



Crear recursos de base de datos

Workload Factory for NetApp Console

NetApp
October 07, 2026

This PDF was generated from <https://docs.netapp.com/es-es/data-services-workloads/fsx-databases/create-sql-database-server.html> on October 07, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Crear recursos de base de datos 1
 - Crea un Microsoft SQL Server en NetApp Workload Factory for Databases 1
 - Acerca de esta tarea 1
 - Antes de empezar 2
 - Paso 1: crear un servidor de bases de datos 2
 - Paso 2: habilita la conexión remota en Microsoft SQL Server 10
 - Crea un servidor PostgreSQL en NetApp Workload Factory for Databases 10
 - Acerca de esta tarea 11
 - Antes de empezar 11
 - Crear un servidor PostgreSQL 11
- Crear una base de datos de Microsoft SQL en NetApp Workload Factory for Databases 17
 - Crear una base de datos 18
- Crear un clon de sandbox en NetApp Workload Factory for Databases 19

Crear recursos de base de datos

Crea un Microsoft SQL Server en NetApp Workload Factory for Databases

Para crear un nuevo Microsoft SQL Server, o host de bases de datos, en Workload Factory for Databases, es necesario implementar un sistema de archivos FSx for ONTAP y disponer de recursos para Active Directory.

Acerca de esta tarea

Antes de crear un Microsoft SQL Server desde Workload Factory, infórmate sobre los tipos de implementación de almacenamiento disponibles para la configuración del host de la base de datos, la configuración de E/S multirruta de Microsoft, la implementación de Active Directory, los detalles de red y los requisitos necesarios para llevar a cabo esta operación.

Tras la implementación, tendrás que [habilita la conexión remota en Microsoft SQL Server](#).

FSx para implementaciones del sistema de archivos ONTAP

Para crear un nuevo Microsoft SQL Server, necesitas un sistema de archivos FSx for ONTAP como back-end de almacenamiento. Puedes usar un sistema de archivos FSx for ONTAP existente o crear uno nuevo. Si seleccionas un sistema de archivos FSx for ONTAP existente como back-end de almacenamiento de tu servidor de bases de datos, crearemos una nueva máquina virtual de almacenamiento para las cargas de trabajo de Microsoft SQL.

Los sistemas de archivos FSx for ONTAP tienen dos modelos de implementación de Microsoft SQL Server: *instancia de clúster de conmutación por error (FCI)* o *independiente*. Se crean distintos recursos para el sistema de archivos FSx for ONTAP según el modelo de implementación de FSx for ONTAP que selecciones.

- **Implementación de Microsoft SQL en Failover Cluster Instance (FCI):** se implementa un sistema de archivos FSx for NetApp ONTAP de Multiple Availability Zone cuando seleccionas un nuevo sistema de archivos FSx for ONTAP para la implementación de FCI. Se crean volúmenes y LUN independientes para los archivos de datos, registro y tempdb para una implementación de FCI. Se crean un volumen y un LUN adicionales para el disco de quorum o testigo del clúster de Windows.
- **Implementación independiente de Microsoft SQL:** al crear un nuevo Microsoft SQL Server, se crea un sistema de archivos Single Availability Zone FSx for ONTAP. Además, se crean volúmenes y LUN independientes para los archivos de datos, de registro y de tempdb.

Configuración de E/S multirruta de Microsoft

Ambos modelos de implementación de Microsoft SQL Server requieren la creación de LUN mediante el protocolo de almacenamiento iSCSI. Workload Factory configura Microsoft Multi-path I/O (MPIO) como parte de la configuración de LUN para SQL Server sobre FSx for ONTAP. MPIO se configura según las prácticas recomendadas de AWS y NetApp.

Para obtener más información, consulta ["Implementaciones de alta disponibilidad de SQL Server con Amazon FSx for NetApp ONTAP"](#).

Active Directory

Durante la implementación, en Active Directory (AD) ocurre lo siguiente:

- Se crea una nueva cuenta de servicio de Microsoft SQL en el dominio si no proporcionas una cuenta de

servicio de SQL existente.

- El clúster de Windows, los nombres de host de los nodos y el nombre FCI de Microsoft SQL se añaden como equipos gestionados a la cuenta de servicio de Microsoft SQL.
- La entrada del clúster de Windows tiene permisos para agregar equipos al dominio.

Grupos de seguridad de Active Directory gestionados por el usuario

Si seleccionas «Active Directory gestionado por el usuario» durante la implementación de Microsoft SQL Server en Workload Factory, debes proporcionar un grupo de seguridad que permita el tráfico entre las instancias de EC2 y el servicio de directorio para la implementación. Workload Factory no adjunta automáticamente el grupo de seguridad para Active Directory gestionado por el usuario, como sí lo hace para AWS Managed Microsoft AD.

Reversión de recursos

Si decides revertir los recursos del Sistema de Nombres de Dominio (DNS), los registros de recursos de AD y DNS no se eliminan automáticamente. Puedes eliminar los registros del servidor DNS y de AD de la siguiente manera.

- Para un AD gestionado por el usuario, primero ["eliminar el equipo de AD"](#). A continuación, conéctate al servidor DNS desde DNS manager y ["elimina los registros de recursos DNS"](#).
- Para AWS Managed Microsoft AD, ["instalar las herramientas de administración de AD"](#). A continuación, ["eliminar el equipo de AD"](#). Por último, conéctate al servidor DNS desde el gestor de DNS y ["elimina los registros de recursos DNS"](#).

Antes de empezar

Asegúrate de que cumples los siguientes requisitos previos antes de crear un nuevo host de base de datos.

Credenciales y permisos

Debes ["concede permisos para la creación de hosts de bases de datos"](#) en tu cuenta de AWS para crear un nuevo host de base de datos en Workload Factory.

Active Directory

Al conectarte a Active Directory, debes tener acceso de administrador con permisos para hacer lo siguiente:

- Únete al dominio
- Crear objetos de equipo
- Crear objetos en la unidad organizativa (OU) predeterminada
- Ver todas las propiedades
- Convierte al usuario del dominio en administrador local en los nodos de AD
- Crea un usuario de servicio de Microsoft SQL Server en AD, si aún no existe

Paso 1: crear un servidor de bases de datos

Puedes utilizar los modos de implementación *Quick create* o *Advanced create* para completar esta tarea en Workload Factory con permisos del modo *Automate*. También puedes utilizar las siguientes herramientas disponibles en Codebox: API de REST, AWS CLI, AWS CloudFormation y Terraform. ["Descubre cómo utilizar Codebox para la automatización"](#).



Al utilizar Terraform desde Codebox, el código que copias o descargas oculta las contraseñas

de `fsxadmin` y `vsadmin`. Tendrás que volver a introducir las contraseñas cuando ejecutes el código. Tendrás que incluir los siguientes permisos para la cuenta de usuario además de los permisos del modo *Automate*: `iam:TagRole` y `iam:TagInstanceProfile`. ["Aprende a usar Terraform desde Codebox"](#).

