



Empezar

NetApp Disaster Recovery

NetApp

February 04, 2026

Tabla de contenidos

Empezar	1
Obtenga más información sobre NetApp Disaster Recovery para VMware	1
NetApp Console	2
Beneficios de utilizar NetApp Disaster Recovery para VMware	2
Qué puede hacer con NetApp Disaster Recovery para VMware	3
Costo	4
Licencias	4
Prueba gratuita de 30 días	5
Cómo funciona NetApp Disaster Recovery	5
Objetivos de protección y tipos de almacén de datos admitidos	7
Términos que podrían ayudarle con NetApp Disaster Recovery	8
Requisitos previos de NetApp Disaster Recovery	8
Versiones de software	8
Requisitos previos y consideraciones de Google Cloud	9
Requisitos previos de almacenamiento de ONTAP	10
Requisitos previos de los clústeres de VMware vCenter	10
Requisitos previos de la NetApp Console	10
Requisitos previos de la carga de trabajo	12
Más información	12
Inicio rápido para NetApp Disaster Recovery	12
Configure su infraestructura para NetApp Disaster Recovery	13
Nube híbrida con VMware Cloud y Amazon FSx for NetApp ONTAP	13
Nube privada	15
Acceda a NetApp Disaster Recovery	16
Configurar licencias para NetApp Disaster Recovery	18
Pruébelo utilizando una prueba gratuita de 30 días	19
Una vez finalizada la prueba, suscríbete a través de uno de los Marketplaces	20
Una vez finalizada la prueba, compre una licencia BYOL a través de NetApp	21
Actualice su licencia cuando expire	21
Finalizar la prueba gratuita	21

Empezar

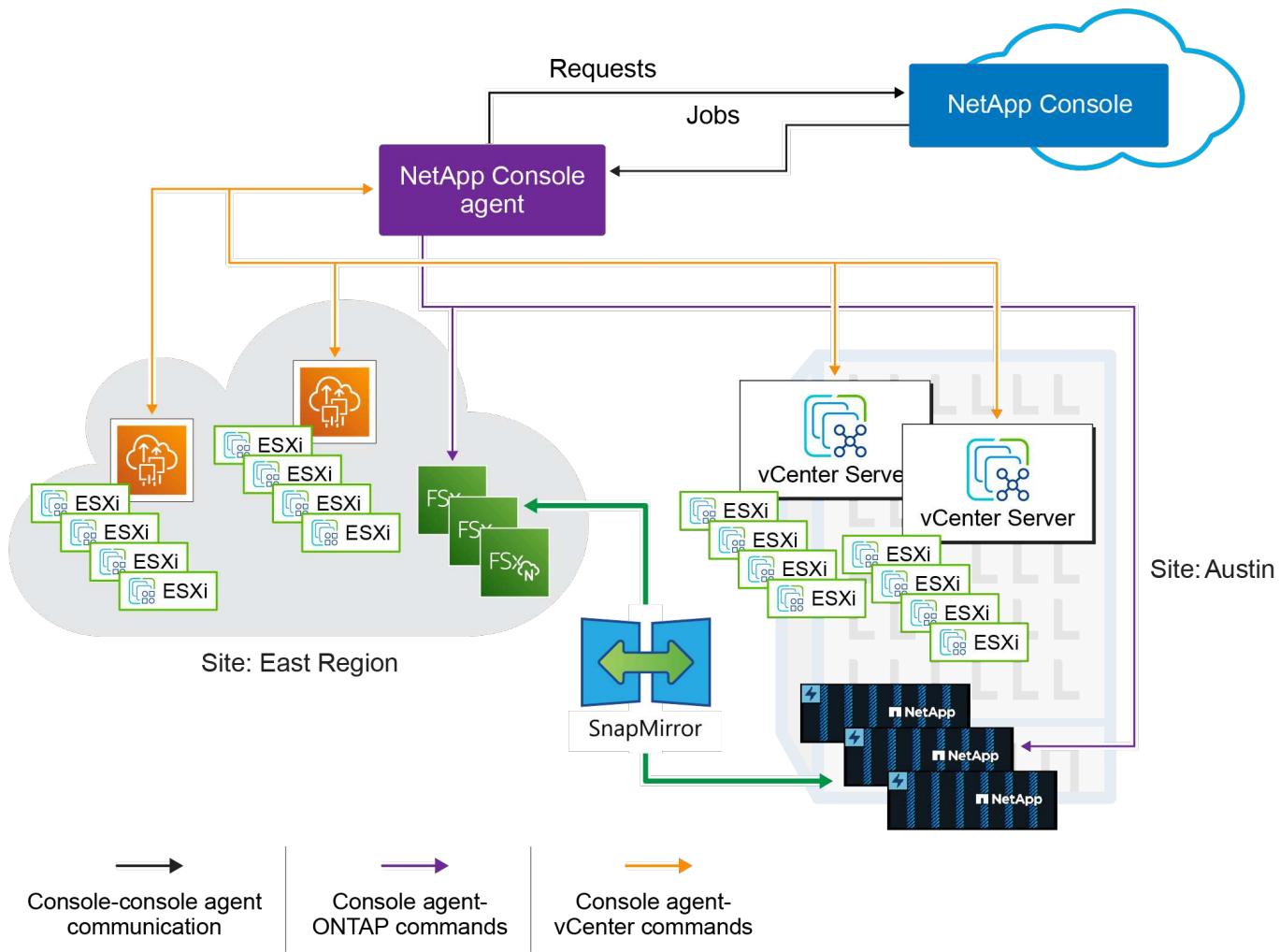
Obtenga más información sobre NetApp Disaster Recovery para VMware

La recuperación ante desastres en la nube es una forma resiliente y rentable de proteger las cargas de trabajo contra interrupciones del sitio y eventos de corrupción de datos. Con NetApp Disaster Recovery para VMware, puede replicar sus cargas de trabajo de almacén de datos o máquinas virtuales VMware locales que ejecutan almacenamiento ONTAP en un centro de datos definido por software VMware en una nube pública mediante almacenamiento en la nube de NetApp o en otro entorno VMware local con almacenamiento ONTAP como sitio de recuperación ante desastres. También puede utilizar Disaster Recovery para migrar cargas de trabajo de máquinas virtuales de un sitio a otro.

NetApp Disaster Recovery es un servicio de recuperación ante desastres basado en la nube que automatiza los flujos de trabajo de recuperación ante desastres. Con NetApp Disaster Recovery, puede proteger sus cargas de trabajo locales basadas en NFS y los almacenes de datos del sistema de archivos de máquina virtual (VMFS) VMware vSphere para iSCSI y FC que ejecutan almacenamiento NetApp en uno de los siguientes:

- Amazon Elastic VMware Service (EVS) con Amazon FSx for NetApp ONTAP Para obtener más detalles, consulte "[Introducción de NetApp Disaster Recovery mediante Amazon Elastic VMware Service y Amazon FSx for NetApp ONTAP](#)" .
- VMware Cloud (VMC) en AWS con Amazon FSx for NetApp ONTAP
- Azure VMware Solution (AVS) con NetApp Cloud Volumes ONTAP (iSCSI) (versión preliminar privada)
- Google Cloud VMware Engine (GCVE) con Google Cloud NetApp Volumes
- Otro entorno VMware local basado en NFS y/o VMFS (iSCSI/FC) con almacenamiento ONTAP

NetApp Disaster Recovery utiliza la tecnología ONTAP SnapMirror con orquestación nativa VMware integrada para proteger las máquinas virtuales VMware y sus imágenes de sistema operativo en disco asociadas, al tiempo que conserva todos los beneficios de eficiencia de almacenamiento de ONTAP. La recuperación ante desastres utiliza estas tecnologías como transporte de replicación al sitio de recuperación ante desastres. Esto permite la mejor eficiencia de almacenamiento de la industria (compresión y deduplicación) en sitios primarios y secundarios.



NetApp Console

Se puede acceder a NetApp Disaster Recovery a través de la NetApp Console.

La NetApp Console proporciona una gestión centralizada de los servicios de datos y almacenamiento de NetApp en entornos locales y en la nube a nivel empresarial. La consola es necesaria para acceder y utilizar los servicios de datos de NetApp. Como interfaz de administración, le permite administrar muchos recursos de almacenamiento desde una sola interfaz. Los administradores de la consola pueden controlar el acceso al almacenamiento y los servicios para todos los sistemas dentro de la empresa.

No necesita una licencia o suscripción para comenzar a usar NetApp Console y solo incurre en cargos cuando necesita implementar agentes de Console en su nube para garantizar la conectividad con sus sistemas de almacenamiento o servicios de datos de NetApp. Sin embargo, algunos servicios de datos de NetApp accesibles desde la consola requieren licencia o suscripción.

