



Datenbankressourcen erstellen

Workload Factory for NetApp Console

NetApp
October 07, 2026

Inhalt

- Datenbankressourcen erstellen 1
 - Erstellen eines Microsoft SQL Servers in NetApp Workload Factory für Datenbanken 1
 - Über diese Aufgabe 1
 - Bevor Sie beginnen 2
 - Schritt 1: Einen Datenbankserver erstellen 2
 - Schritt 2: Aktivierung der Remote-Verbindung auf dem Microsoft SQL Server 10
 - Einen PostgreSQL-Server in der NetApp Workload Factory für Datenbanken erstellen 10
 - Über diese Aufgabe 11
 - Bevor Sie beginnen 11
 - Einen PostgreSQL-Server erstellen 11
 - Erstellen einer Microsoft SQL Datenbank in NetApp Workload Factory for Databases 17
 - Erstellen einer Datenbank 18
 - Erstellung eines Sandbox-Klons in NetApp Workload Factory for Databases 19

Datenbankressourcen erstellen

Erstellen eines Microsoft SQL Servers in NetApp Workload Factory für Datenbanken

Die Erstellung eines neuen Microsoft SQL Server oder Datenbankhosts in Workload Factory for Databases erfordert ein FSx for ONTAP Dateisystem Deployment und Ressourcen für Active Directory.

Über diese Aufgabe

Vor dem Erstellen eines Microsoft SQL Server aus Workload Factory sollten die verfügbaren Storage Deployment-Typen für die Datenbankhostkonfiguration, die Microsoft Multi-path I/O-Konfiguration, das Active Directory-Deployment, die Netzwerkdetails und die Anforderungen für den Abschluss dieses Vorgangs bekannt sein.

Nach dem Deployment sind [Aktivierung der Remoteverbindung auf dem Microsoft SQL Server](#) erforderlich.

FSx for ONTAP Dateisystem Deployments

Zum Erstellen eines neuen Microsoft SQL Server ist ein FSx for ONTAP Dateisystem als Storage-Backend erforderlich. Sie können ein vorhandenes FSx for ONTAP Dateisystem verwenden oder ein neues Dateisystem erstellen. Wenn Sie ein vorhandenes FSx for ONTAP Dateisystem als Storage-Backend für Ihren Datenbankserver auswählen, erstellen wir eine neue Storage VM für die Microsoft SQL Workloads.

FSx for ONTAP-Dateisysteme verfügen über zwei Microsoft SQL Server Deployment-Modelle: *Failover Cluster Instance (FCI)* oder *Standalone*. Je nach ausgewähltem FSx for ONTAP Deployment-Modell werden für das FSx for ONTAP-Dateisystem unterschiedliche Ressourcen erstellt.

- **Failover Cluster Instance (FCI) Microsoft SQL Deployment:** Bei Auswahl eines neuen FSx for ONTAP Dateisystems für das FCI Deployment wird ein FSx for NetApp ONTAP Dateisystem mit Multiple Availability Zone bereitgestellt. Für ein FCI Deployment werden separate Volumes und LUNs für Daten-, Protokoll- und tempdb-Dateien erstellt. Für den Windows-Cluster werden zusätzlich ein weiteres Volume und eine weitere LUN als Quorum- oder Zeugendatenträger erstellt.
- **Eigenständiges Microsoft SQL Deployment:** Beim Erstellen eines neuen Microsoft SQL Server wird ein FSx for ONTAP Dateisystem mit einer Single Availability Zone erstellt. Zusätzlich erstellt das System separate Volumes und LUNs für Daten-, Protokoll- und tempdb-Dateien.

Microsoft Multi-path I/O Konfiguration

Beide Deployment Modelle für Microsoft SQL Server erfordern die Erstellung von LUNs mithilfe des iSCSI Storage Protokolls. Workload Factory konfiguriert Microsoft Multi-path I/O (MPIO) im Rahmen der Konfiguration von LUNs für SQL Server über FSx for ONTAP. MPIO wird auf der Grundlage von Best Practices von AWS und NetApp konfiguriert.

Weitere Informationen sind unter ["SQL Server Hochverfügbarkeits-Deployments mit Amazon FSx for NetApp ONTAP"](#) verfügbar.

Active Directory

Für Active Directory (AD) tritt während des Deployments Folgendes auf:

- Wenn kein vorhandenes SQL-Dienstkonto angegeben wird, wird in der Domäne ein neues Microsoft SQL-Dienstkonto erstellt.

- Der Windows-Cluster, die Knotenhostnamen und der Microsoft SQL FCI-Name werden dem Microsoft SQL-Dienstkonto als verwaltete Computer hinzugefügt.
- Dem Windows Clustereintrag werden Berechtigungen zum Hinzufügen von Computern zur Domäne zugewiesen.

Benutzerverwaltete Active Directory-Sicherheitsgruppen

Wenn Sie während des Microsoft SQL Server Deployments in Workload Factory „user-managed Active Directory“ auswählen, müssen Sie eine Sicherheitsgruppe angeben, die den Datenverkehr zwischen den EC2-Instanzen und dem Verzeichnisdienst für das Deployment ermöglicht. Workload Factory ordnet die Sicherheitsgruppe für user-managed Active Directory nicht automatisch zu, wie dies bei AWS Managed Microsoft AD der Fall ist.

Rollback der Ressource

Wenn Sie ein Rollback Ihrer Domain Name System (DNS)-Ressourcen durchführen, werden die Ressourceneinträge in AD und DNS nicht automatisch entfernt. Die Einträge können wie folgt vom DNS-Server und aus AD entfernt werden.

- Bei benutzerverwaltetem AD zunächst ["Entfernen des AD-Computers"](#). Anschließend erfolgt über den DNS-Manager die Verbindung zum DNS-Server, und ["Löschen der DNS-Ressourceneinträge"](#).
- Für AWS Managed Microsoft AD ["Installation der AD-Verwaltungstools"](#). Als Nächstes ["Entfernen des AD-Computers"](#). Zum Schluss erfolgt über den DNS-Manager die Verbindung mit dem DNS-Server und ["Löschen der DNS-Ressourceneinträge"](#).

Bevor Sie beginnen

Vor der Erstellung eines neuen Datenbankhosts müssen die folgenden Voraussetzungen erfüllt sein.

Anmeldeinformationen und Berechtigungen

Sie müssen ["Berechtigungen für die Erstellung des Datenbankhosts"](#) in Ihrem AWS-Konto einen neuen Datenbankhost in Workload Factory erstellen.

Active Directory

Für die Verbindung mit Active Directory benötigen Sie Administratorrechte mit folgenden Berechtigungen:

- Beitritt zur Domäne
- Erstellung von Computerobjekten
- Objekte in der Standard-Organisationseinheit (OU) erstellen
- Alle Eigenschaften auslesen
- Der Domänenbenutzer muss auf den AD-Knoten über lokale Administratorrechte verfügen.
- Erstellung eines Microsoft SQL Server-Dienstbenutzers in AD, falls noch keiner vorhanden ist

Schritt 1: Einen Datenbankserver erstellen

Zum Abschließen dieser Aufgabe in Workload Factory mit Berechtigungen für den Modus *Automate* können die Deployment-Modi *Quick create* oder *Advanced create* verwendet werden. Außerdem können die folgenden in der Codebox verfügbaren Tools verwendet werden: REST API, AWS CLI, AWS CloudFormation und Terraform. ["Informationen zur Verwendung von Codebox für die Automatisierung"](#).



Wenn Sie Terraform aus Codebox verwenden, blendet der Code, den Sie kopieren oder herunterladen, `fsxadmin` und `vsadmin` Passwörter aus. Bei der Ausführung des Codes

müssen Sie die Passwörter erneut eingeben. Zusätzlich zu den Berechtigungen für den *Automate*-Modus benötigt das Benutzerkonto die folgenden Berechtigungen: `iam:TagRole` und `iam:TagInstanceProfile`. ["Informationen zur Verwendung von Terraform aus Codebox"](#).

Während des Deployments aktiviert Workload Factory CredSSP für die Delegierung von Anmeldeinformationen an Skripte zur Provisionierung von SQL. Wenn die Gruppenrichtlinie die CredSSP-Delegierung für alle Domänencomputer blockiert, schlägt das Deployment fehl. Nach dem Deployment deaktiviert Workload Factory CredSSP.