Durante la implementación, Workload Factory habilita CredSSP para la delegación de credenciales a scripts destinados a aprovisionar SQL. Si la política de grupo bloquea la delegación de CredSSP para todos los equipos del dominio, la implementación falla. Tras la implementación, Workload Factory deshabilita CredSSP.

Creación rápida



En *Quick create*, FCI es el modelo de implementación predeterminado, Windows 2016 es la versión predeterminada de Windows y SQL 2019 Standard Edition es la versión predeterminada de SQL.

Pasos

1. Inicia sesión en ["NetApp Console"](#).
2. Selecciona el menú , **Cargas de trabajo > Bases de datos**.
3. En Databases Overview, selecciona **Deploy host** y luego selecciona **Microsoft SQL Server** del menú.
4. Selecciona **Creación rápida**.
5. En **Configuración de AWS**, introduce lo siguiente:
 - a. **Credenciales de AWS**: selecciona las credenciales de AWS con permisos de automatización para implementar el nuevo host de base de datos.

Las credenciales de AWS con permisos para la *creación de hosts de bases de datos* permiten a Workload Factory implementar y gestionar el nuevo host de base de datos desde tu cuenta de AWS dentro de workload factory.

Las credenciales de AWS con permisos de *visualización, planificación y análisis* permiten a Workload Factory generar una plantilla de CloudFormation para que la utilices en la consola de AWS CloudFormation.

Si no tienes credenciales de AWS asociadas en Workload Factory y quieres crear el nuevo servidor en Workload Factory, sigue la **Option 1** para ir a la página Credentials. Añade manualmente las credenciales necesarias y los permisos de *creación del host de la base de datos* para las cargas de trabajo de bases de datos.

Si deseas rellenar el formulario de creación de un nuevo servidor en Workload Factory para poder descargar una plantilla completa del archivo YAML para su implementación en AWS CloudFormation, sigue la **Opción 2** para asegurarte de que dispones de los permisos necesarios para crear el nuevo servidor en AWS CloudFormation. Añade manualmente las credenciales necesarias y los permisos de *visualización, planificación y análisis* para las cargas de trabajo de bases de datos.

Si lo prefieres, puedes descargar una plantilla de archivo YAML parcialmente completada desde el Codebox para crear la pila fuera de Workload Factory sin necesidad de credenciales ni permisos. Selecciona **CloudFormation** en el menú desplegable del Codebox para descargar el archivo YAML.

b. **Región & VPC:** selecciona una región y una red VPC.

Asegúrate de que las subredes de implementación estén asociadas a los puntos finales de interfaz existentes y de que los grupos de seguridad permitan el acceso al protocolo HTTPS (443) a las subredes seleccionadas.

Los puntos de conexión de la interfaz de los servicios de AWS (SQS, FSx, EC2, CloudWatch, CloudFormation, SSM) y el punto de conexión de la pasarela de S3 se crean durante la implementación si no existen.

Los atributos DNS de la VPC `EnableDnsSupport` y `EnableDnsHostnames` se modifican para habilitar la resolución de direcciones de endpoints si aún no están configurados como `true`.

Al utilizar un DNS entre VPC, el grupo de seguridad de los endpoints de la otra VPC donde reside el DNS debe permitir el acceso al puerto 443 desde las subredes de implementación. De no ser así, deberás proporcionar un resolutor DNS desde la VPC local al unirte a un Active Directory entre VPC. En un entorno con varios controladores de dominio replicados, si no puedes acceder a algunos controladores de dominio desde la subred, puedes **redirigir a CloudFormation** e introducir `Preferred domain controller` para conectarte a Active Directory.

c. **Zonas de disponibilidad:** selecciona las zonas de disponibilidad y las subredes de acuerdo con el modelo de implementación de la instancia de clúster de conmutación por error (FCI).



Las implementaciones de FCI solo son compatibles con configuraciones de FSx for ONTAP de Multiple Availability Zone (MAZ).

- i. En el campo **Cluster configuration - Node 1**, selecciona la zona de disponibilidad principal para la configuración de MAZ FSx for ONTAP en el menú desplegable **Availability zone** y una subred de la zona de disponibilidad principal en el menú desplegable **Subnet**.
- ii. En el campo **Configuración del clúster - Nodo 2**, selecciona la zona de disponibilidad secundaria para la configuración de MAZ FSx for ONTAP en el menú desplegable **Zona de disponibilidad** y una subred de la zona de disponibilidad secundaria en el menú desplegable **Subred**.

6. En **Configuración de la aplicación**, introduce un nombre de usuario y una contraseña para **Credenciales de la base de datos**.

Para las cuentas GovCloud, introduce el valor del parámetro ARN de AWS SSM en el siguiente formato: `{fsx:{"username":"fsxadmin","password":"pass"}}`.

El valor se proporciona en el Parameter Store bajo Parameter details en la AWS Management Console. El tipo de parámetro AWS SSM debe ser "Secure String" con el nombre en el formato `/netapp/wlmdb/<anyname>`. Obtén más información sobre cómo recuperar parámetros SSM desde ["AWS GovCloud documentación"](#).

7. En el apartado **Conectividad**, indica lo siguiente:

a. **Par de claves:** selecciona un par de claves.

b. **Active Directory:**

- i. En el campo **Nombre de dominio**, selecciona o introduce un nombre para el dominio.

A. En el caso de los directorios Active Directory administrados por AWS, los nombres de dominio aparecen en el menú desplegable.

- B. En el caso de un Active Directory gestionado por el usuario, introduce un nombre en el campo **Search and Add** y haz clic en **Add**.
- ii. En el campo **Dirección DNS**, introduce la dirección IP del DNS del dominio. Puedes añadir hasta 3 direcciones IP.

En el caso de los Active Directory gestionados por AWS, las direcciones IP de DNS aparecen en el menú desplegable.

- iii. En el campo **Nombre de usuario**, introduce el nombre de usuario del dominio de Active Directory.
- iv. En el campo **Contraseña**, introduce una contraseña para el dominio de Active Directory.

Para las cuentas GovCloud, introduce el valor ARN del parámetro SSM de AWS para las credenciales de Active Directory en el siguiente formato:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. El tipo de parámetro AWS SSM debe ser "Secure String" con el nombre en el formato `/netapp/wlmdb/<anyname>`. Obtén más información sobre cómo recuperar parámetros SSM desde ["AWS GovCloud documentación"](#).

8. En **Configuración de infraestructura**, introduce lo siguiente:

- a. **FSx for ONTAP system**: crea un nuevo sistema de archivos FSx for ONTAP o usa un sistema de archivos FSx for ONTAP existente.

- i. **Crear un nuevo FSx para ONTAP**: introduce el nombre de usuario y la contraseña.

Para las cuentas GovCloud, introduce el valor ARN del parámetro AWS SSM para las credenciales de FSx para ONTAP en el siguiente formato:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. El tipo de parámetro AWS SSM debe ser "Secure String" con el nombre en el formato `/netapp/wlmdb/<anyname>`. Obtén más información sobre cómo recuperar parámetros SSM desde ["AWS GovCloud documentación"](#).

