



Crie recursos de banco de dados

Workload Factory for NetApp Console

NetApp
October 07, 2026

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

Índice

- Crie recursos de banco de dados 1
 - Crie um Microsoft SQL Server no NetApp Workload Factory para bancos de dados 1
 - Sobre esta tarefa 1
 - Antes de começar 2
 - Passo 1: criar um servidor de banco de dados 2
 - Etapa 2: habilitar a conexão remota no Microsoft SQL Server 10
 - Crie um servidor PostgreSQL no NetApp Workload Factory para Bancos de Dados 10
 - Sobre esta tarefa 10
 - Antes de começar 11
 - Criar um servidor PostgreSQL 11
 - Criar um banco de dados Microsoft SQL no NetApp Workload Factory for Databases 16
 - Criar um banco de dados 17
 - Criar um clone de sandbox no NetApp Workload Factory for Databases 19

Crie recursos de banco de dados

Crie um Microsoft SQL Server no NetApp Workload Factory para bancos de dados

A criação de um novo Microsoft SQL Server, ou host de banco de dados, no Workload Factory for Databases requer uma implantação de sistema de arquivos do FSx for ONTAP e recursos para o Active Directory.

Sobre esta tarefa

Antes de criar um Microsoft SQL Server no Workload Factory, saiba mais sobre os tipos disponíveis de implantação de storage para a configuração do host do banco de dados, a configuração do Microsoft Multi-path I/O, a implantação do Active Directory, os detalhes de rede e os requisitos para concluir esta operação.

Após a implantação, você precisará [habilitar conexão remota no Microsoft SQL Server](#).

Implantações de sistemas de arquivos do FSx for ONTAP

A criação de um novo Microsoft SQL Server requer um sistema de arquivos FSx for ONTAP como backend de armazenamento. Você pode usar um sistema de arquivos FSx for ONTAP existente ou criar um novo sistema de arquivos. Se você selecionar um sistema de arquivos FSx for ONTAP existente como backend de armazenamento do seu servidor de banco de dados, criaremos uma nova máquina virtual de storage para as cargas de trabalho do Microsoft SQL Server.

Os sistemas de arquivos FSx for ONTAP têm dois modelos de implantação do Microsoft SQL Server: *instância de cluster de failover (FCI)* ou *autônomo*. Recursos diferentes são criados para o sistema de arquivos FSx for ONTAP, dependendo do modelo de implantação do FSx for ONTAP que você selecionar.

- **Implantação de Failover Cluster Instance (FCI) do Microsoft SQL:** um sistema de arquivos FSx for NetApp ONTAP de várias zonas de disponibilidade é implantado quando um novo sistema de arquivos FSx for ONTAP é selecionado para a implantação de FCI. Volumes e LUNs separados são criados para arquivos de dados, de log e do tempdb em uma implantação de FCI. Um volume e uma LUN adicionais são criados para o disco de quorum ou de testemunha do cluster do Windows.
- **Implantação independente do Microsoft SQL:** um sistema de arquivos FSx for ONTAP de zona de disponibilidade única é criado quando um novo Microsoft SQL Server é criado. Além disso, volumes e LUNs separados são criados para arquivos de dados, log e tempdb.

Configuração de Microsoft Multi-path I/O

Ambos os modelos de implantação do Microsoft SQL Server exigem a criação de LUNs usando o protocolo de storage iSCSI. O Workload Factory configura o Microsoft Multi-path I/O (MPIO) como parte da configuração de LUNs para o SQL Server no FSx for ONTAP. O MPIO é configurado com base nas práticas recomendadas da AWS e da NetApp.

Para obter mais informações, consulte ["Implantações de alta disponibilidade do SQL Server usando o Amazon FSx for NetApp ONTAP"](#).

Active Directory

O seguinte ocorre no Active Directory (AD) durante a implantação:

- Uma nova conta de serviço do Microsoft SQL é criada no domínio caso você não forneça uma conta de serviço do SQL existente.

- O cluster do Windows, os nomes dos hosts dos nós e o nome do FCI do Microsoft SQL são adicionados como computadores gerenciados à conta de serviço do Microsoft SQL.
- A entrada do cluster do Windows recebe permissões para adicionar computadores ao domínio.

Grupos de segurança do Active Directory gerenciados pelo usuário

Se você selecionar "Active Directory gerenciado pelo usuário" durante a implantação do Microsoft SQL Server no Workload Factory, deverá fornecer um grupo de segurança que permita o tráfego entre as instâncias EC2 e o serviço de diretório para a implantação. O Workload Factory não anexa automaticamente o grupo de segurança para o Active Directory gerenciado pelo usuário, como faz para o AWS Managed Microsoft AD.

Reverter recurso

Se você decidir reverter seus recursos do Sistema de Nomes de Domínio (DNS), os registros de recursos no AD e no DNS não serão removidos automaticamente. Você pode remover os registros do servidor DNS e do AD da seguinte forma.

- Para o AD gerenciado pelo usuário, primeiro ["remover o computador do AD"](#). Em seguida, conecte-se ao servidor DNS a partir do gerenciador de DNS e ["Excluir os registros de recurso DNS"](#).
- Para o AWS Managed Microsoft AD, ["instale as ferramentas de administração do AD"](#). Em seguida, ["remover o computador do AD"](#). Por fim, conecte-se ao servidor DNS no DNS manager e ["Excluir os registros de recurso DNS"](#).

Antes de começar

Certifique-se de que você tenha os seguintes pré-requisitos antes de criar um novo host de banco de dados.

Credenciais e permissões

Você precisa ["conceder permissões de criação de host de banco de dados"](#) na sua conta da AWS para criar um novo host de banco de dados no Workload Factory.

Active Directory

Ao conectar-se ao Active Directory, você precisa ter acesso administrativo com permissões para realizar as seguintes ações:

- Ingressar no domínio
- Criar objetos de computador
- Criar objetos na Unidade Organizacional (UO) padrão
- Leia todas as propriedades
- Torne o usuário do domínio um administrador local nos nós do AD
- Crie um usuário de serviço do Microsoft SQL Server no AD, caso ele ainda não exista

Passo 1: criar um servidor de banco de dados

Você pode usar os modos de implantação *Quick create* ou *Advanced create* para concluir esta tarefa no Workload Factory com permissões do modo *Automate*. Você também pode usar as seguintes ferramentas disponíveis no Codebox: API REST, AWS CLI, AWS CloudFormation e Terraform. ["Aprenda a usar o Codebox para automação"](#).



Ao usar o Terraform do Codebox, o código que você copia ou baixa oculta `fsxadmin` e `vsadmin` senhas. Você precisará inserir as senhas novamente ao executar o código. Além das permissões do modo *Automate*, você precisará incluir as seguintes permissões para a conta de

usuário: iam:TagRole e iam:TagInstanceProfile. ["Aprenda a usar o Terraform da Codebox"](#).

