



Soluciones de bases de datos en la nube híbrida con SnapCenter

NetApp database solutions

NetApp
August 18, 2025

Tabla de contenidos

Soluciones de bases de datos en la nube híbrida con SnapCenter	1
TR-4908: Descripción general de soluciones de bases de datos en la nube híbrida con SnapCenter	1
Arquitectura de la solución	2
Requisitos de SnapCenter	3
Requisitos	3
Configuración de prerrequisitos	4
Configuración de prerrequisitos	4
Requisitos previos locales	5
Requisitos previos para la nube pública	10
Descripción general de primeros pasos	11
Descripción general de primeros pasos	11
Introducción a las instalaciones	12
Introducción a la nube pública de AWS	65
Flujo de trabajo para desarrollo y pruebas que se trasladan a la nube	90
Clonar una base de datos Oracle para desarrollo/prueba a partir de una copia de seguridad de instantánea replicada	90
Clonar una base de datos SQL para desarrollo/prueba desde una copia de seguridad instantánea replicada	100
Configuración posterior a la clonación	107
Actualizar la base de datos de clones	108
¿A dónde acudir para obtener ayuda?	108
Flujo de trabajo de recuperación ante desastres	108
Clonar una base de datos de producción Oracle local a la nube para recuperación ante desastres ...	108
Validación y configuración posterior a la clonación DR para Oracle	118
Clonar una base de datos de producción SQL local a la nube para recuperación ante desastres	119
Validación y configuración posterior a la clonación DR para SQL	125
¿A dónde acudir para obtener ayuda?	126

Soluciones de bases de datos en la nube híbrida con SnapCenter

TR-4908: Descripción general de soluciones de bases de datos en la nube híbrida con SnapCenter

Alan Cao, Félix Melligan, NetApp

Esta solución proporciona a los clientes y al campo de NetApp instrucciones y orientación para configurar, operar y migrar bases de datos a un entorno de nube híbrida utilizando la herramienta basada en GUI SnapCenter de NetApp y el servicio de almacenamiento CVO de NetApp en nubes públicas para los siguientes casos de uso:

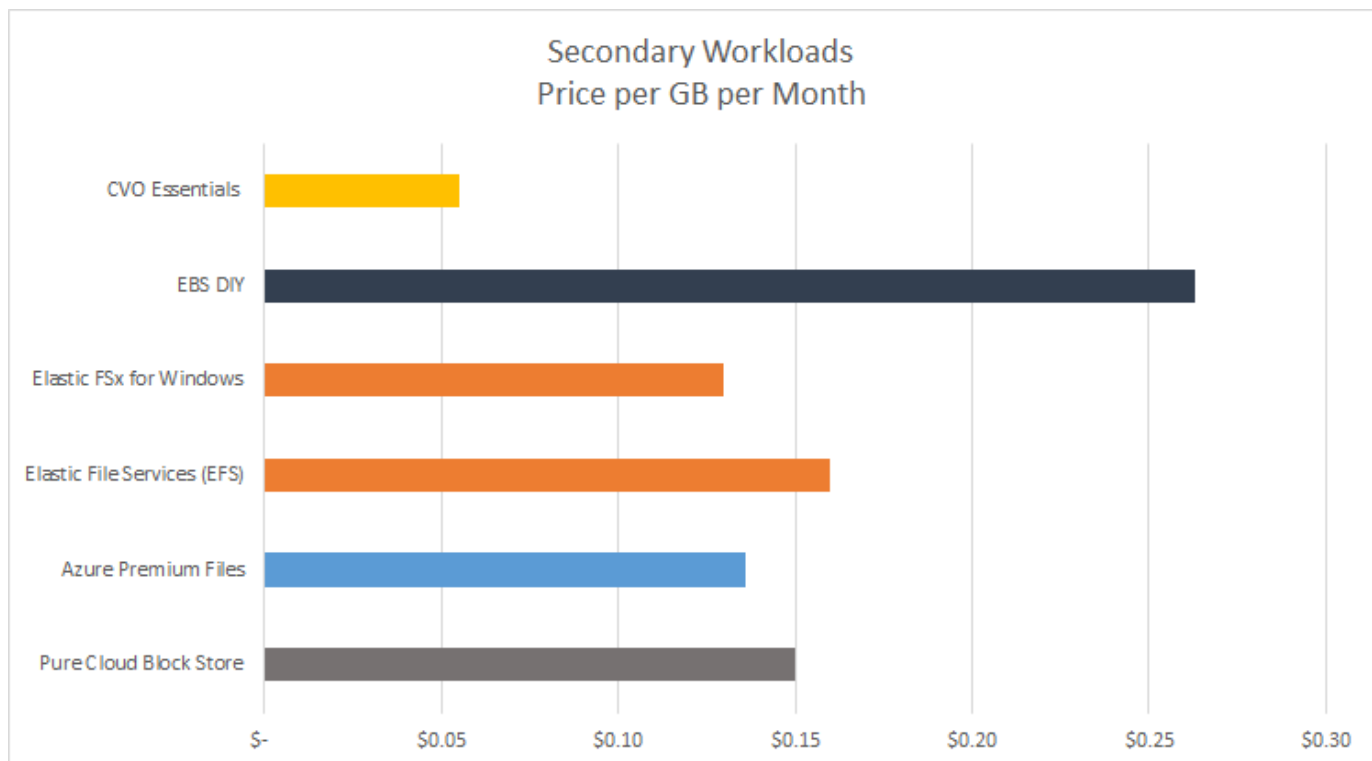
- Operaciones de desarrollo y prueba de bases de datos en la nube híbrida
- Recuperación ante desastres de bases de datos en la nube híbrida

Hoy en día, muchas bases de datos empresariales todavía residen en centros de datos corporativos privados por motivos de rendimiento, seguridad u otros. Esta solución de base de datos en nube híbrida permite a las empresas operar sus bases de datos principales en el sitio mientras utilizan una nube pública para operaciones de base de datos de desarrollo y prueba, así como para recuperación ante desastres a fin de reducir los costos operativos y de licencias.

Muchas bases de datos empresariales, como Oracle, SQL Server, SAP HANA, etc., conllevan altos costos operativos y de licencia. Muchos clientes pagan una tarifa de licencia única, así como costos de soporte anuales basados en la cantidad de núcleos de cómputo en su entorno de base de datos, ya sea que los núcleos se utilicen para desarrollo, pruebas, producción o recuperación ante desastres. Es posible que muchos de esos entornos no se utilicen por completo durante todo el ciclo de vida de la aplicación.

Las soluciones brindan a los clientes una opción para reducir potencialmente la cantidad de núcleos licenciados al trasladar sus entornos de bases de datos dedicados al desarrollo, las pruebas o la recuperación ante desastres a la nube. Al utilizar la escala de la nube pública, redundancia, alta disponibilidad y un modelo de facturación basado en el consumo, el ahorro en costos de licencia y operación puede ser sustancial, sin sacrificar la usabilidad ni la disponibilidad de las aplicaciones.

Más allá del potencial ahorro en costos de licencia de base de datos, el modelo de licencia CVO basado en capacidad de NetApp permite a los clientes ahorrar costos de almacenamiento por GB al tiempo que les brinda un alto nivel de capacidad de administración de base de datos que no está disponible en los servicios de almacenamiento de la competencia. El siguiente gráfico muestra una comparación de costos de almacenamiento de los servicios de almacenamiento más populares disponibles en la nube pública.



Esta solución demuestra que, al utilizar la herramienta de software basada en GUI SnapCenter y la tecnología SnapMirror de NetApp, las operaciones de bases de datos en nube híbrida se pueden configurar, implementar y operar fácilmente.

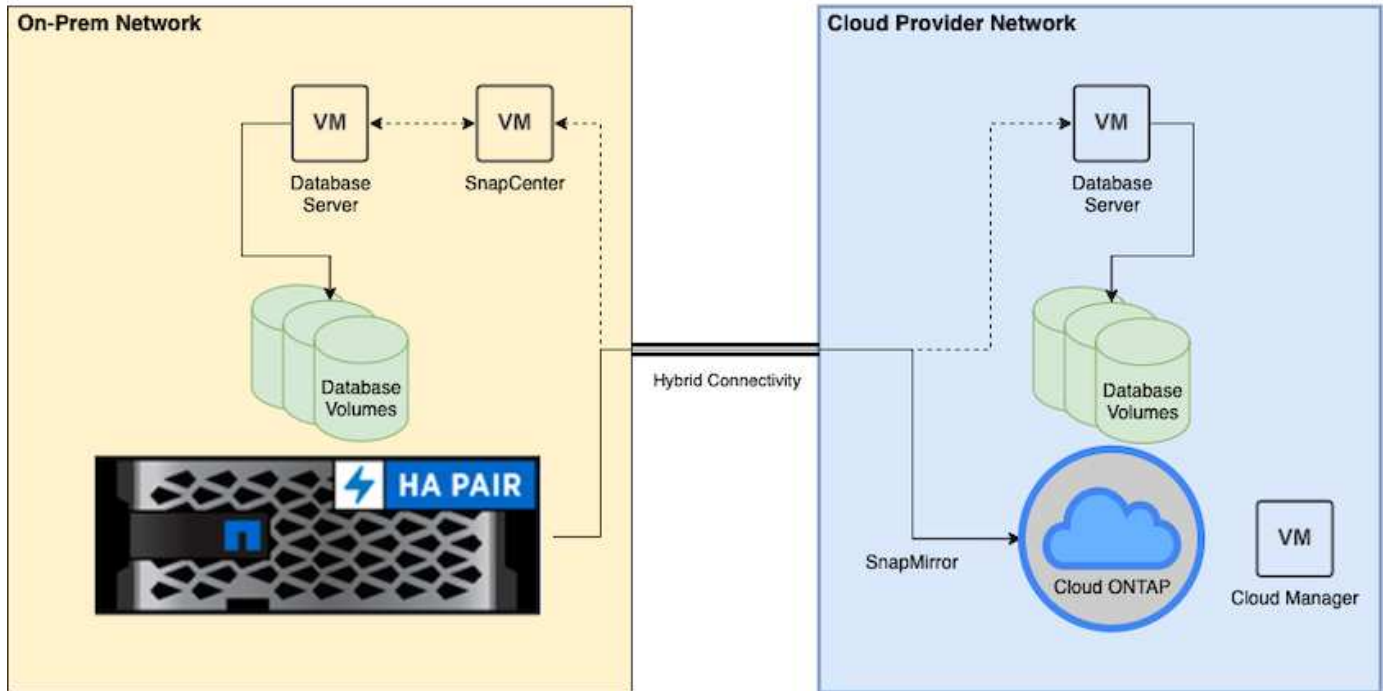
Los siguientes videos muestran SnapCenter en acción:

- ["Copia de seguridad de una base de datos Oracle en una nube híbrida mediante SnapCenter"](#)
- ["SnapCenter: clonación de DEV/TEST en AWS Cloud para una base de datos Oracle"](#)

En particular, si bien las ilustraciones de este documento muestran a CVO como una instancia de almacenamiento de destino en la nube pública, la solución también está completamente validada para la nueva versión del motor de almacenamiento FSx ONTAP para AWS.

Arquitectura de la solución

El siguiente diagrama de arquitectura ilustra una implementación típica de la operación de una base de datos empresarial en una nube híbrida para operaciones de desarrollo/prueba y recuperación ante desastres.



En operaciones comerciales normales, los volúmenes de bases de datos sincronizados en la nube se pueden clonar y montar en instancias de bases de datos de desarrollo/prueba para el desarrollo o prueba de aplicaciones. En caso de fallo, los volúmenes de base de datos sincronizados en la nube se pueden activar para la recuperación ante desastres.

Requisitos de SnapCenter

Esta solución está diseñada en un entorno de nube híbrida para soportar bases de datos de producción locales que pueden conectarse a todas las nubes públicas populares para operaciones de desarrollo/prueba y recuperación ante desastres.

Esta solución admite todas las bases de datos actualmente compatibles con SnapCenter, aunque aquí solo se muestran las bases de datos Oracle y SQL Server. Esta solución está validada con cargas de trabajo de bases de datos virtualizadas, aunque también se admiten cargas de trabajo de hardware.

Suponemos que los servidores de bases de datos de producción están alojados localmente y los volúmenes de bases de datos se presentan a los hosts de bases de datos desde un clúster de almacenamiento ONTAP. El SnapCenter software se instala localmente para realizar copias de seguridad de bases de datos y replicar datos en la nube. Se recomienda un controlador Ansible, pero no es obligatorio, para la automatización de la implementación de bases de datos o la sincronización de la configuración de la base de datos y el kernel del sistema operativo con una instancia de recuperación ante desastres en espera o instancias de desarrollo y prueba en la nube pública.

Requisitos

Ambiente	Requisitos
En las instalaciones	Cualquier base de datos y versiones compatibles con SnapCenter
	SnapCenter v4.4 o superior
	Ansible v2.09 o superior
	Clúster ONTAP 9.x
	LIF entre clústeres configurados
	Conectividad desde las instalaciones locales a una VPC en la nube (VPN, interconexión, etc.)
	Puertos de red abiertos: ssh 22, tcp 8145, 8146, 10000, 11104, 11105
Nube - AWS	"Conector de Cloud Manager"
	"Cloud Volumes ONTAP"
	Coincidencia de instancias EC2 de DB OS con las instalaciones locales
Nube - Azure	"Conector de Cloud Manager"
	"Cloud Volumes ONTAP"
	Adecuación de las máquinas virtuales de Azure del sistema operativo de base de datos a las instalaciones locales
Nube - GCP	"Conector de Cloud Manager"
	"Cloud Volumes ONTAP"
	Coincidencia de las instancias de Google Compute Engine del sistema operativo de base de datos con las instalaciones locales

Configuración de prerequisites

Configuración de prerequisites

Se deben configurar ciertos requisitos previos tanto en las instalaciones como en la nube antes de la ejecución de cargas de trabajo de bases de datos en la nube híbrida. La siguiente sección proporciona un resumen de alto nivel de este proceso, y los siguientes enlaces proporcionan más información sobre la configuración necesaria del sistema.

En las instalaciones

- Instalación y configuración de SnapCenter
- Configuración de almacenamiento del servidor de base de datos local
- Requisitos de licencia
- Redes y seguridad
- Automatización

Nube pública

- Un inicio de sesión en NetApp Cloud Central
- Acceso a la red desde un navegador web a varios puntos finales
- Una ubicación de red para un conector
- Permisos del proveedor de la nube
- Redes para servicios individuales

Consideraciones importantes:

1. ¿Dónde implementar el conector de Cloud Manager?
2. Dimensionamiento y arquitectura de Cloud Volume ONTAP
3. ¿Nodo único o alta disponibilidad?

Los siguientes enlaces proporcionan más detalles:

["En las instalaciones"](#)

["Nube pública"](#)

Requisitos previos locales

Las siguientes tareas deben completarse localmente para preparar el entorno de carga de trabajo de la base de datos en la nube híbrida de SnapCenter .

Instalación y configuración de SnapCenter

La herramienta NetApp SnapCenter es una aplicación basada en Windows que normalmente se ejecuta en un entorno de dominio de Windows, aunque también es posible la implementación en grupos de trabajo. Se basa en una arquitectura de varios niveles que incluye un servidor de administración centralizado (el servidor SnapCenter) y un complemento de SnapCenter en los hosts del servidor de base de datos para las cargas de trabajo de la base de datos. A continuación se presentan algunas consideraciones clave para la implementación de la nube híbrida.

- **Implementación de instancia única o HA.** La implementación de HA proporciona redundancia en el caso de una falla en un solo servidor de instancia de SnapCenter .
- **Resolución de nombres.** Se debe configurar el DNS en el servidor SnapCenter para resolver todos los hosts de la base de datos, así como en el SVM de almacenamiento para búsquedas directas e inversas. El DNS también debe configurarse en los servidores de bases de datos para resolver el servidor SnapCenter y el SVM de almacenamiento para búsquedas directas e inversas.
- **Configuración de control de acceso basado en roles (RBAC).** Para cargas de trabajo de bases de datos mixtas, es posible que desee utilizar RBAC para segregar la responsabilidad de administración para diferentes plataformas de base de datos, como un administrador para una base de datos Oracle o un administrador para SQL Server. Se deben conceder los permisos necesarios para el usuario administrador de la base de datos.
- **Habilitar estrategia de respaldo basada en políticas.** Para garantizar la consistencia y confiabilidad de las copias de seguridad.
- **Abra los puertos de red necesarios en el firewall.** Para que el servidor SnapCenter local se comunique con los agentes instalados en el host de base de datos en la nube.

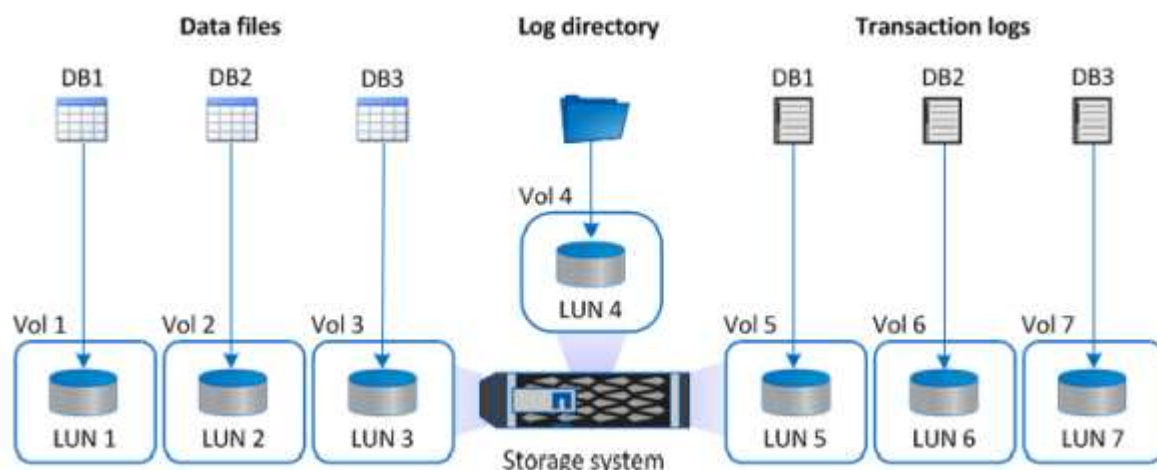
- **Los puertos deben estar abiertos para permitir el tráfico de SnapMirror entre las instalaciones locales y la nube pública.** El servidor SnapCenter se basa en ONTAP SnapMirror para replicar las copias de seguridad Snapshot locales en las SVM de almacenamiento CVO en la nube.

Después de una cuidadosa planificación y consideración previa a la instalación, haga clic aquí "[Requisitos previos para la instalación de SnapCenter](#)" para obtener detalles sobre la instalación y configuración de SnapCenter .

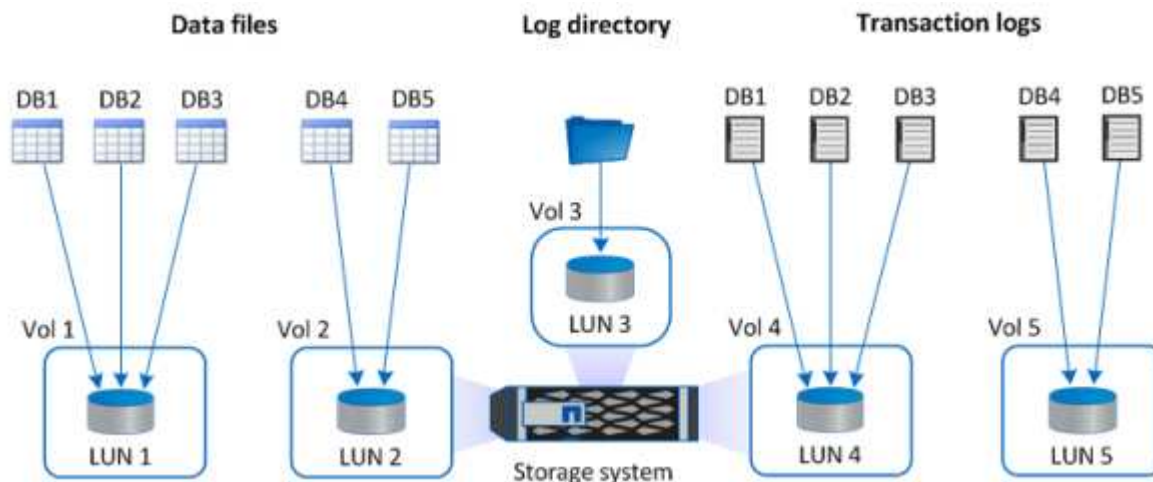
Configuración de almacenamiento del servidor de base de datos local

El rendimiento del almacenamiento juega un papel importante en el rendimiento general de las bases de datos y las aplicaciones. Un diseño de almacenamiento bien diseñado no solo puede mejorar el rendimiento de la base de datos, sino que también facilita la gestión de la copia de seguridad y la recuperación de la base de datos. Se deben tener en cuenta varios factores al definir el diseño de almacenamiento, incluido el tamaño de la base de datos, la tasa de cambio de datos esperada para la base de datos y la frecuencia con la que realiza copias de seguridad.

La conexión directa de LUN de almacenamiento a la máquina virtual invitada mediante NFS o iSCSI para cargas de trabajo de bases de datos virtualizadas generalmente proporciona un mejor rendimiento que el almacenamiento asignado a través de VMDK. NetApp recomienda el diseño de almacenamiento para una base de datos grande de SQL Server en LUN que se muestra en la siguiente figura.



La siguiente figura muestra el diseño de almacenamiento recomendado por NetApp para bases de datos de SQL Server pequeñas o medianas en LUN.





El directorio de registro está dedicado a SnapCenter para realizar la acumulación de registros de transacciones para la recuperación de la base de datos. Para una base de datos extra grande, se pueden asignar múltiples LUN a un volumen para lograr un mejor rendimiento.

Para las cargas de trabajo de bases de datos de Oracle, SnapCenter admite entornos de bases de datos respaldados por almacenamiento ONTAP que se montan en el host como dispositivos físicos o virtuales. Puede alojar la base de datos completa en uno o varios dispositivos de almacenamiento según la criticidad del entorno. Normalmente, los clientes aíslan los archivos de datos en un almacenamiento dedicado de todos los demás archivos, como archivos de control, archivos de rehacer y archivos de registro de archivo. Esto ayuda a los administradores a restaurar rápidamente (ONTAP SnapRestore de un solo archivo) o clonar una base de datos crítica grande (escala de petabytes) utilizando la tecnología Snapshot en cuestión de segundos a minutos.



Para cargas de trabajo de misión crítica que son sensibles a la latencia, se debe implementar un volumen de almacenamiento dedicado a diferentes tipos de archivos de Oracle para lograr la mejor latencia posible. Para una base de datos grande, se deben asignar varios LUN (NetApp recomienda hasta ocho) por volumen a los archivos de datos.



Para bases de datos Oracle más pequeñas, SnapCenter admite diseños de almacenamiento compartido en los que puede alojar varias bases de datos o parte de una base de datos en el mismo volumen de almacenamiento o LUN. Como ejemplo de este diseño, puede alojar archivos de datos para todas las bases de datos en un grupo de discos +DATA ASM o en un grupo de volúmenes. El resto de los archivos (rehacer, registro de archivo y archivos de control) se pueden alojar en otro grupo de discos dedicado o grupo de volúmenes (LVM). A continuación se ilustra un escenario de implementación de este tipo.



Para facilitar la reubicación de las bases de datos de Oracle, el binario de Oracle debe instalarse en un LUN separado que esté incluido en la política de respaldo regular. Esto garantiza que en el caso de reubicación de la base de datos a un nuevo servidor host, la pila Oracle se puede iniciar para la recuperación sin posibles

problemas debido a un binario Oracle desincronizado.

Requisitos de licencia

SnapCenter es un software con licencia de NetApp. Generalmente se incluye en una licencia ONTAP local. Sin embargo, para la implementación de nube híbrida, también se requiere una licencia de nube para SnapCenter para agregar CVO a SnapCenter como destino de replicación de datos. Revise los siguientes enlaces para obtener detalles sobre la licencia basada en capacidad estándar de SnapCenter :

["Licencias basadas en capacidad estándar de SnapCenter"](#)

Redes y seguridad

En una operación de base de datos híbrida que requiere una base de datos de producción local que se pueda expandir a la nube para desarrollo/prueba y recuperación ante desastres, la red y la seguridad son factores importantes a tener en cuenta al configurar el entorno y conectarse a la nube pública desde un centro de datos local.

Las nubes públicas generalmente utilizan una nube privada virtual (VPC) para aislar a diferentes usuarios dentro de una plataforma de nube pública. Dentro de una VPC individual, la seguridad se controla mediante medidas como grupos de seguridad que se pueden configurar según las necesidades del usuario para el bloqueo de una VPC.

La conectividad desde el centro de datos local a la VPC se puede proteger a través de un túnel VPN. En la puerta de enlace VPN, la seguridad se puede reforzar utilizando reglas de firewall y NAT que bloquean los intentos de establecer conexiones de red desde hosts en Internet a hosts dentro del centro de datos corporativo.

Para consideraciones de red y seguridad, revise las reglas CVO entrantes y salientes relevantes para su nube pública elegida:

- ["Reglas de grupo de seguridad para CVO - AWS"](#)
- ["Reglas de grupo de seguridad para CVO - Azure"](#)
- ["Reglas de firewall para CVO - GCP"](#)

Uso de la automatización de Ansible para sincronizar instancias de base de datos entre las instalaciones locales y la nube (opcional)

Para simplificar la administración de un entorno de base de datos de nube híbrida, NetApp recomienda enfáticamente, pero no exige, que implemente un controlador Ansible para automatizar algunas tareas de administración, como mantener sincronizadas las instancias de cómputo locales y en la nube. Esto es particularmente importante porque una instancia de cómputo desincronizada en la nube podría hacer que la base de datos recuperada en la nube sea propensa a errores debido a paquetes de kernel faltantes y otros problemas.

La capacidad de automatización de un controlador Ansible también se puede utilizar para ampliar SnapCenter para ciertas tareas, como dividir la instancia de SnapMirror para activar la copia de datos de DR para producción.

Siga estas instrucciones para configurar su nodo de control Ansible para máquinas RedHat o CentOS:

1. Requisitos para el nodo de control de Ansible:
 - a. Una máquina RHEL/CentOS con los siguientes paquetes instalados:

- i. Python3
- ii. Pip3
- iii. Ansible (versión superior a 2.10.0)
- iv. Git

Si tiene una máquina RHEL/CentOS nueva sin los requisitos anteriores instalados, siga los pasos a continuación para configurar esa máquina como el nodo de control de Ansible:

1. Habilitar el repositorio de Ansible para RHEL-8/RHEL-7

- a. Para RHEL-8 (ejecute el siguiente comando como root)

```
subscription-manager repos --enable ansible-2.9-for-rhel-8-x86_64-rpms
```

- b. Para RHEL-7 (ejecute el siguiente comando como root)

```
subscription-manager repos --enable rhel-7-server-ansible-2.9-rpms
```

2. Pegue el siguiente contenido en la Terminal

```
sudo yum -y install python3 >> install.log
sudo yum -y install python3-pip >> install.log
python3 -W ignore -m pip --disable-pip-version-check install ansible >>
install.log
sudo yum -y install git >> install.log
```

Siga estas instrucciones para configurar su nodo de control Ansible para máquinas Ubuntu o Debian:

1. Requisitos para el nodo de control de Ansible:

- a. Una máquina Ubuntu/Debian con los siguientes paquetes instalados:

- i. Python3
- ii. Pip3
- iii. Ansible (versión superior a 2.10.0)
- iv. Git

Si tiene una máquina Ubuntu/Debian nueva sin los requisitos anteriores instalados, siga los pasos a continuación para configurar esa máquina como el nodo de control de Ansible:

1. Pegue el siguiente contenido en la terminal

```
sudo apt-get -y install python3 >> outputlog.txt
sudo apt-get -y install python3-pip >> outputlog.txt
python3 -W ignore -m pip --disable-pip-version-check install ansible >>
outputlog.txt
sudo apt-get -y install git >> outputlog.txt
```

Requisitos previos para la nube pública

Antes de instalar el conector de Cloud Manager y Cloud Volumes ONTAP y configurar SnapMirror, debemos realizar algunos preparativos para nuestro entorno de nube. Esta página describe el trabajo que debe realizarse, así como las consideraciones al implementar Cloud Volumes ONTAP.

Lista de verificación de requisitos previos para la implementación de Cloud Manager y Cloud Volumes ONTAP

- Un inicio de sesión en NetApp Cloud Central
- Acceso a la red desde un navegador web a varios puntos finales
- Una ubicación de red para un conector
- Permisos del proveedor de la nube
- Redes para servicios individuales

Para obtener más información sobre lo que necesita para comenzar, visite nuestro ["documentación en la nube"](#).

Consideraciones

1. ¿Qué es un conector de Cloud Manager?

En la mayoría de los casos, un administrador de cuenta de Cloud Central debe implementar un conector en su nube o red local. El conector permite a Cloud Manager administrar recursos y procesos dentro de su entorno de nube pública.

Para obtener más información sobre los conectores, visite nuestra ["documentación en la nube"](#).

2. Dimensionamiento y arquitectura de Cloud Volumes ONTAP

Al implementar Cloud Volumes ONTAP, se le ofrece la opción de elegir entre un paquete predefinido o la creación de su propia configuración. Si bien muchos de estos valores se pueden cambiar más adelante sin generar interrupciones, hay algunas decisiones clave que se deben tomar antes de la implementación en función de las cargas de trabajo que se implementarán en la nube.

Cada proveedor de nube tiene diferentes opciones de implementación y casi cada carga de trabajo tiene sus propias propiedades únicas. NetApp tiene una ["Calculadora de TCO"](#) que puede ayudar a dimensionar las implementaciones correctamente en función de la capacidad y el rendimiento, pero se ha construido en torno a algunos conceptos básicos que vale la pena considerar:

- Capacidad requerida

- Capacidad de red de la máquina virtual en la nube
- Características de rendimiento del almacenamiento en la nube

La clave es planificar una configuración que no sólo satisfaga los requisitos actuales de capacidad y rendimiento, sino que también tenga en cuenta el crecimiento futuro. Esto generalmente se conoce como margen de capacidad y margen de rendimiento.

Si desea más información, lea la documentación sobre cómo planificar correctamente ["AWS"](#) , ["Azur"](#) , y ["GCP"](#) .

3. ¿Nodo único o alta disponibilidad?

En todas las nubes, existe la opción de implementar CVO en un solo nodo o en un par de nodos agrupados de alta disponibilidad. Dependiendo del caso de uso, es posible que desee implementar un solo nodo para ahorrar costos o un par HA para brindar mayor disponibilidad y redundancia.

Para un caso de uso de recuperación ante desastres o para crear almacenamiento temporal para desarrollo y pruebas, los nodos individuales son comunes ya que el impacto de una interrupción repentina de la zona o de la infraestructura es menor. Sin embargo, para cualquier caso de uso de producción, cuando los datos están en una sola ubicación o cuando el conjunto de datos debe tener más redundancia y disponibilidad, se recomienda alta disponibilidad.

Para obtener más información sobre la arquitectura de la versión de alta disponibilidad de cada nube, visite la documentación de ["AWS"](#) , ["Azur"](#) y ["GCP"](#) .

Descripción general de primeros pasos

Descripción general de primeros pasos

Esta sección proporciona un resumen de las tareas que deben completarse para cumplir con los requisitos previos descritos en la sección anterior. La siguiente sección proporciona una lista de tareas de alto nivel para operaciones locales y en la nube pública. Se puede acceder a los procesos y procedimientos detallados haciendo clic en los enlaces correspondientes.

En las instalaciones

- Configurar el usuario administrador de la base de datos en SnapCenter
- Requisitos previos para la instalación del complemento SnapCenter
- Instalación del complemento de host de SnapCenter
- Descubrimiento de recursos de base de datos
- Configurar el emparejamiento de clústeres de almacenamiento y la replicación de volúmenes de base de datos
- Agregue el almacenamiento de base de datos CVO SVM a SnapCenter
- Configurar la política de copia de seguridad de la base de datos en SnapCenter
- Implementar una política de respaldo para proteger la base de datos
- Validar copia de seguridad

Nube pública de AWS

- Comprobación previa al vuelo
- Pasos para implementar Cloud Manager y Cloud Volumes ONTAP en AWS
- Implementar una instancia de cómputo EC2 para la carga de trabajo de la base de datos

Haga clic en los siguientes enlaces para obtener más detalles:

["En las instalaciones"](#), ["Nube pública - AWS"](#)

Introducción a las instalaciones

La herramienta NetApp SnapCenter utiliza control de acceso basado en roles (RBAC) para administrar el acceso a los recursos de los usuarios y las concesiones de permisos, y la instalación de SnapCenter crea roles precargados. También puede crear roles personalizados según sus necesidades o aplicaciones.