Obtenga más información sobre el ["NetApp Console"](#).

Beneficios de utilizar NetApp Disaster Recovery para VMware

NetApp Disaster Recovery ofrece los siguientes beneficios:

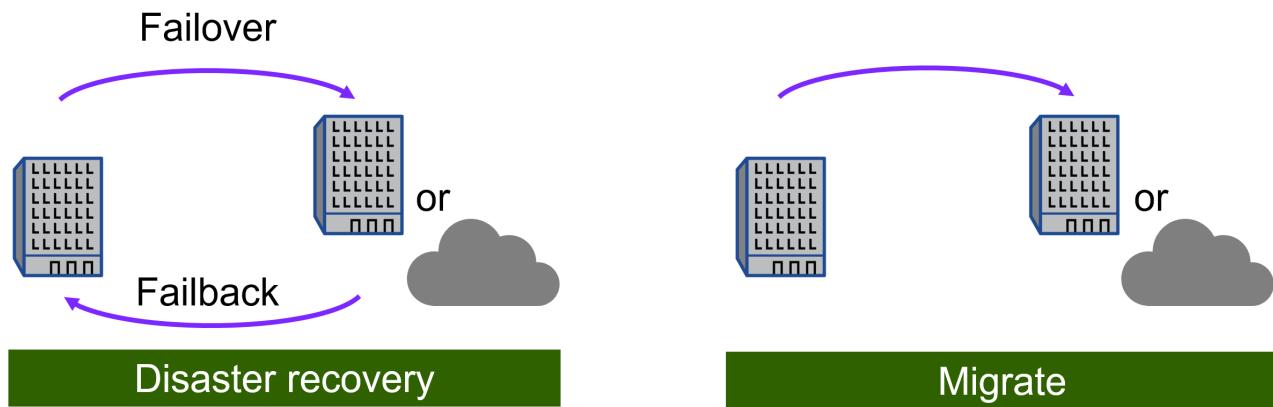
- Experiencia de usuario simplificada para el descubrimiento y la recuperación de aplicaciones de vCenter con múltiples operaciones de recuperación en puntos específicos del tiempo.

- Menor costo total de propiedad con menor costo de operaciones y capacidad de crear y ajustar planes de recuperación ante desastres con recursos mínimos.
- Preparación para la recuperación ante desastres continua con pruebas de conmutación por error virtual que no interrumpen las operaciones. Puede probar periódicamente sus planes de conmutación por error de DR sin afectar las cargas de trabajo de producción.
- Tiempos más rápidos para obtener valor con cambios dinámicos en su entorno de TI y capacidad de abordarlos en sus planes de recuperación ante desastres.
- Capacidad de administrar tanto las capas de almacenamiento como las virtuales a través de la orquestación de back-end de ONTAP y VMware al mismo tiempo sin la necesidad de contar con dispositivos de servidor virtuales (VSA) que deban implementarse y mantenerse.
- Las soluciones de recuperación ante desastres para VMware pueden consumir muchos recursos. Muchas soluciones de DR replican máquinas virtuales en la capa virtual de VMware mediante VSA, lo que puede consumir más recursos computacionales y perder la valiosa eficiencia de almacenamiento de ONTAP. Debido a que Disaster Recovery utiliza la tecnología ONTAP SnapMirror, puede replicar datos desde almacenes de datos de producción al sitio de DR utilizando nuestro modelo de replicación incremental permanente con todas las eficiencias de compresión y deduplicación de datos nativos de ONTAP.

Qué puede hacer con NetApp Disaster Recovery para VMware

NetApp Disaster Recovery le proporciona el uso completo de varias tecnologías de NetApp para lograr los siguientes objetivos:

- Replique las aplicaciones de VMware en su sitio de producción local a un sitio remoto de recuperación ante desastres en la nube o en las instalaciones mediante la replicación SnapMirror.
- Migré cargas de trabajo de VMware desde su sitio original a otro sitio.
- Realizar una prueba de conmutación por error. Al hacer esto, el servicio crea máquinas virtuales temporales. Disaster Recovery crea un nuevo volumen FlexClone a partir de la instantánea seleccionada, y un almacén de datos temporal, respaldado por el volumen FlexClone, se asigna a los hosts ESXi. Este proceso no consume capacidad física adicional en el almacenamiento ONTAP local ni en FSx para el almacenamiento ONTAP de NetApp en AWS. El volumen de origen original no se modifica y los trabajos de réplica pueden continuar incluso durante la recuperación ante desastres.
- En caso de desastre, commute su sitio principal a pedido al sitio de recuperación ante desastres, que puede ser VMware Cloud on AWS con Amazon FSx for NetApp ONTAP o un entorno VMware local con ONTAP.
- Una vez resuelto el desastre, se realiza un retorno a pedido desde el sitio de recuperación ante desastres al sitio principal.
- Agrupe máquinas virtuales o almacenes de datos en grupos de recursos lógicos para una gestión eficiente.



La configuración del servidor vSphere se realiza fuera de NetApp Disaster Recovery en vSphere Server.

Costo

NetApp no le cobra por utilizar la versión de prueba de NetApp Disaster Recovery.

NetApp Disaster Recovery se puede utilizar con una licencia de NetApp o con un plan de suscripción anual a través de Amazon Web Services.



Algunos lanzamientos incluyen una vista previa de la tecnología. NetApp no le cobrará por ninguna capacidad de carga de trabajo previsualizada. Ver "["Novedades en NetApp Disaster Recovery"](#) para obtener información sobre los últimos avances tecnológicos.

Licencias

Puede utilizar los siguientes tipos de licencia:

- Regístrese para una prueba gratuita de 30 días.
- Compre una suscripción de pago por uso (PAYGO) con Amazon Web Services (AWS) Marketplace o Microsoft Azure Marketplace. Esta licencia le permite adquirir una licencia de capacidad protegida fija sin ningún compromiso a largo plazo.
- Traiga su propia licencia (BYOL), que es un archivo de licencia de NetApp (NLF) que obtiene de su representante de ventas de NetApp. Puede utilizar el número de serie de la licencia para activar el BYOL en la NetApp Console.

Las licencias para todos los servicios de datos de NetApp se administran a través de suscripciones en la NetApp Console. Después de configurar su BYOL, podrá ver una licencia activa para el servicio en la Consola.

El servicio se licencia en función de la cantidad de datos alojados en volúmenes ONTAP protegidos. El servicio determina qué volúmenes se deben considerar para fines de licencia mediante la asignación de máquinas virtuales protegidas a sus almacenes de datos de vCenter. Cada almacén de datos está alojado en un volumen ONTAP o LUN. La capacidad utilizada informada por ONTAP para ese volumen o LUN se utiliza para determinaciones de licencias.

Los volúmenes protegidos pueden alojar muchas máquinas virtuales. Es posible que algunos no formen parte de un grupo de recursos de NetApp Disaster Recovery . De todos modos, el almacenamiento consumido por todas las máquinas virtuales en ese volumen o LUN se utiliza para la capacidad máxima de la licencia.

 Los cargos de NetApp Disaster Recovery se basan en la capacidad utilizada de los almacenes de datos en el sitio de origen cuando hay al menos una máquina virtual que tiene un plan de replicación. La capacidad para un almacén de datos comutado por error no está incluida en la capacidad asignada. En el caso de un BYOL, si los datos exceden la capacidad permitida, las operaciones en el servicio estarán limitadas hasta que obtenga una licencia de capacidad adicional o actualice la licencia en la NetApp Console.

Para obtener detalles sobre la configuración de licencias para NetApp Disaster Recovery, consulte "["Configurar la licencia de NetApp Disaster Recovery"](#) .

Prueba gratuita de 30 días

Puede probar NetApp Disaster Recovery mediante una prueba gratuita de 30 días.

