Use Database workloads

Database workloads

NetApp
February 04, 2026

Table of Contents

Use Database workloads

Explore savings in NetApp Workload Factory for Databases

Explore savings in NetApp Workload Factory for Databases for your database workloads by comparing the costs of using Microsoft SQL Server on Amazon Elastic Block Store (EBS), FSx for Windows File Server, and on-premises storage with FSx for ONTAP storage.

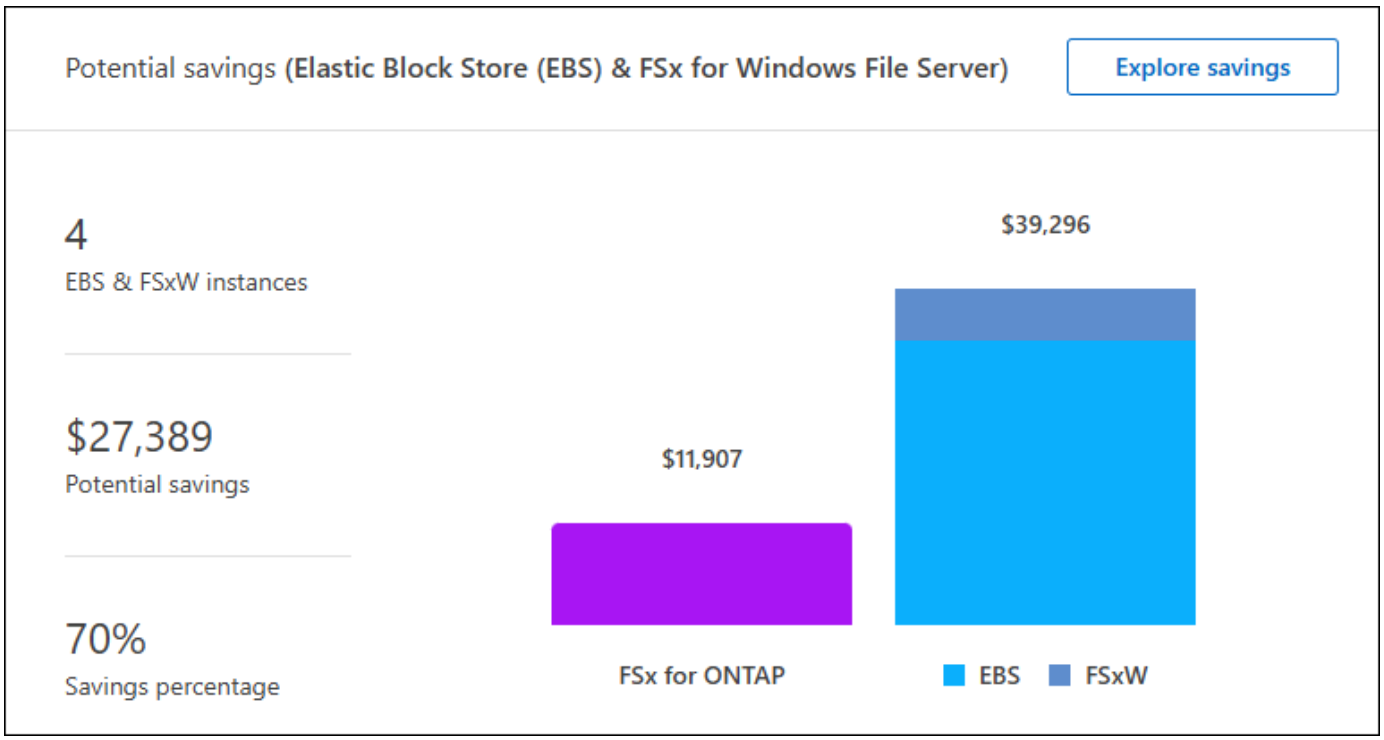
About this task

Workload Factory has several ways for you to explore savings for your database workloads running on Amazon Elastic Block Store (EBS), FSx for Windows File Server, and on-premises storage - from the Dashboard, from the Inventory tab, and from the Explore savings tab. In all cases, you can use the savings calculator to compare various cost components of running Microsoft SQL Server workloads like storage, compute, SQL license, snapshots, and clones for your database workloads on FSx for ONTAP file systems against Elastic Block Store (EBS), FSx for Windows File Server, and on-premises storage.

If Workload Factory determines that you could save money by running these workloads on an FSx for ONTAP file system, you can deploy Microsoft SQL over FSx for ONTAP directly from the savings calculator in the Workload Factory console. When you have multiple Microsoft SQL Server instances over Elastic Block Store, FSx for Windows File Server, or on-premises storage, we'll recommend an FSx for ONTAP configuration with a single SQL instance.

Potential savings for all database workloads

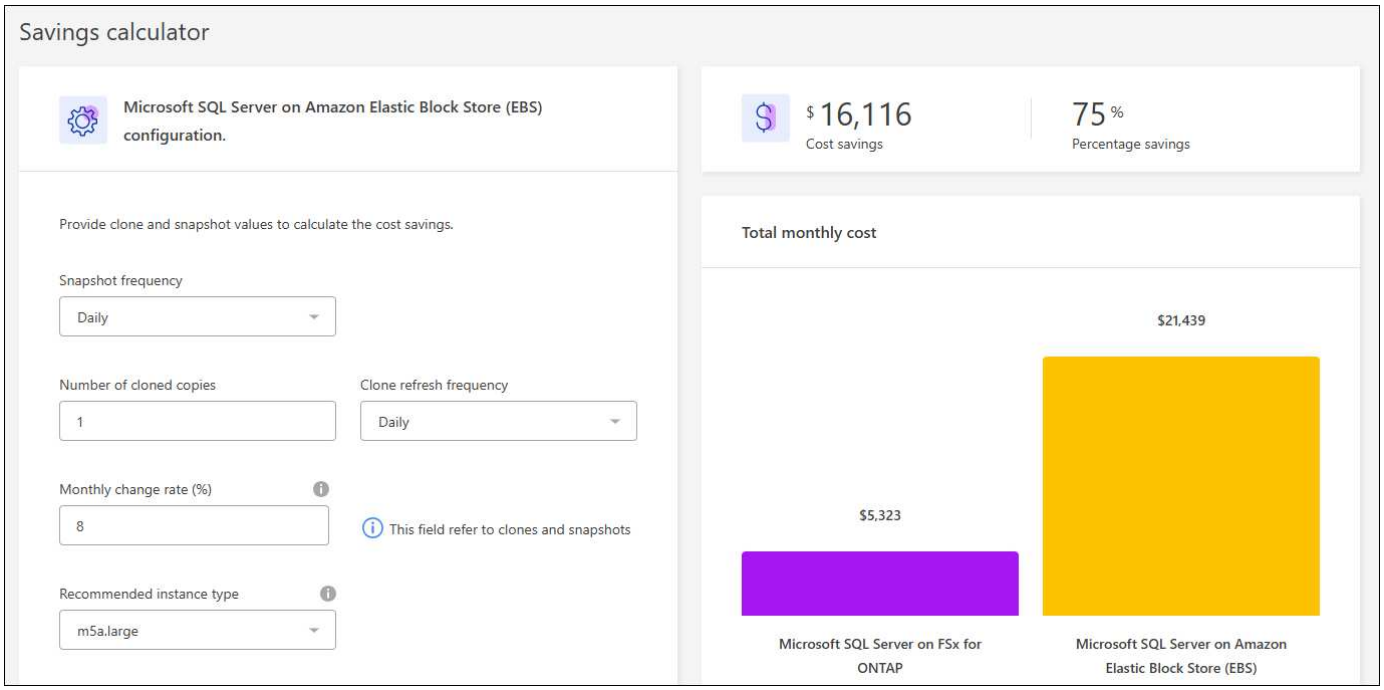
Visit the Databases **Dashboard** in the Workload Factory console to get an overview of potential cost savings for running all of your database workloads on FSx for ONTAP. In the **Potential savings** tile, you can view the number of all database workloads you have on Elastic Block Store and FSx for Windows File Server, the potential cost savings, the savings percentage, and visual representation in the bar graph.



Savings calculator

You can utilize the savings calculator so you can compare various cost components of running Microsoft SQL Server workloads like storage, compute, SQL license, snapshots, and clones for your database workloads on FSx for ONTAP file systems against Elastic Block Store (EBS), FSx for Windows File Server, and on-premises storage. Depending on your storage requirements, you might find that FSx for ONTAP file systems are the most cost effective for your database workloads.

The calculator displays whether the storage for the database workloads on these Microsoft SQL Servers would cost less if you used an FSx for ONTAP file system. Learn how to use the calculator.