Durante a implantação, o Workload Factory habilita o CredSSP para delegação de credenciais a scripts para provisionar SQL. Quando a delegação do CredSSP é bloqueada para todos os computadores do domínio por meio da política de grupo, a implantação falha. Após a implantação, o Workload Factory desabilita o CredSSP.

Criação rápida



Na opção *Criação rápida*, o FCI é o modelo de implantação padrão, o Windows 2016 é a versão padrão do Windows, e o SQL 2019 Standard Edition é a versão padrão do SQL.

Passos

1. Faça login no ["NetApp Console"](#).
2. Selecione o menu , **Cargas de trabalho > Bancos de dados**.
3. Na visão geral dos bancos de dados, selecione **Deploy host** e, em seguida, selecione **Microsoft SQL Server** no menu.
4. Selecione **Criação rápida**.
5. Em **Configurações da AWS**, forneça as seguintes informações:
 - a. **Credenciais da AWS**: selecione as credenciais da AWS com permissões de automação para implantar o novo host do banco de dados.

As credenciais da AWS com permissões de *criação de host de banco de dados* permitem que o Workload Factory implante e gerencie o novo host de banco de dados a partir da sua conta da AWS na workload factory.

As credenciais da AWS com permissões de *visualização, planejamento e análise* permitem que o Workload Factory gere um modelo do CloudFormation para você usar no console do AWS CloudFormation.

Se você não tiver credenciais da AWS associadas ao Workload Factory e quiser criar o novo servidor no Workload Factory, siga a **Opção 1** para acessar a página Credentials. Adicione manualmente as credenciais necessárias e as permissões de *criação de host de banco de dados* para workloads de banco de dados.

Se você deseja preencher o formulário de criação de novo servidor no Workload Factory para poder baixar um modelo de arquivo YAML completo para implantação no AWS CloudFormation, siga a **Opção 2** para garantir que você tenha as permissões necessárias para criar o novo servidor no AWS CloudFormation. Adicione manualmente as credenciais necessárias e as permissões de *visualização, planejamento e análise* para cargas de trabalho de banco de dados.

Opcionalmente, você pode baixar um modelo de arquivo YAML parcialmente preenchido do Codebox para criar a pilha fora do Workload Factory sem credenciais ou permissões. Selecione **CloudFormation** no menu suspenso do Codebox para baixar o arquivo YAML.

- b. **Região e VPC**: selecione uma região e uma rede VPC.

Certifique-se de que as sub-redes de implantação estejam associadas aos endpoints de interface existentes e que os grupos de segurança permitam acesso ao protocolo HTTPS (443) para as sub-redes selecionadas.

Os endpoints de interface de serviço da AWS (SQS, FSx, EC2, CloudWatch, CloudFormation, SSM) e o endpoint de gateway do S3 são criados durante a implantação, caso não sejam encontrados.

Os atributos DNS da VPC `EnableDnsSupport` e `EnableDnsHostnames` são modificados para habilitar a resolução de endereços de endpoint, caso ainda não estejam definidos como `true`.

Ao usar um DNS entre VPCs, o grupo de segurança dos endpoints na outra VPC em que o DNS reside deve permitir a porta 443 para as sub-redes de implantação. Caso contrário, você deve fornecer um resolvidor DNS da VPC local ao ingressar no Active Directory entre VPCs. Em um ambiente com vários controladores de domínio replicados, se alguns controladores de domínio não estiverem acessíveis pela sub-rede, você pode **Redirecionar para CloudFormation** e inserir `Preferred domain controller` para se conectar ao Active Directory.

- c. **Zonas de disponibilidade:** selecione as zonas de disponibilidade e sub-redes de acordo com o modelo de implantação da Instância de Cluster de Failover (FCI).



As implantações de FCI são suportadas apenas em configurações do FSx for ONTAP de Multiple Availability Zone (MAZ).

- i. No campo **Configuração do cluster - Nó 1**, selecione a zona de disponibilidade principal para a configuração do MAZ FSx for ONTAP no menu suspenso **Zona de disponibilidade** e uma sub-rede da zona de disponibilidade principal no menu suspenso **Sub-rede**.
 - ii. No campo **Configuração do cluster - Nó 2**, selecione a zona de disponibilidade secundária para a configuração do MAZ FSx for ONTAP no menu suspenso **Zona de disponibilidade** e uma sub-rede da zona de disponibilidade secundária no menu suspenso **Sub-rede**.
6. Em **Configurações do aplicativo**, insira um nome de usuário e uma senha para **Credenciais do banco de dados**.

Para contas GovCloud, insira o valor do ARN do parâmetro AWS SSM no seguinte formato:
`{fsx:{"username":"fsxadmin","password":"pass"}}`.

O valor é fornecido no Parameter Store, em Detalhes do parâmetro, no Console de Gerenciamento da AWS. O tipo de parâmetro do AWS SSM deve ser "Secure String" com o nome no formato `/netapp/wlmdb/<anyname>`. Saiba mais sobre como recuperar parâmetros do SSM em ["Documentação da AWS GovCloud"](#).

7. Em **Conectividade**, forneça as seguintes informações:

a. **Par de chaves:** selecione um par de chaves.

b. **Active Directory:**

- i. No campo **Nome de domínio**, selecione ou insira um nome para o domínio.
 - A. Para diretórios Active Directory gerenciados pela AWS, os nomes de domínio aparecem no menu suspenso.
 - B. Para um Active Directory gerenciado pelo usuário, insira um nome no campo **Pesquisar e adicionar** e clique em **Adicionar**.
- ii. No campo **Endereço DNS**, insira o endereço IP de DNS do domínio. Você pode adicionar até 3 endereços IP.

Para diretórios do Active Directory gerenciados pela AWS, os endereços IP de DNS aparecem no menu suspenso.

- iii. No campo **Nome de usuário**, insira o nome de usuário do domínio do Active Directory.
- iv. No campo **Senha**, insira uma senha para o domínio do Active Directory.

Para contas GovCloud, insira o valor ARN do parâmetro AWS SSM para credenciais do Active Directory no seguinte formato:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. O tipo de parâmetro do AWS SSM deve ser "Secure String" com o nome no formato `/netapp/wlmdb/<anyname>`. Saiba mais sobre como recuperar parâmetros do SSM em ["Documentação da AWS GovCloud"](#).

8. Em **Configurações de infraestrutura**, forneça as seguintes informações:

- a. **sistema FSx for ONTAP**: crie um novo sistema de arquivos FSx for ONTAP ou use um sistema de arquivos FSx for ONTAP existente.

- i. **Criar novo FSx for ONTAP**: insira o nome de usuário e a senha.

Para contas GovCloud, insira o valor ARN do parâmetro AWS SSM para as credenciais do FSx for ONTAP no seguinte formato:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. O tipo de parâmetro do AWS SSM deve ser "Secure String" com o nome no formato `/netapp/wlmdb/<anyname>`. Saiba mais sobre como recuperar parâmetros do SSM em ["Documentação da AWS GovCloud"](#).

