Soluciones de bases de datos de cloud híbrido con SnapCenter

NetApp Solutions

NetApp
April 23, 2024

This PDF was generated from https://docs.netapp.com/es-es/netapp-solutions/databases/hybrid_dbops_snapcenter_usecases.html on April 23, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Soluciones de bases de datos de cloud híbrido con SnapCenter

TR-4908: Soluciones de bases de datos para el cloud híbrido con información general de SnapCenter

Alan Cao, Felix Melligan, NetApp

Esta solución proporciona a NetApp y a los clientes instrucciones y directrices para configurar, operar y migrar bases de datos a un entorno de cloud híbrido mediante la herramienta basada en la interfaz gráfica de usuario de SnapCenter de NetApp y el servicio de almacenamiento de NetApp CVO en clouds públicos para los siguientes casos de uso:

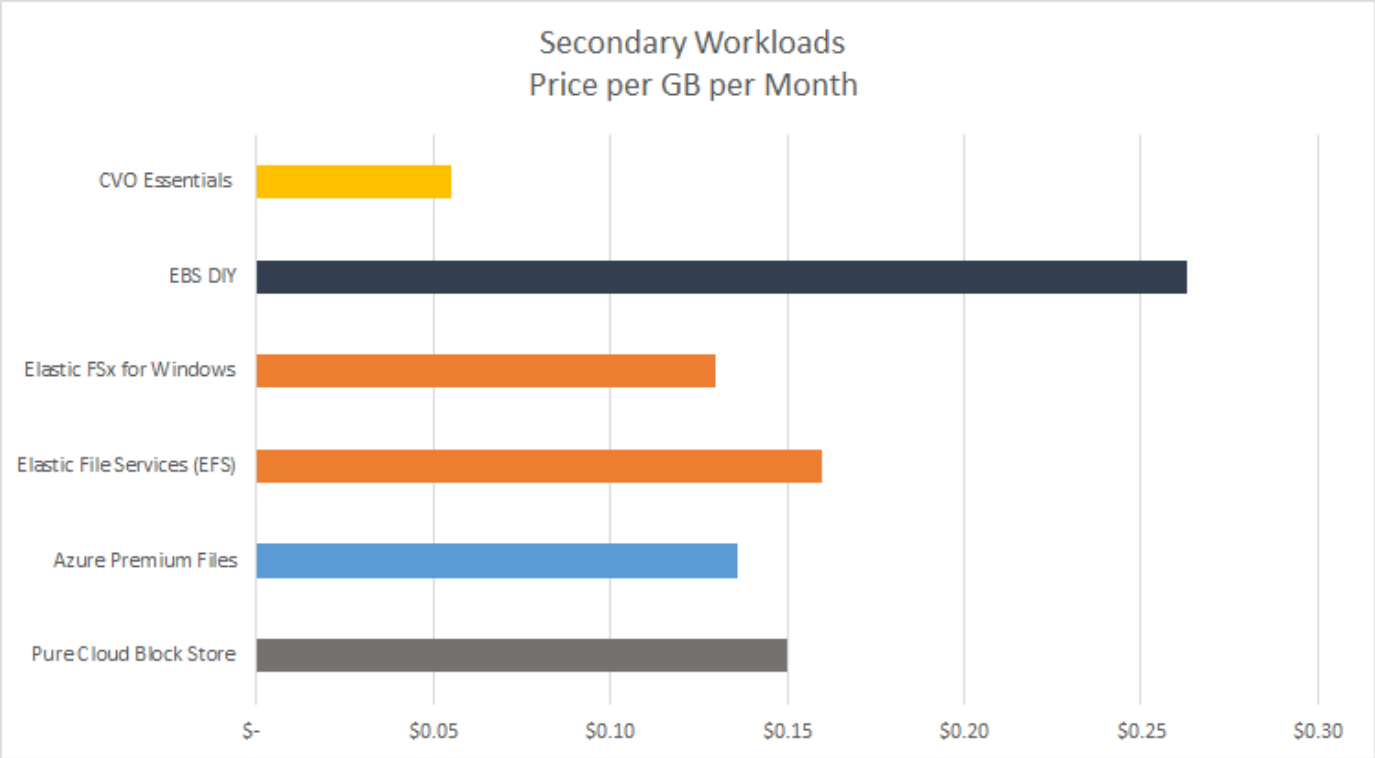
- Las operaciones de desarrollo y pruebas de bases de datos en el cloud híbrido
- Recuperación ante desastres de bases de datos en el cloud híbrido

En la actualidad, muchas bases de datos empresariales siguen residiendo en centros de datos corporativos privados por motivos de rendimiento, seguridad u otros motivos. Esta solución de bases de datos de cloud híbrido permite a las empresas operar sus bases de datos principales in situ mientras utilizan un cloud público para operaciones de bases de datos de desarrollo y pruebas, así como para recuperación ante desastres, con el fin de reducir los costes operativos y de licencias.

Muchas bases de datos empresariales, como Oracle, SQL Server, SAP HANA, etc., lleve consigo elevados costes operativos y de licencias. Muchos clientes pagan una licencia única y los costes de soporte anuales en función del número de núcleos informáticos de su entorno de bases de datos, independientemente de si se utilizan núcleos para desarrollo, pruebas, producción o recuperación ante desastres. Es posible que muchos de estos entornos no se utilicen por completo a lo largo de todo el ciclo de vida de las aplicaciones.

Las soluciones proporcionan a los clientes una opción para reducir potencialmente el número de núcleos con licencia mediante el movimiento de sus entornos de base de datos dedicados al desarrollo, la prueba o la recuperación ante desastres al cloud. Al usar el escalado de cloud público, la redundancia, la alta disponibilidad y un modelo de facturación basado en el consumo, el ahorro en costes de licencias y operaciones puede ser sustancial sin sacrificar la facilidad de uso o la disponibilidad de las aplicaciones.

Más allá del posible ahorro en costes de licencias de bases de datos, el modelo de licencias de CVO basado en capacidad de NetApp permite a los clientes ahorrar costes de almacenamiento por GB al tiempo que les permite disfrutar de un alto nivel de capacidad de gestión de bases de datos que no se encuentra disponible con los servicios de almacenamiento de la competencia. El siguiente gráfico muestra una comparación de costes del almacenamiento de los servicios de almacenamiento populares disponibles en el cloud público.



Esta solución demuestra que, al utilizar la herramienta de software basada en interfaz gráfica de usuario de SnapCenter y la tecnología SnapMirror de NetApp, las operaciones de bases de datos del cloud híbrido se pueden configurar, implementar y utilizar fácilmente.

Los siguientes vídeos demostrarán que SnapCenter está en acción:

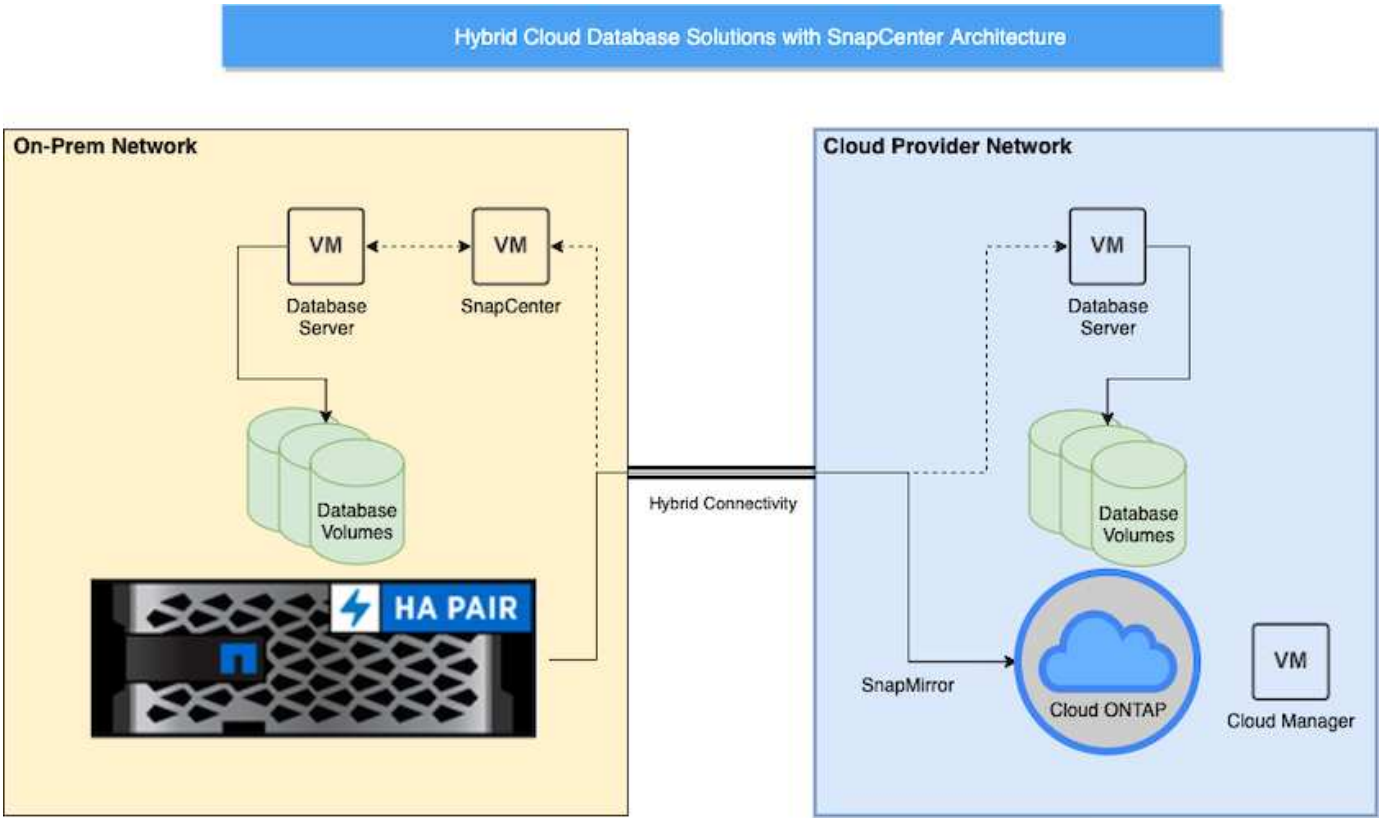
- "Backup de una base de datos de Oracle en un cloud híbrido con SnapCenter"
- "SnapCenter: Clone EL PROCESO DE DESARROLLO y PRUEBAS en AWS Cloud para una base de datos de Oracle"

En particular, aunque las ilustraciones de este documento muestran CVO como una instancia de almacenamiento objetivo en el cloud público, la solución también está completamente validada para la nueva versión del motor de almacenamiento de ONTAP FSX para AWS.

Para probar usted mismo la solución y los casos de uso, puede solicitarse un laboratorio de NetApp bajo demanda SL10680 en el siguiente enlace: TL_AWS_004 HCoD: AWS - NW,SnapCenter(OnPrem).

Arquitectura de la solución

En el siguiente diagrama de arquitectura se ilustra una implementación típica de operaciones de bases de datos empresariales en un cloud híbrido para operaciones de recuperación ante desastres y desarrollo y pruebas.



En operaciones empresariales normales, los volúmenes de bases de datos sincronizados en el cloud se pueden clonar y montar en instancias de base de datos de desarrollo y pruebas para desarrollar o probar aplicaciones. En caso de que se produzca un fallo, los volúmenes de la base de datos sincronizados en el cloud pueden activarse para realizar la recuperación ante desastres.

Requisitos de SnapCenter

Esta solución está diseñada en un entorno de cloud híbrido para admitir bases de datos de producción en las instalaciones que pueden usar en ráfagas en todos los clouds públicos populares para operaciones de desarrollo, pruebas y recuperación ante desastres.

Esta solución admite todas las bases de datos compatibles actualmente con SnapCenter, aunque solo se muestran aquí las bases de datos de Oracle y SQL Server. Esta solución se valida con cargas de trabajo de bases de datos virtualizadas, aunque también son compatibles las cargas de trabajo con configuración básica.

Asumimos que los servidores de bases de datos de producción se alojan en las instalaciones con volúmenes de bases de datos presentados a los hosts de bases de datos de un clúster de almacenamiento de ONTAP. El software SnapCenter se instala en las instalaciones para realizar tareas de backup de bases de datos y replicación de datos en el cloud. Se recomienda utilizar una controladora de Ansible, pero no es necesario para la automatización de la puesta en marcha de la base de datos o para la sincronización de la configuración del kernel de sistema operativo y la base de datos con una instancia de recuperación ante desastres en espera o instancias de desarrollo y pruebas en el cloud público.

Requisitos

Entorno Oracle	Requisitos
En el local	Cualquier base de datos y versiones que SnapCenter admita
	SnapCenter v4.4 o superior
	Ansible v2.09 o superior
	Clúster de ONTAP 9.x.
	LIF de interconexión de clústeres configuradas
	Conectividad desde las instalaciones a un VPC de cloud (VPN, interconexión, etc.)
	Puertos de red abiertos - ssh 22 - tcp 8145, 8146, 10000, 11104, 11105
Cloud: AWS	"Conector de Cloud Manager"
	"Cloud Volumes ONTAP"
	Coincidencia de instancias de EC2 del sistema operativo de la base de datos con las instalaciones
Cloud - Azure	"Conector de Cloud Manager"
	"Cloud Volumes ONTAP"
	Comparación de máquinas virtuales de Azure con sistema operativo de base de datos a las instalaciones
Cloud - GCP	"Conector de Cloud Manager"
	"Cloud Volumes ONTAP"
	Emparejamiento de instancias de Google Compute Engine del sistema operativo de base de datos a las instalaciones

Configuración de requisitos previos

Ciertos requisitos previos deben configurarse tanto en las instalaciones como en el cloud antes de ejecutar las cargas de trabajo de las bases de datos del cloud híbrido. En la siguiente sección se proporciona un resumen de alto nivel de este proceso, y los siguientes enlaces proporcionan información adicional sobre la configuración necesaria del sistema.

En el entorno local

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

Cloud público

- Un inicio de sesión en Cloud Central de NetApp
- Acceso a la red desde un explorador Web hasta varios puntos finales
- Una ubicación de red para un conector
- Permisos del proveedor de cloud
- Creación de redes para servicios individuales

Consideraciones importantes:

1. ¿Dónde se debe poner en marcha Cloud Manager Connector?
2. Ajuste de tamaño y arquitectura de Cloud Volume ONTAP
3. ¿Nodo único o alta disponibilidad?

Los siguientes enlaces proporcionan más información:

"En el entorno local"

"Cloud público"

Requisitos previos en las instalaciones

Las siguientes tareas deben completarse en las instalaciones para preparar el entorno de cargas de trabajo de bases de datos del cloud híbrido de SnapCenter.

Instalación y configuración de SnapCenter

La herramienta SnapCenter de NetApp es una aplicación basada en Windows que se ejecuta normalmente en un entorno de dominio de Windows, aunque también es posible instalar un grupo de trabajo. Se basa en una arquitectura de varios niveles que incluye un servidor de gestión centralizado (el servidor SnapCenter) y un complemento de SnapCenter en los hosts de servidores de bases de datos para cargas de trabajo de bases de datos. Estas son algunas consideraciones clave para la puesta en marcha del cloud híbrido.

- **Implementación de una sola instancia o de alta disponibilidad.** la implementación de alta disponibilidad ofrece redundancia en caso de un fallo del servidor de instancia de SnapCenter.
- **Resolución de nombres.** se debe configurar DNS en el servidor SnapCenter para resolver todos los hosts de base de datos, así como en la SVM de almacenamiento para la búsqueda directa e inversa. El DNS también debe configurarse en los servidores de bases de datos para resolver el servidor SnapCenter y la SVM de almacenamiento para la búsqueda directa e inversa.
- **Configuración de control de acceso basado en funciones (RBAC).** para cargas de trabajo mixtas de bases de datos, es posible que desee utilizar RBAC para separar la responsabilidad de la administración de una plataforma de base de datos diferente, como un administrador para bases de datos Oracle o un administrador para SQL Server. Se deben conceder los permisos necesarios para el usuario administrador de la base de datos.
- **Active la estrategia de copia de seguridad basada en directivas.** para aplicar la consistencia y fiabilidad de las copias de seguridad.
- **Abra los puertos de red necesarios en el firewall.** para que el servidor SnapCenter en las instalaciones se comunique con los agentes instalados en el host de la base de datos en la nube.
- **Los puertos deben estar abiertos para permitir el tráfico SnapMirror entre el cloud público y en las**

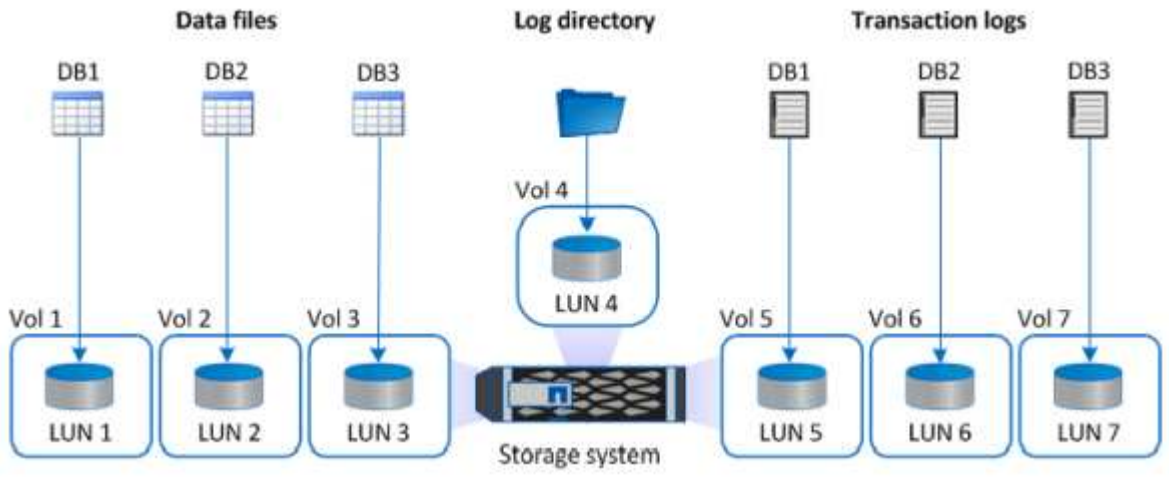
instalaciones. El servidor SnapCenter confía en SnapMirror de ONTAP para replicar los backups de Snapshot in situ en las SVM de almacenamiento CVO en el cloud.

Tras una planificación y consideración cuidadosas previas a la instalación, haga clic en esto "Flujo de trabajo de instalación de SnapCenter" Para obtener más información acerca de la instalación y configuración de SnapCenter.

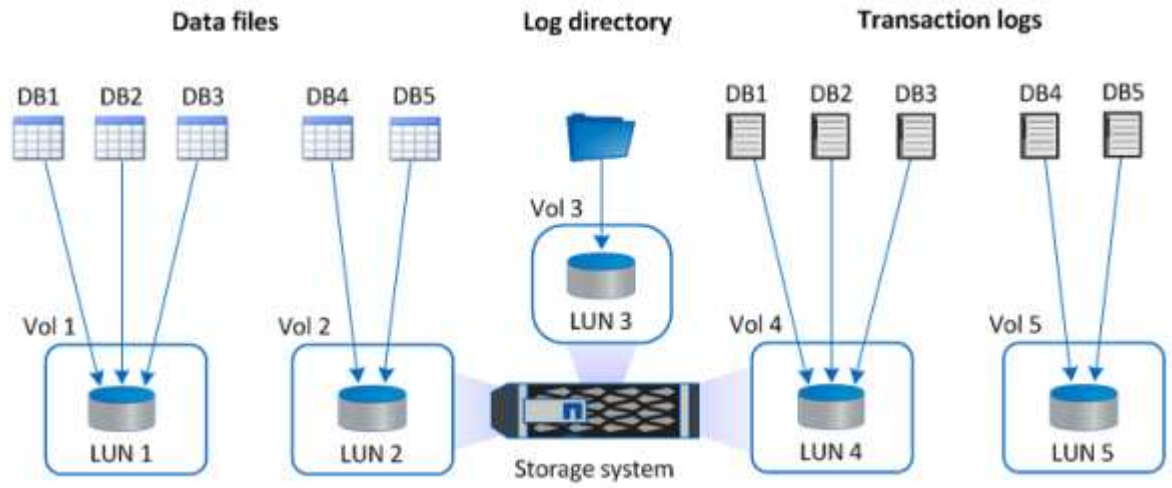
Configuración del almacenamiento del servidor de bases de datos local

El rendimiento del almacenamiento desempeña un papel importante en el rendimiento general de las bases de datos y las aplicaciones. Un sistema de almacenamiento bien diseñado no solo puede mejorar el rendimiento de las bases de datos, sino que también facilita la gestión de los procesos de backup y recuperación de bases de datos. Se deben tener en cuenta varios factores al definir la distribución de almacenamiento, como el tamaño de la base de datos, la tasa de cambio esperado de los datos y la frecuencia con la que se realizan backups.

La conexión directa de LUN de almacenamiento al equipo virtual «guest» mediante NFS o iSCSI para cargas de trabajo de bases de datos virtualizadas suele proporcionar un mejor rendimiento que el almacenamiento asignado a través de VMDK. NetApp recomienda el diseño del almacenamiento para una base de datos de SQL Server grande en las LUN descritas en la siguiente figura.



La siguiente figura muestra la distribución de almacenamiento recomendada por NetApp para bases de datos de SQL Server pequeñas o medianas en LUN.

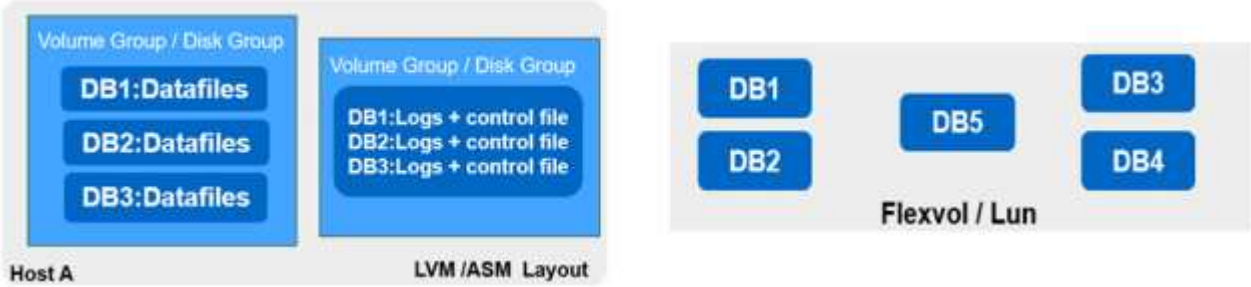


El directorio de registro se dedica a SnapCenter para realizar un paquete acumulativo de registros de transacciones para la recuperación de la base de datos. Para una base de datos extra grande, se pueden asignar varios LUN a un volumen para mejorar el rendimiento.

Para cargas de trabajo de bases de datos de Oracle, SnapCenter admite entornos de base de datos respaldados por almacenamiento ONTAP que están montados en el host como dispositivos físicos o virtuales. Puede alojar toda la base de datos en un único dispositivo de almacenamiento o en varios en función de la importancia del entorno. Normalmente, los clientes aíslan los archivos de datos del almacenamiento dedicado de todos los demás archivos, como los archivos de control, los archivos de recuperación y los archivos de registro de archivos. De este modo, los administradores pueden restaurar rápidamente (SnapRestore de un solo archivo de ONTAP) o clonar una base de datos crítica de gran tamaño (a escala de petabytes) mediante la tecnología Snapshot en unos pocos segundos o minutos.

En el caso de cargas de trabajo críticas que sean sensibles a la latencia, se debe poner en marcha un volumen de almacenamiento dedicado en 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.

En el caso de bases de datos de 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 una LUN. Como ejemplo de este diseño, es posible alojar archivos de datos de todas las bases de datos en un grupo de discos +DATA ASM o un grupo de volúmenes. El resto de los archivos (archivos de recuperación, registro de archivo y de control) se puede alojar en otro grupo de discos o grupo de volúmenes dedicado (LVM). A continuación se ilustra un escenario de despliegue de este tipo.



Para facilitar la reubicación de las bases de datos de Oracle, el binario de Oracle debe instalarse en un LUN independiente que se incluya en la política de backup normal. Esto garantiza que, en caso de reubicación de la base de datos a un nuevo host de servidor, la pila de Oracle se pueda iniciar para la recuperación sin

ningún problema potencial debido a un binario de Oracle que no está sincronizado.

Requisitos de licencia

SnapCenter es un software con licencia de NetApp. Por lo general se incluye en una licencia ONTAP en las instalaciones. Sin embargo, para la puesta en marcha de cloud híbrido, también es necesaria una licencia de cloud para SnapCenter para añadir CVO a SnapCenter como destino de replicación de datos objetivo. Consulte los siguientes enlaces de las licencias estándar basadas en capacidad de SnapCenter para obtener más información:

"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 en las instalaciones que sea estable al cloud para desarrollo y pruebas y recuperación ante desastres, es importante tener en cuenta la relación con redes y seguridad cuando se configura el entorno y se conecta al cloud público desde un centro de datos en las instalaciones.

Los clouds públicos normalmente utilizan un cloud privado virtual (VPC) para aislar a diferentes usuarios dentro de una plataforma de cloud público. Dentro de un VPC individual, la seguridad se controla mediante medidas como los grupos de seguridad que se pueden configurar de acuerdo con las necesidades del usuario para el bloqueo de un VPC.

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

Para conocer las consideraciones de redes y seguridad, revise las reglas de CVO entrantes y salientes pertinentes para el cloud público que elija:

- "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 bases de datos entre las instalaciones y el cloud, opcional

Para simplificar la gestión de un entorno de bases de datos de cloud híbrido, NetApp recomienda encarecidamente, pero no requiere que ponga en marcha una controladora Ansible para automatizar algunas tareas de gestión, como mantener las instancias informáticas locales y en el cloud sincronizadas. Esto es especialmente importante porque una instancia de computación fuera de sincronización en el cloud puede hacer que la base de datos recuperada en el cloud sea propensa a errores debido a que faltan paquetes del kernel y otros problemas.

También se puede usar la funcionalidad de automatización de una controladora de Ansible para aumentar el número de SnapCenter a fin de realizar ciertas tareas, como dividir la instancia de SnapMirror para activar la copia de datos de recuperación ante desastres para producción.

Siga estas instrucciones para configurar el nodo de control de Ansible para máquinas RedHat o CentOS: "Configuración de la controladora Red Hat/CentOS Ansible". Siga estas instrucciones para configurar el nodo de control de Ansible para máquinas Ubuntu o Debian: "Configuración de la controladora Ubuntu/Debian Ansible".

Requisitos previos para el cloud público

Antes de instalar el conector de Cloud Manager y Cloud Volumes ONTAP y configurar SnapMirror, debemos preparar algo para nuestro entorno de cloud. Esta página describe el trabajo que se debe realizar así como las consideraciones que se deben tener en cuenta al implementar Cloud Volumes ONTAP.

Lista de comprobación de requisitos previos de puesta en marcha de Cloud Manager y Cloud Volumes ONTAP

- Un inicio de sesión en Cloud Central de NetApp
- Acceso a la red desde un explorador Web hasta varios puntos finales
- Una ubicación de red para un conector
- Permisos del proveedor de cloud
- Creación de redes para servicios individuales

Para obtener más información sobre lo que necesita para empezar, visite nuestra "documentación sobre cloud".

Consideraciones

1. ¿Qué es un conector de Cloud Manager?

En la mayoría de los casos, un administrador de cuenta de Cloud Central debe poner en marcha un conector en la red local o en el cloud. El conector permite a Cloud Manager gestionar recursos y procesos dentro de su entorno de cloud público.

Para obtener más información sobre conectores, visite nuestra "documentación sobre cloud".

2. Ajuste de tamaño y arquitectura de Cloud Volumes ONTAP

Al implementar Cloud Volumes ONTAP, se ofrece la opción de un paquete predefinido o de la creación de su propia configuración. A pesar de que muchos de estos valores se pueden cambiar más adelante de forma no disruptiva, existen algunas decisiones clave que deben tomarse antes de la puesta en marcha en función de las cargas de trabajo que se van a poner en marcha en el cloud.

Cada proveedor de cloud tiene diferentes opciones de puesta en marcha y casi todas las cargas de trabajo tienen sus propias propiedades únicas. NetApp tiene una "Herramienta de ajuste de tamaño CVO" esto puede ayudar a dimensionar correctamente las puestas en marcha en función de la capacidad y el rendimiento, pero se ha desarrollado a partir de algunos conceptos básicos que vale la pena considerar:

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

La clave está en planificar una configuración que satisfaga no solo los requisitos de capacidad y rendimiento actuales, sino que también tenga en cuenta el crecimiento futuro. Esto suele denominarse margen adicional de capacidad y margen adicional de rendimiento.

Si desea obtener más información, lea la documentación acerca de la planificación correcta para "AWS", "Azure", y. "GCP".

3. ¿Nodo único o alta disponibilidad?

En todos los clouds, existe la opción de poner en marcha CVO tanto en un único nodo como en un par de alta disponibilidad en clúster con dos nodos. En función del caso de uso, puede que desee poner en marcha un solo nodo para ahorrar costes o un par de alta disponibilidad para proporcionar mayor disponibilidad y redundancia.

En un caso de uso de recuperación ante desastres o durante el aumento del almacenamiento temporal para las fases de desarrollo y pruebas, los nodos individuales son habituales, ya que el impacto de una interrupción repentina del servicio de la infraestructura es menor. Sin embargo, en cualquier caso de uso de producción, si los datos solo se encuentran en una única ubicación o si el conjunto de datos debe tener más redundancia y disponibilidad, se recomienda una alta disponibilidad.

Para obtener más información sobre la arquitectura de la alta disponibilidad de cada versión cloud, visite la documentación de "AWS", "Azure" y.. "GCP".

Información general del inicio

En esta sección se proporciona un resumen de las tareas que deben completarse para cumplir los requisitos previos, tal como se describen en la sección anterior. En la siguiente sección, se proporciona una lista de tareas de alto nivel para las operaciones de cloud público y en las instalaciones. Se puede acceder a los procesos y procedimientos detallados haciendo clic en los enlaces correspondientes.

Localmente

- Configure el usuario administrador de la base de datos en SnapCenter
- Requisitos previos de instalación del plugin de SnapCenter
- Instalación del complemento de host de SnapCenter
- Descubrimiento de recursos DE BASE de datos
- Configurar la conexión entre iguales de clústeres de almacenamiento y la replicación de volúmenes de base de datos
- Añada la SVM de almacenamiento de base de datos de CVO a SnapCenter
- Configure la política de backup de la base de datos en SnapCenter
- Implemente una política de backup para proteger la base de datos
- Validar el backup

Cloud público de AWS

- Comprobación previa al vuelo
- Pasos para implementar Cloud Manager y Cloud Volumes ONTAP en AWS
- Ponga en marcha la instancia de EC2 para cargas de trabajo de bases de datos

Haga clic en los siguientes enlaces para obtener información detallada:

"En el entorno local", "Cloud público: AWS"

Introducción a las instalaciones

La herramienta NetApp SnapCenter utiliza el control de acceso basado en roles (RBAC) para gestionar el acceso a recursos de usuario y las concesiones de permisos, y la instalación de SnapCenter crea roles predefinidos. También puede crear funciones personalizadas según sus necesidades o aplicaciones.

En el entorno local

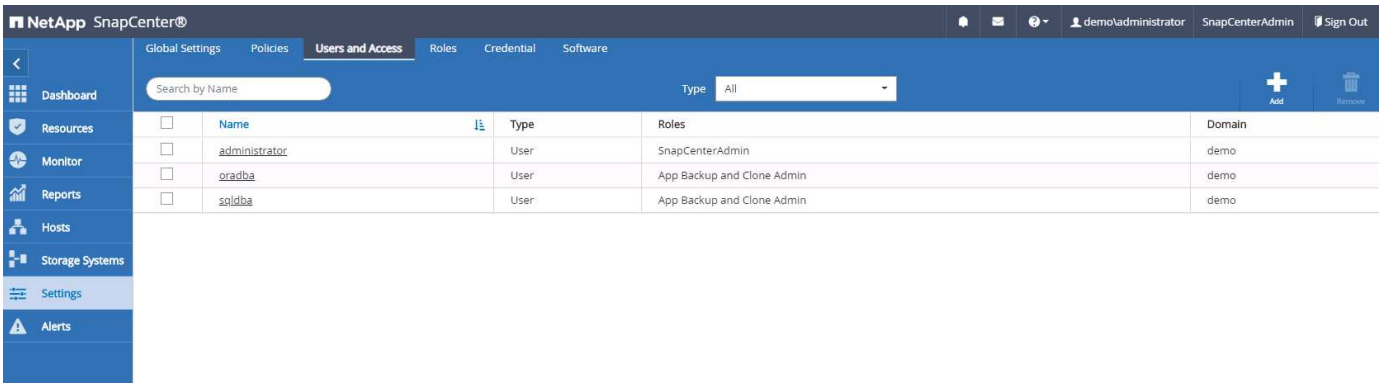
1. Configurar el usuario administrador de la base de datos en SnapCenter

Tiene sentido tener un ID de usuario administrador dedicado para cada plataforma de base de datos compatible con SnapCenter para backup, restauración y/o recuperación ante desastres de bases de datos. También es posible usar un ID único para gestionar todas las bases de datos. En nuestros casos de prueba y demostración, creamos un usuario de administrador dedicado para Oracle y SQL Server, respectivamente.

Ciertos recursos de SnapCenter solo pueden aprovisionarse con el rol de administrador de SnapCenter. Los recursos se pueden asignar a otros ID de usuario para tener acceso.

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

1. Agregue el usuario admin a Windows Active Directory.
2. Inicie sesión en SnapCenter con un ID que cuenta con el rol de administrador de SnapCenter.
3. Vaya a la ficha Access 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. Asigne recursos al usuario administrador según corresponda.



2. Requisitos previos de instalación del complemento SnapCenter

SnapCenter realiza funciones de backup, restauración, clonado y otras mediante un agente de complementos 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 mediante credenciales configuradas en la pestaña Setting and Credentials para la instalación del plugin 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 plugin de SnapCenter. Generalmente, desea utilizar cuentas de usuario de administrador en el host de la base de datos como credenciales de conexión de host para la instalación del plugin. 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 utilizar la autenticación de la base de datos con distintos ID de usuario de la base de datos para el acceso a la administración de la base de datos. Si decide utilizar la autenticación basada en el sistema operativo, debe concederse acceso a la base de datos al ID de usuario administrador del sistema operativo. Para la instalación de SQL Server basada en dominios de Windows, se puede utilizar una cuenta de administrador de dominio para administrar todos los servidores SQL Server dentro del dominio.

Host Windows para SQL Server:

1. Si utiliza credenciales de Windows para la autenticación, debe configurar la credencial para poder instalar plugins.
2. Si utiliza una instancia de SQL Server para la autenticación, debe añadir las credenciales después de instalar plugins.
3. Si habilitó la autenticación por SQL durante la configuración de las credenciales, la instancia o la base de datos detectadas se mostrarán con un icono de candado rojo. Si se muestra el icono de candado, es necesario especificar las credenciales de la instancia o la base de datos para añadir correctamente la instancia o la base de datos al grupo de recursos.
4. Debe asignar la credencial a un usuario de 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 el host de SQL se asignan a un usuario de RBAC.
    - El usuario administrador de la base de datos de RBAC debe tener privilegios de backup y grupo de recursos.

Host UNIX para Oracle:

1. Debe haber habilitado la conexión SSH basada en contraseña para el usuario raíz o no raíz 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 sudo para el usuario que no sea raíz para instalar e iniciar el proceso del plugin. Después de instalar el plugin, 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 el host Linux.
5. La instalación del complemento Oracle Database también instala el complemento SnapCenter para Unix.

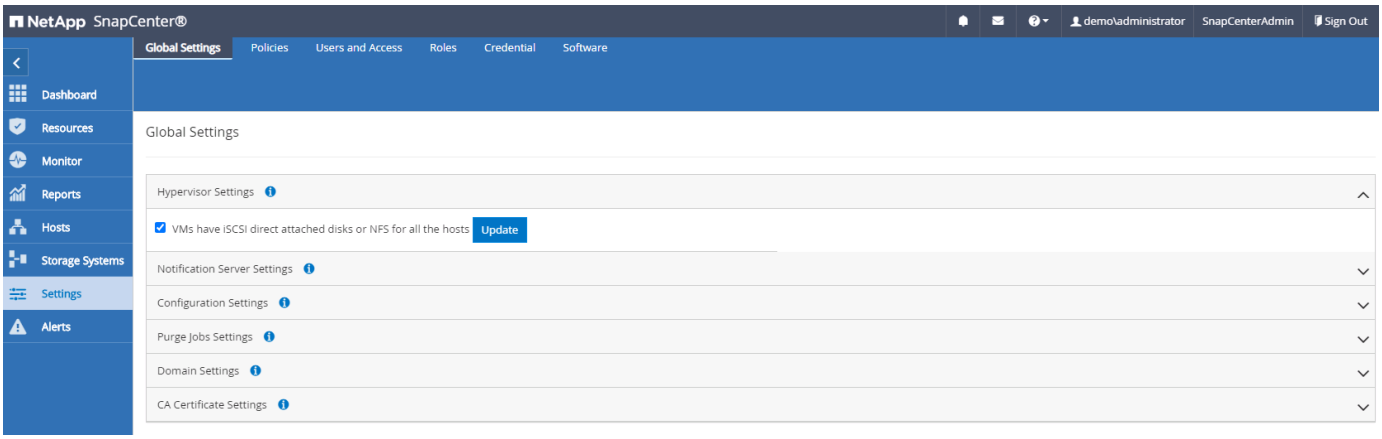
3. Instalación del complemento de host de SnapCenter

> Antes de intentar instalar los plugins de SnapCenter en instancias de servidor de la base de datos en la nube, asegúrese de que todos los pasos de configuración se han completado como se indica en la sección pertinente de la nube para la implementación de la instancia de computación.

Los siguientes pasos ilustran cómo se añade un host de base de datos a SnapCenter mientras se instala un plugin de SnapCenter en el host. El procedimiento aplica a añadir hosts en las instalaciones y hosts de cloud. La siguiente demostración añade un host de Windows o Linux que reside en AWS.

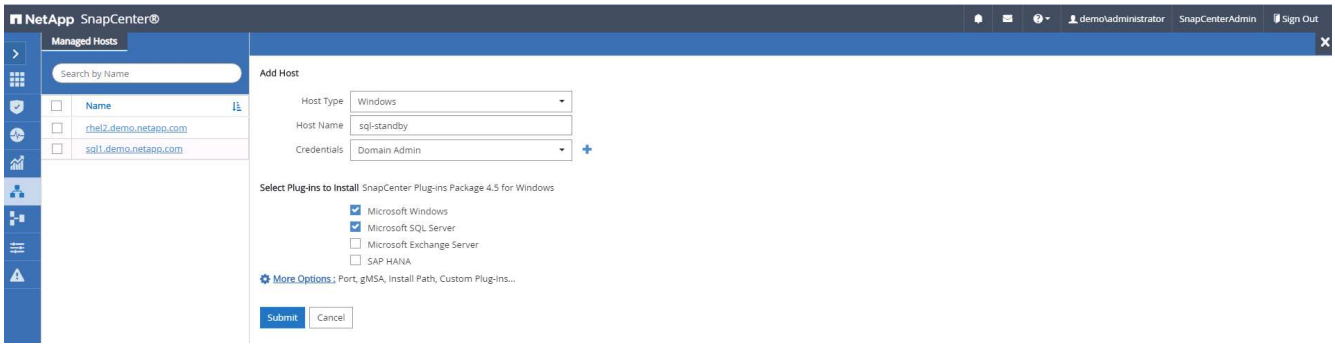
Configuración de los ajustes globales de VMware de SnapCenter

Vaya a Configuración > Configuración global. Seleccione "VMs have iSCSI direct attached disks or NFS for all the hosts" en Hypervisor Settings y haga clic en Update.



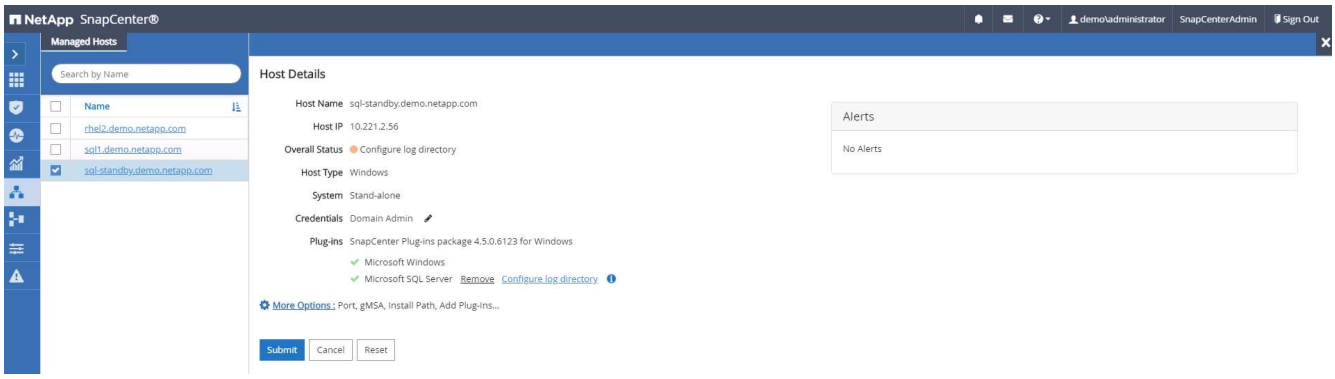
Añada el host de Windows y la instalación del plugin en el host

1. Inicie sesión en SnapCenter con un ID de usuario con privilegios de administrador de SnapCenter.
2. Haga clic en la ficha hosts del menú de la izquierda y, a continuación, haga clic en Agregar para abrir el flujo de trabajo Agregar host.
3. Elija Windows para Tipo de host; el nombre de host puede ser un nombre de host o una dirección IP. El nombre de host debe solucionarse con la dirección IP de host correcta desde el host SnapCenter. Seleccione las credenciales de host creadas en el paso 2. Elija Microsoft Windows y Microsoft SQL Server como los paquetes de complementos que se van a instalar.

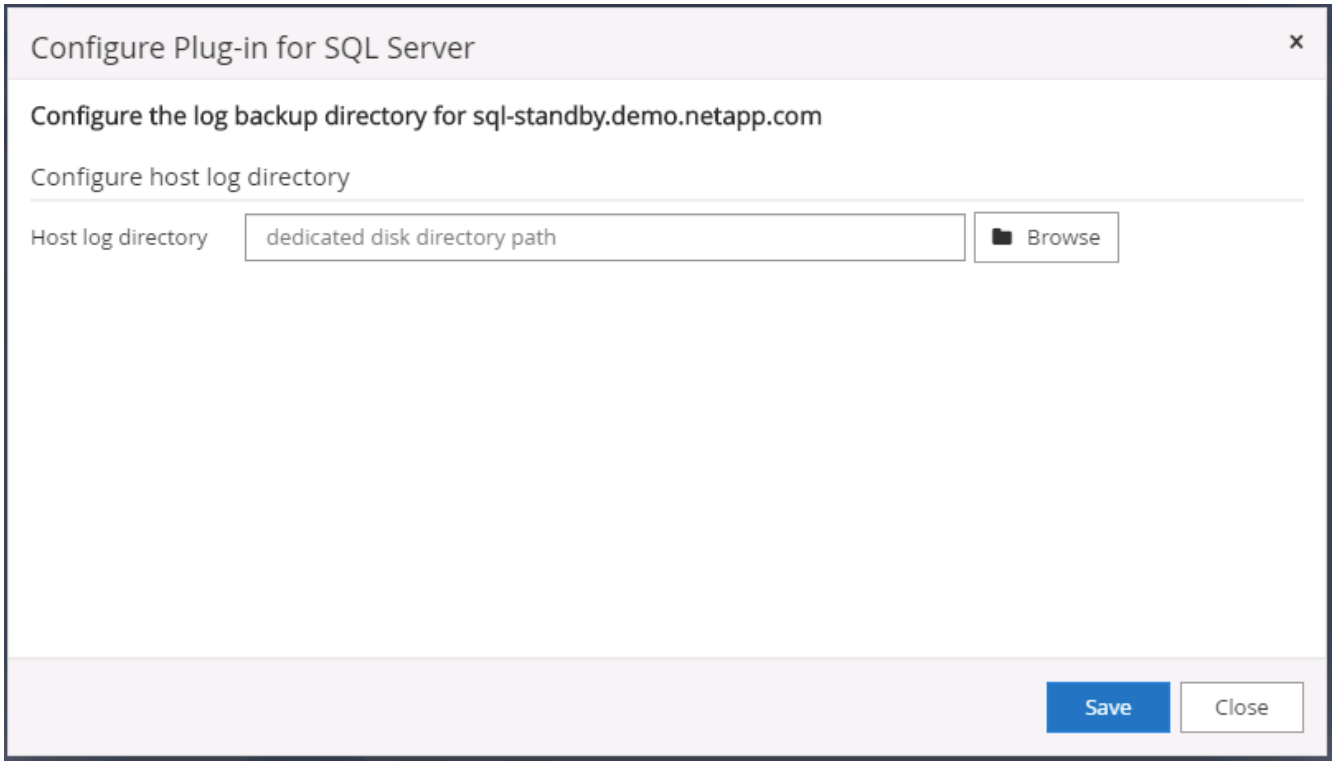


4. Una vez instalado el plugin en un host de Windows, su estado general se muestra como "Configure log directory".

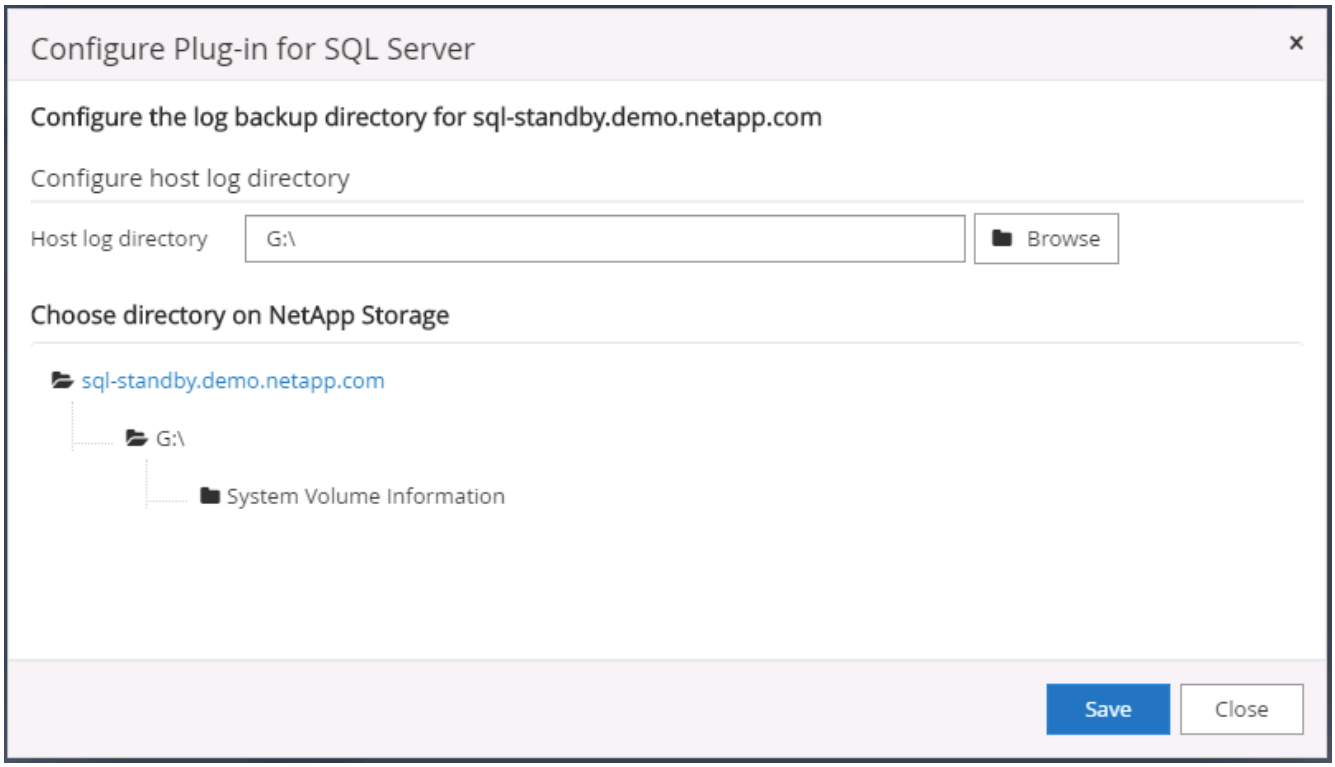
5. Haga clic en Nombre de host para abrir la configuración del directorio de registro de SQL Server.



6. Haga clic en "Configure log directory" para abrir "Configure Plug-in for SQL Server".

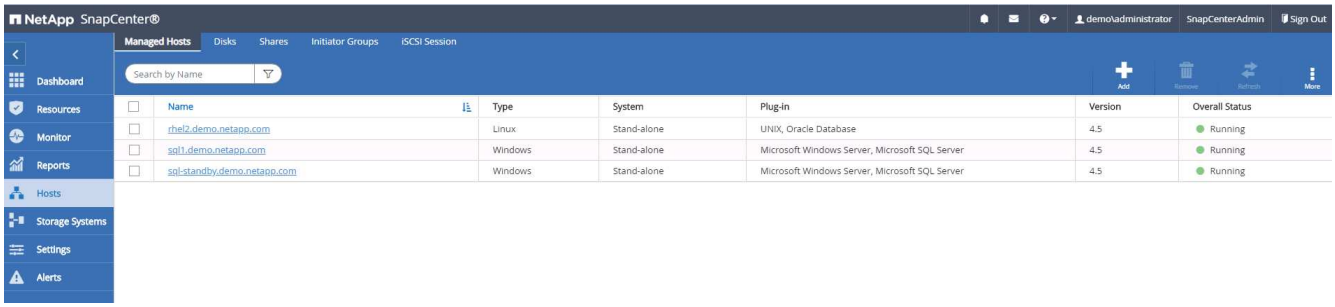


7. Haga clic en examinar para detectar el almacenamiento de NetApp de manera que se pueda configurar un directorio de registro; SnapCenter utiliza este directorio de registro para revertir los archivos de registro de transacciones de SQL Server. A continuación, haga clic en Guardar.

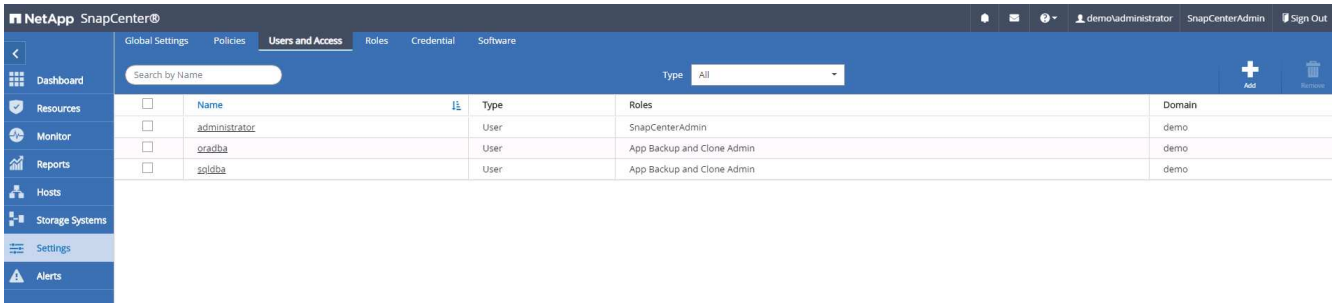


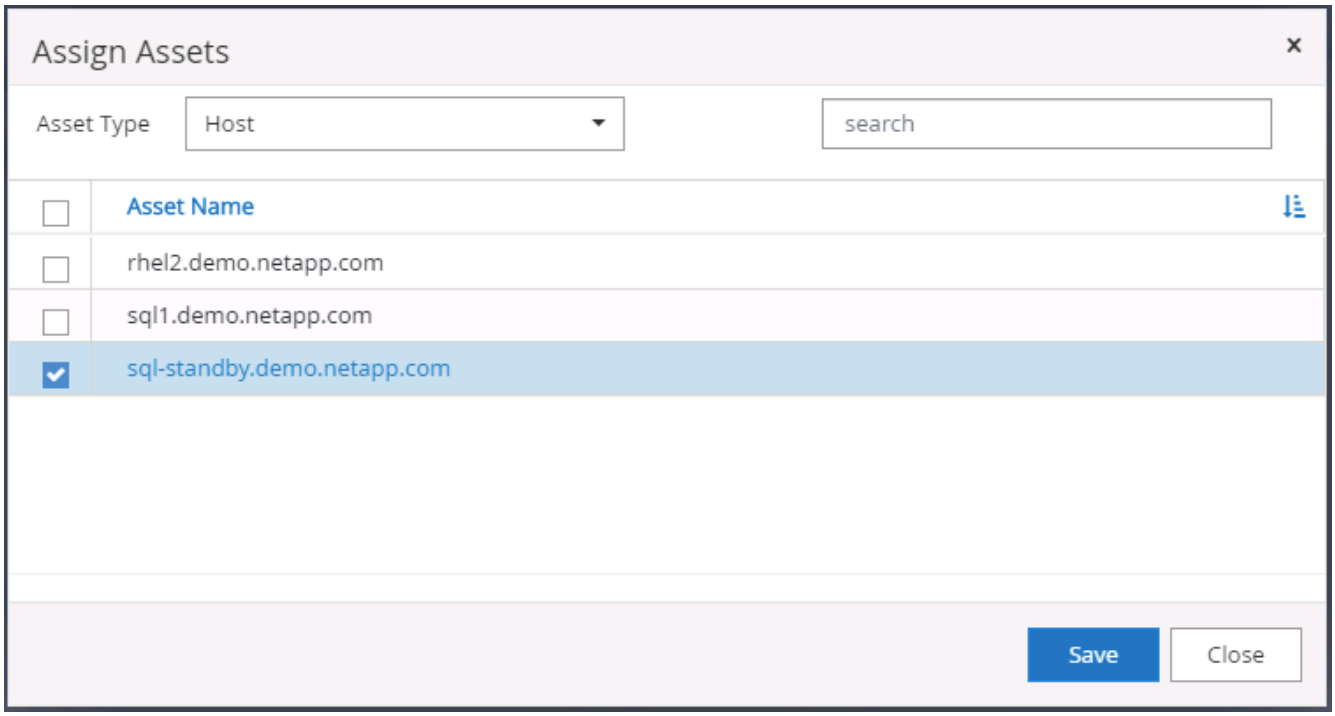
> Para que el almacenamiento de NetApp aprovisionado a un host de base de datos se detecte, es necesario añadir el almacenamiento (local o CVO) a SnapCenter, como se muestra en el paso 6 para CVO como ejemplo.

8. Una vez configurado el directorio de registro, el estado general del plugin del host de Windows cambia a Running.



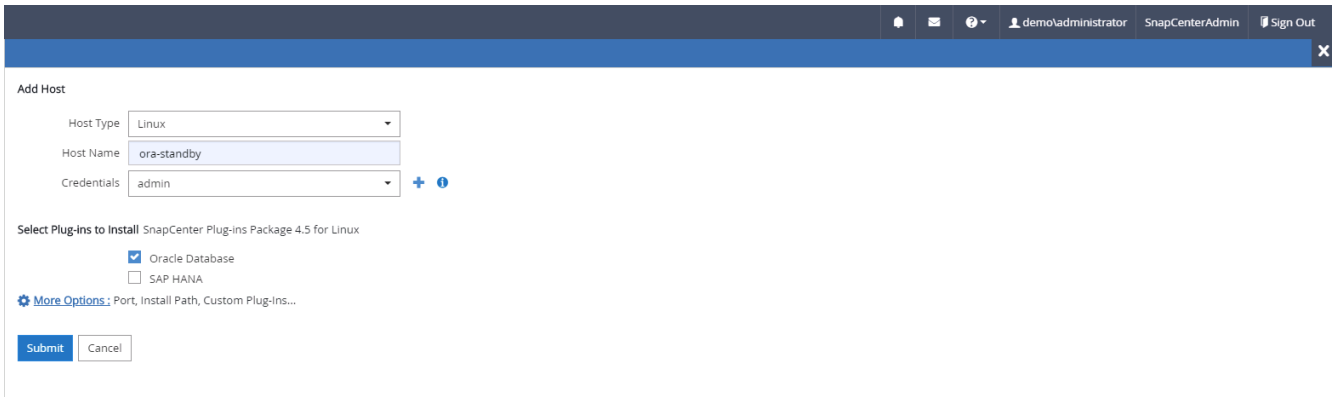
9. Para asignar el host al ID de usuario de administración de base de datos, desplácese a la ficha Access en Configuración y usuarios, haga clic en el ID de usuario de administración de la base de datos (en nuestro caso, la sqldba a la que se debe asignar el host) y haga clic en Save para completar la asignación de recursos del host.



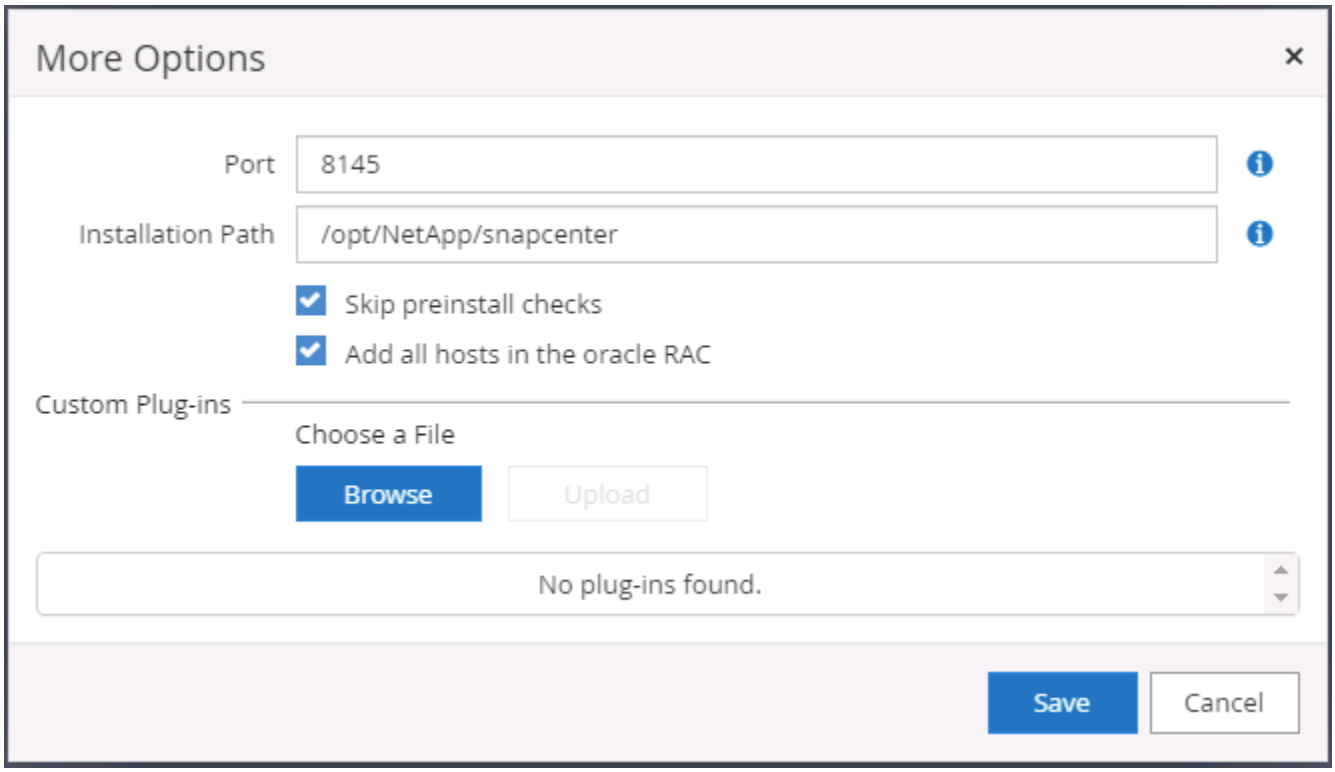


Agregar el host Unix y la instalación del plugin en el host

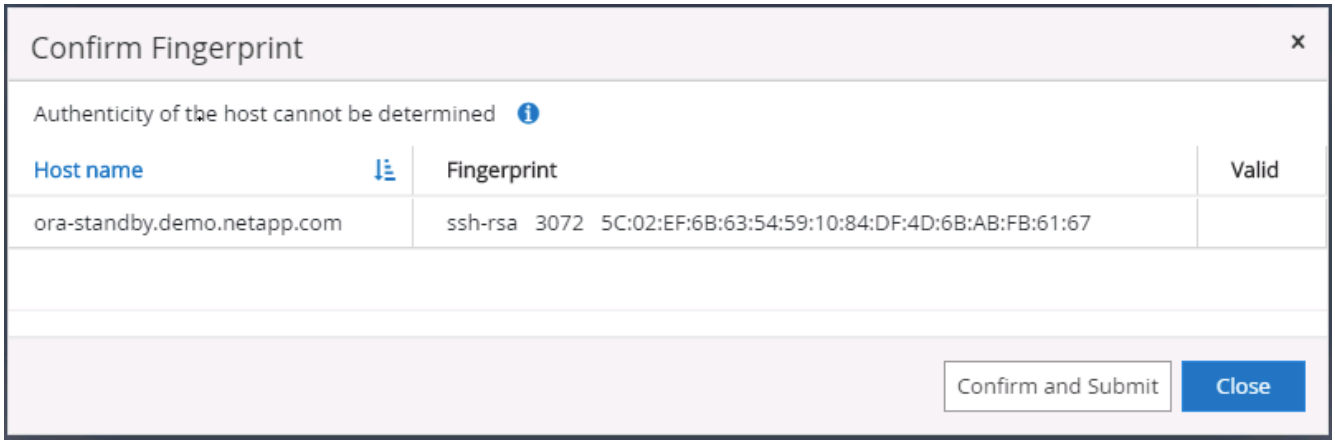
1. Inicie sesión en SnapCenter con un ID de usuario con privilegios de administrador de SnapCenter.
2. Haga clic en la ficha hosts del menú de la izquierda y haga clic en Agregar para abrir el flujo de trabajo Agregar host.
3. Elija Linux como el tipo de host. El nombre del host puede ser el nombre de host o una dirección IP. Sin embargo, se debe resolver el nombre de host para corregir la dirección IP del host desde el host SnapCenter. Seleccione las credenciales de host creadas en el paso 2. Las credenciales del host requieren privilegios sudo. Compruebe Oracle Database como el plugin que se va a instalar, que instala complementos de host de Oracle y Linux.



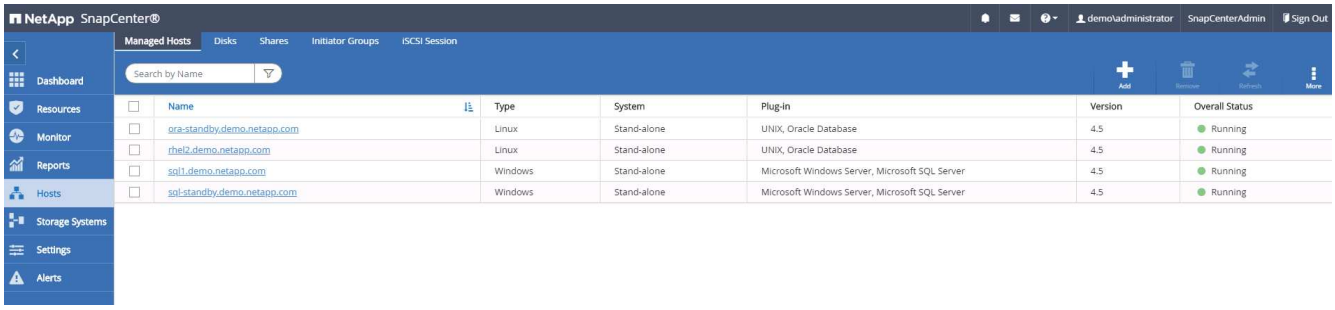
4. Haga clic en más opciones y seleccione "Omitir comprobaciones previas a la instalación". Se le pedirá que confirme la omisión de la comprobación de preinstalación. Haga clic en Yes y, a continuación, Save.



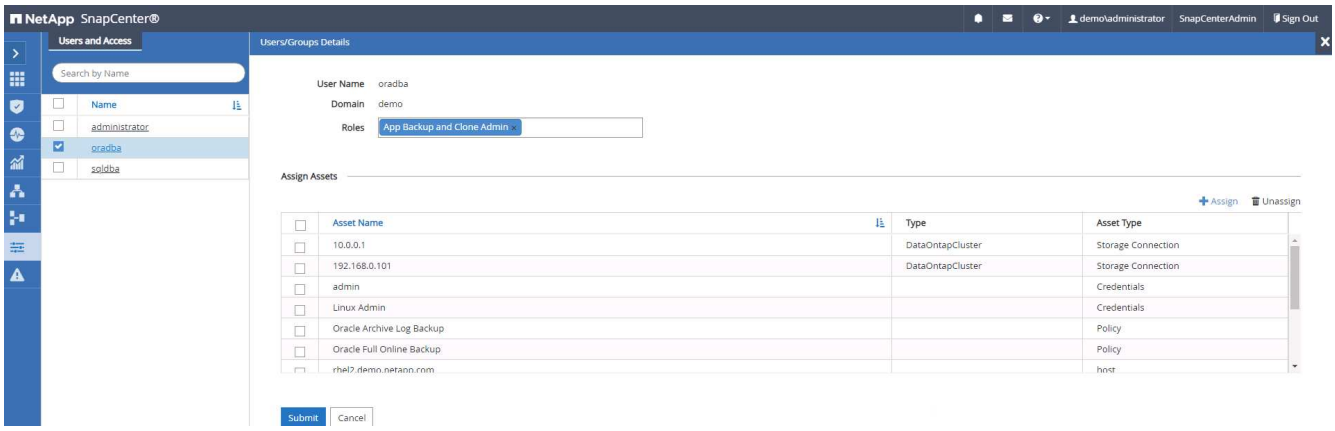
5. Haga clic en Enviar para iniciar la instalación del complemento. Se le pedirá que confirme la huella dactilar, tal como se muestra a continuación.

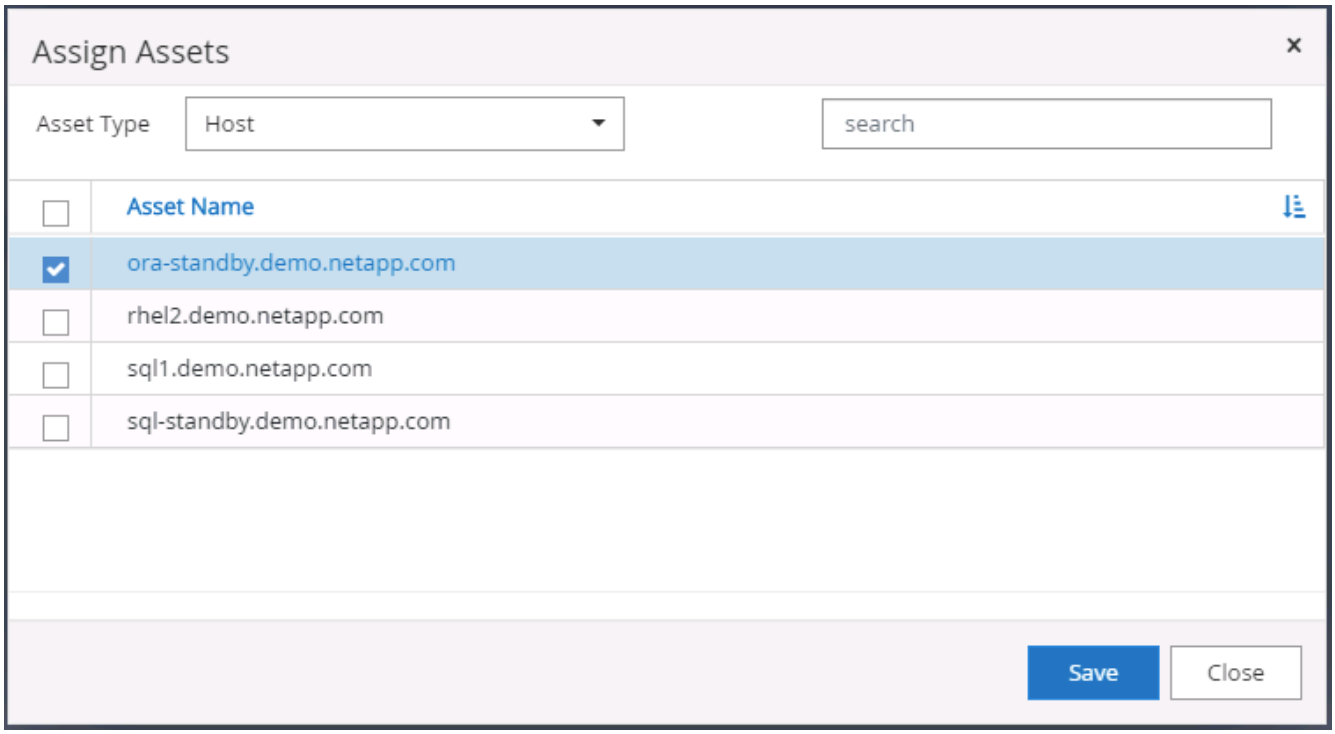


6. SnapCenter realiza la validación y el registro del host y, a continuación, se instala el plugin en el host Linux. El estado cambia de Installing Plugin a Running.



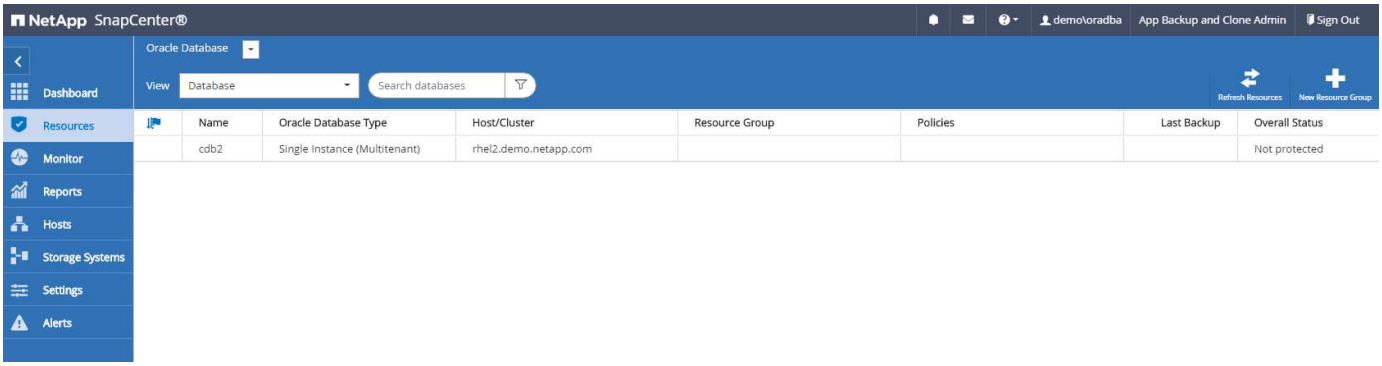
7. Asigne el host recién añadido al ID de usuario de administración de base de datos adecuado (en nuestro caso, oradba).





