Erstellen Sie einen neuen Datenbankserver

Database workloads

NetApp
March 02, 2026

This PDF was generated from https://docs.netapp.com/de-de/workload-databases/create-database-server.html on March 02, 2026. Always check docs.netapp.com for the latest.

Inhalt

Erstellen Sie einen neuen Datenbankserver

Erstellen Sie einen Microsoft SQL Server in Workload Factory für Datenbanken

Zum Erstellen eines neuen Microsoft SQL Servers oder Datenbankhosts in Workload Factory für Datenbanken sind eine FSx für die ONTAP Dateisystembereitstellung und Ressourcen für Active Directory erforderlich.

Über diese Aufgabe

Informieren Sie sich vor dem Erstellen eines Microsoft SQL Servers aus Workload Factory über die verfügbaren Speicherbereitstellungstypen für die Datenbankhostkonfiguration, die Microsoft Multi-Path I/O-Konfiguration, die Active Directory-Bereitstellung, Netzwerkdetails und die Anforderungen zum Abschließen dieses Vorgangs.

Nach der Bereitstellung müssen Sie Aktivieren Sie die Remoteverbindung auf dem Microsoft SQL Server.

FSX für ONTAP-File-System-Implementierungen

Die Erstellung eines neuen Microsoft SQL Servers erfordert ein FSX für ONTAP Filesystem als Storage-Backend. Sie können ein bestehendes FSX für ONTAP-Dateisystem verwenden oder ein neues Dateisystem erstellen. Wenn Sie ein vorhandenes FSX für ONTAP-Dateisystem als Ihr Datenbankserver-Storage-Back-End auswählen, erstellen wir eine neue Storage-VM für die Microsoft SQL-Workloads.

FSX for ONTAP-Dateisysteme verfügen über zwei Microsoft SQL Server-Bereitstellungsmodelle: *Failover Cluster Instance (FCI)* oder *Standalone*. Abhängig vom von dem von Ihnen gewählten FSX for ONTAP-Bereitstellungsmodell werden verschiedene Ressourcen für das FSX for ONTAP-Dateisystem erstellt.

- **Failover Cluster Instance (FCI) Microsoft SQL Deployment**: Ein Dateisystem mit mehreren Verfügbarkeitszonen FSX für NetApp ONTAP wird bereitgestellt, wenn ein neues Dateisystem FSX für ONTAP für die FCI-Bereitstellung ausgewählt wird. Separate Volumes und LUNs werden für Daten-, Protokoll- und tempdb-Dateien für eine FCI-Implementierung erstellt. Ein zusätzliches Volume und eine LUN werden für Quorum oder Witness Disk für Windows Cluster erstellt.
- **Eigenständige Microsoft SQL-Bereitstellung**: Ein einzelnes Verfügbarkeitszonen-FSX für ONTAP-Dateisystem wird erstellt, wenn ein neuer Microsoft SQL-Server erstellt wird. Darüber hinaus werden separate Volumes und LUNs für Daten-, Protokoll- und tempdb-Dateien erstellt.

Microsoft Multi-Path-I/O-Konfiguration

Für beide Bereitstellungsmodelle von Microsoft SQL Server ist die LUN-Erstellung mithilfe des iSCSI-Speicherprotokolls erforderlich. Workload Factory konfiguriert Microsoft Multi-Path I/O (MPIO) als Teil der Konfiguration von LUNs für SQL Server über FSx für ONTAP. MPIO wird basierend auf den Best Practices von AWS und NetApp konfiguriert.

Weitere Informationen finden Sie unter "SQL Server-Hochverfügbarkeitsbereitstellungen mit Amazon FSx for NetApp ONTAP" .

Active Directory

Während der Bereitstellung geschieht Folgendes für Active Directory (AD):

- Ein neues Microsoft SQL-Dienstkonto wird in der Domäne erstellt, wenn Sie kein vorhandenes SQL-Dienstkonto angeben.

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

Vom Benutzer gemanagte Active Directory-Sicherheitsgruppen

Wenn Sie während der Microsoft SQL Server-Bereitstellung in Workload Factory „benutzerverwaltetes Active Directory“ auswählen, müssen Sie eine Sicherheitsgruppe angeben, die den Datenverkehr zwischen den EC2-Instanzen und dem Verzeichnisdienst für die Bereitstellung zulässt. Workload Factory fügt die Sicherheitsgruppe für benutzerverwaltetes Active Directory nicht automatisch an, wie dies bei AWS Managed Microsoft AD der Fall ist.

Ressourcen-Rollbacks

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

- Für benutzerverwaltetes AD, zuerst "Entfernen Sie den AD-Computer". Verbinden Sie sich dann mit dem DNS-Server vom DNS-Manager und "Löschen Sie die DNS-Ressourceneinträge".
- Für AWS Managed Microsoft AD, "Installieren Sie die AD-Verwaltungstools" Weiter, "Entfernen Sie den AD-Computer". Schließlich verbinden Sie sich mit dem DNS-Server von DNS-Manager und "Löschen Sie die DNS-Ressourceneinträge".

Bevor Sie beginnen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie einen neuen Datenbank-Host erstellen.

Anmeldeinformationen und Berechtigungen

Du musst "Berechtigungen zum Erstellen des Datenbankhosts erteilen" Erstellen Sie in Ihrem AWS-Konto einen neuen Datenbankhost in Workload Factory.

Active Directory

Wenn Sie eine Verbindung zu Active Directory herstellen, müssen Sie über Administratorzugriff mit Berechtigungen verfügen, um Folgendes tun zu können:

- Treten Sie der Domain bei
- Erstellen Sie Computerobjekte
- Objekte in der Standardorganisation (OU) erstellen
- Lesen Sie alle Eigenschaften
- Machen Sie den Domänenbenutzer zu einem lokalen Administrator auf den AD-Knoten
- Erstellen Sie einen Microsoft SQL Server-Dienstbenutzer im AD, falls er nicht bereits vorhanden ist

Schritt 1: Erstellen Sie einen Datenbankserver

Sie können die Bereitstellungsmodi „Schnell erstellen“ oder „Erweiterte Erstellung“ verwenden, um diese Aufgabe in Workload Factory mit Berechtigungen für den Modus „Automatisieren“ abzuschließen. Sie können auch die folgenden in der Codebox verfügbaren Tools verwenden: REST-API, AWS CLI, AWS CloudFormation und Terraform. "Erfahren Sie, wie Sie Codebox für die Automatisierung verwenden" .