SQL Server deployment analysis

The calculator performs a comprehensive analysis of your SQL Server deployment to ensure that the resources and features being utilized are appropriately matched to the SQL Server edition. Here are the key factors and conditions the calculator checks before recommending a downgrade to Standard Edition:

Deployment model

The calculator evaluates the deployment model and whether Enterprise edition is required.

Allocated resources

The calculator assesses the conditions of the following license-dependent allocated resources:

- Target Instance vCPUs: The instance has 48 or fewer virtual CPUs.
- Memory Allocation: The instance has 128GB or less of memory.

Enterprise feature usage

The calculator verifies if any of the following Enterprise features are in use:

- Database-level Enterprise features
- Online index operations
- Resource Governor

- Peer-to-peer or Oracle replication
- R/Python extensions
- Memory-optimized TempDB

If the assessed SQL Server instance doesn't utilize any of the above Enterprise features and meets the resource constraints, the calculator will recommend downgrading the license to Standard Edition. This recommendation is made to help you optimize your SQL Server licensing costs without compromising performance or functionality.

Calculator options

Two calculator options are available for making the cost comparison between your systems and FSx for ONTAP — customization and detection.

Explore savings via customization: You provide the configuration settings for Microsoft SQL server on Amazon EC2 with EBS or FSx for Windows File Server including the region, deployment model, SQL server edition, monthly data change rate, snapshot frequency, and more.

Explore savings for detected hosts: Workload Factory links to your existing Microsoft SQL servers and pulls in the details to the calculator for automatic comparison. You'll need to grant *view, planning, and analysis* permissions to use this calculator option. You can change the use case, but all other details are automatically determined in the calculation.

Additionally, you can add AWS credentials to improve the accuracy of the calculator analysis. Select **Calculate savings based on existing resources**. You'll be redirected to the Add credentials page. After you add credentials, select the existing resources to compare with FSx for ONTAP, and select **Explore savings**.

Explore savings via customization

Follow the steps under the tab for your storage type.

Amazon Elastic Block Store (EBS)

Steps

1. Log in using one of the console experiences.
2. Select the menu and then select **Databases**.
3. From Databases, select **Explore savings** then **Microsoft SQL Server on EBS**.
4. In the Savings calculator, provide the following details:
    a. **Region**: Select a region from the dropdown menu.
    b. **Deployment model**: Select a deployment model from the dropdown menu.
    c. **SQL server edition**: Select the SQL server edition from the dropdown menu.
    d. **Monthly data change rate (%)**: Enter the percentage that clone and snapshot data changes on average per month.
    e. **Snapshot frequency**: Select a snapshot frequency from the dropdown menu.
    f. **Number of cloned copies**: Enter the number of cloned copies in the EBS configuration.
    g. **Monthly SQL BYOL cost ($)**: Optionally, enter the monthly SQL BYOL cost in dollars.
    h. Under EC2 specifications, provide the following:
        - **Machine description**: Optionally, enter a name to describe the machine.
        - **Instance type**: Select the EC2 instance type from the dropdown menu.
    i. Under Volume types, provide the following details for at least one volume type. IOPS and throughput apply to certain disk type volumes.
        - **Number of volumes**
        - **Storage amount per volume (GiB)**
        - **Provisioned IOPS per volume**
        - **Throughput MB/s**
    j. If you selected the Always On availability deployment model, provide details for **Secondary EC2 specifications** and **Volume types**.

Amazon FSx for Windows File Server

Steps

1. Log in using one of the console experiences.
2. Select the menu and then select **Databases**.
3. From Databases, select **Explore savings** then **Microsoft SQL Server on FSx for Windows**.
4. In the Savings calculator, provide the following details:
    a. **Region**: Select a region from the dropdown menu.
    b. **Deployment model**: Select a deployment model from the dropdown menu.
    c. **SQL server edition**: Select the SQL server edition from the dropdown menu.
    d. **Monthly data change rate (%)**: Enter the percentage that clone and snapshot data changes on average per month.
    e. **Snapshot frequency**: Select a snapshot frequency from the dropdown menu.
    f. **Number of cloned copies**: Enter the number of cloned copies in the EBS configuration.

g. **Monthly SQL BYOL cost ($)**: Optionally, enter the monthly SQL BYOL cost in dollars.

h. Under FSx for Windows File Server settings, provide the following:

- **Deployment type**: Select the deployment type from the dropdown menu.
- **Storage type**: SSD storage is the supported storage type.
- **Total storage capacity**: Enter the storage capacity and select the capacity unit for the configuration.
- **Provisioned SSD IOPS**: Enter the provisioned SSD IOPS for the configuration.
- **Throughput (MB/s)**: Enter throughput in MB/s.

i. Under EC2 specifications, select the **Instance type** from the dropdown menu.

After you provide details for your database host configuration, review the calculations and recommendations provided on the page.

Additionally, scroll down to the bottom of the page to view the report by selecting one of the following:

- **Export PDF**
- **Send by email**
- **View the calculations**

To switch to FSx for ONTAP, follow the instructions to deploy Microsoft SQL Server on AQS EC2 using FSx for ONTAP file systems.

Explore savings for detected hosts

Workload Factory enters the detected Elastic Block Store and FSx for Windows File Server host characteristics so that you can explore savings automatically.

Before you begin

Complete the following prerequisites before you begin:

- Grant *view, planning, and analysis* permissions in your AWS account to detect Elastic Block Store (EBS) and FSx for Windows systems under the **Explore savings** tab and to show the savings calculation in the savings calculator.
- To get instance type recommendations and improve cost accuracy, do the following:
  1. Grant Amazon CloudWatch and AWS Compute Optimizer permissions.
     a. Sign in to the AWS Management Console and open the IAM service.
     b. Edit the policy for the IAM role. Copy and add the following Amazon CloudWatch and AWS Compute Optimizer permissions.

```
{
"Version": "2012-10-17",
"Statement": [
  {
   "Effect": "Allow",
   "Action": "compute-optimizer:GetEnrollmentStatus",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "compute-optimizer:PutRecommendationPreferences",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "compute-
optimizer:GetEffectiveRecommendationPreferences",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "compute-optimizer:GetEC2InstanceRecommendations",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "autoscaling:DescribeAutoScalingGroups",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "autoscaling:DescribeAutoScalingInstances",
   "Resource": "*"
  }
]
}
```

2. Opt the billable AWS account in to AWS Compute Optimizer.

Follow the steps under the tab for your storage type.

Amazon Elastic Block Store (EBS)

Steps

1. Log in using one of the console experiences.
2. Select the menu and then select **Databases**.
3. From the Databases menu, select **Explore savings**.
4. In Explore savings, select the **SQL Server on Elastic Block Store (EBS)** tab.

   If Workload Factory detects EBS hosts, you'll be redirected to the Explore savings tab. If Workload Factory doesn't detect EBS hosts, you'll be redirected to the calculator to explore savings via customization.

5. From **Explore savings**, select one or more database hosts running on EBS and then select **Explore savings**.
6. If required, authenticate the database host with SQL Server credentials, Windows credentials, or by adding missing SQL Server permissions.

   If the Explore savings page doesn't load data after successful authentication, select the **Inventory** tab to reload the data, and then select the **Explore savings** tab again.

7. In the Savings calculator, optionally, provide the following details on clones and snapshots in your EBS storage for a more accurate cost savings estimate.
   a. **Snapshot frequency**: Select a snapshot frequency from the menu.
   b. **Clone refresh frequency**: Select the frequency that clones refresh from the menu.
   c. **Number of cloned copies**: Enter the number of cloned copies in the EBS configuration.
   d. **Monthly change rate**: Enter the percentage that clone and snapshot data changes on average per month.
   e. **Add hosts**: Optionally, select up to five detected EBS hosts to include in the savings calculation.

      Workload Factory consolidates multiple SQL Server hosts into a single FSx for ONTAP configuration recommendation to optimize cost savings unless the selected EBS hosts exceed throughput, capacity, or IOPS limits for a single FSx for ONTAP file system.

Amazon FSx for Windows File Server

Steps

1. Log in using one of the console experiences.
2. Select the menu and then select **Databases**.
3. From the Databases menu, select **Explore savings**.
4. In Explore savings, select the **SQL Server on FSx for Windows** tab.

   If Workload Factory detects FSx for Windows hosts, you'll be redirected to the Explore savings tab. If Workload Factory doesn't detect FSx for Windows hosts, you'll be redirected to the calculator to explore savings via customization.