4. Detección de recursos de base de datos

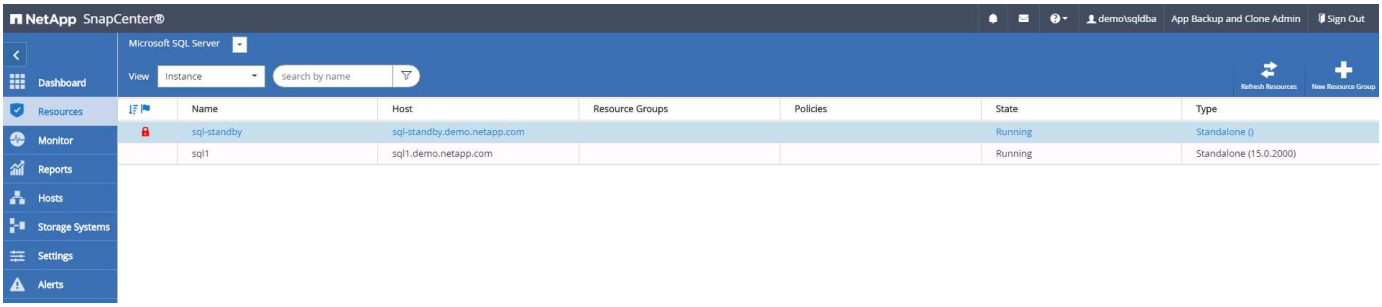
Cuando el plugin se instala correctamente, los recursos de la base de datos en el host se pueden detectar de inmediato. Haga clic en la ficha Recursos del menú de la izquierda. En función del tipo de plataforma de base de datos, hay disponibles varias vistas, como la base de datos, el grupo de recursos, etc. Puede ser necesario hacer clic en la pestaña Refresh Resources si no se detectan y se muestran los recursos en el host.

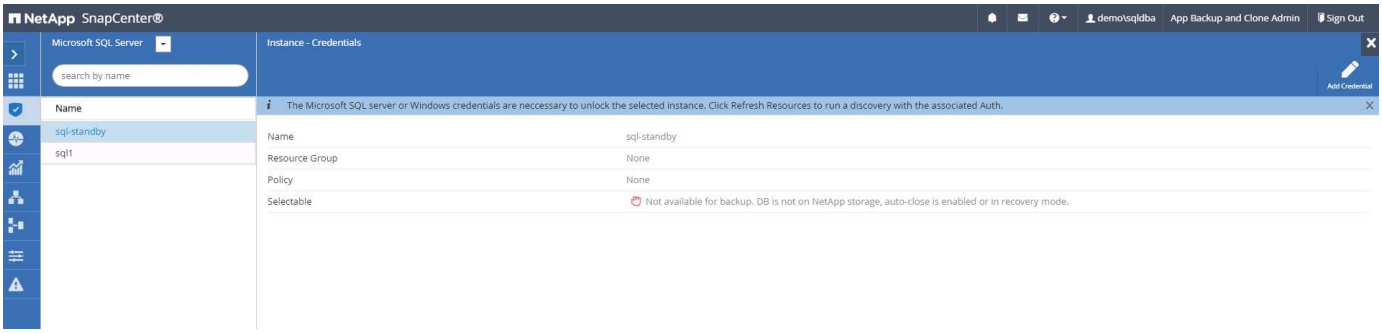


Cuando se detecta inicialmente la base de datos, el estado general se muestra como "no protegido". La captura de pantalla anterior muestra que una base de datos Oracle aún no está protegida por una política de backup.

Cuando se configura una política o configuración de backup y se ejecuta un backup, el estado general de la base de datos muestra el estado de backup como "Backup succeeded" y la Marca temporal del último backup. La siguiente captura de pantalla muestra el estado de la copia de seguridad de una base de datos de usuario de SQL Server.

Si las credenciales de acceso a la base de datos no están configuradas correctamente, un botón de bloqueo rojo indica que no se puede acceder a la base de datos. Por ejemplo, si las credenciales de Windows no tienen acceso de administrador del sistema a una instancia de base de datos, las credenciales de la base de datos deben volver a configurarse para desbloquear el bloqueo rojo.





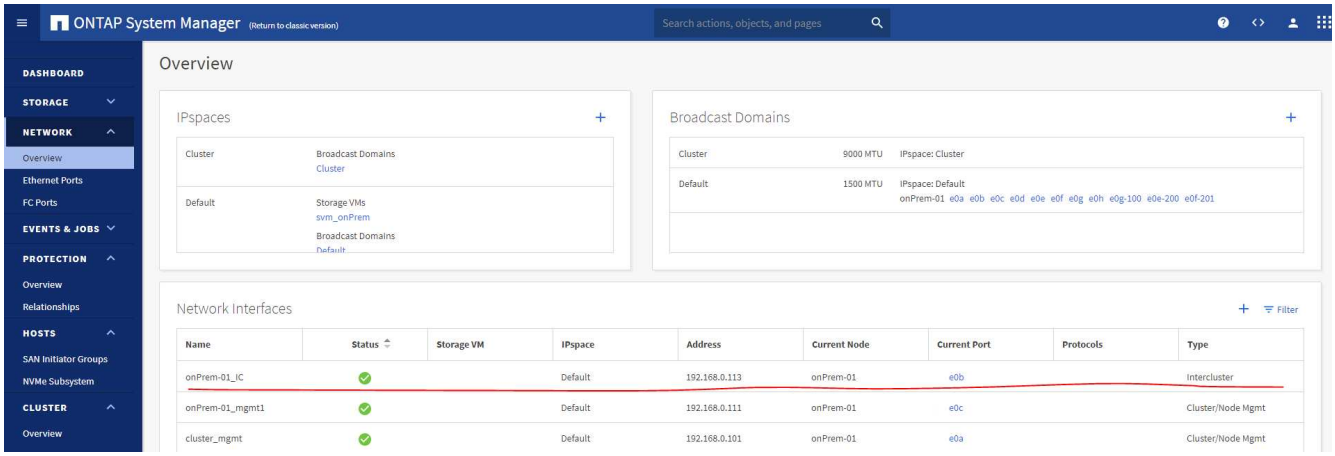
Una vez configuradas las credenciales adecuadas en el nivel de Windows o en la base de datos, desaparece el bloqueo rojo y se recopila y revisa la información de SQL Server Type.

5. Configurar la conexión entre clústeres de almacenamiento y la replicación de volúmenes de base de datos

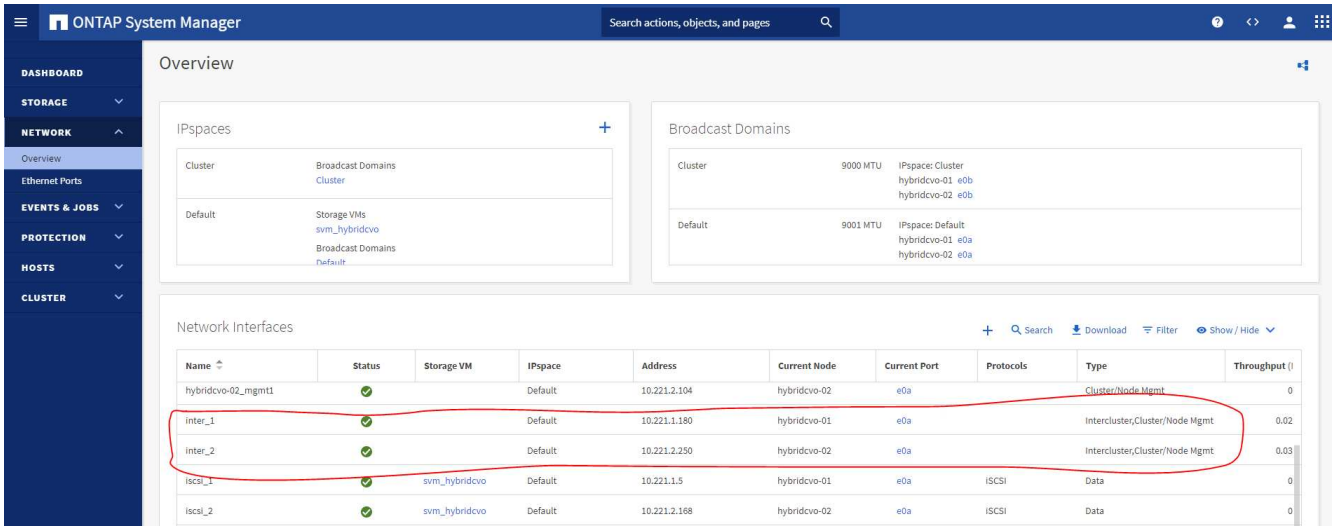
Para proteger los datos de sus bases de datos locales mediante un cloud público como destino, los volúmenes de base de datos de clúster ONTAP en las instalaciones se replican en el cloud CVO mediante la tecnología SnapMirror de NetApp. A continuación, los volúmenes de destino replicados se pueden clonar para ACTIVIDADES DE DESARROLLO y operaciones, o bien para la recuperación ante desastres. Los siguientes pasos de alto nivel le permiten configurar la replicación entre iguales de clústeres y volúmenes de base de datos.

1. Configure las LIF de interconexión de clústeres para la agrupación de clústeres en el clúster local y en la instancia de clúster de CVO. Este paso se puede llevar a cabo con ONTAP System Manager. Una puesta en marcha predeterminada de CVO tiene LIF entre clústeres configurados automáticamente.

   Clúster en las instalaciones:



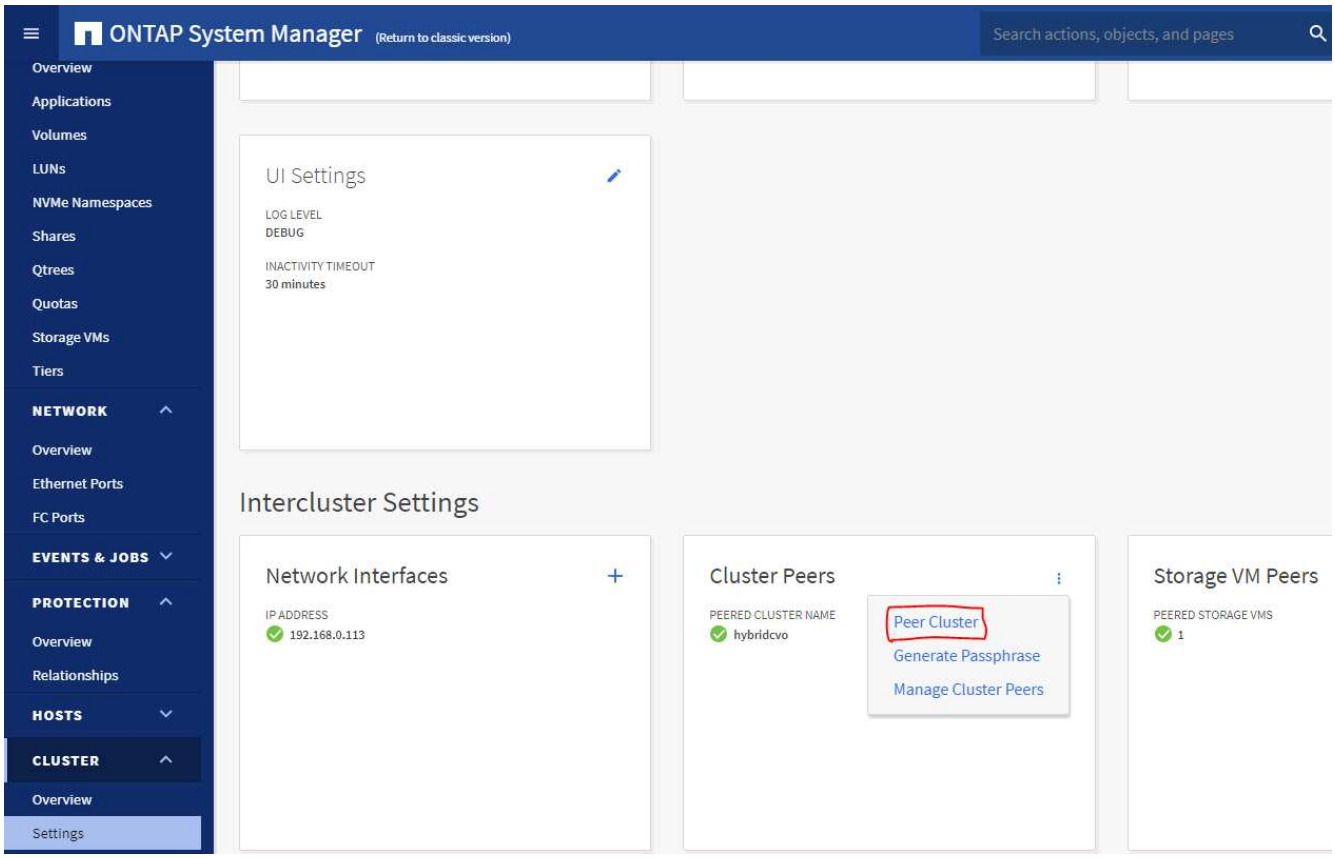
   Clúster de CVO de destino:



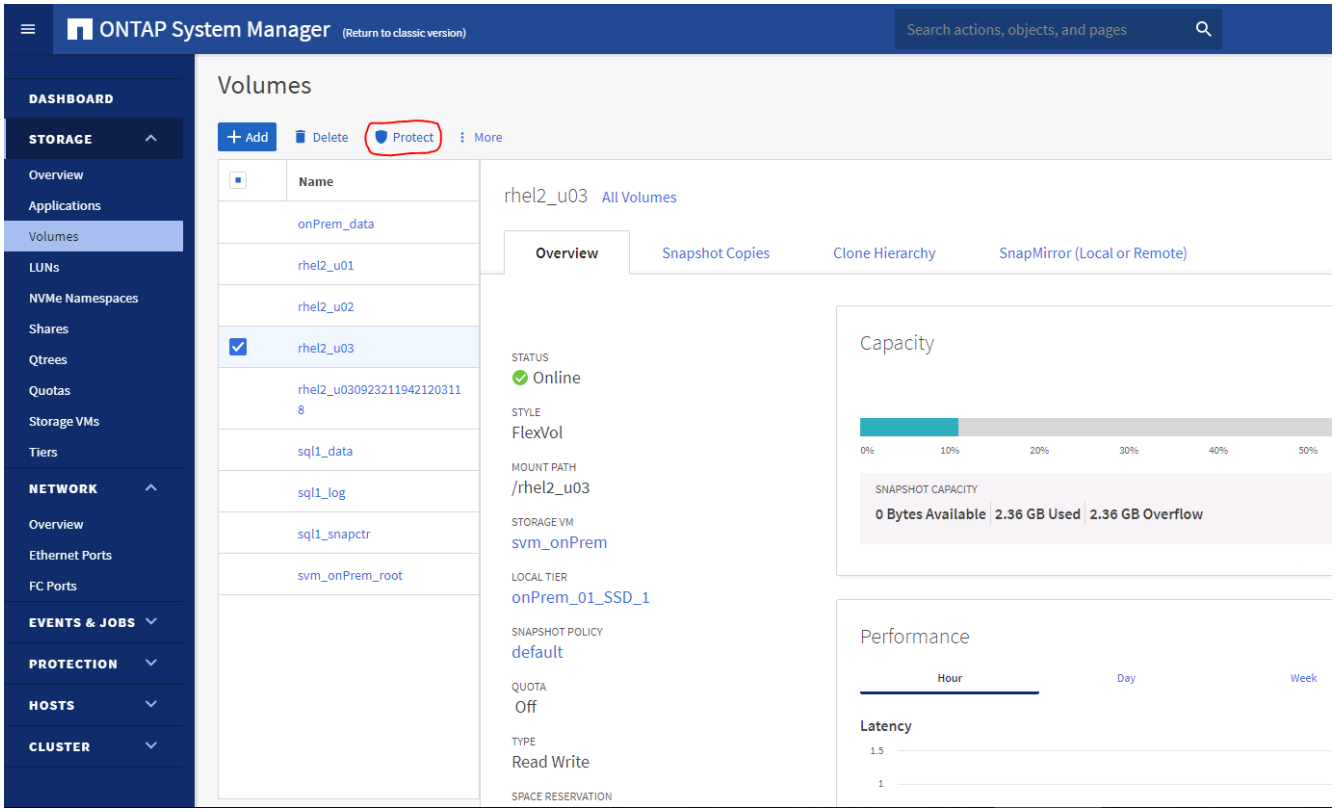
2. Con las LIF de interconexión de clústeres configuradas, la interconexión de clústeres entre iguales y la replicación de volúmenes se pueden configurar mediante el método de arrastrar y soltar en Cloud Manager de NetApp. Consulte "Introducción: Cloud público de AWS" para obtener más detalles.

   Como alternativa, se puede llevar a cabo la paridad de clústeres y la replicación de volúmenes de base de datos mediante System Manager de ONTAP de la siguiente manera:

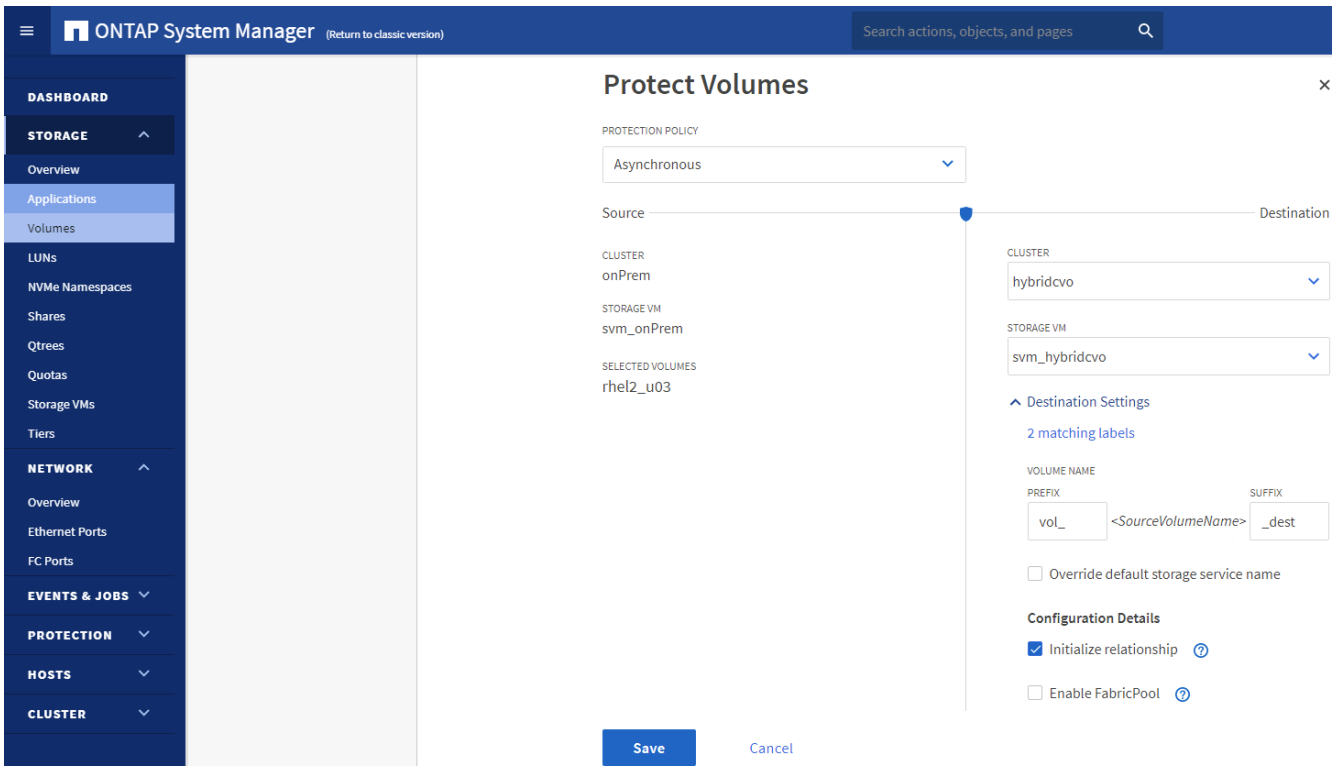
3. Inicie sesión en el Administrador del sistema de ONTAP. Acceda a Cluster > Settings y haga clic en Peer Cluster para configurar Cluster peering con la instancia de CVO en el cloud.



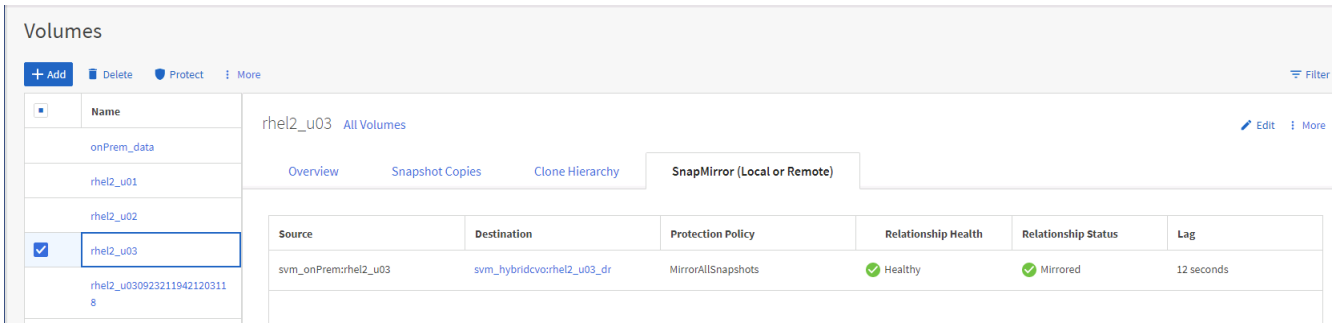
4. Vaya a la pestaña Volumes. Seleccione el volumen de la base de datos que se va a replicar y haga clic en Protect.



5. Establezca la directiva de protección en Asynchronous. Seleccione el clúster de destino y la SVM de almacenamiento.

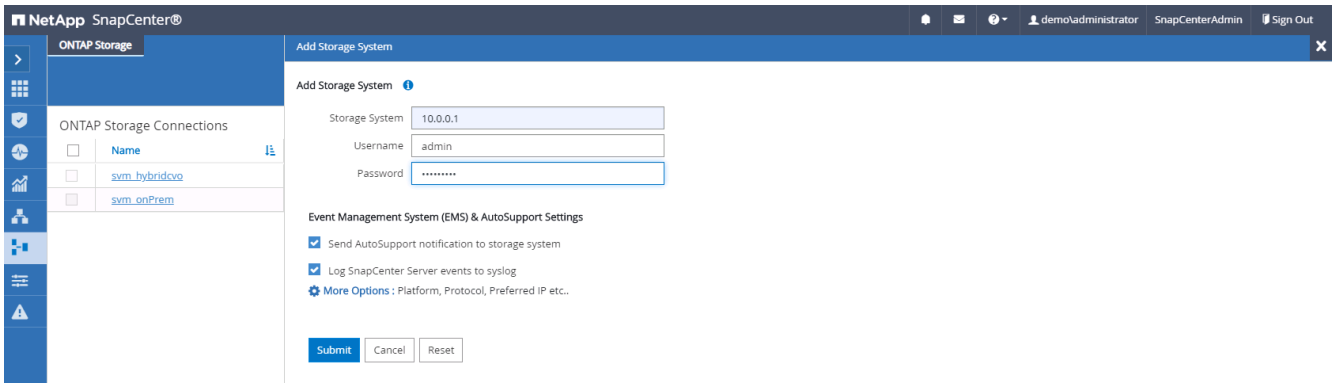


6. Compruebe que el volumen esté sincronizado entre el origen y el destino y que la relación de replicación sea correcta.

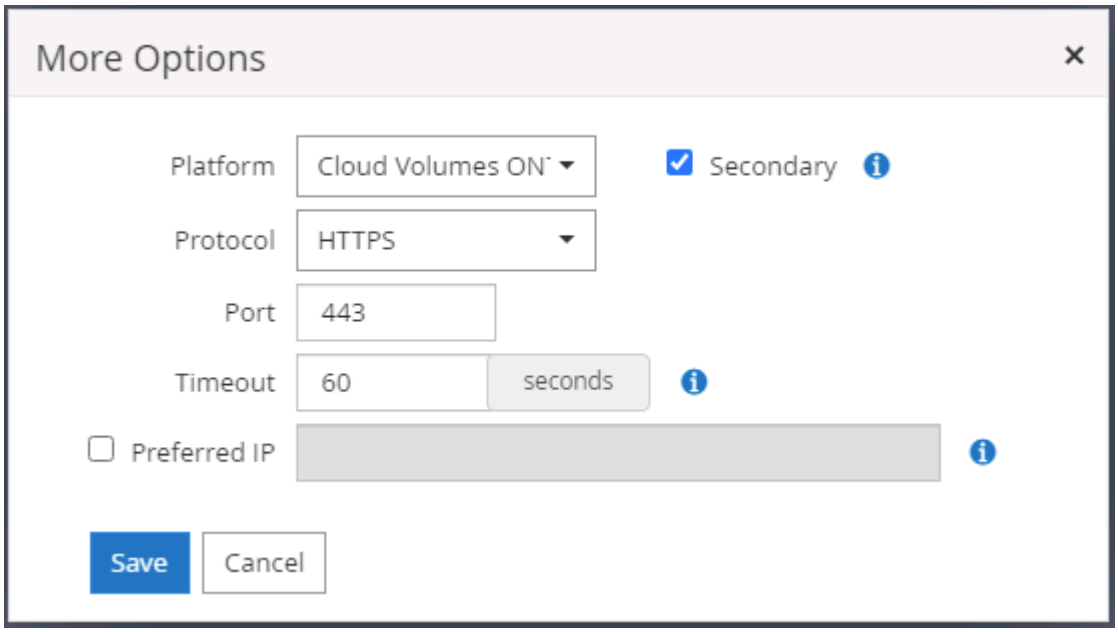


6. Añada SVM de almacenamiento de base de datos de CVO a SnapCenter

1. Inicie sesión en SnapCenter con un ID de usuario con privilegios de administrador de SnapCenter.
2. Haga clic en la pestaña Storage System del menú y, a continuación, haga clic en New para añadir una SVM de almacenamiento CVO que aloja volúmenes de base de datos de destino replicados a SnapCenter. Introduzca la IP de gestión del clúster en el campo Storage System e introduzca el nombre de usuario y la contraseña correspondientes.

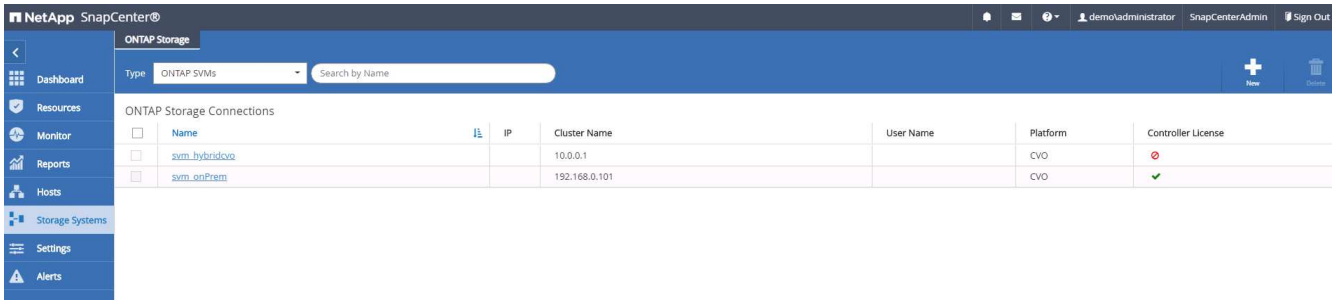


3. Haga clic en más opciones para abrir opciones de configuración de almacenamiento adicional. En el campo Plataforma, seleccione Cloud Volumes ONTAP, seleccione secundario y haga clic en Guardar.



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

SnapCenter tal y como se muestra en 3. Instalación del complemento de host de SnapCenter.

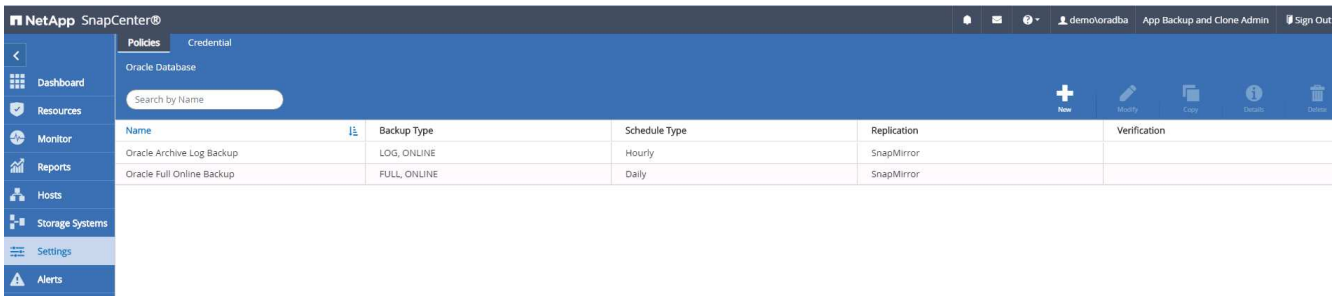


7. Configuración de la política de copia de seguridad de la base de datos en SnapCenter

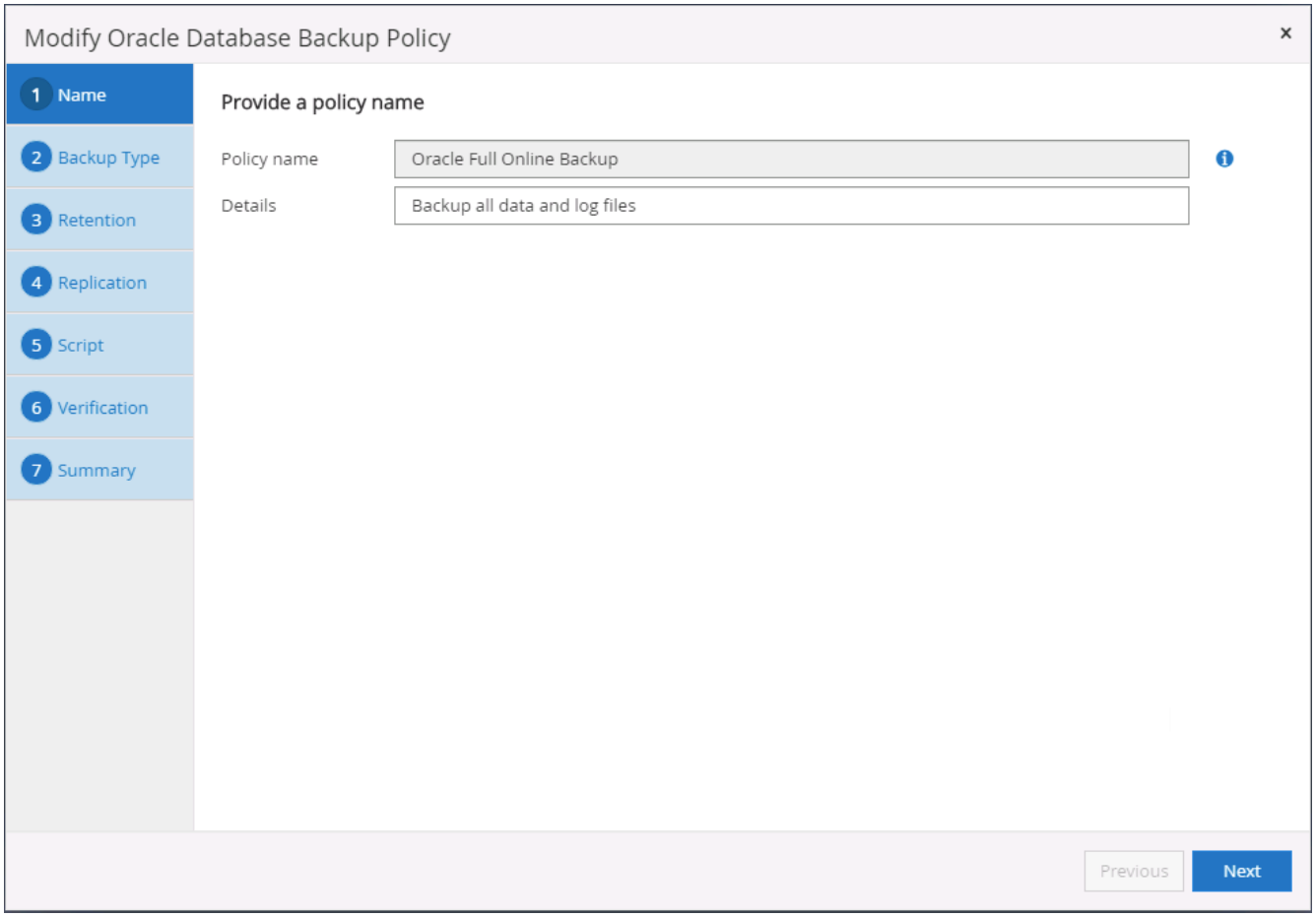
En los siguientes procedimientos se muestra cómo crear una base de datos completa o una política de backup de archivos de registro. Luego, la política puede implementarse para proteger los recursos de las bases de datos. El objetivo de punto de recuperación (RPO) o el objetivo de tiempo de recuperación (RTO) determina la frecuencia de los backups de la base de datos o de registros.

Cree una política de backup de base de datos completa para Oracle

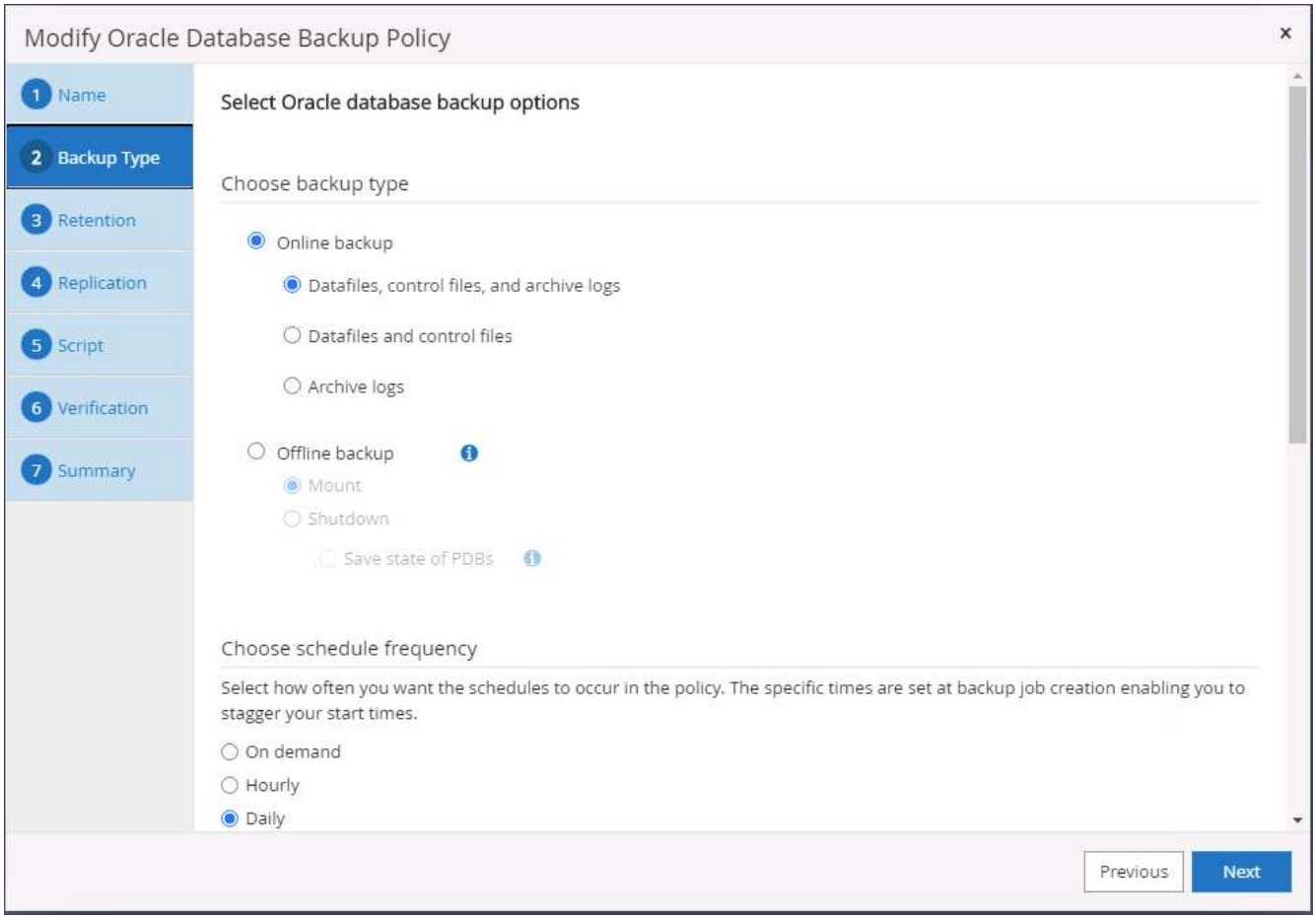
1. Inicie sesión en SnapCenter como identificador de usuario de administración de bases de datos, haga clic en Configuración y, a continuación, en políticas.



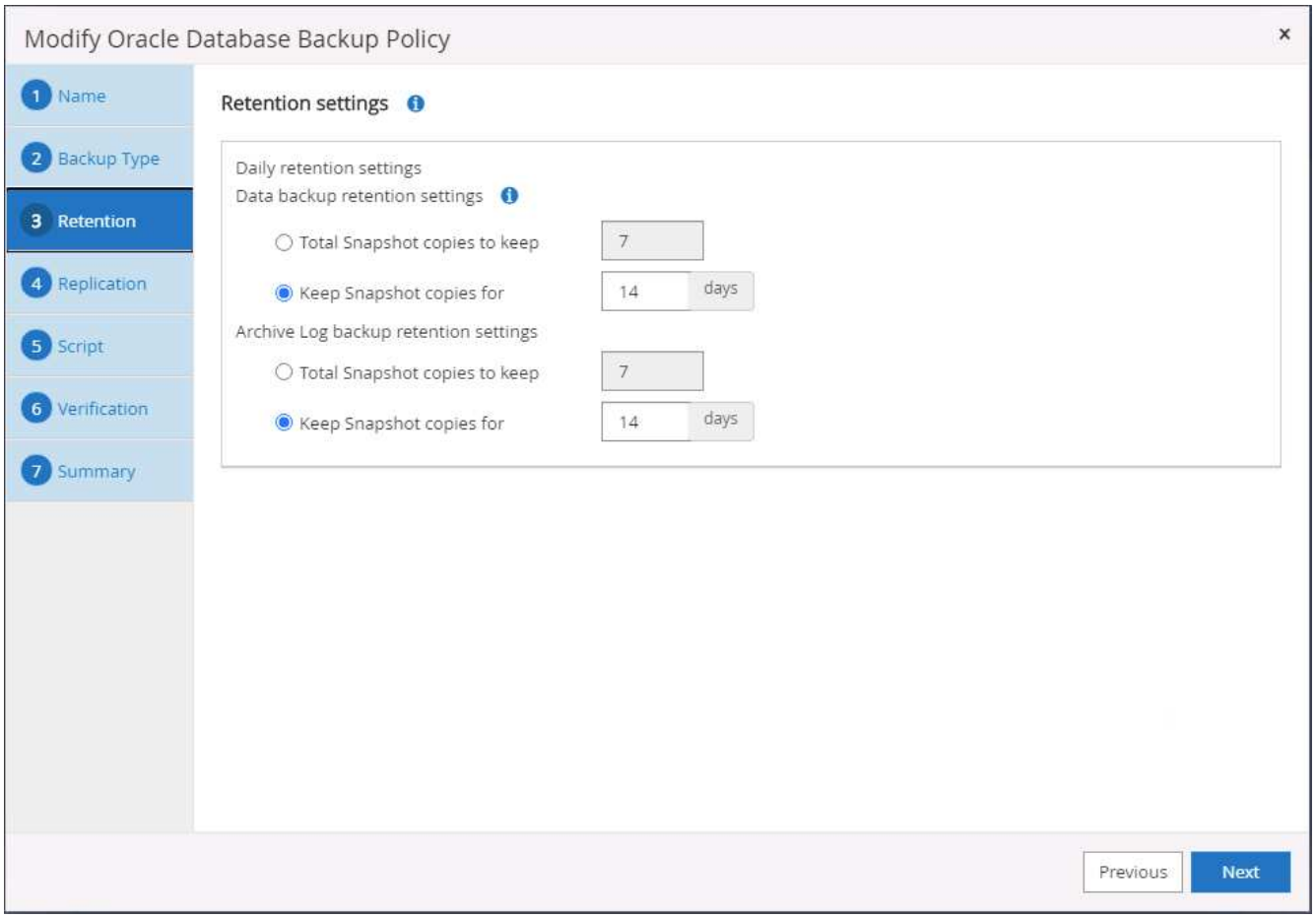
2. Haga clic en New para iniciar un nuevo flujo de trabajo de creación de políticas de backup o seleccione una política existente para modificarla.



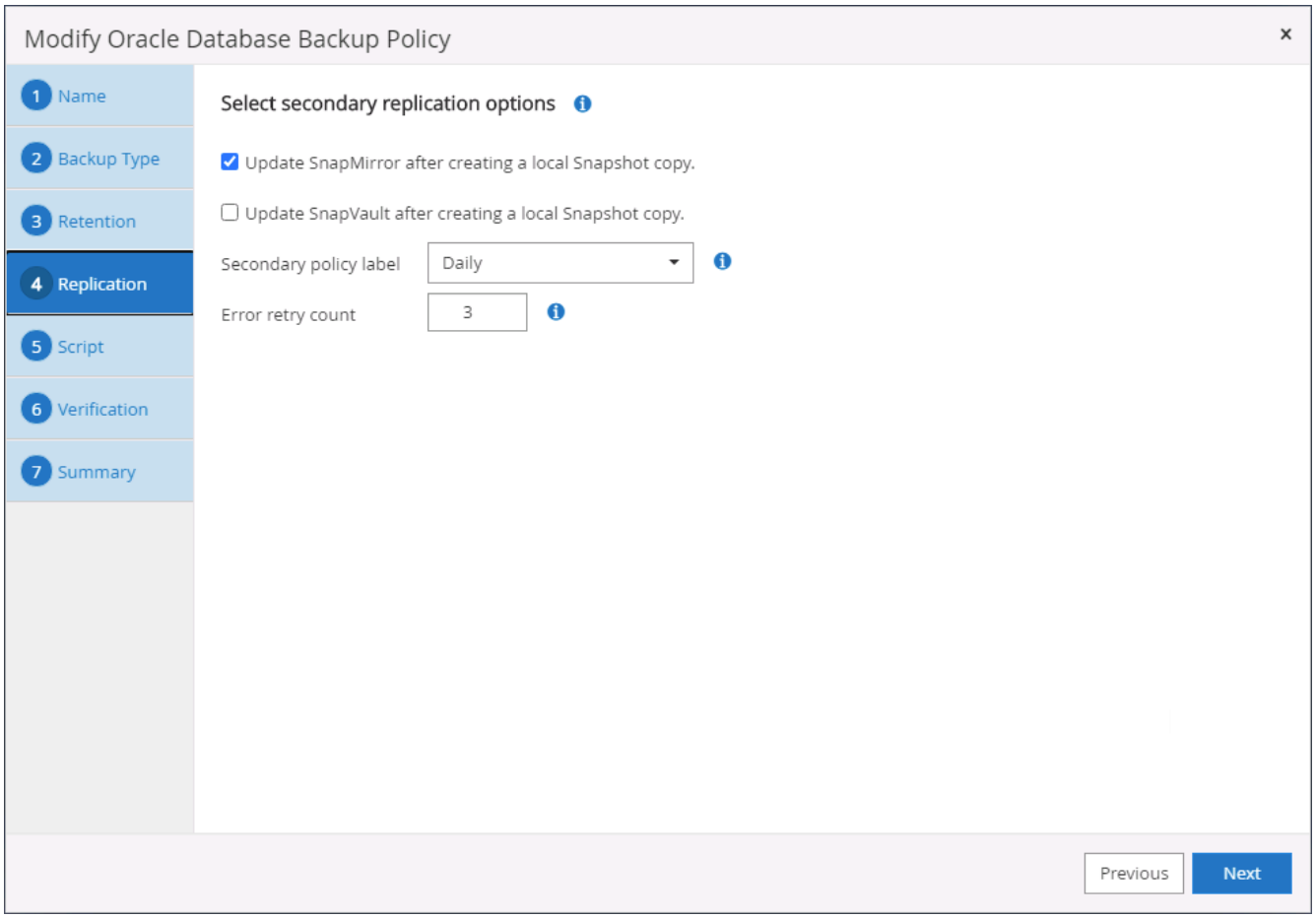
3. Seleccione el tipo de backup y la frecuencia de programación.



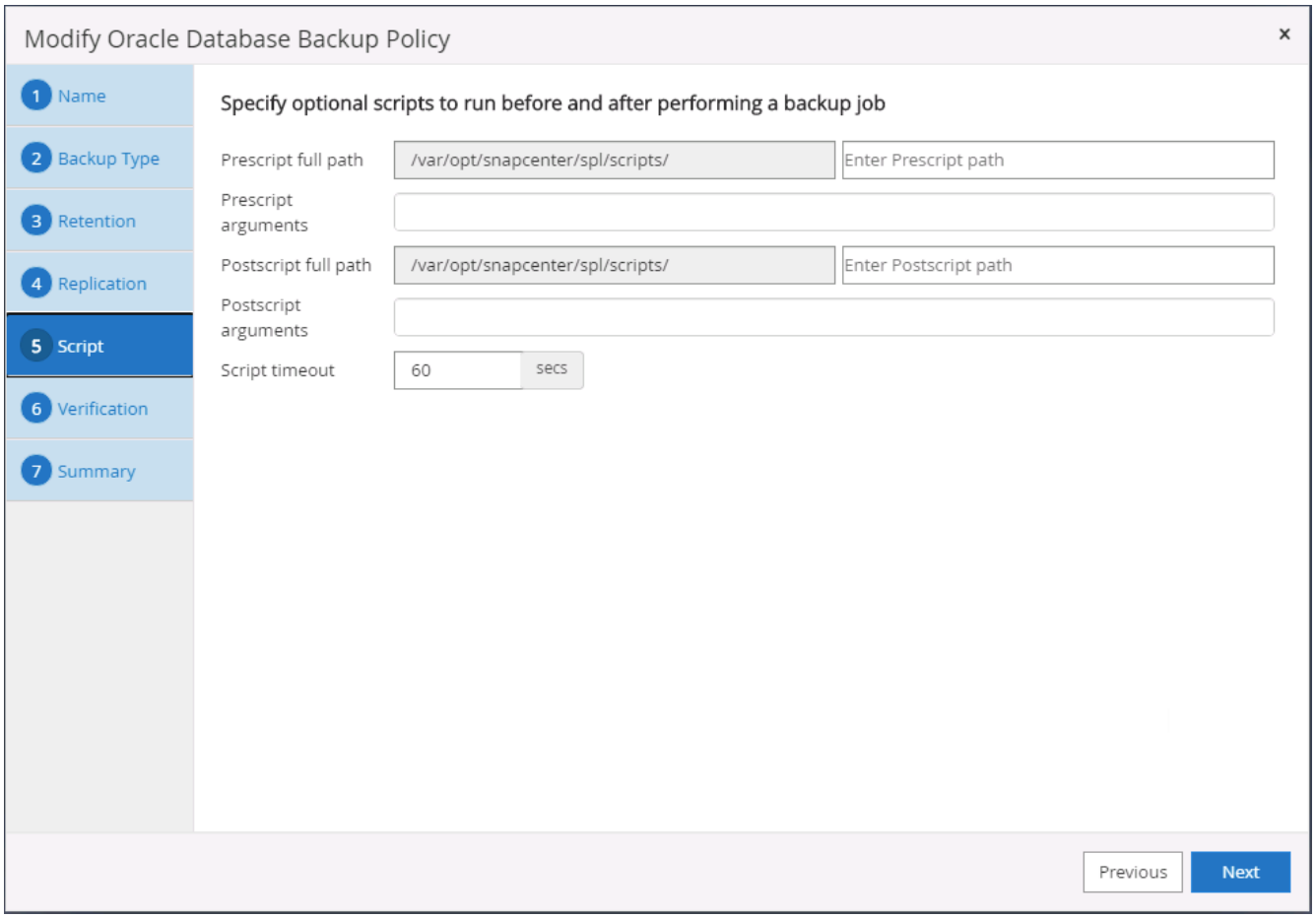
4. Establezca el valor de retención de copias de seguridad. Esto define cuántas copias de backup de base de datos completas se deben conservar.



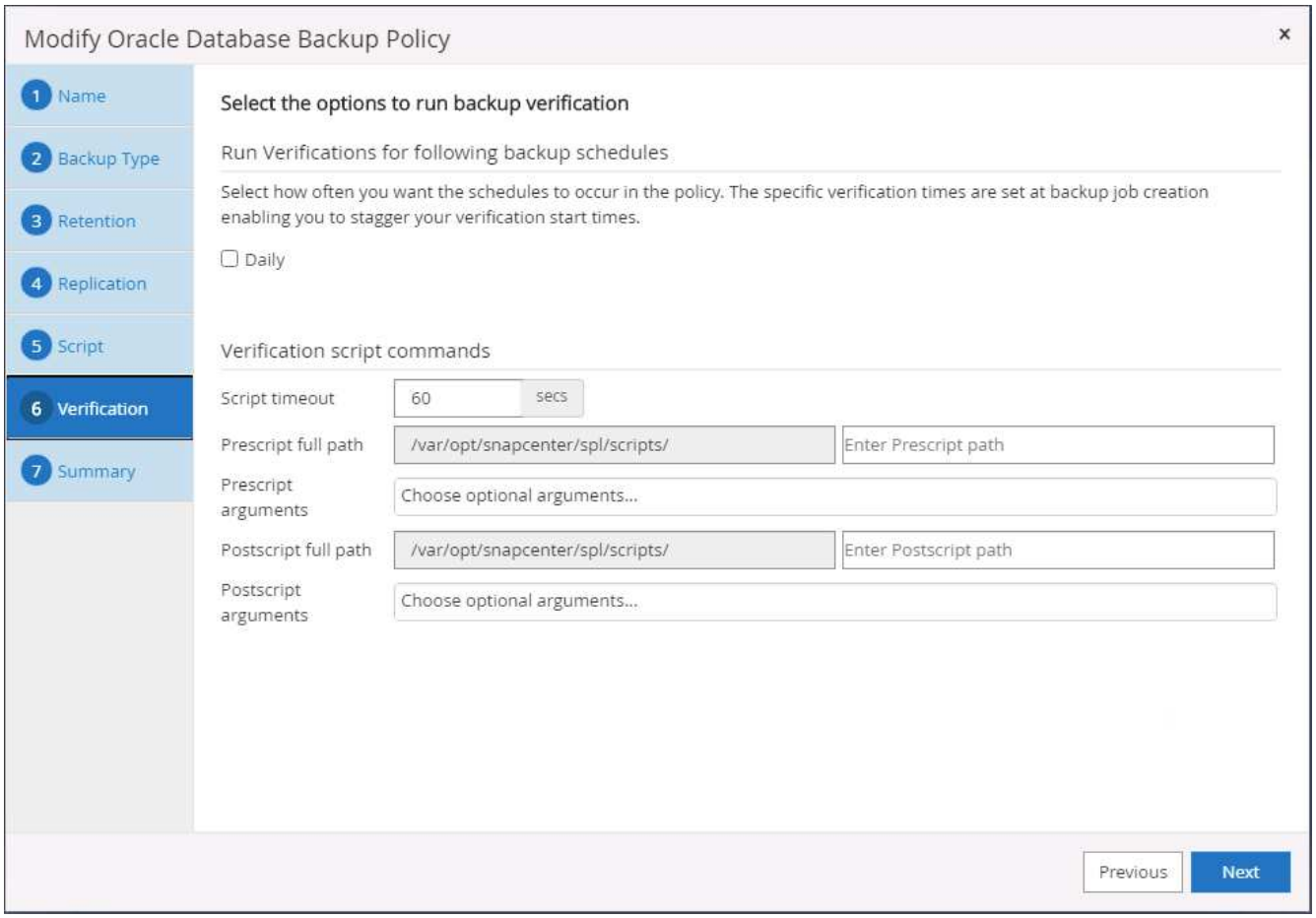
5. Seleccione las opciones de replicación secundaria para insertar los backups de las snapshots primarias locales que se van a replicar en una ubicación secundaria en el cloud.



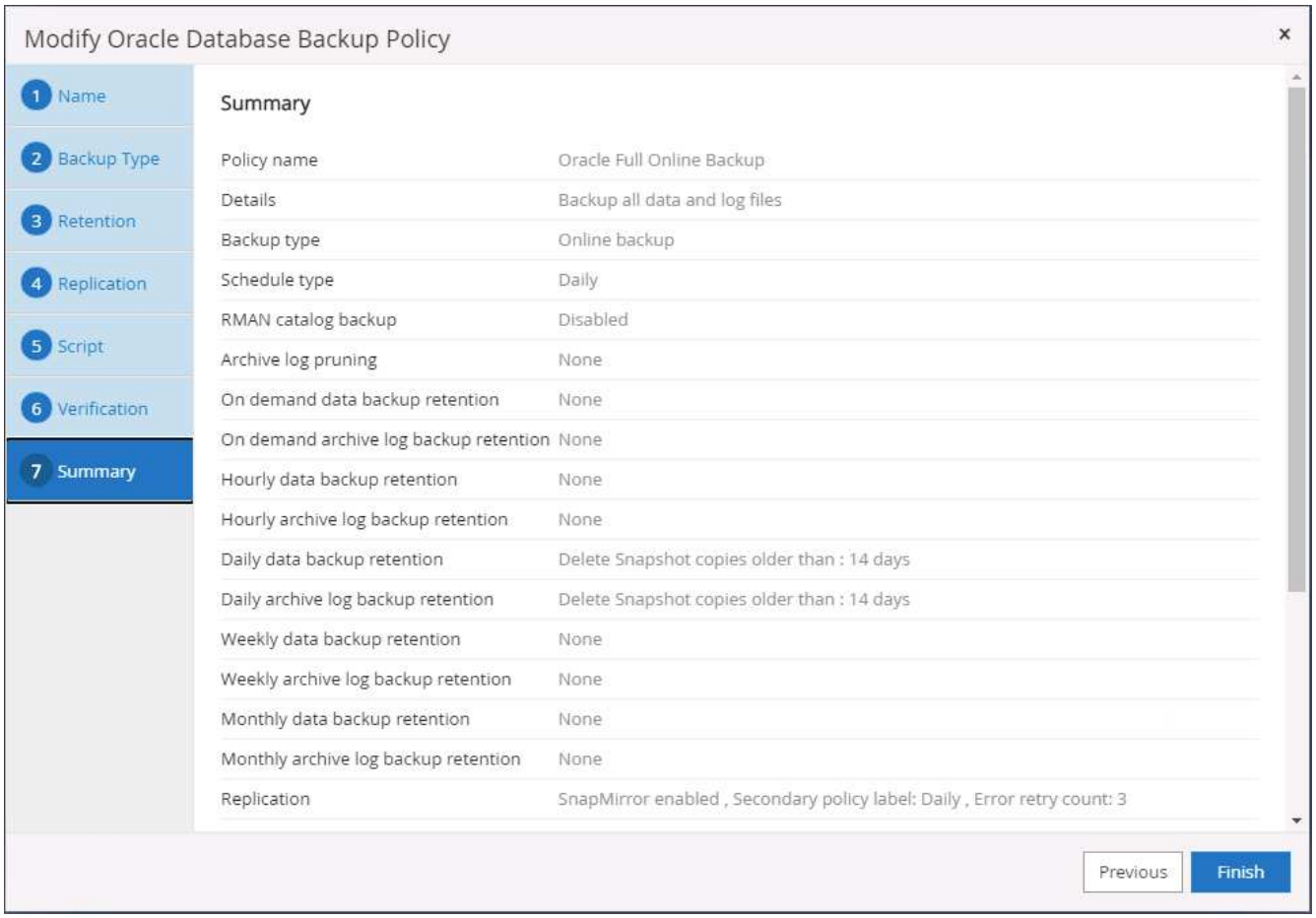
6. Especifique cualquier script opcional antes y después de la ejecución de un backup.



7. Ejecute la verificación del backup si lo desea.

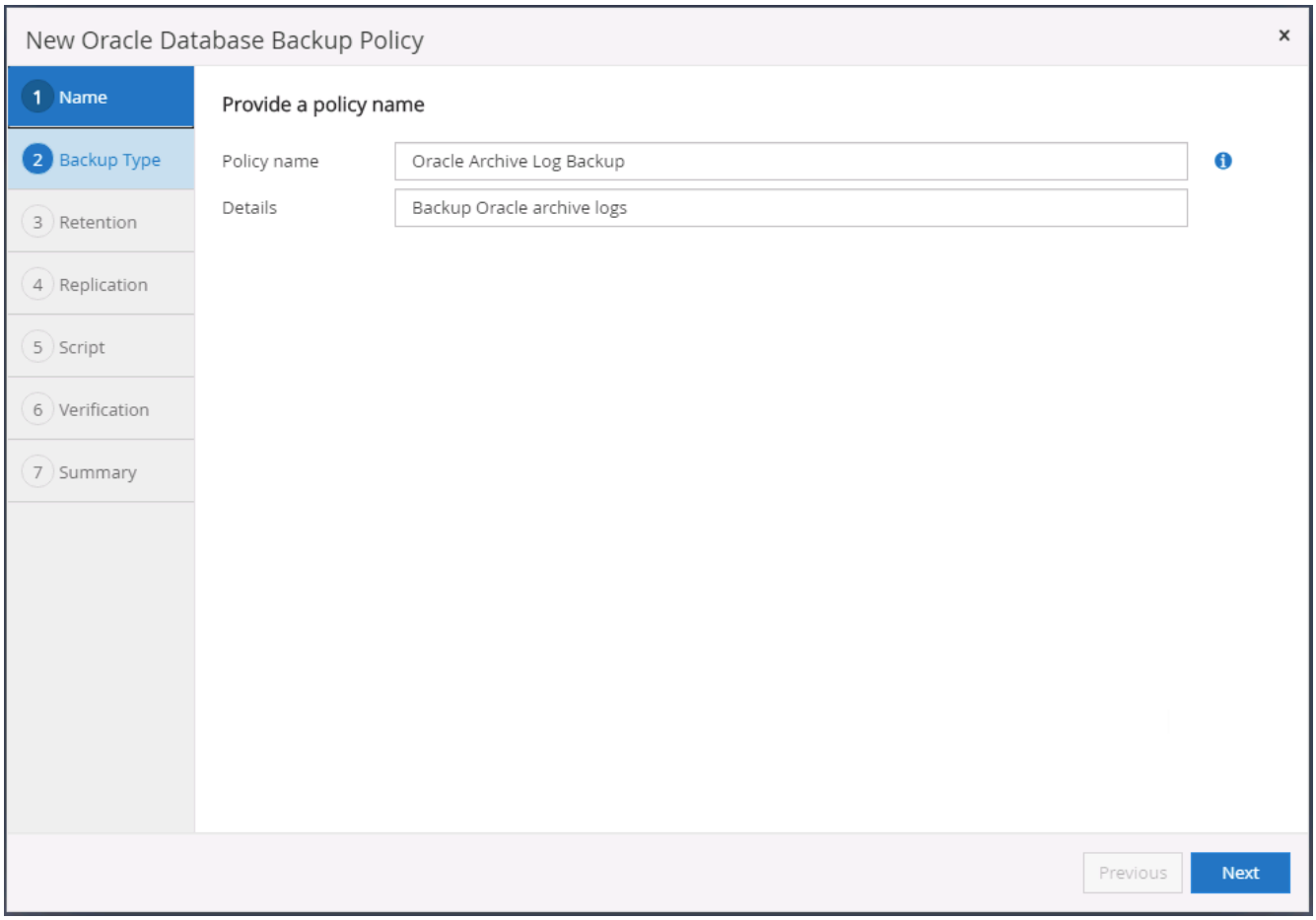

Modify Oracle Database Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Select the options to run backup verification
Run Verifications for following backup schedules
Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.
Daily
Verification script commands
Script timeout
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.

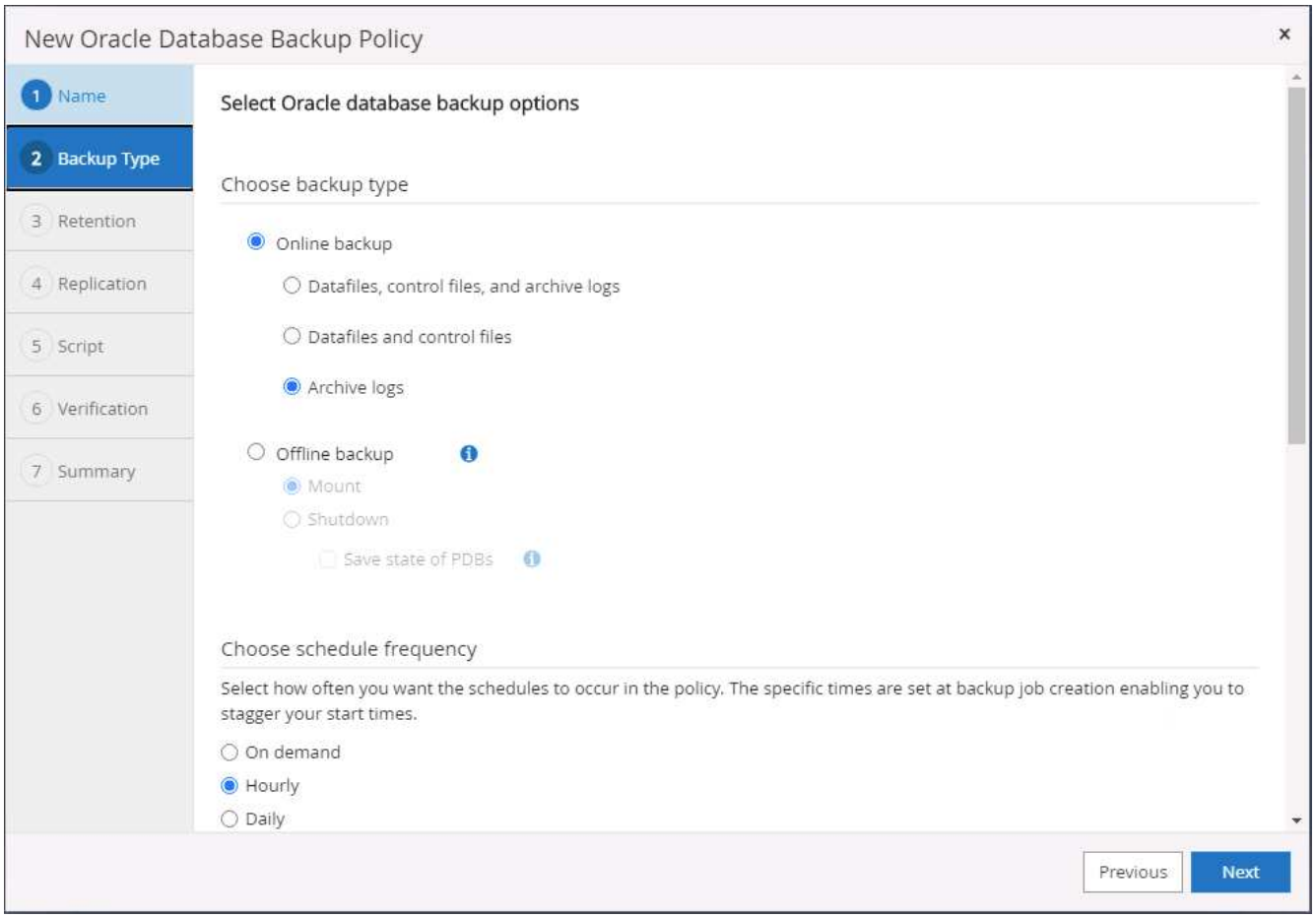


Cree una política de backup del registro de la base de datos para Oracle

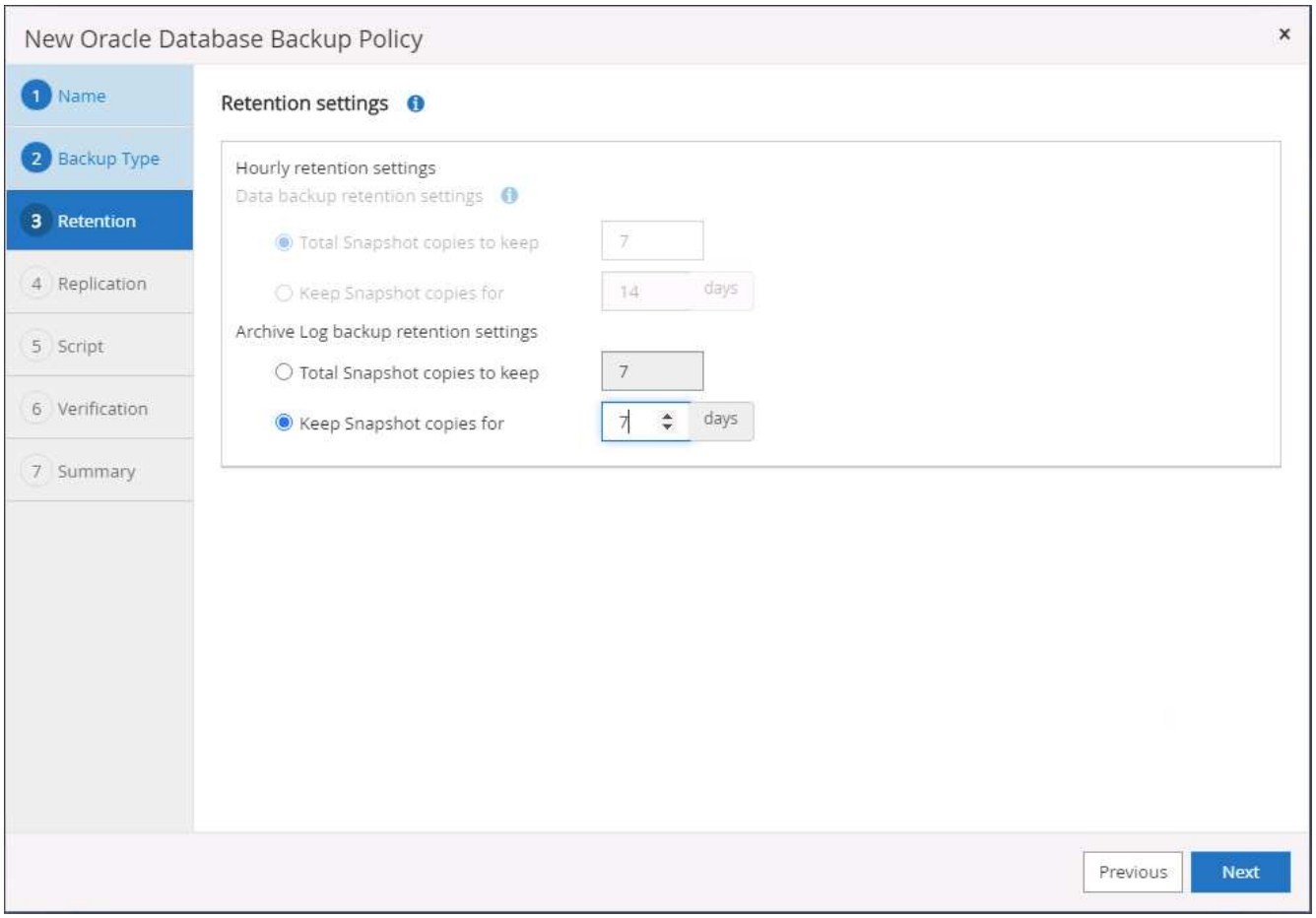
1. Inicie sesión en SnapCenter con un ID de usuario de administración de bases de datos, haga clic en Configuración y, a continuación, en políticas.
2. Haga clic en New para iniciar un nuevo flujo de trabajo de creación de políticas de backup o seleccione una política existente para modificarla.



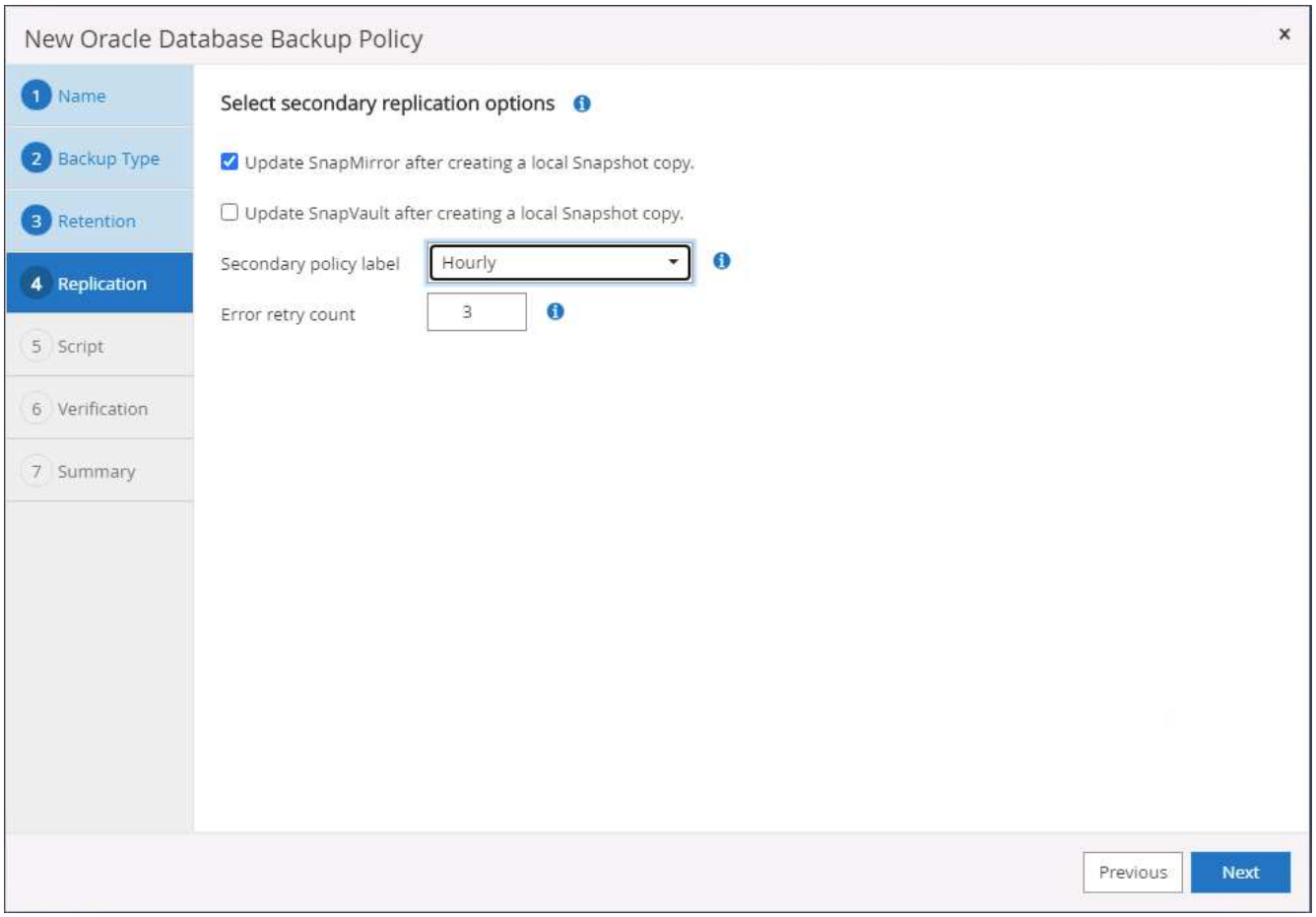
3. Seleccione el tipo de backup y la frecuencia de programación.