Bei der Verwendung von Terraform aus der Codebox werden der Code, den Sie kopieren oder herunterladen, ausgeblendet `fsxadmin` und `vsadmin` Passwörter. Sie müssen die Passwörter erneut eingeben, wenn Sie den Code ausführen. Zusätzlich zu den *Automate*-Modus -Berechtigungen müssen Sie die folgenden Berechtigungen für das Benutzerkonto hinzufügen: `iam:TagRole` Und `iam:TagInstanceProfile`. "Lernen Sie die Verwendung von Terraform von Codebox".

Während der Bereitstellung aktiviert Workload Factory CredSSP für die Anmeldeinformationsdelegierung an Skripts zur Bereitstellung von SQL. Wenn die CredSSP-Delegierung für alle Domänencomputer mit der Gruppenrichtlinie blockiert wird, schlägt die Bereitstellung fehl. Nach der Bereitstellung deaktiviert Workload Factory CredSSP.

Schnelle Erstellung

In *Quick Create* ist FCI das Standardbereitgabemodell, Windows 2016 die Standardversion von Windows und SQL 2019 Standard Edition die Standardversion von SQL.

Schritte

1. Melden Sie sich mit einem der "Konsolenerfahrungen"an.
2. Wählen Sie in der Kachel „Datenbanken“ die Option „Host bereitstellen“ und dann im Menü „Microsoft SQL Server“ aus.
3. Wählen Sie **Schnellerstelle**.
4. Geben Sie unter **AWS settings** Folgendes an:
   a. **AWS Credentials**: Wählen Sie AWS Credentials mit Automatisierungsberechtigungen aus, um den neuen Datenbank-Host bereitzustellen.

      Mit AWS-Anmeldeinformationen mit Lese-/Schreibberechtigungen kann Workload Factory den neuen Datenbankhost von Ihrem AWS-Konto innerhalb von Workload Factory bereitstellen und verwalten.

      Mit AWS-Anmeldeinformationen mit *Nur-Lese*-Berechtigungen kann Workload Factory eine CloudFormation-Vorlage generieren, die Sie in der AWS CloudFormation-Konsole verwenden können.

      Wenn Sie keine AWS-Anmeldeinformationen in Workload Factory verknüpft haben und den neuen Server in Workload Factory erstellen möchten, folgen Sie **Option 1**, um zur Seite „Anmeldeinformationen“ zu gelangen. Fügen Sie die erforderlichen Anmeldeinformationen und Berechtigungen für den Lese-/Schreibmodus für Datenbank-Workloads manuell hinzu.

      Wenn Sie das Formular zum Erstellen eines neuen Servers in Workload Factory ausfüllen möchten, um eine vollständige YAML-Dateivorlage für die Bereitstellung in AWS CloudFormation herunterzuladen, folgen Sie **Option 2**, um sicherzustellen, dass Sie über die erforderlichen Berechtigungen zum Erstellen des neuen Servers in AWS CloudFormation verfügen. Fügen Sie die erforderlichen Anmeldeinformationen und Berechtigungen für den Lesemodus für Datenbank-Workloads manuell hinzu.

      Optional können Sie eine teilweise ausgefüllte YAML-Dateivorlage aus der Codebox herunterladen, um den Stapel außerhalb von Workload Factory ohne Anmeldeinformationen oder Berechtigungen zu erstellen. Wählen Sie **CloudFormation** aus der Dropdown-Liste in der Codebox, um die YAML-Datei herunterzuladen.

   b. **Region & VPC**: Wählen Sie eine Region und ein VPC-Netzwerk.

      Stellen Sie sicher, dass Bereitstellungssubnetze mit vorhandenen Schnittstellenendpunkten verknüpft sind und Sicherheitsgruppen den Zugriff auf das HTTPS-Protokoll (443) auf die ausgewählten Subnetze ermöglichen.

      AWS-Serviceschnittstellen-Endpunkte (SQS, FSX, EC2, CloudWatch, CloudFormation, SSM) und der S3-Gateway-Endpunkt werden während der Bereitstellung erstellt, wenn nicht gefunden.

      VPC-DNS-Attribute `EnableDnsSupport` und `EnableDnsHostnames` werden geändert, um die Auflösung der Endpunktadresse zu aktivieren, wenn sie nicht bereits auf festgelegt sind `true`.

      Bei Verwendung eines Cross-VPC-DNS sollte die Sicherheitsgruppe für Endpunkte in der

anderen VPC, in der sich der DNS befindet, Port 443 für Bereitstellungssubnetze freigeben. Andernfalls sollten Sie beim Beitritt zu einem Cross-VPC-Active Directory einen DNS-Resolver aus der lokalen VPC bereitstellen. In einer Umgebung mit mehreren replizierten Domänencontrollern können Sie, wenn einige Domänencontroller vom Subnetz aus nicht erreichbar sind, **zu CloudFormation umleiten** und Folgendes eingeben: `Preferred domain controller` um eine Verbindung mit Active Directory herzustellen.

c. **Verfügbarkeitszonen**: Wählen Sie Verfügbarkeitszonen und Subnetze gemäß dem Failover Cluster Instance (FCI)-Bereitstellungsmodell aus.

> FCI-Implementierungen werden nur in Konfigurationen mit Multiple Availability Zone (MAZ) FSX for ONTAP unterstützt.

i. Wählen Sie im Feld **Clusterkonfiguration - Knoten 1** die primäre Verfügbarkeitszone für die MAZ FSX for ONTAP-Konfiguration aus dem Dropdown-Menü **Verfügbarkeitszone** und ein Subnetz aus der primären Verfügbarkeitszone aus dem Dropdown-Menü **Subnetz** aus.

ii. Wählen Sie im Feld **Cluster-Konfiguration - Knoten 2** die sekundäre Verfügbarkeitszone für die MAZ FSX for ONTAP-Konfiguration aus dem Dropdown-Menü **Verfügbarkeitszone** und ein Subnetz aus der sekundären Verfügbarkeitszone aus dem Dropdown-Menü **Subnetz** aus.

5. Geben Sie unter **Anwendungseinstellungen** einen Benutzernamen und ein Passwort für **Datenbankanmeldeinformationen** ein.
6. Geben Sie unter **Connectivity** Folgendes an:
   a. **Schlüsselpaar**: Wählen Sie ein Schlüsselpaar.
   b. **Active Directory**:
      i. Wählen Sie im Feld **Domain Name** einen Namen für die Domain aus oder geben Sie ihn ein.
         A. Bei von AWS gemanagten Active Directories werden Domänennamen im Dropdown-Menü angezeigt.
         B. Geben Sie für ein benutzerverwaltetes Active Directory einen Namen in das Feld **Suchen und Hinzufügen** ein, und klicken Sie auf **Hinzufügen**.
      ii. Geben Sie im Feld **DNS-Adresse** die DNS-IP-Adresse für die Domain ein. Sie können bis zu 3 IP-Adressen hinzufügen.

