
Amazon Relational Database Service on VMware

User Guide



Amazon Relational Database Service on VMware: User Guide

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

What is Amazon RDS on VMware?	1
Features of Amazon RDS on VMware	1
Accessing Amazon RDS on VMware	1
How Amazon RDS on VMware works	2
Onboarding	2
Connecting	3
Provisioning and managing	3
Backing up and restoring	4
Terminology	5
VMware terminology	5
Amazon RDS on VMware terminology	5
RDS feature support	6
Setting up	10
Sign up for AWS	10
Create and configure an IAM user	10
Create an IAM user	10
Create access keys	12
SSL/TLS certificate requirements	12
Getting started	13
Complete the prerequisites	14
Onboard your vSphere cluster	20
Import the Installer VM certificate	31
Working with Amazon RDS on VMware	35
Installing the media	35
Supported media	35
Install the media	36
Troubleshooting	41
Choosing the DB instance class	42
DB instance class types	42
Terminology	42
Specifications	42
Creating a DB instance	43
Available settings	48
Creating additional custom AZs	49
Creating read replicas	50
Limitations	50
Creating a read replica	51
Promoting a read replica	52
Managing on-premises DB instances	53
Troubleshooting	54
Can't connect to the RDS connector	54
Custom AZ is unregistered or creating	54
Custom AZ is disconnected	55
Can't create a new custom AZ	55
Edge Router can't ping the ESXi Edge Gateway	55
Error in the OVF template	56
Proxy server connection problems or changes	56
Document history	57
Earlier Updates	58
AWS glossary	59

What is Amazon RDS on VMware?

Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. It provides cost-efficient, resizeable capacity for an industry-standard relational database and manages common database administration tasks. Amazon RDS includes Amazon RDS on VMware, which provides these services in an on-premises, private environment. For more information about Amazon RDS, see the [Amazon RDS User Guide](#).

Using Amazon RDS on VMware, you can set up, operate, and scale databases in VMware environments. Amazon RDS on VMware automates time-consuming database management tasks, such as provisioning, patching, and backups. This automation frees you to focus on developing and tuning your applications.

Amazon RDS on VMware supports Amazon RDS for MySQL, PostgreSQL, and Microsoft SQL Server databases in customer-owned private cloud environments. These databases can run workloads that must remain on-premises in compliance with security, privacy, regulatory, or data sovereignty policies. You can get started by downloading Amazon RDS on VMware onto a VMware vSphere cluster and installing it.

Amazon RDS on VMware reduces operational overhead for database management in your on-premises VMware data centers. Amazon RDS on VMware automates administrative tasks including software installation, patching, monitoring, and backups. Amazon RDS on VMware includes a software package for your VMware vSphere environment that provides easy provisioning, automatic monitoring, and simple manageability of your databases, enabling database management through a dedicated connection to the AWS Region.

To learn more about Amazon RDS on VMware, see the following topics:

- [Features of Amazon RDS on VMware \(p. 1\)](#)
- [Accessing Amazon RDS on VMware \(p. 1\)](#)
- [How Amazon RDS on VMware works \(p. 2\)](#)
- [Terminology \(p. 5\)](#)
- [Support for RDS features in Amazon RDS on VMware \(p. 6\)](#)

To start work with Amazon RDS on VMware, see [Setting up Amazon RDS on VMware \(p. 10\)](#).

Features of Amazon RDS on VMware

Amazon RDS on VMware provides the following features:

- Automates administrative tasks for your on-premises databases in VMware vSphere environments
- Provides a simple interface for creating, modifying, and managing your databases using the AWS Management Console, AWS CLI, and RDS API
- Enables easy scaling of the compute, storage, and memory resources in your on-premises DB instance
- Provides CloudWatch metrics for your on-premises databases
- Enables manual or automatic backup of your on-premises databases
- Supports restoring a DB instance from a snapshot and point-in-time restore

Accessing Amazon RDS on VMware

Amazon RDS on VMware provides a web-based user interface, the AWS Management Console. You can sign into the AWS Management Console and manage your on-premises databases.

If you prefer to use a command line interface, you can use the AWS CLI. The RDS API provides a programmatic interface.

How Amazon RDS on VMware works

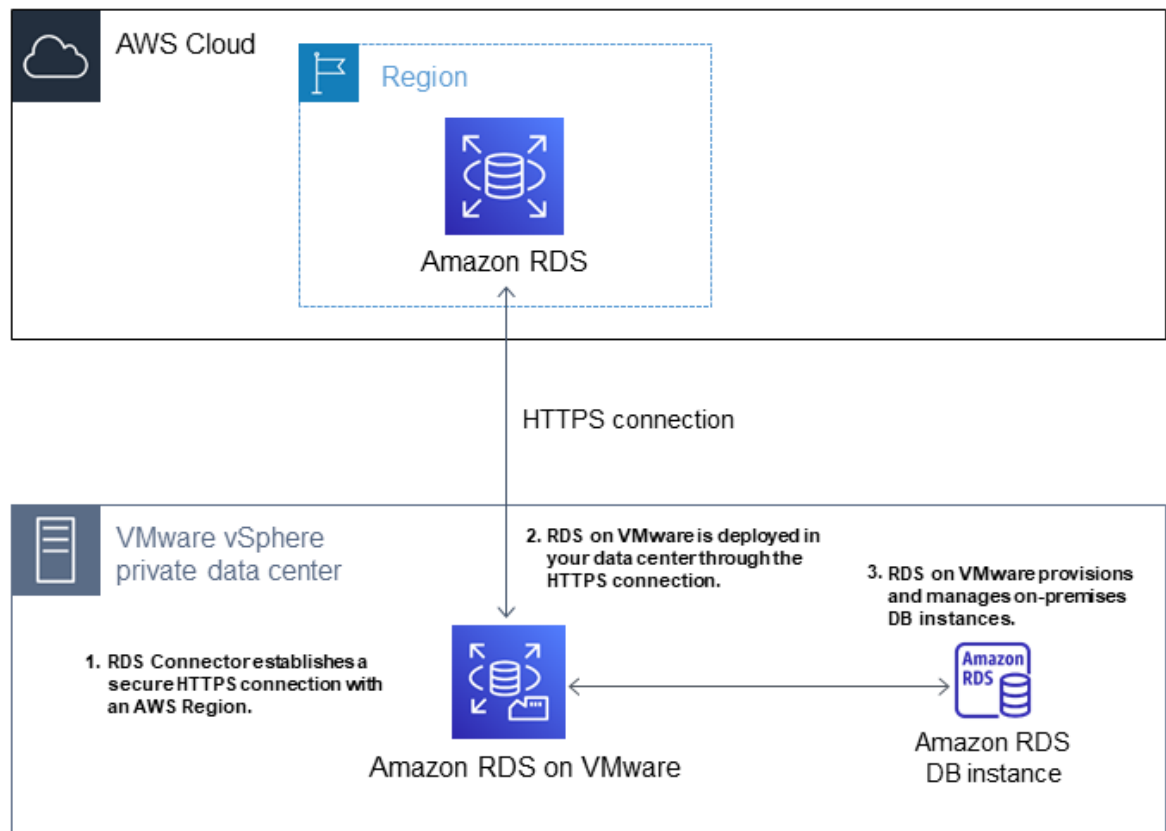
The Amazon RDS on VMware architecture uses the RDS connector, a software appliance for your VMware vSphere environment. With the RDS connector, you can manage on-premises DB instances through an HTTPS connection.

