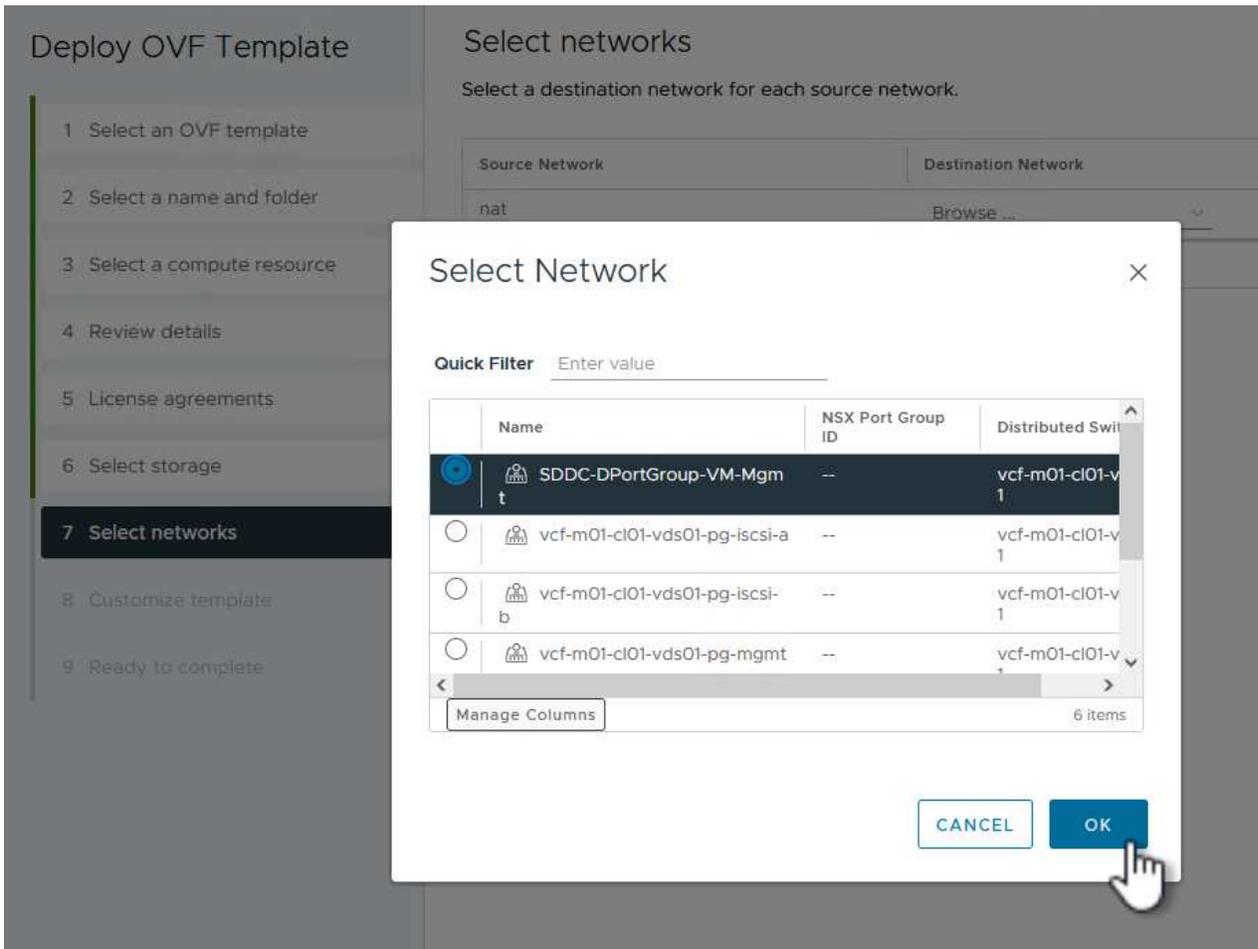
✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

8. En la página **Seleccionar red**, seleccione la red de administración que pueda comunicarse con el dispositivo vCenter del dominio de carga de trabajo y con los sistemas de almacenamiento ONTAP primario y secundario.



9. En la página **Personalizar plantilla** complete toda la información necesaria para la implementación:

- El FQDN o la IP, y credenciales para la carga de trabajo el dispositivo vCenter de dominio.
- Credenciales para la cuenta administrativa de SCV.
- Credenciales para la cuenta de mantenimiento de SCV.
- IPv4 Detalles de las propiedades de red (también se puede utilizar IPv6).
- Configuración de fecha y hora.

Haga clic en **Siguiente** para continuar.

## Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template**
- 9 Ready to complete

## Customize template

Customize the deployment properties of this software solution.

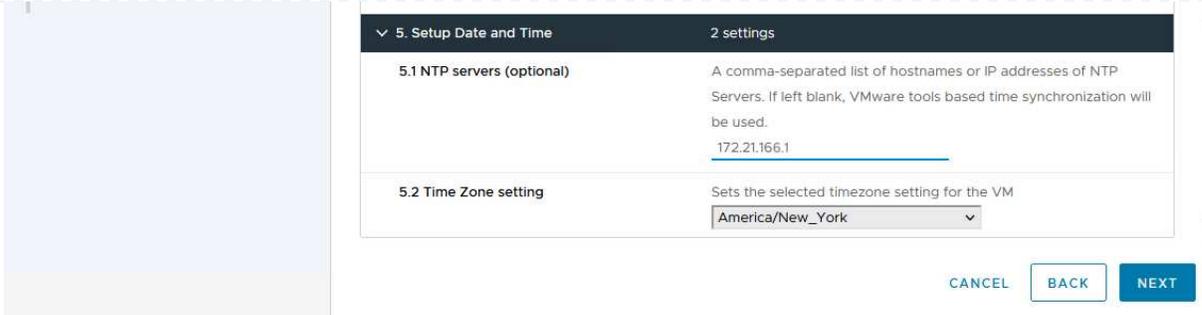
<b>1. Register to existing vCenter</b>		4 settings
1.1 vCenter Name(FQDN) or IP Address	<input type="text" value="cf-wkld-vc01.sddc.netapp.com"/>	
1.2 vCenter username	<input type="text" value="administrator@vcf.local"/>	
1.3 vCenter password	Password	<input type="password" value="....."/>
	Confirm Password	<input type="password" value="....."/>
1.4 vCenter port	<input type="text" value="443"/>	
<b>2. Create SCV Credentials</b>		2 settings
2.1 Username	<input type="text" value="admin"/>	
2.2 Password	Password	<input type="password" value="....."/>
	Confirm Password	<input type="password" value="....."/>
<b>3. System Configuration</b>		1 settings

## Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template**
- 9 Ready to complete

## Customize template

<b>4.2 Setup IPv4 Network Properties</b>		6 settings
4.2.1 IPv4 Address	IP address for the appliance. (Leave blank if DHCP is desired) <input type="text" value="172.21.166.148"/>	
4.2.2 IPv4 Netmask	Subnet to use on the deployed network. (Leave blank if DHCP is desired) <input type="text" value="255.255.255.0"/>	
4.2.3 IPv4 Gateway	Gateway on the deployed network. (Leave blank if DHCP is desired) <input type="text" value="172.21.166.1"/>	
4.2.4 IPv4 Primary DNS	Primary DNS server's IP address. (Leave blank if DHCP is desired) <input type="text" value="10.61.185.231"/>	
4.2.5 IPv4 Secondary DNS	Secondary DNS server's IP address. (optional - Leave blank if DHCP is desired) <input type="text" value="10.61.186.231"/>	
4.2.6 IPv4 Search Domains (optional)	Comma separated list of search domain names to use when resolving host names. (Leave blank if DHCP is desired) <input type="text" value="netapp.com,sddc.netapp.com"/>	
<b>3.3 Setup IPv6 Network Properties</b>		6 settings
4.3.1 IPv6 Address	IP address for the appliance. (Leave blank if DHCP is desired) <input type="text"/>	
4.3.2 IPv6 PrefixLen	Prefix length to use on the deployed network. (Leave blank if DHCP is desired) <input type="text"/>	

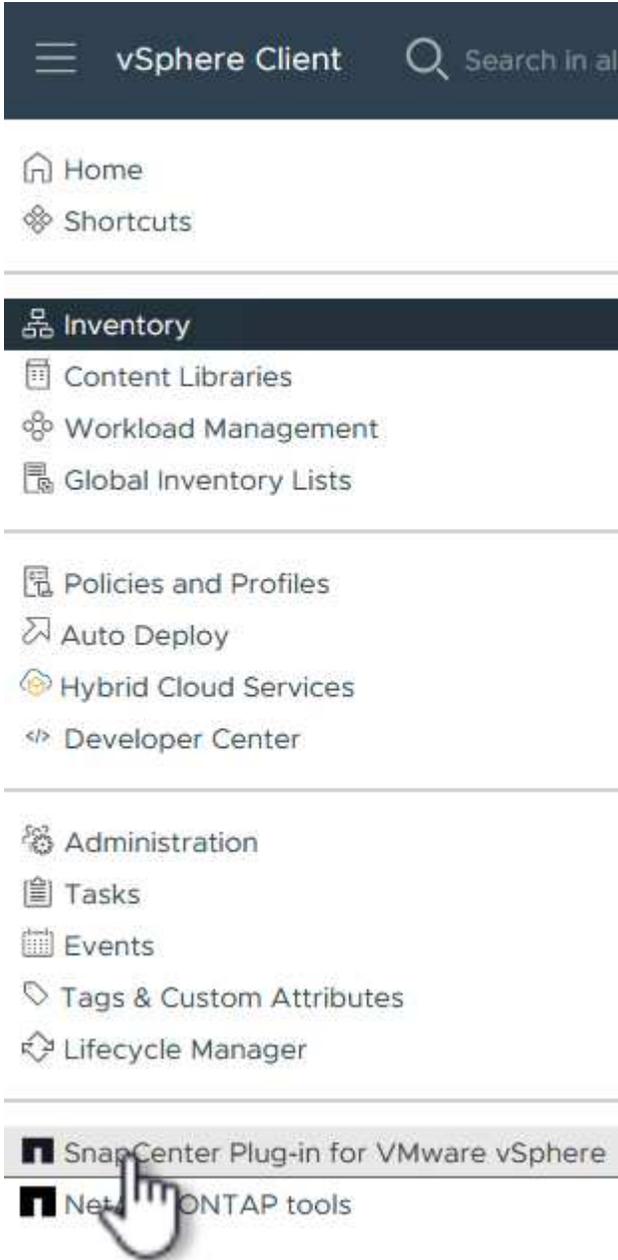


10. Por último, en la página **Listo para completar**, revise todos los ajustes y haga clic en Finalizar para iniciar la implementación.

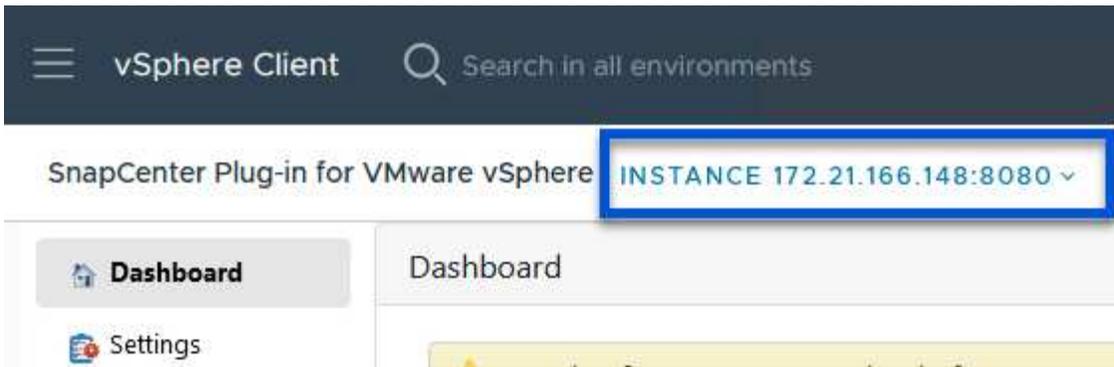
## Añada sistemas de almacenamiento a SCV

Una vez instalado el plugin de SnapCenter, complete los siguientes pasos para añadir sistemas de almacenamiento a SCV:

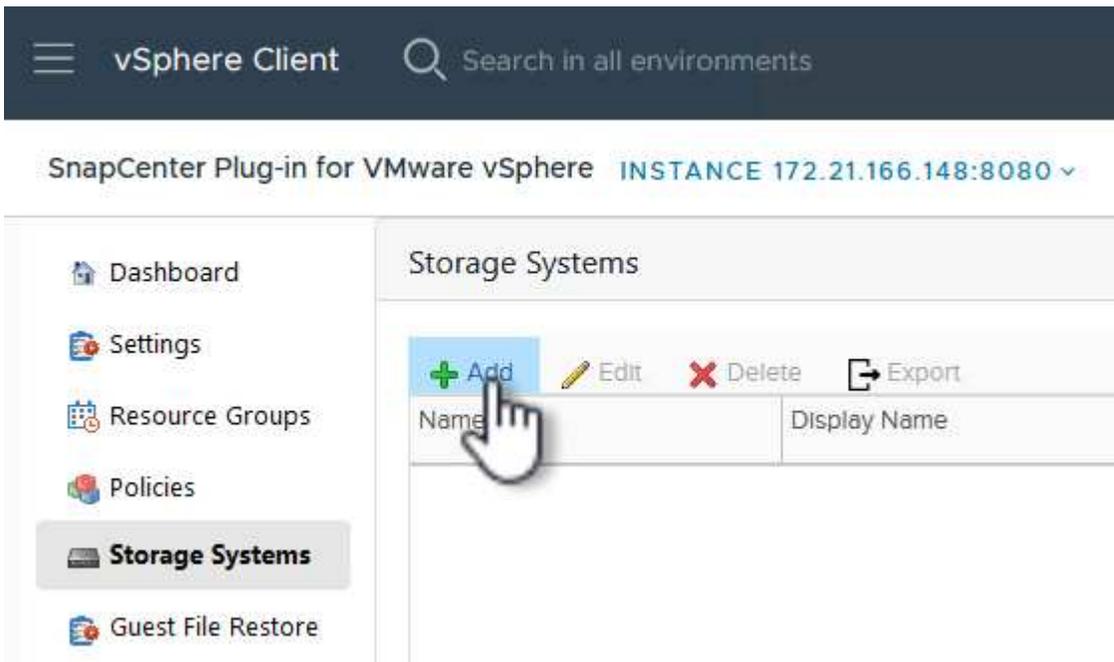
1. Es posible acceder a SCV desde el menú principal de vSphere Client.



2. En la parte superior de la interfaz de usuario de SCV, seleccione la instancia de SCV correcta que coincida con el clúster de vSphere que va a proteger.



3. Navegue a **Storage Systems** en el menú de la izquierda y haga clic en **Add** para comenzar.



4. En el formulario **Agregar sistema de almacenamiento**, rellene la dirección IP y las credenciales del sistema de almacenamiento ONTAP que se va a agregar, y haga clic en **Agregar** para completar la acción.

## Add Storage System



Storage System	<input type="text" value="172.16.9.25"/>
Authentication Method	<input checked="" type="radio"/> Credentials <input type="radio"/> Certificate
Username	<input type="text" value="admin"/>
Password	<input type="password" value="••••••••"/>
Protocol	<input type="text" value="HTTPS"/>
Port	<input type="text" value="443"/>
Timeout	<input type="text" value="60"/> Seconds
<input type="checkbox"/> Preferred IP	<input type="text" value="Preferred IP"/>

### Event Management System(EMS) & AutoSupport Setting

- Log Snapcenter server events to syslog
- Send AutoSupport Notification for failed operation to storage system

CANCEL

ADD



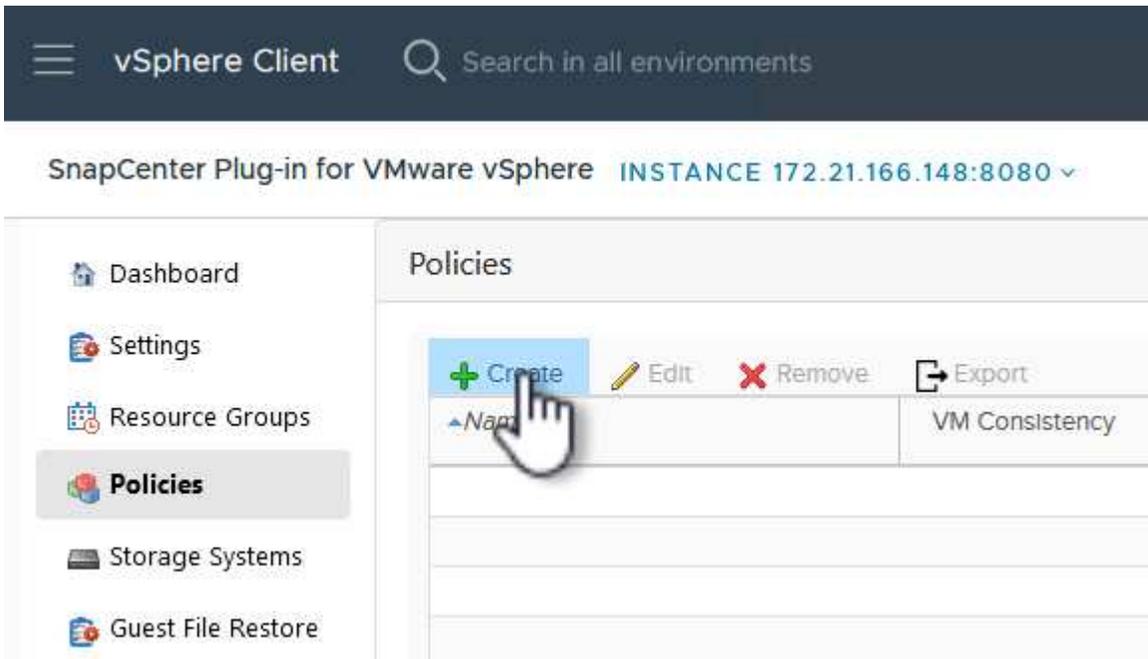
5. Repita este procedimiento para gestionar cualquier sistema de almacenamiento adicional, incluidos los sistemas que se van a utilizar como destino de backup secundario.

## Configure políticas de backup en SCV

Para obtener más información sobre la creación de políticas de backup de SCV, consulte "[Crear políticas de backup para máquinas virtuales y almacenes de datos](#)".

Complete los siguientes pasos para crear una nueva política de backup:

1. En el menú de la izquierda, seleccione **Políticas** y haga clic en **Crear** para comenzar.



2. En el formulario **Nueva política de copia de seguridad**, proporcione un **Nombre** y **Descripción** para la política, la **Frecuencia** en la que se realizarán las copias de seguridad y el período **Retención** que especifica cuánto tiempo se mantendrá la copia de seguridad.

**El período de bloqueo** permite que la función ONTAP SnapLock cree instantáneas a prueba de manipulaciones y permite la configuración del período de bloqueo.

Para **Replicación** Seleccione si desea actualizar las relaciones subyacentes de SnapMirror o SnapVault para el volumen de almacenamiento de ONTAP.



La replicación de SnapMirror y de SnapVault es similar ya que ambos utilizan la tecnología SnapMirror de ONTAP para replicar de forma asíncrona los volúmenes de almacenamiento en un sistema de almacenamiento secundario para mejorar la protección y la seguridad. Para las relaciones de SnapMirror, la programación de retención especificada en la política de backup de SCV gobernará la retención tanto del volumen primario como secundario. Con las relaciones de SnapVault, es posible establecer un programa de retención separado en el sistema de almacenamiento secundario para programas de retención a largo plazo o distintos. En este caso, la etiqueta de Snapshot se especifica en la política de backup de SCV y en la política asociada con el volumen secundario, para identificar a qué volúmenes va a aplicar la programación de retención independiente a.

Elija cualquier opción avanzada adicional y haga clic en **Agregar** para crear la política.

# New Backup Policy



**Name**

**Description**

**Frequency**

**Locking Period**  Enable Snapshot Locking ⓘ

**Retention**   ⓘ

**Replication**  Update SnapMirror after backup ⓘ  
 Update SnapVault after backup ⓘ

**Snapshot label**

**Advanced** ▾  VM consistency ⓘ  
 Include datastores with independent disks

**Scripts** ⓘ

CANCEL

ADD

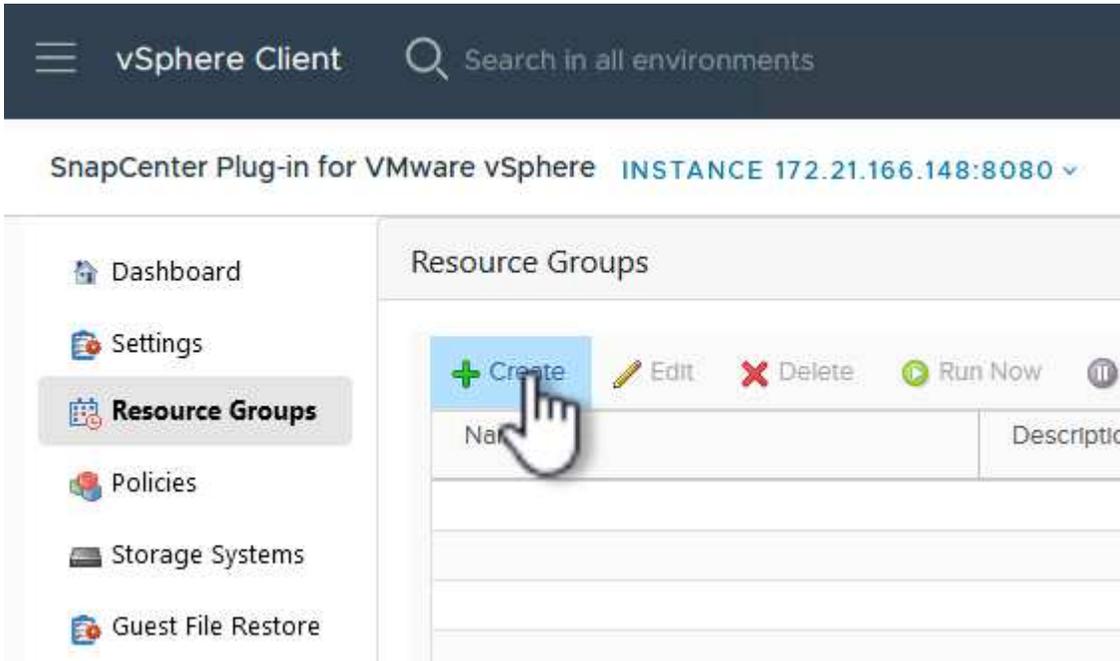


## Cree grupos de recursos en SCV

Para obtener más información sobre la creación de SCV Resource Groups, consulte "[Crear grupos de recursos](#)".

Complete los siguientes pasos para crear un grupo de recursos nuevo:

1. En el menú de la izquierda, seleccione **Grupos de recursos** y haga clic en **Crear** para comenzar.



2. En la página **Información general y notificación**, proporcione un nombre para el grupo de recursos, la configuración de notificación y cualquier otra opción adicional para el nombre de las instantáneas.
3. En la página **Recurso**, seleccione los almacenes de datos y las máquinas virtuales que se van a proteger en el grupo de recursos. Haga clic en **Siguiente** para continuar.



Incluso cuando solo se seleccionan máquinas virtuales específicas, siempre se realiza un backup de todo el almacén de datos. Esto se debe a que ONTAP toma instantáneas del volumen que aloja el almacén de datos. Sin embargo, tenga en cuenta que la selección únicamente de máquinas virtuales específicas para backup limita la posibilidad de restaurar únicamente a dichas máquinas virtuales.

## Create Resource Group

1. General info & notification

2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Scope: Virtual Machines

Parent entity: VCF\_WKLD\_03\_iSCSI

Enter available entity name

Available entities

OracleSrv\_01  
OracleSrv\_02  
OracleSrv\_03  
OracleSrv\_04

Selected entities

SQLSRV-01  
SQLSRV-02  
SQLSRV-03  
SQLSRV-04

BACK

NEXT

FINISH

CANCEL

4. En la página **Spanning Disks**, seleccione la opción de cómo manejar las máquinas virtuales con VMDK que abarcan varios almacenes de datos. Haga clic en **Siguiente** para continuar.

## Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Always exclude all spanning datastores

This means that only the datastores directly added to the resource group and the primary datastore of VMs directly added to the resource group will be backed up

Always include all spanning datastores

All datastores spanned by all included VMs are included in this backup

Manually select the spanning datastores to be included ⓘ

You will need to modify the list every time new VMs are added

There are no spanned entities in the selected virtual entities list.

BACK

NEXT

FINISH

CANCEL

5. En la página **Policies** seleccione una política creada previamente o varias políticas que se utilizarán con este grupo de recursos. Haga clic en **Siguiente** para continuar.

## Create Resource Group

- ✓ 1. General info & notification
- ✓ 2. Resource
- ✓ 3. Spanning disks
- 4. Policies**
- 5. Schedules
- 6. Summary

+ Create

<input type="checkbox"/>	Name	VM Consistent	Include independent di...	Schedule
<input checked="" type="checkbox"/>	Daily_Snapmirror	No	No	Daily
<input type="checkbox"/>				

BACK NEXT FINISH CANCEL



6. En la página **Schedules** establezca cuándo se ejecutará la copia de seguridad configurando la recurrencia y la hora del día. Haga clic en **Siguiente** para continuar.

## Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

✓ 3. Spanning disks

✓ 4. Policies

5. Schedules

6. Summary

Daily\_Snapmi... ▼

Type Daily

Every 1 Day(s)

Starting 04/04/2024

At 04 45 PM

BACK

NEXT

FINISH

CANCEL

7. Finalmente revise el **Summary** y haga clic en **Finish** para crear el grupo de recursos.

## Create Resource Group

- 1. General info & notification
- 2. Resource
- 3. Spanning disks
- 4. Policies
- 5. Schedules
- 6. Summary**

Name	SQL_Servers		
Description			
Send email	Never		
Latest Snapshot name	None ⓘ		
Custom snapshot format	None ⓘ		
Entities	SQLSRV-01, SQLSRV-02, SQLSRV-03, SQLSRV-04		
Spanning	False		
Policies	<b>Name</b>	<b>Frequency</b>	<b>Snapshot Locking Period</b>
	Daily_Snapmir...	Daily	-

BACK

NEXT

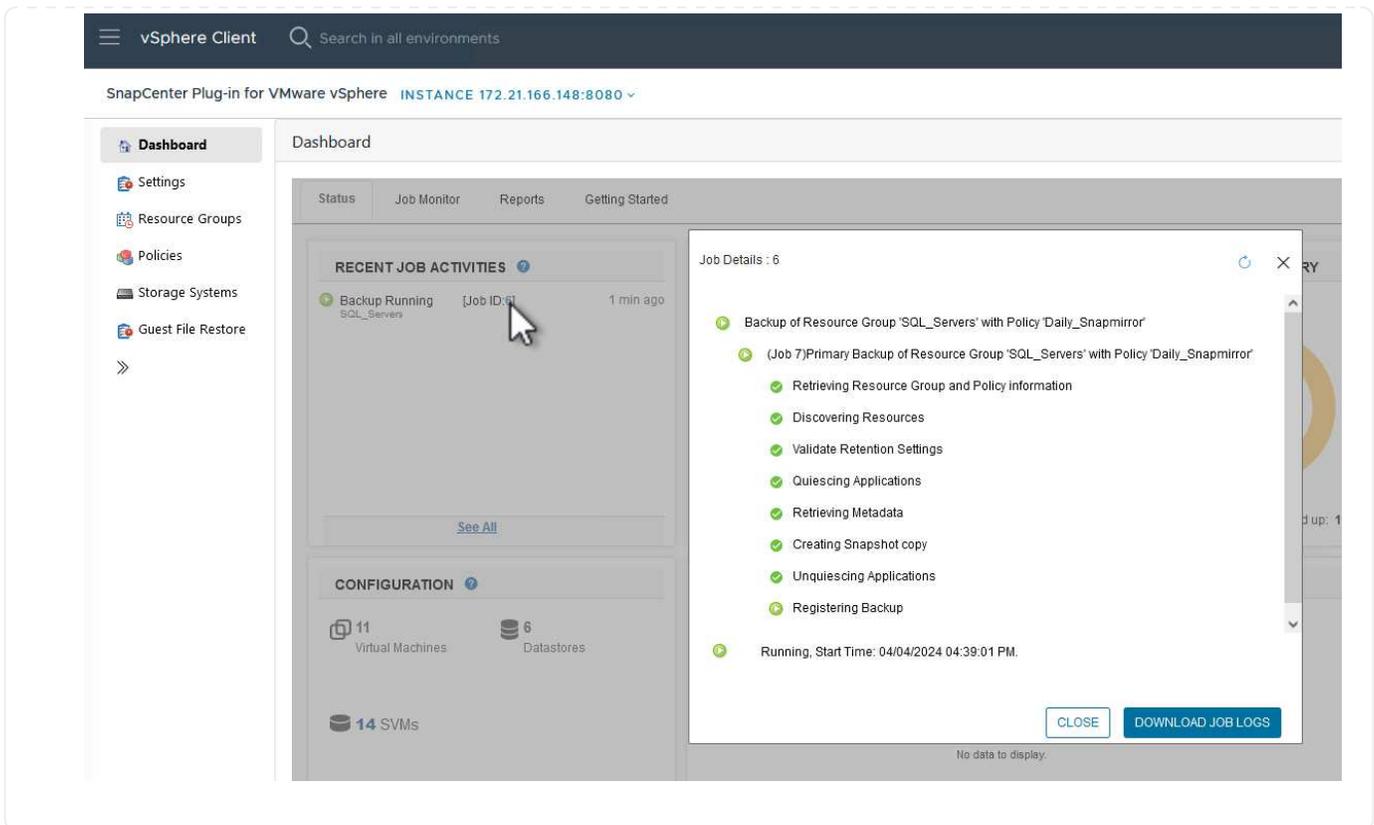
FINISH

CANCEL

8. Con el grupo de recursos creado haga clic en el botón **Ejecutar ahora** para ejecutar la primera copia de seguridad.

The screenshot shows the vSphere Client interface. At the top, there is a search bar and the text 'vSphere Client'. Below that, it says 'SnapCenter Plug-in for VMware vSphere' and 'INSTANCE 172.21.166.148:8080'. On the left, there is a navigation menu with 'Resource Groups' selected. The main area shows a table of 'Resource Groups' with columns for 'Name', 'Description', and 'Policy'. The 'SQL\_Servers' group is highlighted. Above the table, there are action buttons: '+ Create', 'Edit', 'Delete', 'Run Now', 'Suspend', 'Resume', and 'Export'. The 'Run Now' button is highlighted with a hand cursor.

9. Navegue hasta el **Panel** y, en **Actividades recientes** haga clic en el número que aparece junto a **ID de trabajo** para abrir el monitor de trabajos y ver el progreso del trabajo en ejecución.



## Utilice SCV para restaurar máquinas virtuales, VMDK y archivos

El plugin de SnapCenter permite restaurar máquinas virtuales, VMDK, archivos y carpetas a partir de backups principales o secundarios.

Las máquinas virtuales pueden restaurarse al host original, o bien a un host alternativo de la misma instancia de vCenter Server, o bien a un host ESXi alternativo gestionado por la misma instancia de vCenter o cualquier instancia de vCenter en modo vinculado.

Las máquinas virtuales VVol pueden restaurarse en el host original.

Los VMDK de máquinas virtuales tradicionales pueden restaurarse tanto a un almacén de datos original como a uno alternativo.

Los VMDK de las máquinas virtuales VVol pueden restaurarse en el almacén de datos original.

Pueden restaurarse archivos y carpetas individuales en una sesión de restauración de archivos invitados, lo que conecta una copia de backup de un disco virtual y luego restaura los archivos y las carpetas que se seleccionan.

Complete los siguientes pasos para restaurar máquinas virtuales, VMDK o carpetas individuales.

## Restaura máquinas virtuales mediante el plugin de SnapCenter

Complete los siguientes pasos para restaurar una máquina virtual con SCV:

1. Navegue hasta la máquina virtual que se restaurará en el cliente vSphere, haga clic con el botón derecho y desplácese hasta **SnapCenter Plug-in for VMware vSphere**. Seleccione **Restaurar** en el submenú.

The screenshot displays the vSphere Client interface. On the left, a tree view shows the inventory structure, including folders like 'vcf-m01-vc01.sddc.netapp.com' and 'vcf-wkld-01-IT-INF-WKLD-01-vc'. The 'OracleSrv\_04' VM is selected. A context menu is open over the VM, listing various actions. The 'Restore' option is highlighted, and a mouse cursor is pointing at it. The background shows the VM's summary page with tabs for 'Summary', 'Monitor', 'Configure', and 'Permissions'. The 'Summary' tab is active, showing details for the 'Guest OS' and 'Virtual Machine' sections. The 'Recent Tasks' pane is visible at the bottom left.

**Actions - OracleSrv\_04**

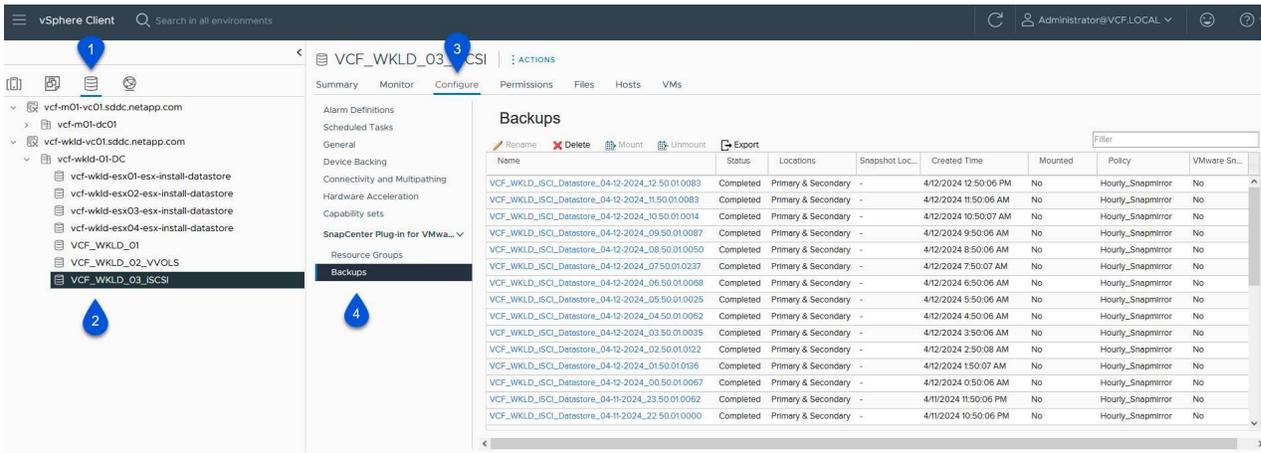
- Power
- Guest OS
- Snapshots
- Open Remote Console
- Migrate...
- Clone
- Fault Tolerance
- VM Policies
- Template
- Compatibility
- Export System Logs...
- Edit Settings...
- Move to folder...
- Rename...
- Edit Notes...
- Tags & Custom Attributes
- Add Permission...
- Alarms
- Remove from Inventory
- Delete from Disk
- vSAN
- NetApp ONTAP tools
- SnapCenter Plug-in for VMware vSphere

**Restore**

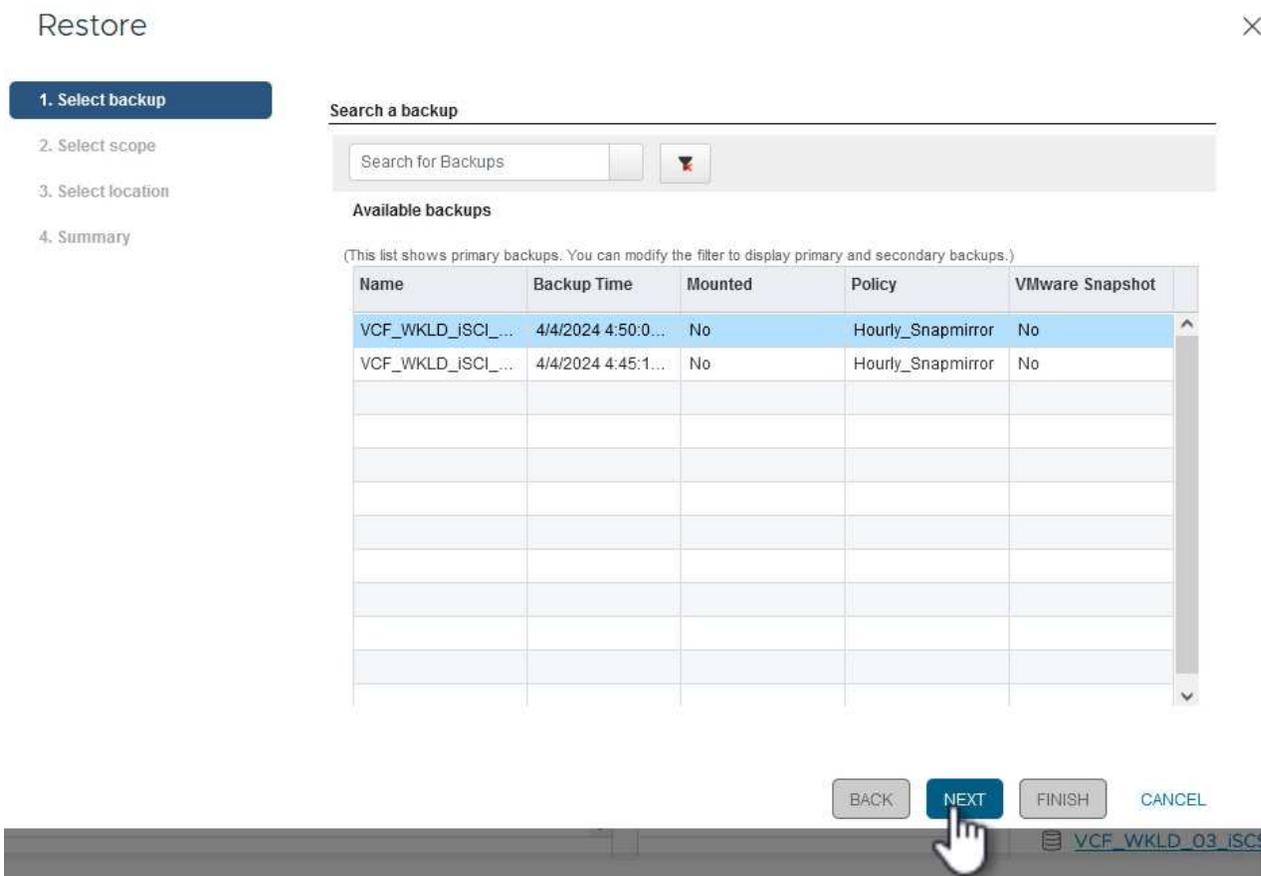
File Restore



Una alternativa es navegar al almacén de datos en inventario y, a continuación, en la pestaña **Configurar**, ir a **SnapCenter Plug-in for VMware vSphere > Backups**. Desde el backup elegido, seleccione las máquinas virtuales que se van a restaurar.



2. En el asistente **Restore**, seleccione la copia de seguridad que se va a utilizar. Haga clic en **Siguiente** para continuar.



3. En la página **Select Scope**, rellene todos los campos requeridos:

- **Restore Scope** - Seleccione esta opción para restaurar toda la máquina virtual.
- **Restart VM** - Elija si desea iniciar la VM después de la restauración.
- **Restaurar ubicación** - Elija restaurar a la ubicación original o a una ubicación alternativa. Al elegir una ubicación alternativa, seleccione las opciones de cada uno de los campos:
  - **Destination vCenter Server:** VCenter local o vCenter alternativo en modo vinculado
  - **Destino ESXi host**
  - **Red**
  - **Nombre de VM después de restaurar**
  - **Seleccione el almacén de datos:**

Restore

1. Select backup

2. Select scope

3. Select location

4. Summary

Restore scope: Entire virtual machine

Restart VM:

Restore Location:

Original Location  
(This will restore the entire VM to the original Hypervisor with the original settings. Existing VM will be unregistered and replaced with this VM.)

Alternate Location  
(This will create a new VM on selected vCenter and Hypervisor with the customized settings.)

Destination vCenter Server: 172.21.166.143

Destination ESXi host: vcf-wkld-esx04.sddc.netapp.com

Network: vcf-wkld-01-HT-INF-WKLD-01-vds-01-pg-

VM name after restore: OracleSrv\_04\_restored

Select Datastore: VCF\_WKLD\_03\_iSCSI

BACK NEXT FINISH CANCEL

VCF\_WKLD\_03\_iSCSI

Haga clic en **Siguiente** para continuar.

4. En la página **Seleccionar ubicación**, elija restaurar la VM desde el sistema de almacenamiento primario o secundario de ONTAP. Haga clic en **Siguiente** para continuar.

## Restore

- ✓ 1. Select backup
- ✓ 2. Select scope
- 3. Select location**
- 4. Summary

Destination datastore	Locations
VCF_WKLD_03_iSCSI	(Primary) VCF_iSCSI:VCF_WKLD_03_iSCSI
	(Primary) VCF_iSCSI:VCF_WKLD_03_iSCSI
	(Secondary) svm_iscsi:VCF_WKLD_03_iSCSI_dest
	< >

5. Finalmente, revise el **Resumen** y haga clic en **Finalizar** para iniciar el trabajo de restauración.

## Restore

- ✓ 1. Select backup
- ✓ 2. Select scope
- ✓ 3. Select location
- 4. Summary**

<b>Virtual machine to be restored</b>	OracleSrv_04
<b>Backup name</b>	VCF_WKLD_iSCSI_Datastore_04-04-2024_16.50.00.0940
<b>Restart virtual machine</b>	No
<b>Restore Location</b>	Alternate Location
<b>Destination vCenter Server</b>	172.21.166.143
<b>ESXi host to be used to mount the backup</b>	vcf-wkld-esx04.sddc.netapp.com
<b>VM Network</b>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt
<b>Destination datastore</b>	VCF_WKLD_03_iSCSI
<b>VM name after restore</b>	OracleSrv_04_restored



Change IP address of the newly created VM after restore operation to avoid IP conflict.

BACK

NEXT

**FINISH**

CANCEL

6. El progreso de los trabajos de restauración puede supervisarse desde el panel **Recent Tasks** de vSphere Client y desde el monitor de trabajos de SCV.

- Dashboard
- Settings
- Resource Groups
- Policies
- Storage Systems
- Guest File Restore
- >>

Dashboard

Status Job Monitor Reports Getting Started

RECENT JOB ACTIVITIES

- Restore Running [Job ID:18] 1 min ago  
VCF\_WKLD\_ISCI\_Datastore\_04-04-2024...
- Backup Successful [Job ID:15] 8 min ago  
VCF\_WKLD\_ISCI\_Datastore
- Backup Successful [Job ID:12] 13 min ago  
VCF\_WKLD\_ISCI\_Datastore
- Backup Successful [Job ID:9] 13 min ago  
SQL\_Servers
- Backup Successful [Job ID:6] 19 min ago  
SQL\_Servers

[See All](#)

CONFIGURATION

11 Virtual Machines    6 Datastores

14 SVMs

2 Resource Groups    2 Backup Policies

Job Details : 18

- Restoring backup with name: VCF\_WKLD\_ISCI\_Datastore\_04-04-2024\_16:50:00.0940
- Preparing for Restore: Retrieving Backup metadata from Repository.
- Pre Restore
- Restore

Running, Start Time: 04/04/2024 04:58:24 PM.

CLOSE DOWNLOAD JOB LOGS

No data to display.

Recent Tasks Alarms

Task Name	Target	Status	Details	Initiator	Queued For	Start Time
NetApp Mount Datastore	<a href="#">vcf-wkld-esx04.sdd</a> <a href="#">c.netapp.com</a>	35%	Mount operation completed successfully.	VCF.LOCAL\Administrator	6 ms	04/04/2024, 4:58:27 P M
NetApp Restore	<a href="#">vcf-wkld-esx04.sdd</a> <a href="#">c.netapp.com</a>	2%	Restore operation started.	VCF.LOCAL\Administrator	10 ms	04/04/2024, 4:58:27 P M

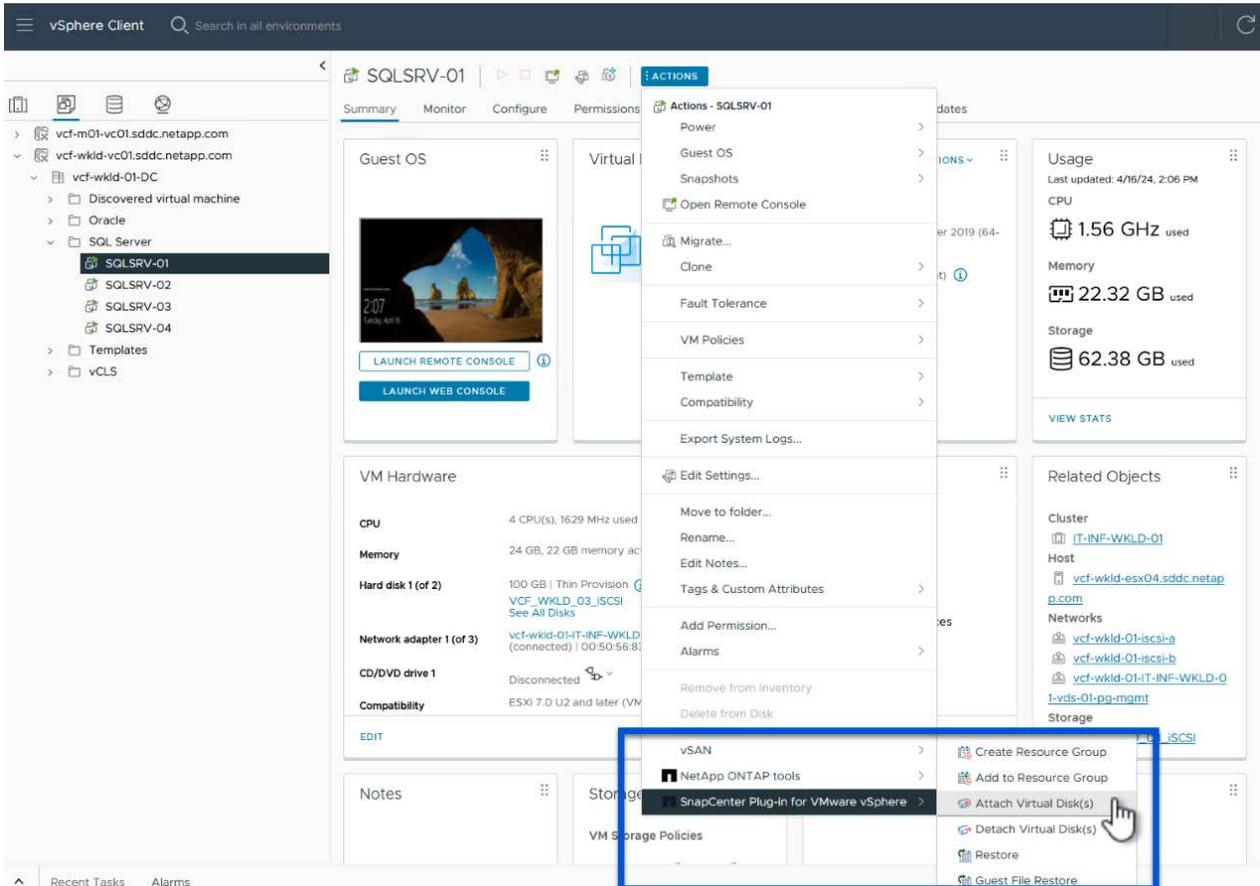
Manage Columns Running More Tasks

## Restaurar VMDK mediante el plugin de SnapCenter

ONTAP Tools permite restaurar por completo los VMDK a su ubicación original o conectar un VMDK como disco nuevo a un sistema host. En este caso, se conectará un VMDK a un host Windows para acceder al sistema de archivos.

Para asociar un VMDK a partir de un backup, complete los siguientes pasos:

1. En vSphere Client, desplácese a una máquina virtual y, en el menú **Acciones**, seleccione **SnapCenter Plug-in for VMware vSphere > Attach Virtual Disk(s)**.



2. En el asistente **Attach Virtual Disk(s)**, seleccione la instancia de copia de seguridad que se va a utilizar y el VMDK que se va a asociar.

# Attach Virtual Disk(s)



[Click here to attach to alternate VM](#)

## Backup

(This list shows primary backups. **1** modify the filter to display primary and secondary backups.)

Name	Backup Time	Mounted	Policy	VMware Snapshot
VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0218	4/17/2024 9:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_08.50.01.0223	4/17/2024 8:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_07.50.01.0204	4/17/2024 7:50:00 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_06.50.01.0194	4/17/2024 6:50:00 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_05.50.01.0245	4/17/2024 5:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_04.50.01.0231	4/17/2024 4:50:01 AM	No	Hourly_Snapmirror	No

## Select disks

Virtual disk	Location
<input type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01.vmdk	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0...
<input checked="" type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01_1.v...	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0...

Las opciones de filtro pueden utilizarse para localizar backups y mostrar backups de sistemas de almacenamiento primarios y secundarios.

# Attach Virtual Disk(s)



[Click here to attach to alternate VM](#)

## Backup

(This list shows primary backups)

Name
VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0218
VCF_WKLD_iSCSI_Datastore_04-17-2024_08.50.01.0223
VCF_WKLD_iSCSI_Datastore_04-17-2024_07.50.01.0204
VCF_WKLD_iSCSI_Datastore_04-17-2024_06.50.01.0194
VCF_WKLD_iSCSI_Datastore_04-17-2024_05.50.01.0245
VCF_WKLD_iSCSI_Datastore_04-17-2024_04.50.01.0231

## Select disks

Virtual disk	Location
<input type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01.vmdk	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0...
<input checked="" type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01_1.v...	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0...

Time range

From

Hour  Minute  Second

To

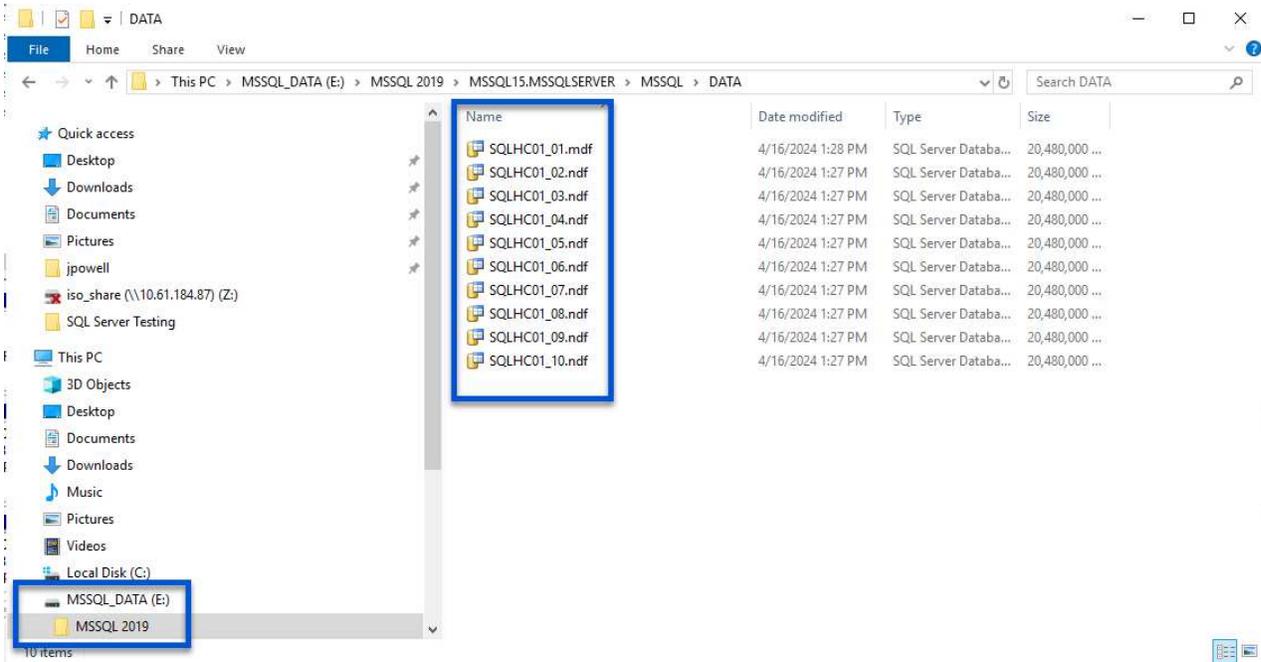
Hour  Minute  Second

VMware snapshot

Mounted

Location

3. Después de seleccionar todas las opciones, haga clic en el botón **Adjuntar** para iniciar el proceso de restauración y adjuntar el VMDK al host.
4. Una vez completado el procedimiento de asociación, se puede acceder al disco desde el sistema operativo del sistema host. En este caso SCV conectó el disco con su sistema de archivos NTFS a la unidad E: De nuestro Windows SQL Server y los archivos de base de datos SQL en el sistema de archivos son accesibles a través del Explorador de archivos.