En las instalaciones

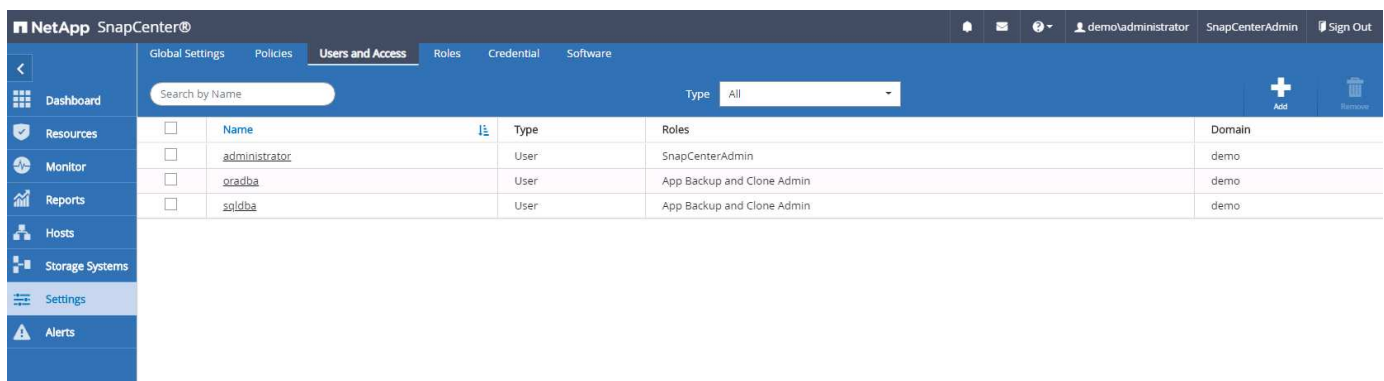
1. Configurar el usuario administrador de la base de datos en SnapCenter

Tiene sentido tener un ID de usuario administrador dedicado para cada plataforma de base de datos compatible con SnapCenter para realizar copias de seguridad, restaurar o recuperar ante desastres de bases de datos. También puede utilizar una única ID para administrar todas las bases de datos. En nuestros casos de prueba y demostración, creamos un usuario administrador dedicado tanto para Oracle como para SQL Server, respectivamente.

Ciertos recursos de SnapCenter solo se pueden aprovisionar con el rol SnapCenterAdmin. Luego se pueden asignar recursos a otros ID de usuario para acceder a ellos.

En un entorno de SnapCenter local preinstalado y configurado, es posible que ya se hayan completado las siguientes tareas. En caso contrario, los siguientes pasos crean un usuario administrador de base de datos:

1. Agregue el usuario administrador al Directorio Activo de Windows.
2. Inicie sesión en SnapCenter utilizando una ID otorgada con el rol SnapCenterAdmin.
3. Vaya a la pestaña Acceso en Configuración y Usuarios, y haga clic en Agregar para agregar un nuevo usuario. El nuevo ID de usuario está vinculado al usuario administrador creado en Windows Active Directory en el paso 1. . Asigne el rol adecuado al usuario según sea necesario. Asignar recursos al usuario administrador según corresponda.



	Name	Type	Roles	Domain
☐	administrator	User	SnapCenterAdmin	demo
☐	oradbba	User	App Backup and Clone Admin	demo
☐	sqldbba	User	App Backup and Clone Admin	demo

2. Requisitos previos para la instalación del complemento SnapCenter

SnapCenter realiza copias de seguridad, restauraciones, clonaciones y otras funciones mediante un agente de complemento que se ejecuta en los hosts de la base de datos. Se conecta al host de la base de datos y a la base de datos a través de credenciales configuradas en la pestaña Configuración y Credenciales para la instalación del complemento y otras funciones de administración. Existen requisitos de privilegios específicos según el tipo de host de destino, como Linux o Windows, así como el tipo de base de datos.

Las credenciales de los hosts de la base de datos deben configurarse antes de instalar el complemento SnapCenter. Generalmente, conviene utilizar cuentas de usuario de administrador en el host de la base de datos como credenciales de conexión del host para la instalación del complemento. También puede otorgar el mismo ID de usuario para el acceso a la base de datos mediante la autenticación basada en el sistema operativo. Por otro lado, también puede emplear la autenticación de base de datos con diferentes ID de usuario de base de datos para el acceso a la gestión de la base de datos. Si decide utilizar la autenticación basada en sistema operativo, se debe conceder acceso a la base de datos al ID de usuario administrador del sistema operativo. Para la instalación de SQL Server basada en dominio de Windows, se puede usar una cuenta de administrador de dominio para administrar todos los servidores SQL dentro del dominio.

Host de Windows para servidor SQL:

1. Si utiliza credenciales de Windows para la autenticación, debe configurar sus credenciales antes de instalar complementos.
2. Si está utilizando una instancia de SQL Server para la autenticación, debe agregar las credenciales después de instalar los complementos.
3. Si ha habilitado la autenticación SQL al configurar las credenciales, la instancia o base de datos detectada se muestra con un ícono de candado rojo. Si aparece el ícono de candado, debe especificar las credenciales de la instancia o base de datos para agregar correctamente la instancia o base de datos a un grupo de recursos.
4. Debe asignar la credencial a un usuario RBAC sin acceso de administrador del sistema cuando se cumplan las siguientes condiciones:
 - La credencial se asigna a una instancia de SQL.
 - La instancia o host de SQL se asigna a un usuario RBAC.
 - El usuario administrador de base de datos RBAC debe tener privilegios de grupo de recursos y de respaldo.

Host Unix para Oracle:

1. Debe haber habilitado la conexión SSH basada en contraseña para el usuario root o no root editando sshd.conf y reiniciando el servicio sshd. La autenticación SSH basada en contraseña en la instancia de AWS está desactivada de forma predeterminada.
2. Configure los privilegios de sudo para que el usuario no root pueda instalar e iniciar el proceso del complemento. Después de instalar el complemento, los procesos se ejecutan como un usuario root efectivo.
3. Cree credenciales con el modo de autenticación de Linux para el usuario de instalación.
4. Debe instalar Java 1.8.x (64 bits) en su host Linux.
5. La instalación del complemento de base de datos de Oracle también instala el complemento SnapCenter para Unix.

3. Instalación del complemento de host de SnapCenter

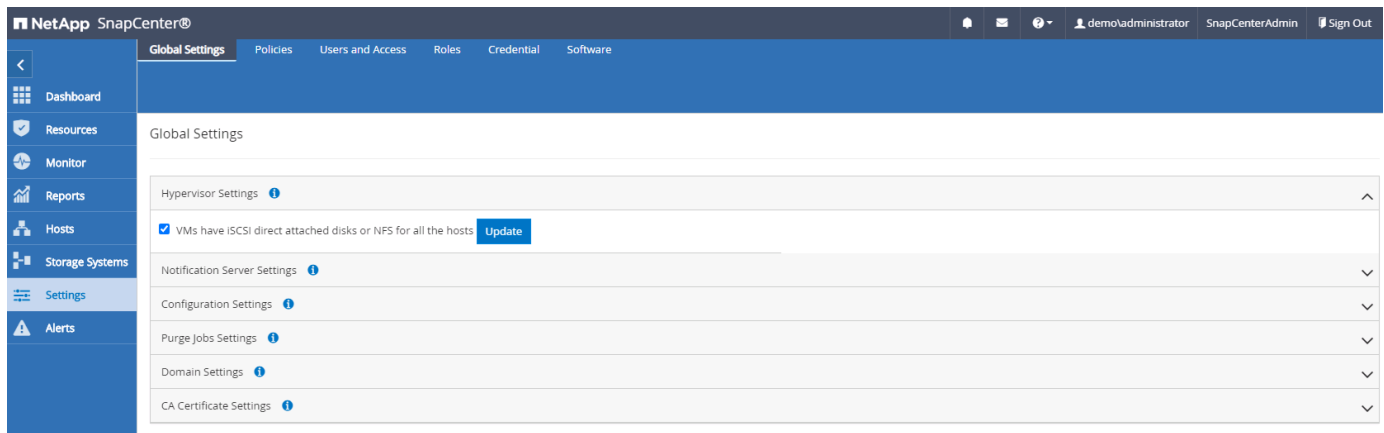


Antes de intentar instalar los complementos de SnapCenter en las instancias del servidor de base de datos en la nube, asegúrese de que se hayan completado todos los pasos de configuración enumerados en la sección de nube correspondiente para la implementación de la instancia de cómputo.

Los siguientes pasos ilustran cómo se agrega un host de base de datos a SnapCenter mientras un complemento de SnapCenter está instalado en el host. El procedimiento se aplica para agregar hosts locales y en la nube. La siguiente demostración agrega un host Windows o Linux que reside en AWS.

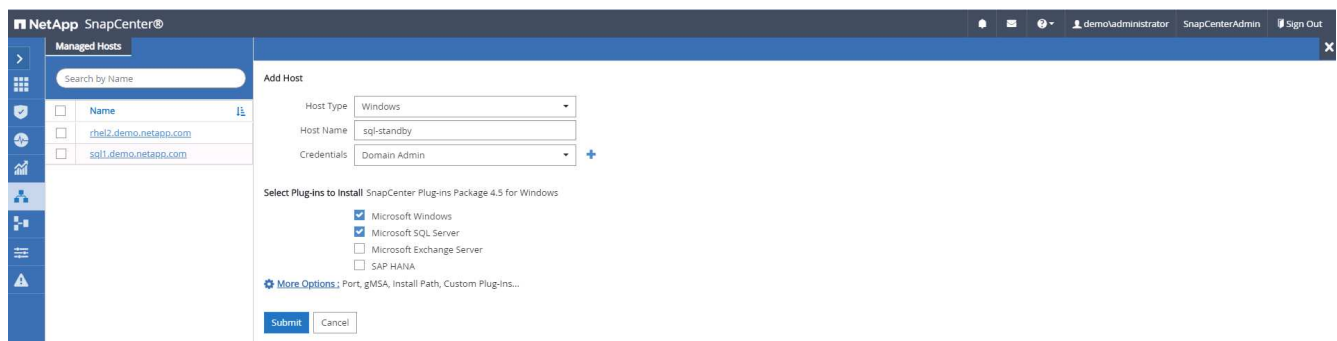
Configurar los ajustes globales de VMware de SnapCenter

Vaya a Configuración > Configuración global. Seleccione “Las máquinas virtuales tienen discos conectados directamente iSCSI o NFS para todos los hosts” en Configuración del hipervisor y haga clic en Actualizar.

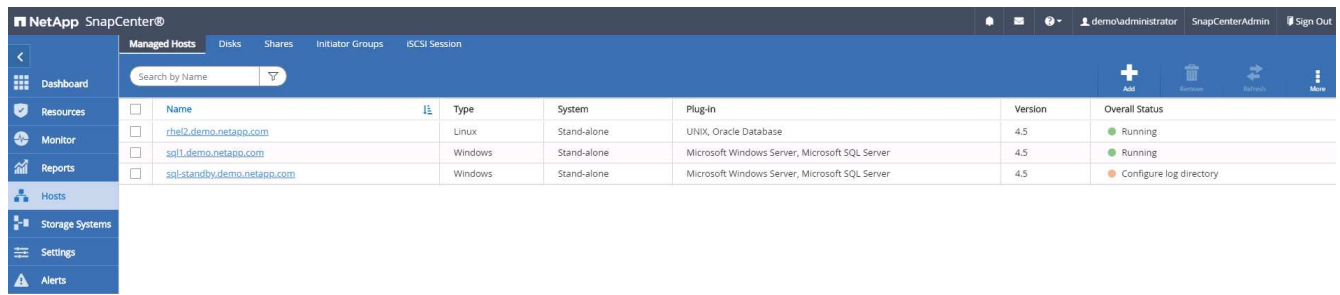


Agregar host de Windows e instalación del complemento en el host

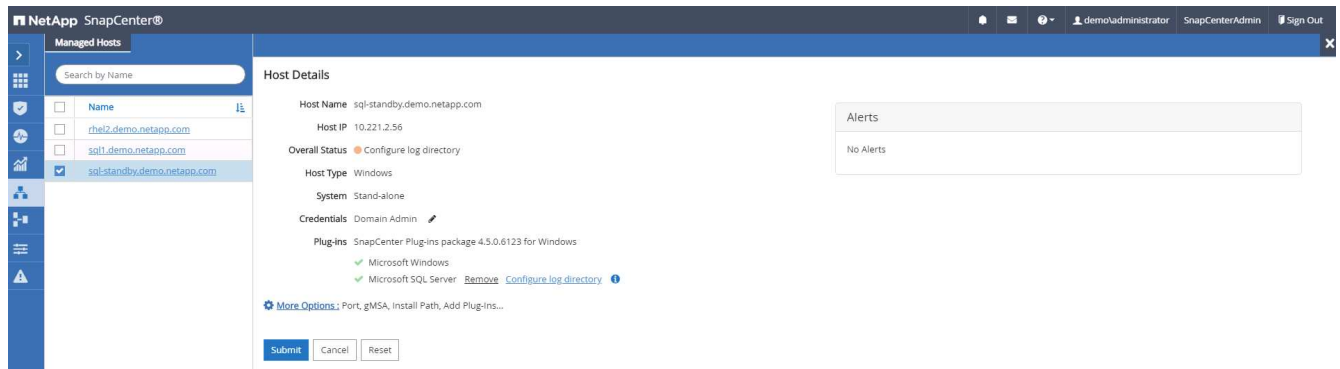
1. Inicie sesión en SnapCenter con un ID de usuario con privilegios de SnapCenterAdmin.
2. Haga clic en la pestaña Hosts en el menú de la izquierda y luego haga clic en Agregar para abrir el flujo de trabajo Agregar host.
3. Seleccione Windows como Tipo de host; el Nombre de host puede ser un nombre de host o una dirección IP. El nombre del host debe resolverse a la dirección IP del host correcta desde el host de SnapCenter . Elija las credenciales de host creadas en el paso 2. Elija Microsoft Windows y Microsoft SQL Server como los paquetes de complementos que se instalarán.



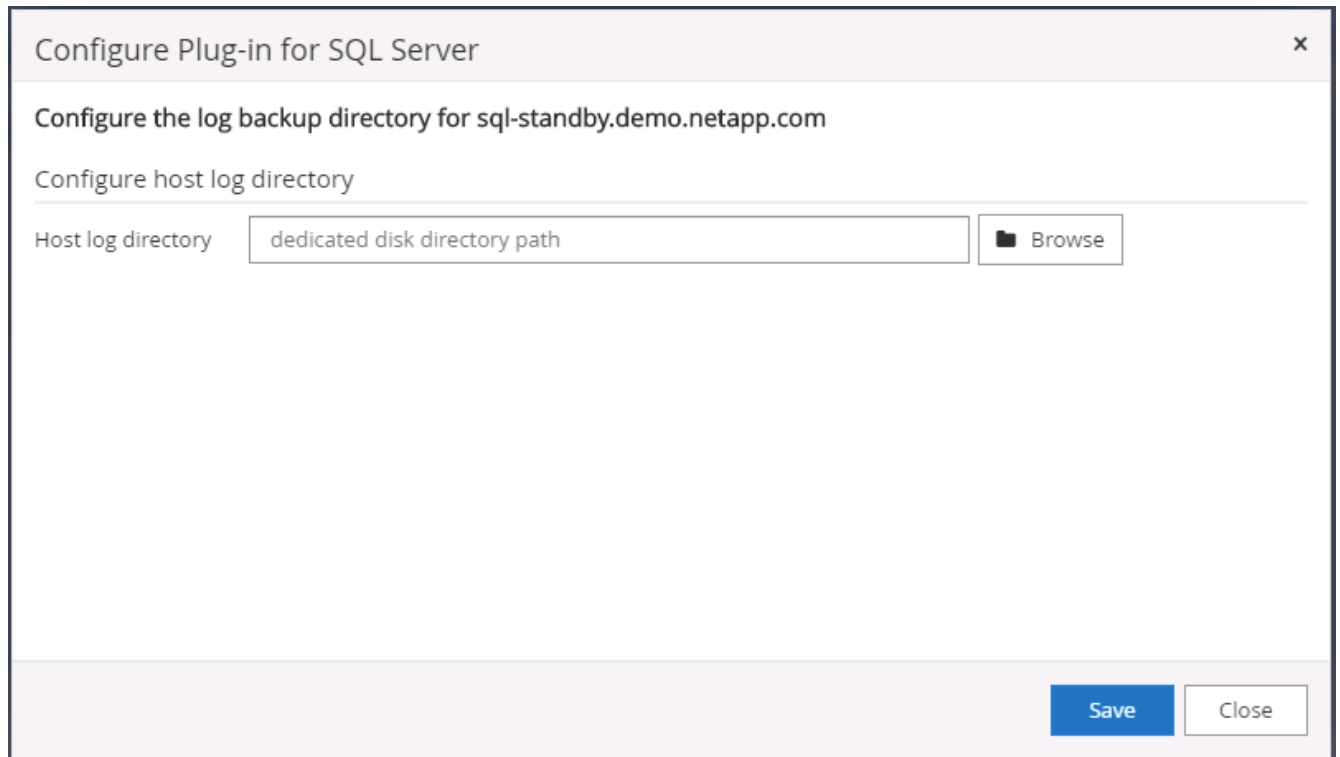
4. Una vez instalado el complemento en un host de Windows, su estado general se muestra como "Configurar directorio de registro".



5. Haga clic en el nombre del host para abrir la configuración del directorio de registro de SQL Server.



6. Haga clic en "Configurar directorio de registro" para abrir "Configurar complemento para SQL Server".



7. Haga clic en Explorar para descubrir el almacenamiento de NetApp para que se pueda configurar un directorio de registro; SnapCenter utiliza este directorio de registro para recopilar los archivos de registro de transacciones del servidor SQL. Luego haga clic en Guardar.

Configure Plug-in for SQL Server

Configure the log backup directory for sql-standby.demo.netapp.com

Configure host log directory

Host log directory Browse

Choose directory on NetApp Storage

sql-standby.demo.netapp.com

- G:\
 - System Volume Information

Save
Close



Para que se descubra el almacenamiento de NetApp provisionado en un host de base de datos, el almacenamiento (local o CVO) se debe agregar a SnapCenter, como se ilustra en el paso 6 para CVO como ejemplo.

- Una vez configurado el directorio de registro, el Estado general del complemento de host de Windows cambia a En ejecución.

NetApp SnapCenter®							
Managed Hosts							
Dashboard Search by Name + + + +							
Resources	☐	Name	Type	System	Plug-in	Version	Overall Status
Monitor	☐	rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running
Reports	☐	sql1.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running
Hosts	☐	sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running
Storage Systems							
Settings							
Alerts							

- Para asignar el host al ID de usuario de administración de la base de datos, navegue a la pestaña Acceso en Configuración y Usuarios, haga clic en el ID de usuario de administración de la base de datos (en nuestro caso, el sqldba al que se debe asignar el host) y haga clic en Guardar para completar la asignación de recursos del host.

NetApp SnapCenter®					
Global Settings Policies Users and Access Roles Credential Software					
Dashboard Search by Name Type All + +					
Resources	☐	Name	Type	Roles	Domain
Monitor	☐	administrator	User	SnapCenterAdmin	demo
Reports	☐	sqldba	User	App Backup and Clone Admin	demo
Hosts	☐	sqldba	User	App Backup and Clone Admin	demo
Storage Systems					
Settings					
Alerts					

Assign Assets

Asset Type
Host
search

	Asset Name
☐	rhel2.demo.netapp.com
☐	sql1.demo.netapp.com
☒	sql-standby.demo.netapp.com

Save
Close

Agregar host Unix e instalación del complemento en el host

1. Inicie sesión en SnapCenter con un ID de usuario con privilegios de SnapCenterAdmin.
2. Haga clic en la pestaña Hosts en el menú de la izquierda y haga clic en Agregar para abrir el flujo de trabajo Agregar host.
3. Elija Linux como tipo de host. El nombre de host puede ser el nombre de host o una dirección IP. Sin embargo, el nombre de host debe resolverse a la dirección IP de host correcta desde el host de SnapCenter . Elija las credenciales de host creadas en el paso 2. Las credenciales del host requieren privilegios de sudo. Marque Oracle Database como el complemento que se instalará, lo cual instala complementos de host de Oracle y Linux.

demoadministrator
SnapCenterAdmin
Sign Out

Add Host

Host Type
Linux
Host Name
ora-standby
Credentials
admin

Select Plug-ins to Install SnapCenter Plug-ins Package 4.5 for Linux
☒ Oracle Database
☐ SAP HANA
[More Options](#): Port, Install Path, Custom Plug-ins...

Submit
Cancel

4. Haga clic en Más opciones y seleccione “Omitir comprobaciones de preinstalación”. Se le solicitará que confirme que desea omitir la comprobación de preinstalación. Haga clic en Sí y luego en Guardar.

More Options

Port

8145

Installation Path

/opt/NetApp/snapcenter

☒

Skip preinstall checks

☒

Add all hosts in the oracle RAC

Custom Plug-ins

Choose a File

Browse

Upload

No plug-ins found.

Save

Cancel

- Haga clic en Enviar para iniciar la instalación del complemento. Se le solicitará que confirme la huella digital como se muestra a continuación.

Confirm Fingerprint

Authenticity of the host cannot be determined

Host name	Fingerprint	Valid
ora-standby.demo.netapp.com	ssh-rsa 3072 5C:02:EF:6B:63:54:59:10:84:DF:4D:6B:AB:FB:61:67	

Confirm and Submit

Close

- SnapCenter realiza la validación y el registro del host y luego el complemento se instala en el host Linux. El estado cambia de Instalando complemento a En ejecución.

NetApp SnapCenter®

Managed Hosts

Disks

Shares

Initiator Groups

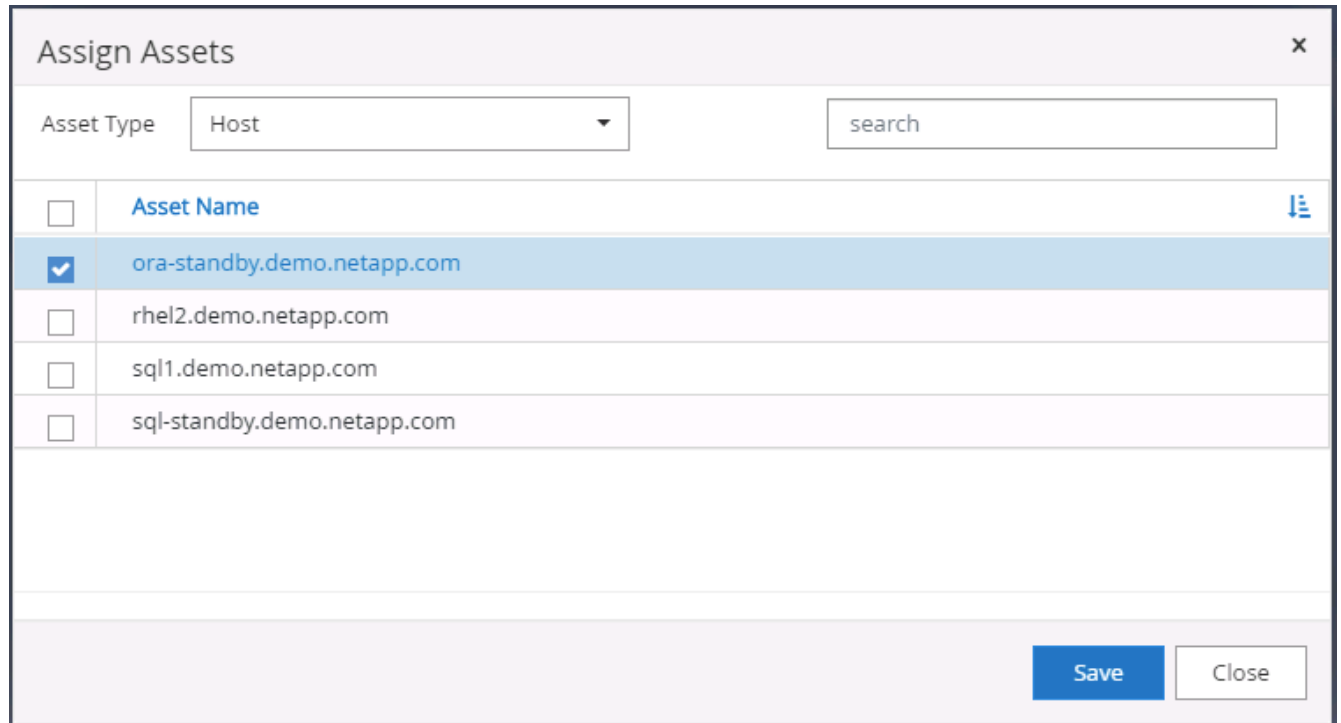
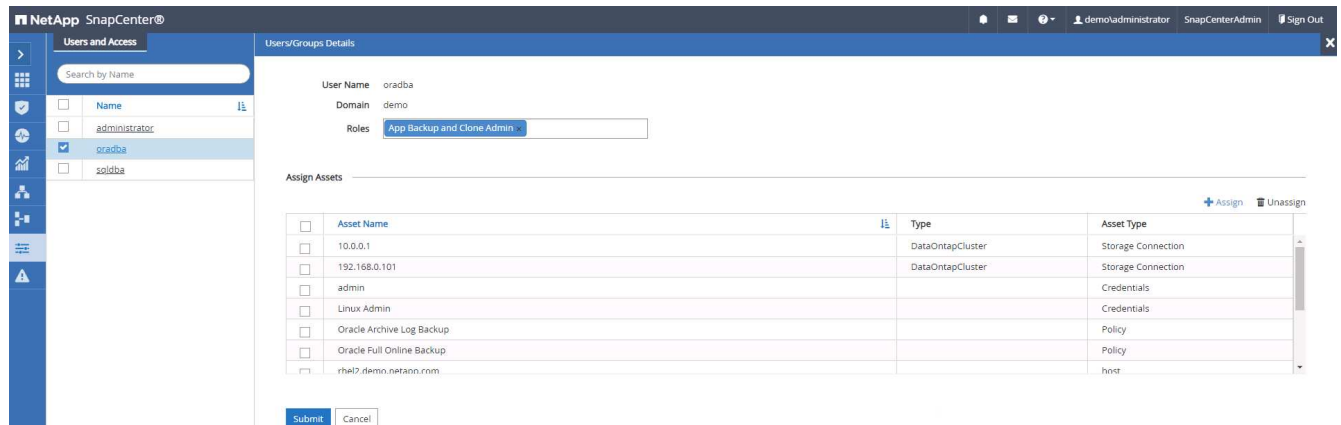
ISCSI Session

Search by Name

+

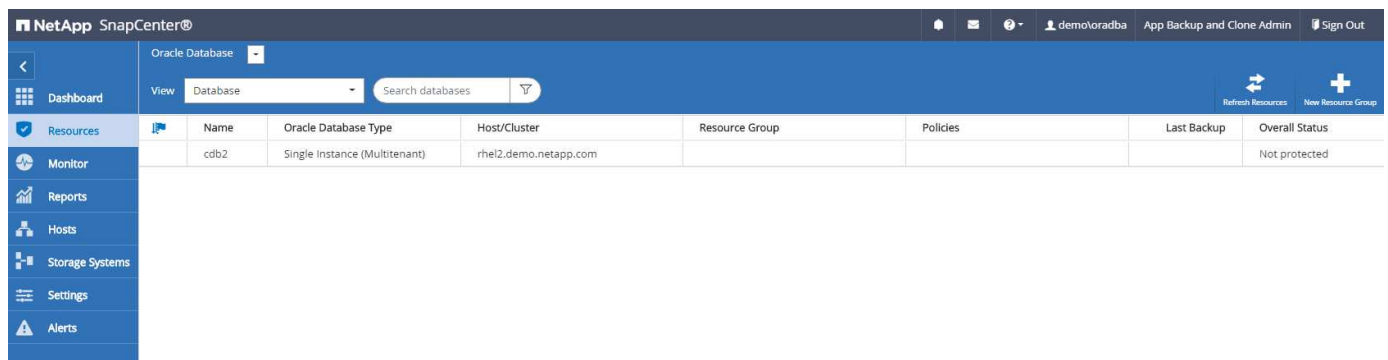
	Name	Type	System	Plug-in	Version	Overall Status
☐	ora-standby.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running
☐	rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running
☐	sql1.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running
☐	sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running

- Asigne el host recién agregado al ID de usuario de administración de base de datos adecuado (en nuestro caso, oradba).



4. Descubrimiento de recursos de bases de datos

Con una instalación exitosa del complemento, los recursos de la base de datos en el host se pueden descubrir de inmediato. Haga clic en la pestaña Recursos en el menú de la izquierda. Dependiendo del tipo de plataforma de base de datos, hay varias vistas disponibles, como la base de datos, el grupo de recursos, etc. Es posible que tengas que hacer clic en la pestaña Actualizar recursos si no se detectan ni se muestran los recursos del host.



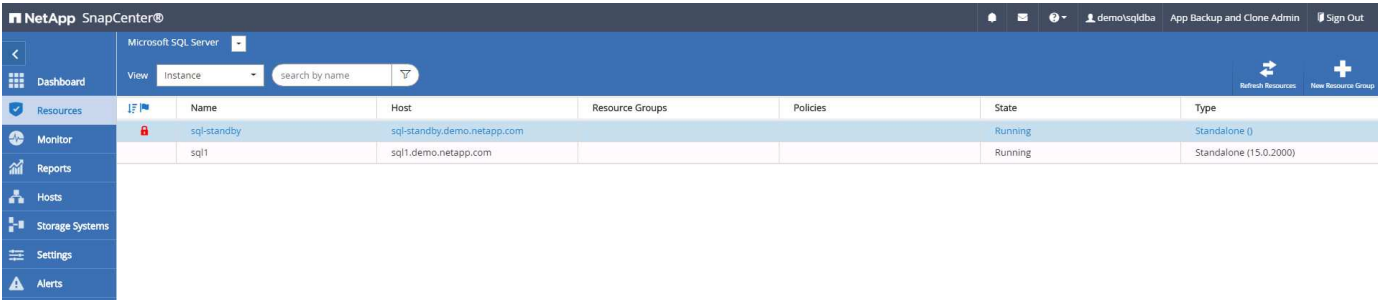
Cuando se descubre la base de datos inicialmente, el estado general se muestra como "No protegido". La captura de pantalla anterior muestra una base de datos Oracle que aún no está protegida por una política de respaldo.

Cuando se configura o se establece una política de copia de seguridad y se ha ejecutado una copia de seguridad, el Estado general de la base de datos muestra el estado de la copia de seguridad como "Copia de seguridad realizada correctamente" y la marca de tiempo de la última copia de seguridad. La siguiente captura de pantalla muestra el estado de la copia de seguridad de una base de datos de usuario de SQL Server.

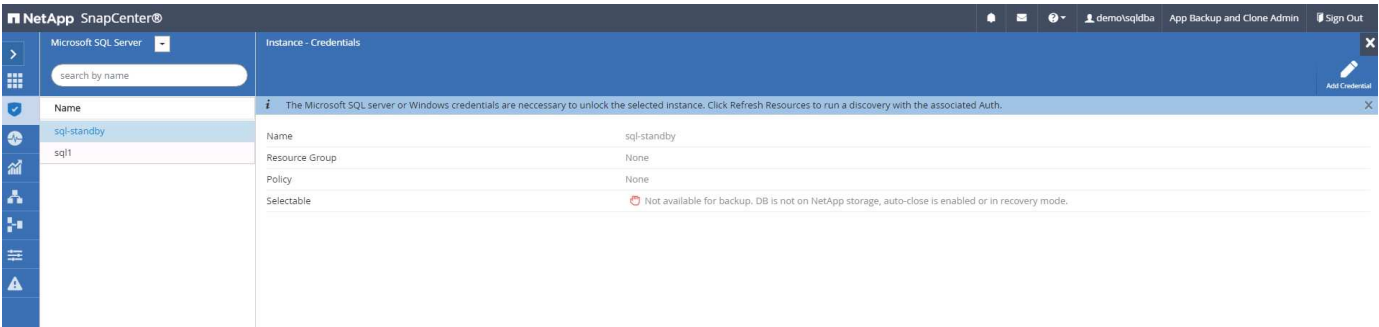


Name	Instance	Host	Last Backup	Overall Status	Type
master	sql1	sql1.demo.netapp.com		Not available for backup	System database
model	sql1	sql1.demo.netapp.com		Not available for backup	System database
msdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tempdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tpcc	sql1	sql1.demo.netapp.com	09/14/2021 2:35:07 PM	Backup succeeded	User database

Si las credenciales de acceso a la base de datos no están configuradas correctamente, un botón de candado rojo indica que la base de datos no es accesible. Por ejemplo, si las credenciales de Windows no tienen acceso de administrador del sistema a una instancia de base de datos, entonces las credenciales de la base de datos deben reconfigurarse para desbloquear el candado rojo.



Name	Host	Resource Groups	Policies	State	Type
sql-standby	sql-standby.demo.netapp.com			Running	Standalone ()
sql1	sql1.demo.netapp.com			Running	Standalone (15.0.2000)



Name	Instance - Credentials
sql-standby	The Microsoft SQL server or Windows credentials are necessary to unlock the selected instance. Click Refresh Resources to run a discovery with the associated Auth. Name: sql-standby Resource Group: None Policy: None Selectable: Not available for backup. DB is not on NetApp storage, auto-close is enabled or in recovery mode.

Una vez configuradas las credenciales adecuadas, ya sea en el nivel de Windows o en el nivel de base de datos, el candado rojo desaparece y se recopila y revisa la información del tipo de SQL Server.

NetApp SnapCenter

Microsoft SQL Server

View: Instance search by name

Name	Host	Resource Groups	Policies	State	Type
sql1	sql1.demo.netapp.com			Running	Standalone (15.0.2000)
sql-standby	sql-standby.demo.netapp.com			Running	Standalone (15.0.2000)

5. Configurar el emparejamiento de clústeres de almacenamiento y la replicación de volúmenes de bases de datos

Para proteger los datos de su base de datos local utilizando una nube pública como destino, los volúmenes de base de datos del clúster ONTAP local se replican en el CVO de la nube mediante la tecnología SnapMirror de NetApp . Los volúmenes de destino replicados se pueden clonar luego para DEV/OPS o recuperación ante desastres. Los siguientes pasos de alto nivel le permiten configurar el emparejamiento de clústeres y la replicación de volúmenes de bases de datos.

1. Configure LIF entre clústeres para el emparejamiento de clústeres tanto en el clúster local como en la instancia del clúster CVO. Este paso se puede realizar con ONTAP System Manager. Una implementación de CVO predeterminada tiene LIF entre clústeres configurados automáticamente.