5. In the Explore savings tab, select **Explore savings** of the database host using FSx for Windows File Server storage.
6. If required, authenticate the database host with SQL Server credentials, Windows credentials, or by

adding missing SQL Server permissions.

If the Explore savings page doesn't load data after successful authentication, select the **Inventory** tab to reload the data, and then select the **Explore savings** tab again.

7. In the Savings calculator, optionally, provide the following details on clones (shadow copies) and snapshots in your FSx for Windows storage for a more accurate cost savings estimate.
   a. **Snapshot frequency**: Select a snapshot frequency from the menu.

      If FSx for Windows shadow copies are detected, the default value is **Daily**. If shadow copies aren't detected, the default value is **No snapshot frequency**.

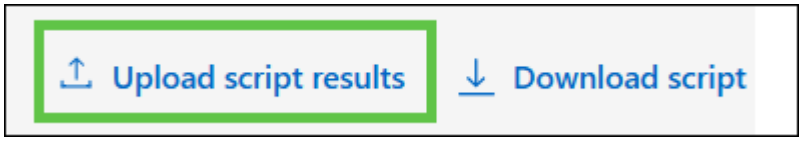
   b. **Clone refresh frequency**: Select the frequency that clones refresh from the menu.
   c. **Number of cloned copies**: Enter the number of cloned copies in the FSx for Windows configuration.
   d. **Monthly change rate**: Enter the percentage that clone and snapshot data changes on average per month.

Microsoft SQL Server on-premises

Steps

1. Log in using one of the console experiences.
2. Select the menu and then select **Databases**.
3. From the Databases menu, select **Explore savings**.
4. In Explore savings, select the **SQL Server on-premises** tab.
5. From the SQL Server on-premises tab, download the script to assess your on-premises SQL Server environments.
   a. Download the assessment script. The script is a data collection tool based on PowerShell. It gathers and then uploads SQL Server configuration and performance data to Workload Factory. The migration advisor assesses the data and plans FSx for ONTAP deployment for your SQL Server environment.

   b. Run the script on the SQL Server host.
   c. Upload the script output in the SQL Server on-premises tab in Workload Factory.



6. From the SQL Server on-premises tab, select up to five database hosts and then select **Explore savings** to run a cost analysis of the SQL Server on-premises host(s) against FSx for ONTAP.
7. In the Savings calculator, select the region for the on-premises host.
8. Optionally, provide the following details on clones (shadow copies) and snapshots in your on-premises database environment for a more accurate cost savings estimate.

a. **Snapshot frequency**: Select a snapshot frequency from the menu.

   If FSx for Windows shadow copies are detected, the default value is **Daily**. If shadow copies aren't detected, the default value is **No snapshot frequency**.

b. **Clone refresh frequency**: Select the frequency that clones refresh from the menu.

c. **Number of cloned copies**: Enter the number of cloned copies in the on-premises configuration.

d. **Monthly change rate**: Enter the percentage that clone and snapshot data changes on average per month.

9. For more accurate results, update Compute information and Storage and performance details.

   Workload Factory consolidates multiple SQL Server on-premises hosts into a single FSx for ONTAP configuration recommendation to optimize cost savings unless the selected on-premises hosts exceed throughput, capacity, or IOPS limits for a single FSx for ONTAP file system.

After you provide details for your database host configuration, review the calculations and recommendations provided on the page.

Additionally, scroll down to the bottom of the page to view the report by selecting one of the following:

- **Export PDF**
- **Send by email**
- **View the calculations**

To switch to FSx for ONTAP, follow the instructions to deploy Microsoft SQL Server on AQS EC2 using FSx for ONTAP file systems.

On-premises host removal

After you've explored savings for a Microsoft SQL server on-premises host, you have the option to remove the on-premises host record from Workload Factory. Select the action menu of the Microsoft SQL Server on-premises host and then select **Delete**.

Deploy Microsoft SQL Server on AWS EC2 using FSx for ONTAP

If you'd like to switch to FSx for ONTAP to realize cost savings, click **Create** to create the recommended configuration(s) directly from the Create new Microsoft SQL server wizard or click **Save** to save the recommended configuration(s) for later.

Workload Factory doesn't support saving or creating multiple FSx for ONTAP file systems.

Deployment methods

With *database host creation permissions*, you can deploy the new Microsoft SQL server on AWS EC2 using FSx for ONTAP directly from Workload Factory. You can also copy the content from the Codebox window and deploy the recommended configuration using one of the Codebox methods.

Without permissions, you can copy the content from the Codebox window and deploy the recommended configuration using one of the Codebox methods.

Related information

Workload Factory permissions reference

Create a new database server

Create a Microsoft SQL Server in Workload Factory for Databases

Creating a new Microsoft SQL Server, or database host, in Workload Factory for Databases requires an FSx for ONTAP file system deployment and resources for Active Directory.

About this task

Before creating a Microsoft SQL Server from Workload Factory, learn about the available storage deployment types for the database host configuration, Microsoft Multi-path I/O configuration, Active Directory deployment, networking details, and the requirements to complete this operation.

After deployment, you'll need to enable remote connection on the Microsoft SQL Server.

FSx for ONTAP file system deployments

Creating a new Microsoft SQL Server requires an FSx for ONTAP file system as the storage backend. You can use an existing FSx for ONTAP file system or create a new file system. If you select an existing FSx for ONTAP file system as your database server storage backend, we create a new storage VM for the Microsoft SQL workloads.

FSx for ONTAP file systems have two Microsoft SQL Server deployment models: *Failover Cluster Instance (FCI)* or *Standalone*. Different resources are created for the FSx for ONTAP file system depending on the FSx for ONTAP deployment model you select.

- **Failover Cluster Instance (FCI) Microsoft SQL deployment**: A Multiple Availability Zone FSx for NetApp ONTAP file system is deployed when a new FSx for ONTAP file system is selected for FCI deployment. Separate volumes and LUNs are created for data, log, and tempdb files for an FCI deployment. An additional volume and LUN are created for Quorum or witness disk for Windows cluster.
- **Standalone Microsoft SQL deployment**: A Single Availability Zone FSx for ONTAP file system is created when a new Microsoft SQL Server is created. In addition, separate volumes and LUNs are created for data, log, and tempdb files.

Microsoft Multi-path I/O configuration

Microsoft SQL Server deployment models both require LUN creation using the iSCSI storage protocol. Workload Factory configures Microsoft Multi-path I/O (MPIO) as part of configuring LUNs for SQL Server over FSx for ONTAP. MPIO is configured based on AWS and NetApp best practices.

For more information, refer to SQL Server High Availability Deployments using Amazon FSx for NetApp ONTAP.

Active Directory

The following occurs for Active Directory (AD) during deployment:

- A new Microsoft SQL service account is created in the domain if you don't provide an existing SQL service account.
- The Windows cluster, node host names, and Microsoft SQL FCI name are added as managed computers to the Microsoft SQL service account.
- The Windows cluster entry is assigned permissions to add computers to the domain.

User-managed Active Directory security groups

If you select “user-managed Active Directory” during Microsoft SQL Server deployment in Workload Factory, you must provide a security group that allows traffic between the EC2 instances to the directory service for deployment. Workload Factory doesn’t automatically attach the security group for user-managed Active Directory like it does for AWS Managed Microsoft AD.

Resource rollback

If you decide to rollback your Domain Name System (DNS) resources, the resource records in AD and DNS are not removed automatically. You can remove the records from the DNS server and AD as follows.

- For user-managed AD, first remove the AD computer. Then, connect to the DNS server from DNS manager and delete the DNS Resource Records.
- For AWS Managed Microsoft AD, install the AD administration tools. Next, remove the AD computer. Lastly, connect to the DNS server from DNS manager and delete the DNS Resource Records.

Before you begin

Ensure you have the following prerequisites before you create a new database host.

Credentials and permissions

You must grant *database host creation* permissions in your AWS account to create a new database host in Workload Factory.

Active Directory

When connecting to Active Directory, you must have administrative access with permissions to do the following:

- Join the domain
- Create Computer Objects
- Create objects in the default Organization Unit (OU)
- Read all properties
- Make the domain user a local admin on the AD nodes
- Create a Microsoft SQL Server service user in the AD, if it doesn’t exist already

Step 1: Create a database server

You can use *Quick create* or *Advanced create* deployment modes to complete this task in Workload Factory with *Automate* mode permissions. You can also use the following tools available in the Codebox: REST API, AWS CLI, AWS CloudFormation, and Terraform. Learn how to use Codebox for automation.