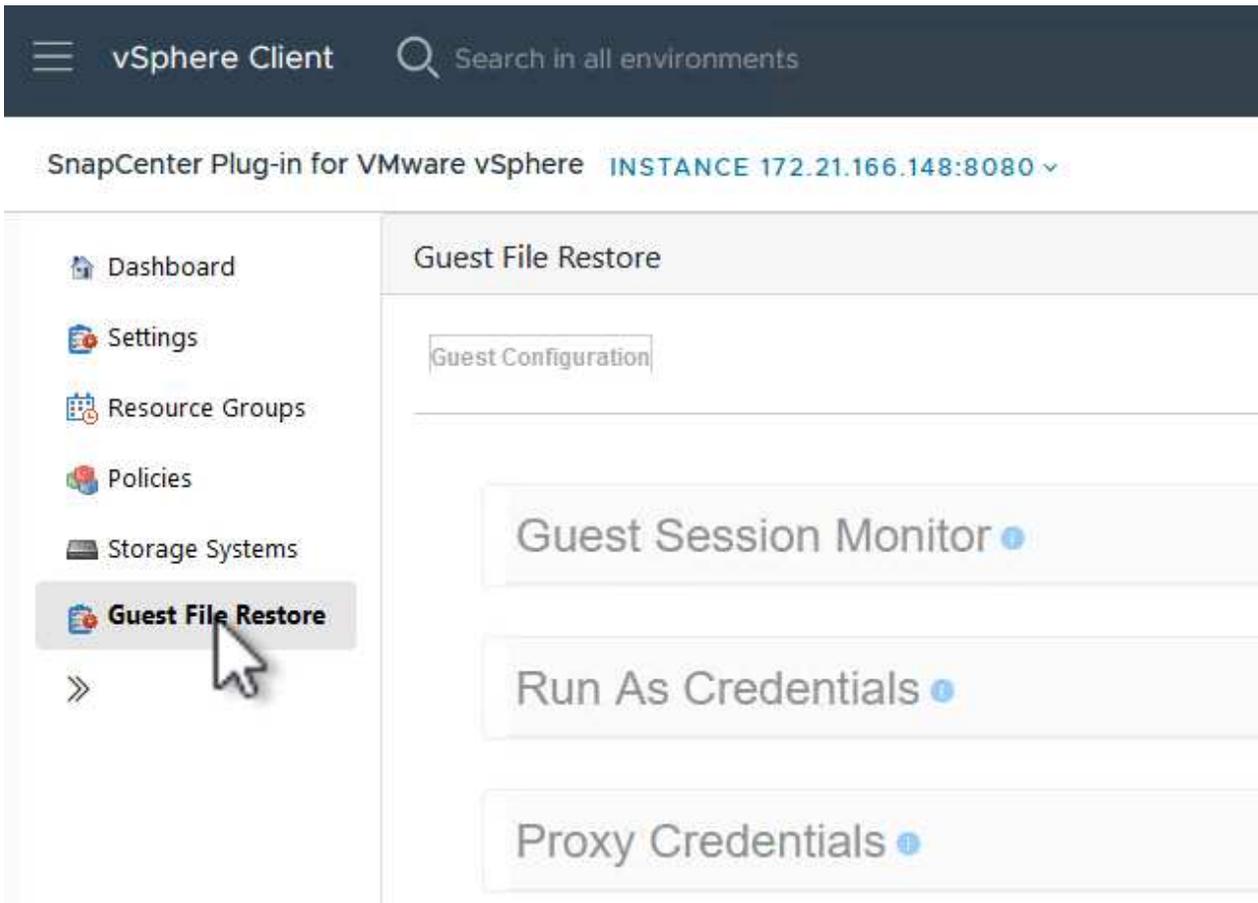
## Restauración de sistemas de archivos invitados mediante el plugin de SnapCenter

ONTAP Tools cuenta con restauraciones de sistemas de archivos invitados desde un VMDK en sistemas operativos Windows Server. Este proceso está preformado de forma centralizada a partir de la interfaz del plugin de SnapCenter.

Para obtener información detallada, consulte "[Restaurar archivos y carpetas invitados](#)" En el sitio de documentación de SCV.

Para realizar una restauración de sistema de archivos invitados para un sistema Windows, complete los siguientes pasos:

1. El primer paso es crear credenciales Run As para facilitar el acceso al sistema host de Windows. En vSphere Client, vaya a la interfaz del plugin CSV y haga clic en **Guest File Restore** en el menú principal.



2. En **Ejecutar como Credenciales** haz clic en el icono + para abrir la ventana **Ejecutar como Credenciales**.
3. Introduzca un nombre para el registro de credenciales, un nombre de usuario de administrador y una contraseña para el sistema Windows y, a continuación, haga clic en el botón **Select VM** para seleccionar una VM proxy opcional que se utilizará para la restauración.

## Run As Credentials



Run As Name	<input type="text" value="Administrator"/>	
Username	<input type="text" value="administrator"/>	
Password	<input type="password" value="••••••••"/>	
Authentication Mode	<input type="text" value="Windows"/>	
VM Name	<input type="text"/>	



<input type="button" value="CANCEL"/>	<input type="button" value="SAVE"/>
---------------------------------------	-------------------------------------

4. En la página Proxy VM, proporcione un nombre para la máquina virtual y búsquela buscando por host ESXi o por nombre. Una vez seleccionado, haga clic en **Guardar**.

## Proxy VM



VM Name

Search by ESXi Host

ESXi Host

Virtual Machine

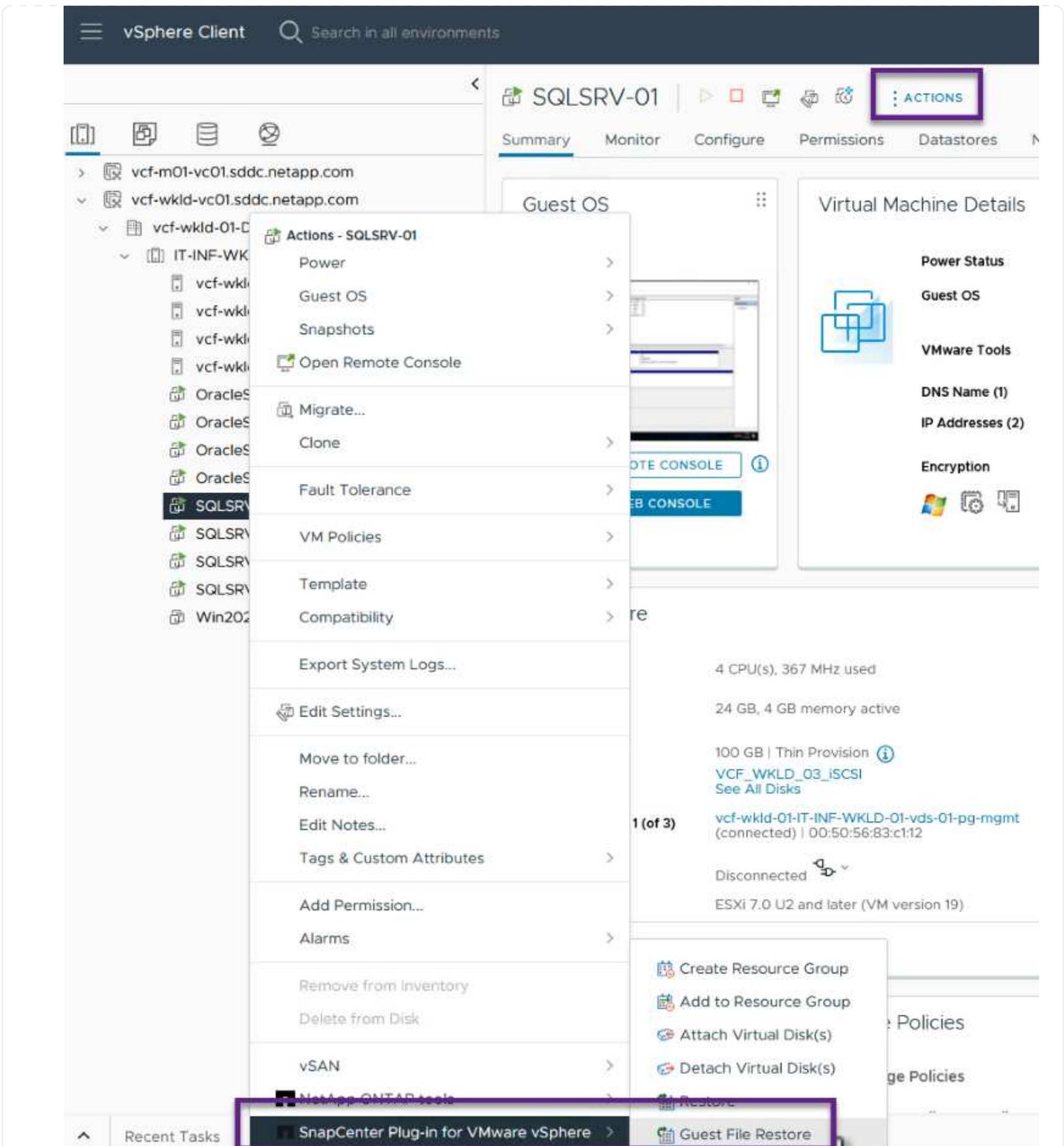
Search by Virtual Machine name

CANCEL

SAVE



5. Haga clic en **Guardar** de nuevo en la ventana **Ejecutar como Credenciales** para completar el guardado del registro.
6. A continuación, desplácese a una máquina virtual del inventario. En el menú **Acciones**, o haciendo clic derecho en la máquina virtual, seleccione **SnapCenter Plug-in for VMware vSphere > Guest File Restore**.



7. En la página **Restore Scope** del asistente **Guest File Restore**, seleccione la copia de seguridad desde la que desea restaurar, el VMDK en particular y la ubicación (primaria o secundaria) desde la que desea restaurar el VMDK. Haga clic en **Siguiente** para continuar.

## Guest File Restore



### 1. Restore Scope

2. Guest Details

3. Summary

Backup Name	Start Time	End Time
SQL_Servers_04-16-2024_13.52.3...	4/16/2024 1:52:34 PM	4/16/2024 1:52:40 PM
VCF_WKLD_iscsi_Datastore_04-1...	4/16/2024 1:50:01 PM	4/16/2024 1:50:08 PM

VMDK
[VCF_WKLD_03_iscsi] SQLSRV-01/SQLSRV-01.vmdk
[VCF_WKLD_03_iscsi] SQLSRV-01/SQLSRV-01_1.vmdk

Locations
Primary:VCF_iscsi:VCF_WKLD_03_iscsi:SQL_Servers_04-16-2024_13.52.34.0329
Secondary:svm_iscsi:VCF_WKLD_03_iscsi_dest:SQL_Servers_04-16-2024_13.52.34.0329

BACK NEXT FINISH CANCEL



8. En la página **Detalles del invitado**, seleccione usar **VM invitado** o **Usar gues File Restore proxy VM** para la restauración. Además, rellene aquí la configuración de notificaciones por correo electrónico si lo desea. Haga clic en **Siguiente** para continuar.

## Guest File Restore



### 1. Restore Scope

### 2. Guest Details

### 3. Summary

#### Use Guest VM

Guest File Restore operation will attach disk to guest VM

Run As Name	Username	Authentication Mode
Administrator	administrator	WINDOWS

#### Use Guest File Restore proxy VM

#### Send email notification

Email send from:

Email send to:

Email subject:

BACK

NEXT

FINISH

CANCEL

9. Por último, revise la página **Summary** y haga clic en **Finish** para comenzar la sesión de Restauración del sistema de archivos invitados.
10. De nuevo en la interfaz del plugin de SnapCenter, navegue a **Restauración de archivos invitados** de nuevo y vea la sesión en ejecución en **Monitor de sesión de invitado**. Haga clic en el icono en **Examinar archivos** para continuar.

The screenshot shows the vSphere Client interface with the SnapCenter Plug-in for VMware vSphere. The main content area displays the "Guest File Restore" configuration page. Below the configuration, there is a "Guest Session Monitor" table with the following data:

Backup Name	Source VM	Disk Path	Guest Mount Path	Time To Expire	Browse Files
SQL_Servers_04-16-2024_13.52.34.0329	SQLSRV-01	[VCF_WKLD_03_JSCSI]sc-202404161419...	E:\	23h:58m	

Below the table, there are sections for "Run As Credentials" and "Proxy Credentials", both with expandable dropdown menus.

11. En el asistente de **Guest File Browse**, seleccione la carpeta o los archivos que desea restaurar y la ubicación del sistema de archivos en la que desea restaurarlos. Finalmente, haga clic en **Restaurar** para iniciar el proceso **Restaurar**.

## Guest File Browse



### Select File(s)/Folder(s) to Restore



E:\MSSQL 2019

	Name	Size	
<input type="checkbox"/>	MSSQL15.MSSQLSERVER		^
			v

Selected 0 Files / 1 Directory

Name	Path	Size	Delete	
MSSQL 2019	E:\MSSQL 2019			^
				v

### Select Restore Location



Select address family for UNC path:

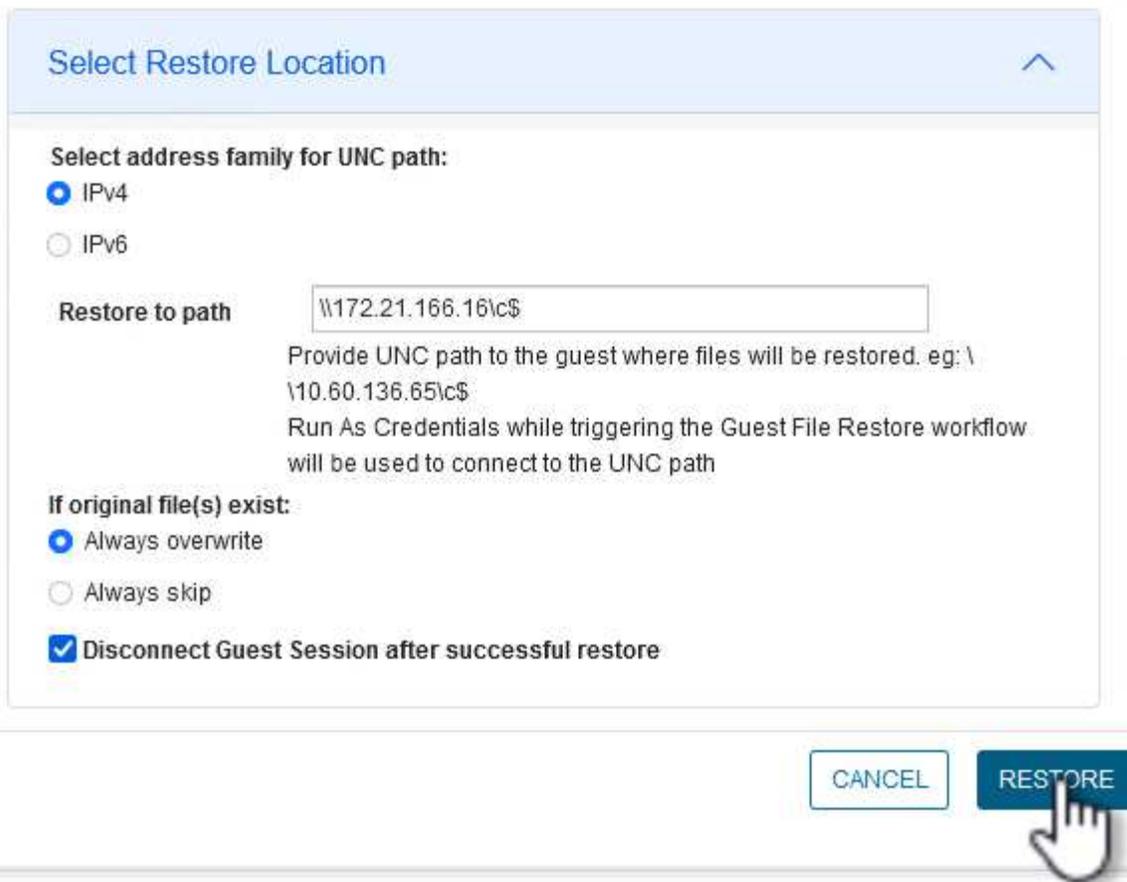
IPv4

IPv6

**Either Files to Restore or Restore Location is not selected!**

CANCEL

RESTORE



12. El trabajo de restauración se puede supervisar desde el panel de tareas de vSphere Client.

### Información adicional

Para obtener información sobre la configuración de VCF, consulte ["Documentación de VMware Cloud Foundation"](#).

Para obtener información acerca de la configuración de los sistemas de almacenamiento ONTAP, consulte la ["Documentación de ONTAP 9"](#) centro.

Para obtener información sobre el uso del plugin de SnapCenter para VMware vSphere, consulte el ["Documentación del plugin de SnapCenter para VMware vSphere"](#).

## VMware Cloud Foundation con cabinas NetApp AFF

Autor: Josh Powell, Ravi BCB

### VMware Cloud Foundation con cabinas NetApp AFF

VMware Cloud Foundation (VCF) es una plataforma integrada de centro de datos definido por software (SDDC) que proporciona una pila completa de infraestructura definida por software para ejecutar aplicaciones empresariales en un entorno de cloud híbrido. Combina funcionalidades de computación, almacenamiento, redes y gestión en una plataforma unificada que ofrece una experiencia operativa consistente en clouds privados y públicos.

Este documento proporciona información sobre las opciones de almacenamiento disponibles para VMware Cloud Foundation mediante el sistema de almacenamiento AFF All-Flash de NetApp. Las opciones de almacenamiento compatibles se tratan con instrucciones específicas para la creación de dominios de carga de trabajo con almacenes de datos NFS y VVOL como almacenamiento principal, así como una serie de opciones de almacenamiento complementarias.

## Casos de uso

Casos de uso cubiertos en esta documentación:

- Opciones de almacenamiento para los clientes que buscan entornos uniformes tanto en clouds públicos como privados.
- Solución automatizada para poner en marcha infraestructura virtual para dominios de cargas de trabajo.
- Solución de almacenamiento escalable adaptada para satisfacer las necesidades en constante evolución, incluso cuando no se alinea directamente con los requisitos de recursos informáticos.
- Implemente dominios de carga de trabajo VCF VI usando ONTAP como almacenamiento principal.
- Ponga en marcha almacenamiento complementario en dominios de cargas de trabajo de infraestructuras virtuales mediante ONTAP Tools para VMware vSphere.

## Destinatarios

Esta solución está dirigida a las siguientes personas:

- Arquitectos de soluciones que buscan opciones de almacenamiento más flexibles para entornos VMware diseñadas para maximizar el TCO.
- Arquitectos de soluciones que buscan opciones de almacenamiento VCF que ofrezcan opciones de protección de datos y recuperación ante desastres con los principales proveedores de cloud.
- Los administradores de almacenamiento que desean comprender cómo configurar VCF con almacenamiento principal y complementario.

## Visión general de la tecnología

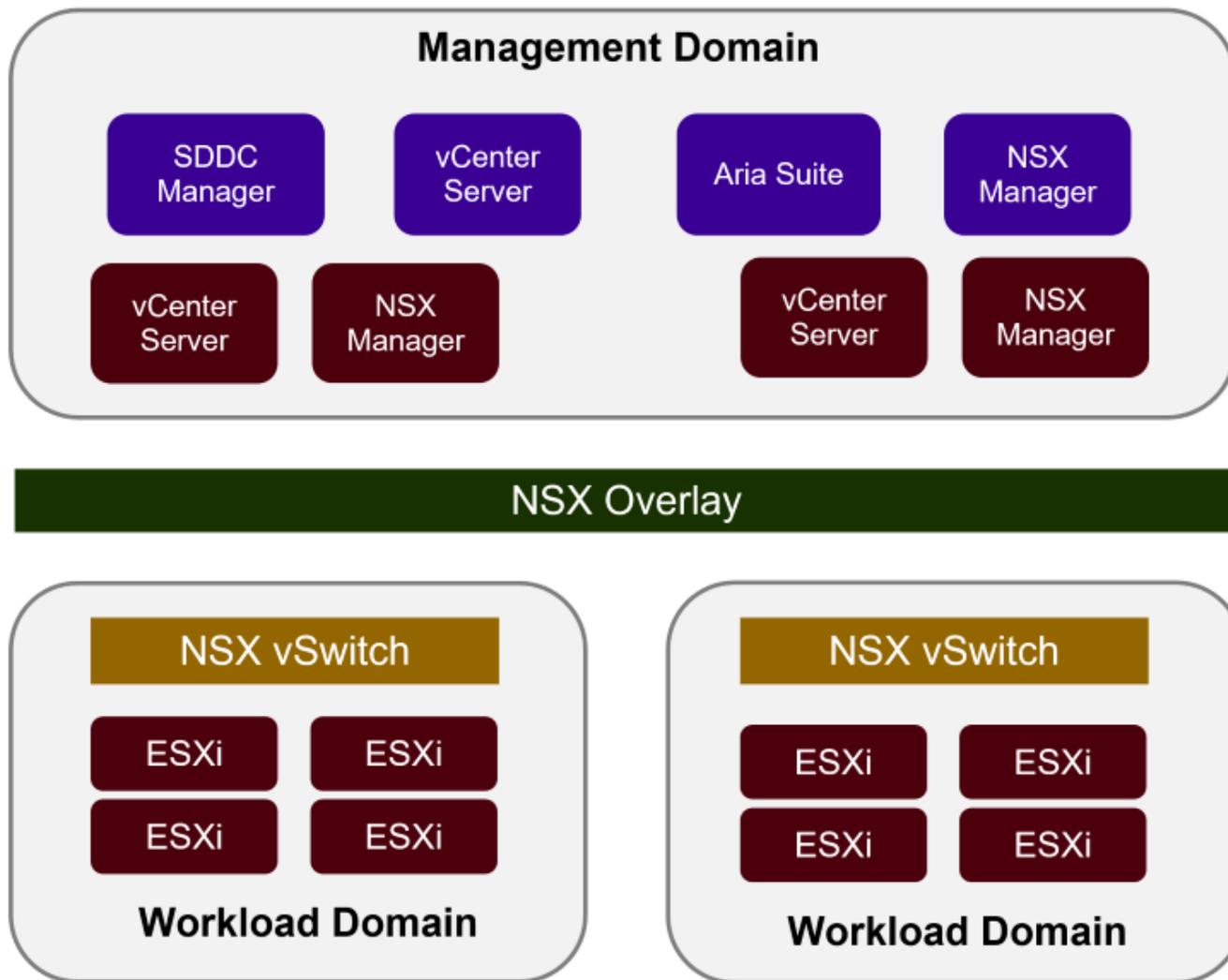
La solución VCF con NetApp AFF consta de los siguientes componentes principales:

### Base de cloud de VMware

VMware Cloud Foundation amplía las ofertas de hipervisores vSphere de VMware combinando componentes clave como SDDC Manager, vSphere, vSAN, NSX y VMware Aria Suite para crear un centro de datos virtualizado.

La solución VCF es compatible tanto con cargas de trabajo nativas de Kubernetes como con máquinas virtuales. Los servicios clave, como VMware vSphere, VMware vSAN, VMware NSX-T Data Center y VMware vRealize Cloud Management, son componentes integrales del paquete VCF. Al combinarse, estos servicios establecen una infraestructura definida por software capaz de gestionar con eficiencia la informática, el almacenamiento, las redes, la seguridad y la gestión del cloud.

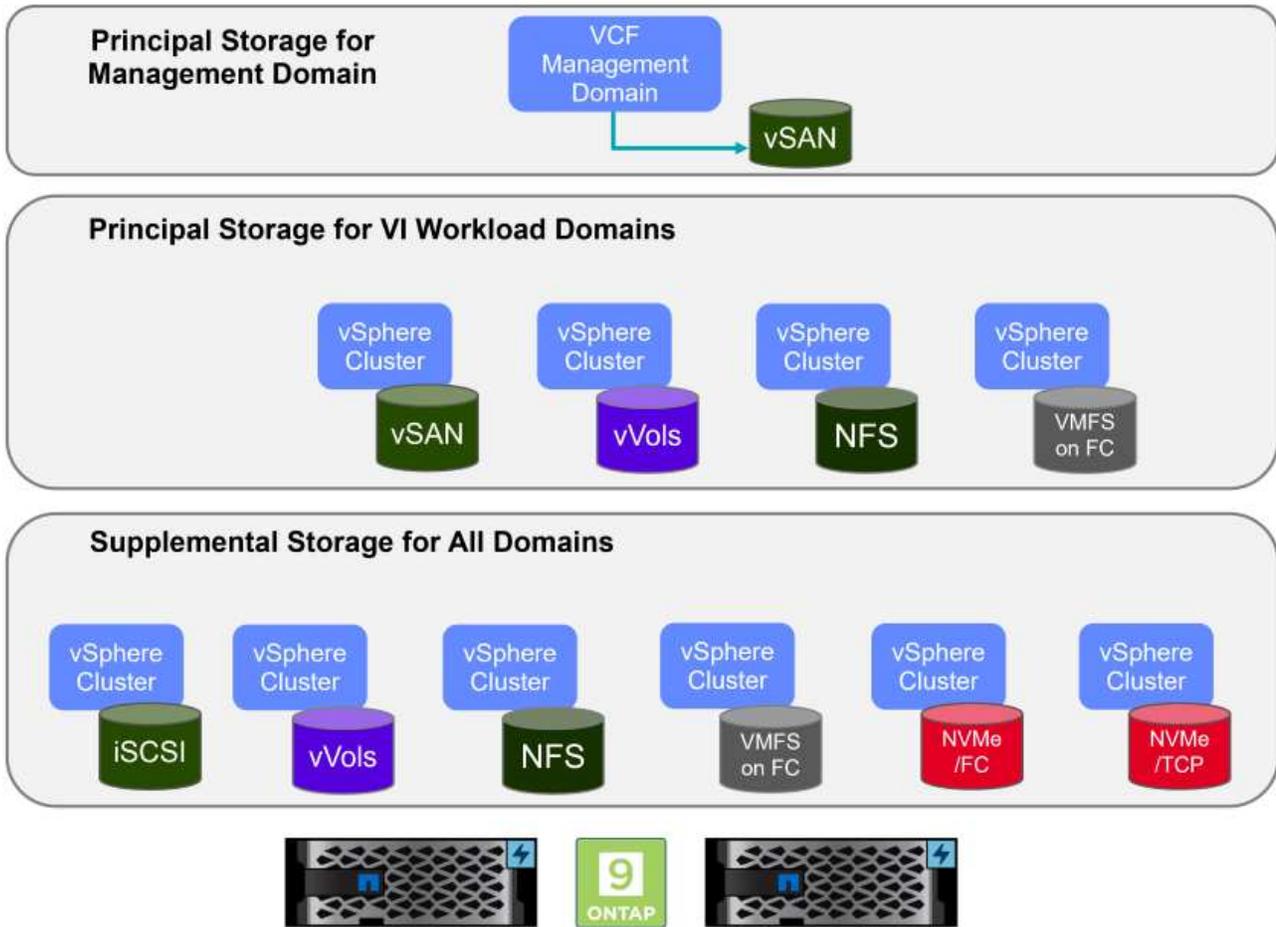
VCF se compone de un único dominio de gestión y hasta 24 dominios de carga de trabajo VI que representan una unidad de infraestructura lista para aplicaciones. Un dominio de carga de trabajo se compone de uno o más clústeres de vSphere que gestiona una única instancia de vCenter.



Para obtener más información sobre la arquitectura y planificación de VCF, consulte "[Modelos de arquitectura y tipos de dominio de carga de trabajo en VMware Cloud Foundation](#)".

### Opciones de almacenamiento de VCF

VMware divide las opciones de almacenamiento para VCF en almacenamiento **principal** y **suplementario**. El dominio de gestión VCF debe utilizar vSAN como su almacenamiento principal. Sin embargo, hay muchas opciones de almacenamiento suplementarias para el dominio de gestión y las opciones de almacenamiento principal y suplementario disponibles para los dominios de carga de trabajo VI.



### Almacenamiento principal para dominios de carga de trabajo

Almacenamiento principal se refiere a cualquier tipo de almacenamiento que se puede conectar directamente a un dominio de carga de trabajo VI durante el proceso de configuración dentro de SDDC Manager. El almacenamiento principal es el primer almacén de datos configurado para un dominio de carga de trabajo e incluye vSAN, vVols (VMFS), NFS y VMFS en Fibre Channel.

### Almacenamiento suplementario para dominios de gestión y carga de trabajo

El almacenamiento complementario es el tipo de almacenamiento que se puede añadir a los dominios de las cargas de trabajo o gestión en cualquier momento una vez que se ha creado el clúster. El almacenamiento complementario representa la gama más amplia de opciones de almacenamiento compatibles, que son compatibles con las cabinas de NetApp AFF.

Recursos de documentación adicionales para VMware Cloud Foundation:

- \* ["Documentación de VMware Cloud Foundation"](#)
- \* ["Tipos de almacenamiento compatibles para VMware Cloud Foundation"](#)
- \* ["Gestión del almacenamiento en VMware Cloud Foundation"](#)

### Cabinas de almacenamiento all-flash de NetApp

Las cabinas de NetApp AFF (All Flash FAS) son soluciones de almacenamiento de alto rendimiento diseñadas para aprovechar la velocidad y la eficiencia de la tecnología flash. Las cabinas de AFF incorporan funciones de gestión de datos integradas, como backups basados en Snapshot, replicación, thin provisioning y funcionalidades de protección de datos.

Las cabinas NetApp AFF utilizan el sistema operativo de almacenamiento ONTAP y ofrecen compatibilidad integral con protocolos de almacenamiento para todas las opciones de almacenamiento compatibles con VCF, todo ello en una arquitectura unificada.

Las cabinas de almacenamiento NetApp AFF están disponibles en los Sistemas C-Series basados en flash de mayor rendimiento, A-Series y QLC. Ambas series usan unidades flash NVMe.

Para obtener más información sobre las cabinas de almacenamiento NetApp AFF A-Series, consulte la ["AFF A-Series de NetApp"](#) página de destino.

Para obtener más información sobre las cabinas de almacenamiento C-Series de NetApp, consulte la ["NetApp AFF C-Series"](#) página de destino.

### Herramientas de ONTAP de NetApp para VMware vSphere

ONTAP Tools para VMware vSphere (OTV) permite a los administradores gestionar el almacenamiento de NetApp directamente desde vSphere Client. ONTAP Tools permite poner en marcha y gestionar almacenes de datos, así como aprovisionar almacenes de datos VVOL.

Herramientas ONTAP permite la asignación de almacenes de datos a perfiles de capacidades de almacenamiento que determinan un conjunto de atributos del sistema de almacenamiento. Esto permite la creación de almacenes de datos con atributos específicos como el rendimiento del almacenamiento y la calidad de servicio.

Las herramientas de ONTAP también incluyen un proveedor de API de VMware vSphere para el conocimiento del almacenamiento (VASA)\* para sistemas de almacenamiento de ONTAP que permite el aprovisionamiento de almacenes de datos de VMware Virtual Volumes (vVols), la creación y el uso de perfiles de capacidades de almacenamiento, la verificación de cumplimiento y la supervisión del rendimiento.

Para obtener más información sobre las herramientas de NetApp ONTAP, consulte la ["Herramientas de ONTAP para documentación de VMware vSphere"](#) página.

### Descripción general de la solución

En los escenarios presentados en esta documentación, demostraremos cómo utilizar los sistemas de almacenamiento de ONTAP como almacenamiento principal para las implementaciones de dominio de carga de trabajo VCF VI. Además, instalaremos y utilizaremos ONTAP Tools para VMware vSphere para configurar almacenes de datos complementarios para Dominios de carga de trabajo de VI.

Escenarios cubiertos en esta documentación:

- **Configure y use un almacén de datos NFS como almacenamiento principal durante la implementación del dominio de carga de trabajo VI.** Haga clic ["aquí"](#) para pasos de despliegue.
- **Instale y demuestre el uso de las herramientas de ONTAP para configurar y montar almacenes de datos NFS como almacenamiento complementario en dominios de carga de trabajo VI.** Haga clic ["aquí"](#) para pasos de despliegue.

### NFS como almacenamiento principal para dominios de cargas de trabajo VI

Autor: Josh Powell, Ravi BCB

### Descripción general del escenario

En este escenario, demostraremos cómo configurar un almacén de datos NFS como almacenamiento principal para la implementación de un dominio de carga de trabajo VI en VCF. Cuando sea necesario, consultaremos la documentación externa para conocer los pasos que deben realizarse en el SDDC Manager de VCF y cubriremos los pasos específicos de la parte de configuración del almacenamiento.

Este escenario cubre los siguientes pasos de alto nivel:

- Verifique las redes de la máquina virtual de almacenamiento (SVM) de ONTAP y de que haya una interfaz lógica (LIF) presente para transportar el tráfico de NFS.
- Cree una política de exportación para permitir que los hosts ESXi accedan al volumen NFS.
- Cree un volumen NFS en el sistema de almacenamiento de ONTAP.
- Cree un pool de redes para el tráfico NFS y vMotion en SDDC Manager.
- Hosts de comisión en VCF para su uso en un dominio de carga de trabajo de VI.
- Implemente un dominio de carga de trabajo de VI en VCF utilizando un almacén de datos NFS como almacenamiento principal.
- Instale el plugin de NetApp NFS para VMware VAAI

### Requisitos previos

Este escenario requiere los siguientes componentes y configuraciones:

- Sistema de almacenamiento de NetApp AFF con una máquina virtual de almacenamiento (SVM) configurada para permitir el tráfico de NFS.
- La interfaz lógica (LIF) se ha creado en la red IP que es para transportar el tráfico NFS y está asociada con la SVM.
- La puesta en marcha del dominio de gestión de VCF ha finalizado y se puede acceder a la interfaz del administrador de SDDC.
- 4 hosts ESXi configurados para la comunicación en la red de gestión de VCF.
- Direcciones IP reservadas para el tráfico de almacenamiento vMotion y NFS en la VLAN o el segmento de red establecido para este fin.



Al desplegar un dominio de carga de trabajo VI, VCF valida la conectividad con el servidor NFS. Esto se realiza mediante el adaptador de gestión de los hosts ESXi antes de agregar ningún adaptador vmkernel adicional con la dirección IP de NFS. Por lo tanto, es necesario asegurarse de que 1) la red de gestión se pueda enrutar al servidor NFS o 2) se haya añadido una LIF para la red de gestión a la SVM que aloja el volumen de almacenamientos de datos NFS, para garantizar que se pueda continuar con la validación.

Para obtener información acerca de la configuración de los sistemas de almacenamiento ONTAP, consulte la ["Documentación de ONTAP 9"](#) centro.

Para obtener información sobre la configuración de VCF, consulte ["Documentación de VMware Cloud Foundation"](#).

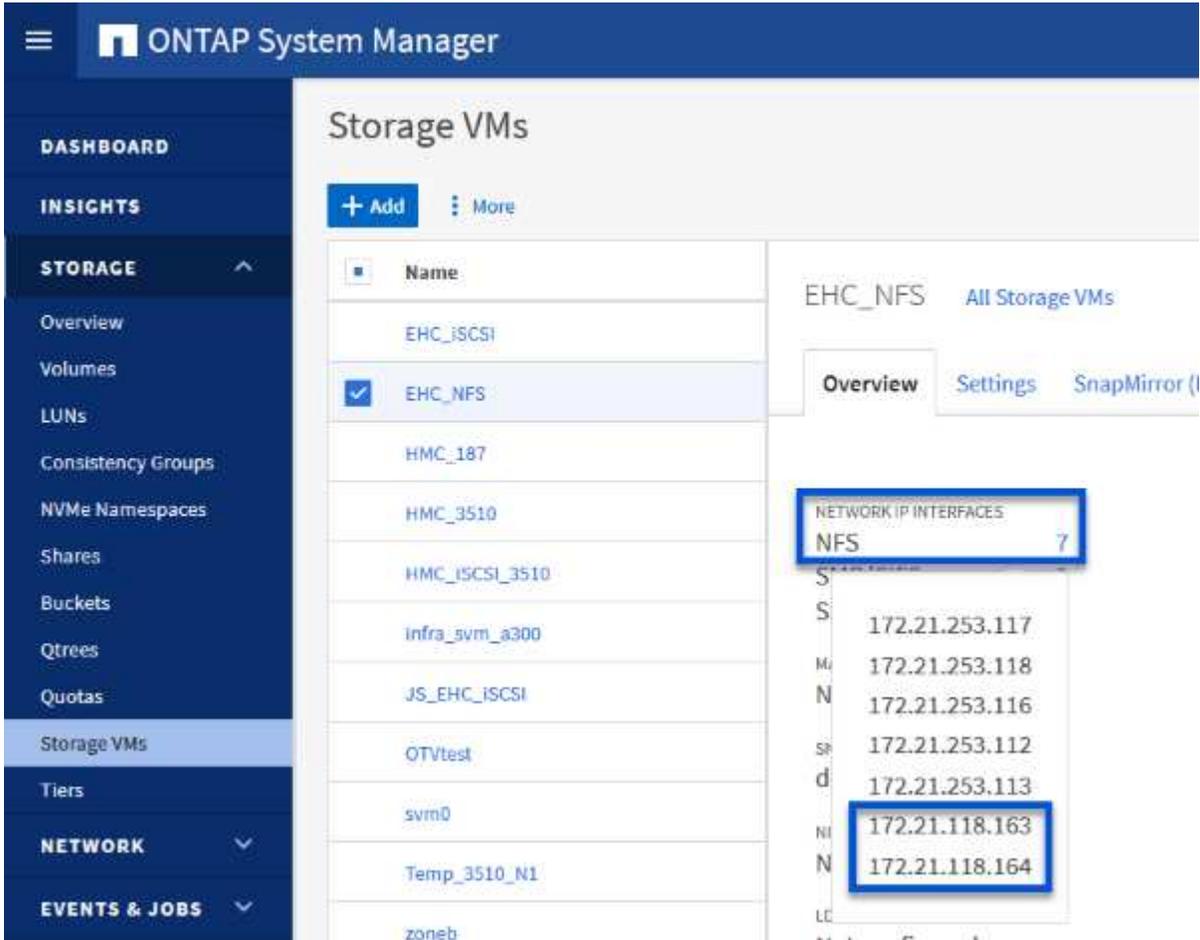
## **Pasos de despliegue**

Para implementar un dominio de carga de trabajo VI con un almacén de datos NFS como almacenamiento principal, complete los siguientes pasos:

## Verifique la conexión a redes de la SVM de ONTAP

Compruebe que se han establecido las interfaces lógicas necesarias para la red que transportará tráfico NFS entre el clúster de almacenamiento de ONTAP y el dominio de carga de trabajo VI.

1. Desde el Administrador del sistema de ONTAP navegue a **VM de almacenamiento** en el menú de la izquierda y haga clic en la SVM que se utilizará para el tráfico NFS. En la pestaña **Overview**, en **NETWORK ip INTERFACES**, haz clic en el valor numérico a la derecha de **nfs**. En la lista, compruebe que aparecen las direcciones IP de LIF necesarias.



The screenshot shows the ONTAP System Manager interface. The left sidebar contains navigation menus for DASHBOARD, INSIGHTS, STORAGE, and NETWORK. The main content area is titled 'Storage VMs' and shows a list of storage virtual machines. The 'EHC\_NFS' SVM is selected. On the right, the 'Overview' tab is active, and the 'NETWORK IP INTERFACES' section is expanded. A table lists network interfaces, with the 'nfs' interface highlighted. The IP addresses 172.21.118.163 and 172.21.118.164 are circled in blue.

Interface	IP Address
S	172.21.253.117
S	172.21.253.118
M	172.21.253.116
N	172.21.253.112
SP	172.21.253.112
d	172.21.253.113
NI	172.21.118.163
N	172.21.118.164

Como alternativa, compruebe las LIF asociadas a una SVM desde la CLI de ONTAP con el siguiente comando:

```
network interface show -vserver <SVM_NAME>
```

1. Compruebe que los hosts ESXi se puedan comunicar con el servidor NFS de ONTAP. Inicie sesión en el host ESXi mediante SSH y haga ping en el LIF de la SVM:

```
vmkping <IP Address>
```

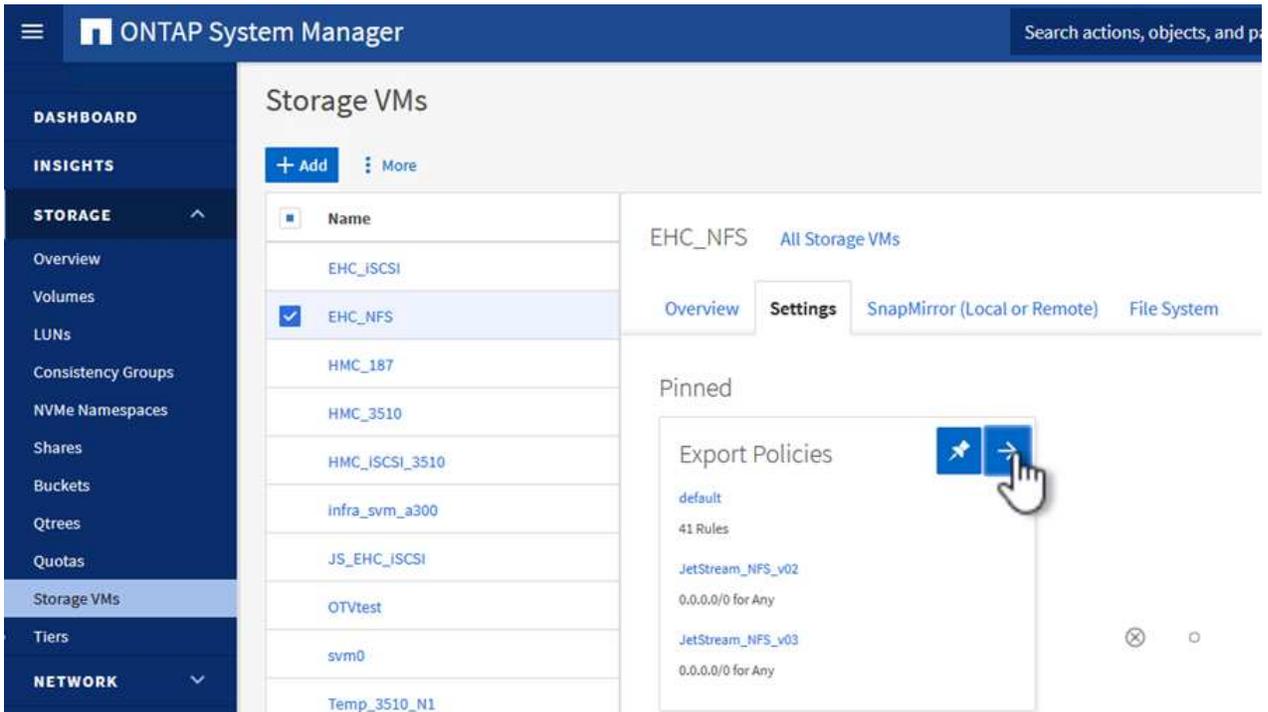


Al desplegar un dominio de carga de trabajo VI, VCF valida la conectividad con el servidor NFS. Esto se realiza mediante el adaptador de gestión de los hosts ESXi antes de agregar ningún adaptador vmkernel adicional con la dirección IP de NFS. Por lo tanto, es necesario asegurarse de que 1) la red de gestión se pueda enrutar al servidor NFS o 2) se haya añadido una LIF para la red de gestión a la SVM que aloja el volumen de almacenes de datos NFS, para garantizar que se pueda continuar con la validación.

## Crear una política de exportación para compartir el volumen NFS

Cree una política de exportación en ONTAP System Manager para definir el control de acceso para los volúmenes de NFS.

1. En el Administrador del sistema de ONTAP, haga clic en **VM de almacenamiento** en el menú de la izquierda y seleccione una SVM de la lista.
2. En la pestaña **Configuración**, busque **Políticas de exportación** y haga clic en la flecha para acceder.



3. En la ventana **Nueva política de exportación**, agregue un nombre para la política, haga clic en el botón **Agregar nuevas reglas** y luego en el botón **+Agregar** para comenzar a agregar una nueva regla.

## New export policy

NAME

WKLD\_DM01

Copy rules from existing policy

STORAGE VM

svm0

EXPORT POLICY

default

RULES

No data

+ Add



Add New Rules

Save

Cancel

4. Rellene las direcciones IP, el rango de direcciones IP o la red que desee incluir en la regla. Desmarque las casillas **SMB/CIFS** y **FlexCache** y realice selecciones para los detalles de acceso a continuación. Seleccionar los cuadros UNIX es suficiente para el acceso a los hosts ESXi.

## New Rule



### CLIENT SPECIFICATION

172.21.166.0/24

### ACCESS PROTOCOLS

SMB/CIFS

FlexCache

NFS  NFSv3  NFSv4

### ACCESS DETAILS

Type	Read-only Access	Read/Write Access	Superuser Access
All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All (As anonymous user)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kerberos 5i	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kerberos 5p	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
NTLM	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Cancel

Save



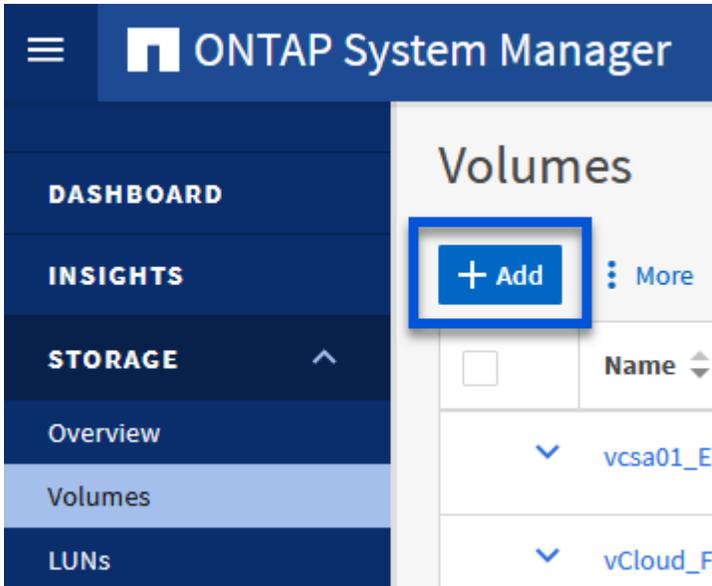
Al desplegar un dominio de carga de trabajo VI, VCF valida la conectividad con el servidor NFS. Esto se realiza mediante el adaptador de gestión de los hosts ESXi antes de agregar ningún adaptador vmkernel adicional con la dirección IP de NFS. Por lo tanto, es necesario garantizar que la política de exportación incluya la red de gestión de VCF para permitir que la validación continúe.

- Una vez introducidas todas las reglas, haz clic en el botón **Guardar** para guardar la nueva Política de exportación.
- Como alternativa, puede crear políticas y reglas de exportación en la CLI de ONTAP. Consulte los pasos para crear una política de exportación y añadir reglas en la documentación de ONTAP.
  - Utilice la interfaz de línea de comandos de ONTAP para "[Cree una política de exportación](#)".
  - Utilice la interfaz de línea de comandos de ONTAP para "[Añada una regla a una política de exportación](#)".

## Crear volumen NFS

Cree un volumen NFS en el sistema de almacenamiento de ONTAP que se utilizará como almacén de datos en la puesta en marcha del dominio de carga de trabajo.

1. Desde el Administrador del sistema de ONTAP, vaya a **Almacenamiento > Volúmenes** en el menú de la izquierda y haga clic en **+Agregar** para crear un nuevo volumen.



2. Añada un nombre para el volumen, rellene la capacidad deseada y seleccione la máquina virtual de almacenamiento que alojará el volumen. Haga clic en **Más opciones** para continuar.

## Add Volume



NAME

VCF\_WKLD\_01

CAPACITY

5



TiB



STORAGE VM

EHC\_NFS



Export via NFS

[More Options](#)

Cancel

Save

3. En Permisos de acceso, seleccione la política de exportación, que incluye la red de gestión VCF o la dirección IP y las direcciones IP de red NFS que se utilizarán para la validación del tráfico NFS Server y NFS.

## Access Permissions

Export via NFS

GRANT ACCESS TO HOST

default 

JetStream\_NFS\_v04  
Clients : 0.0.0.0/0 | Access protocols : Any

NFSmountTest01  
3 rules

NFSmountTestReno01  
Clients : 0.0.0.0/0 | Access protocols : Any

PerfTestVols  
Clients : 172.21.253.0/24 | Access protocols : NFSv3, NFSv4, NFS

TestEnv\_VPN  
Clients : 172.21.254.0/24 | Access protocols : Any

VCF\_WKLD  
2 rules

WKLD\_DM01  
2 rules

Wkld01\_NFS  
Clients : 172.21.252.205, 172.21.252.206, 172.21.252.207, 172.21.2

+



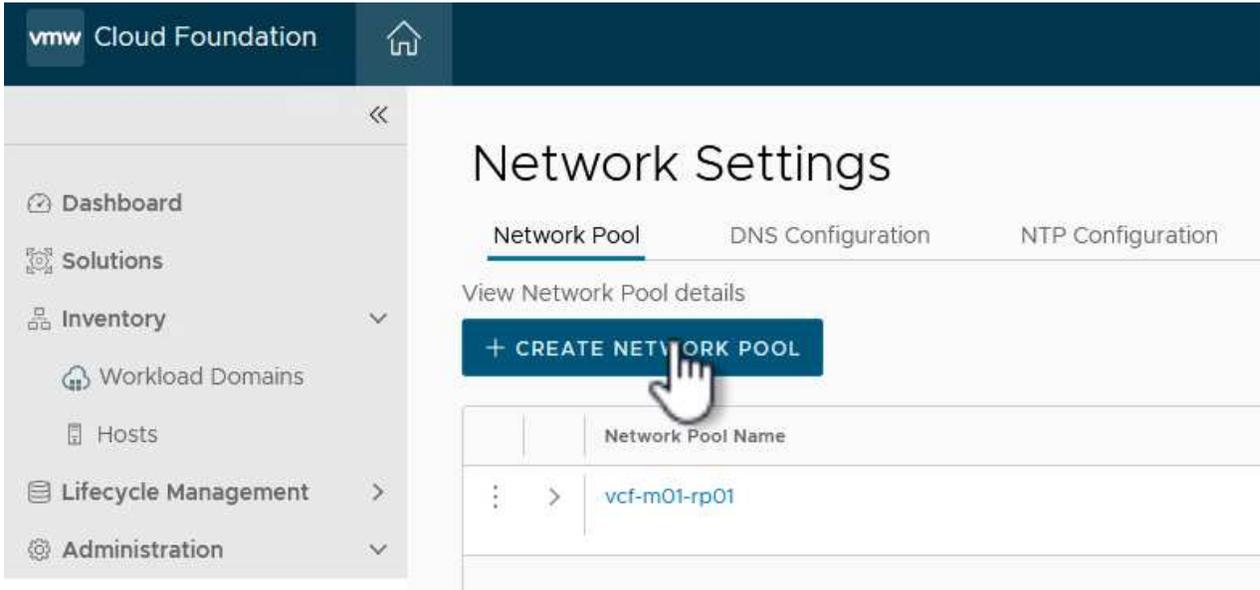
Al desplegar un dominio de carga de trabajo VI, VCF valida la conectividad con el servidor NFS. Esto se realiza mediante el adaptador de gestión de los hosts ESXi antes de agregar ningún adaptador vmkernel adicional con la dirección IP de NFS. Por lo tanto, es necesario asegurarse de que 1) la red de gestión se pueda enrutar al servidor NFS o 2) se haya añadido una LIF para la red de gestión a la SVM que aloja el volumen de almacenes de datos NFS, para garantizar que se pueda continuar con la validación.

