# Cree un nuevo servidor de base de datos

Database workloads

NetApp
January 05, 2026

This PDF was generated from https://docs.netapp.com/es-es/workload-databases/create-database-server.html on January 05, 2026. Always check docs.netapp.com for the latest.

# Tabla de contenidos

# Cree un nuevo servidor de base de datos

## Crear un servidor Microsoft SQL Server en Workload Factory para bases de datos

Para crear un nuevo Microsoft SQL Server o un host de base de datos en Workload Factory for Databases se requiere una implementación del sistema de archivos FSx para ONTAP y recursos para Active Directory.

### Acerca de esta tarea

Antes de crear un Microsoft SQL Server desde Workload Factory, obtenga información sobre los tipos de implementación de almacenamiento disponibles para la configuración del host de base de datos, la configuración de E/S de múltiples rutas de Microsoft, la implementación de Active Directory, los detalles de red y los requisitos para completar esta operación.

Después de la implementación, deberá Active la conexión remota en Microsoft SQL Server.

#### FSX para puestas en marcha del sistema de archivos ONTAP

Para crear un nuevo servidor Microsoft SQL Server, se requiere un sistema de archivos FSx para ONTAP como back-end de almacenamiento. Puede utilizar un sistema de archivos FSX for ONTAP existente o crear un nuevo sistema de archivos. Si selecciona un sistema de archivos FSx para ONTAP existente como back-end de almacenamiento de servidor de bases de datos, creamos un nuevo equipo virtual de almacenamiento para las cargas de trabajo de Microsoft SQL.

Los sistemas de archivos FSX para ONTAP tienen dos modelos de implementación de Microsoft SQL Server: *Failover Cluster Instance (FCI)* o *Standalone*. Se crean distintos recursos para el sistema de archivos FSx para ONTAP en función del modelo de puesta en marcha de FSx para ONTAP que seleccione.

- *Implementación de Microsoft SQL de instancia de clúster de conmutación por error (FCI): Se implementa un sistema de archivos FSX para NetApp ONTAP de zona de disponibilidad múltiple cuando se selecciona un nuevo sistema de archivos FSX para ONTAP para la implementación de FCI. Se crean volúmenes y LUN independientes para archivos de datos, registros y tempdb para una implementación de FCI. Se crean un volumen y LUN adicionales para el disco de quórum o de testigo para el clúster de Windows.
- **Implementación independiente de Microsoft SQL**: Se crea un sistema de archivos FSX de zona de disponibilidad única para ONTAP cuando se crea un nuevo servidor Microsoft SQL. Además, se crean volúmenes y LUN independientes para archivos de datos, registros y 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 para ONTAP. MPIO se configura según las mejores prácticas de AWS y NetApp .

Para obtener más información, consulte "Implementaciones de alta disponibilidad de SQL Server con Amazon FSx for NetApp ONTAP" .

#### Active Directory

Lo siguiente ocurre en Active Directory (AD) durante la implementación:

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

servicio SQL existente.

- El clúster de Windows, los nombres de host de nodo y el nombre de FCI de Microsoft SQL se agregan como equipos gestionados a la cuenta de servicio Microsoft SQL.
- A la entrada del clúster de Windows se le asignan permisos para agregar equipos al dominio.

**Grupos de seguridad de Active Directory gestionados por el usuario**

Si selecciona “Active Directory administrado por el usuario” durante la implementación de Microsoft SQL Server en Workload Factory, debe proporcionar un grupo de seguridad que permita el tráfico entre las instancias de EC2 al servicio de directorio para la implementación. Workload Factory no adjunta automáticamente el grupo de seguridad para Active Directory administrado por el usuario como lo hace para AWS Managed Microsoft AD.

**Reversión de recursos**

Si decide revertir los recursos del sistema de nombres de dominio (DNS), los registros de recursos en AD y DNS no se eliminan automáticamente. Puede eliminar los registros del servidor DNS y AD de la siguiente manera.

- Para AD gestionado por el usuario, primero "Extraiga el equipo AD". A continuación, conéctese al servidor DNS desde el administrador DNS y "Elimine los registros de recursos DNS".
- Para AWS Managed Microsoft AD, "Instale las herramientas de administración de AD". A continuación, "Extraiga el equipo AD". Por último, conéctese al servidor DNS desde el administrador DNS y "Elimine los registros de recursos DNS".

## Antes de empezar

Asegúrese de tener los siguientes requisitos previos antes de crear un nuevo host de base de datos.

**Credenciales y permisos**

Usted debe "otorgar permisos de creación de host de base de datos" en su cuenta de AWS para crear un nuevo host de base de datos en Workload Factory.

**Active Directory**

Al conectarse a Active Directory, debe tener acceso administrativo con permisos para hacer lo siguiente:

- Únase al dominio
- Crear objetos de computadora
- Crear objetos en la unidad de organización (OU) por defecto
- Leer todas las propiedades
- Convierta al usuario de dominio en un administrador local en los nodos de AD
- Cree un usuario de servicio de Microsoft SQL Server en AD, si aún no existe

## Paso 1: Crear un servidor de base de datos

Puede utilizar los modos de implementación *Creación rápida* o *Creación avanzada* para completar esta tarea en Workload Factory con permisos del modo *Automatizar*. También puede utilizar las siguientes herramientas disponibles en Codebox: API REST, AWS CLI, AWS CloudFormation y Terraform. "Aprende a usar CodeBox para la automatización" .