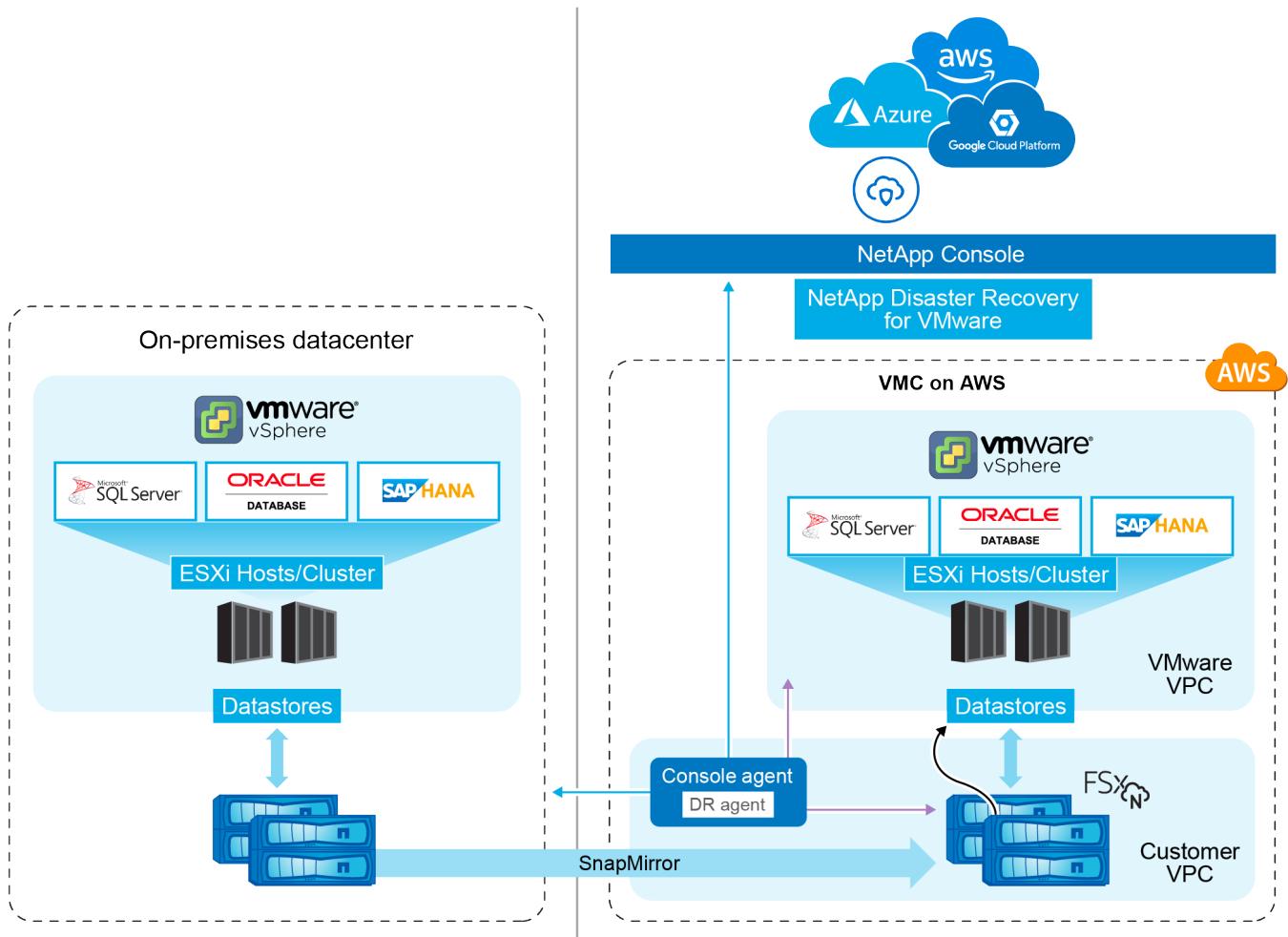
Para continuar después de la prueba de 30 días, deberá obtener una suscripción de pago por uso (PAYGO) de su proveedor de nube o comprar una licencia BYOL de NetApp.

Puede comprar una licencia en cualquier momento y no se le cobrará hasta que finalice el período de prueba de 30 días.

Cómo funciona NetApp Disaster Recovery

NetApp Disaster Recovery es un servicio alojado dentro del entorno de software como servicio (SaaS) de NetApp Console . La recuperación ante desastres puede recuperar cargas de trabajo replicadas desde un sitio local a Amazon FSx para ONTAP o a otro sitio local. Este servicio automatiza la recuperación desde el nivel de SnapMirror , mediante el registro de máquinas virtuales en VMware Cloud on AWS y las asignaciones de red directamente en la plataforma de virtualización y seguridad de red de VMware, NSX-T. Esta función está incluida en todos los entornos de Virtual Machine Cloud.

NetApp Disaster Recovery utiliza la tecnología ONTAP SnapMirror , que proporciona una replicación altamente eficiente y preserva la eficiencia de las instantáneas incrementales de ONTAP para siempre. La replicación de SnapMirror garantiza que las copias de instantáneas consistentes con la aplicación estén siempre sincronizadas y que los datos se puedan utilizar inmediatamente después de una comutación por error.



Cuando ocurre un desastre, este servicio le ayuda a recuperar máquinas virtuales en el otro entorno local de VMware o VMC rompiendo las relaciones de SnapMirror y activando el sitio de destino.

- El servicio también le permite revertir las máquinas virtuales a la ubicación de origen original.
- Puede probar el proceso de conmutación por error de recuperación ante desastres sin interrumpir las máquinas virtuales originales. La prueba recupera máquinas virtuales en una red aislada mediante la creación de un FlexClone del volumen.
- Para el proceso de conmutación por error o de prueba, puede elegir la instantánea más reciente (predeterminada) o seleccionada desde la cual recuperar su máquina virtual.

Componentes de la recuperación ante desastres

La recuperación ante desastres utiliza los siguientes componentes para proporcionar recuperación ante desastres para cargas de trabajo de VMware:

- * NetApp Console*: la interfaz de usuario para administrar sus planes de recuperación ante desastres. Puede utilizar la NetApp Console para crear y administrar planes de replicación, grupos de recursos y operaciones de conmutación por error en sus entornos locales y en la nube.
- **Agente de consola**: un componente de software liviano que se ejecuta en su red alojada en la nube o en su entorno VMware local. Se comunica con la NetApp Console y administra la replicación de datos entre su entorno local y el sitio de recuperación ante desastres. El agente de consola se instala en una máquina virtual en su entorno VMware.

- * Clústeres de almacenamiento ONTAP *: Los clústeres de almacenamiento ONTAP son los sistemas de almacenamiento principales que alojan sus cargas de trabajo de VMware. Los clústeres de almacenamiento de ONTAP proporcionan la infraestructura de almacenamiento subyacente para sus planes de recuperación ante desastres. Disaster Recovery utiliza las API de almacenamiento de ONTAP para administrar clústeres de almacenamiento de ONTAP, como matrices locales y soluciones basadas en la nube, como Amazon FSx for NetApp ONTAP.

- **Servidores vCenter:** VMware vCenter es el servidor de administración para su entorno VMware. Administra los hosts ESXi y sus almacenes de datos asociados. El agente de consola se comunica con VMware vCenter para administrar la replicación de datos entre su entorno local y el sitio de recuperación ante desastres. Esto incluye registrar LUN y volúmenes de ONTAP como almacenes de datos, reconfigurar máquinas virtuales e iniciar y detener máquinas virtuales.

El flujo de trabajo de protección de recuperación ante desastres

Cuando se asigna un plan de replicación a un grupo de recursos, Disaster Recovery realiza una verificación de detección de todos los componentes del grupo de recursos y del plan para garantizar que el plan pueda activarse.

Si esta comprobación es exitosa, Disaster Recovery realiza los siguientes pasos de inicialización:

1. Para cada máquina virtual en el grupo de recursos de destino, identifique el almacén de datos VMware que lo aloja.
2. Para cada almacén de datos de VMware encontrado, identifique el volumen o LUN ONTAP FlexVol volume que lo aloja.
3. Para cada volumen ONTAP y LUN encontrado, determine si existe una relación SnapMirror entre los volúmenes de origen y un volumen de destino en el sitio de destino.
 - a. Si no existe una relación SnapMirror preexistente, cree cualquier nuevo volumen de destino y cree una nueva relación SnapMirror entre cada volumen de origen no protegido.
 - b. Si existe una relación SnapMirror preexistente, utilice esa relación para realizar todas las operaciones de replicación.

Después de que Disaster Recovery crea e inicializa todas las relaciones, en cada copia de seguridad programada, el servicio realiza los siguientes pasos de protección de datos:

1. Para cada máquina virtual marcada como “compatible con la aplicación”, utilice VMtools para colocar la aplicación compatible en un estado de respaldo.
2. Cree una nueva instantánea de todos los volúmenes ONTAP que alojan almacenes de datos VMware protegidos.
3. Realice una operación de actualización de SnapMirror para replicar esas instantáneas en el clúster ONTAP de destino.
4. Determine si la cantidad de instantáneas retenidas ha excedido la retención máxima de instantáneas definida en el plan de replicación y elimine cualquier instantánea extraña de los volúmenes de origen y destino.

Objetivos de protección y tipos de almacén de datos admitidos

Tipos de almacenes de datos compatibles NetApp Disaster Recovery admite los siguientes tipos de almacenes de datos:

- Almacenes de datos NFS alojados en volúmenes ONTAP FlexVol que residen en clústeres ONTAP .