Un nuevo sistema de archivos FSx para ONTAP puede añadir 30 minutos o más al tiempo de instalación.

- i. **Selecciona un FSx for ONTAP** existente: selecciona el nombre de FSx for ONTAP e introduce un nombre de usuario y una contraseña para el sistema de archivos.

En el caso de los sistemas de archivos FSx for ONTAP ya existentes, asegúrate de lo siguiente:

- El grupo de enrutamiento asociado a FSx for ONTAP permite usar rutas a las subredes para el despliegue.
- El grupo de seguridad permite el tráfico desde las subredes usadas para el despliegue, concretamente los puertos TCP HTTPS (443) e iSCSI (3260).

- b. **Tamaño de la unidad de datos**: introduce la capacidad de la unidad de datos y selecciona la unidad de capacidad.

9. Resumen:

- a. **Vista previa predeterminada**: revisa las configuraciones predeterminadas establecidas por Quick create.
- b. **Coste estimado**: ofrece una estimación de los gastos en los que podrías incurrir si

implementaras los recursos que se muestran.

10. Haz clic en **Crear**.

Como alternativa, si quieres cambiar ahora alguna de estas configuraciones predeterminadas, crea el servidor de bases de datos con Advanced create.

También puedes seleccionar **Guardar configuración** para implementar el host más adelante.

Creación avanzada

Pasos

1. Inicia sesión en "NetApp Console".
2. Selecciona el menú , **Cargas de trabajo > Bases de datos**.
3. En Databases Overview, selecciona **Deploy host** y luego selecciona **Microsoft SQL Server** del menú.
4. Selecciona **Advanced create**.
5. En **Modelo de implementación**, selecciona **Instancia de clúster de conmutación por error o Instancia única**.
6. En **Configuración de AWS**, introduce lo siguiente:
 - a. **Credenciales de AWS**: selecciona las credenciales de AWS con permisos de automatización para implementar el nuevo host de base de datos.

Las credenciales de AWS con permisos para la *creación de hosts de bases de datos* permiten a Workload Factory implementar y gestionar el nuevo host de base de datos desde tu cuenta de AWS dentro de workload factory.

Las credenciales de AWS con permisos de *visualización, planificación y análisis* permiten a Workload Factory generar una plantilla de CloudFormation para que la utilices en la consola de AWS CloudFormation.

Si no tienes credenciales de AWS asociadas en Workload Factory y quieres crear el nuevo servidor en Workload Factory, sigue la **Option 1** para ir a la página Credentials. Añade manualmente las credenciales necesarias y los permisos de *creación del host de la base de datos* para las cargas de trabajo de bases de datos.

Si deseas rellenar el formulario de creación de un nuevo servidor en Workload Factory para poder descargar una plantilla completa del archivo YAML para su implementación en AWS CloudFormation, sigue la **Opción 2** para asegurarte de que dispones de los permisos necesarios para crear el nuevo servidor en AWS CloudFormation. Añade manualmente las credenciales necesarias y los permisos de *visualización, planificación y análisis* para las cargas de trabajo de bases de datos.

Si lo prefieres, puedes descargar una plantilla de archivo YAML parcialmente completada desde el Codebox para crear la pila fuera de Workload Factory sin necesidad de credenciales ni permisos. Selecciona **CloudFormation** en el menú desplegable del Codebox para descargar el archivo YAML.

- b. **Región & VPC**: selecciona una región y una red VPC.

Asegúrate de que los grupos de seguridad de un punto final de interfaz existente permitan el acceso al protocolo HTTPS (443) a las subredes seleccionadas.

Los puntos de conexión de la interfaz de los servicios de AWS (SQS, FSx, EC2, CloudWatch, Cloud Formation, SSM) y el punto de conexión de la puerta de enlace de S3 se crean durante la implementación si no se encuentran.

Los atributos DNS de la VPC `EnableDnsSupport` y `EnableDnsHostnames` se modifican para habilitar la resolución de direcciones de puntos finales si aún no están configurados en `true`.

- c. **Zonas de disponibilidad:** selecciona las zonas de disponibilidad y las subredes según el modelo de implementación que hayas elegido. Las subredes no deben compartir la misma tabla de rutas para garantizar la alta disponibilidad.



Las implementaciones de FCI solo son compatibles con configuraciones de FSx for ONTAP de Multiple Availability Zone (MAZ).

- Para implementaciones de una sola instancia:
 - En el campo **Configuración del clúster - Nodo 1**, selecciona una zona de disponibilidad en el menú desplegable **Zona de disponibilidad** y una subred en el menú desplegable **Subred**.
- Para implementaciones de FCI:
 - En el campo **Cluster configuration - Node 1**, selecciona la zona de disponibilidad principal para la configuración de MAZ FSx for ONTAP en el menú desplegable **Availability zone** y una subred de la zona de disponibilidad principal en el menú desplegable **Subnet**.
 - En el campo **Configuración del clúster - Nodo 2**, selecciona la zona de disponibilidad secundaria para la configuración de MAZ FSx for ONTAP en el menú desplegable **Zona de disponibilidad** y una subred de la zona de disponibilidad secundaria en el menú desplegable **Subred**.

- d. **Grupo de seguridad:** Se crea un grupo de seguridad de carga de trabajo para permitir los puertos y protocolos necesarios para la comunicación en clúster de Microsoft SQL y Windows en los nodos. Además, puedes seleccionar uno o varios grupos de seguridad.

7. En **Configuración de la aplicación**, introduce lo siguiente:

- a. En **Tipo de instalación de SQL Server**, selecciona **AMI con licencia incluida** o **Usar AMI personalizada**.

- i. Si seleccionas «AMI con licencia incluida», introduce los siguientes datos:

- A. **Sistema operativo:** selecciona **Windows server 2016**, **Windows server 2019** o **Windows server 2022**.
- B. **Edición de la base de datos:** selecciona **SQL Server Standard Edition** o **SQL Server Enterprise Edition**.
- C. **Versión de la base de datos:** selecciona **SQL Server 2016**, **SQL Server 2019** o **SQL Server 2022**.
- D. **AMI de SQL Server:** selecciona una AMI de SQL Server del menú desplegable.

- ii. Si seleccionas **Use custom AMI**, elige una AMI del menú desplegable.

- b. **Intercalación de SQL Server:** selecciona un conjunto de intercalación para el servidor.



Si el conjunto de intercalación seleccionado no es compatible para la instalación, te recomendamos que selecciones la intercalación predeterminada

"SQL_Latin1_General_CP1_CI_AS".

- c. **Nombre de la base de datos:** Introduce el nombre del clúster de la base de datos.
- d. **Credenciales de la base de datos:** introduce un nombre de usuario y una contraseña para una nueva cuenta de servicio o utiliza las credenciales de una cuenta de servicio existente en Active Directory.

Opcional: selecciona **Usar cuenta de servicio administrada** para la cuenta de servicio de SQL Server. Utiliza esta opción si tu entorno usa MSA (Managed Service Account) o Group Managed Service Accounts (gMSA), donde Active Directory se encarga de la gestión de contraseñas.