1. Como alternativa, los volúmenes ONTAP se pueden crear en la interfaz de línea de comandos de ONTAP. Para obtener más información, consulte "[lun create](#)" Comando del en la documentación de los comandos de la ONTAP.

## Cree un pool de redes en SDDC Manager

Se debe crear el pool de anetwork en SDDC Manager antes de poner en marcha los hosts ESXi, como preparación para desplegarlos en un dominio de carga de trabajo VI. El pool de red debe incluir la información de red y los rangos de direcciones IP para los adaptadores de VMkernel que se utilizarán para la comunicación con el servidor NFS.

1. Desde la interfaz web de SDDC Manager, navegue hasta **Network Settings** en el menú de la izquierda y haga clic en el botón **+ Create Network Pool**.



2. Rellene un nombre para el pool de redes, seleccione la casilla de verificación para NFS y rellene todos los detalles de redes. Repita esto para la información de red de vMotion.

The screenshot shows the VMware Cloud Foundation interface for creating a Network Pool. The page is titled "Network Settings" and "Create Network Pool". The "Network Pool Name" is "NFS\_NPOOL". The "Network Type" is set to "NFS".

**NFS Network Information**

VLAN ID	3374
MTU	9000
Network	172.21.118.0
Subnet Mask	255.255.255.0
Default Gateway	172.21.118.1

**Included IP Address Ranges**

Once a network pool has been created, you are not able to edit or remove IP ranges from that pool.

172.21.118.145	To	172.21.118.148	REMOVE
xxx.xxx.xxx.xxx	To	xxx.xxx.xxx.xxx	ADD

**vMotion Network Information**

VLAN ID	3423
MTU	9000
Network	172.21.167.0
Subnet Mask	255.255.255.0
Default Gateway	172.21.167.1

**Included IP Address Ranges**

Once a network pool has been created, you are not able to edit or remove IP ranges from that pool.

172.21.167.121	To	172.21.167.124	REMOVE
xxx.xxx.xxx.xxx	To	xxx.xxx.xxx.xxx	ADD

At the bottom, there are "CANCEL" and "SAVE" buttons.

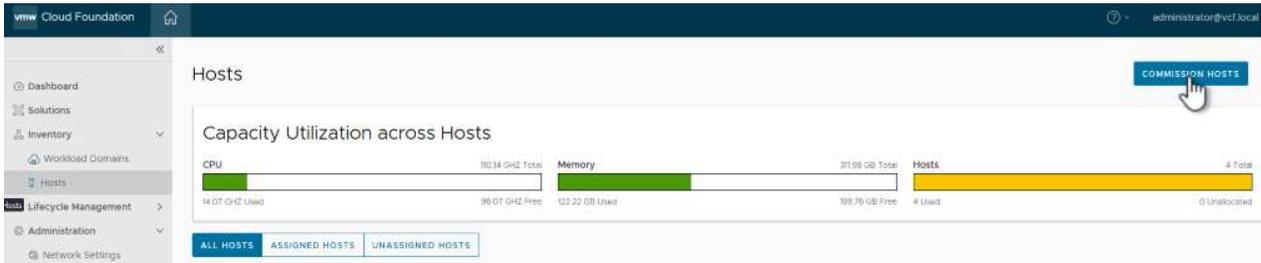
3. Haga clic en el botón **Guardar** para completar la creación del grupo de redes.

## Anfitriones de comisión

Para que los hosts ESXi puedan implementarse como dominio de carga de trabajo, deben agregarse al inventario de SDDC Manager. Esto implica proporcionar la información requerida, pasar la validación e iniciar el proceso de puesta en marcha.

Para obtener más información, consulte "[Anfitriones de comisión](#)" En la Guía de administración de VCF.

1. Desde la interfaz del Administrador de SDDC navega a **HOSTS** en el menú de la izquierda y haz clic en el botón **COMISION HOSTS**.



2. La primera página es una lista de comprobación de requisitos previos. Marque dos veces todos los requisitos previos y seleccione todas las casillas de verificación para continuar.

## Checklist

Commissioning a host adds it to the VMware Cloud Foundation inventory. The host you want to commission must meet the checklist criterion below.

- Select All**
- Host for vSAN/vSAN ESA workload domain should be vSAN/vSAN ESA compliant and certified per the VMware Hardware Compatibility Guide. BIOS, HBA, SSD, HDD, etc. must match the VMware Hardware Compatibility Guide.
- Host has a standard switch with two NIC ports with a minimum 10 Gbps speed.
- Host has the drivers and firmware versions specified in the VMware Compatibility Guide.
- Host has ESXi installed on it. The host must be preinstalled with supported versions (8.0.2-22380479)
- Host is configured with DNS server for forward and reverse lookup and FQDN.
- Hostname should be same as the FQDN.
- Management IP is configured to first NIC port.
- Ensure that the host has a standard switch and the default uplinks with 10Gb speed are configured starting with traditional numbering (e.g., vmnic0) and increasing sequentially.
- Host hardware health status is healthy without any errors.
- All disk partitions on HDD / SSD are deleted.
- Ensure required network pool is created and available before host commissioning.
- Ensure hosts to be used for VSAN workload domain are associated with VSAN enabled network pool.
- Ensure hosts to be used for NFS workload domain are associated with NFS enabled network pool.
- Ensure hosts to be used for VMFS on FC workload domain are associated with NFS or VMOTION only enabled network pool.
- Ensure hosts to be used for vVol FC workload domain are associated with NFS or VMOTION only enabled network pool.
- Ensure hosts to be used for vVol NFS workload domain are associated with NFS and VMOTION only enabled network pool.
- Ensure hosts to be used for vVol iSCSI workload domain are associated with iSCSI and VMOTION only enabled network pool.
- For hosts with a DPU device, enable SR-IOV in the BIOS and in the vSphere Client (if required by your DPU vendor).

CANCEL

PROCEED

3. En la ventana **Host Addition and Validation**, rellene el **Host FQDN**, **Storage Type**, el nombre **Network Pool** que incluye las direcciones IP de almacenamiento vMotion y NFS que se utilizarán para el dominio de carga de trabajo y las credenciales para acceder al host ESXi. Haga clic en **Add** para agregar el host al grupo de hosts que se van a validar.

## Host Addition and Validation

## Add Hosts

You can either choose to add host one at a time or download [JSON](#) template and perform bulk commission.

Add new  Import

Host FQDN

Storage Type  vSAN  NFS  VMFS on FC  vVol

Network Pool Name

User Name

Password

ADD

## Hosts Added

Hosts added successfully. Add more or confirm fingerprint and validate host

REMOVE

Confirm all Finger Prints

VALIDATE ALL

<input checked="" type="checkbox"/>	FQDN	Network Pool	IP Address	Confirm FingerPrint	Validation Status
<input checked="" type="checkbox"/>	vcf-wkld-esx01.sddc.netapp.com	NFS_NP01	172.21.166.135	<input checked="" type="checkbox"/> SHA256:CKbsinf EOG+Hz/ lpFUoFDI2tLuY FZ47WicVdp6v EGM	<input type="checkbox"/> Not Validated

CANCEL

NEXT

- Una vez que todos los hosts a validar se hayan agregado, haga clic en el botón **Validar todo** para continuar.
- Suponiendo que todos los hosts estén validados, haga clic en **Siguiente** para continuar.

## Hosts Added

✔ Host Validated Successfully. ✕

REMOVE  Confirm all Finger Prints (i) VALIDATE ALL

<input checked="" type="checkbox"/>	⋮	FGDN	Network Pool	IP Address	Confirm FingerPrint	Validation Status
<input checked="" type="checkbox"/>	⋮	vcf-wkld-esx04.sddc.netapp.com	NFS_NP01 <span style="font-size: 0.8em;">(i)</span>	172.21.166.138	<span style="color: green; font-size: 1.2em;">✔</span> SHA256:9Kg+9nQaE4SQkOMsQPON/k5gZB9zyKN+6CBPmXsvLBc	<span style="color: green; font-size: 1.2em;">✔</span> Valid
<input checked="" type="checkbox"/>	⋮	vcf-wkld-esx03.sddc.netapp.com	NFS_NP01 <span style="font-size: 0.8em;">(i)</span>	172.21.166.137	<span style="color: green; font-size: 1.2em;">✔</span> SHA256:nPX4/mei/2zmLJHfmPwbk6zhapoUxV2IOWZDPFH+z0	<span style="color: green; font-size: 1.2em;">✔</span> Valid
<input checked="" type="checkbox"/>	⋮	vcf-wkld-esx02.sddc.netapp.com	NFS_NP01 <span style="font-size: 0.8em;">(i)</span>	172.21.166.136	<span style="color: green; font-size: 1.2em;">✔</span> SHA256:AMhyR60OpTQ1YYq0DJhqVbj/M/GvrQaqUy7Ce+M4IWY	<span style="color: green; font-size: 1.2em;">✔</span> Valid
<input checked="" type="checkbox"/>	⋮	vcf-wkld-esx01.sddc.netapp.com	NFS_NP01 <span style="font-size: 0.8em;">(i)</span>	172.21.166.135	<span style="color: green; font-size: 1.2em;">✔</span> SHA256:CKbsinfEOG+ +z/lpFUoFDI2tLuYFZ47WicVDp6vEQM	<span style="color: green; font-size: 1.2em;">✔</span> Valid

CANCEL NEXT

6. Revise la lista de hosts a los que se va a poner en servicio y haga clic en el botón **Comisión** para iniciar el proceso. Supervise el proceso de puesta en marcha desde el panel Tarea del gestor de SDDC.

## Commission Hosts

1 Host Addition and Validation

2 **Review**

## Review

Skip failed hosts during commissioning   On

Validated Host(s)	
vcf-wkld-esx04.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.138 Storage Type: NFS
vcf-wkld-esx03.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.137 Storage Type: NFS
vcf-wkld-esx02.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.136 Storage Type: NFS
vcf-wkld-esx01.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.135 Storage Type: NFS

CANCEL

BACK

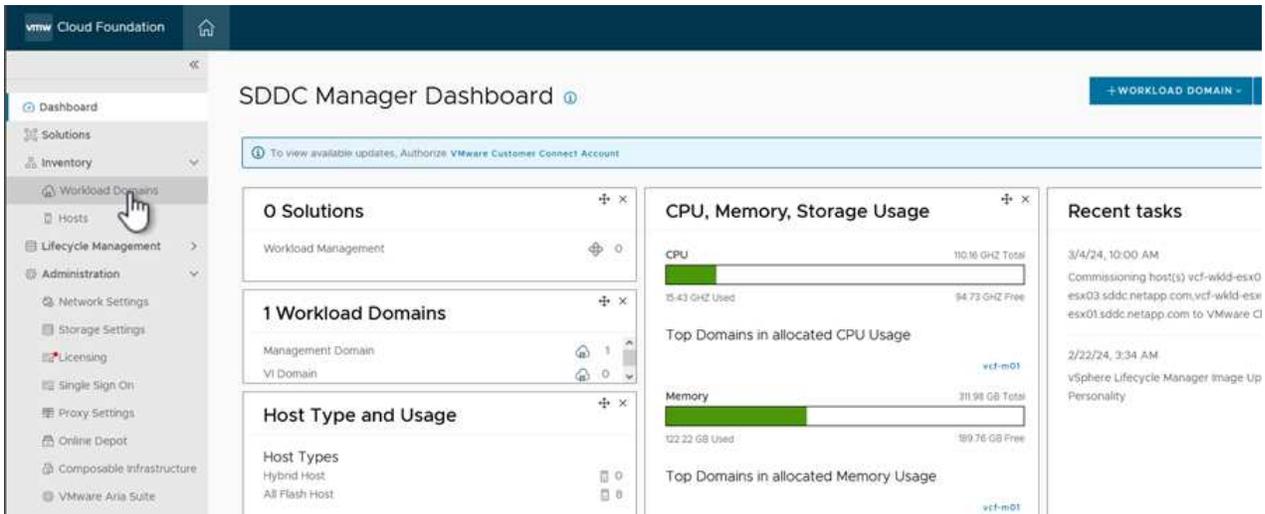
COMMISSION

## Desplegar dominio de carga de trabajo VI

La implementación de dominios de carga de trabajo de VI se realiza mediante la interfaz de VCF Cloud Manager. Aquí solo se presentarán los pasos relacionados con la configuración del almacenamiento.

Para obtener instrucciones detalladas sobre la implementación de un dominio de carga de trabajo de VI, consulte ["Despliegue un dominio de carga de trabajo de VI mediante la interfaz de usuario de SDDC Manager"](#).

1. Desde el panel de control de SDDC Manager, haga clic en **+ Workload Domain** en la esquina superior derecha para crear un nuevo dominio de carga de trabajo.



2. En el asistente de configuración VI, rellene las secciones de **Información general**, **Cluster**, **Compute**, **Networking** y **Selección de host** según sea necesario.

Para obtener información sobre cómo rellenar la información necesaria en el Asistente de configuración de VI, consulte ["Despliegue un dominio de carga de trabajo de VI mediante la interfaz de usuario de SDDC Manager"](#).

+

# VI Configuration

## 1 General Info

2 Cluster

3 Compute

4 Networking

5 Host Selection

6 NFS Storage

7 Switch Configuration

8 License

9 Review

1. En la sección Almacenamiento NFS rellene el nombre del almacén de datos, el punto de montaje de la carpeta del volumen NFS y la dirección IP de la LIF de la máquina virtual de almacenamiento NFS de ONTAP.

The screenshot shows the 'VI Configuration' interface with a sidebar on the left containing a list of steps: 1 General Info, 2 Cluster, 3 Compute, 4 Networking, 5 Host Selection, 6 NFS Storage (highlighted), 7 Switch Configuration, 8 License, and 9 Review. The main content area is titled 'NFS Storage' and contains a section for 'NFS Share Details' with three input fields:

NFS Share Details	
Datastore Name ⓘ	VCF_WKLD_01
Folder ⓘ	/VCF_WKLD_01
NFS Server IP Address ⓘ	172.21.118.163

2. En el asistente de configuración de VI, complete los pasos de configuración y licencia del switch y, a continuación, haga clic en \* Finalizar \* para iniciar el proceso de creación del dominio de carga de trabajo.

### VI Configuration

- 1 General Info
- 2 Cluster
- 3 Compute
- 4 Networking
- 5 Host Selection
- 6 NFS Storage
- 7 Switch Configuration
- 8 License
- 9 Review

### Review

General	
Virtual Infrastructure Name	vcf-wkld-01
Organization Name	it-inf
SSO Domain Option	Joining Management SSO Domain
Cluster	
Cluster Name	IT-INF-WKLD-01
Compute	
vCenter IP Address	172.21.166.143
vCenter DNS Name	vcf-wkld-vc01.sddc.netapp.com
vCenter Subnet Mask	255.255.255.0
vCenter Default Gateway	172.21.166.1
Networking	
NSX Manager Instance Option	Creating new NSX instance
NSX Manager Cluster IP	172.21.166.147
NSX Manager Cluster FQDN	vcf-w01-nsxc101.sddc.netapp.com
NSX Manager IP Addresses	172.21.166.144, 172.21.166.145, 172.21.166.146

CANCEL
BACK
FINISH

3. Supervise el proceso y resuelva los problemas de validación que surjan durante el proceso.

### Instale el plugin de NetApp NFS para VMware VAAI

El plugin NFS de NetApp para VAAI de VMware integra las bibliotecas de discos virtuales de VMware instaladas en el host ESXi y ofrece operaciones de clonado de mayor rendimiento que finalizan más rápido. Este es un procedimiento recomendado cuando se usan sistemas de almacenamiento de ONTAP con VMware vSphere.

Para obtener instrucciones paso a paso sobre la puesta en marcha del plugin de NFS de NetApp para VMware VAAI siga las instrucciones en "[Instale el plugin de NetApp NFS para VMware VAAI](#)".

### Demostración en vídeo de esta solución

[Almacenes de datos NFS como almacenamiento principal para dominios de carga de trabajo de VCF](#)

## Introducción a la automatización para ONTAP y vSphere

### Automatización de VMware

La automatización ha sido un aspecto integral de la gestión de entornos VMware desde los primeros días de VMware ESX. La capacidad de poner en marcha infraestructura como código y ampliar las prácticas en

operaciones de cloud privado ayuda a paliar las cuestiones relacionadas con el escalado, la flexibilidad, el aprovisionamiento automático y la eficiencia.

La automatización se puede organizar en las siguientes categorías:

- **Implementación de infraestructura virtual**
- **Operaciones de máquina invitada**
- **Operaciones en la nube**

Los administradores tienen a su disposición muchas opciones en lo que respecta a la automatización de su infraestructura. Ya sea mediante el uso de funciones nativas de vSphere como Perfiles de host o especificaciones de personalización para máquinas virtuales hasta las API disponibles en los componentes de software, los sistemas operativos y los sistemas de almacenamiento de NetApp, existe una documentación y guía significativas disponibles.

Data ONTAP 8.0.1 y versiones posteriores admiten ciertas funciones de API de VMware vSphere para la integración de cabinas (VAAI) cuando el host ESX ejecuta ESX 4.1 o versiones posteriores. VAAI es un conjunto de API que permiten la comunicación entre hosts ESXi de VMware vSphere y dispositivos de almacenamiento. Estas funciones ayudan a descargar las operaciones del host ESX al sistema de almacenamiento y aumentan el rendimiento de la red. El host ESX habilita las funciones automáticamente en el entorno correcto. Puede determinar la extensión hasta la cual el sistema utiliza las funciones de VAAI si se comprueban las estadísticas contenidas en los contadores VAAI.

El punto de partida más común para automatizar la puesta en marcha de un entorno VMware es el aprovisionamiento de almacenes de datos basados en bloques o archivos. Es importante trazar el mapa de los requisitos de las tareas reales antes de desarrollar la automatización correspondiente.

Si quiere más información sobre la automatización de los entornos VMware, consulte los siguientes recursos:

- ["ThePub de NetApp"](#). Gestión y automatización de la configuración de NetApp.
- ["La comunidad de Ansible Galaxy para VMware"](#). Una colección de recursos de Ansible para VMware.
- ["Recursos de VMware {code}"](#). Los recursos necesarios para diseñar soluciones para el centro de datos definido mediante software, incluidos foros, estándares de diseño, código de muestra y herramientas de desarrollo.

## Aprovisionamiento de almacenamiento en bloques vSphere tradicional con ONTAP

VMware vSphere admite las siguientes opciones de almacenes de datos VMFS con la compatibilidad con el protocolo SAN de ONTAP indicada.

Opciones de almacén de datos VMFS	Compatibilidad con el protocolo SAN de ONTAP
<a href="#">"Fibre Channel (FC)"</a>	sí
<a href="#">"Fibre Channel sobre Ethernet (FCoE)"</a>	sí
<a href="#">"iSCSI"</a>	sí
Extensiones iSCSI para RDMA (Iser)	no

Opciones de almacén de datos VMFS	Compatibilidad con el protocolo SAN de ONTAP
"NVMe sobre estructura con FC (NVMe/FC)"	sí
NVMe over Fabric con RDMA sobre Ethernet convergente (NVMe/roce)	no



Si se requiere lser o VMFS NVMe/roce, compruebe los sistemas de almacenamiento basados en SANtricity.

## Almacén de datos VMFS de vSphere: Back-end de almacenamiento de Fibre Channel con ONTAP

### Acerca de esta tarea

En esta sección se describe la creación de un almacén de datos VMFS con el almacenamiento Fibre Channel (FC) de ONTAP.

Para el aprovisionamiento automatizado, utilice uno de los siguientes scripts: [\[PowerShell\]](#), [\[Ansible\]](#), o [\[Terraform\]](#).

### Lo que necesita

- Las habilidades básicas necesarias para gestionar un entorno de vSphere y ONTAP
- Un sistema de almacenamiento de ONTAP (FAS/AFF/CVO/ONTAP Select/ASA) que ejecute ONTAP 9,8 o versiones posteriores
- Credenciales de ONTAP (nombre de SVM, ID de usuario y contraseña)
- WWPN de ONTAP con información sobre el host, el destino y la SVM y LUN
- ["La hoja de datos de configuración de FC completada"](#)
- Credenciales de vCenter Server
- Información sobre los hosts de vSphere
  - VSphere 7,0 o posterior
- Switch(es) de estructura
  - Con los puertos de datos FC de ONTAP conectados y los hosts de vSphere
  - Con la función de virtualización N\_Port ID (NPIV) habilitada
  - Cree una zona de destino única de iniciador.
    - Cree una zona para cada iniciador (zona iniciador única).
    - Para cada zona, incluya un destino que sea la interfaz lógica ONTAP FC (WWPN) para las SVM. Debe haber al menos dos interfaces lógicas por nodo por SVM. No utilice el WWPN de los puertos físicos.
- Una herramienta ONTAP para VMware vSphere puesta en marcha, configurada y lista para usar.

### Aprovisionamiento de un almacén de datos VMFS

Para aprovisionar un almacén de datos VMFS, complete los siguientes pasos:

1. Compruebe la compatibilidad con ["Herramienta de matriz de interoperabilidad \(IMT\)"](#)

2. Compruebe que el ["Es compatible con la configuración de FCP"](#).

## Tareas de ONTAP

1. ["Comprobar que tiene una licencia de ONTAP para FCP."](#)
  - a. Utilice la `system license show` Comando para comprobar que FCP aparece.
  - b. Uso `licen se add -license-code <license code>` para añadir la licencia.
2. Asegúrese de que el protocolo FCP esté habilitado en la SVM.
  - a. ["Comprobar el FCP en una SVM existente."](#)
  - b. ["Configure el FCP en una SVM existente."](#)
  - c. ["Cree una nueva SVM con FCP."](#)
3. Asegúrese de que las interfaces lógicas FCP estén disponibles en una SVM.
  - a. Uso `Network Interface show` Para comprobar el adaptador FCP.
  - b. Cuando se crea una SVM con la interfaz gráfica de usuario, las interfaces lógicas forman parte de ese proceso.
  - c. Para cambiar el nombre de las interfaces de red, utilice `Network Interface modify`.
4. ["Cree y asignar una LUN."](#) Omita este paso si utiliza herramientas de ONTAP para VMware vSphere.

## Tareas de VMware vSphere

1. Es decir, que están instalados los controladores HBA. Los HBA compatibles con VMware tienen controladores instalados de fábrica y deben estar visibles en la ["Información del adaptador de almacenamiento"](#).
2. ["Aprovisione un almacén de datos VMFS con herramientas de ONTAP"](#).

## Almacén de datos VMFS de vSphere: Protocolo de almacenamiento Fibre Channel sobre Ethernet con ONTAP

### Acerca de esta tarea

En esta sección se describe la creación de un almacén de datos VMFS con el protocolo de transporte Fibre Channel over Ethernet (FCoE) al almacenamiento de ONTAP.

Para el aprovisionamiento automatizado, utilice uno de los siguientes scripts: [\[PowerShell\]](#), [\[Ansible\]](#), o [\[Terraform\]](#).

### Lo que necesita

- Las habilidades básicas necesarias para gestionar un entorno de vSphere y ONTAP
- Un sistema de almacenamiento de ONTAP (FAS/AFF/CVO/ONTAP Select) que ejecute ONTAP 9,8 o versiones posteriores
- Credenciales de ONTAP (nombre de SVM, ID de usuario y contraseña)
- ["Una combinación de FCoE compatible"](#)
- ["Una hoja de datos de configuración completada"](#)
- Credenciales de vCenter Server

- Información sobre los hosts de vSphere
  - VSphere 7,0 o posterior
- Switch(es) de estructura
  - Con los puertos de datos FC de ONTAP o los hosts de vSphere conectados
  - Con la función de virtualización N\_Port ID (NPIV) habilitada
  - Cree una zona de destino única de iniciador.
  - ["Se ha configurado la división en zonas de FC/FCoE"](#)
- Switches de red
  - Compatibilidad con FCoE
  - Compatibilidad con DCB
  - ["Tramas gigantes para FCoE"](#)
- Herramienta ONTAP para VMware vSphere puesta en marcha, configurada y lista para usar

#### Aprovisione un almacén de datos de VMFS

- Compruebe la compatibilidad con ["Herramienta de matriz de interoperabilidad \(IMT\)"](#).
- ["Compruebe que la configuración de FCoE es compatible"](#).

#### Tareas de ONTAP

1. ["Comprobar la licencia de ONTAP para FCP."](#)
  - a. Utilice la `system license show` Comando para verificar que el FCP aparece.
  - b. Uso `license add -license-code <license code>` para añadir una licencia.
2. Compruebe que el protocolo FCP esté habilitado en la SVM.
  - a. ["Comprobar el FCP en una SVM existente."](#)
  - b. ["Configure el FCP en una SVM existente."](#)
  - c. ["Cree una nueva SVM con el FCP."](#)
3. Comprobar que las interfaces lógicas FCP están disponibles en la SVM.
  - a. Uso `Network Interface show` Para comprobar el adaptador FCP.
  - b. Cuando se crea la SVM con la interfaz gráfica de usuario, las interfaces lógicas forman parte de ese proceso.
  - c. Para cambiar el nombre de la interfaz de red, utilice `Network Interface modify`.
4. ["Cree y asigne una LUN"](#); Omita este paso si utiliza las herramientas de ONTAP para VMware vSphere.

#### Tareas de VMware vSphere

1. Compruebe que los controladores HBA están instalados. Los HBA compatibles con VMware tienen controladores instalados de fábrica y deben estar visibles en la ["información del adaptador de almacenamiento"](#).
2. ["Aprovisione un almacén de datos VMFS con herramientas de ONTAP"](#).

# Almacén de datos VMFS de vSphere: Entorno de administración del almacenamiento iSCSI con ONTAP

## Acerca de esta tarea

En esta sección, se describe la creación de un almacén de datos VMFS con almacenamiento ONTAP iSCSI.

Para el aprovisionamiento automatizado, utilice uno de los siguientes scripts: [\[PowerShell\]](#), [\[Ansible\]](#), o [\[Terraform\]](#).

## Lo que necesita

- Las habilidades básicas necesarias para gestionar un entorno de vSphere y ONTAP.
- Un sistema de almacenamiento de ONTAP (FAS/AFF/CVO/ONTAP Select/ASA) que ejecute ONTAP 9,8 o versiones posteriores
- Credenciales de ONTAP (nombre de SVM, ID de usuario y contraseña)
- Información sobre los puertos de red de ONTAP, SVM y LUN para iSCSI
- ["Hoja de datos de configuración de iSCSI completada"](#)
- Credenciales de vCenter Server
- Información sobre los hosts de vSphere
  - VSphere 7,0 o posterior
- Información de IP del adaptador de VMkernel de iSCSI
- Switches de red
  - Con los puertos de datos de red del sistema ONTAP y los hosts de vSphere conectados
  - VLAN configuradas para iSCSI
  - (Opcional) agregación de enlaces configurada para los puertos de datos de red ONTAP
- Herramienta ONTAP para VMware vSphere puesta en marcha, configurada y lista para usar

## Pasos

1. Compruebe la compatibilidad con ["Herramienta de matriz de interoperabilidad \(IMT\)"](#).
2. ["Compruebe que la configuración de iSCSI es compatible."](#)
3. Complete las siguientes tareas de ONTAP y vSphere.

## Tareas de ONTAP

1. ["Compruebe la licencia de ONTAP para iSCSI"](#).
  - a. Utilice la `system license show` Comando para comprobar si iSCSI aparece.
  - b. Uso `license add -license-code <license code>` para añadir la licencia.
2. ["Compruebe que el protocolo iSCSI está habilitado en la SVM."](#)
3. Confirmar que las interfaces lógicas de red iSCSI están disponibles en la SVM.



Cuando se crea una SVM mediante la interfaz gráfica de usuario, también se crean interfaces de red iSCSI.

4. Utilice la `Network interface` comando para ver o realizar cambios en la interfaz de red.



Se recomiendan dos interfaces de red iSCSI por nodo.

5. ["Cree una interfaz de red iSCSI."](#) Puede usar la política de servicio de bloques de datos predeterminada.
6. ["Comprobar que el servicio de datos iscsi está incluido en la normativa de servicio."](#) Puede utilizar `network interface service-policy show` para verificar.
7. ["Compruebe que las tramas gigantes están habilitadas."](#)
8. ["Cree y asigne la LUN."](#) Omita este paso si utiliza herramientas de ONTAP para VMware vSphere. Repita este paso con cada LUN.

### Tareas de VMware vSphere

1. Verifique que hay al menos un NIC disponible para la VLAN iSCSI. Se prefieren dos NIC para mejorar el rendimiento y la tolerancia a fallos.
2. ["Identifique la cantidad de NIC físicas disponibles en el host vSphere."](#)
3. ["Configure el iniciador de iSCSI."](#) Un caso de uso típico es un iniciador iSCSI de software.
4. ["Compruebe que la pila TCP/IP para iSCSI está disponible"](#).
5. ["Compruebe que los grupos de puertos iSCSI estén disponibles"](#).
  - Normalmente utilizamos un único switch virtual con varios puertos de enlace ascendente.
  - Utilice la asignación de adaptador 1:1.
6. Compruebe que los adaptadores de VMkernel iSCSI están habilitados para coincidir con el número de NIC y que las IP están asignadas.
7. ["Vincule el adaptador de software iSCSI a los adaptadores de VMkernel iSCSI."](#)
8. ["Aprovisione el almacén de datos VMFS con herramientas de ONTAP"](#). Repita este paso para todos los almacenes de datos.
9. ["Comprobar la compatibilidad con la aceleración de hardware."](#)

### El futuro

Una vez completadas estas tareas, el almacén de datos VMFS estará listo para consumir para aprovisionar máquinas virtuales.

### Libro de estrategia de Ansible

```
## Disclaimer: Sample script for reference purpose only.

- hosts: '{{ vsphere_host }}'
  name: Play for vSphere iSCSI Configuration
  connection: local
  gather_facts: false
  tasks:
    # Generate Session ID for vCenter
    - name: Generate a Session ID for vCenter
      uri:
        url: "https://{{ vcenter_hostname }}/rest/com/vmware/cis/session"
        validate_certs: false
        method: POST
```

```

    user: "{{ vcenter_username }}"
    password: "{{ vcenter_password }}"
    force_basic_auth: yes
    return_content: yes
    register: vclogin

# Generate Session ID for ONTAP tools with vCenter
- name: Generate a Session ID for ONTAP tools with vCenter
  uri:
    url: "https://{{ ontap_tools_ip
}}:8143/api/rest/2.0/security/user/login"
    validate_certs: false
    method: POST
    return_content: yes
    body_format: json
    body:
      vcenterUserName: "{{ vcenter_username }}"
      vcenterPassword: "{{ vcenter_password }}"
    register: login

# Get existing registered ONTAP Cluster info with ONTAP tools
- name: Get ONTAP Cluster info from ONTAP tools
  uri:
    url: "https://{{ ontap_tools_ip
}}:8143/api/rest/2.0/storage/clusters"
    validate_certs: false
    method: Get
    return_content: yes
    headers:
      vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
    register: clusterinfo

- name: Get ONTAP Cluster ID
  set_fact:
    ontap_cluster_id: "{{ clusterinfo.json |
json_query(clusteridquery) }}"
  vars:
    clusteridquery: "records[?ipAddress == '{{ netapp_hostname }}' &&
type=='Cluster'].id | [0]"

- name: Get ONTAP SVM ID
  set_fact:
    ontap_svm_id: "{{ clusterinfo.json | json_query(svmidquery) }}"
  vars:
    svmidquery: "records[?ipAddress == '{{ netapp_hostname }}' &&
type=='SVM' && name == '{{ svm_name }}'].id | [0]"

```

```

- name: Get Aggregate detail
  uri:
    url: "https://{{ ontap_tools_ip
}}:8143/api/rest/2.0/storage/clusters/{{ ontap_svm_id }}/aggregates"
    validate_certs: false
    method: GET
    return_content: yes
    headers:
      vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
      cluster-id: "{{ ontap_svm_id }}"
  when: ontap_svm_id != ''
  register: aggrinfo

- name: Select Aggregate with max free capacity
  set_fact:
    aggr_name: "{{ aggrinfo.json | json_query(aggrquery) }}"
  vars:
    aggrquery: "max_by(records, &freeCapacity).name"

- name: Convert datastore size in MB
  set_fact:
    datastoreSizeInMB: "{{ iscsi_datastore_size |
human_to_bytes/1024/1024 | int }}"

- name: Get vSphere Cluster Info
  uri:
    url: "https://{{ vcenter_hostname }}/api/vcenter/cluster?names={{
vsphere_cluster }}"
    validate_certs: false
    method: GET
    return_content: yes
    body_format: json
    headers:
      vmware-api-session-id: "{{ vclogin.json.value }}"
  when: vsphere_cluster != ''
  register: vcenterclusterid

- name: Create iSCSI VMFS-6 Datastore with ONTAP tools
  uri:
    url: "https://{{ ontap_tools_ip
}}:8143/api/rest/3.0/admin/datastore"
    validate_certs: false
    method: POST
    return_content: yes
    status_code: [200]

```

```

body_format: json
body:
  traditionalDatastoreRequest:
    name: "{{ iscsi_datastore_name }}"
    datastoreType: VMFS
    protocol: ISCSI
    spaceReserve: Thin
    clusterID: "{{ ontap_cluster_id }}"
    svmID: "{{ ontap_svm_id }}"
    targetMoref: ClusterComputeResource:{{
vcenterclusterid.json[0].cluster }}
    datastoreSizeInMB: "{{ datastoreSizeInMB | int }}"
    vmfsFileSystem: VMFS6
    aggrName: "{{ aggr_name }}"
    existingFlexVolName: ""
    volumeStyle: FLEXVOL
    datastoreClusterMoref: ""
  headers:
    vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
  when: ontap_cluster_id != '' and ontap_svm_id != '' and aggr_name !=
''
register: result
changed_when: result.status == 200

```

## Almacén de datos VMFS de vSphere: NVMe/FC con ONTAP

### Acerca de esta tarea

En esta sección se describe la creación de un almacén de datos VMFS con almacenamiento ONTAP mediante NVMe/FC.

Para el aprovisionamiento automatizado, utilice uno de los siguientes scripts: [\[PowerShell\]](#), [\[Ansible\]](#), o [\[Terraform\]](#).

### Lo que necesita

- Se necesitan habilidades básicas para gestionar un entorno de vSphere y ONTAP.
- ["Comprensión básica de NVMe/FC"](#).
- Un sistema de almacenamiento de ONTAP (FAS/AFF/CVO/ONTAP Select/ASA) que ejecute ONTAP 9,8 o versiones posteriores
- Credenciales de ONTAP (nombre de SVM, ID de usuario y contraseña)
- WWPN de ONTAP para información sobre el host, el destino y las SVM y la LUN
- ["Una hoja de datos de configuración de FC completada"](#)
- VCenter Server
- Información de hosts de vSphere (vSphere 7,0 o posterior)
- Switch(es) de estructura

- Con los puertos de datos FC de ONTAP y los hosts de vSphere conectados.
- Con la función de virtualización N\_Port ID (NPIV) habilitada.
- Cree una sola zona de destino de iniciador.
- Cree una zona para cada iniciador (zona iniciador única).
- Para cada zona, incluya un destino que sea la interfaz lógica ONTAP FC (WWPN) para las SVM. Debe haber al menos dos interfaces lógicas por nodo por SVM. No utilice el WWPN de los puertos físicos.

### Aprovisione el almacén de datos VMFS

1. Compruebe la compatibilidad con ["Herramienta de matriz de interoperabilidad \(IMT\)"](#).
2. ["Compruebe que la configuración de NVMe/FC sea compatible."](#)

### Tareas de ONTAP

1. ["Comprobar la licencia de ONTAP para FCP."](#) Utilice la `system license show` Y compruebe si aparece `NVMe_of`. Use `license add -license-code <license code>` para añadir una licencia.
2. Compruebe que el protocolo NVMe esté habilitado en la SVM.
  - a. ["Configure SVM para NVMe."](#)
3. Compruebe que las interfaces lógicas de NVMe/FC estén disponibles en las SVM.
  - a. Use `Network Interface show` Para comprobar el adaptador FCP.
  - b. Cuando se crea una SVM con la interfaz gráfica de usuario, las interfaces lógicas se forman parte de ese proceso.
  - c. Para cambiar el nombre de la interfaz de red, utilice el comando `Network Interface modify`.
4. ["Cree el espacio de nombres y el subsistema NVMe"](#)

### Tareas de VMware vSphere

1. Compruebe que los controladores HBA están instalados. Los HBA compatibles con VMware tienen los controladores instalados de fábrica y deben ser visibles en ["Información del adaptador de almacenamiento"](#)
2. ["Realice tareas de instalación y validación del controlador vSphere NVMe host"](#)
3. ["Crear almacén de datos VMFS"](#)

## Aprovisionamiento de almacenamiento de archivos tradicional de vSphere con ONTAP

VMware vSphere admite los siguientes protocolos NFS, los cuales son compatibles con ONTAP.

- ["NFS Versión 3"](#)
- ["NFS Versión 4.1"](#)

Si necesita ayuda para seleccionar la versión de NFS correcta para vSphere, compruebe ["Esta comparativa de las versiones del cliente NFS"](#).

### Referencia

## "Funciones de protocolo y almacén de datos de vSphere: NFS"

### Almacén de datos NFS de vSphere: Versión 3 con ONTAP

#### Acerca de esta tarea

Creación de un almacén de datos de NFS versión 3 con almacenamiento NAS de ONTAP.

Para el aprovisionamiento automatizado, utilice uno de los siguientes scripts: [\[PowerShell\]](#), [\[Ansible\]](#), o [\[Terraform\]](#).

#### Lo que necesita

- Las habilidades básicas necesarias para gestionar un entorno de vSphere y ONTAP.
- Un sistema de almacenamiento de ONTAP (FAS/AFF/CVO/ONTAP Select/Servicio de volumen de cloud/Azure NetApp Files) con ONTAP 9.8 o posterior
- Credenciales de ONTAP (nombre de SVM, ID de usuario, contraseña)
- Información sobre el puerto de red de ONTAP, SVM y LUN para NFS
  - ["Una hoja de trabajo de configuración de NFS completada"](#)
- Credenciales de vCenter Server
- Información sobre los hosts de vSphere para vSphere 7.0 o una versión posterior
- Información de IP del adaptador de VMkernel de NFS
- Switches de red
  - Con los puertos de datos de red del sistema ONTAP y los hosts de vSphere conectados
  - VLAN configuradas para NFS
  - (Opcional) agregación de enlaces configurada para los puertos de datos de red ONTAP
- Herramienta ONTAP para VMware vSphere puesta en marcha, configurada y lista para usar

#### Pasos

- Compruebe la compatibilidad con ["Herramienta de matriz de interoperabilidad \(IMT\)"](#)
  - ["Compruebe que la configuración de NFS es compatible."](#)
- Complete las siguientes tareas de ONTAP y vSphere.

#### Tareas de ONTAP

1. ["Comprobar la licencia de ONTAP para NFS."](#)
  - a. Utilice la `system license show` Y compruebe que NFS aparece en la lista.
  - b. Uso `license add -license-code <license code>` para añadir una licencia.
2. ["Siga el flujo de trabajo de configuración de NFS."](#)

#### Tareas de VMware vSphere

["Siga el flujo de trabajo de configuración del cliente NFS para vSphere."](#)

## Referencia

["Funciones de protocolo y almacén de datos de vSphere: NFS"](#)

## El futuro

Una vez completadas estas tareas, el almacén de datos NFS estará listo para consumir para aprovisionar máquinas virtuales.

## Almacén de datos NFS de vSphere: Versión 4.1 con ONTAP

### Acerca de esta tarea

En esta sección se describe la creación de un almacén de datos de NFS versión 4.1 con almacenamiento NAS de ONTAP.

Para el aprovisionamiento automatizado, utilice uno de los siguientes scripts: [\[PowerShell\]](#), [\[Ansible\]](#), o [\[Terraform\]](#).

### Lo que necesita

- Las habilidades básicas necesarias para gestionar un entorno de vSphere y ONTAP
- Sistema de almacenamiento de ONTAP (FAS/AFF/CVO/ONTAP Select/Cloud Volume Service/Azure NetApp Files) que ejecute ONTAP 9,8 o posterior
- Credenciales de ONTAP (nombre de SVM, ID de usuario, contraseña)
- Información sobre el puerto de red de ONTAP, SVM y LUN para NFS
- ["Una hoja de trabajo de configuración de NFS completada"](#)
- Credenciales de vCenter Server
- Información sobre los hosts de vSphere vSphere 7,0 o posterior
- Información de IP del adaptador de VMkernel de NFS
- Switches de red
  - Con los puertos de datos de red del sistema ONTAP, los hosts de vSphere y los están conectados
  - VLAN configuradas para NFS
  - (Opcional) agregación de enlaces configurada para los puertos de datos de red ONTAP
- Herramientas de ONTAP para VMware vSphere puestas en marcha, configuradas y listas para usar

### Pasos

- Compruebe la compatibilidad con ["Herramienta de matriz de interoperabilidad \(IMT\)."](#)
  - ["Compruebe que la configuración de NFS es compatible."](#)
- Complete las tareas de ONTAP y vSphere que se proporcionan a continuación.

### Tareas de ONTAP

1. ["Comprobar la licencia de ONTAP para NFS"](#)
  - a. Úselos `system license show` Comando para comprobar si NFS aparece en la lista.
  - b. Use `license add -license-code <license code>` para añadir una licencia.

## 2. "Siga el flujo de trabajo de configuración de NFS"

### Tareas de VMware vSphere

"Siga el flujo de trabajo de configuración del cliente de NFS para vSphere."

### El futuro

Una vez completadas estas tareas, el almacén de datos NFS estará listo para consumir para aprovisionar máquinas virtuales.

## Multicloud híbrido de NetApp con soluciones de VMware

### Casos de uso de multicloud híbrido de VMware

#### Casos de uso del multicloud híbrido de NetApp con VMware

Una descripción de los casos de uso que son importantes para la organización TECNOLÓGICA al planificar una puesta en marcha de cloud híbrido o cloud-first.

#### Casos de uso populares

Sus casos de uso son:

- Recuperación tras desastres,
- Alojamiento de cargas de trabajo durante el mantenimiento del centro de datos; \* explosión rápida en la que se necesitan recursos adicionales más allá de lo aprovisionado en el centro de datos local,
- Ampliación de sitios de VMware,
- Migración rápida al cloud,
- Desarrollo/pruebas, y
- Modernización de aplicaciones aprovechando tecnologías complementarias de cloud.

A lo largo de esta documentación, las referencias de cargas de trabajo del cloud se detallarán por medio de casos de uso de VMware. Estos casos de uso son:

- Protect (incluye recuperación ante desastres y backup/restauración)
- Migración
- Extender

#### En el camino hacia la TECNOLOGÍA

La mayoría de las organizaciones se encuentran en un camino hacia la transformación y la modernización. Como parte de este proceso, las empresas intentan aprovechar sus inversiones existentes en VMware al mismo tiempo que aprovechan las ventajas de la nube y exploran las formas de hacer el proceso de migración de la forma más fluida posible. Este enfoque facilita enormemente sus esfuerzos de modernización, ya que los datos ya están en el cloud.

La respuesta más sencilla a este escenario son las ofertas de VMware en cada proveedor a hiperescala. Al igual que Cloud Volumes de NetApp®, VMware proporciona una forma de mover o ampliar los entornos VMware locales a cualquier cloud, lo que le permite conservar activos, habilidades y herramientas existentes

en las instalaciones al tiempo que ejecuta cargas de trabajo de forma nativa en el cloud. De este modo se reduce el riesgo, ya que no se producirán interrupciones del servicio ni se necesitarán cambios en la IP, y el equipo DE TECNOLOGÍA podrá utilizar las habilidades y herramientas existentes de la manera en que lo hacen en las instalaciones. Esto puede llevar a migraciones de cloud aceleradas y a una transición mucho más fluida a una arquitectura multicloud híbrida.

### **Descripción de la importancia de las opciones de almacenamiento de NFS suplementario**

Mientras que VMware en cualquier cloud ofrece funcionalidades híbridas únicas a todos los clientes, las opciones de almacenamiento NFS suplementario limitadas han restringido su utilidad para las organizaciones con cargas de trabajo que requieren un gran nivel de almacenamiento. Debido a que el almacenamiento está directamente ligado a los hosts, la única forma de escalar el almacenamiento es añadir más hosts, lo cual puede aumentar los costes entre un 35 y un 40 % o más para cargas de trabajo con un uso intensivo del almacenamiento. Estas cargas de trabajo solo necesitan almacenamiento adicional, no una potencia adicional. Pero eso significa pagar por los anfitriones adicionales.

Consideremos este caso:

Un cliente solo necesita cinco hosts para CPU y memoria, pero tiene muchas necesidades de almacenamiento y necesita 12 hosts para satisfacer sus requisitos de almacenamiento. Este requisito acaba realmente a la altura del escalado financiero al tener que comprar la potencia adicional cuando solo necesitan aumentar el almacenamiento.

Cuando planifica la adopción y las migraciones de la nube, siempre es importante evaluar el mejor enfoque y tomar el camino más sencillo que reduzca las inversiones totales. El método más habitual y sencillo para la migración de cualquier aplicación es el realojamiento (también conocido como lift and shift), en el que no hay ningún equipo virtual (VM) ni conversión de datos. Al utilizar Cloud Volumes de NetApp con el centro de datos definido por software (SDDC) de VMware, al tiempo que complementa VSAN, proporciona una opción de elevación y cambio sencilla.

## **Escritorios virtuales**

### **Servicios de puestos de trabajo virtuales (VDS)**

#### **TR-4861: VDI de cloud híbrido con servicio de puestos de trabajo virtuales**

Suresh Thoppay, NetApp

El servicio de escritorios virtuales (VDS) de NetApp organiza los servicios de escritorios remotos (RDS) en los principales clouds públicos y en clouds privados. VDS es compatible con Windows Virtual Desktop (WVD) en Microsoft Azure. VDS automatiza muchas tareas que se deben realizar después de la implementación de WVD o RDS, incluida la configuración de recursos compartidos de archivos SMB (para perfiles de usuario, datos compartidos y la unidad de inicio del usuario), habilitar funciones de Windows, instalación de aplicaciones y agentes, firewall y políticas, etc.

Los usuarios consumen VDS para escritorios dedicados, escritorios compartidos y aplicaciones remotas. VDS proporciona eventos con secuencias de comandos para automatizar la administración de aplicaciones en los escritorios y reduce el número de imágenes que se van a gestionar.

VDS proporciona un único portal de gestión para gestionar las puestas en marcha de entornos de cloud público y privado.

## Valor para el cliente

La explosión de personal remoto en 2020 ha cambiado los requisitos de continuidad del negocio. Los departamentos DE TECNOLOGÍA deben hacer frente a nuevos retos para aprovisionar con rapidez puestos de trabajo virtuales y, por tanto, requerir agilidad de aprovisionamiento, gestión remota y las ventajas del TCO de un cloud híbrido que facilita el aprovisionamiento de recursos en las instalaciones y en el cloud. Necesitan una solución de cloud híbrido que:

- Aborda la realidad del espacio de trabajo post-COVID para hacer posibles modelos de trabajo flexibles con dinámica global
- Permite el trabajo en turnos simplificando y acelerando la implementación de entornos de trabajo para todos los empleados, desde trabajadores de tareas hasta usuarios avanzados
- Moviliza a su personal proporcionando recursos de infraestructura de puestos de trabajo virtuales seguros y enriquecidos independientemente de la ubicación física
- Simplifica la puesta en marcha del cloud híbrido
- Automatiza y simplifica la gestión de la reducción de riesgos

## Casos de uso

La infraestructura de puestos de trabajo virtuales híbrida con VDS de NetApp permite a los proveedores de servicios y a los administradores de puestos de trabajo virtuales empresariales ampliar fácilmente los recursos a otro entorno de cloud sin que ello afecte a los usuarios. Contar con recursos en las instalaciones proporciona un mejor control de los recursos y ofrece una amplia selección de opciones (computación, GPU, almacenamiento y red) para satisfacer la demanda.

Esta solución se aplica a los siguientes casos de uso:

- Desbordamiento del cloud por el aumento en la demanda de aplicaciones y puestos de trabajo remotos
- Reducir el TCO en aplicaciones y puestos de trabajo remotos de larga duración alojándolos en las instalaciones con almacenamiento flash y recursos GPU
- Facilidad de gestión de puestos de trabajo y aplicaciones remotos en todos los entornos cloud
- Disfrute de aplicaciones y puestos de trabajo remotos usando un modelo de software como servicio con recursos en las instalaciones

## Público objetivo

El público objetivo de la solución incluye los siguientes grupos:

- Arquitectos de EUC/VDI que quieren comprender los requisitos de una instancia de VDS híbrida
- Los partners de NetApp que desean ayudar a sus clientes con sus necesidades de aplicaciones y puesto de trabajo remoto
- Clientes de NetApp HCI existentes que desean atender las demandas de las aplicaciones y los puestos de trabajo remotos

## Descripción general de Virtual Desktop Service de NetApp

NetApp ofrece muchos servicios cloud, como el aprovisionamiento rápido de puestos de trabajo virtuales con WVD o aplicaciones remotas, y la rápida integración con Azure

## NetApp Files.

Tradicionalmente, se necesitan semanas para aprovisionar y prestar servicios de escritorios remotos a los clientes. Además del aprovisionamiento, puede resultar difícil gestionar aplicaciones, perfiles de usuario, datos compartidos y objetos de normativa de grupo para aplicar normativas. Las reglas de firewall pueden aumentar la complejidad y requerir habilidades y herramientas separadas.