- Almacenes de datos del sistema de archivos de máquina virtual (VMFS) de VMware vSphere que utilizan el protocolo iSCSI o FC

Objetivos de protección admitidos

- VMware Cloud (VMC) en AWS con Amazon FSx for NetApp ONTAP
- Otro entorno VMware basado en NFS local con almacenamiento ONTAP o un VMSF FC/iSCSI local
- Servicio Amazon Elastic VMware
- Azure VMware Solution (AVS) con NetApp Cloud Volumes ONTAP (iSCSI) (versión preliminar privada)
- Google Cloud VMware Engine (GCVE) con Google Cloud NetApp Volumes

Términos que podrían ayudarle con NetApp Disaster Recovery

Podría resultarle beneficioso comprender algunos términos relacionados con la recuperación ante desastres.

- **Almacén de datos:** un contenedor de datos de VMware vCenter, que utiliza un sistema de archivos para almacenar archivos VMDK. Los tipos de almacenes de datos típicos son NFS, VMFS, vSAN o vVol. Disaster Recovery admite almacenes de datos NFS y VMFS. Cada almacén de datos de VMware está alojado en un único volumen o LUN de ONTAP . Disaster Recovery admite almacenes de datos NFS y VMFS alojados en volúmenes FlexVol que residen en clústeres ONTAP .
- **Plan de replicación:** un conjunto de reglas sobre la frecuencia con la que se realizan las copias de seguridad y cómo manejar eventos de conmutación por error. Los planes se asignan a uno o más grupos de recursos.
- **Objetivo de punto de recuperación (RPO):** La cantidad máxima de pérdida de datos que es aceptable en caso de desastre. El RPO se define en la frecuencia de replicación de datos o en el cronograma de replicación del plan de replicación.
- **Objetivo de tiempo de recuperación (RTO):** La cantidad máxima de tiempo que es aceptable para recuperarse de un desastre. El RTO se define en el plan de replicación y es el tiempo que lleva realizar una conmutación por error al sitio de recuperación ante desastres y reiniciar todas las máquinas virtuales.
- **Grupo de recursos:** un contenedor lógico que le permite administrar varias máquinas virtuales como una sola unidad. Una máquina virtual solo puede estar en un grupo de recursos a la vez. Puede crear un grupo de recursos para cada aplicación o carga de trabajo que desee proteger.
- **Sitio:** Un contenedor lógico generalmente asociado con un centro de datos físico o una ubicación en la nube que aloja uno o más clústeres de vCenter y almacenamiento ONTAP .

Requisitos previos de NetApp Disaster Recovery

Antes de utilizar NetApp Disaster Recovery, asegúrese de que su entorno cumpla con los requisitos de almacenamiento ONTAP , clúster VMware vCenter y NetApp Console .

Versión de software

Componente	Versión mínima
Amazon FSx for NetApp ONTAP	Última versión disponible
Google Cloud VMware Engine con Google Cloud NetApp Volumes	Última versión disponible

Componente	Versión mínima
Software ONTAP	ONTAP 9.10.0 o posterior
VMware Cloud para AWS	Última versión disponible
VMware vCenter local	7.0u3 o posterior

Requisitos previos y consideraciones de Google Cloud

Con la recuperación ante desastres en Google Cloud VMware Engine mediante Google Cloud NetApp Volumes, asegúrese de configurar los permisos correctos y cumplir con las consideraciones señaladas.

- Comuníquese con el equipo de SRE de Google para incluir en la lista de permitidos lo siguiente:
 - API de sincronización para transferir instantáneas desde el almacenamiento local a Google Cloud NetApp Volumes.
 - el proyecto de Google con el motor VMware para crear, montar y desmontar almacenes de datos.
- Usted debe ["Presente una solicitud para incluir en la lista de permitidos sus volúmenes de replicación híbrida"](#) .
- Tenga en cuenta la ["Cuota y límites de Google Cloud NetApp Volumes"](#) .
- Solo puede agregar un volumen o almacén de datos a un plan de replicación.
- Revisar el ["limitaciones"](#) .

Consideraciones sobre conmutación por error

- La conmutación por error solo es compatible usando la última instantánea. Si es necesario, puedes crear una nueva instantánea durante la conmutación por error (es decir, la opción de instantánea selectiva debe estar desactivada).
- No es posible crear una nueva instantánea después de una conmutación por error.
- No es posible conservar ni conciliar instantáneas después de una conmutación por error.

Consideraciones sobre la recuperación

- La recuperación solo es posible con la opción de instantánea selectiva. No es posible realizar una conmutación por recuperación tomando una nueva instantánea.
- Si elimina el emparejamiento de clústeres entre el almacenamiento local y los clústeres de almacenamiento de Google Cloud NetApp Volumes , debe borrar manualmente la entrada de emparejamiento de clústeres y máquinas virtuales de almacenamiento del clúster local. Para obtener más información, consulte ["Eliminar una relación de pares vserver"](#) .

Permisos de Google Cloud

Al principal de servicio en Google Cloud se le deben asignar los siguientes roles o permisos equivalentes:

- ["Rol de administrador de cómputo"](#)
- ["Permisos de Google Cloud para la NetApp Console"](#)
- ["Administrador de Google Cloud NetApp Volumes"](#)

- "[Administrador de servicios de VMware Engine](#)"

Permisos de la NetApp Console

El usuario de la NetApp Console debe tener los siguientes roles:

- "[Administrador de Google Cloud NetApp Volumes](#)"
- "[Administrador de SnapCenter](#)"
- "[Administrador de conmutación por error de recuperación ante desastres](#)"

Requisitos previos de almacenamiento de ONTAP

Estos requisitos previos se aplican a las instancias de ONTAP o Amazon FSX para NetApp ONTAP .

- Los clústeres de origen y destino deben tener una relación de pares.
- La SVM que aloja los volúmenes de recuperación ante desastres debe existir en el clúster de destino.
- El SVM de origen y el SVM de destino deben tener una relación de pares.
- Si se implementa con Amazon FSx for NetApp ONTAP, se aplica el siguiente requisito previo:
 - Debe existir una instancia de Amazon FSx for NetApp ONTAP para alojar almacenes de datos de VMware DR en su VPC. Para empezar, consulte "[Documentación de Amazon FSx para ONTAP](#)" .

Requisitos previos de los clústeres de VMware vCenter

Estos requisitos previos se aplican tanto a los clústeres de vCenter locales como al centro de datos definido por software (SDDC) de VMware Cloud para AWS.

- Revisar "[Privilegios de vCenter](#)" requerido para NetApp Disaster Recovery.
- Todos los clústeres de VMware que desea que NetApp Disaster Recovery administre utilizan volúmenes ONTAP para alojar cualquier máquina virtual que desee proteger.
- Todos los almacenes de datos de VMware que administrará NetApp Disaster Recovery deben utilizar uno de los siguientes protocolos:
 - Sistema Nacional de Archivos
 - VMFS utilizando el protocolo iSCSI o FC
- VMware vSphere versión 7.0 Actualización 3 (7.0v3) o posterior
- Si utiliza VMware Cloud SDDC, se aplican estos requisitos previos.
 - En VMware Cloud Console, utilice los roles de servicio de Administrador y Administrador de NSX Cloud. Utilice también el propietario de la organización para el rol de Organización. Referirse a "[Uso de VMware Cloud Foundations con AWS FSx para la documentación de NetApp ONTAP](#)" .
 - Vincule VMware Cloud SDDC con la instancia de Amazon FSx for NetApp ONTAP . Referirse a "[Información sobre la integración de VMware Cloud on AWS con Amazon FSx for NetApp ONTAP](#)" .

Requisitos previos de la NetApp Console

Comience a utilizar la NetApp Console

Si aún no lo has hecho, "[Regístrate en la NetApp Console y cree una organización](#)" .

Recopilar credenciales para ONTAP y VMware

- Las credenciales de Amazon FSx para ONTAP y AWS deben agregarse al sistema dentro del proyecto de la NetApp Console que administra la NetApp Disaster Recovery.
- NetApp Disaster Recovery requiere credenciales de vCenter. Ingresa las credenciales de vCenter cuando agrega un sitio en NetApp Disaster Recovery.

Para obtener una lista de los privilegios de vCenter necesarios, consulte "["Privilegios de vCenter necesarios para NetApp Disaster Recovery"](#)". Para obtener instrucciones sobre cómo agregar un sitio, consulte "["Agregar un sitio"](#)".

Crear el agente de la NetApp Console

El agente de consola es un componente de software que permite que la consola se comunique con su almacenamiento ONTAP y los clústeres VMware vCenter. Es necesario para que la recuperación ante desastres funcione correctamente. El agente reside en su red privada (ya sea un centro de datos local o una VPC en la nube) y se comunica con sus instancias de almacenamiento ONTAP y cualquier componente adicional de servidor y aplicación. Para la recuperación ante desastres, este es el acceso a sus clústeres de vCenter administrados.