Schnellerstellung



In *Quick create* ist FCI das standardmäßige Deployment-Modell, Windows 2016 die Standard-Windows-Version und SQL 2019 Standard Edition die Standard-SQL-Version.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. In der Datenbankübersicht erfolgt die Auswahl von **Deploy host** und anschließend von **Microsoft SQL Server** im Menü.
4. Die Option **Quick create** auswählen.
5. Unter **AWS settings** sind folgende Angaben erforderlich:

- a. **AWS-Anmeldeinformationen:** Auswahl von AWS-Anmeldeinformationen mit automatisierten Berechtigungen zum Einsetzen des neuen Datenbankhosts.

AWS-Anmeldeinformationen mit Berechtigungen zum Erstellen von Datenbankhosts ermöglichen es Workload Factory, den neuen Datenbankhost über Ihr AWS-Konto innerhalb von workload factory einzusetzen und zu managen.

AWS-Anmeldeinformationen mit den Berechtigungen *view, planning und analysis* ermöglichen es Workload Factory, eine CloudFormation Vorlage zu generieren, die in der AWS CloudFormation Konsole verwendet werden kann.

Wenn in Workload Factory keine AWS-Anmeldeinformationen verknüpft sind und der neue Server in Workload Factory erstellt werden soll, ist **Option 1** zu verwenden, um zur Seite „Anmeldeinformationen“ zu gelangen. Dort erfolgt das manuelle Hinzufügen der erforderlichen Anmeldeinformationen und der Berechtigungen für die *Erstellung von Datenbankhosts* bei Datenbank-Workloads.

Wenn Sie das Formular zum Erstellen eines neuen Servers in Workload Factory ausfüllen möchten, um eine vollständige YAML-Dateivorlage für das Deployment in AWS CloudFormation herunterzuladen, ist **Option 2** zu verwenden, damit die erforderlichen Berechtigungen zum Erstellen des neuen Servers in AWS CloudFormation vorhanden sind. Die erforderlichen Anmeldeinformationen sowie die Berechtigungen für *Ansicht, Planung und Analyse* für Datenbank-Workloads sind manuell hinzuzufügen.

Optional können Sie eine teilweise ausgefüllte YAML-Dateivorlage aus der Codebox herunterladen, um den Stack außerhalb von Workload Factory ohne Anmeldeinformationen oder Berechtigungen zu erstellen. Für den Download der YAML-Datei steht in der Codebox im Dropdown-Menü **CloudFormation** zur Auswahl.

b. **Region & VPC:** Auswahl einer Region und eines VPC-Netzwerks.

Es ist sicherzustellen, dass Deployment-Subnetze vorhandenen Schnittstellenendpunkten zugeordnet sind und dass Sicherheitsgruppen den Zugriff auf das HTTPS-Protokoll (443) für die ausgewählten Subnetze ermöglichen.

AWS-Service-Schnittstellenendpunkte (SQS, FSx, EC2, CloudWatch, CloudFormation, SSM) und der S3-Gateway-Endpunkt werden während des Deployments erstellt, sofern sie nicht gefunden werden.

VPC DNS Attribute `EnableDnsSupport` und `EnableDnsHostnames` werden so geändert, dass die Auflösung von Endpunktadressen aktiviert wird, falls sie nicht bereits auf `true` gesetzt sind.

Bei Verwendung eines VPC-übergreifenden DNS muss die Sicherheitsgruppe für Endpunkte in der anderen VPC, in der sich das DNS befindet, Port 443 für Deployment Subnetze zulassen. Andernfalls ist beim Beitritt zu einem VPC-übergreifenden Active Directory ein DNS-Resolver aus der lokalen VPC bereitzustellen. In einer Umgebung mit mehreren replizierten Domain Controllers kann, wenn einige Domain Controllers vom Subnetz aus nicht erreichbar sind, **Zu CloudFormation umleiten** ausgewählt und `Preferred domain controller` eingegeben werden, um die Verbindung zu Active Directory herzustellen.

c. **Verfügbarkeitszonen:** Verfügbarkeitszonen und Subnetze werden gemäß dem Failover Cluster Instance (FCI) Deployment-Modell ausgewählt.



FCI Deployments werden nur auf FSx for ONTAP Konfigurationen mit Multiple Availability Zone (MAZ) unterstützt.

- i. Im Feld **Clusterkonfiguration - Knoten 1** erfolgt die Auswahl der primären Verfügbarkeitszone für die MAZ FSx for ONTAP Konfiguration aus dem Dropdown-Menü **Verfügbarkeitszone** sowie eines Subnetzes aus der primären Verfügbarkeitszone aus dem Dropdown-Menü **Subnetz**.
- ii. Im Feld **Clusterkonfiguration - Knoten 2** wird die sekundäre Availability Zone für die MAZ FSx for ONTAP Konfiguration im Dropdown-Menü **Availability zone** ausgewählt sowie ein Subnetz aus der sekundären Availability Zone im Dropdown-Menü **Subnet**.

6. Unter **Anwendungseinstellungen** werden ein Benutzername und ein Passwort für die **Datenbankzugangsdaten** eingegeben.

Für GovCloud-Konten geben Sie den Wert für den AWS SSM Parameter-ARN im folgenden Format ein: `{fsx:{"username":"fsxadmin","password":"pass"}}`.

Der Wert wird im Parameter Store unter Parameterdetails in der AWS Management Console bereitgestellt. Der AWS SSM-Parametertyp muss „Secure String“ sein, mit dem Namen im Format `/netapp/wlmdb/<anyname>`. Weitere Informationen zum Abrufen von SSM-Parametern finden Sie unter ["AWS GovCloud-Dokumentation"](#).

7. Unter **Konnektivität** sind folgende Angaben erforderlich:

a. **Schlüsselpaar:** Auswahl eines Schlüsselpaars.

b. **Active Directory:**

- i. Im Feld **Domänenname** wird ein Name für die Domäne ausgewählt oder eingegeben.
 - A. Bei AWS-verwalteten Active Directories erscheinen Domännennamen im Dropdown-Menü.
 - B. Bei einem benutzerverwalteten Active Directory erfolgt die Eingabe eines Namens im Feld

Suchen und Hinzufügen; anschließend wird **Hinzufügen** ausgewählt.

- ii. Im Feld **DNS-Adresse** wird die DNS-IP-Adresse für die Domain eingegeben. Es können bis zu 3 IP-Adressen hinzugefügt werden.

Bei von AWS verwalteten Active Directories werden die DNS-IP-Adressen im Dropdown-Menü angezeigt.

- iii. Im Feld **Benutzername** ist der Benutzername für die Active Directory-Domäne einzugeben.
- iv. Im Feld **Passwort** geben Sie ein Passwort für die Active Directory-Domäne ein.

Für GovCloud-Konten geben Sie den AWS SSM Parameter-ARN-Wert für Active Directory-Anmeldeinformationen im folgenden Format ein:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Der AWS SSM-Parametertyp muss „Secure String“ sein, mit dem Namen im Format `/netapp/wlmdb/<anyname>`.

Weitere Informationen zum Abrufen von SSM-Parametern finden Sie unter ["AWS GovCloud-Dokumentation"](#).

8. Unter **Infrastruktureinstellungen** sind die folgenden Angaben erforderlich:

- a. **FSx for ONTAP System**: Ein neues FSx for ONTAP Dateisystem erstellen oder ein vorhandenes FSx for ONTAP Dateisystem verwenden.

- i. **Neues FSx for ONTAP erstellen**: Eingabe von Benutzername und Passwort.

Für GovCloud-Konten geben Sie den AWS SSM Parameter-ARN-Wert für FSx for ONTAP-Anmeldeinformationen im folgenden Format ein:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Der AWS SSM-Parametertyp muss „Secure String“ sein, mit dem Namen im Format `/netapp/wlmdb/<anyname>`.

Weitere Informationen zum Abrufen von SSM-Parametern finden Sie unter ["AWS GovCloud-Dokumentation"](#).

Ein neues FSx for ONTAP Dateisystem kann die Installationszeit um 30 Minuten oder mehr verlängern.

- i. **Vorhandenes FSx für ONTAP**: Wählen Sie den FSx für ONTAP Namen aus und geben Sie einen Benutzernamen und ein Passwort für das Dateisystem ein.