Para las cuentas GovCloud, introduce el valor del parámetro ARN de AWS SSM en el siguiente formato: `{fsx:{"username":"fsxadmin","password":"pass"}}`.

El valor se proporciona en el Parameter Store bajo Parameter details en la AWS Management Console. El tipo de parámetro AWS SSM debe ser "Secure String" con el nombre en el formato `/netapp/wlmdb/<anyname>`. Obtén más información sobre cómo recuperar parámetros SSM desde ["AWS GovCloud documentación"](#).

8. En el apartado **Conectividad**, indica lo siguiente:

- a. **Par de claves:** selecciona un par de claves para conectarte de forma segura a tu instancia.
- b. **Active Directory:** indica los siguientes datos de Active Directory:
 - i. En el campo **Nombre de dominio**, selecciona o introduce un nombre para el dominio.
 - A. En el caso de los directorios Active Directory administrados por AWS, los nombres de dominio aparecen en el menú desplegable.
 - B. En el caso de un Active Directory gestionado por el usuario, introduce un nombre en el campo **Search and Add** y haz clic en **Add**.
 - ii. En el campo **Dirección DNS**, introduce la dirección IP del DNS del dominio. Puedes añadir hasta 3 direcciones IP.

En el caso de los Active Directory gestionados por AWS, las direcciones IP de DNS aparecen en el menú desplegable.

- iii. Introduce el nombre de usuario y la contraseña del dominio de Active Directory.

Para las cuentas GovCloud, introduce el valor ARN del parámetro SSM de AWS para las credenciales de Active Directory en el siguiente formato:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. El tipo de parámetro AWS SSM debe ser "Secure String" con el nombre en el formato `/netapp/wlmdb/<anyname>`. Obtén más información sobre cómo recuperar parámetros SSM desde ["AWS GovCloud documentación"](#).

- iv. **Controlador de dominio preferido:** si lo deseas, introduce el controlador de dominio preferido que usará Active Directory para unirse.
- v. **Ruta de la unidad organizativa preferida:** si lo deseas, introduce la unidad organizativa (OU) de Active Directory a la que deseas unirte.
- vi. **Grupo de Active Directory de destino:** si lo deseas, introduce el grupo de Active Directory de destino al que se añadirán los ordenadores.

9. En **Configuración de infraestructura**, introduce lo siguiente:

- a. **Tipo de instancia de base de datos:** selecciona el tipo de instancia de base de datos en el menú desplegable.
- b. **FSx for ONTAP system:** crea un nuevo sistema de archivos FSx for ONTAP o usa un sistema de archivos FSx for ONTAP existente.
 - i. **Crear un nuevo FSx para ONTAP:** introduce el nombre de usuario y la contraseña.

Para las cuentas GovCloud, introduce el valor ARN del parámetro AWS SSM para las credenciales FSx para ONTAP en el siguiente formato:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. El tipo de parámetro AWS SSM debe ser "Secure String" con el nombre en el formato `/netapp/wlmdb/<anyname>`. Obtén más información sobre cómo recuperar parámetros SSM desde ["AWS GovCloud documentación"](#).

Un nuevo sistema de archivos FSx para ONTAP puede añadir 30 minutos o más al tiempo de instalación.

- ii. **Seleccionar un FSx para ONTAP ya existente:** selecciona el nombre del FSx para ONTAP en el menú desplegable e introduce un nombre de usuario y una contraseña para el sistema de archivos.

En el caso de los sistemas de archivos FSx for ONTAP ya existentes, asegúrate de lo siguiente:

- El grupo de enrutamiento asociado a FSx for ONTAP permite usar rutas a las subredes para el despliegue.
- El grupo de seguridad permite el tráfico desde las subredes usadas para el despliegue, concretamente los puertos TCP HTTPS (443) e iSCSI (3260).

- c. **Política de SnapVault:** Activada por defecto. Las instantáneas se realizan a diario y tienen un periodo de retención de 7 días.

Las instantáneas se asignan a los volúmenes creados para las cargas de trabajo de SQL.

- d. **Tamaño de la unidad de datos:** introduce la capacidad de la unidad de datos y selecciona la unidad de capacidad.
- e. **IOPS aprovisionadas:** selecciona **Automático** o **Aprovisionadas por el usuario**. Si seleccionas **Aprovisionadas por el usuario**, introduce el valor de IOPS.
- f. **Capacidad de rendimiento:** selecciona la capacidad de rendimiento del menú desplegable.

En determinadas regiones, puedes seleccionar una capacidad de rendimiento de 4 GBps. Para aprovisionar 4 GBps de capacidad de rendimiento, tu sistema de archivos FSx for ONTAP debe estar configurado con un mínimo de 5,120 GiB de capacidad de almacenamiento SSD y 160,000 IOPS SSD.

- g. **Cifrado:** selecciona una clave de tu cuenta o una clave de otra cuenta. Debes introducir el ARN de la clave de cifrado de otra cuenta.

Las claves de cifrado personalizadas de FSx para ONTAP no aparecen en la lista según la aplicabilidad del servicio. Selecciona una clave de cifrado de FSx adecuada. Las claves de cifrado que no sean de FSx provocarán un error en la creación del servidor.

Las claves gestionadas por AWS se filtran en función de la aplicabilidad del servicio.

- h. **Etiquetas:** si lo deseas, puedes añadir hasta 40 etiquetas.
- i. **Simple Notification Service:** si lo deseas, puedes activar Simple Notification Service (SNS) para esta configuración seleccionando un tema de SNS para Microsoft SQL Server en el menú desplegable.
 - i. Activa el Simple Notification Service.
 - ii. Selecciona un ARN del menú desplegable.
- j. **supervisión de CloudWatch:** opcionalmente, puedes activar la supervisión de CloudWatch.

Recomendamos habilitar CloudWatch para depurar en caso de fallo. Los eventos que aparecen en la consola de AWS CloudFormation se muestran a grandes rasgos y no especifican la causa raíz. Todos los registros detallados se guardan en la C:\cfn\logs carpeta de las instancias de EC2.

En CloudWatch, se crea un grupo de registros con el nombre de la pila. Debajo del grupo de registros, aparece un flujo de registros para cada nodo de validación y nodo SQL. CloudWatch muestra el progreso del script y proporciona información para ayudarte a entender si la implementación falla y cuándo lo hace.

- a. **Reversión de recursos:** esta función no está disponible actualmente.

10. Resumen

- a. **Coste estimado:** ofrece una estimación de los gastos en los que podrías incurrir si implementaras los recursos que se muestran.

11. Haz clic en **Create** para implementar el nuevo host de bases de datos.

Como alternativa, puedes guardar la configuración.

Paso 2: habilita la conexión remota en Microsoft SQL Server

Una vez implementado el servidor, Workload Factory no habilita la conexión remota en Microsoft SQL Server. Para habilitar la conexión remota, sigue estos pasos.