Se debe configurar un agente de consola en la NetApp Console. Cuando utilice el agente, incluirá las capacidades adecuadas para el servicio de recuperación ante desastres.

- NetApp Disaster Recovery solo funciona con la implementación del agente en modo estándar. Ver "["Introducción a la NetApp Console en modo estándar"](#)".
- Asegúrate de que tanto el clúster de origen como el de destino vCenter usen el mismo agente de Console.
- Tipo de agente de consola necesario:
 - **Recuperación de desastres de local a local:** Instala el agente de la Console local en el sitio de recuperación ante desastres. Usando este método, una falla en el sitio principal no impide que el servicio reinicie tus recursos virtuales en el sitio de DR. Consulta "["Instalar y configurar el agente de consola en las instalaciones"](#)".

La recuperación ante desastres también admite el uso de múltiples agentes de consola con configuraciones locales. Para este escenario, los agentes de la consola dirigen acciones a los vCenters y a los clústeres de matrices ONTAP, y el origen y el destino tendrían cada uno su propio agente de consola. Se recomienda utilizar varios agentes de consola para reducir la latencia y mejorar el tiempo de recuperación si falla un agente de consola o un sitio.

- **En las instalaciones de AWS:** instale el agente de consola para AWS en su VPC de AWS. Referirse a "["Opciones de instalación del agente de consola en AWS"](#)".



Para conexiones locales a locales, utilice el agente de consola local. Para las instalaciones locales en AWS, utilice el agente de la consola de AWS, que tiene acceso al vCenter local de origen y al vCenter local de destino.

- El agente de consola instalado debe poder acceder a cualquier instancia de clúster de VMware vCenter y a los hosts ESXi administrados por esos clústeres de vCenter que gestionará la Recuperación ante Desastres.
- Todas las matrices ONTAP que serán administradas por NetApp Disaster Recovery deben agregarse a cualquier sistema dentro del proyecto de la NetApp Console que se utilizará para administrar NetApp Disaster Recovery.

Ver "Descubra los clústeres ONTAP locales" .

- Para obtener información sobre cómo configurar un proxy inteligente para NetApp Disaster Recovery, consulte "[Configure su infraestructura para NetApp Disaster Recovery](#)" .

Requisitos previos de la carga de trabajo

Para garantizar que los procesos de coherencia de aplicaciones sean exitosos, aplique estos requisitos previos:

- Asegúrese de que las herramientas de VMware (o las herramientas de OpenVM) se estén ejecutando en las máquinas virtuales que estarán protegidas.
- Para las máquinas virtuales Windows que ejecutan Microsoft SQL Server, Oracle Database o ambos, las bases de datos deben tener habilitados sus escritores VSS.
- Las bases de datos Oracle que se ejecutan en un sistema operativo Linux deben tener habilitada la autenticación de usuario del sistema operativo para el rol SYSDBA de la base de datos Oracle.

Más información

- [Privilegios requeridos de vCenter](#)
- [Requisitos previos para Amazon EVS con NetApp Disaster Recovery](#)

Inicio rápido para NetApp Disaster Recovery

A continuación se muestra una descripción general de los pasos necesarios para comenzar a utilizar NetApp Disaster Recovery. Los enlaces dentro de cada paso lo llevarán a una página que proporciona más detalles.

1

Revisar los prerequisitos

"[Asegúrese de que su sistema cumpla estos requisitos](#)" .

2

Configurar NetApp Disaster Recovery

- "[Configurar la infraestructura para el servicio](#)" .
- "[Configurar licencias](#)" .

3

¿Qué sigue?

Después de configurar el servicio, esto es lo que puedes hacer a continuación.

- "[Agregue sus sitios de vCenter a NetApp Disaster Recovery](#)" .
- "[Crea tu primer grupo de recursos](#)" .
- "[Crea tu primer plan de replicación](#)" .
- "[Replicar aplicaciones a otro sitio](#)" .
- "[Conmutar por error las aplicaciones a un sitio remoto](#)" .

- "Regresar las aplicaciones al sitio de origen original" .
- "Administrar sitios, grupos de recursos y planes de replicación" .
- "Supervisar las operaciones de recuperación ante desastres" .

Configure su infraestructura para NetApp Disaster Recovery

Para utilizar NetApp Disaster Recovery, realice algunos pasos para configurarlo tanto en Amazon Web Services (AWS) como en la NetApp Console.



Revisar "[prerrequisitos](#)" para garantizar que su sistema esté listo.

Puede utilizar NetApp Disaster Recovery en las siguientes infraestructuras:

- DR en nube híbrida que replica un centro de datos VMware plus ONTAP local a una infraestructura de DR de AWS basada en VMware Cloud on AWS y Amazon FSx for NetApp ONTAP.
- DR en nube privada que replica un VMware plus ONTAP vCenter local a otro VMware plus ONTAP vCenter local.

Nube híbrida con VMware Cloud y Amazon FSx for NetApp ONTAP

Este método consiste en una infraestructura de vCenter de producción local que utiliza almacenes de datos alojados en volúmenes ONTAP FlexVol mediante un protocolo NFS. El sitio de DR consta de una o más instancias de VMware Cloud SDDC que utilizan almacenes de datos alojados en volúmenes FlexVol proporcionados por una o más instancias de FSx para ONTAP mediante un protocolo NFS.

Los sitios de producción y DR están conectados mediante una conexión segura compatible con AWS. Los tipos de conexión comunes son una VPN segura (privada o proporcionada por AWS), AWS Direct Connect u otros métodos de interconexión aprobados.

Para la recuperación ante desastres que involucra la infraestructura de nube de AWS, debe utilizar el agente de consola para AWS. El agente debe instalarse en la misma VPC que la instancia de FSx para ONTAP . Si se implementaron instancias adicionales de FSx para ONTAP en otras VPC, la VPC que aloja al agente debe tener acceso a las otras VPC.

Zonas de disponibilidad de AWS

AWS admite la implementación de soluciones en una o más zonas de disponibilidad (AZ) dentro de una región determinada. La recuperación ante desastres utiliza dos servicios alojados en AWS: VMware Cloud para AWS y AWS FSx para NetApp ONTAP.

- **VMware Cloud para AWS:** admite la implementación en un entorno SDDC de clúster extendido de una sola AZ o de dos AZ. Disaster Recovery admite una implementación de SDDC de zona única solo para Amazon VMware Cloud para AWS.
- **AWS FSx para NetApp ONTAP:** cuando se implementa en una configuración de doble AZ, cada volumen es propiedad de un solo sistema FSx. Cada volumen es propiedad de un único sistema FSx. Los datos del volumen se reflejan en el segundo sistema FSx. Los sistemas FSx para ONTAP se pueden implementar en implementaciones de zona de disponibilidad única o doble. La recuperación ante desastres admite FSx de una o varias zonas de disponibilidad para implementaciones de FSx para ONTAP .

MEJORES PRÁCTICAS: Para la configuración del sitio de AWS DR, NetApp recomienda usar implementaciones de zona de disponibilidad única tanto para VMware Cloud como para AWS FSx para instancias de ONTAP. Dado que AWS se utiliza para recuperación ante desastres, no hay ninguna ventaja en introducir múltiples AZ. Las multi-AZ pueden aumentar los costos y la complejidad.

Local a AWS

AWS proporciona los siguientes métodos para conectar centros de datos privados a la nube de AWS. Cada solución tiene sus beneficios y consideraciones de costos.

- **AWS Direct Connect:** se trata de una interconexión en la nube de AWS ubicada en la misma área geográfica que su centro de datos privado y proporcionada por un socio de AWS. Esta solución proporciona una conexión segura y privada entre su centro de datos local y la nube de AWS sin la necesidad de una conexión a Internet pública. Este es el método de conexión más directo y eficiente que ofrece AWS.
- **AWS Internet Gateway:** Proporciona conectividad pública entre los recursos de la nube de AWS y los recursos informáticos externos. Este tipo de conexión se utiliza normalmente para ofrecer servicios a clientes externos, como el servicio HTTP/HTTPS donde la seguridad no es un requisito. No hay control de calidad de servicio, seguridad ni garantía de conectividad. Por este motivo, este método de conexión no se recomienda para conectar un centro de datos de producción a la nube.
- **AWS Site-Site VPN:** esta conexión de red privada virtual se puede utilizar para proporcionar conexiones de acceso seguro junto con un proveedor de servicios de Internet público. La VPN cifra y descifra todos los datos que viajan hacia y desde la nube de AWS. Las VPN pueden basarse en software o hardware. Para las aplicaciones empresariales, el proveedor de servicios de Internet (ISP) público debe ofrecer garantías de calidad de servicio para asegurar que se proporcione el ancho de banda y la latencia adecuados para la replicación de DR.