Clúster local:

ONTAP System Manager (Return to classic version)

Search actions, objects, and pages

Overview

IPspaces

Cluster	Broadcast Domains
Default	Storage VMs svm_onPrem Broadcast Domains Default

Broadcast Domains

Cluster	9000 MTU	IPspace: Cluster
Default	1500 MTU	IPspace: Default onPrem-01 e0a e0b e0c e0d e0e e0f e0g e0h e0i e0j e0k e0l e0m e0n e0o e0p e0q e0r e0s e0t e0u e0v e0w e0x e0y e0z

Network Interfaces

Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Protocols	Type
onPrem-01_IC	✓		Default	192.168.0.111	onPrem-01	e0b		Intercluster
onPrem-01_mgmt1	✓		Default	192.168.0.111	onPrem-01	e0c		Cluster/Node Mgmt
cluster_mgmt	✓		Default	192.168.0.101	onPrem-01	e0a		Cluster/Node Mgmt

Clúster CVO objetivo:

ONTAP System Manager

Search actions, objects, and pages

Overview

IPspaces

Cluster	Broadcast Domains
Default	Storage VMs svm_hybridcvo Broadcast Domains Default

Broadcast Domains

Cluster	9000 MTU	IPspace: Cluster
Default	9001 MTU	IPspace: Default hybridcvo-01 e0a hybridcvo-02 e0b

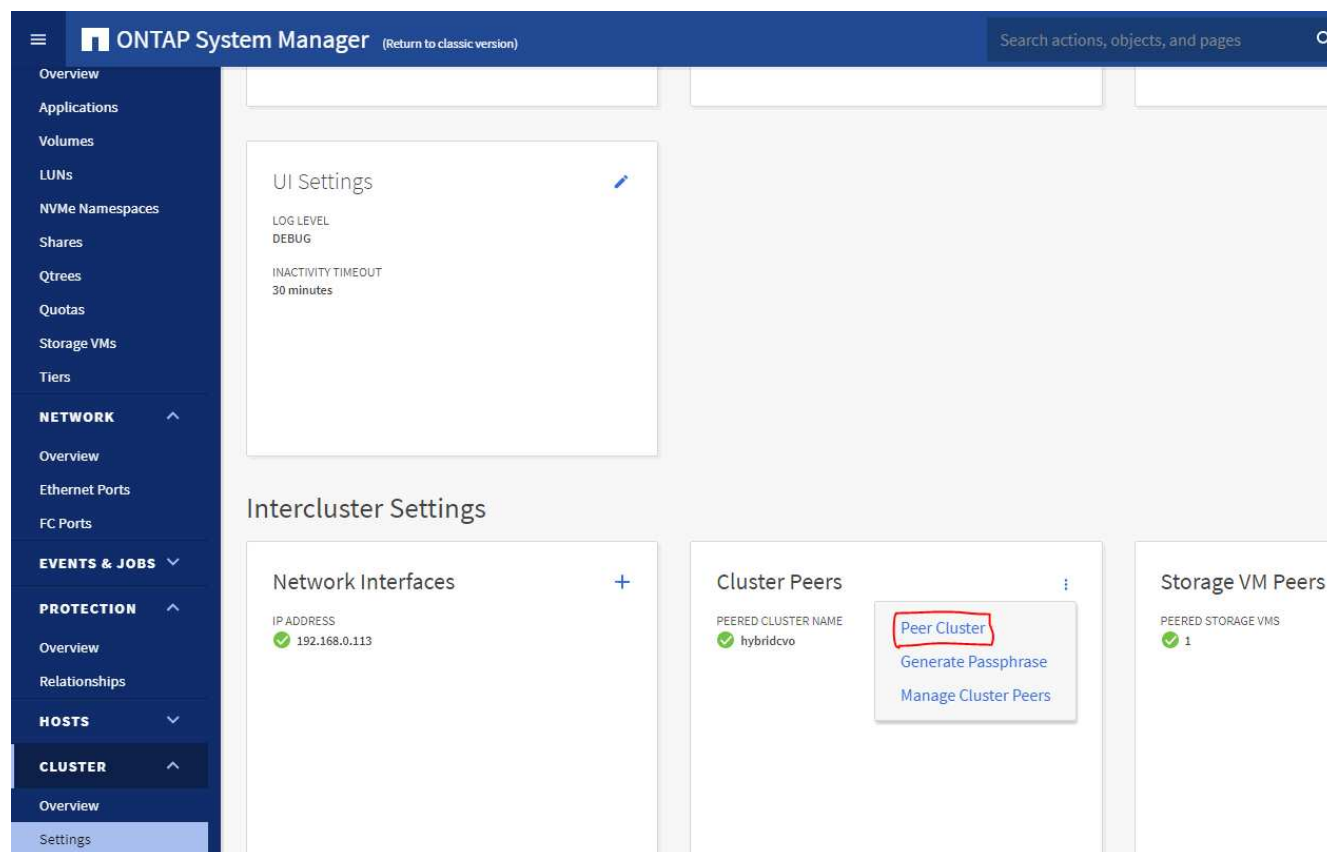
Network Interfaces

Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Protocols	Type	Throughput (I)
hybridcvo-02_mgmt1	✓		Default	10.221.2.104	hybridcvo-02	e0a		Cluster/Node Mgmt	0
Inter_1	✓		Default	10.221.1.180	hybridcvo-01	e0a		Intercluster, Cluster/Node Mgmt	0.02
Inter_2	✓		Default	10.221.2.250	hybridcvo-02	e0a		Intercluster, Cluster/Node Mgmt	0.03
iscsi_1	✓	svm_hybridcvo	Default	10.221.1.5	hybridcvo-01	e0a	ISCSI	Data	0
iscsi_2	✓	svm_hybridcvo	Default	10.221.2.168	hybridcvo-02	e0a	ISCSI	Data	0

2. Una vez configurados los LIF entre clústeres, se puede configurar el emparejamiento de clústeres y la replicación de volúmenes mediante arrastrar y soltar en NetApp Cloud Manager. Ver "[Introducción a la nube pública de AWS](#)" Para más detalles.

Como alternativa, el emparejamiento de clústeres y la replicación de volúmenes de base de datos se pueden realizar mediante el Administrador del sistema ONTAP de la siguiente manera:

3. Inicie sesión en el Administrador del sistema ONTAP . Vaya a Clúster > Configuración y haga clic en Clúster de pares para configurar el emparejamiento del clúster con la instancia CVO en la nube.



4. Vaya a la pestaña Volúmenes. Seleccione el volumen de base de datos que desea replicar y haga clic en Proteger.

ONTAP System Manager (Return to classic version)

Search actions, objects, and pages

DASHBOARD

STORAGE

Overview

Applications

Volumes

LUNs

NVMe Namespaces

Shares

Qtrees

Quotas

Storage VMs

Tiers

NETWORK

Overview

Ethernet Ports

FC Ports

EVENTS & JOBS

PROTECTION

HOSTS

CLUSTER

Volumes

+ Add Delete **Protect** More

Name

rhel2_u03 All Volumes

Overview Snapshot Copies Clone Hierarchy SnapMirror (Local or Remote)

onPrem_data

rhel2_u01

rhel2_u02

☒ rhel2_u03

rhel2_u0309232119421203118

sql1_data

sql1_log

sql1_snapctr

svm_onPrem_root

STATUS

Online

STYLE

FlexVol

MOUNT PATH

/rhel2_u03

STORAGE VM

svm_onPrem

LOCAL TIER

onPrem_01_SSD_1

SNAPSHOT POLICY

default

QUOTA

Off

TYPE

Read Write

SPACE RESERVATION

Capacity

0% 10% 20% 30% 40% 50%

SNAPSHOT CAPACITY

0 Bytes Available 2.36 GB Used 2.36 GB Overflow

Performance

Hour Day Week

Latency

1.5

1

- Establezca la política de protección en Asincrónica. Seleccione el clúster de destino y el SVM de almacenamiento.

ONTAP System Manager (Return to classic version)

Search actions, objects, and pages

DASHBOARD

STORAGE

Overview

Applications

Volumes

LUNs

NVMe Namespaces

Shares

Qtrees

Quotas

Storage VMs

Tiers

NETWORK

Overview

Ethernet Ports

FC Ports

EVENTS & JOBS

PROTECTION

HOSTS

CLUSTER

Protect Volumes

PROTECTION POLICY

Asynchronous

Source

CLUSTER

onPrem

STORAGE VM

svm_onPrem

SELECTED VOLUMES

rhel2_u03

Destination

CLUSTER

hybridcvo

STORAGE VM

svm_hybridcvo

Destination Settings

2 matching labels

VOLUME NAME

PREFIX

vol_ <SourceVolumeName> SUFFIX

_dest

☐ Override default storage service name

Configuration Details

☒ Initialize relationship

☐ Enable FabricPool

Save Cancel

- Valide que el volumen esté sincronizado entre el origen y el destino y que la relación de replicación sea saludable.

Volumes																	
+ Add Delete Protect More																	
☐ ☐ ☐ ☒ ☐	Name	rhel2_u03 All Volumes															
	onPrem_data																
	rhel2_u01																
	rhel2_u02																
	rhel2_u03																
		Overview Snapshot Copies Clone Hierarchy SnapMirror (Local or Remote)															
		<table> <tr> <th>Source</th><th>Destination</th><th>Protection Policy</th><th>Relationship Health</th><th>Relationship Status</th><th>Lag</th></tr> <tr> <td>svm_onPremrhel2_u03</td><td>svm_hybridcvorhel2_u03_dr</td><td>MirrorAllSnapshots</td><td>Healthy</td><td>Mirrored</td><td>12 seconds</td></tr> </table>				Source	Destination	Protection Policy	Relationship Health	Relationship Status	Lag	svm_onPremrhel2_u03	svm_hybridcvorhel2_u03_dr	MirrorAllSnapshots	Healthy	Mirrored	12 seconds
Source	Destination	Protection Policy	Relationship Health	Relationship Status	Lag												
svm_onPremrhel2_u03	svm_hybridcvorhel2_u03_dr	MirrorAllSnapshots	Healthy	Mirrored	12 seconds												

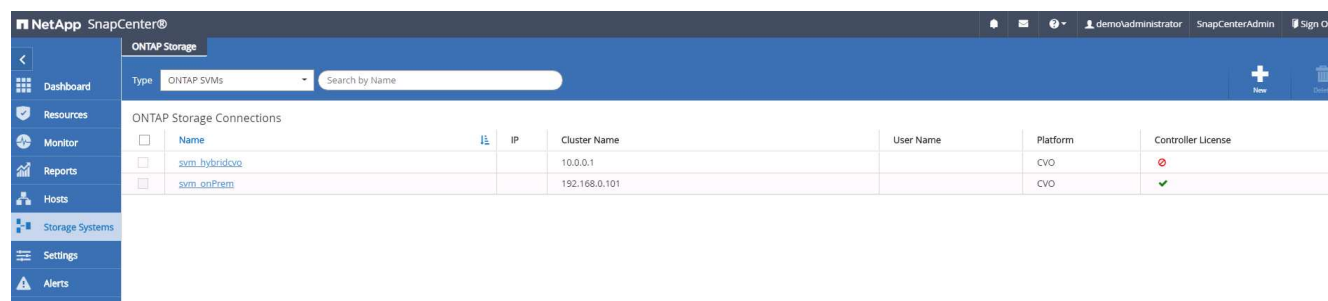
6. Agregue el almacenamiento de base de datos CVO SVM a SnapCenter

1. Inicie sesión en SnapCenter con un ID de usuario con privilegios de SnapCenterAdmin.
2. Haga clic en la pestaña Sistema de almacenamiento en el menú y, a continuación, haga clic en Nuevo para agregar un SVM de almacenamiento CVO que aloje volúmenes de base de datos de destino replicados en SnapCenter. Ingrese la IP de administración del clúster en el campo Sistema de almacenamiento e ingrese el nombre de usuario y la contraseña adecuados.

3. Haga clic en Más opciones para abrir opciones de configuración de almacenamiento adicionales. En el campo Plataforma, seleccione Cloud Volumes ONTAP, marque Secundario y luego haga clic en Guardar.

4. Asigne los sistemas de almacenamiento a los ID de usuario de administración de la base de datos de

SnapCenter como se muestra en [3. Instalación del complemento de host de SnapCenter](#).

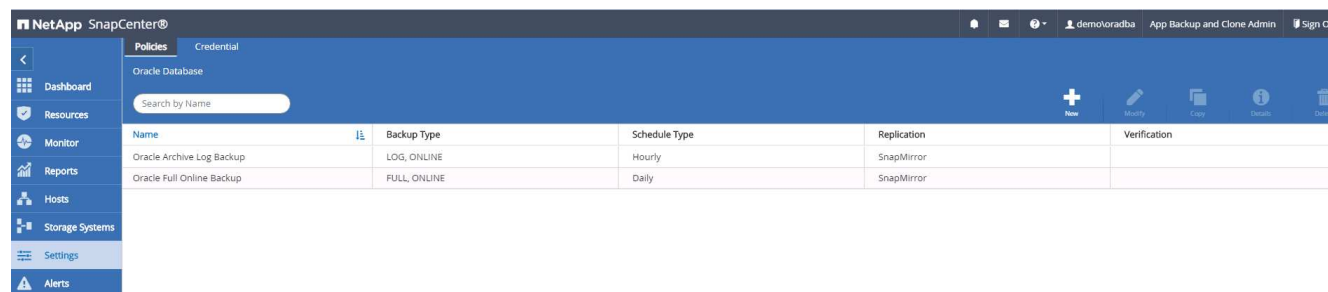


7. Configurar la política de copia de seguridad de la base de datos en SnapCenter

Los siguientes procedimientos demuestran cómo crear una política de copia de seguridad completa de una base de datos o de un archivo de registro. La política puede luego implementarse para proteger los recursos de las bases de datos. El objetivo de punto de recuperación (RPO) o el objetivo de tiempo de recuperación (RTO) dicta la frecuencia de las copias de seguridad de bases de datos y/o registros.

Cree una política de copia de seguridad de base de datos completa para Oracle

1. Inicie sesión en SnapCenter como un ID de usuario de administración de base de datos, haga clic en Configuración y, a continuación, en Políticas.



2. Haga clic en Nuevo para iniciar un nuevo flujo de trabajo de creación de una política de respaldo o elegir una política existente para modificarla.

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Provide a policy name

Policy name

Oracle Full Online Backup

Details

Backup all data and log files

Previous

Next

3. Seleccione el tipo de copia de seguridad y la frecuencia de programación.

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Modify Oracle Database Backup Policy

Select Oracle database backup options

Choose backup type

☒ Online backup

☒ Datafiles, control files, and archive logs

☐ Datafiles and control files

☐ Archive logs

☐ Offline backup

i

☒ Mount

☐ Shutdown

☐ Save state of PDBs

i

Choose schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

☐ On demand

☐ Hourly

☒ Daily

Previous

Next

4. Establezca la configuración de retención de copias de seguridad. Esto define cuántas copias de seguridad de la base de datos completa se deben conservar.

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Retention settings

Daily retention settings

Data backup retention settings

Total Snapshot copies to keep

7

Keep Snapshot copies for

14

days

Archive Log backup retention settings

Total Snapshot copies to keep

7

Keep Snapshot copies for

14

days

Previous

Next

5. Seleccione las opciones de replicación secundaria para enviar copias de seguridad de instantáneas primarias locales para que se repliquen en una ubicación secundaria en la nube.

28

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options ⓘ

☒ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Daily ⓘ

Error retry count

3 ⓘ

Previous

Next

6. Especifique cualquier script opcional para ejecutar antes y después de ejecutar una copia de seguridad.

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Specify optional scripts to run before and after performing a backup job

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Prescript arguments

Postscript full path

/var/opt/snapcenter/spl/scripts/

Enter Postscript path

Postscript arguments

Script timeout

60

secs

Previous

Next

7. Ejecute la verificación de copia de seguridad si lo desea.

30

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select the options to run backup verification

Run Verifications for following backup schedules

Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.

☐ Daily

Verification script commands

Script timeout

60secs

Prescript full path

/var/opt/snapcenter/spl/scripts/Enter Prescript path

Prescript arguments

Choose optional arguments...

Postscript full path

/var/opt/snapcenter/spl/scripts/Enter Postscript path

Postscript arguments

Choose optional arguments...

Previous

Next

8. Resumen.

31

1

Name

2

Backup Type

3

Retention

4

Replication

5

Script

6

Verification

7

Summary

Summary

Policy name	Oracle Full Online Backup
Details	Backup all data and log files
Backup type	Online backup
Schedule type	Daily
RMAN catalog backup	Disabled
Archive log pruning	None
On demand data backup retention	None
On demand archive log backup retention	None
Hourly data backup retention	None
Hourly archive log backup retention	None
Daily data backup retention	Delete Snapshot copies older than : 14 days
Daily archive log backup retention	Delete Snapshot copies older than : 14 days
Weekly data backup retention	None
Weekly archive log backup retention	None
Monthly data backup retention	None
Monthly archive log backup retention	None
Replication	SnapMirror enabled , Secondary policy label: Daily , Error retry count: 3

Previous

Finish

Crear una política de copia de seguridad del registro de base de datos para Oracle

1. Inicie sesión en SnapCenter con un ID de usuario de administración de base de datos, haga clic en Configuración y, a continuación, en Políticas.
2. Haga clic en Nuevo para iniciar un nuevo flujo de trabajo de creación de una política de respaldo o elija una política existente para modificarla.

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Provide a policy name

Policy name

Details

Oracle Archive Log Backup

Backup Oracle archive logs

Previous

Next

3. Seleccione el tipo de copia de seguridad y la frecuencia de programación.

33

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select Oracle database backup options

Choose backup type

☒ Online backup

☐ Datafiles, control files, and archive logs

☐ Datafiles and control files

☒ Archive logs

☐ Offline backup

☒ Mount

☐ Shutdown

☐ Save state of PDBs

Choose schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

☐ On demand

☒ Hourly

☐ Daily

Previous

Next

4. Establecer el período de retención de registros.

34

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Retention settings

Hourly retention settings

Data backup retention settings

Total Snapshot copies to keep

7

Keep Snapshot copies for

14 days

Archive Log backup retention settings

Total Snapshot copies to keep

7

Keep Snapshot copies for

7 days

Previous

Next

5. Habilitar la replicación a una ubicación secundaria en la nube pública.

35

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options

☒ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Hourly

Error retry count

3

Previous

Next

6. Especifique cualquier script opcional para ejecutar antes y después de la copia de seguridad del registro.

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Specify optional scripts to run before and after performing a backup job

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Prescript arguments

Postscript full path

/var/opt/snapcenter/spl/scripts/

Enter Postscript path

Postscript arguments

Script timeout

60

secs

Previous

Next

7. Especifique cualquier script de verificación de copia de seguridad.

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select the options to run backup verification

Run Verifications for following backup schedules

Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.

Verification script commands

Script timeout

60

secs

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Prescript arguments

Choose optional arguments...

Postscript full path

/var/opt/snapcenter/spl/scripts/

Enter Postscript path

Postscript arguments

Choose optional arguments...

Previous

Next

8. Resumen.

1

Name

2

Backup Type

3

Retention

4

Replication

5

Script

6

Verification

7

Summary

Summary

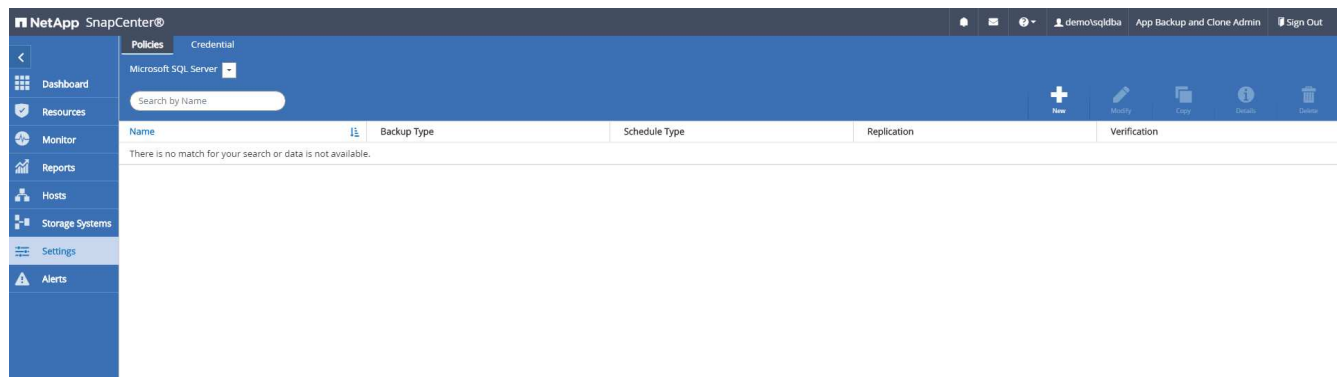
Policy name	Oracle Archive Log Backup
Details	Backup Oracle archive logs
Backup type	Online backup
Schedule type	Hourly
RMAN catalog backup	Disabled
Archive log pruning	None
On demand data backup retention	None
On demand archive log backup retention	None
Hourly data backup retention	None
Hourly archive log backup retention	Delete Snapshot copies older than : 7 days
Daily data backup retention	None
Daily archive log backup retention	None
Weekly data backup retention	None
Weekly archive log backup retention	None
Monthly data backup retention	None
Monthly archive log backup retention	None
Replication	SnapMirror enabled , Secondary policy label: Hourly , Error retry count: 3

Previous

Finish

Crear una política de copia de seguridad de base de datos completa para SQL

1. Inicie sesión en SnapCenter con un ID de usuario de administración de base de datos, haga clic en Configuración y, a continuación, en Políticas.



2. Haga clic en Nuevo para iniciar un nuevo flujo de trabajo de creación de una política de respaldo o elija una política existente para modificarla.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Provide a policy name

Policy name

SQL Server Full Backup

Details

Backup all data and log files

Previous

Next

3. Defina la opción de copia de seguridad y programe la frecuencia. Para SQL Server configurado con un grupo de disponibilidad, se puede configurar una réplica de respaldo preferida.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select SQL server backup options

Choose backup type

☒ Full backup and log backup

☐ Full backup

☐ Log backup

☐ Copy only backup

Maximum databases backed up per Snapshot copy:

Availability Group Settings

Schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

☐ On demand

☐ Hourly

☒ Daily

☐ Weekly

☐ Monthly

Previous

Next

4. Establecer el período de retención de la copia de seguridad.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Retention settings

Retention settings for up-to-the-minute restore operation ⓘ

☒ Keep log backups applicable to last

7

full backups

☐ Keep log backups applicable to last

14

days

Full backup retention settings ⓘ

Daily

☒ Total Snapshot copies to keep

7

☐ Keep Snapshot copies for

14

days

Previous

Next

5. Habilitar la replicación de copias de seguridad en una ubicación secundaria en la nube.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options

☒ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Daily

Error retry count

3

Previous

Next

6. Especifique cualquier script opcional para ejecutar antes o después de un trabajo de copia de seguridad.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Specify optional scripts to run before performing a backup job

Prescript full path

Prescript arguments

Specify optional scripts to run after performing a backup job

Postscript full path

Postscript arguments

Script timeout

Choose optional arguments...

Choose optional arguments...

60secs

Previous

Next

7. Especifique las opciones para ejecutar la verificación de copia de seguridad.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select the options to run backup verification

Run verifications for the following backup schedules

Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.

☐ Daily

Database consistency checks options

☒ Limit the integrity structure to physical structure of the database (PHYSICAL_ONLY)

☒ Suppress all information message (NO_INFOMSGS)

☐ Display all reported error messages per object (ALL_ERRORMSGSGS)

☐ Do not check non-clustered indexes (NOINDEX)

☐ Limit the checks and obtain the locks instead of using an internal database Snapshot copy (TABLOCK)

Log backup

☐ Verify log backup.

Verification script settings

Script timeout secs

Previous

Next

8. Resumen.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Summary

Policy name	SQL Server Full Backup
Details	Backup all data and log files
Backup type	Full backup and log backup
Availability group settings	Backup only on preferred backup replica
Schedule Type	Daily
UTM retention	Total backup copies to retain : 7
Daily Full backup retention	Total backup copies to retain : 7
Replication	SnapMirror enabled , Secondary policy label: Daily , Error retry count: 3
Backup prescript settings	undefined Prescript arguments:
Backup postscript settings	undefined Postscript arguments:
Verification for backup schedule type	none
Verification prescript settings	undefined Prescript arguments:
Verification postscript settings	undefined Postscript arguments:

Previous

Finish

Cree una política de copia de seguridad del registro de base de datos para SQL.

1. Inicie sesión en SnapCenter con un ID de usuario de administración de base de datos, haga clic en Configuración > Políticas y luego en Nuevo para iniciar un nuevo flujo de trabajo de creación de políticas.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Provide a policy name

Policy name

Details

SQL Server Log Backup

Backup SQL server log

Previous

Next

2. Defina la opción de copia de seguridad del registro y programe la frecuencia. Para SQL Server configurado con un grupo de disponibilidad, se puede configurar una réplica de respaldo preferida.

47

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select SQL server backup options

Choose backup type

☐ Full backup and log backup

☐ Full backup

☒ Log backup

☐ Copy only backup

Maximum databases backed up per Snapshot copy:

100

Availability Group Settings

Schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

☐ On demand

☒ Hourly

☐ Daily

☐ Weekly

☐ Monthly

Previous

Next

3. La política de copia de seguridad de datos del servidor SQL define la retención de la copia de seguridad del registro; acepte los valores predeterminados aquí.

48

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Log backup retention settings

Up-to-the-minute (UTM) retention settings retains log backups created as part of full backup and full and log backup operations. UTM retention settings also decides for how many full backups the log backups are to be retained. For example, if UTM retention settings is configured to retain log backups of the last 5 full backups, then the log backups of the last 5 full backups are retained and the rest are deleted.

Previous

Next

4. Habilitar la replicación de copias de seguridad de registros en un servidor secundario en la nube.

New SQL Server Backup Policy ✕

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options ⓘ

☒ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label Hourly ⓘ

Error retry count 3 ⓘ

Previous

Next

5. Especifique cualquier script opcional para ejecutar antes o después de un trabajo de copia de seguridad.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Specify optional scripts to run before performing a backup job

Prescript full path

Prescript arguments

Specify optional scripts to run after performing a backup job

Postscript full path

Postscript arguments

Script timeout

Choose optional arguments...

Choose optional arguments...

60secs

Previous

Next

6. Resumen.

1

Name

2

Backup Type

3

Retention

4

Replication

5

Script

6

Verification

7

Summary

Summary

Policy name	SQL Server Log Backup
Details	Backup SQL server log
Backup type	Log transaction backup
Availability group settings	Backup only on preferred backup replica
Schedule Type	Hourly
Replication	SnapMirror enabled , Secondary policy label: Hourly , Error retry count: 3
Backup prescript settings	undefined Prescript arguments:
Backup postscript settings	undefined Postscript arguments:
Verification for backup schedule type	none
Verification prescript settings	undefined Prescript arguments:
Verification postscript settings	undefined Postscript arguments:

Previous

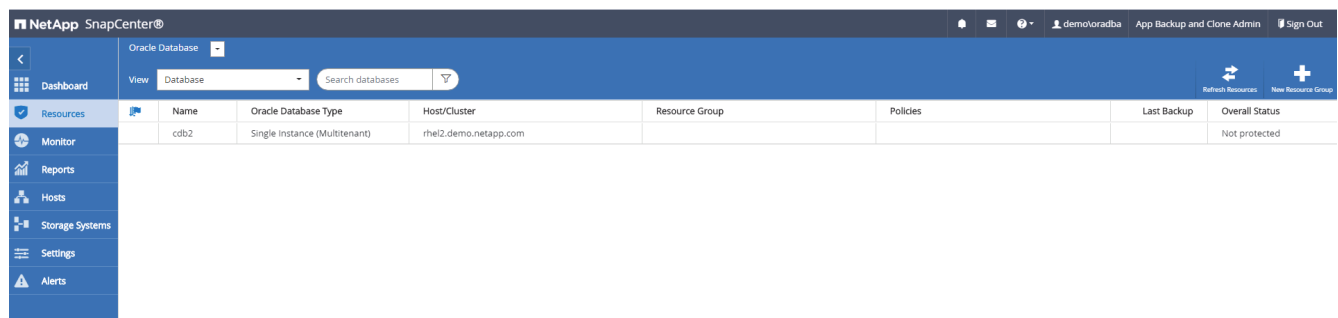
Finish

8. Implementar una política de respaldo para proteger la base de datos

SnapCenter utiliza un grupo de recursos para realizar copias de seguridad de una base de datos en una agrupación lógica de recursos de base de datos, como varias bases de datos alojadas en un servidor, una base de datos que comparte los mismos volúmenes de almacenamiento, varias bases de datos que respaldan una aplicación comercial, etc. La protección de una única base de datos crea un grupo de recursos propio. Los siguientes procedimientos demuestran cómo implementar una política de respaldo creada en la sección 7 para proteger las bases de datos de Oracle y SQL Server.

Cree un grupo de recursos para realizar una copia de seguridad completa de Oracle

1. Inicie sesión en SnapCenter con un ID de usuario de administración de base de datos y navegue a la pestaña Recursos. En la lista desplegable Ver, elija Base de datos o Grupo de recursos para iniciar el flujo de trabajo de creación del grupo de recursos.



2. Proporcione un nombre y etiquetas para el grupo de recursos. Puede definir un formato de nombre para la

copia de instantánea y omitir el destino del registro de archivo redundante si está configurado.

NetApp SnapCenter®

Oracle Database

Search databases

Name

cdb2

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide a name and tags for the resource group

Name

Tags

☒ Use custom name format for Snapshot copy

Backup settings

Exclude archive log destinations from backup

3. Agregue recursos de base de datos al grupo de recursos.

NetApp SnapCenter®

Oracle Database

Search databases

Name

cdb2

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Add resources to Resource Group

Host

Available Resources

search available resources

Selected Resources

cdb2 (rhe12.demo.netapp.com)

4. Seleccione una política de copia de seguridad completa creada en la sección 7 de la lista desplegable.

NetApp SnapCenter®

Oracle Database

Search databases

Name

cdb2

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select one or more policies and configure schedules

Configure schedules for selected policies

Policy	Applied Schedules	Configure Schedules
Oracle Full Online Backup	None	+

Total 1

5. Haga clic en el signo (+) para configurar la programación de copia de seguridad deseada.

NetApp SnapCenter®

Oracle Database

New Resource Group

If you want to send notifications for scheduled or on demand jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide email settings

Select the service accounts or people to notify regarding protection issues.

Email preference: Never

From: From email

To: Email to

Subject: Notification

☐ Attach job report

8. Resumen.

NetApp SnapCenter®

Oracle Database

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Resource group name: rhei2_cdb2

Tags: orafulbkup

Policy: Oracle Full Online Backup: Daily

Plug-in: SnapCenter Plug-in for Oracle Database

Verification enabled for policy: None

Send email: No

Previous Finish

Crear un grupo de recursos para la copia de seguridad de registros de Oracle

1. Inicie sesión en SnapCenter con un ID de usuario de administración de base de datos y navegue a la pestaña Recursos. En la lista desplegable Ver, elija Base de datos o Grupo de recursos para iniciar el flujo de trabajo de creación del grupo de recursos.

NetApp SnapCenter®

Oracle Database

View: Resource Group Search resource group

Name	Resources	Tags	Policies	Last Backup	Overall Status
rhei2_cdb2	1	orafulbkup	Oracle Full Online Backup		

Dashboard Resources Monitor Reports Hosts Storage Systems Settings Alerts

2. Proporcione un nombre y etiquetas para el grupo de recursos. Puede definir un formato de nombre para la copia de instantánea y omitir el destino del registro de archivo redundante si está configurado.

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhel2_cdb2

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide a name and tags for the resource group

Name: rhel2_cdb2_log

Tags: orologbkup

☒ Use custom name format for Snapshot copy

CustomText: rhel2_cdb2_log

Backup settings

Exclude archive log destinations from backup: []

3. Agregue recursos de base de datos al grupo de recursos.

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhel2_cdb2

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Add resources to Resource Group

Host: All

Available Resources

search available resources

Selected Resources

cdb2 (rhel2.demo.netapp.com)

Total 1

Previous Next

4. Seleccione una política de copia de seguridad de registros creada en la sección 7 de la lista desplegable.

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhel2_cdb2

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select one or more policies and configure schedules

Oracle Archive Log Backup

Oracle Full Online Backup

Oracle Archive Log Backup

Policy: Oracle Archive Log Backup

Applied Schedules: None

Configure Schedules: +

Total 1

Previous Next

5. Haga clic en el signo (+) para configurar la programación de copia de seguridad deseada.

Add schedules for policy Oracle Archive Log Backup

Hourly

Start date

09/10/2021 3:00 PM

☒ Expires on

12/31/2021 3:00 PM

Repeat every

1

hours

0

mins

i The schedules are triggered in the SnapCenter Server time zone.