      Bei von AWS gemanagten Active Directories wird die DNS-IP-Adresse(n) im Dropdown-Menü angezeigt.

      iii. Geben Sie im Feld **Benutzername** den Benutzernamen für die Active Directory-Domäne ein.
      iv. Geben Sie im Feld **Passwort** ein Passwort für die Active Directory-Domain ein.
7. Geben Sie unter **Infrastruktur-Einstellungen** Folgendes an:
   a. **FSX für ONTAP-System**: Erstellen Sie ein neues FSX für ONTAP-Dateisystem oder verwenden Sie ein vorhandenes FSX für ONTAP-Dateisystem.
      i. * Erstellen Sie ein neues FSX für ONTAP*: Geben Sie Benutzernamen und Passwort ein.

      Ein neues FSX für ONTAP-Dateisystem kann 30 Minuten oder mehr der Installationszeit hinzufügen.

      ii. **Wählen Sie ein vorhandenes FSX für ONTAP**: Wählen Sie FSX für ONTAP-Namen aus dem Dropdown-Menü und geben Sie einen Benutzernamen und ein Passwort für das Dateisystem ein.

Stellen Sie für vorhandene FSX for ONTAP-Dateisysteme Folgendes sicher:

- Die an FSX for ONTAP angeschlossene Routinggruppe ermöglicht die Verwendung von Routen zu den Subnetzen für die Bereitstellung.
- Die Sicherheitsgruppe ermöglicht Datenverkehr aus den für die Bereitstellung verwendeten Subnetzen, insbesondere HTTPS- (443) und iSCSI- (3260) TCP-Ports.

b. **Größe des Datenlaufwerks**: Geben Sie die Kapazität des Datenlaufwerks ein und wählen Sie die Kapazitätseinheit aus.

8. Zusammenfassung:
   a. **Voreinstellung Vorschau**: Überprüfen Sie die Standardkonfigurationen, die von Quick Create festgelegt wurden.
   b. **Geschätzte Kosten**: Gibt eine Schätzung der Kosten an, die Ihnen entstehen könnten, wenn Sie die angezeigten Ressourcen bereitgestellt haben.
9. Klicken Sie Auf **Erstellen**.

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

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

Erweiterte Erstellung

Schritte

1. Melden Sie sich mit einem der"Konsolenerfahrungen" . Wählen Sie in der Kachel „Datenbanken“ die Option „Host bereitstellen“ und dann im Menü „Microsoft SQL Server“ aus.
2. Wählen Sie **Advanced Create**.
3. Wählen Sie für **Deployment model Failover Cluster Instance** oder **Single Instance** aus.
4. Geben Sie unter **AWS settings** Folgendes an:
   a. **AWS Credentials**: Wählen Sie AWS Credentials mit Automatisierungsberechtigungen aus, um den neuen Datenbank-Host bereitzustellen.

   Mit AWS-Anmeldeinformationen mit Lese-/Schreibberechtigungen kann Workload Factory den neuen Datenbankhost von Ihrem AWS-Konto innerhalb von Workload Factory bereitstellen und verwalten.

   Mit AWS-Anmeldeinformationen mit *Nur-Lese*-Berechtigungen kann Workload Factory eine CloudFormation-Vorlage generieren, die Sie in der AWS CloudFormation-Konsole verwenden können.

   Wenn Sie keine AWS-Anmeldeinformationen in Workload Factory verknüpft haben und den neuen Server in Workload Factory erstellen möchten, folgen Sie **Option 1**, um zur Seite „Anmeldeinformationen“ zu gelangen. Fügen Sie die erforderlichen Anmeldeinformationen und Berechtigungen für den Lese-/Schreibmodus für Datenbank-Workloads manuell hinzu.

   Wenn Sie das Formular zum Erstellen eines neuen Servers in Workload Factory ausfüllen möchten, um eine vollständige YAML-Dateivorlage für die Bereitstellung in AWS CloudFormation herunterzuladen, folgen Sie **Option 2**, um sicherzustellen, dass Sie über die erforderlichen Berechtigungen zum Erstellen des neuen Servers in AWS CloudFormation verfügen. Fügen Sie die erforderlichen Anmeldeinformationen und Berechtigungen für den schreibgeschützten Modus für Datenbank-Workloads manuell hinzu.

Optional können Sie eine teilweise ausgefüllte YAML-Dateivorlage aus der Codebox herunterladen, um den Stapel außerhalb von Workload Factory ohne Anmeldeinformationen oder Berechtigungen zu erstellen. Wählen Sie **CloudFormation** aus der Dropdown-Liste in der Codebox, um die YAML-Datei herunterzuladen.

b. **Region & VPC**: Wählen Sie eine Region und ein VPC-Netzwerk.

   Stellen Sie sicher, dass Sicherheitsgruppen für einen vorhandenen Schnittstellenendpunkt den Zugriff auf das HTTPS-Protokoll (443) auf die ausgewählten Subnetze ermöglichen.

   AWS-Service-Schnittstellen-Endpunkte (SQS, FSX, EC2, CloudWatch, Cloud-Bildung, SSM) und S3-Gateway-Endpunkt werden während der Implementierung erstellt, wenn nicht gefunden wird.

   VPC-DNS-Attribute `EnableDnsSupport` und `EnableDnsHostnames` werden geändert, um Auflösung der Endpunktadresse zu aktivieren, falls nicht bereits auf gesetzt `true`.

c. **Verfügbarkeitszonen**: Wählen Sie Verfügbarkeitszonen und Subnetze entsprechend dem von Ihnen ausgewählten Bereitstellungsmodell aus. Um eine hohe Verfügbarkeit zu gewährleisten, sollten Subnetze nicht dieselbe Routentabelle gemeinsam nutzen.

   FCI-Implementierungen werden nur in Konfigurationen mit Multiple Availability Zone (MAZ) FSX for ONTAP unterstützt.