Für bestehende FSx for ONTAP Dateisysteme sind die folgenden Punkte zu beachten:

- Die an FSx for ONTAP angehängte Routing-Gruppe ermöglicht, Routen zu den Subnetzen für das Deployment zu verwenden.
- Die Sicherheitsgruppe erlaubt Datenverkehr aus den für das Deployment verwendeten Subnetzen, insbesondere über die TCP-Ports HTTPS (443) und iSCSI (3260).

- b. **Datenträgergröße**: Die Kapazität des Datenträgers und die Kapazitätseinheit angeben.

9. Zusammenfassung:

- a. **Vorschau der Standardeinstellungen**: Prüfung der von Quick create festgelegten Standardkonfigurationen.
- b. **Geschätzte Kosten**: Enthält eine Schätzung der Kosten, die Ihnen entstehen könnten, wenn Sie die angezeigten Ressourcen einsetzen.

10. Klicken Sie auf **Create**.

Alternativ können Sie, falls Sie eine dieser Standardeinstellungen jetzt ändern möchten, den

Datenbankserver mit Advanced create erstellen.

Sie können auch **Konfiguration speichern** auswählen, um den Host später einzusetzen.

Erweiterte Erstellung

Schritte

1. Melden Sie sich bei der "NetApp Console" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. In der Datenbankübersicht erfolgt die Auswahl von **Deploy host** und anschließend von **Microsoft SQL Server** im Menü.
4. **Advanced create** ist auszuwählen.
5. Für **Deployment-Modell** stehen **Failover Cluster Instance** oder **Single instance** zur Auswahl.
6. Unter **AWS settings** sind folgende Angaben erforderlich:
 - a. **AWS-Anmeldeinformationen**: Auswahl von AWS-Anmeldeinformationen mit automatisierten Berechtigungen zum Einsetzen des neuen Datenbankhosts.

AWS-Anmeldeinformationen mit Berechtigungen zum Erstellen von Datenbankhosts ermöglichen es Workload Factory, den neuen Datenbankhost über Ihr AWS-Konto innerhalb von workload factory einzusetzen und zu managen.

AWS-Anmeldeinformationen mit den Berechtigungen *view, planning und analysis* ermöglichen es Workload Factory, eine CloudFormation Vorlage zu generieren, die in der AWS CloudFormation Konsole verwendet werden kann.

Wenn in Workload Factory keine AWS-Anmeldeinformationen verknüpft sind und der neue Server in Workload Factory erstellt werden soll, ist **Option 1** zu verwenden, um zur Seite „Anmeldeinformationen“ zu gelangen. Dort erfolgt das manuelle Hinzufügen der erforderlichen Anmeldeinformationen und der Berechtigungen für die *Erstellung von Datenbankhosts* bei Datenbank-Workloads.

Wenn Sie das Formular zum Erstellen eines neuen Servers in Workload Factory ausfüllen möchten, um eine vollständige YAML-Dateivorlage für das Deployment in AWS CloudFormation herunterzuladen, ist **Option 2** zu verwenden, damit die erforderlichen Berechtigungen zum Erstellen des neuen Servers in AWS CloudFormation vorhanden sind. Die erforderlichen Anmeldeinformationen sowie die Berechtigungen für *Ansicht, Planung und Analyse* für Datenbank-Workloads sind manuell hinzuzufügen.

Optional können Sie eine teilweise ausgefüllte YAML-Dateivorlage aus der Codebox herunterladen, um den Stack außerhalb von Workload Factory ohne Anmeldeinformationen oder Berechtigungen zu erstellen. Für den Download der YAML-Datei steht in der Codebox im Dropdown-Menü **CloudFormation** zur Auswahl.

- b. **Region & VPC**: Auswahl einer Region und eines VPC-Netzwerks.

Sicherheitsgruppen für einen vorhandenen Schnittstellenendpunkt müssen den Zugriff über das HTTPS-Protokoll (443) auf die ausgewählten Subnetze zulassen.

AWS Service-Schnittstellenendpunkte (SQS, FSx, EC2, CloudWatch, Cloud Formation, SSM) und der S3-Gateway-Endpunkt werden während des Deployment erstellt, wenn sie nicht gefunden werden.

Die VPC-DNS-Attribute `EnableDnsSupport` und `EnableDnsHostnames` werden so geändert, dass die Auflösung von Endpunktadressen ermöglicht wird, falls sie nicht bereits auf `true` festgelegt sind.

- c. **Verfügbarkeitszonen:** Verfügbarkeitszonen und Subnetze sind entsprechend dem ausgewählten Deployment-Modell auszuwählen. Subnetze sollten aus Gründen der Hochverfügbarkeit nicht dieselbe Routingtabelle verwenden.



FCI Deployments werden nur auf FSx for ONTAP Konfigurationen mit Multiple Availability Zone (MAZ) unterstützt.

- Für Einzelinstanzbereitstellungen:
 - Im Feld **Clusterkonfiguration - Knoten 1** stehen im Dropdown-Menü **Verfügbarkeitszone** eine Verfügbarkeitszone und im Dropdown-Menü **Subnetz** ein Subnetz zur Auswahl.
- Für FCI Deployments:
 - Im Feld **Clusterkonfiguration - Knoten 1** erfolgt die Auswahl der primären Verfügbarkeitszone für die MAZ FSx for ONTAP Konfiguration aus dem Dropdown-Menü **Verfügbarkeitszone** sowie eines Subnetzes aus der primären Verfügbarkeitszone aus dem Dropdown-Menü **Subnetz**.
 - Im Feld **Clusterkonfiguration - Knoten 2** wird die sekundäre Availability Zone für die MAZ FSx for ONTAP Konfiguration im Dropdown-Menü **Availability zone** ausgewählt sowie ein Subnetz aus der sekundären Availability Zone im Dropdown-Menü **Subnet**.

- d. **Sicherheitsgruppe:** Eine Arbeitslast-Sicherheitsgruppe wird erstellt, um die für die Kommunikation zwischen Microsoft SQL und Windows-Cluster auf den Knoten erforderlichen Ports und Protokolle zuzulassen. Zusätzlich können Sie eine oder mehrere Sicherheitsgruppen auswählen.

7. Unter **Anwendungseinstellungen** sind folgende Angaben erforderlich:

- a. Unter **SQL Server Installationsart** erfolgt die Auswahl von **License included AMI** oder **Use custom AMI**.
- i. Bei Auswahl von **License included AMI** sind folgende Angaben erforderlich:
- A. **Betriebssystem:** Zur Auswahl stehen **Windows server 2016**, **Windows server 2019** oder **Windows server 2022**.
 - B. **Datenbankedition:** Zur Auswahl stehen **SQL Server Standard Edition** oder **SQL Server Enterprise Edition**.
 - C. **Datenbankversion:** Zur Auswahl stehen **SQL Server 2016**, **SQL Server 2019** oder **SQL Server 2022**.
 - D. **SQL Server AMI:** Auswahl eines SQL Server AMI aus dem Dropdown-Menü.
- ii. Wenn **Benutzerdefiniertes AMI verwenden** ausgewählt wird, erfolgt die Auswahl eines AMI im Dropdown-Menü.
- b. **SQL Server Sortierung:** Auswahl eines Sortierungssatzes für den Server.



Falls die ausgewählte Kollation für die Installation nicht kompatibel ist, empfehlen wir Ihnen, die Standardkollation „SQL_Latin1_General_CP1_CI_AS“ auszuwählen.

- c. **Datenbankname:** Eingabe des Namens des Datenbankclusters.

- d. **Datenbank-Anmeldeinformationen:** Eingabe eines Benutzernamens und Kennworts für ein neues Dienstkonto oder Verwendung der Anmeldedaten eines vorhandenen Dienstkontos im Active Directory.

Optional: Auswahl von **Use managed service account** für das SQL Server-Dienstkonto. Diese Option eignet sich, wenn Ihre Umgebung MSA (Managed Service Account) oder Group Managed Service Accounts (gMSA) verwendet und die Kennwortverwaltung von Active Directory übernommen wird.

Für GovCloud-Konten geben Sie den Wert für den AWS SSM Parameter-ARN im folgenden Format ein: `{fsx:{"username":"fsxadmin","password":"pass"}}`.