Um novo sistema de arquivos do FSx for ONTAP pode adicionar 30 minutos ou mais ao tempo de instalação.

- i. **Selecione um FSx for ONTAP existente**: Selecione o nome do FSx for ONTAP e insira um nome de usuário e senha para o sistema de arquivos.

Para os sistemas de arquivos FSx for ONTAP existentes, certifique-se do seguinte:

- O grupo de roteamento associado ao FSx for ONTAP permite que as rotas para as sub-redes sejam usadas para implantação.
 - O grupo de segurança permite tráfego das sub-redes usadas para implantação, especificamente as portas TCP HTTPS (443) e iSCSI (3260).

- b. **Tamanho da unidade de dados**: insira a capacidade da unidade de dados e selecione a unidade de capacidade.

9. Resumo:

- a. **Visualização padrão**: revise as configurações padrão definidas pelo Quick create.
 - b. **Custo estimado**: fornece uma estimativa das cobranças que você pode incorrer se implantar os recursos mostrados.

10. Clique em **Create**.

Como alternativa, se você quiser alterar alguma dessas configurações padrão agora, crie o servidor de banco de dados com Advanced create.

Você também pode selecionar **Salvar configuração** para implantar o host posteriormente.

Criação avançada

Passos

1. Faça login no ["NetApp Console"](#).
- 2.

Selecione o menu , **Cargas de trabalho > Bancos de dados**.

3. Na visão geral dos bancos de dados, selecione **Deploy host** e, em seguida, selecione **Microsoft SQL Server** no menu.
4. Selecione **Advanced create**.
5. Para **Modelo de implantação**, selecione **Instância de cluster de failover** ou **Instância única**.
6. Em **Configurações da AWS**, forneça as seguintes informações:

- a. **Credenciais da AWS:** selecione as credenciais da AWS com permissões de automação para implantar o novo host do banco de dados.

As credenciais da AWS com permissões de *criação de host de banco de dados* permitem que o Workload Factory implante e gerencie o novo host de banco de dados a partir da sua conta da AWS na workload factory.

As credenciais da AWS com permissões de *visualização, planejamento e análise* permitem que o Workload Factory gere um modelo do CloudFormation para você usar no console do AWS CloudFormation.

Se você não tiver credenciais da AWS associadas ao Workload Factory e quiser criar o novo servidor no Workload Factory, siga a **Opção 1** para acessar a página Credentials. Adicione manualmente as credenciais necessárias e as permissões de *criação de host de banco de dados* para workloads de banco de dados.

Se você deseja preencher o formulário de criação de novo servidor no Workload Factory para poder baixar um modelo de arquivo YAML completo para implantação no AWS CloudFormation, siga a **Opção 2** para garantir que você tenha as permissões necessárias para criar o novo servidor no AWS CloudFormation. Adicione manualmente as credenciais necessárias e as permissões de *visualização, planejamento e análise* para cargas de trabalho de banco de dados.

Opcionalmente, você pode baixar um modelo de arquivo YAML parcialmente preenchido do Codebox para criar a pilha fora do Workload Factory sem credenciais ou permissões. Selecione **CloudFormation** no menu suspenso do Codebox para baixar o arquivo YAML.

- b. **Região e VPC:** selecione uma região e uma rede VPC.

Garanta que os grupos de segurança de um endpoint de interface existente permitam acesso ao protocolo HTTPS (443) para as sub-redes selecionadas.

Os endpoints de interface de serviço da AWS (SQS, FSx, EC2, CloudWatch, Cloud Formation, SSM) e o endpoint de gateway do S3 são criados durante a implantação, caso não sejam encontrados.

Os atributos DNS da VPC `EnableDnsSupport` e `EnableDnsHostnames` são modificados para habilitar a resolução de endereço do endpoint, caso ainda não estejam configurados como `true`.

- c. **Zonas de disponibilidade:** selecione as zonas de disponibilidade e as sub-redes de acordo com o modelo de implantação escolhido. Para alta disponibilidade, as sub-redes não devem compartilhar a mesma tabela de roteamento.



As implantações de FCI são suportadas apenas em configurações do FSx for ONTAP de Multiple Availability Zone (MAZ).

- Para implantações de instância única:
 - No campo **Configuração do cluster - Nó 1**, selecione uma zona de disponibilidade no menu suspenso **Zona de disponibilidade** e uma sub-rede no menu suspenso **Sub-rede**.
 - Para implantações de FCI:
 - No campo **Configuração do cluster - Nó 1**, selecione a zona de disponibilidade principal para a configuração do MAZ FSx for ONTAP no menu suspenso **Zona de disponibilidade** e uma sub-rede da zona de disponibilidade principal no menu suspenso **Sub-rede**.
 - No campo **Configuração do cluster - Nó 2**, selecione a zona de disponibilidade secundária para a configuração do MAZ FSx for ONTAP no menu suspenso **Zona de disponibilidade** e uma sub-rede da zona de disponibilidade secundária no menu suspenso **Sub-rede**.
- d. **Grupo de segurança:** Um grupo de segurança de carga de trabalho é criado para permitir as portas e os protocolos necessários para a comunicação do cluster Microsoft SQL e Windows nos nós. Além disso, você pode selecionar um ou mais grupos de segurança.
7. Em **Configurações do aplicativo**, forneça as seguintes informações:
- a. Em **Tipo de instalação do SQL Server**, selecione **AMI com licença incluída** ou **Usar AMI personalizada**.
- i. Se você selecionar **AMI com licença incluída**, forneça o seguinte:
- A. **Sistema operacional:** selecione **Windows server 2016**, **Windows server 2019** ou **Windows server 2022**.
 - B. **Edição do banco de dados:** selecione **o SQL Server Standard Edition** ou **o SQL Server Enterprise Edition**.
 - C. **Versão do banco de dados:** selecione **SQL Server 2016**, **SQL Server 2019** ou **SQL Server 2022**.
 - D. **AMI do SQL Server:** Selecione uma AMI do SQL Server no menu suspenso.
- ii. Se selecionar **Usar AMI personalizada**, selecione uma AMI no menu suspenso.
- b. **Agrupamento do SQL Server:** selecione um conjunto de agrupamento para o servidor.



Caso o conjunto de ordenação selecionado não seja compatível com a instalação, recomendamos que você selecione a ordenação padrão "SQL_Latin1_General_CP1_CI_AS".

- c. **Nome do banco de dados:** insira o nome do cluster do banco de dados.
- d. **Credenciais do banco de dados:** insira um nome de usuário e uma senha para uma nova conta de serviço ou use as credenciais de uma conta de serviço existente no Active Directory.