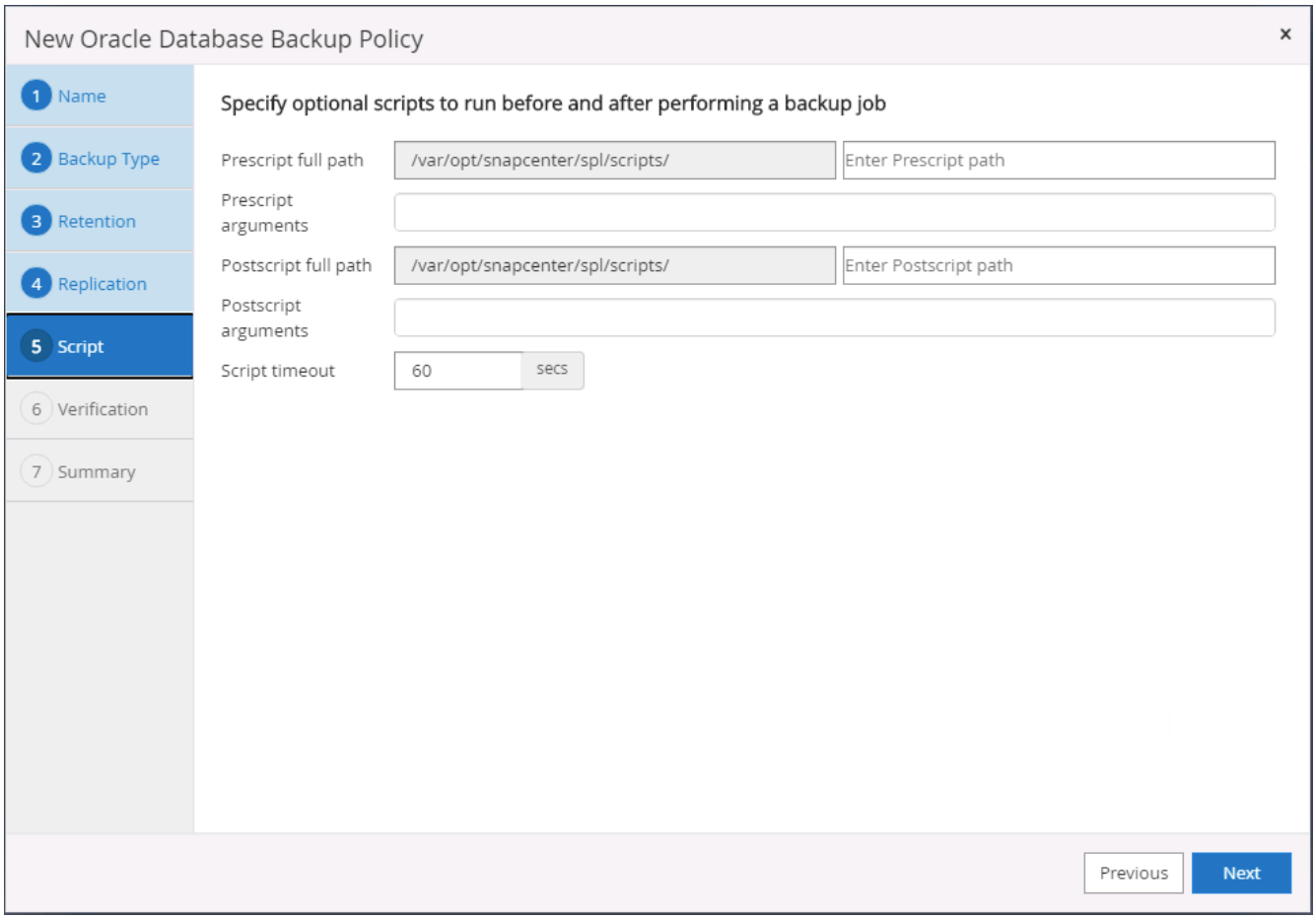
4. Configure el período de retención del registro.



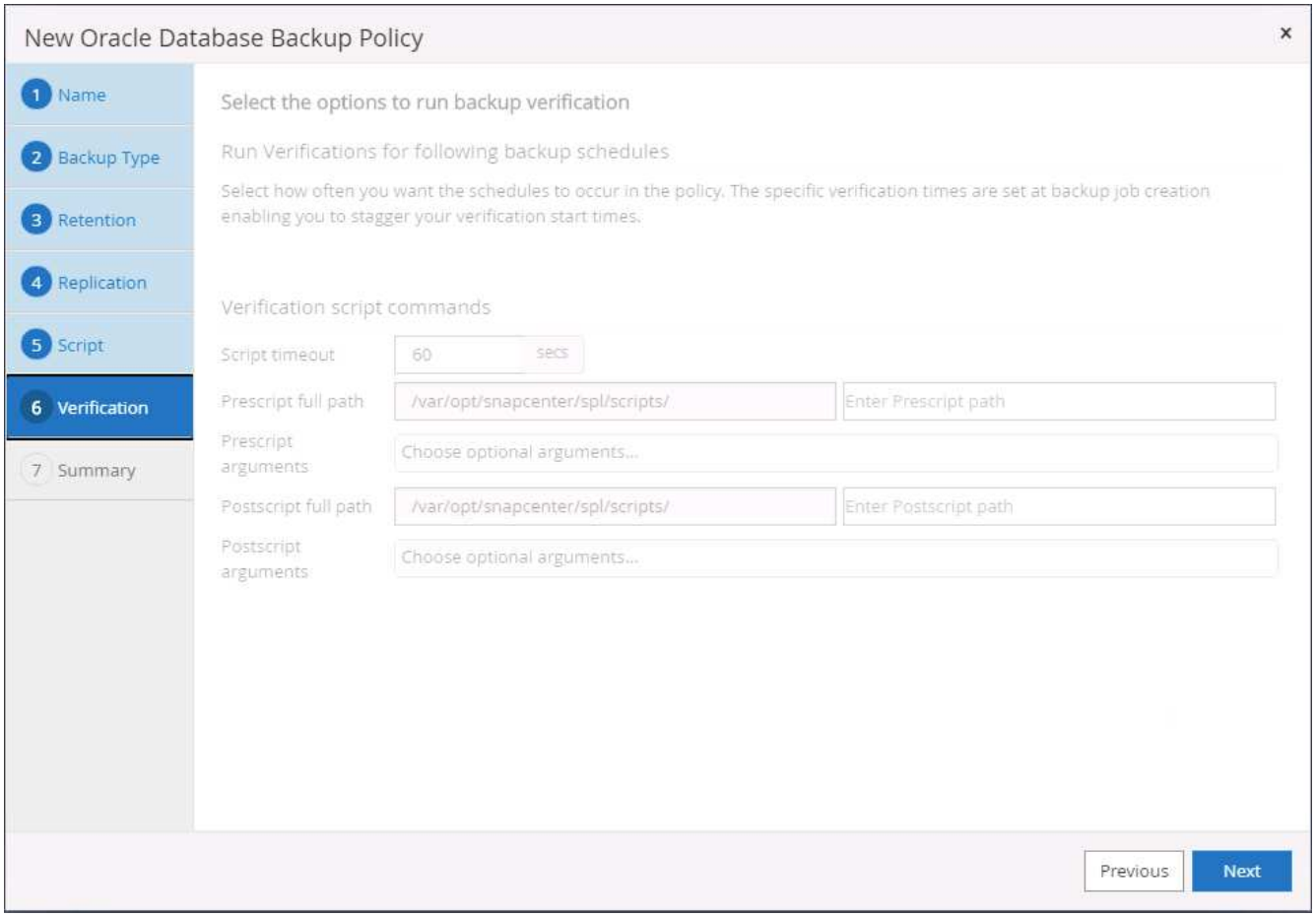
5. Habilite la replicación en una ubicación secundaria en el cloud público.



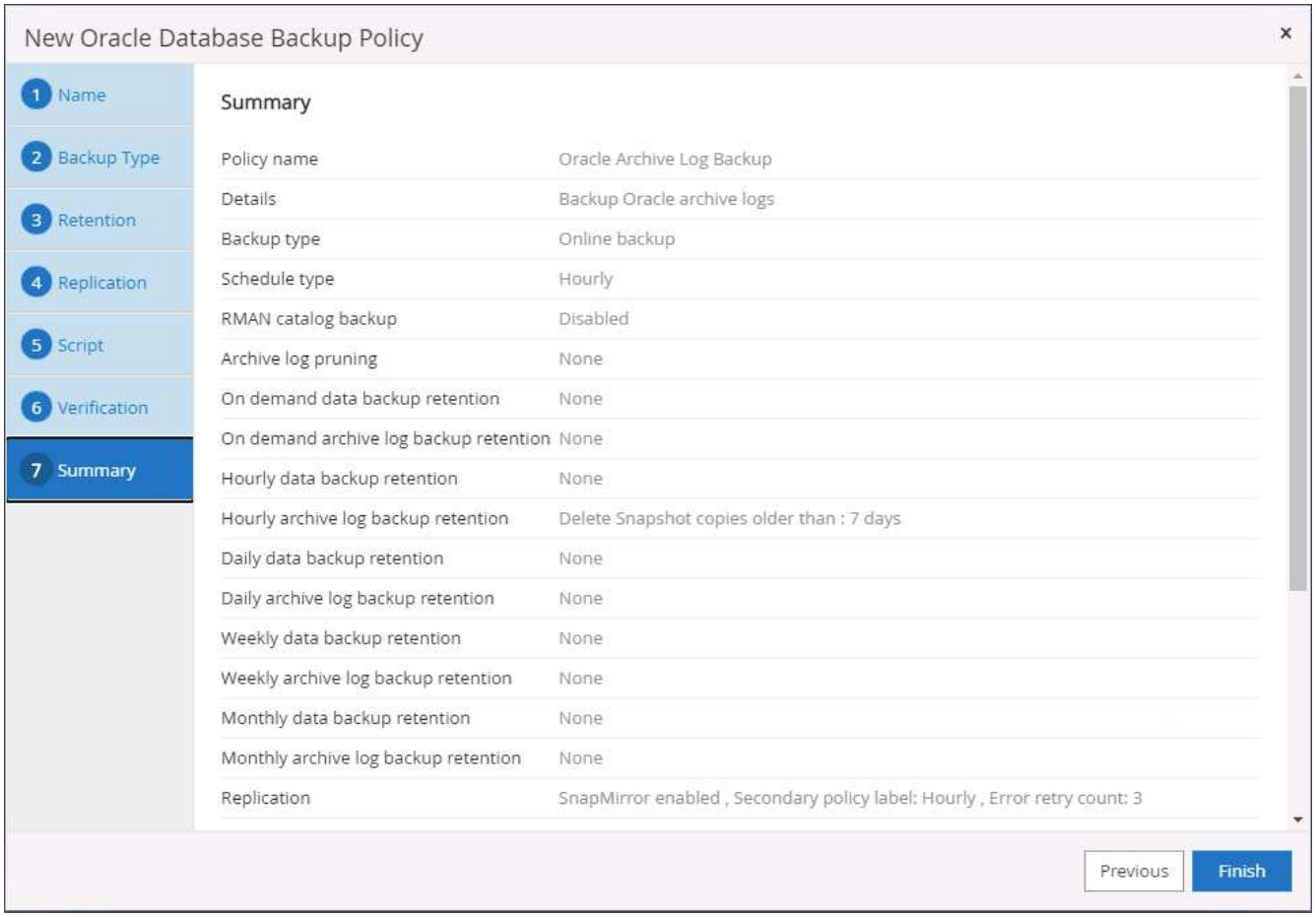
6. Especifique cualquier script opcional para ejecutar antes y después del backup de registros.



7. Especifique cualquier script de verificación de backup.

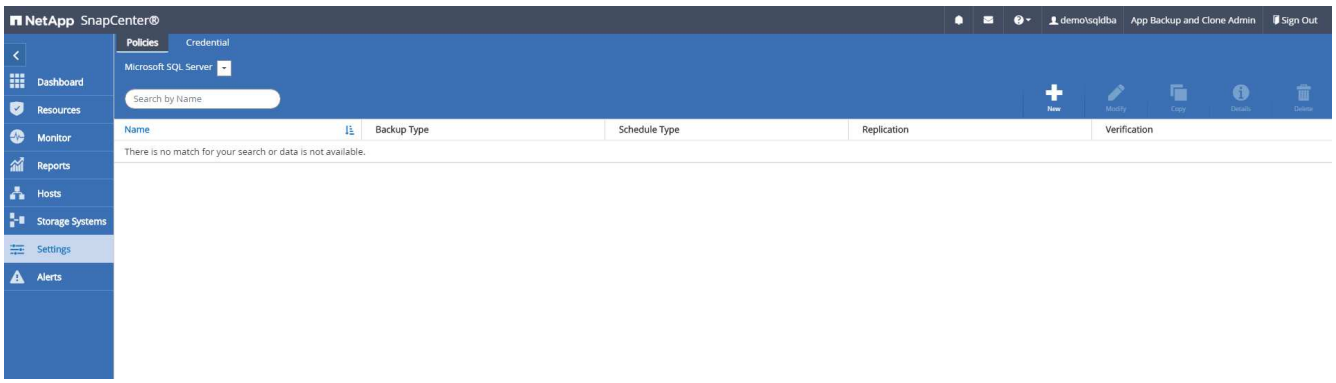

New Oracle Database Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Select the options to run backup verification
Run Verifications for following backup schedules
Select how often you want the schedules to occur in the policy. The specific verification times 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.

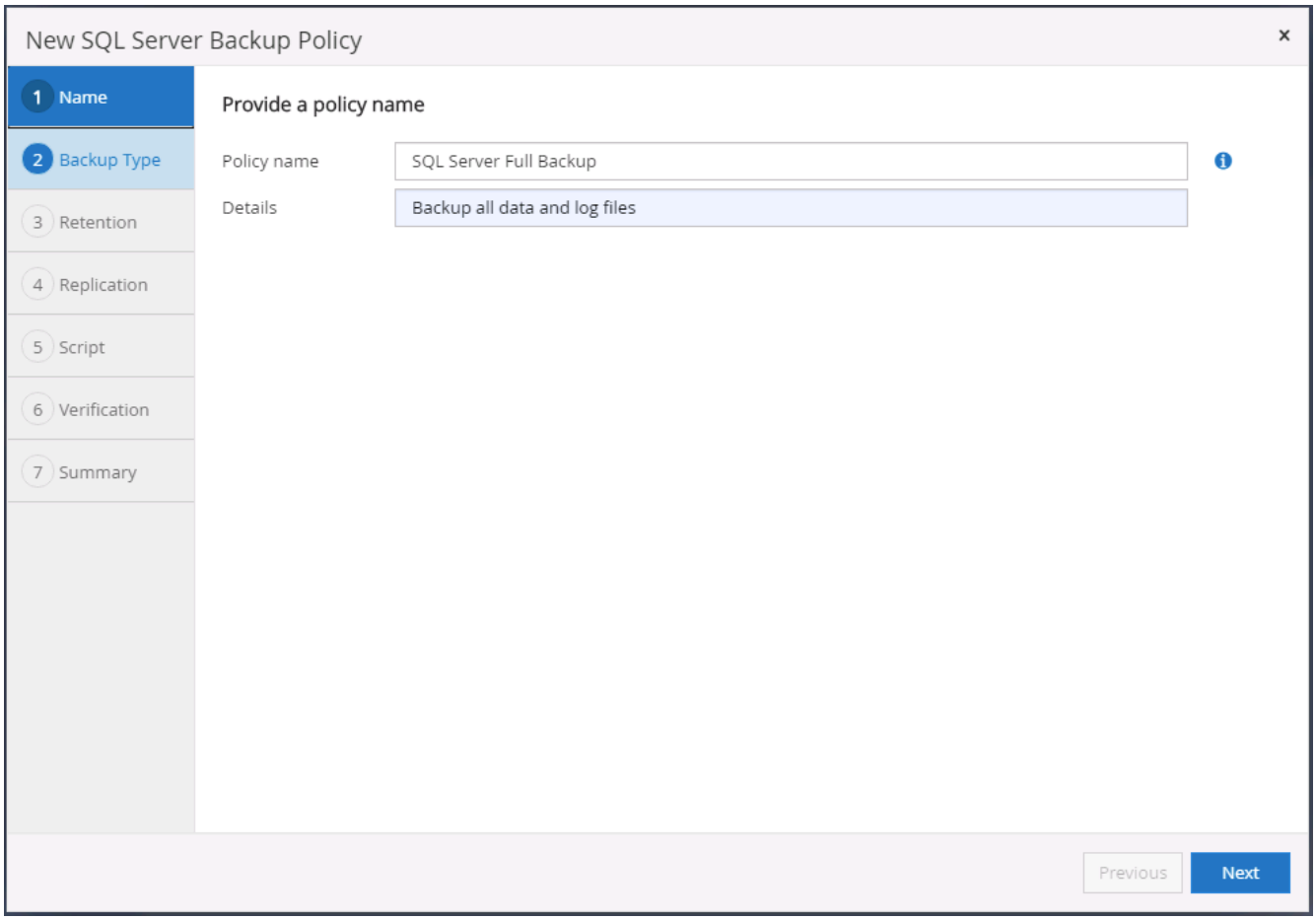


Cree una política de backup de base de datos completa para SQL

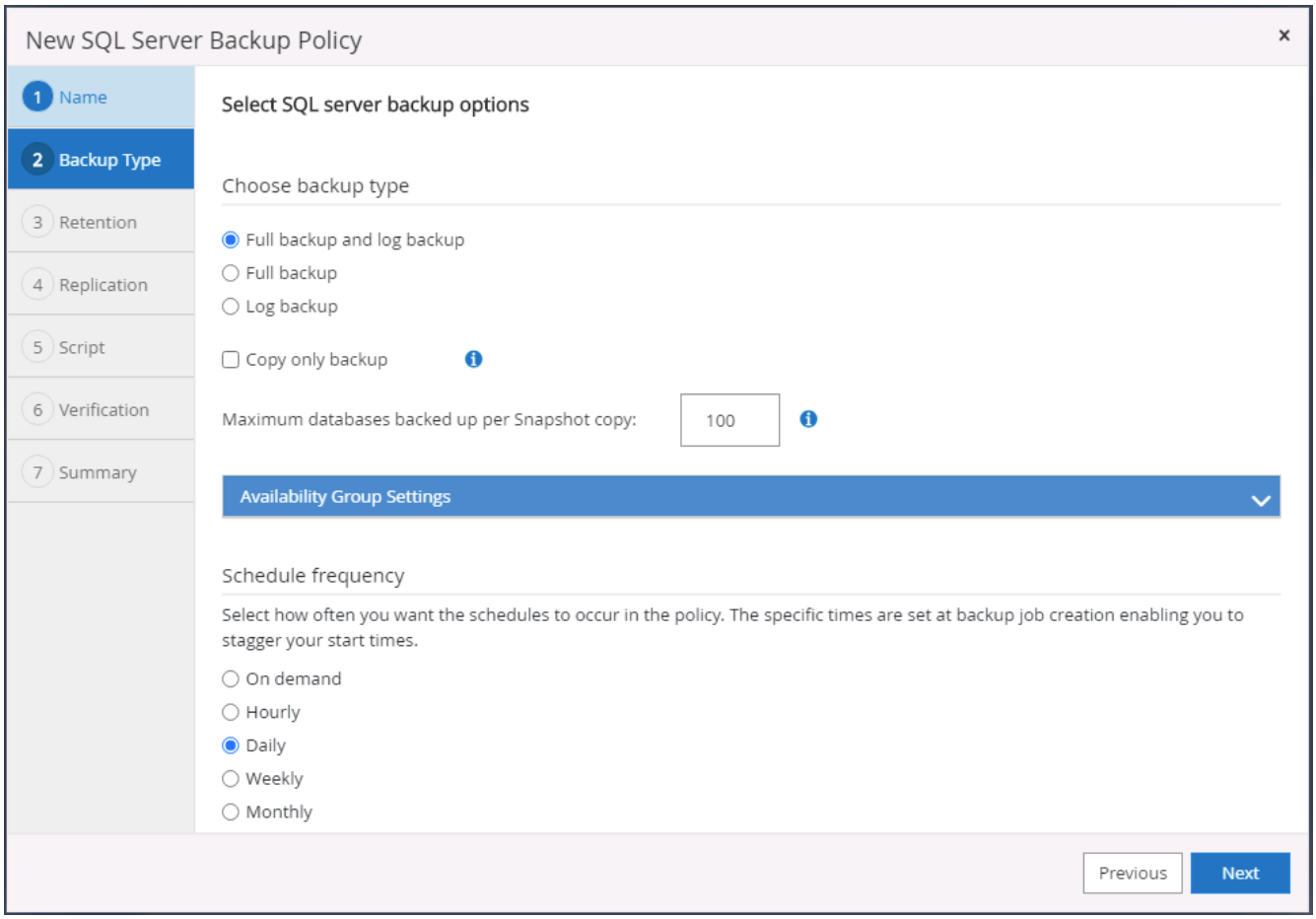
1. Inicie sesión en SnapCenter con un ID de usuario de administración de bases de datos, haga clic en Configuración y, a continuación, en políticas.



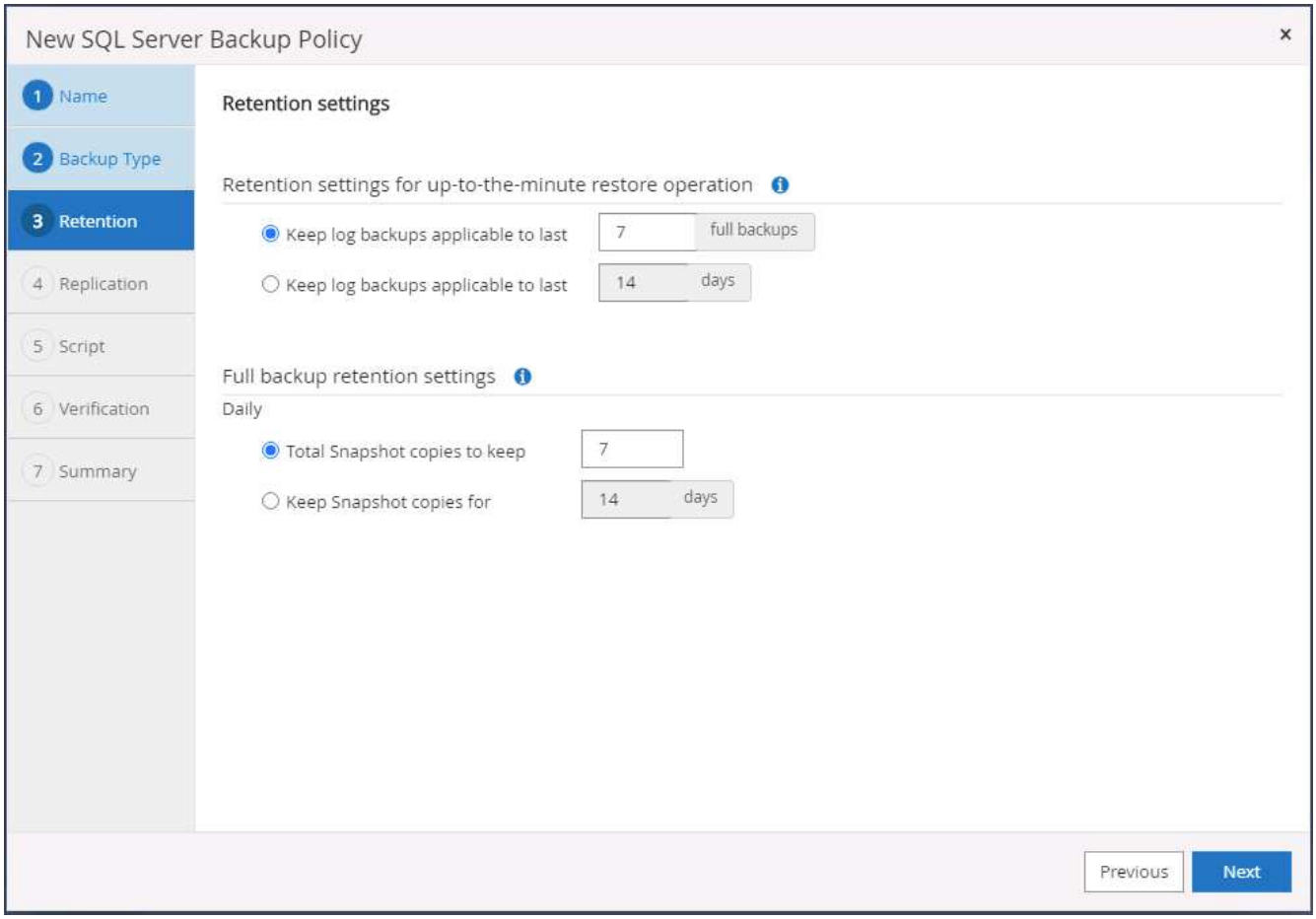
2. Haga clic en New para iniciar un nuevo flujo de trabajo de creación de políticas de backup o seleccione una política existente para modificarla.



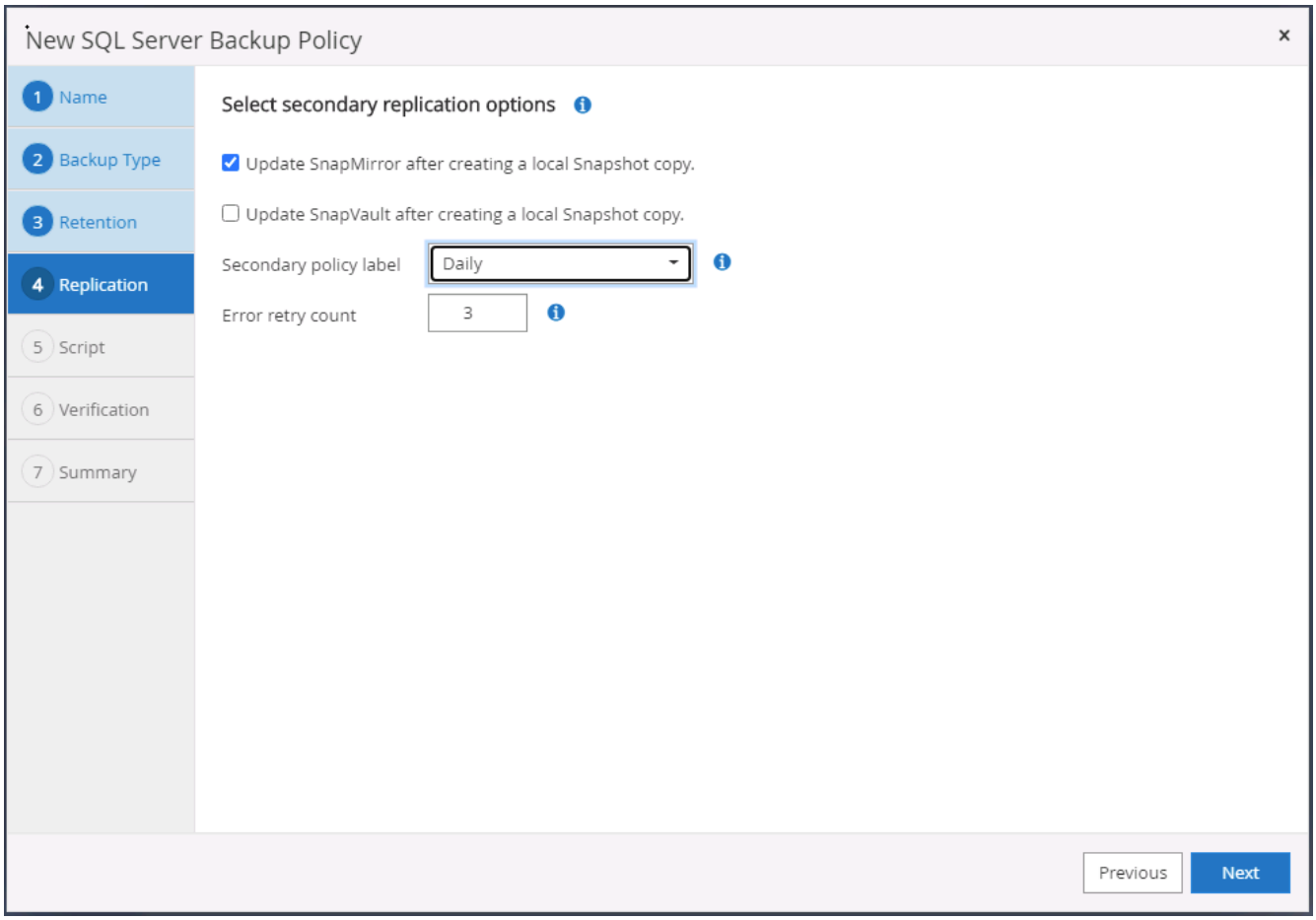
3. Defina las opciones de backup y la frecuencia de programación. Para SQL Server configurado con un grupo de disponibilidad, es posible establecer una réplica de backup preferida.



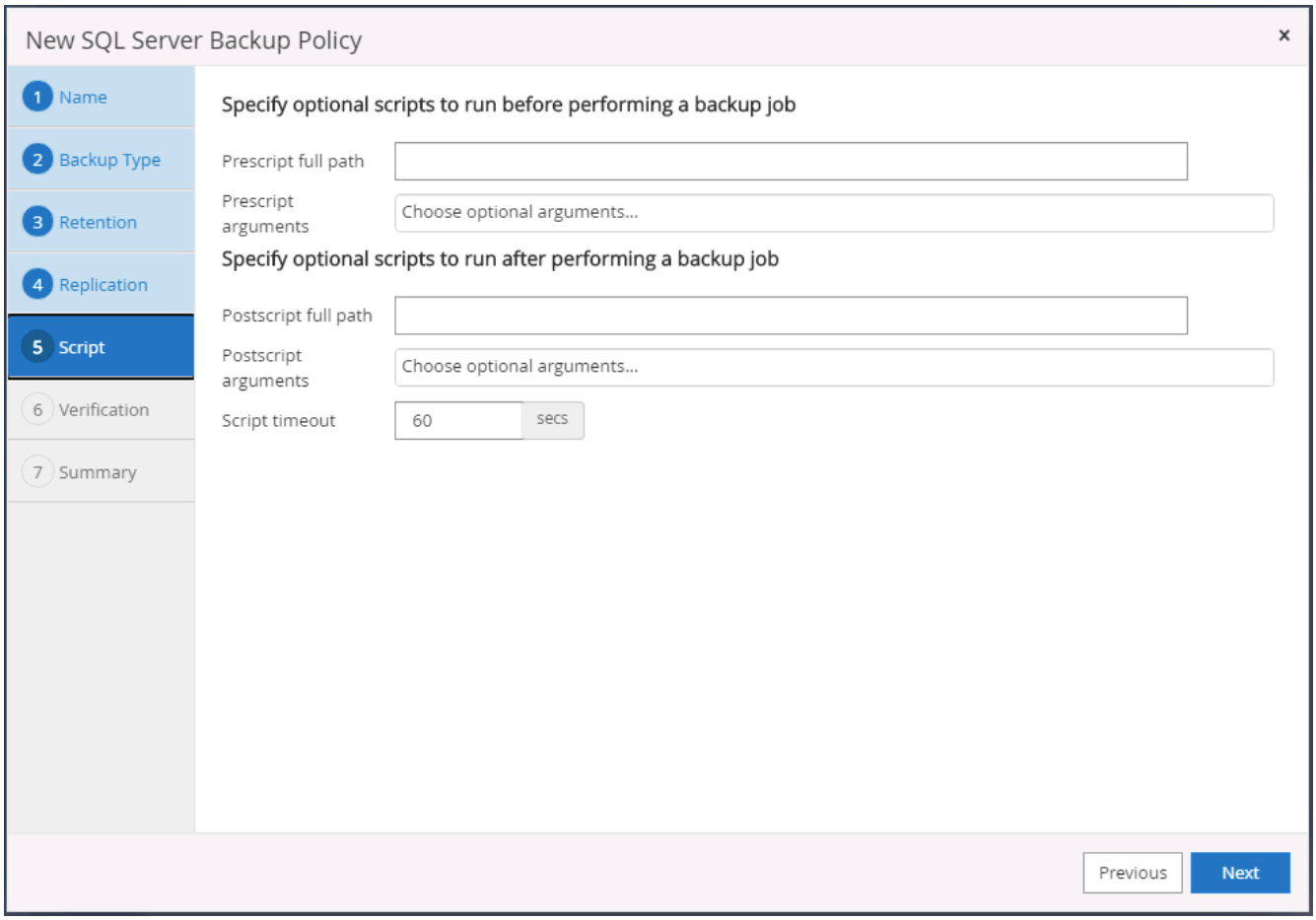
4. Establezca el período de retención de las copias de seguridad.



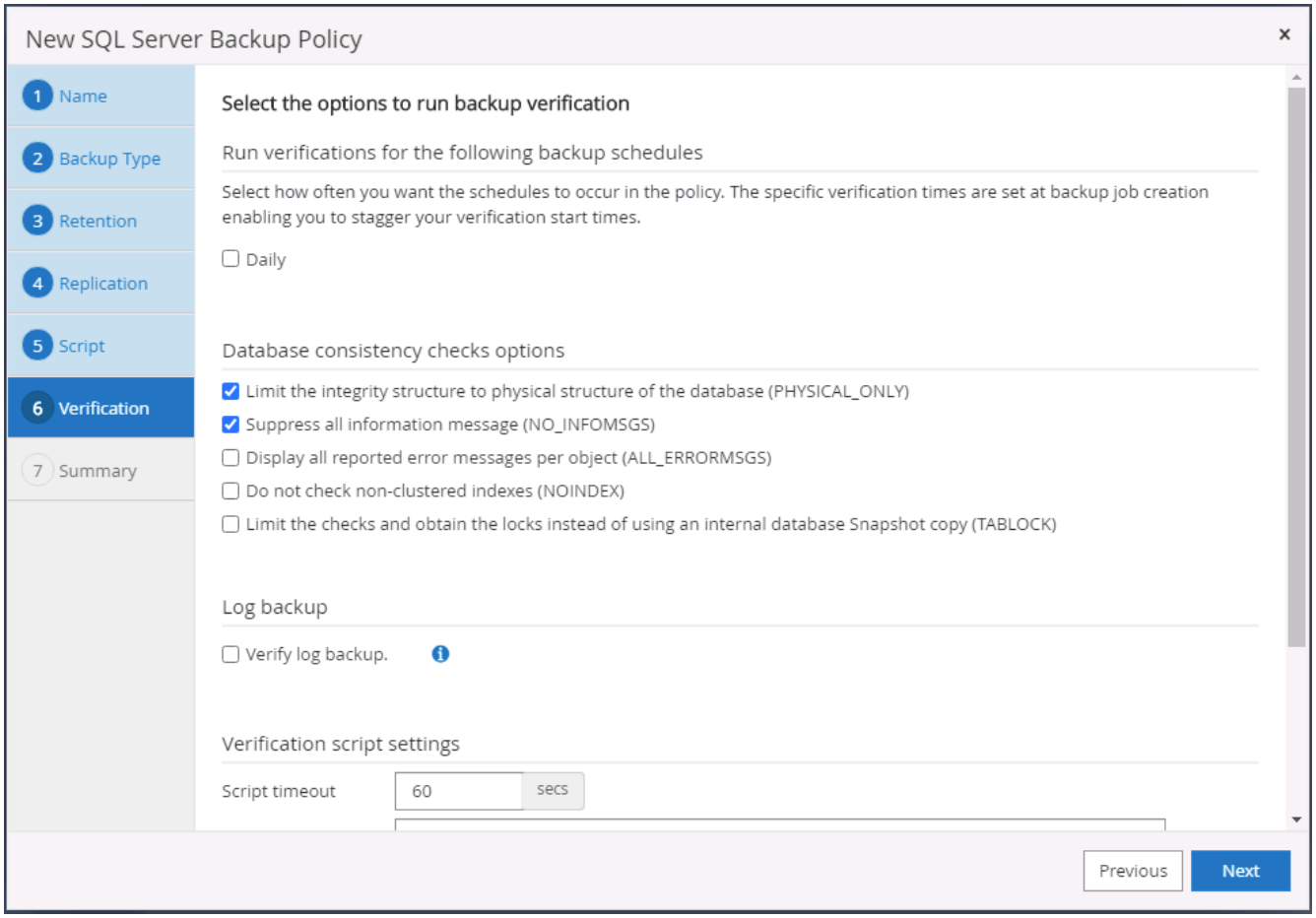
5. Habilite la replicación de copias de backup en una ubicación secundaria en el cloud.



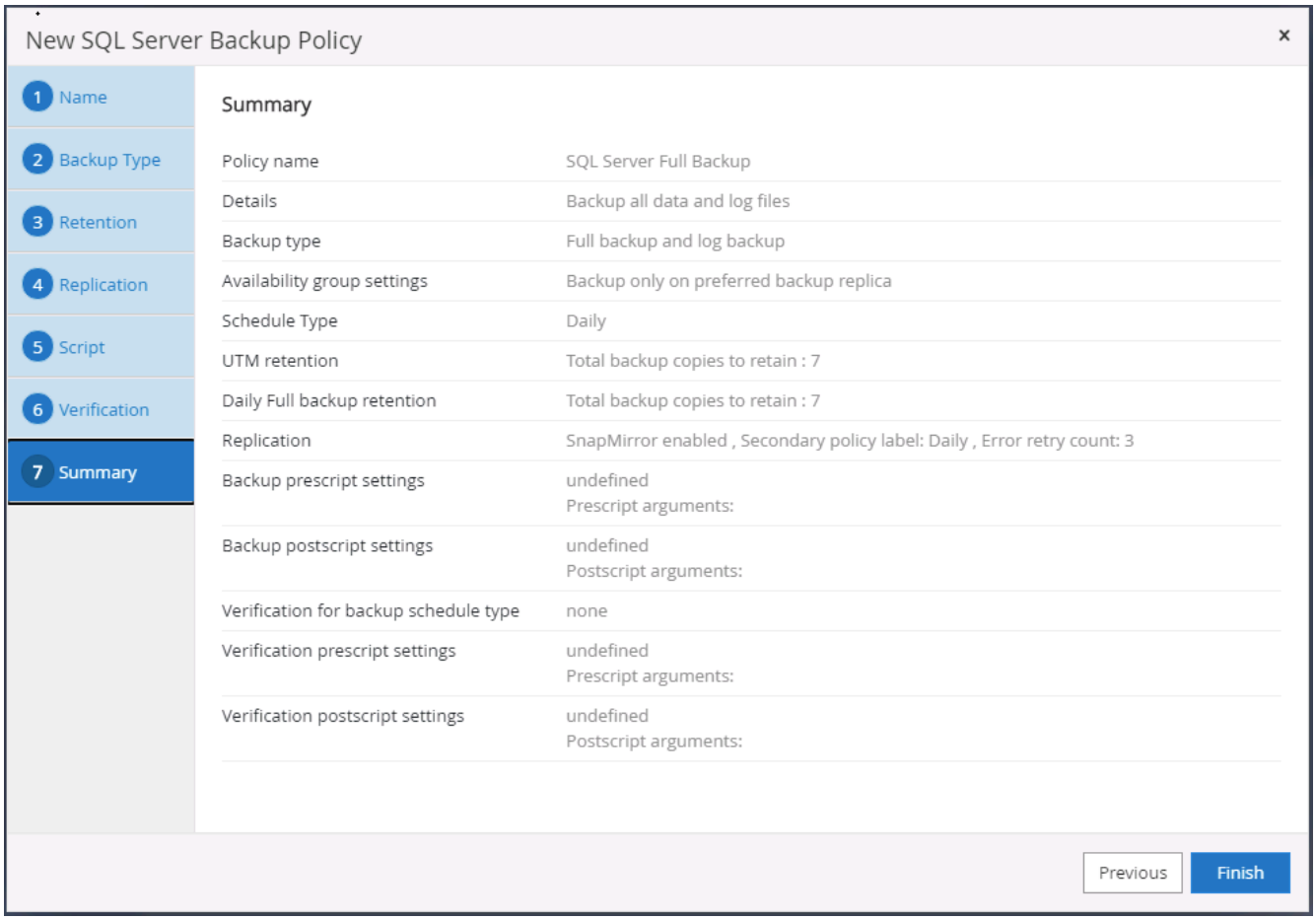
6. Especifique cualquier script opcional que se ejecute antes o después de un trabajo de backup.



7. Especifique las opciones para ejecutar la verificación de backup.

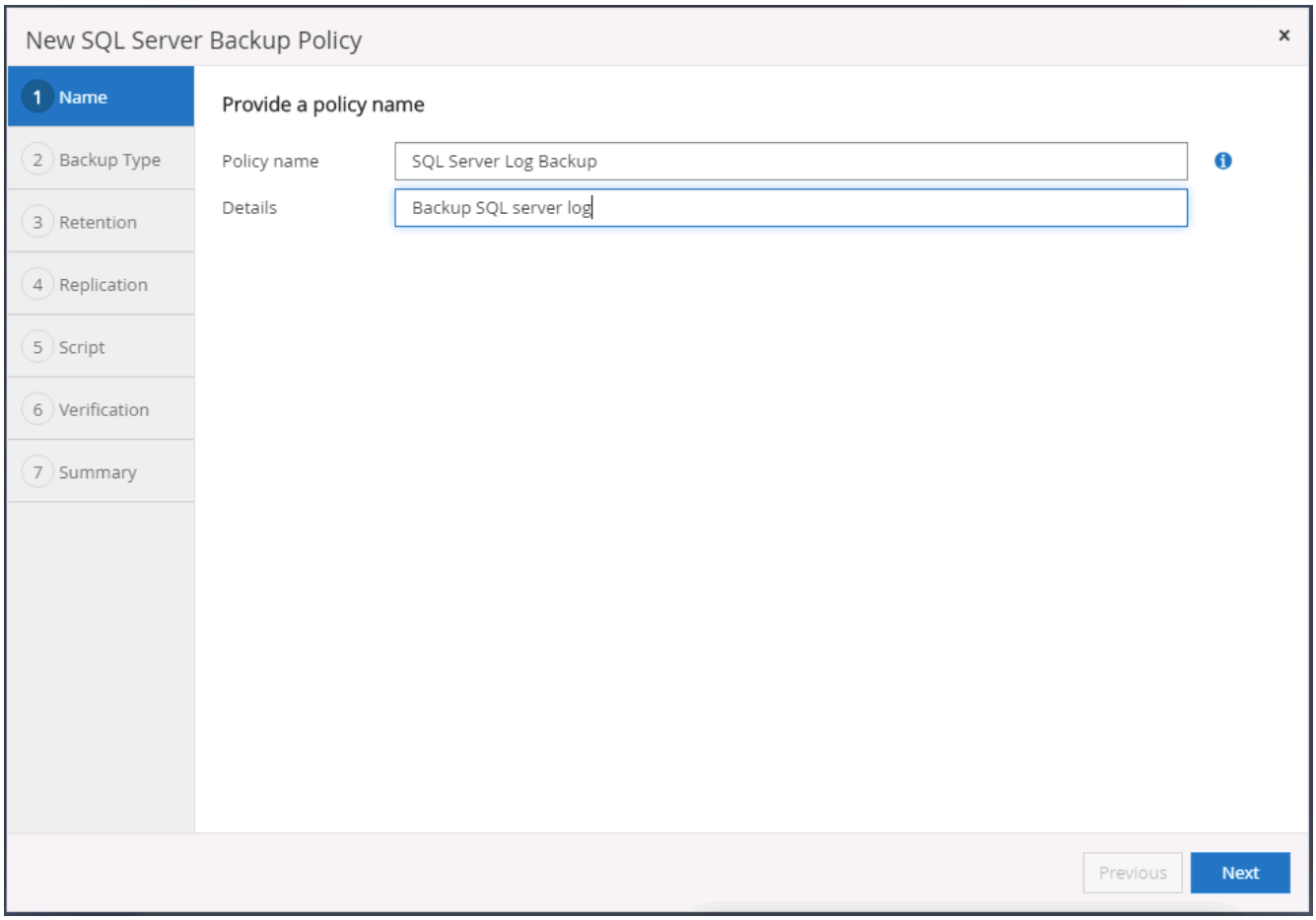

New SQL Server Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Select the options to run backup verification
Run verifications for the following backup schedules
Select how often you want the schedules to occur in the policy. The specific verification times 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_ERRORMSGS)
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
60
secs
Previous
Next

8. Resumen.

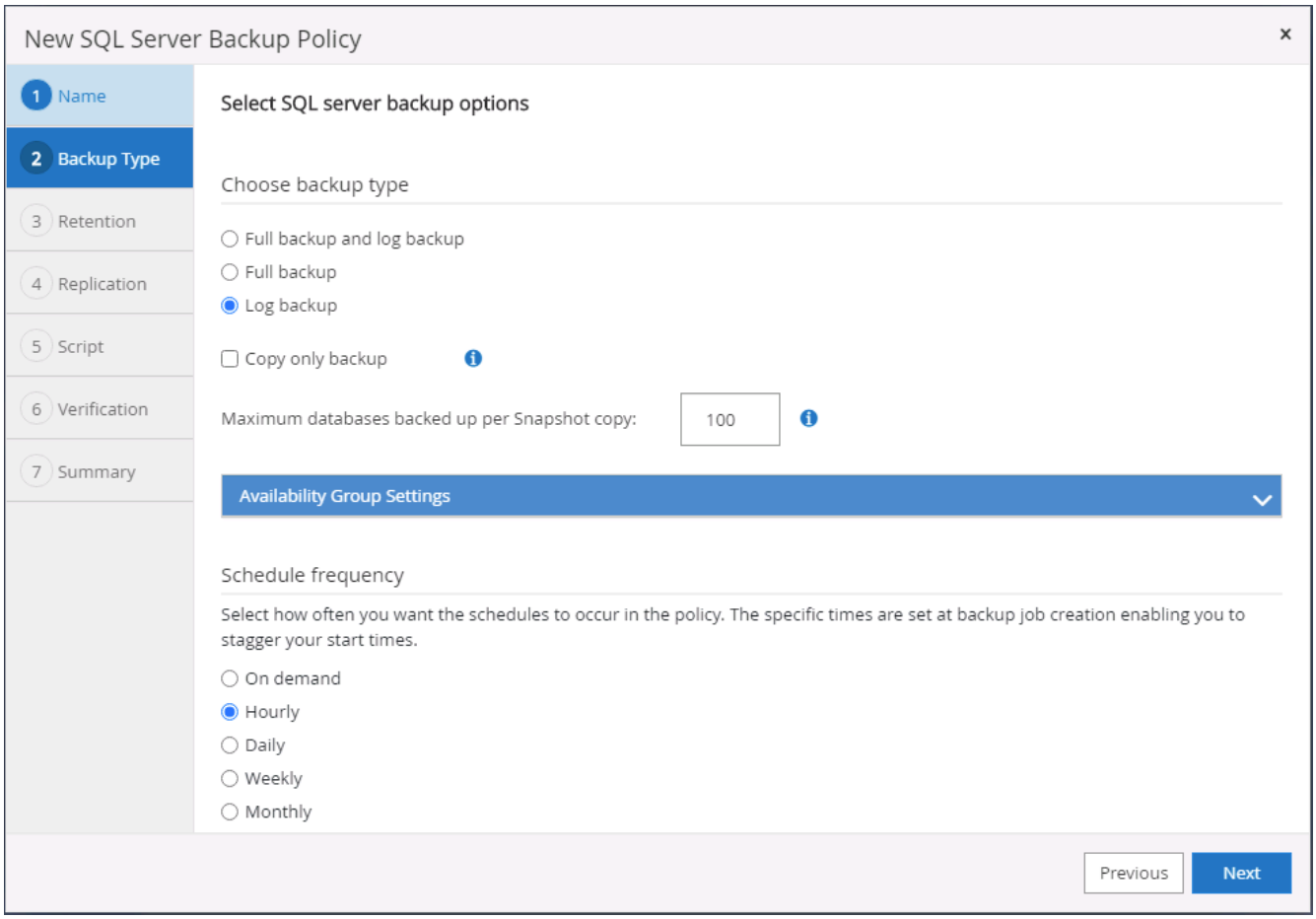


Crear una política de backup del registro de la base de datos para SQL.

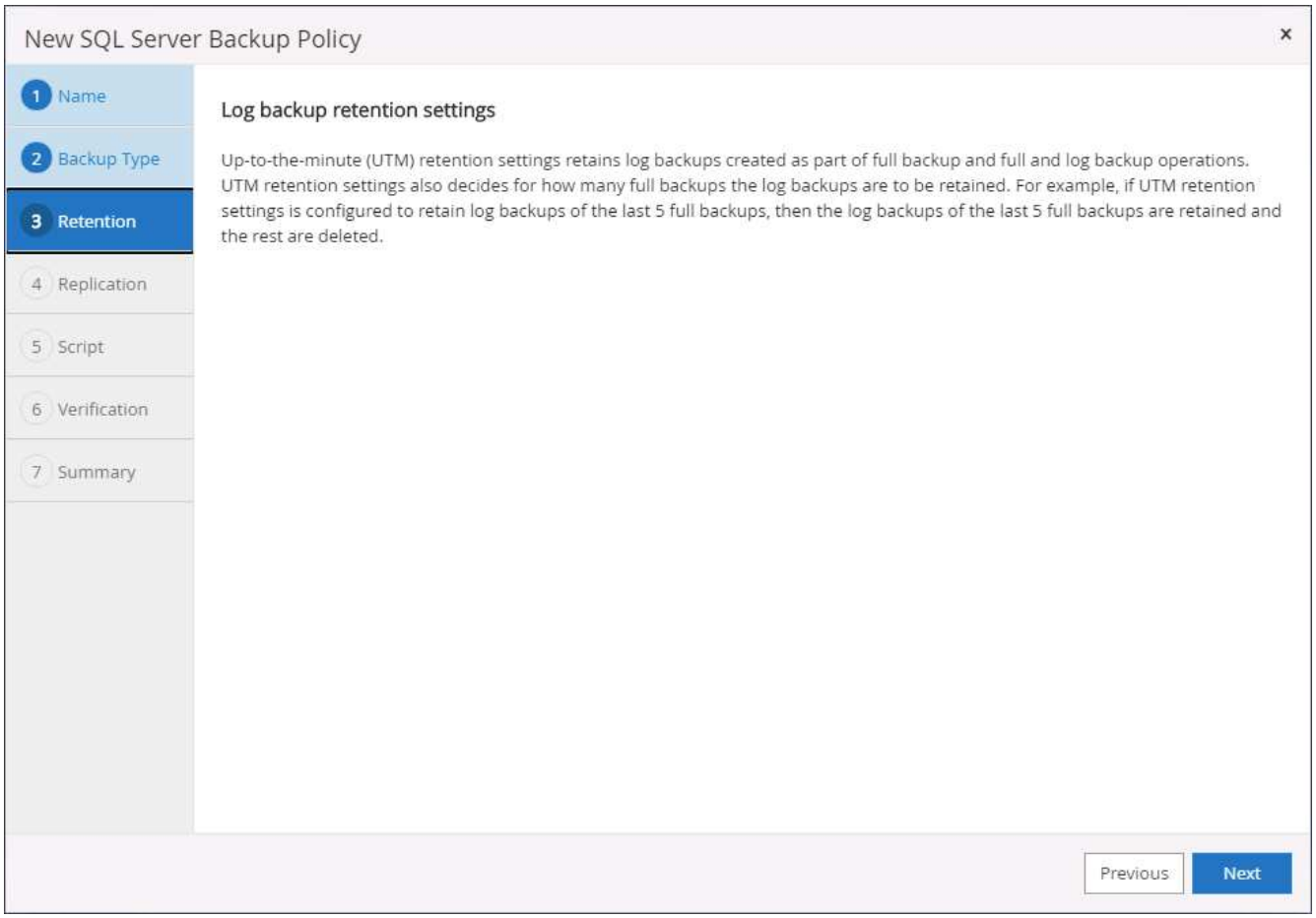
1. Inicie sesión en SnapCenter con un ID de usuario de administración de bases de datos, haga clic en Configuración > políticas y, a continuación, en Nuevo para iniciar un nuevo flujo de trabajo de creación de directivas.



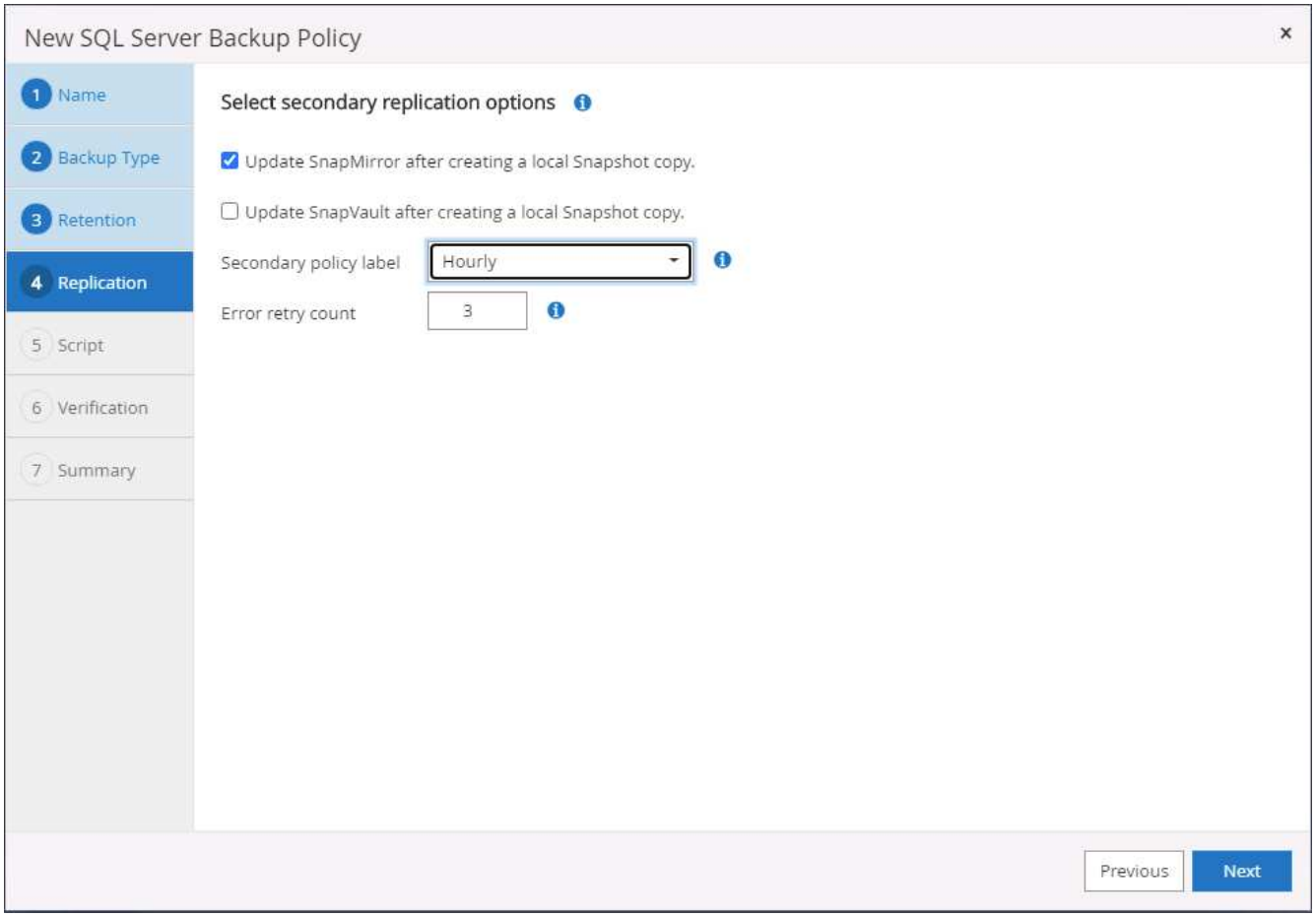
2. Defina las opciones de backup de registros y la frecuencia de programación. Para SQL Server configurado con un grupo de disponibilidad, se puede establecer una réplica de backup preferida.



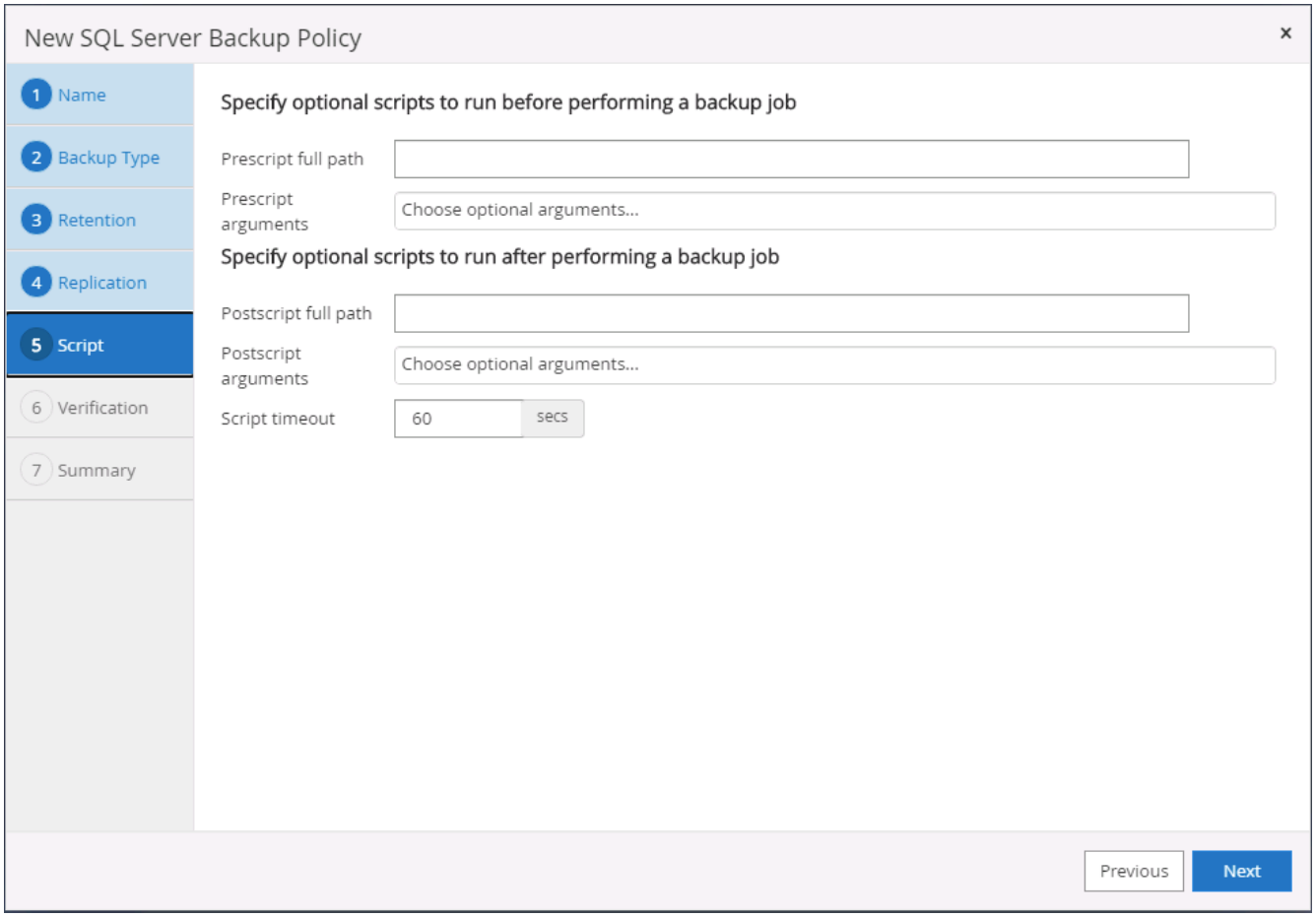
3. La política de backup de datos de SQL Server define la retención de backup de registros; acepte los valores predeterminados aquí.



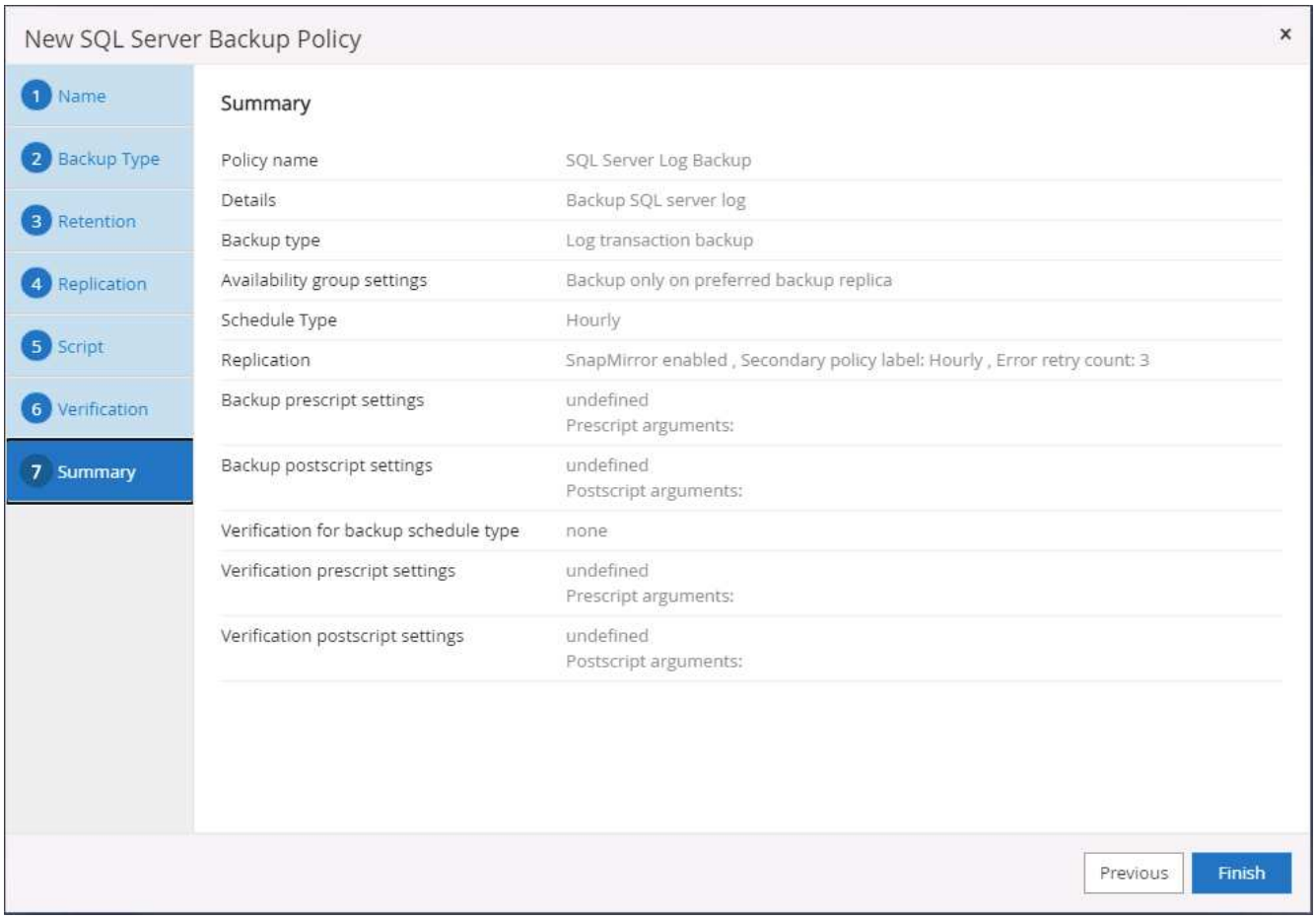
4. Habilite la replicación de backups de registros en almacenamiento secundario en el cloud.



5. Especifique cualquier script opcional que se ejecute antes o después de un trabajo de backup.


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
Choose optional arguments...
Specify optional scripts to run after performing a backup job
Postscript full path
Postscript arguments
Choose optional arguments...
Script timeout
60
secs
Previous
Next

6. Resumen.

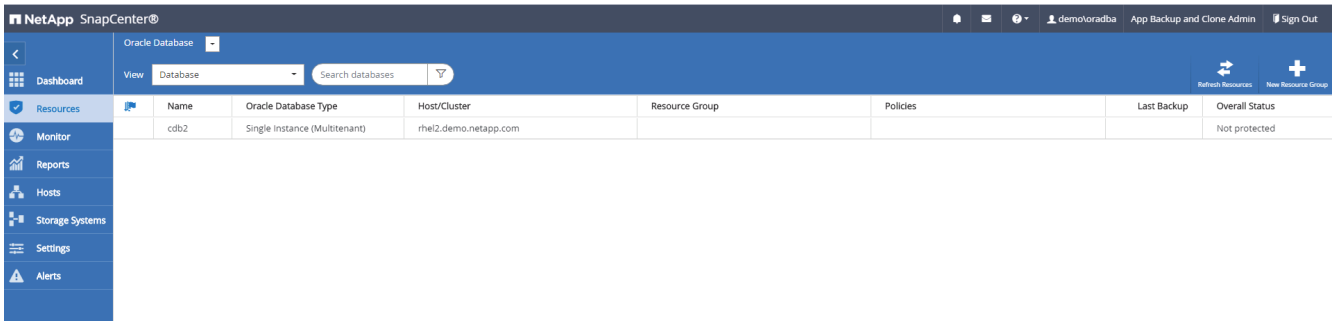


8. Implementar la política de copia de seguridad para proteger la base de datos

SnapCenter utiliza un grupo de recursos para realizar el backup 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 admiten una aplicación empresarial, etc. Proteger una sola base de datos crea un grupo de recursos propio. Los siguientes procedimientos muestran cómo implementar una política de backup creada en la sección 7 para proteger las bases de datos de Oracle y SQL Server.

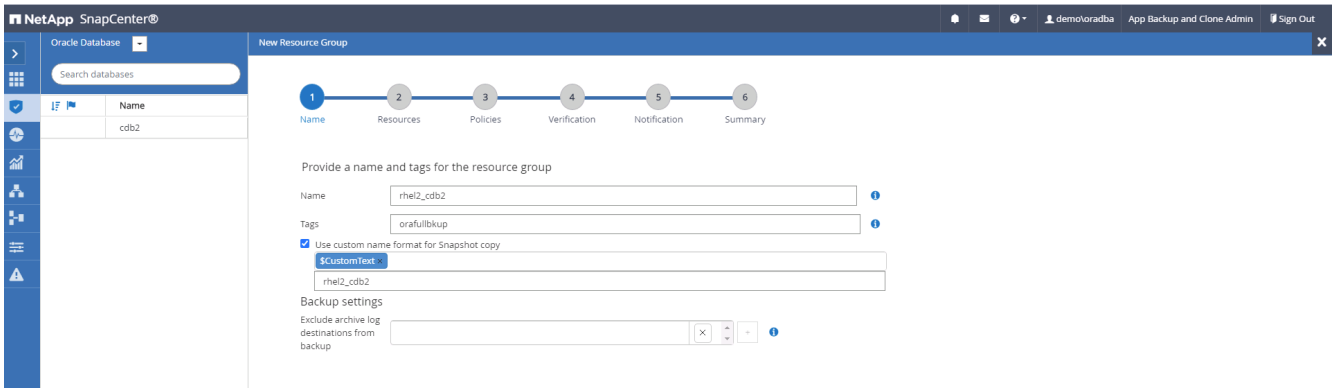
Cree un grupo de recursos para un backup completo de Oracle

1. Inicie sesión en SnapCenter con un ID de usuario de gestión de bases de datos y vaya a la pestaña Resources. En la lista desplegable View, seleccione Database o Resource Group para iniciar el flujo de trabajo de creación de grupos de recursos.