Al usar Terraform de CodeBox, el código que copie o descargue oculta `fsxadmin` y `vsadmin` las contraseñas. Deberá volver a introducir las contraseñas cuando ejecute el código. Deberá 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 de CodeBox".

Durante la implementación, Workload Factory habilita CredSSP para la delegación de credenciales a scripts para aprovisionar SQL. Cuando la delegación de CredSSP está bloqueada para todos los equipos del dominio con la política de grupo, la implementación falla. Después de 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. Inicie sesión con uno de los "experiencias de consola"botones .
2. En el mosaico Bases de datos, seleccione **Implementar host** y luego seleccione **Microsoft SQL Server** en el menú.
3. Seleccione **Quick create**.
4. En **AWS settings**, proporcione lo siguiente:
   a. **Credenciales de AWS**: Seleccione las credenciales de AWS con permisos automatizados para implementar el nuevo host de base de datos.

      Las credenciales de AWS con permisos de *lectura/escritura* permiten que Workload Factory implemente y administre el nuevo host de base de datos desde su cuenta de AWS dentro de Workload Factory.

      Las credenciales de AWS con permisos de *solo lectura* permiten que Workload Factory genere una plantilla de CloudFormation para que usted la use en la consola de AWS CloudFormation.

      Si no tiene credenciales de AWS asociadas en Workload Factory y desea crear el nuevo servidor en Workload Factory, siga la **Opción 1** para ir a la página Credenciales. Agregue manualmente las credenciales y los permisos necesarios para el modo *lectura/escritura* para las cargas de trabajo de la base de datos.

      Si desea completar el formulario de creación de nuevo servidor en Workload Factory para poder descargar una plantilla de archivo YAML completa para su implementación en AWS CloudFormation, siga la **Opción 2** para asegurarse de tener los permisos necesarios para crear el nuevo servidor dentro de AWS CloudFormation. Agregue manualmente las credenciales y los permisos necesarios para el modo *lectura* para las cargas de trabajo de la base de datos.

      Opcionalmente, puede descargar una plantilla de archivo YAML parcialmente completada desde Codebox para crear la pila fuera de Workload Factory sin credenciales ni permisos. Seleccione **CloudFormation** del menú desplegable en el cuadro de código para descargar el archivo YAML.

   b. **Región y VPC**: Seleccione una región y una red de VPC.

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

      Extremos de la interfaz de servicio de AWS (SQS, FSx, EC2, CloudWatch, CloudFormation, SSM) y el punto final de la puerta de enlace S3 se crean durante el despliegue si no se encuentra.

      Los atributos DNS de VPC `EnableDnsSupport` y `EnableDnsHostnames` se modifican para activar la resolución de direcciones de punto final si aún no están establecidos en `true`.

      Al usar un DNS entre VPC, el grupo de seguridad de los endpoints en la otra VPC donde reside el DNS debe permitir el puerto 443 a las subredes de implementación. De lo contrario, debe

proporcionar un solucionador de DNS desde la VPC local al unirse a un Active Directory entre VPC. En un entorno con varios controladores de dominio replicados, si algunos controladores de dominio no son accesibles desde la subred, puede **Redirigir a CloudFormation** e ingresar `Preferred domain controller` para conectarse a Active Directory.

c. **Zonas de disponibilidad**: Seleccione zonas de disponibilidad y subredes de acuerdo con el modelo de implementación de Failover Cluster Instance (FCI).

> ⓘ Las implementaciones de FCI solo se admiten en configuraciones FSx para ONTAP de varias zonas de disponibilidad (MAZ).

i. En el campo **Configuración de clúster - Nodo 1**, seleccione la zona de disponibilidad principal para la configuración de MAZ FSX para ONTAP en el menú desplegable **Zona de disponibilidad** y una subred de la zona de disponibilidad principal desde el menú desplegable **Subred**.

ii. En el campo **Configuración de clúster - Nodo 2**, seleccione la zona de disponibilidad secundaria para la configuración de MAZ FSX para ONTAP en el menú desplegable **Zona de disponibilidad** y una subred de la zona de disponibilidad secundaria desde el menú desplegable **Subred**.

5. En **Configuración de la aplicación**, introduzca un nombre de usuario y una contraseña para **Credenciales de la base de datos**.
6. En **Conectividad**, proporcione lo siguiente:
   a. **Par claves**: Selecciona un par de claves.
   b. **Active Directory**:
      i. En el campo **Nombre de dominio**, seleccione o introduzca un nombre para el dominio.
         A. En el caso de Active Directories gestionados por AWS, los nombres de dominio aparecen en el menú desplegable.
         B. Para un Active Directory gestionado por el usuario, introduzca un nombre en el campo **Buscar y Agregar** y haga clic en **Agregar**.
      ii. En el campo **DNS address**, ingrese la dirección IP DNS para el dominio. Puede añadir hasta 3 direcciones IP.