> When using Terraform from Codebox, the code you copy or download hides `fsxadmin` and `vsadmin` passwords. You’ll need to re-enter the passwords when you run the code. You’ll need to include the following permissions for the user account in addition to *Automate* mode permissions: `iam:TagRole` and `iam:TagInstanceProfile`. Learn how to use Terraform from Codebox.

During deployment, Workload Factory enables CredSSP for credential delegation to scripts for provisioning SQL. When the CredSSP delegation is blocked for all domain computers with the group policy, deployment fails. Post-deployment, Workload Factory disables CredSSP.

Quick create

In *Quick create*, FCI is the default deployment model, Windows 2016 is the default Windows version, and SQL 2019 Standard Edition is the default SQL version.

Steps

1. Log in using one of the console experiences.
2. In the Databases tile, select **Deploy host** and then select **Microsoft SQL Server** from the menu.
3. Select **Quick create**.
4. Under **AWS settings**, provide the following:
   a. **AWS credentials**: Select AWS credentials with automate permissions to deploy the new database host.

      AWS credentials with *read/write* permissions let Workload Factory deploy and manage the new database host from your AWS account within Workload Factory.

      AWS credentials with *read-only* permissions let Workload Factory generate a CloudFormation template for you to use in the AWS CloudFormation console.

      If you don't have AWS credentials associated in Workload Factory and you want to create the new server in Workload Factory, follow **Option 1** to go to the Credentials page. Manually add the required credentials and permissions for *read/write* mode for Database workloads.

      If you want to complete the create new server form in Workload Factory so you can download a complete YAML file template for deployment in AWS CloudFormation, follow **Option 2** to ensure you have the required permissions to create the new server within AWS CloudFormation. Manually add the required credentials and permissions for *read* mode for Database workloads.

      Optionally, you can download a partially completed YAML file template from the Codebox to create the stack outside Workload Factory without any credentials or permissions. Select **CloudFormation** from the dropdown in the Codebox to download the YAML file.

   b. **Region & VPC**: Select a Region and VPC network.

      Ensure deployment subnets are associated with existing interface endpoints and security groups allow access to HTTPS (443) protocol to the selected subnets.

      AWS service interface endpoints (SQS, FSx, EC2, CloudWatch, CloudFormation, SSM) and the S3 gateway endpoint are created during deployment if not found.

      VPC DNS attributes `EnableDnsSupport` and `EnableDnsHostnames` are modified to enable endpoint address resolution if they aren't already set to `true`.

      When using a cross-VPC DNS, the security group for endpoints on the other VPC where DNS resides should allow port 443 to deployment subnets. If not, you should provide a DNS resolver from the local VPC when joining a cross-VPC Active Directory. In a multiple replicated Domain Controller environment, if some domain controllers are not reachable from the subnet, you can **Redirect to CloudFormation** and enter `Preferred domain controller` to connect to Active Directory.

   c. **Availability zones**: Select availability zones and subnets according to the Failover Cluster Instance (FCI) deployment model.

FCI deployments are only supported on Multiple Availability Zone (MAZ) FSx for ONTAP configurations.

i. In the **Cluster configuration - Node 1** field, select the primary availability zone for the MAZ FSx for ONTAP configuration from the **Availability zone** dropdown menu and a subnet from the primary availability zone from the **Subnet** dropdown menu.

ii. In the **Cluster configuration - Node 2** field, select the secondary availability zone for the MAZ FSx for ONTAP configuration from the **Availability zone** dropdown menu and a subnet from the secondary availability zone from the **Subnet** dropdown menu.

5. Under **Application settings**, enter a user name and password for **Database credentials**.
6. Under **Connectivity**, provide the following:
   a. **Key pair**: Select a key pair.
   b. **Active Directory**:
      i. In the **Domain name** field, select or enter a name for the domain.
         A. For AWS-managed Active Directories, domain names appear in the dropdown menu.
         B. For a user-managed Active Directory, enter a name in the **Search and Add** field, and click **Add**.
      ii. In the **DNS address** field, enter the DNS IP address for the domain. You can add up to 3 IP addresses.

          For AWS-managed Active Directories, the DNS IP address(es) appear in the dropdown menu.

      iii. In the **User name** field, enter the user name for the Active Directory domain.
      iv. In the **Password** field, enter a password for the Active Directory domain.
7. Under **Infrastructure settings**, provide the following:
   a. **FSx for ONTAP system**: Create a new FSx for ONTAP file system or use an existing FSx for ONTAP file system.
      i. **Create new FSx for ONTAP**: Enter user name and password.

         A new FSx for ONTAP file system may add 30 minutes or more of installation time.

      ii. **Select an existing FSx for ONTAP**: Select FSx for ONTAP name from the dropdown menu, and enter a user name and password for the file system.

          For existing FSx for ONTAP file systems, ensure the following:

          - The routing group attached to FSx for ONTAP allows routes to the subnets to be used for deployment.
          - The security group allows traffic from the subnets used for deployment, specifically HTTPS (443) and iSCSI (3260) TCP ports.
   b. **Data drive size**: Enter the data drive capacity and select the capacity unit.
8. Summary:
   a. **Preview default**: Review the default configurations set by Quick create.
   b. **Estimated cost**: Provides an estimate of charges that you might incur if you deployed the resources shown.

9. Click **Create**.

   Alternatively, if you want to change any of these default settings now, create the database server with Advanced create.

   You can also select **Save configuration** to deploy the host later.

Advanced create

Steps

1. Log in using one of the console experiences. In the Databases tile, select **Deploy host** and then select **Microsoft SQL Server** from the menu.
2. Select **Advanced create**.
3. For **Deployment model**, select **Failover Cluster Instance** or **Single instance**.
4. Under **AWS settings**, provide the following:
   a. **AWS credentials**: Select AWS credentials with automate permissions to deploy the new database host.

      AWS credentials with *read/write* permissions let Workload Factory deploy and manage the new database host from your AWS account within Workload Factory.

      AWS credentials with *read-only* permissions let Workload Factory generate a CloudFormation template for you to use in the AWS CloudFormation console.

      If you don't have AWS credentials associated in Workload Factory and you want to create the new server in Workload Factory, follow **Option 1** to go to the Credentials page. Manually add the required credentials and permissions for *read/write* mode for Database workloads.

      If you want to complete the create new server form in Workload Factory so you can download a complete YAML file template for deployment in AWS CloudFormation, follow **Option 2** to ensure you have the required permissions to create the new server within AWS CloudFormation. Manually add the required credentials and permissions for *read-only* mode for Database workloads.

      Optionally, you can download a partially completed YAML file template from the Codebox to create the stack outside Workload Factory without any credentials or permissions. Select **CloudFormation** from the dropdown in the Codebox to download the YAML file.

   b. **Region & VPC**: Select a Region and VPC network.

      Ensure security groups for an existing interface endpoint allow access to HTTPS (443) protocol to the selected subnets.

      AWS Service interface endpoints (SQS, FSx, EC2, CloudWatch, Cloud Formation, SSM) and S3 gateway endpoint are created during deployment if not found.

      VPC DNS attributes `EnableDnsSupport` and `EnableDnsHostnames` are modified to enable resolve endpoint address resolution if not already set to `true`.

   c. **Availability zones**: Select availability zones and subnets according to the deployment model you selected. Subnets should not share the same route table for high availability.

FCI deployments are only supported on Multiple Availability Zone (MAZ) FSx for ONTAP configurations.

- For single instance deployments:
  - In the **Cluster configuration - Node 1** field, select an availability zone from the **Availability zone** from the dropdown menu and a subnet from the **Subnet** dropdown menu.
- For FCI deployments:
  - In the **Cluster configuration - Node 1** field, select the primary availability zone for the MAZ FSx for ONTAP configuration from the **Availability zone** dropdown menu and a subnet from the primary availability zone from the **Subnet** dropdown menu.
  - In the **Cluster configuration - Node 2** field, select the secondary availability zone for the MAZ FSx for ONTAP configuration from the **Availability zone** dropdown menu and a subnet from the secondary availability zone from the **Subnet** dropdown menu.

d. **Security group**: Select an existing security group or create a new security group. Three security groups get attached to the SQL nodes (EC2 instances) during new server deployment.

1. A workload security group is created to allow ports and protocols required for Microsoft SQL and Windows cluster communication on nodes.
2. In case of AWS-managed Active Directory, the security group attached to the directory service gets automatically added to the Microsoft SQL nodes to allow communication with Active Directory.
3. For an existing FSx for ONTAP file system, the security group associated with it is added automatically to the SQL nodes which allows communication to the file system. When a new FSx for ONTAP system is created, a new security group is created for the FSx for ONTAP file system and the same security group also gets attached to SQL nodes.