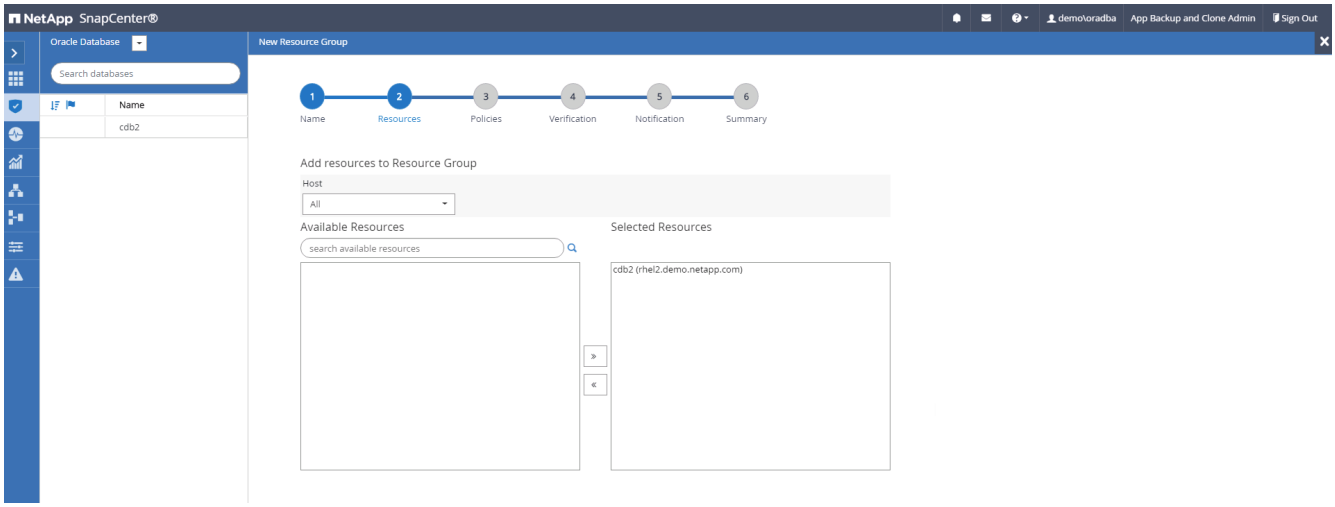


2. Proporcione un nombre y etiquetas para el grupo de recursos. Puede definir un formato de nomenclatura

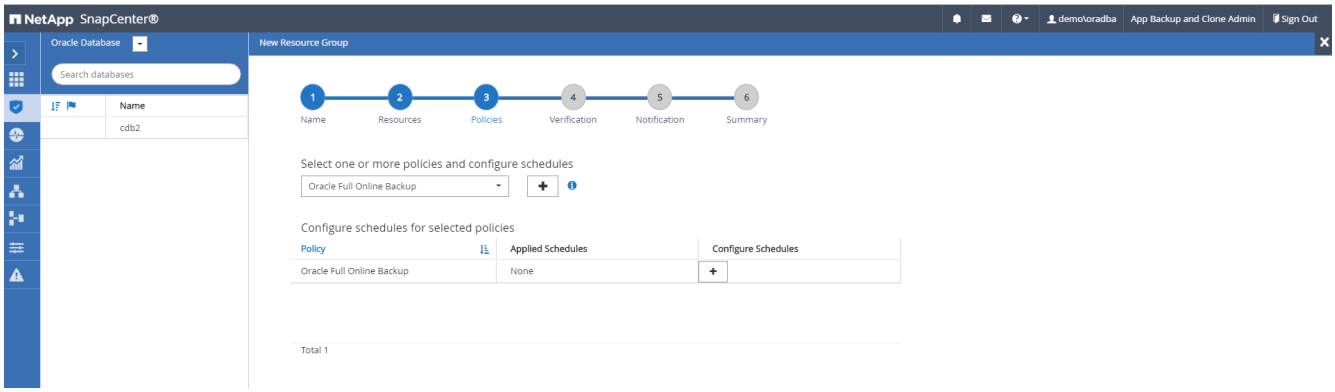
para la copia Snapshot y omitir el destino de registro de archivos redundante, si se ha configurado.



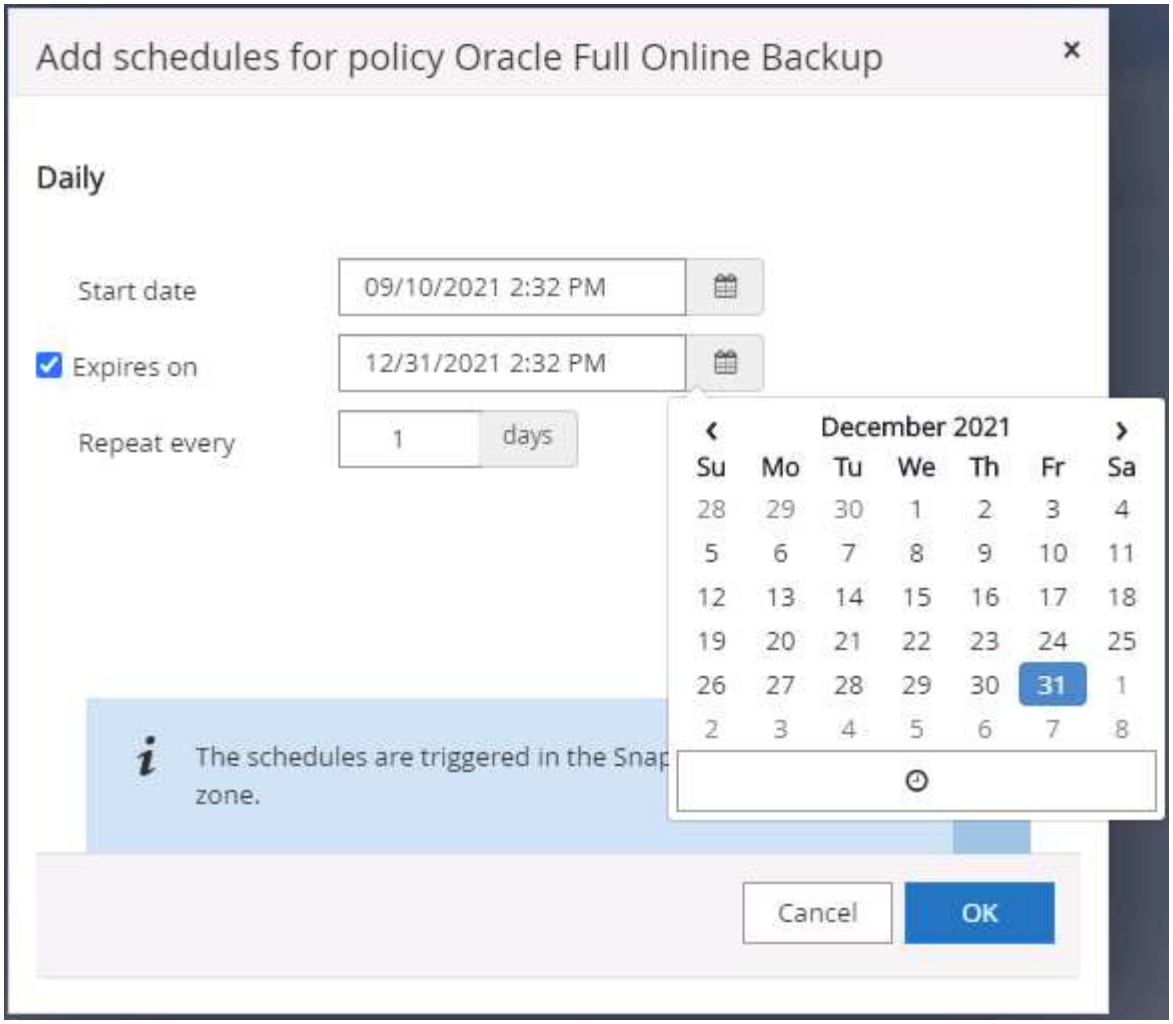
3. Añada los recursos de la base de datos al grupo de recursos.



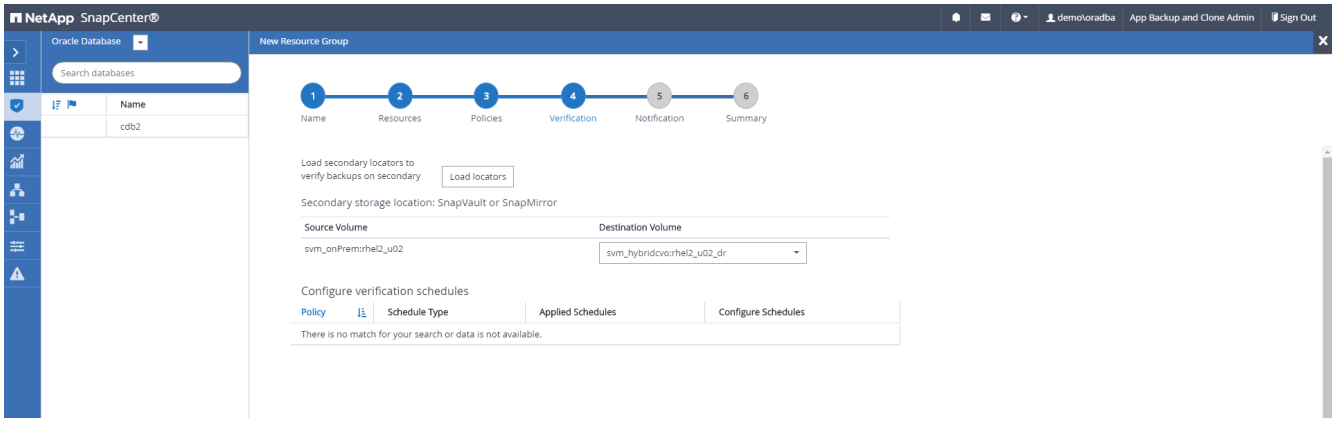
4. Seleccione una política de backup completa creada en la sección 7 de la lista desplegable.



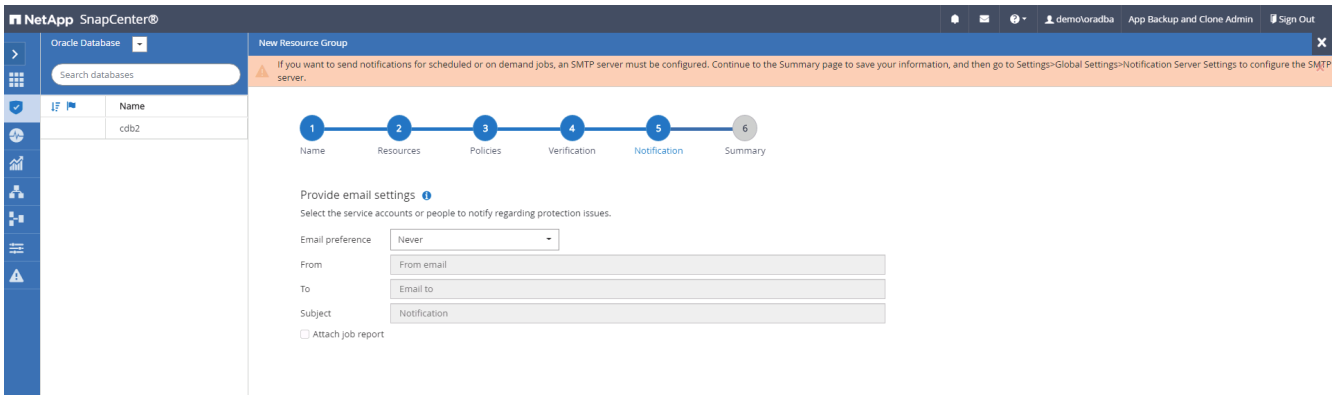
5. Haga clic en el signo (+) para configurar la programación de copia de seguridad deseada.



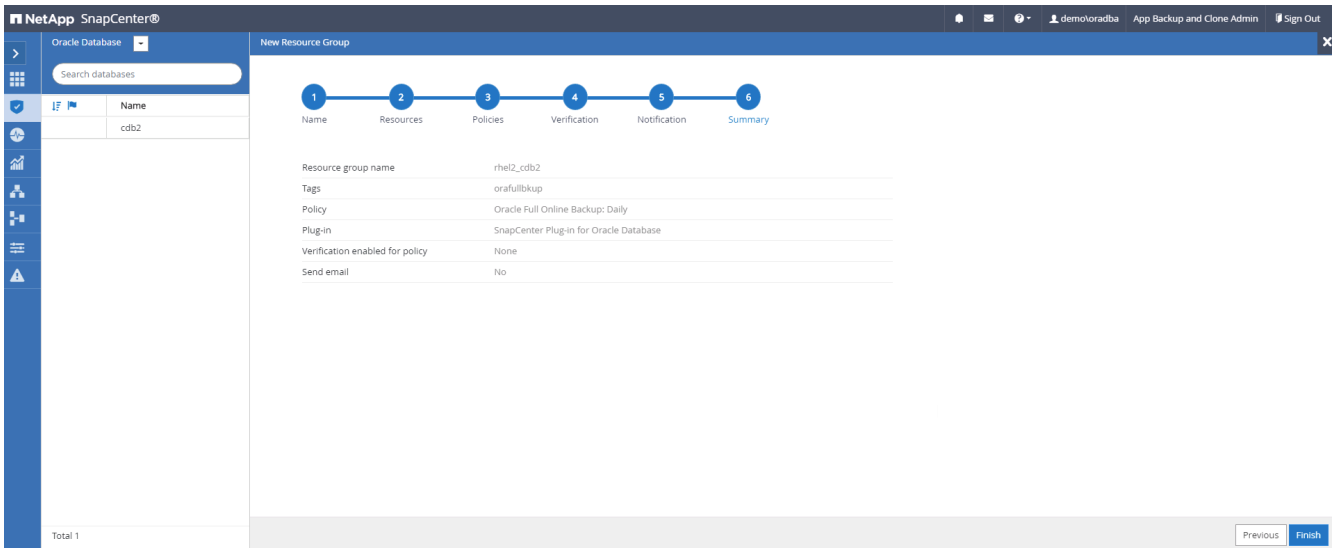
6. Haga clic en Load Locators para cargar el volumen de origen y destino.



7. Configure el servidor SMTP para la notificación por correo electrónico si lo desea.

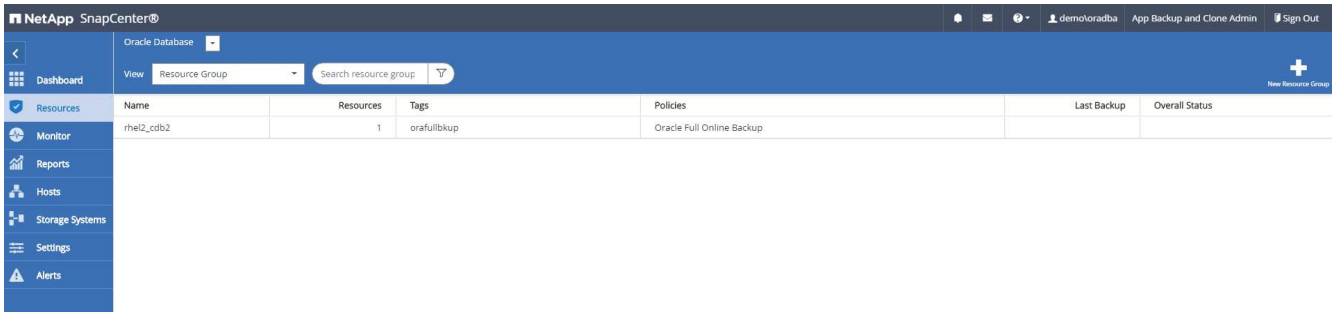


8. Resumen.

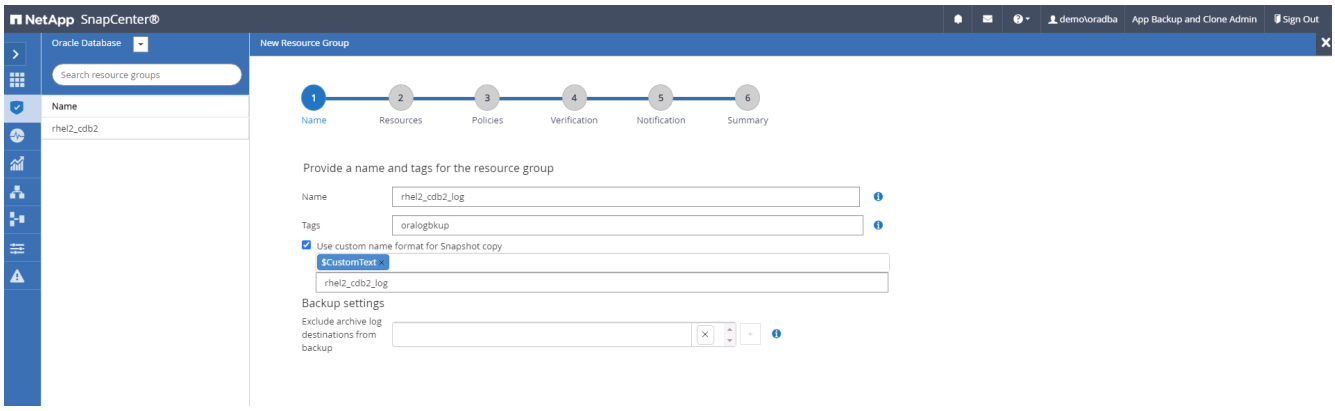


Cree un grupo de recursos para el backup de registros de Oracle

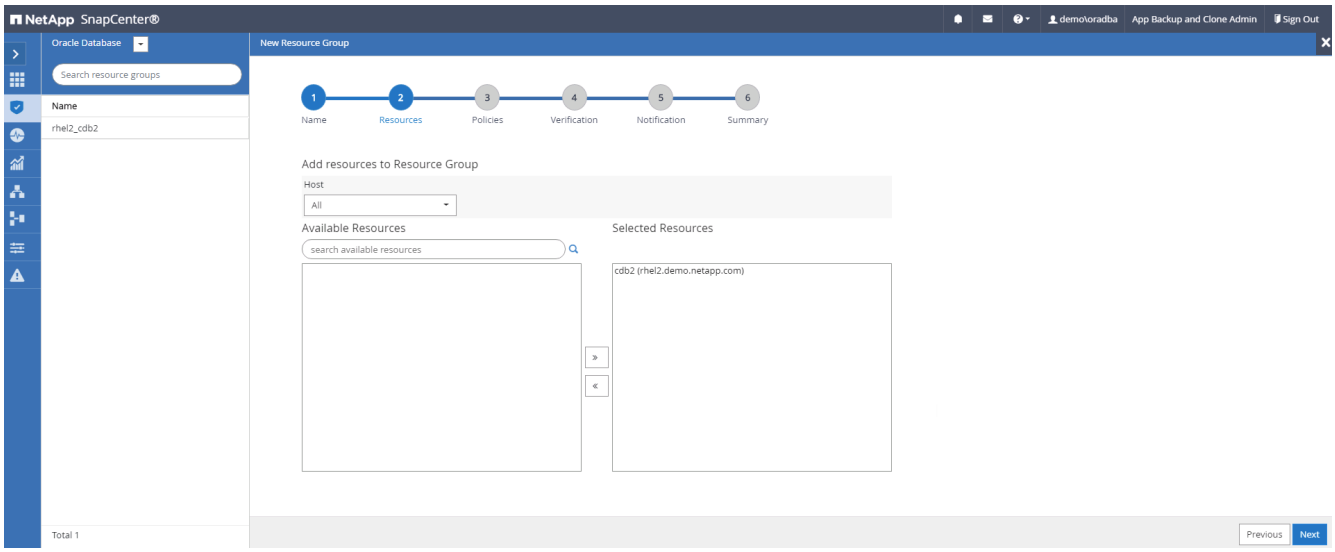
1. Inicie sesión en SnapCenter con un ID de usuario de gestión de bases de datos y vaya a la pestaña Resources. En la lista desplegable View, seleccione Database o Resource Group para iniciar el flujo de trabajo de creación de grupos de recursos.



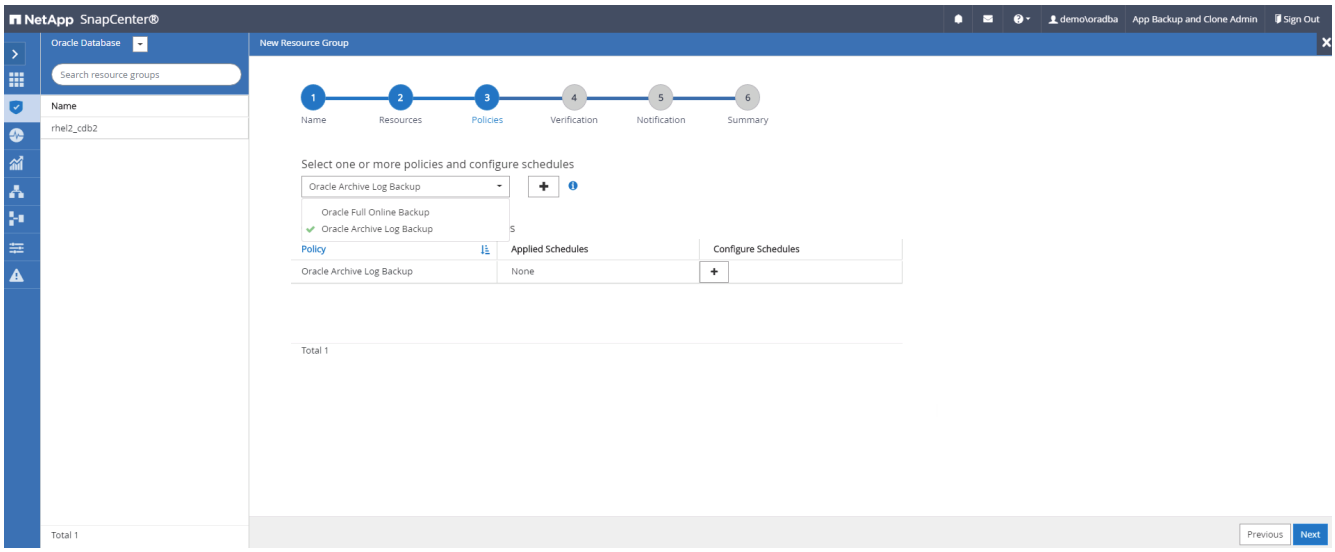
2. Proporcione un nombre y etiquetas para el grupo de recursos. Puede definir un formato de nomenclatura para la copia Snapshot y omitir el destino de registro de archivos redundante, si se ha configurado.



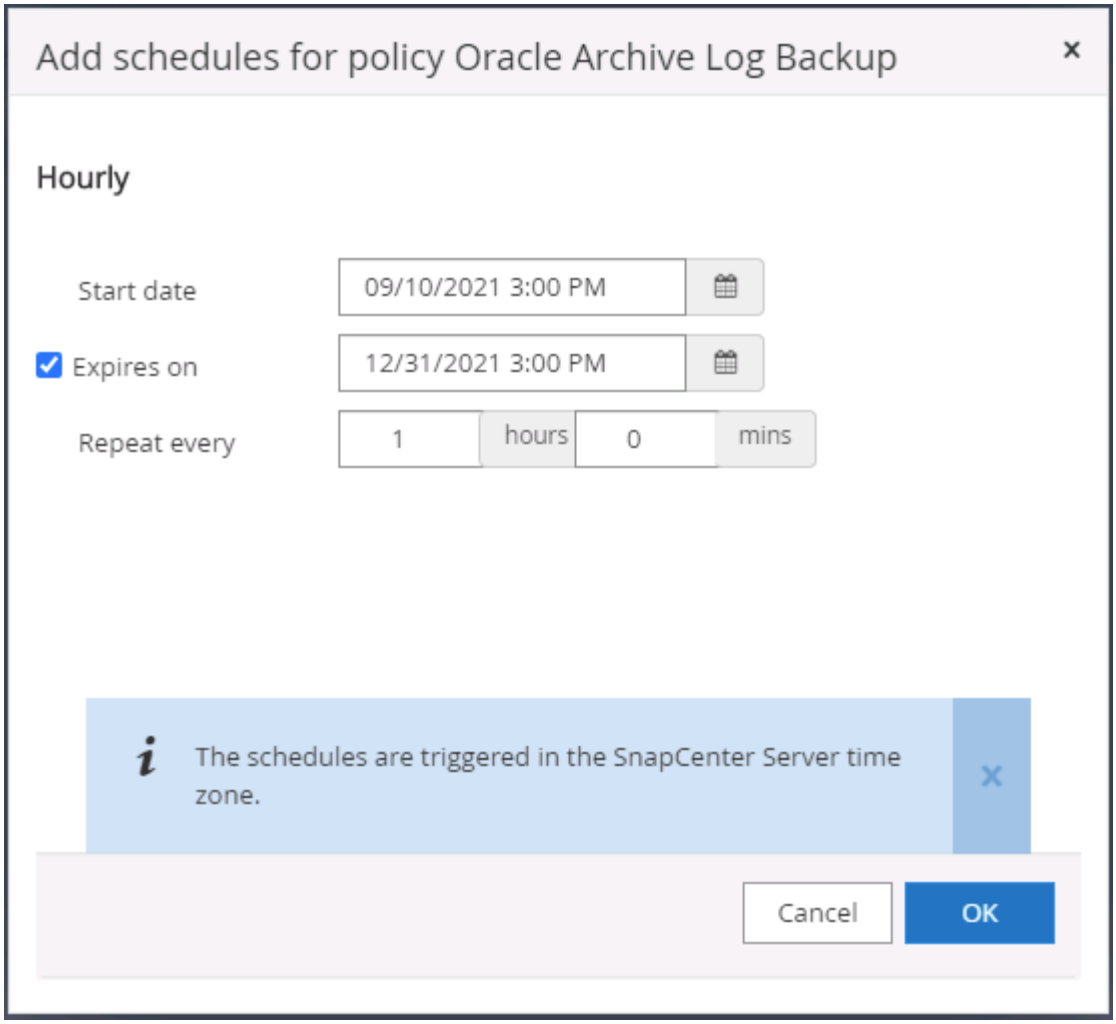
3. Añada los recursos de la base de datos al grupo de recursos.



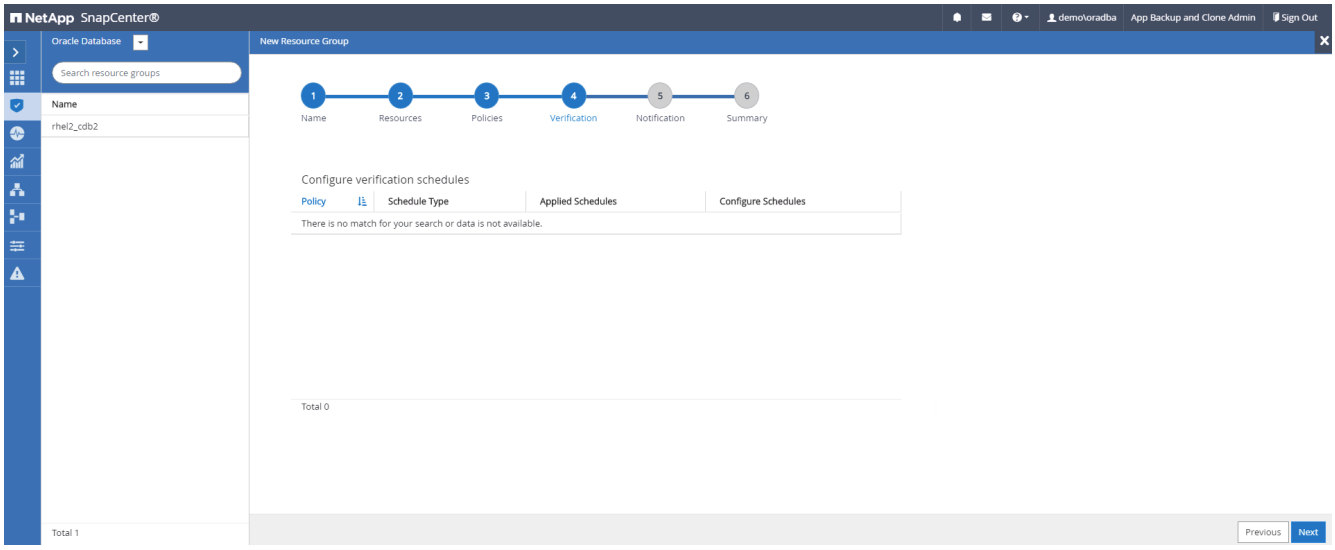
4. Seleccione una política de backup de registros creada en la sección 7 de la lista desplegable.



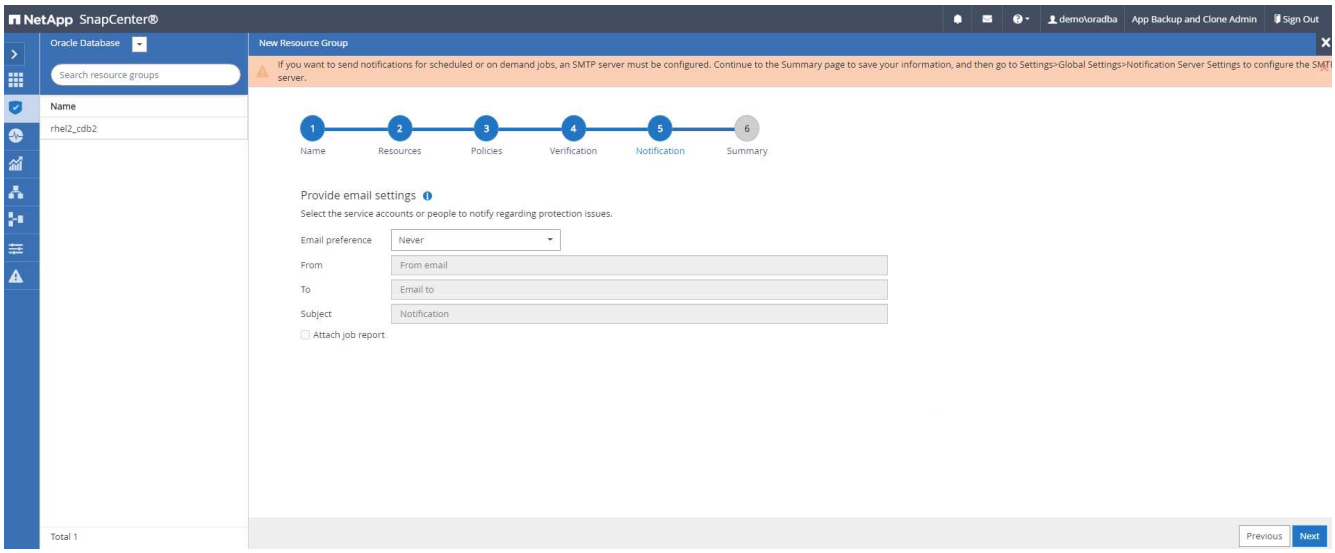
5. Haga clic en el signo (+) para configurar la programación de copia de seguridad deseada.



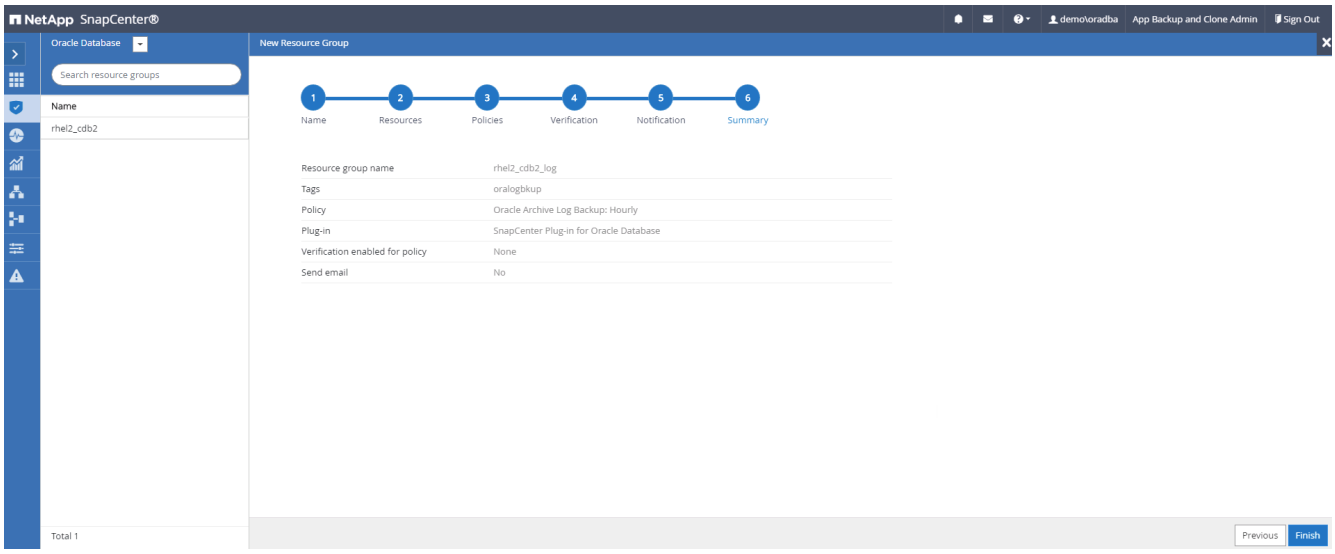
6. Si la verificación del backup está configurada, se muestra aquí.



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

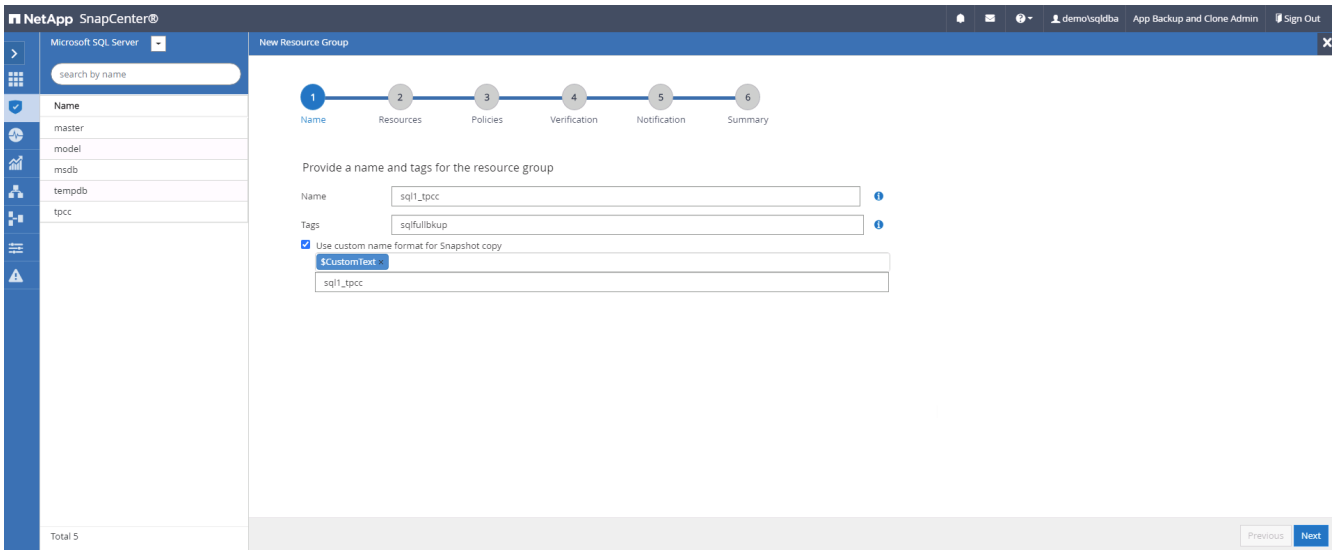


8. Resumen.

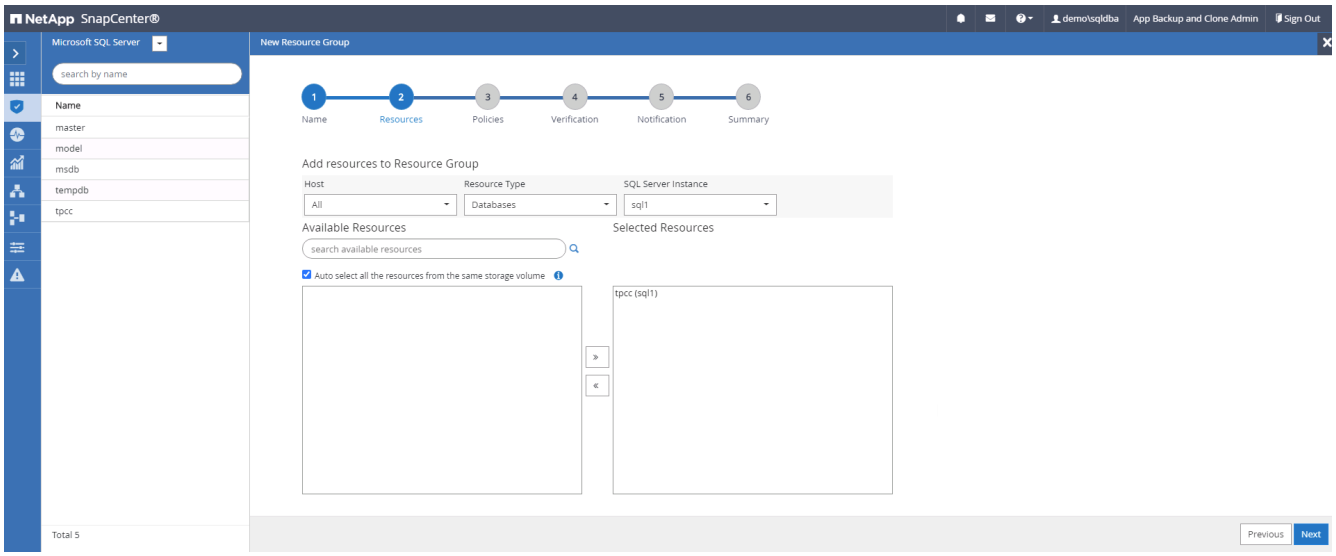


Cree un grupo de recursos para backup completo de SQL Server

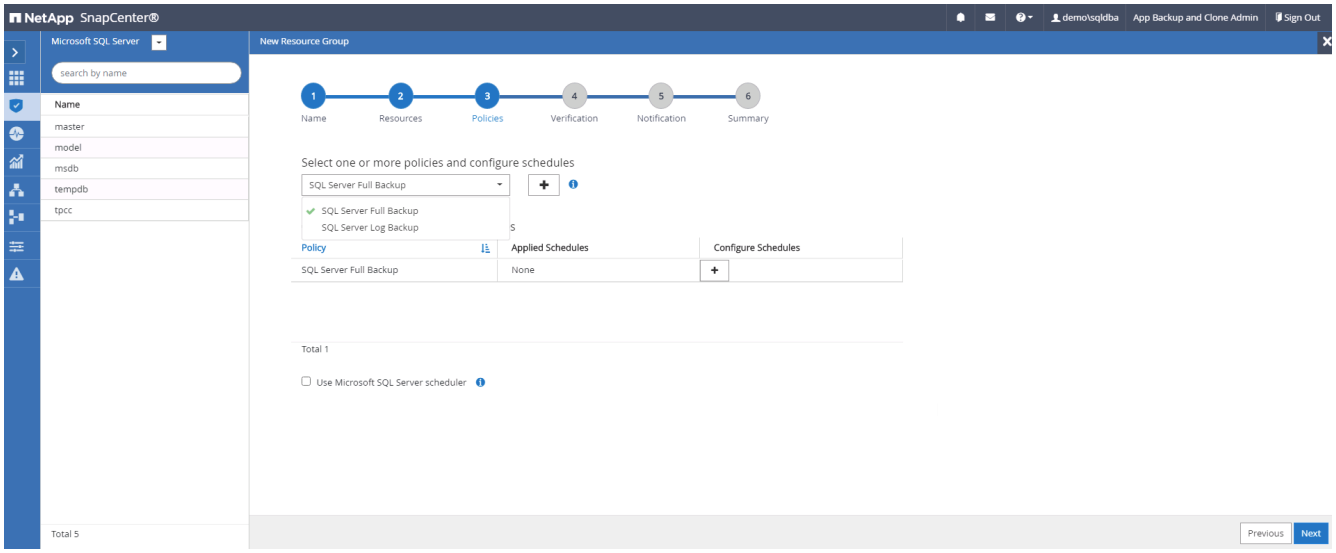
1. Inicie sesión en SnapCenter con un ID de usuario de gestión de bases de datos y vaya a la pestaña Resources. En la lista desplegable View, seleccione una base de datos o un grupo de recursos para iniciar el flujo de trabajo de creación de grupo de recursos. Proporcione un nombre y etiquetas para el grupo de recursos. Puede definir un formato de nomenclatura para la copia Snapshot.



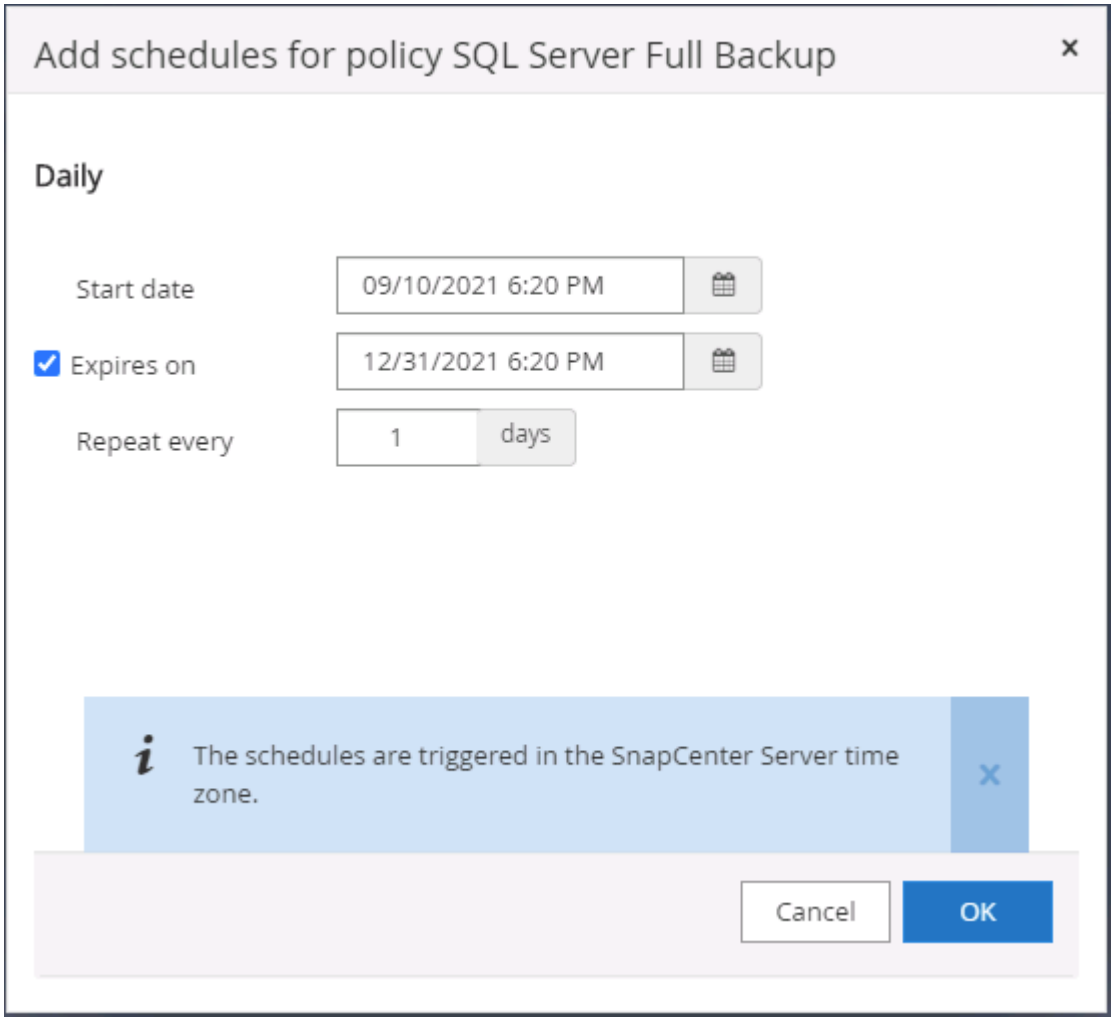
2. Seleccione los recursos de la base de datos que desea incluir en el backup.



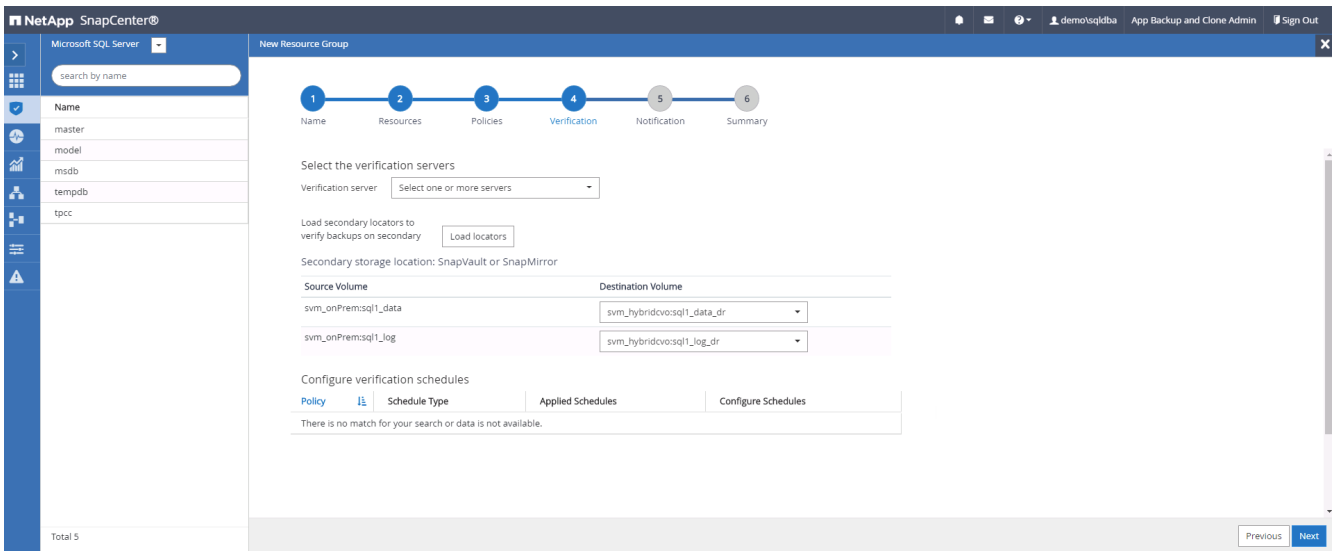
3. Seleccione una política de backup de SQL completa creada en la sección 7.



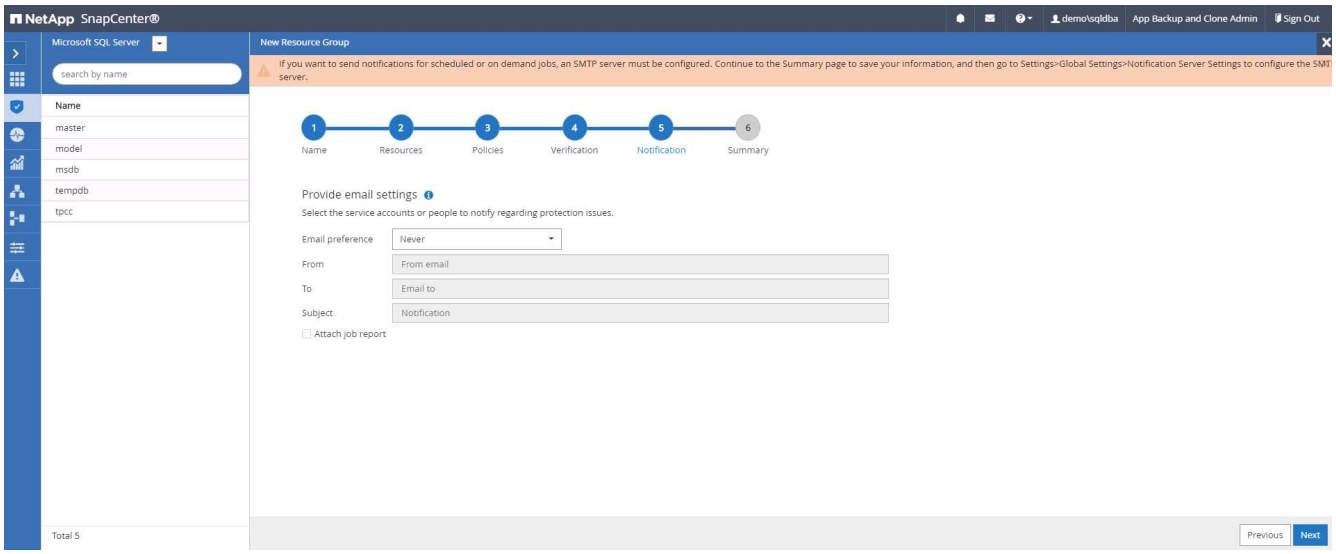
4. Añada una hora exacta para backups y la frecuencia.



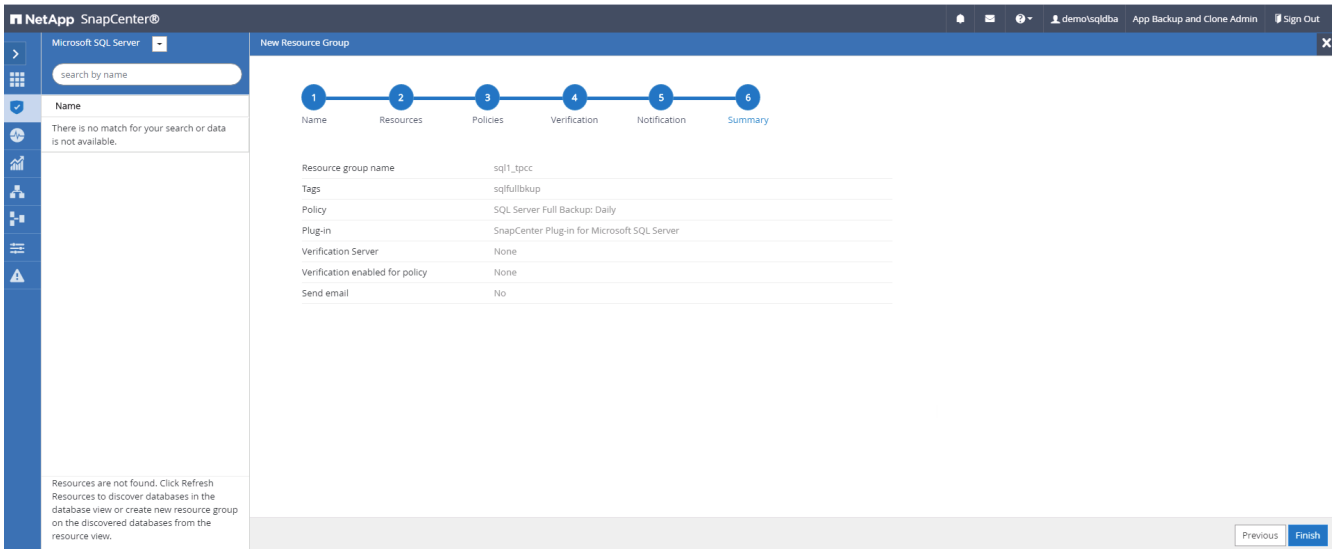
5. Seleccione el servidor de verificación para el backup en secundario si desea realizar la verificación de backup. Haga clic en Load Locator para rellenar la ubicación de almacenamiento secundario.



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

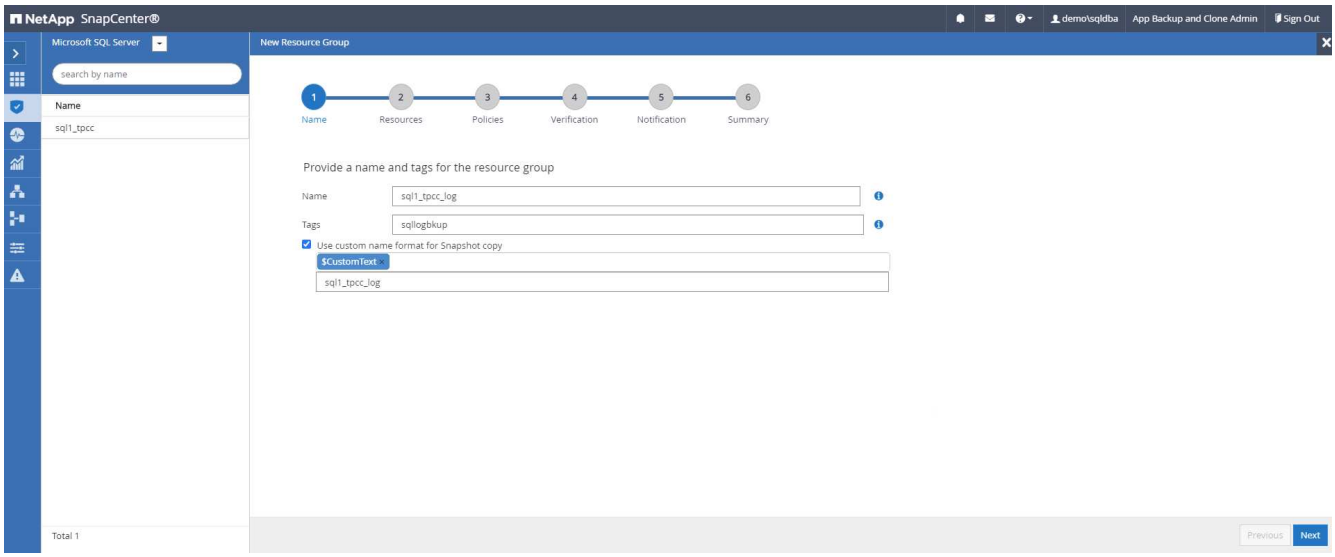


7. Resumen.

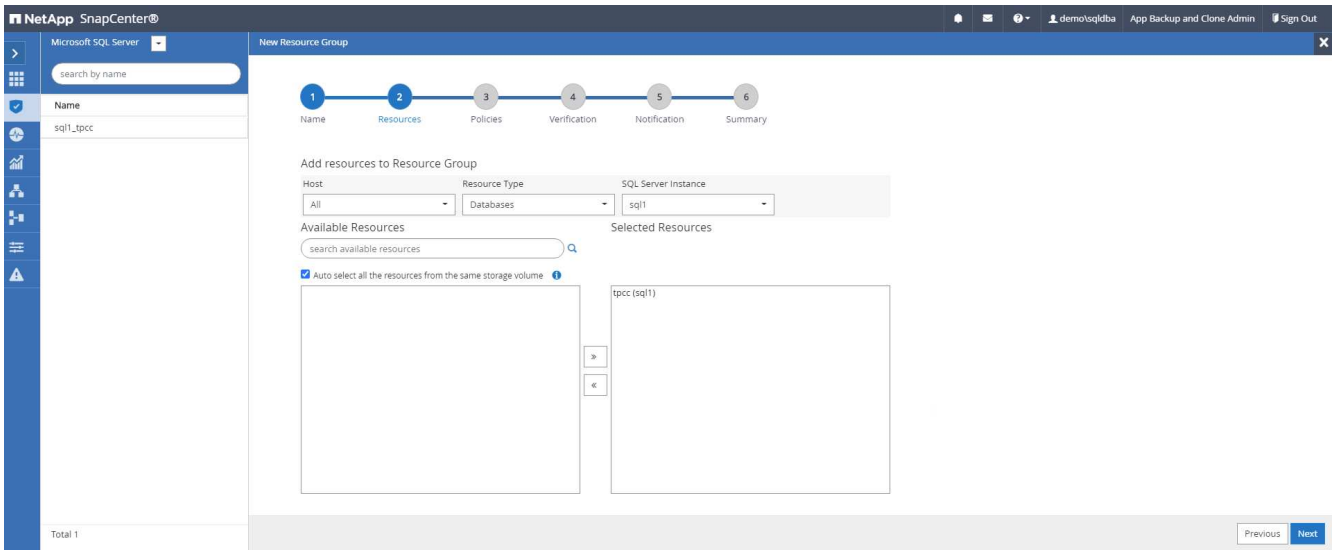


Crear un grupo de recursos para backup de registros de SQL Server

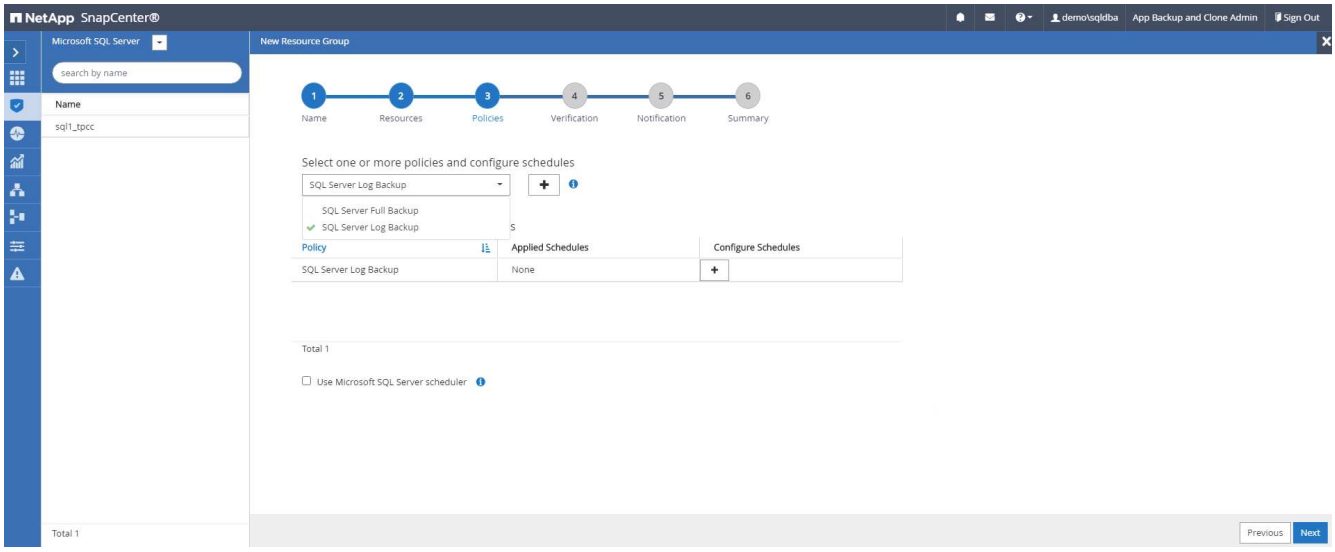
1. Inicie sesión en SnapCenter con un ID de usuario de gestión de bases de datos y vaya a la pestaña Resources. En la lista desplegable View, seleccione una base de datos o un grupo de recursos para iniciar el flujo de trabajo de creación de grupo de recursos. Proporcione el nombre y las etiquetas del grupo de recursos. Puede definir un formato de nomenclatura para la copia Snapshot.



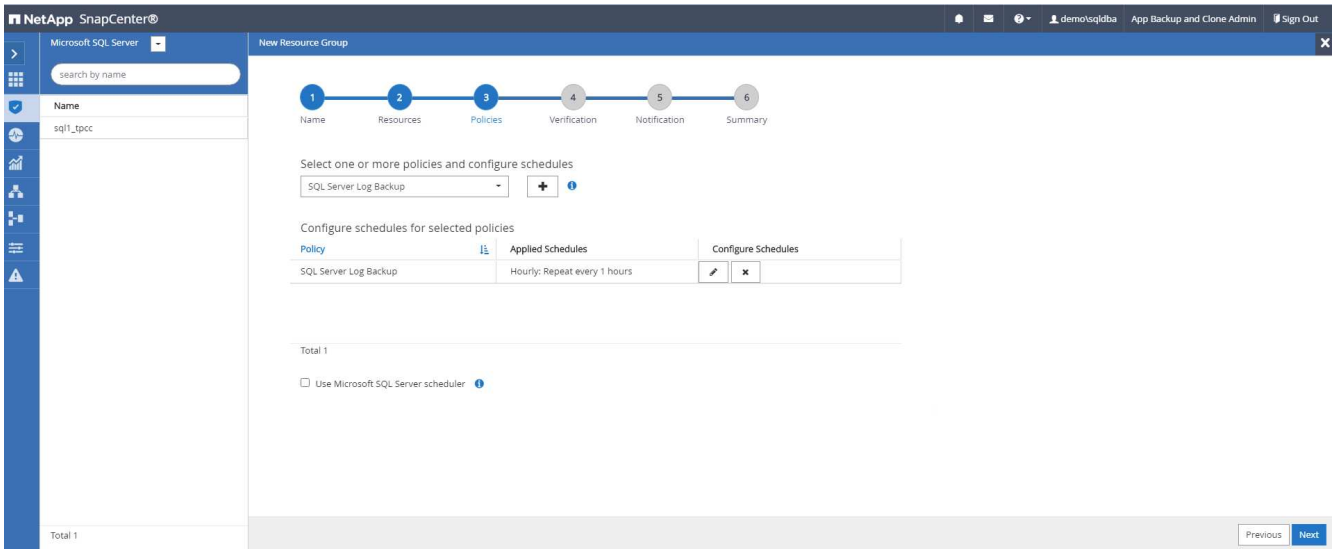
2. Seleccione los recursos de la base de datos que desea incluir en el backup.



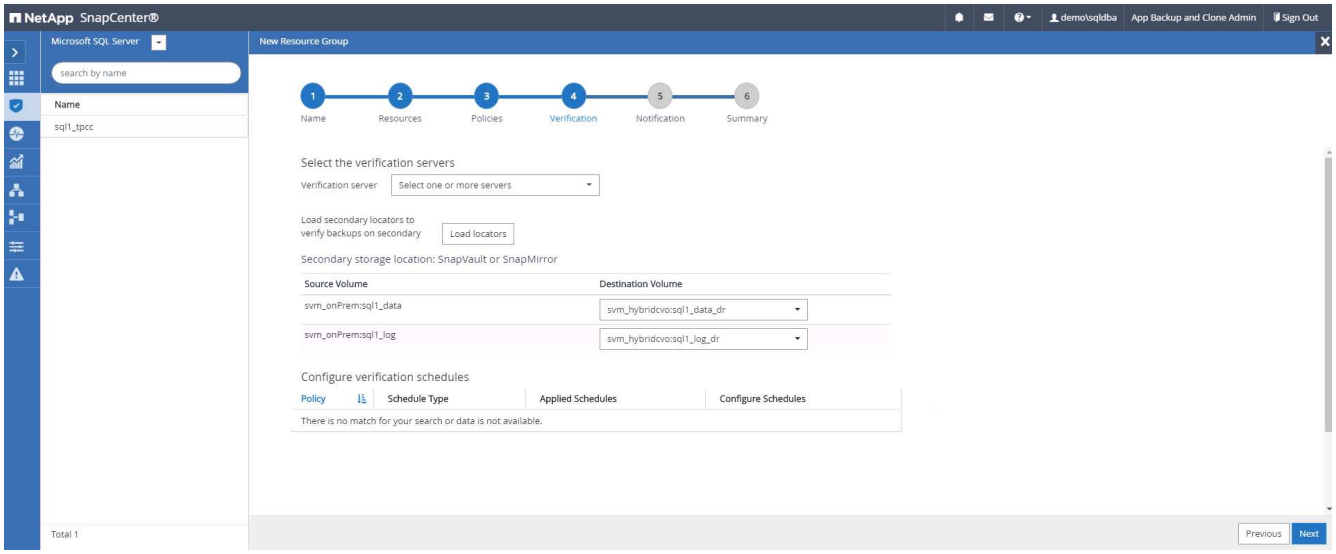
3. Seleccione una política de backup de registro SQL creada en la sección 7.



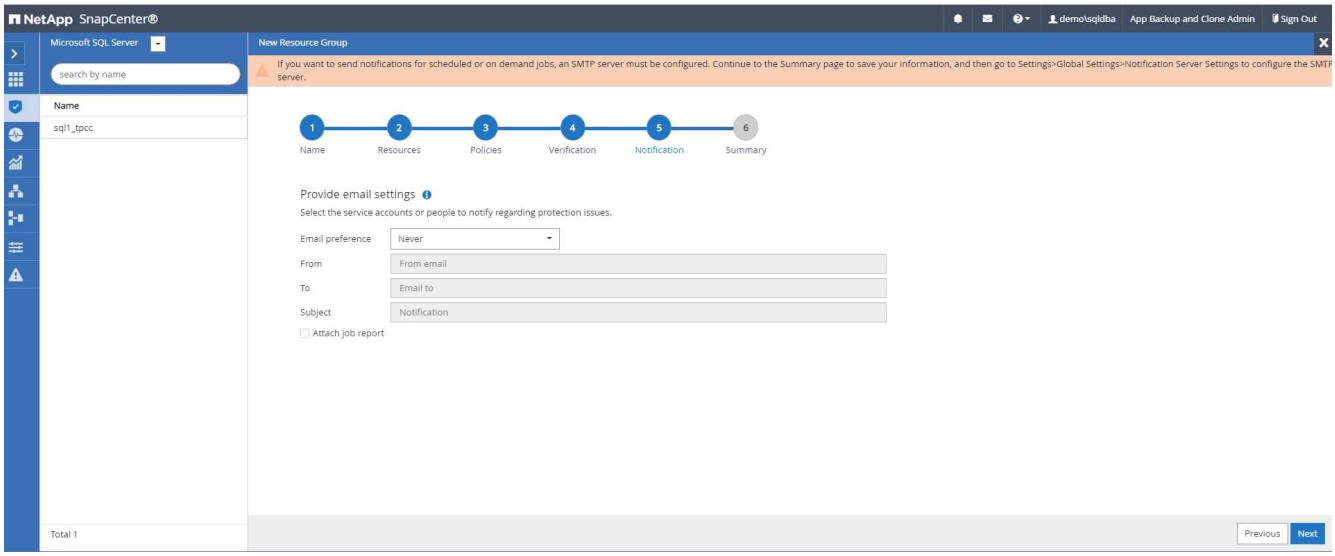
4. Añada la hora exacta para la copia de seguridad así como la frecuencia.



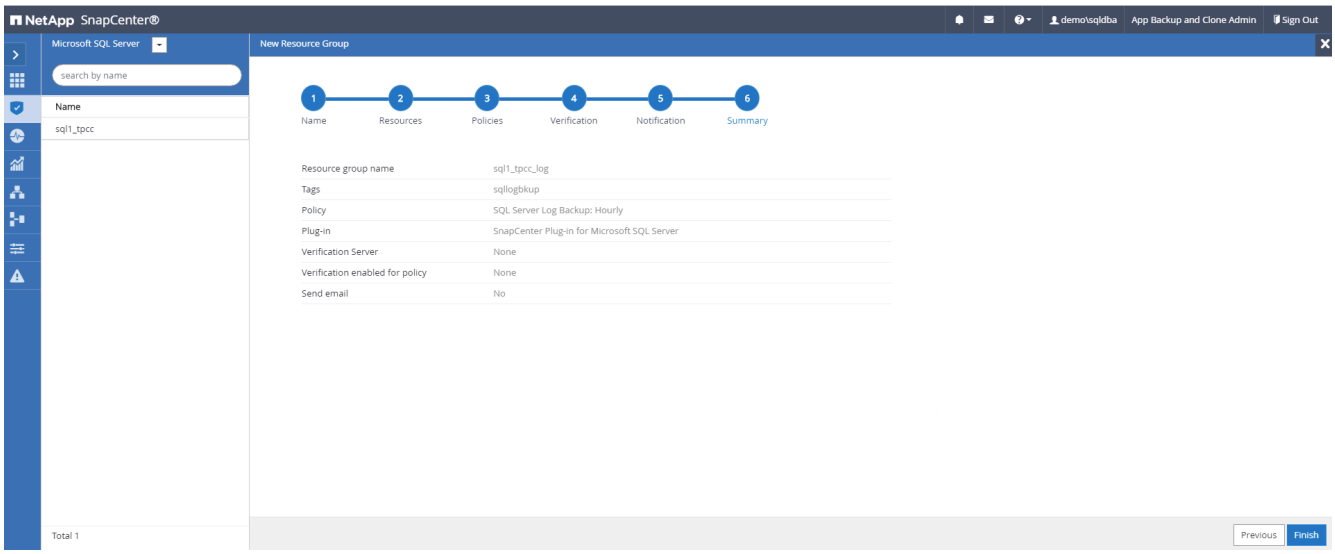
5. Seleccione el servidor de verificación para el backup en secundario si desea realizar la verificación de backup. Haga clic en Load Locator para rellenar la ubicación de almacenamiento secundario.



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



7. Resumen.

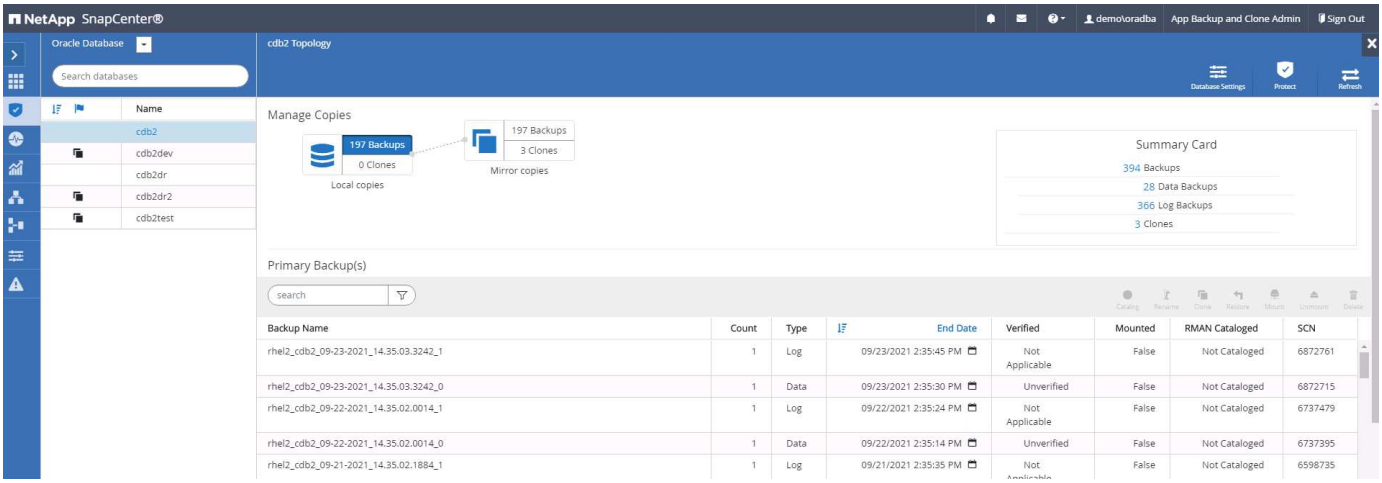


9. Validar el backup

Después de crear grupos de recursos de backup de bases de datos para proteger los recursos de las bases de datos, las tareas de backup se ejecutan según la programación predefinida. Compruebe el estado de ejecución del trabajo en la pestaña Monitor.

Vaya a la pestaña Resources, haga clic en el nombre de la base de datos para ver los detalles del backup de la base de datos, y cambie entre copias locales y copias de mirroring para verificar que los backups de

Snapshot se replican en una ubicación secundaria en el cloud público.



En este momento, las copias de backup de base de datos en el cloud están listas para clonar para ejecutar los procesos de desarrollo y pruebas o para la recuperación ante desastres en caso de un fallo principal.

Introducción al cloud público de AWS

En esta sección se describe el proceso de puesta en marcha de Cloud Manager y Cloud Volumes ONTAP en AWS.

Cloud público de AWS

> Para facilitar el seguimiento de las cosas, hemos creado este documento a partir de una puesta en marcha en AWS. Sin embargo, el proceso es muy similar para Azure y GCP.