Topics

- [Onboarding Amazon RDS on VMware \(p. 2\)](#)
- [Connecting to an AWS Region from a vSphere cluster \(p. 3\)](#)
- [Provisioning and managing on-premises DB instances \(p. 3\)](#)
- [Backing up and restoring on-premises DB instances \(p. 4\)](#)

Onboarding Amazon RDS on VMware

The following diagram shows the onboarding process for Amazon RDS on VMware.

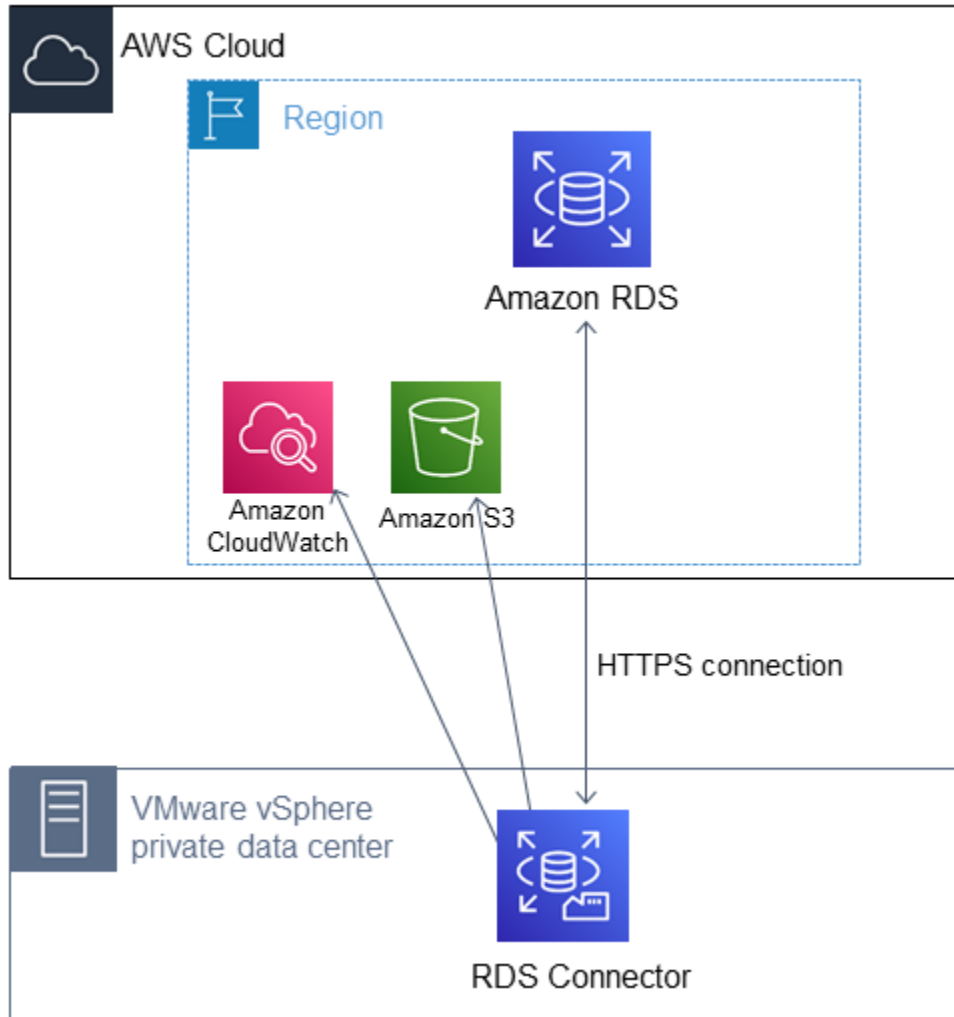


To onboard Amazon RDS on VMware, you create a custom Availability Zone from the AWS Management Console in the AWS Region. You then download the Amazon RDS on VMware Installer from the AWS Management Console to the on-premises vSphere cluster where you want to use the service. When you run the Installer, it deploys the local components for Amazon RDS on VMware on your vSphere cluster.

and connects your cluster to the Amazon RDS service running in the AWS Region. You can then create a new database using the AWS Management Console, AWS CLI, or RDS API by choosing the appropriate database engine and DB instance class size.