Pasos

1. Utiliza la identidad del equipo para NTLM consultando "[Seguridad de red: permitir que Sistema local use la identidad del ordenador para NTLM](#)" en la documentación de Microsoft.
2. Comprueba la configuración dinámica de puertos consultando "[Se produjo un error relacionado con la red o específico de la instancia al establecer una conexión con SQL Server](#)" en la documentación de Microsoft.
3. Permite la IP o la subred del cliente requeridas en el grupo de seguridad.

Qué sigue

Ahora puedes "[crear una base de datos en Workload Factory for Databases](#)".

Crea un servidor PostgreSQL en NetApp Workload Factory for Databases

Para crear un nuevo servidor PostgreSQL, o host de base de datos, en NetApp Workload Factory for Databases, es necesario implementar un sistema de archivos FSx for ONTAP

y disponer de recursos para Active Directory.

Acerca de esta tarea

Antes de crear un servidor PostgreSQL desde Workload Factory, infórmate sobre los tipos de implementación de almacenamiento disponibles para la configuración del host de la base de datos, los modos de funcionamiento de Workload Factory y los requisitos necesarios para llevar a cabo esta operación.

FSx para implementaciones del sistema de archivos ONTAP

Para crear un nuevo servidor PostgreSQL, se requiere un sistema de archivos FSx for ONTAP como back-end de almacenamiento. Puedes usar un sistema de archivos FSx for ONTAP existente o crear un nuevo sistema de archivos. Si seleccionas un sistema de archivos FSx for ONTAP existente como back-end de almacenamiento de tu servidor de bases de datos, crearemos una nueva máquina virtual de almacenamiento para las cargas de trabajo de PostgreSQL.

+ Los sistemas de archivos FSx for ONTAP cuentan con dos modelos de implementación del servidor PostgreSQL: *alta disponibilidad (HA)* o *instancia única*. Se crean diferentes recursos para el sistema de archivos FSx for ONTAP según el modelo de implementación de FSx for ONTAP que elijas.

- **Implementación de alta disponibilidad (HA):** se implementa un sistema de archivos FSx for NetApp ONTAP de varias zonas de disponibilidad cuando se selecciona un nuevo sistema de archivos FSx for ONTAP para una implementación de HA. Se crean volúmenes y LUN independientes para los archivos de datos, registro y tempdb en una implementación de HA. Se crean un volumen y un LUN adicionales para el disco de quórum o testigo de Windows cluster. La implementación de HA configura la replicación de streaming entre los servidores PostgreSQL primario y secundario.
- **Implementación de instancia única:** cuando se crea un nuevo servidor PostgreSQL, se crea un sistema de archivos FSx for ONTAP en una única zona de disponibilidad. Además, se crean volúmenes y LUN independientes para los archivos de datos, de registro y de tempdb.

Antes de empezar

Debes tener ["concede permisos para la creación de hosts de bases de datos"](#) en tu cuenta de AWS para crear un nuevo host de base de datos en workload factory.

Crear un servidor PostgreSQL

Puedes usar los modos de implementación *Quick create* o *Advanced create* para completar esta tarea en workload factory con permisos del modo *Automate*. También puedes usar las siguientes herramientas disponibles en Codebox: API de REST, AWS CLI, AWS CloudFormation y Terraform. ["Descubre cómo utilizar Codebox para la automatización"](#).



Al utilizar Terraform desde Codebox, el código que copias o descargas oculta las contraseñas de `fsxadmin` y `vsadmin`. Tendrás que volver a introducir las contraseñas cuando ejecutes el código. Tendrás que incluir los siguientes permisos para la cuenta de usuario además de los permisos del modo *Automate*: `iam:TagRole` y `iam:TagInstanceProfile`. ["Aprende a usar Terraform desde Codebox"](#).

Creación rápida



En *Quick create*, HA es el modelo de implementación predeterminado, Windows 2016 es la versión predeterminada de Windows y SQL 2019 Standard Edition es la versión predeterminada de SQL.

Pasos

1. Inicia sesión en "[NetApp Console](#)".
2. Selecciona el menú , **Cargas de trabajo > Bases de datos**.
3. En Databases Overview, selecciona **Deploy host** y luego selecciona **PostgreSQL Server** en el menú.
4. Selecciona **Creación rápida**.
5. En el apartado **zona de aterrizaje**, indica lo siguiente:

- a. **Credenciales de AWS:** selecciona las credenciales de AWS con permisos de automatización para implementar el nuevo host de base de datos.

Las credenciales de AWS con permisos para la *creación de hosts de bases de datos* permiten a Workload Factory implementar y gestionar el nuevo host de base de datos desde tu cuenta de AWS dentro de workload factory.

Las credenciales de AWS con permisos de *visualización, planificación y análisis* permiten a Workload Factory generar una plantilla de CloudFormation para que la utilices en la consola de AWS CloudFormation.

Si no tienes credenciales de AWS asociadas en Workload Factory y quieres crear el nuevo servidor en Workload Factory, sigue la **Option 1** para ir a la página Credentials. Añade manualmente las credenciales necesarias y los permisos de *creación del host de la base de datos* para las cargas de trabajo de bases de datos.

Si deseas rellenar el formulario de creación de un nuevo servidor en Workload Factory para poder descargar una plantilla completa del archivo YAML para su implementación en AWS CloudFormation, sigue la **Opción 2** para asegurarte de que dispones de los permisos necesarios para crear el nuevo servidor en AWS CloudFormation. Añade manualmente las credenciales necesarias y los permisos de *visualización, planificación y análisis* para las cargas de trabajo de bases de datos.

Si lo prefieres, puedes descargar una plantilla de archivo YAML parcialmente completada desde el Codebox para crear la pila fuera de Workload Factory sin necesidad de credenciales ni permisos. Selecciona **CloudFormation** en el menú desplegable del Codebox para descargar el archivo YAML.

- b. **Región & VPC:** selecciona una región y una red VPC.

Asegúrate de que los grupos de seguridad de un punto final de interfaz existente permitan el acceso al protocolo HTTPS (443) a las subredes seleccionadas.

Los puntos de conexión de la interfaz de los servicios de AWS (SQS, FSx, EC2, CloudWatch, CloudFormation, SSM) y el punto de conexión de la pasarela de S3 se crean durante la implementación si no existen.

Los atributos DNS de la VPC `EnableDnsSupport` y `EnableDnsHostnames` se modifican para habilitar la resolución de direcciones de endpoints si aún no están configurados como `true`.

- c. **Zonas de disponibilidad:** selecciona las zonas de disponibilidad y las subredes.



Las implementaciones de HA solo son compatibles con configuraciones de FSx for ONTAP de Multiple Availability Zone (MAZ).

Las subredes no deben compartir la misma tabla de rutas para garantizar una alta disponibilidad.