      Para los directorios activos gestionados por AWS, las direcciones IP de DNS aparecen en el menú desplegable.

      iii. En el campo **Nombre de usuario**, introduzca el nombre de usuario para el dominio de Active Directory.
      iv. En el campo **Contraseña**, introduzca una contraseña para el dominio de Active Directory.
7. En **Configuración de infraestructura**, proporcione lo siguiente:
   a. **FSX para el sistema ONTAP**: Crea un nuevo sistema de archivos FSX para ONTAP o usa un sistema de archivos FSX para ONTAP existente.
      i. * Crear nuevo FSX para ONTAP*: Introduzca el nombre de usuario y la contraseña.

      Un nuevo sistema de archivos FSX para ONTAP puede agregar 30 minutos o más de tiempo de instalación.

      ii. **Seleccione un FSX para ONTAP**: Seleccione FSX para el nombre de ONTAP en el menú desplegable, e introduzca un nombre de usuario y una contraseña para el sistema de

archivos.

Para los sistemas de archivos FSx para ONTAP existentes, asegúrate de lo siguiente:

- El grupo de enrutamiento conectado a FSx para ONTAP permite que las rutas a las subredes se utilicen para la implementación.
- El grupo de seguridad permite el tráfico de las subredes utilizadas para la puesta en marcha, específicamente los puertos TCP HTTPS (443) e iSCSI (3260).

b. **Tamaño de la unidad de datos**: Ingrese la capacidad de la unidad de datos y seleccione la unidad de capacidad.

8. Resumen:
   a. **Vista previa predeterminada**: Revise las configuraciones predeterminadas establecidas por Quick Create.
   b. **Costo estimado**: Proporciona una estimación de los cargos en los que podría incurrir si implementa los recursos mostrados.
9. Haga clic en **Crear**.

Como alternativa, si desea cambiar cualquiera de estos valores por defecto ahora, cree el servidor de base de datos con Advanced CREATE.

También puede seleccionar **Guardar configuración** para implementar el host más tarde.

**Creación avanzada**

**Pasos**

1. Inicie sesión utilizando uno de los"experiencias de consola" . En el mosaico Bases de datos, seleccione **Implementar host** y luego seleccione **Microsoft SQL Server** en el menú.
2. Selecciona **Creación avanzada**.
3. Para **Modelo de implementación**, seleccione **Instancia de clúster de conmutación por error** o **Instancia única**.
4. En **AWS settings**, proporcione lo siguiente:
   a. **Credenciales de AWS**: Seleccione las credenciales de AWS con permisos automatizados para implementar el nuevo host de base de datos.

   Las credenciales de AWS con permisos de *lectura/escritura* permiten que Workload Factory implemente y administre el nuevo host de base de datos desde su cuenta de AWS dentro de Workload Factory.

   Las credenciales de AWS con permisos de *solo lectura* permiten que Workload Factory genere una plantilla de CloudFormation para que usted la use en la consola de AWS CloudFormation.

   Si no tiene credenciales de AWS asociadas en Workload Factory y desea crear el nuevo servidor en Workload Factory, siga la **Opción 1** para ir a la página Credenciales. Agregue manualmente las credenciales y los permisos necesarios para el modo *lectura/escritura* para las cargas de trabajo de la base de datos.

   Si desea completar el formulario de creación de nuevo servidor en Workload Factory para poder descargar una plantilla de archivo YAML completa para su implementación en AWS CloudFormation, siga la **Opción 2** para asegurarse de tener los permisos necesarios para crear el nuevo servidor dentro de AWS CloudFormation. Agregue manualmente las credenciales y los permisos necesarios para el modo *solo lectura* para las cargas de trabajo de la base de datos.

Opcionalmente, puede descargar una plantilla de archivo YAML parcialmente completada desde Codebox para crear la pila fuera de Workload Factory sin credenciales ni permisos. Seleccione **CloudFormation** del menú desplegable en el cuadro de código para descargar el archivo YAML.

b. **Región y VPC**: Seleccione una región y una red de VPC.

   Asegúrese de que los grupos de seguridad para un extremo de interfaz existente permiten el acceso al protocolo HTTPS (443) a las subredes seleccionadas.

   Extremos de la interfaz del servicio de AWS (SQS, FSx, EC2, CloudWatch, formación de la nube, SSM) y el punto final de la puerta de enlace S3 se crean durante el despliegue si no se encuentra.

   Los atributos DNS de VPC `EnableDnsSupport` y `EnableDnsHostnames` se modifican para activar la resolución de la dirección de punto final si no se ha establecido ya en `true`.

c. **Zonas de disponibilidad**: seleccione zonas de disponibilidad y subredes según el modelo de implementación que haya seleccionado. Las subredes no deben compartir la misma tabla de rutas para lograr una alta disponibilidad.