Cancel
OK

6. Si la verificación de respaldo está configurada, se muestra aquí.

NetApp SnapCenter®
demolatordba
App Backup and Clone Admin
Sign Out

Oracle Database
Search resource groups
Name
rhe2_cdb2
Total 1

New Resource Group
1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

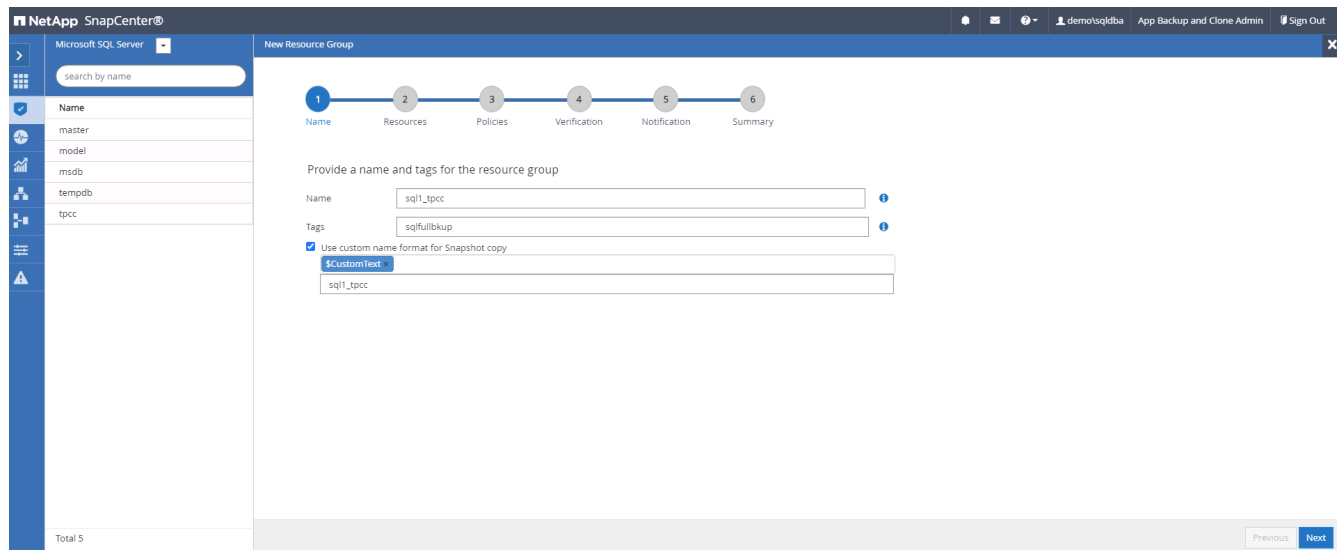
Configure verification schedules
Policy Schedule Type Applied Schedules Configure Schedules
There is no match for your search or data is not available.
Total 0
Previous Next

7. Configure un servidor SMTP para notificaciones por correo electrónico si lo desea.

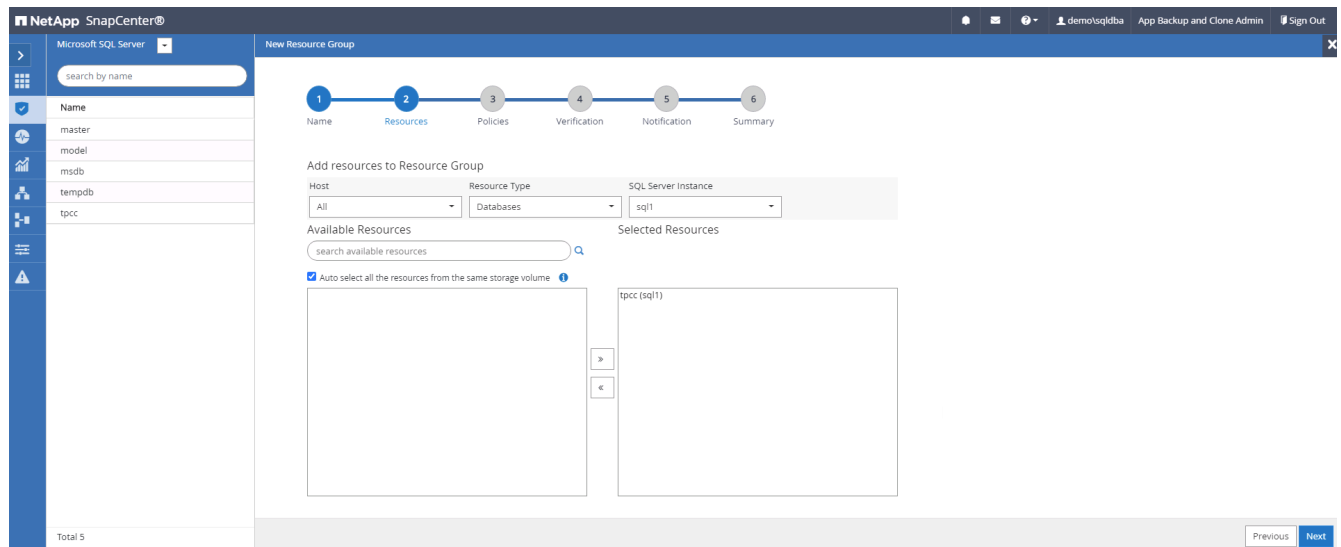
8. Resumen.

Crear un grupo de recursos para realizar una copia de seguridad completa de SQL Server

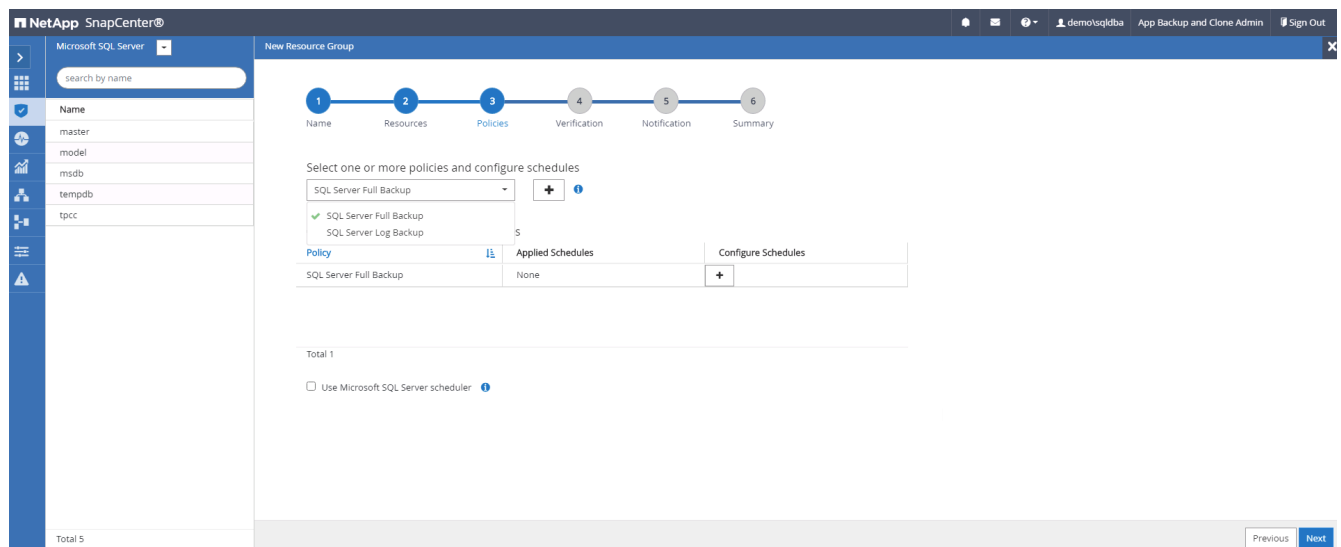
1. Inicie sesión en SnapCenter con un ID de usuario de administración de base de datos y navegue a la pestaña Recursos. En la lista desplegable Ver, elija una base de datos o un grupo de recursos para iniciar el flujo de trabajo de creación del grupo de recursos. Proporcione un nombre y etiquetas para el grupo de recursos. Puede definir un formato de nombre para la copia de instantánea.



2. Seleccione los recursos de base de datos que desea respaldar.



3. Seleccione una política de copia de seguridad de SQL completa creada en la sección 7.



4. Agregue el tiempo exacto para las copias de seguridad, así como la frecuencia.

Add schedules for policy SQL Server Full Backup

Daily

Start date 09/10/2021 6:20 PM

☒ Expires on 12/31/2021 6:20 PM

Repeat every 1 days

The schedules are triggered in the SnapCenter Server time zone.

Cancel OK

5. Seleccione el servidor de verificación para la copia de seguridad secundaria si se debe realizar la verificación de la copia de seguridad. Haga clic en Cargar localizador para completar la ubicación de almacenamiento secundaria.

NetApp SnapCenter

Microsoft SQL Server

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select the verification servers

Verification server Select one or more servers

Load secondary locators to verify backups on secondary Load locators

Secondary storage location: SnapVault or SnapMirror

Source Volume Destination Volume

svm_onPremsql1_data svm_hybridvolsql1_data_dr

svm_onPremsql1_log svm_hybridvolsql1_log_dr

Configure verification schedules

Policy Schedule Type Applied Schedules Configure Schedules

There is no match for your search or data is not available.

Total 5 Previous Next

6. Configure el servidor SMTP para notificaciones por correo electrónico si lo desea.

NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

master

model

msdb

tempdb

tpcc

Total 5

New Resource Group

If you want to send notifications for scheduled or on demand jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide email settings ⓘ

Select the service accounts or people to notify regarding protection issues.

Email preference: Never

From: From email

To: Email to

Subject: Notification

☐ Attach job report

Previous Next

7. Resumen.

NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

There is no match for your search or data is not available.

Resources are not found. Click Refresh Resources to discover databases in the database view or create new resource group on the discovered databases from the resource view.

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Resource group name: sql1_tpcc

Tags: sqlfullbkup

Policy: SQL Server Full Backup: Daily

Plug-in: SnapCenter Plug-in for Microsoft SQL Server

Verification Server: None

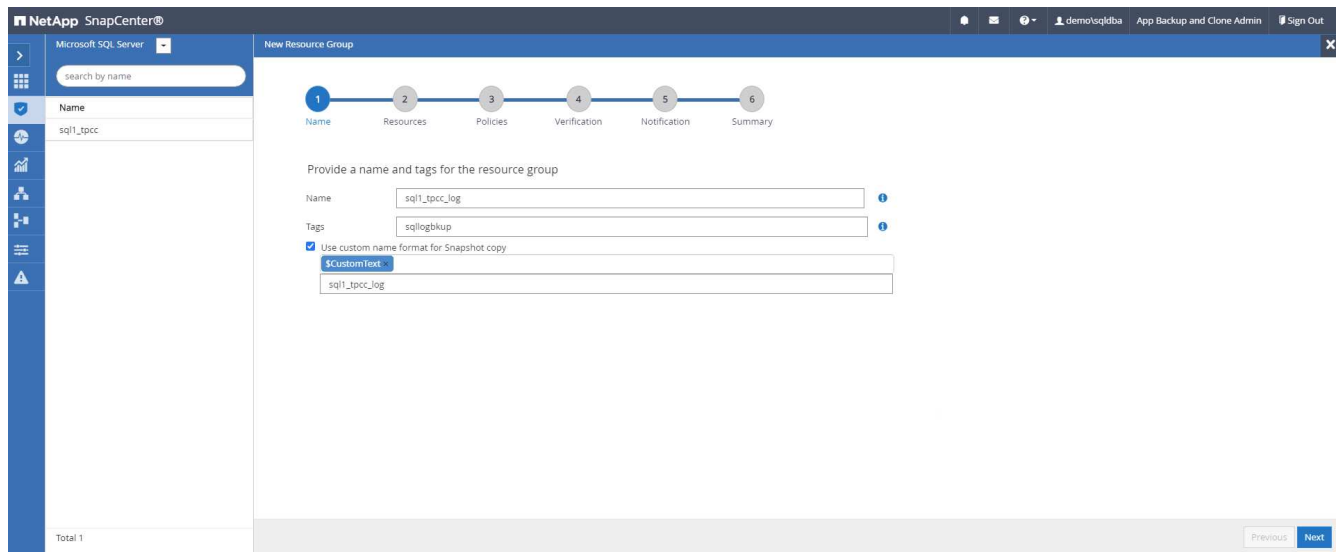
Verification enabled for policy: None

Send email: No

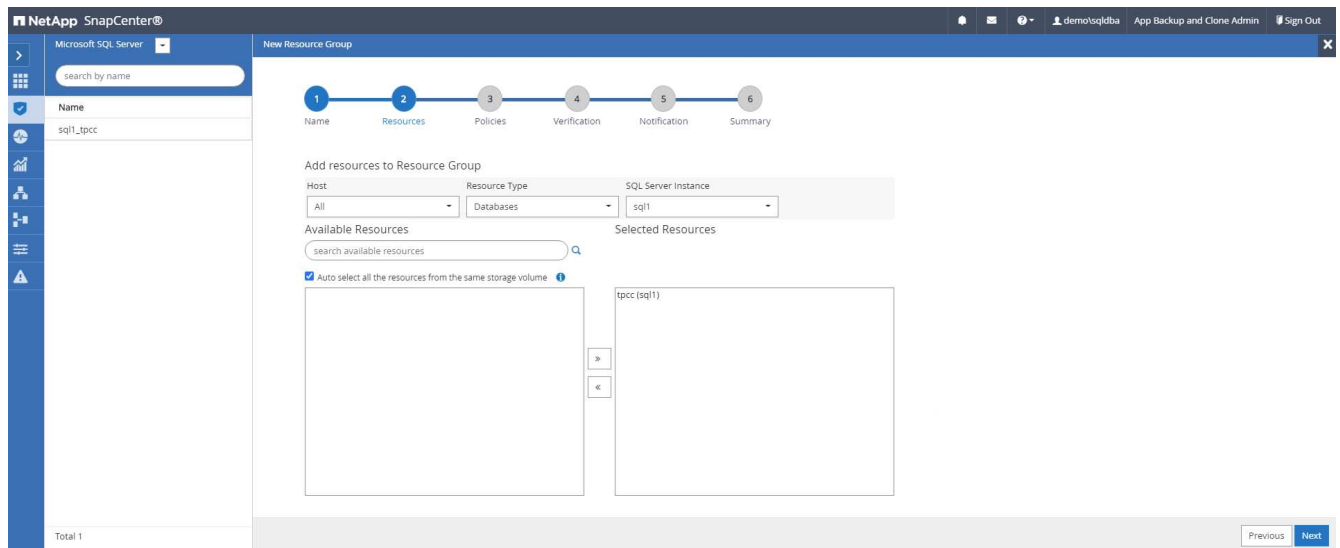
Previous Finish

Crear un grupo de recursos para la copia de seguridad de registros de SQL Server

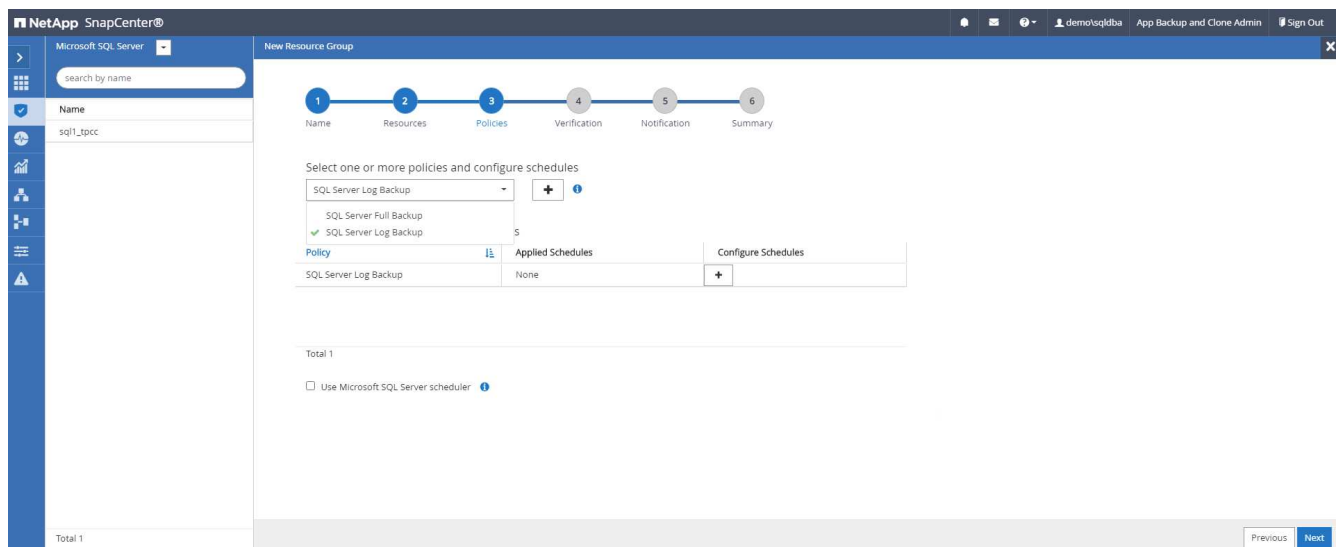
1. Inicie sesión en SnapCenter con un ID de usuario de administración de base de datos y navegue a la pestaña Recursos. En la lista desplegable Ver, elija una base de datos o un grupo de recursos para iniciar el flujo de trabajo de creación del grupo de recursos. Proporcione el nombre y las etiquetas para el grupo de recursos. Puede definir un formato de nombre para la copia de instantánea.



2. Seleccione los recursos de base de datos que desea respaldar.



3. Seleccione una política de copia de seguridad del registro SQL creada en la sección 7.



4. Agregue el tiempo exacto para la copia de seguridad, así como la frecuencia.

NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

sql1_tpcc

Total 1

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select one or more policies and configure schedules

SQL Server Log Backup

Configure schedules for selected policies

Policy	Applied Schedules	Configure Schedules
SQL Server Log Backup	Hourly: Repeat every 1 hours	

Total 1

☐ Use Microsoft SQL Server scheduler

Previous Next

5. Seleccione el servidor de verificación para la copia de seguridad secundaria si se debe realizar la verificación de la copia de seguridad. Haga clic en el Localizador de carga para completar la ubicación de almacenamiento secundaria.

NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

sql1_tpcc

Total 1

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select the verification servers

Verification server: Select one or more servers

Load secondary locators to verify backups on secondary

Load locators

Secondary storage location: SnapVault or SnapMirror

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridcv:sql1_data_dr
svm_onPrem:sql1_log	svm_hybridcv:sql1_log_dr

Configure verification schedules

Policy Schedule Type Applied Schedules Configure Schedules

There is no match for your search or data is not available.

Previous Next

6. Configure el servidor SMTP para notificaciones por correo electrónico si lo desea.

NetApp SnapCenter®

Microsoft SQL Server

search by name

sql1_tpcc

Total 1

New Resource Group

If you want to send notifications for scheduled or on demand jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide email settings

Select the service accounts or people to notify regarding protection issues.

Email preference: Never

From: From email

To: Email to

Subject: Notification

☐ Attach job report

Previous Next

7. Resumen.

NetApp SnapCenter®

Microsoft SQL Server

search by name

sql1_tpcc

Total 1

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Resource group name: sql1_tpcc_log

Tags: sqllogbkup

Policy: SQL Server Log Backup: Hourly

Plug-in: SnapCenter Plug-in for Microsoft SQL Server

Verification Server: None

Verification enabled for policy: None

Send email: No

Previous Finish

9. Validar copia de seguridad

Una vez creados los grupos de recursos de respaldo de la base de datos para proteger los recursos de la base de datos, los trabajos de respaldo se ejecutan de acuerdo con la programación predefinida. Verifique el estado de ejecución del trabajo en la pestaña Monitor.

NetApp SnapCenter®

Jobs Schedules Events Logs

search by name

Dashboard Resources Monitor Reports Hosts Storage Systems Settings Alerts

Jobs - Filter

ID	Status	Name	Start date	End date	Owner
532	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 8:35:01 PM	09/14/2021 8:37:10 PM	demo/sqlqdba
528	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 7:35:01 PM	09/14/2021 7:37:09 PM	demo/sqlqdba
524	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 6:35:01 PM	09/14/2021 6:37:08 PM	demo/sqlqdba
521	✓	Backup of Resource Group 'sql1_tpcc' with policy 'SQL Server Full Backup'	09/14/2021 6:25:01 PM	09/14/2021 6:27:14 PM	demo/sqlqdba
517	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 5:35:01 PM	09/14/2021 5:37:09 PM	demo/sqlqdba
513	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 4:35:01 PM	09/14/2021 4:37:08 PM	demo/sqlqdba
509	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 3:35:01 PM	09/14/2021 3:37:10 PM	demo/sqlqdba
503	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 2:35:01 PM	09/14/2021 2:37:09 PM	demo/sqlqdba

Vaya a la pestaña Recursos, haga clic en el nombre de la base de datos para ver los detalles de la copia de seguridad de la base de datos y alterne entre copias locales y copias reflejadas para verificar que las copias

de seguridad instantáneas se repliquen en una ubicación secundaria en la nube pública.

The screenshot shows the NetApp SnapCenter web interface. On the left is a sidebar with navigation icons. The main area is titled 'cdb2 Topology' and 'Manage Copies'. It displays a visual representation of database copies: 'Local copies' with 197 Backups and 0 Clones, and 'Mirror copies' with 197 Backups and 3 Clones. A 'Summary Card' on the right shows: 394 Backups, 28 Data Backups, 366 Log Backups, and 3 Clones. Below this is a table of 'Primary Backup(s)' with columns: Backup Name, Count, Type, End Date, Verified, Mounted, RMAN Cataloged, and SCN. The table lists several backup entries with their respective details.

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_09-23-2021_14.35.03.3242_1	1	Log	09/23/2021 2:35:45 PM	Not Applicable	False	Not Cataloged	6872761
rhel2_cdb2_09-23-2021_14.35.03.3242_0	1	Data	09/23/2021 2:35:30 PM	Unverified	False	Not Cataloged	6872715
rhel2_cdb2_09-22-2021_14.35.02.0014_1	1	Log	09/22/2021 2:35:24 PM	Not Applicable	False	Not Cataloged	6737479
rhel2_cdb2_09-22-2021_14.35.02.0014_0	1	Data	09/22/2021 2:35:14 PM	Unverified	False	Not Cataloged	6737395
rhel2_cdb2_09-21-2021_14.35.02.1884_1	1	Log	09/21/2021 2:35:35 PM	Not Applicable	False	Not Cataloged	6598735

En este punto, las copias de seguridad de la base de datos en la nube están listas para clonarse para ejecutar procesos de desarrollo y prueba o para recuperación ante desastres en caso de una falla primaria.

Introducción a la nube pública de AWS

Esta sección describe el proceso de implementación de Cloud Manager y Cloud Volumes ONTAP en AWS.

Nube pública de AWS



Para facilitar el seguimiento, hemos creado este documento basado en una implementación en AWS. Sin embargo, el proceso es muy similar para Azure y GCP.

1. Comprobación previa al vuelo

Antes de la implementación, asegúrese de que la infraestructura esté en su lugar para permitir la implementación en la siguiente etapa. Esto incluye lo siguiente:

- Cuenta de AWS
- VPC en la región de su elección
- Subred con acceso a Internet público
- Permisos para agregar roles de IAM a su cuenta de AWS
- Una clave secreta y una clave de acceso para su usuario de AWS

2. Pasos para implementar Cloud Manager y Cloud Volumes ONTAP en AWS



Hay muchos métodos para implementar Cloud Manager y Cloud Volumes ONTAP; este método es el más simple pero requiere la mayor cantidad de permisos. Si este método no es apropiado para su entorno de AWS, consulte el "[Documentación de NetApp Cloud](#)".

Implementar el conector de Cloud Manager

1. Navegar a "[NetApp BlueXP](#)" e inicie sesión o regístrese.



[Continue to Cloud Manager](#)

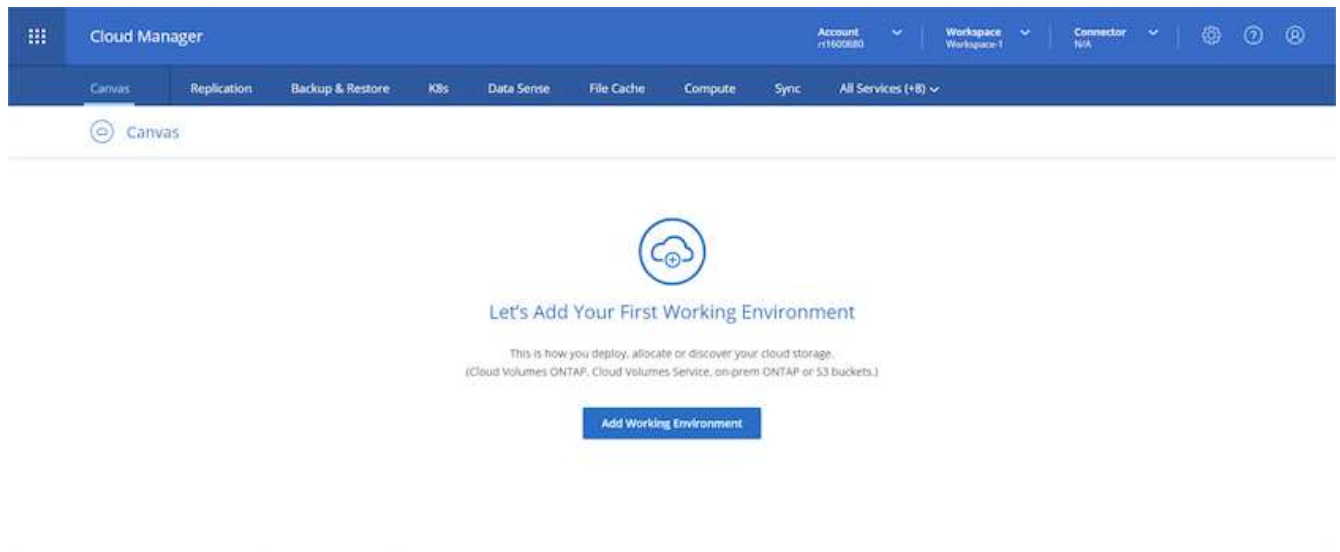
Log In to NetApp Cloud Central

Don't have an account yet? [Sign Up](#)

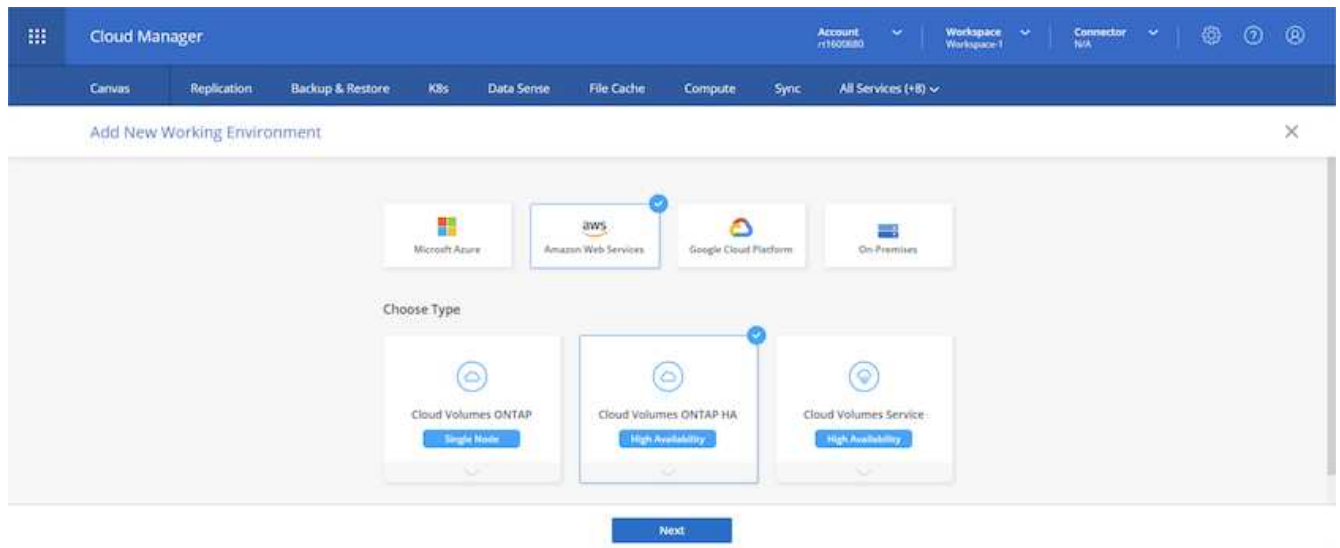
LOGIN

[Forgot your password?](#)

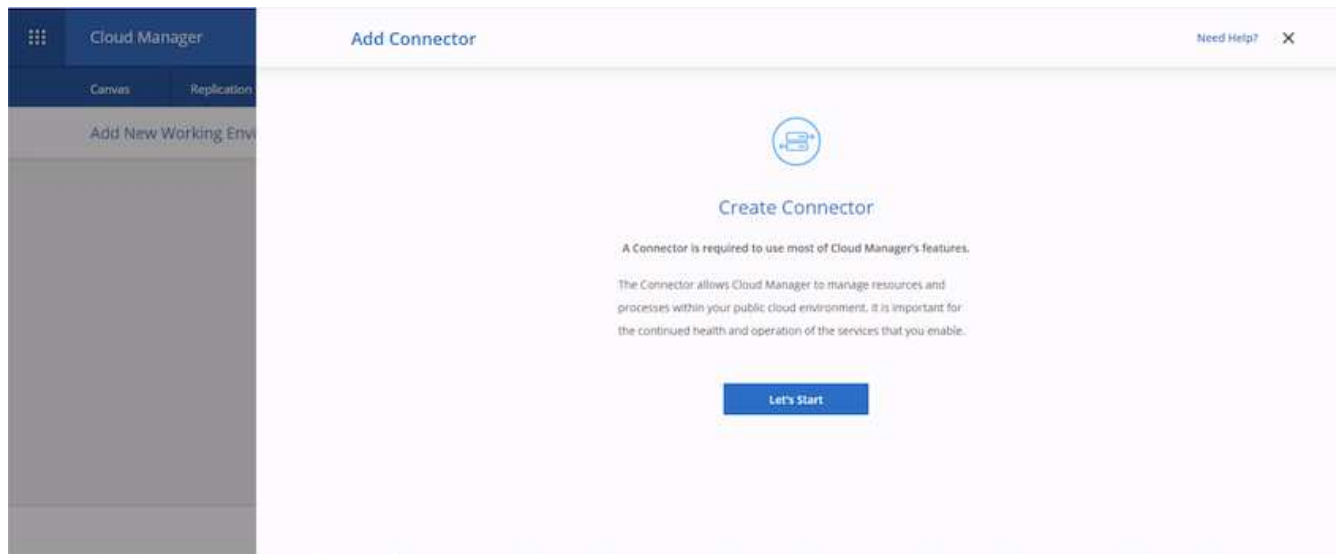
2. Después de iniciar sesión, deberías ser llevado al Canvas.



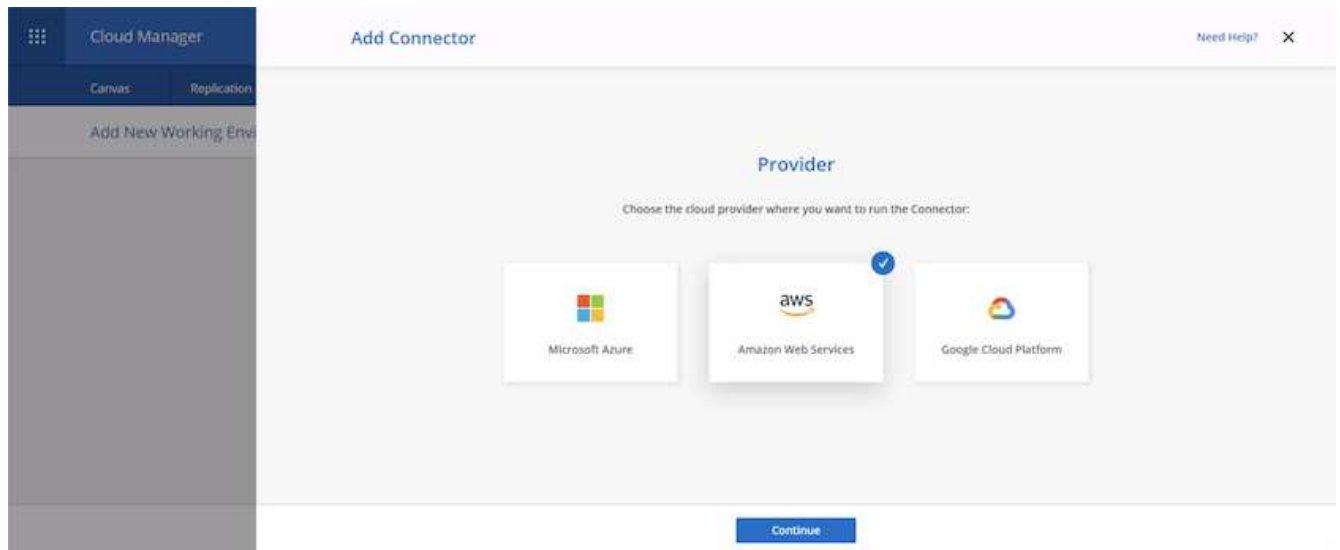
3. Haga clic en “Agregar entorno de trabajo” y elija Cloud Volumes ONTAP en AWS. Aquí también puedes elegir si deseas implementar un sistema de un solo nodo o un par de alta disponibilidad. He optado por implementar un par de alta disponibilidad.



4. Si no se ha creado ningún conector, aparecerá una ventana emergente que le solicitará que cree uno.



5. Haga clic en Comenzamos y luego seleccione AWS.



6. Introduzca su clave secreta y clave de acceso. Asegúrese de que su usuario tenga los permisos correctos descritos en la ["Página de políticas de NetApp"](#) .

Cloud Manager

Add Connector

Need Help? X

Get Ready AWS Credentials Details Network Security Group Review

AWS Credentials

AWS Access Key

AWS Access Key is required

AWS Secret Key

Region

us-east-1 | US East (N. Virginia)

Want to launch an instance without AWS Credentials?

Previous Next

7. Dale un nombre al conector y utiliza un rol predefinido como se describe en la "[Página de políticas de NetApp](#)" o pídale a Cloud Manager que cree el rol para usted.

Cloud Manager

Add Connector

Need Help? X

Get Ready AWS Credentials Details Network Security Group Review

Details

Connector Instance Name

awscloudmanager

Connector Role

Create Role Select an existing Role

Role Name

Cloud-Manager-Operator-IBHt24j

Add Tags to Connector Instance

Previous Next

8. Proporcione la información de red necesaria para implementar el conector. Verifique que el acceso a Internet saliente esté habilitado mediante lo siguiente:
- Darle al conector una dirección IP pública
 - Proporcionarle al conector un proxy para trabajar a través de él
 - Proporcionar al conector una ruta a Internet pública a través de un Internet Gateway

Cloud Manager

Canvas Replication

Add New Working Environment

Add Connector

Need Help? X

Get Ready AWS Credentials Details **4 Network** 5 Security Group 6 Review

Connectivity

VPC: vpc-083fcbd7975dfb6e - 10.221.0.0/16

Subnet: 10.221.4.0/24 | publicSN_us-east-1a_r11600...