Der Wert wird im Parameter Store unter Parameterdetails in der AWS Management Console bereitgestellt. Der AWS SSM-Parametertyp muss „Secure String“ sein, mit dem Namen im Format `/netapp/wlmdb/<anyname>`. Weitere Informationen zum Abrufen von SSM-Parametern finden Sie unter ["AWS GovCloud-Dokumentation"](#).

8. Unter **Konnektivität** sind folgende Angaben erforderlich:

- a. **Schlüsselpaar:** Auswahl eines Schlüsselpaars für eine sichere Verbindung zu Ihrer Instanz.
- b. **Active Directory:** Folgende Angaben zu Active Directory sind erforderlich:
- i. Im Feld **Domänenname** wird ein Name für die Domäne ausgewählt oder eingegeben.
- A. Bei AWS-verwalteten Active Directories erscheinen Domänennamen im Dropdown-Menü.
- B. Bei einem benutzerverwalteten Active Directory erfolgt die Eingabe eines Namens im Feld **Suchen und Hinzufügen**; anschließend wird **Hinzufügen** ausgewählt.
- ii. Im Feld **DNS-Adresse** wird die DNS-IP-Adresse für die Domain eingegeben. Es können bis zu 3 IP-Adressen hinzugefügt werden.

Bei von AWS verwalteten Active Directories werden die DNS-IP-Adressen im Dropdown-Menü angezeigt.

- iii. Geben Sie den Benutzernamen und das Kennwort für die Active Directory-Domain ein.

Für GovCloud-Konten geben Sie den AWS SSM Parameter-ARN-Wert für Active Directory-Anmeldeinformationen im folgenden Format ein:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Der AWS SSM-Parametertyp muss „Secure String“ sein, mit dem Namen im Format `/netapp/wlmdb/<anyname>`. Weitere Informationen zum Abrufen von SSM-Parametern finden Sie unter ["AWS GovCloud-Dokumentation"](#).

- iv. **Bevorzugter Domänencontroller:** Optional lässt sich der bevorzugte Domänencontroller angeben, der für den Beitritt zu Active Directory verwendet werden soll.
- v. **Bevorzugter Pfad der Organisationseinheit:** Optional kann die bevorzugte Organisationseinheit (OU) im Active Directory angegeben werden, die für den Beitritt verwendet werden soll.
- vi. **Ziel Active Directory-Gruppe:** Optional kann die Ziel Active Directory-Gruppe angegeben werden, der die Computer hinzugefügt werden sollen.

9. Unter **Infrastruktureinstellungen** sind die folgenden Angaben erforderlich:

- a. **DB-Instanztyp:** Im Dropdown-Menü wird der Typ der Datenbankinstanz ausgewählt.
- b. **FSx for ONTAP System:** Ein neues FSx for ONTAP Dateisystem erstellen oder ein vorhandenes

FSx for ONTAP Dateisystem verwenden.

- i. **Neues FSx for ONTAP erstellen:** Eingabe von Benutzername und Passwort.

Für GovCloud-Konten geben Sie den AWS SSM-Parameter-ARN-Wert für die FSx for ONTAP-Anmeldeinformationen im folgenden Format ein:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Der AWS SSM-Parametertyp muss „Secure String“ sein, mit dem Namen im Format `/netapp/wlmdb/<anyname>`.

Weitere Informationen zum Abrufen von SSM-Parametern finden Sie unter ["AWS GovCloud-Dokumentation"](#).

Ein neues FSx for ONTAP Dateisystem kann die Installationszeit um 30 Minuten oder mehr verlängern.

- ii. **Vorhandenes FSx for ONTAP auswählen:** Im Dropdown-Menü werden der Name von FSx for ONTAP ausgewählt sowie ein Benutzername und ein Passwort für das Dateisystem eingegeben.

Für bestehende FSx for ONTAP Dateisysteme sind die folgenden Punkte zu beachten:

- Die an FSx for ONTAP angehängte Routing-Gruppe ermöglicht, Routen zu den Subnetzen für das Deployment zu verwenden.
- Die Sicherheitsgruppe erlaubt Datenverkehr aus den für das Deployment verwendeten Subnetzen, insbesondere über die TCP-Ports HTTPS (443) und iSCSI (3260).

- c. **Snapshot-Richtlinie:** Standardmäßig aktiviert. Snapshots werden täglich erstellt und 7 Tage lang aufbewahrt.

Die Snapshots sind den Volumes zugewiesen, die für SQL-Workloads erstellt wurden.

- d. **Datenträgergröße:** Die Kapazität des Datenträgers und die Kapazitätseinheit angeben.

- e. **Provisionierte IOPS:** Zur Auswahl stehen **Automatisch** oder **vom Benutzer provisioniert**. Bei Auswahl von **vom Benutzer provisioniert** ist der IOPS-Wert anzugeben.

- f. **Durchsatzkapazität:** Die Durchsatzkapazität wird im Dropdown-Menü ausgewählt.

In bestimmten Regionen können Sie eine Durchsatzkapazität von 4 GB/s auswählen. Zum Provisionieren einer Durchsatzkapazität von 4 GB/s muss Ihr FSx for ONTAP Dateisystem mit einer SSD Storage Kapazität von mindestens 5.120 GiB und 160.000 SSD IOPS konfiguriert sein.

- g. **Verschlüsselung:** Wählen Sie einen Schlüssel aus Ihrem Konto oder aus einem anderen Konto. Sie müssen den ARN des Verschlüsselungsschlüssels aus einem anderen Konto eingeben.

Benutzerdefinierte Verschlüsselungsschlüssel für FSx for ONTAP werden basierend auf der Dienstkompatibilität nicht aufgeführt. Die Auswahl eines geeigneten FSx-Verschlüsselungsschlüssels ist erforderlich. Nicht-FSx-Verschlüsselungsschlüssel führen dazu, dass die Servererstellung fehlschlägt.

Die von AWS verwalteten Schlüssel werden anhand ihrer Anwendbarkeit für den jeweiligen Dienst gefiltert.

- h. **Tags:** Optional lassen sich bis zu 40 Tags hinzufügen.

- i. **Simple Notification Service:** Optional können Sie den Simple Notification Service (SNS) für diese Konfiguration aktivieren, indem Sie im Dropdown-Menü ein SNS-Topic für Microsoft SQL Server auswählen.

- i. Die Aktivierung des Simple Notification Service ist erforderlich.
- ii. Die Auswahl einer ARN erfolgt über das Dropdown-Menü.
- j. **CloudWatch Überwachung:** Optional können Sie die CloudWatch Überwachung aktivieren.

Wir empfehlen, CloudWatch für die Fehlersuche im Fehlerfall zu aktivieren. Die Ereignisse, die in der AWS CloudFormation Konsole angezeigt werden, sind allgemein gehalten und geben nicht die eigentliche Ursache an. Alle detaillierten Protokolle werden im `C:\cfn\logs` Ordner in den EC2 Instanzen gespeichert.

In CloudWatch wird eine Protokollgruppe mit dem Namen des Stacks erstellt. Unter der Protokollgruppe wird für jeden Validierungsknoten und SQL-Knoten ein Protokollstream angezeigt. CloudWatch zeigt den Skriptfortschritt an und liefert Informationen, anhand derer Sie erkennen können, ob und wann ein Deployment fehlschlägt.

- a. **Ressourcen-Rollback:** Für diese Funktion gibt es derzeit keine Unterstützung.

10. Zusammenfassung

- a. **Geschätzte Kosten:** Enthält eine Schätzung der Kosten, die Ihnen entstehen könnten, wenn Sie die angezeigten Ressourcen einsetzen.

11. Mit **Erstellen** wird der neue Datenbankhost eingesetzt.

Alternativ können Sie die Konfiguration speichern.

Schritt 2: Aktivierung der Remote-Verbindung auf dem Microsoft SQL Server

Nach der Serverbereitstellung aktiviert Workload Factory die Remote-Verbindung zum Microsoft SQL Server nicht. Die Aktivierung der Remote-Verbindung erfolgt in den folgenden Schritten.