Opcional: selecione **Usar conta de serviço gerenciada** para a conta de serviço do SQL Server. Use esta opção se o seu ambiente usar MSA (Conta de Serviço Gerenciada) ou Contas de Serviço Gerenciadas em Grupo (gMSA), em que o gerenciamento de senhas é feito pelo Active Directory.

Para contas GovCloud, insira o valor do ARN do parâmetro AWS SSM no seguinte formato:
`{ "fsx": { "username": "fsxadmin", "password": "pass" } }`.

O valor é fornecido no Parameter Store, em Detalhes do parâmetro, no Console de Gerenciamento da AWS. O tipo de parâmetro do AWS SSM deve ser "Secure String" com o nome no formato

/netapp/wlmdb/<anyname>. Saiba mais sobre como recuperar parâmetros do SSM em ["Documentação da AWS GovCloud"](#).

8. Em **Conectividade**, forneça as seguintes informações:

- a. **Par de chaves:** selecione um par de chaves para se conectar com segurança à sua instância.
- b. **Active Directory:** forneça os seguintes detalhes do Active Directory:
 - i. No campo **Nome de domínio**, selecione ou insira um nome para o domínio.
 - A. Para diretórios Active Directory gerenciados pela AWS, os nomes de domínio aparecem no menu suspenso.
 - B. Para um Active Directory gerenciado pelo usuário, insira um nome no campo **Pesquisar e adicionar** e clique em **Adicionar**.
 - ii. No campo **Endereço DNS**, insira o endereço IP de DNS do domínio. Você pode adicionar até 3 endereços IP.

Para diretórios do Active Directory gerenciados pela AWS, os endereços IP de DNS aparecem no menu suspenso.

- iii. Insira o nome de usuário e a senha do domínio do Active Directory.

Para contas GovCloud, insira o valor ARN do parâmetro AWS SSM para credenciais do Active Directory no seguinte formato:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. O tipo de parâmetro do AWS SSM deve ser "Secure String" com o nome no formato /netapp/wlmdb/<anyname>. Saiba mais sobre como recuperar parâmetros do SSM em ["Documentação da AWS GovCloud"](#).

- iv. **Controlador de domínio preferencial:** opcionalmente, insira o controlador de domínio preferencial a ser usado para ingresso no Active Directory.
- v. **Caminho da unidade organizacional preferencial:** opcionalmente, insira a unidade organizacional (UO) preferencial no Active Directory à qual você deseja ingressar.
- vi. **grupo do Active Directory de destino:** opcionalmente, insira o grupo do Active Directory ao qual deseja adicionar os computadores.

9. Em **Configurações de infraestrutura**, forneça as seguintes informações:

- a. **Tipo de instância de banco de dados:** selecione o tipo de instância de banco de dados no menu suspenso.
- b. **sistema FSx for ONTAP:** crie um novo sistema de arquivos FSx for ONTAP ou use um sistema de arquivos FSx for ONTAP existente.
 - i. **Criar novo FSx for ONTAP:** insira o nome de usuário e a senha.

Para contas GovCloud, insira o valor ARN do parâmetro AWS SSM para as credenciais do FSx for ONTAP no seguinte formato:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. O tipo de parâmetro do AWS SSM deve ser "Secure String" com o nome no formato /netapp/wlmdb/<anyname>. Saiba mais sobre como recuperar parâmetros do SSM em ["Documentação da AWS GovCloud"](#).

Um novo sistema de arquivos do FSx for ONTAP pode adicionar 30 minutos ou mais ao tempo de instalação.

- ii. **Selecione um FSx for ONTAP existente:** selecione o nome do FSx for ONTAP no menu suspenso e insira um nome de usuário e uma senha para o sistema de arquivos.

Para os sistemas de arquivos FSx for ONTAP existentes, certifique-se do seguinte:

- O grupo de roteamento associado ao FSx for ONTAP permite que as rotas para as sub-redes sejam usadas para implantação.
 - O grupo de segurança permite tráfego das sub-redes usadas para implantação, especificamente as portas TCP HTTPS (443) e iSCSI (3260).
- c. **política do Snapshot:** ativada por padrão. Os Snapshots são feitos diariamente e têm um período de retenção de 7 dias.

Os snapshots são atribuídos a volumes criados para cargas de trabalho SQL.

- d. **Tamanho da unidade de dados:** insira a capacidade da unidade de dados e selecione a unidade de capacidade.
- e. **IOPS provisionadas:** selecione **Automático** ou **Provisionado pelo usuário**. Se selecionar **Provisionado pelo usuário**, insira o valor de IOPS.
- f. **Capacidade de throughput:** selecione a capacidade de throughput no menu suspenso.

Em determinadas regiões, você pode selecionar uma capacidade de throughput de 4 GBps. Para provisionar 4 GBps de capacidade de throughput, seu sistema de arquivos FSx for ONTAP deve ser configurado com um mínimo de 5.120 GiB de capacidade de storage e 160.000 IOPS de SSD.

- g. **Criptografia:** selecione uma chave da sua conta ou uma chave de outra conta. Você deve inserir o ARN da chave de criptografia de outra conta.

As chaves de criptografia personalizadas do FSx for ONTAP não estão listadas com base na aplicabilidade do serviço. Selecione uma chave de criptografia do FSx apropriada. Chaves de criptografia que não sejam do FSx causarão falha na criação do servidor.

As chaves gerenciadas pela AWS são filtradas com base na aplicabilidade do serviço.

- h. **Etiquetas:** opcionalmente, você pode adicionar até 40 etiquetas.
- i. **Simple Notification Service:** opcionalmente, você pode habilitar o Simple Notification Service (SNS) para esta configuração selecionando um tópico do SNS para Microsoft SQL Server no menu suspenso.
- i. Ative o Simple Notification Service.
 - ii. Selecione um ARN no menu suspenso.
- j. **Monitoramento do CloudWatch:** opcionalmente, você pode ativar o monitoramento do CloudWatch.

Recomendamos habilitar o CloudWatch para depuração em caso de falha. Os eventos exibidos no console do AWS CloudFormation são de alto nível e não especificam a causa raiz. Todos os logs detalhados são salvos na pasta `C:\cfn\logs` nas instâncias EC2.

Em CloudWatch, um grupo de logs é criado com o nome da pilha. Um fluxo de logs para cada nó de validação e nó SQL aparece no grupo de logs. CloudWatch mostra o progresso do script e fornece informações para ajudar você a entender se e quando a implantação falha.

- a. **Reverter recurso:** este recurso não é suportado atualmente.

10. Resumo

a. **Custo estimado:** fornece uma estimativa das cobranças que você pode incorrer se implantar os recursos mostrados.

11. Clique em **Criar** para implantar o novo host de banco de dados.

Alternativamente, você pode salvar a configuração.

Etapa 2: habilitar a conexão remota no Microsoft SQL Server

Após a implantação do servidor, o Workload Factory não habilita a conexão remota no Microsoft SQL Server. Para habilitar a conexão remota, siga as etapas a seguir.