Key Pair: r11600680

Public IP: Enable

Proxy Configuration (Optional)

HTTP Proxy: Example: https://172.16.254.1:8080

Define Credentials for this Proxy

Upload a root certificate

Previous Next

9. Proporcione comunicación con el conector a través de SSH, HTTP y HTTPS proporcionando un grupo de seguridad o creando un nuevo grupo de seguridad. He habilitado el acceso al conector únicamente desde mi dirección IP.

Cloud Manager

Canvas Replication

Add New Working Environment

Add Connector

Need Help? X

Get Ready AWS Credentials Details Network **5 Security Group** 6 Review

The security group must allow inbound HTTP, HTTPS and SSH access.

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

HTTP (Port 80)	HTTPS (Port 443)	SSH (Port 22)
Source Type: My IP	Source Type: My IP	Source Type: My IP
Source (CIDR): 216.240.31.145/32	Source (CIDR): 216.240.31.145/32	Source (CIDR): 216.240.31.145/32

Previous Next

10. Revise la información en la página de resumen y haga clic en Agregar para implementar el conector.

Cloud Manager

Canvas Replication

Add New Working Env

Add Connector

Need Help? X

Get Ready AWS Credentials Details Network Security Group Review

Code for Terraform Automation

Connector Name	awscoudmanager
Region	us-east-1
VPC	vpc-083fcbd79f75dfb6e - 10.221.0.0/16
Subnet	10.221.4.0/24 publicSN-us-east-1a-rt1600680
Key Pair	rt1600680
Public IP	Enable
Proxy	None
Security Group	HTTP: 216.240.31.145/32, HTTPS: 216.240.31.145/32, SSH: 216.240.31.145/32

Previous Add

11. El conector ahora se implementa utilizando una pila de formación de nubes. Puede supervisar su progreso desde Cloud Manager o mediante AWS.

Cloud Manager

Canvas Replication

Add New Working Env

Deploying a Connector

Show Details

- Keep this wizard open until the deployment process is complete. It usually takes about 7 minutes.
- No other Cloud Manager features are available during deployment.
- When the process is complete, you can continue the operation that you started.

12. Cuando se completa la implementación, aparece una página de éxito.

Cloud Manager

Canvas Replication

Add New Working Env

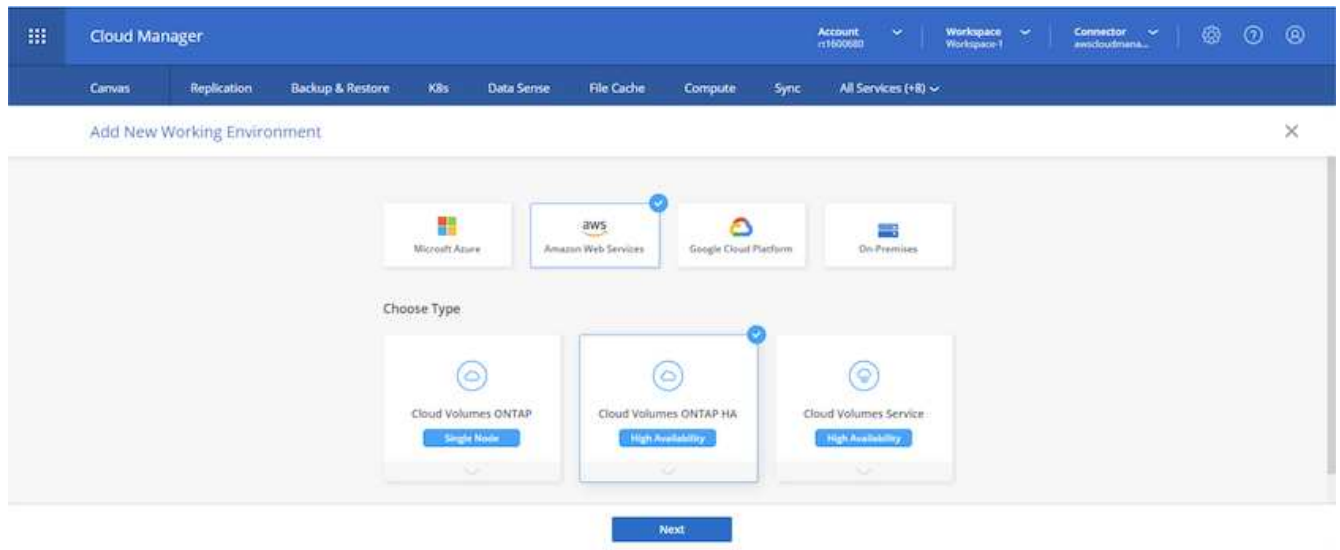
Connector Successfully Created

The Connector was created successfully.

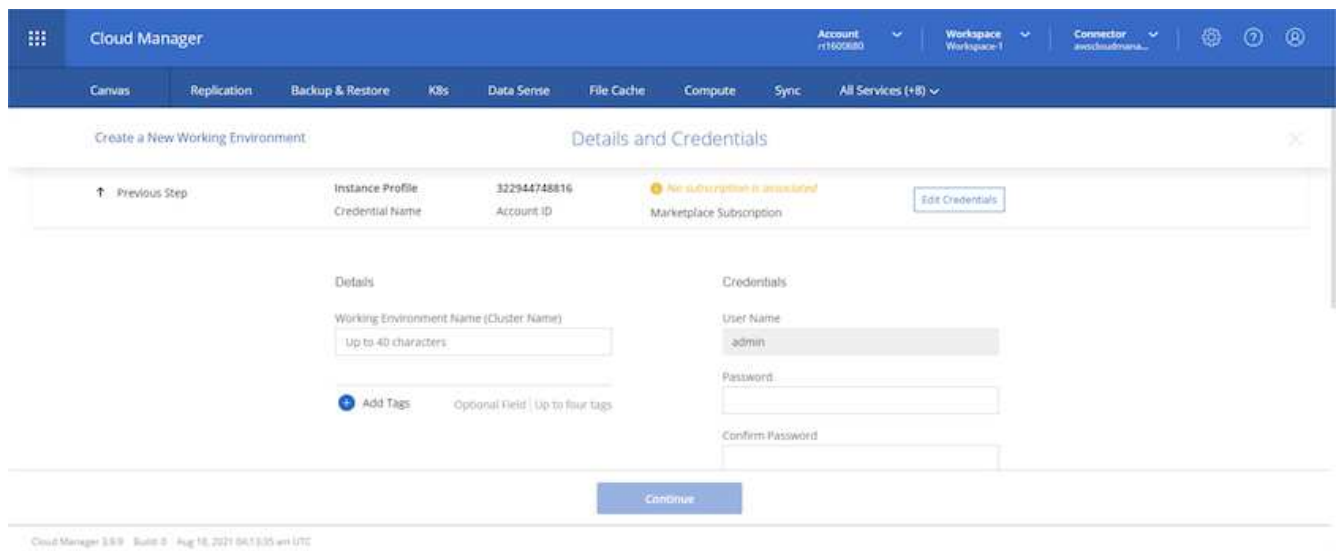
Continue

Implementar Cloud Volumes ONTAP

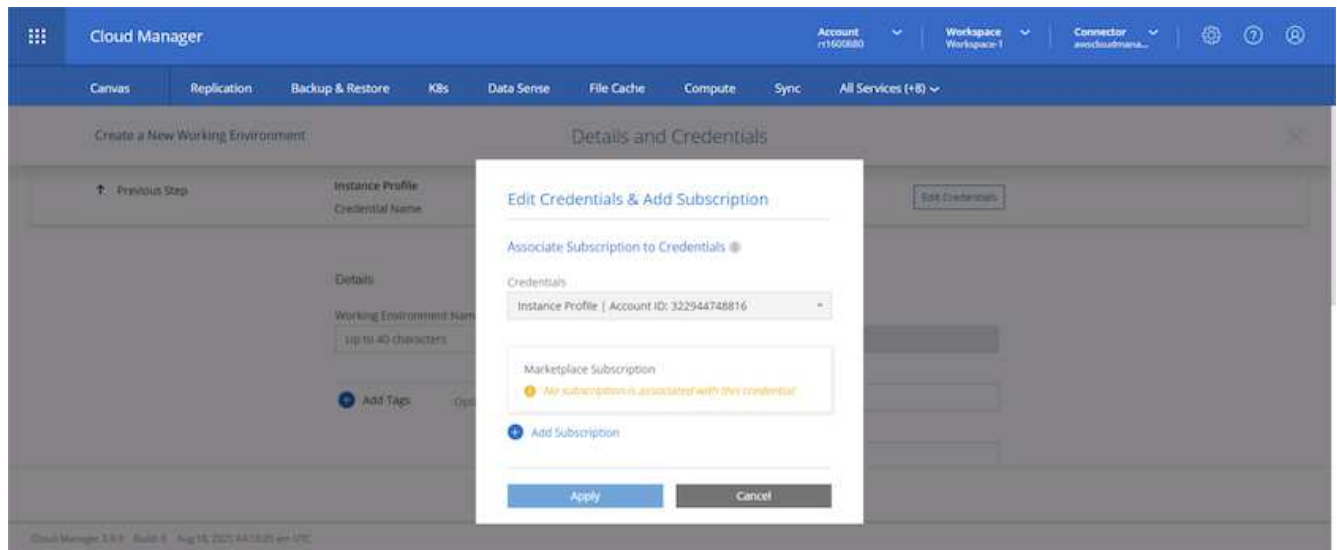
1. Seleccione AWS y el tipo de implementación según sus requisitos.



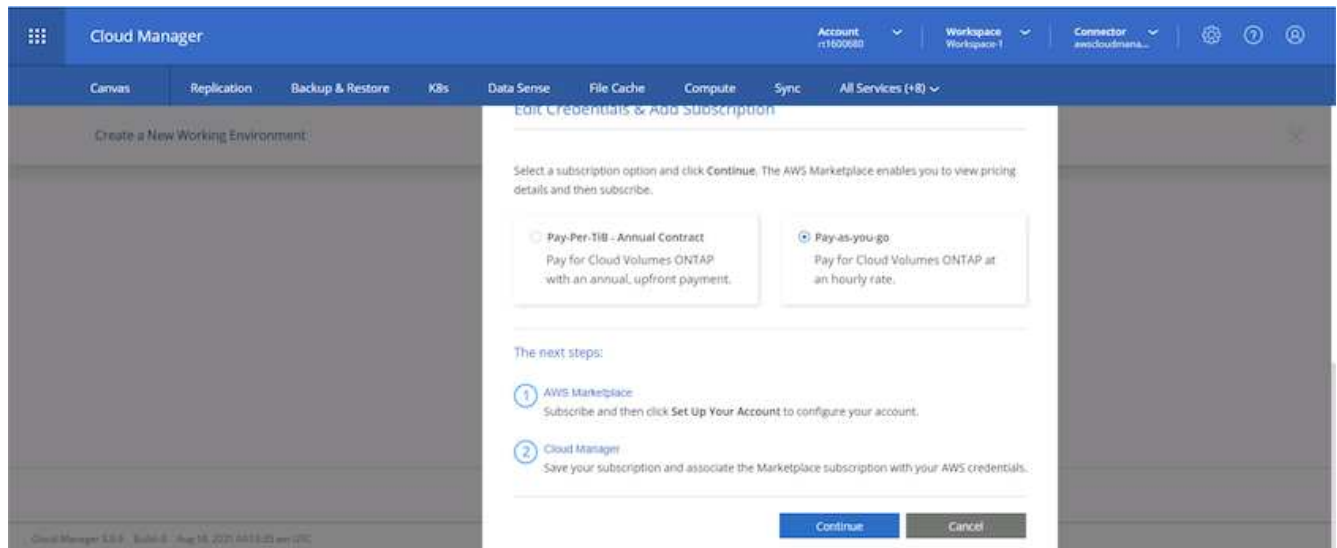
2. Si no se ha asignado ninguna suscripción y desea comprar con PAYGO, seleccione Editar credenciales.



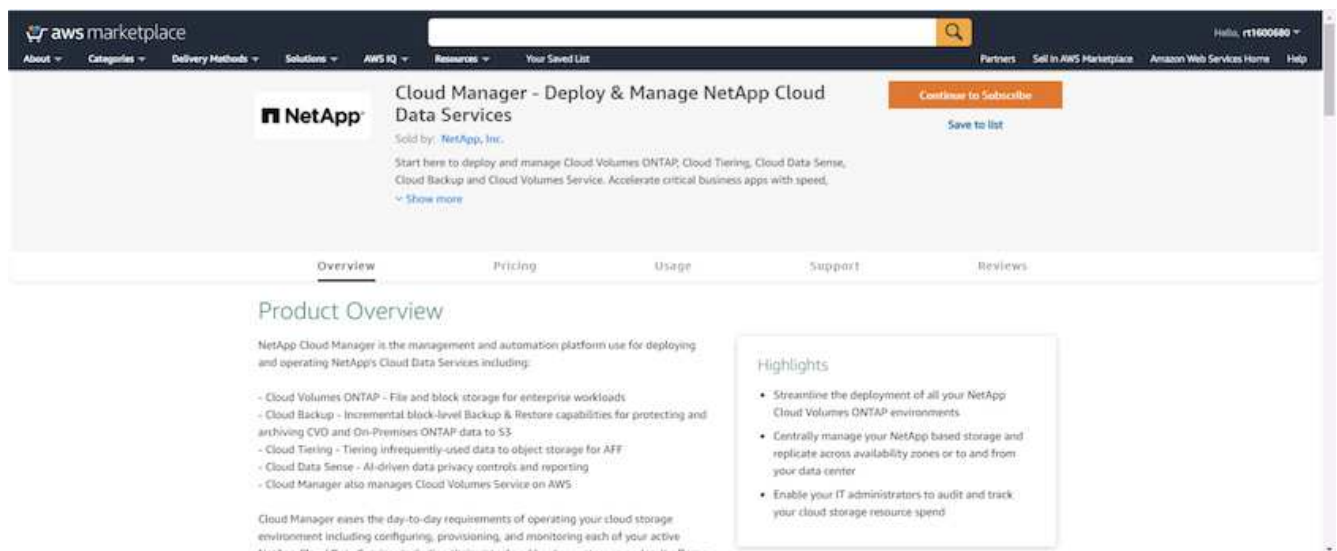
3. Seleccione Agregar suscripción.



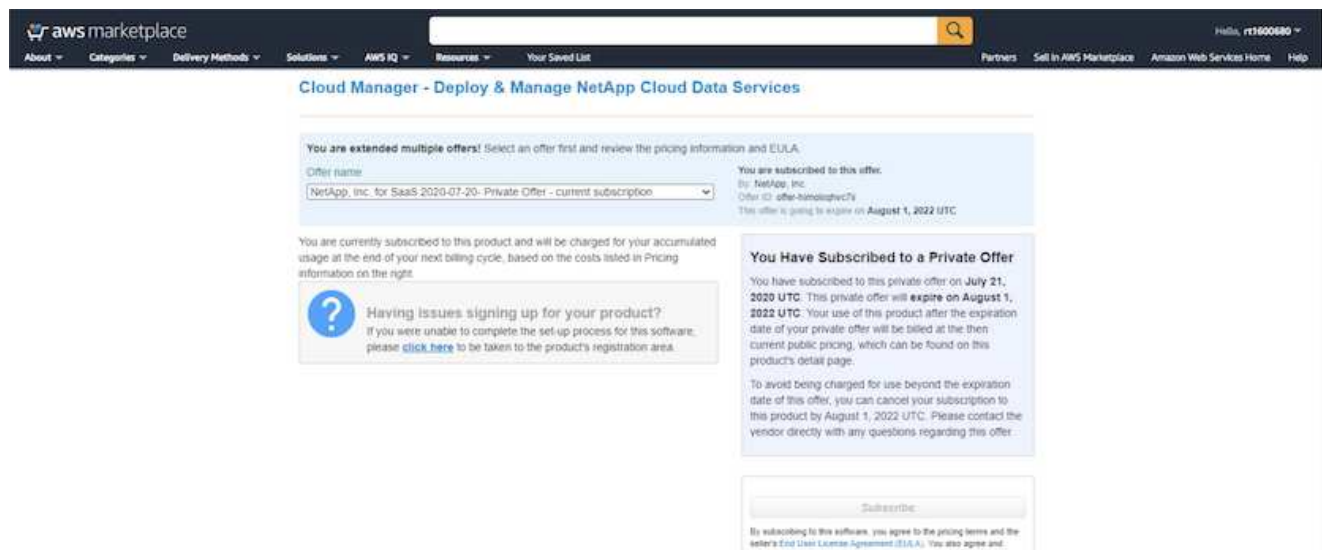
4. Elige el tipo de contrato al que deseas suscribirte. Elegí pagar por uso.



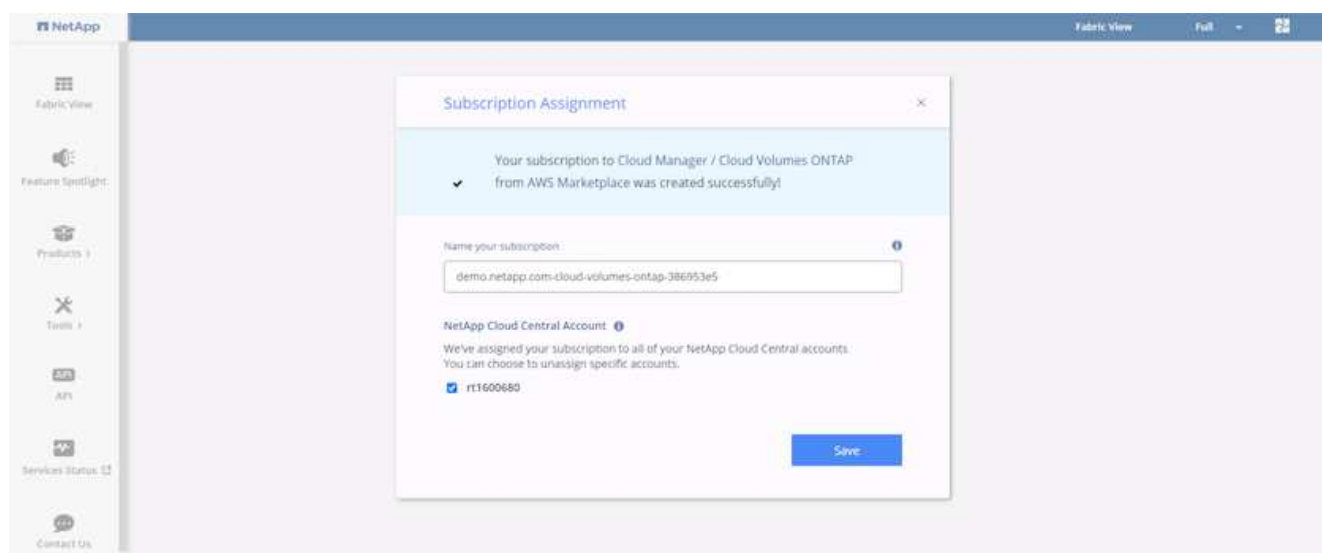
5. Serás redirigido a AWS; selecciona Continuar para suscribirte.



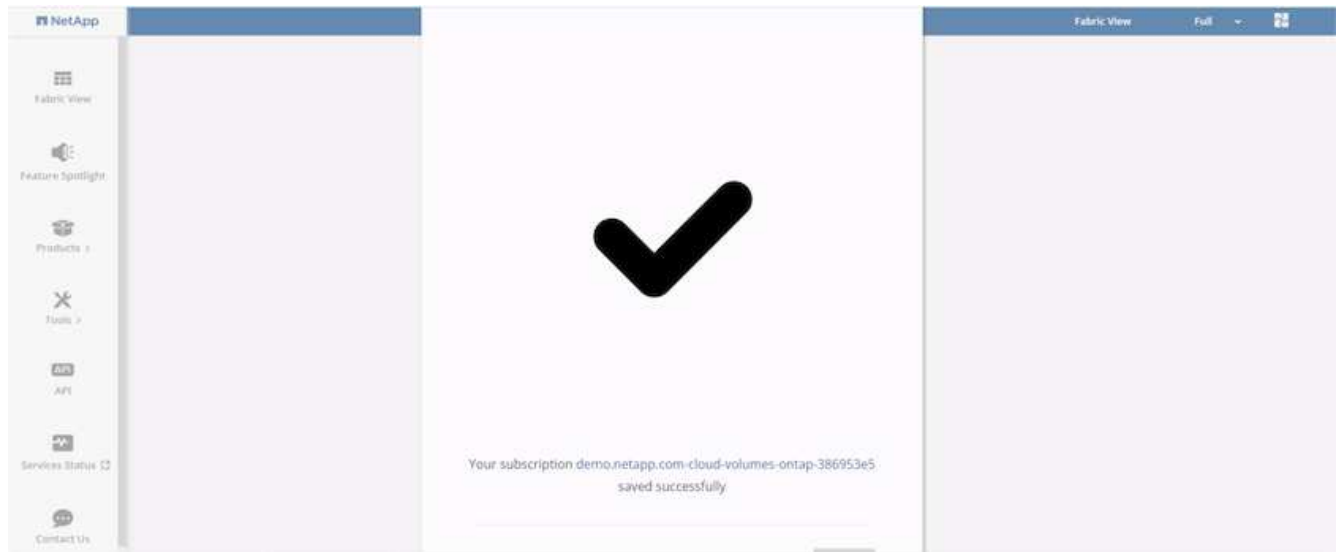
6. Suscríbete y serás redirigido nuevamente a NetApp Cloud Central. Si ya estás suscrito y no eres redirigido elige el enlace “Haz clic aquí”.



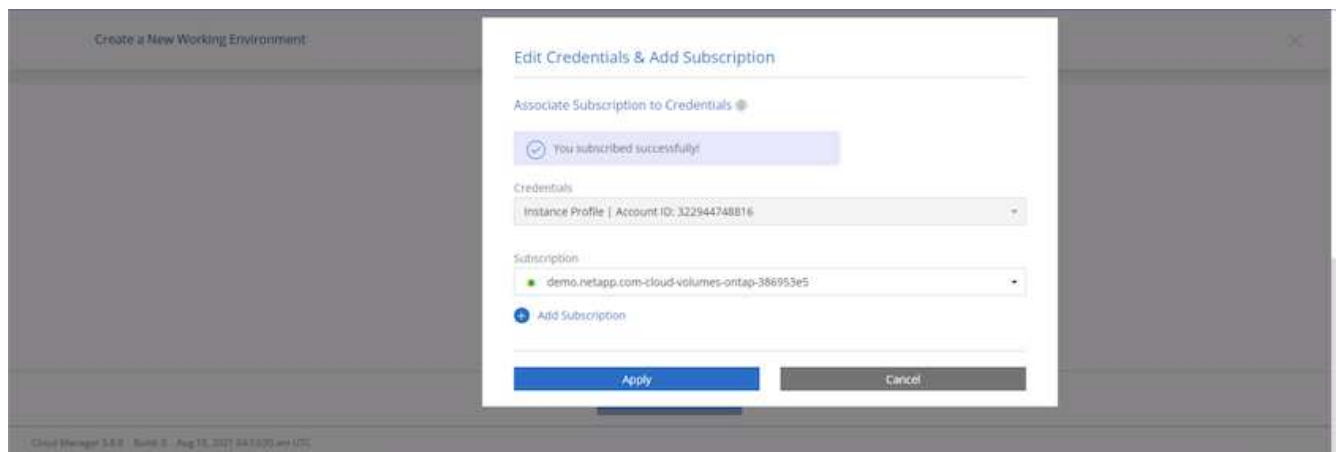
7. Serás redirigido a Cloud Central, donde deberás nombrar tu suscripción y asignarla a tu cuenta de Cloud Central.



8. Cuando tenga éxito, aparecerá una página de marca de verificación. Regrese a la pestaña Administrador de nube.



9. La suscripción ahora aparece en Cloud Central. Haga clic en Aplicar para continuar.



10. Ingrese los detalles del entorno de trabajo como:

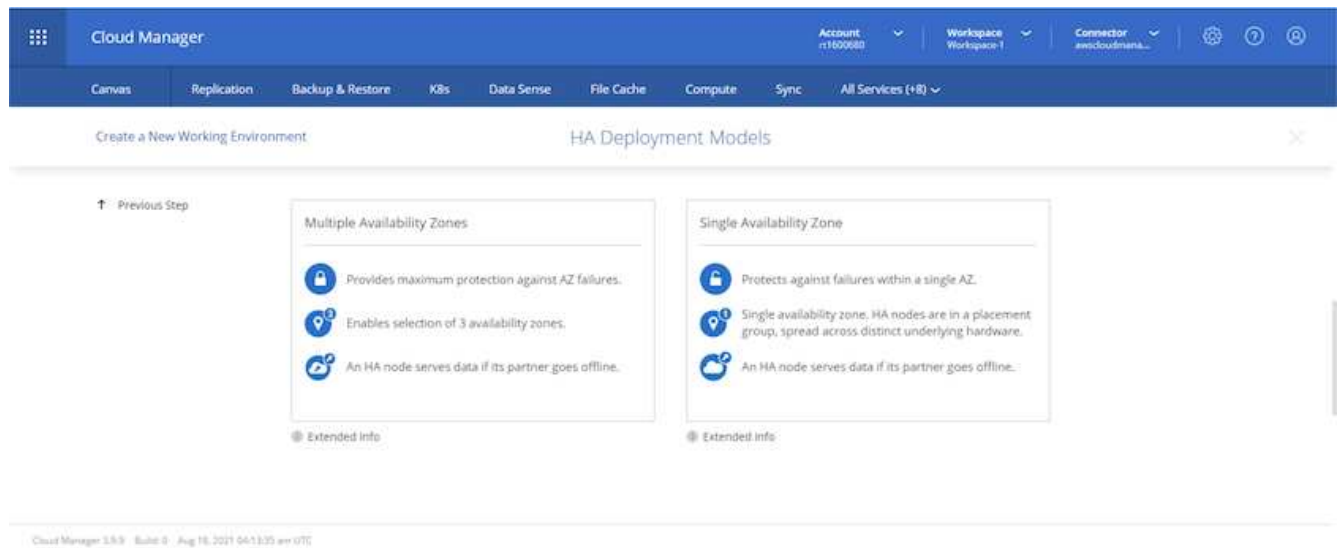
- a. Nombre del clúster
- b. Contraseña del clúster
- c. Etiquetas de AWS (opcional)

The screenshot shows the 'Details and Credentials' step in the Cloud Manager console. The top navigation bar includes 'Canvas', 'Replication', 'Backup & Restore', 'K8s', 'Data Sense', 'File Cache', 'Compute', 'Sync', and 'All Services (+8)'. The main content area is divided into two sections: 'Details' and 'Credentials'. In the 'Details' section, the 'Working Environment Name (Cluster Name)' is 'hybridawsco'. Below it, there is an 'Add Tags' button and a note 'Optional Field | Up to four tags'. In the 'Credentials' section, the 'User Name' is 'admin', and there are fields for 'Password' and 'Confirm Password', both masked with asterisks. A 'Continue' button is at the bottom right. The footer indicates 'Cloud Manager 3.9.9 - Build 0 - Aug 18, 2021 06:13:35 am UTC'.

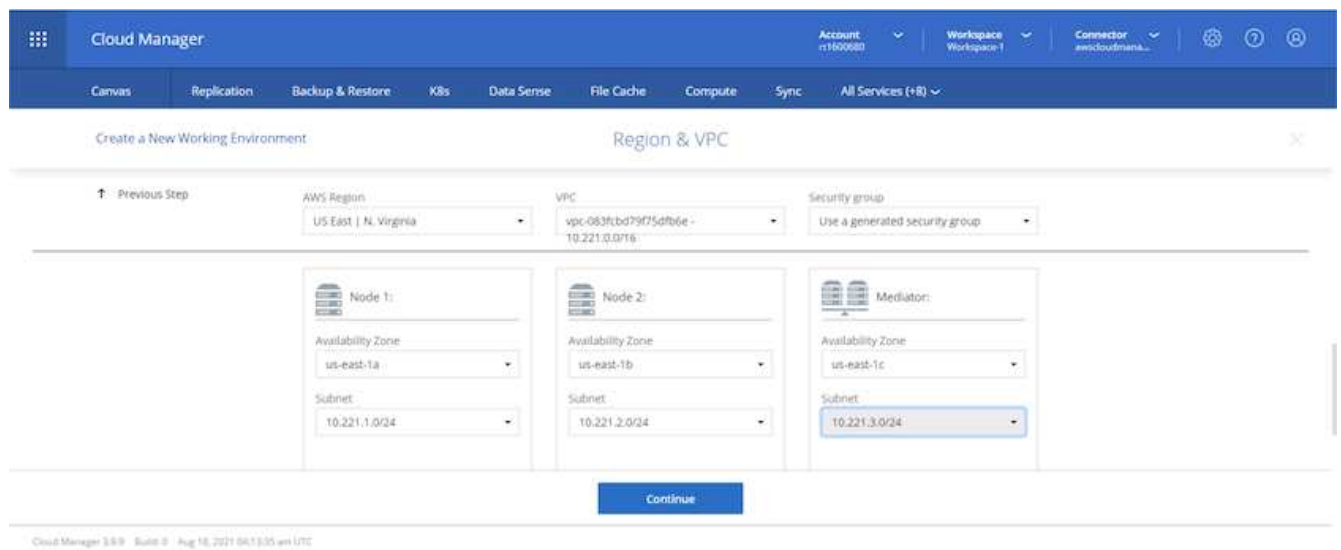
11. Elija qué servicios adicionales desea implementar. Para descubrir más sobre estos servicios, visite el ["BlueXP: Operaciones modernas de patrimonio de datos simplificadas"](#) .

The screenshot shows the 'Services' step in the Cloud Manager console. The top navigation bar is the same as the previous screenshot. The main content area lists three services with toggle switches and dropdown menus: 'Data Sense & Compliance', 'Backup to Cloud', and 'Monitoring'. All three services are currently enabled (toggles are blue). A 'Continue' button is at the bottom right. The footer indicates 'Cloud Manager 3.9.9 - Build 0 - Aug 18, 2021 06:13:35 am UTC'.

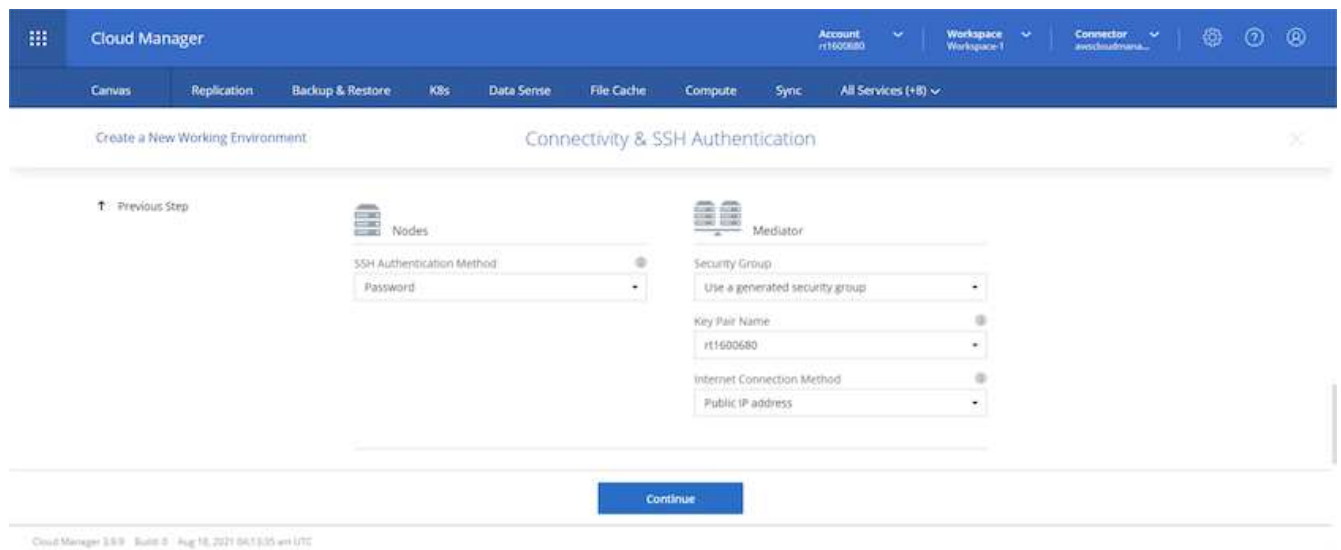
12. Elija si desea implementar en múltiples zonas de disponibilidad (requiere tres subredes, cada una en una zona de disponibilidad diferente) o en una sola zona de disponibilidad. Elegí varias AZ.



13. Elija la región, la VPC y el grupo de seguridad donde se implementará el clúster. En esta sección también se asignan las zonas de disponibilidad por nodo (y mediador), así como las subredes que ocupan.



14. Elija los métodos de conexión para los nodos así como el mediador.





El mediador requiere comunicación con las API de AWS. No se requiere una dirección IP pública siempre que se pueda acceder a las API después de que se haya implementado la instancia EC2 del mediador.