Schritte

1. Die Verwendung der Computeridentität für NTLM ist in der Microsoft-Dokumentation unter ["Netzwerksicherheit: Lokalem System die Verwendung der Computeridentität für NTLM erlauben"](#) beschrieben.
2. Die dynamische Portkonfiguration lässt sich anhand von ["Beim Herstellen einer Verbindung zu SQL Server ist ein netzwerkbezogener oder instanzspezifischer Fehler aufgetreten"](#) in der Microsoft-Dokumentation überprüfen.
3. Die Sicherheitsgruppe muss die erforderliche Client-IP oder das Subnetz zulassen.

Was kommt als Nächstes

Jetzt können Sie ["Erstellen einer Datenbank in Workload Factory for Databases"](#).

Einen PostgreSQL-Server in der NetApp Workload Factory für Datenbanken erstellen

Die Erstellung eines neuen PostgreSQL-Servers oder Datenbankhosts in NetApp Workload Factory for Databases erfordert ein FSx for ONTAP Dateisystem-Deployment und Ressourcen für Active Directory.

Über diese Aufgabe

Bevor Sie einen PostgreSQL-Server aus der Workload Factory erstellen, sollten Sie sich über die verfügbaren Storage Deployment-Typen für die Datenbankhostkonfiguration, die Betriebsmodi der Workload Factory und die Anforderungen für die Durchführung dieses Vorgangs informieren.

FSx for ONTAP Dateisystem Deployments

Für die Erstellung eines neuen PostgreSQL-Servers wird ein FSx for ONTAP Dateisystem als Storage-Backend benötigt. Sie können ein vorhandenes FSx for ONTAP Dateisystem verwenden oder ein neues Dateisystem erstellen. Wenn Sie ein vorhandenes FSx for ONTAP Dateisystem als Storage-Backend für Ihren Datenbankserver auswählen, erstellen wir eine neue Storage VM für die PostgreSQL-Workloads.

+ FSx for ONTAP Dateisysteme haben zwei PostgreSQL Server Deployment-Modelle: *High Availability (HA)* oder *Einzelinstanz*. Für das FSx for ONTAP Dateisystem entstehen je nach ausgewähltem FSx for ONTAP Deployment-Modell unterschiedliche Ressourcen.

- **High Availability (HA) Deployment:** Ein FSx for NetApp ONTAP Dateisystem mit mehreren Availability Zones wird eingesetzt, wenn ein neues FSx for ONTAP Dateisystem für ein HA Deployment ausgewählt wird. Für ein HA Deployment werden separate Volumes und LUNs für Daten-, Protokoll- und tempdb-Dateien erstellt. Für den Quorum- oder Zeugendatenträger für den Windows-Cluster werden ein zusätzliches Volume und eine zusätzliche LUN erstellt. Das HA Deployment konfiguriert die Streaming-Replikation zwischen den primären und sekundären PostgreSQL-Servern.
- **Single Instance Deployment:** Ein FSx for ONTAP Dateisystem in einer einzelnen Availability Zone wird erstellt, wenn ein neuer PostgreSQL Server erstellt wird. Zusätzlich werden separate Volumes und LUNs für Daten-, Protokoll- und tempdb-Dateien erstellt.

Bevor Sie beginnen

Sie müssen ["Berechtigungen für die Erstellung des Datenbankhosts"](#) in Ihrem AWS-Konto haben, um einen neuen Datenbankhost in Workload Factory zu erstellen.

Einen PostgreSQL-Server erstellen

Sie können die Deployment-Modi „Quick create“ oder „Advanced create“ verwenden, um diese Aufgabe in workload factory mit den Berechtigungen des Modus „Automate“ abzuschließen. Außerdem können die folgenden in der Codebox verfügbaren Tools verwendet werden: REST API, AWS CLI, AWS CloudFormation und Terraform. ["Informationen zur Verwendung von Codebox für die Automatisierung"](#).



Wenn Sie Terraform aus Codebox verwenden, werden im Code, den Sie kopieren oder herunterladen, Passwörter ausgeblendet `fsxadmin` und `vsadmin`. Sie müssen die Passwörter erneut eingeben, wenn Sie den Code ausführen. Zusätzlich zu den Berechtigungen für den *Automate*-Modus müssen Sie für das Benutzerkonto die folgenden Berechtigungen einschließen: `iam:TagRole` und `iam:TagInstanceProfile`. ["Informationen zur Verwendung von Terraform aus Codebox"](#).

Schnellerstellung



Bei der *Schnellerstellung* ist HA das Standard-Deployment-Modell, Windows 2016 die Standard-Windows-Version und SQL 2019 Standard Edition die Standard-SQL-Version.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.

2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. In der Datenbankübersicht erfolgt die Auswahl von **Host einsetzen** und anschließend im Menü von **PostgreSQL Server**.
4. Die Option **Quick create** auswählen.
5. Unter **Landing zone** sind die folgenden Angaben erforderlich:

- a. **AWS-Anmeldeinformationen:** Auswahl von AWS-Anmeldeinformationen mit automatisierten Berechtigungen zum Einsetzen des neuen Datenbankhosts.

AWS-Anmeldeinformationen mit Berechtigungen zum Erstellen von Datenbankhosts ermöglichen es Workload Factory, den neuen Datenbankhost über Ihr AWS-Konto innerhalb von workload factory einzusetzen und zu managen.

AWS-Anmeldeinformationen mit den Berechtigungen *view, planning und analysis* ermöglichen es Workload Factory, eine CloudFormation Vorlage zu generieren, die in der AWS CloudFormation Konsole verwendet werden kann.

Wenn in Workload Factory keine AWS-Anmeldeinformationen verknüpft sind und der neue Server in Workload Factory erstellt werden soll, ist **Option 1** zu verwenden, um zur Seite „Anmeldeinformationen“ zu gelangen. Dort erfolgt das manuelle Hinzufügen der erforderlichen Anmeldeinformationen und der Berechtigungen für die *Erstellung von Datenbankhosts* bei Datenbank-Workloads.

Wenn Sie das Formular zum Erstellen eines neuen Servers in Workload Factory ausfüllen möchten, um eine vollständige YAML-Dateivorlage für das Deployment in AWS CloudFormation herunterzuladen, ist **Option 2** zu verwenden, damit die erforderlichen Berechtigungen zum Erstellen des neuen Servers in AWS CloudFormation vorhanden sind. Die erforderlichen Anmeldeinformationen sowie die Berechtigungen für *Ansicht, Planung und Analyse* für Datenbank-Workloads sind manuell hinzuzufügen.

Optional können Sie eine teilweise ausgefüllte YAML-Dateivorlage aus der Codebox herunterladen, um den Stack außerhalb von Workload Factory ohne Anmeldeinformationen oder Berechtigungen zu erstellen. Für den Download der YAML-Datei steht in der Codebox im Dropdown-Menü **CloudFormation** zur Auswahl.

- b. **Region & VPC:** Auswahl einer Region und eines VPC-Netzwerks.

Sicherheitsgruppen für einen vorhandenen Schnittstellenendpunkt müssen den Zugriff über das HTTPS-Protokoll (443) auf die ausgewählten Subnetze zulassen.

AWS-Service-Schnittstellenendpunkte (SQS, FSx, EC2, CloudWatch, CloudFormation, SSM) und der S3-Gateway-Endpunkt werden während des Deployments erstellt, sofern sie nicht gefunden werden.

VPC DNS Attribute `EnableDnsSupport` und `EnableDnsHostnames` werden so geändert, dass die Auflösung von Endpunktadressen aktiviert wird, falls sie nicht bereits auf `true` gesetzt sind.

- c. **Verfügbarkeitszonen:** Auswahl von Verfügbarkeitszonen und Subnetzen.



HA Deployments werden nur für Multiple Availability Zone (MAZ) FSx for ONTAP Konfigurationen unterstützt.

Aus Gründen der Hochverfügbarkeit sollten Subnetze nicht dieselbe Routingtabelle verwenden.