   For a user-managed Active Directory, ensure the security group configured on the AD instance allows traffic from subnets used for deployment. The security group should allow communication to the Active Directory domain controllers from the subnets where EC2 instances for Microsoft SQL are configured.

5. Under **Application settings**, provide the following:

a. Under **SQL Server install type**, select **License included AMI** or **Use custom AMI**.

i. If you select **License included AMI**, provide the following:

A. **Operating system**: Select **Windows server 2016**, **Windows server 2019**, or **Windows server 2022**.

B. **Database edition**: Select **SQL Server Standard Edition** or **SQL Server Enterprise Edition**.

C. **Database version**: Select **SQL Server 2016**, **SQL Server 2019**, or **SQL Server 2022**.

D. **SQL Server AMI**: Select a SQL Server AMI from the dropdown menu.

ii. If you select **Use custom AMI**, select an AMI from the dropdown menu.

b. **SQL Server collation**: Select a collation set for the server.

If the selected collation set isn't compatible for installation, we recommend that you select the default collation "SQL_Latin1_General_CP1_CI_AS".

c. **Database name**: Enter the database cluster name.

d. **Database credentials**: Enter a user name and password for a new service account or use existing service account credentials in the Active Directory.

   Optional: Select to **Use managed service account** for the SQL Server service account. Use this option if your environment uses MSA (Managed Service Account) or Group Managed Service Accounts (gMSA) where password management is handled by Active Directory.

6. Under **Connectivity**, provide the following:

   a. **Key pair**: Select a key pair to connect securely to your instance.

   b. **Active Directory**: Provide the following Active Directory details:

      i. In the **Domain name** field, select or enter a name for the domain.

         A. For AWS-managed Active Directories, domain names appear in the dropdown menu.

         B. For a user-managed Active Directory, enter a name in the **Search and Add** field, and click **Add**.

      ii. In the **DNS address** field, enter the DNS IP address for the domain. You can add up to 3 IP addresses.

         For AWS-managed Active Directories, the DNS IP address(es) appear in the dropdown menu.

      iii. In the **User name** field, enter the user name for the Active Directory domain.

      iv. In the **Password** field, enter a password for the Active Directory domain.

      v. **Preferred domain controller**: Optionally, enter the preferred domain controller to use for the Active Directory to join.

      vi. **Preferred organizational unit path**: Optionally, enter the preferred organizational unit (OU) in the Active Directory to join.

      vii. **Target Active Directory group**: Optionally, enter the target Active Directory group to add the computers to.

7. Under **Infrastructure settings**, provide the following:

   a. **DB Instance type**: Select the database instance type from the dropdown menu.

   b. **FSx for ONTAP system**: Create a new FSx for ONTAP file system or use an existing FSx for ONTAP file system.

      i. **Create new FSx for ONTAP**: Enter user name and password.

         A new FSx for ONTAP file system may add 30 minutes or more of installation time.

      ii. **Select an existing FSx for ONTAP**: Select FSx for ONTAP name from the dropdown menu, and enter a user name and password for the file system.

         For existing FSx for ONTAP file systems, ensure the following:

         - The routing group attached to FSx for ONTAP allows routes to the subnets to be used for deployment.
         - The security group allows traffic from the subnets used for deployment, specifically HTTPS (443) and iSCSI (3260) TCP ports.

   c. **Snapshot policy**: Enabled by default. Snapshots are taken daily and have a 7-day retention period.

The snapshots are assigned to volumes created for SQL workloads.

d. **Data drive size**: Enter the data drive capacity and select the capacity unit.

e. **Provisioned IOPS**: Select **Automatic** or **User-provisioned**. If you select **User-provisioned**, enter the IOPS value.

f. **Throughput capacity**: Select the throughput capacity from the dropdown menu.

In certain regions, you may select 4 GBps throughput capacity. To provision 4 GBps of throughput capacity, your FSx for ONTAP file system must be configured with a minimum of 5,120 GiB of SSD storage capacity and 160,000 SSD IOPS.

g. **Encryption**: Select a key from your account or a key from another account. You must enter the encryption key ARN from another account.

FSx for ONTAP custom encryption keys aren't listed based on service applicability. Select an appropriate FSx encryption key. Non-FSx encryption keys will cause server creation failure.

AWS-managed keys are filtered based on service applicability.

h. **Tags**: Optionally, you can add up to 40 tags.

i. **Simple Notification Service**: Optionally, you can enable the Simple Notification Service (SNS) for this configuration by selecting an SNS topic for Microsoft SQL Server from the dropdown menu.

i. Enable the Simple Notification Service.

ii. Select an ARN from the dropdown menu.

j. **CloudWatch monitoring**: Optionally, you can enable CloudWatch monitoring.

We recommend enabling CloudWatch for debugging in case of failure. The events that appear in the AWS CloudFormation console are high-level and don't specify the root cause. All detailed logs are saved in the `C:\cfn\logs` folder in the EC2 instances.

In CloudWatch, a log group is created with the name of the stack. A log stream for every validation node and SQL node appear under the log group. CloudWatch shows script progress and provides information to help you understand if and when deployment fails.

k. **Resource rollback**: This feature isn't currently supported.

8. Summary

a. **Estimated cost**: Provides an estimate of charges that you might incur if you deployed the resources shown.

9. Click **Create** to deploy the new database host.

Alternatively, you can save the configuration.

Step 2: Enable remote connection on the Microsoft SQL Server

After the server deploys, Workload Factory does not enable remote connection on the Microsoft SQL Server. To enable the remote connection, complete the following steps.

Steps

1. Use computer identity for NTLM by referring to Network security: Allow Local System to use computer identity for NTLM in Microsoft documentation.
2. Check dynamic port configuration by referring to A network-related or instance-specific error occurred while establishing a connection to SQL Server in Microsoft documentation.
3. Allow the required client IP or subnet in the security group.

What's next

Now you can create a database in Workload Factory for Databases.

Create a PostgreSQL server in NetApp Workload Factory

Creating a new PostgreSQL server, or database host, in NetApp Workload Factory for Databases requires an FSx for ONTAP file system deployment and resources for Active Directory.

About this task

Before creating a PostgreSQL server from Workload Factory, learn about the available storage deployment types for the database host configuration, workload factory modes of operation, and the requirements to complete this operation.

FSx for ONTAP file system deployments

Creating a new PostgreSQL server requires an FSx for ONTAP file system as the storage backend. You can use an existing FSx for ONTAP file system or create a new file system. If you select an existing FSx for ONTAP file system as your database server storage backend, we create a new storage VM for the PostgreSQL workloads.

+ FSx for ONTAP file systems have two PostgreSQL server deployment models: *High Availability (HA)* or *single instance*. Different resources are created for the FSx for ONTAP file system depending on the FSx for ONTAP deployment model you select.

- **High Availability (HA) deployment**: A Multiple Availability Zone FSx for NetApp ONTAP file system is deployed when a new FSx for ONTAP file system is selected for HA deployment. Separate volumes and LUNs are created for data, log, and tempdb files for an HA deployment. An additional volume and LUN are created for Quorum or witness disk for Windows cluster. HA deployment configures Streaming replication between the primary and secondary PostgreSQL servers.
- **Single instance deployment**: A Single Availability Zone FSx for ONTAP file system is created when a new PostgreSQL server is created. In addition, separate volumes and LUNs are created for data, log, and tempdb files.

Before you begin

You must have grant *database host creation* permissions in your AWS account to create a new database host in workload factory.

Create a PostgreSQL server

You can use *Quick create* or *Advanced create* deployment modes to complete this task in workload factory with *Automate* mode permissions. You can also use the following tools available in the Codebox: REST API, AWS CLI, AWS CloudFormation, and Terraform. Learn how to use Codebox for automation.

When using Terraform from Codebox, the code you copy or download hides `fsxadmin` and `vsadmin` passwords. You'll need to re-enter the passwords when you run the code. You'll need to include the following permissions for the user account in addition to *Automate* mode permissions: `iam:TagRole` and `iam:TagInstanceProfile`. Learn how to use Terraform from Codebox.

Quick create

In *Quick create*, HA is the default deployment model, Windows 2016 is the default Windows version, and SQL 2019 Standard Edition is the default SQL version.

Steps

1. Log in using one of the console experiences.
2. In the Databases tile, select **Deploy host** and then select **PostgreSQL Server** from the menu.
3. Select **Quick create**.
4. Under **Landing zone**, provide the following:
   a. **AWS credentials**: Select AWS credentials with automate permissions to deploy the new database host.