Connecting to an AWS Region from a vSphere cluster

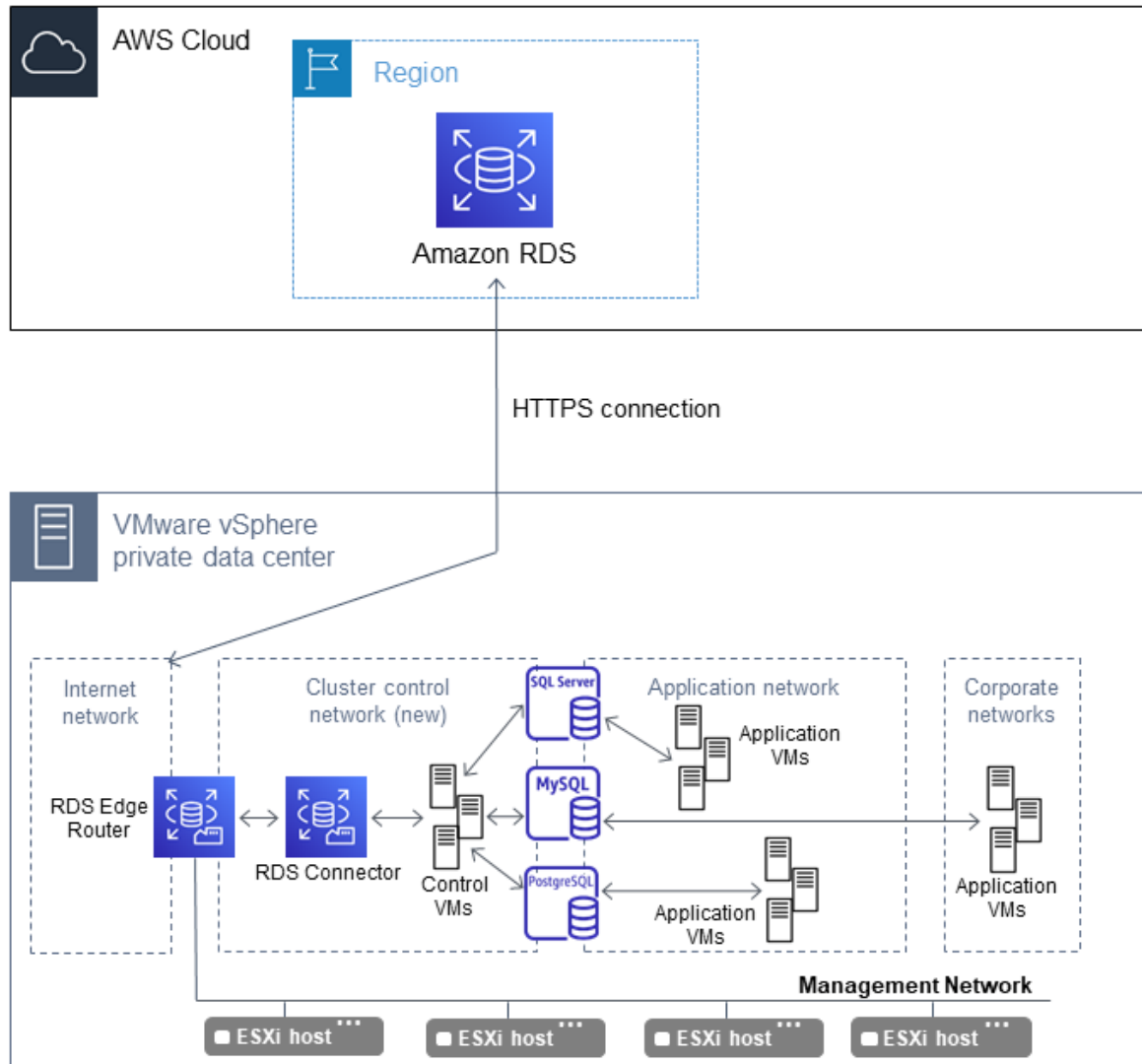
The RDS connector uses an outbound HTTPS connection to connect to an AWS Region.



The connection enables communication between your vSphere cluster and the AWS Region. Amazon RDS on VMware uses the connection for management activities. It also uses the connection to send information, such as Amazon CloudWatch data, from the vSphere cluster to the AWS Region.

Provisioning and managing on-premises DB instances

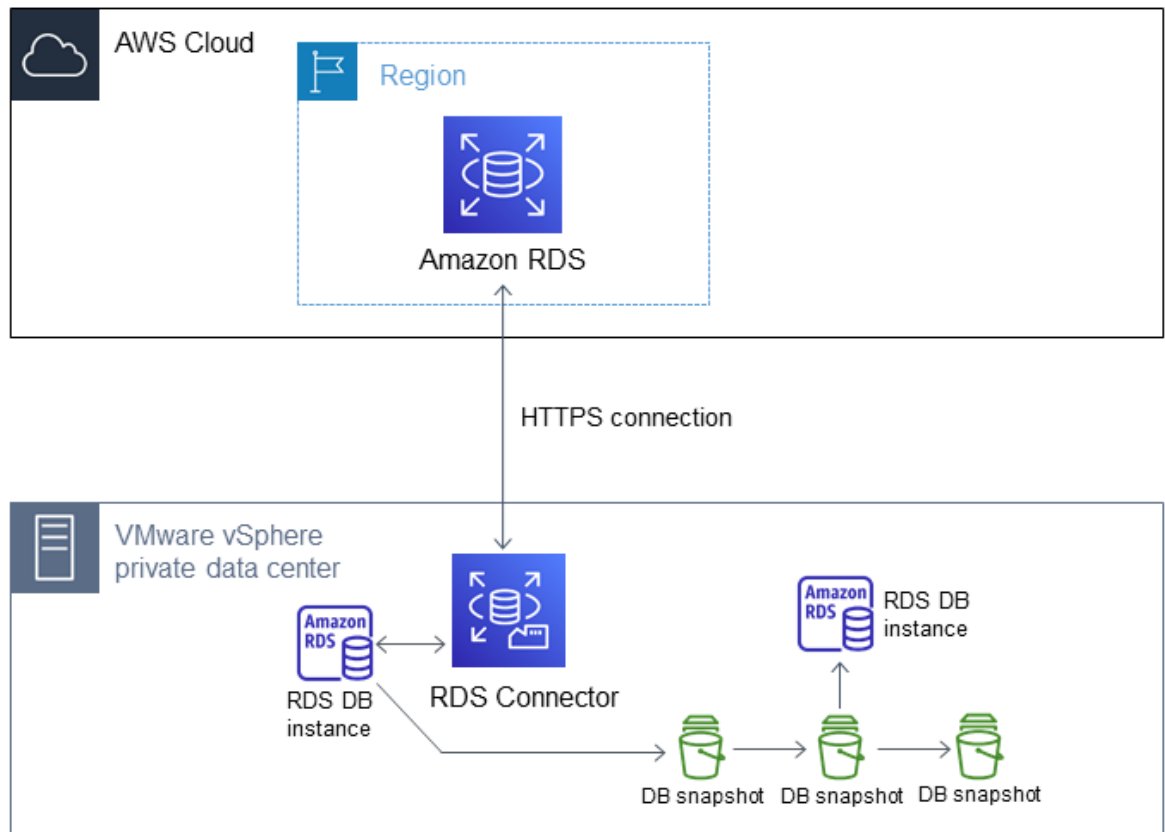
To provision and manage DB instances, you create a Cluster Control Network in your vSphere cluster. You can provision several DB instances and choose from different DB engine types, such as a MySQL, PostgreSQL, and Microsoft SQL Server.