Passos

1. Use a identidade do computador para NTLM consultando ["Segurança de rede: permitir que o sistema local use a identidade do computador para NTLM"](#) na documentação da Microsoft.
2. Verifique a configuração dinâmica de portas consultando ["Ocorreu um erro relacionado à rede ou específico da instância ao estabelecer uma conexão com o SQL Server"](#) na documentação da Microsoft.
3. Permita o endereço IP do cliente ou a sub-rede necessários no grupo de segurança.

O que vem a seguir

Agora você pode ["criar um banco de dados no Workload Factory for Databases"](#).

Crie um servidor PostgreSQL no NetApp Workload Factory para Bancos de Dados

A criação de um novo servidor PostgreSQL, ou host de banco de dados, no NetApp Workload Factory for Databases requer uma implantação de sistema de arquivos FSx for ONTAP e recursos para o Active Directory.

Sobre esta tarefa

Antes de criar um servidor PostgreSQL a partir do Workload Factory, saiba mais sobre os tipos de implantação de storage disponíveis para a configuração do host do banco de dados, os modos de operação do Workload Factory e os requisitos para concluir essa operação.

Implantações de sistemas de arquivos do FSx for ONTAP

A criação de um novo servidor PostgreSQL requer um sistema de arquivos FSx for ONTAP como backend de armazenamento. Você pode usar um sistema de arquivos FSx for ONTAP existente ou criar um novo sistema de arquivos. Se você selecionar um sistema de arquivos FSx for ONTAP existente como backend de armazenamento do seu servidor de banco de dados, criaremos uma nova VM de storage para as workloads do PostgreSQL.

+ Os sistemas de arquivos FSx for ONTAP têm dois modelos de implantação de servidor PostgreSQL: *Alta Disponibilidade (HA)* ou *instância única*. Recursos diferentes são criados para o sistema de arquivos FSx for ONTAP, dependendo do modelo de implantação do FSx for ONTAP que você selecionar.

- **Implantação de alta disponibilidade (HA):** um sistema de arquivos FSx for NetApp ONTAP de múltiplas zonas de disponibilidade é implantado quando um novo sistema de arquivos FSx for ONTAP é selecionado para a implantação de HA. Volumes e LUNs separados são criados para arquivos de dados, log e tempdb em uma implantação de HA. Um volume e uma LUN adicionais são criados para o disco de

quorum ou witness para o cluster do Windows. A implantação de HA configura a replicação de streaming entre os servidores PostgreSQL primário e secundário.

- **Implantação de instância única:** um sistema de arquivos FSx for ONTAP de zona de disponibilidade única é criado quando um novo servidor PostgreSQL é criado. Além disso, volumes e LUNs separados são criados para arquivos de dados, log e tempdb.

Antes de começar

Você precisa ter "[conceder permissões de criação de host de banco de dados](#)" em sua conta da AWS para criar um novo host de banco de dados no workload factory.

Criar um servidor PostgreSQL

Você pode usar os modos de implantação *Quick create* ou *Advanced create* para concluir esta tarefa no workload factory com permissões do modo *Automate*. Você também pode usar as seguintes ferramentas disponíveis no Codebox: API REST, AWS CLI, AWS CloudFormation e Terraform. "[Aprenda a usar o Codebox para automação](#)".



Ao usar o Terraform do Codebox, o código que você copia ou baixa oculta `fsxadmin` e `vsadmin` senhas. Você precisará inserir as senhas novamente ao executar o código. Além das permissões do modo *Automate*, você precisará incluir as seguintes permissões para a conta de usuário: `iam:TagRole` e `iam:TagInstanceProfile`. "[Aprenda a usar o Terraform da Codebox](#)".

Criação rápida



Em *Quick create*, o HA é o modelo de implantação padrão, o Windows 2016 é a versão padrão do Windows e o SQL 2019 Standard Edition é a versão padrão do SQL.

Passos

1. Faça login no "[NetApp Console](#)".
2. Selecione o menu , **Cargas de trabalho > Bancos de dados**.
3. Na Databases Overview, selecione **Deploy host** e, em seguida, selecione **PostgreSQL Server** no menu.
4. Selecione **Criação rápida**.
5. Em **Zona de pouso**, forneça o seguinte:
 - a. **Credenciais da AWS:** selecione as credenciais da AWS com permissões de automação para implantar o novo host do banco de dados.

As credenciais da AWS com permissões de *criação de host de banco de dados* permitem que o Workload Factory implante e gerencie o novo host de banco de dados a partir da sua conta da AWS na workload factory.

As credenciais da AWS com permissões de *visualização, planejamento e análise* permitem que o Workload Factory gere um modelo do CloudFormation para você usar no console do AWS CloudFormation.

Se você não tiver credenciais da AWS associadas ao Workload Factory e quiser criar o novo servidor no Workload Factory, siga a **Opção 1** para acessar a página Credentials. Adicione

manualmente as credenciais necessárias e as permissões de *criação de host de banco de dados* para workloads de banco de dados.

Se você deseja preencher o formulário de criação de novo servidor no Workload Factory para poder baixar um modelo de arquivo YAML completo para implantação no AWS CloudFormation, siga a **Opção 2** para garantir que você tenha as permissões necessárias para criar o novo servidor no AWS CloudFormation. Adicione manualmente as credenciais necessárias e as permissões de *visualização, planejamento e análise* para cargas de trabalho de banco de dados.

Opcionalmente, você pode baixar um modelo de arquivo YAML parcialmente preenchido do Codebox para criar a pilha fora do Workload Factory sem credenciais ou permissões. Selecione **CloudFormation** no menu suspenso do Codebox para baixar o arquivo YAML.

b. **Região e VPC:** selecione uma região e uma rede VPC.

Garanta que os grupos de segurança de um endpoint de interface existente permitam acesso ao protocolo HTTPS (443) para as sub-redes selecionadas.

Os endpoints de interface de serviço da AWS (SQS, FSx, EC2, CloudWatch, CloudFormation, SSM) e o endpoint de gateway do S3 são criados durante a implantação, caso não sejam encontrados.

Os atributos DNS da VPC `EnableDnsSupport` e `EnableDnsHostnames` são modificados para habilitar a resolução de endereços de endpoint, caso ainda não estejam definidos como `true`.

c. **Zonas de disponibilidade:** selecione as zonas de disponibilidade e as sub-redes.



As implantações de HA são compatíveis apenas com configurações do FSx for ONTAP de Multiple Availability Zone (MAZ).

Para garantir alta disponibilidade, as sub-redes não devem compartilhar a mesma tabela de roteamento.