MEJORES PRÁCTICAS: Para la configuración del sitio de AWS DR, NetApp recomienda usar AWS Direct Connect. Esta solución proporciona el máximo rendimiento y seguridad para aplicaciones empresariales. Si no está disponible, se debe utilizar una conexión ISP pública de alto rendimiento junto con una VPN. Asegúrese de que el ISP ofrezca niveles de servicio QoS comerciales para garantizar un rendimiento adecuado de la red.

Interconexiones de VPC a VPC

AWS ofrece los siguientes tipos de interconexiones de VPC a VPC. Cada solución tiene sus beneficios y consideraciones de costos.

- **VPC Peering:** se trata de una conexión privada entre dos VPC. Es el método de conexión más directo y eficiente que ofrece AWS. El peering de VPC se puede utilizar para conectar VPC en la misma región de AWS o en diferentes.
- **AWS Internet Gateway:** normalmente se utiliza para proporcionar conexiones entre recursos de AWS VPC y recursos y puntos finales que no son de AWS. Todo el tráfico sigue una ruta de "horquilla" donde el tráfico de VPC destinado a otra VPC sale de la infraestructura de AWS a través de la puerta de enlace de Internet y regresa a la infraestructura de AWS a través de la misma puerta de enlace o de una diferente. Este no es un tipo de conexión VPC adecuado para soluciones VMware empresariales.
- **AWS Transit Gateway:** este es un tipo de conexión centralizada basada en enrutador que permite que cada VPC se conecte a una única puerta de enlace central, que actúa como un concentrador central para todo el tráfico de VPC a VPC. Esto también se puede conectar a su solución VPN para permitir que los recursos del centro de datos local accedan a los recursos alojados en AWS VPC. Este tipo de conexión generalmente requiere un costo adicional para implementarse.

MEJORES PRÁCTICAS: Para soluciones de recuperación ante desastres que involucran VMware Cloud y un solo FSx para ONTAP VPC, NetApp recomienda que utilice la conexión de pares de VPC. Si se implementan

varias VPC de FSx para ONTAP , recomendamos utilizar AWS Transit Gateway para reducir la sobrecarga de administración de varias conexiones de pares de VPC.

Prepárese para la protección local en la nube con AWS

Para configurar NetApp Disaster Recovery para la protección local en la nube mediante AWS, debe configurar lo siguiente:

- Configurar AWS FSx para NetApp ONTAP
- Configurar VMware Cloud en AWS SDDC

Configurar AWS FSx para NetApp ONTAP

- Cree un sistema de archivos Amazon FSx for NetApp ONTAP .
 - Aprovisionar y configurar FSx para ONTAP. Amazon FSx for NetApp ONTAP es un servicio completamente administrado que proporciona almacenamiento de archivos altamente confiable, escalable, de alto rendimiento y con gran cantidad de funciones, creado sobre el sistema de archivos NetApp ONTAP .
 - Siga los pasos en "[Informe técnico 4938: Monte Amazon FSx ONTAP como un almacén de datos NFS con VMware Cloud en AWS](#)" y "[Inicio rápido de Amazon FSx for NetApp ONTAP](#)" para aprovisionar y configurar FSx para ONTAP.
- Agregue Amazon FSx para ONTAP al sistema y agregue las credenciales de AWS para FSx para ONTAP.
- Cree o verifique su SVM ONTAP de destino en AWS FSx para la instancia de ONTAP .
- Configure la replicación entre su clúster ONTAP local de origen y su instancia de FSx para ONTAP en la NetApp Console.

Referirse a "[Cómo configurar un sistema FSx para ONTAP](#)" para conocer los pasos detallados.

Configurar VMware Cloud en AWS SDDC

"[VMware Cloud en AWS](#)" Proporciona una experiencia nativa de la nube para cargas de trabajo basadas en VMware en el ecosistema de AWS. Cada centro de datos definido por software (SDDC) de VMware se ejecuta en una Amazon Virtual Private Cloud (VPC) y proporciona una pila VMware completa (incluido vCenter Server), redes definidas por software NSX-T, almacenamiento definido por software vSAN y uno o más hosts ESXi que proporcionan recursos informáticos y de almacenamiento a las cargas de trabajo.

Para configurar un entorno de VMware Cloud en AWS, siga los pasos que se indican en "[Implementar y configurar el entorno de virtualización en AWS](#)" Un grupo de luces piloto también se puede utilizar para fines de recuperación ante desastres.

Nube privada

Puede utilizar NetApp Disaster Recovery para proteger las máquinas virtuales VMware alojadas en uno o más clústeres de vCenter replicando los almacenes de datos de las máquinas virtuales en otro clúster de vCenter, ya sea en el mismo centro de datos privado o en un centro de datos remoto privado o ubicado en el mismo lugar.

Para situaciones locales a locales, instale el agente de consola en uno de los sitios físicos.

Disaster Recovery admite la replicación de sitio a sitio mediante Ethernet y TCP/IP. Asegúrese de que haya suficiente ancho de banda disponible para soportar las tasas de cambio de datos en las máquinas virtuales del sitio de producción, de modo que todos los cambios se puedan replicar en el sitio de recuperación ante

desastres dentro del marco de tiempo del Objetivo de punto de recuperación (RPO).

Prepárese para la protección local a local

Asegúrese de que se cumplan los siguientes requisitos antes de configurar NetApp Disaster Recovery para la protección local a local:

- Almacenamiento ONTAP
 - Asegúrese de tener las credenciales de ONTAP .
 - Cree o verifique su sitio de recuperación ante desastres.
 - Cree o verifique su SVM ONTAP de destino.
 - Asegúrese de que sus SVM ONTAP de origen y destino estén emparejados.
- Clústeres de vCenter
 - Asegúrese de que las máquinas virtuales que desea proteger estén alojadas en almacenes de datos NFS (utilizando volúmenes NFS de ONTAP) o almacenes de datos VMFS (utilizando LUN iSCSI de NetApp).
 - Revisar "[Privilegios de vCenter](#)" requerido para NetApp Disaster Recovery.
 - Cree una cuenta de usuario de recuperación ante desastres (no la cuenta de administrador de vCenter predeterminada) y asigne los privilegios de vCenter a la cuenta.

Soporte de proxy inteligente

El agente de la NetApp Console admite proxy inteligente. El proxy inteligente es una forma liviana, segura y eficiente de conectar su entorno local a la NetApp Console. Proporciona una conexión segura entre su sistema y el servicio de consola sin necesidad de una VPN o acceso directo a Internet. Esta implementación de proxy optimizada descarga el tráfico de API dentro de la red local.

Cuando se configura un proxy, NetApp Disaster Recovery intenta comunicarse directamente con VMware o ONTAP y utiliza el proxy configurado si falla la comunicación directa.

La implementación del proxy de NetApp Disaster Recovery requiere comunicación del puerto 443 entre el agente de la consola y cualquier servidor vCenter y matriz ONTAP que utilice un protocolo HTTPS. El agente de NetApp Disaster Recovery dentro del agente de consola se comunica directamente con VMware vSphere, VC u ONTAP cuando realiza cualquier acción.

Para obtener más información sobre la configuración general del proxy en la NetApp Console, consulte "[Configurar el agente de la consola para utilizar un servidor proxy](#)" .

Acceda a NetApp Disaster Recovery

Utilice la NetApp Console para iniciar sesión en el servicio de NetApp Disaster Recovery

Para iniciar sesión, puede utilizar sus credenciales del sitio de soporte de NetApp o puede registrarse para iniciar sesión en la nube de NetApp usando su correo electrónico y una contraseña. "[Obtenga más información sobre cómo iniciar sesión](#)" .

Tareas específicas requieren roles de usuario específicos. "[Obtenga información sobre los roles y permisos de usuario en NetApp Disaster Recovery](#)". "[Obtenga información sobre los roles de acceso a la NetApp Console para todos los servicios](#)" .