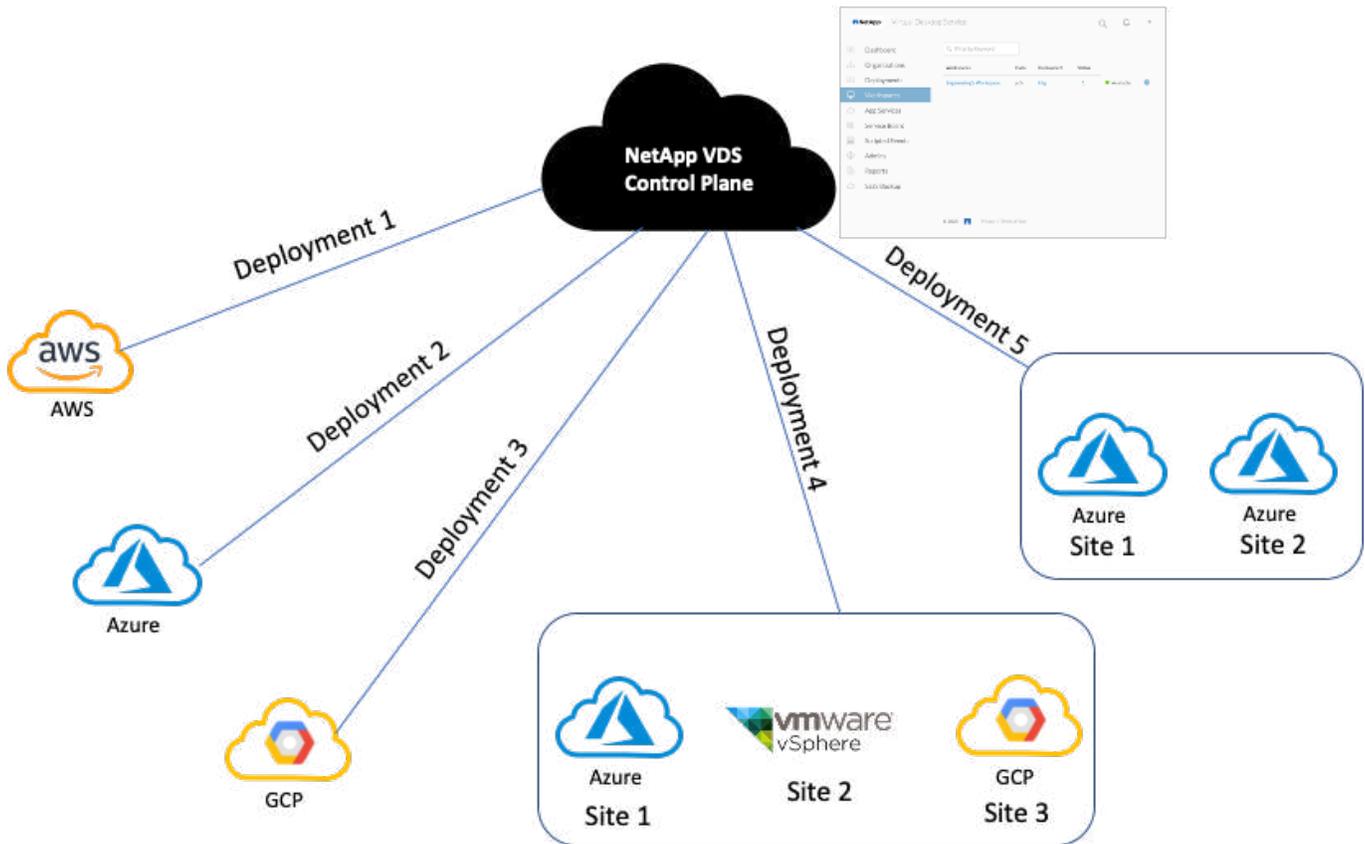
Con el servicio de escritorio virtual de Microsoft Azure Windows, Microsoft se ocupa del mantenimiento de los componentes de Servicios de Escritorio remoto, lo que permite a los clientes centrarse en aprovisionar espacios de trabajo en el cloud. Los clientes deben aprovisionar y gestionar toda la pila, lo cual requiere habilidades especiales para gestionar entornos de VDI.

Con VDS de NetApp, los clientes pueden poner en marcha rápidamente puestos de trabajo virtuales sin tener que preocuparse de dónde instalar los componentes de arquitectura como intermediarios, puertas de enlace, agentes, etc. Los clientes que necesiten un control completo de su entorno pueden trabajar con un equipo de servicios profesionales para lograr sus objetivos. Los clientes consumen VDS como servicio y, por lo tanto, pueden centrarse en sus desafíos empresariales clave.

VDS de NetApp es una oferta de software como servicio para gestionar de forma centralizada varias puestas en marcha en entornos de AWS, Azure, GCP o de cloud privado. Microsoft Windows Virtual Desktop solo está disponible en Microsoft Azure. VDS de NetApp orquesta servicios de Microsoft Remote Desktop en otros entornos

Microsoft ofrece varias sesiones en Windows 10 exclusivamente para entornos de escritorio virtual de Windows en Azure. La autenticación e identidad se gestionan mediante la tecnología de puestos de trabajo virtuales; WVD requiere que Azure Active Directory se sincroniza (con AD Connect) con Active Directory y que las máquinas virtuales de sesión se unen a Active Directory. RDS requiere Active Directory para la identidad de usuario, la autenticación y la unión y la gestión del dominio de VM.

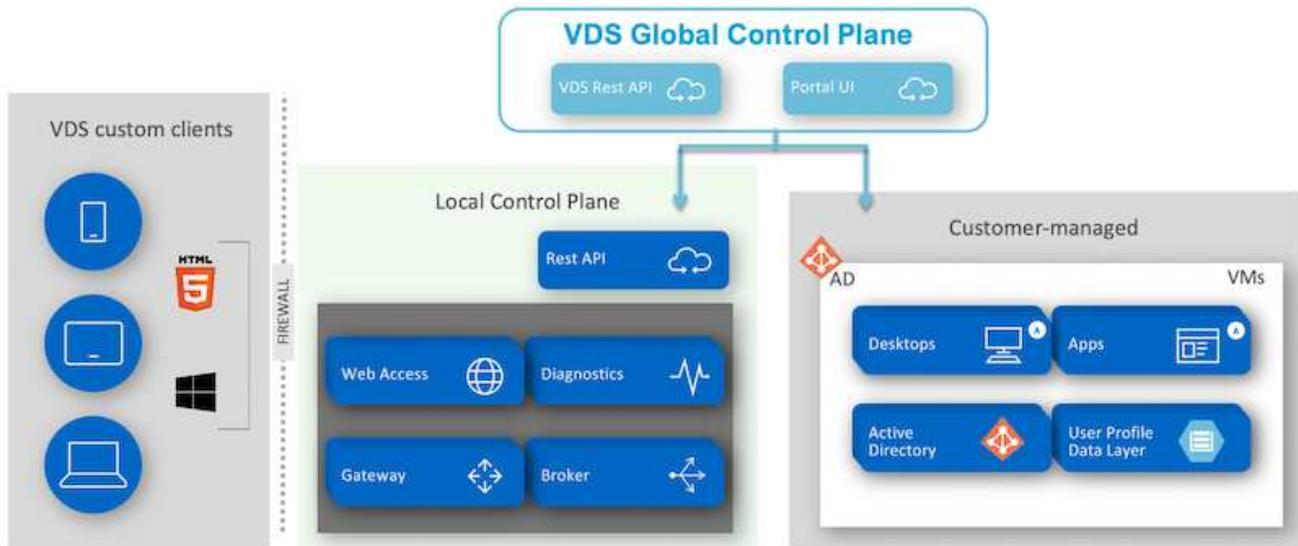
En la siguiente figura se muestra un ejemplo de topología de puesta en marcha.



Cada implementación está asociada a un dominio de directorio activo y proporciona a los clientes un punto de entrada de acceso para áreas de trabajo y aplicaciones. Normalmente, un proveedor de servicios o empresa que tiene varios dominios de Active Directory tiene más puestas en marcha. Un único dominio de Active Directory que abarca varias regiones normalmente tiene una única implementación con varios sitios.

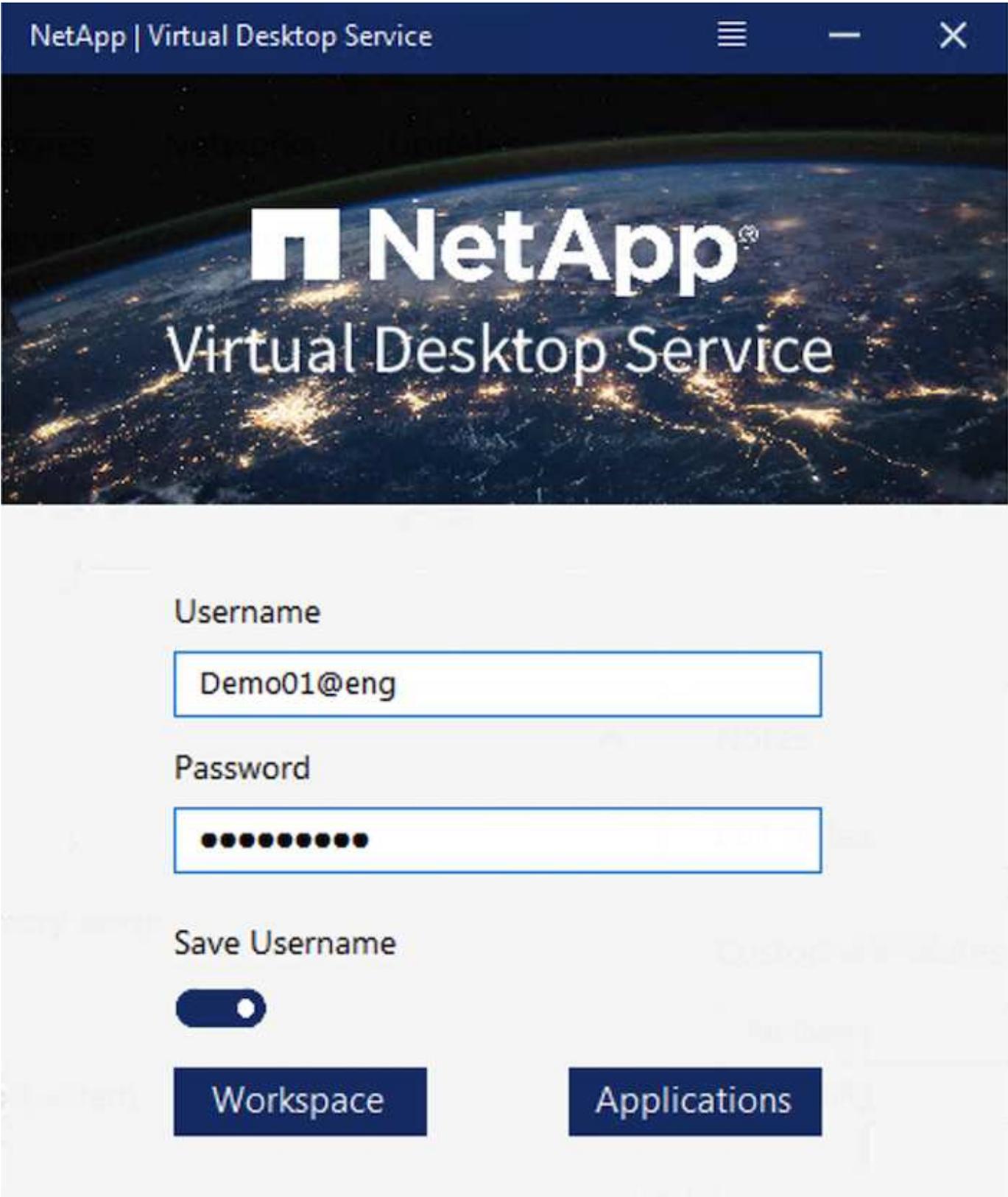
Para WVD en Azure, Microsoft proporciona una plataforma como servicio que VDS de NetApp consume. En otros entornos, VDS de NetApp coordina la implementación y la configuración de Microsoft Remote Desktop Services. VDS de NetApp es compatible con WVD Classic y WVD ARM, y también se puede utilizar para actualizar las versiones existentes.

Cada puesta en marcha tiene sus propios servicios de plataforma, que consisten en Cloud Workspace Manager (extremo de la API DE REST), una puerta de enlace HTML 5 (conexión a equipos virtuales desde un portal de gestión VDS), puertas de enlace RDS (punto de acceso para clientes) y un controlador de dominio. La siguiente figura muestra la arquitectura VDS Control Plane para la implementación RDS.



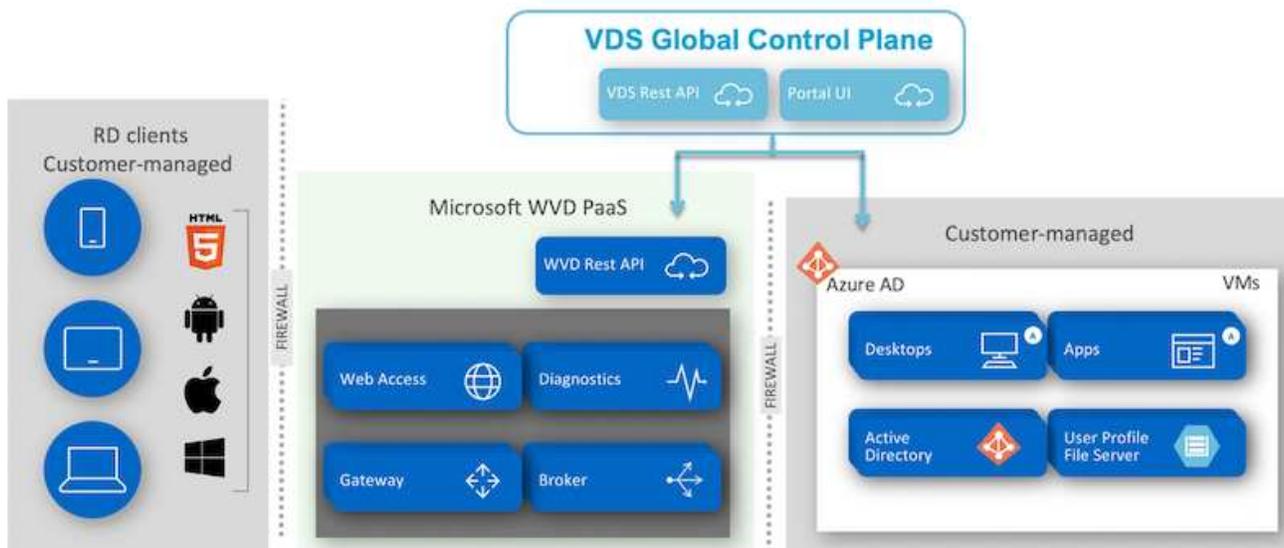
Para implementaciones RDS, se puede acceder fácilmente a VDS de NetApp desde Windows y navegadores con un software de cliente que puede personalizarse para incluir imágenes y el logotipo del cliente. Basándose en las credenciales de usuario, proporciona acceso de los usuarios a los espacios de trabajo y aplicaciones aprobados. No es necesario configurar los detalles de la puerta de enlace.

La siguiente figura muestra el cliente VDS de NetApp.



En la implementación de Azure WVD, Microsoft gestiona el punto de entrada de acceso de los clientes y puede ser consumido por un cliente WVD de Microsoft disponible de forma nativa para varios SO. También se puede acceder a él desde un portal web. La configuración del software cliente debe ser gestionada por el objeto de directiva de grupo (GPO) o de otras formas preferidas por los clientes.

En la siguiente figura se muestra la arquitectura VDS Control Plane para implementaciones de Azure WVD.



Además de la instalación y configuración de los componentes necesarios, NetApp VDS también gestiona la gestión de usuarios, la gestión de aplicaciones, el escalado de recursos y la optimización.

VDS de NetApp puede crear usuarios o conceder acceso a cuentas de usuario existentes al espacio de trabajo del cloud o a los servicios de la aplicación. El portal también se puede utilizar para restablecer contraseñas y para la delegación de administrar un subconjunto de componentes. Los administradores del servicio de asistencia técnica o los técnicos de nivel 3 pueden remedar sesiones de usuario para solucionar problemas o conectarse a servidores desde el portal.

VDS de NetApp puede utilizar las plantillas de imagen que crea o puede usar las existentes del mercado para el aprovisionamiento basado en cloud. Para reducir el número de imágenes que se deben gestionar, puede utilizar una imagen base y aprovisionar cualquier aplicación adicional que necesite utilizando el marco proporcionado para incluir cualquier herramienta de línea de comandos como Chocolatey, conexión de aplicaciones MSIX, PowerShell, etc. Incluso los scripts personalizados pueden utilizarse como parte de los eventos de ciclo de vida de la máquina.

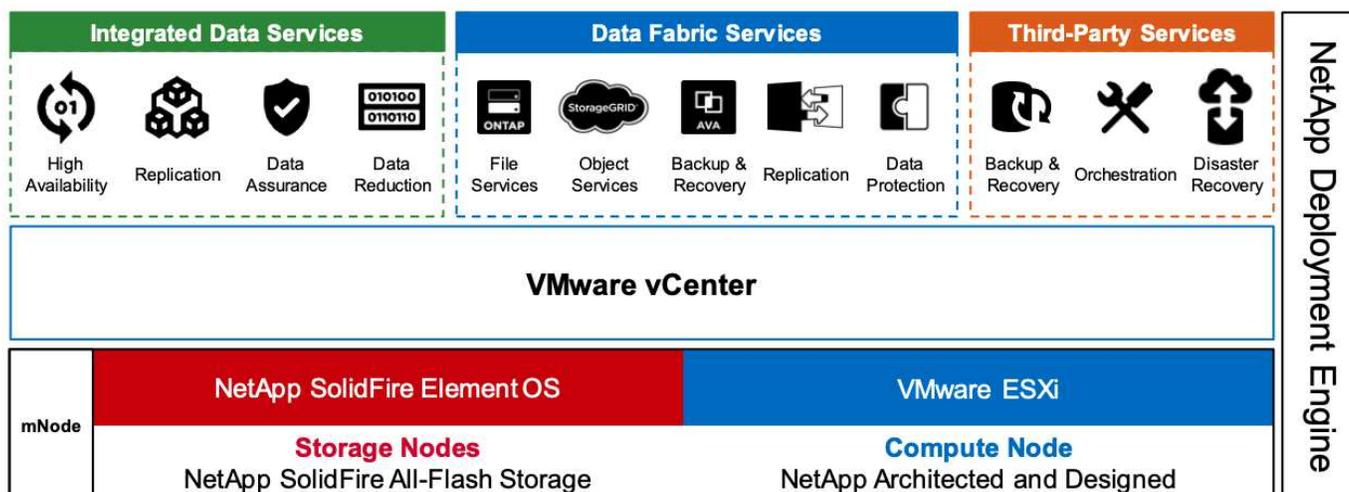
### Información general de NetApp HCI

NetApp HCI es una infraestructura de cloud híbrido que consta de una combinación de nodos de almacenamiento y nodos de computación. Está disponible en función del modelo, como unidad de dos racks o de un solo rack. La instalación y configuración necesarias para poner en marcha máquinas virtuales se automatizan con el motor de puesta en marcha de NetApp (NDE). Los clústeres de computación se gestionan con VMware vCenter y los clústeres de almacenamiento se gestionan con el plugin de vCenter puesto en marcha con NDE. Como parte de NDE, se pone en marcha una máquina virtual de gestión, denominada mNode.

NetApp HCI gestiona las siguientes funciones:

- Actualizaciones de versiones
- Llevar eventos a vCenter
- Gestión del complemento de vCenter
- Un túnel VPN para soporte

- El recopilador Active IQ de NetApp
- La extensión de los servicios cloud de NetApp a las instalaciones, lo cual permite una infraestructura de cloud híbrido. En la siguiente figura, se muestran los componentes HCI.



## Nodos de almacenamiento

Los nodos de almacenamiento están disponibles en una unidad de rack de media anchura o de anchura completa. En primer lugar se requiere un mínimo de cuatro nodos de almacenamiento y un clúster se puede ampliar hasta 40 nodos. Un clúster de almacenamiento se puede compartir entre varios clústeres de computación. Todos los nodos de almacenamiento contienen una controladora de caché para mejorar el rendimiento de escritura. Un único nodo proporciona 50 000 o 100 000 IOPS a un tamaño de bloque de 4 KB.

Los nodos de almacenamiento de NetApp HCI ejecutan el software NetApp Element, que proporciona límites de calidad de servicio mínimos, máximos y de ráfaga. El clúster de almacenamiento admite una combinación de nodos de almacenamiento, aunque un nodo de almacenamiento no puede superar un tercio de la capacidad total.

## Nodos de computación



NetApp admite su almacenamiento conectado a cualquier servidor informático que figure en el ["Guía de compatibilidad de VMware"](#).

Los nodos de computación están disponibles en tamaño de media anchura, de anchura completa y de dos unidades de rack. El NetApp HCI H410C y H610C están basados en procesadores escalables de Intel Skylake. El sistema H615C se basa en los procesadores Intel Cascade Lake escalables de segunda generación. Hay dos modelos de computación que contienen GPU: La H610C contiene dos tarjetas NVIDIA M10 y la H615C contiene tres tarjetas NVIDIA T4.



El NVIDIA T4 cuenta con 40 núcleos RT que proporcionan la potencia de computación necesaria para ofrecer un seguimiento de rayos en tiempo real. El mismo modelo de servidor utilizado por diseñadores e ingenieros ahora también puede ser utilizado por los artistas para crear imágenes fotorrealistas que presenta un rebote ligero de las superficies como lo haría en la vida real. Esta GPU compatible con RTX produce un rendimiento de rastreo de rayos en tiempo real de hasta cinco rayos Giga por segundo. La NVIDIA T4, al combinarse con

el software Quadro Virtual Data Center Workstation (Quadro VDWS), permite a los artistas crear diseños fotorrealistas con sombras, reflejos y refracciones precisas en cualquier dispositivo desde cualquier ubicación.

Los núcleos tensores permiten ejecutar cargas de trabajo de inferencia de aprendizaje profundo. Cuando se ejecutan estas cargas de trabajo, una NVIDIA T4 con Quadro VDWS puede funcionar hasta 25 veces más rápido que un equipo virtual basado en un servidor solo de CPU. Un NetApp H615C con tres tarjetas NVIDIA T4 en una unidad de rack es una solución ideal para cargas de trabajo con un uso intensivo de gráficos y de computación.

La siguiente figura enumera las tarjetas GPU NVIDIA y compara sus características.

NVIDIA GPUs Recommended for Virtualization						
	V100S	RTX 8000	RTX 6000	T4	M10	P6
GPU	1 NVIDIA Volta	1 NVIDIA Turing	1 NVIDIA Turing	1 NVIDIA Turing	4 NVIDIA Maxwell	1 NVIDIA Pascal
CUDA Cores	5,120	4,608	4,608	2,560	2,560 (640 per GPU)	2,048
Tensor Cores	640	576	576	320	—	—
RT Cores	—	72	72	40	—	—
Guaranteed QoS (GPU Scheduler)	✓	✓	✓	✓	—	✓
Live Migration	✓	✓	✓	✓	✓	✓
Multi-vGPU	✓	✓	✓	✓	✓	✓
Memory Size	32/16 GB HBM2	48 GB GDDR6	24 GB GDDR6	16 GB GDDR6	32 GB GDDR5 (8 GB per GPU)	16 GB GDDR5
vGPU Profiles	1 GB, 2 GB, 4 GB, 8 GB, 16 GB, 32 GB	1 GB, 2 GB, 3 GB, 4 GB, 6 GB, 8 GB, 12 GB, 16 GB, 24 GB, 48 GB	1 GB, 2 GB, 3 GB, 4 GB, 6 GB, 8 GB, 12 GB, 24 GB	1 GB, 2 GB, 4 GB, 8 GB, 16 GB	0.5 GB, 1 GB, 2 GB, 4 GB, 8 GB	1 GB, 2 GB, 4 GB, 8 GB, 16 GB
Form Factor	PCIe 3.0 dual slot and SXM2	PCIe 3.0 dual slot	PCIe 3.0 dual slot	PCIe 3.0 single slot	PCIe 3.0 dual slot	MXM (blade servers)
Power	250 W /300 W (SXM2)	250 W	250 W	70 W	225 W	90 W
Thermal	passive	passive	passive	passive	passive	bare board
vGPU Software Support	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer
Use Case	Ultra-high-end rendering, simulation, 3D design with Quadro vDWS; ideal upgrade path for V100	High-end rendering, 3D design and creative workflows with Quadro vDWS	Mid-range to high-end rendering, 3D design and creative workflows with Quadro vDWS	Entry-level to high-end 3D design and engineering workflows with Quadro vDWS. High-density, low power GPU acceleration for knowledge workers with NVIDIA GRID software.	Knowledge workers using modern productivity apps and Windows 10 requiring best density and total cost of ownership (TCO), multimonitor support with NVIDIA GRID vPC/vApps	For customers requiring GPUs in a blade server form factor; ideal upgrade path for M6

La GPU M10 sigue siendo la mejor solución de TCO para casos de uso de trabajadores formados. Sin embargo, la T4 es una excelente alternativa cuando quiere estandarizar en una GPU que se puede utilizar en múltiples casos de uso, como estaciones de trabajo virtuales, rendimiento gráfico, renderizado interactivo en tiempo real e inferencia. Con T4, SE pueden beneficiar de los mismos recursos de GPU para ejecutar cargas de trabajo mixtas—por ejemplo, ejecutar VDI durante el día y reasignar los recursos para ejecutar cargas de trabajo informáticas nocturnas.

El nodo de computación H610C es dos unidades de rack, el tamaño de H615C es una unidad de rack y consume menos energía. H615C admite codificación H.264 y H.265 (codificación de vídeo de alta eficiencia [HEVC]) 4:4:4 y decodificación. También soporta el cada vez más integrado VP9 descodificador; incluso el paquete contenedor WebM que ofrece YouTube utiliza el códec VP9 para vídeo.

La cantidad de nodos de un clúster de computación está dictada por VMware; actualmente, es 96 con VMware vSphere 7.0 Update 1. Se admite la mezcla de diferentes modelos de nodos de computación en un clúster cuando se habilita la función Enhanced vMotion Compatibility (EVC).

### Gestión de licencias de NVIDIA

Cuando se utiliza H610C o H615C, la licencia de la GPU debe obtenerse de los partners de NVIDIA autorizados a revender las licencias. Puede encontrar partners de NVIDIA con el "[localizador de partners](#)". Busque competencias como GPU virtual (vGPU) o Tesla.

El software NVIDIA vGPU está disponible en cuatro ediciones:

- PC virtual DE GRID de NVIDIA (GRID VPC)
- Aplicaciones virtuales DE GRID de NVIDIA (VAPPS DE GRID)
- Estación de trabajo de centro de datos virtual Quadro (Quadro VDWS) NVIDIA
- Virtual ComputeServer de NVIDIA (vComputeServer)

### **PC virtual DE GRID**

Este producto es ideal para usuarios que desean un escritorio virtual que proporcione una gran experiencia de usuario para aplicaciones de Microsoft Windows, exploradores, vídeo de alta definición y soporte para varios monitores. El PC virtual GRID de NVIDIA ofrece una experiencia nativa en un entorno virtual, lo que le permite ejecutar todas las aplicaciones de su PC a pleno rendimiento.

### **Aplicaciones virtuales GRID**

LAS vApps DE GRID se utilizan para organizaciones que implementan un host de sesión de Escritorio remoto (RDSH) u otras soluciones basadas en sesiones o en streaming de aplicaciones. Diseñado para ofrecer aplicaciones de Microsoft Windows a todo rendimiento, los escritorios RDSH alojados en Windows Server también son compatibles con GRID vApps.

### **Estación de trabajo Quadro Virtual Data Center**

Esta edición es ideal para diseñadores generales y de gama alta que utilizan potentes herramientas de creación de contenido en 3D como Dassault CATIA, SOLIDWORKS, 3Dxsite, Siemens NX, PTC Creo, Schlumberger Petrel o Autodesk Maya. NVIDIA Quadro VDWS permite a los usuarios acceder a sus aplicaciones gráficas profesionales con todas las características y el rendimiento en cualquier lugar de cualquier dispositivo.

### **Virtual ComputeServer de NVIDIA**

Muchas organizaciones ejecutan cargas de trabajo de servidores con un uso intensivo de la computación, como la inteligencia artificial (IA), el aprendizaje profundo (DL) y la ciencia de los datos. Para estos casos de uso, el software NVIDIA vComputeServer virtualiza la GPU NVIDIA, lo que acelera las cargas de trabajo de servidores con un uso intensivo de recursos informáticos con características como el código de corrección de errores, la retirada de páginas, la paridad a punto en NVLink y multi-vGPU.



Una licencia Quadro VDWS permite utilizar GRID VPC y NVIDIA vComputeServer.

### **Puesta en marcha**

VDS de NetApp puede ponerse en marcha en Microsoft Azure mediante una aplicación de configuración disponible en función de la base de código necesaria. La versión actual está disponible ["aquí"](#) y el lanzamiento de vista previa del próximo producto está disponible ["aquí"](#).

Consulte ["este vídeo"](#) para obtener instrucciones de puesta en funcionamiento.



# NetApp Virtual Desktop Service

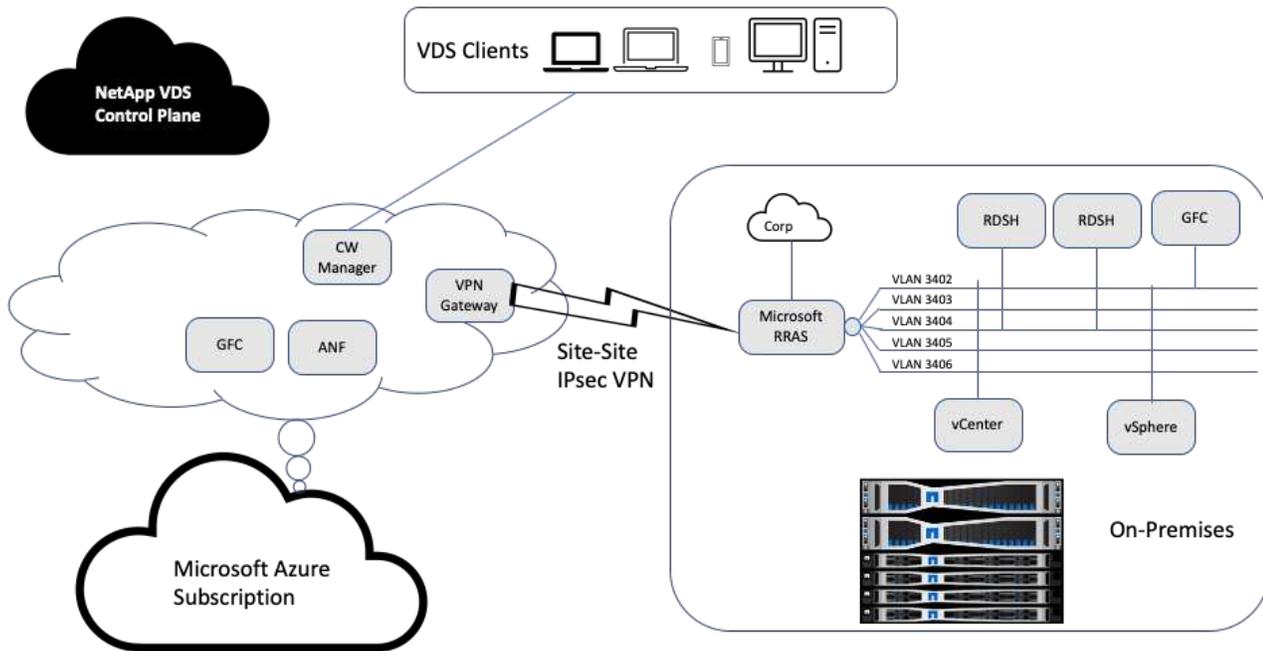
## Deployment & AD Connect

Toby vanRoojen  
Product Marketing Manager  
June, 2020

### Entorno de cloud híbrido

El servicio de puestos de trabajo virtuales de NetApp se puede ampliar a las instalaciones cuando existe conectividad entre los recursos en las instalaciones y los recursos cloud. Las empresas pueden establecer el vínculo a Microsoft Azure mediante Express Route o una conexión VPN IPsec de sitio a sitio. También puede crear vínculos a otras nubes de forma similar mediante un enlace dedicado o con un túnel VPN IPsec.

Para la validación de soluciones, utilizamos el entorno descrito en la siguiente figura.



En las instalaciones, teníamos varias VLAN para gestión, hosts de sesiones de puesto de trabajo remoto, etc. Se encontraban en la subred 172.21.146-150.0/24 y se enrutaron a la red corporativa mediante el Servicio de acceso de enrutamiento remoto de Microsoft. También realizamos las siguientes tareas:

1. Notamos la IP pública del servidor de enrutamiento y acceso remoto de Microsoft (RRAS; identificado con IPchicken.com).
2. Creamos un recurso de Virtual Network Gateway (VPN basado en rutas) en la suscripción a Azure.
3. Creamos la conexión que proporciona la dirección de pasarela de red local para la IP pública del servidor RRAS de Microsoft.
4. Hemos completado la configuración de VPN en RRAS para crear una interfaz virtual mediante la autenticación precompartida que se proporcionó al crear la puerta de enlace VPN. Si se configura correctamente, la VPN debe estar en el estado conectado. En lugar de RRAS de Microsoft, también puede utilizar pfSense u otras herramientas relevantes para crear el túnel VPN IPsec de sitio a sitio. Dado que se basa en rutas, el túnel redirige el tráfico en función de las subredes específicas configuradas.

Microsoft Azure Active Directory proporciona autenticación de identidad basada en OAuth. Las autenticaciones de cliente empresarial normalmente requieren autenticación basada en NTLM o Kerberos. Microsoft Azure Active Directory Domain Services realiza una sincronización hash de contraseña entre Azure Active Directory y los controladores de dominio en las instalaciones mediante ADConnect.

Para esta validación de la solución VDS híbrida, inicialmente implementamos Microsoft Azure y añadimos un sitio adicional con vSphere. La ventaja de este método es que los servicios de plataforma se pusieron en marcha en Microsoft Azure y se incluyeron después en un backup fácilmente mediante el portal. A continuación, se puede acceder fácilmente a los servicios desde cualquier lugar, incluso si el enlace VPN del sitio no está disponible.

Para agregar otro sitio, utilizamos una herramienta llamada DCCConfig. El acceso directo a esa aplicación está disponible en el escritorio del equipo virtual del administrador de espacio de trabajo en la nube (CWMgr). Una vez que se haya iniciado esta aplicación, desplácese a la ficha Sitios de centro de datos, agregue el nuevo

sitio del centro de datos y rellene la información necesaria como se muestra a continuación. La URL apunta a la IP de vCenter. Asegúrese de que el equipo virtual de CWMgr pueda comunicarse con vCenter antes de agregar la configuración.



Asegúrese de que está instalado vSphere PowerCLI 5.1 en CloudWorkspace Manager para habilitar la comunicación con el entorno de VMware vSphere.

La siguiente figura muestra la configuración del sitio del centro de datos local.

The screenshot shows the 'Configuration' window with several tabs: DataCenter, Accounts, Email, DatabaseConnection, Exclude, DataCenter Sites, Product Keys, Static IpAddress, and Drive Mapping. The 'DataCenter Sites' tab is active, displaying a table with two sites:

DataCenter Site	Type	Is Primary	DataCenter Site Detail
Site 1	AzureRM	<input checked="" type="checkbox"/>	
Site 2	vSphere	<input type="checkbox"/>	

Below the table, there is a red text instruction: "To delete DataCenter Site(s), Select it and right click to delete".

The right side of the window shows the configuration details for 'Site 2':

- DataCenter Site:** Site 2
- Hypervisor:** vSphere
- General Settings:**
  - Local VM Account:** Username: Administrator, Password: [masked]
  - Hypervisor Account:** Username: Administrator@vsphere, Password: [masked]
  - URL:** https://172.21.146.150/sdk/
  - VM Name Prefix:** [empty]
  - Max Concurrent Create Server:** 20
  - Subnet Mask:** 255.255.255.0
  - Default Gateway:** 172.21.148.250
  - Is Primary Hypervisor?:**  Yes  No
  - Must Set IpAddress Of VM:**  Yes  No
- DNS:**
  - Primary DNS:** 10.67.78.11
  - Secondary DNS:** [empty]
  - Set DNS Address:**  Yes  No
- vSphere:**
  - Data Center:** NetApp-HCI-Datacenter
  - Cluster:** [empty]
  - Resource Pool:** [empty]
  - Host Name:** [empty]
  - VM Folder:** VDS
  - Max VMs In Datastore:** -1
  - Min HD Free Space In Datastore GB:** -1
  - Min Ram Free GB:** -1

At the bottom, there are two checkboxes: 'Exclude vSphere DataStore' and 'Exclude vSphere ResourcePools', both of which are currently unchecked.

Tenga en cuenta que existen opciones de filtrado disponibles para los recursos de computación en función del clúster específico, el nombre de host o el espacio de RAM libre. Las opciones de filtrado para recursos de almacenamiento incluyen el espacio libre mínimo en los almacenes de datos o la cantidad máxima de máquinas virtuales por almacén de datos. Los almacenes de datos se pueden excluir con expresiones regulares. Haga clic en el botón Guardar para guardar la configuración.

Para validar la configuración, haga clic en el botón Test, o bien haga clic en Load Hypervisor y compruebe cualquier lista desplegable en la sección vSphere. Debe rellenarse con los valores adecuados. Se recomienda mantener el hipervisor principal establecido en yes para el sitio de aprovisionamiento predeterminado.

Las plantillas de máquinas virtuales creadas en VMware vSphere se consumen como colecciones de aprovisionamiento en VDS. Las colecciones para aprovisionamiento se presentan de dos formas: Compartidas

e infraestructuras de puestos de trabajo virtuales. El tipo de colección de aprovisionamiento compartido se utiliza para los servicios de escritorio remoto para los que se aplica una única política de recursos a todos los servidores. El tipo de VDI se utiliza para las instancias de WVD para las que se asigna la política de recursos de forma individual. Los servidores de una colección de aprovisionamiento pueden asignarse una de las siguientes tres funciones:

- **TSDATA.** combinación de Servicios de Terminal Server y función de servidor de datos.
- **Servicios de terminal TS.** (Host de sesión).
- **DATA.** servidor de archivos o servidor de bases de datos. Al definir el rol de servidor, debe seleccionar la plantilla y el almacenamiento (almacén de datos) de la máquina virtual. El almacén de datos elegido puede restringirse a un almacén de datos específico o puede usar la opción menos utilizada en la que se elige el almacén de datos en función del uso de los datos.

Cada implementación tiene valores predeterminados de recursos de equipo virtual para la asignación de recursos de cloud en función de usuarios activos, fijos, carga de servidor o recuento de usuarios.

#### Prueba de carga de servidor único con Login VSI

Virtual Desktop Service de NetApp utiliza el protocolo de Microsoft Remote Desktop para acceder a aplicaciones y sesiones de puestos de trabajo virtuales, y la herramienta Login VSI determina el número máximo de usuarios que pueden alojarse en un modelo de servidor específico. Login VSI simula el inicio de sesión de usuario a intervalos específicos y realiza operaciones de usuario como abrir documentos, leer y redactar correos electrónicos, trabajar con Excel y PowerPoint, imprimir documentos, comprimir archivos y efectuar pausas aleatorias. Luego mide los tiempos de respuesta. El tiempo de respuesta del usuario es bajo cuando el uso del servidor es bajo y aumenta cuando se añaden más sesiones de usuario. Login VSI determina la línea de base en función de las sesiones iniciales de inicio de sesión de usuario e informa de la sesión de usuario máxima cuando la respuesta del usuario supera los 2 segundos de la línea de base.

El servicio de puestos de trabajo virtuales de NetApp utiliza el protocolo de Microsoft Remote Desktop para acceder a las aplicaciones y sesiones de puestos de trabajo virtuales. Para determinar el número máximo de usuarios que se pueden alojar en un modelo de servidor específico, utilizamos la herramienta Login VSI. Login VSI simula el inicio de sesión de usuario a intervalos específicos y realiza operaciones de usuario como abrir documentos, leer y redactar correos electrónicos, trabajar con Excel y PowerPoint, imprimir documentos, comprimir archivos, tomar pausas aleatorias, etc. También mide los tiempos de respuesta. El tiempo de respuesta del usuario es bajo cuando el uso del servidor es bajo y aumenta cuando se añaden más sesiones de usuario. Login VSI determina la línea de base en función de las sesiones iniciales de inicio de sesión de usuario e informa de la cantidad máxima de sesiones de usuario cuando la respuesta del usuario supera los 2 segundos de la línea de base.

La siguiente tabla contiene el hardware utilizado para esta validación.

Modelo	Cuente	Descripción
NetApp HCI H610C	4	Tres de un clúster para lanzadores, AD, DHCP, etc. Un servidor para la prueba de carga.
NetApp HCI H615C	1	2 x Intel Xeon Gold 24C 6282 a 2,1 GHz. 1,5 TB DE RAM.

La siguiente tabla contiene el software utilizado para esta validación.

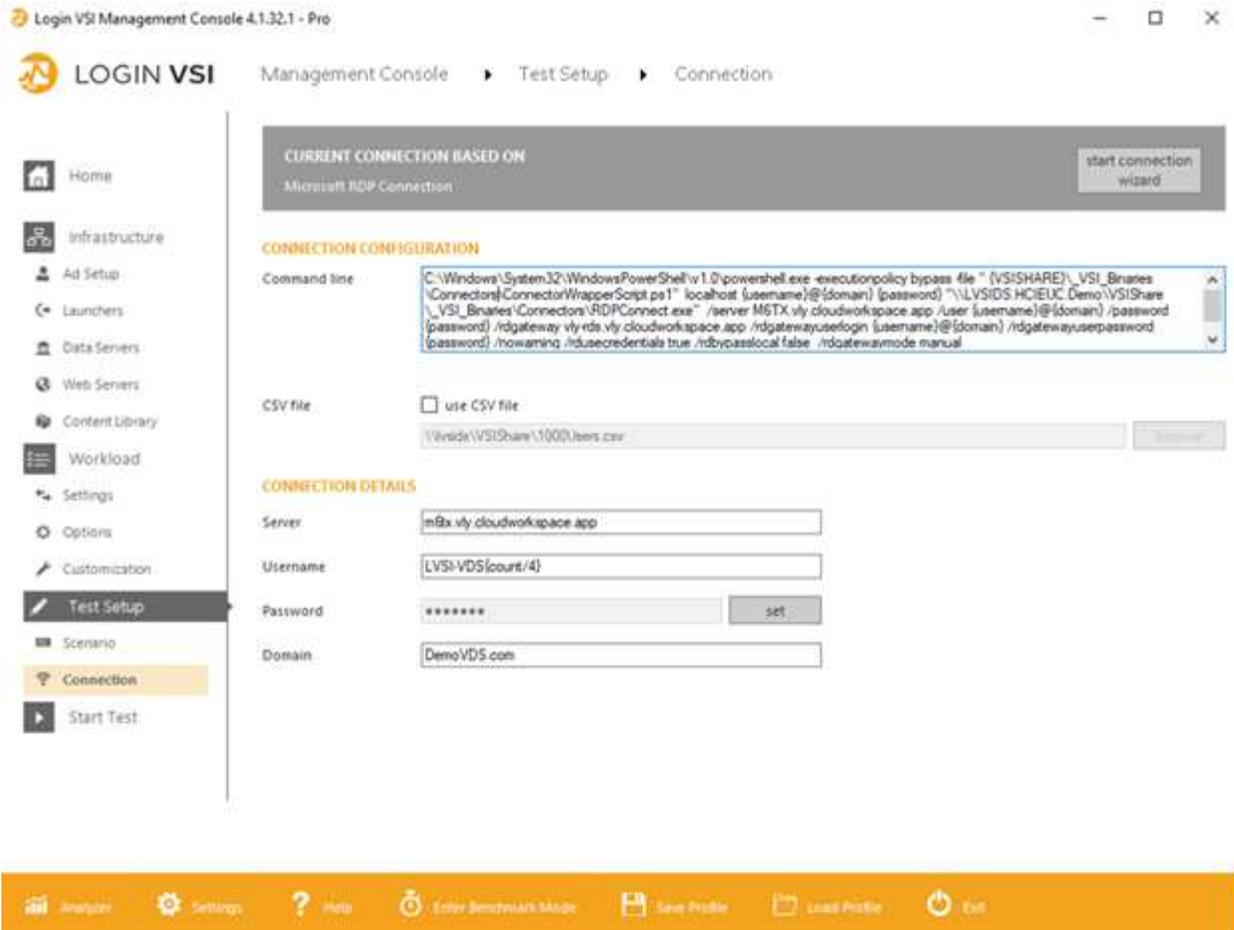
<b>Producto</b>	<b>Descripción</b>
VDS 5.4 de NetApp	Coordinación
Ventanas de plantilla de equipo virtual 2019 1809	Sistema operativo del servidor PARA RDSH
Login VSI	4.1.32.1
VMware vSphere 6.7 Update 3	Hipervisor
VMware vCenter 6.7 Update 3f	Herramienta de gestión de VMware

Los resultados de la prueba Login VSI son los siguientes:

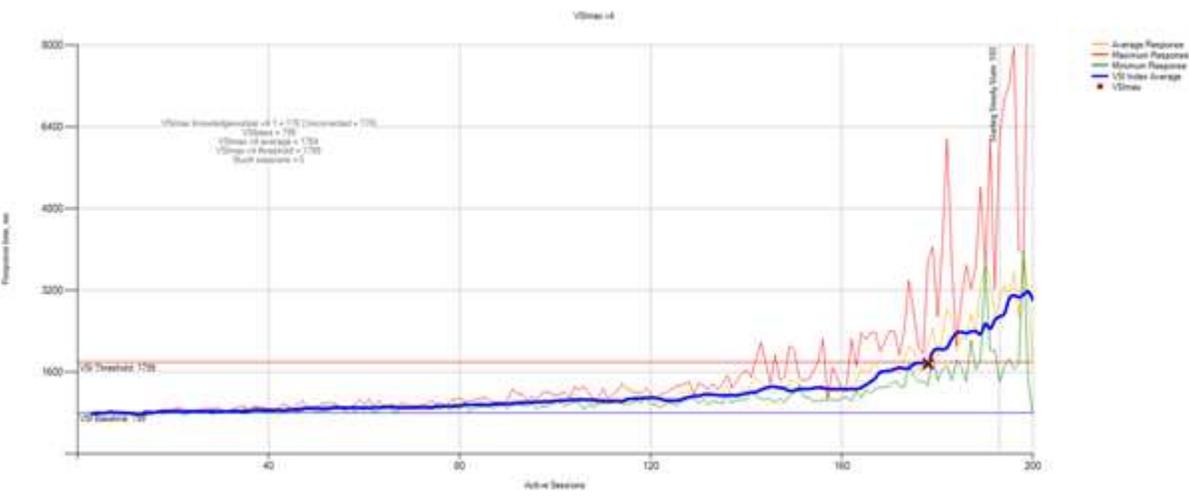
<b>Modelo</b>	<b>Configuración de las máquinas virtuales</b>	<b>Línea de base de inicio de sesión VSI</b>	<b>Inicio de sesión VSI Max</b>
H610C	8 vCPU, 48 GB de RAM, disco de 75 GB, perfil de vGPU 8Q	799	178
H615C	12 vCPU, 128 GB de RAM, 75 GB de disco	763	272

Teniendo en cuenta los límites e hiperprocesos de NUMA, los ocho equipos virtuales elegidos para la prueba y la configuración de equipos virtuales dependen de los núcleos disponibles en el host.

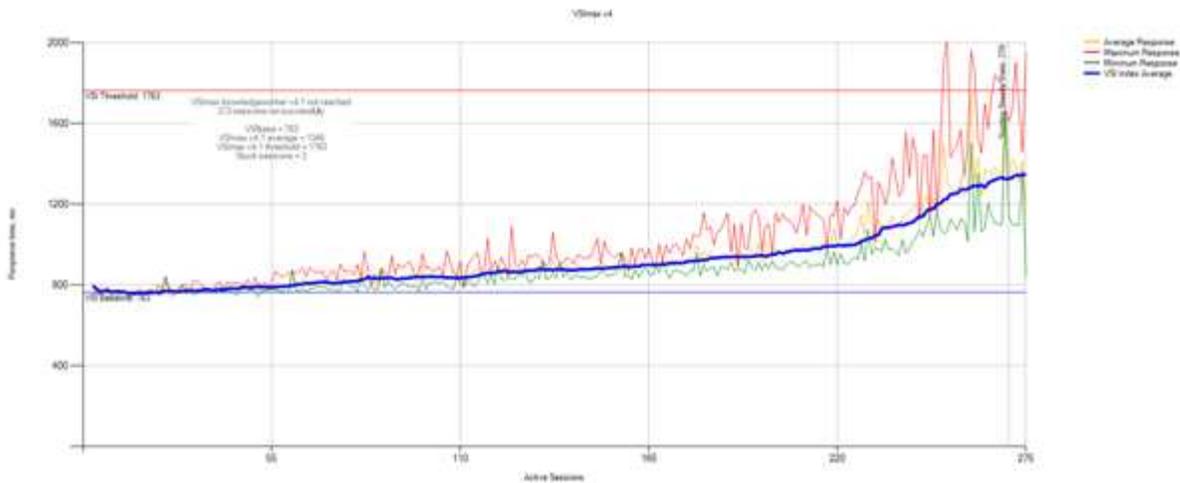
Utilizamos 10 equipos virtuales de inicio en H610C, la cual utilizó el protocolo RDP para conectarse a la sesión de usuario. En la siguiente figura se muestra la información de conexión de Login VSI.



En la siguiente figura, se muestra el tiempo de respuesta de Login VSI frente a las sesiones activas para H610C.



En la siguiente figura, se muestra el tiempo de respuesta de Login VSI con las sesiones activas para H615C.



En la siguiente figura, se muestran las métricas de rendimiento de Cloud Insights durante la prueba de H615C Login VSI al host de vSphere y las máquinas virtuales.



## Portal de gestión

El portal VDS Cloud Workspace Management Suite de NetApp está disponible ["aquí"](#) y la próxima versión está disponible ["aquí"](#).

El portal permite la administración centralizada de varias implementaciones de VDS, incluida una que tiene sitios definidos para los usuarios locales, administrativos, el catálogo de aplicaciones y eventos con secuencias de comandos. El portal también lo utilizan los usuarios administrativos para el aprovisionamiento manual de aplicaciones si es necesario y para conectarse a cualquier equipo para la solución de problemas.

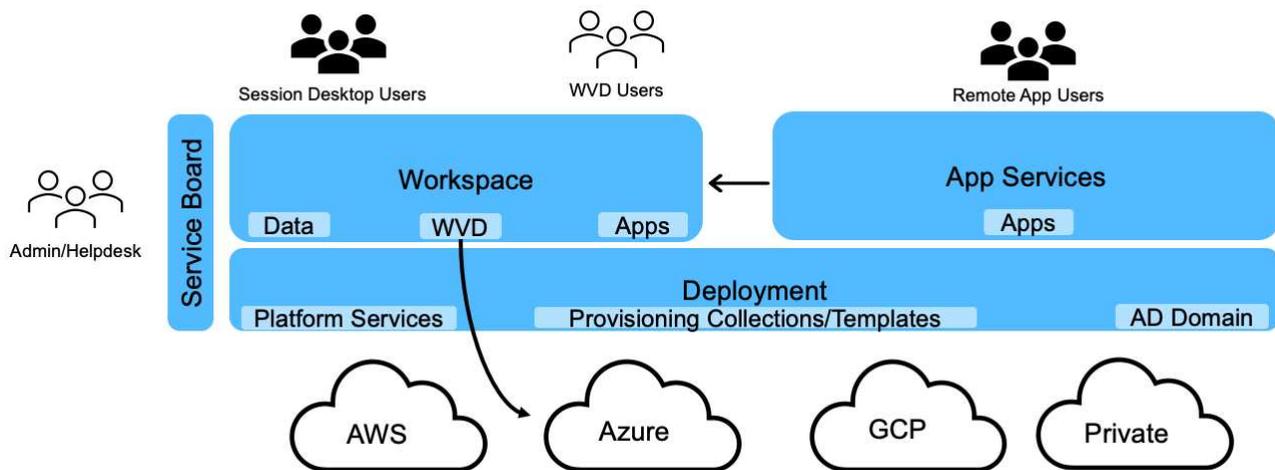
Los proveedores de servicios pueden utilizar este portal para agregar sus propios socios de canal y permitirles gestionar sus propios clientes.