1. Control previo al vuelo

Antes de la puesta en marcha, asegúrese de que se ha implementado la infraestructura para permitir la puesta en marcha en la siguiente etapa. Esto incluye lo siguiente:

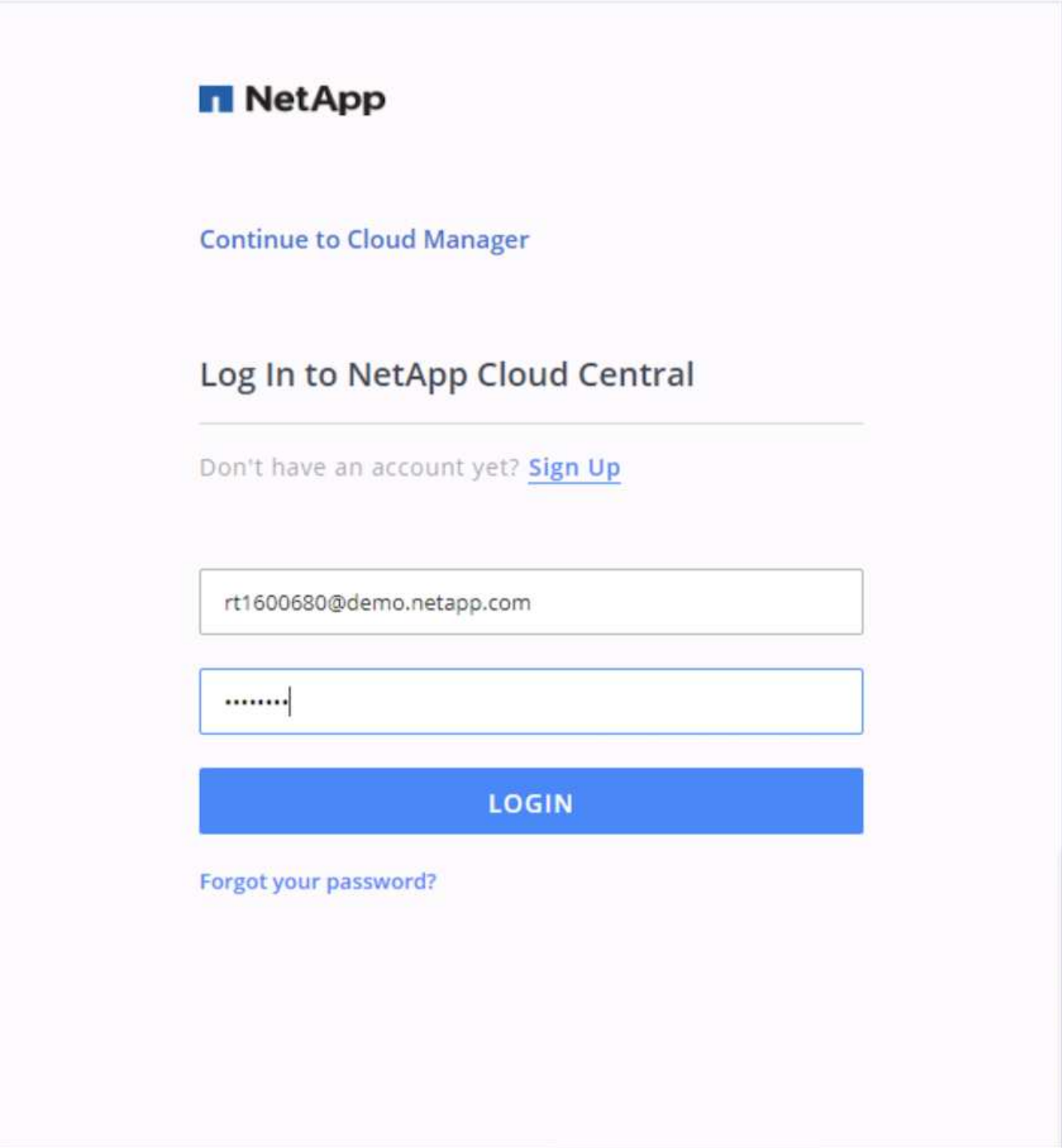
- Cuenta de AWS
- VPC en su región de preferencia
- Subred con acceso a Internet pública
- Permisos para añadir roles IAM a la cuenta de AWS
- Una clave secreta y una clave de acceso para el usuario de AWS

2. Pasos para poner en marcha Cloud Manager y Cloud Volumes ONTAP en AWS

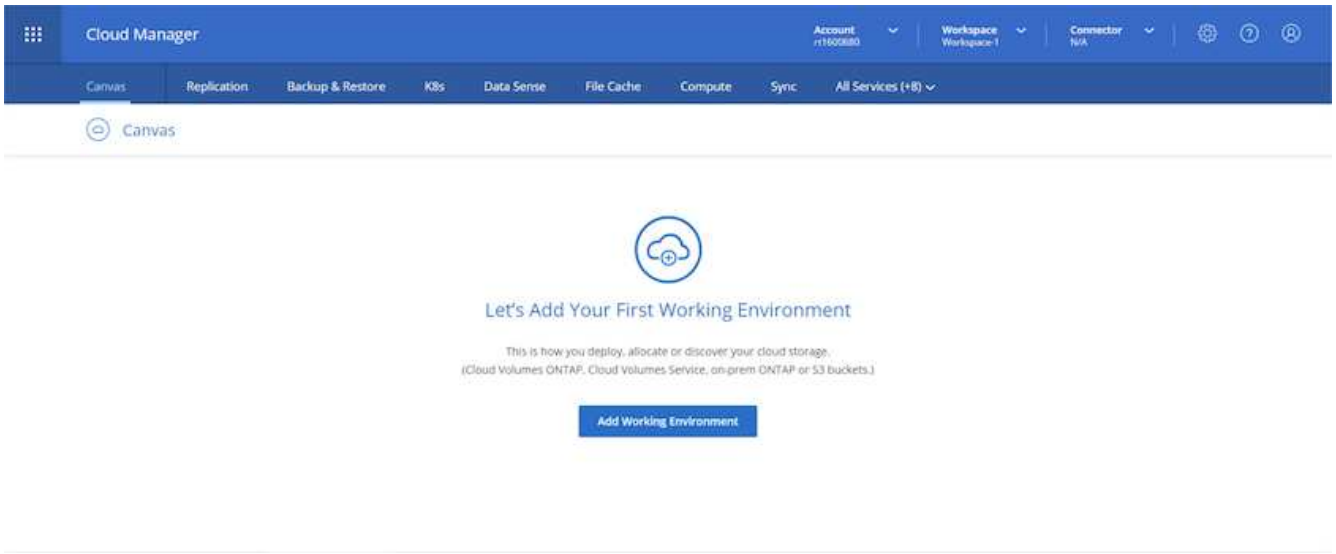
> Existen muchos métodos para poner en marcha Cloud Manager y Cloud Volumes ONTAP; este método es el más sencillo pero requiere el mayor número de permisos. Si este método no es adecuado para su entorno AWS, consulte "Documentación sobre cloud de NetApp".

Ponga en marcha el conector Cloud Manager

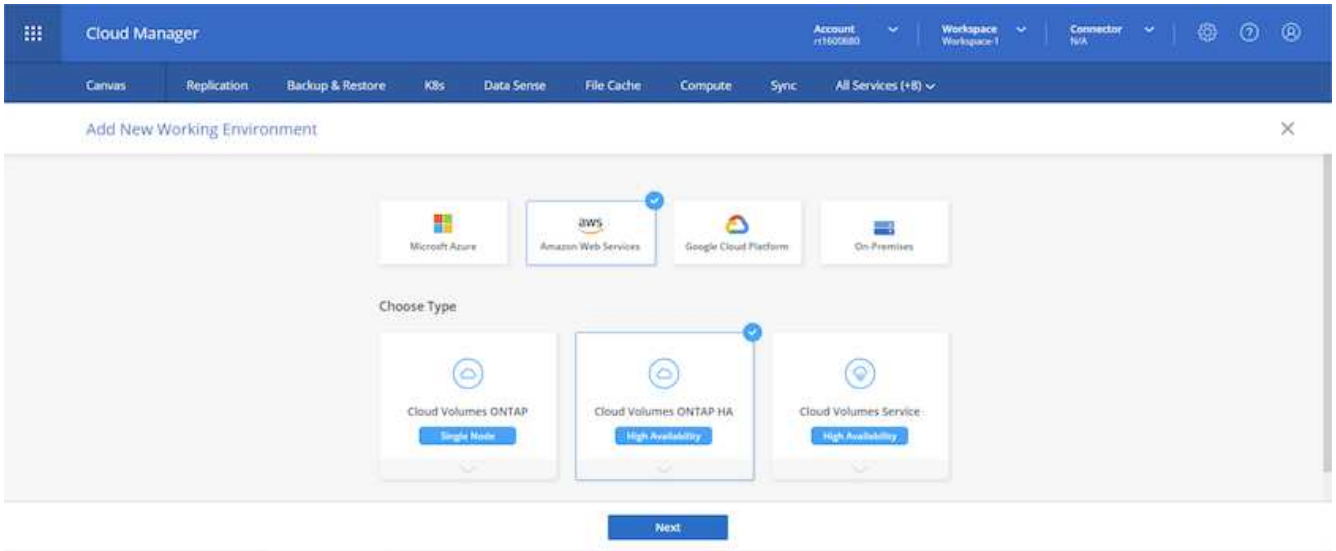
1. Vaya a. "Cloud Central de NetApp" e inicie sesión o regístrese.



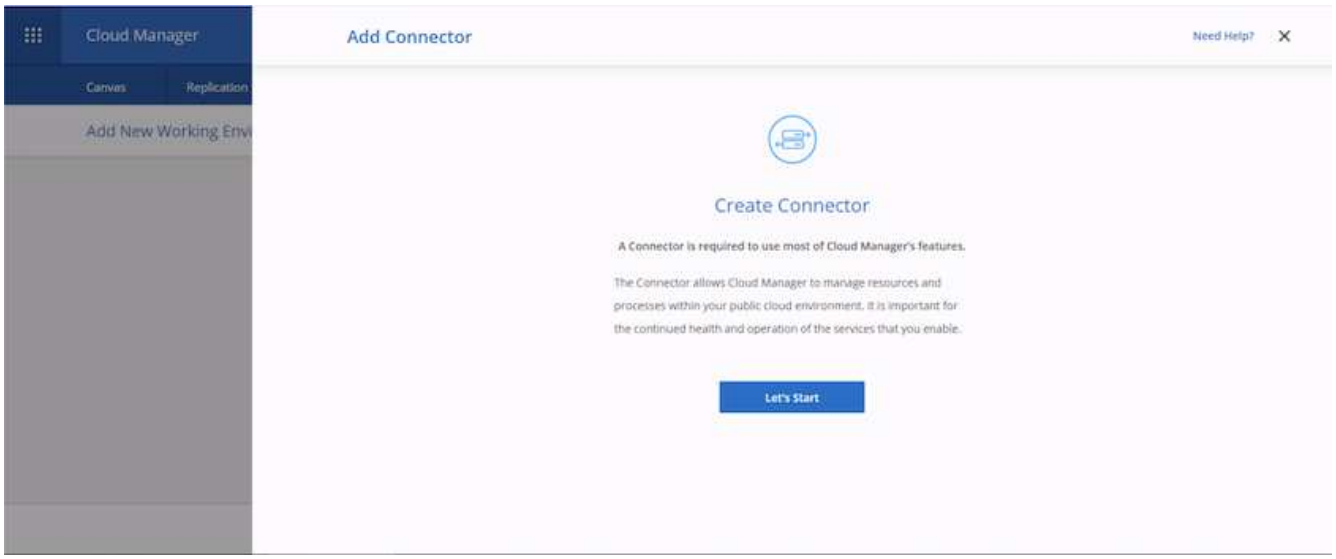
2. Después de iniciar sesión, se le debe llevar al lienzo.



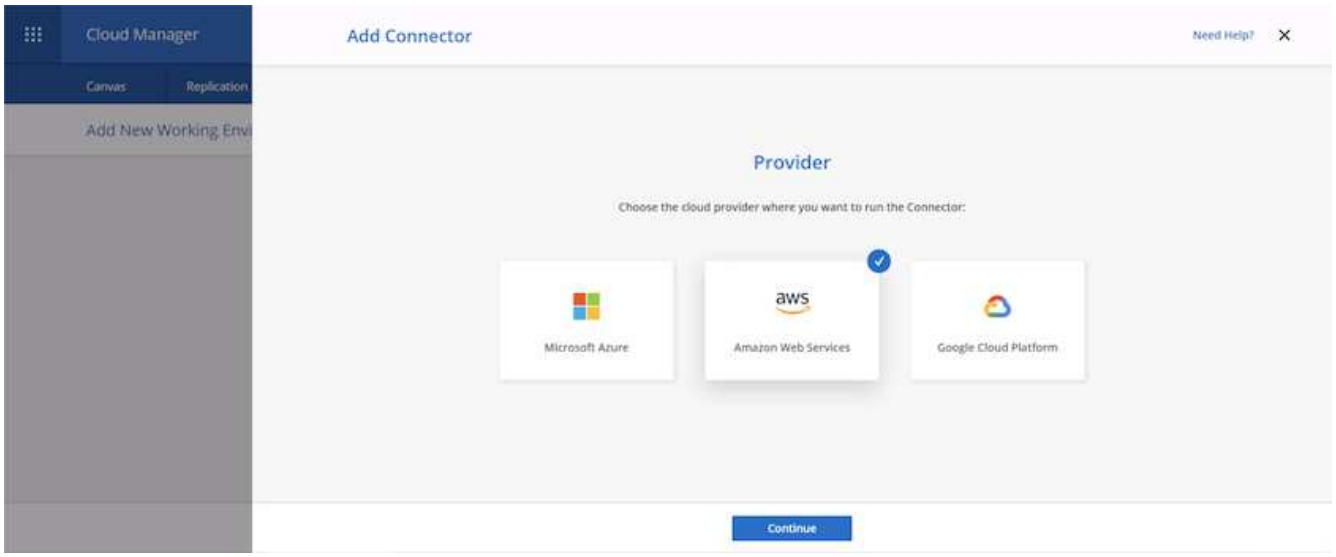
3. Haga clic en "Add Working Environment" y elija Cloud Volumes ONTAP en AWS. Aquí, también puede elegir si desea poner en marcha un sistema de nodo único o un par de alta disponibilidad. He decidido implementar un par de alta disponibilidad.



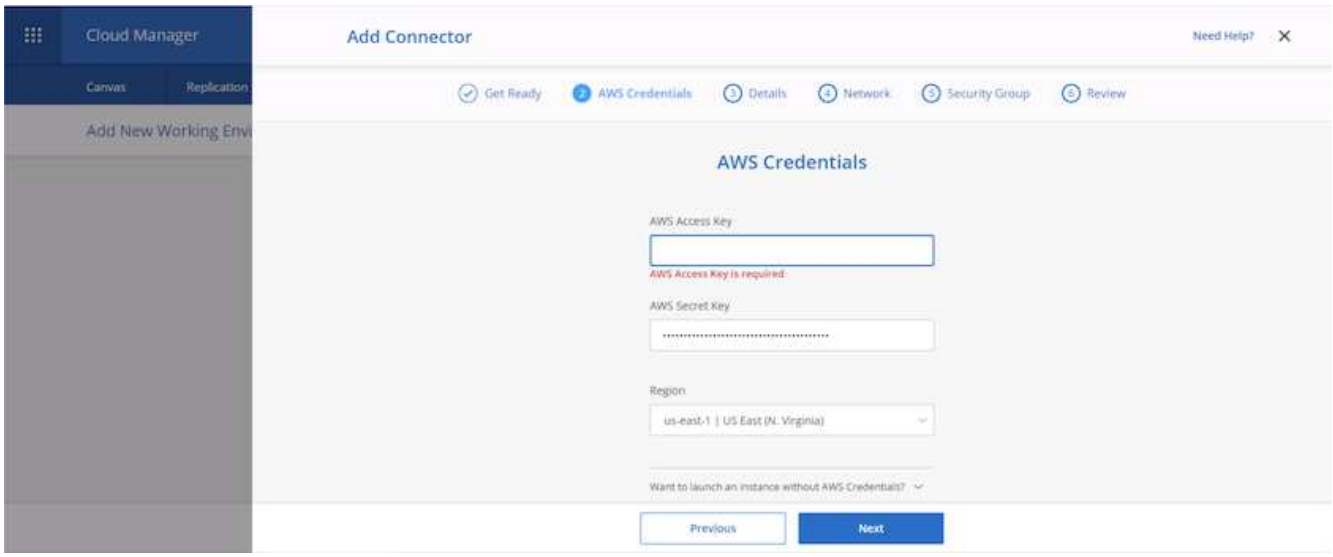
4. Si no se ha creado ningún conector, aparece una ventana emergente que le pide que cree un conector.



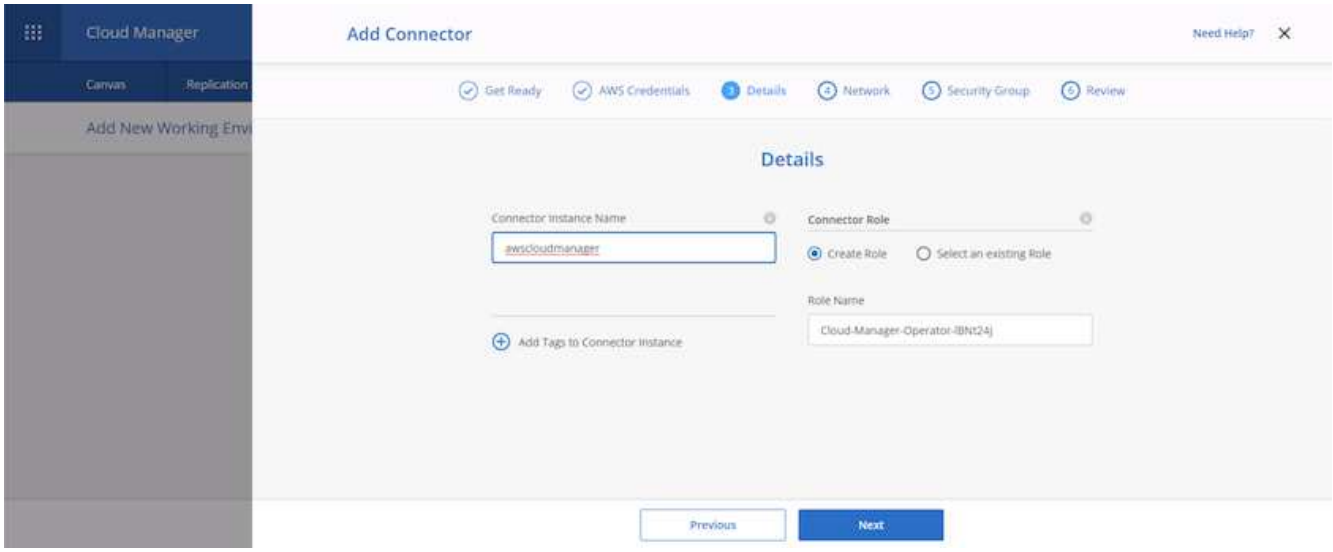
5. Haga clic en lets Start y, a continuación, seleccione AWS.



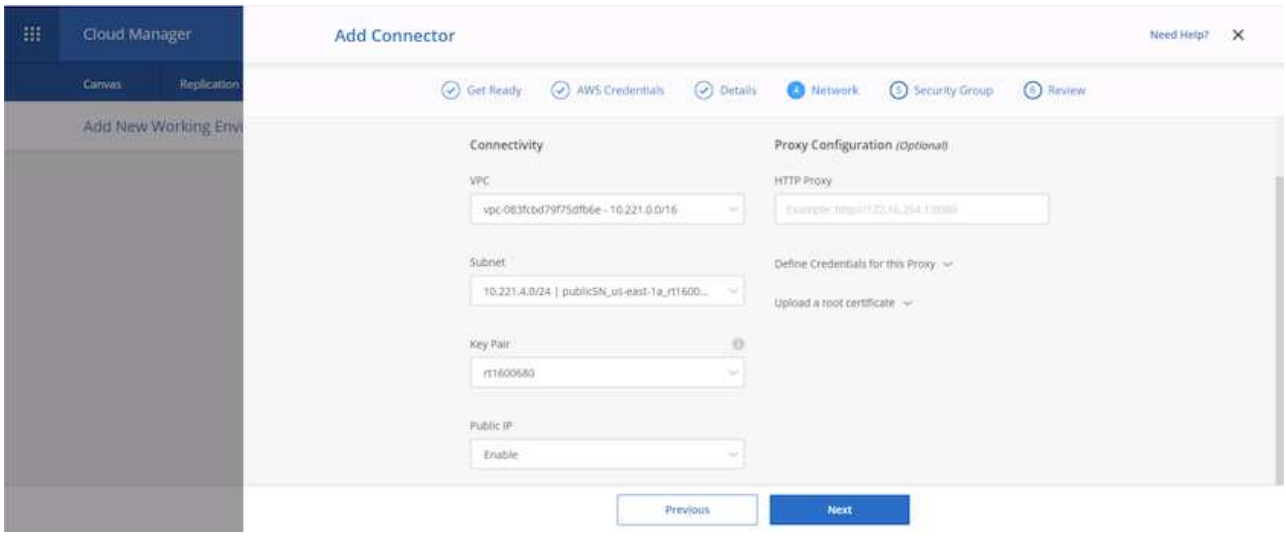
6. Introduzca la clave secreta y la clave de acceso. Asegúrese de que el usuario tiene los permisos correctos descritos en "Página de políticas de NetApp".



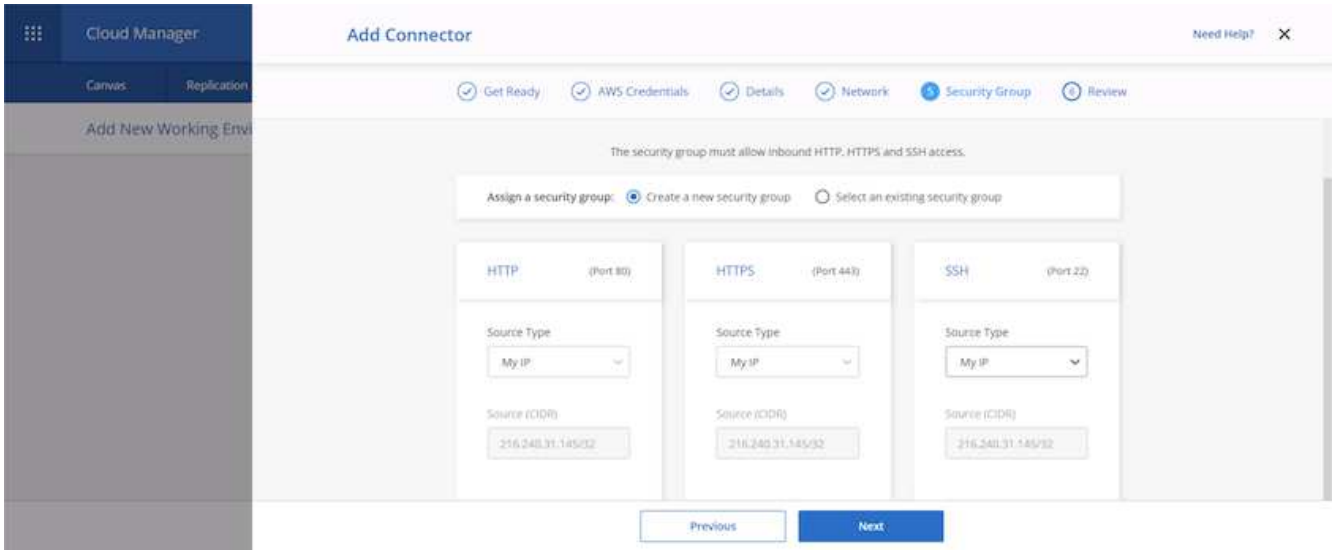
7. Asigne al conector un nombre y utilice una función predefinida como se describe en "Página de políticas de NetApp" O pida a Cloud Manager que cree la función que usted desempeña.



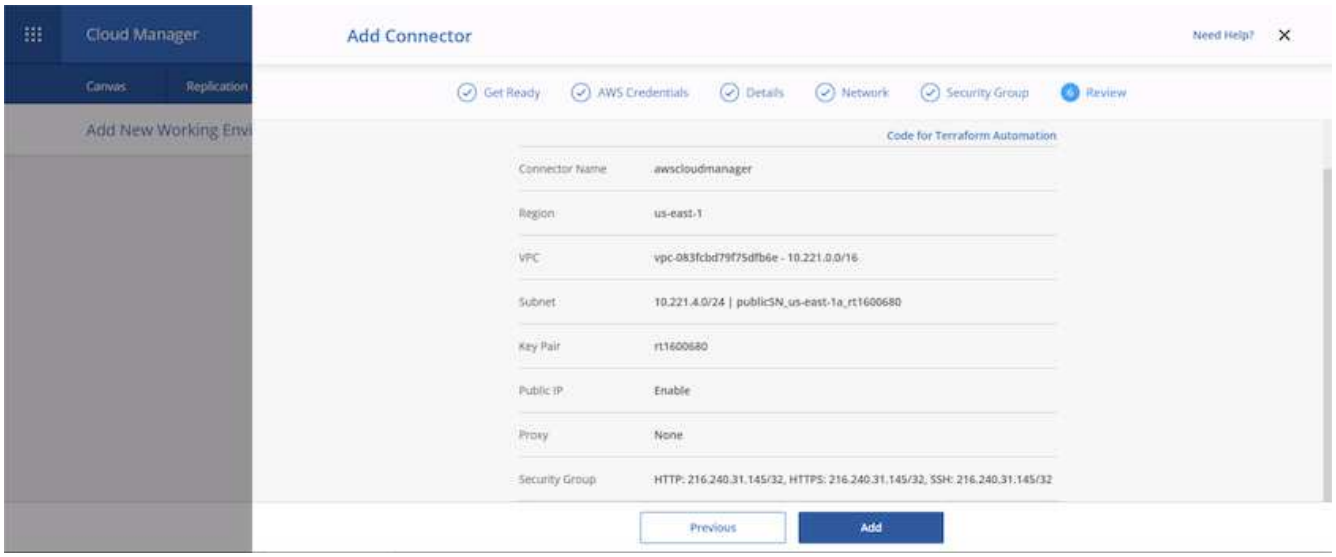
8. Proporcione la información de red necesaria para implementar el conector. Verifique que el acceso saliente a Internet esté habilitado por:
   a. Dar al conector una dirección IP pública
   b. Dar al conector un proxy a través del cual trabajar
   c. Dar al conector una ruta a Internet pública a través de una puerta de enlace de Internet



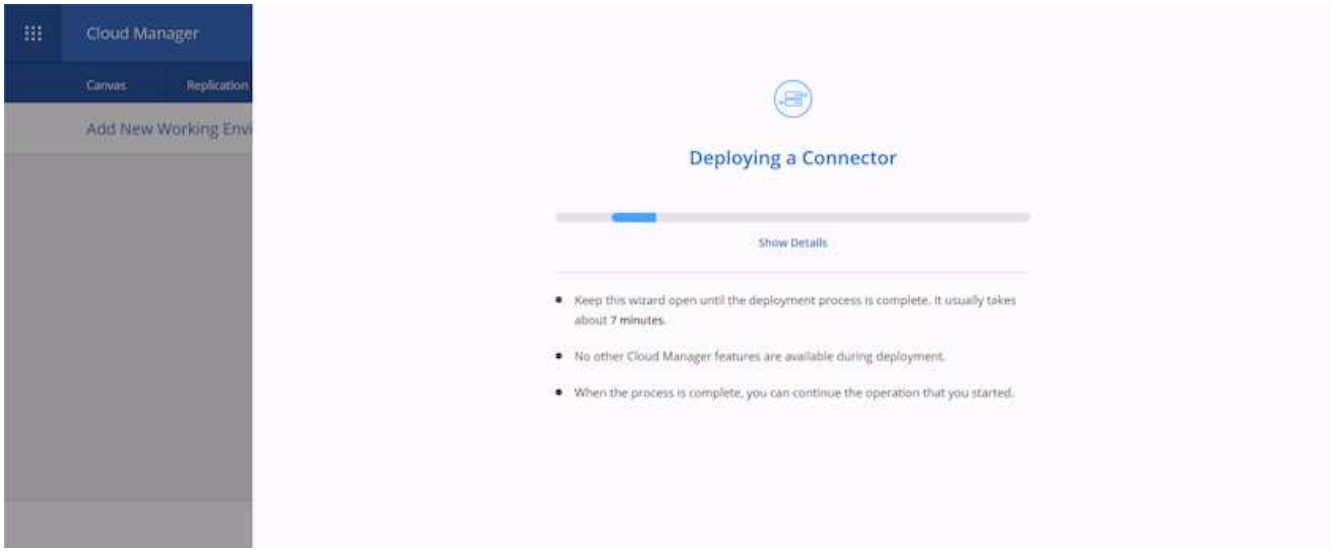
9. Proporcione comunicación con el conector a través de SSH, HTTP y HTTPS ya sea proporcionando un grupo de seguridad o creando un nuevo grupo de seguridad. Sólo he habilitado el acceso al conector desde mi dirección IP.



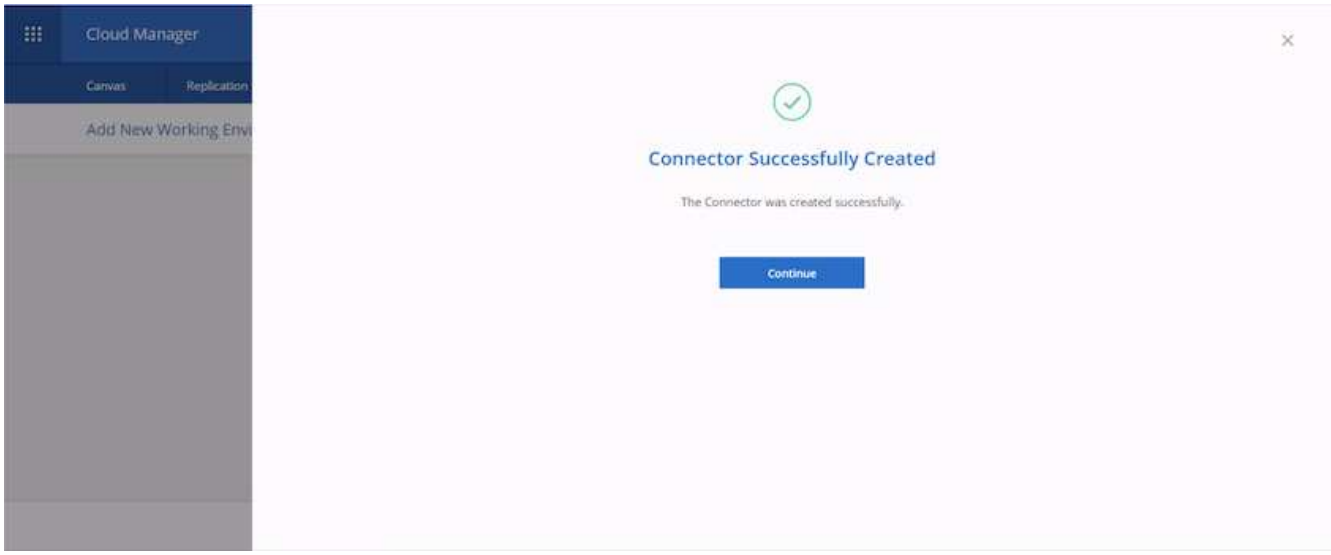
10. Revise la información de la página de resumen y haga clic en Agregar para implementar el conector.



11. El conector ahora se pone en marcha utilizando una pila de formación de cloud. Puede supervisar su progreso desde Cloud Manager o a través de AWS.

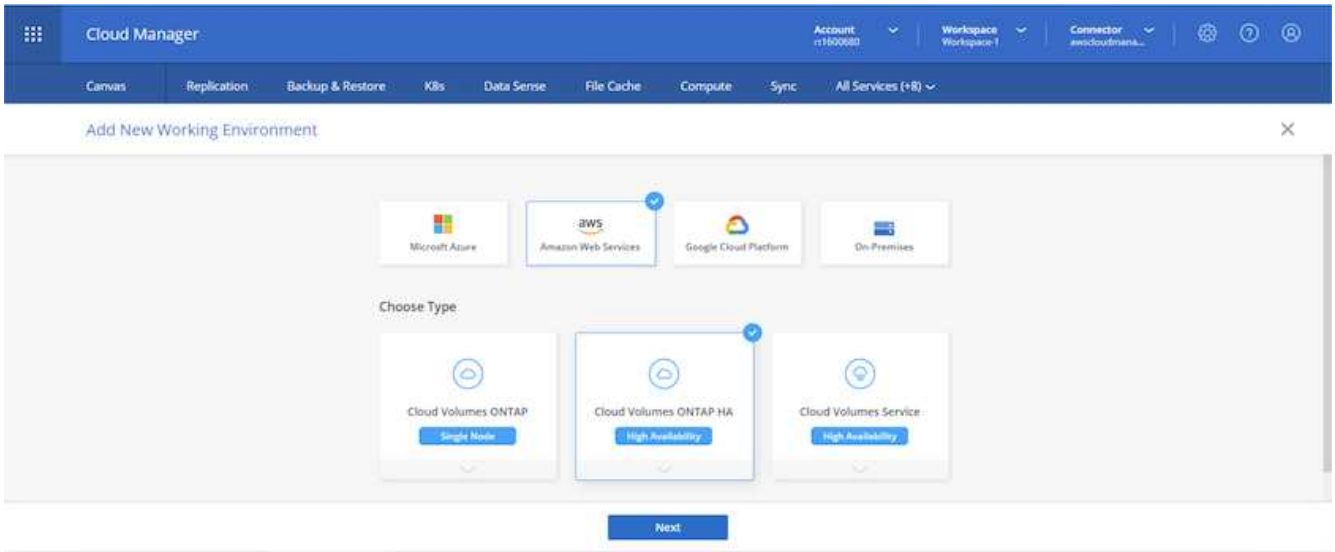


12. Una vez completada la implementación, aparece una página Success.

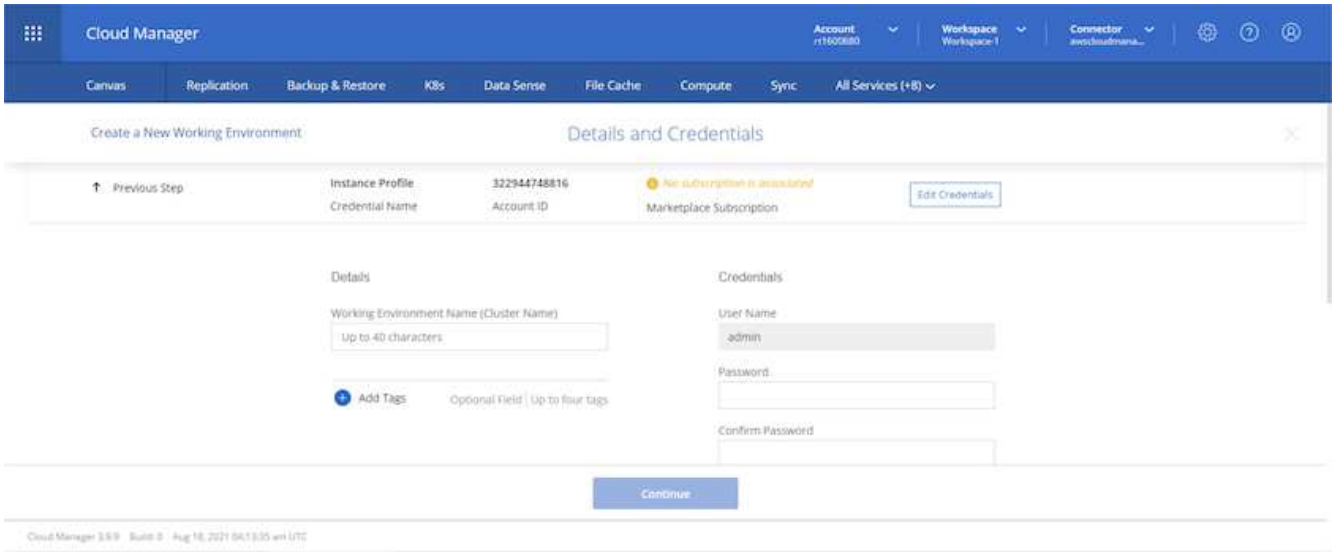


Ponga en marcha Cloud Volumes ONTAP

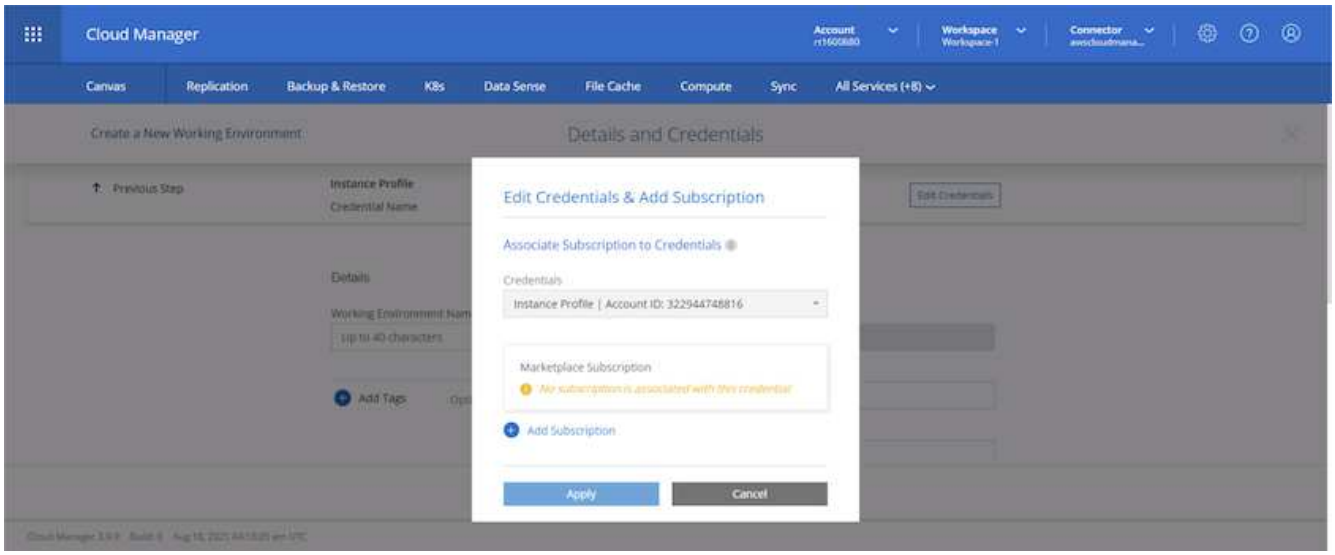
1. Seleccione AWS y el tipo de implementación según sus requisitos.



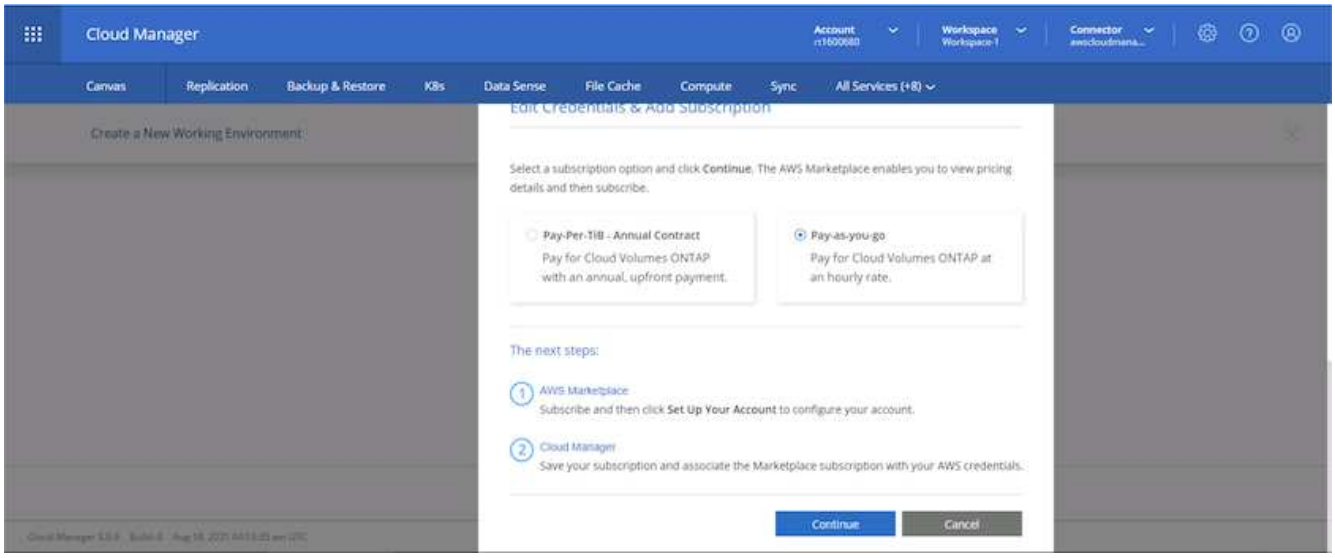
2. Si no se ha asignado ninguna suscripción y desea comprarla con PAYGO, seleccione Editar credenciales.



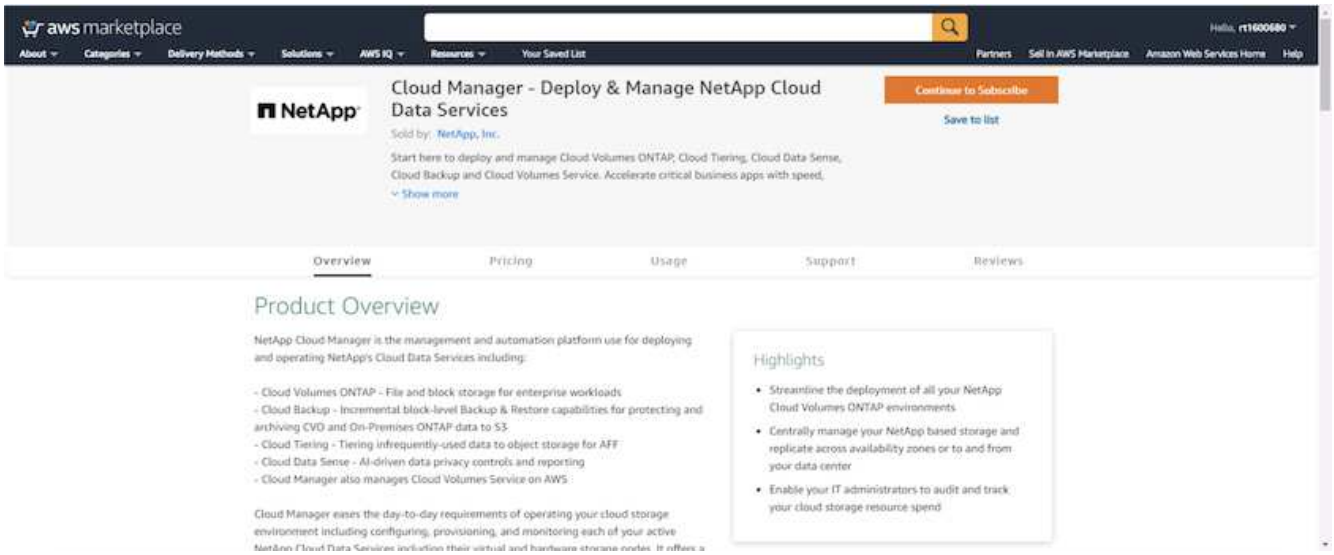
3. Seleccione Agregar suscripción.



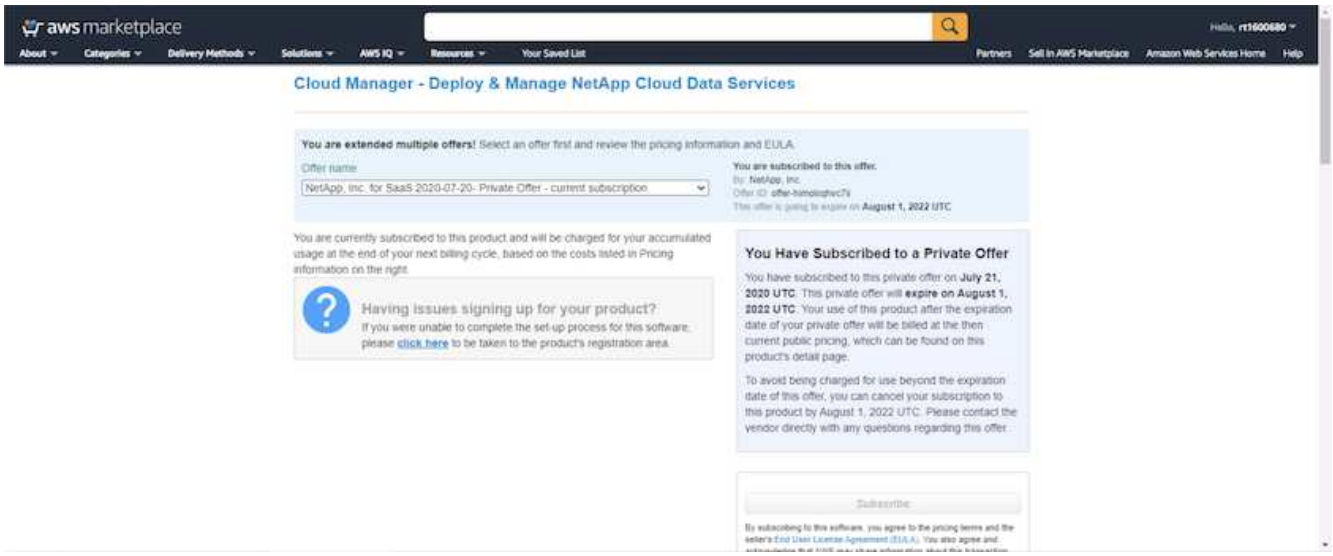
4. Elija el tipo de contrato al que desea suscribirse. Elegí el pago por uso.



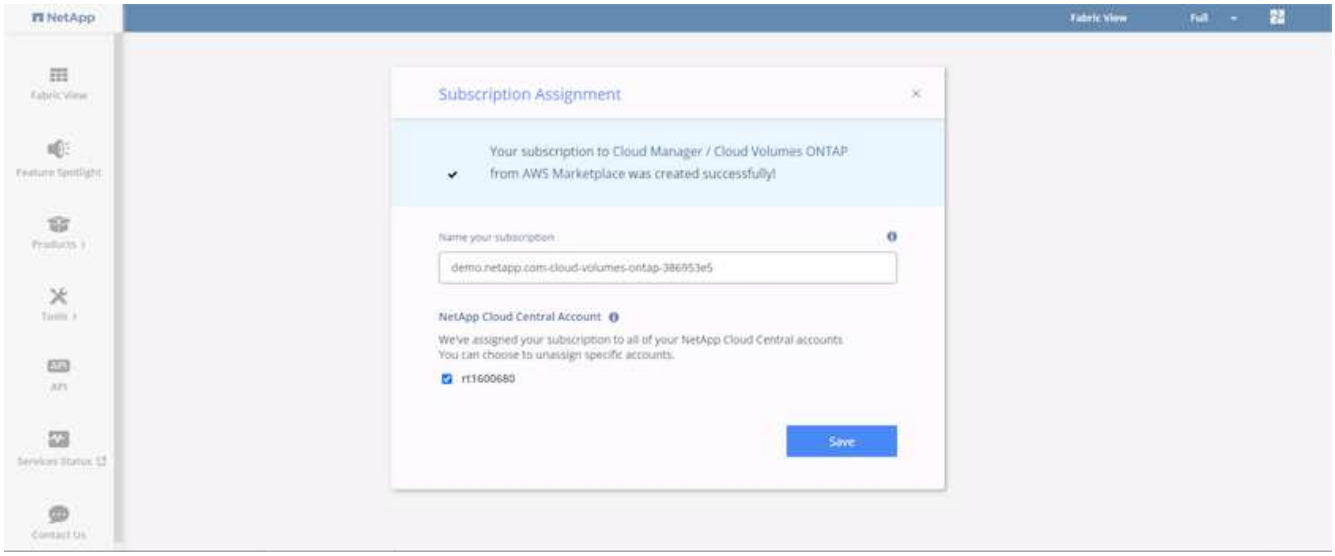
5. Se le redirigirá a AWS; elija continuar Suscribirse.



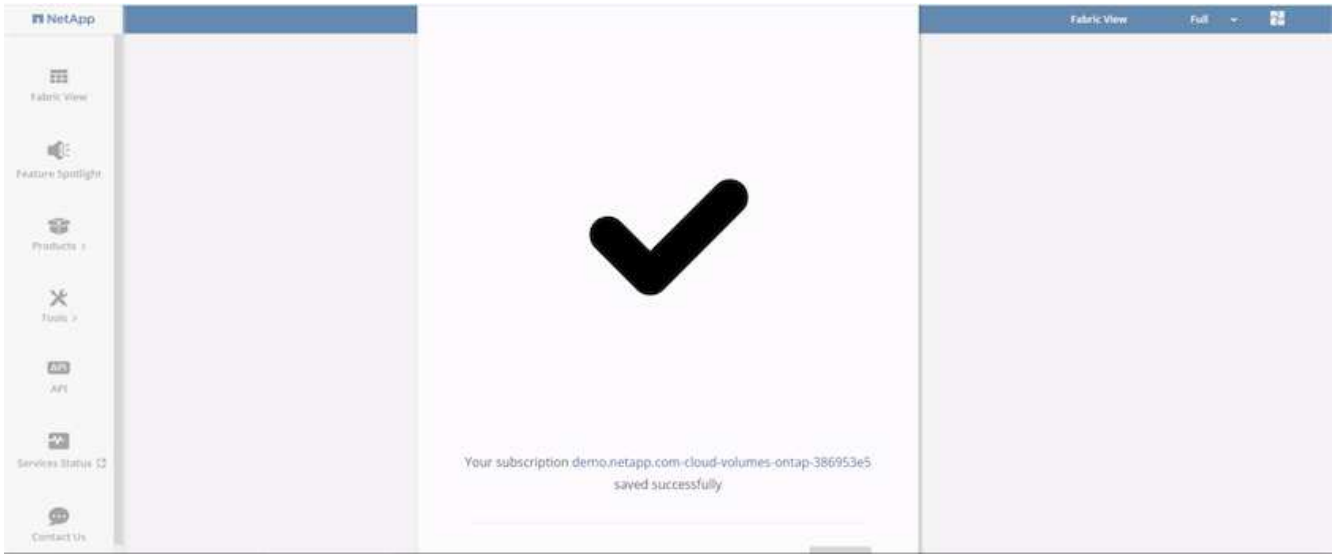
6. Suscríbase y se le redirigirá a Cloud Central de NetApp. Si ya se ha suscrito y no se redirecciona, elija el enlace "haga clic aquí".



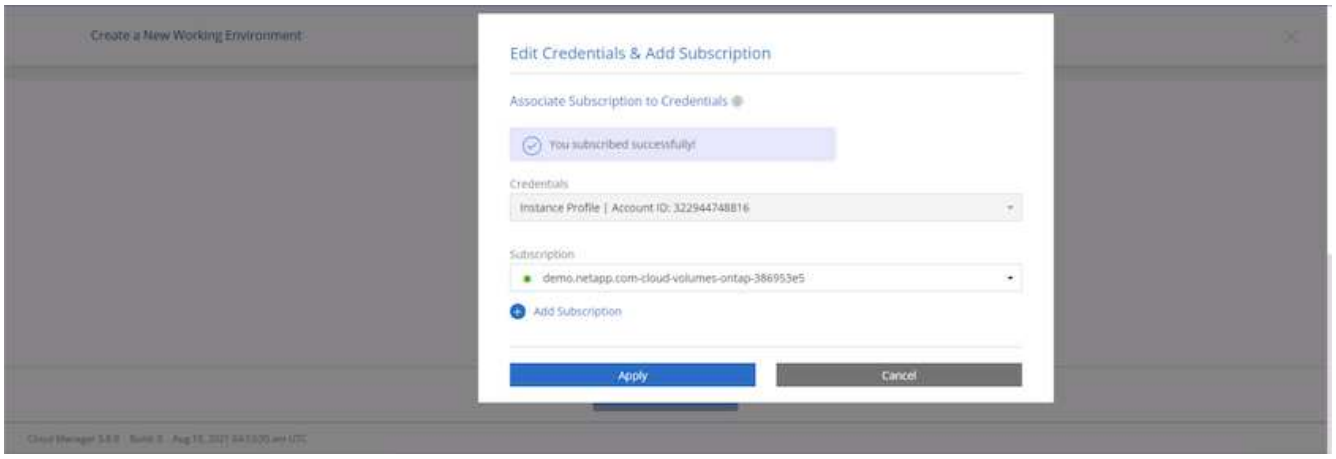
7. Se le redirigirá a Cloud Central, donde debe dar un nombre a su suscripción y asignarla a su cuenta de Cloud Central.



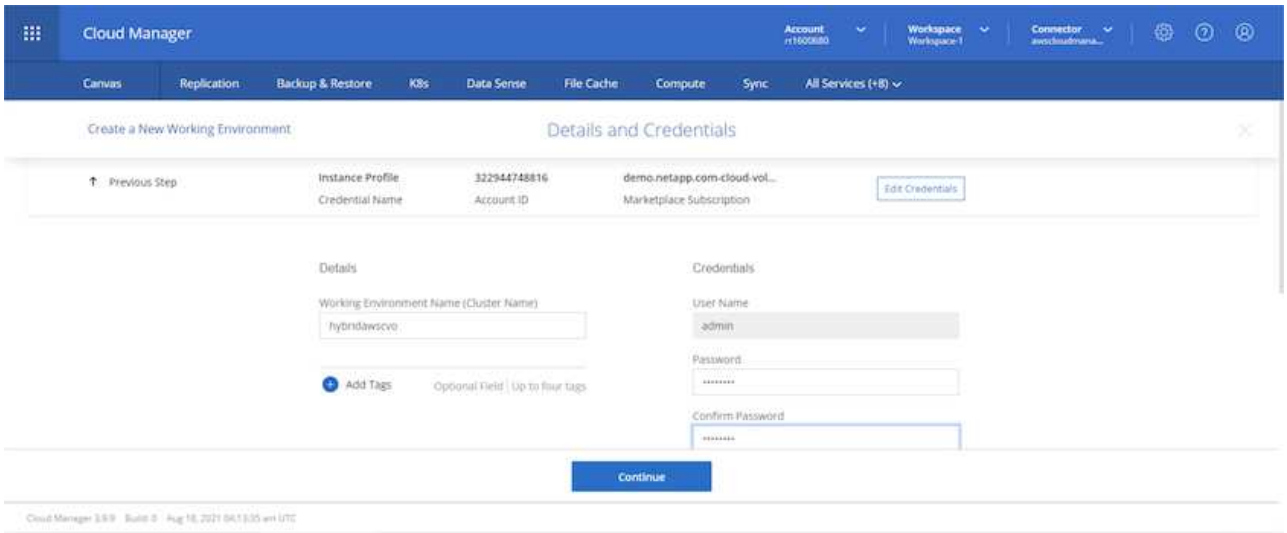
8. Cuando se realiza correctamente, aparece una página de Marca de verificación. Vuelva a la pestaña Cloud Manager.



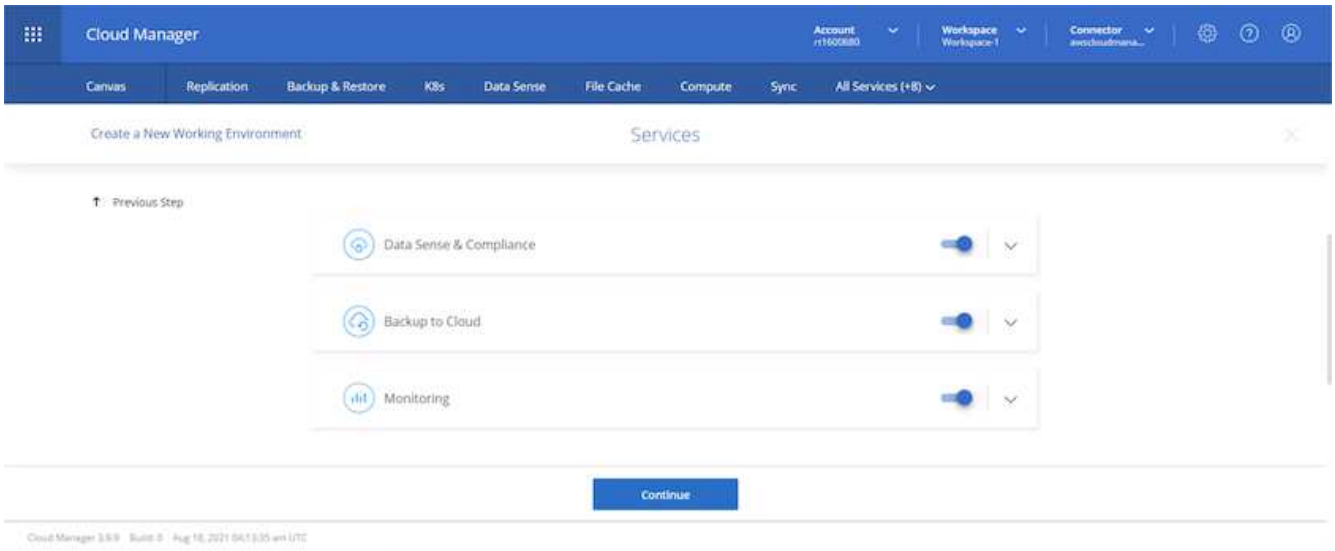
9. La suscripción aparece ahora en Cloud Central. Haga clic en aplicar para continuar.



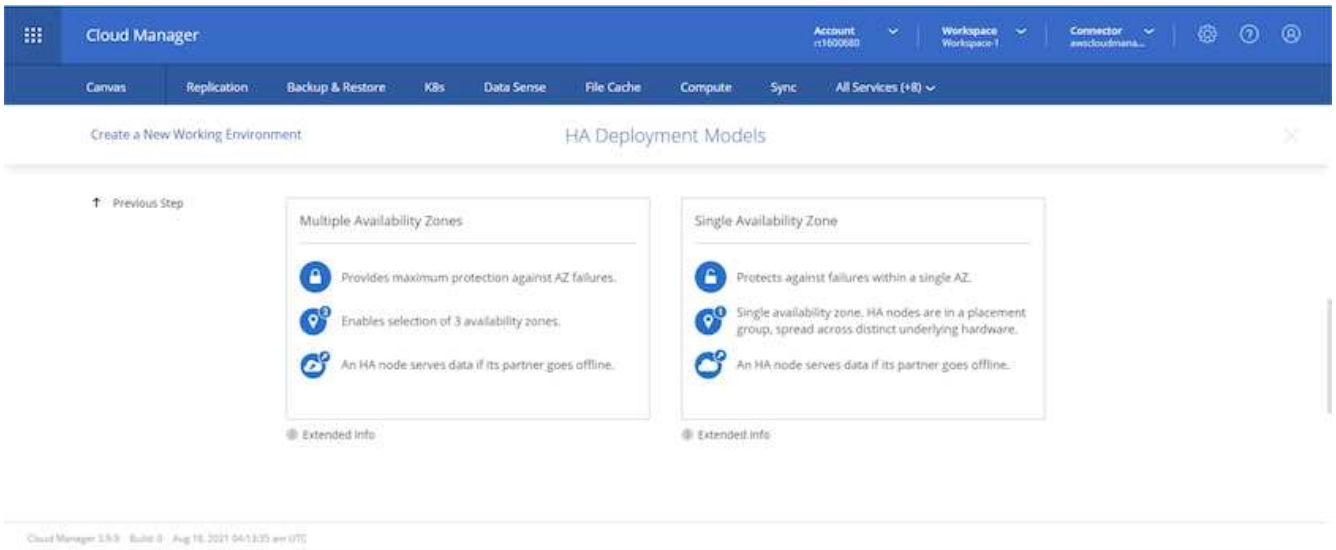
10. Introduzca los detalles del entorno de trabajo como:
    a. Nombre del clúster
    b. Contraseña del clúster
    c. Etiquetas de AWS (opcional)



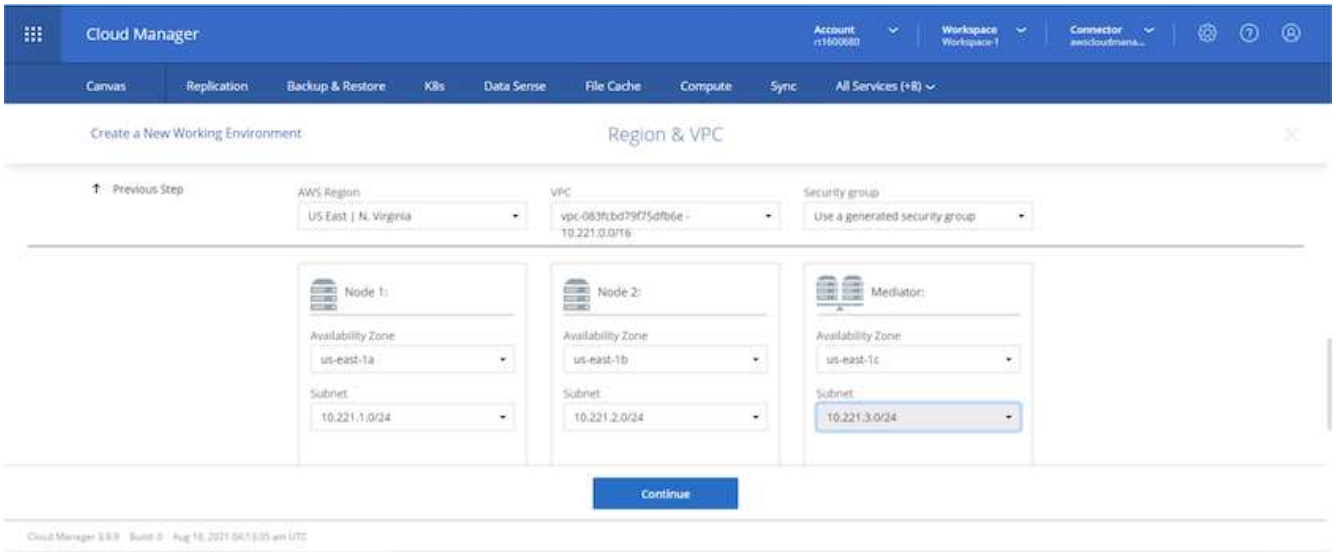
11. Elija los servicios adicionales que le gustaría poner en marcha. Para obtener más información sobre estos servicios, visite la "Página de inicio de cloud de NetApp".



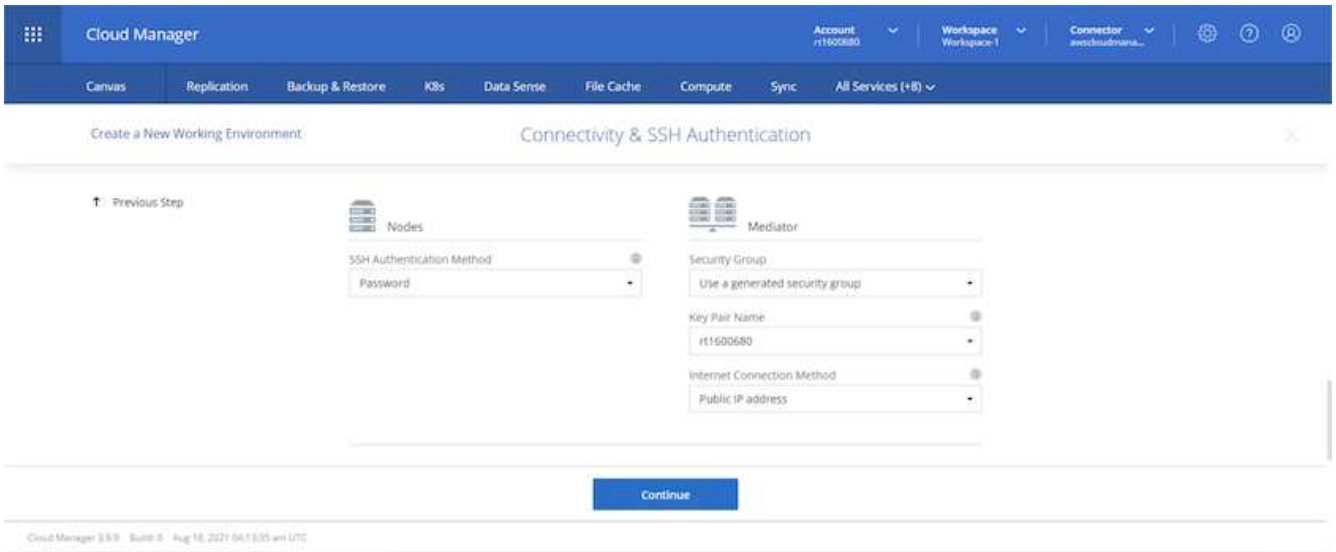
12. Elija si desea implementar en varias zonas de disponibilidad (reguarida tres subredes, cada una en una zona AZ diferente) o una única zona de disponibilidad. Elegí varios AZs.



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

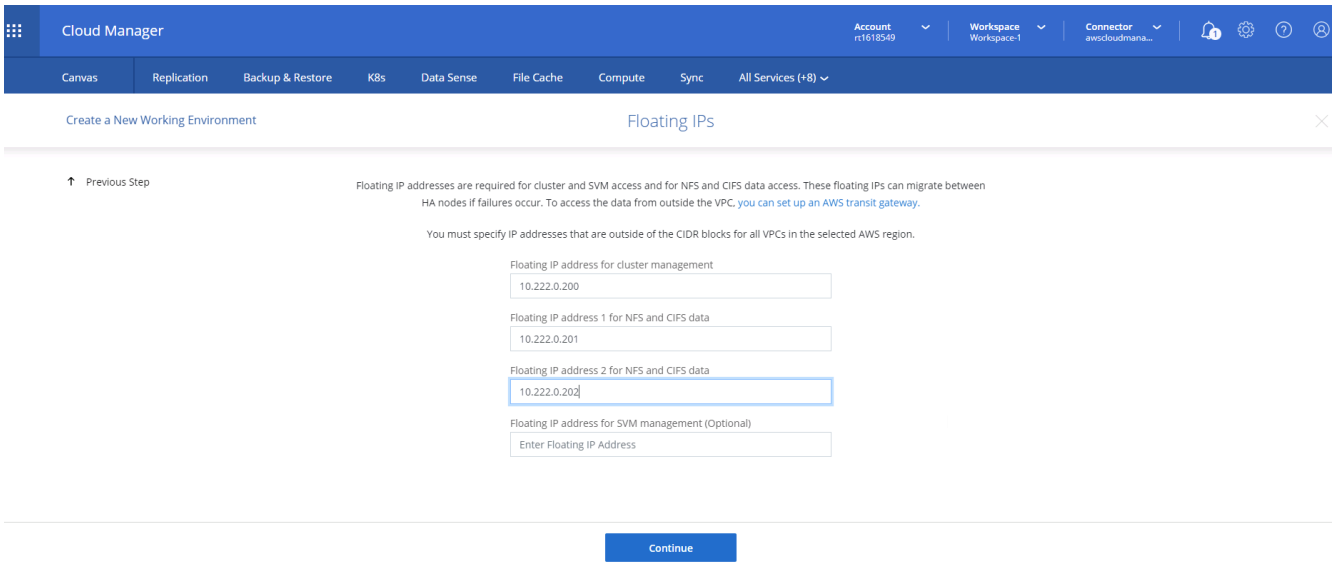


14. Elija los métodos de conexión tanto para los nodos como para el mediador.

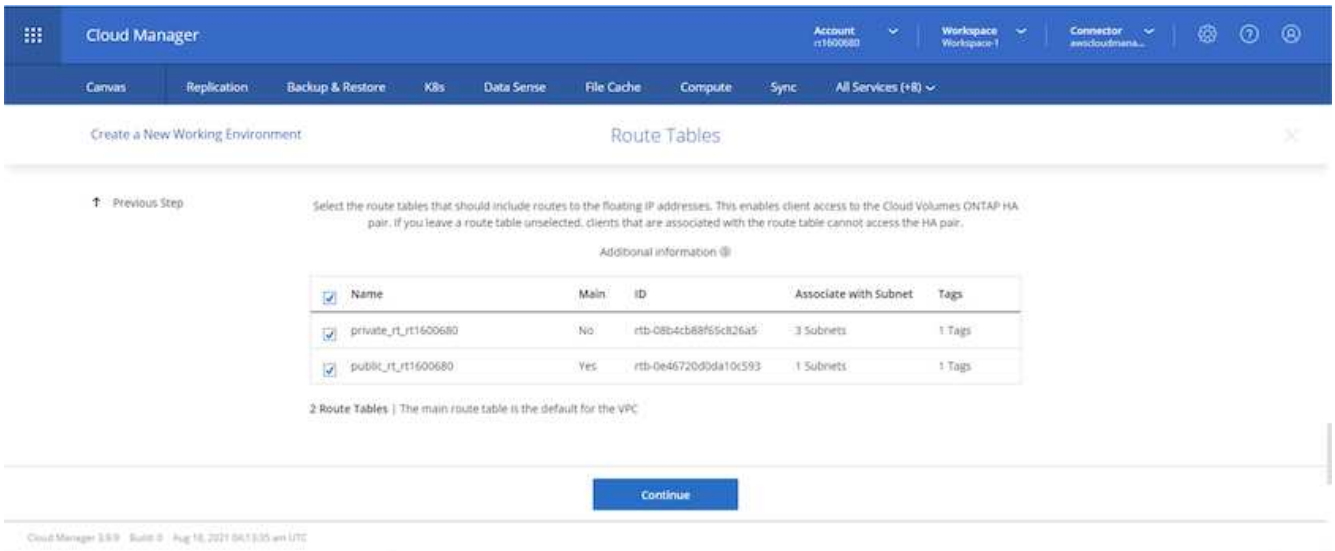


El mediador requiere comunicación con las API de AWS. No se requiere una dirección IP pública mientras se pueda acceder a las API después de que se haya puesto en marcha la instancia del mediador EC2.

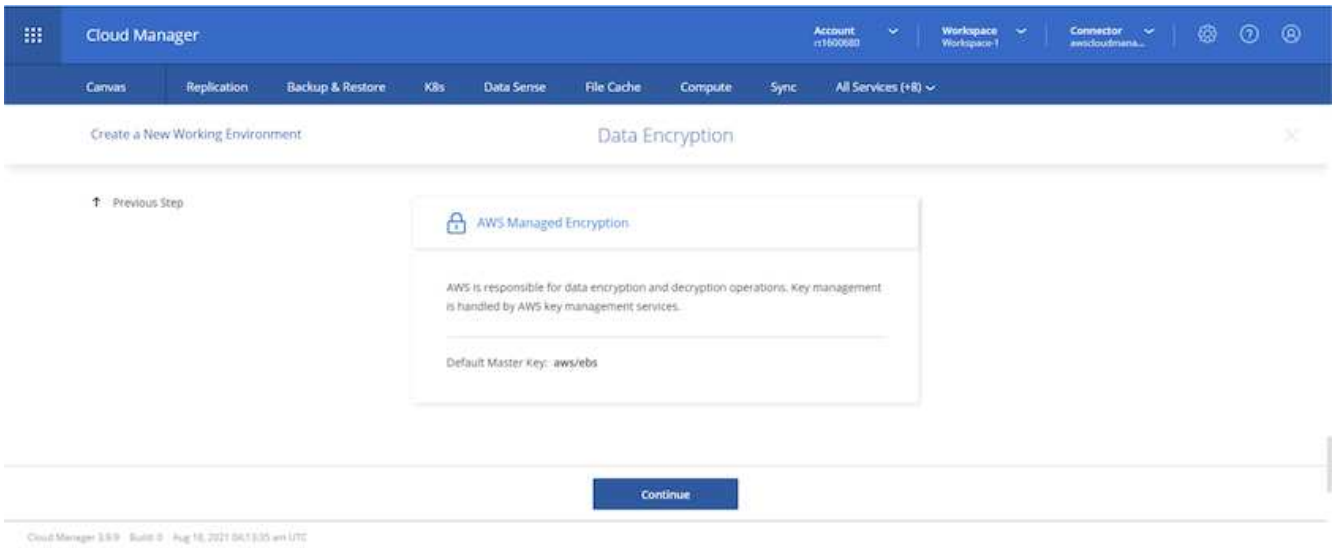
1. Las direcciones IP flotantes se usan para permitir el acceso a las diferentes direcciones IP que usa Cloud Volumes ONTAP, incluidas las IP de administración de clústeres y servicio de datos. Deben ser direcciones que no se puedan enrutar ya dentro de su red y que se agreguen a tablas de rutas en su entorno AWS. Estos son necesarios para habilitar direcciones IP constantes para un par de alta disponibilidad durante la conmutación por error. Puede encontrar más información acerca de las direcciones IP flotantes en el "Documentación en cloud de NetApp".