   > Las implementaciones de FCI solo se admiten en configuraciones FSx para ONTAP de varias zonas de disponibilidad (MAZ).

   - Para implementaciones de instancia única:
     - En el campo **Configuración del clúster - Nodo 1**, seleccione una zona de disponibilidad de la **Zona de disponibilidad** del menú desplegable y una subred del menú desplegable **Subred**.
   - Para implementaciones de FCI:
     - En el campo **Configuración de clúster - Nodo 1**, seleccione la zona de disponibilidad principal para la configuración de MAZ FSX para ONTAP en el menú desplegable **Zona de disponibilidad** y una subred de la zona de disponibilidad principal desde el menú desplegable **Subred**.
     - En el campo **Configuración de clúster - Nodo 2**, seleccione la zona de disponibilidad secundaria para la configuración de MAZ FSX para ONTAP en el menú desplegable **Zona de disponibilidad** y una subred de la zona de disponibilidad secundaria desde el menú desplegable **Subred**.

d. **Grupo de seguridad**: Seleccione un grupo de seguridad existente o cree un nuevo grupo de seguridad. Tres grupos de seguridad se conectan a los nodos SQL (instancias EC2) durante el despliegue del nuevo servidor.

   i. Se crea un grupo de seguridad de cargas de trabajo para permitir la comunicación de los puertos y protocolos necesarios para la comunicación de los clústeres de Microsoft SQL y Windows en los nodos.

   ii. En el caso de Active Directory gestionado por AWS, el grupo de seguridad asociado al servicio de directorio se agrega automáticamente a los nodos de Microsoft SQL para permitir la comunicación con Active Directory.

   iii. Para un sistema de archivos FSX for ONTAP existente, el grupo de seguridad asociado con él se agrega automáticamente a los nodos SQL, lo que permite la comunicación con el sistema de archivos. Cuando se crea un nuevo sistema FSx para ONTAP, se crea un nuevo grupo de seguridad para el sistema de archivos FSx para ONTAP y el mismo grupo de seguridad también se conecta a los nodos SQL.

Para un Active Directory gestionado por el usuario, asegúrese de que el grupo de seguridad configurado en la instancia de AD permite el tráfico de las subredes utilizadas para la implementación. El grupo de seguridad debe permitir la comunicación con los controladores de dominio de Active Directory desde las subredes donde se configuran EC2 instancias para Microsoft SQL.

5. En **Configuración de la aplicación**, proporcione lo siguiente:
   a. En **Tipo de instalación de SQL Server**, selecciona **Licencia incluida AMI** o **Usar AMI personalizada**.
      i. Si selecciona **Licencia incluida AMI**, proporcione lo siguiente:
         A. **Sistema operativo**: Seleccione **Servidor Windows 2016**, **Servidor Windows 2019** o **Servidor Windows 2022**.
         B. **Edición de base de datos**: Seleccione **SQL Server Standard Edition** o **SQL Server Enterprise Edition**.
         C. **Versión de base de datos**: Seleccione **SQL Server 2016**, **SQL Server 2019** o **SQL Server 2022**.
         D. **SQL Server AMI**: Seleccione un AMI de SQL Server en el menú desplegable.
      ii. Si selecciona **Usar AMI personalizada**, seleccione una AMI en el menú desplegable.
   b. **SQL Server collation**: Seleccione un juego de intercalación para el servidor.

      Si el juego de intercalación seleccionado no es compatible para la instalación, se recomienda seleccionar la intercalación por defecto SQL_Latin1_General_CP1_CI_AS.

   c. **Nombre de la base de datos**: Introduzca el nombre del cluster de la base de datos.
   d. **Credenciales de la base de datos**: Introduzca un nombre de usuario y una contraseña para una nueva cuenta de servicio o utilice las credenciales de la cuenta de servicio existentes en Active Directory.

      Opcional: seleccione **Usar cuenta de servicio administrada** para la cuenta de servicio de SQL Server. Utilice esta opción si su entorno utiliza MSA (cuenta de servicio administrada) o cuentas de servicio administradas por grupo (gMSA) donde la administración de contraseñas la gestiona Active Directory.

6. En **Conectividad**, proporcione lo siguiente:
   a. **Par claves**: Selecciona un par de claves para conectarte de forma segura a tu instancia.
   b. **Active Directory**: Proporcione los siguientes detalles de Active Directory:
      i. En el campo **Nombre de dominio**, seleccione o introduzca un nombre para el dominio.
         A. En el caso de Active Directories gestionados por AWS, los nombres de dominio aparecen en el menú desplegable.
         B. Para un Active Directory gestionado por el usuario, introduzca un nombre en el campo **Buscar y Agregar** y haga clic en **Agregar**.
      ii. En el campo **DNS address**, ingrese la dirección IP DNS para el dominio. Puede añadir hasta 3 direcciones IP.