## Gestión de usuarios

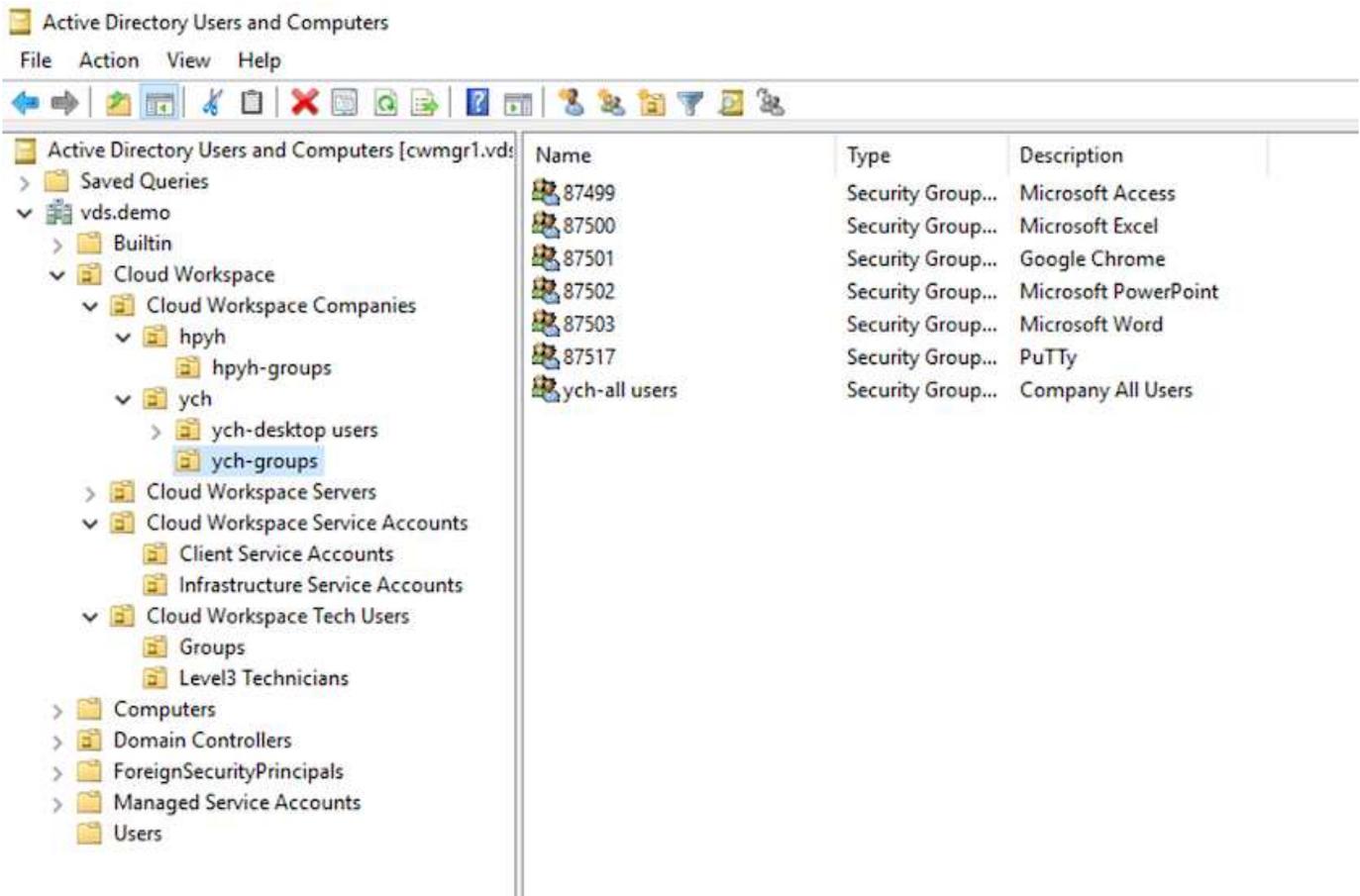
VDS de NetApp utiliza Azure Active Directory para la autenticación de identidades y Azure Active Directory Domain Services para la autenticación NTLM/Kerberos. La herramienta ADConnect se puede utilizar para sincronizar un dominio de Active Directory en las instalaciones con Azure Active Directory.

Es posible añadir nuevos usuarios desde el portal o habilitar espacios de trabajo cloud para los usuarios existentes. Los permisos para los espacios de trabajo y los servicios de aplicaciones pueden ser controlados por usuarios individuales o por grupos. Desde el portal de gestión, los usuarios administrativos pueden definirse para controlar los permisos del portal, los espacios de trabajo, etc.

La siguiente figura muestra la gestión de usuarios en VDS de NetApp.



Cada espacio de trabajo reside en su propia unidad organizativa (OU) de Active Directory bajo la unidad organizativa de Cloud Workspace como se muestra en la siguiente figura.



Para obtener más información, consulte ["este vídeo"](#) Sobre los permisos de usuario y la gestión de usuarios en NetApp VDS.

Cuando un grupo de Active Directory se define como un grupo CRAUserGroup mediante una llamada API para el centro de datos, todos los usuarios de ese grupo se importan en CloudWorkspace para la administración mediante la interfaz de usuario. Cuando el espacio de trabajo en la nube está habilitado para el usuario, VDS crea carpetas de inicio de usuario, permisos de configuración, actualizaciones de propiedades de usuario, etc.

Si se activa el usuario de VDI activado, VDS crea un equipo RDS de una sola sesión dedicado a ese usuario. Solicita la plantilla y el almacén de datos que se deben aprovisionar.

The screenshot shows a 'Security Settings' window with the following configuration:

- VDI User Enabled
- Mobile Drive Enabled
- Hypervisor Template: Windows20192899ver1
- Storage Type: DS02
- Account Expiration Enabled
- Local Drive Access Enabled
- Force Password Reset at Next Login
- Wake On Demand Enabled
- Multi-factor Auth Enabled

An 'Update' button is located at the bottom left of the settings panel.

### Gestión de espacios de trabajo

Un espacio de trabajo consta de un entorno de puestos de trabajo; se pueden compartir sesiones de puestos de trabajo remotos alojadas en las instalaciones o en cualquier entorno cloud compatible. Con Microsoft Azure, el entorno de puestos de trabajo puede ser persistente con puestos de trabajo virtuales de Windows. Cada área de trabajo está asociada a una organización o cliente específico. Las opciones disponibles al crear un espacio de trabajo nuevo se pueden ver en la siguiente figura.

## New Workspace

Client & Settings
Choose Applications
Add Users
Review & Provision

Select a Client [Add](#)

No Clients Added.

### Workspace Settings

Company Name

Primary Notification Email

### Application Settings

Enable Remote App

Enable App Locker

Enable Application Usage Tracking

### Device Settings

Disable Printing Access

Enable Workspace User Data Storage

### Security Settings

Require Complex User Password

Enable MFA for All Users

Permit Access To Task Manager

Cancel
Continue



Cada área de trabajo está asociada con una implementación específica.

Los espacios de trabajo contienen aplicaciones y servicios de aplicaciones asociados, carpetas de datos compartidos, servidores y una instancia de WVD. Cada espacio de trabajo puede controlar las opciones de seguridad, como la aplicación de la complejidad de las contraseñas, la autenticación multifactorial, las auditorías de archivos, etc.

Los espacios de trabajo pueden controlar la programación de la carga de trabajo para encender servidores adicionales, limitar el número de usuarios por servidor o establecer la programación de los recursos disponibles para un determinado período (siempre activos/apagados). Los recursos también se pueden configurar para activarse a petición.

Si es necesario, el espacio de trabajo puede anular los valores predeterminados de los recursos del equipo virtual de implementación. Para WVD, los pools de hosts WVD (que contienen hosts de sesiones y grupos de aplicaciones) y los espacios de trabajo WVD también se pueden gestionar desde el portal del paquete de gestión de espacios de trabajo en la nube. Para obtener más información sobre el grupo de hosts de WVD, consulte este ["vídeo"](#).

### Gestión de aplicaciones

Los trabajadores de tareas pueden iniciar rápidamente una aplicación desde la lista de aplicaciones que se les han puesto a su disposición. Los servicios de aplicaciones publican aplicaciones desde los hosts de sesión de Remote Desktop Services. Con WVD, los grupos de aplicaciones proporcionan una funcionalidad similar a la de los

grupos de host de Windows 10 con varias sesiones.

Para que los trabajadores de la oficina puedan suministrar las aplicaciones que necesiten mediante una placa de servicio manualmente, o bien se pueden aprovisionar automáticamente con la función de eventos programados de VDS de NetApp.

Para obtener más información, consulte ["Página de autorización de aplicaciones de NetApp"](#).

#### Funciones de ONTAP para el servicio de escritorios virtuales

Las siguientes funciones de ONTAP hacen que resulte atractiva la elección para su uso con un servicio de escritorios virtuales.

- **Sistema de archivos de escalado horizontal.** los volúmenes ONTAP FlexGroup pueden crecer hasta más de 20 PB de tamaño y pueden contener más de 400 mil millones de archivos dentro de un solo espacio de nombres. El clúster puede contener hasta 24 nodos de almacenamiento, cada uno con un número flexible de tarjetas de interfaz de red en función del modelo utilizado.

Los escritorios virtuales del usuario, las carpetas principales, los contenedores de perfiles de usuario, los datos compartidos, etc. pueden crecer en función de la demanda sin preocuparse por las limitaciones del sistema de archivos.

- **Análisis del sistema de archivos.** puede utilizar la herramienta XCP para obtener información detallada sobre los datos compartidos. Con ONTAP 9.8 o ActiveIQ Unified Manager, puede consultar y recuperar fácilmente la información de metadatos de archivos e identificar los datos inactivos.
- **Organización en niveles en el cloud.** puede realizar la migración de datos inactivos a un almacén de objetos en la nube o a cualquier almacenamiento compatible con S3 del centro de datos.
- **Versiones de archivo.** los usuarios pueden recuperar archivos protegidos por copias Snapshot de ONTAP de NetApp. Las copias Snapshot de ONTAP ocupan muy poco espacio, ya que solo registran los bloques cambiados.
- **Espacio de nombre global.** la tecnología ONTAP FlexCache permite almacenar en caché de forma remota el almacenamiento de archivos, lo que facilita la administración de datos compartidos entre ubicaciones que contienen sistemas de almacenamiento ONTAP.
- **Soporte multi-tenancy seguro.** Un único clúster de almacenamiento físico puede presentarse como múltiples matrices de almacenamiento virtual cada una con sus propios volúmenes, protocolos de almacenamiento, interfaces de red lógicas, dominio de identidad y autenticación, usuarios de administración, etc. Por lo tanto, es posible compartir la cabina de almacenamiento en varias unidades de negocio o entornos, como pruebas, desarrollo y producción.

Para garantizar el rendimiento, puede utilizar la calidad de servicio adaptativa para establecer niveles de rendimiento que se basan en el espacio utilizado o asignado y puede controlar la capacidad de almacenamiento mediante cuotas.

- **Integración de VMware.** Herramientas de ONTAP para VMware vSphere proporciona un complemento de vCenter para aprovisionar almacenes de datos, implementar prácticas recomendadas de host de vSphere y supervisar recursos de ONTAP.

ONTAP admite API de vStorage para la integración de cabinas (VAAI) para descargar las operaciones SCSI/archivo en la cabina de almacenamiento. ONTAP también admite API de vStorage para compatibilidad con Storage Awareness (VASA) y Virtual Volumes para protocolos de bloques y archivos.

El plugin de SnapCenter para VMware vSphere ofrece un método sencillo de realizar backups y restaurar máquinas virtuales con la función Snapshot en una cabina de almacenamiento.

ActiveIQ Unified Manager proporciona visibilidad completa de la red de almacenamiento en un entorno de vSphere. Los administradores pueden identificar fácilmente cualquier problema de latencia que pueda producirse en entornos de puestos de trabajo virtuales alojados en ONTAP.

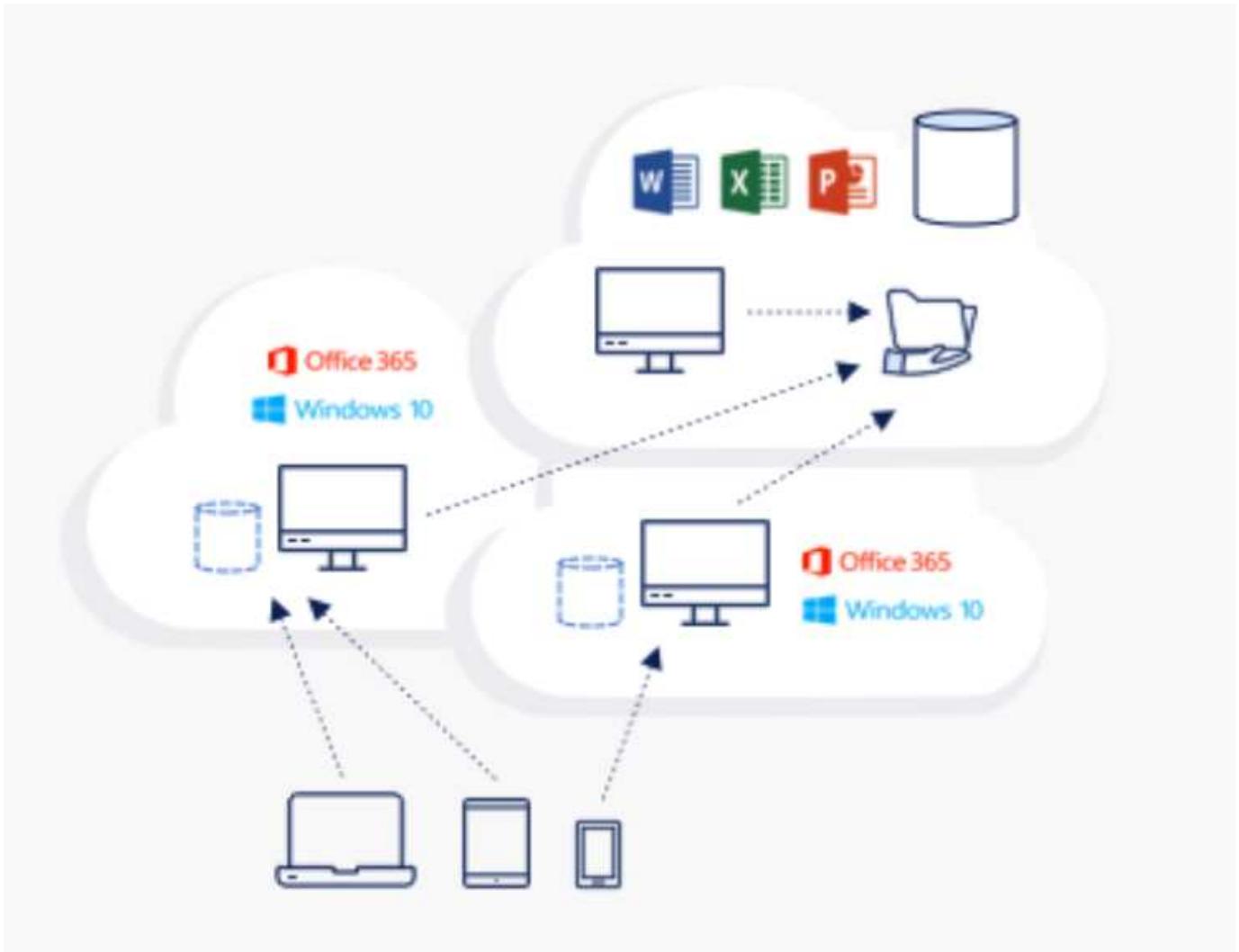
- **Conformidad de seguridad.** con ActiveIQ Unified Manager, puede supervisar múltiples sistemas ONTAP con alertas por cualquier infracción de directivas.
- **Compatibilidad multiprotocolo.** ONTAP admite bloques (iSCSI, FC, FCoE y NVMe/FC), archivos (NFSv3, NFSv4.1, SMB2.x y SMB3.x) y protocolos de almacenamiento de objetos (S3).
- **Compatibilidad con automatización.** ONTAP proporciona módulos API REST, Ansible y PowerShell para automatizar tareas con el portal de administración VDS.

### Gestión de datos

Como parte de la implementación, puede elegir el método de servicios de archivos para alojar el perfil de usuario, los datos compartidos y la carpeta de la unidad principal. Las opciones disponibles son File Server, Azure Files o Azure NetApp Files. Sin embargo, después de la implementación, puede modificar esta opción con la herramienta Command Center para que apunte a cualquier recurso compartido de SMB. ["El alojamiento tiene varias ventajas con ONTAP de NetApp"](#). Para saber cómo cambiar el recurso compartido de SMB, consulte ["Cambiar la capa de datos"](#).

### Caché de archivos global

Cuando los usuarios se distribuyen entre varios sitios dentro de un espacio de nombre global, la caché de archivos global puede ayudar a reducir la latencia de los datos a los que se accede con frecuencia. La implementación de caché global de archivos se puede automatizar mediante una recopilación de datos y eventos programados. La caché de archivos global gestiona las cachés de lectura y escritura localmente y mantiene los bloqueos de archivos entre ubicaciones. La caché de archivos global puede funcionar con cualquier servidor de archivos SMB, incluido Azure NetApp Files.



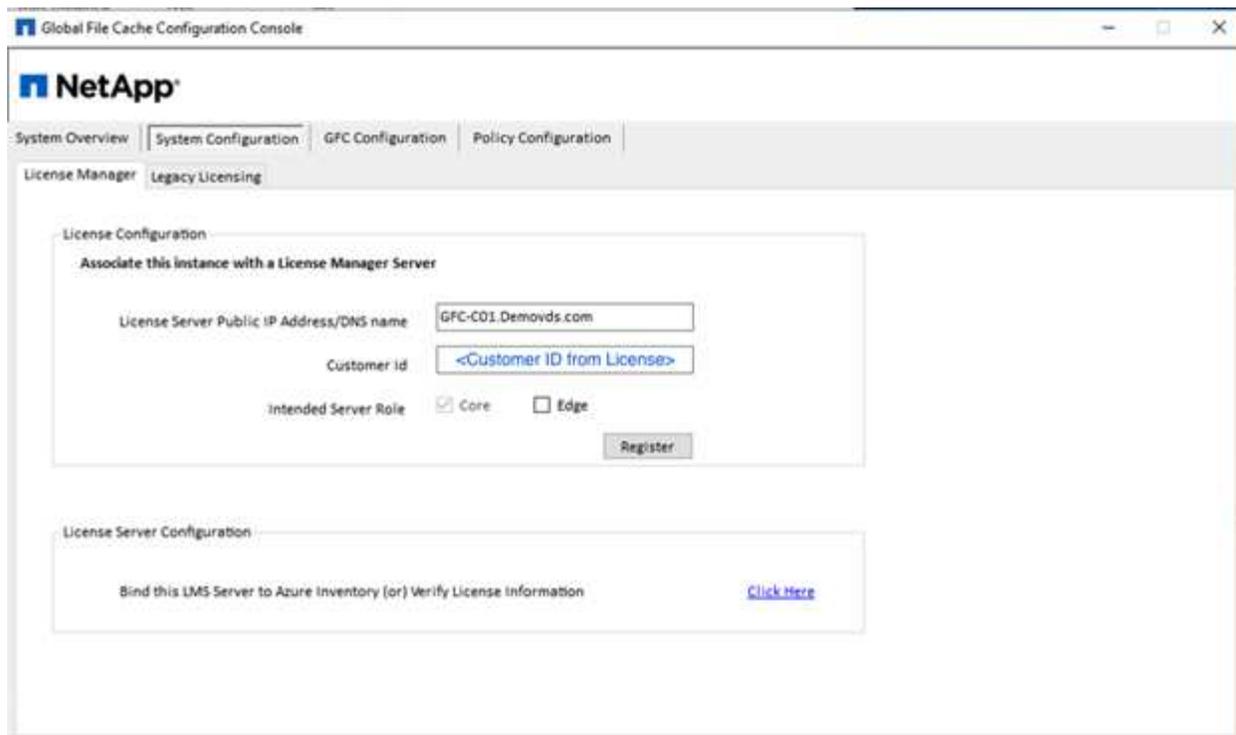
La caché global de archivos requiere lo siguiente:

- Servidor de gestión (servidor de gestión de licencias)
- Núcleo
- Extremo con suficiente capacidad de disco para almacenar en caché los datos

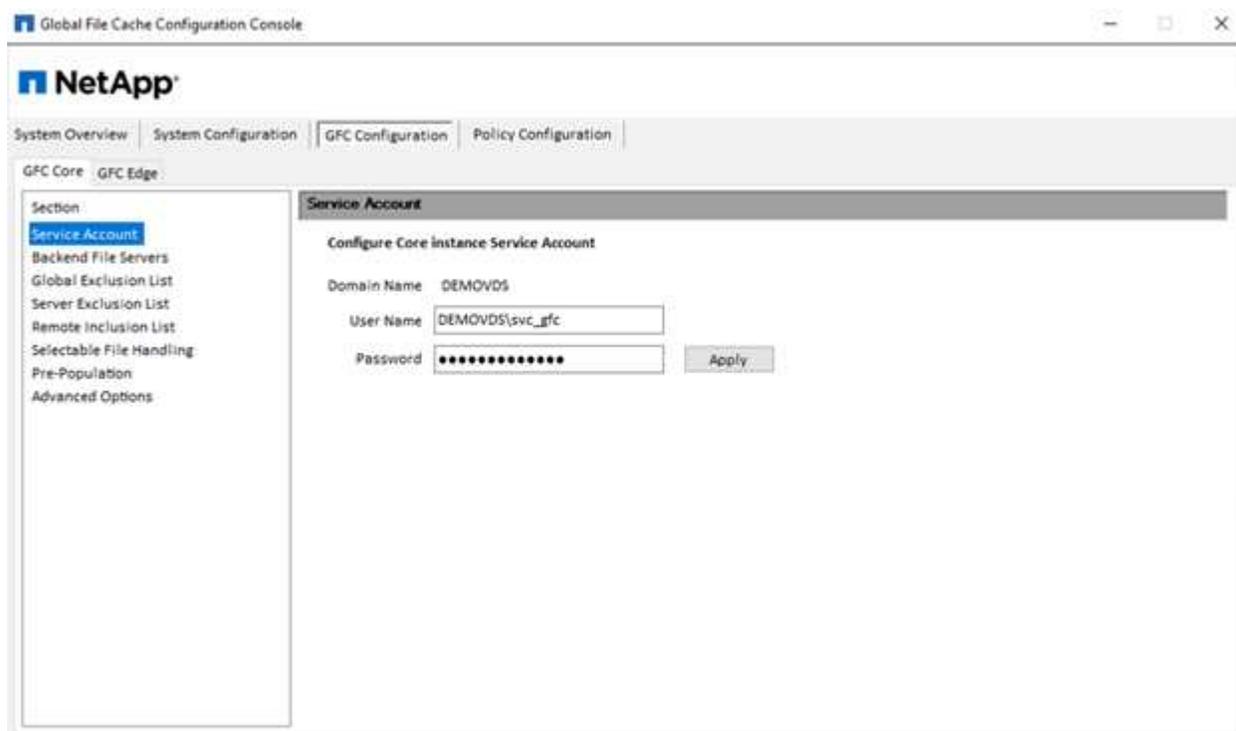
Para descargar el software y calcular la capacidad de la caché en disco de Edge, consulte "[Documentación GFC](#)".

Para nuestra validación, implementamos los recursos principales y de gestión en la misma máquina virtual en Azure y recursos periféricos en NetApp HCI. Tenga en cuenta que el núcleo es donde se requiere acceso a datos de gran volumen y el perímetro es un subconjunto del núcleo. Después de instalar el software, debe activar la licencia antes de utilizarla. Para ello, lleve a cabo los siguientes pasos:

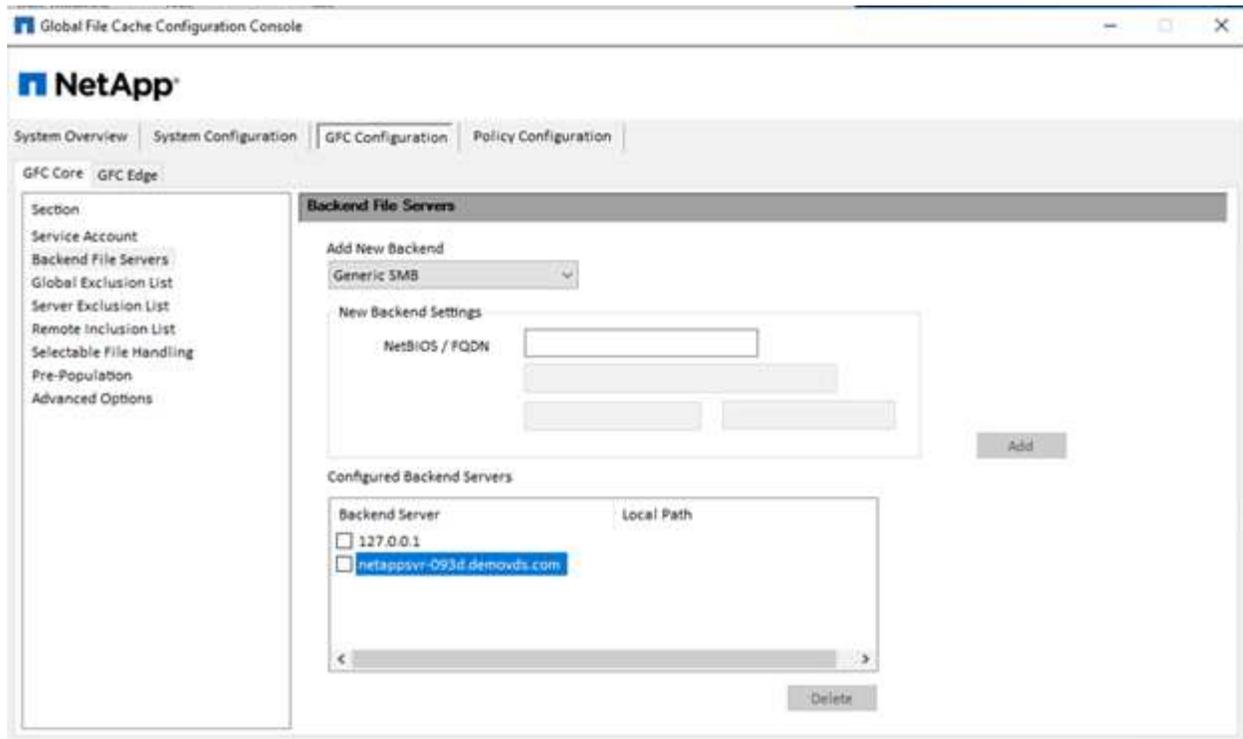
1. En la sección Configuración de licencia, utilice el enlace [haga clic aquí](#) para completar la activación de la licencia. A continuación, registre el núcleo.



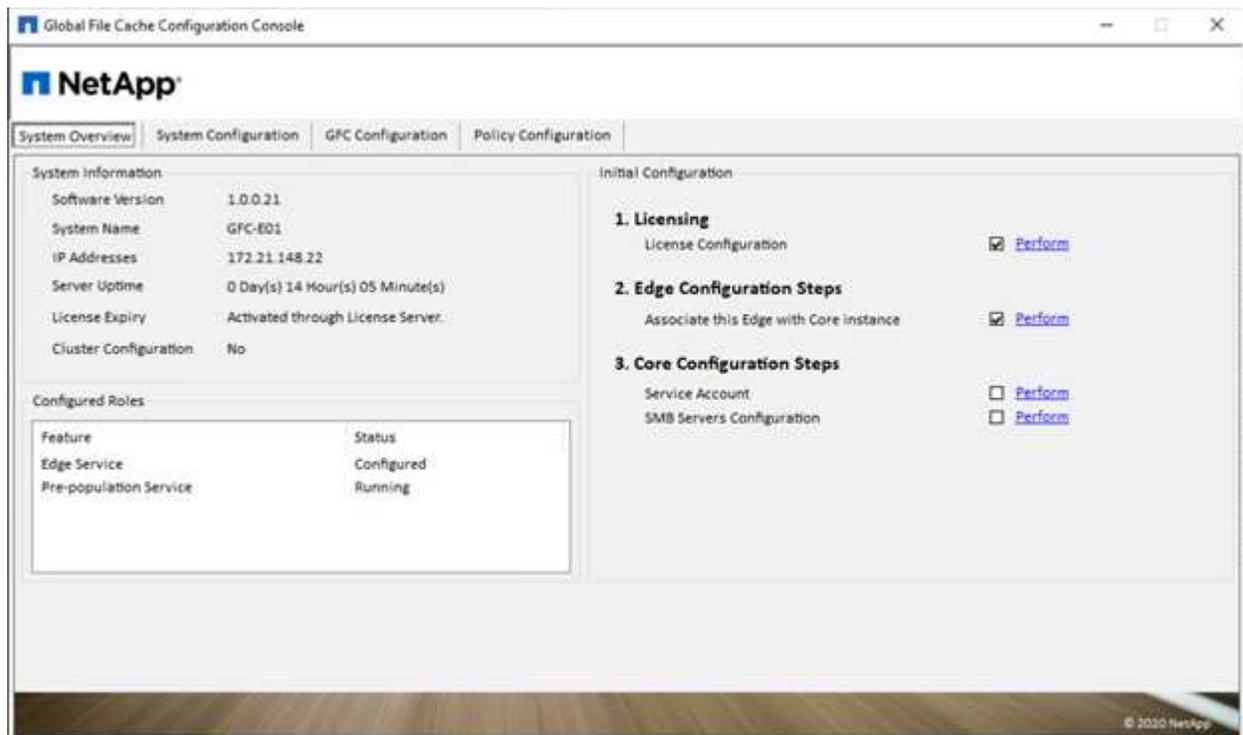
2. Proporcione la cuenta de servicio que se utilizará para la caché de archivos global. Para conocer los permisos necesarios para esta cuenta, consulte "[Documentación GFC](#)".



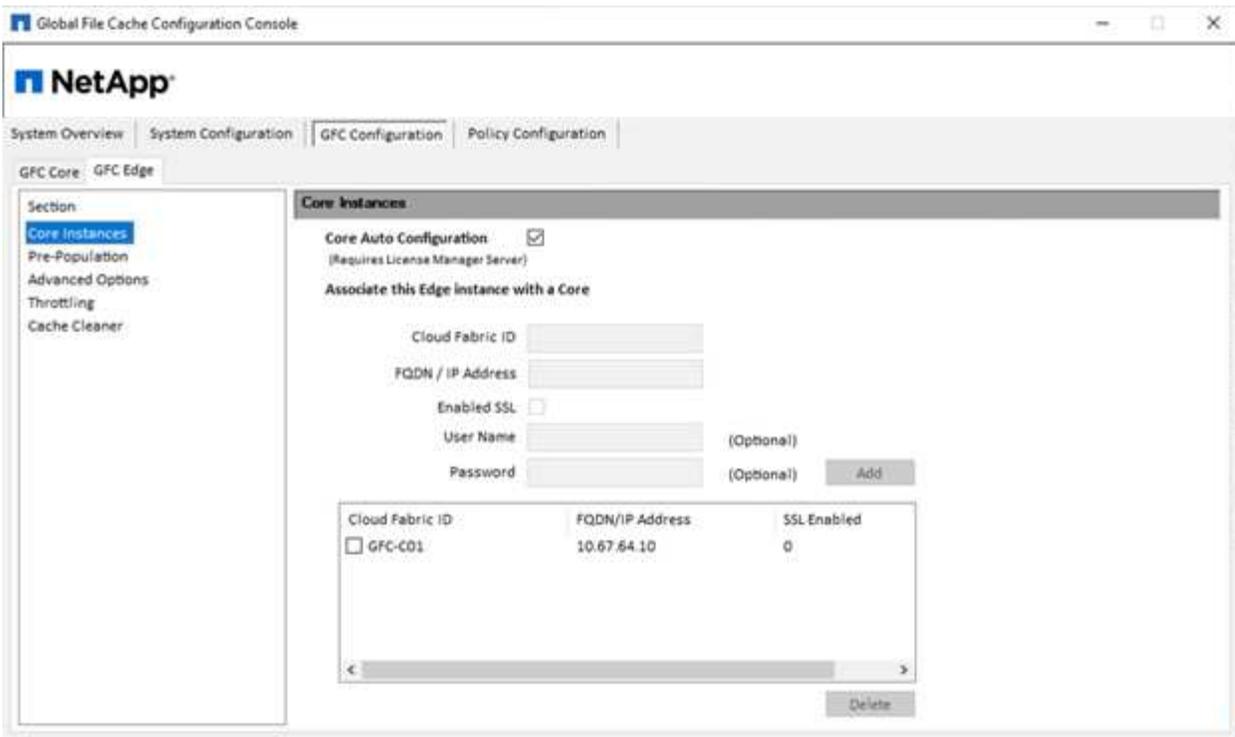
3. Agregue un nuevo servidor de archivos back-end y proporcione el nombre o la IP del servidor de archivos.



4. En el borde, la unidad de caché debe tener la letra de unidad D. Si no lo hace, utilice diskpart.exe para seleccionar el volumen y cambiar la letra de la unidad. Regístrese en el servidor de licencias como EDGE.

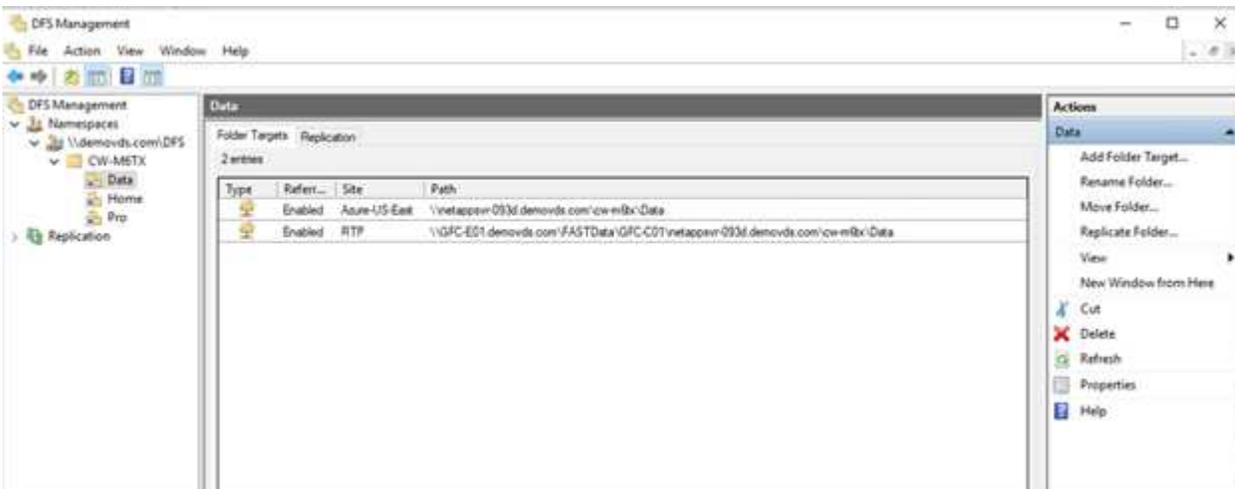


Si la configuración automática de núcleo está habilitada, la información principal se recupera automáticamente del servidor de administración de licencias.

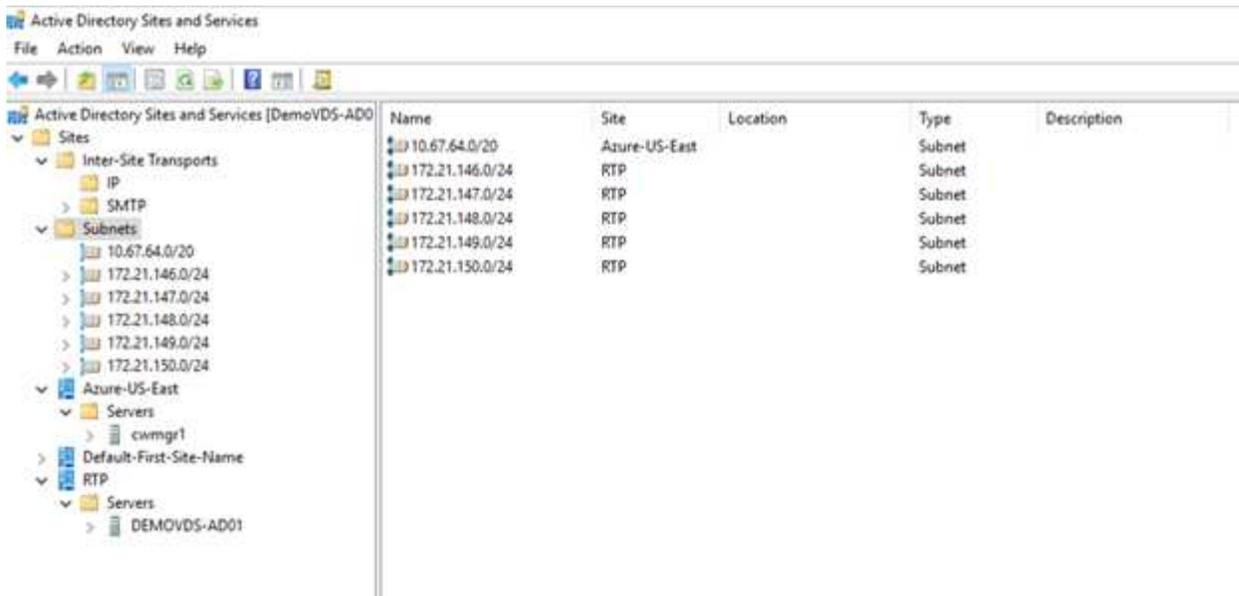


Desde cualquier equipo cliente, los administradores que solían acceder al recurso compartido en el servidor de archivos pueden acceder a él con GFC Edge mediante UNC Path `\\<edge server name>\FASTDATA\<core server name>\<backend file server name>\<share name>`. Los administradores pueden incluir esta ruta de acceso en el script de inicio de sesión de usuario o GPO para la asignación de unidades de usuarios en la ubicación perimetral.

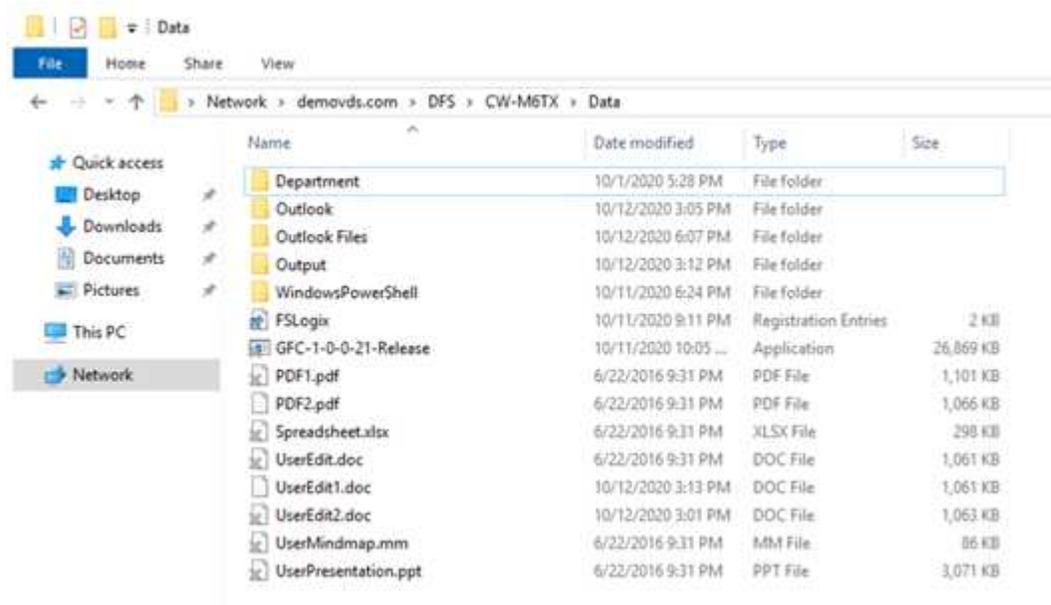
Para proporcionar acceso transparente a los usuarios de todo el mundo, un administrador puede configurar Microsoft Distributed Filesystem (DFS) con enlaces que apuntan a recursos compartidos de servidores de archivos y a ubicaciones perimetrales.



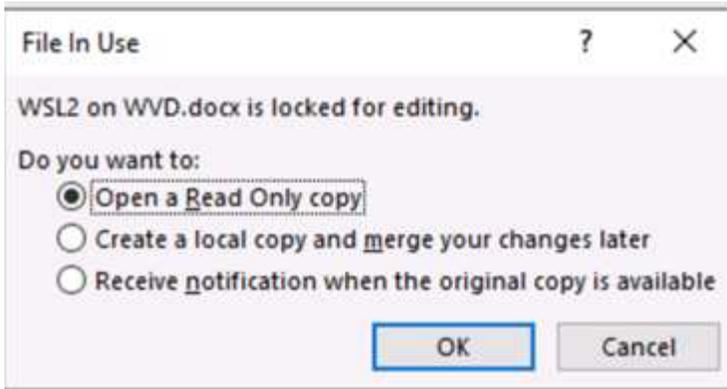
Cuando los usuarios inician sesión con credenciales de Active Directory basadas en las subredes asociadas al sitio, el cliente DFS utiliza el vínculo apropiado para tener acceso a los datos.



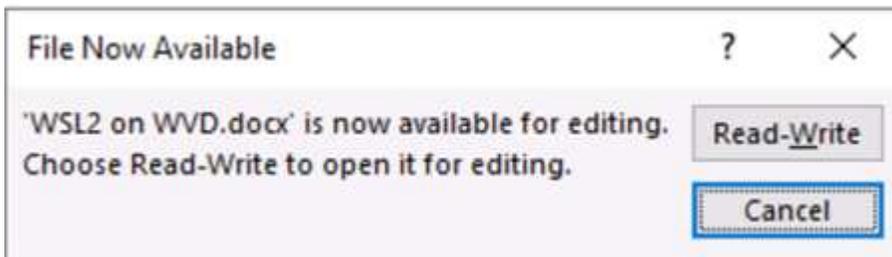
Los iconos de archivo cambian dependiendo de si un archivo está almacenado en caché; los archivos que no están almacenados en caché tienen una X gris en la esquina inferior izquierda del icono. Cuando un usuario de una ubicación perimetral accede a un archivo, dicho archivo se almacena en caché y el icono cambia.



Cuando un archivo está abierto y otro usuario intenta abrir el mismo archivo desde una ubicación de borde, se le solicita al usuario la siguiente selección:



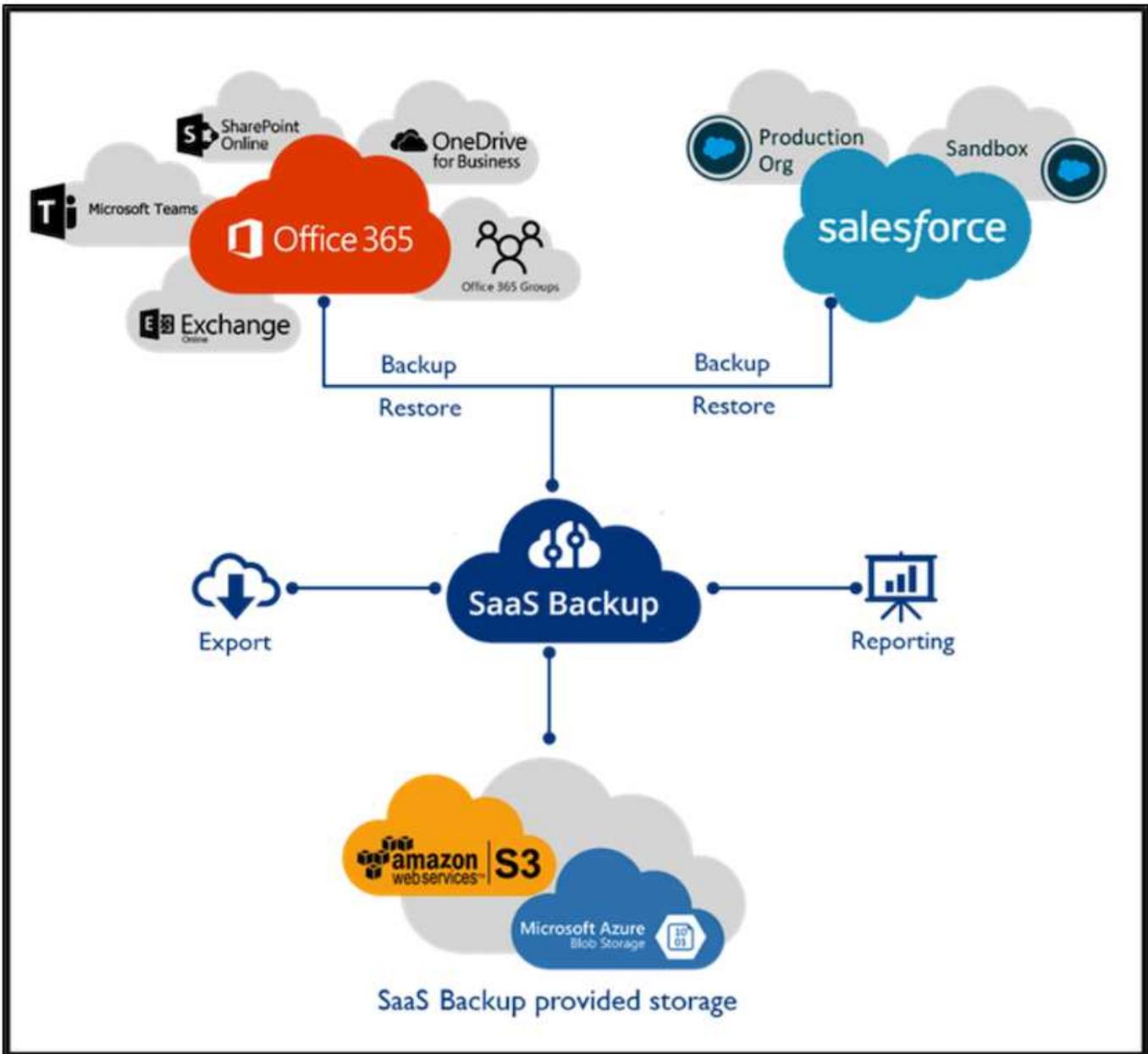
Si el usuario selecciona la opción de recibir una notificación cuando la copia original está disponible, se notifica al usuario de la siguiente manera:



Para obtener más información, consulte este tema ["Vídeo sobre implementación de Talon y Azure NetApp Files"](#).

## Backup de SaaS

VDS de NetApp proporciona protección de datos para Salesforce y Microsoft Office 365, incluidos Exchange, SharePoint y Microsoft OneDrive. La figura siguiente muestra cómo VDS de NetApp proporciona SaaS Backup para estos servicios de datos.



Para ver una demostración de la protección de datos de Microsoft Office 365, consulte ["este vídeo"](#).

Para ver una demostración de la protección de datos de Salesforce, consulte ["este vídeo"](#).

### Gestión de operaciones

Con VDS de NetApp, los administradores pueden delegar tareas a otras. Pueden conectarse a servidores implementados para solucionar problemas, ver registros y ejecutar informes de auditoría. Mientras ayuda a los clientes, al servicio de asistencia técnica o a los técnicos de nivel 3, puede remedar sesiones de usuarios, ver listas de procesos y matar procesos si es necesario.

Para obtener información acerca de los archivos de registro de VDS, consulte ["Solución de problemas de la página de acciones de VDA fallidas"](#).

Para obtener más información sobre los permisos mínimos necesarios, consulte ["Página componentes y](#)

[permisos de VDA](#)".

Si desea clonar manualmente un servidor, consulte ["Página Cloning Virtual Machines"](#).

Para aumentar automáticamente el tamaño del disco de la máquina virtual, consulte ["Página de características aumento automático del espacio en disco"](#).

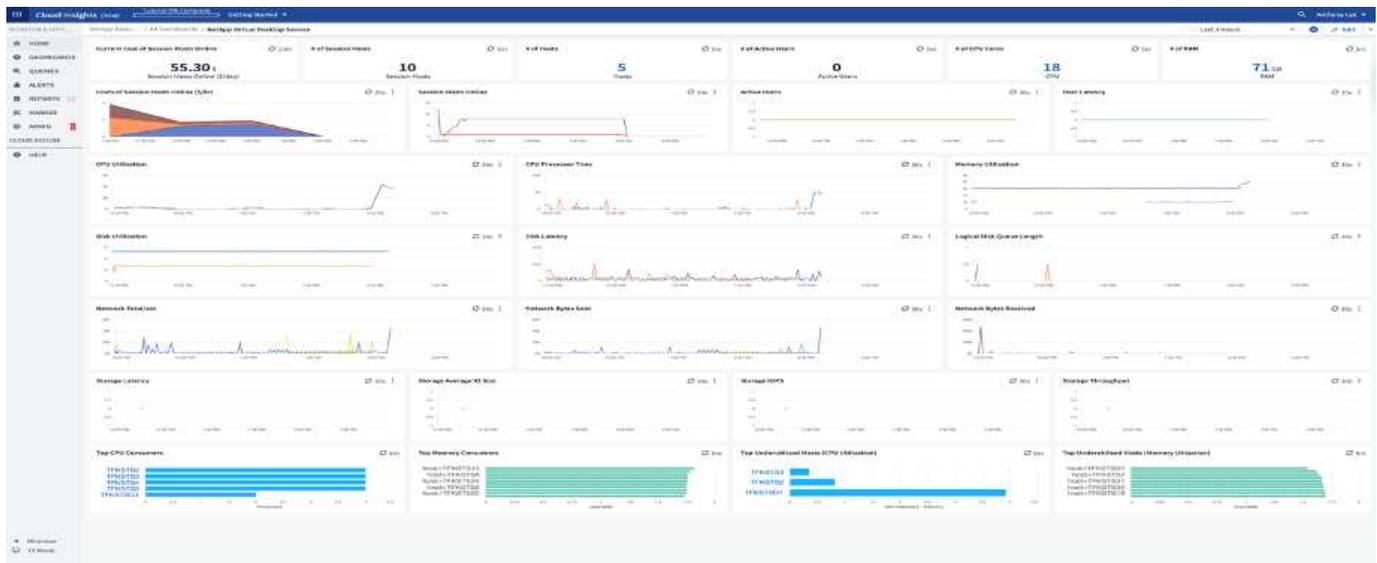
Para identificar la dirección de puerta de enlace para configurar manualmente el cliente, consulte ["Requisitos del usuario final"](#).

## Cloud Insights

Cloud Insights de NetApp es una herramienta de supervisión basada en Web que le ofrece una visibilidad completa de la infraestructura y las aplicaciones que se ejecutan en NetApp y otros componentes de infraestructura de terceros. Cloud Insights admite tanto clouds privados como públicos para supervisar, solucionar problemas y optimizar recursos.

Sólo la unidad de adquisición VM (puede ser Windows o Linux) debe estar instalada en una nube privada para recopilar métricas de recopiladores de datos sin necesidad de agentes. Los recopiladores de datos basados en agentes le permiten extraer métricas personalizadas del Monitor de rendimiento de Windows o de cualquier agente de entrada compatible con Telegraf.