   - Für Einzelinstanzbereitstellungen:
     - Wählen Sie im Feld **Cluster-Konfiguration - Knoten 1** aus dem Dropdown-Menü eine Verfügbarkeitszone aus der **Verfügbarkeitszone** und ein Subnetz aus dem **Subnetz** -Dropdown-Menü aus.
   - Für FCI-Bereitstellungen:
     - Wählen Sie im Feld **Clusterkonfiguration - Knoten 1** die primäre Verfügbarkeitszone für die MAZ FSX for ONTAP-Konfiguration aus dem Dropdown-Menü **Verfügbarkeitszone** und ein Subnetz aus der primären Verfügbarkeitszone aus dem Dropdown-Menü **Subnetz** aus.
     - Wählen Sie im Feld **Cluster-Konfiguration - Knoten 2** die sekundäre Verfügbarkeitszone für die MAZ FSX for ONTAP-Konfiguration aus dem Dropdown-Menü **Verfügbarkeitszone** und ein Subnetz aus der sekundären Verfügbarkeitszone aus dem Dropdown-Menü **Subnetz** aus.

d. **Sicherheitsgruppe**: Wählen Sie eine vorhandene Sicherheitsgruppe aus oder erstellen Sie eine neue Sicherheitsgruppe. Während der Implementierung eines neuen Servers werden drei Sicherheitsgruppen an die SQL Nodes (EC2 Instanzen) angeschlossen.

   i. Eine Sicherheitsgruppe für Workloads wird erstellt, um Ports und Protokolle zu ermöglichen, die für die Microsoft SQL- und Windows-Cluster-Kommunikation auf Knoten erforderlich sind.

   ii. Im Fall von AWS-Managed Active Directory wird die Sicherheitsgruppe, die an den Verzeichnisdienst angeschlossen ist, automatisch zu den Microsoft SQL-Knoten hinzugefügt, um die Kommunikation mit Active Directory zu ermöglichen.

   iii. Für ein vorhandenes FSX für ONTAP-Dateisystem wird die ihm zugeordnete Sicherheitsgruppe automatisch zu den SQL-Knoten hinzugefügt, die die Kommunikation mit dem Dateisystem ermöglicht. Wenn ein neues FSX für ONTAP-System erstellt wird, wird eine neue Sicherheitsgruppe für das FSX für ONTAP-Dateisystem erstellt und die gleiche Sicherheitsgruppe wird auch an SQL-Knoten angeschlossen.

Stellen Sie für ein benutzerverwaltetes Active Directory sicher, dass die auf der AD-Instanz konfigurierte Sicherheitsgruppe Datenverkehr von Subnetzen zulässt, die für die Bereitstellung verwendet werden. Die Sicherheitsgruppe sollte die Kommunikation mit den Active Directory-Domänencontrollern aus den Subnetzen ermöglichen, in denen EC2-Instanzen für Microsoft SQL konfiguriert sind.

5. Geben Sie unter **Anwendungseinstellungen** Folgendes an:
   a. Wählen Sie unter **SQL Server install type Lizenz included AMI** oder **Use Custom AMI** aus.
      i. Wenn Sie **Lizenz enthalten AMI** auswählen, geben Sie Folgendes an:
         A. **Betriebssystem**: Wählen Sie **Windows Server 2016**, **Windows Server 2019** oder **Windows Server 2022**.
         B. **Database Edition**: Wählen Sie **SQL Server Standard Edition** oder **SQL Server Enterprise Edition**.
         C. **Datenbankversion**: Wählen Sie **SQL Server 2016**, **SQL Server 2019** oder **SQL Server 2022**.
         D. **SQL Server AMI**: Wählen Sie aus dem Dropdown-Menü einen SQL Server AMI aus.
      ii. Wenn Sie **Benutzerdefiniertes AMI verwenden** auswählen, wählen Sie im Dropdown-Menü eine AMI aus.
   b. **SQL Server-Sammlung**: Wählen Sie eine Sammlung für den Server aus.

      Wenn der ausgewählte Sortiersatz nicht installationskompatibel ist, empfehlen wir, die Standardsortierung „SQL_Latin1_General_CP1_CI_AS“ auszuwählen.

   c. **Datenbankname**: Geben Sie den Namen des Datenbank-Clusters ein.
   d. **Datenbankanmeldeinformationen**: Geben Sie einen Benutzernamen und ein Passwort für ein neues Dienstkonto ein oder verwenden Sie vorhandene Dienstkontoanmeldeinformationen im Active Directory.

      Optional: Wählen Sie für das SQL Server-Dienstkonto die Option **Verwaltetes Dienstkonto verwenden**. Nutzen Sie diese Option, wenn Ihre Umgebung MSA (Managed Service Account) oder gMSA (Group Managed Service Account) verwendet, bei denen die Kennwortverwaltung von Active Directory übernommen wird.

6. Geben Sie unter **Connectivity** Folgendes an:
   a. **Schlüsselpaar**: Wählen Sie ein Schlüsselpaar, um sich sicher mit Ihrer Instanz zu verbinden.
   b. **Active Directory**: Geben Sie die folgenden Active Directory-Details an:
      i. Wählen Sie im Feld **Domain Name** einen Namen für die Domain aus oder geben Sie ihn ein.
         A. Bei von AWS gemanagten Active Directories werden Domänennamen im Dropdown-Menü angezeigt.
         B. Geben Sie für ein benutzerverwaltetes Active Directory einen Namen in das Feld **Suchen und Hinzufügen** ein, und klicken Sie auf **Hinzufügen**.
      ii. Geben Sie im Feld **DNS-Adresse** die DNS-IP-Adresse für die Domain ein. Sie können bis zu 3 IP-Adressen hinzufügen.

         Bei von AWS gemanagten Active Directories wird die DNS-IP-Adresse(n) im Dropdown-Menü angezeigt.

iii. Geben Sie im Feld **Benutzername** den Benutzernamen für die Active Directory-Domäne ein.

iv. Geben Sie im Feld **Passwort** ein Passwort für die Active Directory-Domain ein.

v. **Bevorzugter Domänencontroller**: Optional können Sie den bevorzugten Domänencontroller eingeben, der für den Beitritt zu Active Directory verwendet werden soll.

vi. **Bevorzugter Pfad zur Organisationseinheit**: Optional können Sie die bevorzugte Organisationseinheit (OU) im Active Directory eingeben, der beigetreten werden soll.

vii. **Ziel-Active-Directory-Gruppe**: Optional können Sie die Ziel-Active-Directory-Gruppe angeben, der die Computer hinzugefügt werden sollen.

7. Geben Sie unter **Infrastruktur-Einstellungen** Folgendes an:

a. **DB Instanztyp**: Wählen Sie den Typ der Datenbankinstanz aus dem Dropdown-Menü aus.

b. **FSX für ONTAP-System**: Erstellen Sie ein neues FSX für ONTAP-Dateisystem oder verwenden Sie ein vorhandenes FSX für ONTAP-Dateisystem.

i. * Erstellen Sie ein neues FSX für ONTAP*: Geben Sie Benutzernamen und Passwort ein.