         Para los directorios activos gestionados por AWS, las direcciones IP de DNS aparecen en el menú desplegable.

iii. En el campo **Nombre de usuario**, introduzca el nombre de usuario para el dominio de Active Directory.

iv. En el campo **Contraseña**, introduzca una contraseña para el dominio de Active Directory.

v. **Controlador de dominio preferido**: de manera opcional, ingrese el controlador de dominio preferido que se utilizará para unirse a Active Directory.

vi. **Ruta de unidad organizativa preferida**: de manera opcional, ingrese la unidad organizativa (OU) preferida en Active Directory a la que desea unirse.

vii. **Grupo de Active Directory de destino**: de manera opcional, ingrese el grupo de Active Directory de destino al que se agregarán las computadoras.

7. En **Configuración de infraestructura**, proporcione lo siguiente:

a. **Tipo de instancia de DB**: Seleccione el tipo de instancia de base de datos en el menú desplegable.

b. **FSX para el sistema ONTAP**: Crea un nuevo sistema de archivos FSX para ONTAP o usa un sistema de archivos FSX para ONTAP existente.

i. * Crear nuevo FSX para ONTAP*: Introduzca el nombre de usuario y la contraseña.

Un nuevo sistema de archivos FSX para ONTAP puede agregar 30 minutos o más de tiempo de instalación.

ii. **Seleccione un FSX para ONTAP**: Seleccione FSX para el nombre de ONTAP en el menú desplegable, e introduzca un nombre de usuario y una contraseña para el sistema de archivos.

Para los sistemas de archivos FSx para ONTAP existentes, asegúrate de lo siguiente:

- El grupo de enrutamiento conectado a FSx para ONTAP permite que las rutas a las subredes se utilicen para la implementación.
- El grupo de seguridad permite el tráfico de las subredes utilizadas para la puesta en marcha, específicamente los puertos TCP HTTPS (443) e iSCSI (3260).

c. **Política de instantáneas**: Habilitado por defecto. Las copias Snapshot se realizan diariamente y tienen un período de retención de 7 días.

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

d. **Tamaño de la unidad de datos**: Ingrese la capacidad de la unidad de datos y seleccione la unidad de capacidad.

e. **IOPS provisionadas**: Selecciona **Automático** o **Provisioned por el usuario**. Si selecciona **Provisioned por el usuario**, introduzca el valor de IOPS.

f. **Capacidad de rendimiento**: Seleccione la capacidad de rendimiento en el menú desplegable.

En algunas regiones, puede seleccionar una capacidad de rendimiento de 4 Gbps. Para aprovisionar 4 Gbps de capacidad de rendimiento, su sistema de archivos FSx para ONTAP debe configurarse 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. Debe introducir la clave de cifrado ARN desde otra cuenta.

Las claves de cifrado personalizadas de FSx para ONTAP no se incluyen en la aplicación del

servicio. Seleccione una clave de cifrado FSX adecuada. Las claves de cifrado no 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**: Opcionalmente, puedes añadir hasta 40 etiquetas.

i. **Servicio de Notificación Simple**: Opcionalmente, puede habilitar el Servicio de Notificación Simple (SNS) para esta configuración seleccionando un tema de SNS para Microsoft SQL Server en el menú desplegable.

   i. Active Simple Notification Service.

   ii. Seleccione un ARN en el menú desplegable.

j. **Monitoreo de CloudWatch**: Opcionalmente, puede habilitar el monitoreo de CloudWatch.

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

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

a. **Retroceder recursos**: Esta característica no es compatible actualmente.

8. Resumen

   a. **Costo estimado**: Proporciona una estimación de los cargos en los que podría incurrir si implementa los recursos mostrados.

9. Haga clic en **Crear** para implementar el nuevo host de base de datos.

   También puede guardar la configuración.

## Paso 2: Habilite 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, complete los siguientes pasos.

**Pasos**

1. Utilice la identidad de equipo para NTLM consultando "Seguridad de red: Permite que el sistema local utilice la identidad de equipo para NTLM" la documentación de Microsoft.
2. Consulte la documentación de Microsoft para comprobar la configuración dinámica del puerto "Se ha producido un error relacionado con la red o específico de la instancia al establecer una conexión con SQL Server" .
3. Permita la IP o subred de cliente requerida en el grupo de seguridad.

**El futuro**

Ahora puedes"crear una base de datos en Workload Factory for Databases" .

# Cree un servidor PostgreSQL en NetApp Workload Factory

Para crear un nuevo servidor PostgreSQL o un host de base de datos en NetApp Workload Factory for Databases se requiere una implementación del sistema de archivos FSx para ONTAP y recursos para Active Directory.

## Acerca de esta tarea

Antes de crear un servidor PostgreSQL desde Workload Factory, obtenga información sobre los tipos de implementación de almacenamiento disponibles para la configuración del host de la base de datos, los modos de operación de Workload Factory y los requisitos para completar esta operación.

#### FSX para puestas en marcha del sistema de archivos ONTAP

Para crear un nuevo servidor PostgreSQL, se requiere un sistema de archivos FSx para ONTAP como back-end de almacenamiento. Puede utilizar un sistema de archivos FSX for ONTAP existente o crear un nuevo sistema de archivos. Si selecciona un sistema de archivos FSx para ONTAP existente como back-end de almacenamiento de servidor de bases de datos, creamos una nueva máquina virtual de almacenamiento para las cargas de trabajo de PostgreSQL.