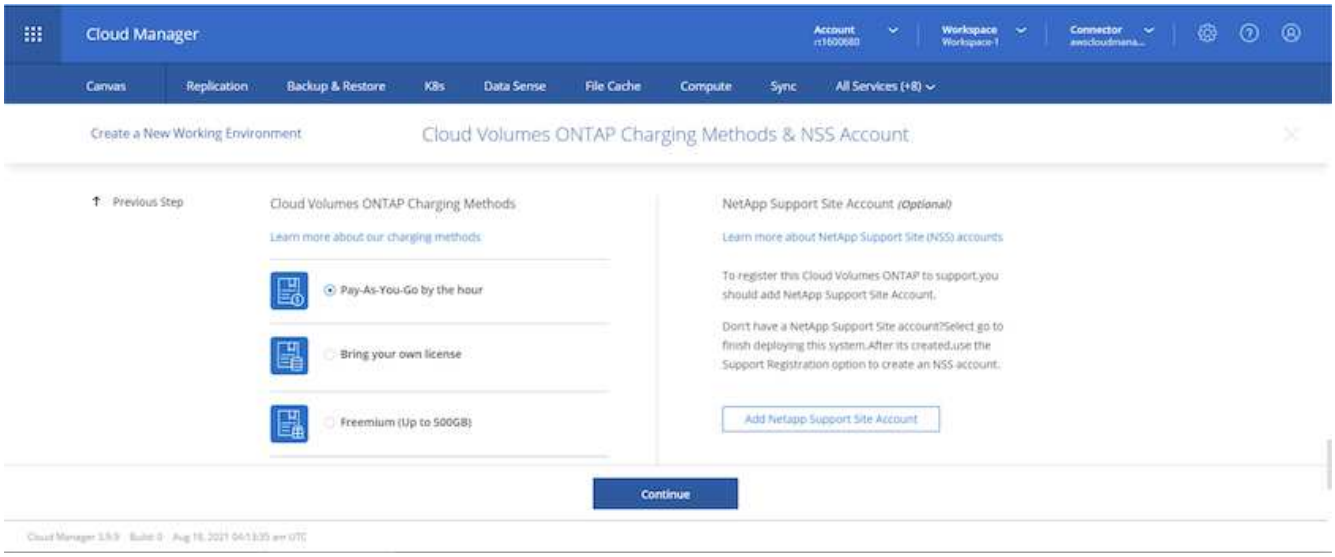
2. Seleccione a qué tablas de rutas se agregan las direcciones IP flotantes. Los clientes utilizan estas tablas de ruta para comunicarse con Cloud Volumes ONTAP.



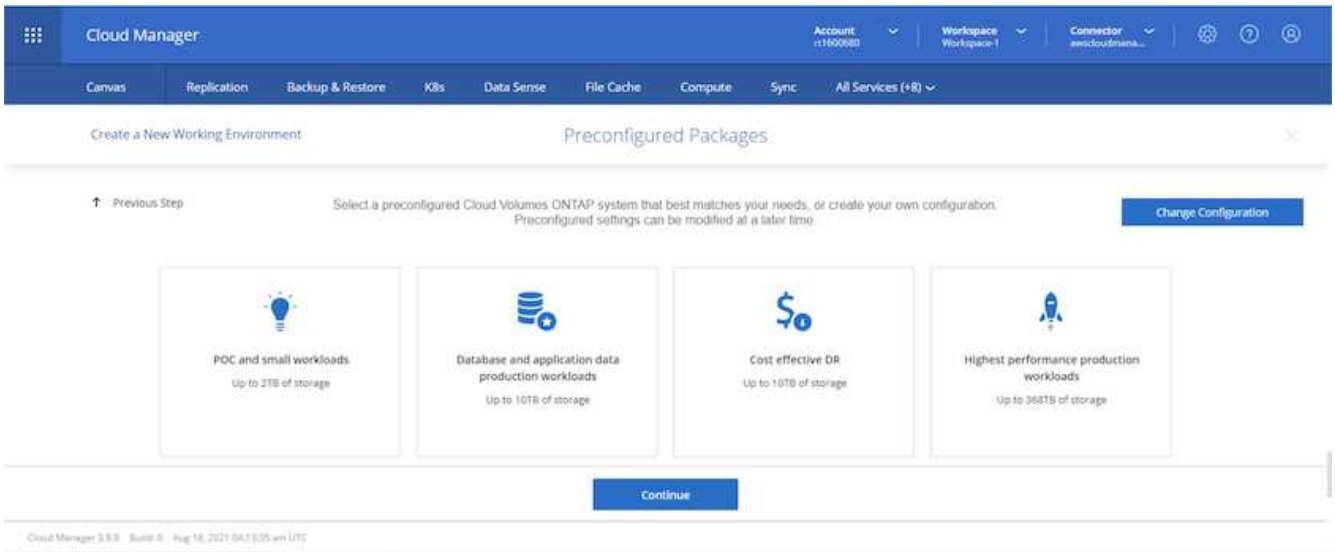
3. Elija si habilitar el cifrado gestionado de AWS o AWS KMS para cifrar los discos raíz, de arranque y de datos de ONTAP.



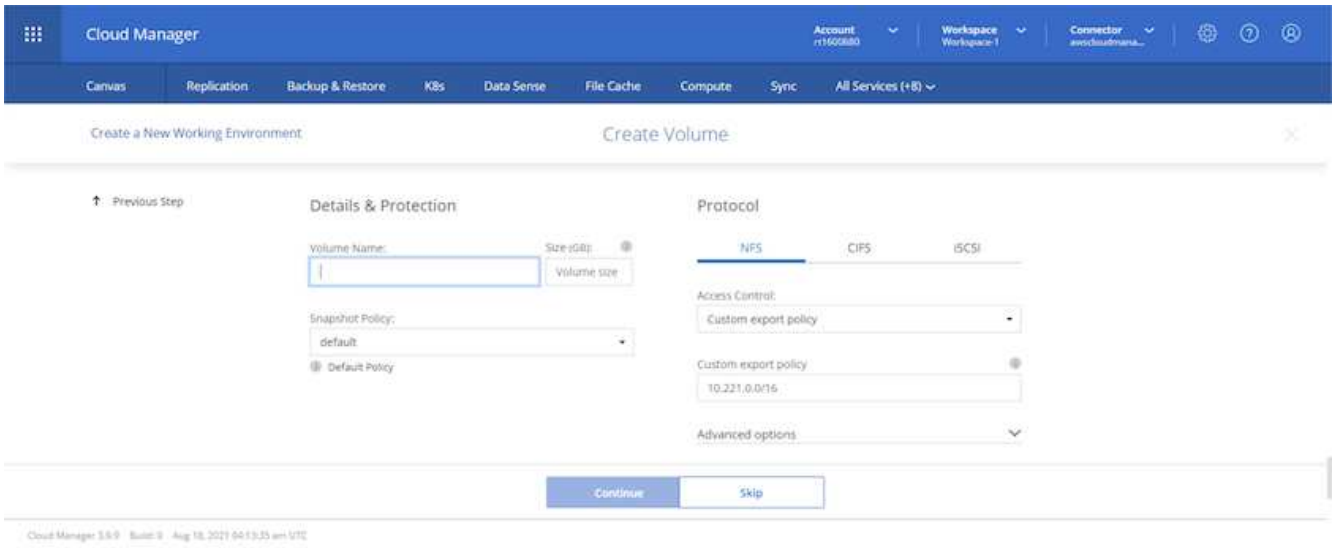
4. Elija su modelo de licencias. Si no sabe qué elegir, póngase en contacto con su representante de NetApp.



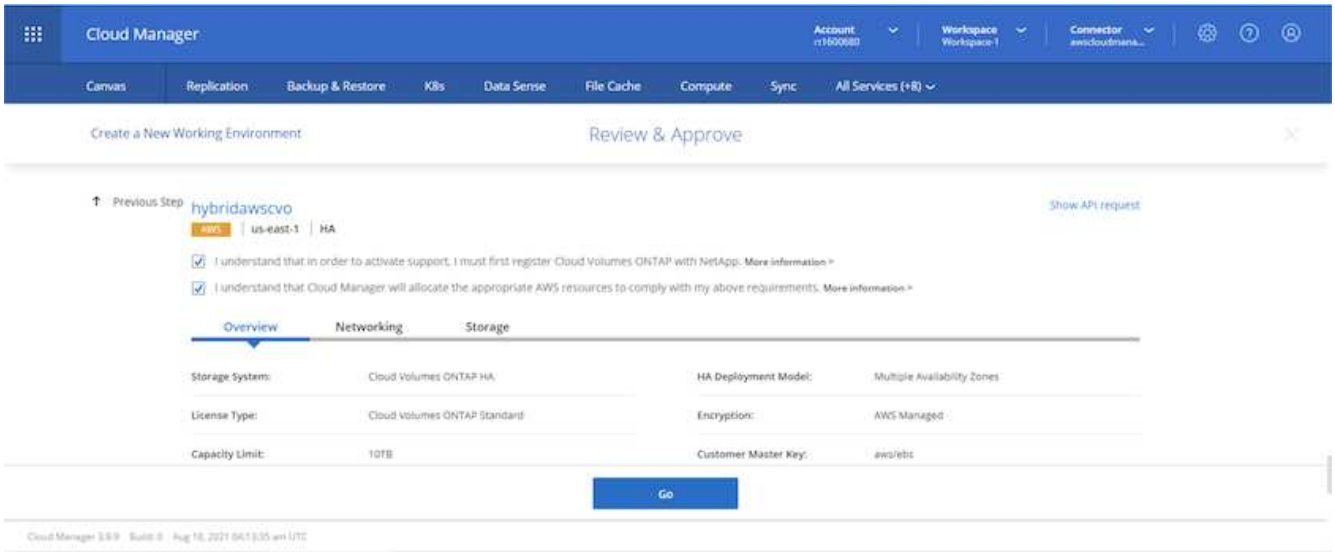
5. Seleccione la configuración que mejor se ajuste a su caso de uso. Esto se relaciona con las consideraciones de tamaño que se tratan en la página de requisitos previos.



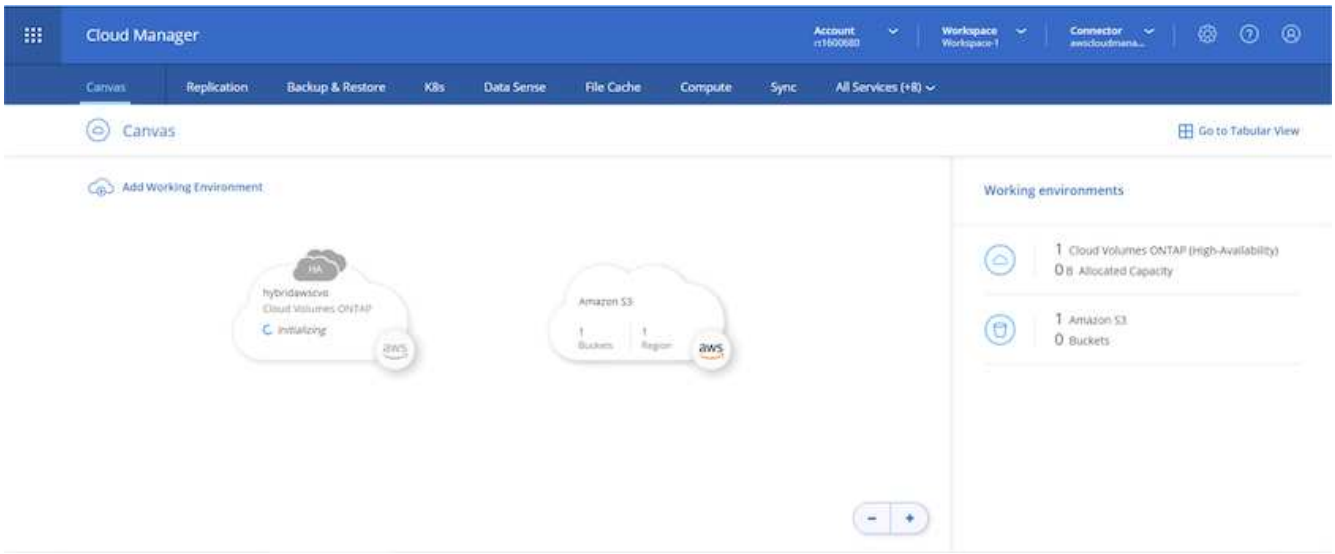
6. Opcionalmente, cree un volumen. Esto no es necesario, ya que los siguientes pasos utilizan SnapMirror, que nos crea los volúmenes.



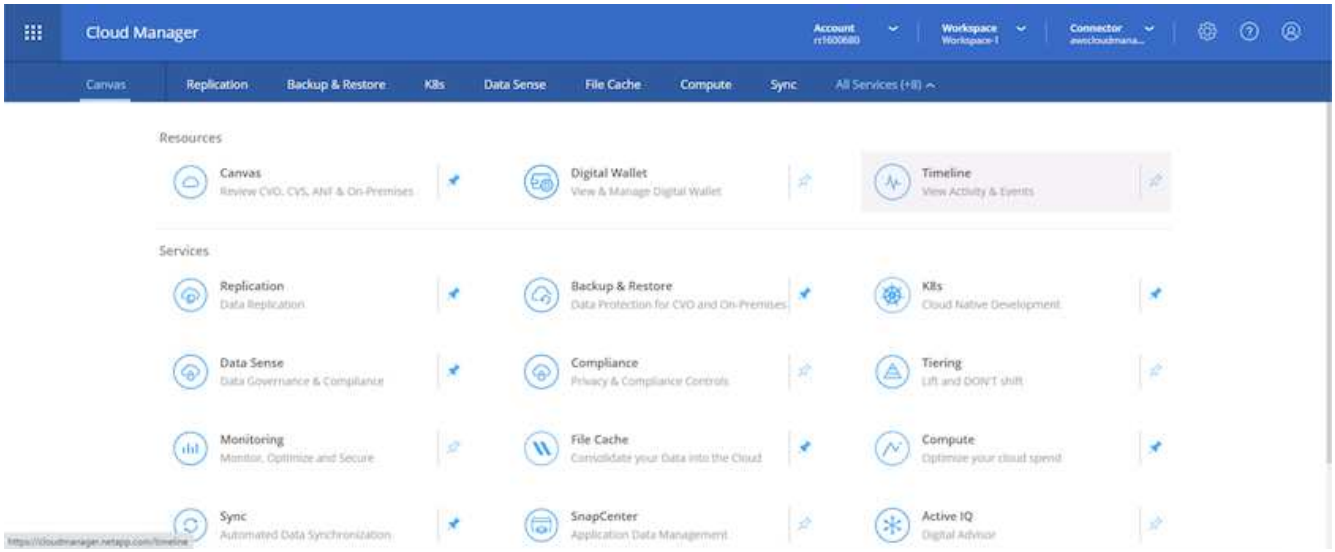
7. Revise las selecciones que se han realizado y marque las casillas para verificar que entiende que Cloud Manager pone en marcha recursos en su entorno AWS. Al terminar, haga clic en Go.



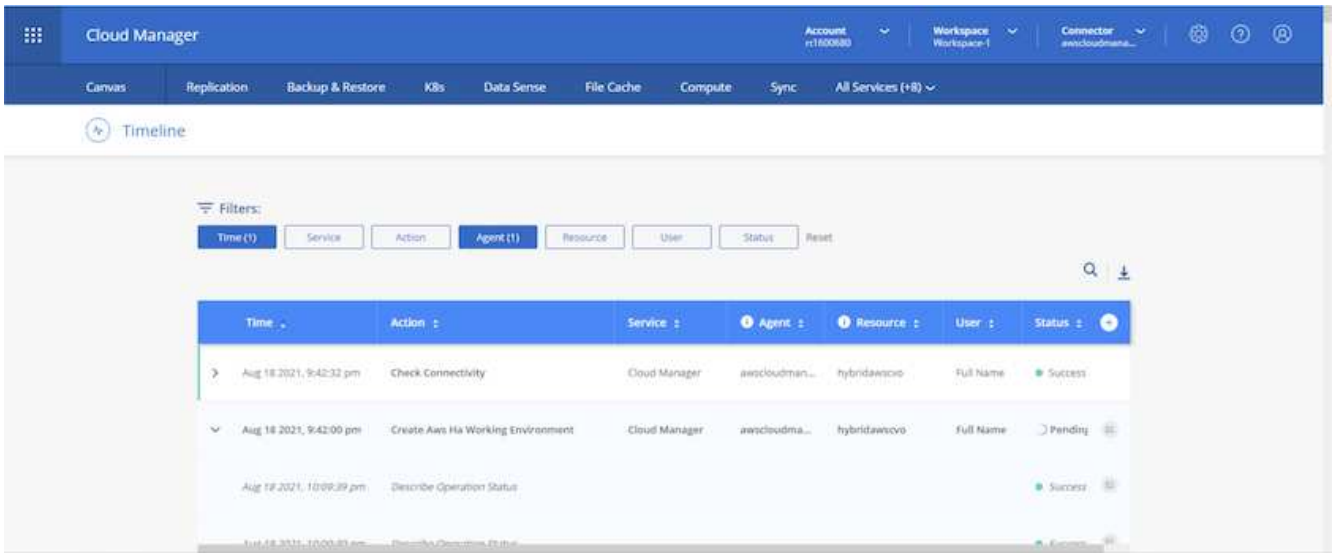
8. Cloud Volumes ONTAP inicia ahora su proceso de puesta en marcha. Cloud Manager utiliza las API de AWS y las pilas de formación de cloud para poner en marcha Cloud Volumes ONTAP. A continuación, configura el sistema de acuerdo con sus especificaciones, lo que le proporciona un sistema listo para usar que se puede utilizar al instante. El tiempo de este proceso varía en función de las selecciones realizadas.



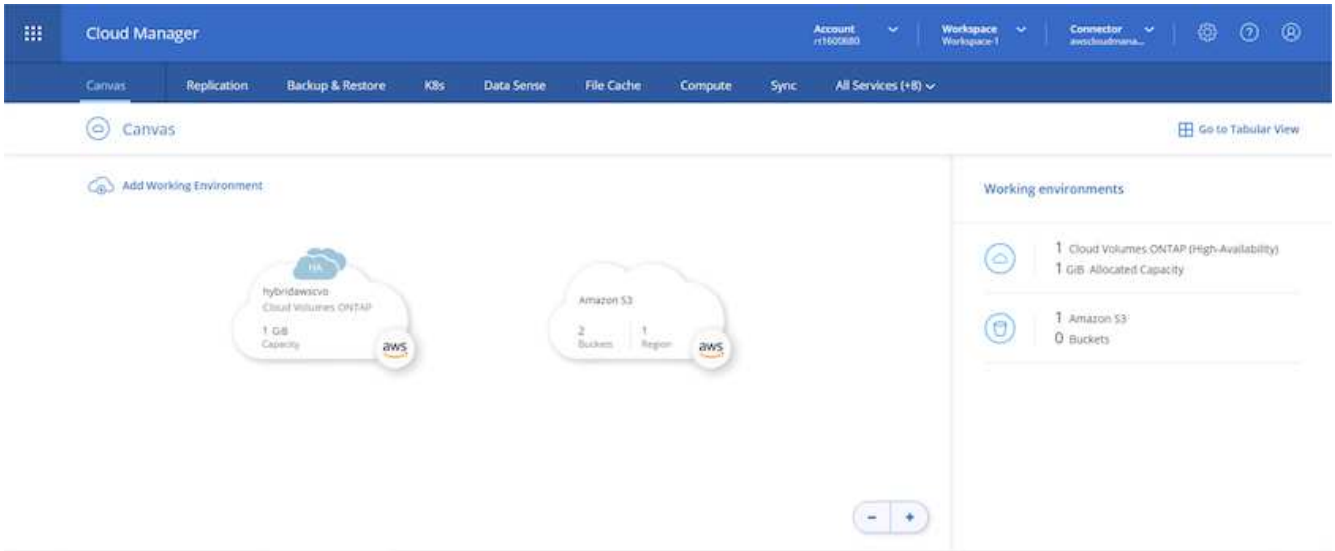
9. Puede supervisar el progreso navegando hasta la línea de tiempo.



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 en AWS y en el clúster de ONTAP. Esto también se puede utilizar de manera eficaz para solucionar cualquier problema que tenga.



11. Una vez completada la implementación, aparece el clúster CVO en el lienzo, que es la capacidad actual. El clúster de ONTAP en su estado actual está totalmente configurado para permitir una experiencia realmente lista para usar.

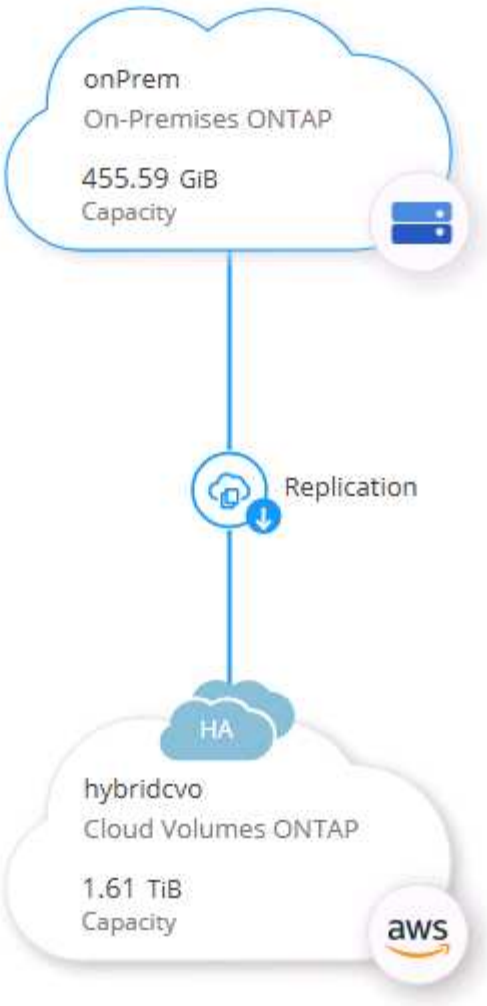


Configure SnapMirror de las instalaciones al cloud

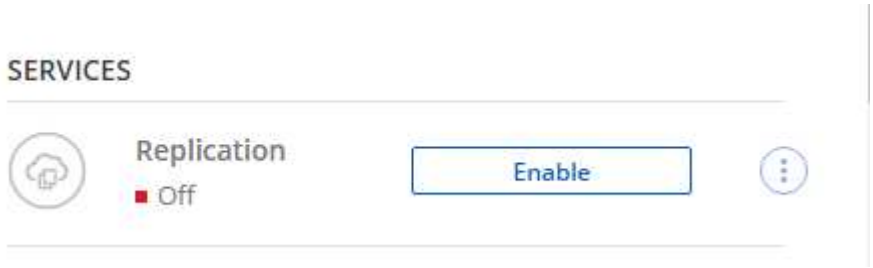
Ahora que tiene un sistema ONTAP de origen y un sistema ONTAP de destino implementados, puede replicar los volúmenes que contienen datos de base de datos en el cloud.

Para obtener una guía sobre las versiones compatibles de ONTAP para SnapMirror, consulte "Matriz de compatibilidad de SnapMirror".

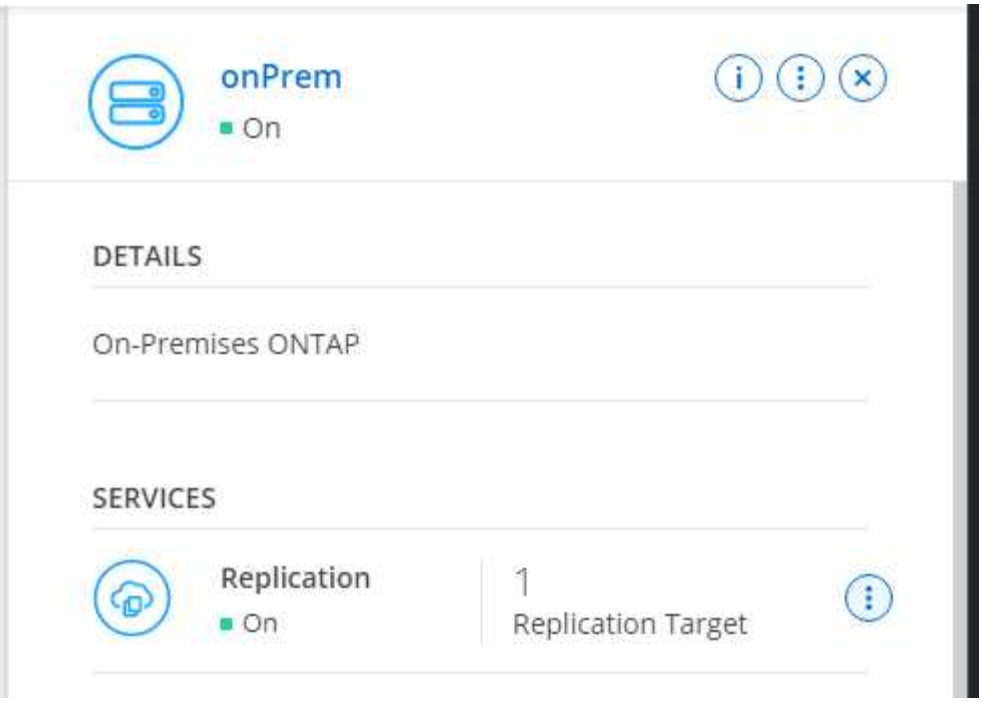
1. Haga clic en el sistema ONTAP de origen (en las instalaciones) y arrástrelo y colóquelo en el destino, seleccione replicación > Habilitar o seleccione replicación > Menú > replicar.



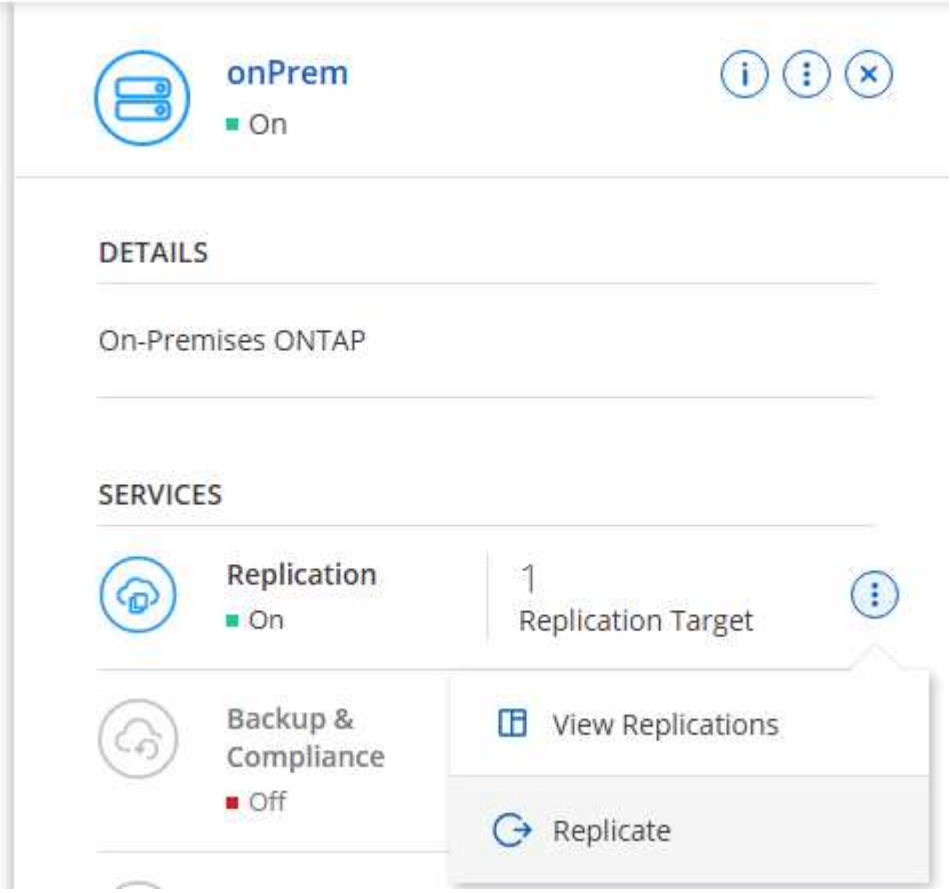
Seleccione Habilitar.



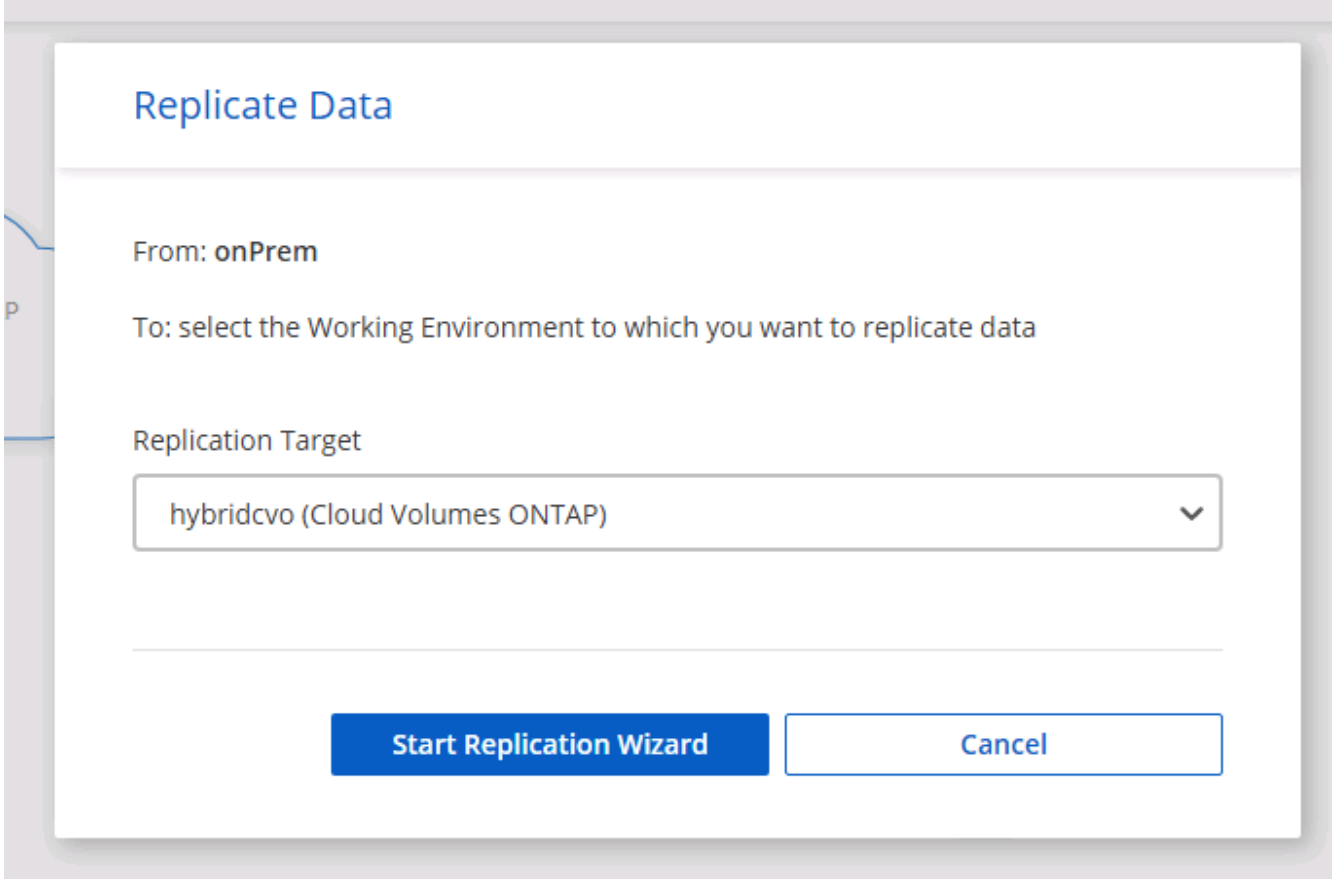
U Opciones.



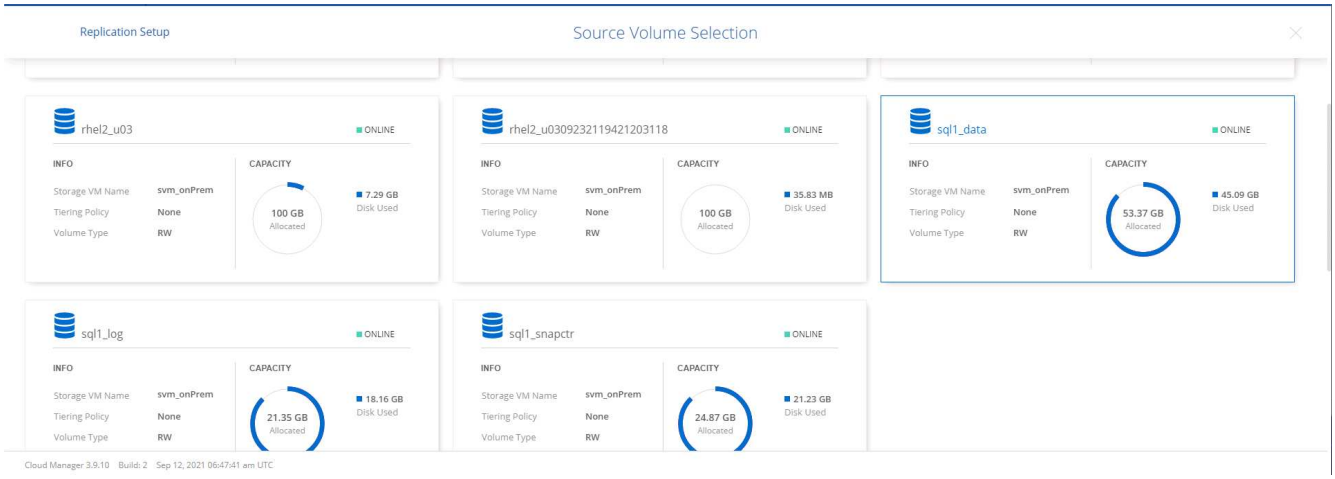
Replicar.



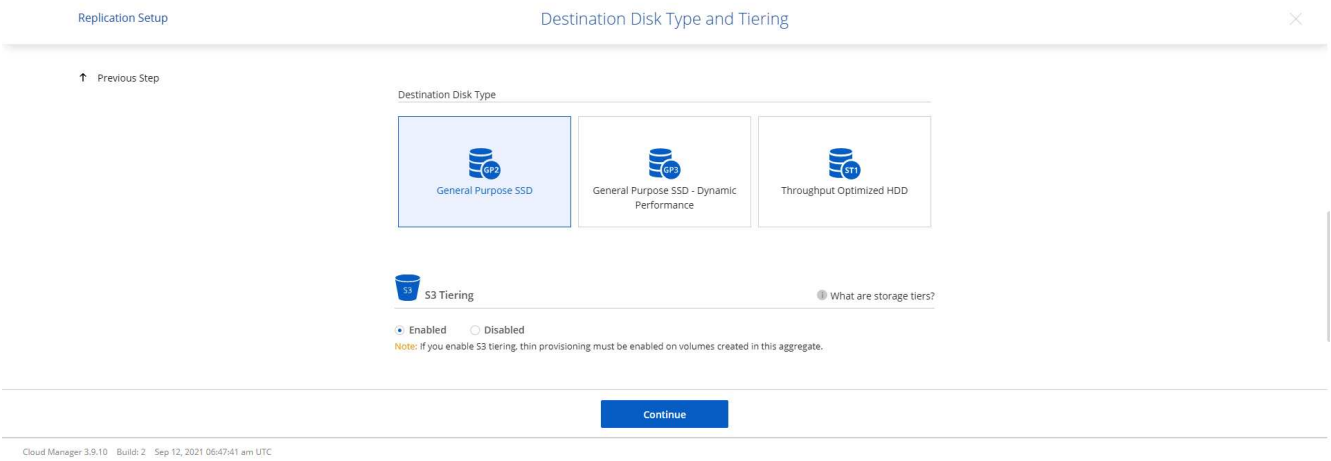
2. Si no ha arrastrado ni solado, elija el clúster de destino al que se va a replicar.



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

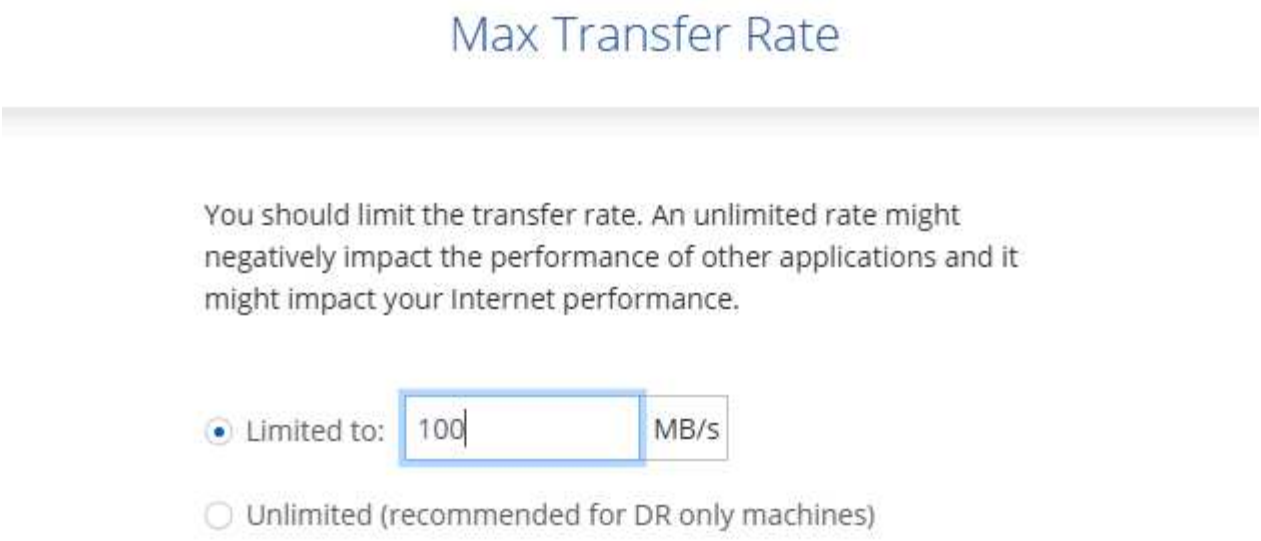


4. Elija el tipo de disco de destino y la política de organización en niveles. Para la recuperación ante desastres, recomendamos un SSD como tipo de disco y mantener la organización en niveles de los datos. Organización en niveles de datos ordena los datos duplicados en un almacenamiento de objetos de bajo coste y ahorra dinero en discos locales. Cuando se rompe la relación o se clona el volumen, los datos utilizan el almacenamiento local rápido.

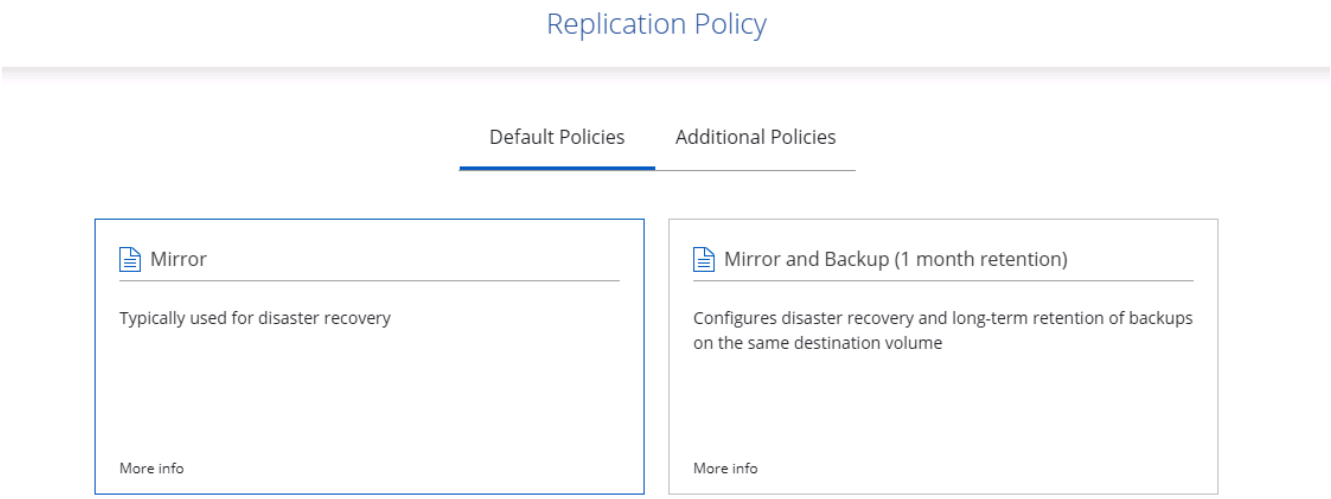


5. Seleccione el nombre del volumen de destino: Se ha elegido `[source_volume_name]_dr`.

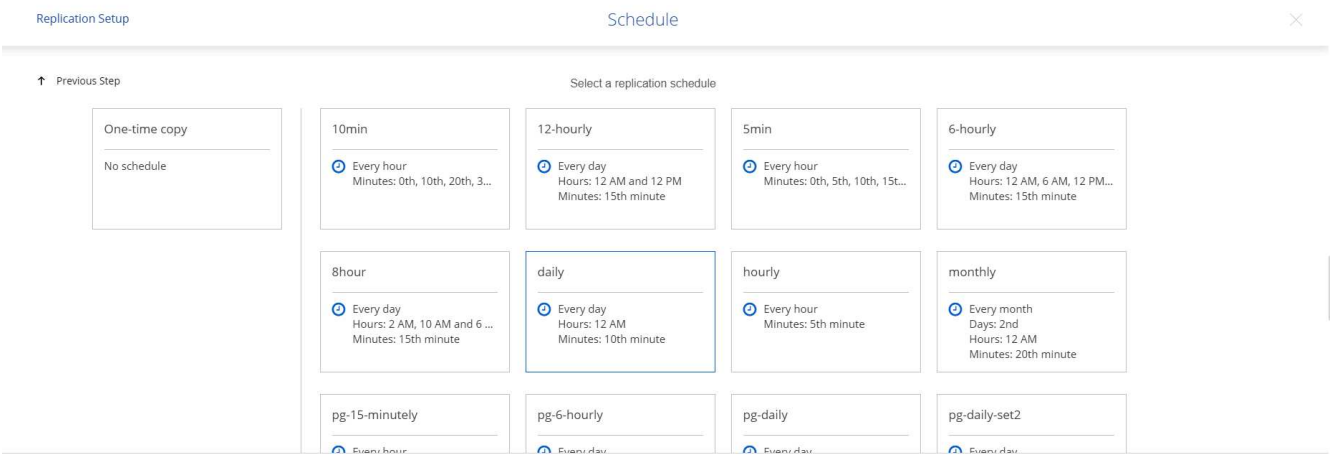
6. Seleccione la tasa de transferencia máxima para la replicación. Esto le permite ahorrar ancho de banda si dispone de una conexión de bajo ancho de banda a la nube, como una VPN.



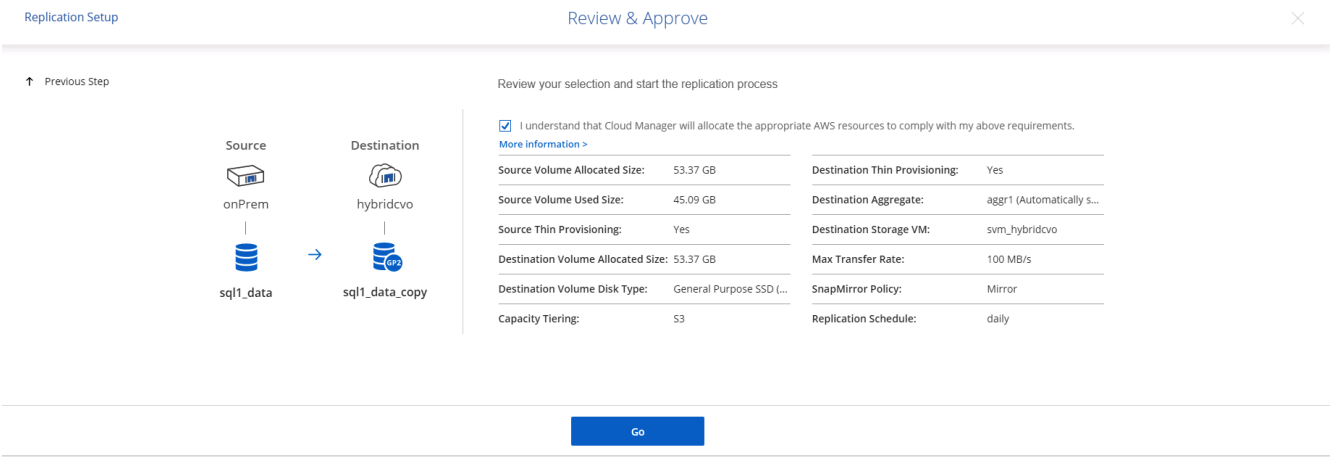
7. Defina la política de replicación. Elegimos un duplicado, que toma el conjunto de datos más reciente y lo replica en el volumen de destino. También puede elegir una política diferente en función de sus requisitos.



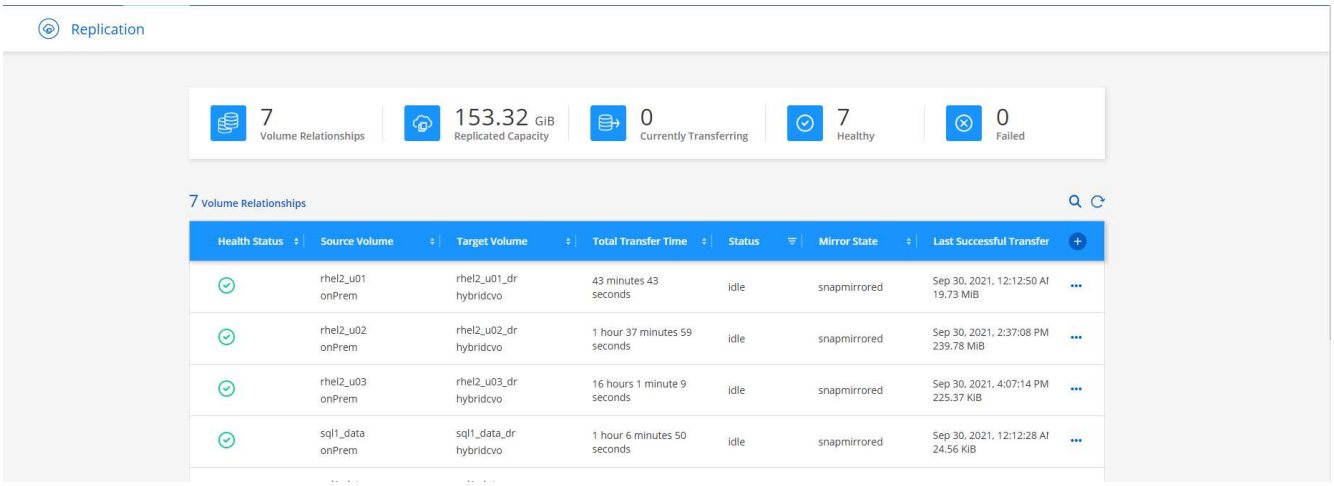
8. Elija la programación para activar la replicación. NetApp recomienda establecer una programación "diaria" de para el volumen de datos y una programación "por hora" para los volúmenes de registro, aunque esto se puede modificar en función de los requisitos.



9. Revise la información introducida, haga clic en Go para activar el par de clústeres y la SVM del mismo nivel (si esta es la primera vez que se replica entre los dos clústeres), y, a continuación, implemente e inicialice la relación de SnapMirror.



10. Continúe este proceso para los volúmenes de datos y los volúmenes de registro.
11. Para comprobar todas sus relaciones, acceda a la pestaña Replication de Cloud Manager. Aquí puede gestionar sus relaciones y comprobar su estado.



12. Una vez que se han replicado todos los volúmenes, tiene un estado constante y listo para pasar a los flujos de trabajo de recuperación ante desastres y de desarrollo y pruebas.

3. Implemente la instancia de computación de EC2 para las cargas de trabajo de bases de datos

AWS ha preconfigurado instancias informáticas de EC2 para distintas cargas de trabajo. La elección del tipo de instancia determina el número de núcleos de CPU, la capacidad de memoria, el tipo de almacenamiento y la capacidad, y el rendimiento de la red. Para los casos de uso, con la 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 que se deben tener en cuenta son la elección de los núcleos de CPU, la memoria y el nivel de rendimiento de la red. Aquí pueden encontrar los tipos de instancia típicos de AWS EC2: "Tipo de instancia de EC2".

Configurar el tamaño de la instancia de computación

1. Seleccione el tipo de instancia correcto en función de la carga de trabajo requerida. Entre los factores a tener en cuenta se incluye el número de transacciones de negocio que se deben admitir, el número de usuarios simultáneos, el tamaño de los conjuntos de datos, etc.
2. La implementación de instancias de EC2 se puede iniciar a través de la consola de EC2. Los procedimientos exactos de puesta en marcha superan el alcance de esta solución. Consulte "Amazon EC2" para obtener más detalles.

Configuración de instancias de Linux para carga de trabajo de Oracle

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

1. Agregue una instancia de Oracle en espera al servidor DNS para la resolución de nombres dentro del dominio de administración de SnapCenter.
2. Añada un ID de usuario de gestión de Linux como las credenciales del sistema operativo SnapCenter con permisos sudo sin contraseña. Habilite el ID con la autenticación de contraseña de SSH en la instancia de EC2. (De forma predeterminada, la autenticación de contraseña SSH y sudo sin contraseñas está desactivada en instancias de EC2).
3. Configurar la instalación de Oracle de modo que coincida con la instalación de Oracle en las instalaciones, como los parches de sistema operativo, las versiones y parches de Oracle, etc.
4. Los roles de automatización de bases de datos de Ansible de NetApp pueden aprovecharse para configurar instancias de EC2 para casos de uso de desarrollo y pruebas de bases de datos y recuperación ante desastres. El código de automatización puede descargarse del sitio de GitHub público de NetApp: "Implementación automatizada de Oracle 19c". El objetivo consiste en instalar y configurar una pila de software de base de datos en una instancia de EC2 para coincidir con las configuraciones de sistemas operativos y bases de datos locales.

Configuración de instancias de Windows para carga de trabajo de SQL Server

En esta sección se enumeran los pasos de configuración adicionales tras la implementación inicial de una instancia de EC2 de Windows.

1. Recupere la contraseña del administrador de Windows para iniciar sesión en una instancia mediante RDP.
2. Deshabilite el firewall de Windows, únase al host al dominio de Windows SnapCenter y agregue la instancia al servidor DNS para la resolución de nombres.
3. Aprovisionar un volumen de registro de SnapCenter para almacenar los archivos de registro de SQL Server.
4. Configure iSCSI en el host Windows para montar el volumen y formatear la unidad de disco.
5. De nuevo, muchas de las tareas anteriores se pueden automatizar con la solución de automatización de

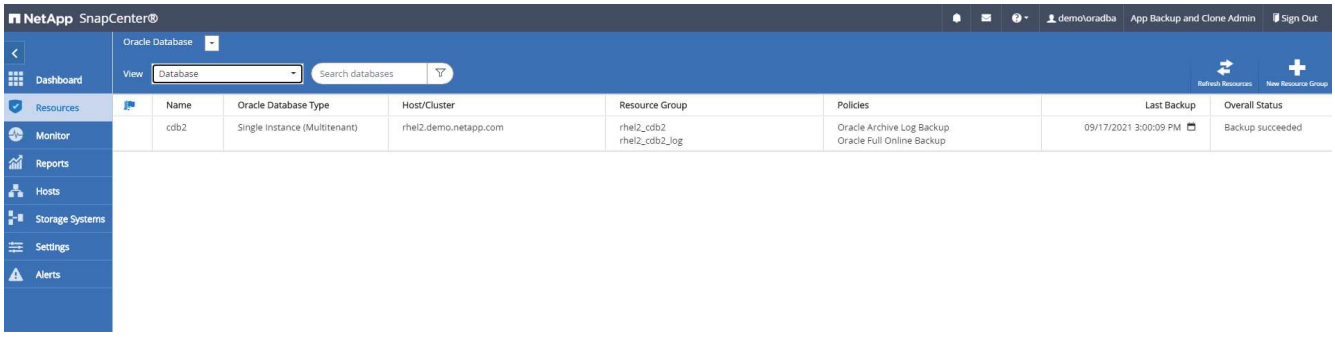
NetApp para SQL Server. Visite el sitio de GitHub público de automatización de NetApp para comprobar las funciones y soluciones recién publicadas: "Automatización de NetApp".

Flujo de trabajo para la descarga de pruebas y desarrollo en el cloud

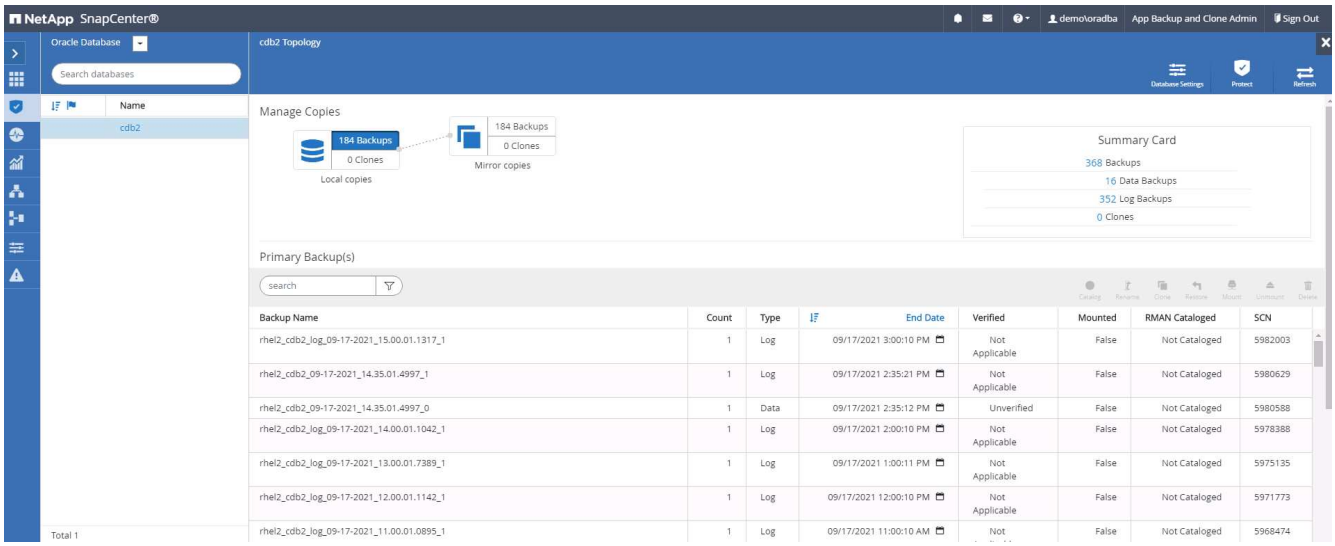
La agilidad del cloud público, la rentabilidad de la inversión y la reducción de los costes son propuestas de valor significativas para empresas que adoptan el cloud público para el esfuerzo de desarrollo y pruebas de aplicaciones de bases de datos. No hay mejor herramienta que SnapCenter para hacer esto una realidad. SnapCenter no solo puede proteger su base de datos de producción localmente, sino que también puede clonar rápidamente una copia para desarrollar o probar código en el cloud público mientras consume muy poco almacenamiento adicional. A continuación se detallan los procesos paso a paso para utilizar esta herramienta.

Clonar una base de datos de Oracle para desarrollo y pruebas a partir de un backup de Snapshot replicado

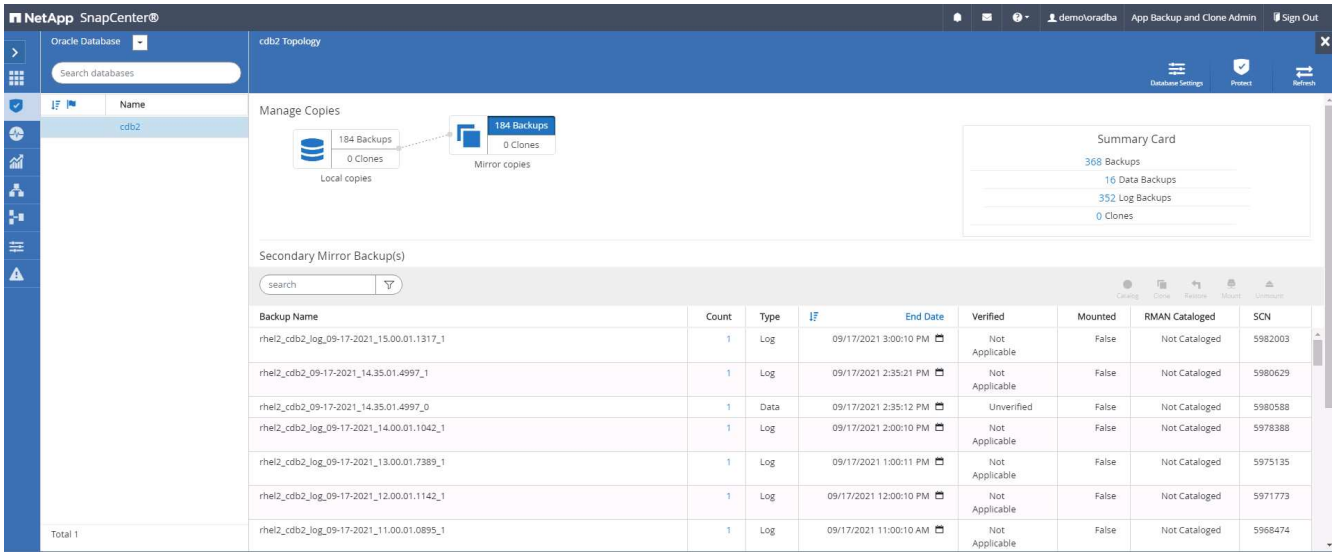
1. Inicie sesión en SnapCenter con un ID de usuario de administración de bases de datos para Oracle. Desplácese hasta la pestaña Resources, donde se muestran las bases de datos de Oracle que está protegida por SnapCenter.



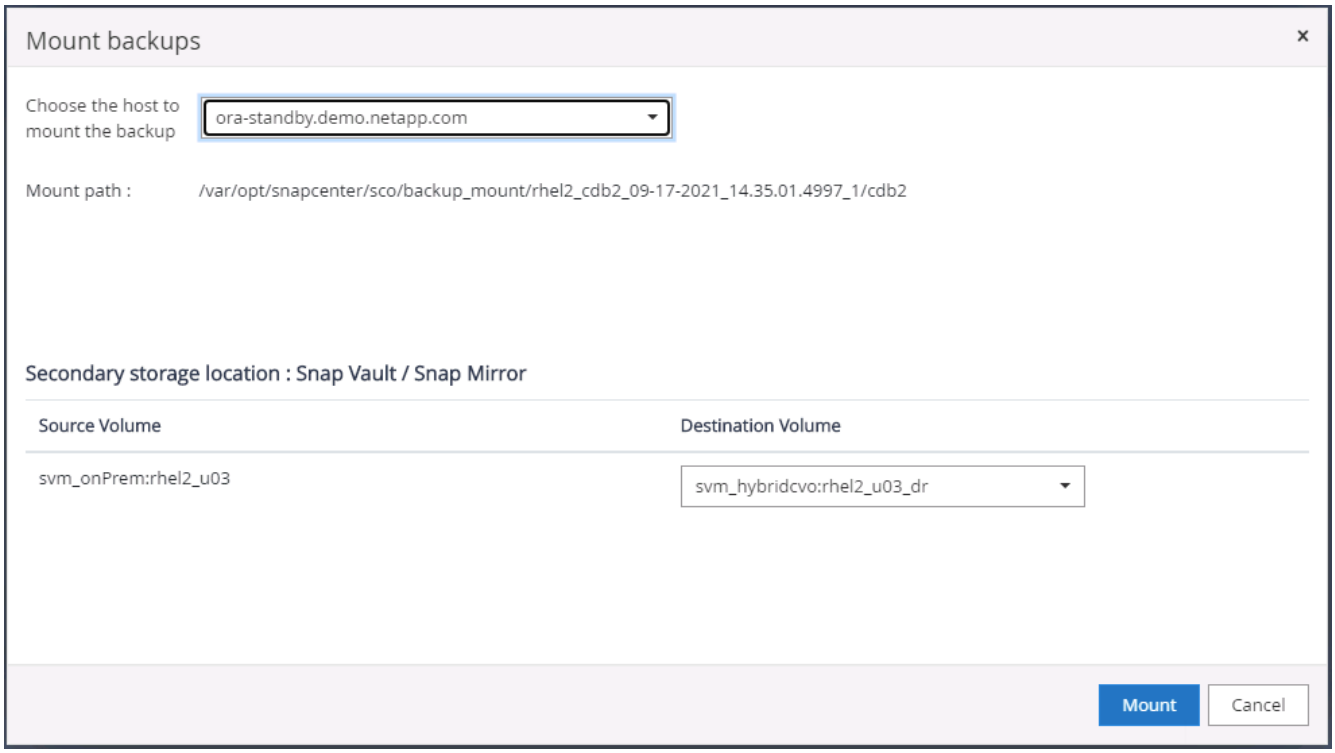
2. Haga clic en el nombre de la base de datos en las instalaciones indicado para la topología de backup y la vista detallada. Si se habilita una ubicación de replicación secundaria, se muestran backups de reflejos vinculados.

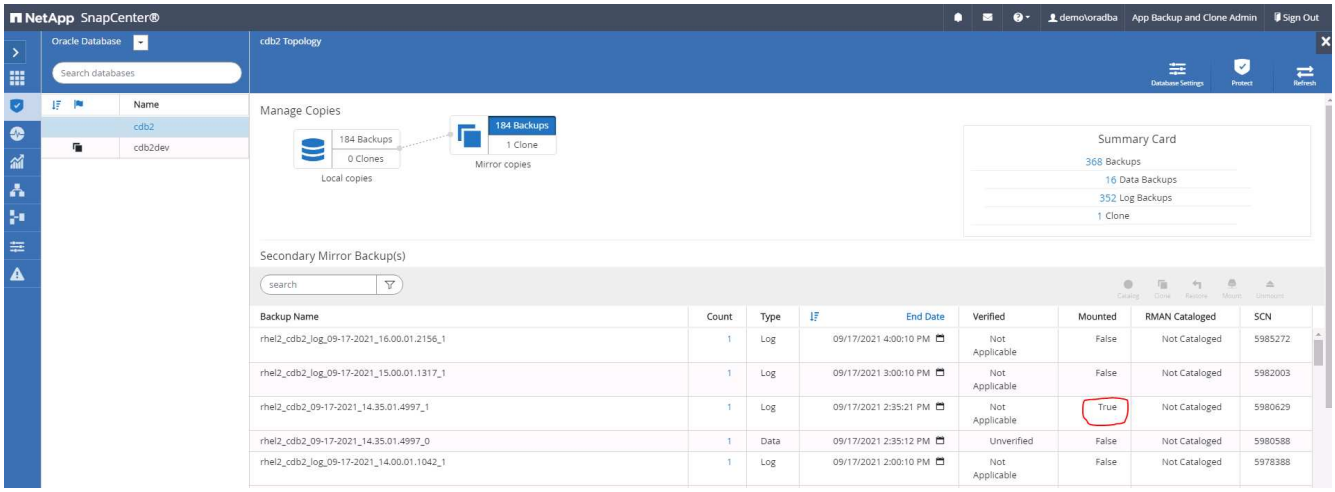


3. Para alternar la vista de backups reflejados, haga clic en backups reflejados. Luego, se muestran los backups de reflejos secundarios.



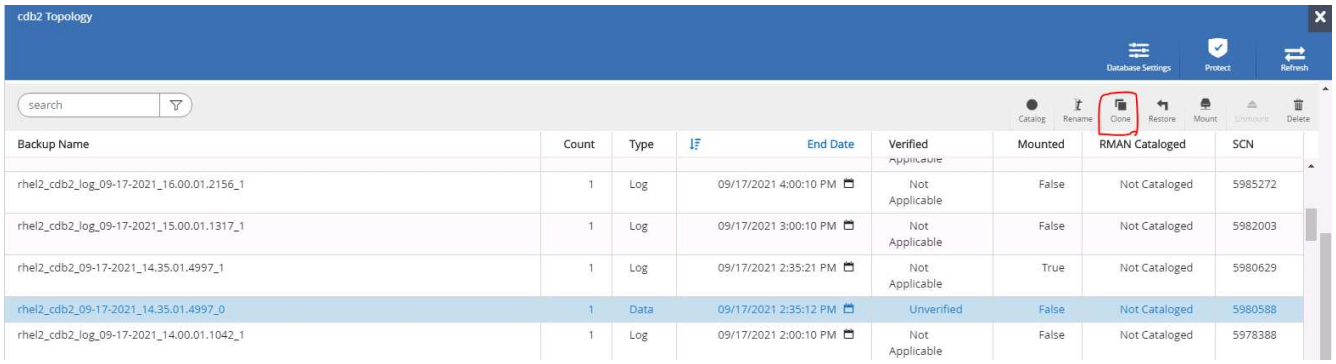
4. Elija una copia de backup de base de datos secundaria reflejada que se clonará y determine un punto de recuperación por tiempo y número de cambio de sistema o por SCN. Por lo general, el punto de recuperación debe contener el tiempo de backup completo de la base de datos o el SCN que se va a clonar. Una vez decidido un punto de recuperación, es necesario montar el backup de archivo de registro necesario para la recuperación. El backup del archivo de registro debe montarse en el servidor de la base de datos de destino donde se va a alojar la base de datos del clon.



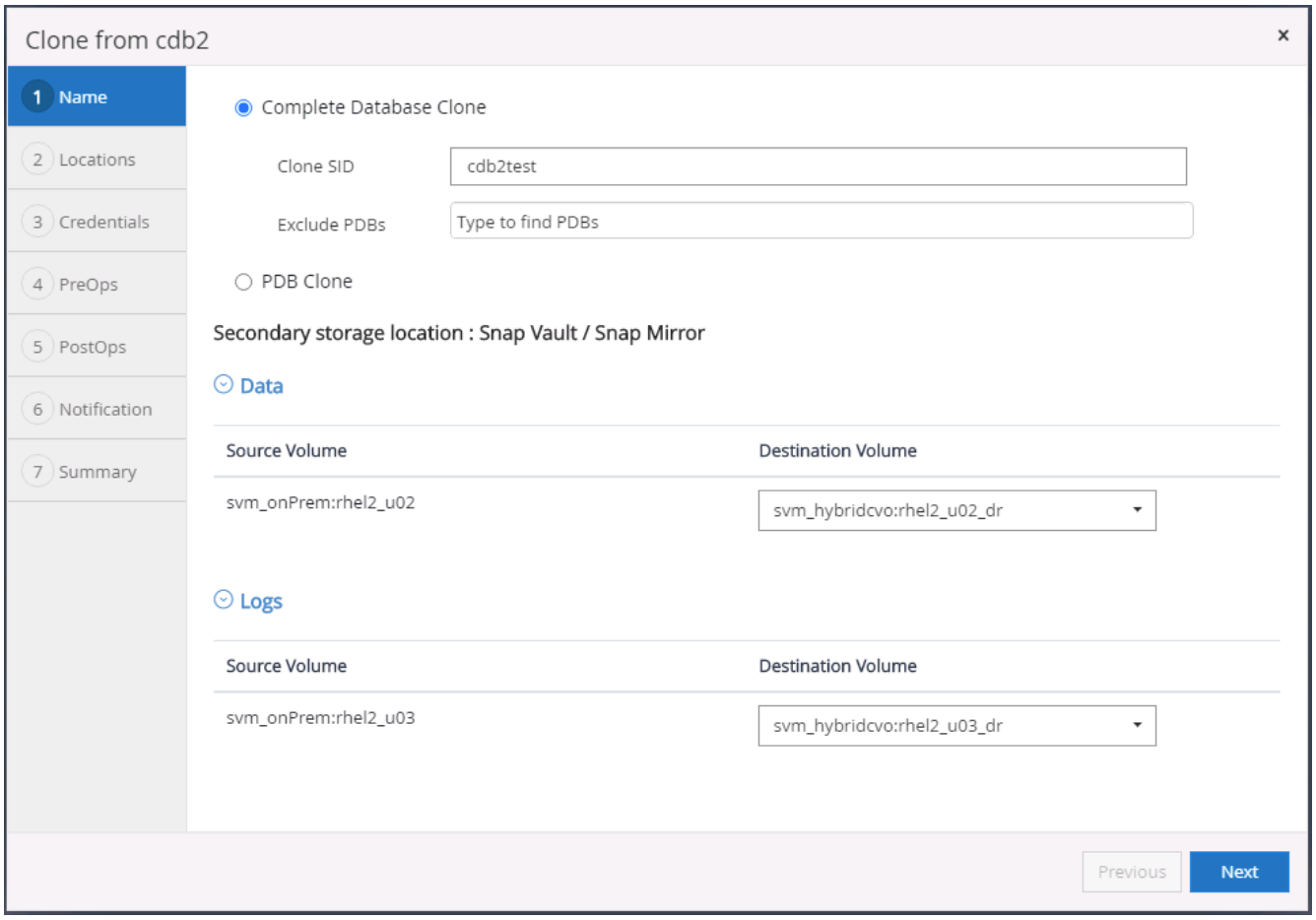


Si se habilita la eliminación de registros y el punto de recuperación se amplía más allá de la última eliminación de registros, es posible que sea necesario montar varios backups de registros de archivo.