- i. En el campo **Cluster configuration - Node 1**, selecciona la zona de disponibilidad principal para la configuración de MAZ FSx for ONTAP en el menú desplegable **Availability zone** y una subred de la zona de disponibilidad principal en el menú desplegable **Subnet**.
 - ii. En el campo **Configuración del clúster - Nodo 2**, selecciona la zona de disponibilidad secundaria para la configuración de MAZ FSx for ONTAP en el menú desplegable **Zona de disponibilidad** y una subred de la zona de disponibilidad secundaria en el menú desplegable **Subred**.
6. En **Configuración de la aplicación**, introduce un nombre de usuario y una contraseña para **Credenciales de la base de datos**.
 7. En **Conectividad**, selecciona un par de claves para conectarte de forma segura a tu instancia.
 8. En **Configuración de infraestructura**, introduce lo siguiente:
 - a. **FSx for ONTAP system**: crea un nuevo sistema de archivos FSx for ONTAP o usa un sistema de archivos FSx for ONTAP existente.

- i. **Crear un nuevo FSx para ONTAP**: introduce el nombre de usuario y la contraseña.

Para las cuentas GovCloud, introduce el valor ARN del parámetro AWS SSM para las credenciales de FSx para ONTAP en el siguiente formato:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. El tipo de parámetro AWS SSM debe ser "Secure String" con el nombre en el formato `/netapp/wlmdb/<anyname>`. Obtén más información sobre cómo recuperar parámetros SSM desde ["AWS GovCloud documentación"](#).

Un nuevo sistema de archivos FSx para ONTAP puede añadir 30 minutos o más al tiempo de instalación.

- i. **Seleccionar un FSx para ONTAP ya existente**: selecciona el nombre del FSx para ONTAP en el menú desplegable e introduce un nombre de usuario y una contraseña para el sistema de archivos.

En el caso de los sistemas de archivos FSx for ONTAP ya existentes, asegúrate de lo siguiente:

- El grupo de enrutamiento asociado a FSx for ONTAP permite usar rutas a las subredes para el despliegue.
- El grupo de seguridad permite el tráfico desde las subredes usadas para el despliegue, concretamente los puertos TCP HTTPS (443) e iSCSI (3260).

- b. **Tamaño de la unidad de datos**: introduce la capacidad de la unidad de datos y selecciona la unidad de capacidad.

9. Resumen:

- a. **Vista previa predeterminada**: revisa las configuraciones predeterminadas establecidas por Quick create.
- b. **Coste estimado**: ofrece una estimación de los gastos en los que podrías incurrir si implementaras los recursos que se muestran.

10. Haz clic en **Crear**.

Como alternativa, si quieres cambiar ahora alguna de estas configuraciones predeterminadas, crea el servidor de bases de datos con Advanced create.

También puedes seleccionar **Guardar configuración** para implementar el host más adelante.

Creación avanzada

Pasos

1. Inicia sesión en ["NetApp Console"](#).
2. Selecciona el menú , **Cargas de trabajo > Bases de datos**.
3. En Databases Overview, selecciona **Deploy host** y luego selecciona **PostgreSQL Server** en el menú.
4. Selecciona **Advanced create**.
5. En **modelo de implementación**, selecciona **instancia independiente** o **alta disponibilidad (HA)**.
6. En el apartado **zona de aterrizaje**, indica lo siguiente:

- a. **Credenciales de AWS:** selecciona las credenciales de AWS con permisos de automatización para implementar el nuevo host de base de datos.

Las credenciales de AWS con permisos para la *creación de hosts de bases de datos* permiten a Workload Factory implementar y gestionar el nuevo host de base de datos desde tu cuenta de AWS dentro de workload factory.

Las credenciales de AWS con permisos de *visualización, planificación y análisis* permiten a Workload Factory generar una plantilla de CloudFormation para que la utilices en la consola de AWS CloudFormation.

Si no tienes credenciales de AWS asociadas en Workload Factory y quieres crear el nuevo servidor en Workload Factory, sigue la **Option 1** para ir a la página Credentials. Añade manualmente las credenciales necesarias y los permisos de *creación del host de la base de datos* para las cargas de trabajo de bases de datos.

Si deseas rellenar el formulario de creación de un nuevo servidor en Workload Factory para poder descargar una plantilla completa del archivo YAML para su implementación en AWS CloudFormation, sigue la **Opción 2** para asegurarte de que dispones de los permisos necesarios para crear el nuevo servidor en AWS CloudFormation. Añade manualmente las credenciales necesarias y los permisos de *visualización, planificación y análisis* para las cargas de trabajo de bases de datos.

Si lo prefieres, puedes descargar una plantilla de archivo YAML parcialmente completada desde el Codebox para crear la pila fuera de Workload Factory sin necesidad de credenciales ni permisos. Selecciona **CloudFormation** en el menú desplegable del Codebox para descargar el archivo YAML.

- b. **Región & VPC:** selecciona una región y una red VPC.

Asegúrate de que los grupos de seguridad de un punto final de interfaz existente permitan el acceso al protocolo HTTPS (443) a las subredes seleccionadas.

Los puntos de conexión de la interfaz de los servicios de AWS (SQS, FSx, EC2, CloudWatch, Cloud Formation, SSM) y el punto de conexión de la puerta de enlace de S3 se crean durante la implementación si no se encuentran.

Los atributos DNS de la VPC `EnableDnsSupport` y `EnableDnsHostnames` se modifican para habilitar la resolución de direcciones de puntos finales si aún no están configurados en `true`.

c. **Zonas de disponibilidad:** selecciona las zonas de disponibilidad y las subredes.

Para implementaciones de una sola instancia

En el campo **Configuración del clúster - Nodo 1**, selecciona una zona de disponibilidad en el menú desplegable **Zona de disponibilidad** y una subred en el menú desplegable **Subred**.

Para implementaciones de HA

- i. En el campo **Cluster configuration - Node 1**, selecciona la zona de disponibilidad principal para la configuración de MAZ FSx for ONTAP en el menú desplegable **Availability zone** y una subred de la zona de disponibilidad principal en el menú desplegable **Subnet**.
 - ii. En el campo **Configuración del clúster - Nodo 2**, selecciona la zona de disponibilidad secundaria para la configuración de MAZ FSx for ONTAP en el menú desplegable **Zona de disponibilidad** y una subred de la zona de disponibilidad secundaria en el menú desplegable **Subred**.
- d. **Grupo de seguridad:** Se crea un grupo de seguridad de carga de trabajo para permitir los puertos y protocolos necesarios para PostgreSQL. Además, puedes seleccionar uno o varios grupos de seguridad.
7. En **Configuración de la aplicación**, introduce lo siguiente:
- a. Selecciona el **sistema operativo** del menú desplegable.
 - b. Selecciona la **versión de PostgreSQL** del menú desplegable.
 - c. **Nombre del servidor de bases de datos:** introduce el nombre del clúster de bases de datos.
 - d. **Credenciales de la base de datos:** introduce un nombre de usuario y una contraseña para una nueva cuenta de servicio o utiliza las credenciales de una cuenta de servicio existente en Active Directory.

Para las cuentas GovCloud, introduce el valor ARN del parámetro SSM de AWS para las credenciales en el siguiente formato:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. El tipo de parámetro AWS SSM debe ser "Secure String" con el nombre en el formato `/netapp/wlmdb/<anyname>`. Obtén más información sobre cómo recuperar parámetros SSM desde ["AWS GovCloud documentación"](#).