Ein neues FSX für ONTAP-Dateisystem kann 30 Minuten oder mehr der Installationszeit hinzufügen.

ii. **Wählen Sie ein vorhandenes FSX für ONTAP**: Wählen Sie FSX für ONTAP-Namen aus dem Dropdown-Menü und geben Sie einen Benutzernamen und ein Passwort für das Dateisystem ein.

Stellen Sie für vorhandene FSX for ONTAP-Dateisysteme Folgendes sicher:

- Die an FSX for ONTAP angeschlossene Routinggruppe ermöglicht die Verwendung von Routen zu den Subnetzen für die Bereitstellung.
- Die Sicherheitsgruppe ermöglicht Datenverkehr aus den für die Bereitstellung verwendeten Subnetzen, insbesondere HTTPS- (443) und iSCSI- (3260) TCP-Ports.

c. **Snapshot Policy**: Standardmäßig aktiviert. Snapshots werden täglich erstellt und haben eine Aufbewahrungsfrist von 7 Tagen.

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

d. **Größe des Datenlaufwerks**: Geben Sie die Kapazität des Datenlaufwerks ein und wählen Sie die Kapazitätseinheit aus.

e. **Bereitgestellte IOPS**: Wählen Sie **automatisch** oder **vom Benutzer bereitgestellt**. Wenn Sie **User-provisioned** auswählen, geben Sie den IOPS-Wert ein.

f. **Durchsatzkapazität**: Wählen Sie die Durchsatzkapazität aus dem Dropdown-Menü.

In bestimmten Regionen können Sie eine Durchsatzkapazität von 4 Gbit/s wählen. Um eine Durchsatzkapazität von 4 GB/s bereitzustellen, muss Ihr FSX für ONTAP-Dateisystem mit mindestens 5,120 gib SSD-Speicherkapazität und 160,000 SSD-IOPS konfiguriert werden.

g. **Verschlüsselung**: Wählen Sie einen Schlüssel aus Ihrem Konto oder einen Schlüssel aus einem anderen Konto. Sie müssen den Verschlüsselungsschlüssel ARN von einem anderen Konto eingeben.

Die benutzerdefinierten FSX for ONTAP-Schlüssel werden basierend auf der Serviceinführbarkeit nicht aufgeführt. Wählen Sie einen geeigneten FSX-Verschlüsselungsschlüssel aus. Nicht-FSX-Verschlüsselungen verursachen Fehler bei der Servererstellung.

Von AWS gemanagte Schlüssel werden nach Servicetauglichkeit gefiltert.

h. **Tags**: Optional können Sie bis zu 40 Tags hinzufügen.

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

   i. Aktivieren Sie den Simple Notification Service.

   ii. Wählen Sie im Dropdown-Menü ein ARN aus.

j. **CloudWatch Monitoring**: Optional können Sie CloudWatch Monitoring aktivieren.

   Wir empfehlen die Aktivierung von CloudWatch zum Debuggen im Fehlerfall. Die Ereignisse, die in der AWS CloudFormation-Konsole angezeigt werden, haben eine hohe Ebene und geben nicht die Ursache an. Alle detaillierten Protokolle werden im Ordner in den EC2-Instanzen gespeichert `C:\cfn\logs` .

In CloudWatch wird eine Protokollgruppe mit dem Namen des Stacks erstellt. Unter der Protokollgruppe wird ein Protokollstrom für jeden Validierungs-Node und jeden SQL-Node angezeigt. CloudWatch zeigt den Skriptfortschritt an und liefert Informationen, um zu verstehen, ob und wann die Bereitstellung fehlschlägt.

a. **Resource Rollback**: Diese Funktion wird derzeit nicht unterstützt.

8. Zusammenfassung

   a. **Geschätzte Kosten**: Gibt eine Schätzung der Kosten an, die Ihnen entstehen könnten, wenn Sie die angezeigten Ressourcen bereitgestellt haben.

9. Klicken Sie auf **Create**, um den neuen Datenbank-Host bereitzustellen.

   Alternativ können Sie die Konfiguration speichern.

Schritt 2: Aktivieren Sie die Remoteverbindung auf dem Microsoft SQL Server

Nach der Serverbereitstellung aktiviert Workload Factory keine Remoteverbindung auf dem Microsoft SQL Server. Führen Sie die folgenden Schritte aus, um die Remoteverbindung zu aktivieren.

Schritte

1. Verwenden Sie die Computeridentität für NTLM unter "Netzwerksicherheit: Zulassen, dass das lokale System die Computeridentität für NTLM verwendet" in der Microsoft-Dokumentation.
2. Überprüfen Sie die Konfiguration der dynamischen Ports mithilfe "Beim Herstellen einer Verbindung zu SQL Server ist ein Netzwerk- oder instanzspezifischer Fehler aufgetreten" der Microsoft-Dokumentation.
3. Lassen Sie die erforderliche Client-IP oder das erforderliche Subnetz in der Sicherheitsgruppe zu.

Wie es weiter geht

Jetzt können Sie"Erstellen Sie eine Datenbank in Workload Factory für Datenbanken" .

Erstellen Sie einen PostgreSQL-Server in NetApp Workload Factory

Zum Erstellen eines neuen PostgreSQL-Servers oder Datenbankhosts in NetApp

Workload Factory für Datenbanken sind eine FSx für die ONTAP Dateisystembereitstellung und Ressourcen für Active Directory erforderlich.

Über diese Aufgabe

Informieren Sie sich vor dem Erstellen eines PostgreSQL-Servers aus Workload Factory über die verfügbaren Speicherbereitstellungstypen für die Datenbankhostkonfiguration, die Betriebsmodi von Workload Factory und die Anforderungen zum Abschließen dieses Vorgangs.

FSX für ONTAP-File-System-Implementierungen

Die Erstellung eines neuen PostgreSQL-Servers erfordert ein FSX für ONTAP-Dateisystem als Storage-Backend. Sie können ein bestehendes FSX für ONTAP-Dateisystem verwenden oder ein neues Dateisystem erstellen. Wenn Sie ein bestehendes FSX für ONTAP-Dateisystem als Datenbankserver-Storage-Back-End auswählen, erstellen wir eine neue Storage-VM für die PostgreSQL-Workloads.

+ FSx für ONTAP Dateisysteme verfügt über zwei PostgreSQL-Serverbereitstellungsmodelle: *High Availability (HA)* oder *Einzelinstanz*. Je nach ausgewähltem FSx for ONTAP -Bereitstellungsmodell werden unterschiedliche Ressourcen für das FSx for ONTAP -Dateisystem erstellt.