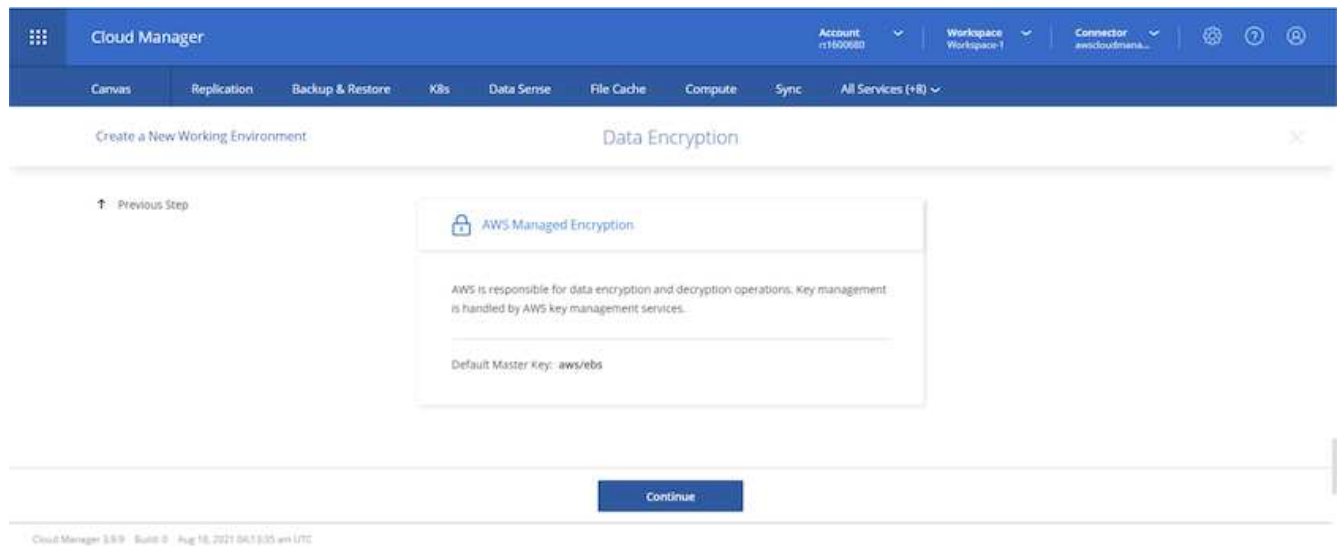
1. Las direcciones IP flotantes se utilizan para permitir el acceso a las distintas direcciones IP que utiliza Cloud Volumes ONTAP, incluidas las IP de administración de clústeres y de servicio de datos. Estas deben ser direcciones que aún no sean enrutables dentro de su red y se agregan a las tablas de ruta en su entorno de AWS. Estos son necesarios para habilitar direcciones IP consistentes para un par HA durante la conmutación por error. Puede encontrar más información sobre las direcciones IP flotantes en "[Documentación de NetApp Cloud](#)".

The screenshot shows the 'Floating IPs' configuration page in the NetApp Cloud Manager console. The page title is 'Floating IPs'. Below the title, there is a 'Previous Step' button. The main content area contains the following text: 'Floating IP addresses are required for cluster and SVM access and for NFS and CIFS data access. These floating IPs can migrate between HA nodes if failures occur. To access the data from outside the VPC, you can set up an AWS transit gateway.' Below this text, there is a note: 'You must specify IP addresses that are outside of the CIDR blocks for all VPCs in the selected AWS region.' There are four input fields for floating IP addresses: 'Floating IP address for cluster management' (10.222.0.200), 'Floating IP address 1 for NFS and CIFS data' (10.222.0.201), 'Floating IP address 2 for NFS and CIFS data' (10.222.0.202), and 'Floating IP address for SVM management (Optional)' (Enter Floating IP Address). A 'Continue' button is at the bottom right.

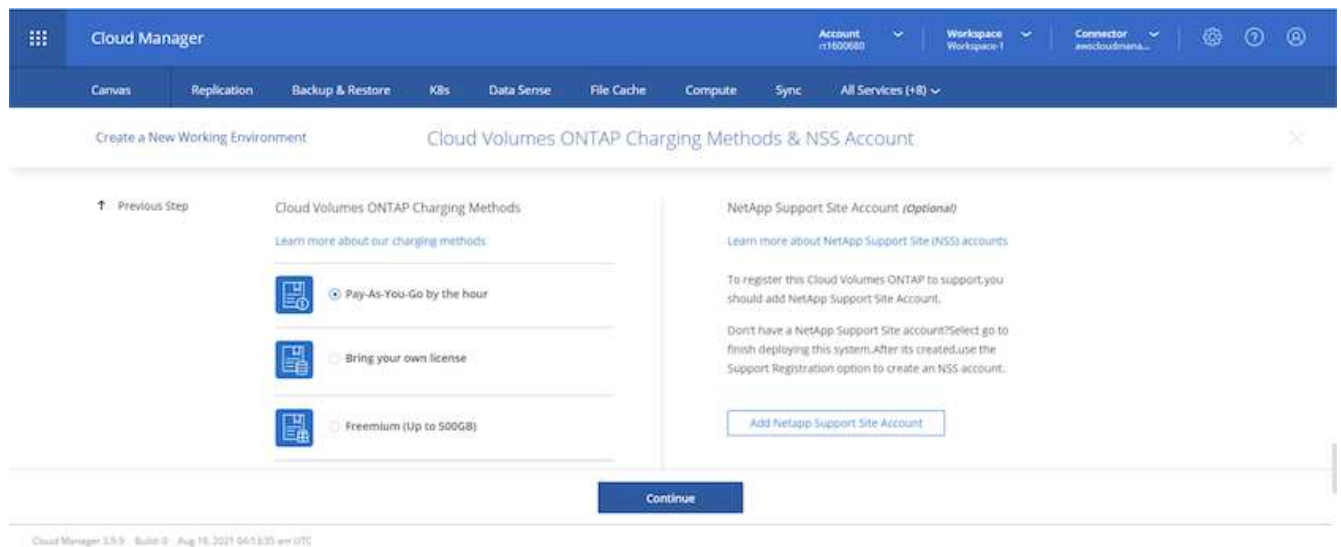
2. Seleccione a qué tablas de rutas se agregarán las direcciones IP flotantes. Los clientes utilizan estas tablas de rutas para comunicarse con Cloud Volumes ONTAP.

The screenshot shows the 'Route Tables' configuration page in the NetApp Cloud Manager console. The page title is 'Route Tables'. Below the title, there is a 'Previous Step' button. The main content area contains the following text: 'Select the route tables that should include routes to the floating IP addresses. This enables client access to the Cloud Volumes ONTAP HA pair. If you leave a route table unselected, clients that are associated with the route table cannot access the HA pair.' Below this text, there is a table with the following columns: 'Name', 'Main', 'ID', 'Associate with Subnet', and 'Tags'. The table contains two rows: 'private_rt_rt1600680' (Main: No, ID: rtb-08b4cb88f5c826a5, Associate with Subnet: 3 Subnets, Tags: 1 Tags) and 'public_rt_rt1600680' (Main: Yes, ID: rtb-0e46720d0da10c593, Associate with Subnet: 1 Subnets, Tags: 1 Tags). Below the table, there is a note: '2 Route Tables | The main route table is the default for the VPC'. A 'Continue' button is at the bottom right.

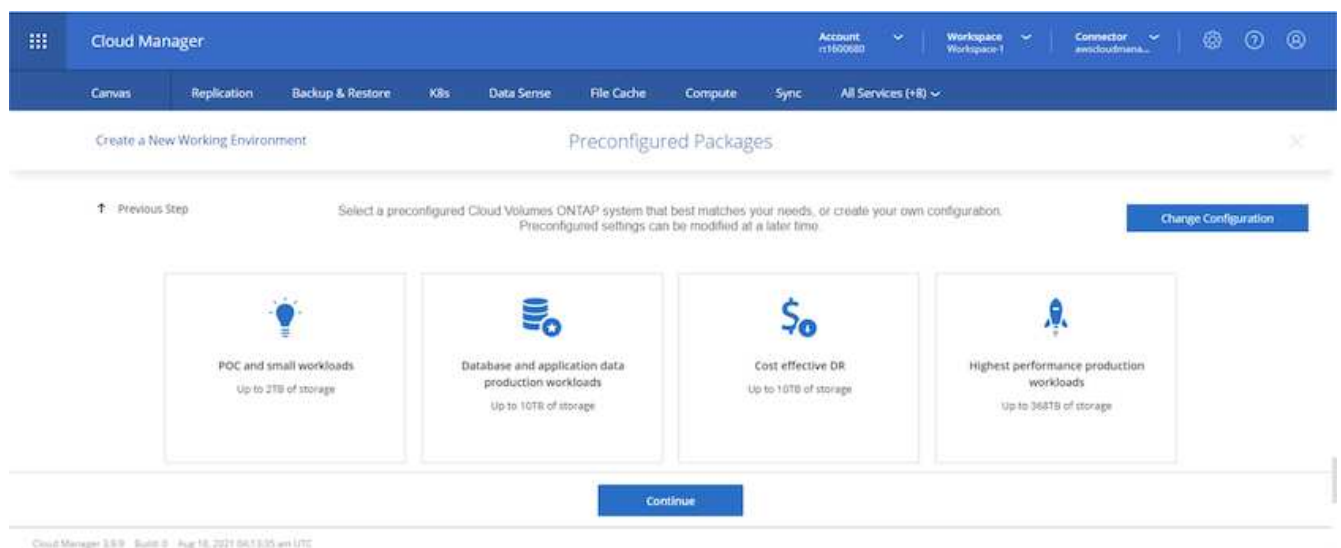
3. Elija si desea habilitar el cifrado administrado por AWS o AWS KMS para cifrar los discos raíz, de arranque y de datos de ONTAP.



4. Elige tu modelo de licencia. Si no sabe cuál elegir, comuníquese con su representante de NetApp .



5. Seleccione la configuración que mejor se adapte a su caso de uso. Esto está relacionado con las consideraciones de tamaño cubiertas en la página de requisitos previos.



6. Opcionalmente, cree un volumen. Esto no es necesario, porque los siguientes pasos utilizan SnapMirror, que crea los volúmenes para nosotros.

The screenshot shows the 'Create Volume' wizard in the Cloud Manager interface. The top navigation bar includes 'Canvas', 'Replication', 'Backup & Restore', 'K8s', 'Data Sense', 'File Cache', 'Compute', 'Sync', and 'All Services (+8)'. The main content area is titled 'Create a New Working Environment' and 'Create Volume'. It features a 'Previous Step' button and a 'Details & Protection' section with fields for 'Volume Name', 'Size (GB)', 'Snapshot Policy', and 'Default Policy'. A 'Protocol' section on the right shows 'NFS' selected, with 'Access Control' set to 'Custom export policy' and 'Custom export policy' set to '10.221.0.0/16'. At the bottom, there are 'Continue' and 'Skip' buttons. The footer indicates 'Cloud Manager 5.8.9 Build 0 Aug 18, 2021 04:13:35 am UTC'.

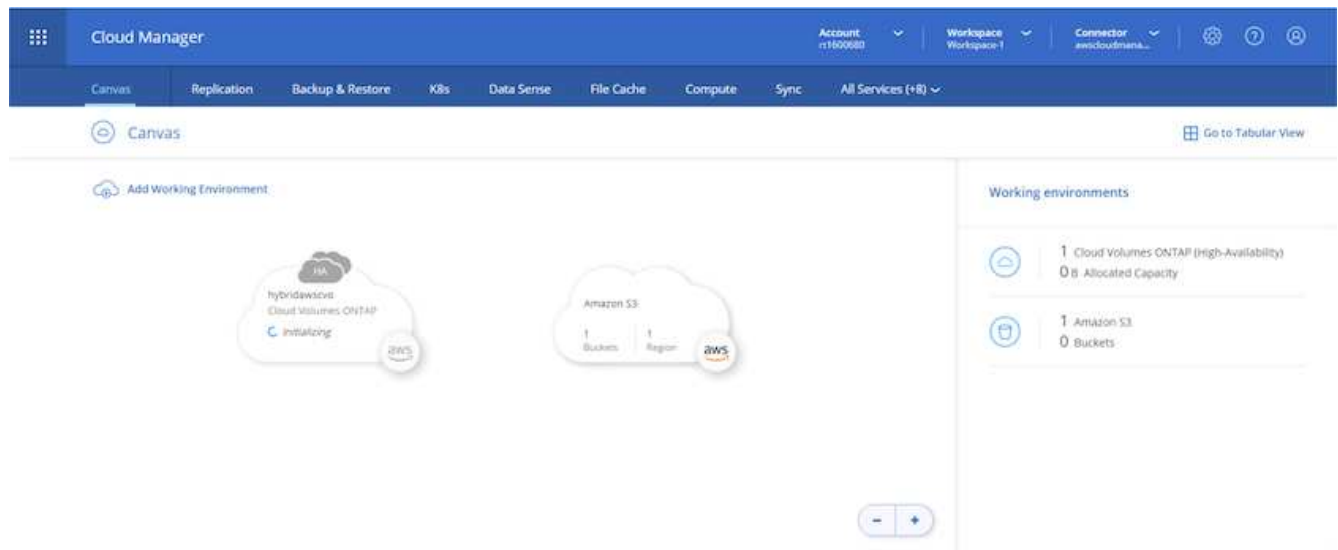
7. Revise las selecciones realizadas y marque las casillas para verificar que comprende que Cloud Manager implementa recursos en su entorno de AWS. Cuando esté listo, haga clic en Ir.

The screenshot shows the 'Review & Approve' wizard in the Cloud Manager interface. The top navigation bar is the same as the previous screenshot. The main content area is titled 'Create a New Working Environment' and 'Review & Approve'. It features a 'Previous Step' button and a 'hybridawscvo' section with 'AWS', 'us-east-1', and 'HA' tabs. Below this, there are two checkboxes: 'I understand that in order to activate support, I must first register Cloud Volumes ONTAP with NetApp. More information >' and 'I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements. More information >'. A 'Show API request' link is also present. The 'Overview' tab is selected, showing a table with the following details:

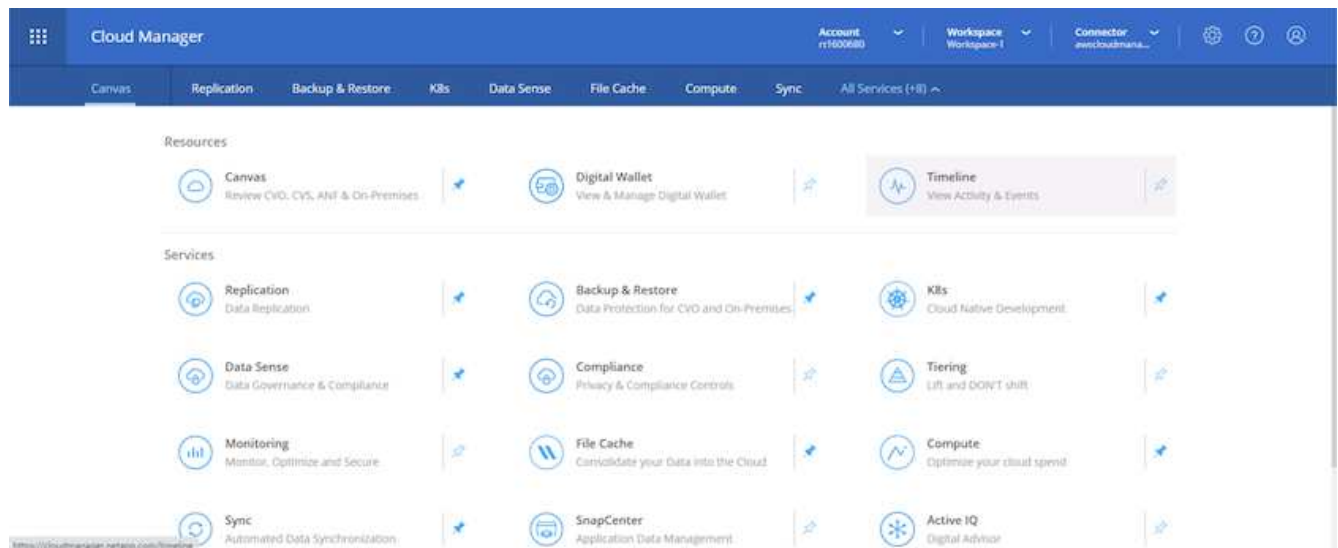
Storage System:	Cloud Volumes ONTAP HA	HA Deployment Model:	Multiple Availability Zones
License Type:	Cloud Volumes ONTAP Standard	Encryption:	AWS Managed
Capacity Limit:	10TB	Customer Master Key:	aws/ebs

At the bottom, there is a 'Go' button. The footer indicates 'Cloud Manager 5.8.9 Build 0 Aug 18, 2021 04:13:35 am UTC'.

8. Cloud Volumes ONTAP ahora comienza su proceso de implementación. Cloud Manager utiliza las API de AWS y pilas de formación de nubes para implementar Cloud Volumes ONTAP. Luego configura el sistema según sus especificaciones, brindándole un sistema listo para usar que puede utilizarse instantáneamente. El tiempo necesario para este proceso varía dependiendo de las selecciones realizadas.



9. Puede supervisar el progreso navegando a la línea de tiempo.



10. La línea de tiempo actúa como una auditoría de todas las acciones realizadas en Cloud Manager. Puede ver todas las llamadas API que realiza Cloud Manager durante la configuración tanto de AWS como del clúster ONTAP . Esto también se puede utilizar de forma eficaz para solucionar cualquier problema que pueda enfrentar.

Cloud Manager Account: r1600680 Workspace: Workspace-1 Connector: awscloudmana...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8)

Timeline

Filters: Time (1) Service Action Agent (1) Resource User Status Reset

Time	Action	Service	Agent	Resource	User	Status
Aug 18 2021, 9:42:32 pm	Check Connectivity	Cloud Manager	awscloudman...	hybridawsco	Full Name	Success
Aug 18 2021, 9:42:00 pm	Create Aws Ha Working Environment	Cloud Manager	awscloudma...	hybridawsco	Full Name	Pending
Aug 18 2021, 10:09:39 pm	Describe Operation Status					Success
Aug 18 2021, 10:09:39 pm	Describe Operation Status					Success

11. Una vez completada la implementación, el clúster CVO aparece en el lienzo, con su capacidad actual. El clúster ONTAP en su estado actual está completamente configurado para permitir una verdadera experiencia lista para usar.

Cloud Manager Account: r1600680 Workspace: Workspace-1 Connector: awscloudmana...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8)

Canvas

Add Working Environment

Working environments

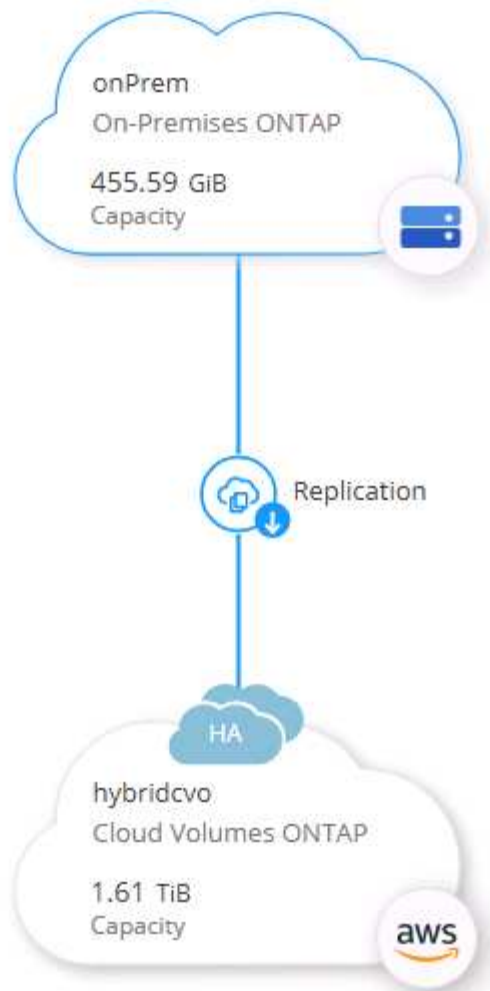
- 1 Cloud Volumes ONTAP (High-Availability)
1 GB Allocated Capacity
- 1 Amazon S3
0 Buckets

Configurar SnapMirror desde las instalaciones locales a la nube

Ahora que tiene un sistema ONTAP de origen y un sistema ONTAP de destino implementados, puede replicar volúmenes que contienen datos de base de datos en la nube.

Para obtener una guía sobre las versiones de ONTAP compatibles con SnapMirror, consulte la ["Matriz de compatibilidad de SnapMirror"](#).

1. Haga clic en el sistema ONTAP de origen (local) y arrástrelo y suéltelo en el destino, seleccione Replicación > Habilitar o seleccione Replicación > Menú > Replicar.



Seleccione Habilitar.

SERVICES



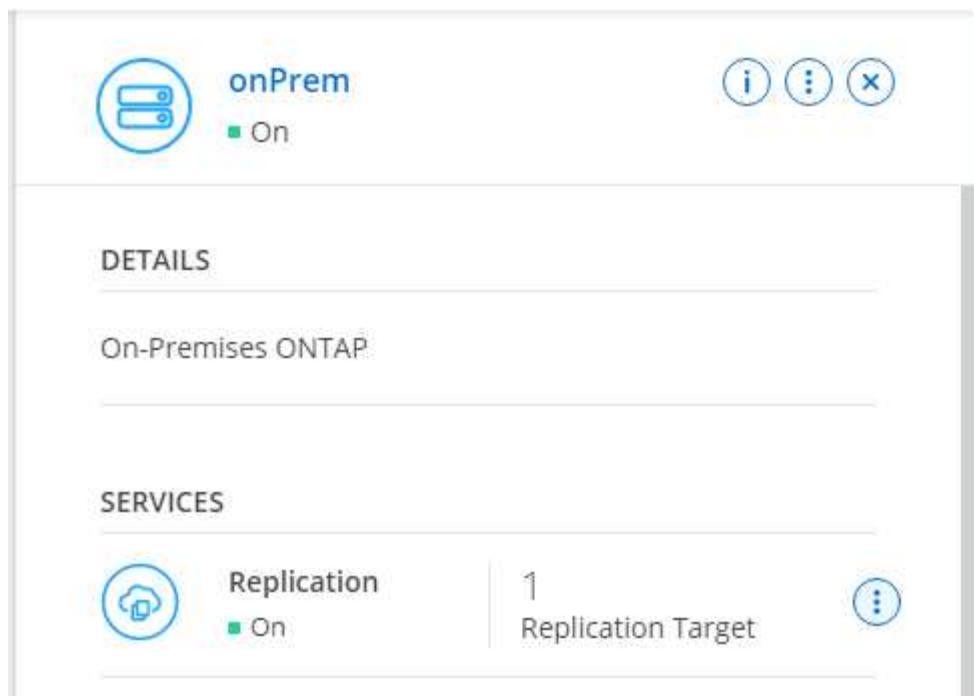
Replication

■ Off

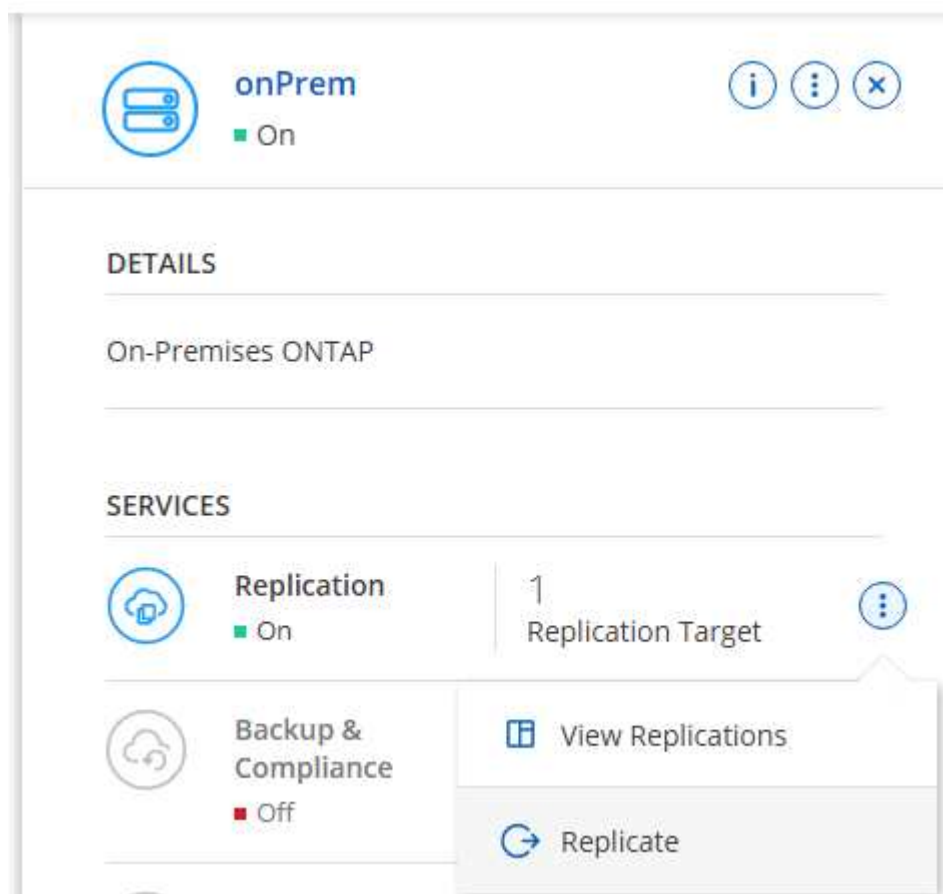
Enable



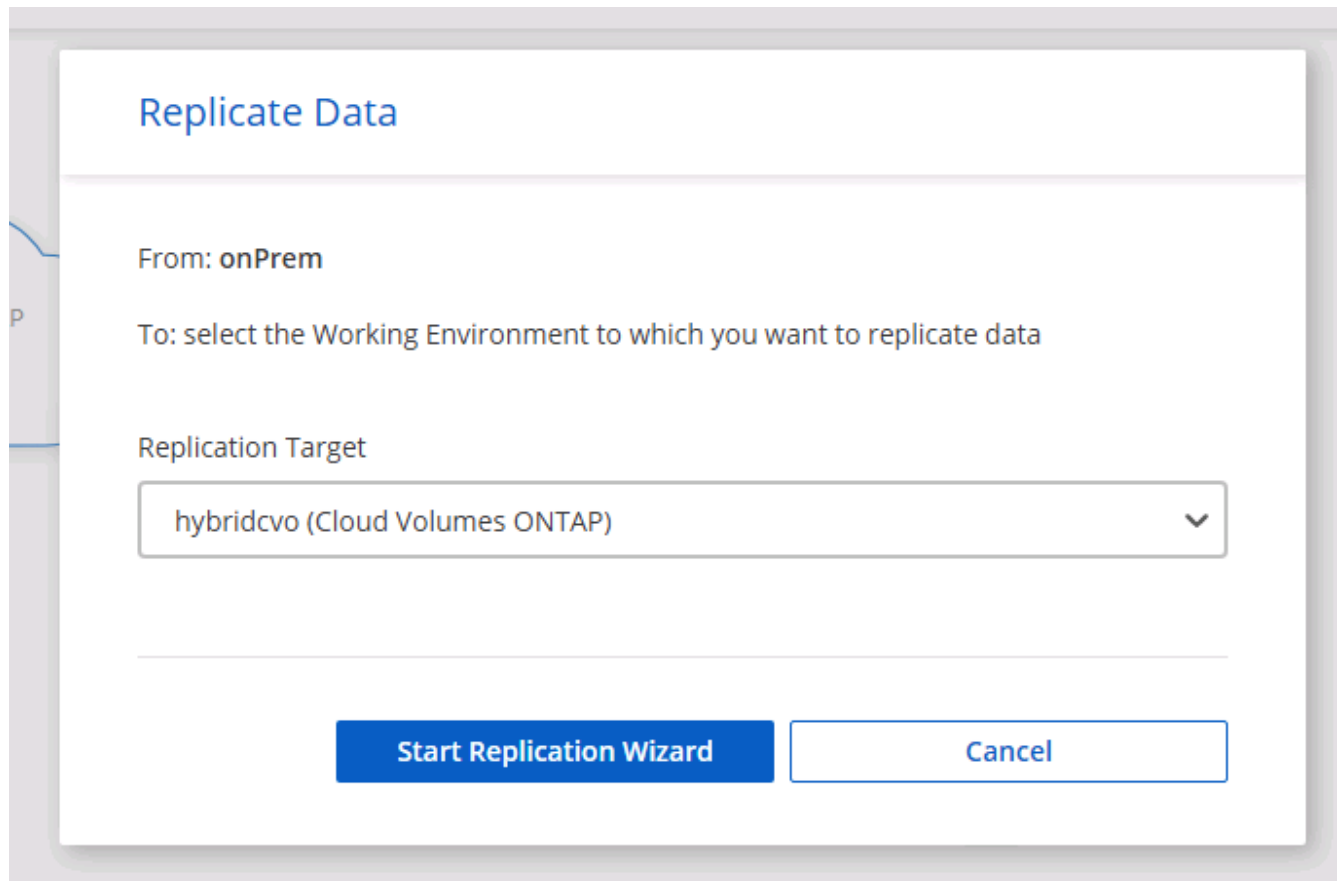
O Opciones.



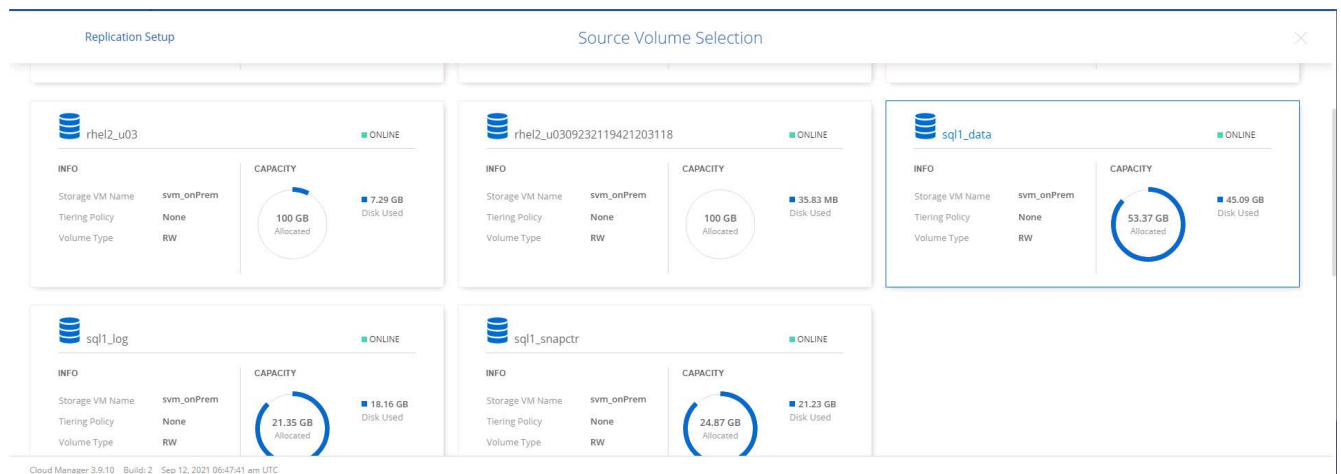
Reproducir exactamente.



2. Si no arrastró y soltó, elija el clúster de destino al que replicar.



3. Elija el volumen que desea replicar. Replicamos los datos y todos los volúmenes de registro.



4. Elija el tipo de disco de destino y la política de niveles. Para la recuperación ante desastres, recomendamos un SSD como tipo de disco y para mantener la organización de los datos. La clasificación de datos organiza los datos reflejados en un almacenamiento de objetos de bajo costo y le permite ahorrar dinero en discos locales. Cuando se rompe la relación o se clona el volumen, los datos utilizan el almacenamiento local rápido.

Replication Setup Destination Disk Type and Tiering ×

[↑ Previous Step](#)

Destination Disk Type


General Purpose SSD


General Purpose SSD - Dynamic Performance


Throughput Optimized HDD

 S3 Tiering [What are storage tiers?](#)

☒ Enabled ☐ Disabled

Note: If you enable S3 tiering, thin provisioning must be enabled on volumes created in this aggregate.

Continue

Cloud Manager 3.9.10 Build: 2 Sep 12, 2021 06:47:41 am UTC

5. Seleccione el nombre del volumen de destino: elegimos `[source_volume_name]_dr`.

Destination Volume Name

Destination Volume Name

`sql1_data_dr`

Destination Aggregate

Automatically select the best aggregate ▼

6. Seleccione la velocidad de transferencia máxima para la replicación. Esto le permite ahorrar ancho de banda si tiene una conexión de bajo ancho de banda a la nube, como una VPN.

Max Transfer Rate

You should limit the transfer rate. An unlimited rate might negatively impact the performance of other applications and it might impact your Internet performance.

☒ Limited to: MB/s

☐ Unlimited (recommended for DR only machines)

7. Definir la política de replicación. Elegimos un espejo, que toma el conjunto de datos más reciente y lo replica en el volumen de destino. También puede elegir una política diferente según sus necesidades.

Replication Policy

Default Policies

Additional Policies

 Mirror

Typically used for disaster recovery

More info

 Mirror and Backup (1 month retention)

Configures disaster recovery and long-term retention of backups on the same destination volume

More info

8. Seleccione el cronograma para activar la replicación. NetApp recomienda establecer una programación "diaria" para el volumen de datos y una programación "por hora" para los volúmenes de registro, aunque esto se puede cambiar según los requisitos.

Replication Setup Schedule

↑ Previous Step Select a replication schedule

One-time copy

No schedule

10min

Every hour
Minutes: 0th, 10th, 20th, 3...

12-hourly

Every day
Hours: 12 AM and 12 PM
Minutes: 15th minute

5min

Every hour
Minutes: 0th, 5th, 10th, 15t...

6-hourly

Every day
Hours: 12 AM, 6 AM, 12 PM...
Minutes: 15th minute

8hour

Every day
Hours: 2 AM, 10 AM and 6 ...
Minutes: 15th minute

daily

Every day
Hours: 12 AM
Minutes: 10th minute

hourly

Every hour
Minutes: 5th minute

monthly

Every month
Days: 2nd
Hours: 12 AM
Minutes: 20th minute

pg-15-minutely

Every hour

pg-6-hourly

Every day

pg-daily

Every day

pg-daily-set2

Every day

9. Revise la información ingresada, haga clic en Ir para activar el par del clúster y el par SVM (si es la primera vez que replica entre los dos clústeres) y luego implemente e inicialice la relación SnapMirror .