8. En **Conectividad**, selecciona un par de claves para conectarte de forma segura a tu instancia.

9. En **Configuración de infraestructura**, introduce lo siguiente:

- a. **Tipo de instancia de base de datos:** selecciona el tipo de instancia de base de datos en el menú desplegable.
- b. **FSx for ONTAP system:** crea un nuevo sistema de archivos FSx for ONTAP o usa un sistema de archivos FSx for ONTAP existente.
 - i. **Crear un nuevo FSx para ONTAP:** introduce el nombre de usuario y la contraseña.

Para las cuentas GovCloud, introduce el valor ARN del parámetro AWS SSM para las credenciales FSx para ONTAP en el siguiente formato:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. El tipo de parámetro AWS SSM debe ser "Secure String" con el nombre en el formato `/netapp/wlmdb/<anyname>`. Obtén más información sobre cómo recuperar parámetros SSM desde ["AWS GovCloud documentación"](#).

Un nuevo sistema de archivos FSx para ONTAP puede añadir 30 minutos o más al tiempo de

instalación.

- ii. **Seleccionar un FSx para ONTAP ya existente:** selecciona el nombre del FSx para ONTAP en el menú desplegable e introduce un nombre de usuario y una contraseña para el sistema de archivos.

En el caso de los sistemas de archivos FSx for ONTAP ya existentes, asegúrate de lo siguiente:

- El grupo de enrutamiento asociado a FSx for ONTAP permite usar rutas a las subredes para el despliegue.
- El grupo de seguridad permite el tráfico desde las subredes usadas para el despliegue, concretamente los puertos TCP HTTPS (443) e iSCSI (3260).

- c. **Política de SnapVault:** Activada por defecto. Las instantáneas se realizan a diario y tienen un periodo de retención de 7 días.

Las instantáneas se asignan a los volúmenes creados para las cargas de trabajo de PostgreSQL.

- d. **Tamaño de la unidad de datos:** introduce la capacidad de la unidad de datos y selecciona la unidad de capacidad.
- e. **IOPS aprovisionadas:** selecciona **Automático** o **Aprovisionadas por el usuario**. Si seleccionas **Aprovisionadas por el usuario**, introduce el valor de IOPS.
- f. **Capacidad de rendimiento:** selecciona la capacidad de rendimiento del menú desplegable.

En determinadas regiones, puedes seleccionar una capacidad de rendimiento de 4 GBps. Para aprovisionar 4 GBps de capacidad de rendimiento, tu sistema de archivos FSx for ONTAP debe estar configurado con un mínimo de 5,120 GiB de capacidad de almacenamiento SSD y 160,000 IOPS SSD.

- g. **Cifrado:** selecciona una clave de tu cuenta o una clave de otra cuenta. Debes introducir el ARN de la clave de cifrado de otra cuenta.

Las claves de cifrado personalizadas de FSx para ONTAP no aparecen en la lista según la aplicabilidad del servicio. Selecciona una clave de cifrado de FSx adecuada. Las claves de cifrado que no sean de FSx provocarán un error en la creación del servidor.

Las claves gestionadas por AWS se filtran en función de la aplicabilidad del servicio.

- h. **Etiquetas:** si lo deseas, puedes añadir hasta 40 etiquetas.
- i. **Servicio de notificación simple:** Opcionalmente, puedes habilitar el Servicio de notificación simple (SNS) para esta configuración seleccionando un tema SNS para PostgreSQL en el menú desplegable.
 - i. Activa el Simple Notification Service.
 - ii. Selecciona un ARN del menú desplegable.
- j. **supervisión de CloudWatch:** opcionalmente, puedes activar la supervisión de CloudWatch.

Recomendamos habilitar CloudWatch para depurar en caso de fallo. Los eventos que aparecen en la consola de AWS CloudFormation se muestran a grandes rasgos y no especifican la causa raíz. Todos los registros detallados se guardan en la `C:\cfn\logs` carpeta de las instancias de EC2.

En CloudWatch, se crea un grupo de registros con el nombre de la pila. Debajo del grupo de registros, aparece un flujo de registros para cada nodo de validación y nodo SQL. CloudWatch muestra el progreso del script y proporciona información para ayudarte a entender si la implementación falla y cuándo lo hace.

a. **Reversión de recursos:** esta función no está disponible actualmente.

10. Resumen

a. **Coste estimado:** ofrece una estimación de los gastos en los que podrías incurrir si implementaras los recursos que se muestran.

11. Haz clic en **Create** para implementar el nuevo host de bases de datos.

Como alternativa, puedes guardar la configuración.

Qué sigue

Puedes configurar manualmente los usuarios, el acceso remoto y las bases de datos en el servidor PostgreSQL implementado.

Crear una base de datos de Microsoft SQL en NetApp Workload Factory for Databases

Crear una nueva base de datos de Microsoft SQL te permite gestionar el recurso dentro de NetApp Workload Factory for Databases.

Acerca de esta tarea

Al crear la base de datos, se crean dos nuevos volúmenes en el sistema de archivos FSx for ONTAP compuestos por LUN independientes para alojar los archivos de datos y de registro de la base de datos. Los archivos de la nueva base de datos cuentan con Thin-Provisioning y solo ocupan unos pocos MB del tamaño total asignado a la nueva base de datos.

Si quieres segregar el almacenamiento de la base de datos, puedes hacerlo usando un *punto de montaje virtual*. El punto de montaje virtual te permite consolidar las bases de datos en unas pocas unidades comunes del host.

Para crear una base de datos en workload factory, necesitas permisos de *visualización, planificación y análisis*. Como alternativa, puedes copiar o descargar una plantilla de código parcialmente completada para completar la operación fuera de workload factory. "[Más información sobre los permisos de Workload Factory](#)" para decidir qué modo quieres usar.



Los Microsoft SQL Servers que utilizan el protocolo SMB no admiten la creación de bases de datos.

Antes de empezar

Cumple los siguientes requisitos previos antes de crear una nueva base de datos.

- **Credenciales y permisos:** Debes tener "[Credenciales de la cuenta de AWS y permisos de operaciones y remediación](#)" para crear una nueva base de datos en Workload Factory.

Como alternativa, puedes utilizar Codebox para copiar una plantilla y así desplegar una base de datos fuera de workload factory mediante la API de REST. "[Más información sobre la automatización de Codebox](#)".

- **Host de Windows:** debes tener suficientes letras de unidad disponibles en Microsoft SQL Server para crear nuevas unidades para la nueva base de datos si usas el modo *Quick create*.
- **Microsoft SQL Server:** debes disponer de un Microsoft SQL Server gestionado en workload factory for Databases para alojar la nueva base de datos.
- **AWS Systems Manager:** asegúrate de que el NT Authority\SYSTEM privilegio de usuario esté habilitado en el host de Microsoft SQL a través de AWS Systems Manager.

Crear una base de datos

Puedes usar los modos de implementación *Quick create* o *Advanced create* para completar esta tarea en Workload Factory.