      AWS credentials with *read/write* permissions let workload factory deploy and manage the new database host from your AWS account within workload factory.

      AWS credentials with *read-only* permissions let workload factory generate a CloudFormation template for you to use in the AWS CloudFormation console.

      If you don't have AWS credentials associated in workload factory and you want to create the new server in workload factory, follow **Option 1** to go to the Credentials page. Manually add the required credentials and permissions for *read/write* mode for Database workloads.

      If you want to complete the create new server form in workload factory so you can download a complete YAML file template for deployment in AWS CloudFormation, follow **Option 2** to ensure you have the required permissions to create the new server within AWS CloudFormation. Manually add the required credentials and permissions for *read-only* mode for Database workloads.

      Optionally, you can download a partially completed YAML file template from the Codebox to create the stack outside workload factory without any credentials or permissions. Select **CloudFormation** from the dropdown in the Codebox to download the YAML file.

   b. **Region & VPC**: Select a Region and VPC network.

      Ensure security groups for an existing interface endpoint allow access to HTTPS (443) protocol to the selected subnets.

      AWS service interface endpoints (SQS, FSx, EC2, CloudWatch, CloudFormation, SSM) and the S3 gateway endpoint are created during deployment if not found.

      VPC DNS attributes `EnableDnsSupport` and `EnableDnsHostnames` are modified to enable endpoint address resolution if they aren't already set to `true`.

   c. **Availability zones**: Select availability zones and subnets.

      HA deployments are only supported on Multiple Availability Zone (MAZ) FSx for ONTAP configurations.

      Subnets should not share the same route table for high availability.

i. In the **Cluster configuration - Node 1** field, select the primary availability zone for the MAZ FSx for ONTAP configuration from the **Availability zone** dropdown menu and a subnet from the primary availability zone from the **Subnet** dropdown menu.

ii. In the **Cluster configuration - Node 2** field, select the secondary availability zone for the MAZ FSx for ONTAP configuration from the **Availability zone** dropdown menu and a subnet from the secondary availability zone from the **Subnet** dropdown menu.

5. Under **Application settings**, enter a user name and password for **Database credentials**.
6. Under **Connectivity**, select a key pair to connect securely to your instance.
7. Under **Infrastructure settings**, provide the following:
   a. **FSx for ONTAP system**: Create a new FSx for ONTAP file system or use an existing FSx for ONTAP file system.
      i. **Create new FSx for ONTAP**: Enter user name and password.

      A new FSx for ONTAP file system may add 30 minutes or more of installation time.

      ii. **Select an existing FSx for ONTAP**: Select FSx for ONTAP name from the dropdown menu, and enter a user name and password for the file system.

      For existing FSx for ONTAP file systems, ensure the following:

      - The routing group attached to FSx for ONTAP allows routes to the subnets to be used for deployment.
      - The security group allows traffic from the subnets used for deployment, specifically HTTPS (443) and iSCSI (3260) TCP ports.

   b. **Data drive size**: Enter the data drive capacity and select the capacity unit.
8. Summary:
   a. **Preview default**: Review the default configurations set by Quick create.
   b. **Estimated cost**: Provides an estimate of charges that you might incur if you deployed the resources shown.
9. Click **Create**.

Alternatively, if you want to change any of these default settings now, create the database server with Advanced create.

You can also select **Save configuration** to deploy the host later.

Advanced create

Steps

1. Log in using one of the console experiences.
2. In the Databases tile, select **Deploy host** and then select **PostgreSQL Server** from the menu.
3. Select **Advanced create**.
4. Under **Deployment model**, select **Standalone instance** or **High availability (HA)**.
5. Under **Landing zone**, provide the following:
   a. **AWS credentials**: Select AWS credentials with automate permissions to deploy the new database host.

AWS credentials with *automate* permissions let workload factory deploy and manage the new database host from your AWS account within workload factory.

AWS credentials with *read-only* permissions let workload factory generate a CloudFormation template for you to use in the AWS CloudFormation console.

If you don't have AWS credentials associated in workload factory and you want to create the new server in workload factory, follow **Option 1** to go to the Credentials page. Manually add the required credentials and permissions for *read/write* mode for Database workloads.

If you want to complete the create new server form in workload factory so you can download a complete YAML file template for deployment in AWS CloudFormation, follow **Option 2** to ensure you have the required permissions to create the new server within AWS CloudFormation. Manually add the required credentials and permissions for *read-only* mode for Database workloads.

Optionally, you can download a partially completed YAML file template from the Codebox to create the stack outside workload factory without any credentials or permissions. Select **CloudFormation** from the dropdown in the Codebox to download the YAML file.

b. **Region & VPC**: Select a Region and VPC network.

   Ensure security groups for an existing interface endpoint allow access to HTTPS (443) protocol to the selected subnets.

   AWS Service interface endpoints (SQS, FSx, EC2, CloudWatch, Cloud Formation, SSM) and S3 gateway endpoint are created during deployment if not found.

   VPC DNS attributes `EnableDnsSupport` and `EnableDnsHostnames` are modified to enable resolve endpoint address resolution if not already set to `true`.

c. **Availability zones**: Select availability zones and subnets.

   For single instance deployments

   In the **Cluster configuration - Node 1** field, select an availability zone from the **Availability zone** dropdown menu and a subnet from the **Subnet** dropdown menu.

   For HA deployments

   i. In the **Cluster configuration - Node 1** field, select the primary availability zone for the MAZ FSx for ONTAP configuration from the **Availability zone** dropdown menu and a subnet from the primary availability zone from the **Subnet** dropdown menu.

   ii. In the **Cluster configuration - Node 2** field, select the secondary availability zone for the MAZ FSx for ONTAP configuration from the **Availability zone** dropdown menu and a subnet from the secondary availability zone from the **Subnet** dropdown menu.

d. **Security group**: Select an existing security group or create a new security group.

   Two security groups get attached to the SQL nodes (EC2 instances) during new server deployment.

   1. A workload security group is created to allow ports and protocols required for PostgreSQL.
   2. For a new FSx for ONTAP file system, a new security group is created and attached to the SQL node. For an existing FSx for ONTAP file system, the security group associated with it is

added automatically to the PostgreSQL node which allows communication to the file system.

6. Under **Application settings**, provide the following:
   a. Select the **Operating system** from the dropdown menu.
   b. Select the **PostgreSQL version** from the dropdown menu.
   c. **Database server name**: Enter the database cluster name.
   d. **Database credentials**: Enter a user name and password for a new service account or use existing service account credentials in the Active Directory.
7. Under **Connectivity**, select a key pair to connect securely to your instance.
8. Under **Infrastructure settings**, provide the following:
   a. **DB Instance type**: Select the database instance type from the dropdown menu.
   b. **FSx for ONTAP system**: Create a new FSx for ONTAP file system or use an existing FSx for ONTAP file system.
      i. **Create new FSx for ONTAP**: Enter user name and password.

         A new FSx for ONTAP file system may add 30 minutes or more of installation time.

      ii. **Select an existing FSx for ONTAP**: Select FSx for ONTAP name from the dropdown menu, and enter a user name and password for the file system.

         For existing FSx for ONTAP file systems, ensure the following:

         - The routing group attached to FSx for ONTAP allows routes to the subnets to be used for deployment.
         - The security group allows traffic from the subnets used for deployment, specifically HTTPS (443) and iSCSI (3260) TCP ports.

   c. **Snapshot policy**: Enabled by default. Snapshots are taken daily and have a 7-day retention period.

      The snapshots are assigned to volumes created for PostgreSQL workloads.

   d. **Data drive size**: Enter the data drive capacity and select the capacity unit.
   e. **Provisioned IOPS**: Select **Automatic** or **User-provisioned**. If you select **User-provisioned**, enter the IOPS value.
   f. **Throughput capacity**: Select the throughput capacity from the dropdown menu.

      In certain regions, you may select 4 GBps throughput capacity. To provision 4 GBps of throughput capacity, your FSx for ONTAP file system must be configured with a minimum of 5,120 GiB of SSD storage capacity and 160,000 SSD IOPS.

   g. **Encryption**: Select a key from your account or a key from another account. You must enter the encryption key ARN from another account.

      FSx for ONTAP custom encryption keys aren’t listed based on service applicability. Select an appropriate FSx encryption key. Non-FSx encryption keys will cause server creation failure.