- i. No campo **Configuração do cluster - Nó 1**, selecione a zona de disponibilidade principal para a configuração do MAZ FSx for ONTAP no menu suspenso **Zona de disponibilidade** e uma sub-rede da zona de disponibilidade principal no menu suspenso **Sub-rede**.
 - ii. No campo **Configuração do cluster - Nó 2**, selecione a zona de disponibilidade secundária para a configuração do MAZ FSx for ONTAP no menu suspenso **Zona de disponibilidade** e uma sub-rede da zona de disponibilidade secundária no menu suspenso **Sub-rede**.
6. Em **Configurações do aplicativo**, insira um nome de usuário e uma senha para **Credenciais do banco de dados**.
7. Em **Conectividade**, selecione um par de chaves para se conectar com segurança à sua instância.
8. Em **Configurações de infraestrutura**, forneça as seguintes informações:
- a. **sistema FSx for ONTAP:** crie um novo sistema de arquivos FSx for ONTAP ou use um sistema de arquivos FSx for ONTAP existente.
 - i. **Criar novo FSx for ONTAP:** insira o nome de usuário e a senha.

Para contas GovCloud, insira o valor ARN do parâmetro AWS SSM para as credenciais do FSx for ONTAP no seguinte formato:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. O tipo de parâmetro do AWS SSM deve ser "Secure String" com o nome no formato `/netapp/wlmdb/<anyname>`. Saiba

mais sobre como recuperar parâmetros do SSM em "[Documentação da AWS GovCloud](#)".

Um novo sistema de arquivos do FSx for ONTAP pode adicionar 30 minutos ou mais ao tempo de instalação.

- i. **Selecione um FSx for ONTAP existente:** selecione o nome do FSx for ONTAP no menu suspenso e insira um nome de usuário e uma senha para o sistema de arquivos.

Para os sistemas de arquivos FSx for ONTAP existentes, certifique-se do seguinte:

- O grupo de roteamento associado ao FSx for ONTAP permite que as rotas para as sub-redes sejam usadas para implantação.
- O grupo de segurança permite tráfego das sub-redes usadas para implantação, especificamente as portas TCP HTTPS (443) e iSCSI (3260).

- b. **Tamanho da unidade de dados:** insira a capacidade da unidade de dados e selecione a unidade de capacidade.

9. Resumo:

- a. **Visualização padrão:** revise as configurações padrão definidas pelo Quick create.
- b. **Custo estimado:** fornece uma estimativa das cobranças que você pode incorrer se implantar os recursos mostrados.

10. Clique em **Create**.

Como alternativa, se você quiser alterar alguma dessas configurações padrão agora, crie o servidor de banco de dados com Advanced create.

Você também pode selecionar **Salvar configuração** para implantar o host posteriormente.

Criação avançada

Passos

1. Faça login no "[NetApp Console](#)".
2. Selecione o menu , **Cargas de trabalho > Bancos de dados**.
3. Na Databases Overview, selecione **Deploy host** e, em seguida, selecione **PostgreSQL Server** no menu.
4. Selecione **Advanced create**.
5. Em **modelo de implantação**, selecione **instância independente** ou **alta disponibilidade (HA)**.
6. Em **Zona de pouso**, forneça o seguinte:
 - a. **Credenciais da AWS:** selecione as credenciais da AWS com permissões de automação para implantar o novo host do banco de dados.

As credenciais da AWS com permissões de *criação de host de banco de dados* permitem que o Workload Factory implante e gerencie o novo host de banco de dados a partir da sua conta da AWS na workload factory.

As credenciais da AWS com permissões de *visualização, planejamento e análise* permitem que o Workload Factory gere um modelo do CloudFormation para você usar no console do AWS CloudFormation.

Se você não tiver credenciais da AWS associadas ao Workload Factory e quiser criar o novo

servidor no Workload Factory, siga a **Opção 1** para acessar a página Credentials. Adicione manualmente as credenciais necessárias e as permissões de *criação de host de banco de dados* para workloads de banco de dados.

Se você deseja preencher o formulário de criação de novo servidor no Workload Factory para poder baixar um modelo de arquivo YAML completo para implantação no AWS CloudFormation, siga a **Opção 2** para garantir que você tenha as permissões necessárias para criar o novo servidor no AWS CloudFormation. Adicione manualmente as credenciais necessárias e as permissões de *visualização, planejamento e análise* para cargas de trabalho de banco de dados.

Opcionalmente, você pode baixar um modelo de arquivo YAML parcialmente preenchido do Codebox para criar a pilha fora do Workload Factory sem credenciais ou permissões. Selecione **CloudFormation** no menu suspenso do Codebox para baixar o arquivo YAML.

- b. **Região e VPC:** selecione uma região e uma rede VPC.

Garanta que os grupos de segurança de um endpoint de interface existente permitam acesso ao protocolo HTTPS (443) para as sub-redes selecionadas.

Os endpoints de interface de serviço da AWS (SQS, FSx, EC2, CloudWatch, Cloud Formation, SSM) e o endpoint de gateway do S3 são criados durante a implantação, caso não sejam encontrados.

Os atributos DNS da VPC `EnableDnsSupport` e `EnableDnsHostnames` são modificados para habilitar a resolução de endereço do endpoint, caso ainda não estejam configurados como `true`.

- c. **Zonas de disponibilidade:** selecione as zonas de disponibilidade e as sub-redes.

Para implantações de instância única

No campo **Configuração do cluster - Nó 1**, selecione uma zona de disponibilidade no menu suspenso **Zona de disponibilidade** e uma sub-rede no menu suspenso **Sub-rede**.

Para implantações de HA

- i. No campo **Configuração do cluster - Nó 1**, selecione a zona de disponibilidade principal para a configuração do MAZ FSx for ONTAP no menu suspenso **Zona de disponibilidade** e uma sub-rede da zona de disponibilidade principal no menu suspenso **Sub-rede**.
 - ii. No campo **Configuração do cluster - Nó 2**, selecione a zona de disponibilidade secundária para a configuração do MAZ FSx for ONTAP no menu suspenso **Zona de disponibilidade** e uma sub-rede da zona de disponibilidade secundária no menu suspenso **Sub-rede**.
- d. **Grupo de segurança:** Um grupo de segurança de carga de trabalho é criado para permitir as portas e os protocolos necessários para o PostgreSQL. Além disso, você pode selecionar um ou mais grupos de segurança.
7. Em **Configurações do aplicativo**, forneça as seguintes informações:
- a. Selecione o **Sistema operacional** no menu suspenso.
 - b. Selecione a **versão do PostgreSQL** no menu suspenso.
 - c. **Nome do servidor de banco de dados:** insira o nome do cluster de banco de dados.
 - d. **Credenciais do banco de dados:** insira um nome de usuário e uma senha para uma nova conta de serviço ou use as credenciais de uma conta de serviço existente no Active Directory.