La siguiente figura muestra el panel de VDS de Cloud Insights.



Para obtener más información sobre Cloud Insights de NetApp, consulte ["este vídeo"](#).

## Herramientas y registros

### Herramienta DCCConfig

La herramienta DCCconfig admite las siguientes opciones de hipervisor para agregar un sitio:

DataCenter Site

DataCenter Site

Hypervisor

Cancel New Save

Load Hypervisor Test

Select Hypervisor

- Aws
- AzureClassic
- AzureRM
- ComputeEngine
- HyperV
- ProfitBricks
- vCloud
- vCloudRest
- vSphere
- XenServer

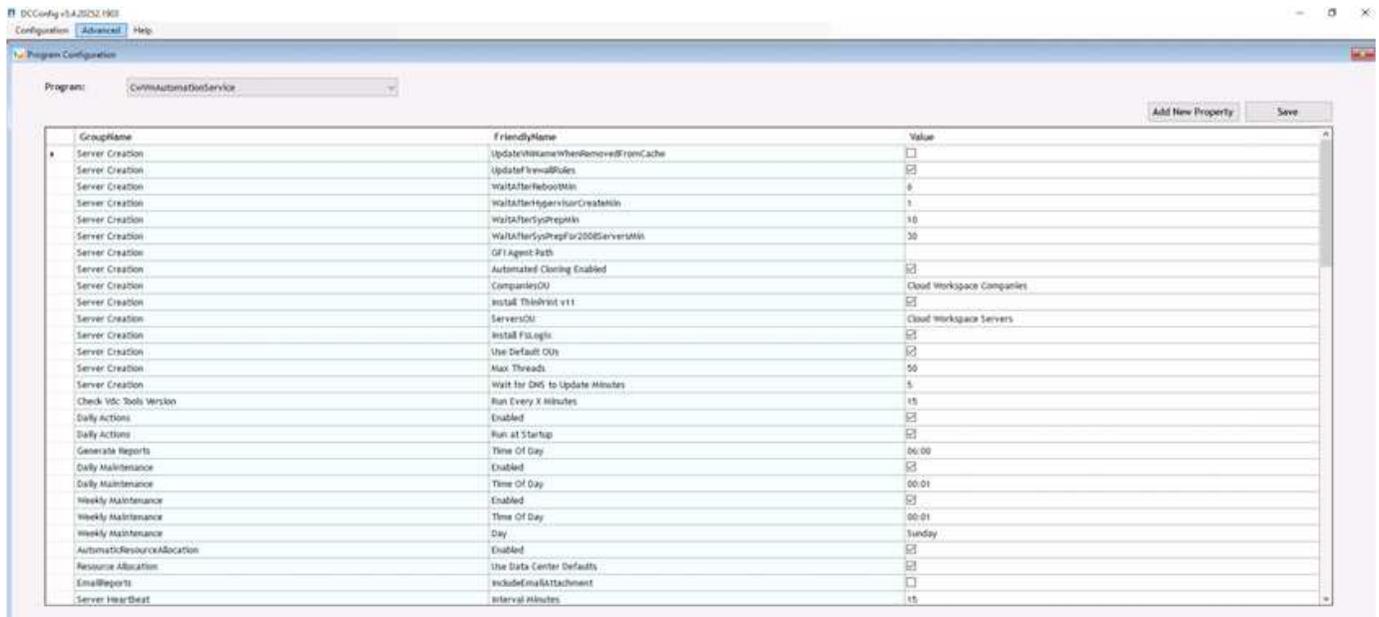
Configuration

DataCenter Accounts Email DatabaseConnection Exclude DataCenter Sites Product Keys Static IpAddress Drive Mapping

Save

	Description	DriveLetter
	Shared Data	P
	FTP	F
▶	User Home	H

La asignación de letras de unidades específicas del espacio de trabajo para datos compartidos se puede gestionar mediante GPO. Los Servicios profesionales o el equipo de soporte pueden utilizar la ficha Avanzadas para personalizar configuraciones como nombres de OU de Active Directory, la opción para activar o desactivar la implementación de FSLogix, varios valores de tiempo de espera, etc.

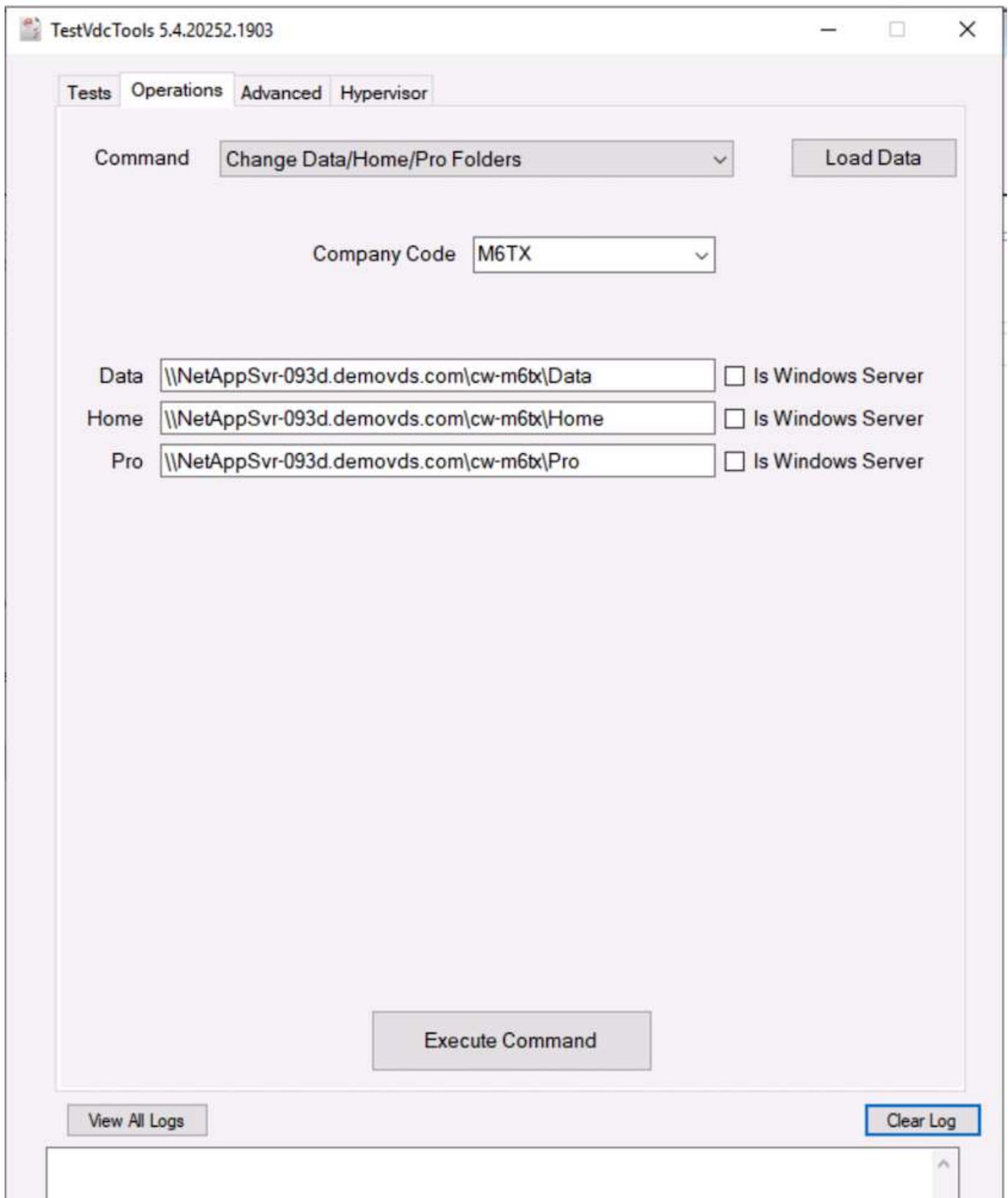


## Centro de comandos (anteriormente conocido como Herramientas de TestVdc)

Para iniciar Command Center y el rol necesario, consulte "[Descripción general del Centro de comandos](#)".

Es posible realizar las siguientes operaciones:

- Cambiar la ruta del bloque de mensajes del servidor de un espacio de trabajo.



- Cambie el sitio para la colección de abastecimiento.

Tests Operations **Advanced** Hypervisor

Command Edit Provisioning Collection ▾

Load Data

Provisioning Collection Windows2019 ▾

Description On vSphere Site 2

Share Drive P ▾

Minimum Cache Level 1 ▾

Operating System Windows Server 2019 ▾

Collection Type Shared ▾

	Data Center Site	Role	Template	Storage
▶	Site 2 ▾	TSDData ▾	Windows2019 ▾	DS01
*	▾	▾	▾	▾

Execute Command

View All Logs

Clear Log

Archivos de registro

Name	Date modified	Type	Size
 CwAgent	9/19/2020 12:35 PM	File folder	
 CWAutomationService	9/19/2020 12:34 PM	File folder	
 CWManagerX	9/19/2020 12:53 PM	File folder	
 CwVmAutomationService	9/19/2020 12:34 PM	File folder	
 TestVdcTools	9/22/2020 8:20 PM	File folder	
 report	9/19/2020 12:18 PM	Executable Jar File	705 KB

Comprobar "[registros de automatización](#)" para obtener más información.

### Consideraciones sobre la GPU

Normalmente, las GPU se utilizan para la visualización gráfica (renderización) mediante cálculos aritméticos repetitivos. Esta funcionalidad de computación repetitiva se utiliza a menudo para casos de uso de IA y aprendizaje profundo.

Para aplicaciones con un uso intensivo de gráficos, Microsoft Azure ofrece la serie NV basada en la tarjeta NVIDIA Tesla M60 con una a cuatro GPU por máquina virtual. Cada tarjeta NVIDIA Tesla M60 incluye dos GPU basadas en Maxwell, cada una con 8 GB de memoria GDDR5 para un total de 16 GB.



Se incluye una licencia de NVIDIA con la serie NV.

TechPowerUp GPU-Z 2.36.0

Graphics Card | Sensors | Advanced | Validation

Name: NVIDIA Tesla M60 [Lookup](#)

GPU: GM204 | Revision: FF

Technology: 28 nm | Die Size: 398 mm<sup>2</sup>

Release Date: Aug 30, 2015 | Transistors: 5200M

BIOS Version: 84.04.85.00.03 [Share](#)  UEFI

Subvendor: NVIDIA | Device ID: 10DE 13F2 - 10DE 115E

ROPs/TMUs: 64 / 128 | Bus Interface: PCI

Shaders: 2048 Unified | DirectX Support: 12 (12\_1)

Pixel Fillrate: 75.4 GPixel/s | Texture Fillrate: 150.8 GTexel/s

Memory Type: GDDR5 (Hynix) | Bus Width: 256 bit

Memory Size: 8192 MB | Bandwidth: 160.4 GB/s

Driver Version: 27.21.14.5257 (NVIDIA 452.57) / 2016

Driver Date: Oct 22, 2020 | Digital Signature: WHQL

GPU Clock: 557 MHz | Memory: 1253 MHz | Boost: 1178 MHz

Default Clock: 557 MHz | Memory: 1253 MHz | Boost: 1178 MHz

NVIDIA SLI: Disabled

Computing:  OpenCL  CUDA  DirectCompute  DirectML

Technologies:  Vulkan  Ray Tracing  PhysX  OpenGL 4.6

NVIDIA Tesla M60 [Close](#)

Con NetApp HCI, la GPU H615C contiene tres tarjetas NVIDIA Tesla T4. Cada tarjeta NVIDIA Tesla T4 dispone de una GPU basada en Turing con 16 GB de memoria GDDR6. Si se utiliza en un entorno VMware vSphere, los equipos virtuales pueden compartir la GPU y cada equipo virtual tiene una memoria de búfer de trama dedicada. El seguimiento de rayos está disponible con las GPU en la NetApp HCI H615C para generar imágenes realistas, incluidos reflejos de luz. Tenga en cuenta que debe tener un servidor de licencias de

NVIDIA con una licencia para las funciones de GPU.

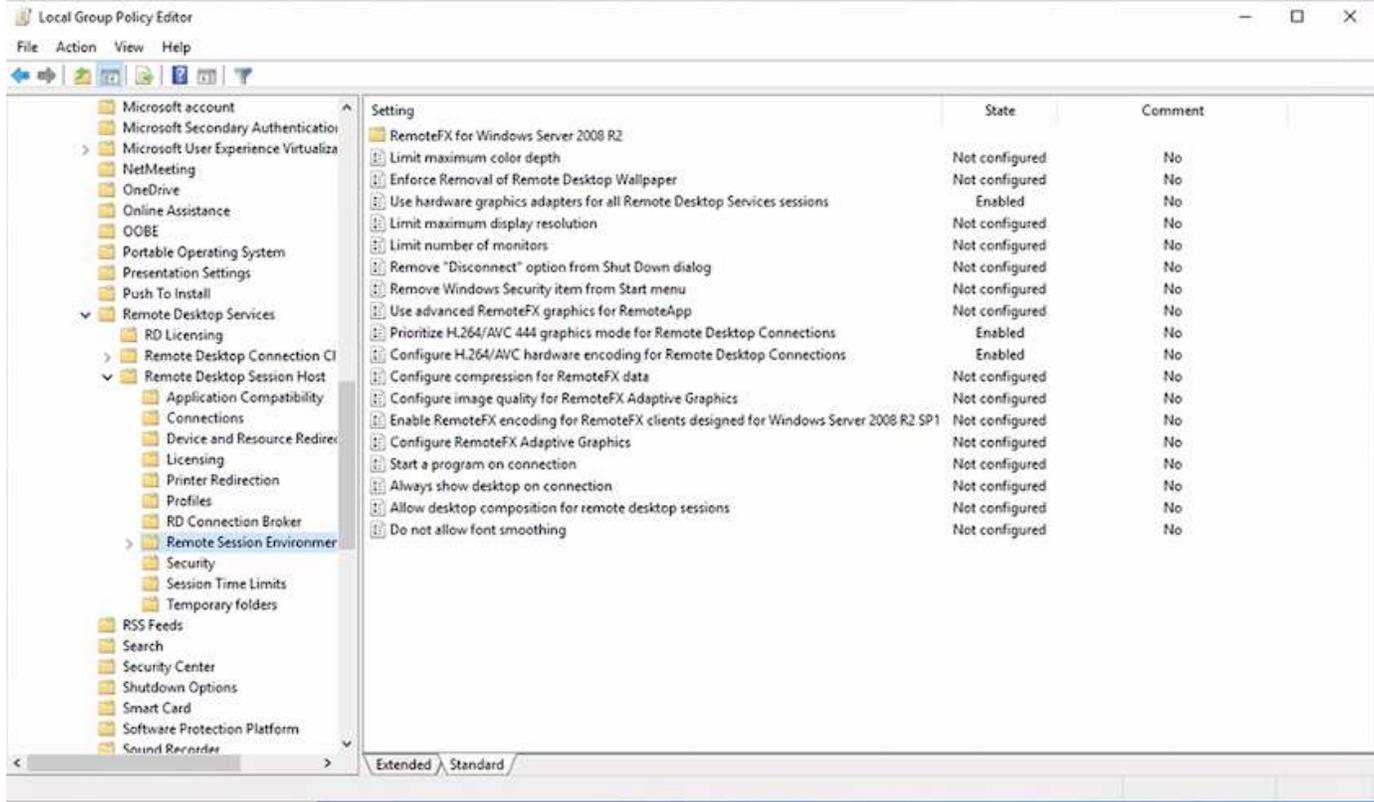
The screenshot shows the TechPowerUp GPU-Z 2.36.0 application window. The main content area displays the following information for the NVIDIA GRID T4-8Q GPU:

- Name:** NVIDIA GRID T4-8Q
- GPU:** TU104, **Revision:** A1
- Technology:** 12 nm, **Die Size:** 545 mm<sup>2</sup>
- Release Date:** Sep 13, 2018, **Transistors:** 13600M
- BIOS Version:** 0.00.00.00.00
- Subvendor:** NVIDIA, **Device ID:** 10DE 1EB8 - 10DE 130F
- ROPs/TMUs:** 8 / 160, **Bus Interface:** PCI
- Shaders:** 2560 Unified, **DirectX Support:** 12 (12\_2)
- Pixel Fillrate:** 4.7 GPixel/s, **Texture Fillrate:** 93.6 GTexel/s
- Memory Type:** GDDR6, **Bus Width:** 256 bit
- Memory Size:** 8192 MB, **Bandwidth:** Unknown
- Driver Version:** 27.21.14.5257 (NVIDIA 452.57) / 2016
- Driver Date:** Oct 22, 2020, **Digital Signature:** WHQL
- GPU Clock:** 585 MHz, **Memory:** 0 MHz, **Shader:** N/A
- Default Clock:** 585 MHz, **Memory:** 0 MHz, **Shader:** N/A
- NVIDIA SLI:** Disabled
- Computing:**  OpenCL,  CUDA,  DirectCompute,  DirectML
- Technologies:**  Vulkan,  Ray Tracing,  PhysX,  OpenGL 4.6

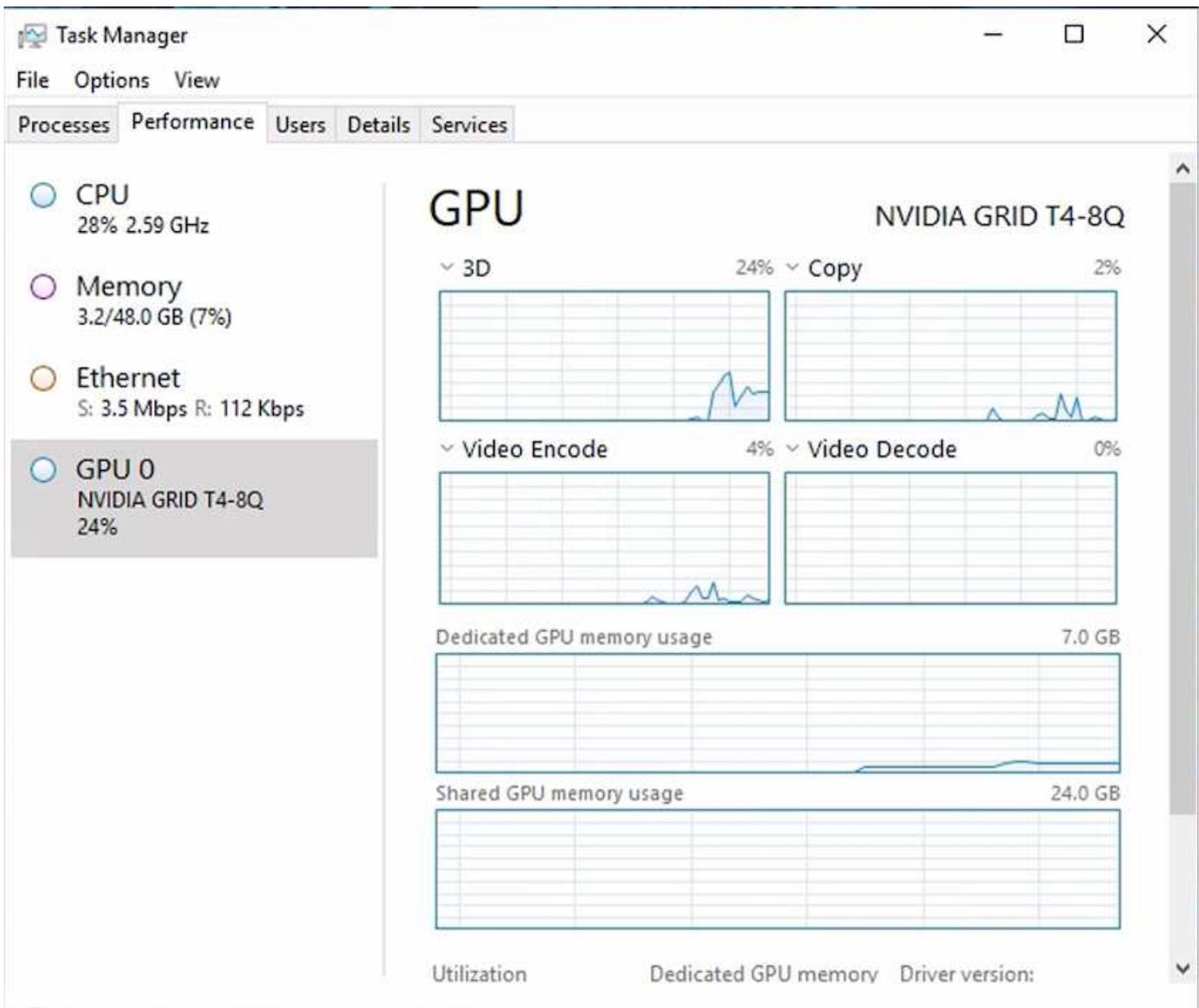
The application window includes a 'Graphics Card' tab, a 'Lookup' button, and a 'Close' button at the bottom right. The NVIDIA logo is also visible on the right side of the interface.

Para utilizar la GPU, debe instalar el controlador apropiado, que puede descargarse desde el portal de licencias de NVIDIA. En un entorno de Azure, el controlador NVIDIA está disponible como extensión del controlador GPU. A continuación, las políticas de grupo de la siguiente captura de pantalla deben actualizarse

para utilizar hardware GPU para sesiones de servicio de escritorio remoto. Debe priorizar el modo de gráficos H.264 y activar la funcionalidad de codificador.



Valide la supervisión del rendimiento de la GPU con el Administrador de tareas o utilizando la interfaz de línea de comandos nvidia-smi cuando ejecute muestras WebGL. Asegúrese de que se están consumiendo recursos de GPU, memoria y codificador.



Para asegurarse de que la máquina virtual se despliegue en NetApp HCI H615C con Virtual Desktop Service, defina un sitio con el recurso de clúster de vCenter que tenga hosts H615C. La plantilla de VM debe tener conectado el perfil vGPU requerido.

En los entornos de varias sesiones compartidos, considere la posibilidad de asignar varios perfiles homogéneos de vGPU. Sin embargo, en el caso de aplicaciones gráficas profesionales de gama alta, es mejor hacer que cada equipo virtual esté dedicado a un usuario para mantener las máquinas virtuales aisladas.

El procesador de GPU puede controlarse mediante una política de calidad de servicio, y cada perfil de vGPU puede tener búferes de trama dedicados. Sin embargo, el codificador y el decodificador son compartidos para cada tarjeta. La ubicación de un perfil vGPU en una tarjeta de GPU está controlada por la política de asignación de GPU del host de vSphere, que puede hacer hincapié en el rendimiento (propagación de VM) o la consolidación (grupo de VM).

#### Soluciones para el sector

Las estaciones de trabajo gráficas suelen utilizarse en sectores como la fabricación, la sanidad, la energía, los medios de comunicación y el entretenimiento, la educación, y así sucesivamente. La movilidad suele ser limitada a aplicaciones que hacen un uso

## intensivo de los gráficos.

Para abordar el problema de la movilidad, Virtual Desktop Services proporciona un entorno de escritorio para todo tipo de trabajadores, desde trabajadores de tareas a usuarios expertos, utilizando recursos de hardware en el cloud o con NetApp HCI, incluidas opciones para configuraciones de GPU flexibles. VDS permite a los usuarios acceder a su entorno de trabajo desde cualquier lugar con portátiles, tablets y otros dispositivos móviles.

Para ejecutar cargas de trabajo de fabricación con software como ANSYS Fluent, ANSYS Mechanical, Autodesk AutoCAD, Autodesk Inventor, Autodesk 3ds Max, Dassault Systèmes SOLIDWORKS, Dassault Systèmes CATIA, PTC Creo, Siemens PLM NX, etc. En la siguiente tabla figuran las GPU disponibles en varios clouds (a fecha de enero de 2021).

Modelo GPU	Microsoft Azure	Google Compute (GCP)	Amazon Web Services (AWS)	En las instalaciones (NetApp HCI)
NVIDIA M60	Sí	Sí	Sí	No
NVIDIA T4	No	Sí	Sí	Sí
P100 DE NVIDIA	No	Sí	No	No
NVIDIA P4	No	Sí	No	No

También están disponibles sesiones de escritorio compartidas con otros usuarios y escritorios personales dedicados. Los escritorios virtuales pueden tener de una a cuatro GPU o pueden utilizar GPU parciales con NetApp HCI. NVIDIA T4 es una tarjeta GPU versátil que puede hacer frente a las demandas de una amplia gama de cargas de trabajo de usuarios. Cada tarjeta GPU de NetApp HCI H615C tiene 16 GB de memoria de búfer de trama y tres tarjetas por servidor. El número de usuarios que se puede alojar en un único servidor H615C depende de la carga de trabajo del usuario.

Usuarios/servidor	Luz (4 GB)	Medio (8 GB)	Pesado (16 GB)
H615C	12	6	3

Para determinar el tipo de usuario, ejecute la herramienta de perfilador de GPU mientras los usuarios trabajan con aplicaciones que realizan tareas típicas. El perfilador de GPU captura las demandas de memoria, el número de pantallas y la resolución que los usuarios necesitan. A continuación, puede elegir el perfil vGPU que satisfaga sus necesidades.

Los puestos de trabajo virtuales con GPU pueden admitir una resolución de visualización de hasta 8K y la utilidad nView puede dividir un único monitor en regiones para trabajar con diferentes conjuntos de datos.

Con el almacenamiento de archivos de ONTAP, puede obtener las siguientes ventajas:

- Un espacio de nombres único que puede aumentar hasta 20 PB de almacenamiento con 400 000 millones de archivos sin necesidad de mucha intervención administrativa
- Un espacio de nombres que puede extenderse por todo el mundo con una caché global de archivos
- Multi-tenancy seguro con almacenamiento gestionado de NetApp
- La migración de datos inactivos a almacenes de objetos con FabricPool de NetApp
- Rápida estadística de archivos con análisis del sistema de archivos
- Escalar un clúster de almacenamiento hasta 24 nodos aumentando la capacidad y el rendimiento

- La capacidad de controlar el espacio de almacenamiento usando cuotas y un rendimiento garantizado con límites de calidad de servicio
- Proteja los datos mediante el cifrado
- Cumplimiento de una amplia gama de requisitos de protección de datos y cumplimiento de normativas
- Ofrecer opciones flexibles de continuidad empresarial

## Conclusión

El servicio de escritorios virtuales de NetApp ofrece un entorno de aplicaciones y puestos de trabajo virtuales fácil de usar, prestando especial atención a los desafíos empresariales. Al ampliar VDS con el entorno ONTAP en las instalaciones, es posible utilizar potentes funciones de NetApp en un entorno VDS, que incluyen un clonado rápido, deduplicación en línea, compactación, thin provisioning, y compresión. Estas funciones ahorran en costes de almacenamiento y mejoran el rendimiento con el almacenamiento all-flash. Con el hipervisor VMware vSphere, que minimiza el tiempo de aprovisionamiento del servidor mediante Virtual Volumes y la API de vSphere para la integración de cabina. Con el cloud híbrido, los clientes pueden elegir el entorno adecuado para sus cargas de trabajo exigentes y ahorrar dinero. La sesión de escritorio que se ejecuta en las instalaciones puede acceder a los recursos cloud en función de políticas.

## Dónde encontrar información adicional

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

- ["Cloud de NetApp"](#)
- ["Documentación de producto VDS de NetApp"](#)
- ["Conecte su red local a Azure con VPN Gateway"](#)
- ["Portal de Azure"](#)
- ["Escritorio virtual de Microsoft Windows"](#)
- ["Registro de Azure NetApp Files"](#)

## Horizon de VMware

### NVA-1132-DESIGN: Computación de usuario final de VMware con NetApp HCI

Suresh Thoppay, NetApp

La computación de usuario final de VMware con NetApp HCI es una arquitectura de centro de datos prevalidada y con mejores prácticas para poner en marcha cargas de trabajo de puestos de trabajo virtuales a escala empresarial. Este documento describe el diseño de la arquitectura y las mejores prácticas para poner en marcha la solución a escala de producción de forma fiable y sin riesgos.

["NVA-1132-DESIGN: Computación de usuario final de VMware con NetApp HCI"](#)

## **NVA-1129-DESIGN: Computación de usuario final de VMware con NetApp HCI y GPU de NVIDIA**

Suresh Thoppay, NetApp

La computación de usuario final de VMware con NetApp HCI es una arquitectura de centro de datos prevalidada y con mejores prácticas para poner en marcha cargas de trabajo de puestos de trabajo virtuales a escala empresarial. Este documento describe el diseño de la arquitectura y las mejores prácticas para poner en marcha la solución a escala de producción de forma fiable y sin riesgos.

["NVA-1129-DESIGN: Computación de usuario final de VMware con NetApp HCI y GPU de NVIDIA"](#)

## **NVA-1129-DEPLOY: Computación de usuario final de VMware con NetApp HCI y GPU de NVIDIA**

Suresh Thoppay, NetApp

La computación de usuario final de VMware con NetApp HCI es una arquitectura de centro de datos prevalidada y de mejores prácticas para la puesta en marcha de cargas de trabajo de puestos de trabajo virtuales a escala empresarial. Este documento describe cómo poner en marcha la solución a escala de producción de una manera fiable y sin riesgos

["NVA-1129-DEPLOY: Computación de usuario final de VMware con NetApp HCI y GPU de NVIDIA"](#)

## **NetApp HCI para la infraestructura de puestos de trabajo virtuales con VMware Horizon 7: Impulse a los usuarios avanzados con gráficos 3D**

Suresh Thoppay, NetApp

El informe técnico TR-4792 proporciona orientación sobre el uso del nodo de computación H615C de NetApp para cargas de trabajo de gráficos 3D en un entorno VMware Horizon impulsado por las unidades de procesamiento gráfico (GPU) de NVIDIA y el software de virtualización. También proporciona los resultados de las pruebas preliminares de SPECviewperf 13 para el H615C.

["NetApp HCI para la infraestructura de puestos de trabajo virtuales con VMware Horizon 7: Impulse a los usuarios avanzados con gráficos 3D"](#)

## **Soluciones de virtualización de puestos de trabajo de FlexPod**

Para obtener más información sobre las soluciones de virtualización de FlexPod, consulte la ["Guías de diseño de FlexPod"](#)

## **Cabina All-Flash SAN de NetApp con VMware vSphere 8**

Autor: Josh Powell: Ingeniería de soluciones de NetApp

# Descripción general de la solución

## Introducción

Durante casi dos décadas, el software NetApp ONTAP se ha situado como una solución de almacenamiento de primera categoría para entornos vSphere de VMware, introduciendo continuamente funciones innovadoras que simplifican la gestión y reducen los costes. NetApp es un líder establecido en el desarrollo de NAS y plataformas de almacenamiento unificado que ofrecen una amplia gama de compatibilidad con protocolos y conectividad. Junto con este segmento del mercado, hay muchos clientes que prefieren la simplicidad y las ventajas de coste de las plataformas de almacenamiento SAN basadas en bloques centradas en optimizar su trabajo. La cabina all-flash SAN (ASA) de NetApp cumple esa promesa con sencillez a escala y con funciones de gestión y automatización consistentes para todas las aplicaciones y los proveedores de cloud.

## Objetivo de este documento

En este documento, trataremos el valor exclusivo del uso de sistemas de almacenamiento de NetApp ASA con vSphere de VMware y proporcionaremos una descripción general de la tecnología de la cabina SAN all-flash de NetApp. Además, veremos herramientas adicionales para simplificar el aprovisionamiento de almacenamiento y la protección de datos y la supervisión de tu centro de datos de VMware y ONTAP.

Las secciones de puesta en marcha de este documento tratan la creación de almacenes de datos VVOL con herramientas de ONTAP para VMware vSphere y la observabilidad del centro de datos moderno con NetApp Cloud Insights.

## Visión general de la tecnología

Esta solución incluye tecnologías innovadoras de VMware y NetApp.

### VMware vSphere 8,0

VMware vSphere es una plataforma de virtualización que transforma los recursos físicos en pools de informática, red y almacenamiento que se pueden utilizar para satisfacer los requisitos de las aplicaciones y las cargas de trabajo de los clientes. Entre los principales componentes de VMware vSphere se incluyen:

- **ESXi** - Hipervisor de VMware que permite la abstracción de procesadores de cómputo, memoria, red y otros recursos y los pone a disposición de máquinas virtuales y cargas de trabajo de contenedores.
- **vCenter** - VMware vCenter es una plataforma de gestión centralizada para interactuar con recursos informáticos, redes y almacenamiento como parte de una infraestructura virtual. vCenter desempeña un papel crucial en la simplificación de la administración de infraestructura virtualizada.

### Nuevas mejoras en vSphere 8,0

vSphere 8,0 introduce algunas mejoras nuevas, entre las que se incluyen:

**Escalabilidad** - vSphere 8,0 es compatible con las CPU Intel y AMD más recientes y tiene límites extendidos para dispositivos vGPU, hosts ESXi, VM por clúster y dispositivos de E/S DirectPath de VM.

**Distributed Services Engine** - Descarga de red con NSX a unidades de procesamiento de datos (DPU).

- Eficiencia mejorada de dispositivos \* - vSphere 8,0 aumenta las capacidades de administración de dispositivos con funciones como grupos de dispositivos y extensiones de virtualización de dispositivos (DVX).
- Seguridad mejorada \* - La inclusión de un tiempo de espera SSH y la Política de provisión TPM fortalece el marco de seguridad.

**Integración con servicios de nube híbrida** - Esta característica facilita la transición sin interrupciones entre las cargas de trabajo en las instalaciones y en la nube.

- Tiempo de ejecución de Kubernetes integrado \* - Con la inclusión de Tanzu, vSphere 8,0 simplifica la orquestación de contenedores.

Para obtener más información, consulte el blog, "[¿Qué novedades hay en vSphere 8?](#)".

### **Volúmenes virtuales de VMware (vVols)**

vVols es un nuevo y revolucionario método de la gestión del almacenamiento en clústeres de vSphere que ofrece una gestión simplificada y un control más granular de los recursos de almacenamiento. En un almacén de datos vVols, cada disco virtual es un VVOL y se convierte en un objeto LUN nativo del sistema de almacenamiento. La integración del sistema de almacenamiento y vSphere se lleva a cabo a través del proveedor de la API de VMware para el conocimiento del almacenamiento (VASA)\* y permite que el sistema de almacenamiento sea consciente de los datos de la VM y lo gestione en consecuencia. Las políticas de almacenamiento, definidas en vCenter Client, se utilizan para asignar y gestionar recursos de almacenamiento.

Los vVols constituyen un método simplificado de la gestión del almacenamiento y son preferibles en algunos casos prácticos.

Para obtener más información sobre vVols, consulte la "[Guía de inicio de vVols](#)".

### **NVMe sobre entramados**

Con el lanzamiento de vSphere 8,0, ahora se admite NVMe integral, con compatibilidad total con vVols con NVMe-TCP y NVMe-FC.

Para obtener información detallada sobre el uso de NVMe con vSphere, consulte "[Acerca del almacenamiento NVMe de VMware](#)". En la documentación de vSphere Storage.

---

### **ONTAP de NetApp**

El software ONTAP de NetApp lleva casi dos décadas siendo una solución de almacenamiento líder para entornos VMware vSphere y sigue agregando funcionalidades innovadoras que simplifican la gestión y reducen los costes. El uso de ONTAP junto con vSphere es una excelente combinación que le permite reducir los gastos en hardware del host y software de VMware. También puede proteger sus datos con un coste menor y un alto rendimiento uniforme, al tiempo que aprovecha las eficiencias del almacenamiento nativo.

#### **Funciones básicas de ONTAP**

Copias Snapshot de NetApp: Copias Snapshot de una máquina virtual o un almacén de datos, lo que garantiza que el rendimiento no afecte a la creación o utilización de una snapshot. Estas réplicas pueden servir como puntos de restauración para equipos virtuales o como una sencilla protección de datos. Estas copias Snapshot basadas en cabina son diferentes de las copias Snapshot de VMware (coherencia). El método más sencillo para generar una copia Snapshot de ONTAP es mediante el plugin de SnapCenter para VMware vSphere, que realiza backups de máquinas virtuales y almacenes de datos.

- **Eficiencia de almacenamiento** - ONTAP proporciona deduplicación y compresión en tiempo real y en segundo plano, deduplicación de bloques cero y compactación de datos.
- \* Volumen y movimiento de LUN \* - Permite el movimiento no disruptivo de volúmenes y LUN que admiten almacenes de datos de vSphere y vVols dentro del clúster de ONTAP para equilibrar el rendimiento y la

capacidad o admitir mantenimiento y actualizaciones no disruptivas.

- **Reubicación de volumen y LUN** - ONTAP permite el movimiento no disruptivo de volúmenes y LUN que alojan almacenes de datos vSphere y vVols dentro del clúster de ONTAP. De este modo, se consigue equilibrar el rendimiento y la capacidad, y se pueden realizar actualizaciones sin interrupciones.
- **Calidad de servicio** - QoS es una característica que permite la administración del rendimiento en un LUN, volumen o archivo individual. Puede utilizarse para limitar una máquina virtual agresiva o para garantizar que una máquina virtual crítica reciba suficientes recursos de rendimiento.
- **Cifrado** - Cifrado de volumen NetApp y Cifrado agregado NetApp. Estas opciones proporcionan un enfoque sencillo basado en software para cifrar los datos en reposo y garantizar su protección.
- **Fabric Pool** - Esta función organiza en niveles los datos a los que se accede con menos frecuencia en un almacén de objetos separado, liberando valioso almacenamiento flash. Al operar a nivel de bloque, se identifican y clasifican en niveles los datos más inactivos de manera eficiente, lo que ayuda a optimizar los recursos de almacenamiento y reducir los costes.
- **\* Automatización \*** - Simplifica las tareas de almacenamiento y gestión de datos utilizando las API REST DE ONTAP para la automatización y aprovechando los módulos de Ansible para una gestión de configuración perfecta de los sistemas de ONTAP. Los módulos de Ansible ofrecen una solución práctica para gestionar de manera eficiente las configuraciones de los sistemas ONTAP. La combinación de estas potentes herramientas permite agilizar los flujos de trabajo y mejorar la gestión global de la infraestructura de almacenamiento.

#### **Funcionalidades de recuperación ante desastres de ONTAP**

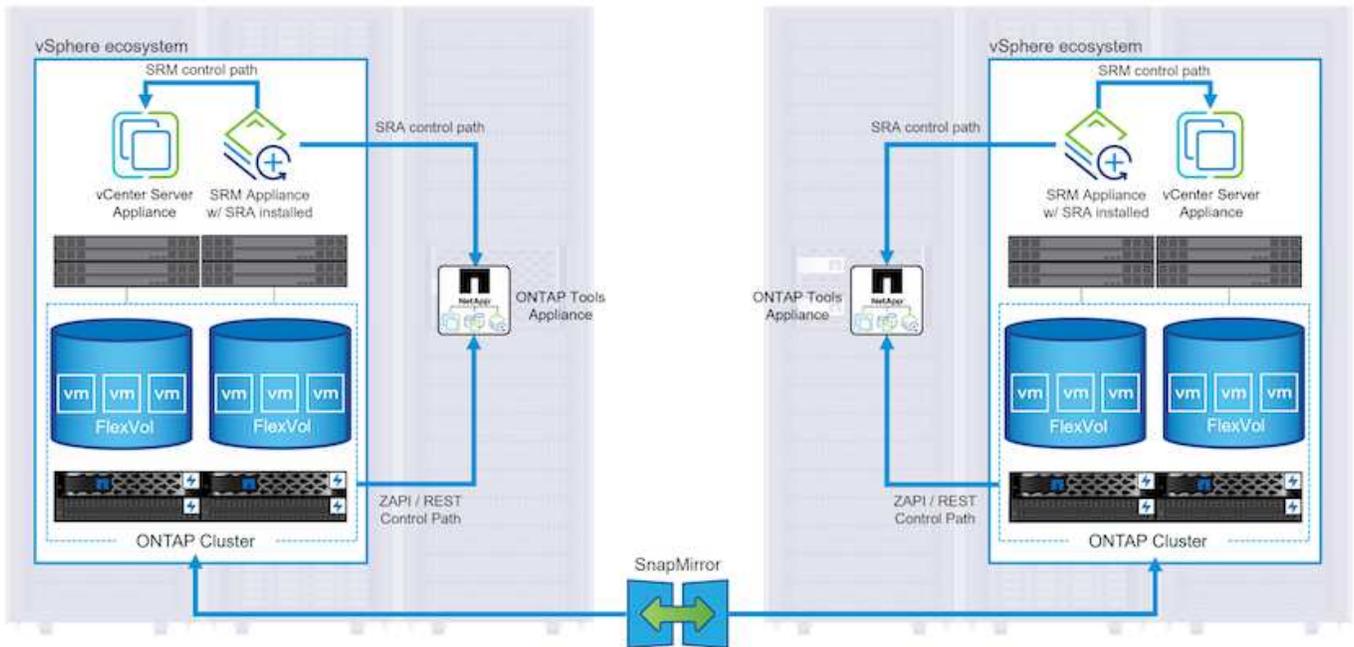
NetApp ONTAP ofrece soluciones sólidas de recuperación ante desastres para entornos VMware. Estas soluciones aprovechan las tecnologías de replicación de SnapMirror entre los sistemas de almacenamiento primario y secundario para permitir la recuperación tras fallos y una rápida recuperación en caso de fallo.

#### **Adaptador de Replicación de Almacenamiento:**

El adaptador de replicación de almacenamiento (SRA) de NetApp es un componente de software que ofrece integración entre los sistemas de almacenamiento de NetApp y el administrador de recuperación de sitio (SRM) de VMware. Facilita la replicación de datos de máquinas virtuales (VM) en las cabinas de almacenamiento de NetApp y ofrece funcionalidades sólidas de protección de datos y recuperación ante desastres. El SRA utiliza SnapMirror y SnapVault para lograr la replicación de datos de VM en sistemas de almacenamiento dispares o ubicaciones geográficas.

El adaptador proporciona replicación asíncrona en el nivel de máquina virtual de almacenamiento (SVM) mediante la tecnología SnapMirror y amplía la compatibilidad con VMFS en entornos de almacenamiento SAN (iSCSI y FC) y NFS en entornos de almacenamiento NAS.

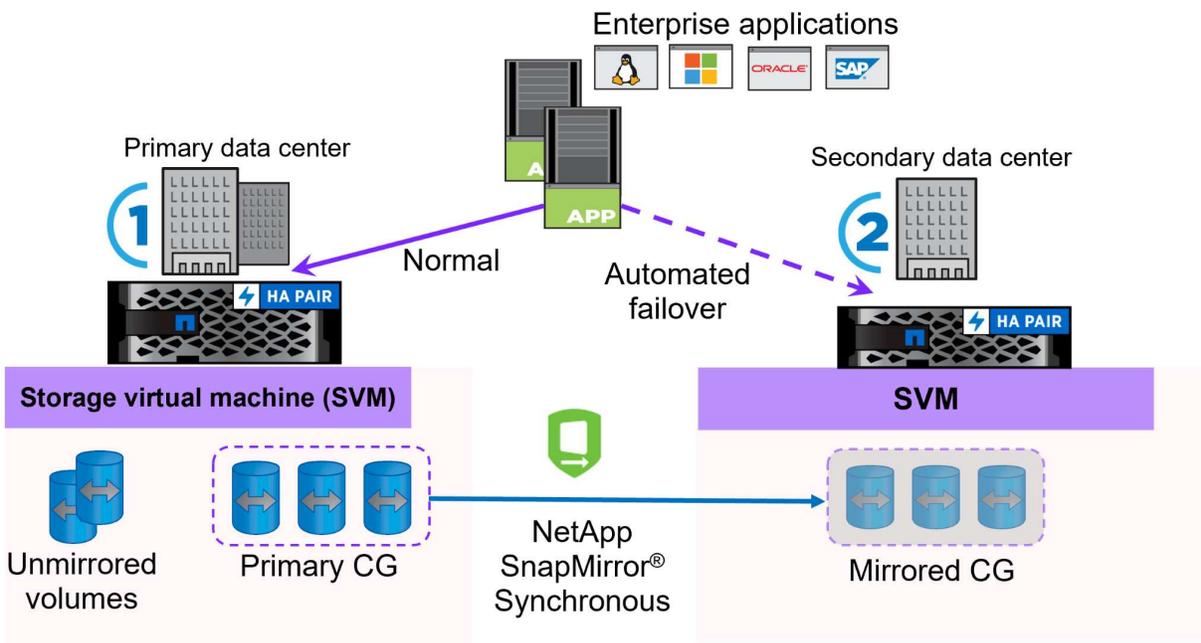
El SRA de NetApp se instala como parte de las herramientas de ONTAP para VMware vSphere.



Para obtener información sobre el adaptador de replicación de almacenamiento de NetApp para SRM, consulte ["VMware Site Recovery Manager con NetApp ONTAP"](#).

### Continuidad del negocio de SnapMirror:

SnapMirror es una tecnología de replicación de datos de NetApp que proporciona replicación síncrona de datos entre sistemas de almacenamiento. Permite la creación de varias copias de los datos en ubicaciones diferentes, proporcionando la posibilidad de recuperar los datos en caso de desastre o pérdida de datos. SnapMirror ofrece flexibilidad en términos de frecuencia de replicación y permite la creación de copias de un momento específico de datos para fines de backup y recuperación de datos. SM-BC replica los datos a nivel del grupo de consistencia.



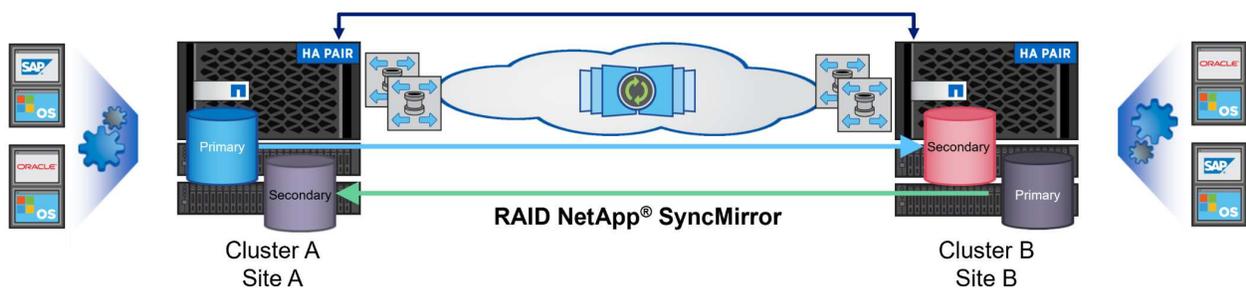
Si quiere más información, consulte SnapMirror ["Información general sobre la continuidad del negocio"](#).

### NetApp MetroCluster:

NetApp MetroCluster es una solución de alta disponibilidad y de recuperación ante desastres que ofrece replicación de datos síncrona entre dos sistemas de almacenamiento de NetApp distribuidos geográficamente. Está diseñado para garantizar la disponibilidad y la protección continuas de los datos en caso de que se produzca un fallo en todo el site.

MetroCluster utiliza SyncMirror para replicar datos de manera síncrona justo por encima del nivel de RAID. SyncMirror se ha diseñado para realizar una transición eficiente entre modos síncronos y asíncronos. Esto permite que el clúster de almacenamiento principal siga funcionando en un estado no replicado en situaciones en las que el sitio secundario quede temporalmente inaccesible. SyncMirror también se volverá a replicar en un estado RPO = 0 cuando se restaure la conectividad.

MetroCluster puede funcionar sobre redes basadas en IP o utilizando Fibre Channel.



Para obtener información detallada sobre la arquitectura y configuración de MetroCluster, consulte la ["Sitio de documentación de MetroCluster"](#).

### Modelo de licencias de ONTAP One

ONTAP One es un completo modelo de licencias que proporciona acceso a todas las funciones de ONTAP sin necesidad de licencias adicionales. Esto incluye la protección de datos, recuperación ante desastres, alta disponibilidad, integración del cloud, eficiencia del almacenamiento, rendimiento y seguridad. Los clientes con sistemas de almacenamiento de NetApp con licencias Flash, Core más Data Protection o Premium pueden obtener licencias de ONTAP One y así maximizar el aprovechamiento de sus sistemas de almacenamiento.

La licencia de ONTAP One incluye todas las siguientes funciones:

**NVMeoF** – Permite el uso de NVMe over Fabrics para la E/S de cliente front-end, tanto NVMe/FC como NVMe/TCP.

**FlexClone** – Permite la creación rápida de la clonación eficiente del espacio de datos basada en instantáneas.

**S3** – Permite el protocolo S3 para la E/S del cliente front-end.

**SnapRestore** – Permite la rápida recuperación de datos de instantáneas.

**Protección contra ransomware autónoma** - Permite la protección automática de los recursos compartidos de archivos del NAS cuando se detecta una actividad anormal del sistema de archivos.

- Multi Tenant Key Manager \* - Permite la capacidad de tener varios administradores de claves para diferentes inquilinos en el sistema.

**SnapLock** – Permite la protección de los datos contra la modificación, eliminación o corrupción en el sistema.

**SnapMirror Cloud** – Permite la replicación de volúmenes del sistema a objetivos de objetos.

**S3 SnapMirror** – Permite la replicación de objetos de ONTAP S3 para alternar destinos compatibles con S3.

## Cabina All-Flash SAN NetApp

La cabina all-flash SAN (ASA) de NetApp es una solución de almacenamiento de alto rendimiento diseñada para satisfacer los requisitos más exigentes de los centros de datos modernos. Combina la velocidad y la fiabilidad del almacenamiento flash con las funciones avanzadas de gestión de datos de NetApp para ofrecer un rendimiento, una escalabilidad y una protección de datos excepcionales.

La gama ASA está compuesta por los modelos A-Series y C-Series.

Las cabinas flash all-NVMe NetApp A-Series están diseñadas para cargas de trabajo de alto rendimiento, con una latencia ultrabaja y una alta resiliencia, lo que las convierte en adecuadas para aplicaciones de misión crítica.



Las cabinas flash QLC de C-Series se dirigen a casos de uso de mayor capacidad, y ofrecen la velocidad de la tecnología flash con la economía del flash híbrido.



Para obtener información detallada, consulte ["Página de destino de NetApp ASA"](#).

## Funciones de NetApp ASA

La cabina all-flash SAN NetApp incluye las siguientes funciones:

**Rendimiento** - La cabina SAN All-Flash aprovecha las unidades de estado sólido (SSD), con una arquitectura

NVMe integral, para proporcionar un rendimiento increíblemente rápido, reduciendo significativamente la latencia y mejorando los tiempos de respuesta de las aplicaciones. Ofrece una alta tasa constante de IOPS y baja latencia, lo que lo convierte en adecuado para cargas de trabajo sensibles a la latencia, como bases de datos, virtualización y análisis.

- Escalabilidad \* - Las cabinas SAN All-Flash de NetApp se crean con una arquitectura de escalado horizontal, lo que permite a las organizaciones escalar sin problemas su infraestructura de almacenamiento a medida que crecen sus necesidades. Gracias a la capacidad de añadir nodos de almacenamiento adicionales, las organizaciones pueden ampliar la capacidad y el rendimiento sin interrupciones, lo que garantiza que su almacenamiento pueda satisfacer las crecientes demandas de datos.
- Gestión de datos \*: El sistema operativo Data ONTAP de NetApp incorpora la cabina All-Flash SAN, que ofrece un conjunto completo de funciones de gestión de datos. Estas incluyen thin provisioning, la deduplicación, la compresión y la compactación de datos, que optimizan el aprovechamiento del almacenamiento y reducen los costes. Las funciones de protección de datos avanzadas, como snapshots, replicación y cifrado, garantizan la integridad y la seguridad de los datos almacenados.