You also create an Application Network in your vSphere cluster. Your applications, users, and database administrators (DBAs) use this network to interact with Amazon RDS on VMware DB instances.

Backing up and restoring on-premises DB instances

You can create automated or manual snapshots of your DB instances. These snapshots are stored on your vSphere cluster.



You can restore from a snapshot or to a point in time to create new on-premises DB instances.

Terminology

Using Amazon RDS on VMware requires an understanding of VMware terminology and of terminology that is specific to Amazon RDS on VMware.

VMware terminology

This guide uses VMware terminology, such as data center, cluster, and resource pools. For information about VMware terminology, see the [VMware vSphere Documentation](#).

Amazon RDS on VMware terminology

This guide uses the following Amazon RDS on VMware terminology.

Topics

- [Custom Availability Zones](#) (p. 6)
- [RDS Edge Router](#) (p. 6)
- [RDS Connector](#) (p. 6)
- [RDS Cluster Control Network](#) (p. 6)
- [Application Network](#) (p. 6)

Custom Availability Zones

Each AWS Region is a separate geographic area. Each AWS Region has multiple, isolated locations known as Availability Zones (AZs). For more information, see [Regions and Availability Zones](#) in the *Amazon RDS User Guide*.

A *custom Availability Zone (custom AZ)* is an on-premises AZ that is integrated with your vSphere cluster. Custom AZs are similar to Amazon RDS AZs, but each custom AZ is limited to a specific VMware environment.

RDS Edge Router

The *RDS Edge Router* is a software package that you install in your network. It's configured as a router between the public internet, the ESXi Host network (the Management Network), and the Cluster Control Network. It also acts as an authoritative Domain Name Service (DNS) server and Dynamic Host Configuration Protocol (DHCP) server for the RDS Cluster Control Network.

RDS Connector

The *RDS Connector* is a software package that is installed on the on-premises vSphere environment. It manages the interaction between various software components so that the on-premises environment can interact with the on-premises databases.

RDS Cluster Control Network

The *RDS Cluster Control Network* controls and monitors traffic for Amazon RDS on VMware. All Amazon RDS on VMware components and database instances have one interface on this network.

This network is analogous to the network that Amazon RDS uses to manage your databases. It's similar to a virtual private cloud (VPC) based on the Amazon Virtual Private Cloud (Amazon VPC) service, but in your environment. All the DB instances are managed by control virtual machines (VMs). Some of the VMs are built by AWS and some are built by VMware. Each Amazon RDS on VMware VM and DB instance has one interface on this network.

Application Network

The *Application Network* is the network that your applications use to interact with the DB instances that you provision on Amazon RDS on VMware.

Support for RDS features in Amazon RDS on VMware

The primary use case for Amazon RDS on VMware is to support the Amazon RDS service with your choice of database on a VMware infrastructure.

The following table shows current Amazon RDS on VMware support for Amazon RDS features.

Feature	Supported	Notes	More Information
DB instance provisioning	Yes	—	Creating an Amazon RDS DB instance
Modifying the master user password	No	—	Modifying an Amazon RDS DB instance

Amazon Relational Database
Service on VMware User Guide
RDS feature support

Feature	Supported	Notes	More Information
Modifying the DB engine version	Yes	For the PostgreSQL DB engine, RDS on VMware supports version 10.9-R1 and 10.10-R1. For the Microsoft SQL Server and MySQL DB engines, RDS on VMware currently only supports one DB engine version.	Modifying an Amazon RDS DB instance
Renaming a DB instance	Yes	—	Renaming a DB instance
Rebooting a DB instance	Yes	—	Rebooting a DB instance
Stopping a DB instance	No	—	Stopping an Amazon RDS DB instance temporarily
Starting a DB instance	No	—	Starting an Amazon RDS DB instance that was previously stopped
Multi-AZ deployments	No	—	High availability (Multi-AZ) for Amazon RDS
DB parameter groups	No	—	Working with DB parameter groups
Read replicas	Yes	Currently, this feature is supported for MySQL and PostgreSQL.	Working with read replicas
Encryption at rest and compliance certification	No	—	Encrypting Amazon RDS resources
Tagging Amazon RDS resources	Yes	—	Tagging Amazon RDS resources
Option groups	No	—	Working with option groups
Modifying the maintenance window	Yes	Modifying the maintenance window is supported, but you can't view or apply maintenance updates.	Maintaining a DB instance
Modifying the backup window	No	—	Working with backups

Amazon Relational Database
Service on VMware User Guide
RDS feature support

Feature	Supported	Notes	More Information
DB instance scaling	Yes	Modify the on-premises DB instance class to scale the DB instance.	Modifying an Amazon RDS DB instance Choosing the on-premises DB instance class (p. 42)
Manual and automatic DB snapshots	Yes	All DB snapshots are stored locally. DB snapshots aren't stored in Amazon S3. DB snapshot copying and sharing aren't supported.	Creating a DB snapshot
Restoring from a DB snapshot	Yes	—	Restoring from a DB snapshot
Point-in-time recovery	Yes	Currently, this feature is supported for Microsoft SQL Server, MySQL, and PostgreSQL.	Restoring a DB instance to a specified time
Enhanced Monitoring	No	—	Enhanced Monitoring
Amazon CloudWatch monitoring	Yes	—	Monitoring with Amazon CloudWatch
Publishing database engine logs to Amazon CloudWatch Logs	No	—	Publishing database engine logs to Amazon CloudWatch Logs
Event notification	No	—	Using Amazon RDS event notification
Amazon RDS Performance Insights	No	—	Using Amazon RDS Performance Insights
Stored procedures for Amazon RDS for MySQL	Yes	—	MySQL on Amazon RDS SQL reference
Automatic minor engine version upgrade	Yes	RDS on VMware doesn't support importing a DB instance from Amazon S3, so enabling auto minor version upgrade during this operation doesn't apply to RDS on VMware DB instances.	Automatically upgrading the minor engine version
Replication with external databases (MySQL)	No	—	Replication with a MySQL or MariaDB instance running external to Amazon RDS

Amazon Relational Database
Service on VMware User Guide
RDS feature support

Feature	Supported	Notes	More Information
Importing backups from Amazon S3 (Microsoft SQL Server)	No	—	Importing and exporting SQL Server databases
Reserved DB instances	Yes	<p>You can reserve RDS on VMware DB instances for a period of time. Reserved RDS on VMware DB instances provide a discount compared to on-demand DB instance pricing.</p> <p>Currently, reserved RDS on VMware DB instances are only available with the All Upfront offering type for a one-year term.</p> <p>Find terms and definitions for RDS on VMware reserved DB instances at RDS on VMware pricing.</p>	Reserved DB instances for Amazon RDS (for general information about reserved DB instances)

Note

Amazon RDS DB instance classes and storage types don't apply to Amazon RDS on VMware.