Para contas GovCloud, insira o valor ARN do parâmetro SSM da AWS para as credenciais no

seguinte formato: `{fsx:{"username":"fsxadmin","password":"pass"}}`. O tipo de parâmetro do AWS SSM deve ser "Secure String" com o nome no formato `/netapp/wlmdb/<anyname>`. Saiba mais sobre como recuperar parâmetros do SSM em ["Documentação da AWS GovCloud"](#).

8. Em **Conectividade**, selecione um par de chaves para se conectar com segurança à sua instância.

9. Em **Configurações de infraestrutura**, forneça as seguintes informações:

- a. **Tipo de instância de banco de dados**: selecione o tipo de instância de banco de dados no menu suspenso.
- b. **sistema FSx for ONTAP**: crie um novo sistema de arquivos FSx for ONTAP ou use um sistema de arquivos FSx for ONTAP existente.
 - i. **Criar novo FSx for ONTAP**: insira o nome de usuário e a senha.

Para contas GovCloud, insira o valor ARN do parâmetro AWS SSM para as credenciais do FSx for ONTAP no seguinte formato:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. O tipo de parâmetro do AWS SSM deve ser "Secure String" com o nome no formato `/netapp/wlmdb/<anyname>`. Saiba mais sobre como recuperar parâmetros do SSM em ["Documentação da AWS GovCloud"](#).

Um novo sistema de arquivos do FSx for ONTAP pode adicionar 30 minutos ou mais ao tempo de instalação.

- ii. **Selecione um FSx for ONTAP existente**: selecione o nome do FSx for ONTAP no menu suspenso e insira um nome de usuário e uma senha para o sistema de arquivos.

Para os sistemas de arquivos FSx for ONTAP existentes, certifique-se do seguinte:

- O grupo de roteamento associado ao FSx for ONTAP permite que as rotas para as sub-redes sejam usadas para implantação.
 - O grupo de segurança permite tráfego das sub-redes usadas para implantação, especificamente as portas TCP HTTPS (443) e iSCSI (3260).
- c. **política do Snapshot**: ativada por padrão. Os Snapshots são feitos diariamente e têm um período de retenção de 7 dias.

Os snapshots são atribuídos a volumes criados para cargas de trabalho do PostgreSQL.

- d. **Tamanho da unidade de dados**: insira a capacidade da unidade de dados e selecione a unidade de capacidade.
- e. **IOPS provisionadas**: selecione **Automático** ou **Provisionado pelo usuário**. Se selecionar **Provisionado pelo usuário**, insira o valor de IOPS.
- f. **Capacidade de throughput**: selecione a capacidade de throughput no menu suspenso.

Em determinadas regiões, você pode selecionar uma capacidade de throughput de 4 GBps. Para provisionar 4 GBps de capacidade de throughput, seu sistema de arquivos FSx for ONTAP deve ser configurado com um mínimo de 5.120 GiB de capacidade de storage e 160.000 IOPS de SSD.

- g. **Criptografia**: selecione uma chave da sua conta ou uma chave de outra conta. Você deve inserir o ARN da chave de criptografia de outra conta.

As chaves de criptografia personalizadas do FSx for ONTAP não estão listadas com base na

aplicabilidade do serviço. Selecione uma chave de criptografia do FSx apropriada. Chaves de criptografia que não sejam do FSx causarão falha na criação do servidor.

As chaves gerenciadas pela AWS são filtradas com base na aplicabilidade do serviço.

- h. **Etiquetas:** opcionalmente, você pode adicionar até 40 etiquetas.
- i. **Serviço de Notificação Simples:** Opcionalmente, você pode habilitar o Serviço de Notificação Simples (SNS) para esta configuração selecionando um tópico SNS para PostgreSQL no menu suspenso.
 - i. Ative o Simple Notification Service.
 - ii. Selecione um ARN no menu suspenso.
- j. **Monitoramento do CloudWatch:** opcionalmente, você pode ativar o monitoramento do CloudWatch.

Recomendamos habilitar o CloudWatch para depuração em caso de falha. Os eventos exibidos no console do AWS CloudFormation são de alto nível e não especificam a causa raiz. Todos os logs detalhados são salvos na pasta `C:\cfn\logs` nas instâncias EC2.

Em CloudWatch, um grupo de logs é criado com o nome da pilha. Um fluxo de logs para cada nó de validação e nó SQL aparece no grupo de logs. CloudWatch mostra o progresso do script e fornece informações para ajudar você a entender se e quando a implantação falha.

- a. **Reverter recurso:** este recurso não é suportado atualmente.

10. Resumo

- a. **Custo estimado:** fornece uma estimativa das cobranças que você pode incorrer se implantar os recursos mostrados.

11. Clique em **Criar** para implantar o novo host de banco de dados.

Alternativamente, você pode salvar a configuração.

O que vem a seguir

Você pode configurar manualmente usuários, acesso remoto e bancos de dados no servidor PostgreSQL implantado.

Criar um banco de dados Microsoft SQL no NetApp Workload Factory for Databases

A criação de um novo banco de dados Microsoft SQL permite gerenciar o recurso no NetApp Workload Factory for Databases.

Sobre esta tarefa

Após a criação do banco de dados, dois novos volumes são criados no sistema de arquivos FSx for ONTAP, consistindo em LUNs independentes para hospedar os arquivos de dados e de log do banco de dados. Os arquivos do novo banco de dados são com thin provisioning e consomem apenas alguns MBs do tamanho total alocado para o novo banco de dados.

Se você quiser segregar o storage para o banco de dados, pode fazer isso usando um *ponto de montagem virtual*. O ponto de montagem virtual permite consolidar bancos de dados em algumas unidades comuns no host.

Criar um banco de dados no workload factory requer permissões de *visualização, planejamento e análise*. Como alternativa, você pode copiar ou baixar um modelo de código parcialmente preenchido para concluir a operação fora do workload factory. ["Saiba mais sobre as permissões do Workload Factory"](#) para decidir qual modo você gostaria de usar.



Os Microsoft SQL Servers que utilizam o protocolo SMB não suportam a criação de bancos de dados.

Antes de começar

Complete os seguintes pré-requisitos antes de criar um novo banco de dados.

- **Credenciais e permissões:** Você deve ter ["Credenciais da conta AWS e permissões de operações e remediação"](#) para criar um novo banco de dados no Workload Factory.

Alternativamente, você pode usar o Codebox para copiar um modelo e, assim, implantar um banco de dados fora do workload factory usando a API REST. ["Saiba mais sobre a automação do Codebox"](#).

- **Host Windows:** você precisa ter letras de unidade suficientes disponíveis no Microsoft SQL Server para criar novas unidades para o novo banco de dados se usar o modo de *Criação rápida*.
- **Microsoft SQL Server:** você precisa ter o Microsoft SQL Server gerenciado no workload factory para Databases para hospedar o novo banco de dados.
- **AWS Systems Manager:** certifique-se de que o NT Authority\SYSTEM privilégio de usuário esteja habilitado no host do Microsoft SQL por meio do AWS Systems Manager.