      AWS-managed keys are filtered based on service applicability.

   h. **Tags**: Optionally, you can add up to 40 tags.

i. **Simple Notification Service**: Optionally, you can enable the Simple Notification Service (SNS) for this configuration by selecting an SNS topic for Microsoft SQL Server from the dropdown menu.

   i. Enable the Simple Notification Service.

   ii. Select an ARN from the dropdown menu.

j. **CloudWatch monitoring**: Optionally, you can enable CloudWatch monitoring.

   We recommend enabling CloudWatch for debugging in case of failure. The events that appear in the AWS CloudFormation console are high-level and don't specify the root cause. All detailed logs are saved in the `C:\cfn\logs` folder in the EC2 instances.

   In CloudWatch, a log group is created with the name of the stack. A log stream for every validation node and SQL node appear under the log group. CloudWatch shows script progress and provides information to help you understand if and when deployment fails.

k. **Resource rollback**: This feature isn't currently supported.

9. Summary

   a. **Estimated cost**: Provides an estimate of charges that you might incur if you deployed the resources shown.

10. Click **Create** to deploy the new database host.

    Alternatively, you can save the configuration.

What's next

You can manually configure users, remote access, and databases on the deployed PostgreSQL server.

Manage resources

Resource management in NetApp Workload Factory for Databases

Managing resources in NetApp Workload Factory for Databases allows you to use advanced features including database and clone creation, resource utilization and monitoring. Additionally, you can analyze the well-architected status of your database configurations and implement configuration best practices to improve performance and lower operational costs. Resource management is only for Microsoft SQL Server and Oracle environments running on FSx for ONTAP file system storage.

You must register resources to do any of the following management tasks.

Management tasks include:

- Viewing databases from the Inventory
- Creating a database
- Creating a database clone (sandbox)
- Implementing well-architected database configurations

Register resources in NetApp Workload Factory for Databases

Register instances for Microsoft SQL Server and databases for Oracle so that you can monitor instance and database status, resource utilization, protection, and storage performance in NetApp Workload Factory for Databases.

You can register your resources only if they run on FSx for ONTAP file system storage.

About the task

Registering an instance (SQL Server) or database (Oracle) has three steps - instance or database authentication, FSx for ONTAP authentication, and preparation. Preparation involves making sure that all AWS, NetApp, and PowerShell modules are installed on the instance or database, and that the minimum requirements for Workload Factory for Databases features like error log analysis or well-architected review are met.

Workload Factory supports only Microsoft SQL Server instance and Oracle database registration and management. Depending on the AWS account credentials you select in Workload Factory, PostgreSQL hosts might appear in the Inventory. Currently, Workload Factory supports unregistered PostgreSQL instances running only on Amazon Linux operating systems.

Before you begin

The host for the instance or database must appear in the Inventory. For hosts to appear in the inventory, you must grant *view, planning, and analysis* permissions in your AWS account.

Registering an instance in a private network

To register an instance (SQL Server) or database (Oracle) in a private network with no external connectivity, the following endpoints need to be available in the VPC with association to the subnets where SQL servers are present. Ensure the interface endpoints allow port 443 in the attached Security Group.

- `S3 Gateway/endpoint`
- `ssm`
- `ssmmessages`
- `fsx`

  If you use a proxy server for all outbound connections from EC2 instances, you must allow access to the following domains so that management operations work:

- `.microsoft.com` (SQL Server)
- `.powershellgallery.com` (SQL Server)
- `.aws.amazon.com`
- `.amazonaws.com`

Register a Microsoft SQL Server instance

Registering an instance has three steps - instance authentication, FSx for ONTAP authentication, and preparation to complete missing prerequisites. You can register single or multiple instances.

Workload Factory supports registration for Failover Cluster Instance (FCI) and Standalone deployment for SQL Server.

Steps

1. Log in using one of the console experiences.
2. Select the menu and then select **Databases**.
3. From the Databases menu, select **Inventory**.
4. In the Inventory, select **Microsoft SQL Server** as the engine type.
5. Select the **Instances** tab.
6. Select to register a single instance or multiple instances.
7. To Authenticate instances (step 1), do the following and then select **Next**:
   a. Select to **Use the same credentials for all instances** or **Manage credentials manually**.
   b. Authenticate SQL Server and Windows by providing user name and password information.

      If instances are authenticated, select **Next**.
8. To Authenticate FSx for ONTAP (step 2), do the following:
   a. Select to **Use the same credentials for all resources** or **Manage credentials manually**.
   b. Enter the FSx for ONTAP file system user name and password, and then select **Next**.

      If the FSx for ONTAP file system is authenticated, select **Next**.
9. To Prepare (step 3), make sure the instance(s) meets the minimum requirements.

   To meet the minimum requirements, the instance must have AWS and NetApp PowerShell modules and PowerShell 7 modules installed, and you must complete the prerequisites for at least one of the capabilities listed under Prerequisite check.

   a. Review the prerequisites in the **Prerequisite check view**.

      You must complete all prerequisites for a single capability like **Review well-architected issues and recommendations** to register the instance.

   b. Select **Setup details** for each capability to learn about the capability prerequisites and follow the on-screen instructions to complete any missing prerequisites for a capability.

      To have Workload Factory review and fix well-architected issues for your instances, complete all prerequisites listed under **Review well-architected issues and recommendations** and **Fix well-architected issues** capabilities.
10. When prerequisites are complete, **Register** the instance(s).

Result

Instance registration initiates. Select the **Job monitoring** tab to track progress.

Register an Oracle database

Registering an instance has three steps - database authentication, FSx for ONTAP authentication, and preparation to complete missing prerequisites. You can register single or multiple databases.

Steps

1. Log in using one of the console experiences.
2. Select the menu and then select **Databases**.
3. From the Databases menu, select **Inventory**.
4. In the Inventory, select **Oracle** as the engine type.
5. Select the **Databases** tab.
6. Select to register a single database or multiple databases.
7. To Authenticate databases (step 1), do the following:
   - Select to **Use the same credentials for all instances** or **Manage credentials manually**.
   - Authenticate Oracle user and Automatic Storage Management (ASM) grid user (if applicable) by providing user name and password information.

     If databases are authenticated, select **Next**.
8. To Authenticate FSx for ONTAP (step 2), do the following and then select **Next**:
   - Select to **Use the same credentials for all resources** or **Manage credentials manually**.
   - Enter the FSx for ONTAP file system user name and password.

     If the FSx for ONTAP file system is authenticated, select **Next**.
9. To Prepare (step 3), make sure the database(s) meets required prerequisites. If all required modules are installed and prerequisites are met, select **Next** to register the database. Otherwise, follow these steps.
   a. Review the prerequisites in the **Prerequisite check view**.

      You must complete all prerequisites for a single capability like **Review well-architected issues and recommendations** to register the database.

   b. Select **Setup details** for each capability to learn about the capability prerequisites and follow the on-screen instructions to complete any missing prerequisites for a capability.

      To have Workload Factory review and fix well-architected issues for your databases, complete all prerequisites listed under **Review well-architected issues and recommendations** and **Fix well-architected issues** capabilities.
10. When prerequisites are complete, **Register** the database(s).

Result

Database registration initiates. Select the **Job monitoring** tab to track progress.

What's next

After resource registration, you can perform the following tasks.

- View databases from the inventory
- Create a database
- Create a database clone (sandbox)
- Implement well-architected database configurations

Create a Microsoft SQL database in NetApp Workload Factory for Databases

Creating a new Microsoft SQL database enables you to manage the resource within NetApp Workload Factory for Databases.

About this task

Upon database creation, two new volumes are created in the FSx for ONTAP file system consisting of independent LUNs to host data and log files for the database. The database files in the new database are thin-provisioned and consume only a few MBs of the total size allocated for the new database.

If you want to segregate storage for the database, you can do this by using a *virtual mount point*. The virtual mount point lets you consolidate databases to a few common drives on the host.

Creating a database in workload factory requires *view, planning, and analysis* permissions. Alternatively, you can copy or download a partially completed code template to complete the operation outside workload factory. Learn about Workload Factory permissions to decide which mode you'd like to use.

Microsoft SQL Servers using SMB protocol don't support database creation.

Before you begin

Ensure you complete the following prerequisites before you create a new database.

- **Credentials and permissions**: You must have AWS account credentials and *view, planning, and analysis* permissions to create a new database in Workload Factory.

  Alternatively, you can use the Codebox to copy a template so that you can deploy a database outside of workload factory using REST API. Learn more about Codebox automation.

- **Windows host**: You must have enough drive letters available on the Microsoft SQL Server to create new drives for the new database if you use *Quick create* mode.
- **Microsoft SQL Server**: You must have a managed Microsoft SQL Server in workload factory for Databases to host the new database.
- **AWS Systems Manager**: Ensure the `NT Authority\SYSTEM` user privilege is enabled in the Microsoft SQL host via AWS Systems Manager.