**Integración y flexibilidad:** La cabina SAN All-Flash se integra con el ecosistema más amplio de NetApp, lo que permite una integración perfecta con otras soluciones de almacenamiento de NetApp, como implementaciones de clouds híbridos con NetApp Cloud Volumes ONTAP. Además, admite protocolos estándares del sector como Fibre Channel (FC) e iSCSI, lo que permite la integración fácil en las infraestructuras SAN existentes.

- Análisis y automatización\*: El software de gestión de NetApp, incluido NetApp Cloud Insights, proporciona funcionalidades completas de supervisión, análisis y automatización. Estas herramientas permiten a los administradores obtener información sobre su entorno de almacenamiento, optimizar el rendimiento y automatizar las tareas rutinarias, simplificar la gestión del almacenamiento y mejorar la eficiencia operativa.
- Protección de datos y continuidad empresarial \*: La cabina SAN All-Flash ofrece funciones integradas de protección de datos, como instantáneas puntuales, replicación y capacidades de recuperación ante desastres. Estas funciones garantizan la disponibilidad de datos y facilitan una rápida recuperación en caso de pérdida de datos o de fallos del sistema.

#### Compatibilidad con protocolos

ASA admite todos los protocolos SAN estándar, incluidos iSCSI, Fibre Channel (FC), Fibre Channel sobre Ethernet (FCoE) y NVMe over Fabrics.

**iSCSI** - NetApp ASA proporciona una sólida compatibilidad con iSCSI, lo que permite el acceso a nivel de bloque a dispositivos de almacenamiento a través de redes IP. Ofrece una integración perfecta con iniciadores iSCSI, lo que permite aprovisionar y gestionar LUN iSCSI de manera eficaz. Funciones avanzadas de ONTAP, como rutas múltiples, autenticación CHAP y compatibilidad con ALUA.

Para obtener una guía de diseño sobre configuraciones de iSCSI, consulte .

**Canal de fibra** - NetApp ASA ofrece soporte integral para el canal de fibra (FC), una tecnología de red de alta velocidad comúnmente utilizada en redes de área de almacenamiento (SAN). ONTAP se integra sin problemas con la infraestructura de FC y proporciona un acceso por bloques fiable y eficiente a los dispositivos de almacenamiento. Ofrece funciones como la división en zonas, las rutas múltiples y el inicio de sesión estructural (FLOGI) para optimizar el rendimiento, mejorar la seguridad y garantizar una conectividad perfecta en entornos FC.

Para obtener directrices de diseño sobre configuraciones de Fibre Channel, consulte ["Documentación de referencia de configuración de SAN"](#).

**NVMe over Fabrics** - NetApp ONTAP y ASA admiten NVMe over Fabrics. NVMe/FC permite utilizar dispositivos de almacenamiento NVMe sobre infraestructura Fibre Channel y NVMe/TCP sobre redes IP de almacenamiento.

Para obtener directrices de diseño en NVMe, consulte ["Configuración, compatibilidad y limitaciones de NVMe"](#).

### Tecnología activo-activo

Las cabinas NetApp All-Flash SAN permiten rutas activo-activo que pasan por ambas controladoras, por lo que no es necesario que el sistema operativo host espere a que se produzca un error en una ruta activa antes de activar la ruta alternativa. Esto significa que el host puede utilizar todas las rutas disponibles en todas las controladoras, asegurando que las rutas activas siempre estén presentes sin importar si el sistema está en estado constante o si se debe someter a una operación de conmutación por error de la controladora.

Además, NetApp ASA ofrece una función distintiva que mejora significativamente la velocidad de la conmutación por error de SAN. Cada controladora replica continuamente los metadatos LUN esenciales con su asociado. Como resultado, cada controladora está preparada para asumir las responsabilidades del servicio de datos en caso de un fallo repentino de su compañero. Esta preparación es posible debido a que la controladora ya posee la información necesaria para comenzar a utilizar las unidades que se gestionaron previamente por la controladora con el error.

Con rutas activo-activo, las tomas de control planificadas y sin planificar tienen tiempos de reanudación de I/O de 2-3 segundos.

Para obtener más información, consulte ["TR-4968, cabina All-SAS NetApp: Disponibilidad e integridad de los datos con NetApp ASA"](#).

### Garantías de almacenamiento

NetApp ofrece un conjunto único de garantías de almacenamiento con cabinas SAN All-Flash NetApp. Sus ventajas únicas incluyen:

- **Garantía de eficiencia de almacenamiento:** \* Consiga un alto rendimiento al tiempo que minimiza el costo de almacenamiento con la Garantía de Eficiencia de Almacenamiento. 4:1 para cargas de trabajo SAN.

**Garantía de disponibilidad de datos de 6 Nines (99,9999%):** garantiza la corrección de los tiempos de inactividad no planificados en más de 31,56 segundos al año.

**Garantía de recuperación de ransomware:** Recuperación de datos garantizada en caso de un ataque de ransomware.

Consulte ["Portal de productos de NetApp ASA"](#) si quiere más información.

---

### Complementos de NetApp para VMware vSphere

Los servicios de almacenamiento de NetApp se integran perfectamente con VMware vSphere mediante el uso de los siguientes plugins:

#### Herramientas de ONTAP para VMware vSphere

Las herramientas de ONTAP para VMware permiten a los administradores gestionar el almacenamiento de NetApp directamente desde vSphere Client. ONTAP Tools permite poner en marcha y gestionar almacenes de datos, así como aprovisionar almacenes de datos VVOL.

Herramientas ONTAP permite la asignación de almacenes de datos a perfiles de capacidades de almacenamiento que determinan un conjunto de atributos del sistema de almacenamiento. Esto permite la creación de almacenes de datos con atributos específicos como el rendimiento del almacenamiento y la calidad de servicio.

Las herramientas de ONTAP incluyen los siguientes componentes:

**Virtual Storage Console (VSC):** El VSC incluye la interfaz integrada con el cliente vSphere, donde puede agregar controladores de almacenamiento, aprovisionar almacenes de datos, supervisar el rendimiento de los almacenes de datos y ver y actualizar la configuración del host ESXi.

- Proveedor VASA: \* El proveedor de API de VMware vSphere para ONTAP envía información sobre el almacenamiento utilizado por VMware vSphere al servidor vCenter, lo que permite el aprovisionamiento de almacenes de datos de VMware Virtual Volumes (vVols), la creación y el uso de perfiles de capacidad de almacenamiento, la verificación de cumplimiento y la supervisión del rendimiento.

**Adaptador de replicación de almacenamiento (SRA):** Cuando se habilita y se usa con VMware Site Recovery Manager (SRM), SRA facilita la recuperación de los almacenes de datos de vCenter Server y las máquinas virtuales en caso de fallo, lo que permite la configuración de sitios protegidos y sitios de recuperación para recuperación ante desastres.

Para obtener más información sobre las herramientas de NetApp ONTAP para VMware, consulte ["Herramientas de ONTAP para documentación de VMware vSphere"](#).

#### **Plugin de SnapCenter para VMware vSphere**

El plugin de SnapCenter para VMware vSphere (SCV) es una solución de software de NetApp que ofrece una protección de datos completa para entornos VMware vSphere. Está diseñado para simplificar y agilizar el proceso de protección y gestión de máquinas virtuales y almacenes de datos.

El plugin de SnapCenter para VMware vSphere ofrece las siguientes funcionalidades en una interfaz unificada, integrada con el cliente de vSphere:

**Instantáneas basadas en políticas** - SnapCenter le permite definir políticas para crear y administrar instantáneas consistentes con aplicaciones de máquinas virtuales (VM) en VMware vSphere.

- Automatización \* - La creación y gestión automatizada de instantáneas basadas en políticas definidas ayudan a garantizar una protección de datos consistente y eficiente.

**VM-Level Protection** - La protección granular a nivel de VM permite una gestión y recuperación eficientes de máquinas virtuales individuales.

- Características de eficiencia del almacenamiento \* - La integración con las tecnologías de almacenamiento de NetApp proporciona funciones de eficiencia del almacenamiento como deduplicación y compresión para instantáneas, minimizando los requisitos de almacenamiento.

El complemento de SnapCenter orquesta el modo inactivo de máquinas virtuales junto con los snapshots basados en hardware en las cabinas de almacenamiento de NetApp. La tecnología SnapMirror se utiliza para replicar copias de backups en sistemas de almacenamiento secundarios, incluso en el cloud.

Para obtener más información, consulte ["Documentación del plugin de SnapCenter para VMware vSphere"](#).

La integración de BlueXP habilita estrategias de backup de 3-2-1 que amplían las copias de datos en el almacenamiento de objetos en el cloud.

Para obtener más información sobre estrategias de backup 3-2-1 con BlueXP, visita ["3-2-1 Protección de](#)

datos para VMware con complemento SnapCenter y backup y recuperación de datos de BlueXP para máquinas virtuales".

---

## Cloud Insights de NetApp

NetApp Cloud Insights simplifica la observación de la infraestructura on-premises y de nube, y proporciona funcionalidades de análisis y solución de problemas para ayudar a resolver problemas complejos. Cloud Insights funciona recogiendo datos de un entorno de centro de datos y enviándolos al cloud. Esto se realiza con un software instalado localmente denominado Unidad de adquisición y con recopiladores específicos habilitados para los activos en el centro de datos.

Los activos de Cloud Insights se pueden etiquetar con anotaciones que proporcionan un método de organizar y clasificar los datos. El panel de control se puede crear utilizando una amplia variedad de widgets para mostrar los datos y se pueden crear consultas de métricas para obtener vistas tabulares detalladas de los datos.

Cloud Insights viene con un gran número de paneles de control listos para usar que ayudan a centrarse en tipos específicos de áreas problemáticas y categorías de datos.

Cloud Insights es una herramienta heterogénea diseñada para recopilar datos de una amplia gama de dispositivos. Sin embargo, existe una biblioteca de plantillas, llamada ONTAP Essentials, que permite a los clientes de NetApp empezar a trabajar rápidamente.

Si desea obtener información detallada sobre cómo empezar a usar Cloud Insights, consulte la ["Página de inicio de BlueXP y Cloud Insights de NetApp"](#).

## Cabina All-Flash SAN de NetApp con VMware vSphere 8

Autor: Josh Powell: Ingeniería de soluciones de NetApp

### Gestión del almacenamiento en bloques con las herramientas de ONTAP para VMware vSphere

Las herramientas de ONTAP para VMware permiten a los administradores gestionar el almacenamiento de NetApp directamente desde vSphere Client. ONTAP Tools permite poner en marcha y gestionar almacenes de datos, así como aprovisionar almacenes de datos VVOL.

Herramientas ONTAP permite la asignación de almacenes de datos a perfiles de capacidades de almacenamiento que determinan un conjunto de atributos del sistema de almacenamiento. Esto permite la creación de almacenes de datos con atributos específicos como el rendimiento del almacenamiento y la calidad de servicio.

Las herramientas de ONTAP incluyen los siguientes componentes:

**Virtual Storage Console (VSC):** El VSC incluye la interfaz integrada con el cliente vSphere, donde puede agregar controladores de almacenamiento, aprovisionar almacenes de datos, supervisar el rendimiento de los almacenes de datos y ver y actualizar la configuración del host ESXi.

- Proveedor VASA: \* El proveedor de API de VMware vSphere para ONTAP envía información sobre el almacenamiento utilizado por VMware vSphere al servidor vCenter, lo que permite el aprovisionamiento de almacenes de datos de VMware Virtual Volumes (vVols), la creación y el uso de perfiles de capacidad de almacenamiento, la verificación de cumplimiento y la supervisión del rendimiento.

**Adaptador de replicación de almacenamiento (SRA):** Cuando se habilita y se usa con VMware Site Recovery Manager (SRM), SRA facilita la recuperación de los almacenes de datos de vCenter Server y las

máquinas virtuales en caso de fallo, lo que permite la configuración de sitios protegidos y sitios de recuperación para recuperación ante desastres.

Para obtener más información sobre las herramientas de NetApp ONTAP para VMware, consulte ["Herramientas de ONTAP para documentación de VMware vSphere"](#).

### **Descripción general de la puesta en marcha de soluciones**

En esta solución demostraremos el uso de las herramientas ONTAP para VMware vSphere para aprovisionar almacenes de datos de VMware Virtual Volumes (VVOL) y crear una máquina virtual en un almacén de datos de VVOL.

En un almacén de datos vVols, cada disco virtual es un VVOL y se convierte en un objeto LUN nativo del sistema de almacenamiento. La integración del sistema de almacenamiento y vSphere se realiza a través del proveedor VASA (que se instala con las herramientas de ONTAP) de las API de VMware y permite al sistema de almacenamiento conocer los datos de los equipos virtuales y gestionarlos de la forma correspondiente. Las políticas de almacenamiento, definidas en vCenter Client, se utilizan para asignar y gestionar recursos de almacenamiento.

Para obtener información detallada sobre vVols con ONTAP, consulte ["Volúmenes virtuales vVols\) con ONTAP"](#).

Esta solución cubre los siguientes pasos generales:

1. Añadir un sistema de almacenamiento en Herramientas de ONTAP.
2. Crear un perfil de capacidad de almacenamiento en las herramientas de ONTAP.
3. Cree un almacén de datos vVols en Herramientas de ONTAP.
4. Cree una política de almacenamiento de máquinas virtuales en el cliente de vSphere.
5. Cree una máquina virtual nueva en el almacén de datos de VVol.

### **Requisitos previos**

En esta solución se utilizaron los siguientes componentes:

1. Cabina All-Flash SAN A400 de NetApp con ONTAP 9,13.
2. ISCSI SVM creada en la ASA con conectividad de red a los hosts ESXi.
3. Herramientas de ONTAP para VMware vSphere 9,13 (proveedor VASA habilitado de forma predeterminada).
4. Clúster 8,0 de vSphere (dispositivo de vCenter y hosts ESXi).

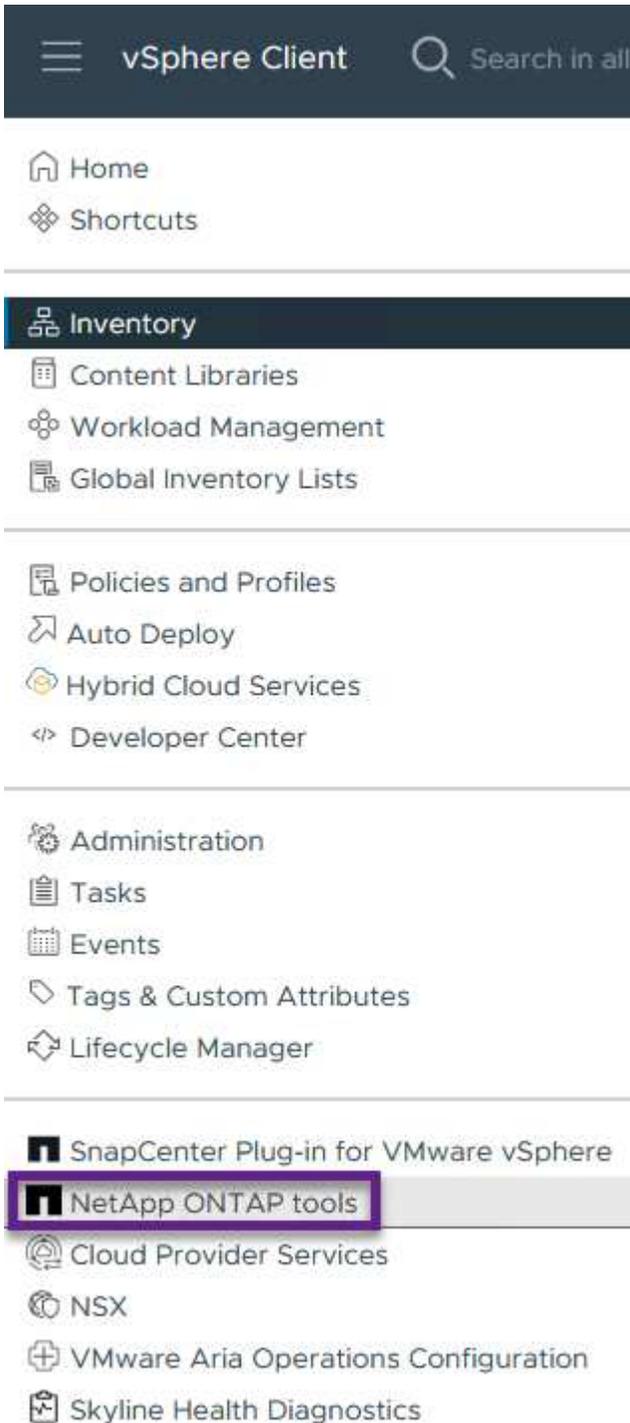
### **Puesta en marcha de la solución**

#### **Cree un almacén de datos vVols en Herramientas de ONTAP**

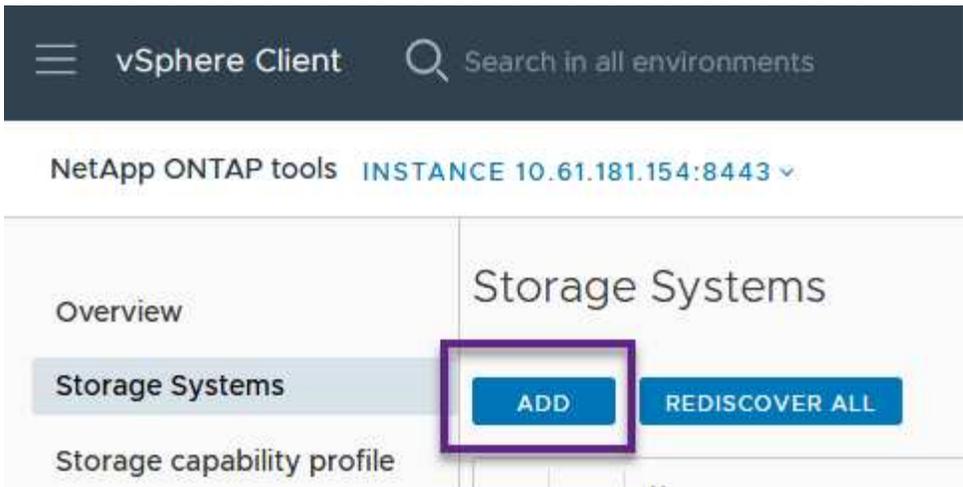
Para crear un almacén de datos vVols en Herramientas de ONTAP, lleve a cabo los siguientes pasos:

## Agregar un sistema de almacenamiento a las herramientas de ONTAP.

1. Acceda a herramientas de NetApp ONTAP seleccionándolo en el menú principal del vSphere Client.



2. En Herramientas de ONTAP seleccione **Sistemas de almacenamiento** en el menú de la izquierda y luego presione **Añadir**.



3. Rellene la dirección IP, las credenciales del sistema de almacenamiento y el número de puerto. Haga clic en **Add** para iniciar el proceso de descubrimiento.

## Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server	10.61.181.205 ▾
Name or IP address:	10.192.102.103
Username:	admin
Password:	●●●●●●●●
Port:	443

### Advanced options ^

ONTAP Cluster Certificate:  Automatically fetch  Manually upload

CANCEL

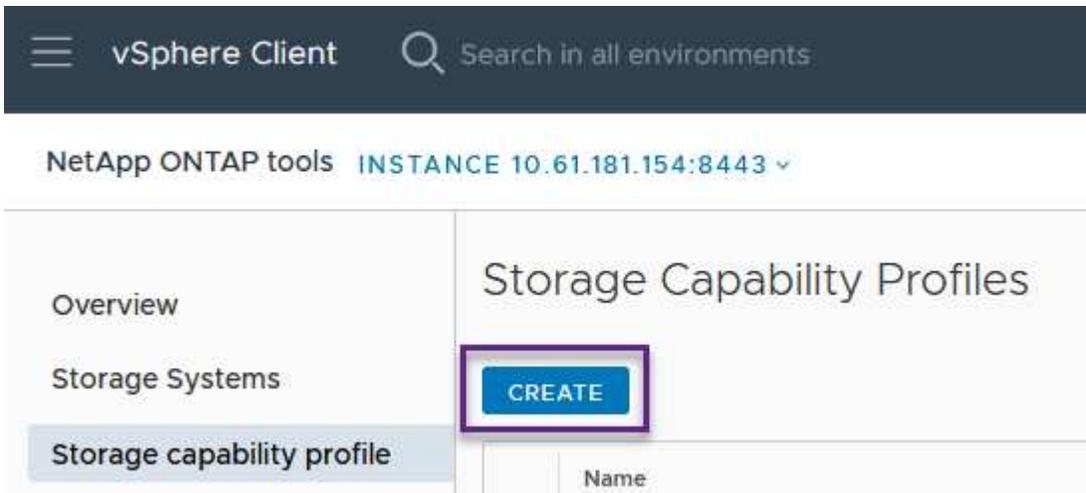
ADD

## Crear un perfil de capacidad de almacenamiento en las herramientas de ONTAP

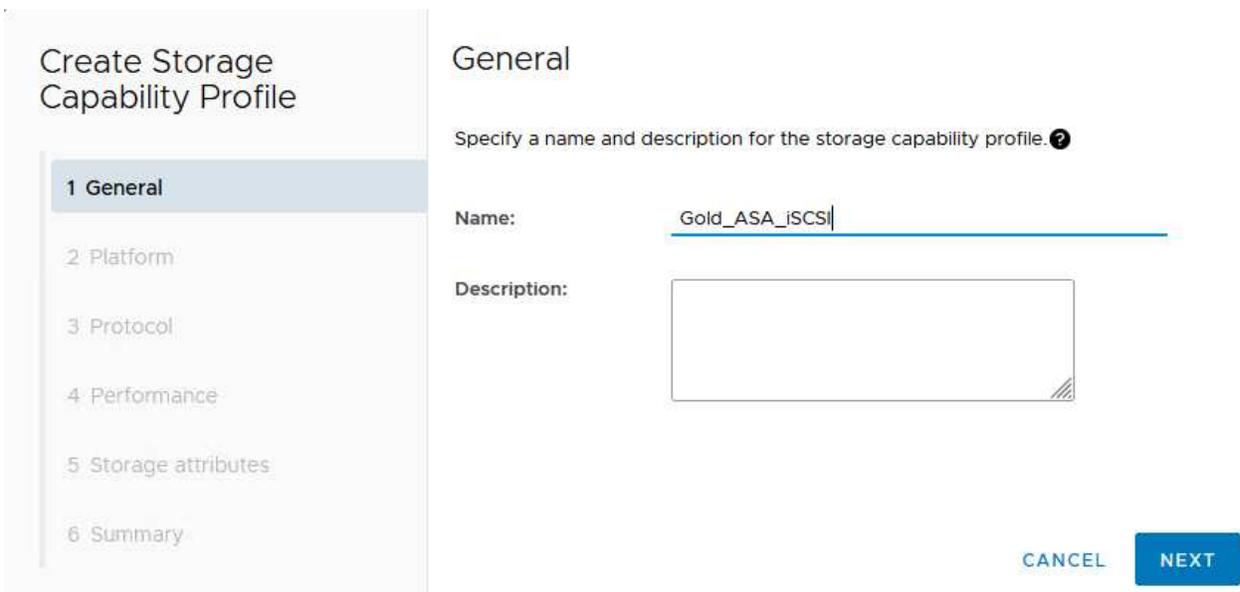
Los perfiles de funcionalidad de almacenamiento describen las funciones de una cabina de almacenamiento o un sistema de almacenamiento. Incluyen definiciones de calidad de servicio y se utilizan para seleccionar sistemas de almacenamiento que cumplan con los parámetros definidos en el perfil.

Para crear un perfil de funcionalidad del almacenamiento en las herramientas de ONTAP, complete los siguientes pasos:

1. En Herramientas de ONTAP seleccione **Perfil de capacidad de almacenamiento** en el menú de la izquierda y luego presione **Crear**.



2. En el asistente de **Crear perfil de capacidad de almacenamiento**, proporcione un nombre y una descripción del perfil y haga clic en **Siguiente**.



3. Seleccione el tipo de plataforma y especifique que el sistema de almacenamiento debe ser una cabina SAN All-Flash establecida en **asimétrica** en false.

## Create Storage Capability Profile

- 1 General
- 2 Platform**
- 3 Protocol
- 4 Performance
- 5 Storage attributes
- 6 Summary

### Platform

Platform: Performance

Asymmetric:

CANCEL

BACK

NEXT

4. A continuación, seleccione la opción de protocolo o \* cualquiera \* para permitir todos los protocolos posibles. Haga clic en **Siguiente** para continuar.

## Create Storage Capability Profile

- 1 General
- 2 Platform
- 3 Protocol**
- 4 Performance
- 5 Storage attributes
- 6 Summary

### Protocol

Protocol: Any

- Any
- FCP
- iSCSI
- NVMe/FC

CANCEL

BACK

NEXT

5. La página **PERFORMANCE** permite establecer la calidad del servicio en forma de IOPS mínima y máxima permitida.

## Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

## Performance

None ⓘ

QoS policy group ⓘ

Min IOPS:

\_\_\_\_\_

Max IOPS:

6000

Unlimited

CANCEL

BACK

NEXT

6. Complete la página **atributos de almacenamiento** seleccionando eficiencia de almacenamiento, reserva de espacio, cifrado y cualquier política de organización en niveles según sea necesario.

## Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

## Storage attributes

Deduplication:

Yes

Compression:

Yes

Space reserve:

Thin

Encryption:

No

Tiering policy (FabricPool):

None

CANCEL

BACK

NEXT

7. Por último, revise el resumen y haga clic en Finalizar para crear el perfil.

## Create Storage Capability Profile

- 1 General
- 2 Platform
- 3 Protocol
- 4 Performance
- 5 Storage attributes
- 6 Summary**

## Summary

Name:	ASA_Gold
Description:	N/A
Platform:	Performance
Asymmetric:	No
Protocol:	Any
Max IOPS:	6000 IOPS
Space reserve:	Thin
Deduplication:	Yes
Compression:	Yes
Encryption:	No
Tiering policy (FabricPool):	None

CANCEL

BACK

FINISH

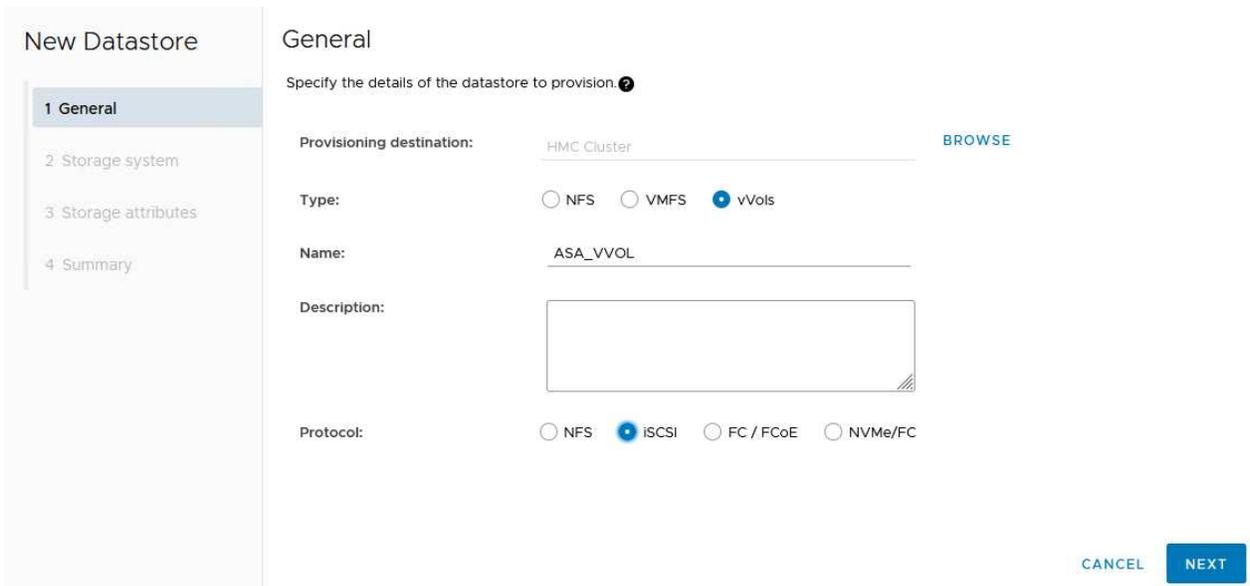
## Cree un almacén de datos vVols en Herramientas de ONTAP

Para crear un almacén de datos vVols en Herramientas de ONTAP, lleve a cabo los siguientes pasos:

1. En Herramientas de ONTAP seleccione **Descripción general** y en la pestaña **Introducción** haga clic en **Provisión** para iniciar el asistente.



2. En la página **General** del asistente New Datastore, seleccione el centro de datos de vSphere o el destino del clúster. Seleccione **vVols** como tipo de datastore, rellene un nombre para el almacén de datos y seleccione el protocolo.



3. En la página **Sistema de almacenamiento**, seleccione el perfil de capacidad de almacenamiento, el sistema de almacenamiento y SVM. Haga clic en **Siguiente** para continuar.

## New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

## Storage system

Specify the storage capability profiles and the storage system you want to use.

Storage capability profiles:

FAS\_Default  
FAS\_Max20  
**Custom profiles**  
Gold\_ASA\_JSCSI  
Gold\_ASA

Storage system:

HCG-NetApp-A400-E3U03 (10.192.102.103)

Storage VM:

svml

CANCEL

BACK

NEXT

4. En la página **Atributos de almacenamiento**, seleccione crear un nuevo volumen para el almacén de datos y completar los atributos de almacenamiento del volumen que se va a crear. Haga clic en **Agregar** para crear el volumen y luego en **Siguiente** para continuar.

## New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

## Storage attributes

Specify the storage details for provisioning the datastore.

Volumes:  Create new volumes  Select volumes

Create new volumes

Name	Size	Storage Capability Profile	Aggregate
 FlexVol volumes are not added.			

Name	Size(GB) ⓘ	Storage capability profile	Aggregates	Space reserve
ASA_VVOL	2000	Gold_ASA	HCG_A400_E3u3b_NVMe	Thin

ADD

CANCEL

BACK

NEXT

5. Por último, revise el resumen y haga clic en **Finish** para iniciar el proceso de creación del almacén de datos de VVol.

### New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

### Summary

**General**

vCenter server: 10.61.181.205

Provisioning destination: HMC Cluster

Datastore name: ASA\_VVOL

Datastore type: vVols

Protocol: iSCSI

Storage capability profile: Gold\_ASA

**Storage system details**

Storage system: HCG-NetApp-A400-E3U03

SVM: svm1

**Storage attributes**

New FlexVol Name	New FlexVol Size	Aggregate	Storage Capability Profile

CANCEL
BACK
FINISH

## Cree una política de almacenamiento de máquinas virtuales en el cliente de vSphere

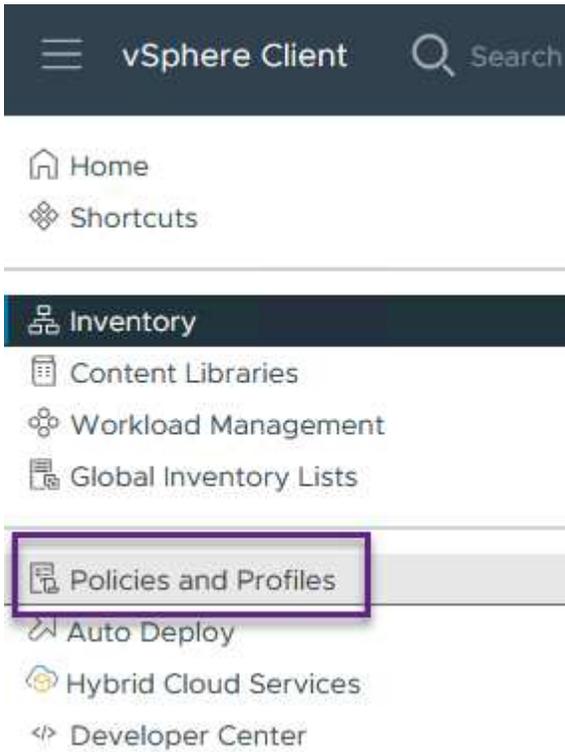
Una política de almacenamiento de máquina virtual es un conjunto de reglas y requisitos que definen cómo deben almacenarse y gestionarse los datos de máquinas virtuales (VM). Especifica las características de almacenamiento deseadas, como el rendimiento, la disponibilidad y los servicios de datos, para una máquina virtual determinada.

En este caso, la tarea implica crear una normativa de almacenamiento de máquinas virtuales para especificar que se generará una máquina virtual en almacenes de datos de VVol y establecer una asignación uno a uno con el perfil de funcionalidad de almacenamiento generado previamente.

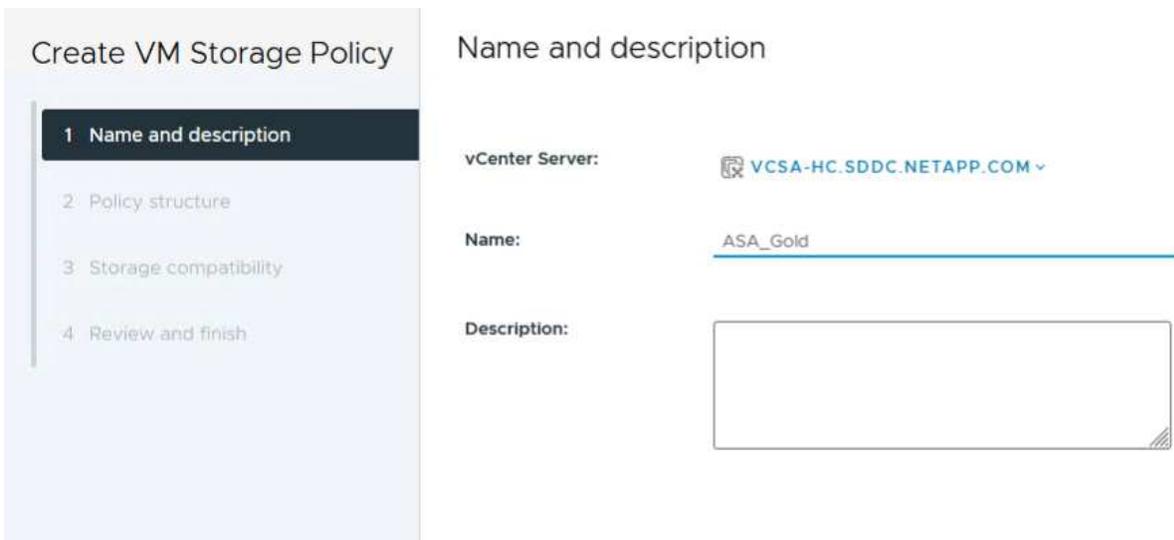
## Cree una normativa de almacenamiento de equipos virtuales

Para crear una política de almacenamiento de VM, complete los siguientes pasos:

1. En el menú principal de vSphere Clients, seleccione **Políticas y perfiles**.



2. En el asistente de **Create VM Storage Policy**, primero complete un nombre y una descripción para la política y haga clic en **Next** para continuar.

The image shows the 'Create VM Storage Policy' wizard. On the left, there is a vertical sidebar with four steps: '1 Name and description' (highlighted in dark blue), '2 Policy structure', '3 Storage compatibility', and '4 Review and finish'. The main area is titled 'Name and description' and contains three fields: 'vCenter Server:' with a dropdown menu showing 'VCSA-HC.SDDC.NETAPP.COM', 'Name:' with a text input field containing 'ASA\_Gold', and 'Description:' with a large empty text area.

3. En la página **Estructura de políticas**, seleccione habilitar las reglas para el almacenamiento de VVOL de Clustered Data ONTAP de NetApp y haga clic en **Siguiente**.

- En la siguiente página, especifica de la estructura de políticas elegida, seleccione el perfil de funcionalidad de almacenamiento que describe los sistemas de almacenamiento que se utilizarán en la normativa de almacenamiento de los equipos virtuales. Haga clic en **Siguiente** para continuar.

- En la página **Compatibilidad de almacenamiento**, revise la lista de almacenes de datos vSAN que coincidan con esta política y haga clic en **Siguiente**.
- Por último, revise la política a implementar y haga clic en **Finalizar** para crear la política.

## Cree una política de almacenamiento de máquinas virtuales en el cliente de vSphere

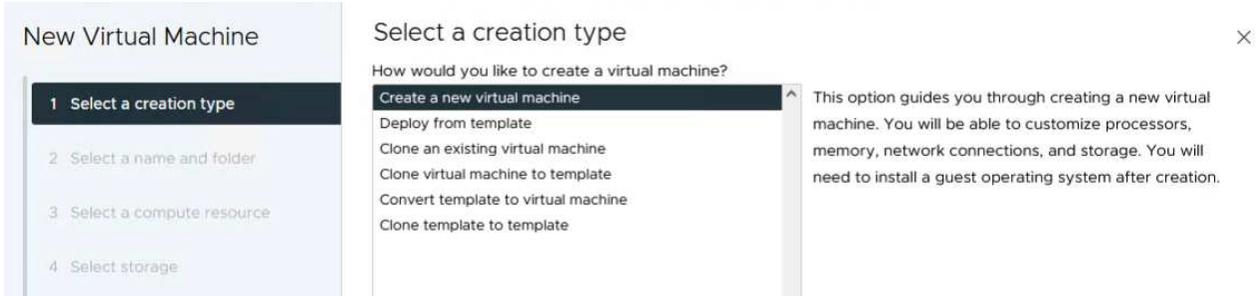
Una política de almacenamiento de máquina virtual es un conjunto de reglas y requisitos que definen cómo deben almacenarse y gestionarse los datos de máquinas virtuales (VM). Especifica las características de almacenamiento deseadas, como el rendimiento, la disponibilidad y los servicios de datos, para una máquina virtual determinada.

En este caso, la tarea implica crear una normativa de almacenamiento de máquinas virtuales para especificar que se generará una máquina virtual en almacenes de datos de VVol y establecer una asignación uno a uno con el perfil de funcionalidad de almacenamiento generado previamente.

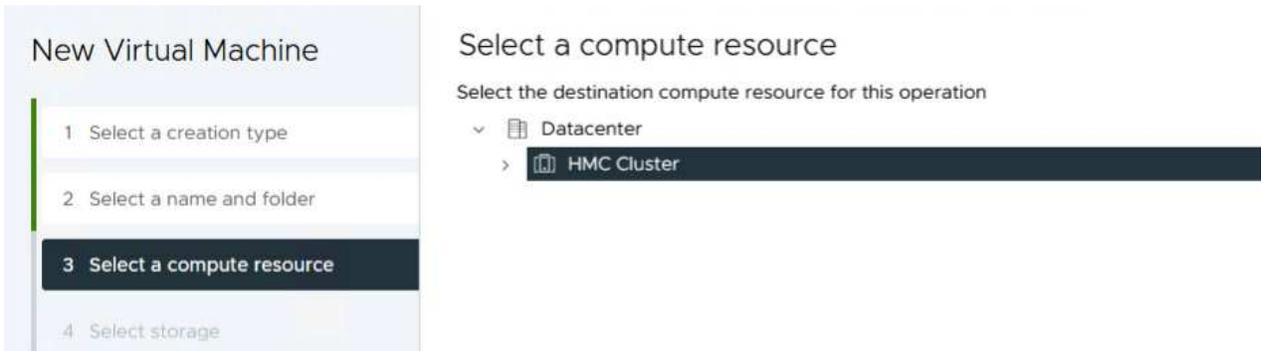
## Cree una máquina virtual en un almacén de datos de VVol

El último paso es crear una máquina virtual utilizando las políticas de almacenamiento de VM creadas previamente:

1. Desde el asistente de **Nueva máquina virtual**, selecciona **Crear una nueva máquina virtual** y selecciona **Siguiente** para continuar.



2. Introduzca un nombre y seleccione una ubicación para la máquina virtual y haga clic en **Siguiente**.
3. En la página **Seleccionar un recurso de cálculo** seleccione un destino y haga clic en **Siguiente**.



4. En la página **Select storage** seleccione una política de almacenamiento de VM y el almacén de datos vVols que será el destino de la VM. Haga clic en **Siguiente**.

## New Virtual Machine

- 1 Select a creation type
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Select storage**
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

## Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine [?](#)

VM Storage Policy ASA\_Gold ▾

Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	ASA_VVOLS_1	Compatible	1.95 TB	9 MB	1.95 TB	V
<input type="radio"/>	ASA400_ISCSI01	Incompatible	2 TB	185.32 GB	1.9 TB	V
<input type="radio"/>	DemoDS	Incompatible	800 GB	6.99 GB	793.01 GB	N
<input type="radio"/>	destination	Incompatible	250 GB	32.66 MB	249.97 GB	N
<input type="radio"/>	DRaaSTest	Incompatible	1 TB	133.27 GB	956.83 GB	N
<input type="radio"/>	esxi-hc-01 local	Incompatible	349.25 GB	1.41 GB	347.84 GB	V
<input type="radio"/>	esxi-hc-02 local	Incompatible	349.25 GB	1.41 GB	347.84 GB	V
<input type="radio"/>	esxi-hc-03 local	Incompatible	349.25 GB	1.41 GB	347.84 GB	V

Manage Columns      Items per page: 10      1 - 10 of 15 items      1 / 2

Compatibility

Validating...

CANCEL

BACK

NEXT

5. En la página **Seleccionar compatibilidad**, seleccione las versiones de vSphere con las que será compatible la VM.
6. Seleccione la familia y la versión del SO invitado para la nueva VM y haga clic en **Next**.
7. Rellene la página **Personalizar hardware**. Tenga en cuenta que puede seleccionarse una normativa de almacenamiento de equipos virtuales independiente para cada disco duro (archivo VMDK).

### New Virtual Machine

- 1 Select a creation type
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Select storage
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

### Customize hardware

Configure the virtual machine hardware

Virtual Hardware   VM Options   Advanced Parameters

ADD NEW DEVICE ▾

> CPU *	4	i
> Memory *	32	GB ▾
> New Hard disk *	150	GB ▾

<b>Maximum Size</b>	1.95 TB
<b>VM storage policy</b>	ASA_Gold ▾
<b>Location</b>	Store with the virtual machine ▾
<b>Disk Provisioning</b>	Thin Provision ▾
<b>Sharing</b>	Unspecified ▾
<b>Disk Mode</b>	Dependent ▾
<b>Virtual Device Node</b>	New SCSI controller ▾   SCSI(0:0) New Hard disk ▾
> New SCSI controller	LSI Logic SAS
> New Network	VM Network ▾ <input checked="" type="checkbox"/> Connected

CANCEL
BACK
NEXT

8. Por último, revise la página de resumen y haga clic en **Finish** para crear la VM.

En resumen, Herramientas de NetApp ONTAP automatiza el proceso de creación de almacenes de datos VVOL en sistemas de almacenamiento de ONTAP. Los perfiles de funcionalidades de almacenamiento no solo definen los sistemas de almacenamiento que deben usarse para la creación de almacenes de datos, sino que también dictan las políticas de calidad de servicio que se pueden implementar sobre una base individual de VMDK. VVols proporciona un paradigma de gestión del almacenamiento simplificado y una estrecha integración entre NetApp y VMware hacen de esta solución una solución práctica para un control optimizado, eficiente y granular sobre entornos virtualizados.

## Cabina All-Flash SAN de NetApp con VMware vSphere 8

Autor: Josh Powell: Ingeniería de soluciones de NetApp

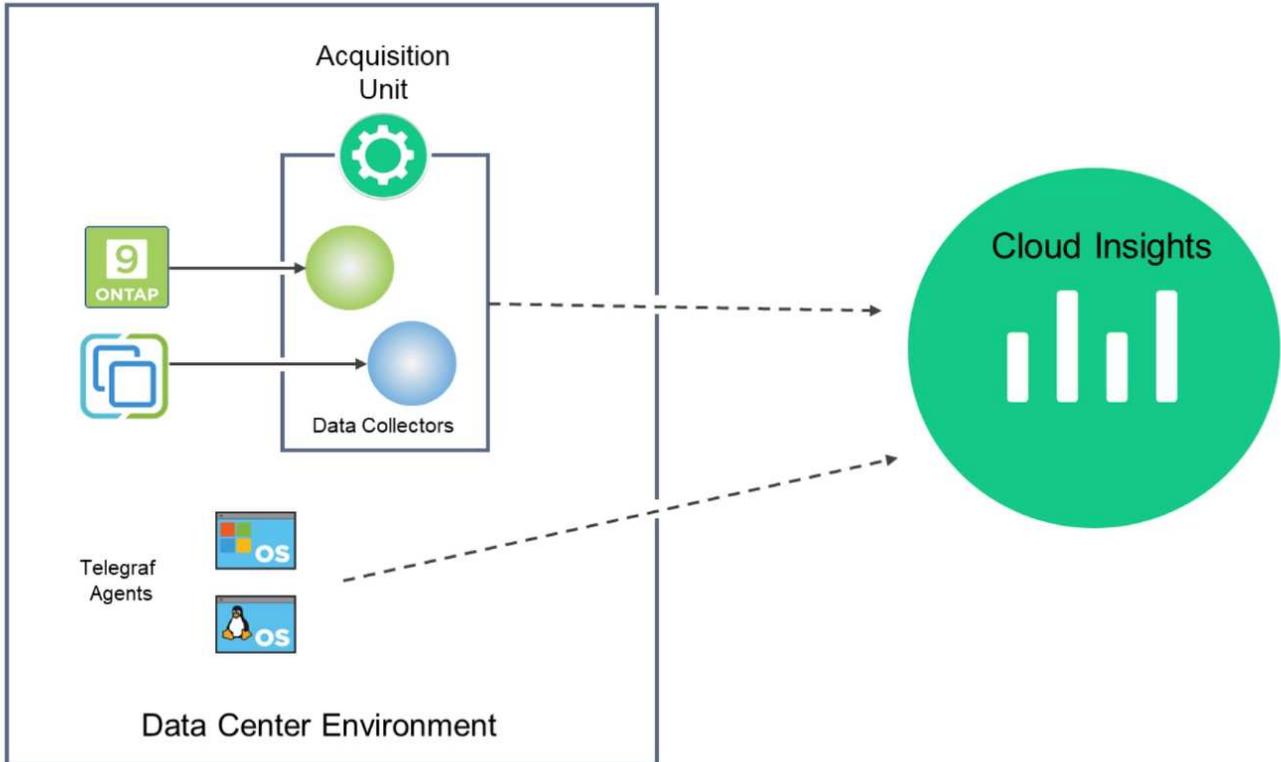
### Supervisión del almacenamiento en las instalaciones con NetApp Cloud Insights

NetApp Cloud Insights es una plataforma de supervisión y análisis de infraestructuras basada en la nube diseñada para proporcionar una visibilidad e información exhaustiva sobre el rendimiento, el estado y los costes de las INFRAESTRUCTURAS TECNOLÓGICAS, tanto on-premises como en la nube. Las funciones clave de NetApp Cloud Insights incluyen supervisión en tiempo real, consolas personalizables, análisis predictivo y herramientas de optimización de costes, lo que permite a las organizaciones gestionar y optimizar con eficiencia sus entornos en las instalaciones y en el cloud.

NetApp Cloud Insights funciona a través del software Acquisition Unit, configurado con recopiladores de datos para activos como VMware vSphere y sistemas de almacenamiento NetApp ONTAP. Estos recolectores recopilan datos y los transmiten a Cloud Insights. A continuación, la plataforma utiliza una variedad de paneles

de control, widgets y consultas de métricas para organizar los datos en análisis perspicaces para que los usuarios los interpreten.

Diagrama de la arquitectura de Cloud Insights:



### Descripción general de la puesta en marcha de soluciones

Esta solución proporciona una introducción a la supervisión de los sistemas de almacenamiento ONTAP y VMware vSphere en las instalaciones mediante NetApp Cloud Insights.

Esta lista proporciona los pasos generales que se tratan en esta solución:

1. Configure el recopilador de datos para un clúster de vSphere.
2. Configurar el Recopilador de datos para un sistema de almacenamiento de ONTAP
3. Utilice reglas de anotación para etiquetar activos.
4. Explorar y correlacionar activos.
5. Utilice una consola Top VM Latency para aislar los vecinos ruidosos.
6. Identifique oportunidades para ajustar el tamaño de los equipos virtuales.
7. Utilice consultas para aislar y ordenar métricas.

### Requisitos previos

Esta solución usa los siguientes componentes:

1. Cabina All-Flash SAN A400 de NetApp con ONTAP 9,13.
2. Clúster de vSphere 8,0 de VMware.

3. Cuenta de NetApp Cloud Insights.
4. Software de unidad de adquisición NetApp Cloud Insights instalado en una VM local con conectividad de red a activos para la recopilación de datos.

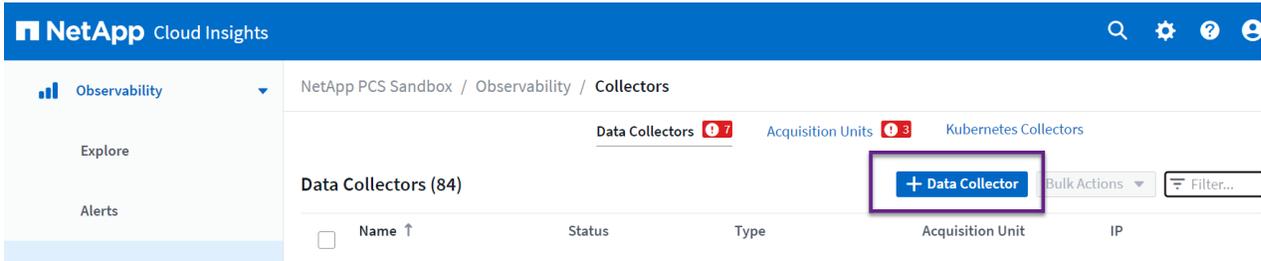
#### **Puesta en marcha de la solución**

#### **Configurar colectores de datos**

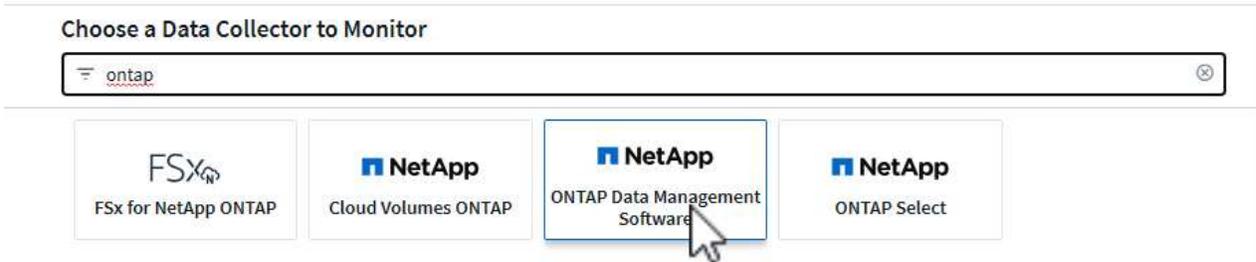
Para configurar los recopiladores de datos para los sistemas de almacenamiento VMware vSphere y ONTAP, lleve a cabo los siguientes pasos:

## Agregar un recopilador de datos para un sistema de almacenamiento de ONTAP

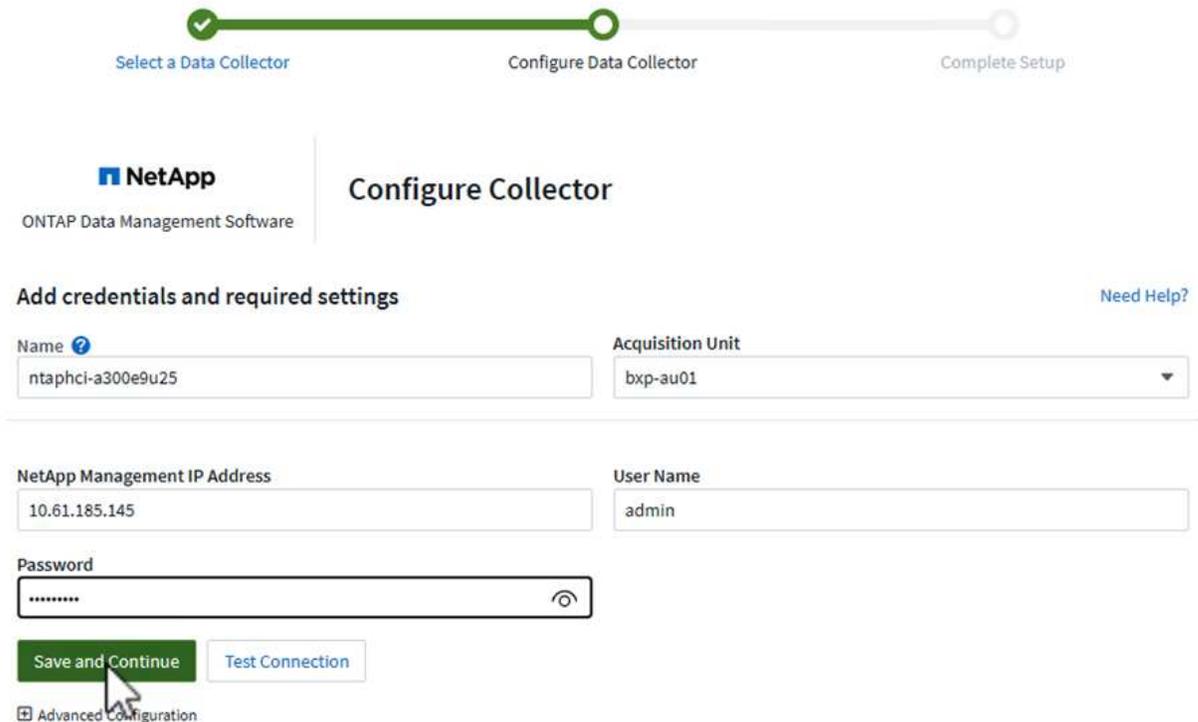
1. Una vez que haya iniciado sesión en Cloud Insights, vaya a **Observabilidad > Recopiladores > Recopiladores de datos** y pulse el botón para instalar un nuevo Recopilador de datos.