+ FSx para sistemas de archivos ONTAP tiene dos modelos de implementación de servidor PostgreSQL: *Alta disponibilidad (HA)* o *instancia única*. Se crean diferentes recursos para el sistema de archivos FSx para ONTAP según el modelo de implementación de FSx para ONTAP que seleccione.

- **Despliegue de alta disponibilidad**: Se implementa un sistema de archivos FSX para NetApp ONTAP de varias zonas de disponibilidad cuando se selecciona un nuevo sistema de archivos FSX para ONTAP para la implementación de alta disponibilidad. Se crean volúmenes y LUN independientes para archivos de datos, registros y tempdb para una implementación de HA. Se crean un volumen y LUN adicionales para el disco de quórum o de testigo para el clúster de Windows. La implementación de HA configura la replicación de streaming entre los servidores PostgreSQL primarios y secundarios.
- **Implementación de instancia única**: Se crea un sistema de archivos FSX de zona de disponibilidad única para ONTAP cuando se crea un nuevo servidor PostgreSQL. Además, se crean volúmenes y LUN independientes para archivos de datos, registros y tempdb.

## Antes de empezar

Debes tener "otorgar permisos de creación de host de base de datos" en su cuenta de AWS para crear un nuevo host de base de datos en Workload Factory.

## Crear un servidor PostgreSQL

Puede utilizar los modos de implementación *Quick create* o *Advanced create* para completar esta tarea en la fábrica de cargas de trabajo con permisos de modo *automate*. También puede usar las siguientes herramientas disponibles en CodeBox: API REST, CLI de AWS, AWS CloudFormation y Terraform. "Aprende a usar CodeBox para la automatización".

> Al usar Terraform de CodeBox, el código que copie o descargue oculta `fsxadmin` y `vsadmin` las contraseñas. Deberá volver a introducir las contraseñas cuando ejecute el código. Deberá 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 de 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. Inicie sesión con uno de los "experiencias de consola"botones .
2. En el mosaico Bases de datos, seleccione **Implementar host** y luego seleccione **Servidor PostgreSQL** en el menú.
3. Seleccione **Quick create**.
4. En **Zona de aterrizaje**, proporcione lo siguiente:
   a. **Credenciales de AWS**: Seleccione las credenciales de AWS con permisos automatizados para implementar el nuevo host de base de datos.

      Las credenciales de AWS con permisos de *lectura/escritura* permiten que Workload Factory implemente y administre el nuevo host de base de datos desde su cuenta de AWS dentro de Workload Factory.

      Las credenciales de AWS con permisos de *solo lectura* permiten que la fábrica de carga de trabajo genere una plantilla de CloudFormation para que usted la use en la consola de AWS CloudFormation.

      Si no tiene las credenciales de AWS asociadas en la fábrica de cargas de trabajo y desea crear el nuevo servidor en la fábrica de cargas de trabajo, siga la opción **1** para ir a la página Credenciales. Agregue manualmente las credenciales y los permisos necesarios para el modo *lectura/escritura* para las cargas de trabajo de la base de datos.

      Si desea completar el formulario Crear nuevo servidor en la fábrica de cargas de trabajo para poder descargar una plantilla de archivo YAML completa para su implementación en AWS CloudFormation, siga **Opción 2** para asegurarse de que tiene los permisos necesarios para crear el nuevo servidor en AWS CloudFormation. Agregue manualmente las credenciales y los permisos necesarios para el modo *solo lectura* para las cargas de trabajo de la base de datos.

      Opcionalmente, puede descargar una plantilla de archivo YAML parcialmente completada desde CodeBox para crear la pila fuera de la fábrica de cargas de trabajo sin credenciales ni permisos. Seleccione **CloudFormation** en el menú desplegable del CodeBox para descargar el archivo YAML.

   b. **Región y VPC**: Seleccione una región y una red de VPC.

      Asegúrese de que los grupos de seguridad para un extremo de interfaz existente permiten el acceso al protocolo HTTPS (443) a las subredes seleccionadas.

      Extremos de la interfaz de servicio de AWS (SQS, FSx, EC2, CloudWatch, CloudFormation, SSM) y el punto final de la puerta de enlace S3 se crean durante el despliegue si no se encuentra.

      Los atributos DNS de VPC `EnableDnsSupport` y `EnableDnsHostnames` se modifican para activar la resolución de direcciones de punto final si aún no están establecidos en `true`.

   c. **Zonas de disponibilidad**: Seleccione zonas de disponibilidad y subredes.

Las implementaciones de HA solo se admiten en configuraciones FSx para ONTAP de varias zonas de disponibilidad (MAZ).

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

i. En el campo **Configuración de clúster - Nodo 1**, seleccione la zona de disponibilidad principal para la configuración de MAZ FSX para ONTAP en el menú desplegable **Zona de disponibilidad** y una subred de la zona de disponibilidad principal desde el menú desplegable **Subred**.

ii. En el campo **Configuración de clúster - Nodo 2**, seleccione la zona de disponibilidad secundaria para la configuración de MAZ FSX para ONTAP en el menú desplegable **Zona de disponibilidad** y una subred de la zona de disponibilidad secundaria desde el menú desplegable **Subred**.