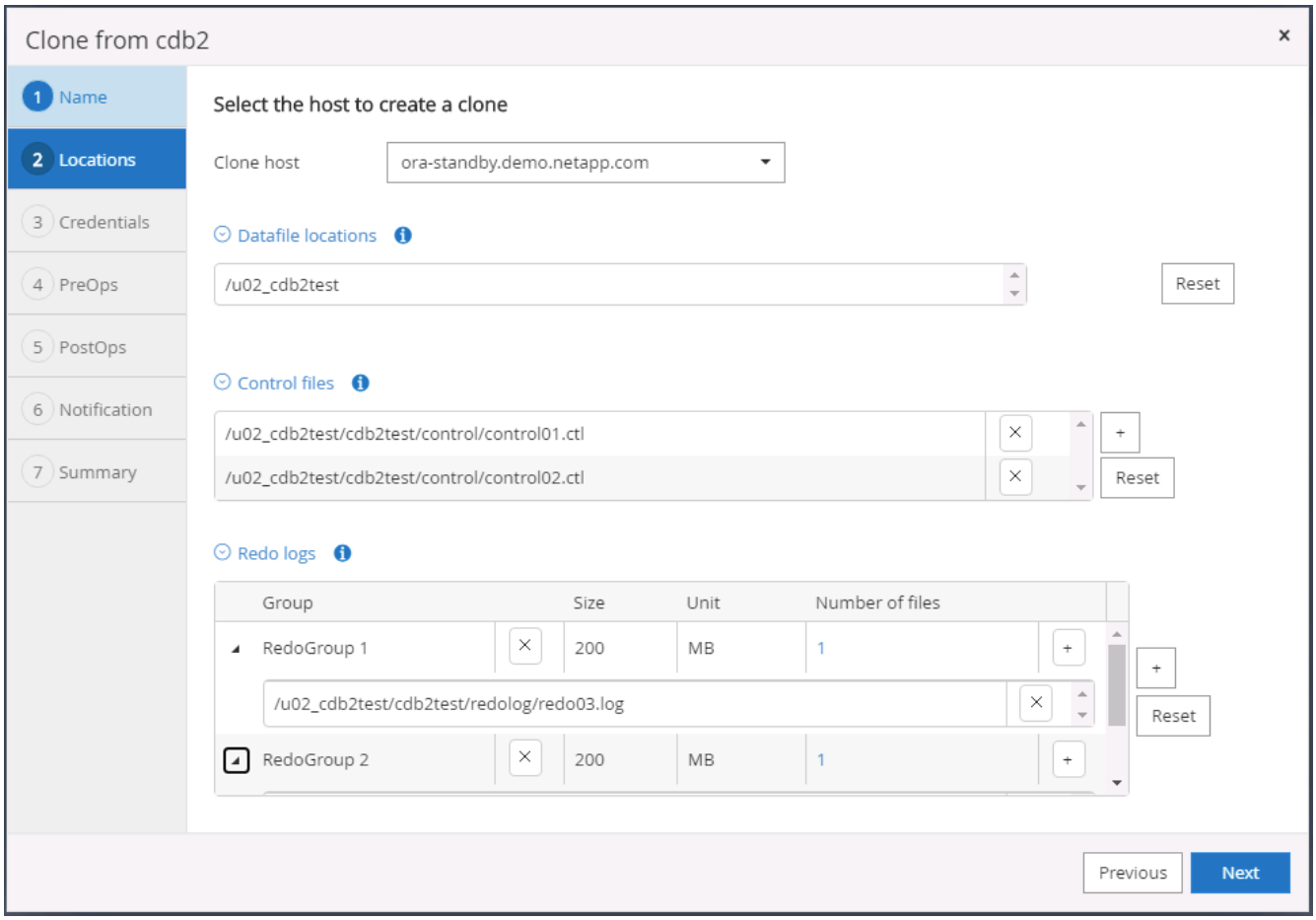
5. Destaque la copia de backup completa de la base de datos que se va a clonar y haga clic en el botón clonar para iniciar el flujo de trabajo de clonado de base de datos.



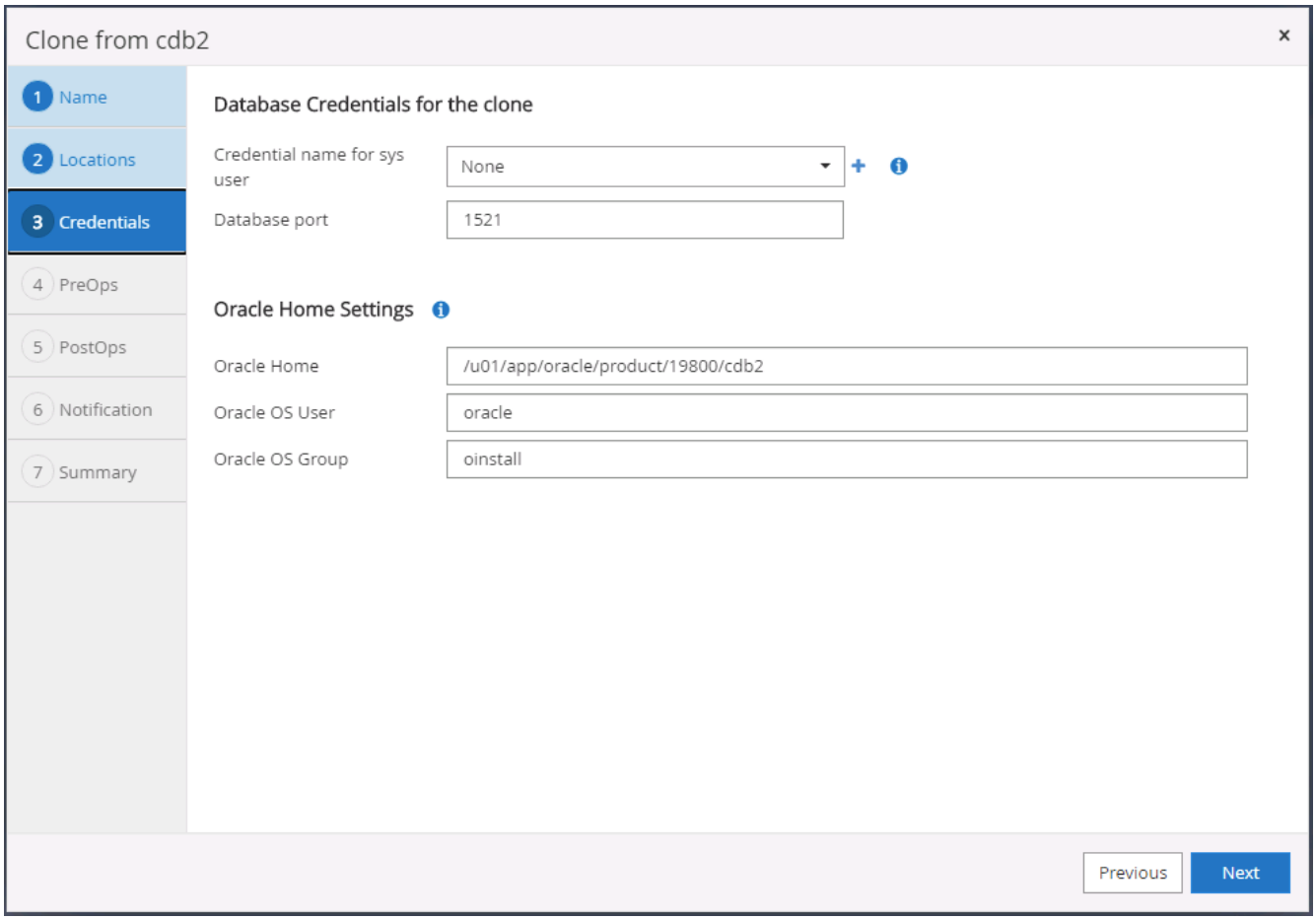
6. Elija un SID de base de datos del clon adecuado para una base de datos completa del contenedor o un clon de la CDB.



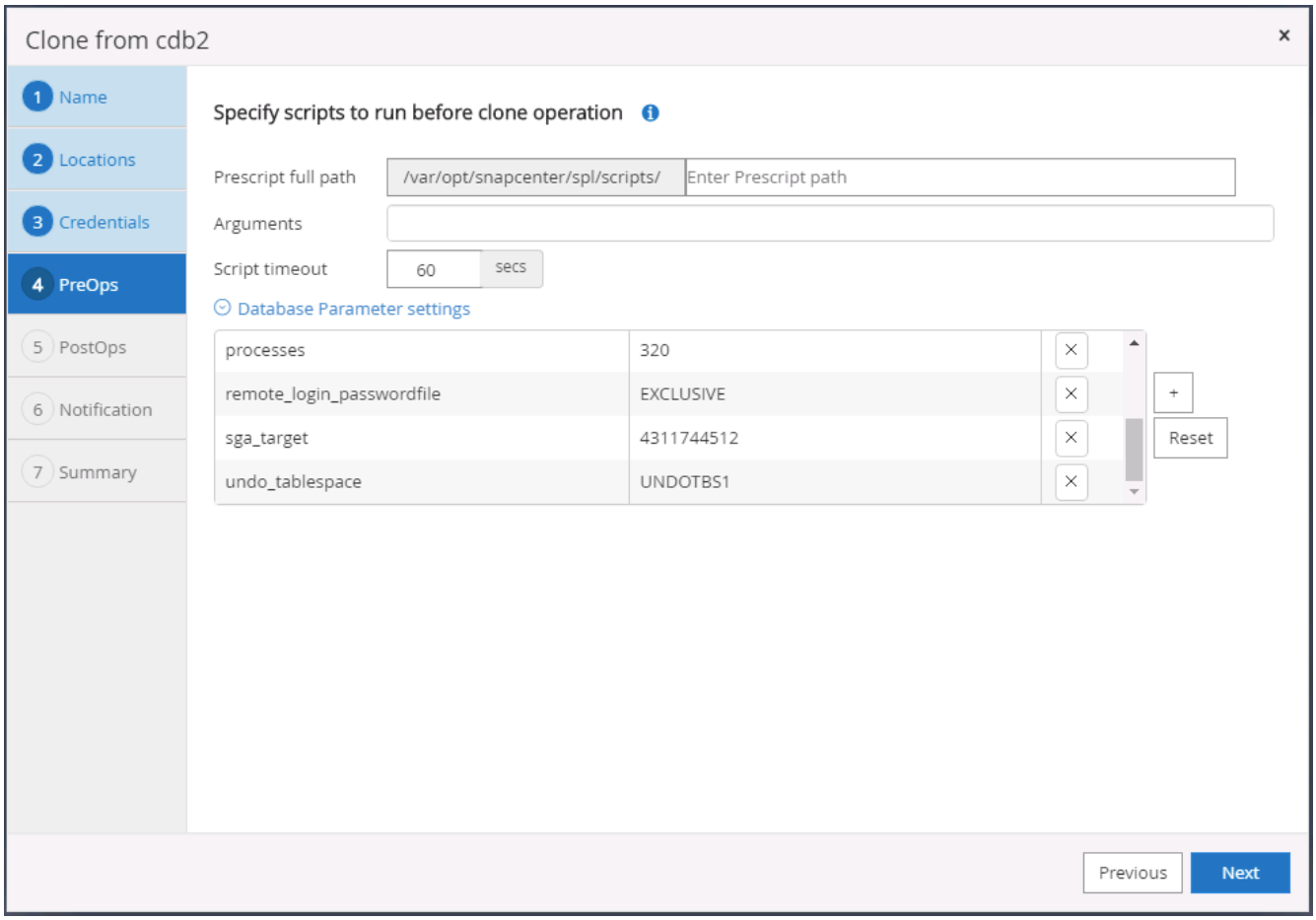
7. Seleccione el host del clon objetivo en el cloud y el flujo de trabajo del clon creará el archivo de datos, el archivo de control y los directorios de registro de recuperación.



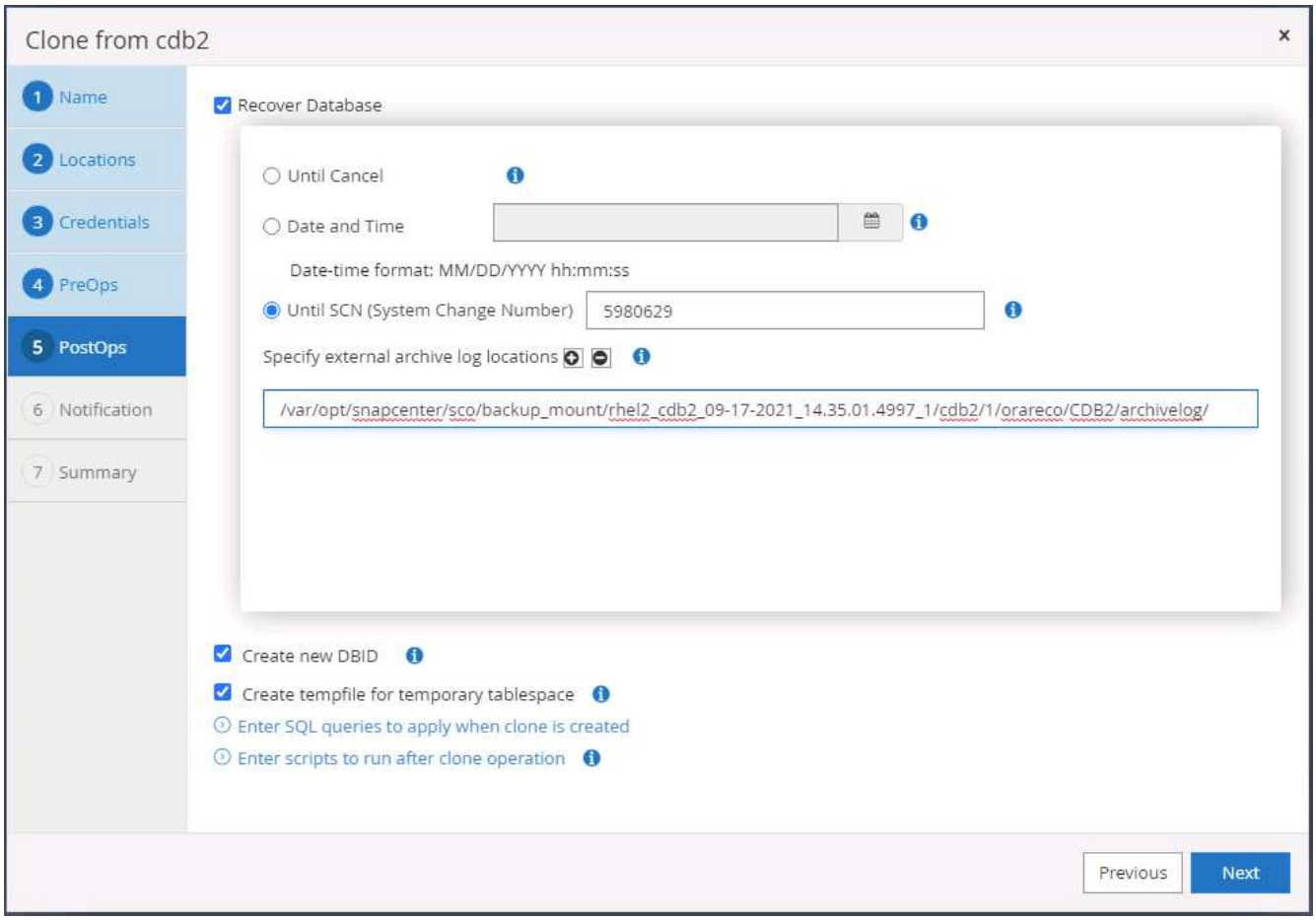
8. El nombre de la credencial None se utiliza para la autenticación basada en el sistema operativo, lo que hace que el puerto de la base de datos sea irrelevante. Rellene el directorio inicial de Oracle, el usuario del sistema operativo Oracle y el grupo del sistema operativo Oracle que se hayan configurado en el servidor de la base de datos del clon de destino.

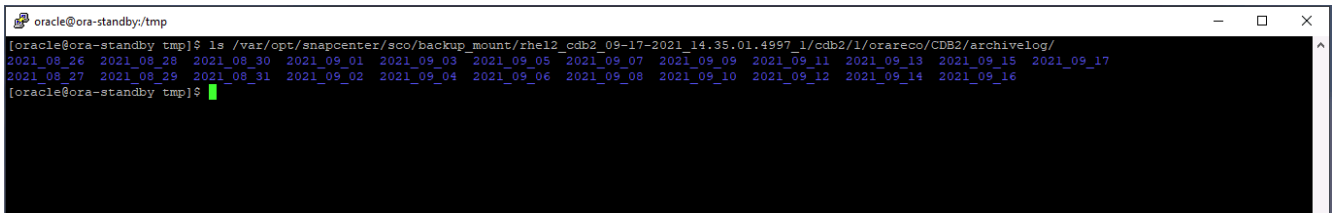


9. Especifique los scripts que se ejecutarán antes de la operación de clonado. Lo que es más importante, el parámetro de instancia de base de datos se puede ajustar o definir aquí.

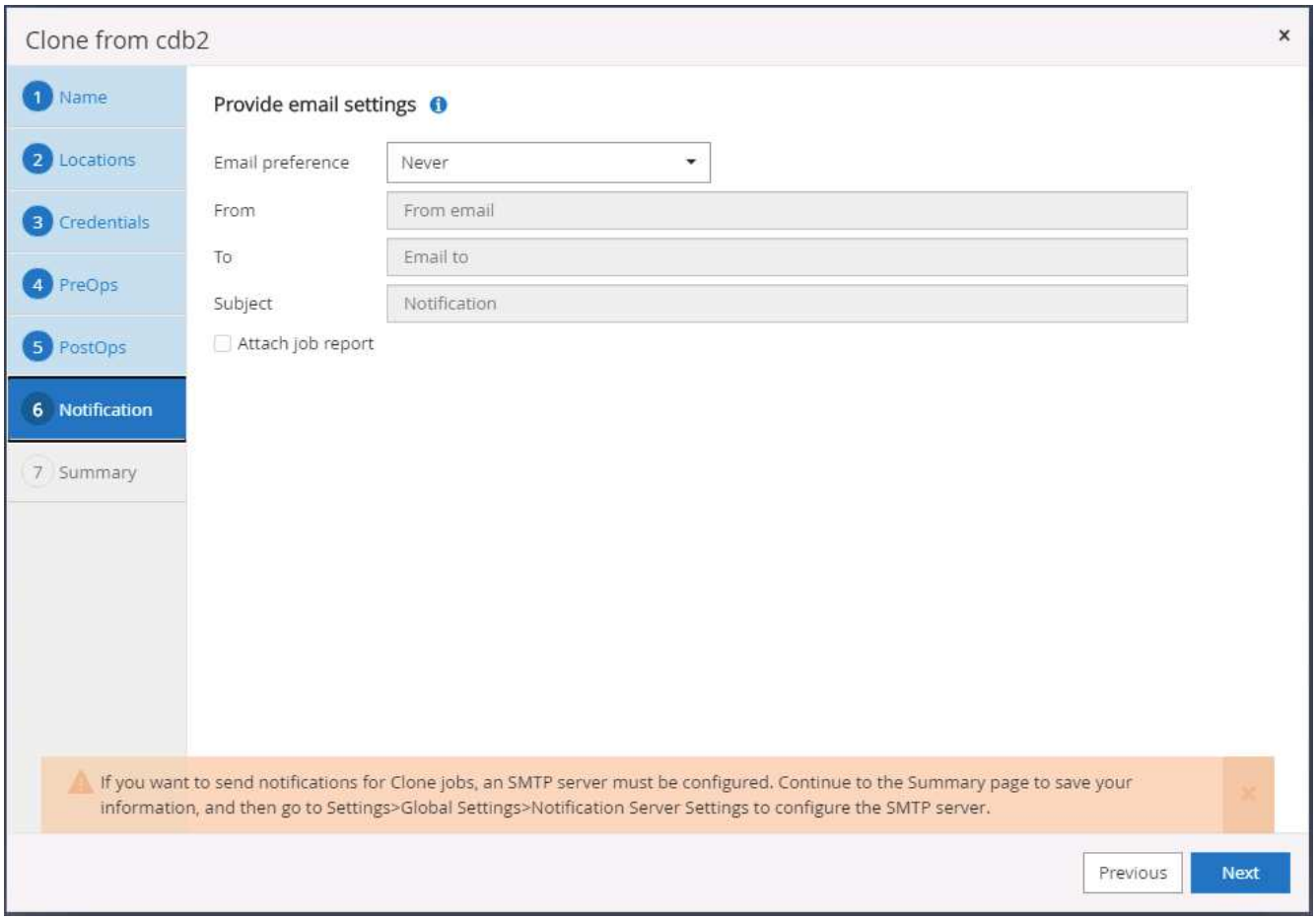


10. Especifique el punto de recuperación por fecha y hora o SCN. Until Cancel recupera la base de datos hasta los registros de archivo disponibles. Especifique la ubicación del registro de archivos externo desde el host de destino donde se monta el volumen de registro de archivos. Si el propietario de Oracle del servidor de destino es diferente del servidor de producción local, compruebe que el propietario de Oracle del servidor de destino puede leer el directorio de registro de archivado.

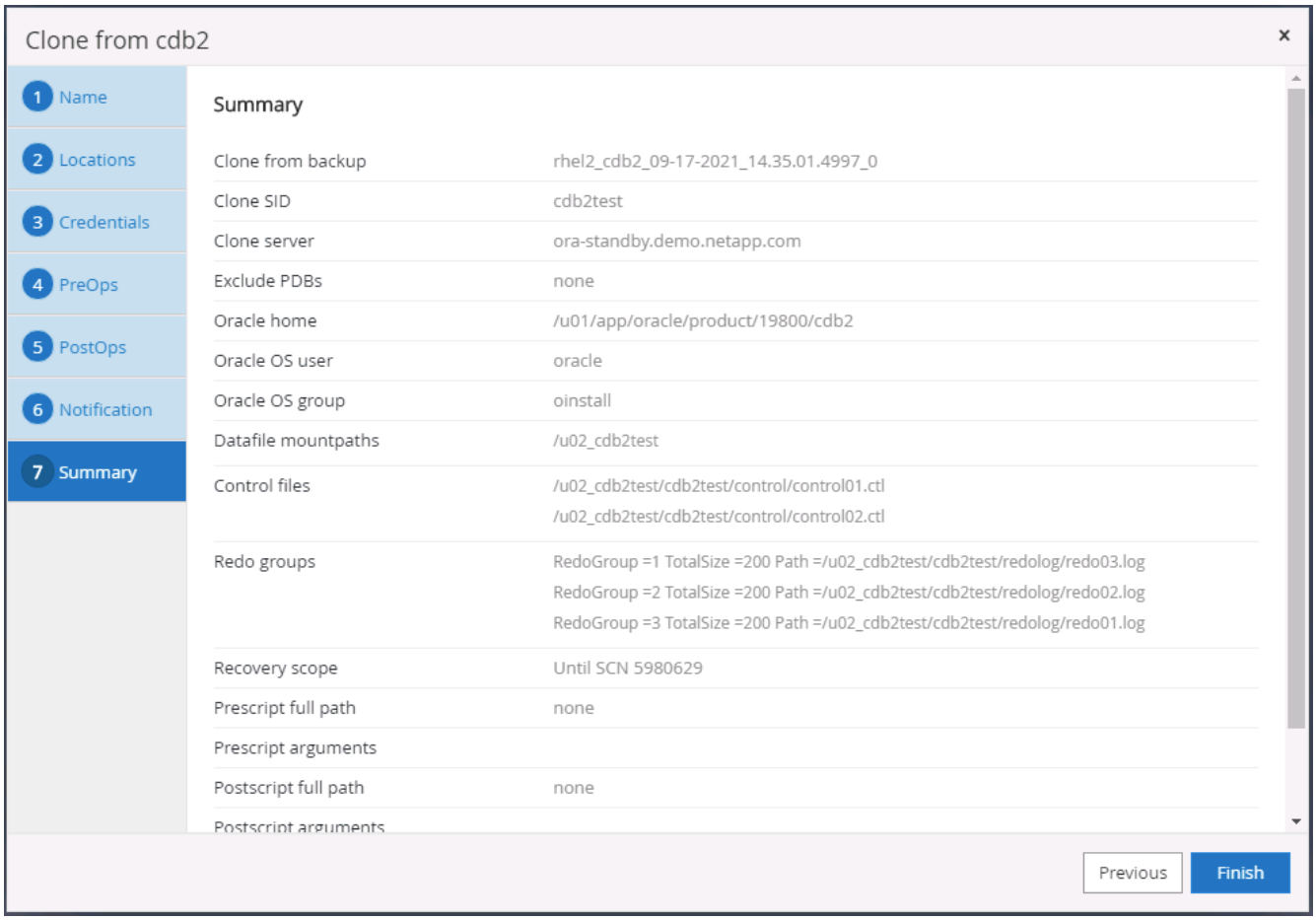




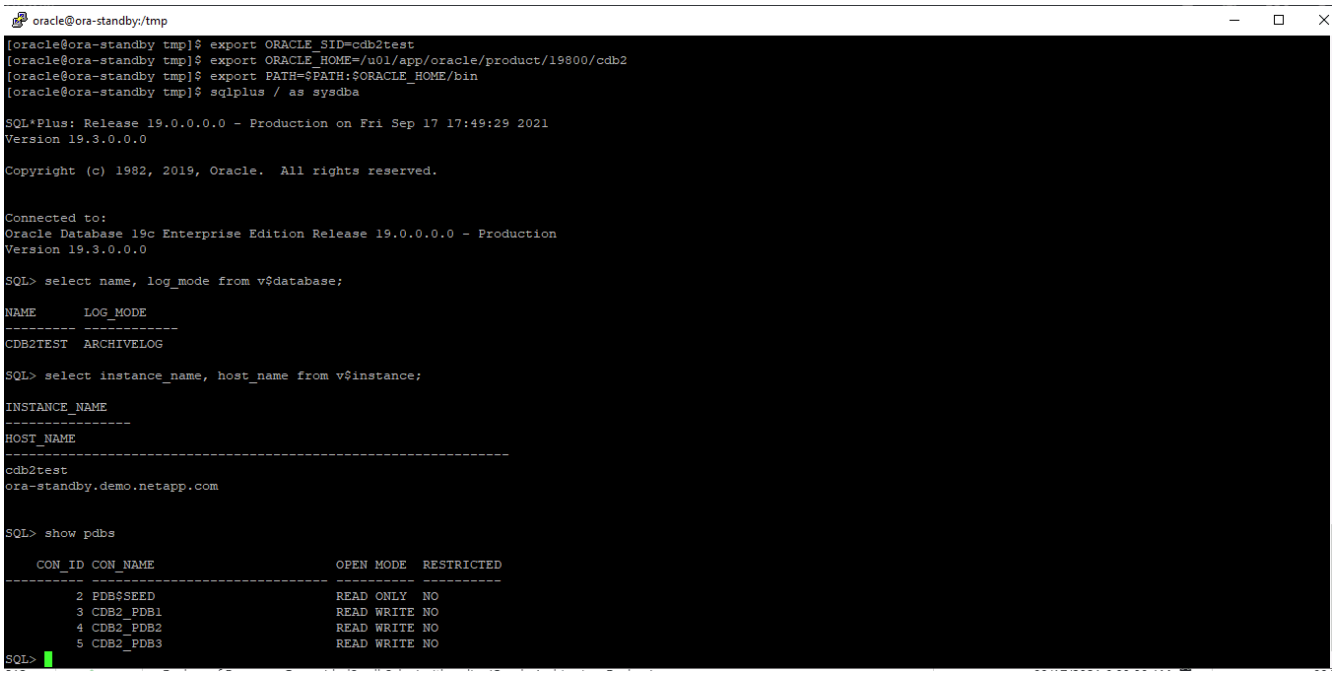
11. Configure el servidor SMTP para la notificación por correo electrónico si lo desea.



12. Resumen de clones.

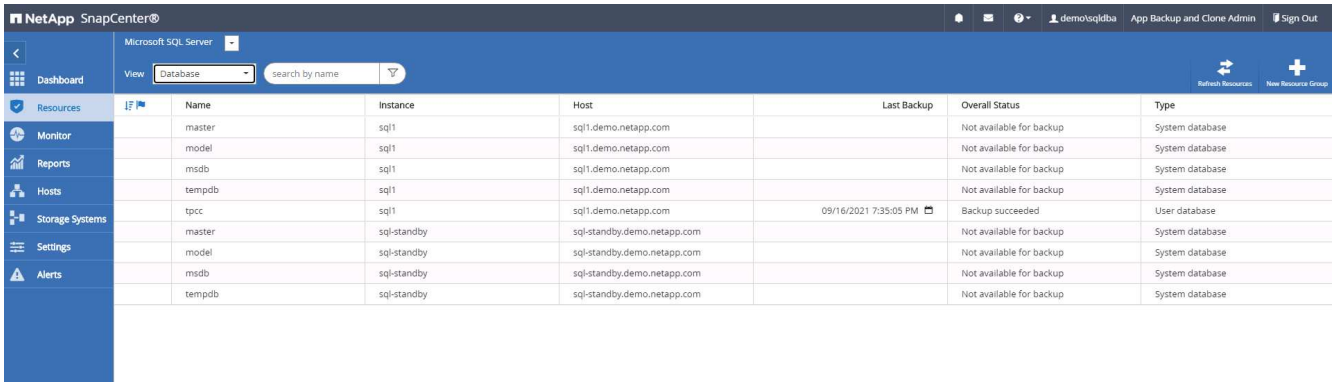


13. Debe validar después de la clonación para asegurarse de que la base de datos clonada funcione. Algunas tareas adicionales, como iniciar el listener o desactivar el modo de archivo de registro de DB, se pueden realizar en la base de datos de prueba/desarrollo.

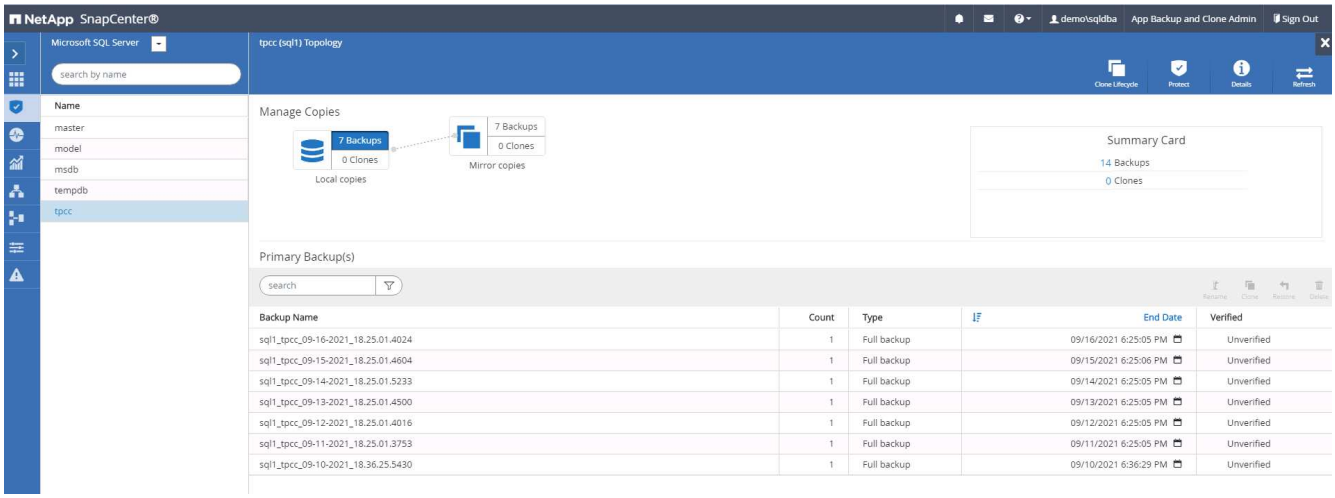


Clonar una base de datos de SQL para desarrollo y pruebas a partir de un backup de Snapshot replicado

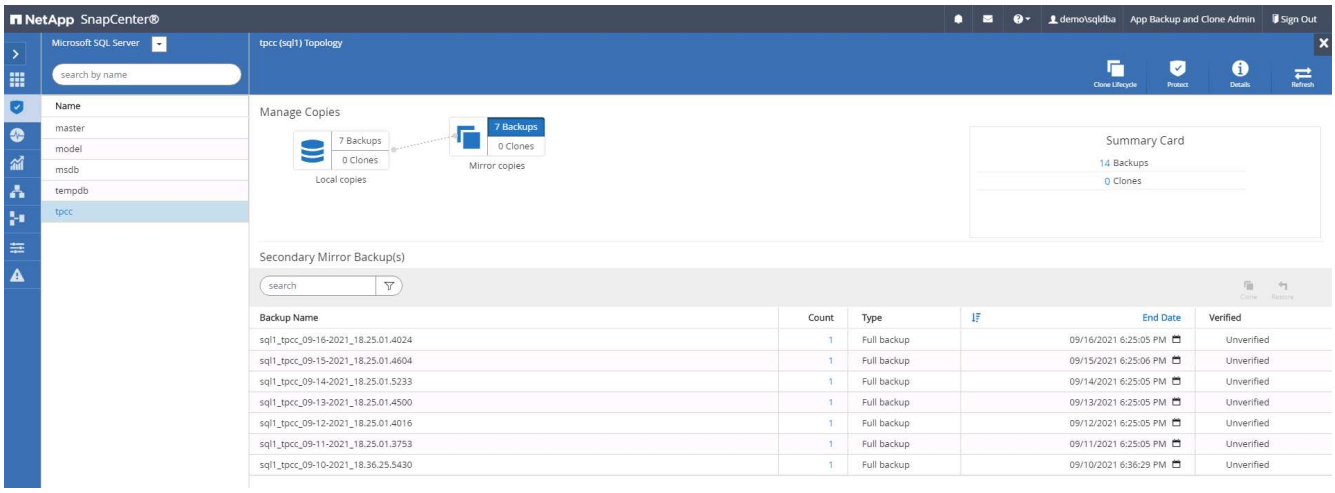
1. Inicie sesión en SnapCenter con un ID de usuario de administración de bases de datos para SQL Server. Desplácese hasta la pestaña Resources, donde se muestran las bases de datos de usuario SQL Server protegidas por SnapCenter y una instancia de SQL en espera de destino en la nube pública.



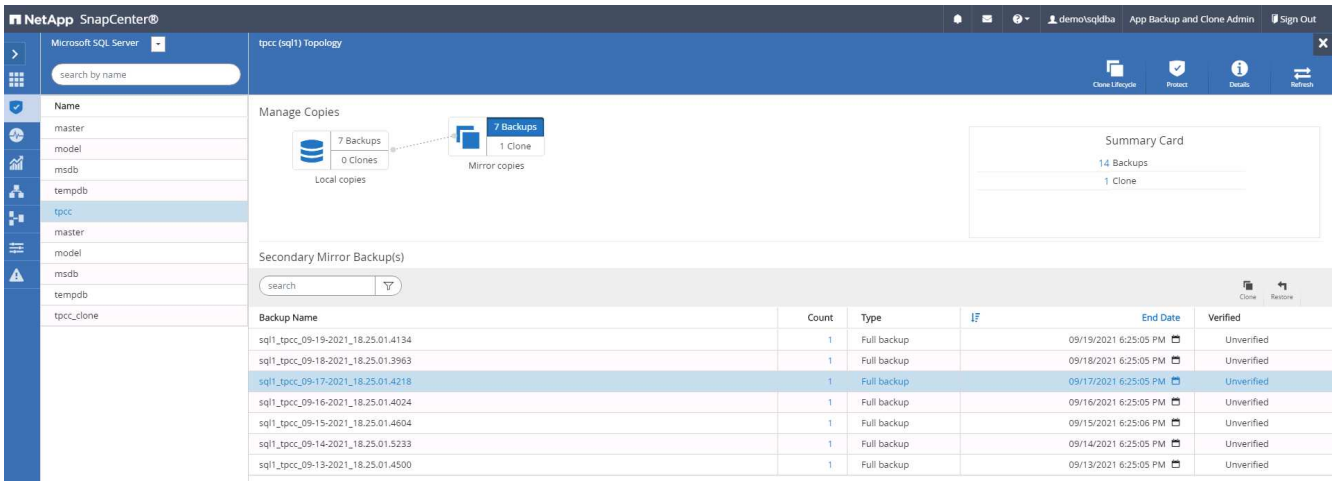
2. Haga clic en el nombre previsto de la base de datos de usuario de SQL Server en las instalaciones para obtener la topología y la vista detallada de las copias de seguridad. Si se habilita una ubicación de replicación secundaria, se muestran backups de reflejos vinculados.

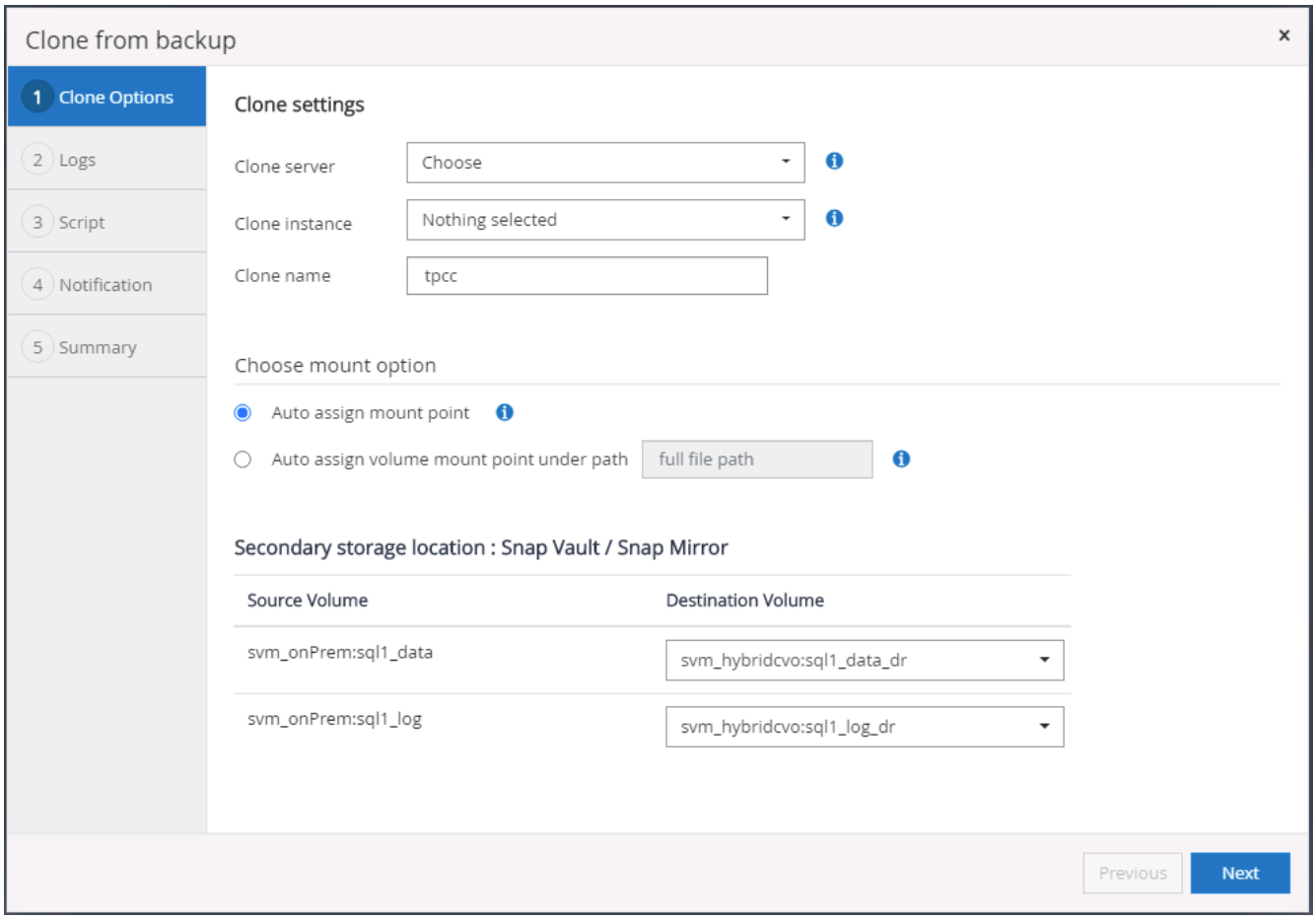


3. Para alternar a la vista Mirrored backups, haga clic en Mirrored backups. Luego, se mostrarán los backups de reflejo secundarios. Dado que SnapCenter realiza un backup del registro de transacciones de SQL Server en una unidad dedicada para la recuperación, solo se muestran aquí backups completos de la base de datos.

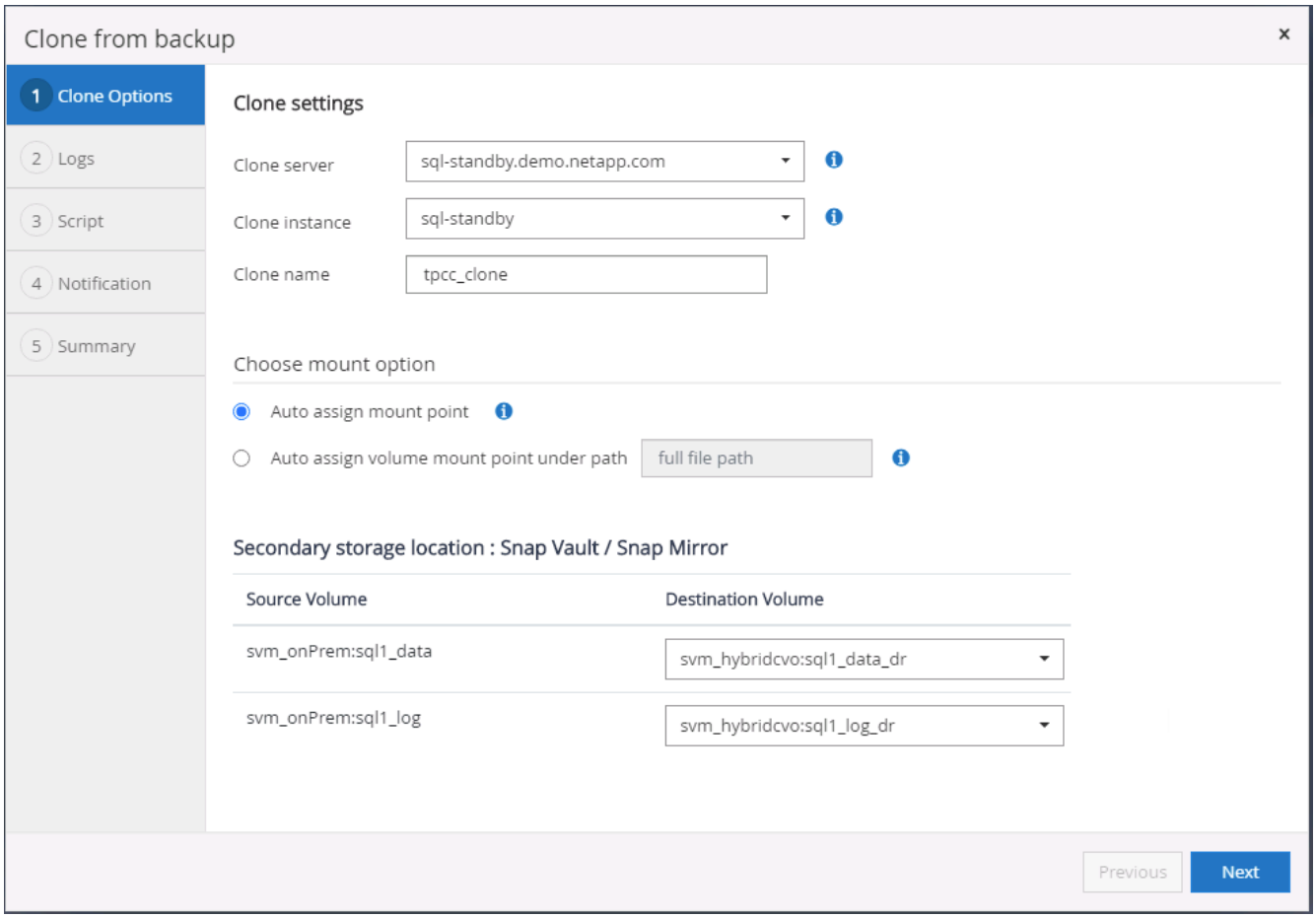


4. Seleccione una copia de backup y, a continuación, haga clic en el botón Clone para iniciar el flujo de trabajo Clone desde Backup.

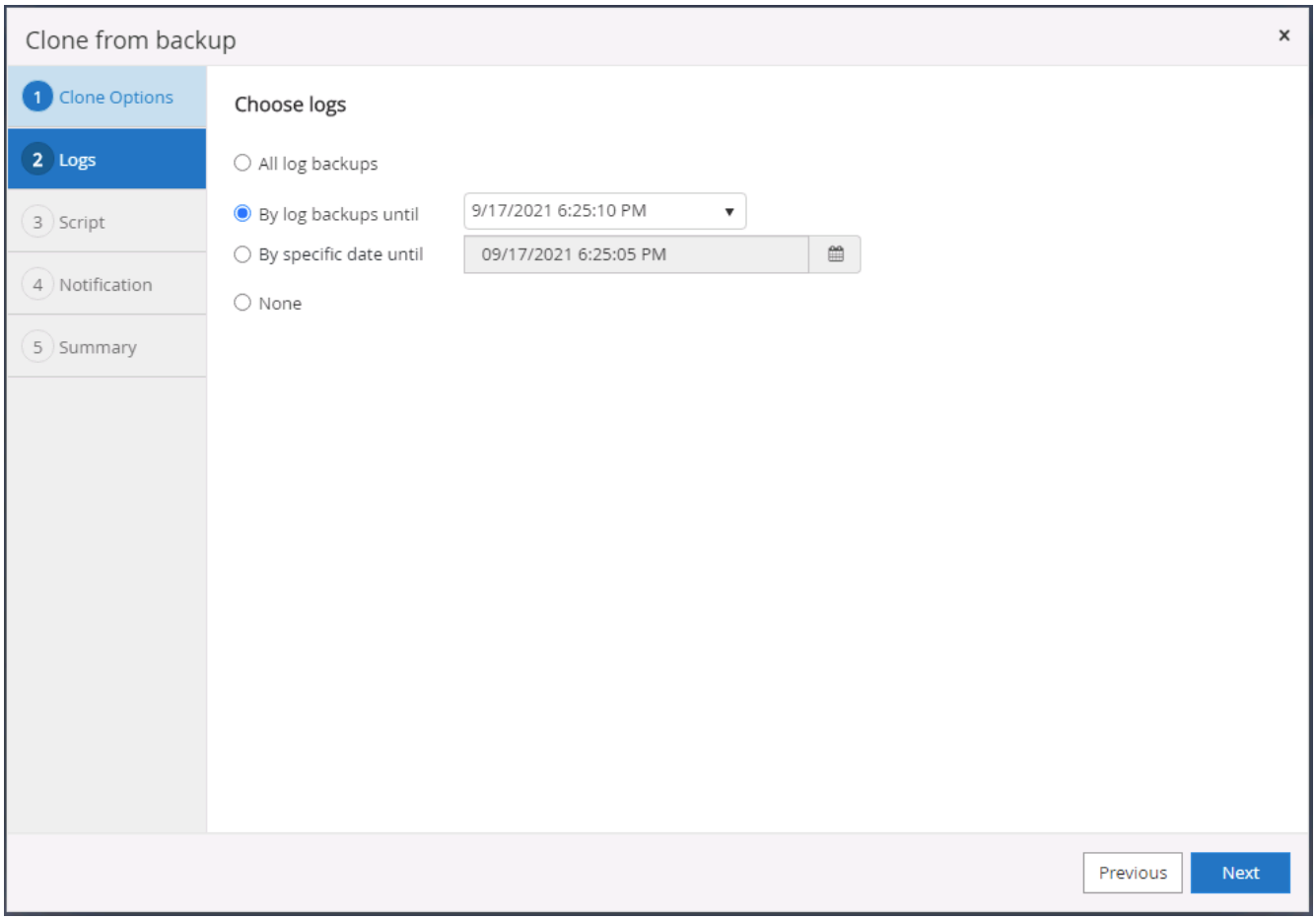




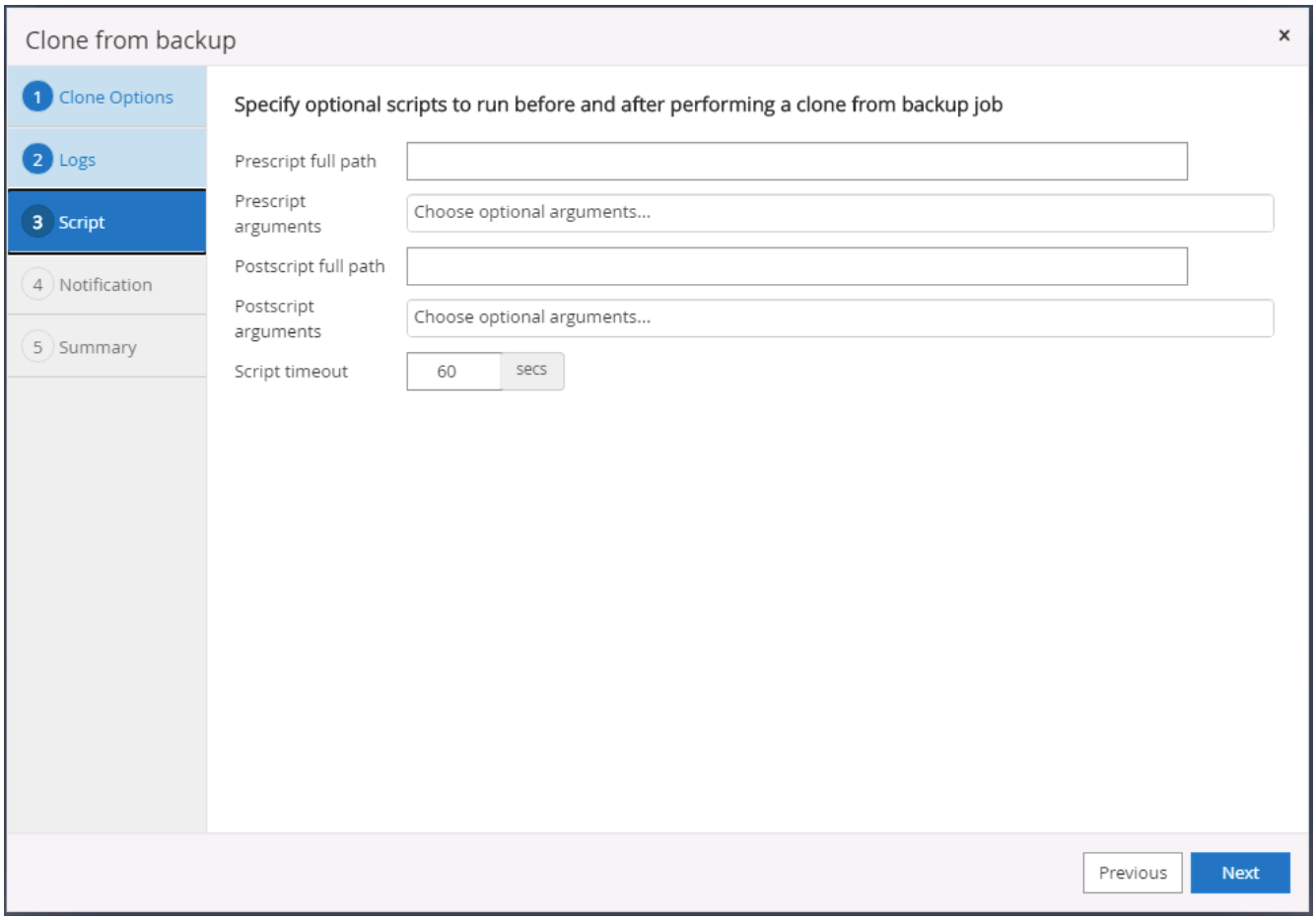
5. Seleccione un servidor en cloud como el servidor de clonado de destino, el nombre de la instancia de clon y el nombre de la base de datos de clonado. Seleccione un punto de montaje de asignación automática o una ruta de punto de montaje definida por el usuario.



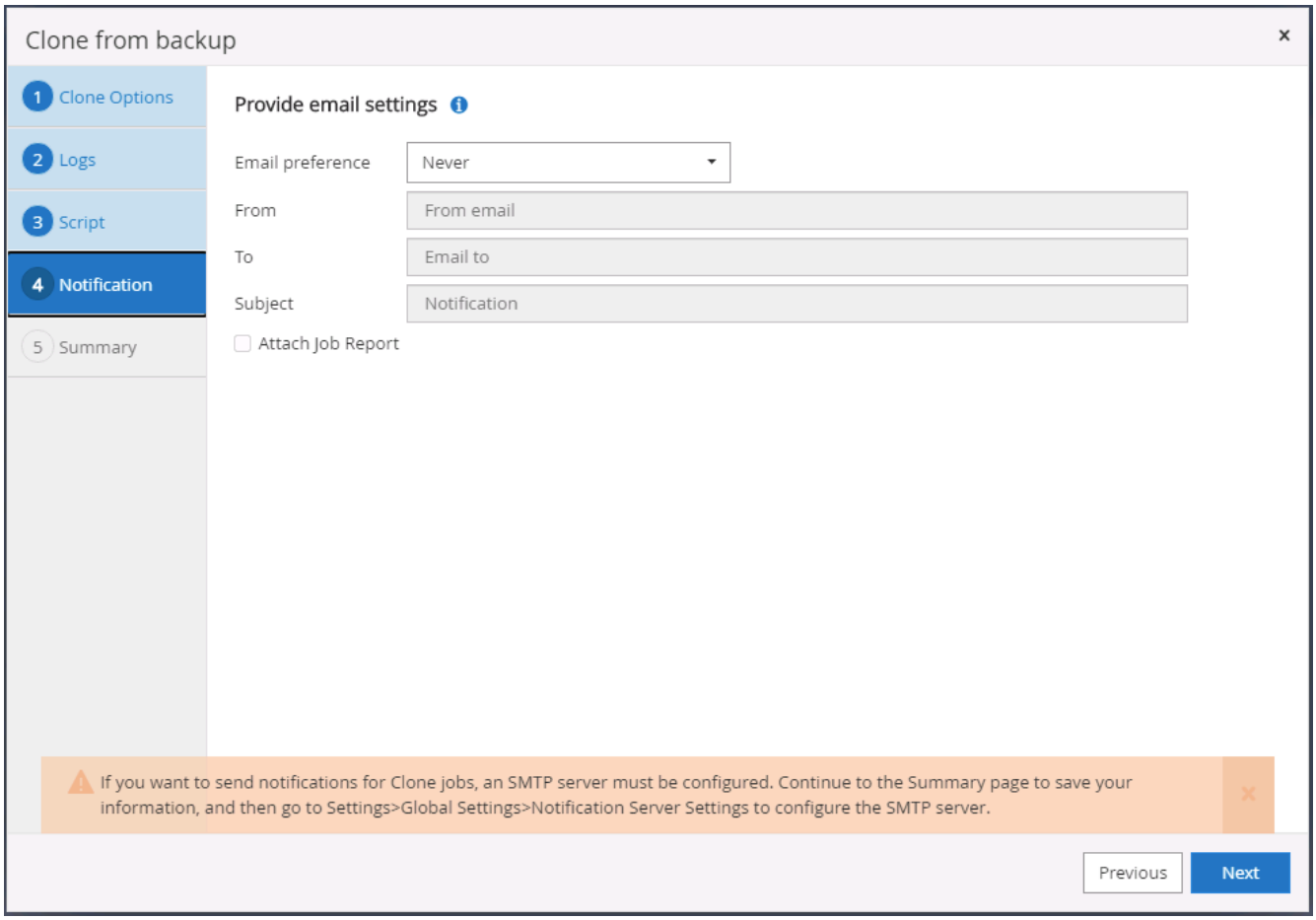
6. Determine un punto de recuperación por hora de backup del registro o por una fecha y hora específicas.



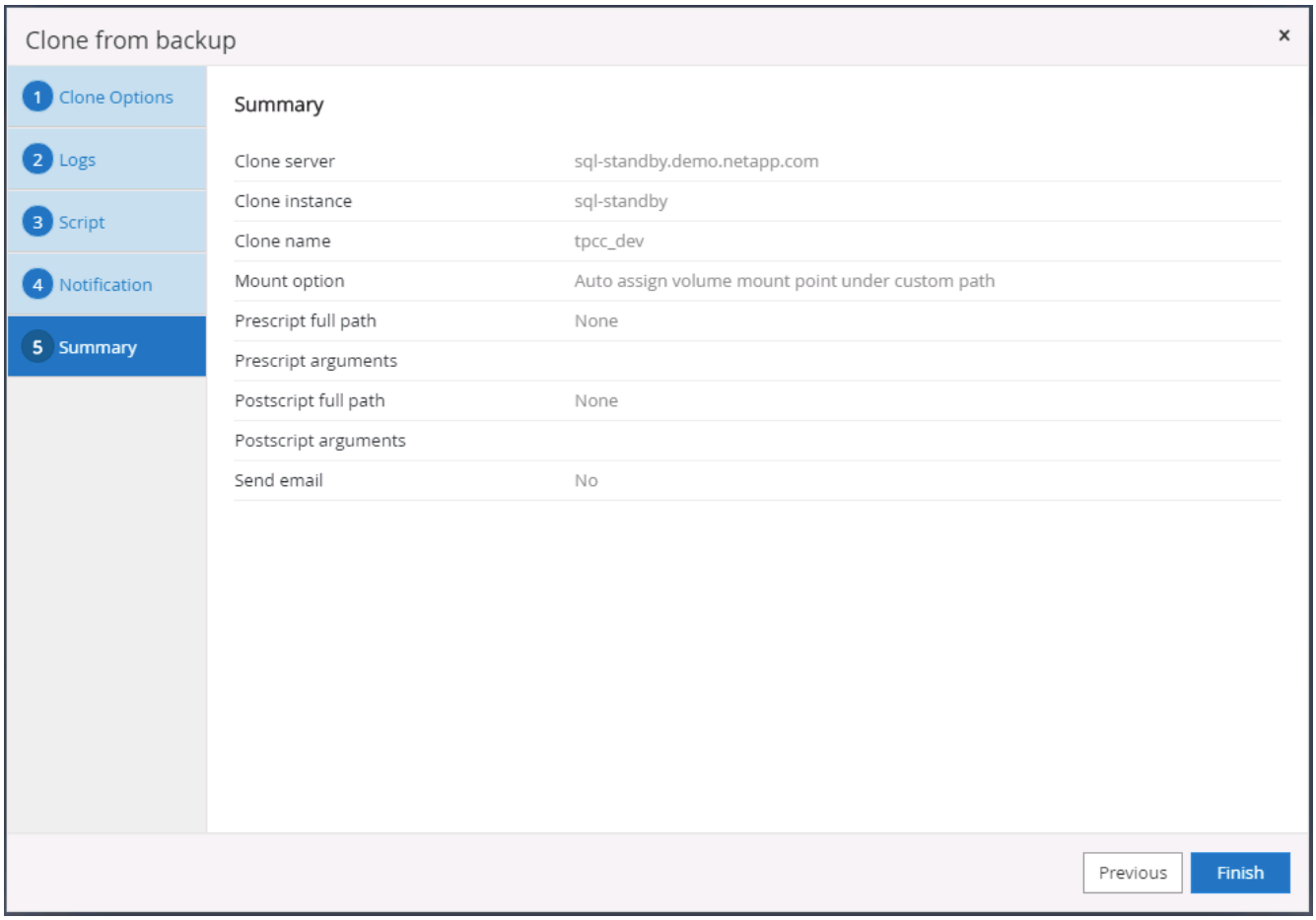
7. Especifique scripts opcionales que ejecutar antes y después de la operación de clonado.



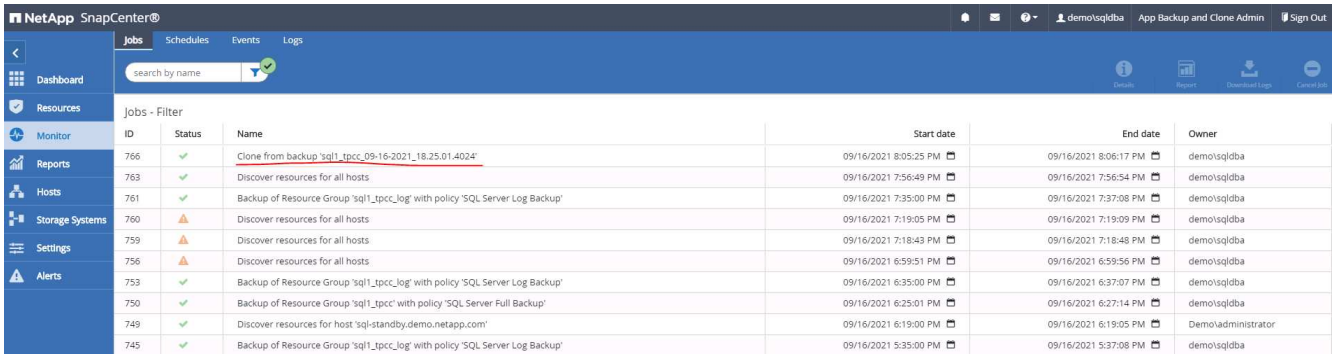
8. Configure un servidor SMTP si se desea recibir una notificación por correo electrónico.



9. Resumen de clones.



10. Supervise el estado del trabajo y valide que la base de datos de usuario prevista se ha adjuntado a una instancia de SQL de destino en el servidor de clones en cloud.



Configuración posterior al clon

1. Normalmente, una base de datos de producción de Oracle en las instalaciones se ejecuta en modo de archivado de registros. 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 la base de datos Oracle como sysdba, ejecute un comando de cambio de modo de registro e inicie la base de datos para obtener acceso.
2. Configurar un listener de Oracle o registrar la base de datos que se acaba de clonar con un listener existente para que el usuario pueda acceder a ella.
3. En SQL Server, cambie el modo de registro de Full a Easy para que el archivo de registro de prueba/desarrollo de SQL Server se pueda reducir fácilmente al llenar el volumen de registro.

Actualice el clon de la base de datos

1. Borre las bases de datos clonadas y borre el entorno del servidor de bases de datos de cloud. A continuación, siga los procedimientos anteriores para clonar una nueva base de datos con datos nuevos. Solo se tarda unos minutos en clonar una nueva base de datos.
2. Apague la base de datos de clonado, ejecute un comando de actualización de clonado mediante la CLI. Consulte la siguiente documentación de SnapCenter para obtener detalles: "Actualizar un clon".

¿Dónde obtener ayuda?

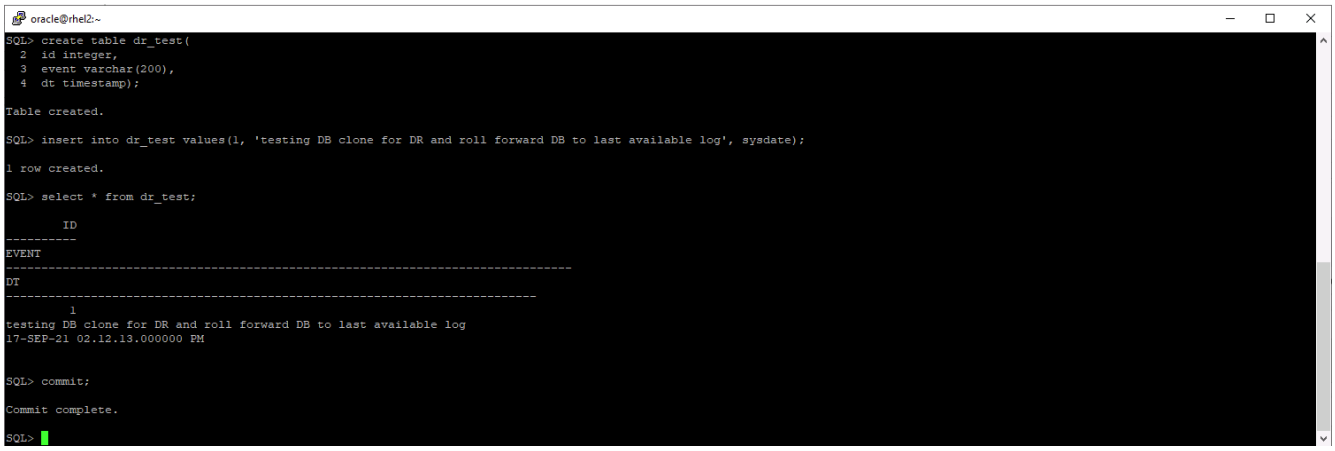
Si necesita ayuda con esta solución y los casos de uso, únase al "La comunidad de automatización de soluciones de NetApp admite el canal de Slack" y busque el canal de automatización de soluciones para publicar sus preguntas o preguntas.

Flujo de trabajo de recuperación ante desastres

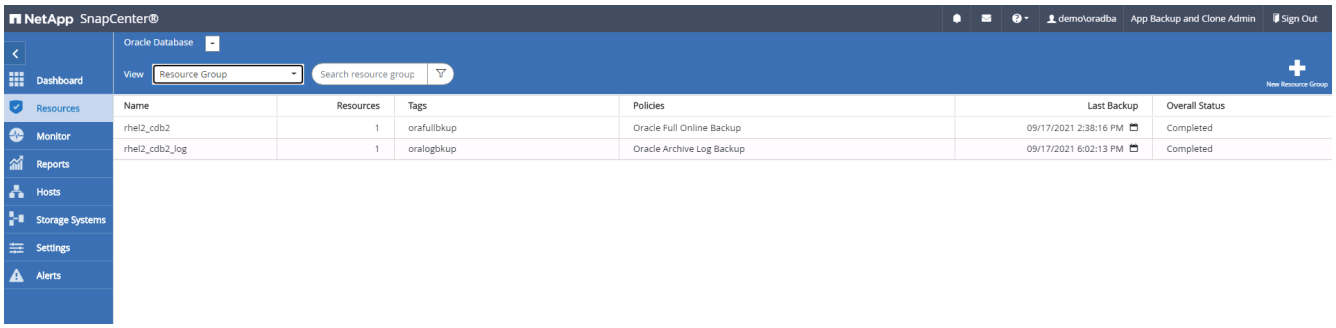
Las empresas han adoptado el cloud público como recurso viable y destino para la recuperación ante desastres. SnapCenter hace que este proceso sea lo más sencillo posible. Este flujo de trabajo de recuperación ante desastres es muy similar al flujo de trabajo clonado, pero la recuperación de las bases de datos se ejecuta a través del último registro disponible replicado en el cloud para recuperar todas las transacciones de negocio posibles. No obstante, existen pasos adicionales de preconfiguración y posconfiguración específicos para la recuperación ante desastres.

Clonar una base de datos de producción de Oracle en las instalaciones al cloud para realizar la recuperación ante desastres

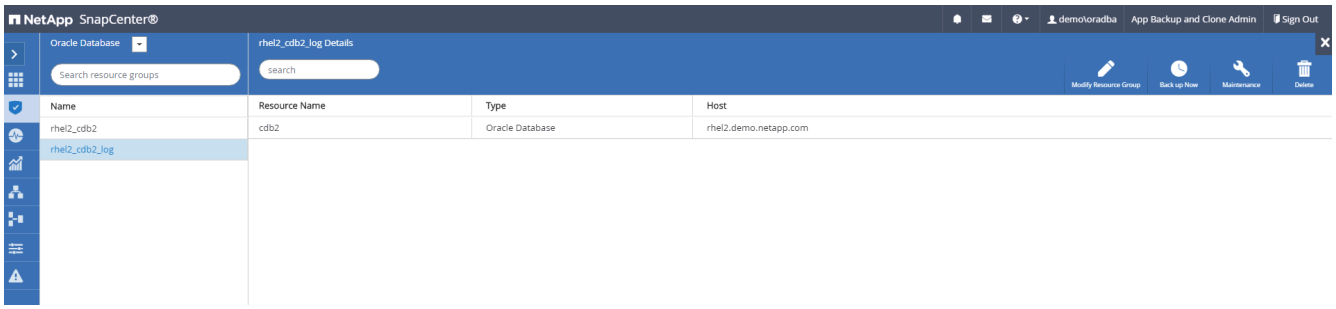
1. Para validar que la recuperación tras clones se ejecuta en el último registro disponible, creamos una pequeña tabla de prueba e insertamos una fila. Los datos de prueba se recuperarían después de una recuperación completa para el último registro disponible.

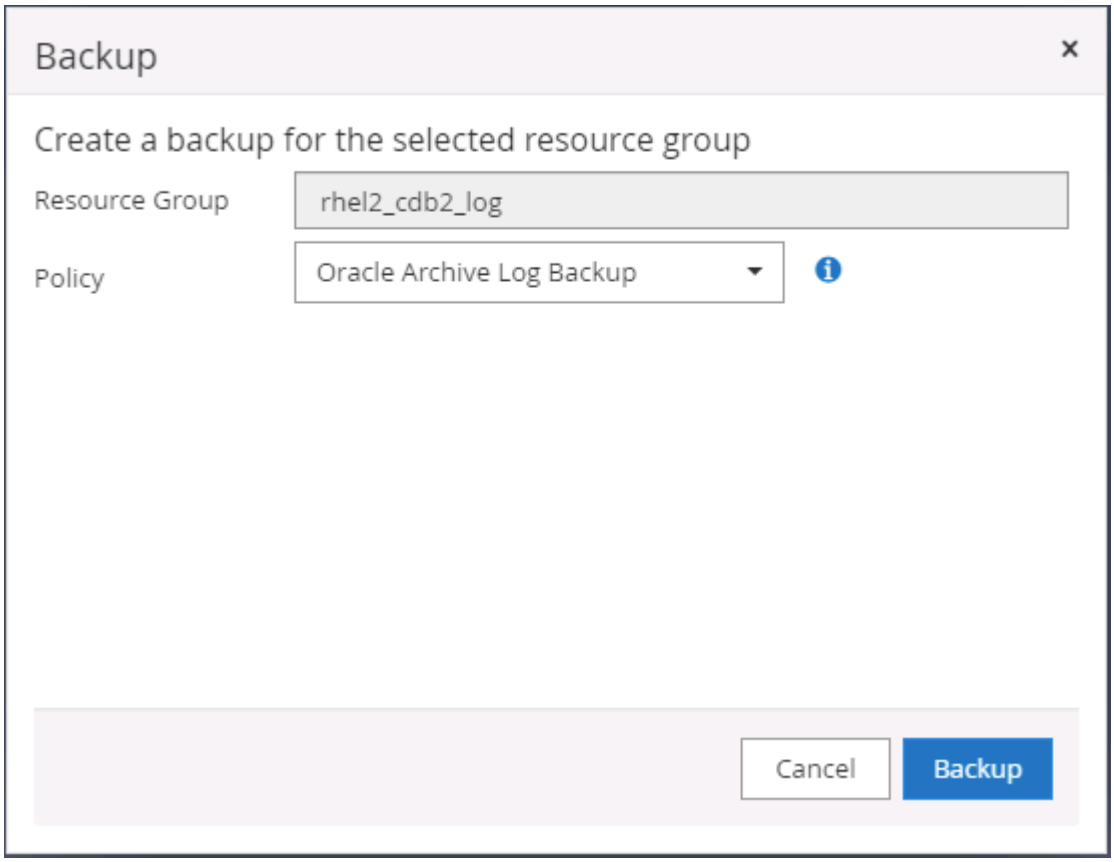


2. Inicie sesión en SnapCenter como un ID de usuario de gestión de bases de datos para Oracle. Desplácese hasta la pestaña Resources, donde se muestran las bases de datos de Oracle que está protegida por SnapCenter.