2. Desde aquí busque **ONTAP** y haga clic en **Software de gestión de datos ONTAP**.

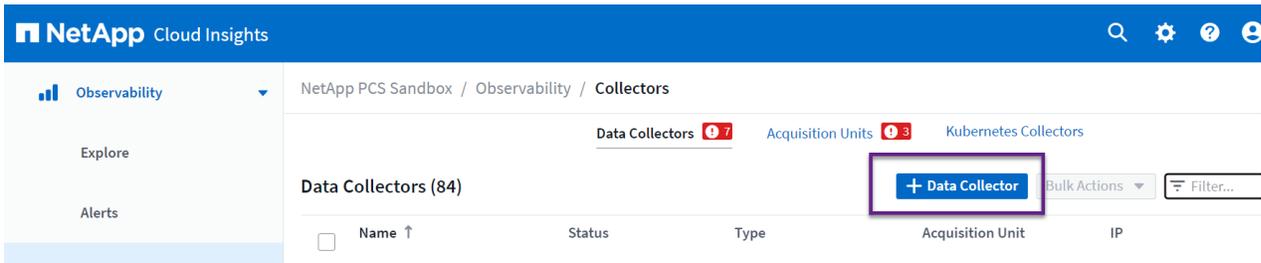


3. En la página **Configurar recopilador**, rellene un nombre para el recopilador, especifique la **Unidad de adquisición** correcta y proporcione las credenciales para el sistema de almacenamiento ONTAP. Haga clic en **Guardar y continuar** y luego en **Completar configuración** en la parte inferior de la página para completar la configuración.

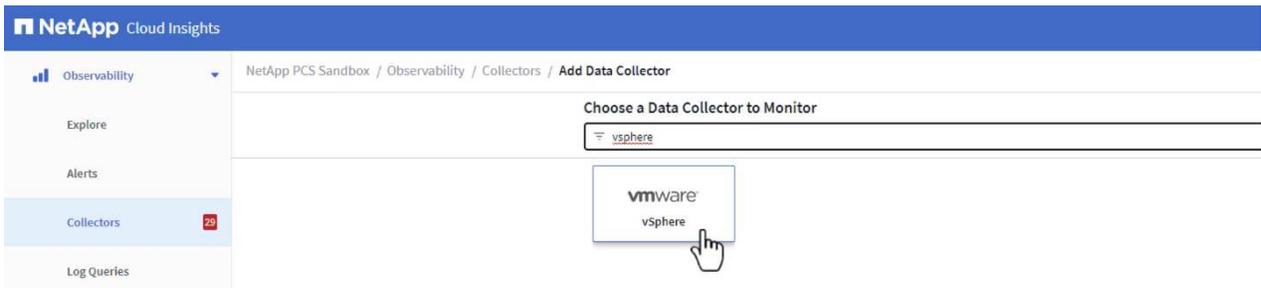


## Añadir un recopilador de datos para un clúster de VMware vSphere

1. Una vez más, navegue hasta **Observabilidad > Recopiladores > Recopiladores de datos** y pulse el botón para instalar un nuevo Recopilador de datos.



2. Desde aquí busca **vsphere** y haz clic en **vmware vsphere**.



3. En la página **Configure Collector**, rellene un nombre para el recopilador, especifique la **Acquisition Unit** correcta y proporcione las credenciales para el servidor vCenter. Haga clic en **Guardar y continuar** y luego en **Completar configuración** en la parte inferior de la página para completar la configuración.



## Configure Collector

### Add credentials and required settings

[Need Help?](#)

Name <a href="#">?</a> VCSA7	Acquisition Unit bxp-au01
---------------------------------	------------------------------

Virtual Center IP Address 10.61.181.210	User Name administrator@vsphere.local
--	--

Password *****
-------------------

<input type="button" value="Complete Setup"/>	<input type="button" value="Test Connection"/>
---	--

#### Advanced Configuration

##### Collecting:

- Inventory
- VM Performance

Inventory Poll Interval (min) 20	Communication Port 443
-------------------------------------	---------------------------

Filter VMs by ESX_HOST	Choose 'Exclude' or 'Include' to Specify a List Exclude
---------------------------	--

Filter Device List (Comma Separated Values For Filtering By ESX_HOST, CLUSTER, and DATACENTER Only)	Performance Poll Interval (sec) 300
---	--

 Collect basic performance metrics only

<input type="button" value="Complete Setup"/>	<input type="button" value="Test Connection"/>
---	--

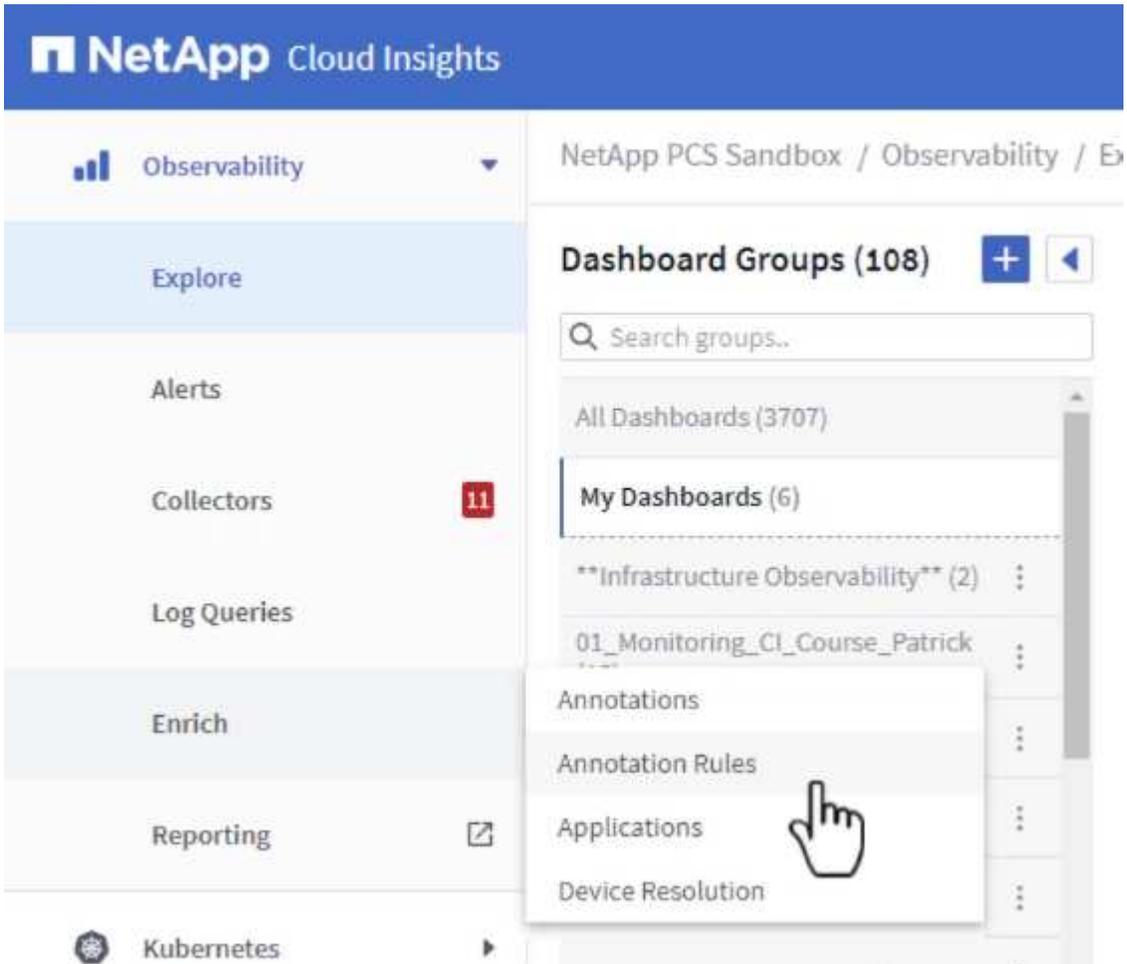
## Agregar anotaciones a activos

Las anotaciones son un método útil para etiquetar activos para que se puedan filtrar e identificar de otro modo en las distintas vistas y consultas de métricas disponibles en Cloud Insights.

En esta sección, se agregarán anotaciones a los activos de las máquinas virtuales para filtrarlos por **Data Center**.

## Utilice reglas de anotación para etiquetar activos

1. En el menú de la izquierda, navegue hasta **Observabilidad > Enriquecimiento > Reglas de anotación** y haga clic en el botón **+ Regla** en la parte superior derecha para agregar una nueva regla.



2. En el cuadro de diálogo **Agregar regla**, rellene un nombre para la regla, localice una consulta a la que se aplicará la regla, el campo de anotación afectado y el valor que se va a rellenar.

**Add Rule**
✕

**Name**

**Query**

**Annotation**

**Value**

- Por último, en la esquina superior derecha de la página **Reglas de anotación** haga clic en **Ejecutar todas las reglas** para ejecutar la regla y aplicar la anotación a los activos.

NetApp PCS Sandbox / Observability / Enrich / **Annotation Rules**

Rules running... **Run All Rules**

**Annotation rules (217)** + Rule Filter...

Name	Resource Type	Query	Annotation	Value
Annotate Tier 1 Storage Pools	Storage Pool	Find Storage Pools (no aggro) for Tier...	Tier	Tier 1
Annotate Tier 2 Storage Pools	Storage Pool	Find Storage Pools (no aggro) for Tier...	Tier	Tier 2

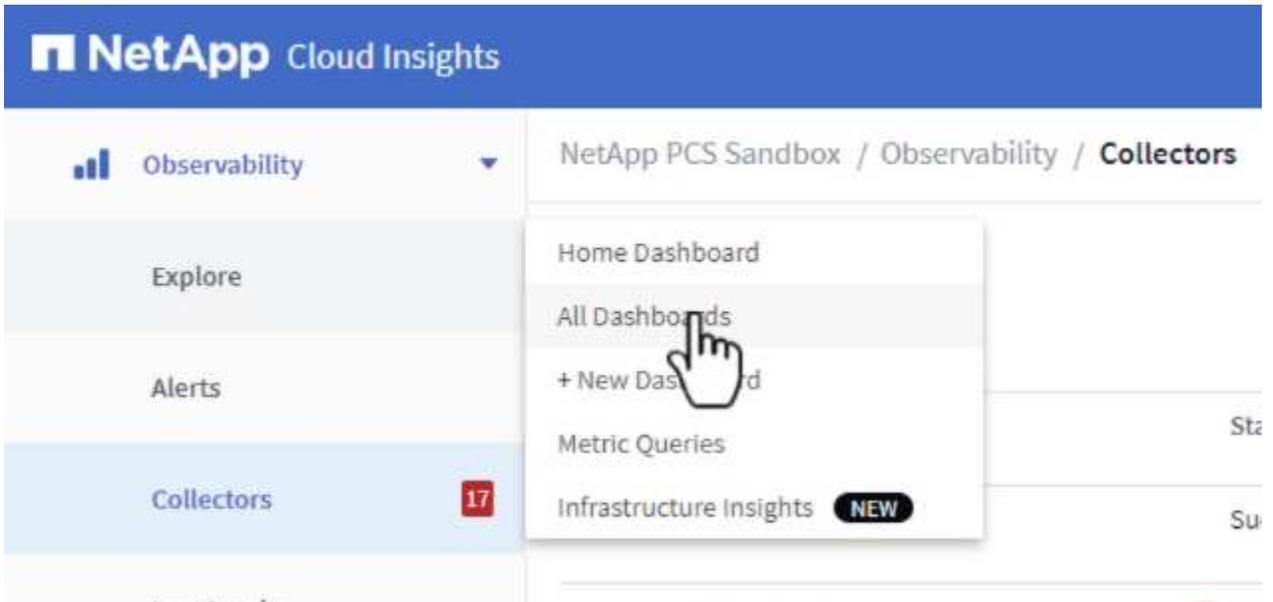
### Explorar y correlacionar activos

Cloud Insights saca conclusiones lógicas sobre los activos que se ejecutan juntos en los sistemas de almacenamiento y clústeres de vsphere.

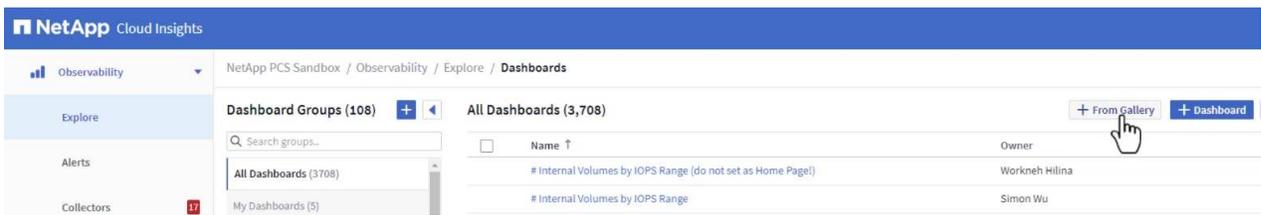
En esta sección se muestra cómo utilizar paneles de control para correlacionar activos.

## Correlación de activos de una consola de rendimiento del almacenamiento

1. En el menú de la izquierda, navegue hasta **Observabilidad > Explorar > Todos los paneles**.



2. Haga clic en el botón **+ From Gallery** para ver una lista de los paneles de control ya preparados que se pueden importar.



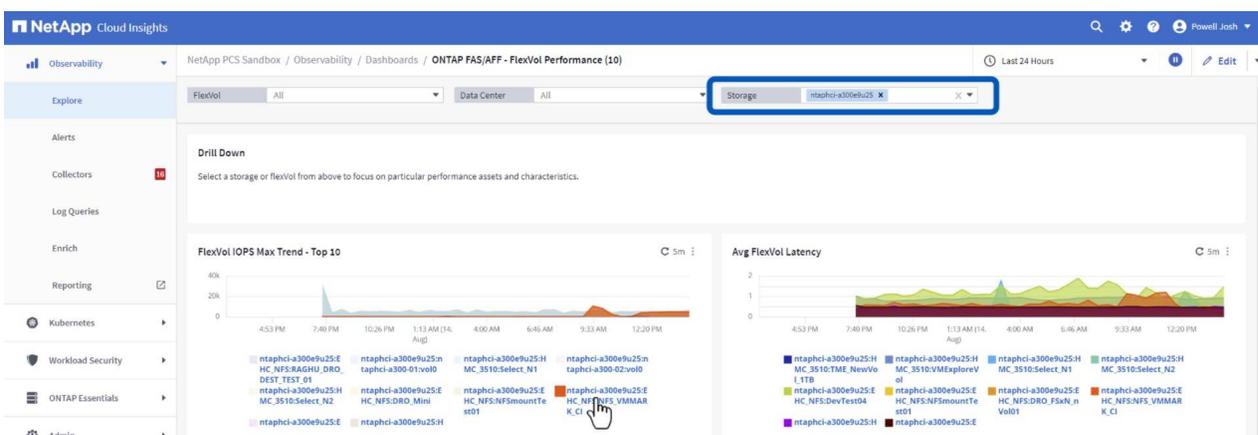
3. Elija un panel de control para el rendimiento de FlexVol de la lista y haga clic en el botón **Agregar paneles de control** en la parte inferior de la página.

- ONTAP FAS/AFF - Cluster Capacity
- ONTAP FAS/AFF - Efficiency
- ONTAP FAS/AFF - FlexVol Performance
- ONTAP FAS/AFF - Node Operational/Optimal Points
- ONTAP FAS/AFF - PrePost Capacity Efficiencies
- Storage Admin - Which nodes are in high demand?
- Storage Admin - Which pools are in high demand?
- StorageGRID - Capacity Summary
- StorageGRID - ILM Performance Monitoring
- StorageGRID - MetaData Usage
- StorageGRID - S3 Performance Monitoring
- VMware Admin - ESX Hosts Overview
- VMware Admin - Overview
- VMware Admin - VM Performance
- VMware Admin - Where are opportunities to right size?
- VMware Admin - Where can I potentially reclaim waste?
- VMware Admin - Where do I have VM Latency?

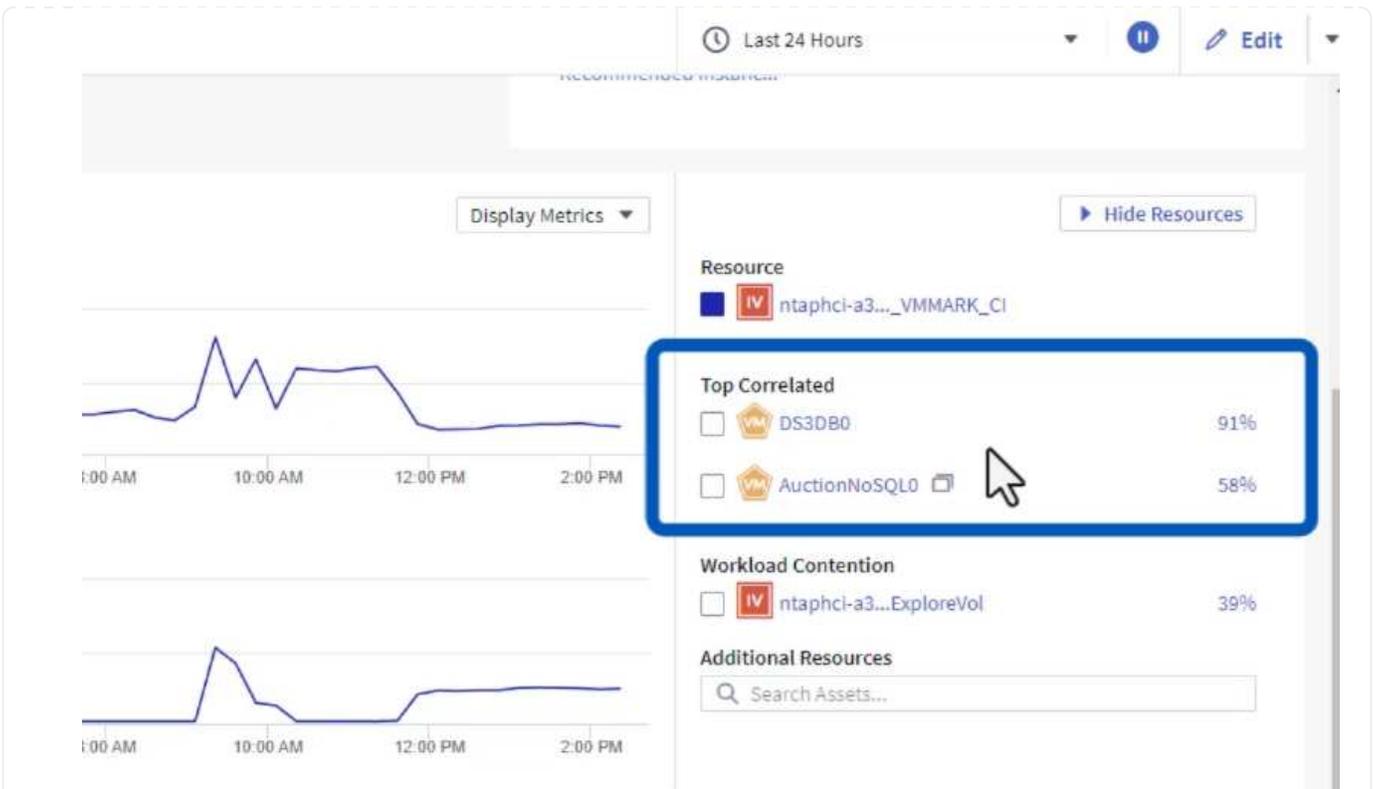
**+ Additional Dashboards (13)**  
 These dashboards require additional data collectors to be installed. [Add More](#)

Add Dashboards Go Back

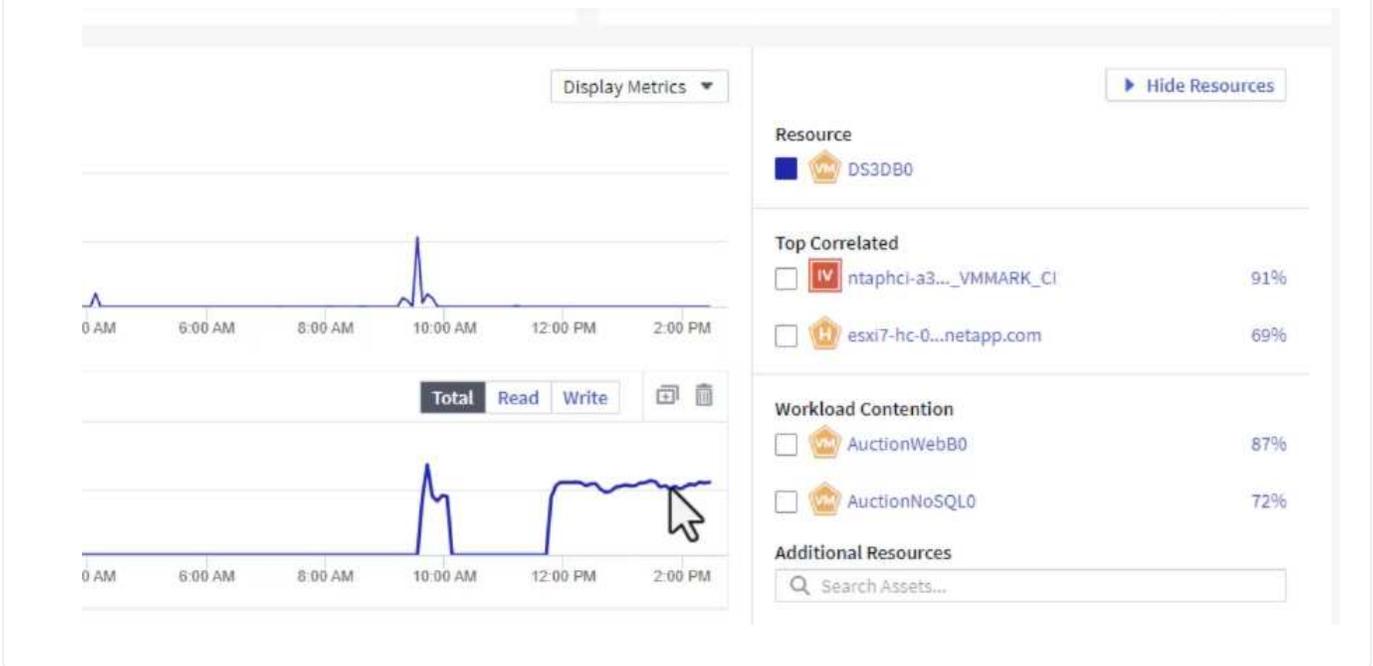
4. Una vez importado, abra el panel de control. Desde aquí puede ver varios widgets con datos de rendimiento detallados. Añada un filtro para ver un único sistema de almacenamiento y seleccione un volumen de almacenamiento para examinar sus detalles.



5. Desde esta vista, se pueden observar diferentes métricas relacionadas con este volumen de almacenamiento y los equipos virtuales más utilizados y correlacionados que se ejecutan en el volumen.



6. Al hacer clic en el VM con la mayor utilización, se profundiza en las métricas para ese VM para ver cualquier problema potencial.



### Use Cloud Insights para identificar los vecinos ruidosos

Cloud Insights incluye consolas que pueden aislar fácilmente máquinas virtuales iguales que afectan negativamente a otras máquinas virtuales que se ejecutan en el mismo volumen de almacenamiento.

## Utilice una consola Top VM Latency para aislar los vecinos ruidosos

1. En este ejemplo, acceda a un panel de control disponible en la **Galería** llamado **VMware Admin - ¿Dónde tengo la latencia de VM?**

NetApp PCS Sandbox / Observability / Explore / Dashboards

Dashboard Groups (108) + My Dashboards (6) + From Gallery + Dashboard

Search groups..

All Dashboards (3709)

My Dashboards (6)

- \*\*Infrastructure Observability\*\* (2)
- 01\_Monitoring\_CI\_Course\_Patrick (15)
- 02\_Monitoring\_CI\_Course\_Vish (5)
- 1\_Str Dashboards (8)

Name ↑	Owner
All SAN Array Status (2)	Powell Josh
Cloud Volumes ONTAP - FlexVol Performance (6)	Powell Josh
ONTAP - Volume Workload Performance (Frontend) (7)	Powell Josh
VMware Admin - Where are opportunities to right size? (37)	Powell Josh
VMware Admin - Where can I potentially reclaim waste? (11)	Powell Josh
<input checked="" type="checkbox"/> VMware Admin - Where do I have VM Latency? (9)	Powell Josh

2. A continuación, filtra por la anotación **Data Center** creada en un paso anterior para ver un subconjunto de activos.

/ VMware Admin - Where do I have VM Latency? (9) Last 3 Hours

VirtualMachine All Data Center Solutions Engineering X diskLatency.total ≥ All

! 5m Avg Latency (all hypervisors) C 5m VM Count With Latency Concern C 5m Avg Latency (all VMs)

3. Esta consola muestra una lista de las 10 máquinas virtuales principales por latencia media. A partir de aquí, haga clic en la VM de la preocupación para profundizar en sus detalles.

VM Count With Latency Concern

5m

50

VM's

Avg Latency (all VMs)

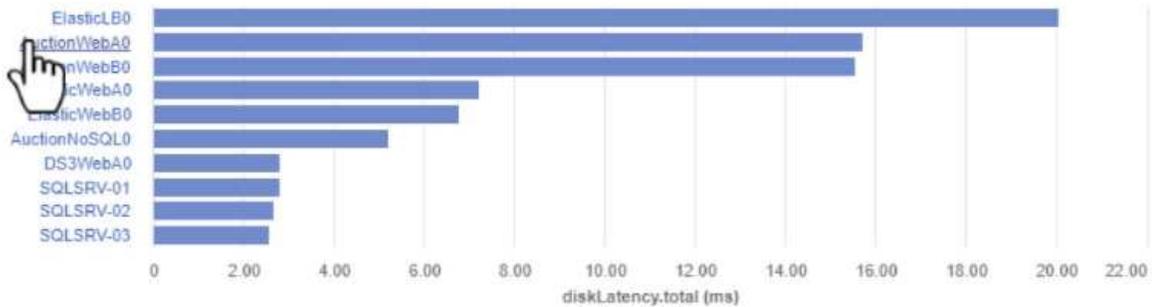
5m

1.55 ms

diskLatency.total

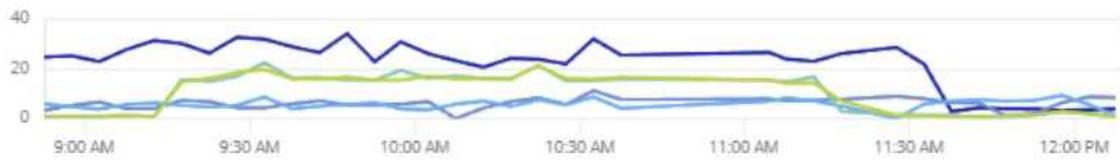
Avg VM Latency - Top 10

5m

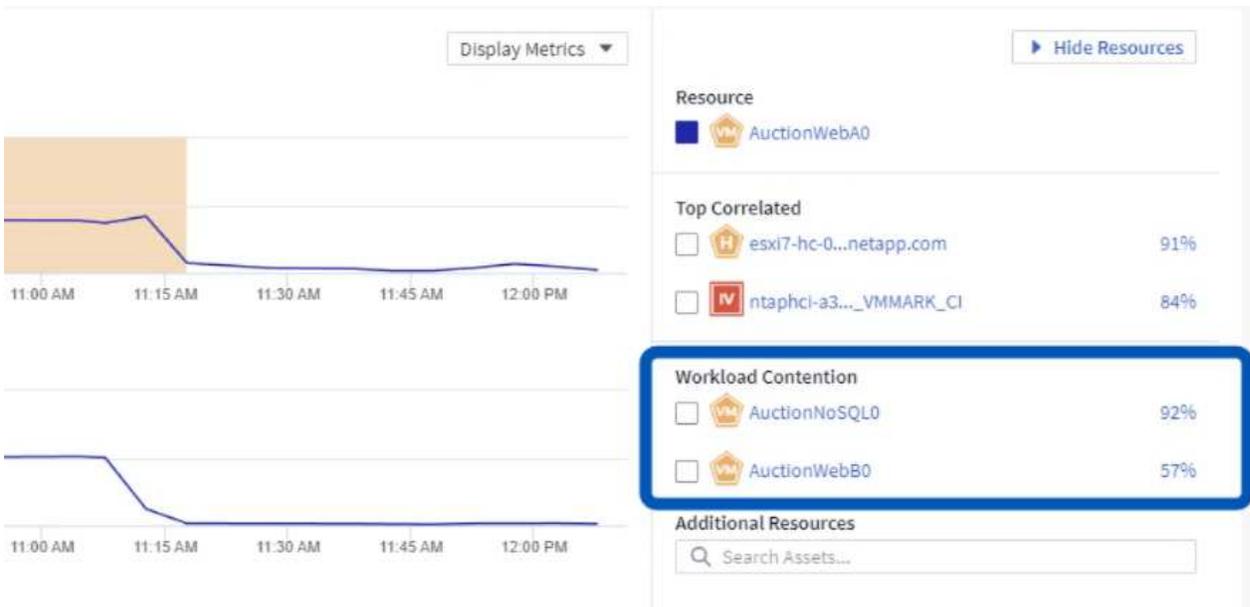


Top 5 Avg VM Latency Trend

30s



4. Las máquinas virtuales que potencialmente causan la contención de las cargas de trabajo aparecen y están disponibles. Examine estas métricas de rendimiento de las máquinas virtuales para investigar cualquier posible problema.



## **Visualice los recursos infrautilizados en Cloud Insights**

Al adecuar los recursos de las máquinas virtuales a los requisitos reales de la carga de trabajo, se puede optimizar la utilización de recursos, lo que genera ahorros de costes de la infraestructura y los servicios en cloud. Los datos de Cloud Insights se pueden personalizar para mostrar fácilmente sobre o infrautilizados equipos virtuales.

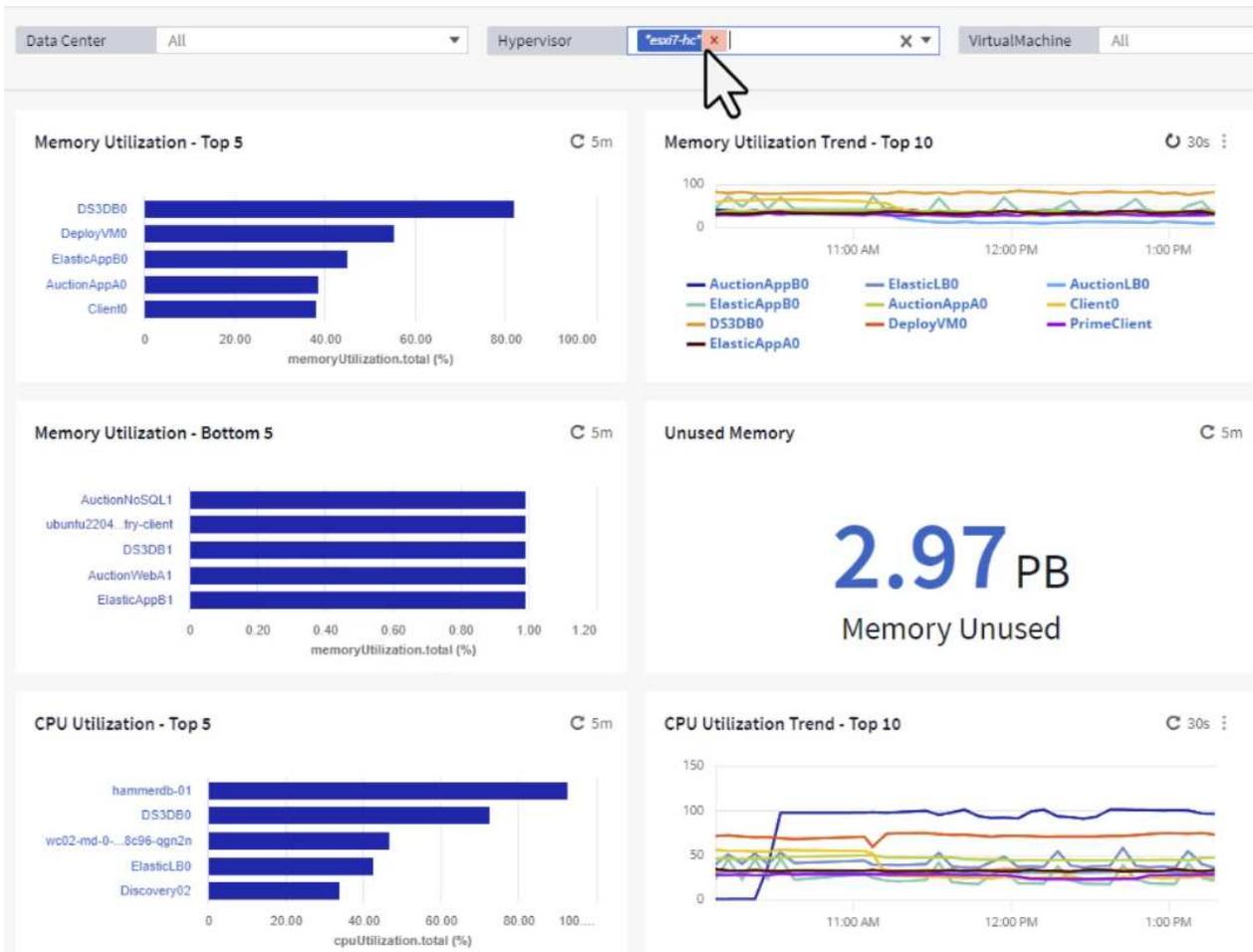
## Identifique oportunidades para ajustar el tamaño de los equipos virtuales

1. En este ejemplo, acceda a un panel de control disponible en la **Galería** llamado **VMware Admin - ¿Dónde están las oportunidades para el tamaño adecuado?**

### My Dashboards (6)

<input type="checkbox"/>	Name ↑
	<a href="#">All SAN Array Status (2)</a>
	<a href="#">Cloud Volumes ONTAP - FlexVol Performance (6)</a>
	<a href="#">ONTAP - Volume Workload Performance (Frontend) (7)</a>
<input type="checkbox"/>	<a href="#">★ <u>VMware Admin - Where are opportunities to right size? (37)</u></a>
	<a href="#">VMware Admin - Where do I potentially reclaim waste? (11)</a>
	<a href="#">VMware Admin - Where do I have VM Latency? (9)</a>

2. Primer filtro por todos los hosts ESXi del clúster. Entonces puede ver clasificación de los equipos virtuales principales e inferiores por uso de la memoria y la CPU.



3. Las tablas permiten ordenar y proporcionar más detalles en función de las columnas de datos elegidas.

## Memory Usage

5m

121 items found

Virtual Machine	memory (MiB)	memoryUt... ↓
DS3DB0	768.0	81.64
DeployVM0	92.0	55.06
ElasticAppB0	92.0	44.91
AuctionAppA0	336.0	38.42
Client0	480.0	37.98
AuctionAppB0	336.0	37.83
ElasticAppA0	92.0	35.63
ElasticLB0	96.0	35.13
user-cluster1-8872k-78c65dd794...	92.0	32.47
PrimeClient	48.0	30.30

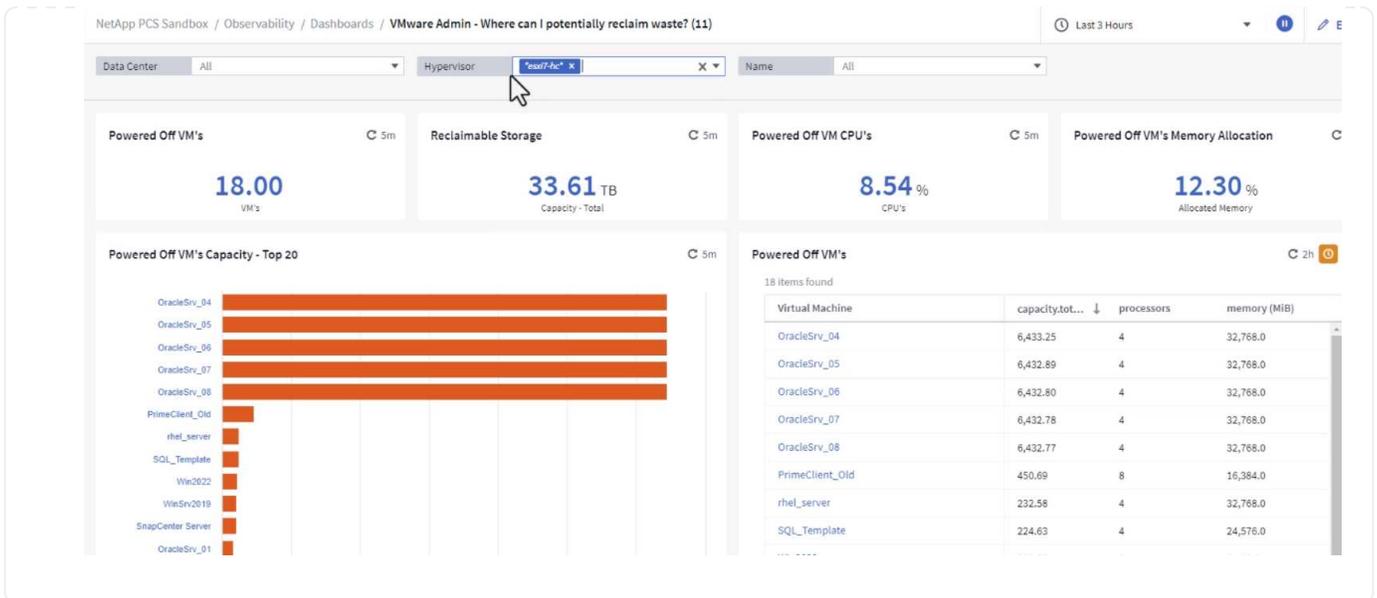
## CPU Utilization

5m

121 items found

Virtual Machine	name
hammerdb-01	hammerdb-01
DS3DB0	DS3DB0
wc02-md-0-xwdgb-8cf48c96-qgn...	wc02-md-0-xwdgb-8cf48c96-qg...
ElasticLB0	ElasticLB0

- Otro panel llamado **VMware Admin** - ¿Dónde puedo recuperar residuos? muestra VM apagadas ordenadas por su uso de capacidad.

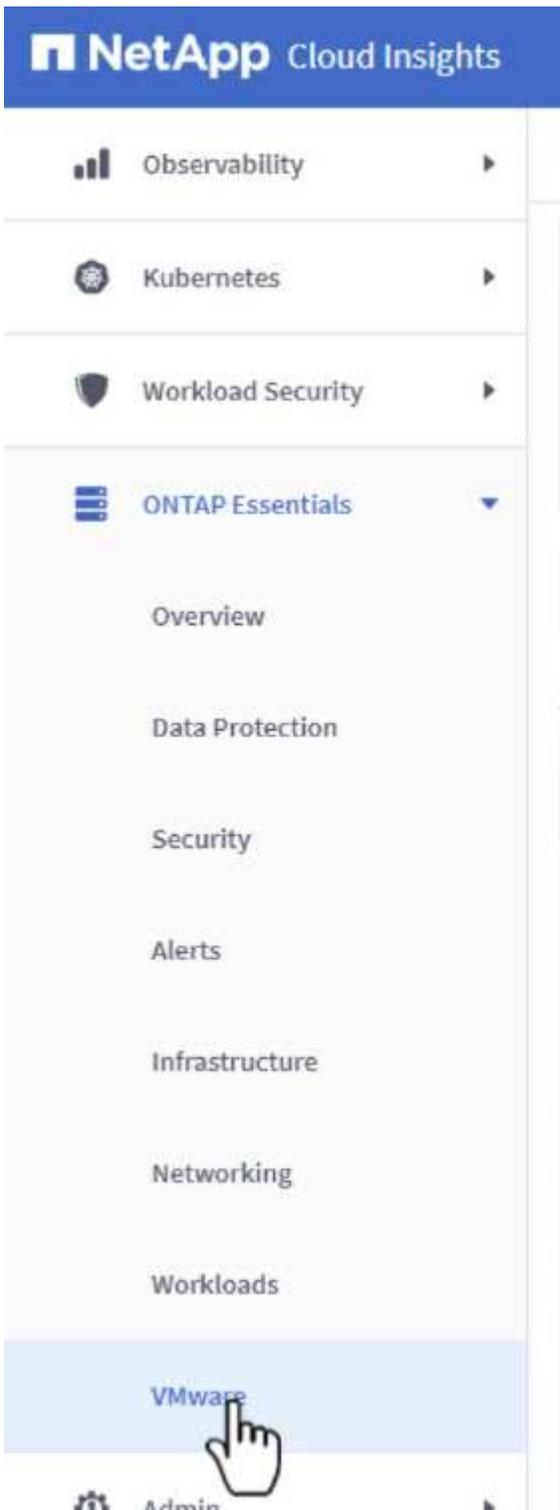


## Utilice consultas para aislar y ordenar métricas

La cantidad de datos capturados por Cloud Insights es bastante completa. Las consultas de métricas proporcionan una forma eficaz de ordenar y organizar grandes cantidades de datos de formas útiles.

## Consulte una consulta detallada de VMware en ONTAP Essentials

1. Navegue hasta **ONTAP Essentials > VMware** para acceder a una consulta de métricas de VMware completa.



2. En esta vista se le presentan varias opciones para filtrar y agrupar los datos en la parte superior. Todas las columnas de datos son personalizables y se pueden agregar columnas adicionales fácilmente.

VirtualMachine | All Virtual Machines

Filter by Attribute | storageResources.storage.vendor | NetApp | host.Los | VMware

Filter by Metric | +

Group By | Virtual Machine

Formatting: Show Expanded Details | Conditional Formatting | Background Color | Show In Range as green

281 Items found

Virtual Machine	name ↑	powerState	capacity.used (GiB)	capacity.total (GiB)	capacityRatio.us...	diskIops.total (I/O/s)	diskLatency.total...	diskThroughput...
01rfk8sprodclient	01rfk8sprodclient	On	49.38	69.86	70.68	1.21	8.13	0.01
02rfk8sprodserver	02rfk8sprodserver	On	63.64	74.06	85.93	22.80	4.13	0.11
03rfk8sprodmaster01	03rfk8sprodmaster01	On	65.13	77.21	84.36	26.64	5.64	0.20
04rfk8sprodmaster02	04rfk8sprodmaster02	On	63.89	76.27	83.77	26.82	5.14	0.16
05rfk8sprodmaster03	05rfk8sprodmaster03	On	63.77	75.58	84.38	28.23	4.63	0.17
AIQUM 9.11 (vApp)	AIQUM 9.11 (vApp)	On	152.00	152.00	100.00	23.24	0.19	0.41
AIQUM 9.12 (Linux)	AIQUM 9.12 (Linux)	On	55.28	100.00	55.28	0.01	11.83	0.00
AN-JumpHost01	AN-JumpHost01	On	90.00	90.00	100.00	1.39	0.19	0.01
AuctionAppA0	AuctionAppA0	On	9.38	16.00	58.62	1.21	0.44	0.12
AuctionAppA1	AuctionAppA1	On	6.44	16.00	40.26	0.00	3.00	0.00

## Conclusión

Esta solución se diseñó como un manual básico para aprender a comenzar a usar NetApp Cloud Insights y mostrar algunas de las potentes capacidades que puede ofrecer esta solución de observabilidad. Hay cientos de paneles de control y consultas métricas integradas en el producto, lo que facilita la puesta en marcha inmediata. La versión completa de Cloud Insights está disponible como prueba de 30 días y la versión básica está disponible de forma gratuita para los clientes de NetApp.

## Información adicional

Para obtener más información sobre las tecnologías presentadas en esta solución, consulte la siguiente información adicional.

- ["Página de inicio de BlueXP y Cloud Insights de NetApp"](#)
- ["Documentación de NetApp Cloud Insights"](#)

# Demostraciones y tutoriales

## Vídeos y demostraciones sobre virtualización

Vea los siguientes vídeos y demostraciones en los que se destacan características específicas de las soluciones de cloud híbrido, virtualización y contenedores.

### Herramientas de ONTAP de NetApp para VMware vSphere

[Herramientas de ONTAP para VMware: Información general](#)

[Aprovisionamiento de almacén de datos iSCSI de VMware con ONTAP](#)

[Aprovisionamiento del almacén de datos NFS de VMware con ONTAP](#)

## Plugin de SnapCenter para VMware vSphere

El software SnapCenter de NetApp es una plataforma empresarial fácil de usar para coordinar y administrar de un modo seguro la protección de datos en todas las aplicaciones, bases de datos y sistemas de archivos.

El plugin de SnapCenter para VMware vSphere permite ejecutar operaciones de backup, restauración y conexión para máquinas virtuales, así como operaciones de backup y montaje para almacenes de datos que se registran en SnapCenter directamente en VMware vCenter.

Para obtener más información sobre el plugin de SnapCenter para VMware vSphere, consulte ["Información general sobre el plugin de SnapCenter de NetApp para VMware vSphere"](#).

[Plugin de SnapCenter para VMware vSphere: Requisitos previos de la solución](#)

[Plugin de SnapCenter para VMware vSphere: Implementación](#)

[Plugin de SnapCenter para VMware vSphere: Flujo de trabajo de backup](#)

[Plugin de SnapCenter para VMware vSphere: Flujo de trabajo de restauración](#)

[SnapCenter - flujo de trabajo de restauración SQL](#)

## Soluciones de protección de datos 3-2-1

Las soluciones de protección de datos 3-2-1 combinan backups primarios y secundarios en las instalaciones mediante la tecnología SnapMirror y copias replicadas en almacenamiento de objetos mediante el backup y la recuperación de datos de BlueXP.

[3-2-1 Protección de datos para almacenes de datos VMFS con plugin SnapCenter para VMware vSphere y backup y recuperación de BlueXP para máquinas virtuales](#)

## VMware Cloud en AWS con AWS FSX para ONTAP de NetApp

[Almacenamiento conectado como invitado de Windows con FSX ONTAP mediante iSCSI](#)

[Almacenamiento conectado invitado de Linux con FSX ONTAP mediante NFS](#)

[Ahorro de VMware Cloud en AWS TCO con Amazon FSX para ONTAP de NetApp](#)

[VMware Cloud en un almacén de datos complementario con Amazon FSX para ONTAP de NetApp](#)

[Instalación y configuración de VMware HCX para VMC](#)

[Demostración de migración de VMotion con VMware HCX para VMC y FSxN](#)

[Demostración de migración en frío con VMware HCX para VMC y FSxN](#)

## Azure VMware Services en Azure con Azure NetApp Files (ANF)

[Descripción general adicional del almacén de datos de la solución para VMware Azure con Azure NetApp Files](#)

[Recuperación ante desastres de la solución VMware para Azure con Cloud Volumes ONTAP, SnapCenter y JetStream](#)

[Demostración de migración en frío con VMware HCX para AVS y ANF](#)

[Demostración de VMotion con VMware HCX para AVS y ANF](#)

[Demostración de migración masiva con VMware HCX para AVS y ANF](#)

## VMware Cloud Foundation con NetApp ONTAP

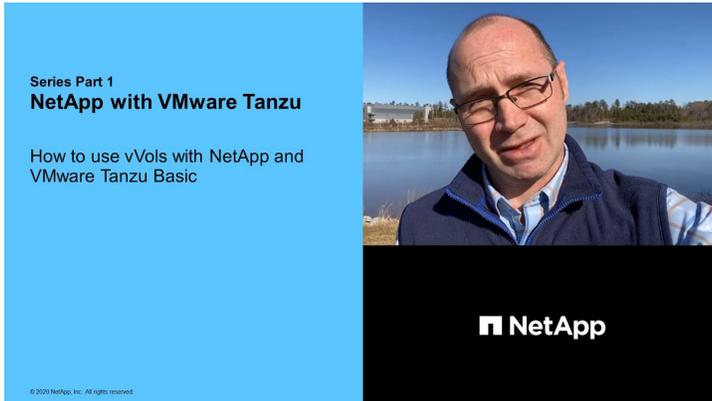
[Almacenes de datos NFS como almacenamiento principal para dominios de carga de trabajo de VCF](#)

[Almacenes de datos iSCSI como almacenamiento complementario para dominios de gestión de VCF](#)

## NetApp con VMware Tanzania

VMware Tanzania permite a los clientes poner en marcha, administrar y gestionar su entorno de Kubernetes a través de vSphere o de VMware Cloud Foundation. Esta cartera de productos de VMware permite a los clientes gestionar todos sus clústeres de Kubernetes relevantes desde un único plano de control al elegir la edición de VMware Tanzu que mejor se adapte a sus necesidades.

Si quiere más información sobre VMware Tanzania, consulte "[Descripción general de VMware Tanzania](#)". Esta revisión incluye casos de uso, adiciones disponibles y mucho más sobre VMware Tanzu.



**Cómo usar vVols con NetApp y VMware Tanzu Basic, parte 1**



**Cómo usar vVols con NetApp y VMware Tanzu Basic, parte 2**



**Cómo utilizar vVols con NetApp y VMware Tanzu Basic, parte 3**

## Cloud Insights de NetApp

NetApp Cloud Insights es una plataforma completa de análisis y supervisión diseñada para proporcionar visibilidad y control sobre tu infraestructura on-premises y en la nube.

[NetApp Cloud Insights: Observabilidad para el centro de datos moderno](#)

## Información de copyright

Copyright © 2024 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 INTERRUPTIÓN 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.