Create a database

You can use *Quick create* or *Advanced create* deployment modes to complete this task in Workload Factory.

Quick create

Steps

1. Log in using one of the console experiences.
2. Select the menu and then select **Databases**.
3. From the Databases menu, select **Inventory**.
4. In the Inventory, select **Microsoft SQL Server** as the database engine type.
5. Select a database server with a managed SQL server instance to create the database in.
6. Click the action menu of the managed instance and then select **Create user database**.
7. On the Create user database page, under Database information, provide the following:
   a. **Database name**: Enter name for the database.
   b. **Collation**: Select a collation for the database. The default collation SQL_Latin1_General_CP1_CI_AS" on Microsoft SQL Server is selected.
8. Under File settings, provide the following:
   a. **File settings mode**: Select **Quick create**.
   b. **File names & path**:
      - **Data file name**: Enter the data file name.
      - **Log file name**: Enter the log file name.
   c. **File sizes**: Enter the data size and log size for the database.
9. Click **Create**.

   Alternatively, if you want to change any of these default settings now, change the **File settings mode** to **Advanced create**.

Advanced create

Steps

1. Log in using one of the console experiences.
2. Select the menu and then select **Databases**.
3. From the Databases menu, select **Inventory**.
4. In the Inventory, select **Microsoft SQL Server** as the database engine type.
5. Select a database server with a managed SQL server instance to create the database in.
6. Click the action menu of the managed instance and then select **Create user database**.
7. Select **Create user database**.
8. On the Create user database page, under Database information, provide the following:
   a. **Database name**: Enter name for the database.
   b. **Collation**: Select the collation for the database. The default collation SQL_Latin1_General_CP1_CI_AS" on Microsoft SQL Server is selected.
9. Under File settings, provide the following:
   a. **File settings mode**: Select **Advanced create**.
   b. **File names & path**:

i. **Data file**: Select a drive letter and enter the data file name.

   Optionally, click the box for **Virtual mount point**.

ii. **Log file**: Select a drive letter and enter the log file name.

   Optionally, click the box for **Virtual mount point**.

c. **File sizes**: Enter the data size and log size for the database.

10. Click **Create**.

If you created the database host, you can check the job's progress in the **Job monitoring** tab.

Create a sandbox clone in NetApp Workload Factory for Databases

Creating a sandbox clone of a database in NetApp Workload Factory for Databases lets you use the clone for development, testing, integration, analytics, training, QA, and more without altering the source database.

About this task

A sandbox clone is created from the most recent snapshot on the source database. It may be cloned in the same Microsoft SQL Server as the source database or cloned in another Microsoft SQL Server as long as they share the same FSx for ONTAP file system.

Before you begin

Ensure you complete the following prerequisites before you create a sandbox clone.

- **Credentials and permissions**: You must have AWS account credentials and *view, planning, and analysis* permissions to create a sandbox clone in Workload Factory.

  Alternatively, you can use the Codebox to copy a partially completed template or create a completed template so that you can create the sandbox clone outside of Workload Factory using REST API. Learn more about Codebox automation.

- **Microsoft SQL Server**: You must have a managed Microsoft SQL Server in Workload Factory for Databases to host the new sandbox clone.
- **AWS Systems Manager**: Ensure the `NT Authority\SYSTEM` user privilege is enabled in the Microsoft SQL host via AWS Systems Manager.
- **Source database**: You need a source database available for the clone.

Steps

1. Log in using one of the console experiences.
2. Select the menu and then select **Databases**.
3. In Databases, select the **Sandboxes** tab.
4. In the Sandboxes tab, select **Create new sandbox**.
5. On the Create new sandbox page, under Database source, provide the following:
   a. **Source database host**: Select the source database host.
   b. **Source database instance**: Select the source database instance.

c. **Source database**: Select the source database to clone from.

6. Under Database target, provide the following:
   a. **Target database host**: Select a target database host for the sandbox clone that is in the same VPC and has the same FSx for ONTAP file system as the source host.
   b. **Target database instance**: Select the target database instance for the sandbox clone.
   c. **Target database**: Enter a name for the sandbox clone.
7. **Mount**: When cloning a SQL database that has multiple data and/or log files, Workload Factory clones all files under the auto-assigned or defined drive letter.

   Select one of the following options:

   a. **Auto-assign mount point**
   b. **Define mount point path**

      Provide the following to define the mount point path:

      - Enter the drive letter for the data file path.
      - Enter the drive letter for the log file path.
8. **Define tag**: Select a tag to define the sandbox clone.
9. Click **Create**.

To check the job's progress, go to the **Job monitoring** tab.

Automate with Codebox in NetApp Workload Factory for Databases

You can automate host deployment, database creation, and more with Codebox in NetApp Workload Factory for Databases. Codebox is an infrastructure as code (IaC) co-pilot that helps you generate code to execute any operations supported by Workload Factory.

Learn more about Codebox automation and how to use it.

Protect Microsoft SQL Server workloads

Protect your Microsoft SQL Server applications data using NetApp Backup and Recovery from the Workload Factory console. With this integration, you can achieve the following protection goals: back up workloads with local snapshots on local primary Amazon FSx for NetApp ONTAP (FSx for ONTAP) storage, and replicate workloads to secondary FSx for ONTAP storage.

About this task

Workload Factory automates discovering resources, validating prerequisites, and configuring and installing the Plug-in for Microsoft SQL Server to prepare for protecting your workloads with NetApp Backup and Recovery. The plug-in is a host-side component of NetApp Software that enables you to protect your Microsoft SQL

Server workloads.

NetApp Backup and Recovery leverages NetApp SnapMirror data replication technology to ensure that all the backups are fully synchronized by creating snapshot copies and transferring them to the backup locations.

For details about protection with Backup and Recovery, refer to the Protect Microsoft SQL workloads overview with Backup and Recovery.

Before you begin

The following requirements must be met to protect Microsoft SQL Server workloads with Backup and Recovery.

- Ensure that your environment meets the Backup and Recovery SQL Server requirements.
- Complete NetApp Console requirements including setting up, assigning IAM roles, and installing a Console agent.

If you have organization administrator access to the NetApp account, the `backup and recovery super admin` role is automatically assigned when you prepare for protection with NetApp Backup and Recovery.

- Set the host resolution on the Connector

  To discover databases, you must set host resolution on the Connector. On the hosted device, add the mapping of the IP address to the hostname in the `/etc/hosts` file.

  - Set up licensing for NetApp Backup and Recovery

Prepare for protection with NetApp Backup and Recovery

Complete the preparation process to protect your Microsoft SQL Server resources with NetApp Backup and Recovery.

Steps

1. Log in using one of the console experiences.
2. Select the menu and then select **Databases**.
3. From the Databases menu, select **Inventory**.
4. In the Inventory, select **Microsoft SQL Server** as the engine type.
5. Locate the instance that you want to protect, and then select **Protect** from the menu.
6. If prompted, provide Windows credentials with administrative access.

   To use NetApp Backup and Recovery for protection, SQL Server instances must be registered in Workload Factory with Windows credentials.

7. If several Console agents are active and available, select the **Console agent** where you want the workload to be registered and protected.
8. To prepare for data protection, Workload Factory automatically registers your SQL Server resources in Backup and Recovery, configures and installs the Plug-in for Microsoft SQL Server, and discovers resources to meet the prerequisites for protecting your SQL Server instance. Select **Start** to begin the process.
9. After meeting the prerequisites, select **Redirect** to access Backup and Recovery.

What's next

From Backup and Recovery, create a policy to protect your Microsoft SQL Server instance and databases.

Learn how to create a policy to protect your Microsoft SQL Server instance and databases.

For related information, refer to the Backup and Recovery documentation for managing Microsoft SQL Server workloads.

Edit protection for Microsoft SQL Server resources

You can edit protection for Microsoft SQL Server instances and databases that are already protected in NetApp Backup and Recovery. Editing protection allows you to modify the protection policy or schedule for your protected SQL Server instances.

1. Log in using one of the console experiences.
2. Select the menu and then select **Databases**.
3. From the Databases menu, select **Inventory**.
4. In the Inventory, select **Microsoft SQL Server** as the engine type.
5. Select the **Databases** tab.
6. Locate the database to edit protection for, and then select **Edit protection** from the menu.

   You'll be redirected to Backup and Recovery in the NetApp Console where you can modify the protection policy or schedule.

Copyright information

Trademark information