Replication Setup Review & Approve

↑ Previous Step Review your selection and start the replication process

Source

onPrem

sql1_data

Destination

hybridcvo

sql1_data_copy

☒ I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements.
[More information >](#)

Source Volume Allocated Size:	53.37 GB	Destination Thin Provisioning:	Yes
Source Volume Used Size:	45.09 GB	Destination Aggregate:	aggr1 (Automatically s...
Source Thin Provisioning:	Yes	Destination Storage VM:	svm_hybridcvo
Destination Volume Allocated Size:	53.37 GB	Max Transfer Rate:	100 MB/s
Destination Volume Disk Type:	General Purpose SSD (...)	SnapMirror Policy:	Mirror
Capacity Tiering:	S3	Replication Schedule:	daily

[Go](#)

10. Continúe este proceso para los volúmenes de datos y de registro.
11. Para verificar todas sus relaciones, navegue a la pestaña Replicación dentro de Cloud Manager. Aquí puedes administrar tus relaciones y consultar su estado.

Replication

7 Volume Relationships

153.32 GiB Replicated Capacity

0 Currently Transferring

7 Healthy

0 Failed

7 Volume Relationships

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
	rhel2_u01 onPrem	rhel2_u01_dr hybridcvo	43 minutes 43 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:50 AI 19.73 MiB
	rhel2_u02 onPrem	rhel2_u02_dr hybridcvo	1 hour 37 minutes 59 seconds	idle	snapmirrored	Sep 30, 2021, 2:37:08 PM 239.78 MiB
	rhel2_u03 onPrem	rhel2_u03_dr hybridcvo	16 hours 1 minute 9 seconds	idle	snapmirrored	Sep 30, 2021, 4:07:14 PM 225.37 KiB
	sql1_data onPrem	sql1_data_dr hybridcvo	1 hour 6 minutes 50 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:28 AI 24.56 KiB

12. Una vez replicados todos los volúmenes, se encontrará en un estado estable y listo para avanzar a los flujos de trabajo de recuperación ante desastres y de desarrollo y prueba.

3. Implementar una instancia de cómputo EC2 para la carga de trabajo de la base de datos

AWS ha preconfigurado instancias de cómputo EC2 para diversas cargas de trabajo. La elección del tipo de instancia determina la cantidad de núcleos de CPU, la capacidad de memoria, el tipo y la capacidad de almacenamiento y el rendimiento de la red. Para los casos de uso, con excepción de la partición del sistema operativo, el almacenamiento principal para ejecutar la carga de trabajo de la base de datos se asigna desde CVO o el motor de almacenamiento FSx ONTAP . Por lo tanto, los principales factores a considerar son la elección de los núcleos de CPU, la memoria y el nivel de rendimiento de la red. Los tipos de instancias típicos de AWS EC2 se pueden encontrar aquí: ["Tipo de instancia EC2"](#) .

Dimensionamiento de la instancia de cómputo

1. Seleccione el tipo de instancia correcto según la carga de trabajo requerida. Los factores a tener en cuenta incluyen la cantidad de transacciones comerciales que se deben respaldar, la cantidad de usuarios simultáneos, el tamaño del conjunto de datos, etc.
2. La implementación de una instancia EC2 se puede iniciar a través del Panel de EC2. Los procedimientos de implementación exactos están más allá del alcance de esta solución. Ver ["Amazon EC2"](#) Para más detalles.

Configuración de instancia de Linux para la carga de trabajo de Oracle

Esta sección contiene pasos de configuración adicionales después de implementar una instancia EC2 Linux.

1. Agregue una instancia de reserva de Oracle al servidor DNS para la resolución de nombres dentro del dominio de administración de SnapCenter .
2. Agregue un ID de usuario de administración de Linux como credenciales del sistema operativo SnapCenter con permisos de sudo sin contraseña. Habilite la ID con autenticación de contraseña SSH en la instancia EC2. (De manera predeterminada, la autenticación de contraseña SSH y el sudo sin contraseña están desactivados en las instancias EC2).
3. Configure la instalación de Oracle para que coincida con la instalación local de Oracle, como parches del sistema operativo, versiones y parches de Oracle, etc.
4. Los roles de automatización de NetApp Ansible DB se pueden aprovechar para configurar instancias EC2 para casos de uso de desarrollo/prueba de bases de datos y recuperación ante desastres. El código de automatización se puede descargar desde el sitio público de GitHub de NetApp : ["Implementación automatizada de Oracle 19c"](#) . El objetivo es instalar y configurar una pila de software de base de datos en una instancia EC2 para que coincida con las configuraciones de base de datos y sistema operativo locales.

Configuración de instancia de Windows para la carga de trabajo de SQL Server

En esta sección se enumeran los pasos de configuración adicionales después de implementar inicialmente una instancia EC2 de Windows.

1. Recupere la contraseña de administrador de Windows para iniciar sesión en una instancia a través de RDP.
2. Deshabilite el firewall de Windows, una el host al dominio de Windows SnapCenter y agregue la instancia al servidor DNS para la resolución de nombres.
3. Aprovechone un volumen de registro de SnapCenter para almacenar archivos de registro de SQL Server.
4. Configure iSCSI en el host de Windows para montar el volumen y formatear la unidad de disco.
5. Nuevamente, muchas de las tareas anteriores se pueden automatizar con la solución de automatización de NetApp para SQL Server. Consulte el sitio público de GitHub de automatización de NetApp para

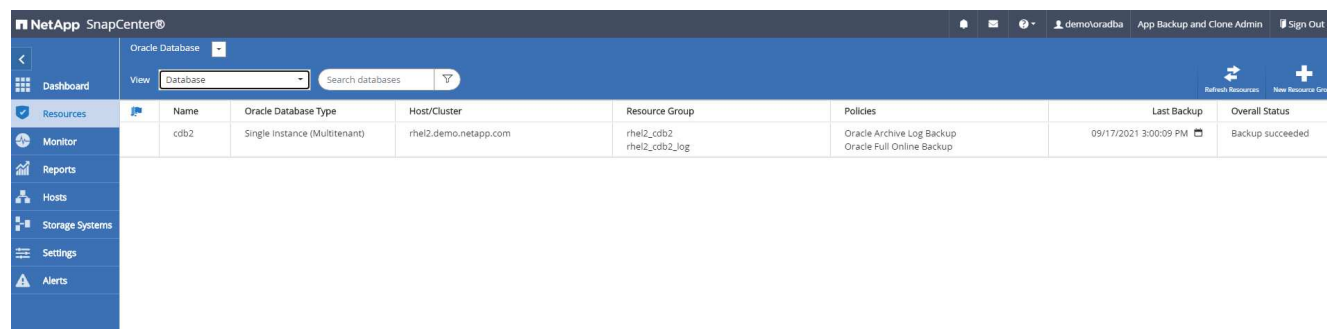
conocer los roles y las soluciones recientemente publicados: ["Automatización de NetApp"](#) .

Flujo de trabajo para desarrollo y pruebas que se trasladan a la nube

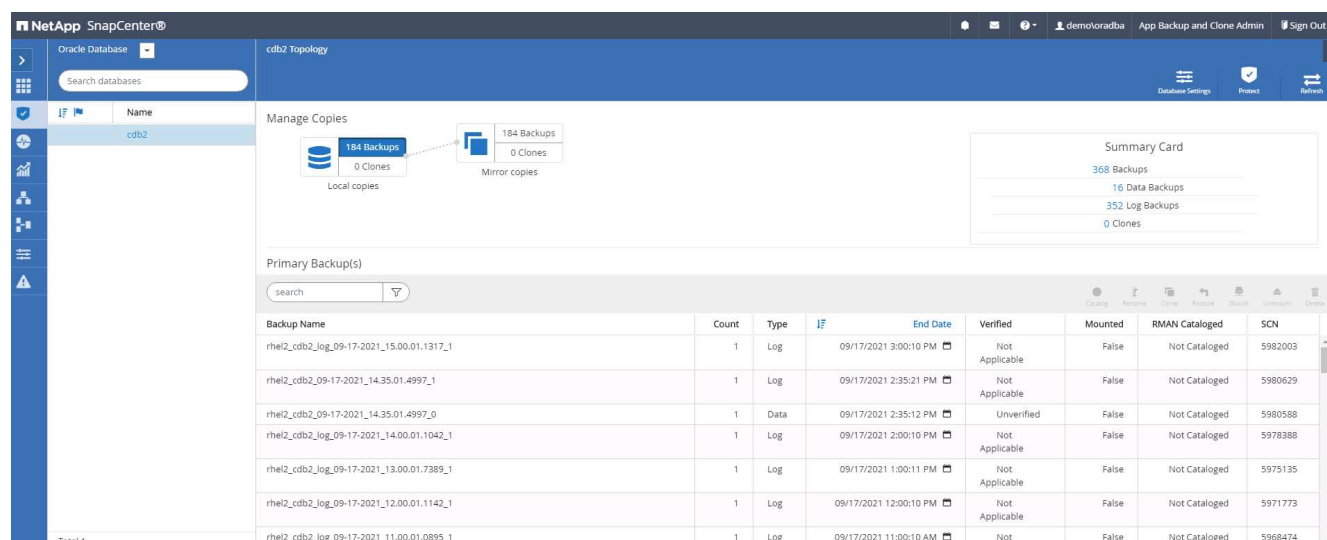
La agilidad de la nube pública, el tiempo para obtener valor y el ahorro de costos son propuestas de valor significativas para las empresas que adoptan la nube pública para el desarrollo de aplicaciones de bases de datos y el esfuerzo de prueba. No hay mejor herramienta que SnapCenter para hacer esto realidad. SnapCenter no solo puede proteger su base de datos de producción local, sino que también puede clonar rápidamente una copia para el desarrollo de aplicaciones o pruebas de código en la nube pública consumiendo muy poco almacenamiento adicional. A continuación se detallan los procesos paso a paso para utilizar esta herramienta.

Clonar una base de datos Oracle para desarrollo/prueba a partir de una copia de seguridad de instantánea replicada

1. Inicie sesión en SnapCenter con un ID de usuario de administración de base de datos para Oracle. Vaya a la pestaña Recursos, que muestra las bases de datos de Oracle que están protegidas por SnapCenter.



2. Haga clic en el nombre de la base de datos local deseada para la topología de respaldo y la vista detallada. Si se habilita una ubicación replicada secundaria, se muestran copias de seguridad reflejadas vinculadas.



3. Cambié a la vista de copias de seguridad reflejadas haciendo clic en copias de seguridad reflejadas. Luego se muestran las copias de seguridad del espejo secundario.

Manage Copies

Local copies: 184 Backups, 0 Clones
Mirror copies: 184 Backups, 0 Clones

Summary Card

- 368 Backups
- 16 Data Backups
- 352 Log Backups
- 0 Clones

Secondary Mirror Backup(s)

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log	09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_09-17-2021_14.35.01.4997_1	1	Log	09/17/2021 2:35:21 PM	Not Applicable	False	Not Cataloged	5980629
rhel2_cdb2_09-17-2021_14.35.01.4997_0	1	Data	09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhel2_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log	09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388
rhel2_cdb2_log_09-17-2021_13.00.01.7389_1	1	Log	09/17/2021 1:00:11 PM	Not Applicable	False	Not Cataloged	5975135
rhel2_cdb2_log_09-17-2021_12.00.01.1142_1	1	Log	09/17/2021 12:00:10 PM	Not Applicable	False	Not Cataloged	5971773
rhel2_cdb2_log_09-17-2021_11.00.01.0895_1	1	Log	09/17/2021 11:00:10 AM	Not Applicable	False	Not Cataloged	5968474

Total 1

4. Seleccione una copia de seguridad de la base de datos secundaria reflejada para clonar y determine un punto de recuperación ya sea por hora y número de cambio del sistema o por SCN. Generalmente, el punto de recuperación debe estar detrás del tiempo total de la copia de seguridad de la base de datos o del SCN que se va a clonar. Una vez decidido un punto de recuperación, se debe montar la copia de seguridad del archivo de registro necesaria para la recuperación. La copia de seguridad del archivo de registro debe montarse en el servidor de base de datos de destino donde se alojará la base de datos clonada.

Mount backups

Choose the host to mount the backup

ora-standby.demo.netapp.com

Mount path :

/var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_09-17-2021_14.35.01.4997_1/cdb2

Secondary storage location : Snap Vault / Snap Mirror

Source Volume

svm_onPrem:rhel2_u03

Destination Volume

svm_hybridcvo:rhel2_u03_dr

Mount

Cancel

NetApp SnapCenter®

Oracle Database

Search databases

cdb2 Topology

Manage Copies

184 Backups
0 Clones
Local copies

184 Backups
1 Clone
Mirror copies

Summary Card

368 Backups
16 Data Backups
352 Log Backups
1 Clone

Secondary Mirror Backup(s)

search

Backup Name	Count	Type	IF	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_16.00.01.2156_1	1	Log		09/17/2021 4:00:10 PM	Not Applicable	False	Not Cataloged	5985272
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log		09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_log_09-17-2021_14.35.01.4997_1	1	Log		09/17/2021 2:35:21 PM	Not Applicable	True	Not Cataloged	5980629
rhel2_cdb2_log_09-17-2021_14.35.01.4997_0	1	Data		09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhel2_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log		09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388



Si la poda de registros está habilitada y el punto de recuperación se extiende más allá de la última poda de registros, es posible que sea necesario montar varias copias de seguridad de registros de archivo.

- Resalte la copia de seguridad completa de la base de datos que se va a clonar y, a continuación, haga clic en el botón Clonar para iniciar el flujo de trabajo de clonación de base de datos.

cdb2 Topology

search

Backup Name	Count	Type	IF	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_16.00.01.2156_1	1	Log		09/17/2021 4:00:10 PM	Not Applicable	False	Not Cataloged	5985272
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log		09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_log_09-17-2021_14.35.01.4997_1	1	Log		09/17/2021 2:35:21 PM	Not Applicable	True	Not Cataloged	5980629
rhel2_cdb2_log_09-17-2021_14.35.01.4997_0	1	Data		09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhel2_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log		09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388

- Elija un SID de base de datos clonada adecuado para una base de datos de contenedor completa o un clon de CDB.

Clone from cdb2

1

Name

2

Locations

3

Credentials

4

PreOps

5

PostOps

6

Notification

7

Summary

☒ Complete Database Clone

Clone SID

cdb2test

Exclude PDBs

Type to find PDBs

☐ PDB Clone

Secondary storage location : Snap Vault / Snap Mirror

Data

Source Volume

svm_onPrem:rhel2_u02

Destination Volume

svm_hybridcvo:rhel2_u02_dr

Logs

Source Volume

svm_onPrem:rhel2_u03

Destination Volume

svm_hybridcvo:rhel2_u03_dr

Previous

Next

7. Seleccione el host de clonación de destino en la nube, y el flujo de trabajo de clonación creará los directorios de archivo de datos, archivo de control y registro de rehacer.

Clone from cdb2

1

Name

2

Locations

3

Credentials

4

PreOps

5

PostOps

6

Notification

7

Summary

Select the host to create a clone

Clone host
ora-standby.demo.netapp.com

Datafile locations ⓘ

/u02_cdb2test
Reset

Control files ⓘ

/u02_cdb2test/cdb2test/control/control01.ctl
/u02_cdb2test/cdb2test/control/control02.ctl
Reset

Redo logs ⓘ

Group	Size	Unit	Number of files
RedoGroup 1	200	MB	1
/u02_cdb2test/cdb2test/redolog/redo03.log			
RedoGroup 2	200	MB	1

Previous
Next

- El nombre de credencial Ninguno se utiliza para la autenticación basada en el sistema operativo, lo que hace que el puerto de la base de datos sea irrelevante. Complete los datos adecuados de Oracle Home, Oracle OS User y Oracle OS Group tal como están configurados en el servidor de base de datos clonado de destino.

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Database Credentials for the clone

Credential name for sys user

None

+

i

Database port

1521

Oracle Home Settings

i

Oracle Home

/u01/app/oracle/product/19800/cdb2

Oracle OS User

oracle

Oracle OS Group

oinstall

Previous

Next

9. Especifique los scripts que se ejecutarán antes de la operación de clonación. Más importante aún, el parámetro de instancia de base de datos se puede ajustar o definir aquí.

Clone from cdb2

1

Name

2

Locations

3

Credentials

4

5

6

7

Specify scripts to run before clone operation ⓘ

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Arguments

Script timeout

60

secs

Database Parameter settings

processes	320	×	+ Reset
remote_login_passwordfile	EXCLUSIVE	×	
sga_target	4311744512	×	
undo_tablespace	UNDOTBS1	×	

Previous

Next

10. Especifique el punto de recuperación por fecha y hora o por SCN. Hasta Cancelar recupera la base de datos hasta los registros de archivo disponibles. Especifique la ubicación del registro de archivo externo desde el host de destino donde está montado el volumen del registro de archivo. Si el propietario de Oracle del servidor de destino es diferente del servidor de producción local, verifique que el propietario de Oracle del servidor de destino pueda leer el directorio de registro de archivo.

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

☒ Recover Database

☐ Until Cancel

☐ Date and Time

☒ Until SCN (System Change Number)

5980629

Specify external archive log locations

/var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_09-17-2021_14.35.01.4997_1/cdb2/1/orareco/CDB2/archivelog/

☒ Create new DBID

☒ Create tempfile for temporary tablespace

☐ Enter SQL queries to apply when clone is created

☐ Enter scripts to run after clone operation

Previous

Next

```

oracle@ora-standby:tmp$ ls /var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_09-17-2021_14.35.01.4997_1/cdb2/1/orareco/CDB2/archivelog/
2021_08_26 2021_08_28 2021_08_30 2021_09_01 2021_09_03 2021_09_05 2021_09_07 2021_09_09 2021_09_11 2021_09_13 2021_09_15 2021_09_17
2021_08_27 2021_08_29 2021_08_31 2021_09_02 2021_09_04 2021_09_06 2021_09_08 2021_09_10 2021_09_12 2021_09_14 2021_09_16
oracle@ora-standby:tmp$

```

11. Configure el servidor SMTP para notificaciones por correo electrónico si lo desea.

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Provide email settings ⓘ

Email preference

Never

From

From email

To

Email to

Subject

Notification

☐ Attach job report

⚠

If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

✕

Previous

Next

12. Resumen del clon.

Clone from cdb2

1 Name
2 Locations
3 Credentials
4 PreOps
5 PostOps
6 Notification
7 Summary

Summary

Clone from backup	rhel2_cdb2_09-17-2021_14.35.01.4997_0
Clone SID	cdb2test
Clone server	ora-standby.demo.netapp.com
Exclude PDBs	none
Oracle home	/u01/app/oracle/product/19800/cdb2
Oracle OS user	oracle
Oracle OS group	oinstall
Datafile mountpaths	/u02_cdb2test
Control files	/u02_cdb2test/cdb2test/control/control01.ctl /u02_cdb2test/cdb2test/control/control02.ctl
Redo groups	RedoGroup =1 TotalSize =200 Path =/u02_cdb2test/cdb2test/redolog/redo03.log RedoGroup =2 TotalSize =200 Path =/u02_cdb2test/cdb2test/redolog/redo02.log RedoGroup =3 TotalSize =200 Path =/u02_cdb2test/cdb2test/redolog/redo01.log
Recovery scope	Until SCN 5980629
Prescript full path	none
Prescript arguments	
Postscript full path	none
Postscript arguments	

Previous

Finish

13. Debe validar después de la clonación para asegurarse de que la base de datos clonada esté operativa. Se pueden realizar algunas tareas adicionales, como iniciar el escucha o desactivar el modo de archivo de registro de la base de datos, en la base de datos de desarrollo/prueba.

```

oracle@ora-standby/tmp
[oracle@ora-standby tmp]$ export ORACLE_SID=cdb2test
[oracle@ora-standby tmp]$ export ORACLE_HOME=/u01/app/oracle/product/19800/cdb2
[oracle@ora-standby tmp]$ export PATH=$PATH:$ORACLE_HOME/bin
[oracle@ora-standby tmp]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Sep 17 17:49:29 2021
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> select name, log_mode from v$database;

NAME          LOG MODE
-----
CDB2TEST      ARCHIVELOG

SQL> select instance_name, host_name from v$instance;

INSTANCE_NAME
HOST_NAME
-----
cdb2test
ora-standby.demo.netapp.com

SQL> show pdbs

  CON_ID CON_NAME              OPEN MODE  RESTRICTED
-----
2 PDB$SEED                  READ ONLY  NO
3 CDB2_PDB1                  READ WRITE NO
4 CDB2_PDB2                  READ WRITE NO
5 CDB2_PDB3                  READ WRITE NO
SQL>

```

Clonar una base de datos SQL para desarrollo/prueba desde una copia de seguridad instantánea replicada

1. Inicie sesión en SnapCenter con un ID de usuario de administración de base de datos para SQL Server. Navegue a la pestaña Recursos, que muestra las bases de datos de usuario de SQL Server protegidas por SnapCenter y una instancia de SQL en espera de destino en la nube pública.

NetApp SnapCenter

Microsoft SQL Server

View Database search by name

Resources

	Name	Instance	Host	Last Backup	Overall Status	Type
master	sq11	sq11.demo.netapp.com			Not available for backup	System database
model	sq11	sq11.demo.netapp.com			Not available for backup	System database
msdb	sq11	sq11.demo.netapp.com			Not available for backup	System database
tempdb	sq11	sq11.demo.netapp.com			Not available for backup	System database
tpcc	sq11	sq11.demo.netapp.com		09/16/2021 7:35:05 PM	Backup succeeded	User database
master	sq1-standby	sq1-standby.demo.netapp.com			Not available for backup	System database
model	sq1-standby	sq1-standby.demo.netapp.com			Not available for backup	System database
msdb	sq1-standby	sq1-standby.demo.netapp.com			Not available for backup	System database
tempdb	sq1-standby	sq1-standby.demo.netapp.com			Not available for backup	System database

2. Haga clic en el nombre de la base de datos del usuario de SQL Server local deseado para ver la topología de las copias de seguridad y la vista detallada. Si se habilita una ubicación replicada secundaria, se muestran copias de seguridad reflejadas vinculadas.

NetApp SnapCenter

Microsoft SQL Server

tpcc (sq11) Topology

search by name

Manage Copies

7 Backups 0 Clones Local copies

7 Backups 0 Clones Mirror copies

Summary Card

14 Backups 0 Clones

Primary Backup(s)

search

Backup Name	Count	Type	End Date	Verified
sq11_tpcc_09-16-2021_18.25.01.4024	1	Full backup	09/16/2021 6:25:05 PM	Unverified
sq11_tpcc_09-15-2021_18.25.01.4604	1	Full backup	09/15/2021 6:25:06 PM	Unverified
sq11_tpcc_09-14-2021_18.25.01.5233	1	Full backup	09/14/2021 6:25:05 PM	Unverified
sq11_tpcc_09-13-2021_18.25.01.4500	1	Full backup	09/13/2021 6:25:05 PM	Unverified
sq11_tpcc_09-12-2021_18.25.01.4016	1	Full backup	09/12/2021 6:25:05 PM	Unverified
sq11_tpcc_09-11-2021_18.25.01.3753	1	Full backup	09/11/2021 6:25:05 PM	Unverified
sq11_tpcc_09-10-2021_18.36.25.5430	1	Full backup	09/10/2021 6:36:29 PM	Unverified

3. Cambie a la vista Copias de seguridad reflejadas haciendo clic en Copias de seguridad reflejadas. A continuación se muestran las copias de seguridad del espejo secundario. Dado que SnapCenter realiza copias de seguridad del registro de transacciones de SQL Server en una unidad dedicada para la recuperación, aquí solo se muestran las copias de seguridad completas de la base de datos.

NetApp SnapCenter®

Microsoft SQL Server

tpcc (sql1) Topology

search by name

Clone Library | Protect | Details | Refresh

Manage Copies

Local copies: 7 Backups, 0 Clones

Mirror copies: 7 Backups, 0 Clones

Summary Card

14 Backups

0 Clones

Secondary Mirror Backup(s)

search

Backup Name	Count	Type	if	End Date	Verified
sql1_tpcc_09-16-2021_18.25.01.4024	1	Full backup		09/16/2021 6:25:05 PM	Unverified
sql1_tpcc_09-15-2021_18.25.01.4604	1	Full backup		09/15/2021 6:25:06 PM	Unverified
sql1_tpcc_09-14-2021_18.25.01.5233	1	Full backup		09/14/2021 6:25:05 PM	Unverified
sql1_tpcc_09-13-2021_18.25.01.4500	1	Full backup		09/13/2021 6:25:05 PM	Unverified
sql1_tpcc_09-12-2021_18.25.01.4016	1	Full backup		09/12/2021 6:25:05 PM	Unverified
sql1_tpcc_09-11-2021_18.25.01.3753	1	Full backup		09/11/2021 6:25:05 PM	Unverified
sql1_tpcc_09-10-2021_18.36.25.5430	1	Full backup		09/10/2021 6:36:29 PM	Unverified

4. Seleccione una copia de seguridad y luego haga clic en el botón Clonar para iniciar el flujo de trabajo Clonar desde copia de seguridad.

NetApp SnapCenter®

Microsoft SQL Server

tpcc (sql1) Topology

search by name

Clone Library | Protect | Details | Refresh

Manage Copies

Local copies: 7 Backups, 0 Clones

Mirror copies: 7 Backups, 1 Clone

Summary Card

14 Backups

1 Clone

Secondary Mirror Backup(s)

search

Backup Name	Count	Type	if	End Date	Verified
sql1_tpcc_09-19-2021_18.25.01.4134	1	Full backup		09/19/2021 6:25:05 PM	Unverified
sql1_tpcc_09-18-2021_18.25.01.3963	1	Full backup		09/18/2021 6:25:05 PM	Unverified
sql1_tpcc_09-17-2021_18.25.01.4218	1	Full backup		09/17/2021 6:25:05 PM	Unverified
sql1_tpcc_09-16-2021_18.25.01.4024	1	Full backup		09/16/2021 6:25:05 PM	Unverified
sql1_tpcc_09-15-2021_18.25.01.4604	1	Full backup		09/15/2021 6:25:06 PM	Unverified
sql1_tpcc_09-14-2021_18.25.01.5233	1	Full backup		09/14/2021 6:25:05 PM	Unverified
sql1_tpcc_09-13-2021_18.25.01.4500	1	Full backup		09/13/2021 6:25:05 PM	Unverified

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Clone settings

Clone server

Choose

Clone instance

Nothing selected

Clone name

tpcc

Choose mount option

☒ Auto assign mount point

☐ Auto assign volume mount point under path

full file path

Secondary storage location : Snap Vault / Snap Mirror

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridcvo:sql1_data_dr
svm_onPrem:sql1_log	svm_hybridcvo:sql1_log_dr

Previous

Next

5. Seleccione un servidor en la nube como servidor de clonación de destino, el nombre de la instancia de clonación y el nombre de la base de datos de clonación. Elija un punto de montaje asignado automáticamente o una ruta de punto de montaje definida por el usuario.

Clone from backup

1 Clone Options
2 Logs
3 Script
4 Notification
5 Summary

Clone settings

Clone server
sql-standby.demo.netapp.com

Clone instance
sql-standby

Clone name
tpcc_clone

Choose mount option

☒ Auto assign mount point
☐ Auto assign volume mount point under path
full file path

Secondary storage location : Snap Vault / Snap Mirror

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridcvo:sql1_data_dr
svm_onPrem:sql1_log	svm_hybridcvo:sql1_log_dr

Previous
Next

- Determine un punto de recuperación ya sea por el tiempo de copia de seguridad del registro o por una fecha y hora específicas.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Choose logs

☐ All log backups

☒ By log backups until

9/17/2021 6:25:10 PM

☐ By specific date until

09/17/2021 6:25:05 PM

☐ None

Previous

Next

7. Especifique scripts opcionales para ejecutar antes y después de la operación de clonación.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Specify optional scripts to run before and after performing a clone from backup job

Prescript full path

Prescript arguments

Choose optional arguments...

Postscript full path

Postscript arguments

Choose optional arguments...

Script timeout

60

secs

Previous

Next

8. Configure un servidor SMTP si desea recibir notificaciones por correo electrónico.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Provide email settings ⓘ

Email preference

Never

From

From email

To

Email to

Subject

Notification

☐ Attach Job Report

⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

×

Previous

Next

9. Resumen del clon.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Summary

Clone server

sql-standby.demo.netapp.com

Clone instance

sql-standby

Clone name

tpcc_dev

Mount option

Auto assign volume mount point under custom path

Prescript full path

None

Prescript arguments

Postscript full path

None

Postscript arguments

Send email

No

Previous

Finish

- Supervise el estado del trabajo y valide que la base de datos del usuario previsto se haya adjuntado a una instancia de SQL de destino en el servidor clon en la nube.

NetApp SnapCenter®						
Jobs - Filter						
ID	Status	Name	Start date	End date	Owner	
766	✓	Clone from backup 'sql1_tpcc-09-16-2021_18.25.01.4024'	09/16/2021 8:05:25 PM	09/16/2021 8:06:17 PM	demo:sqlqdba	
763	✓	Discover resources for all hosts	09/16/2021 7:56:49 PM	09/16/2021 7:56:54 PM	demo:sqlqdba	
761	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/16/2021 7:35:00 PM	09/16/2021 7:37:08 PM	demo:sqlqdba	
760	⚠	Discover resources for all hosts	09/16/2021 7:19:05 PM	09/16/2021 7:19:09 PM	demo:sqlqdba	
759	⚠	Discover resources for all hosts	09/16/2021 7:18:43 PM	09/16/2021 7:18:48 PM	demo:sqlqdba	
756	⚠	Discover resources for all hosts	09/16/2021 6:59:51 PM	09/16/2021 6:59:56 PM	demo:sqlqdba	
753	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/16/2021 6:35:00 PM	09/16/2021 6:37:07 PM	demo:sqlqdba	
750	✓	Backup of Resource Group 'sql1_tpcc' with policy 'SQL Server Full Backup'	09/16/2021 6:25:01 PM	09/16/2021 6:27:14 PM	demo:sqlqdba	
749	✓	Discover resources for host 'sql-standby.demo.netapp.com'	09/16/2021 6:19:00 PM	09/16/2021 6:19:05 PM	DemoAdministrator	
745	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/16/2021 5:35:00 PM	09/16/2021 5:37:08 PM	demo:sqlqdba	

Configuración posterior a la clonación

- Una base de datos de producción de Oracle local generalmente se ejecuta en modo de archivo de registro. Este modo no es necesario para una base de datos de desarrollo o prueba. Para desactivar el modo de archivo de registro, inicie sesión en Oracle DB como sysdba, ejecute un comando de cambio de modo de registro e inicie la base de datos para acceder.
- Configure un escucha de Oracle o registre la base de datos recién clonada con un escucha existente para el acceso de los usuarios.
- Para SQL Server, cambie el modo de registro de Completo a Fácil para que el archivo de registro de desarrollo/prueba de SQL Server se pueda reducir fácilmente cuando esté llenando el volumen de registro.

Actualizar la base de datos de clones

1. Elimine las bases de datos clonadas y limpie el entorno del servidor de bases de datos en la nube. A continuación, siga los procedimientos anteriores para clonar una nueva base de datos con datos nuevos. Sólo se necesitan unos minutos para clonar una nueva base de datos.
2. Apague la base de datos clonada y ejecute un comando de actualización de clonación mediante la CLI. Consulte la siguiente documentación de SnapCenter para obtener más detalles: ["Actualizar un clon"](#) .

¿A dónde acudir para obtener ayuda?

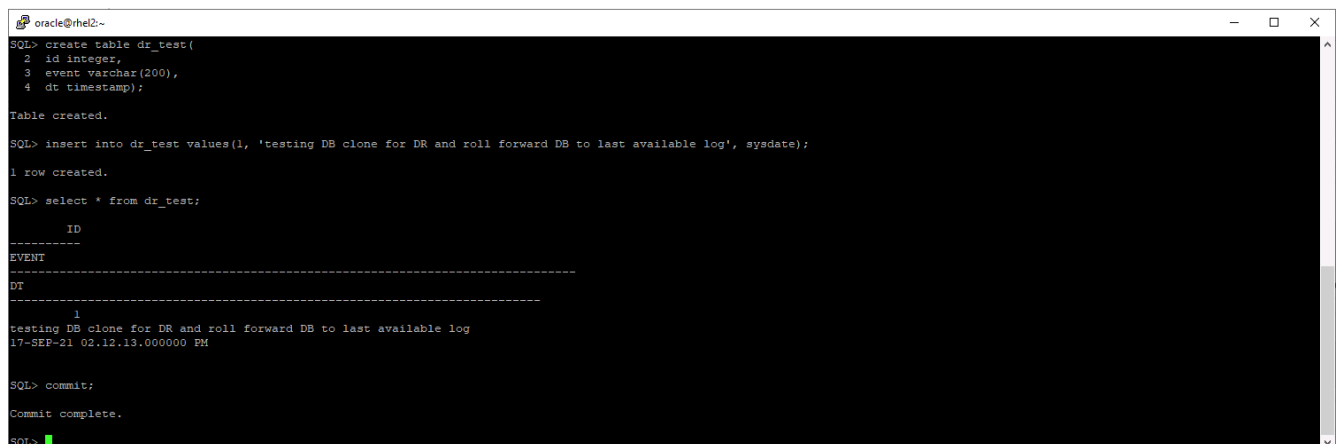
Si necesita ayuda con esta solución y casos de uso, únase a la ["Canal de Slack de soporte de la comunidad de automatización de soluciones de NetApp"](#) y busca el canal de automatización de soluciones para publicar tus dudas o consultas.