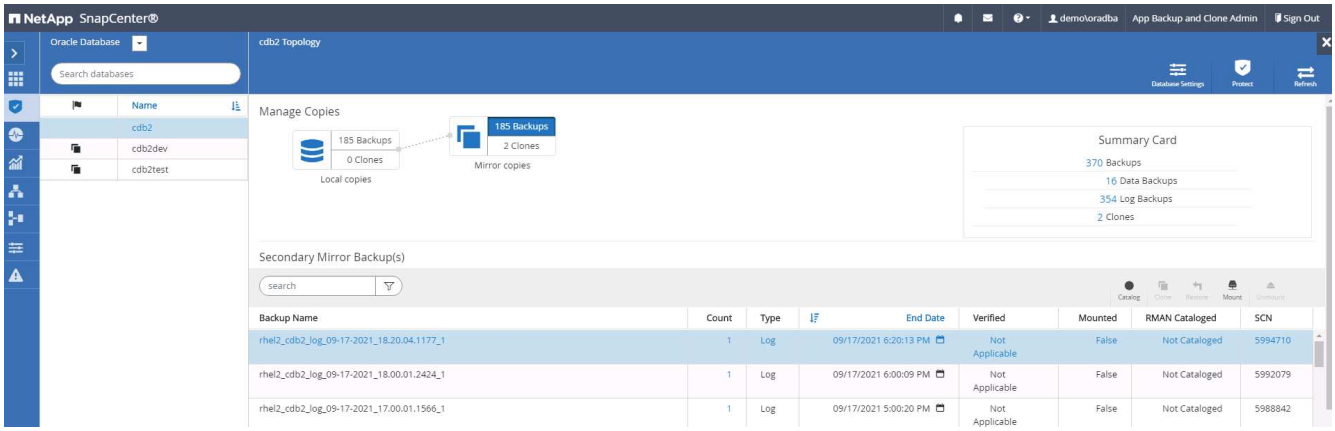
3. Seleccione el grupo de recursos de registro de Oracle y haga clic en Backup Now para ejecutar manualmente un backup del registro de Oracle para vaciar la última transacción al destino en el cloud. En un supuesto de recuperación ante desastres real, la última transacción recuperable depende de la frecuencia de replicación del volumen de registro de la base de datos al cloud, que a su vez depende del objetivo de tiempo de recuperación o de la política de RPO de la empresa.

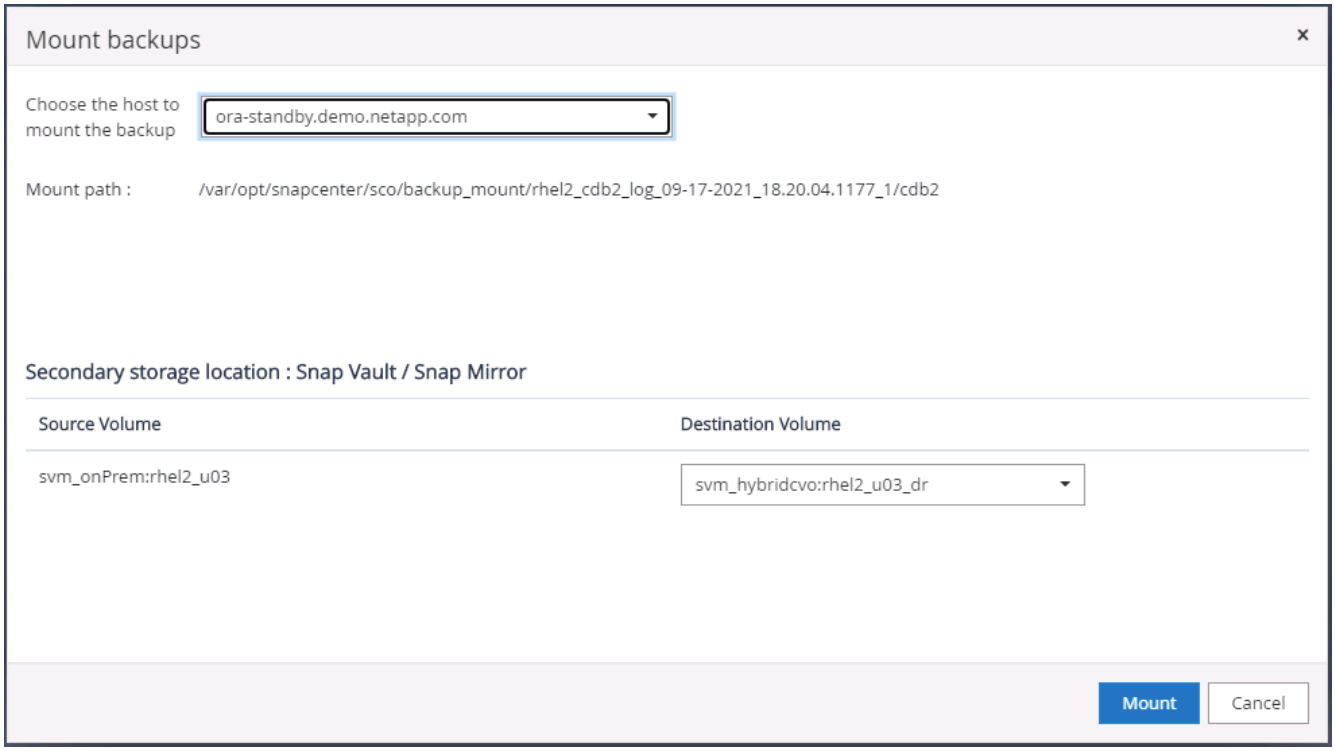




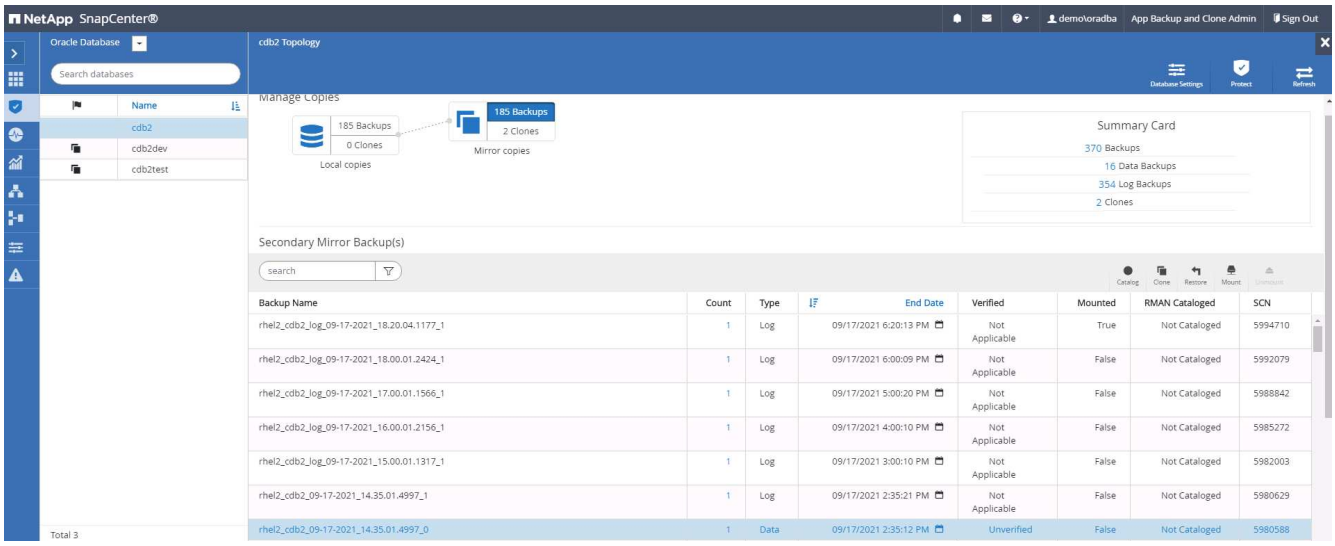
> SnapMirror asíncrono pierde datos que no los ha realizado al destino del cloud en el intervalo de backup del registro de la base de datos en un escenario de recuperación ante desastres. Para minimizar la pérdida de datos, es posible programar backups de registro más frecuentes. Sin embargo, existe un límite para la frecuencia de backup de registros que se puede lograr técnicamente.

4. Seleccione el último backup de registro en los backups de reflejo secundario y monte el backup de registros.

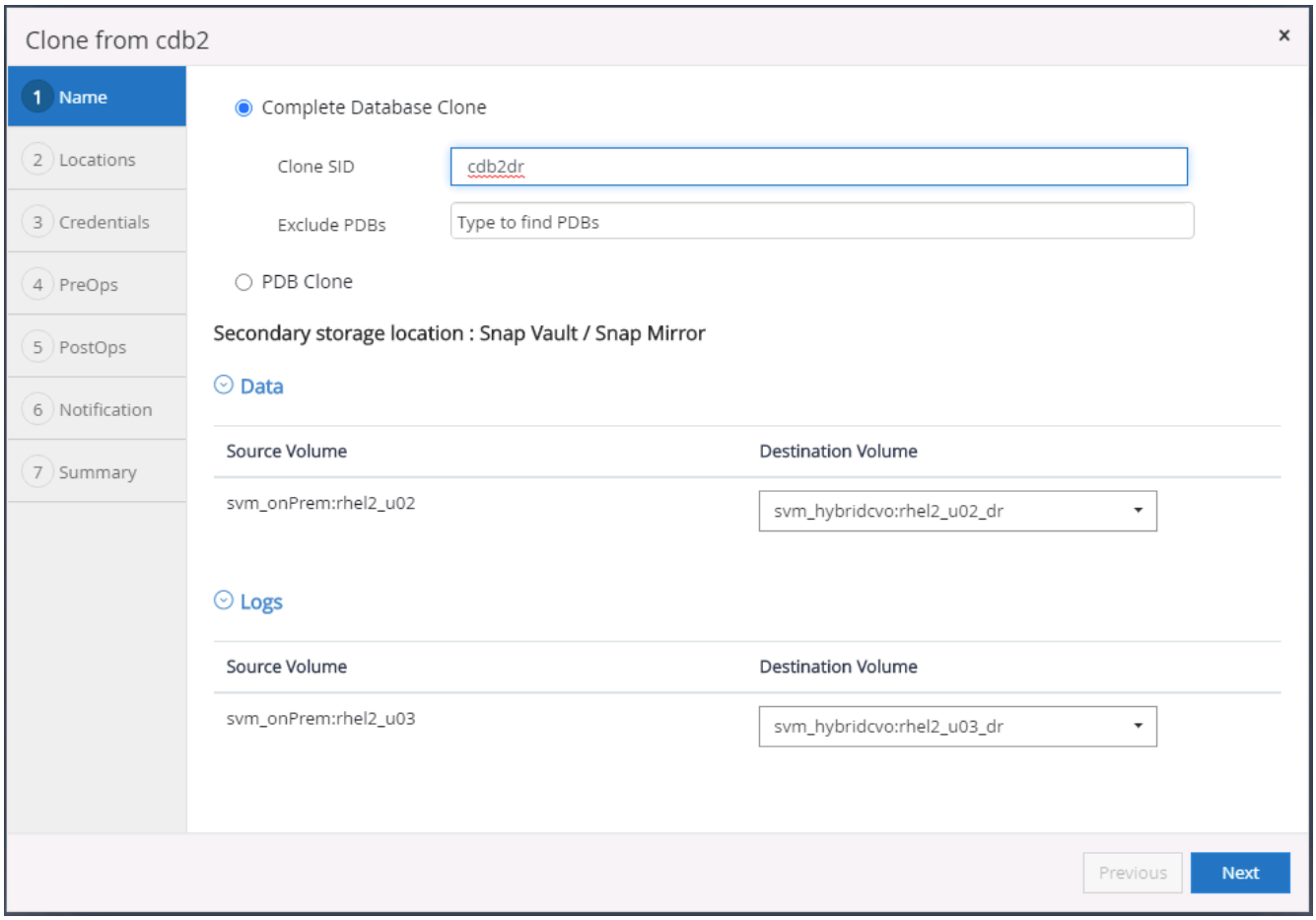




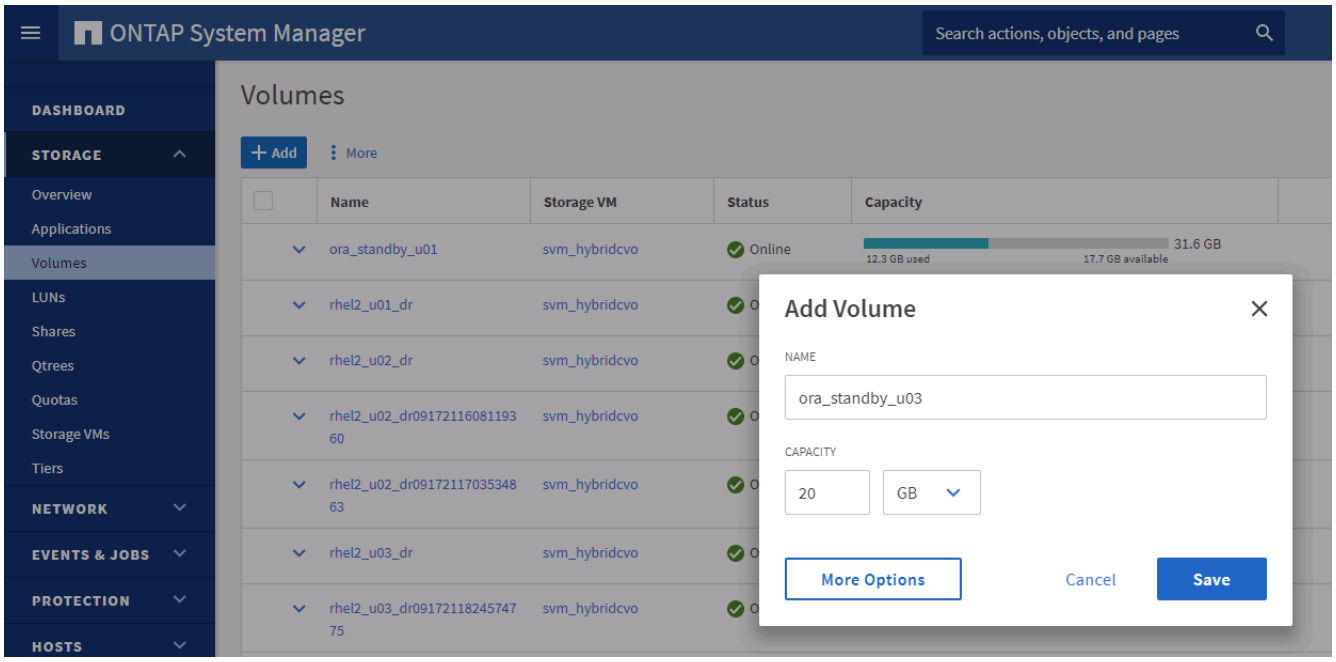
5. Seleccione el último backup completo de la base de datos y haga clic en Clone para iniciar el flujo de trabajo de clonado.

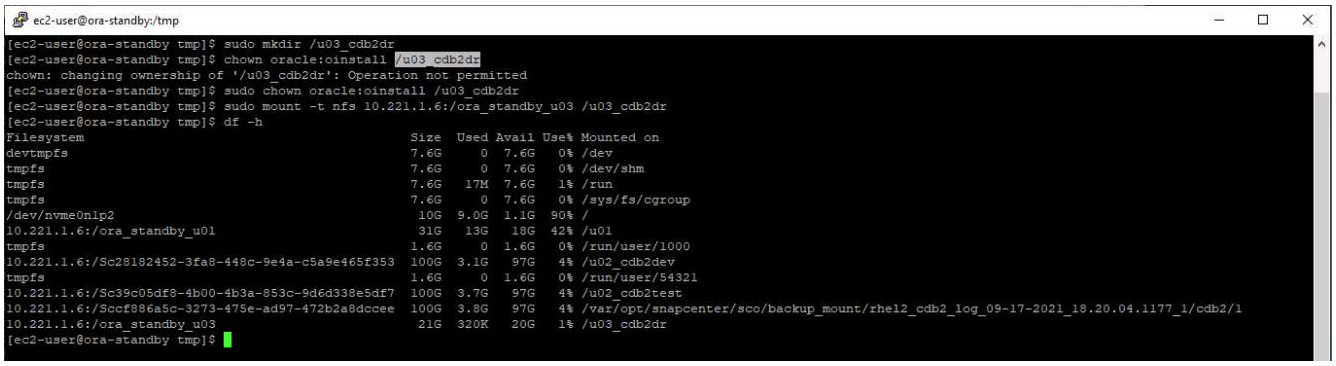


6. Seleccione un ID de base de datos de clon único en el host.



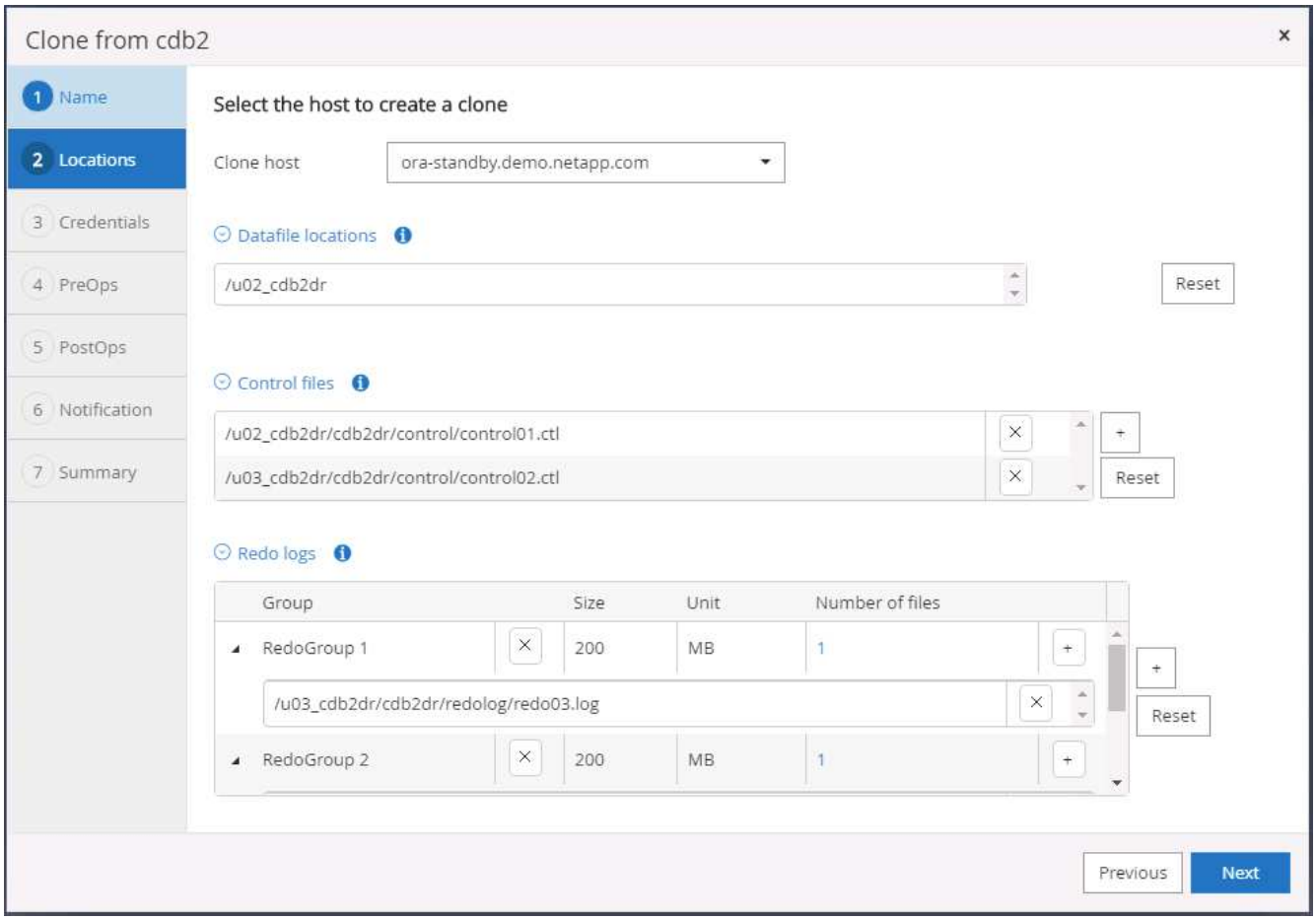
7. Aprovisionar un volumen de registro y montarlo en el servidor de recuperación ante desastres de destino para el área de recuperación flash de Oracle y registros en línea.



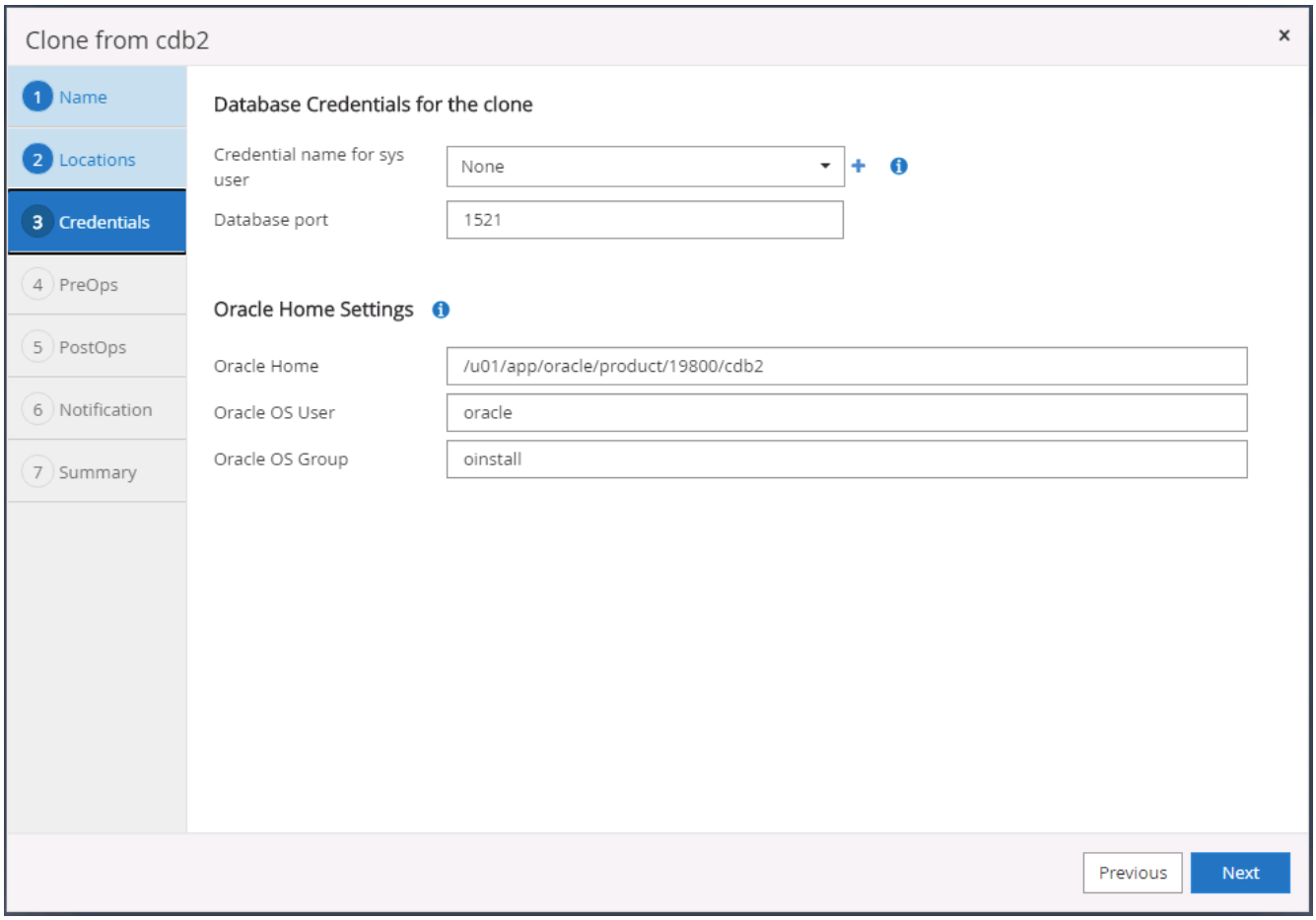


> El procedimiento de clonado de Oracle no crea un volumen de registro, que debe aprovisionarse en el servidor de recuperación ante desastres antes de realizar el clonado.

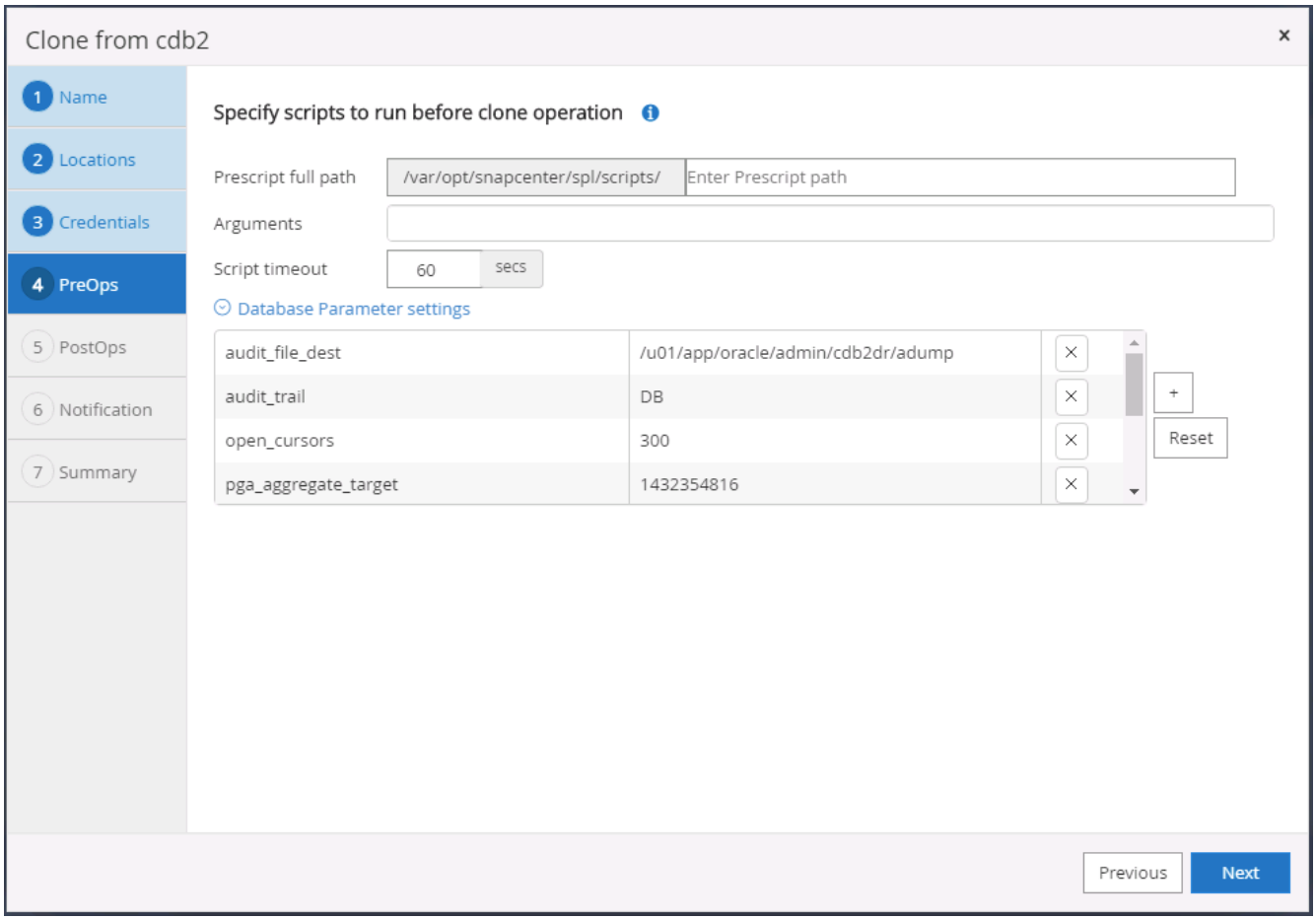
8. Seleccione el host del clon de destino y la ubicación para colocar los archivos de datos, los archivos de control y los registros de recuperación.



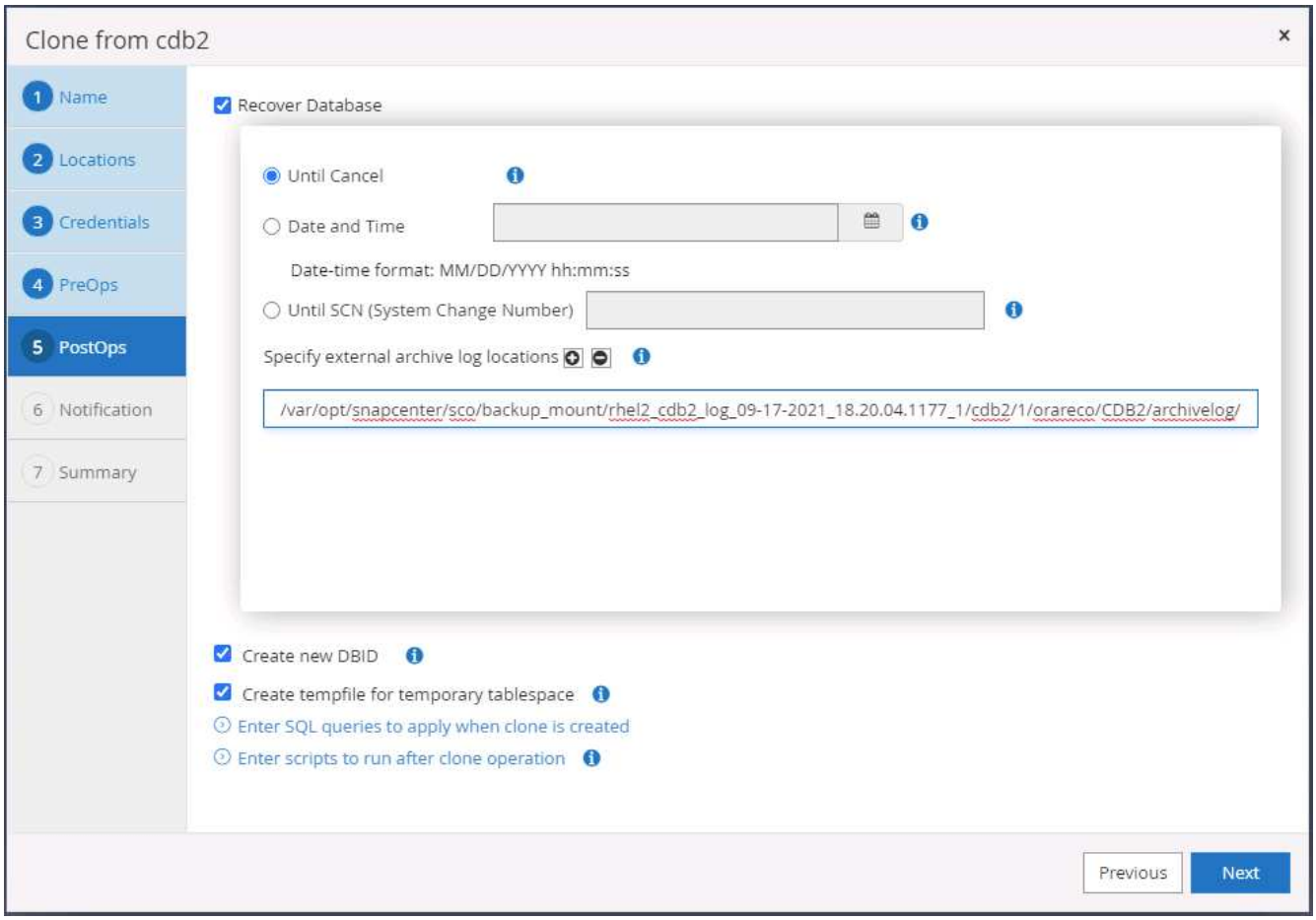
9. Seleccione las credenciales para el clon. Rellene los detalles de la configuración inicial de Oracle en el servidor de destino.



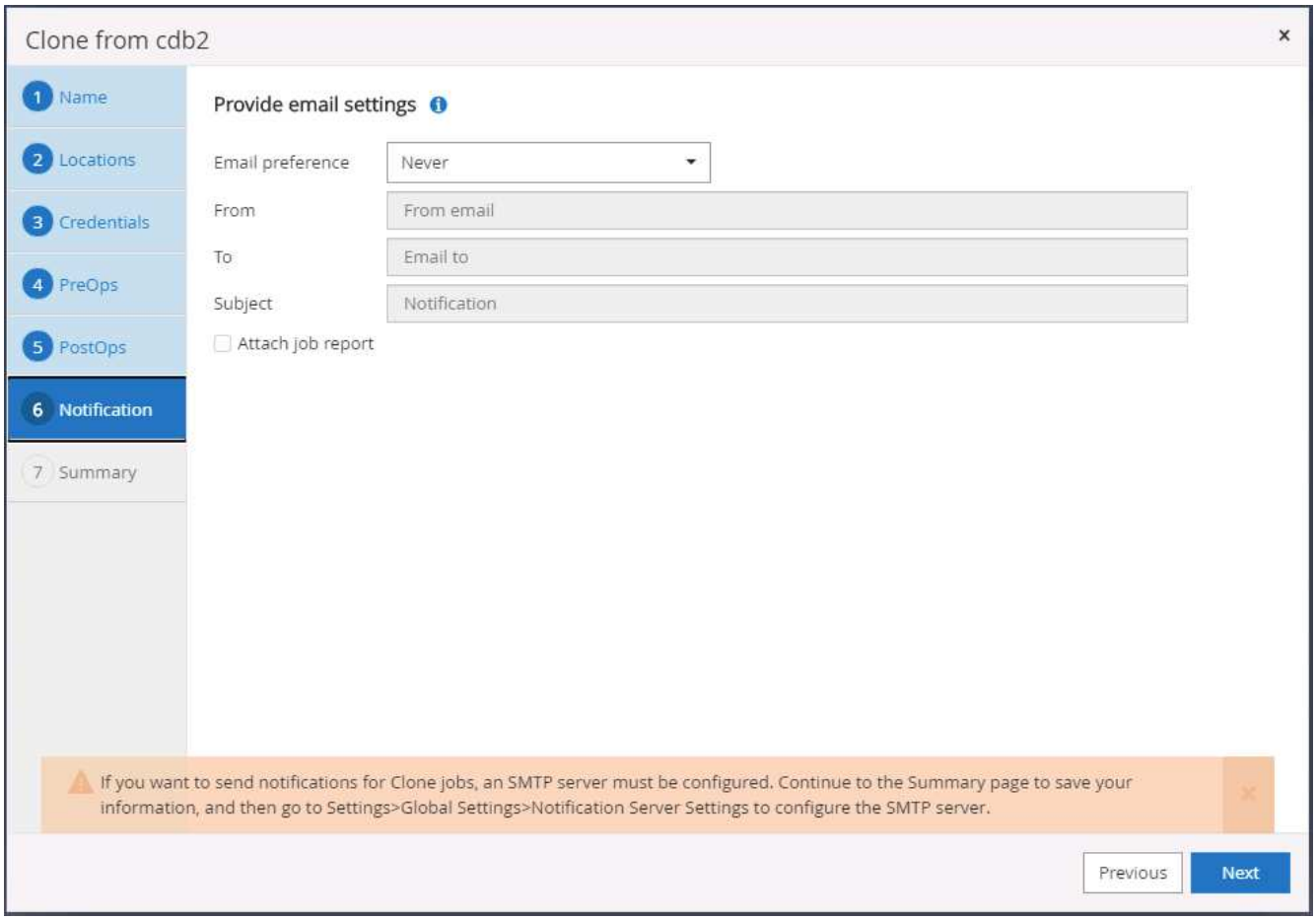
10. Especifique los scripts que se van a ejecutar antes de clonar. Los parámetros de la base de datos se pueden ajustar si es necesario.



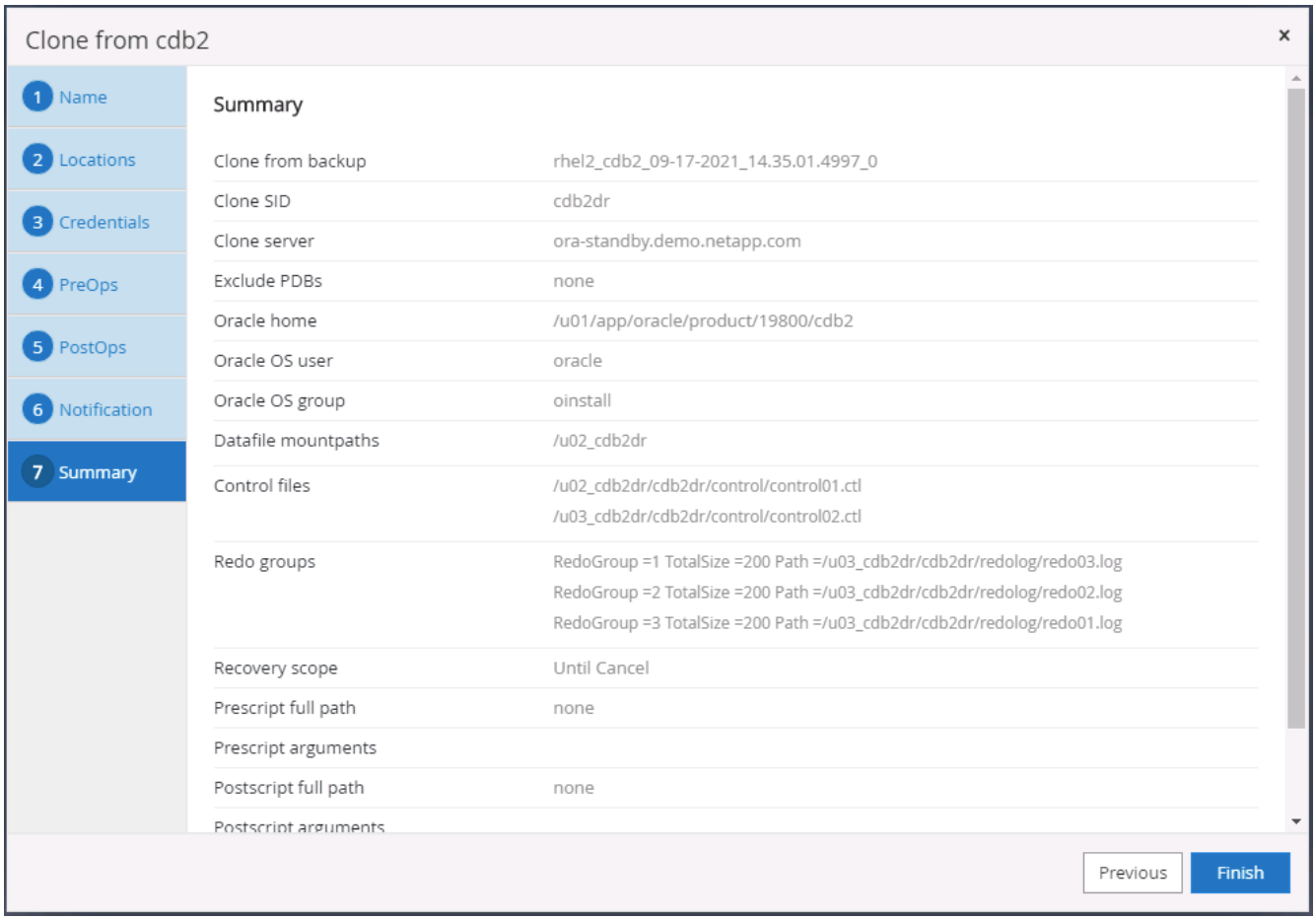
11. Seleccione Until Cancel como opción de recuperación de manera que la recuperación se ejecute en todos los registros de archivos disponibles para recuperar la última transacción replicada en la ubicación del cloud secundario.



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



13. Resumen de los clones de recuperación ante desastres.



14. Las bases de datos clonadas se registran en SnapCenter inmediatamente después de la finalización del clon y, a continuación, se encuentran disponibles para la protección del backup.

Validación y configuración del clon posterior a la recuperación ante desastres para Oracle

1. Validar la última transacción de prueba que se ha vaciado, replicado y recuperado en la ubicación de recuperación ante desastres en el cloud.

```
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. Configure el área de recuperación de 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
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 listener de Oracle para el acceso de los usuarios.
4. Divida el volumen clonado entre el volumen de origen replicado.
5. Invierta la replicación del cloud a las instalaciones y reconstruya el servidor de bases de datos en las instalaciones con fallos.

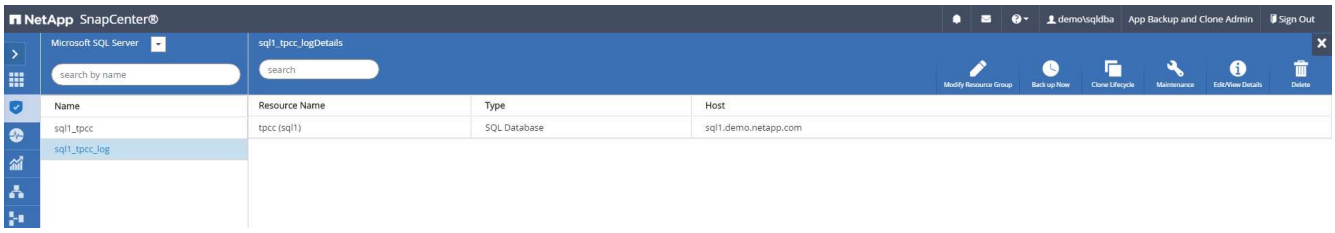
> La división de clones puede incurrir en un uso de espacio de almacenamiento temporal mucho mayor que el funcionamiento normal. Sin embargo, después de reconstruir el servidor de base de datos local, se puede liberar espacio adicional.

Clonar una base de datos de producción de SQL en las instalaciones al cloud para recuperación ante desastres

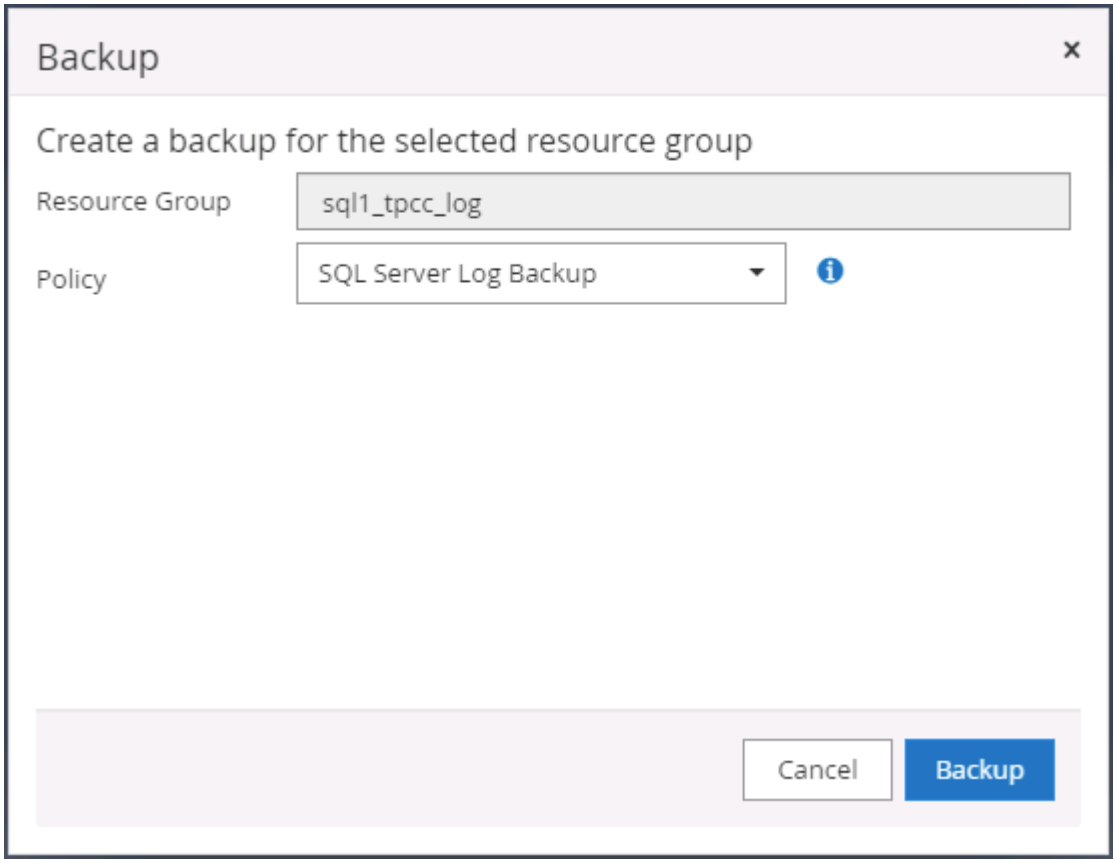
1. De igual modo, para validar que la recuperación del clon SQL se ejecutó mediante el último registro disponible, creamos una tabla de pruebas pequeña e insertamos una fila. Los datos de prueba se recuperarían después de una recuperación completa en el último registro disponible.

```
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>
```

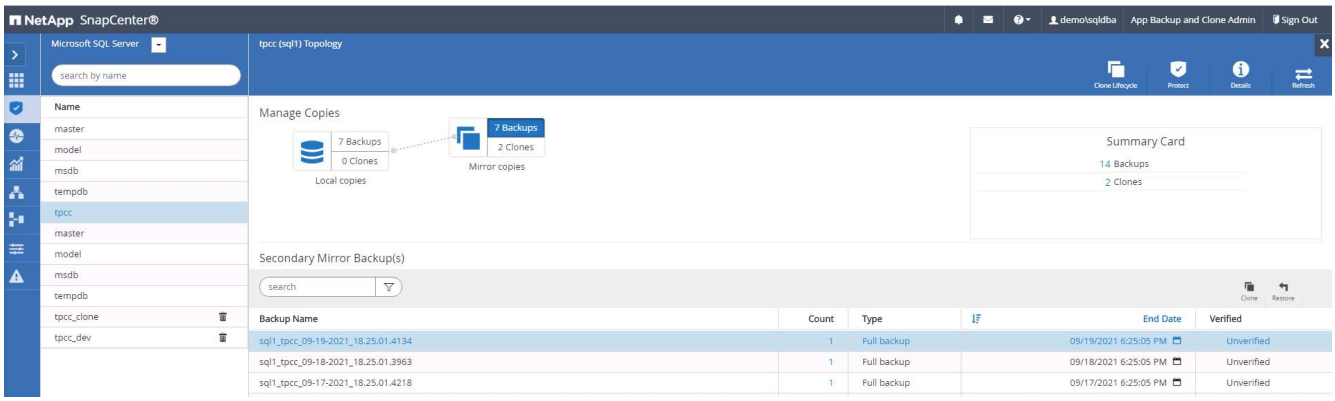
2. Inicie sesión en SnapCenter con un ID de usuario de administración de bases de datos para SQL Server. Desplácese hasta la pestaña Resources, que muestra el grupo de recursos de protección de SQL Server.



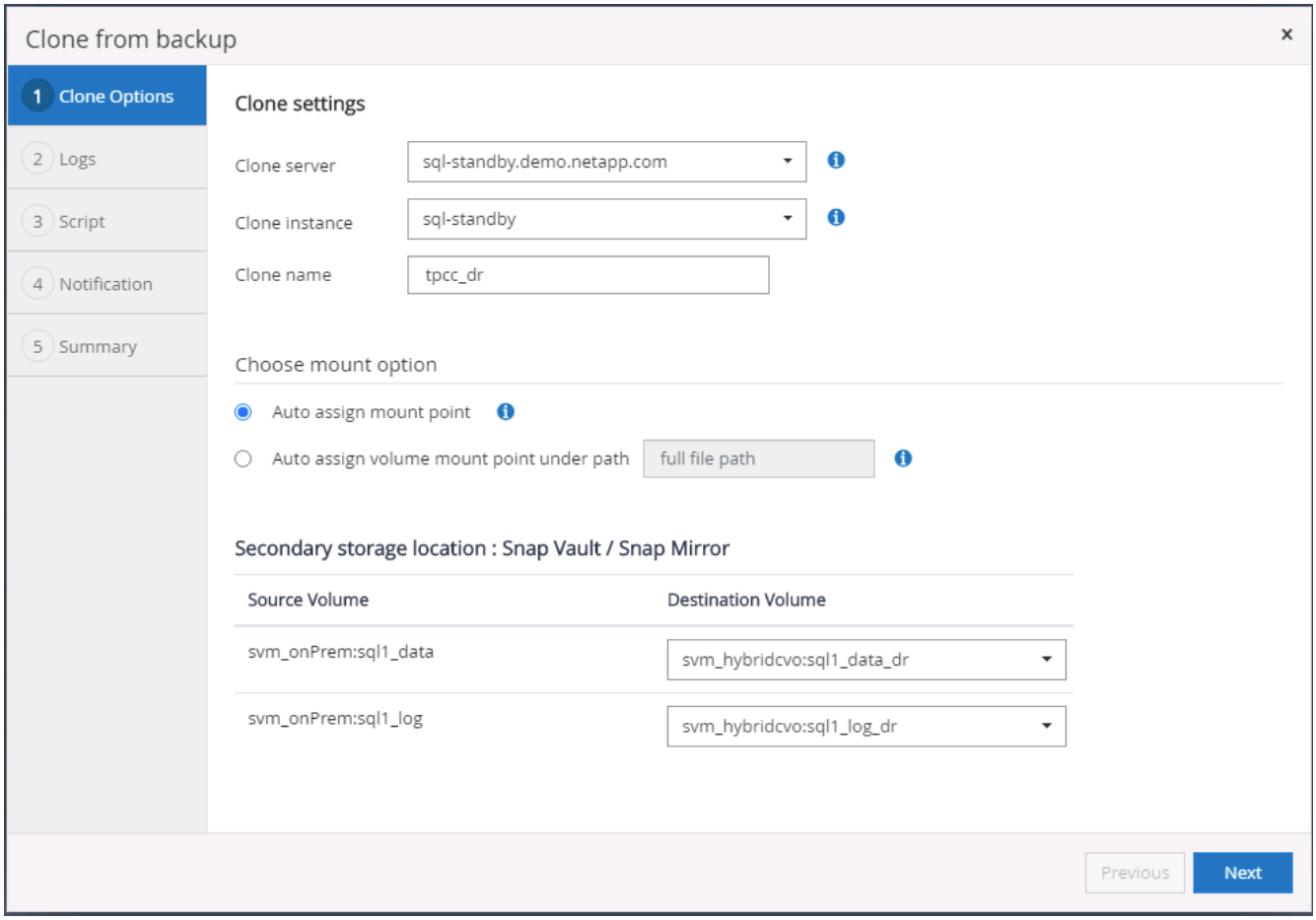
3. Ejecute manualmente un backup de registros para vaciar la última transacción que se replique en el almacenamiento secundario en el cloud público.



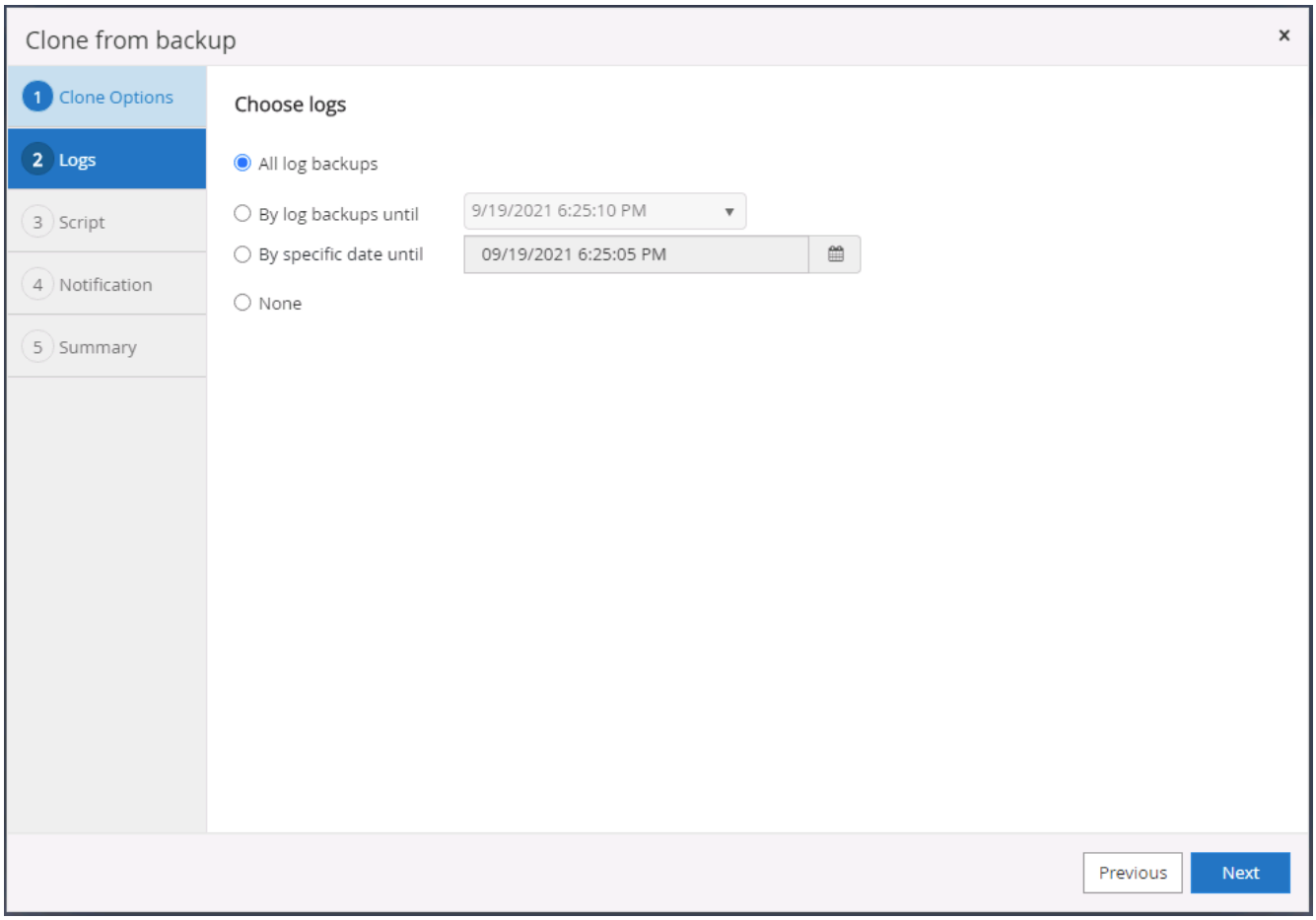
4. Seleccione el último backup completo de SQL Server para el clon.



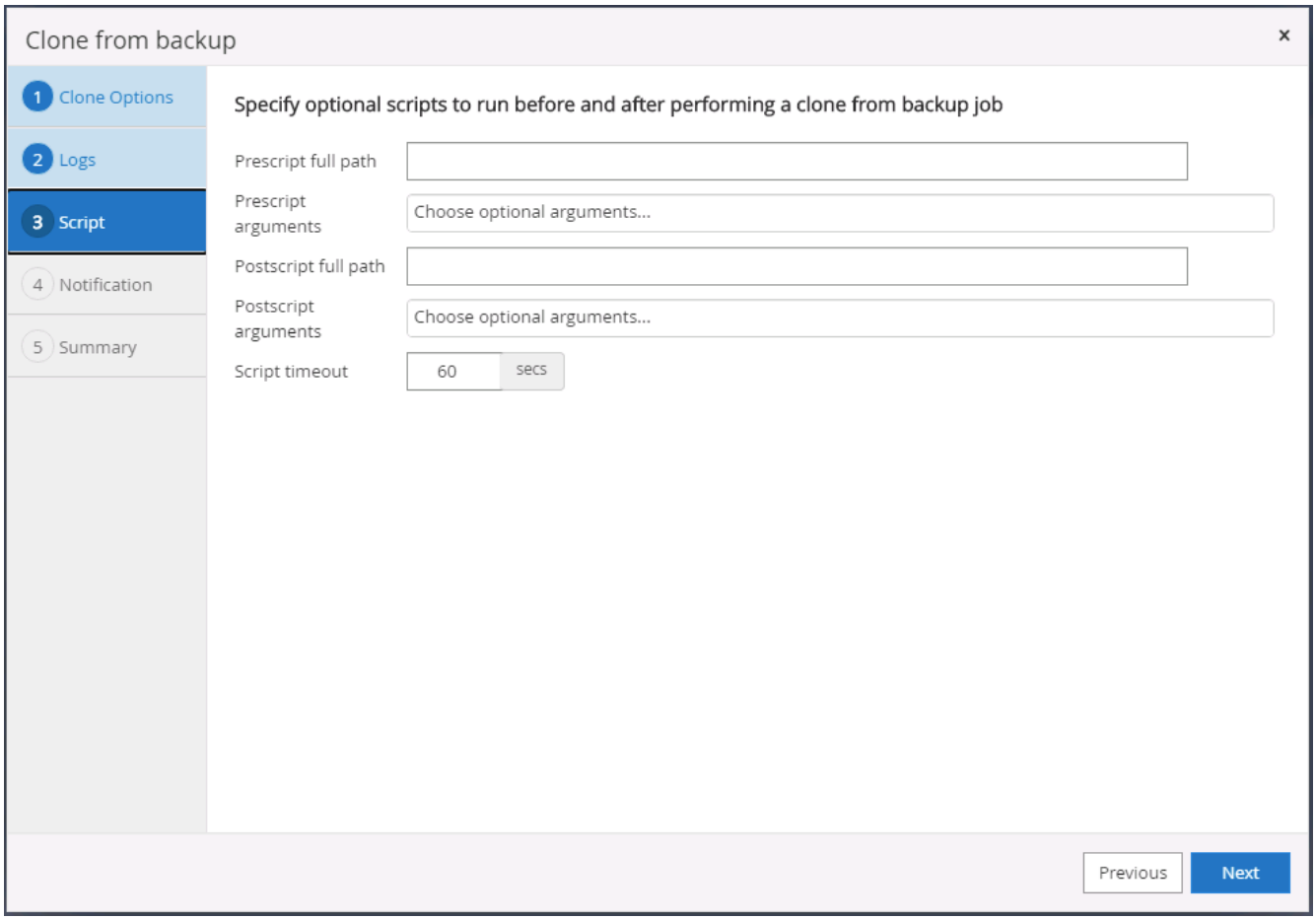
5. Establezca las opciones de configuración de clon, como Clone Server, Clone Instance, Clone Name y Mount. La ubicación de almacenamiento secundario donde se realiza la clonado se completa automáticamente.



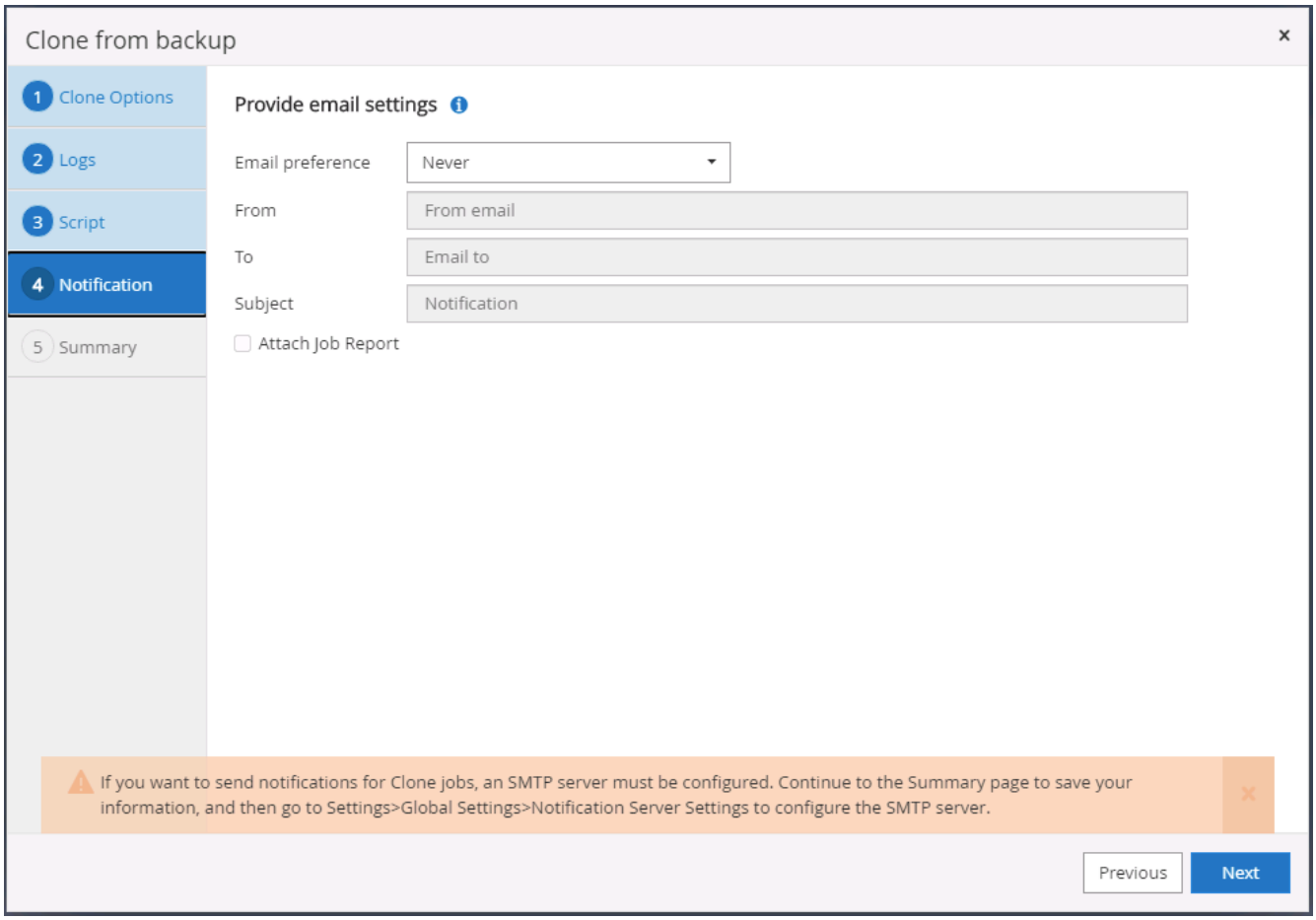
6. Seleccione todos los backups de registros que se aplicarán.



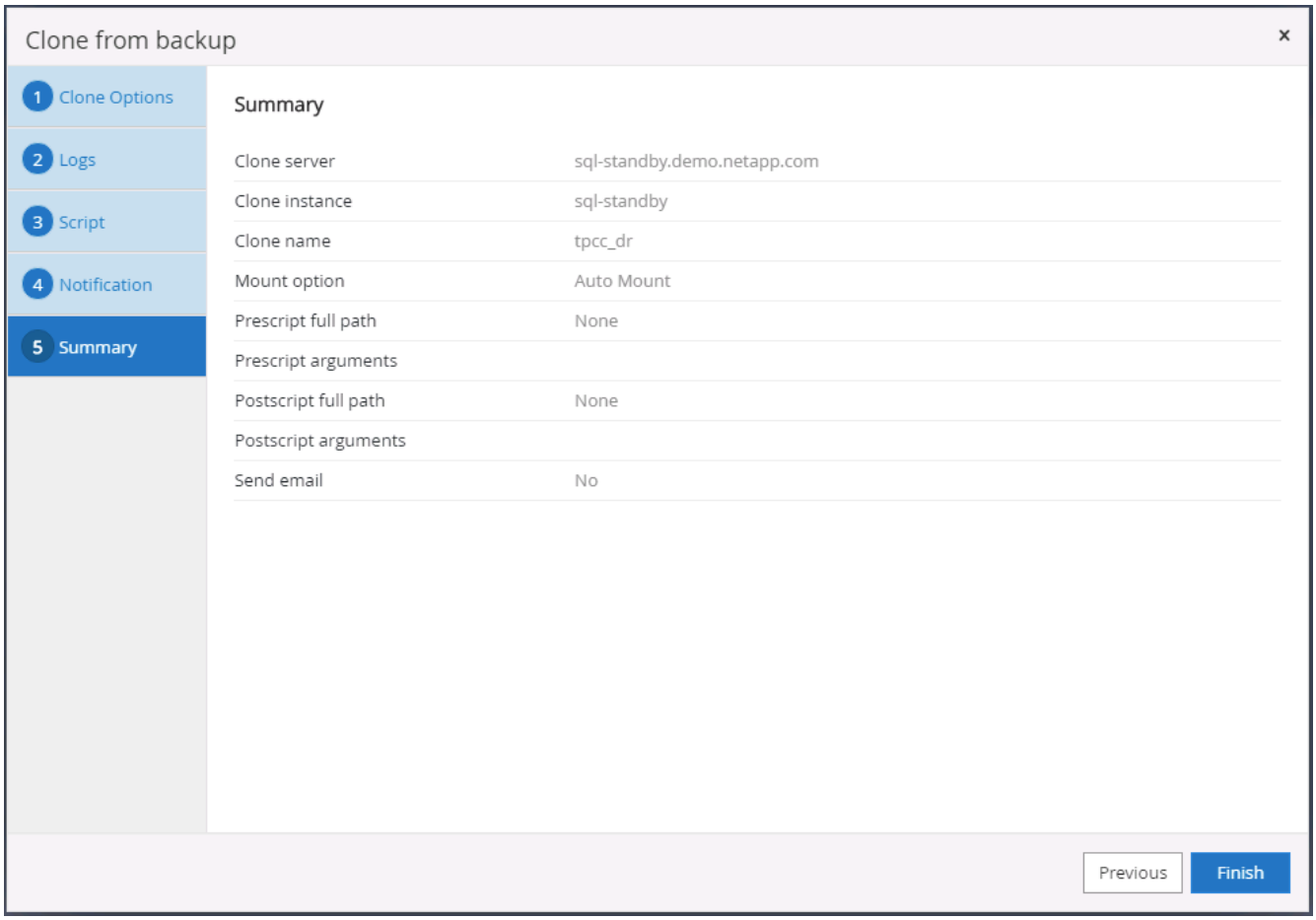
7. Especifique cualquier script opcional que se ejecute antes o después del clonado.

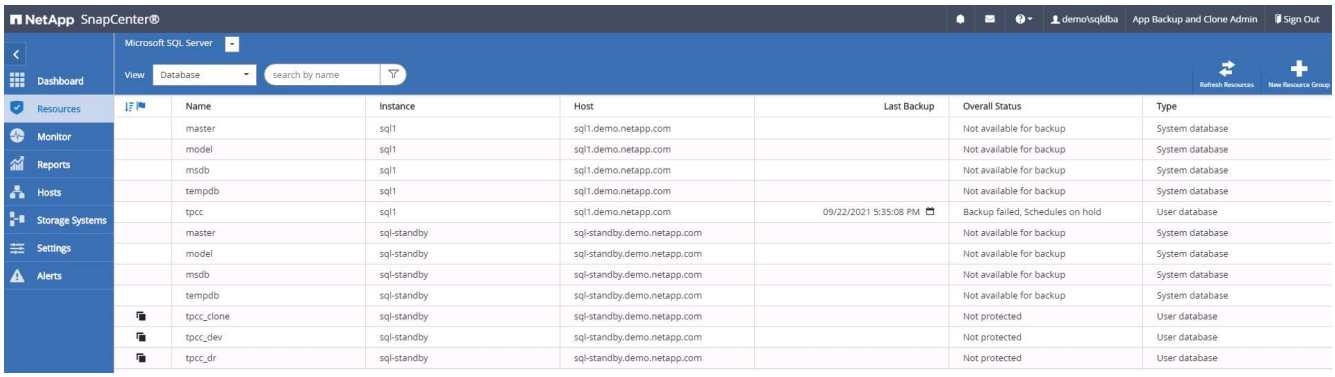


8. Especifique un servidor SMTP si se desea recibir una notificación por correo electrónico.



9. Resumen de los clones de recuperación ante desastres. Las bases de datos clonadas se registran inmediatamente en SnapCenter y se encuentran disponibles para la protección de backups.

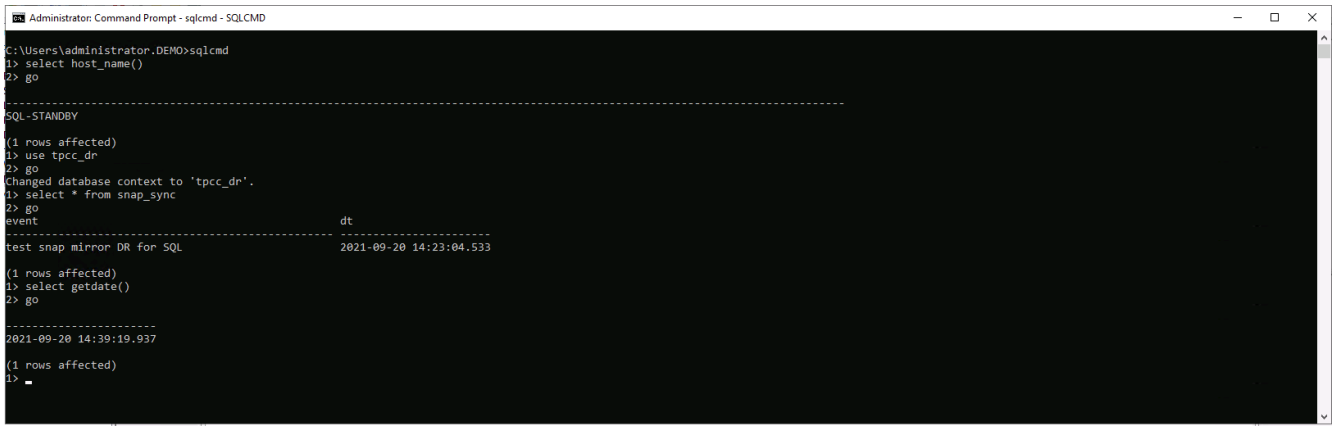




Validación del clon y configuración posteriores a la recuperación ante desastres para SQL

1. Supervise el estado del trabajo de clonado.

2. Validar que se ha replicado y recuperado la última transacción con todos los clones y la recuperación de archivos de registro.



3. Configurar un nuevo directorio de registro de SnapCenter en el servidor DR para el backup de registros de SQL Server.
4. Divida el volumen clonado entre el volumen de origen replicado.
5. Invierta la replicación del cloud a las instalaciones y reconstruya el servidor de bases de datos en las instalaciones con fallos.

¿Dónde obtener ayuda?

Si necesita ayuda con esta solución y casos de uso, únase al "La comunidad de automatización de soluciones de NetApp admite el canal de Slack" y busque el canal de automatización de soluciones para publicar sus preguntas o preguntas.

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

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

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O 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.