Pasos

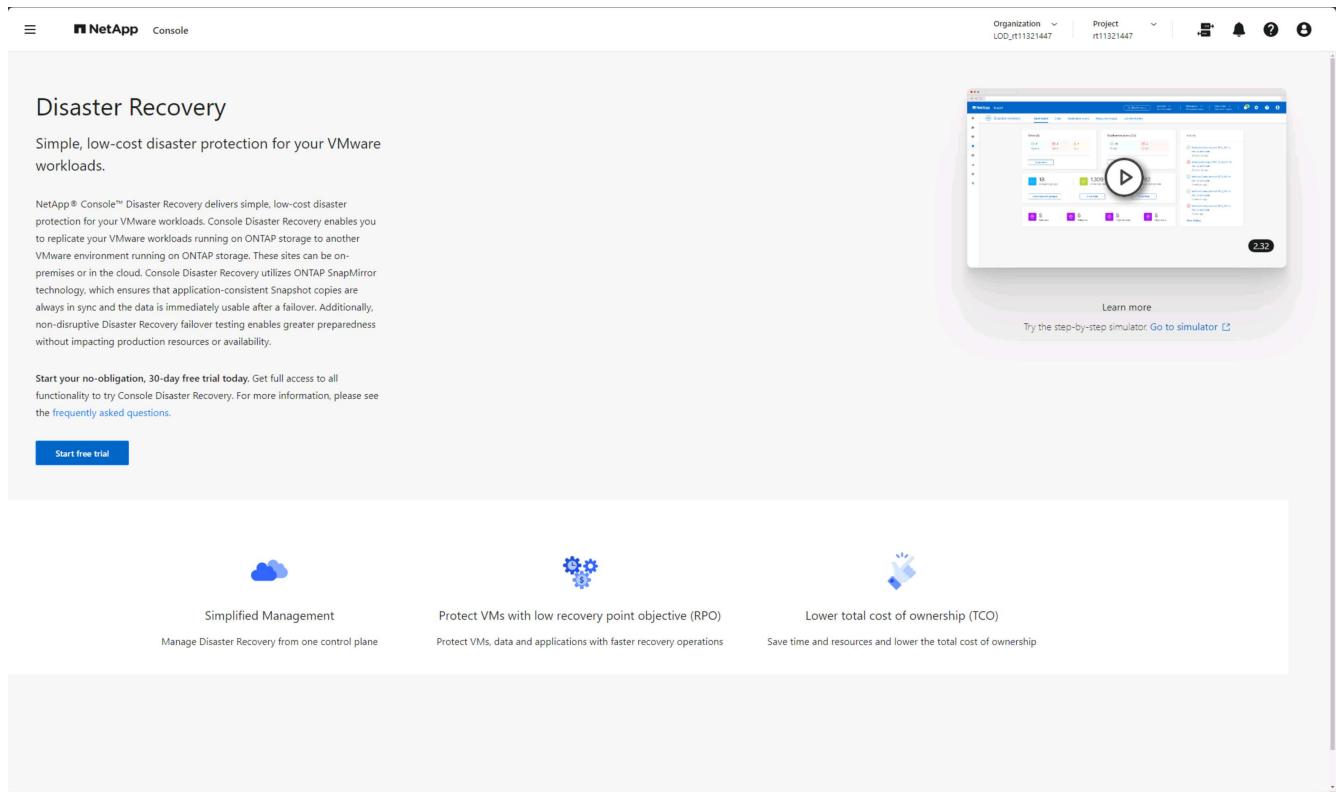
1. Abra un navegador web y vaya a "[NetApp Console](#)" .

Aparece la página de inicio de sesión de la NetApp Console .

2. Inicie sesión en la NetApp Console.

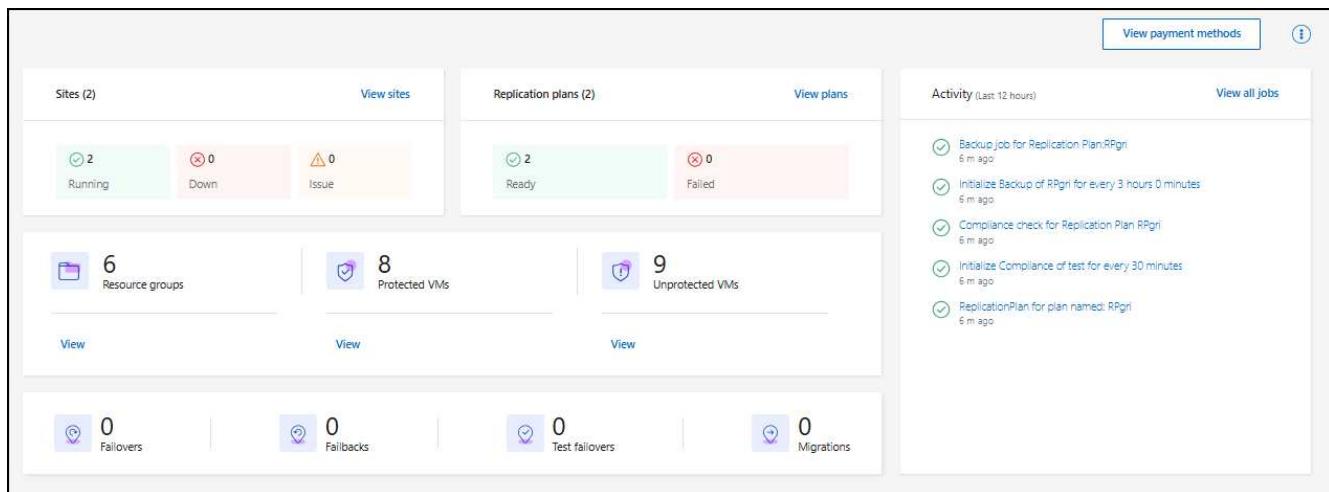
3. Desde el panel de navegación izquierdo de la NetApp Console , seleccione **Protección > Recuperación ante desastres**.

Si es la primera vez que inicia sesión en este servicio, aparecerá la página de inicio y podrá registrarse para una prueba gratuita.



De lo contrario, aparecerá el Panel de NetApp Disaster Recovery .

- Si aún no ha agregado un agente de NetApp Console , deberá agregar uno. Para agregar el agente, consulte "[Obtenga más información sobre los agentes de consola](#)" .
- Si es un usuario de la NetApp Console con un agente existente, cuando selecciona "Recuperación ante desastres", aparece un mensaje sobre cómo registrarse.
- Si ya está utilizando el servicio, cuando seleccione "Recuperación ante desastres", aparecerá el Panel de control.



Configurar licencias para NetApp Disaster Recovery

Con NetApp Disaster Recovery, puede utilizar diferentes planes de licencia, incluida una prueba gratuita, una suscripción de pago por uso o traer su propia licencia.

Rol de NetApp Console requerido Administrador de organización, Administrador de carpeta o proyecto, Administrador de recuperación ante desastres o Administrador de aplicación de recuperación ante desastres.

["Obtenga información sobre los roles y permisos de usuario en NetApp Disaster Recovery".](#) ["Obtenga información sobre los roles de acceso para todos los servicios".](#)

Opciones de licencia Puede utilizar las siguientes opciones de licencia:

- Regístrese para una prueba gratuita de 30 días.
- Compre una suscripción de pago por uso (PAYGO) en Amazon Web Services (AWS) Marketplace o en Microsoft Azure Marketplace.
- Traiga su propia licencia (BYOL), que es un archivo de licencia de NetApp (NLF) que obtiene de su representante de ventas de NetApp . Puede utilizar el número de serie de la licencia para activar el BYOL en la NetApp Console.

i Los cargos de NetApp Disaster Recovery se basan en la capacidad utilizada de los almacenes de datos en el sitio de origen cuando hay al menos una máquina virtual que tiene un plan de replicación. La capacidad para un almacén de datos comutado por error no está incluida en la capacidad asignada. En el caso de un BYOL, si los datos exceden la capacidad permitida, las operaciones en el servicio estarán limitadas hasta que obtenga una licencia de capacidad adicional o actualice la licencia en la NetApp Console.

["Obtenga más información sobre las suscripciones".](#)

Una vez finalizada la prueba gratuita o caducada la licencia, aún puedes hacer lo siguiente en el servicio:

- Ver cualquier recurso, como una carga de trabajo o un plan de replicación.
- Eliminar cualquier recurso, como una carga de trabajo o un plan de replicación.
- Ejecute todas las operaciones programadas que se crearon durante el período de prueba o bajo la licencia.

Pruébelo utilizando una prueba gratuita de 30 días

Puede probar NetApp Disaster Recovery mediante una prueba gratuita de 30 días.



No se aplican límites de capacidad durante la prueba.

Para continuar después de la prueba, deberá comprar una licencia BYOL o una suscripción PAYGO de AWS. Puede obtener una licencia en cualquier momento y no se le cobrará hasta que finalice el período de prueba.

Durante la prueba, tendrás acceso a todas las funciones.

Pasos

1. Iniciar sesión en el ["NetApp Console"](#) .
2. Desde el panel de navegación izquierdo de la NetApp Console , seleccione **Protección > Recuperación ante desastres**.

Si es la primera vez que inicia sesión en este servicio, aparecerá la página de destino.

The screenshot shows the NetApp Disaster Recovery landing page. At the top, there is a navigation bar with the NetApp logo, a search bar, and user information. Below the navigation, the main heading is "Disaster Recovery" with a subtext: "Simple, low-cost disaster protection for your VMware workloads". A "Start free trial" button is visible. To the right, there is a preview of the NetApp Console interface with a play button icon. Below the main heading, there are three sections: "Simplified Management" (Manage Disaster Recovery from one control plane), "Protect VMs with low recovery point objective (RPO)" (Protect VMs, data and applications with faster recovery operations), and "Lower total cost of ownership (TCO)" (Save time and resources and lower the total cost of ownership).