Criar um banco de dados

Você pode usar os modos de implantação *Quick create* ou *Advanced create* para concluir essa tarefa no Workload Factory.

Criação rápida

Passos

1. Faça login no ["NetApp Console"](#).
2. Selecione o menu  **Cargas de trabalho > Bancos de dados**.
3. No menu Bancos de dados, selecione **Inventário**.
4. No Inventário, selecione **Microsoft SQL Server** como o tipo de mecanismo de banco de dados.
5. Selecione um servidor de banco de dados com uma instância gerenciada do SQL server para criar o banco de dados.
6. Clique no menu de ações da instância gerenciada e selecione **Criar banco de dados de usuário**.
7. Na página Criar banco de dados do usuário, em Informações do banco de dados, forneça as seguintes informações:
 - a. **Nome do banco de dados:** insira o nome do banco de dados.
 - b. **Collation:** selecione uma collation para o banco de dados. A collation padrão SQL_Latin1_General_CP1_CI_AS no Microsoft SQL Server está selecionada.
8. Em Configurações de arquivo, forneça as seguintes informações:
 - a. **Modo de configurações de arquivo:** selecione **Criação rápida**.

b. **Nomes de arquivos e caminho:**

- **Nome do arquivo de dados:** insira o nome do arquivo de dados.
- **Nome do arquivo de log:** digite o nome do arquivo de log.

c. **Tamanhos de arquivo:** insira o tamanho dos dados e o tamanho do log do banco de dados.

9. Clique em **Create**.

Como alternativa, se você quiser alterar agora qualquer uma dessas configurações padrão, altere **Modo de configurações de arquivo** para **Criação avançada**.

Criação avançada

Passos

1. Faça login no "NetApp Console".

2. Selecione o menu , **Cargas de trabalho > Bancos de dados**.

3. No menu Bancos de dados, selecione **Inventário**.

4. No Inventário, selecione **Microsoft SQL Server** como o tipo de mecanismo de banco de dados.

5. Selecione um servidor de banco de dados com uma instância gerenciada do SQL server para criar o banco de dados.

6. Clique no menu de ações da instância gerenciada e selecione **Criar banco de dados de usuário**.

7. Selecione **Criar banco de dados de usuários**.

8. Na página Criar banco de dados do usuário, em Informações do banco de dados, forneça as seguintes informações:

a. **Nome do banco de dados:** insira o nome do banco de dados.

b. **Collation:** selecione a ordenação (collation) para o banco de dados. A ordenação padrão SQL_Latin1_General_CP1_CI_AS" no Microsoft SQL Server está selecionada.

9. Em Configurações de arquivo, forneça as seguintes informações:

a. **Modo de configurações de arquivo:** selecione **Criação avançada**.

b. **Nomes de arquivos e caminho:**

i. **Arquivo de dados:** selecione uma letra de unidade e insira o nome do arquivo de dados.

Opcionalmente, clique na caixa para **Ponto de montagem virtual**.

ii. **Arquivo de log:** selecione uma letra da unidade e insira o nome do arquivo de log.

Opcionalmente, clique na caixa para **Ponto de montagem virtual**.

c. **Tamanhos de arquivo:** insira o tamanho dos dados e o tamanho do log do banco de dados.

10. Clique em **Create**.

Se você criou o host do banco de dados, pode verificar o progresso da tarefa na guia **Monitoramento de tarefas**.

Criar um clone de sandbox no NetApp Workload Factory for Databases

Criar um clone sandbox de um banco de dados na NetApp Workload Factory for Databases permite que você use o clone para desenvolvimento, teste, integração, análise, treinamento, controle de qualidade e muito mais, sem alterar o banco de dados de origem.

Sobre esta tarefa

Um clone de sandbox é criado a partir do snapshot mais recente do banco de dados de origem. Ele pode ser clonado no mesmo Microsoft SQL Server que o banco de dados de origem ou em outro Microsoft SQL Server, desde que ambos compartilhem o mesmo sistema de arquivos FSx for ONTAP.

Antes de começar

Certifique-se de concluir os seguintes pré-requisitos antes de criar um clone de sandbox.

- **Credenciais e permissões:** Você deve ter "[Credenciais da conta AWS e permissões de operações e remediação](#)" para criar um clone de sandbox no Workload Factory.

Alternativamente, você pode usar o Codebox para copiar um modelo parcialmente preenchido ou criar um modelo completo para que você possa criar o clone do ambiente de teste fora do Workload Factory usando API REST "[Saiba mais sobre a automação do Codebox](#)".

- **Microsoft SQL Server:** você precisa ter um Microsoft SQL Server gerenciado no Workload Factory for Databases para hospedar o novo clone do sandbox.
- **AWS Systems Manager:** certifique-se de que o NT Authority\SYSTEM privilégio de usuário esteja habilitado no host do Microsoft SQL por meio do AWS Systems Manager.
- **Banco de dados de origem:** você precisa de um banco de dados de origem disponível para a clonagem.

Passos

1. Faça login no "[NetApp Console](#)".
2. Selecione o menu , **Cargas de trabalho > Bancos de dados**.
3. Em Databases, selecione a guia **Sandboxes**.
4. Na aba Sandboxes, selecione **Criar novo sandbox**.
5. Na página Criar novo sandbox, em Origem do banco de dados, forneça as seguintes informações:
 - a. **Host do servidor de banco de dados de origem:** selecione o host do servidor de banco de dados de origem.
 - b. **Instância do banco de dados de origem:** selecione a instância do banco de dados de origem.
 - c. **Banco de dados de origem:** selecione o banco de dados de origem do qual deseja clonar.
6. Em Destino do banco de dados, forneça as seguintes informações:
 - a. **Host do banco de dados de destino:** selecione um host de banco de dados de destino para o clone do sandbox que esteja na mesma VPC e tenha o mesmo sistema de arquivos FSx for ONTAP que o host de origem.
 - b. **Instância de banco de dados de destino:** selecione a instância de banco de dados de destino para o clone do sandbox.

c. **Banco de dados de destino:** insira um nome para o clone do ambiente de teste.

7. **Montagem:** ao clonar um banco de dados SQL que possui vários arquivos de dados e/ou de log, o Workload Factory clona todos os arquivos na letra da unidade atribuída automaticamente ou definida.

Selecione uma das seguintes opções:

a. **Atribuir automaticamente o ponto de montagem**

b. **Definir caminho do ponto de montagem**

Forneça as seguintes informações para definir o caminho do ponto de montagem:

- Digite a letra da unidade para o caminho do arquivo de dados.
- Insira a letra da unidade para o caminho do arquivo de log.

8. **Definir etiqueta:** selecione uma etiqueta para definir o clone da sandbox.

9. Clique em **Create**.

Para verificar o andamento da tarefa, acesse a aba **Monitoramento de tarefas**.

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES DOCUMENTOS, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.