Setting up Amazon RDS on VMware

If you've already signed up for Amazon Web Services (AWS), you can start using Amazon RDS on VMware immediately by completing the tasks in [Getting started with Amazon RDS on VMware \(p. 13\)](#).

If you haven't signed up for AWS yet, complete the following tasks to get set up to use Amazon RDS on VMware.

Topics

- [Sign up for AWS \(p. 10\)](#)
- [Create and configure an IAM user \(p. 10\)](#)
- [SSL/TLS certificate requirements \(p. 12\)](#)

Sign up for AWS

If you have an AWS account already, skip to the next section, [Create and configure an IAM user \(p. 10\)](#).

If you don't have an AWS account, you can use the following procedure to create one.

To create a new AWS account

1. Open <https://portal.aws.amazon.com/billing/signup>.
2. Follow the online instructions.

Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

Create and configure an IAM user

After you create an AWS account and successfully connect to the AWS Management Console, you can create an AWS Identity and Access Management (IAM) user. Instead of signing in with your AWS root account, we recommend that you use an IAM administrative user with Amazon RDS.

One way to do this is to create a new IAM user and grant it administrator permissions. Or you can add an existing IAM user to an IAM group with Amazon RDS administrative permissions. You can then access AWS from a special URL using the credentials for the IAM user.

Topics

- [Create an IAM user \(p. 10\)](#)
- [Create access keys \(p. 12\)](#)

Create an IAM user

If you signed up for AWS but haven't created an IAM user for yourself, you can create one using the IAM console.

To create an administrator user for yourself and add the user to an administrators group (console)

1. Sign in to the [IAM console](#) as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.

Note

We strongly recommend that you adhere to the best practice of using the **Administrator** IAM user that follows and securely lock away the root user credentials. Sign in as the root user only to perform a few [account and service management tasks](#).

2. In the navigation pane, choose **Users** and then choose **Add user**.
3. For **User name**, enter **Administrator**.
4. Select the check box next to **AWS Management Console access**. Then select **Custom password**, and then enter your new password in the text box.
5. (Optional) By default, AWS requires the new user to create a new password when first signing in. You can clear the check box next to **User must create a new password at next sign-in** to allow the new user to reset their password after they sign in.
6. Choose **Next: Permissions**.
7. Under **Set permissions**, choose **Add user to group**.
8. Choose **Create group**.
9. In the **Create group** dialog box, for **Group name** enter **Administrators**.
10. Choose **Filter policies**, and then select **AWS managed - job function** to filter the table contents.
11. In the policy list, select the check box for **AdministratorAccess**. Then choose **Create group**.

Note

You must activate IAM user and role access to Billing before you can use the **AdministratorAccess** permissions to access the AWS Billing and Cost Management console. To do this, follow the instructions in [step 1 of the tutorial about delegating access to the billing console](#).

12. Back in the list of groups, select the check box for your new group. Choose **Refresh** if necessary to see the group in the list.
13. Choose **Next: Tags**.
14. (Optional) Add metadata to the user by attaching tags as key-value pairs. For more information about using tags in IAM, see [Tagging IAM entities](#) in the *IAM User Guide*.
15. Choose **Next: Review** to see the list of group memberships to be added to the new user. When you are ready to proceed, choose **Create user**.

You can use this same process to create more groups and users and to give your users access to your AWS account resources. To learn about using policies that restrict user permissions to specific AWS resources, see [Access management](#) and [Example policies](#).

To sign in as the new IAM user, first sign out of the AWS Management Console. Then use the following URL, where *your_aws_account_id* is your AWS account number without the hyphens. For example, if your AWS account number is 1234-5678-9012, your AWS account ID is 123456789012.

```
https://your_aws_account_id.signin.aws.amazon.com/console/
```

Enter the IAM user name and password that you just created. When you're signed in, the navigation bar displays "*your_user_name @ your_aws_account_id*".

If you don't want the URL for your sign-in page to contain your AWS account ID, you can create an account alias. From the IAM dashboard, choose **Customize** and enter an alias, such as your company name. To sign in after you create an account alias, use the following URL.

```
https://your_account_alias.signin.aws.amazon.com/console/
```

To verify the sign-in link for IAM users for your account, open the IAM console and check under **AWS Account Alias** on the dashboard.

Create access keys

You can also create access keys for your AWS account. These access keys can be used to access AWS through the AWS Command Line Interface (AWS CLI) or through the Amazon RDS API. For more information, see [Understanding and getting your AWS credentials](#), [Installing the AWS CLI](#), and the [Amazon RDS API Reference](#).

SSL/TLS certificate requirements

Amazon RDS on VMware uses the latest AWS certificates (2019) for encryption. For information about downloading these certificates, see [Using SSL/TLS to encrypt a connection to a DB instance](#) in the *RDS User Guide*.

