Configuración de requisitos previos

NetApp Solutions

NetApp
April 25, 2024

Tabla de contenidos

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.

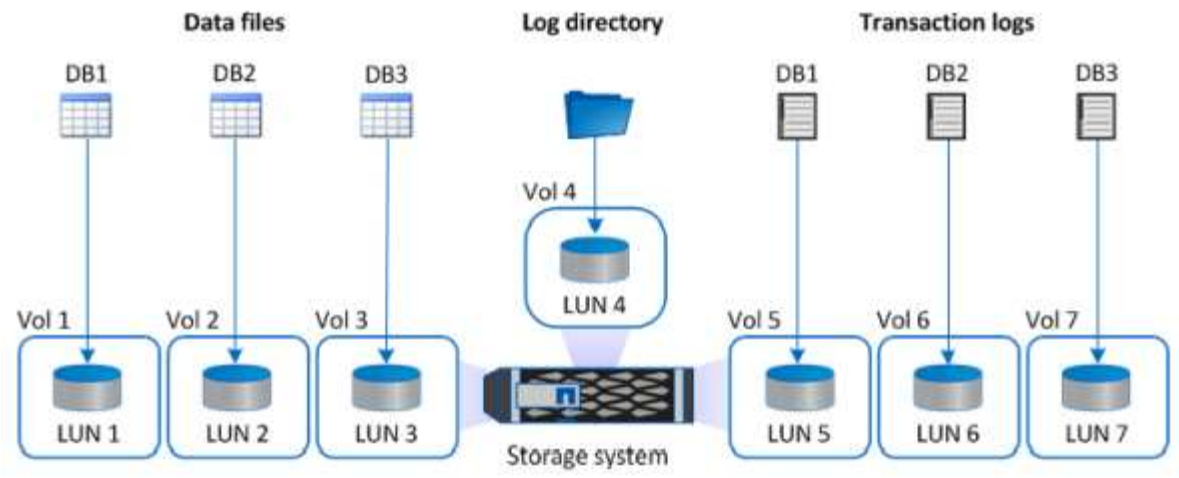
- **Implementación de una sola instancia o de alta disponibilidad.** la implementación de alta disponibilidad ofrece redundancia en caso de un fallo del servidor de instancia de SnapCenter.
- **Resolución de nombres.** se debe configurar DNS en el servidor SnapCenter para resolver todos los hosts de 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.

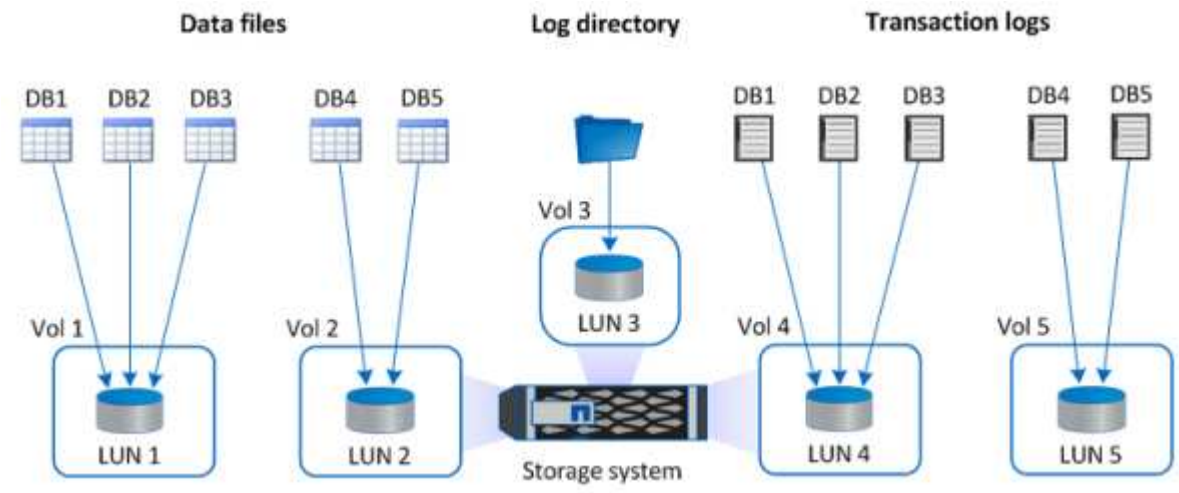
Configuración del almacenamiento del servidor de bases de datos local

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.



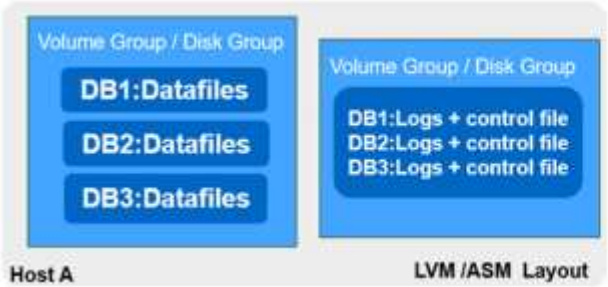
El directorio de registro se dedica a SnapCenter para realizar un paquete acumulativo de registros de transacciones para la recuperación de la base de datos. Para una base de datos extra grande, se pueden asignar varios LUN a un volumen para mejorar el rendimiento.

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".