- i. Im Feld **Clusterkonfiguration - Knoten 1** erfolgt die Auswahl der primären Verfügbarkeitszone für die MAZ FSx for ONTAP Konfiguration aus dem Dropdown-Menü **Verfügbarkeitszone** sowie eines Subnetzes aus der primären Verfügbarkeitszone aus dem Dropdown-Menü **Subnetz**.
 - ii. Im Feld **Clusterkonfiguration - Knoten 2** wird die sekundäre Availability Zone für die MAZ FSx for ONTAP Konfiguration im Dropdown-Menü **Availability zone** ausgewählt sowie ein Subnetz aus der sekundären Availability Zone im Dropdown-Menü **Subnet**.
6. Unter **Anwendungseinstellungen** werden ein Benutzername und ein Passwort für die **Datenbankzugangsdaten** eingegeben.
7. Unter **Konnektivität** wird ein Schlüsselpaar ausgewählt, um eine sichere Verbindung zu Ihrer Instanz herzustellen.
8. Unter **Infrastruktureinstellungen** sind die folgenden Angaben erforderlich:
 - a. **FSx for ONTAP System**: Ein neues FSx for ONTAP Dateisystem erstellen oder ein vorhandenes FSx for ONTAP Dateisystem verwenden.
 - i. **Neues FSx for ONTAP erstellen**: Eingabe von Benutzername und Passwort.

Für GovCloud-Konten geben Sie den AWS SSM Parameter-ARN-Wert für FSx for ONTAP-Anmeldeinformationen im folgenden Format ein:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Der AWS SSM-Parametertyp muss „Secure String“ sein, mit dem Namen im Format `/netapp/wlmdb/<anyname>`. Weitere Informationen zum Abrufen von SSM-Parametern finden Sie unter ["AWS GovCloud-Dokumentation"](#).

Ein neues FSx for ONTAP Dateisystem kann die Installationszeit um 30 Minuten oder mehr verlängern.

- i. **Vorhandenes FSx for ONTAP auswählen**: Im Dropdown-Menü werden der Name von FSx for ONTAP ausgewählt sowie ein Benutzername und ein Passwort für das Dateisystem eingegeben.

Für bestehende FSx for ONTAP Dateisysteme sind die folgenden Punkte zu beachten:

- Die an FSx for ONTAP angehängte Routing-Gruppe ermöglicht, Routen zu den Subnetzen für das Deployment zu verwenden.
- Die Sicherheitsgruppe erlaubt Datenverkehr aus den für das Deployment verwendeten Subnetzen, insbesondere über die TCP-Ports HTTPS (443) und iSCSI (3260).

- b. **Datenträgergröße**: Die Kapazität des Datenträgers und die Kapazitätseinheit angeben.

9. Zusammenfassung:

- a. **Vorschau der Standardeinstellungen**: Prüfung der von Quick create festgelegten Standardkonfigurationen.
 - b. **Geschätzte Kosten**: Enthält eine Schätzung der Kosten, die Ihnen entstehen könnten, wenn Sie die angezeigten Ressourcen einsetzen.

10. Klicken Sie auf **Create**.

Alternativ können Sie, falls Sie eine dieser Standardeinstellungen jetzt ändern möchten, den Datenbankserver mit Advanced create erstellen.

Sie können auch **Konfiguration speichern** auswählen, um den Host später einzusetzen.

Erweiterte Erstellung

Schritte

1. Melden Sie sich bei der "NetApp Console" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. In der Datenbankübersicht erfolgt die Auswahl von **Host einsetzen** und anschließend im Menü von **PostgreSQL Server**.
4. **Advanced create** ist auszuwählen.
5. Unter **Bereitstellungsmodell** steht entweder **Standalone-Instanz** oder **Hochverfügbarkeit (HA)** zur Auswahl.
6. Unter **Landing zone** sind die folgenden Angaben erforderlich:
 - a. **AWS-Anmeldeinformationen**: Auswahl von AWS-Anmeldeinformationen mit automatisierten Berechtigungen zum Einsetzen des neuen Datenbankhosts.

AWS-Anmeldeinformationen mit Berechtigungen zum Erstellen von Datenbankhosts ermöglichen es Workload Factory, den neuen Datenbankhost über Ihr AWS-Konto innerhalb von workload factory einzusetzen und zu managen.

AWS-Anmeldeinformationen mit den Berechtigungen *view, planning und analysis* ermöglichen es Workload Factory, eine CloudFormation Vorlage zu generieren, die in der AWS CloudFormation Konsole verwendet werden kann.

Wenn in Workload Factory keine AWS-Anmeldeinformationen verknüpft sind und der neue Server in Workload Factory erstellt werden soll, ist **Option 1** zu verwenden, um zur Seite „Anmeldeinformationen“ zu gelangen. Dort erfolgt das manuelle Hinzufügen der erforderlichen Anmeldeinformationen und der Berechtigungen für die *Erstellung von Datenbankhosts* bei Datenbank-Workloads.

Wenn Sie das Formular zum Erstellen eines neuen Servers in Workload Factory ausfüllen möchten, um eine vollständige YAML-Dateivorlage für das Deployment in AWS CloudFormation herunterzuladen, ist **Option 2** zu verwenden, damit die erforderlichen Berechtigungen zum Erstellen des neuen Servers in AWS CloudFormation vorhanden sind. Die erforderlichen Anmeldeinformationen sowie die Berechtigungen für *Ansicht, Planung und Analyse* für Datenbank-Workloads sind manuell hinzuzufügen.

Optional können Sie eine teilweise ausgefüllte YAML-Dateivorlage aus der Codebox herunterladen, um den Stack außerhalb von Workload Factory ohne Anmeldeinformationen oder Berechtigungen zu erstellen. Für den Download der YAML-Datei steht in der Codebox im Dropdown-Menü **CloudFormation** zur Auswahl.

- b. **Region & VPC**: Auswahl einer Region und eines VPC-Netzwerks.

Sicherheitsgruppen für einen vorhandenen Schnittstellenendpunkt müssen den Zugriff über das HTTPS-Protokoll (443) auf die ausgewählten Subnetze zulassen.

AWS Service-Schnittstellenendpunkte (SQS, FSx, EC2, CloudWatch, Cloud Formation, SSM) und der S3-Gateway-Endpunkt werden während des Deployment erstellt, wenn sie nicht gefunden werden.

Die VPC-DNS-Attribute `EnableDnsSupport` und `EnableDnsHostnames` werden so geändert, dass die Auflösung von Endpunktadressen ermöglicht wird, falls sie nicht bereits auf `true` festgelegt sind.

c. **Verfügbarkeitszonen:** Auswahl von Verfügbarkeitszonen und Subnetzen.

Für Einzelinstanz-Deployments

Im Feld **Clusterkonfiguration - Knoten 1** ist eine Verfügbarkeitszone aus dem Dropdown-Menü **Verfügbarkeitszone** und ein Subnetz aus dem Dropdown-Menü **Subnetz** auszuwählen.

Für HA Deployments

- i. Im Feld **Clusterkonfiguration - Knoten 1** erfolgt die Auswahl der primären Verfügbarkeitszone für die MAZ FSx for ONTAP Konfiguration aus dem Dropdown-Menü **Verfügbarkeitszone** sowie eines Subnetzes aus der primären Verfügbarkeitszone aus dem Dropdown-Menü **Subnetz**.
 - ii. Im Feld **Clusterkonfiguration - Knoten 2** wird die sekundäre Availability Zone für die MAZ FSx for ONTAP Konfiguration im Dropdown-Menü **Availability zone** ausgewählt sowie ein Subnetz aus der sekundären Availability Zone im Dropdown-Menü **Subnetz**.
- d. **Sicherheitsgruppe:** Es wird eine Arbeitslast-Sicherheitsgruppe erstellt, um die für PostgreSQL erforderlichen Ports und Protokolle zuzulassen. Zusätzlich können Sie eine oder mehrere Sicherheitsgruppen auswählen.
7. Unter **Anwendungseinstellungen** sind folgende Angaben erforderlich:
- a. Die Auswahl des **Betriebssystems** erfolgt über das Dropdown-Menü.
 - b. Die **PostgreSQL Version** wird im Dropdown-Menü ausgewählt.
 - c. **Name des Datenbankservers:** Eingabe des Namens des Datenbankclusters.
 - d. **Datenbank-Anmeldeinformationen:** Eingabe eines Benutzernamens und Kennworts für ein neues Dienstkonto oder Verwendung der Anmeldedaten eines vorhandenen Dienstkontos im Active Directory.