Getting started with Amazon RDS on VMware

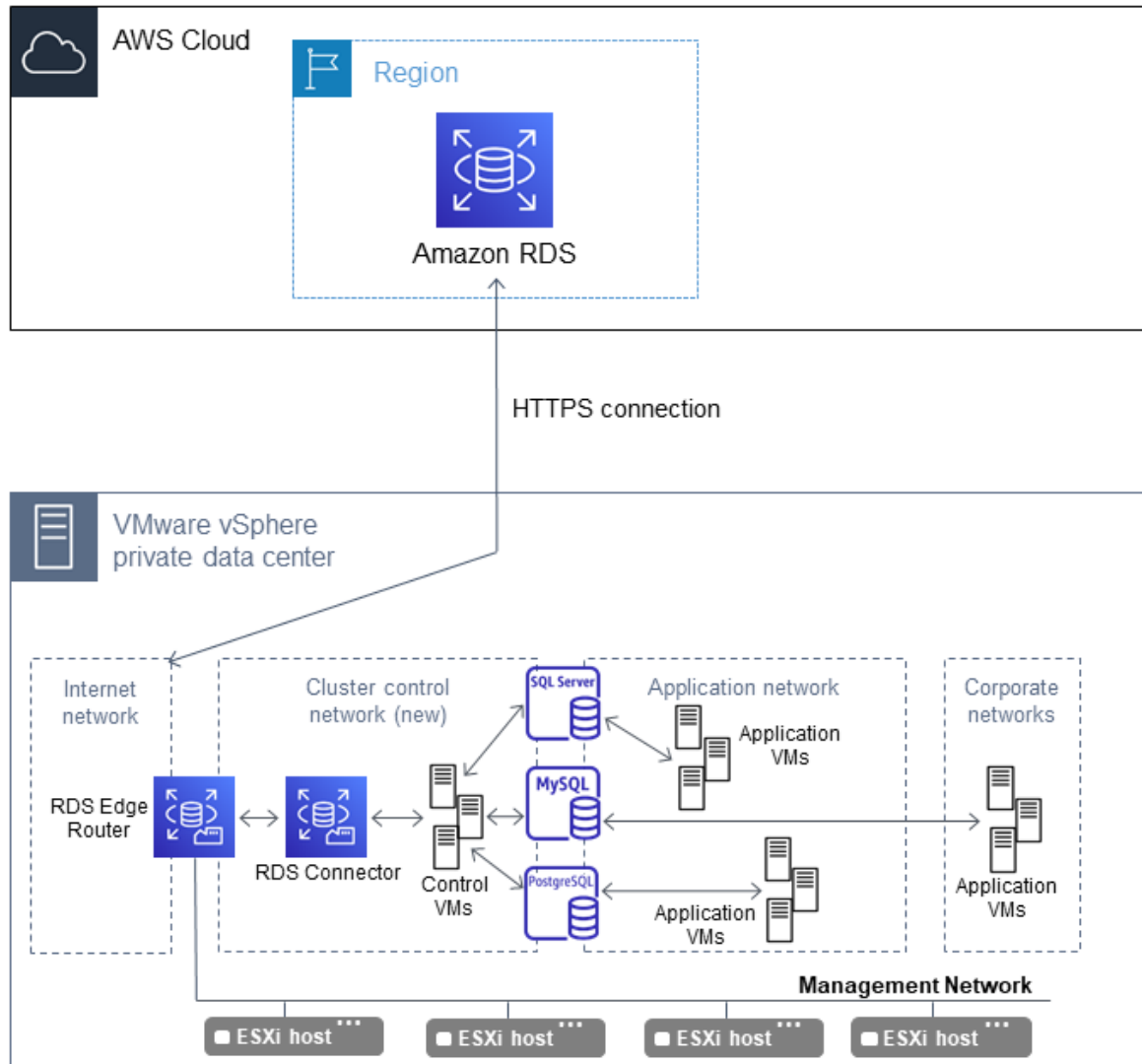
To get started with Amazon RDS on VMware, you onboard a new vSphere cluster as a custom Availability Zone (custom AZ) for Amazon RDS.

You only onboard a particular vSphere cluster once. After you complete the onboarding tasks successfully, you don't need to repeat the tasks for the same vSphere cluster. If you have already configured the vSphere cluster for Amazon RDS on VMware, and you want to add another custom AZ to it, see [Creating additional custom AZs in an AWS Region \(p. 49\)](#).

During onboarding, you configure the following networks.

Network name	Purpose	DHCP server required?
Cluster Control Network	New network for communication between Amazon RDS management virtual machines (VMs) and database VMs	No. Amazon RDS runs its own Dynamic Host Configuration Protocol (DHCP) server on this network.
Internet Network	New or existing network for outbound internet connectivity for Amazon RDS VMs and for establishing an HTTPS connection to the Amazon RDS service	Yes. This network must advertise a default route.
Application Network	New or existing network for communication between your applications and Amazon RDS database VMs	Yes. This network can advertise a default route, but the corresponding default route is not installed.
Management Network	Existing network for communication between Amazon RDS management VMs and ESXi hosts	No. You must provide a static IP address during onboarding.

The following illustration shows how your Amazon RDS on VMware configuration looks after onboarding is complete.



Important

Currently, Amazon RDS on VMware is available only in the US East (N. Virginia) AWS Region.

To create a custom AZ, you take the following two steps:

1. [Complete the prerequisites \(p. 14\)](#)
2. [Onboard your vSphere cluster \(p. 20\)](#)

For more details about working with Amazon RDS on VMware, see [Working with Amazon RDS on VMware \(p. 35\)](#).

Complete the prerequisites

Before you onboard your vSphere cluster, complete the following prerequisites.

To prepare to onboard your vSphere cluster for Amazon RDS on VMware

1. Complete the tasks in [Setting up Amazon RDS on VMware \(p. 10\)](#).
2. Make sure that you have a business-level or enterprise-level AWS Support plan.

Amazon RDS on VMware requires a business-level or enterprise-level AWS Support plan. For information about AWS Support plans, see [Compare AWS Support Plans](#).

3. Configure your VMware environment for resiliency and high availability.

Before deploying Amazon RDS on VMware, we recommend that you configure the resiliency and high availability options available on the underlying VMware platform. VMware offers a variety of resiliency and high availability features to protect your infrastructure and ensure continued infrastructure operation. We recommend configuring the following VMware features.

Amazon RDS on VMware includes a set of VMs running on the on-premises vSphere cluster. In case of an ESXi host failure, you can use vSphere HA to automatically start these VMs on another ESXi host. For more information, see [Create a vSphere HA Cluster](#) in the VMware documentation. You can also find information about enabling vCenter HA at [Configure vCenter HA Basic Option with the vSphere Web Client](#) in the VMware documentation.

You can also use vCenter alarms to alert you about the health of the underlying ESXi hosts on which you are running Amazon RDS on VMware. For more information, see [Using Alarms](#) in the VMware documentation. If you get an alarm on ESXi host degradation, you can use VMware vMotion. VMware vMotion can migrate the Amazon RDS on VMware VMs running on the host that has an issue to another ESXi host. You can also use this capability during scheduled maintenance of your ESXi hosts. For more information on vMotion, see [Migration with vMotion](#) in the VMware documentation.