- **Bereitstellung von Hochverfügbarkeit**: Ein Dateisystem mit mehreren Verfügbarkeitszonen FSX für NetApp ONTAP wird bereitgestellt, wenn ein neues Dateisystem FSX für ONTAP für die Bereitstellung von Hochverfügbarkeit ausgewählt wird. Separate Volumes und LUNs werden für Daten-, Protokoll- und tempdb-Dateien für eine HA-Implementierung erstellt. Ein zusätzliches Volume und eine LUN werden für Quorum oder Witness Disk für Windows Cluster erstellt. DIE HA-Bereitstellung konfiguriert die Streaming-Replikation zwischen dem primären und dem sekundären PostgreSQL-Server.
- **Einzelinstanzbereitstellung**: Ein Einzelverfügbarkeitszonen-FSX für ONTAP-Dateisystem wird erstellt, wenn ein neuer PostgreSQL-Server erstellt wird. Darüber hinaus werden separate Volumes und LUNs für Daten-, Protokoll- und tempdb-Dateien erstellt.

Bevor Sie beginnen

Du musst haben "Berechtigungen zum Erstellen des Datenbankhosts erteilen" Erstellen Sie in Ihrem AWS-Konto einen neuen Datenbankhost in Workload Factory.

Erstellen Sie einen PostgreSQL-Server

Sie können die Bereitstellungsmodi *Quick create* oder *Advanced create* verwenden, um diese Aufgabe in der Workload Factory mit den Berechtigungen *Automate* zu erledigen. Die Codebox bietet auch folgende Tools: REST-API, AWS-CLI, AWS CloudFormation und Terraform. "Erfahren Sie, wie Sie Codebox für die Automatisierung verwenden".

> Bei der Verwendung von Terraform aus der Codebox werden der Code, den Sie kopieren oder herunterladen, ausgeblendet `fsxadmin` und `vsadmin` Passwörter. Sie müssen die Passwörter erneut eingeben, wenn Sie den Code ausführen. Zusätzlich zu den *Automate*-Modus -Berechtigungen müssen Sie die folgenden Berechtigungen für das Benutzerkonto hinzufügen: `iam:TagRole` Und `iam:TagInstanceProfile`. "Lernen Sie die Verwendung von Terraform von Codebox".

Schnelle Erstellung

In *Quick Create* ist HA das Standardbereitgabemodell, Windows 2016 die Standardversion von Windows und SQL 2019 Standard Edition die Standardversion von SQL.

Schritte

1. Melden Sie sich mit einem der "Konsolenerfahrungen"an.
2. Wählen Sie in der Kachel „Datenbanken“ die Option „Host bereitstellen“ und dann im Menü „PostgreSQL-Server“ aus.
3. Wählen Sie **Schnellerstelle**.
4. Geben Sie unter **Landezone** Folgendes an:
   a. **AWS Credentials**: Wählen Sie AWS Credentials mit Automatisierungsberechtigungen aus, um den neuen Datenbank-Host bereitzustellen.

      AWS-Anmeldeinformationen mit Lese-/Schreibberechtigungen ermöglichen der Workload Factory die Bereitstellung und Verwaltung des neuen Datenbankhosts von Ihrem AWS-Konto innerhalb der Workload Factory.

      Mit AWS-Anmeldeinformationen mit Nur-Lese-Berechtigungen kann die Workload Factory eine CloudFormation-Vorlage generieren, die Sie in der AWS CloudFormation-Konsole verwenden können.

      Wenn Sie keine AWS-Anmeldeinformationen in der Workload Factory haben und den neuen Server in der Workload Factory erstellen möchten, folgen Sie **Option 1**, um zur Seite Anmeldedaten zu gelangen. Fügen Sie die erforderlichen Anmeldeinformationen und Berechtigungen für den Lese-/Schreibmodus für Datenbank-Workloads manuell hinzu.

      Wenn Sie das Formular zum Erstellen eines neuen Servers in der Workload Factory ausfüllen möchten, damit Sie eine vollständige YAML-Dateivorlage für die Bereitstellung in AWS CloudFormation herunterladen können, folgen Sie **Option 2**, um sicherzustellen, dass Sie über die erforderlichen Berechtigungen zum Erstellen des neuen Servers in AWS CloudFormation verfügen. Fügen Sie die erforderlichen Anmeldeinformationen und Berechtigungen für den schreibgeschützten Modus für Datenbank-Workloads manuell hinzu.

      Optional können Sie eine teilweise ausgefüllte YAML-Dateivorlage aus der Codebox herunterladen, um den Stack außerhalb der Workload Factory ohne Anmeldeinformationen oder Berechtigungen zu erstellen. Wählen Sie **CloudFormation** aus der Dropdown-Liste in der Codebox aus, um die YAML-Datei herunterzuladen.

   b. **Region & VPC**: Wählen Sie eine Region und ein VPC-Netzwerk.

      Stellen Sie sicher, dass Sicherheitsgruppen für einen vorhandenen Schnittstellenendpunkt den Zugriff auf das HTTPS-Protokoll (443) auf die ausgewählten Subnetze ermöglichen.

      AWS-Serviceschnittstellen-Endpunkte (SQS, FSX, EC2, CloudWatch, CloudFormation, SSM) und der S3-Gateway-Endpunkt werden während der Bereitstellung erstellt, wenn nicht gefunden.

      VPC-DNS-Attribute `EnableDnsSupport` und `EnableDnsHostnames` werden geändert, um die Auflösung der Endpunktadresse zu aktivieren, wenn sie nicht bereits auf festgelegt sind `true`.

   c. **Verfügbarkeitszonen**: Wählen Sie Verfügbarkeitszonen und Subnetze aus.

HA-Implementierungen werden nur in Konfigurationen mit Multiple Availability Zone (MAZ) FSX for ONTAP unterstützt.

Subnetze sollten für hohe Verfügbarkeit nicht dieselbe Routentabelle verwenden.

i. Wählen Sie im Feld **Clusterkonfiguration - Knoten 1** die primäre Verfügbarkeitszone für die MAZ FSX for ONTAP-Konfiguration aus dem Dropdown-Menü **Verfügbarkeitszone** und ein Subnetz aus der primären Verfügbarkeitszone aus dem Dropdown-Menü **Subnetz** aus.

ii. Wählen Sie im Feld **Cluster-Konfiguration - Knoten 2** die sekundäre Verfügbarkeitszone für die MAZ FSX for ONTAP-Konfiguration aus dem Dropdown-Menü **Verfügbarkeitszone** und ein Subnetz aus der sekundären Verfügbarkeitszone aus dem Dropdown-Menü **Subnetz** aus.