5. En **Configuración de la aplicación**, introduzca un nombre de usuario y una contraseña para **Credenciales de la base de datos**.
6. En **Conectividad**, selecciona un par de claves para conectarte de forma segura a tu instancia.
7. En **Configuración de infraestructura**, proporcione lo siguiente:
   a. **FSX para el sistema ONTAP**: Crea un nuevo sistema de archivos FSX para ONTAP o usa un sistema de archivos FSX para ONTAP existente.
      i. * Crear nuevo FSX para ONTAP*: Introduzca el nombre de usuario y la contraseña.

      Un nuevo sistema de archivos FSX para ONTAP puede agregar 30 minutos o más de tiempo de instalación.

      ii. **Seleccione un FSX para ONTAP**: Seleccione FSX para el nombre de ONTAP en el menú desplegable, e introduzca un nombre de usuario y una contraseña para el sistema de archivos.

      Para los sistemas de archivos FSx para ONTAP existentes, asegúrate de lo siguiente:

      - El grupo de enrutamiento conectado a FSx para ONTAP permite que las rutas a las subredes se utilicen para la implementación.
      - El grupo de seguridad permite el tráfico de las subredes utilizadas para la puesta en marcha, específicamente los puertos TCP HTTPS (443) e iSCSI (3260).

   b. **Tamaño de la unidad de datos**: Ingrese la capacidad de la unidad de datos y seleccione la unidad de capacidad.
8. Resumen:
   a. **Vista previa predeterminada**: Revise las configuraciones predeterminadas establecidas por Quick Create.
   b. **Costo estimado**: Proporciona una estimación de los cargos en los que podría incurrir si implementa los recursos mostrados.
9. Haga clic en **Crear**.

Como alternativa, si desea cambiar cualquiera de estos valores por defecto ahora, cree el servidor de base de datos con Advanced CREATE.

También puede seleccionar **Guardar configuración** para implementar el host más tarde.

**Creación avanzada**

**Pasos**

1. Inicie sesión con uno de los "experiencias de consola"botones .
2. En el mosaico Bases de datos, seleccione **Implementar host** y luego seleccione **Servidor PostgreSQL** en el menú.
3. Selecciona **Creación avanzada**.
4. En **Modelo de implementación**, selecciona **Instancia independiente** o **Alta disponibilidad (HA)**.
5. En **Zona de aterrizaje**, proporcione lo siguiente:
   a. **Credenciales de AWS**: Seleccione las credenciales de AWS con permisos automatizados para implementar el nuevo host de base de datos.

      Las credenciales de AWS con permisos *Automate* permiten que la fábrica de cargas de trabajo implemente y administre el nuevo host de base de datos desde su cuenta de AWS dentro de la fábrica de cargas de trabajo.

      Las credenciales de AWS con permisos de *solo lectura* permiten que la fábrica de carga de trabajo genere una plantilla de CloudFormation para que usted la use en la consola de AWS CloudFormation.

      Si no tiene las credenciales de AWS asociadas en la fábrica de cargas de trabajo y desea crear el nuevo servidor en la fábrica de cargas de trabajo, siga la opción **1** para ir a la página Credenciales. Agregue manualmente las credenciales y los permisos necesarios para el modo *lectura/escritura* para las cargas de trabajo de la base de datos.

      Si desea completar el formulario Crear nuevo servidor en la fábrica de cargas de trabajo para poder descargar una plantilla de archivo YAML completa para su implementación en AWS CloudFormation, siga **Opción 2** para asegurarse de que tiene los permisos necesarios para crear el nuevo servidor en AWS CloudFormation. Agregue manualmente las credenciales y los permisos necesarios para el modo *solo lectura* para las cargas de trabajo de la base de datos.

      Opcionalmente, puede descargar una plantilla de archivo YAML parcialmente completada desde CodeBox para crear la pila fuera de la fábrica de cargas de trabajo sin credenciales ni permisos. Seleccione **CloudFormation** en el menú desplegable del CodeBox para descargar el archivo YAML.

   b. **Región y VPC**: Seleccione una región y una red de VPC.

      Asegúrese de que los grupos de seguridad para un extremo de interfaz existente permiten el acceso al protocolo HTTPS (443) a las subredes seleccionadas.

      Extremos de la interfaz del servicio de AWS (SQS, FSx, EC2, CloudWatch, formación de la nube, SSM) y el punto final de la puerta de enlace S3 se crean durante el despliegue si no se encuentra.

      Los atributos DNS de VPC `EnableDnsSupport` y `EnableDnsHostnames` se modifican para activar la resolución de la dirección de punto final si no se ha establecido ya en `true`.

   c. **Zonas de disponibilidad**: Seleccione zonas de disponibilidad y subredes.