Note

vMotion storage is not supported with Amazon RDS on VMware.

Finally, you can enable a Distributed Resource scheduler (DRS) on your vSphere cluster to load balance the host memory and CPU. For more information, see [Enable vSphere HA and vSphere DRS in a Cluster \(MSCS\)](#) in the VMware documentation.

4. Meet the vSphere cluster requirements.
 - a. Meet the following data center requirements:
 - Select or create a virtual data center using vSphere Client or vSphere Web Client.
 - Ensure that you have Admin privilege for the virtual data center.
 - b. Meet the following vSphere storage requirements:
 - All of the ESXi servers on the cluster must be connected to the same datastore.
 - Ensure that your vSphere cluster is backed by a storage device that presents a single datastore using VMware Platform API - VMFS compliant.

Note

Currently, working with a local datastore is not supported.

- c. Meet the following vSphere hardware requirements:
 - 24 vCPU
 - 24 GB memory
 - 180 GB of storage
5. Meet the following vSphere environment requirements:
 - VMware vCenter Server version 6.5 or 6.7

- VMware vSphere Server Enterprise Edition 6.5 or 6.7

For specific release versions, see the [VMware Product Interoperability Matrices](#).

6. Gather the information required for onboarding.
 - a. Gather the following information about your vCenter configuration:
 - **vCenter NTP Server** – The DNS name or IPv4 address of the Network Time Protocol (NTP) server to which your ESXi hosts sync.
 - **DNS server** – The IP address of the DNS server for the vCenter Server that is authoritative for your vCenter Server's private DNS zone.
 - **Domain** – The private DNS subdomain of your vCenter Server.
 - **vCenter DNS** – The DNS name of your vSphere Automation API endpoint.
 - **vCenter Server Certificate** – A PEM-formatted certificate used by your vCenter Server deployment for HTTPS and TLS.
 - b. Gather the following information about your ESXi host network (Management Network):
 - **Subnet** – The network address of the Management Network.
 - **Netmask** – The subnet mask (in dotted quad notation, for example 255.255.255.128) of the Management Network.
 - **Gateway** – The gateway (router) for the Management Network.
 - **Edge Router IP** – An unused IPv4 address on the Management Network, to be statically assigned to the third network interface on the virtual machine (VM) for the RDS Edge Router.

This is the only interface that will interact with your ESXi Management Network.

Note

Make sure that all of the vCenter Server and ESXi hosts are in the same Management Network or can be reached using the default gateway.

7. Meet networking and access requirements.

All the hosts (including the NTP server, vCenter, and DNS server) must fit one of two categories. Either they must be on the Management Network subnet (with the ESXi network as part of the same virtual LAN). Or they must be reachable using the default gateway on the Internet Network (ETH1 on Edge Router).

- a. Meet the requirements for the Internet Network:
 - A network with outbound internet access, with a minimum speed of 1 Gbps.
 - All public and internal URLs, including the vCenter fully qualified domain name (FQDN), must be DNS-resolved.
 - There must be access to public AWS service endpoints over HTTPS.
 - For Microsoft SQL Server DB instances, access to Microsoft endpoints by using HTTPS, such as *.microsoft.com (http://microsoft.com/), must be reachable.

This requirement doesn't apply to MySQL or PostgreSQL DB instances.

- There must be DHCP services on this interface with the default gateway.
 - The DHCP broadcast must not cross over an up-link.
 - The network must allow outbound and related inbound response traffic to TCP port 443 (HTTPS to access public AWS service endpoints).
- b. Meet the requirements for the Cluster Control Network:
 - There must be a new network dedicated to Amazon RDS on VMware with a unique virtual LAN (VLAN) ID.

- Amazon RDS on VMware assigns IP addresses in the predefined 54.239.236.0/22 range using DHCP using the RDS Edge Router virtual appliance. This address is a public IP address range managed by AWS but set aside for Amazon RDS on VMware use. Therefore, it is important that the Cluster Control Network is isolated (using VLAN tagging).
- The network administrator must verify that broadcast packets don't cross over an up-link. Broadcast packets must be associated with a unique VLAN ID.
- The distributed port group must be accessible from all ESXi hosts that are part of the selected vSphere cluster.
- The distributed port group must use the elastic "port allocation" flag.
- After the distributed port group is created, you must provision a VMKernel adapter with replication and replication NFC traffic enabled. This vmkernel adapter should use DHCP because it receives an address from Amazon RDS on VMware.

Note

Provision VMKernel adapters for each of the cluster's ESXi hosts into the Cluster Control Network.

DHCP services are not required on the Cluster Control Network.

- c. Meet the requirements for the Application Network:
- Provide an existing network where you plan to deploy the DB instances. Each DB instance will also have an interface in Cluster Control network, because all Amazon RDS operations happen over the cluster control network.
 - The Application Network must be connected to a DHCP enabled interface. This interface must provide a default gateway for the VMs that will connect to this network.
 - DHCP broadcast must not cross over an up-link.
 - The distributed port group must be accessible from all ESXi hosts underlying the Amazon RDS on VMware cluster.
 - The distributed port group must use the elastic "port allocation" flag.
- d. Meet the requirements for the Management Network:
- It must include the existing ESXi management network that exists on standard vSphere installations.
 - All ESXi hosts that are part of the vSphere Cluster must be on the same Management Network.

Note

DHCP services are not required on the Management Network.

- e. Meet the requirements for the vCenter server credentials.

Amazon RDS on VMware requires a set of vCenter server credentials (a single sign-on user name and password) to use during the onboarding process. This user creates four new SSO users scoped to the cluster. The user also creates the resources to be used by the Amazon RDS on VMware management virtual machines and DB instances. We recommend creating a new user with admin privileges to use during onboarding and removing the user after onboarding is complete. Use a local single sign-on (SSO) domain. Active Directory domains aren't currently supported.

Add the new user to the following groups:

- ADMINISTRATORS
- CAADMINS
- SYSTEMCONFIGURATION.ADMINISTRATORS

- LICENSESERVICE.ADMINISTRATORS
 - COMPONENTMANAGER.ADMINISTRATORS
 - SYSTEMCONFIGURATION.BASHSHELLADMINISTRATORS
8. To use a proxy server for external traffic, complete the following prerequisites. RDS on VMware connects with AWS services, such as Amazon CloudWatch and Amazon S3, over HTTPS.
- a. Make sure that the proxy server is authenticated with transparent or password-based methods.
 - b. Ensure that the proxy server maintains a trust store.