5. Geben Sie unter **Anwendungseinstellungen** einen Benutzernamen und ein Passwort für **Datenbankanmeldeinformationen** ein.
6. Wählen Sie unter **Connectivity** ein Schlüsselpaar aus, um eine sichere Verbindung zu Ihrer Instanz herzustellen.
7. Geben Sie unter **Infrastruktur-Einstellungen** Folgendes an:
   a. **FSX für ONTAP-System**: Erstellen Sie ein neues FSX für ONTAP-Dateisystem oder verwenden Sie ein vorhandenes FSX für ONTAP-Dateisystem.
      i. * Erstellen Sie ein neues FSX für ONTAP*: Geben Sie Benutzernamen und Passwort ein.

      Ein neues FSX für ONTAP-Dateisystem kann 30 Minuten oder mehr der Installationszeit hinzufügen.

      ii. **Wählen Sie ein vorhandenes FSX für ONTAP**: Wählen Sie FSX für ONTAP-Namen aus dem Dropdown-Menü und geben Sie einen Benutzernamen und ein Passwort für das Dateisystem ein.

      Stellen Sie für vorhandene FSX for ONTAP-Dateisysteme Folgendes sicher:

      - Die an FSX for ONTAP angeschlossene Routinggruppe ermöglicht die Verwendung von Routen zu den Subnetzen für die Bereitstellung.
      - Die Sicherheitsgruppe ermöglicht Datenverkehr aus den für die Bereitstellung verwendeten Subnetzen, insbesondere HTTPS- (443) und iSCSI- (3260) TCP-Ports.

   b. **Größe des Datenlaufwerks**: Geben Sie die Kapazität des Datenlaufwerks ein und wählen Sie die Kapazitätseinheit aus.
8. Zusammenfassung:
   a. **Voreinstellung Vorschau**: Überprüfen Sie die Standardkonfigurationen, die von Quick Create festgelegt wurden.
   b. **Geschätzte Kosten**: Gibt eine Schätzung der Kosten an, die Ihnen entstehen könnten, wenn Sie die angezeigten Ressourcen bereitgestellt haben.
9. Klicken Sie Auf **Erstellen**.

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

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

Erweiterte Erstellung

Schritte

1. Melden Sie sich mit einem der "Konsolenerfahrungen"an.
2. Wählen Sie in der Kachel „Datenbanken“ die Option „Host bereitstellen“ und dann im Menü „PostgreSQL-Server“ aus.
3. Wählen Sie **Advanced Create**.
4. Wählen Sie unter **Deployment model Standalone Instance** oder **High Availability (HA)** aus.
5. Geben Sie unter **Landezone** Folgendes an:
   a. **AWS Credentials**: Wählen Sie AWS Credentials mit Automatisierungsberechtigungen aus, um den neuen Datenbank-Host bereitzustellen.

      AWS Zugangsdaten mit *Automate* Berechtigungen ermöglichen die werkseitige Implementierung und das Management des neuen Datenbank-Hosts über Ihr AWS-Konto innerhalb der Workload-Fabrik.

      Mit AWS-Anmeldeinformationen mit Nur-Lese-Berechtigungen kann die Workload Factory eine CloudFormation-Vorlage generieren, die Sie in der AWS CloudFormation-Konsole verwenden können.

      Wenn Sie keine AWS-Anmeldeinformationen in der Workload Factory haben und den neuen Server in der Workload Factory erstellen möchten, folgen Sie **Option 1**, um zur Seite Anmeldedaten zu gelangen. Fügen Sie die erforderlichen Anmeldeinformationen und Berechtigungen für den Lese-/Schreibmodus für Datenbank-Workloads manuell hinzu.

      Wenn Sie das Formular zum Erstellen eines neuen Servers in der Workload Factory ausfüllen möchten, damit Sie eine vollständige YAML-Dateivorlage für die Bereitstellung in AWS CloudFormation herunterladen können, folgen Sie **Option 2**, um sicherzustellen, dass Sie über die erforderlichen Berechtigungen zum Erstellen des neuen Servers in AWS CloudFormation verfügen. Fügen Sie die erforderlichen Anmeldeinformationen und Berechtigungen für den schreibgeschützten Modus für Datenbank-Workloads manuell hinzu.

      Optional können Sie eine teilweise ausgefüllte YAML-Dateivorlage aus der Codebox herunterladen, um den Stack außerhalb der Workload Factory ohne Anmeldeinformationen oder Berechtigungen zu erstellen. Wählen Sie **CloudFormation** aus der Dropdown-Liste in der Codebox aus, um die YAML-Datei herunterzuladen.

   b. **Region & VPC**: Wählen Sie eine Region und ein VPC-Netzwerk.

      Stellen Sie sicher, dass Sicherheitsgruppen für einen vorhandenen Schnittstellenendpunkt den Zugriff auf das HTTPS-Protokoll (443) auf die ausgewählten Subnetze ermöglichen.

      AWS-Service-Schnittstellen-Endpunkte (SQS, FSX, EC2, CloudWatch, Cloud-Bildung, SSM) und S3-Gateway-Endpunkt werden während der Implementierung erstellt, wenn nicht gefunden wird.

      VPC-DNS-Attribute `EnableDnsSupport` und `EnableDnsHostnames` werden geändert, um Auflösung der Endpunktadresse zu aktivieren, falls nicht bereits auf gesetzt `true`.

   c. **Verfügbarkeitszonen**: Wählen Sie Verfügbarkeitszonen und Subnetze aus.

      Für Einzelinstanzbereitstellungen

      Wählen Sie im Feld **Cluster-Konfiguration - Knoten 1** eine Verfügbarkeitszone aus dem Dropdown-Menü **Verfügbarkeitszone** und ein Subnetz aus dem Dropdown-Menü **Subnetz** aus.

Für HA-Bereitstellungen

i. Wählen Sie im Feld **Clusterkonfiguration - Knoten 1** die primäre Verfügbarkeitszone für die MAZ FSX for ONTAP-Konfiguration aus dem Dropdown-Menü **Verfügbarkeitszone** und ein Subnetz aus der primären Verfügbarkeitszone aus dem Dropdown-Menü **Subnetz** aus.

ii. Wählen Sie im Feld **Cluster-Konfiguration - Knoten 2** die sekundäre Verfügbarkeitszone für die MAZ FSX for ONTAP-Konfiguration aus dem Dropdown-Menü **Verfügbarkeitszone** und ein Subnetz aus der sekundären Verfügbarkeitszone aus dem Dropdown-Menü **Subnetz** aus.

d. **Sicherheitsgruppe**: Wählen Sie eine vorhandene Sicherheitsgruppe aus oder erstellen Sie eine neue Sicherheitsgruppe.