      **Para implementaciones de instancia única**

      En el campo **Configuración del clúster - Nodo 1**, seleccione una zona de disponibilidad en el

menú desplegable **Zona de disponibilidad** y una subred en el menú desplegable **Subred**.

**Para implementaciones de alta disponibilidad**

i. En el campo **Configuración de clúster - Nodo 1**, seleccione la zona de disponibilidad principal para la configuración de MAZ FSX para ONTAP en el menú desplegable **Zona de disponibilidad** y una subred de la zona de disponibilidad principal desde el menú desplegable **Subred**.

ii. En el campo **Configuración de clúster - Nodo 2**, seleccione la zona de disponibilidad secundaria para la configuración de MAZ FSX para ONTAP en el menú desplegable **Zona de disponibilidad** y una subred de la zona de disponibilidad secundaria desde el menú desplegable **Subred**.

d. **Grupo de seguridad**: Seleccione un grupo de seguridad existente o cree un nuevo grupo de seguridad.

Dos grupos de seguridad se conectan a los nodos SQL (instancias EC2) durante el despliegue del nuevo servidor.

i. Se crea un grupo de seguridad de carga de trabajo para permitir los puertos y protocolos necesarios para PostgreSQL.

ii. Para un nuevo sistema de archivos FSx for ONTAP, se crea un nuevo grupo de seguridad y se conecta al nodo SQL. Para un sistema de archivos FSX for ONTAP existente, el grupo de seguridad asociado con él se agrega automáticamente al nodo PostgreSQL que permite la comunicación con el sistema de archivos.

6. En **Configuración de la aplicación**, proporcione lo siguiente:

a. Seleccione el **Sistema operativo** en el menú desplegable.

b. Seleccione la **versión PostgreSQL** del menú desplegable.

c. **Nombre del servidor de base de datos**: Introduzca el nombre del cluster de base de datos.

d. **Credenciales de la base de datos**: Introduzca un nombre de usuario y una contraseña para una nueva cuenta de servicio o utilice las credenciales de la cuenta de servicio existentes en Active Directory.

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

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

a. **Tipo de instancia de DB**: Seleccione el tipo de instancia de base de datos en el menú desplegable.

b. **FSX para el sistema ONTAP**: Crea un nuevo sistema de archivos FSX para ONTAP o usa un sistema de archivos FSX para ONTAP existente.

i. * Crear nuevo FSX para ONTAP*: Introduzca el nombre de usuario y la contraseña.

Un nuevo sistema de archivos FSX para ONTAP puede agregar 30 minutos o más de tiempo de instalación.

ii. **Seleccione un FSX para ONTAP**: Seleccione FSX para el nombre de ONTAP en el menú desplegable, e introduzca un nombre de usuario y una contraseña para el sistema de archivos.

Para los sistemas de archivos FSx para ONTAP existentes, asegúrate de lo siguiente:

- El grupo de enrutamiento conectado a FSx para ONTAP permite que las rutas a las subredes se utilicen para la implementación.
- El grupo de seguridad permite el tráfico de las subredes utilizadas para la puesta en marcha, específicamente los puertos TCP HTTPS (443) e iSCSI (3260).

c. **Política de instantáneas**: Habilitado por defecto. Las copias Snapshot se realizan diariamente y tienen un período de retención de 7 días.

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

d. **Tamaño de la unidad de datos**: Ingrese la capacidad de la unidad de datos y seleccione la unidad de capacidad.

e. **IOPS provisionadas**: Selecciona **Automático** o **Provisioned por el usuario**. Si selecciona **Provisioned por el usuario**, introduzca el valor de IOPS.

f. **Capacidad de rendimiento**: Seleccione la capacidad de rendimiento en el menú desplegable.

   En algunas regiones, puede seleccionar una capacidad de rendimiento de 4 Gbps. Para aprovisionar 4 Gbps de capacidad de rendimiento, su sistema de archivos FSx para ONTAP debe configurarse 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. Debe introducir la clave de cifrado ARN desde otra cuenta.

   Las claves de cifrado personalizadas de FSx para ONTAP no se incluyen en la aplicación del servicio. Seleccione una clave de cifrado FSX adecuada. Las claves de cifrado no 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**: Opcionalmente, puedes añadir hasta 40 etiquetas.

i. **Servicio de Notificación Simple**: Opcionalmente, puede habilitar el Servicio de Notificación Simple (SNS) para esta configuración seleccionando un tema de SNS para Microsoft SQL Server en el menú desplegable.

   i. Active Simple Notification Service.

   ii. Seleccione un ARN en el menú desplegable.

j. **Monitoreo de CloudWatch**: Opcionalmente, puede habilitar el monitoreo de CloudWatch.

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

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

a. **Retroceder recursos**: Esta característica no es compatible actualmente.

9. Resumen

a. **Costo estimado**: Proporciona una estimación de los cargos en los que podría incurrir si implementa los recursos mostrados.

10. Haga clic en **Crear** para implementar el nuevo host de base de datos.

    También puede guardar la configuración.

**El futuro**

Puede configurar manualmente usuarios, acceso remoto y bases de datos en el servidor PostgreSQL desplegado.

**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.