Für GovCloud-Konten geben Sie den AWS SSM Parameter-ARN-Wert für die Anmeldeinformationen im folgenden Format ein:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Der AWS SSM-Parametertyp muss „Secure String“ sein, mit dem Namen im Format `/netapp/wlmdb/<anyname>`. Weitere Informationen zum Abrufen von SSM-Parametern finden Sie unter ["AWS GovCloud-Dokumentation"](#).

8. Unter **Konnektivität** wird ein Schlüsselpaar ausgewählt, um eine sichere Verbindung zu Ihrer Instanz herzustellen.
9. Unter **Infrastruktureinstellungen** sind die folgenden Angaben erforderlich:
- a. **DB-Instanztyp:** Im Dropdown-Menü wird der Typ der Datenbankinstanz ausgewählt.
 - b. **FSx for ONTAP System:** Ein neues FSx for ONTAP Dateisystem erstellen oder ein vorhandenes FSx for ONTAP Dateisystem verwenden.
 - i. **Neues FSx for ONTAP erstellen:** Eingabe von Benutzername und Passwort.

Für GovCloud-Konten geben Sie den AWS SSM-Parameter-ARN-Wert für die FSx for ONTAP-Anmeldeinformationen im folgenden Format ein:

`{fsx:{"username":"fsxadmin","password":"pass"}}`. Der AWS SSM-Parametertyp muss „Secure String“ sein, mit dem Namen im Format `/netapp/wlmdb/<anyname>`. Weitere Informationen zum Abrufen von SSM-Parametern finden Sie unter ["AWS GovCloud-Dokumentation"](#).

Ein neues FSx for ONTAP Dateisystem kann die Installationszeit um 30 Minuten oder mehr verlängern.

- ii. **Vorhandenes FSx for ONTAP auswählen:** Im Dropdown-Menü werden der Name von FSx for ONTAP ausgewählt sowie ein Benutzername und ein Passwort für das Dateisystem eingegeben.

Für bestehende FSx for ONTAP Dateisysteme sind die folgenden Punkte zu beachten:

- Die an FSx for ONTAP angehängte Routing-Gruppe ermöglicht, Routen zu den Subnetzen für das Deployment zu verwenden.
 - Die Sicherheitsgruppe erlaubt Datenverkehr aus den für das Deployment verwendeten Subnetzen, insbesondere über die TCP-Ports HTTPS (443) und iSCSI (3260).
- c. **Snapshot-Richtlinie:** Standardmäßig aktiviert. Snapshots werden täglich erstellt und 7 Tage lang aufbewahrt.

Die Snapshots sind Volumes zugewiesen, die für PostgreSQL Workloads erstellt wurden.

- d. **Datenträgergröße:** Die Kapazität des Datenträgers und die Kapazitätseinheit angeben.
- e. **Provisionierte IOPS:** Zur Auswahl stehen **Automatisch** oder **vom Benutzer provisioniert**. Bei Auswahl von **vom Benutzer provisioniert** ist der IOPS-Wert anzugeben.
- f. **Durchsatzkapazität:** Die Durchsatzkapazität wird im Dropdown-Menü ausgewählt.

In bestimmten Regionen können Sie eine Durchsatzkapazität von 4 GB/s auswählen. Zum Provisionieren einer Durchsatzkapazität von 4 GB/s muss Ihr FSx for ONTAP Dateisystem mit einer SSD Storage Kapazität von mindestens 5.120 GiB und 160.000 SSD IOPS konfiguriert sein.

- g. **Verschlüsselung:** Wählen Sie einen Schlüssel aus Ihrem Konto oder aus einem anderen Konto. Sie müssen den ARN des Verschlüsselungsschlüssels aus einem anderen Konto eingeben.

Benutzerdefinierte Verschlüsselungsschlüssel für FSx for ONTAP werden basierend auf der Dienstkompatibilität nicht aufgeführt. Die Auswahl eines geeigneten FSx-Verschlüsselungsschlüssels ist erforderlich. Nicht-FSx-Verschlüsselungsschlüssel führen dazu, dass die Servererstellung fehlschlägt.

Die von AWS verwalteten Schlüssel werden anhand ihrer Anwendbarkeit für den jeweiligen Dienst gefiltert.

- h. **Tags:** Optional lassen sich bis zu 40 Tags hinzufügen.
- i. **Simple Notification Service:** Optional können Sie den Simple Notification Service (SNS) für diese Konfiguration aktivieren, indem Sie im Dropdown-Menü ein SNS-Thema für PostgreSQL auswählen.
- i. Die Aktivierung des Simple Notification Service ist erforderlich.
 - ii. Die Auswahl einer ARN erfolgt über das Dropdown-Menü.
- j. **CloudWatch Überwachung:** Optional können Sie die CloudWatch Überwachung aktivieren.

Wir empfehlen, CloudWatch für die Fehlersuche im Fehlerfall zu aktivieren. Die Ereignisse, die in der AWS CloudFormation Konsole angezeigt werden, sind allgemein gehalten und geben nicht die eigentliche Ursache an. Alle detaillierten Protokolle werden im `C:\cfn\logs` Ordner in den EC2 Instanzen gespeichert.

In CloudWatch wird eine Protokollgruppe mit dem Namen des Stacks erstellt. Unter der Protokollgruppe wird für jeden Validierungsknoten und SQL-Knoten ein Protokollstream angezeigt. CloudWatch zeigt den Skriptfortschritt an und liefert Informationen, anhand derer Sie erkennen können, ob und wann ein Deployment fehlschlägt.

a. **Ressourcen-Rollback:** Für diese Funktion gibt es derzeit keine Unterstützung.

10. Zusammenfassung

a. **Geschätzte Kosten:** Enthält eine Schätzung der Kosten, die Ihnen entstehen könnten, wenn Sie die angezeigten Ressourcen einsetzen.

11. Mit **Erstellen** wird der neue Datenbankhost eingesetzt.

Alternativ können Sie die Konfiguration speichern.

Was kommt als Nächstes

Sie können Benutzer, Fernzugriff und Datenbanken auf dem eingesetzten PostgreSQL Server manuell konfigurieren.

Erstellen einer Microsoft SQL Datenbank in NetApp Workload Factory for Databases

Durch das Erstellen einer neuen Microsoft SQL Datenbank können Sie die Ressource in NetApp Workload Factory for Databases managen.

Über diese Aufgabe

Bei der Erstellung der Datenbank werden im FSx for ONTAP Dateisystem zwei neue Volumes erstellt, die aus unabhängigen LUNs bestehen und Daten- und Protokolldateien für die Datenbank hosten. Die Datenbankdateien in der neuen Datenbank sind thin-provisioniert und belegen nur wenige MB der der neuen Datenbank insgesamt zugewiesenen Größe.

Wenn Sie Storage für die Datenbank trennen möchten, können Sie dies mithilfe eines virtuellen Mountpunkts tun. Der virtuelle Mountpunkt ermöglicht es Ihnen, Datenbanken auf wenigen gemeinsamen Laufwerken auf dem Host zu konsolidieren.

Zum Erstellen einer Datenbank in workload factory sind die Berechtigungen *Anzeigen*, *Planen* und *Analysieren* erforderlich. Alternativ können Sie eine teilweise ausgefüllte Codevorlage kopieren oder herunterladen, um den Vorgang außerhalb von workload factory abzuschließen. "[Informationen zu den Berechtigungen von Workload Factory](#)", um zu entscheiden, welchen Modus Sie verwenden möchten.



Microsoft SQL Servers, die das SMB-Protokoll verwenden, unterstützen keine Datenbankerstellung.

Bevor Sie beginnen

Folgende Voraussetzungen sind zu erfüllen, bevor eine neue Datenbank erstellt wird.

- **Anmeldeinformationen und Berechtigungen:** Sie müssen "[AWS-Kontoanmeldeinformationen und Berechtigungen für Operationen und Behebungen](#)" besitzen, um eine neue Datenbank in Workload Factory zu erstellen.

Alternativ lässt sich die Codebox verwenden, um eine Vorlage zu kopieren, sodass Sie mithilfe der REST API eine Datenbank außerhalb von workload factory einsetzen können. "[Weitere Informationen zur](#)

- **Windows-Host:** Sie müssen auf dem Microsoft SQL Server über genügend Laufwerksbuchstaben verfügen, um neue Laufwerke für die neue Datenbank zu erstellen, wenn Sie den Modus *Quick create* verwenden.
- **Microsoft SQL Server:** Voraussetzung ist ein verwalteter Microsoft SQL Server in workload factory for Databases zum Hosten der neuen Datenbank.
- **AWS Systems Manager:** Es muss sichergestellt sein, dass die NT Authority\SYSTEM Benutzerrechte im Microsoft SQL Host über AWS Systems Manager aktiviert sind.