Während der Implementierung eines neuen Servers werden zwei Sicherheitsgruppen mit den SQL Nodes (EC2 Instanzen) verbunden.

i. Eine Sicherheitsgruppe für Workloads wird erstellt, um die für PostgreSQL erforderlichen Ports und Protokolle zu ermöglichen.

ii. Für ein neues FSX für ONTAP-Dateisystem wird eine neue Sicherheitsgruppe erstellt und an den SQL-Knoten angehängt. Für ein vorhandenes FSX for ONTAP-Dateisystem wird die ihm zugeordnete Sicherheitsgruppe automatisch zum PostgreSQL-Knoten hinzugefügt, der die Kommunikation mit dem Dateisystem ermöglicht.

6. Geben Sie unter **Anwendungseinstellungen** Folgendes an:

a. Wählen Sie das **Betriebssystem** aus dem Dropdown-Menü aus.

b. Wählen Sie die **PostgreSQL-Version** aus dem Dropdown-Menü aus.

c. **Datenbankservername**: Geben Sie den Namen des Datenbank-Clusters ein.

d. **Datenbankanmeldeinformationen**: Geben Sie einen Benutzernamen und ein Passwort für ein neues Dienstkonto ein oder verwenden Sie vorhandene Dienstkontoanmeldeinformationen im Active Directory.

7. Wählen Sie unter **Connectivity** ein Schlüsselpaar aus, um eine sichere Verbindung zu Ihrer Instanz herzustellen.

8. Geben Sie unter **Infrastruktur-Einstellungen** Folgendes an:

a. **DB Instanztyp**: Wählen Sie den Typ der Datenbankinstanz aus dem Dropdown-Menü aus.

b. **FSX für ONTAP-System**: Erstellen Sie ein neues FSX für ONTAP-Dateisystem oder verwenden Sie ein vorhandenes FSX für ONTAP-Dateisystem.

i. * Erstellen Sie ein neues FSX für ONTAP*: Geben Sie Benutzernamen und Passwort ein.

Ein neues FSX für ONTAP-Dateisystem kann 30 Minuten oder mehr der Installationszeit hinzufügen.

ii. **Wählen Sie ein vorhandenes FSX für ONTAP**: Wählen Sie FSX für ONTAP-Namen aus dem Dropdown-Menü und geben Sie einen Benutzernamen und ein Passwort für das Dateisystem ein.

Stellen Sie für vorhandene FSX for ONTAP-Dateisysteme Folgendes sicher:

- Die an FSX for ONTAP angeschlossene Routinggruppe ermöglicht die Verwendung von Routen zu den Subnetzen für die Bereitstellung.
- Die Sicherheitsgruppe ermöglicht Datenverkehr aus den für die Bereitstellung verwendeten Subnetzen, insbesondere HTTPS- (443) und iSCSI- (3260) TCP-Ports.

c. **Snapshot Policy**: Standardmäßig aktiviert. Snapshots werden täglich erstellt und haben eine Aufbewahrungsfrist von 7 Tagen.

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

d. **Größe des Datenlaufwerks**: Geben Sie die Kapazität des Datenlaufwerks ein und wählen Sie die Kapazitätseinheit aus.

e. **Bereitgestellte IOPS**: Wählen Sie **automatisch** oder **vom Benutzer bereitgestellt**. Wenn Sie **User-provisioned** auswählen, geben Sie den IOPS-Wert ein.

f. **Durchsatzkapazität**: Wählen Sie die Durchsatzkapazität aus dem Dropdown-Menü.

   In bestimmten Regionen können Sie eine Durchsatzkapazität von 4 Gbit/s wählen. Um eine Durchsatzkapazität von 4 GB/s bereitzustellen, muss Ihr FSX für ONTAP-Dateisystem mit mindestens 5,120 gib SSD-Speicherkapazität und 160,000 SSD-IOPS konfiguriert werden.

g. **Verschlüsselung**: Wählen Sie einen Schlüssel aus Ihrem Konto oder einen Schlüssel aus einem anderen Konto. Sie müssen den Verschlüsselungsschlüssel ARN von einem anderen Konto eingeben.

   Die benutzerdefinierten FSX for ONTAP-Schlüssel werden basierend auf der Serviceinführbarkeit nicht aufgeführt. Wählen Sie einen geeigneten FSX-Verschlüsselungsschlüssel aus. Nicht-FSX-Verschlüsselungen verursachen Fehler bei der Servererstellung.

   Von AWS gemanagte Schlüssel werden nach Servicetauglichkeit gefiltert.

h. **Tags**: Optional können Sie bis zu 40 Tags hinzufügen.

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

   i. Aktivieren Sie den Simple Notification Service.

   ii. Wählen Sie im Dropdown-Menü ein ARN aus.

j. **CloudWatch Monitoring**: Optional können Sie CloudWatch Monitoring aktivieren.

   Wir empfehlen die Aktivierung von CloudWatch zum Debuggen im Fehlerfall. Die Ereignisse, die in der AWS CloudFormation-Konsole angezeigt werden, haben eine hohe Ebene und geben nicht die Ursache an. Alle detaillierten Protokolle werden im Ordner in den EC2-Instanzen gespeichert `C:\cfn\logs`.

In CloudWatch wird eine Protokollgruppe mit dem Namen des Stacks erstellt. Unter der Protokollgruppe wird ein Protokollstrom für jeden Validierungs-Node und jeden SQL-Node angezeigt. CloudWatch zeigt den Skriptfortschritt an und liefert Informationen, um zu verstehen, ob und wann die Bereitstellung fehlschlägt.

a. **Resource Rollback**: Diese Funktion wird derzeit nicht unterstützt.

9. Zusammenfassung

   a. **Geschätzte Kosten**: Gibt eine Schätzung der Kosten an, die Ihnen entstehen könnten, wenn Sie die angezeigten Ressourcen bereitgestellt haben.

10. Klicken Sie auf **Create**, um den neuen Datenbank-Host bereitzustellen.

    Alternativ können Sie die Konfiguration speichern.

Wie es weiter geht

Sie können Benutzer, Remote-Zugriff und Datenbanken auf dem bereitgestellten PostgreSQL-Server manuell konfigurieren.

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 IRGENDEINER 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.