Creación rápida

Pasos

1. Inicia sesión en "NetApp Console".
2. Selecciona el menú , **Cargas de trabajo > Bases de datos**.
3. En el menú «Bases de datos», selecciona **Inventario**.
4. En el Inventario, selecciona **Microsoft SQL Server** como tipo de motor de base de datos.
5. Selecciona un servidor de bases de datos con una instancia administrada de SQL server para crear la base de datos.
6. Haz clic en el menú de acciones de la instancia gestionada y luego selecciona **Crear base de datos de usuario**.
7. En la página «Crear base de datos de usuarios», en la sección «Información de la base de datos», introduce los siguientes datos:
 - a. **Nombre de la base de datos:** introduce el nombre de la base de datos.
 - b. **Intercalación:** selecciona una intercalación para la base de datos. Se selecciona la intercalación predeterminada SQL_Latin1_General_CP1_CI_AS" en Microsoft SQL Server.
8. En Configuración de archivos, introduce lo siguiente:
 - a. **Modo de configuración de archivos:** selecciona **Creación rápida**.
 - b. **Nombres de archivos y ruta de acceso:**
 - **Nombre del archivo de datos:** introduce el nombre del archivo de datos.
 - **Nombre del archivo de registro:** introduce el nombre del archivo de registro.
 - c. **Tamaños de los archivos:** introduce el tamaño de los datos y el tamaño del archivo de registro de la base de datos.
9. Haz clic en **Crear**.

O bien, si quieres cambiar ahora alguna de estas opciones predeterminadas, cambia **File settings mode** a **Advanced create**.

Creación avanzada

Pasos

1. Inicia sesión en "NetApp Console".
- 2.

Selecciona el menú , **Cargas de trabajo > Bases de datos.**

3. En el menú «Bases de datos», selecciona **Inventario**.
4. En el Inventario, selecciona **Microsoft SQL Server** como tipo de motor de base de datos.
5. Selecciona un servidor de bases de datos con una instancia administrada de SQL server para crear la base de datos.
6. Haz clic en el menú de acciones de la instancia gestionada y luego selecciona **Crear base de datos de usuario**.
7. Selecciona **Crear base de datos de usuario**.
8. En la página «Crear base de datos de usuarios», en la sección «Información de la base de datos», introduce los siguientes datos:
 - a. **Nombre de la base de datos:** introduce el nombre de la base de datos.
 - b. **Intercalación:** selecciona la intercalación para la base de datos. Se selecciona la intercalación predeterminada SQL_Latin1_General_CP1_CI_AS" en Microsoft SQL Server.
9. En Configuración de archivos, introduce lo siguiente:
 - a. **Modo de configuración de archivos:** selecciona **Creación avanzada**.
 - b. **Nombres de archivos y ruta de acceso:**
 - i. **Archivo de datos:** selecciona una letra de la unidad e introduce el nombre del archivo de datos.

Si lo deseas, marca la casilla **Virtual mount point**.
 - ii. **Archivo de registro:** selecciona una letra de la unidad e introduce el nombre del archivo de registro.

Si lo deseas, marca la casilla **Virtual mount point**.
 - c. **Tamaños de los archivos:** introduce el tamaño de los datos y el tamaño del archivo de registro de la base de datos.
10. Haz clic en **Crear**.

Si has creado el host de la base de datos, puedes comprobar el progreso del trabajo en la pestaña **Job monitoring**.

Crear un clon de sandbox en NetApp Workload Factory for Databases

Crear un clon de entorno de pruebas de una base de datos en NetApp Workload Factory for Databases te permite usar el clon para desarrollo, pruebas, integración, análisis, formación, control de calidad y mucho más sin alterar la base de datos de origen.

Acerca de esta tarea

Se crea un clon de entorno de pruebas a partir de la instantánea más reciente de la base de datos de origen. Puede clonarse en el mismo Microsoft SQL Server que la base de datos de origen o en otro Microsoft SQL Server siempre y cuando ambos compartan el mismo sistema de archivos FSx for ONTAP.

Antes de empezar

Asegúrate de cumplir los siguientes requisitos previos antes de crear un clon del entorno de pruebas.

- **Credenciales y permisos:** Debes tener "[Credenciales de la cuenta de AWS y permisos de operaciones y remediación](#)" para crear un clon de entorno de pruebas en Workload Factory.

Como alternativa, puedes usar Codebox para copiar una plantilla completada parcialmente o crear una plantilla completa para que puedas crear el clon de sandbox fuera de Workload Factory mediante la API de REST. "[Más información sobre la automatización de Codebox](#)".

- **Microsoft SQL Server:** debes disponer de un servidor Microsoft SQL Server gestionado en Workload Factory for Databases para alojar el nuevo clon de entorno de pruebas.
- **AWS Systems Manager:** asegúrate de que el `NT Authority\SYSTEM` privilegio de usuario esté habilitado en el host de Microsoft SQL a través de AWS Systems Manager.
- **Base de datos de origen:** necesitas disponer de una base de datos de origen para realizar la clonación.

Pasos

1. Inicia sesión en "[NetApp Console](#)".
2. Selecciona el menú , **Cargas de trabajo > Bases de datos**.
3. En Databases, selecciona la pestaña **Sandboxes**.
4. En la pestaña «Sandboxes», selecciona **Crear nuevo sandbox**.
5. En la página «Crear nuevo entorno de pruebas», en el apartado «Origen de la base de datos», introduce lo siguiente:
 - a. **Host de la base de datos de origen:** selecciona el host de la base de datos de origen.
 - b. **Instancia de base de datos de origen:** selecciona la instancia de base de datos de origen.
 - c. **Base de datos de origen:** selecciona la base de datos de origen desde la que deseas clonar.
6. En el apartado «Base de datos de destino», introduce lo siguiente:
 - a. **Host de base de datos de destino:** selecciona un host de base de datos de destino para el clon del entorno de pruebas que esté en la misma VPC y tenga el mismo sistema de archivos FSx for ONTAP que el host de origen.
 - b. **Instancia de base de datos de destino:** selecciona la instancia de base de datos de destino para el clon del entorno de pruebas.
 - c. **Base de datos de destino:** introduce un nombre para el clon del entorno de pruebas.
7. **Montar:** al clonar una base de datos SQL que contiene varios archivos de datos y/o de registro, Workload Factory clona todos los archivos bajo la letra de unidad asignada automáticamente o definida.

Selecciona una de las siguientes opciones:

- a. **Asignar automáticamente el punto de montaje**
- b. **Definir la ruta del punto de montaje**

Introduce los siguientes datos para definir la ruta del punto de montaje:

- Introduce la letra de la unidad correspondiente a la ruta del archivo de datos.
- Introduce la letra de la unidad para la ruta del archivo de registro.

8. **Definir etiqueta:** selecciona una etiqueta para definir el clon del entorno de pruebas.

9. Haz clic en **Crear**.

Para comprobar el progreso del trabajo, ve a la pestaña **Supervisión de trabajos**.

Información de copyright

Copyright © 2026 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.