Erstellen einer Datenbank

In Workload Factory kann diese Aufgabe mit den Deployment-Modi *Quick create* oder *Advanced create* abgeschlossen werden.

Schnellerstellung

Schritte

1. Melden Sie sich bei der "NetApp Console" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Im Menü Datenbanken wird **Inventar** ausgewählt.
4. Im Inventar wird **Microsoft SQL Server** als Typ der Datenbank-Engine ausgewählt.
5. Auswahl eines Datenbankservers mit einer verwalteten SQL server Instanz, in dem die Datenbank erstellt wird.
6. Anschließend erfolgt im Aktionsmenü der verwalteten Instanz die Auswahl von **Benutzerdatenbank erstellen**.
7. Auf der Seite „Benutzerdatenbank erstellen“ sind unter „Datenbankinformationen“ die folgenden Angaben zu machen:
 - a. **Datenbankname:** Namen für die Datenbank eingeben.
 - b. **Sortierung:** Auswahl einer Sortierung für die Datenbank. Die Standardsortierung "SQL_Latin1_General_CP1_CI_AS" auf Microsoft SQL Server ist ausgewählt.
8. Unter Dateieinstellungen sind die folgenden Angaben erforderlich:
 - a. **Dateieinstellungsmodus:** Auswahl von **Schnell erstellen**.
 - b. **Dateinamen & Pfad:**
 - **Name der Datendatei:** Name der Datendatei eingeben.
 - **Name der Protokolldatei:** Eingabe des Namens der Protokolldatei.
 - c. **Dateigrößen:** Eingabe der Datengröße und der Protokollgröße für die Datenbank.
9. Klicken Sie auf **Create**.

Alternativ können Sie, wenn Sie eine dieser Standardeinstellungen jetzt ändern möchten, den **Dateieinstellungsmodus** in **Erweiterte Erstellung** ändern.

Erweiterte Erstellung

Schritte

1. Melden Sie sich bei der "[NetApp Console](#)" an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Im Menü Datenbanken wird **Inventar** ausgewählt.
4. Im Inventar wird **Microsoft SQL Server** als Typ der Datenbank-Engine ausgewählt.
5. Auswahl eines Datenbankservers mit einer verwalteten SQL server Instanz, in dem die Datenbank erstellt wird.
6. Anschließend erfolgt im Aktionsmenü der verwalteten Instanz die Auswahl von **Benutzerdatenbank erstellen**.
7. Die Auswahl fällt auf **Create user database**.
8. Auf der Seite „Benutzerdatenbank erstellen“ sind unter „Datenbankinformationen“ die folgenden Angaben zu machen:
 - a. **Datenbankname**: Namen für die Datenbank eingeben.
 - b. **Sortierung**: Auswahl der Sortierung für die Datenbank. Die Standardsortierung "SQL_Latin1_General_CP1_CI_AS" auf Microsoft SQL Server ist ausgewählt.
9. Unter Dateieinstellungen sind die folgenden Angaben erforderlich:
 - a. **Modus für Dateieinstellungen**: **Advanced create** auswählen.
 - b. **Dateinamen & Pfad**:
 - i. **Datendatei**: Auswahl eines Laufwerksbuchstabens und Eingabe des Namens der Datendatei.

Optional kann das Kontrollkästchen für **Virtual mount point** aktiviert werden.
 - ii. **Protokolldatei**: Auswahl eines Laufwerksbuchstabens und Eingabe des Namens der Protokolldatei.

Optional kann das Kontrollkästchen für **Virtual mount point** aktiviert werden.
 - c. **Dateigrößen**: Eingabe der Datengröße und der Protokollgröße für die Datenbank.
10. Klicken Sie auf **Create**.

Wenn Sie den Datenbank-Host erstellt haben, können Sie den Fortschritt des Auftrags auf der Registerkarte **Job monitoring** überprüfen.

Erstellung eines Sandbox-Klons in NetApp Workload Factory for Databases

Das Erstellen eines Sandbox-Klons einer Datenbank in NetApp Workload Factory for Databases ermöglicht die Verwendung des Klons für Entwicklung, Tests, Integration, Analysen, Schulungen, Qualitätssicherung und mehr, ohne die Quelldatenbank zu verändern.

Über diese Aufgabe

Ein Sandbox-Klon wird aus dem aktuellsten Snapshot der Quelldatenbank erstellt. Er kann auf demselben Microsoft SQL Server wie die Quelldatenbank oder auf einem anderen Microsoft SQL Server geklont werden, sofern beide dasselbe FSx for ONTAP-Dateisystem verwenden.

Bevor Sie beginnen

Bevor Sie einen Sandbox-Klon erstellen, müssen Sie die folgenden Voraussetzungen erfüllen.

- **Anmeldeinformationen und Berechtigungen:** Es müssen ["AWS-Kontoanmeldeinformationen und Berechtigungen für Operationen und Behebungen"](#) vorhanden sein, um einen Sandbox-Klon in Workload Factory zu erstellen.

Alternativ können Sie die Codebox verwenden, um eine teilweise ausgefüllte Vorlage zu kopieren oder eine fertige Vorlage zu erstellen, sodass Sie den Sandbox-Klon außerhalb der Workload Factory mithilfe der REST-API erstellen können ["Weitere Informationen zur Codebox Automatisierung"](#).

- **Microsoft SQL Server:** Sie benötigen einen verwalteten Microsoft SQL Server in Workload Factory for Databases zum Hosten des neuen Sandbox-Klons.
- **AWS Systems Manager:** Es muss sichergestellt sein, dass die `NT Authority\SYSTEM` Benutzerrechte im Microsoft SQL Host über AWS Systems Manager aktiviert sind.
- **Quelldatenbank:** Sie benötigen eine für den Klon verfügbare Quelldatenbank.

Schritte

1. Melden Sie sich bei der ["NetApp Console"](#) an.
2. Die Auswahl erfolgt im Menü , **Workloads > Datenbanken**.
3. Unter Databases die Registerkarte **Sandboxes** auswählen.
4. Im Reiter „Sandboxes“ ist **Neue Sandbox erstellen** auszuwählen.
5. Auf der Seite „Neue Sandbox erstellen“ sind unter „Datenbankquelle“ folgende Angaben erforderlich:
 - a. **Quelldatenbank-Host:** Auswahl des Quelldatenbank-Hosts.
 - b. **Quell-Datenbankinstanz:** Auswahl der Quell-Datenbankinstanz.
 - c. **Quelldatenbank:** Auswahl der Datenbank, die geklont werden soll.
6. Unter „Datenbankziel“ sind folgende Angaben erforderlich:
 - a. **Ziel-Datenbankhost:** Der für den Sandbox-Klon ausgewählte Zieldatenbankhost befindet sich in derselben VPC und weist dasselbe FSx for ONTAP Dateisystem wie der Quellhost auf.
 - b. **Zieldatenbankinstanz:** Auswahl der Zieldatenbankinstanz für den Sandbox-Klon.
 - c. **Zieldatenbank:** Eingabe eines Namens für den Sandbox-Klon.
7. **Einbinden:** Beim Klonen einer SQL-Datenbank mit mehreren Daten- und/oder Protokolldateien kloniert Workload Factory alle Dateien unter dem automatisch zugewiesenen oder definierten Laufwerksbuchstaben.

Wählen Sie eine der folgenden Optionen:

- a. **Automatische Montagepunktzuweisung**
- b. **Definition des Mountpunktpfads**

Zum Definieren des Mountpunktpfads sind die folgenden Angaben erforderlich:

- Eingabe des Laufwerksbuchstabens für den Datendateipfad.
- Der Laufwerksbuchstabe für den Pfad der Protokolldatei ist anzugeben.

8. **Tag definieren:** Auswahl eines Tags zur Definition des Sandbox-Klons.

9. Klicken Sie auf **Create**.

Zum Überprüfen des Fortschritts des Auftrags dient die Registerkarte **Auftragsüberwachung**.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.