3. Si aún no ha agregado un agente de consola para otros servicios, agregue uno.

Para agregar un agente de consola, consulte ["Obtenga más información sobre los agentes de consola"](#) .

4. Después de configurar el agente, en la página de inicio de NetApp Disaster Recovery , el botón para agregar el agente cambia a un botón para iniciar una prueba gratuita. Seleccione **Iniciar prueba gratuita**.
5. Comience agregando vCenters.

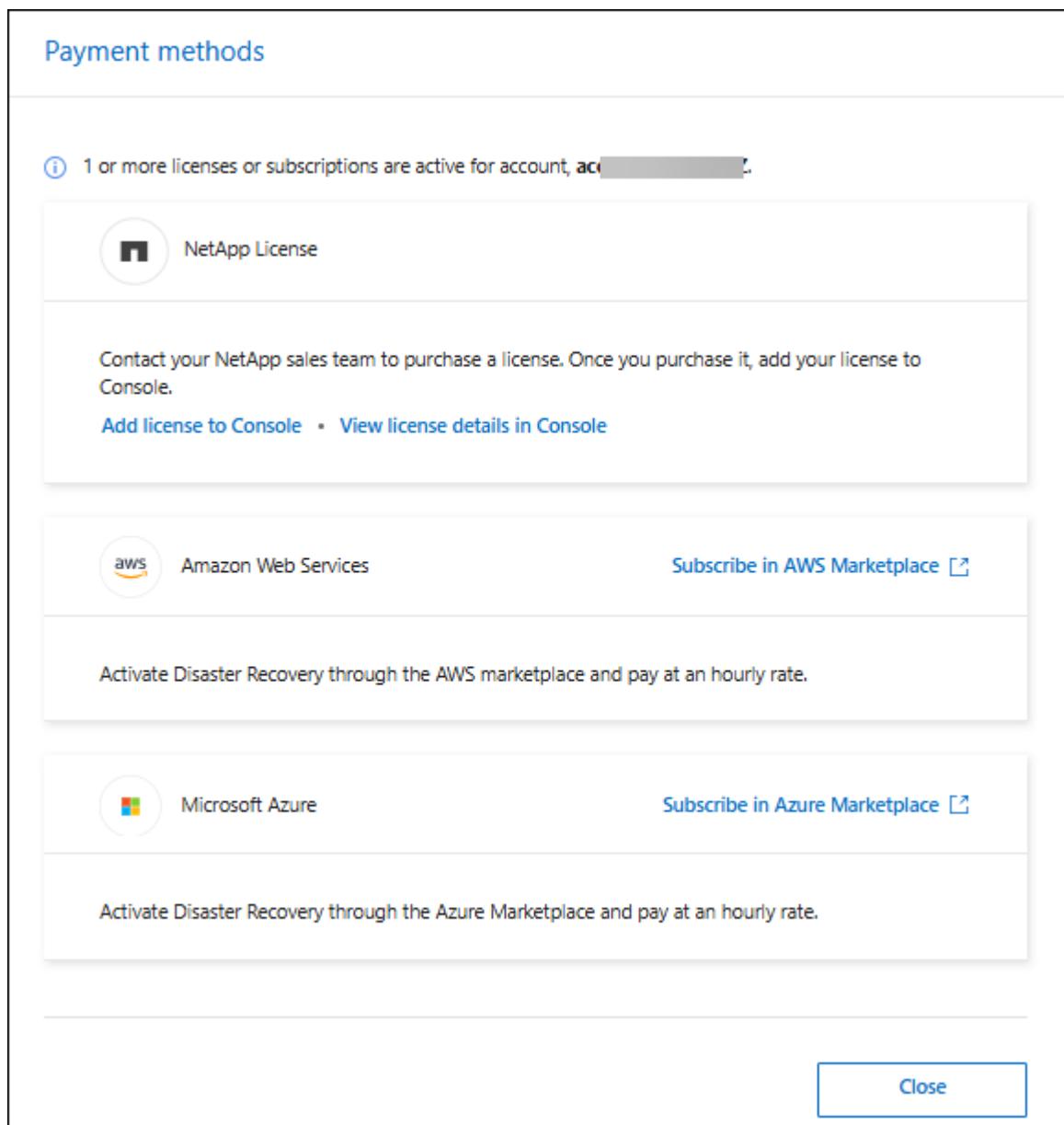
Para obtener más información, consulte ["Agregar sitios de vCenter"](#) .

Una vez finalizada la prueba, suscríbete a través de uno de los Marketplaces

Una vez finalizada la prueba gratuita, puede comprar una licencia de NetApp o suscribirse a través de AWS Marketplace o Microsoft Azure Marketplace. Este procedimiento proporciona una descripción general de alto nivel sobre cómo suscribirse directamente en uno de los Marketplaces.

Pasos

1. En NetApp Disaster Recovery, verá un mensaje que indica que la prueba gratuita está por vencer. En el mensaje, seleccione **Suscríbete o comprar una licencia**.
O bien, desde , seleccione **Ver métodos de pago**.



Payment methods

1 or more licenses or subscriptions are active for account, account ID: [REDACTED]

NetApp License
Contact your NetApp sales team to purchase a license. Once you purchase it, add your license to Console.
[Add license to Console](#) • [View license details in Console](#)

Amazon Web Services [Subscribe in AWS Marketplace](#)

Activate Disaster Recovery through the AWS marketplace and pay at an hourly rate.

Microsoft Azure [Subscribe in Azure Marketplace](#)

Activate Disaster Recovery through the Azure Marketplace and pay at an hourly rate.

Close

2. Seleccione **Suscríbete en AWS Marketplace** o **Suscríbete en Azure Marketplace**.
3. Utilice AWS Marketplace o Microsoft Azure Marketplace para suscribirse a * NetApp Disaster Recovery*.
4. Cuando regrese a NetApp Disaster Recovery, aparecerá un mensaje que indica que está suscrito.

Puede ver los detalles de la suscripción en la página de suscripción de la NetApp Console . ["Obtenga más"](#)

información sobre cómo administrar suscripciones con la NetApp Console".

Una vez finalizada la prueba, compre una licencia BYOL a través de NetApp

Una vez finalizada la prueba, puede comprar una licencia a través de su representante de ventas de NetApp .

Si trae su propia licencia (BYOL), la configuración incluye comprar la licencia, obtener el archivo de licencia de NetApp (NLF) y agregar la licencia a la NetApp Console.

Agregue la licencia a la NetApp Console* Despues de haber comprado su licencia de NetApp Disaster Recovery a un representante de ventas de NetApp , puede administrar la licencia en la consola.

"[Obtenga información sobre cómo agregar licencias con la NetApp Console](#)".

Actualice su licencia cuando expire

Si su período de licencia está cerca de la fecha de vencimiento o si su capacidad de licencia está alcanzando el límite, se le notificará en la interfaz de usuario de NetApp Disaster Recovery . Puede actualizar su licencia de NetApp Disaster Recovery antes de que caduque para que no haya interrupciones en su capacidad de acceder a los datos escaneados.



Este mensaje también aparece en la NetApp Console y en "[Notificaciones](#)" .

"[Obtenga información sobre cómo actualizar licencias con la NetApp Console](#)".

Finalizar la prueba gratuita

Puedes detener la prueba gratuita en cualquier momento o esperar hasta que caduque.

Pasos

1. En NetApp Disaster Recovery, seleccione **Prueba gratuita - Ver detalles**.
2. En los detalles desplegables, seleccione **Finalizar prueba gratuita**.

End free trial

Are you sure that you want to end your free trial on your account  to 1? We will delete your data 60 days after you end your trial. If you subscribe or purchase a license within 60 days, we will retain your data. You may also delete your data immediately when you end your trial.

This action is not reversible.

Delete data immediately after ending my free trial

Comments

Type "end trial" to end your free trial.

End

Cancel

3. Si desea eliminar todos los datos, marque **Eliminar datos inmediatamente después de finalizar mi prueba gratuita.**

Esto elimina todas las programaciones, planes de replicación, grupos de recursos, vCenters y sitios. Los datos de auditoría, los registros de operaciones y el historial de trabajos se conservan hasta el final de la vida útil del producto.



Si finaliza la prueba gratuita, no solicitó la eliminación de datos y no compra una licencia o suscripción, NetApp Disaster Recovery eliminará todos sus datos 60 días después de que finalice la prueba gratuita.

4. Escriba "finalizar prueba" en el cuadro de texto.
5. Seleccione **Fin.**

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Impreso en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

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

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

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

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

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

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

Información de la marca comercial

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