Flujo de trabajo de recuperación ante desastres

Las empresas han adoptado la nube pública como un recurso viable y un destino para la recuperación ante desastres. SnapCenter hace que este proceso sea lo más sencillo posible. Este flujo de trabajo de recuperación ante desastres es muy similar al flujo de trabajo de clonación, pero la recuperación de la base de datos se ejecuta a través del último registro disponible que se replicó en la nube para recuperar todas las transacciones comerciales posibles. Sin embargo, existen pasos adicionales de preconfiguración y posconfiguración específicos para la recuperación ante desastres.

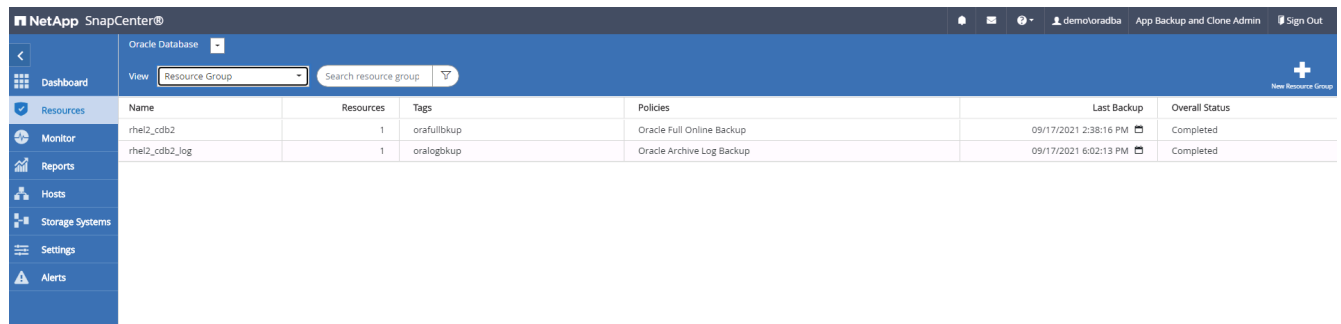
Clonar una base de datos de producción Oracle local a la nube para recuperación ante desastres

1. Para validar que la recuperación del clon se ejecute a través del último registro disponible, creamos una pequeña tabla de prueba e insertamos una fila. Los datos de prueba se recuperarían después de una recuperación completa al último registro disponible.



```
oracle@rhel2~  
SQL> create table dr_test(  
  2 id integer,  
  3 event varchar(200),  
  4 dt timestamp);  
Table created.  
SQL> insert into dr_test values(1, 'testing DB clone for DR and roll forward DB to last available log', sysdate);  
1 row created.  
SQL> select * from dr_test;  
      ID  
-----  
EVENT  
-----  
DT  
-----  
1  
testing DB clone for DR and roll forward DB to last available log  
17-SEP-21 02.12.13.000000 PM  
SQL> commit;  
Commit complete.  
SQL>
```

2. Inicie sesión en SnapCenter como un ID de usuario de administración de base de datos para Oracle. Vaya a la pestaña Recursos, que muestra las bases de datos de Oracle que están protegidas por SnapCenter.



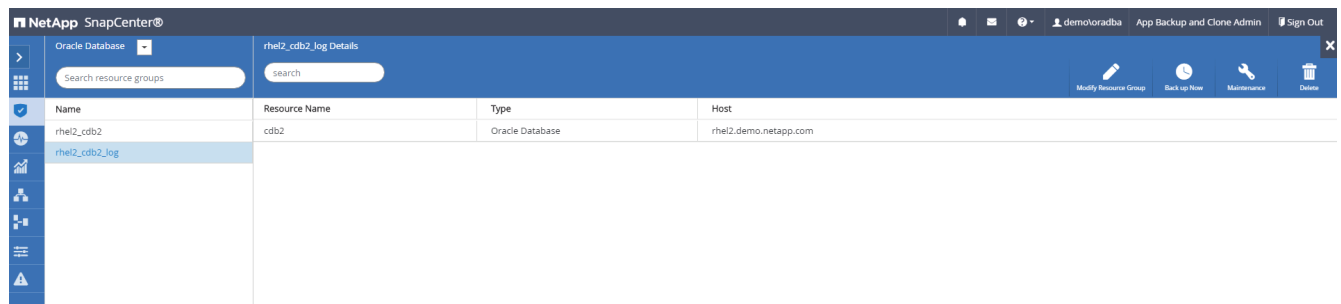
NetApp SnapCenter® Oracle Database

View: Resource Group Search resource group

Name	Resources	Tags	Policies	Last Backup	Overall Status
rhel2_cdb2	1	orafullbkup	Oracle Full Online Backup	09/17/2021 2:38:16 PM	Completed
rhel2_cdb2_log	1	oralogbkup	Oracle Archive Log Backup	09/17/2021 6:02:13 PM	Completed

Dashboard Resources Monitor Reports Hosts Storage Systems Settings Alerts

3. Seleccione el grupo de recursos de registro de Oracle y haga clic en Realizar copia de seguridad ahora para ejecutar manualmente una copia de seguridad del registro de Oracle para vaciar la última transacción en el destino en la nube. En un escenario de DR real, la última transacción recuperable depende de la frecuencia de replicación del volumen del registro de la base de datos a la nube, que a su vez depende de la política de RTO o RPO de la empresa.

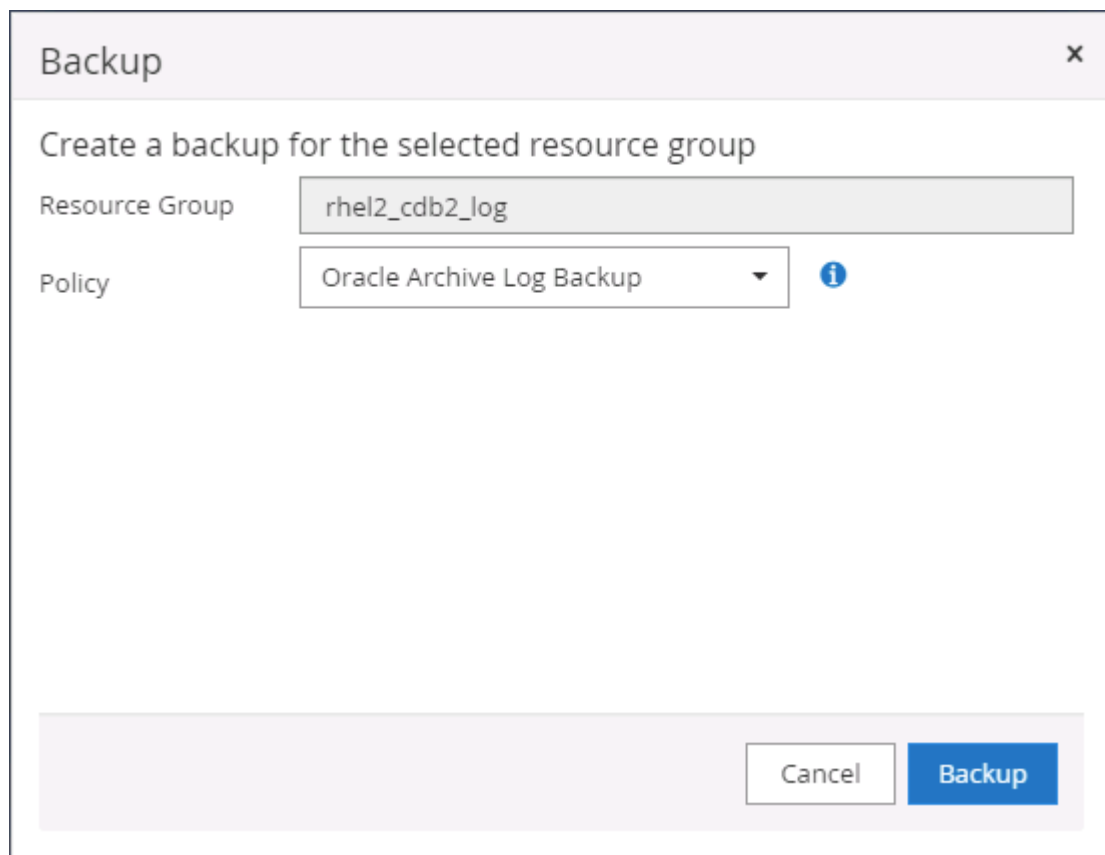


NetApp SnapCenter® Oracle Database rhel2_cdb2_log Details

Search resource groups Search

Name	Resource Name	Type	Host
rhel2_cdb2	cdb2	Oracle Database	rhel2.demo.netapp.com
rhel2_cdb2_log			

Modify Resource Group Back up Now Maintenance Delete



Backup [X]

Create a backup for the selected resource group

Resource Group: rhel2_cdb2_log

Policy: Oracle Archive Log Backup [i]

Cancel Backup



SnapMirror asincrónico pierde datos que no llegaron al destino en la nube en el intervalo de respaldo del registro de la base de datos en un escenario de recuperación ante desastres. Para minimizar la pérdida de datos, se pueden programar copias de seguridad de registros más frecuentes. Sin embargo, existe un límite en la frecuencia de las copias de seguridad de registros que es técnicamente alcanzable.

4. Seleccione la última copia de seguridad del registro en las copias de seguridad del espejo secundario y monte la copia de seguridad del registro.

The screenshot shows the NetApp SnapCenter interface for managing Oracle Database backups. The left sidebar shows a tree view with 'cdb2' selected. The main area displays 'Manage Copies' for 'cdb2 Topology'. It shows 'Local copies' with 185 Backups and 0 Clones, and 'Mirror copies' with 185 Backups and 2 Clones. A 'Summary Card' on the right shows: 370 Backups, 16 Data Backups, 354 Log Backups, and 2 Clones. Below this is a table of 'Secondary Mirror Backup(s)'. The table has columns: Backup Name, Count, Type, I/F, End Date, Verified, Mounted, RMAN Cataloged, and SCN. The data rows are:

Backup Name	Count	Type	I/F	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_18.20.04.1177_1	1	Log		09/17/2021 6:20:13 PM	Not Applicable	False	Not Cataloged	5994710
rhel2_cdb2_log_09-17-2021_18.00.01.2424_1	1	Log		09/17/2021 6:00:09 PM	Not Applicable	False	Not Cataloged	5992079
rhel2_cdb2_log_09-17-2021_17.00.01.1566_1	1	Log		09/17/2021 5:00:20 PM	Not Applicable	False	Not Cataloged	5988842

The 'Mount backups' dialog box is shown. It has a title bar with a close button. The main content area includes:

- 'Choose the host to mount the backup': A dropdown menu showing 'ora-standby.demo.netapp.com'.
- 'Mount path': A text field showing '/var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_log_09-17-2021_18.20.04.1177_1/cdb2'.
- 'Secondary storage location : Snap Vault / Snap Mirror': A section with two columns: 'Source Volume' and 'Destination Volume'.
 - 'Source Volume': A text field showing 'svm_onPrem:rhel2_u03'.
 - 'Destination Volume': A dropdown menu showing 'svm_hybridcvo:rhel2_u03_dr'.

At the bottom right, there are two buttons: 'Mount' and 'Cancel'.

5. Seleccione la última copia de seguridad completa de la base de datos y haga clic en Clonar para iniciar el flujo de trabajo de clonación.

NetApp SnapCenter®

Oracle Database

Search databases

cdb2 Topology

Manage Copies

Local copies: 185 Backups, 0 Clones

Mirror copies: 185 Backups, 2 Clones

Summary Card

- 370 Backups
- 16 Data Backups
- 354 Log Backups
- 2 Clones

Secondary Mirror Backup(s)

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_18.20.04.1177_1	1	Log	09/17/2021 6:20:13 PM	Not Applicable	True	Not Cataloged	5994710
rhel2_cdb2_log_09-17-2021_18.00.01.2424_1	1	Log	09/17/2021 6:00:09 PM	Not Applicable	False	Not Cataloged	5992079
rhel2_cdb2_log_09-17-2021_17.00.01.1566_1	1	Log	09/17/2021 5:00:20 PM	Not Applicable	False	Not Cataloged	5988842
rhel2_cdb2_log_09-17-2021_16.00.01.2156_1	1	Log	09/17/2021 4:00:10 PM	Not Applicable	False	Not Cataloged	5985272
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log	09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_log_09-17-2021_14.35.01.4997_1	1	Log	09/17/2021 2:35:21 PM	Not Applicable	False	Not Cataloged	5980629
rhel2_cdb2_09-17-2021_14.35.01.4997_0	1	Data	09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588

Total 3

6. Seleccione un ID de base de datos clonada único en el host.

Clone from cdb2

1 Name

Complete Database Clone

Clone SID: cdb2dr

Exclude PDBs: Type to find PDBs

PDB Clone

Secondary storage location : Snap Vault / Snap Mirror

Data

Source Volume: svm_onPrem:rhel2_u02

Destination Volume: svm_hybridcvo:rhel2_u02_dr

Logs

Source Volume: svm_onPrem:rhel2_u03

Destination Volume: svm_hybridcvo:rhel2_u03_dr

Previous Next

7. Aprovechone un volumen de registro y móntelo en el servidor DR de destino para el área de recuperación flash de Oracle y los registros en línea.

ONTAP System Manager

Search actions, objects, and pages

DASHBOARD

STORAGE

Overview

Applications

Volumes

LUNs

Shares

Qtrees

Quotas

Storage VMs

Tiers

NETWORK

EVENTS & JOBS

PROTECTION

HOSTS

Volumes

+ Add

More

	Name	Storage VM	Status	Capacity
✓	ora_standby_u01	svm_hybridcvo	Online	12.3 GB used 17.7 GB available 31.6 GB
✓	rhel2_u01_dr	svm_hybridcvo	Online	
✓	rhel2_u02_dr	svm_hybridcvo	Online	
✓	rhel2_u02_dr0917211608119360	svm_hybridcvo	Online	
✓	rhel2_u02_dr0917211703534863	svm_hybridcvo	Online	
✓	rhel2_u03_dr	svm_hybridcvo	Online	
✓	rhel2_u03_dr0917211824574775	svm_hybridcvo	Online	

Add Volume

NAME

ora_standby_u03

CAPACITY

20

GB

More Options

Cancel

Save

```

ec2-user@ora-standby/tmp
[ec2-user@ora-standby tmp]$ sudo mkdir /u03_cdb2dr
[ec2-user@ora-standby tmp]$ chown oracle:oinstall /u03_cdb2dr
chown: changing ownership of '/u03_cdb2dr': Operation not permitted
[ec2-user@ora-standby tmp]$ sudo chown oracle:oinstall /u03_cdb2dr
[ec2-user@ora-standby tmp]$ sudo mount -t nfs 10.221.1.6:/ora_standby_u03 /u03_cdb2dr
[ec2-user@ora-standby tmp]$ df -h
Filesystem              Size  Used Avail Use% Mounted on
devtmpfs                7.6G   0  7.6G   0% /dev
tmpfs                   7.6G   0  7.6G   0% /dev/shm
tmpfs                   7.6G  17M  7.6G   1% /run
tmpfs                   7.6G   0  7.6G   0% /sys/fs/cgroup
/dev/nvme0nlp2          10G   9.0G  1.1G  90% /
10.221.1.6:/ora_standby_u01 31G  13G  18G  42% /u01
tmpfs                   1.6G   0  1.6G   0% /run/user/1000
10.221.1.6:/Sc28182452-3fa8-448c-9e4a-c5a9e465f353 100G  3.1G  97G   4% /u02_cdb2dev
tmpfs                   1.6G   0  1.6G   0% /run/user/54321
10.221.1.6:/Sc39c05df8-4b00-4b3a-853c-9d6d338e5df7 100G  3.7G  97G   4% /u02_cdb2test
10.221.1.6:/Sccf886a5c-3273-479e-ad97-472b2a8dccee 100G  3.8G  97G   4% /var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_log_09-17-2021_18.20.04.1177_1/cdb2/1
10.221.1.6:/ora_standby_u03 21G  320K  20G   1% /u03_cdb2dr
[ec2-user@ora-standby tmp]$

```

El procedimiento de clonación de Oracle no crea un volumen de registro, que debe aprovisionarse en el servidor DR antes de la clonación.

- Seleccione el host de clonación de destino y la ubicación para colocar los archivos de datos, los archivos de control y los registros de rehacer.

112

Clone from cdb2

1

Name

2

Locations

3

Credentials

4

PreOps

5

PostOps

6

Notification

7

Summary

Select the host to create a clone

Clone host
ora-standby.demo.netapp.com

Datafile locations ⓘ

/u02_cdb2dr
Reset

Control files ⓘ

/u02_cdb2dr/cdb2dr/control/control01.ctl
/u03_cdb2dr/cdb2dr/control/control02.ctl
Reset

Redo logs ⓘ

Group	Size	Unit	Number of files
RedoGroup 1	200	MB	1
/u03_cdb2dr/cdb2dr/redolog/redo03.log			
RedoGroup 2	200	MB	1

Previous
Next

- Selecione las credenciales para el clon. Complete los detalles de la configuración de inicio de Oracle en el servidor de destino.

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Database Credentials for the clone

Credential name for sys user

None

+

i

Database port

1521

Oracle Home Settings

i

Oracle Home

/u01/app/oracle/product/19800/cdb2

Oracle OS User

oracle

Oracle OS Group

oinstall

Previous

Next

10. Especifique los scripts que se ejecutarán antes de la clonación. Los parámetros de la base de datos se pueden ajustar si es necesario.

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Specify scripts to run before clone operation

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Arguments

Script timeout

60

secs

Database Parameter settings

audit_file_dest	/u01/app/oracle/admin/cdb2dr/adump	X
audit_trail	DB	X
open_cursors	300	X
pga_aggregate_target	1432354816	X

+

Reset

Previous

Next

11. Seleccione Hasta cancelar como la opción de recuperación para que la recuperación se ejecute en todos los registros de archivo disponibles para recuperar la última transacción replicada en la ubicación de la nube secundaria.

Clone from cdb2

- 1 Name
- 2 Locations
- 3 Credentials
- 4 PreOps
- 5 PostOps**
- 6 Notification
- 7 Summary

☒ Recover Database ⓘ

- ☒ Until Cancel ⓘ
- ☐ Date and Time ⓘ
Date-time format: MM/DD/YYYY hh:mm:ss
- ☐ Until SCN (System Change Number) ⓘ

Specify external archive log locations ⓘ ⓘ ⓘ

```
/var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_log_09-17-2021_18.20.04.1177_1/cdb2/1/orareco/CDB2/archivelog/
```


☒ Create new DBID ⓘ

☒ Create tempfile for temporary tablespace ⓘ

Enter SQL queries to apply when clone is created ⓘ

Enter scripts to run after clone operation ⓘ

12. Configure el servidor SMTP para notificaciones por correo electrónico si es necesario.

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Provide email settings ⓘ

Email preference

Never

From

From email

To

Email to

Subject

Notification

☐ Attach job report

⚠

If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

✕

Previous

Next

13. Resumen del clon DR.

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Summary

Clone from backup

rhel2_cdb2_09-17-2021_14.35.01.4997_0

Clone SID

cdb2dr

Clone server

ora-standby.demo.netapp.com

Exclude PDBs

none

Oracle home

/u01/app/oracle/product/19800/cdb2

Oracle OS user

oracle

Oracle OS group

oinstall

Datafile mountpaths

/u02_cdb2dr

Control files

/u02_cdb2dr/cdb2dr/control/control01.ctl
/u03_cdb2dr/cdb2dr/control/control02.ctl

Redo groups

RedoGroup =1 TotalSize =200 Path =/u03_cdb2dr/cdb2dr/redolog/redo03.log
RedoGroup =2 TotalSize =200 Path =/u03_cdb2dr/cdb2dr/redolog/redo02.log
RedoGroup =3 TotalSize =200 Path =/u03_cdb2dr/cdb2dr/redolog/redo01.log

Recovery scope

Until Cancel

Prescript full path

none

Prescript arguments

Postscript full path

none

Postscript arguments

Previous

Finish

14. Las bases de datos clonadas se registran en SnapCenter inmediatamente después de completarse la clonación y luego están disponibles para protección de respaldo.

NetApp SnapCenter®								
Oracle Database View Database Search databases								
	Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status	
	cdb2	Single Instance (Multitenant)	rhel2.demo.netapp.com	rhel2_cdb2 rhel2_cdb2_log	Oracle Archive Log Backup Oracle Full Online Backup	09/17/2021 7:00:10 PM	Backup succeeded	
	cdb2dev	Single Instance (Multitenant)	ora-standby.demo.netapp.com				Not protected	
	cdb2dr	Single Instance (Multitenant)	ora-standby.demo.netapp.com				Not protected	
	cdb2test	Single Instance (Multitenant)	ora-standby.demo.netapp.com				Not protected	

Validación y configuración posterior a la clonación DR para Oracle

- Valide la última transacción de prueba que se ha vaciado, replicado y recuperado en la ubicación de recuperación ante desastres en la nube.

```
oracle@ora-standby:/u01/app/oracle/product/19800/cdb2/dbs
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> set lin 200
SQL> select instance_name, host_name from v$instance;

INSTANCE_NAME      HOST_NAME
-----
cdb2dr              ora-standby.demo.netapp.com

SQL> alter pluggable database cdb2_pdb1 open;

Pluggable database altered.

SQL> alter session set container=cdb2_pdb1;

Session altered.

SQL> select * from pdbadmin.dr_test;

      ID
-----
EVENT
-----
DT
-----
1
testing DB clone for DR and roll forward DB to last available log
17-SEP-21 02.12.13.000000 PM

SQL>
```

2. Configurar el área de recuperación flash.

```
oracle@ora-standby:/u01/app/oracle/product/19800/cdb2/dbs
[oracle@ora-standby: dbs]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Sep 17 22:07:11 2021
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> show parameter db_recovery_file_dest

NAME                                TYPE                                VALUE
-----                                -                                -
db_recovery_file_dest                string                             /u03_cdb2dr/cdb2dr
db_recovery_file_dest_size            big integer                         17208M
SQL> alter system set db_recovery_file_dest='/u03_cdb2dr/cdb2dr' scope=both;

System altered.

SQL> show parameter db_recovery_file_dest

NAME                                TYPE                                VALUE
-----                                -                                -
db_recovery_file_dest                string                             /u03_cdb2dr/cdb2dr
db_recovery_file_dest_size            big integer                         17208M
SQL>
```

- 3. Configure el escucha de Oracle para el acceso de usuarios.
- 4. Divida el volumen clonado del volumen de origen replicado.
- 5. Replicación inversa de la nube a las instalaciones locales y reconstrucción del servidor de base de datos local fallido.



La división de clones puede generar un uso de espacio de almacenamiento temporal mucho mayor que el funcionamiento normal. Sin embargo, una vez reconstruido el servidor de base de datos local, se puede liberar espacio adicional.

Clonar una base de datos de producción SQL local a la nube para recuperación ante desastres

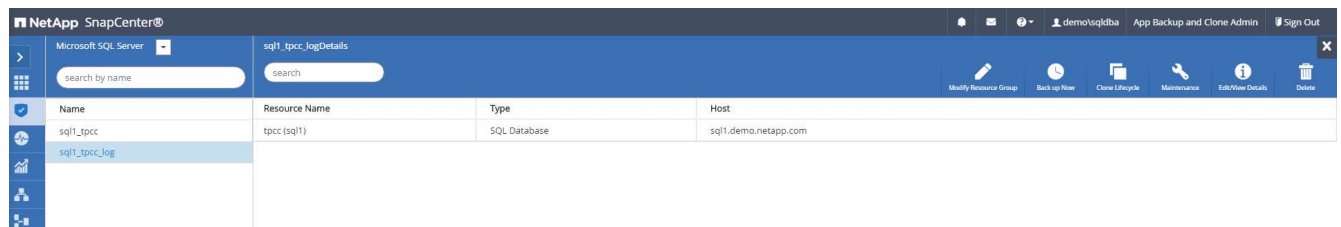
- 1. De manera similar, para validar que la recuperación del clon SQL se ejecutó a través del último registro disponible, creamos una pequeña tabla de prueba e insertamos una fila. Los datos de prueba se recuperarían después de una recuperación completa al último registro disponible.

```
Administrator Command Prompt - sqlcmd - SQLCMD
C:\Users\administrator.DEMO>sqlcmd
1> select host_name()
2> go

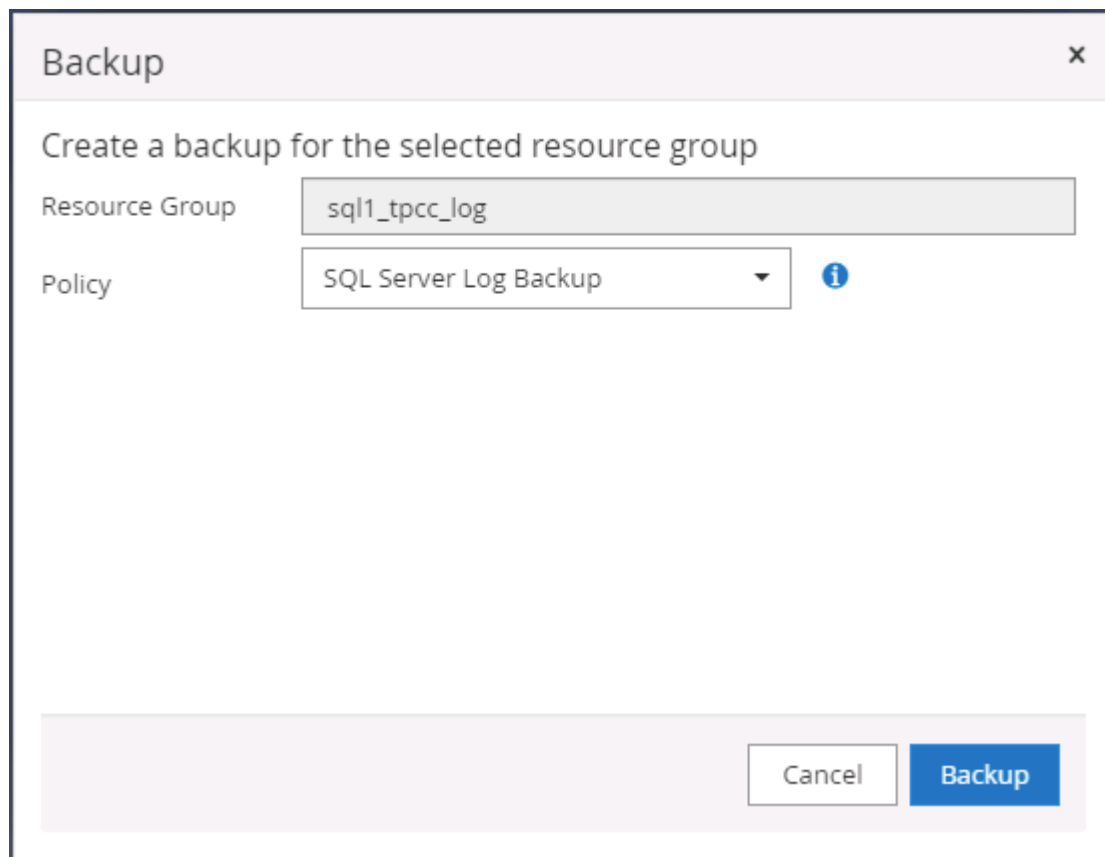
-----
SQL1
(1 rows affected)
1> use tpcc
2> go
Changed database context to 'tpcc'.
1> insert into snap_sync values ('test snap mirror DR for SQL', getdate())
2> go

(1 rows affected)
1> select * from snap_sync
2> go
event                                         dt
-----
test snap mirror DR for SQL                 2021-09-20 14:23:04.533
(1 rows affected)
1>
```

2. Inicie sesión en SnapCenter con un ID de usuario de administración de base de datos para SQL Server. Vaya a la pestaña Recursos, que muestra el grupo de recursos de protección de SQL Server.



3. Ejecute manualmente una copia de seguridad del registro para borrar la última transacción que se replicará en el almacenamiento secundario en la nube pública.



4. Seleccione la última copia de seguridad completa de SQL Server para el clon.

NetApp SnapCenter®

Microsoft SQL Server

tpcc (sql1) Topology

search by name

Clone Lifecycle Protect Details Refresh

Manage Copies

Local copies: 7 Backups, 0 Clones

Mirror copies: 7 Backups, 2 Clones

Summary Card

14 Backups

2 Clones

Secondary Mirror Backup(s)

search

Backup Name	Count	Type	if	End Date	Verified
sql1_tpcc_09-19-2021_18.25.01.4134	1	Full backup		09/19/2021 6:25:05 PM	Unverified
sql1_tpcc_09-18-2021_18.25.01.3963	1	Full backup		09/18/2021 6:25:05 PM	Unverified
sql1_tpcc_09-17-2021_18.25.01.4218	1	Full backup		09/17/2021 6:25:05 PM	Unverified

- Establezca la configuración de clonación, como el servidor de clonación, la instancia de clonación, el nombre de clonación y la opción de montaje. La ubicación de almacenamiento secundaria donde se realiza la clonación se completa automáticamente.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Clone settings

Clone server: sql-standby.demo.netapp.com

Clone instance: sql-standby

Clone name: tpcc_dr

Choose mount option

☒ Auto assign mount point

☐ Auto assign volume mount point under path: full file path

Secondary storage location : Snap Vault / Snap Mirror

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridcvo:sql1_data_dr
svm_onPrem:sql1_log	svm_hybridcvo:sql1_log_dr

Previous Next

- Seleccione todas las copias de seguridad de registros que se aplicarán.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Choose logs

☒ All log backups

☐ By log backups until

9/19/2021 6:25:10 PM

☐ By specific date until

09/19/2021 6:25:05 PM

☐ None

Previous

Next

7. Especifique cualquier script opcional para ejecutar antes o después de la clonación.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Specify optional scripts to run before and after performing a clone from backup job

Prescript full path

Prescript arguments

Choose optional arguments...

Postscript full path

Postscript arguments

Choose optional arguments...

Script timeout

60

secs

Previous

Next

8. Especifique un servidor SMTP si desea recibir notificaciones por correo electrónico.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Provide email settings ⓘ

Email preference

Never

From

From email

To

Email to

Subject

Notification

☐ Attach Job Report

⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

×

Previous

Next

9. Resumen del clon DR. Las bases de datos clonadas se registran inmediatamente en SnapCenter y están disponibles para protección de respaldo.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Summary

Clone server

sql-standby.demo.netapp.com

Clone instance

sql-standby

Clone name

tpcc_dr

Mount option

Auto Mount

Prescript full path

None

Prescript arguments

Postscript full path

None

Postscript arguments

Send email

No

Previous

Finish

NetApp SnapCenter®							
Microsoft SQL Server							
View Database search by name							
Resources	Name	Instance	Host	Last Backup	Overall Status	Type	
Monitor	master	sql1	sql1.demo.netapp.com		Not available for backup	System database	
Reports	model	sql1	sql1.demo.netapp.com		Not available for backup	System database	
Hosts	msdb	sql1	sql1.demo.netapp.com		Not available for backup	System database	
Storage Systems	tempdb	sql1	sql1.demo.netapp.com		Not available for backup	System database	
Settings	tpcc	sql1	sql1.demo.netapp.com	09/22/2021 5:35:08 PM	Backup failed, Schedules on hold	User database	
Alerts	master	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database	
	model	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database	
	msdb	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database	
	tempdb	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database	
	tpcc_clone	sql-standby	sql-standby.demo.netapp.com		Not protected	User database	
	tpcc_dev	sql-standby	sql-standby.demo.netapp.com		Not protected	User database	
	tpcc_dr	sql-standby	sql-standby.demo.netapp.com		Not protected	User database	

Validación y configuración posterior a la clonación DR para SQL

- Supervisar el estado del trabajo de clonación.

NetApp SnapCenter®							
Jobs Schedules Events Logs							
search by name							
Resources	Jobs - Filter						
Monitor	ID	Status	Name	Start date	End date	Owner	
Reports	1052	✓	Clone from backup 'sql1_tpcc_09-19-2021_18.25.01.4134'	09/20/2021 2:36:17 PM	09/20/2021 2:37:06 PM	demo/sqlqdba	
Hosts	1047	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 2:35:01 PM	09/20/2021 2:37:08 PM	demo/sqlqdba	
Storage Systems	1045	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 2:28:17 PM	09/20/2021 2:30:25 PM	demo/sqlqdba	
Settings	1044	✓	Clone from backup 'sql1_tpcc_09-17-2021_18.25.01.4218'	09/20/2021 1:39:24 PM	09/20/2021 1:40:09 PM	demo/sqlqdba	
	1042	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 1:35:01 PM	09/20/2021 1:37:08 PM	demo/sqlqdba	
	1040	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 12:35:01 PM	09/20/2021 12:37:08 PM	demo/sqlqdba	

- Validar que la última transacción se haya replicado y recuperado con todos los clones y la recuperación de

archivos de registro.

```
Administrator: Command Prompt - sqlcmd - SQLCMD
C:\Users\administrator.DEMO>sqlcmd
1> select host_name()
2> go
-----
SQL-STANDBY
(1 rows affected)
1> use tpcc_dr
2> go
Changed database context to 'tpcc_dr'.
1> select * from snap_sync
2> go
event                                     dt
-----
test snap mirror DR for SQL              2021-09-20 14:23:04.533
(1 rows affected)
1> select getdate()
2> go
-----
2021-09-20 14:39:19.937
(1 rows affected)
1> _
```

3. Configure un nuevo directorio de registro de SnapCenter en el servidor DR para la copia de seguridad del registro de SQL Server.
4. Divida el volumen clonado del volumen de origen replicado.
5. Replicación inversa de la nube a las instalaciones locales y reconstrucción del servidor de base de datos local fallido.

¿A dónde acudir para obtener ayuda?

Si necesita ayuda con esta solución y casos de uso, únase a la ["Canal de Slack de soporte de la comunidad de automatización de soluciones de NetApp"](#) y busca el canal de automatización de soluciones para publicar tus dudas o consultas.

Información de copyright

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

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

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

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

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

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

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

Información de la marca comercial

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