The proxy server is a client that initiates Transport Layer Security (TLS) connections with AWS services, such as Amazon CloudWatch and Amazon S3. The proxy server must store CA certificates for these AWS services. For more information, see [Step 3: Install a TLS certificate on on-premises servers and VMs](#) in the *AWS Systems Manager User Guide*.

- c. Ensure that your proxy server is reachable via the Internet Network.
9. Validate the vSphere environment configuration.

Complete the following steps to validate that the vSphere environment is properly prepared for onboarding Amazon RDS on VMware.

- a. Validate the vCenter version and access requirements:
 - 1. Log in to the vSphere Web Client using the user that you plan to provide during onboarding.
 - 2. Choose **Home**.
 - 3. Choose **Hosts and Clusters**.
 - 4. Expand the target data center.
 - 5. Expand the cluster.
 - 6. Choose the ESXi host.
 - 7. Choose the **Summary** tab.
 - 8. Under **Configuration**, note the version in the **ESXi version** field.

For more information, see [Determining the build number of VMware ESX/ESXi and VMware vCenter Server](#) in the VMware documentation.

- b. Validate that the vSphere environment requirements are met:
 - Verify that the user created for onboarding is present in the **Administrator** group.
 - Ensure that a resource pool is present. If one isn't, create one.
 - All of the ESXi hosts must have the Cluster Control Network, Application Network, Internet Network, and Management Network linked to them.
 - Determine whether OVF deployment timeout is applicable. For more information, see [Cannot deploy an OVF in vCenter 6.5.0b \(build 5178943\) and later \(2150693\)](#) in the VMware documentation.
- c. Validate that the networking and access requirements are met:
 - Ensure that the Internet Network is running a DHCP server and that you can ping 8 . 8 . 8 . 8.

To do this, you can put a small Linux VM or a Microsoft Windows VM on the Internet Network. You can then test if the network interface gets the IP address and if you can ping 8 . 8 . 8 . 8.

- Ensure that the Application Network is running a DHCP server.

To do this, you can put a small Linux VM or a Windows VM on the Internet Network. You can then test if the network interface gets the IP address.

- Ensure that the free IP on the Management Network is not attached to any network interface on any other appliance.

Log in to the ESXi host or the vCenter and try to ping the free IP. You *should not* be able to ping it.

- d. Validate that the storage requirements are met:

- Storage must be in Network File System (NFS), VMware Virtual Machine File System (VMFS), or vSAN format.

10. Configure your local DNS server.

You configure your applications to access Amazon RDS on VMware DB instances by DNS name, rather than by the IP address. You do this because dynamically assigned IP addresses can change.

To make sure that DNS resolution can occur for Amazon RDS on VMware DB instance endpoints, configure your local DNS server or servers. You configure these to forward requests for `*.rdsonvmware.rds.amazonaws.com` to one of the IP addresses on the RDS Edge Router VM. Use the IP address of either the Management Network or the internet-facing interface, whichever is better for your network environment. You can find your DB instance endpoints using the AWS Management Console, AWS CLI, or RDS API.

The following is an example of how this might look. In this example, you use BIND (that is, you are modifying `named.conf`) and the RDS Edge Router IP where requests are forwarded is 10.1.2.3.

```
...  
zone rdsonvmware.rds.amazonaws.com {  
    type forward;  
    forward only;  
    forwarders { 10.1.2.3; }  
};  
...
```

11. Authorize a user to onboard Amazon RDS on VMware.

A user must be authorized to onboard Amazon RDS on VMware. To do this, you add a predefined AWS Identity and Access Management (IAM) policy to the user, the `AmazonRDSDataFullAccess` policy.

You can also create an IAM policy that grants the required permissions to onboard Amazon RDS on VMware. After you create the policy, add it to the user who you plan to onboard Amazon RDS on VMware.

The following policy provides the minimum required permissions for a user to onboard Amazon RDS on VMware.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "RDSonVMware",  
      "Effect": "Allow",
```

```
{
  "Action": [
    "rds:DescribeCustomAvailabilityZones",
    "rds:RegisterCustomAvailabilityZone"
  ],
  "Resource": "*"
}
```

For information about creating an IAM policy, see [Creating IAM policies](#) in the *AWS Identity and Access Management User Guide*.

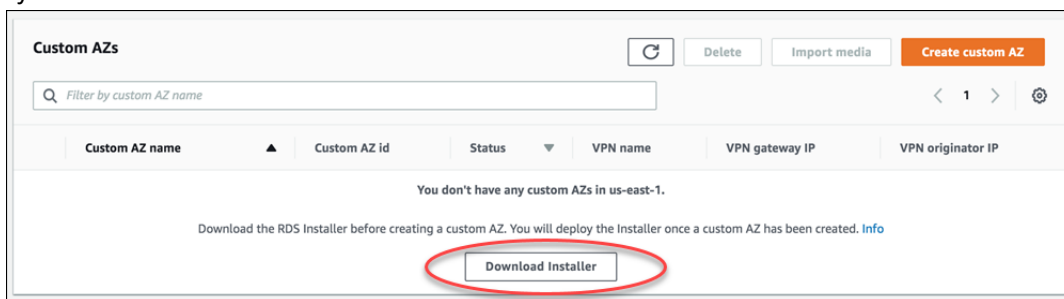
For information about adding an IAM policy to a user, see [Adding and removing IAM identity permissions](#) in the *AWS Identity and Access Management User Guide*.

Onboard your vSphere cluster

After you complete the steps in [Complete the prerequisites \(p. 14\)](#), you can onboard your vSphere cluster. To do this, create a new custom Availability Zone (AZ) and install Amazon RDS on VMware.

To onboard your vSphere cluster

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the upper-right corner of the console, choose the US East (N. Virginia) AWS Region.
3. In the navigation pane, choose **Custom AZs**.
4. Download the Amazon RDS on VMware Installer (Installer) on your vSphere cluster.
 - a. Choose **Download Installer**, accept the terms of the agreement, and save the file on your file system.




- b. Unzip the archive.
5. In the Amazon RDS console, create a custom AZ:
 - a. In the upper-right corner of the console, choose the AWS Region from which you downloaded the Installer.
 - b. In the navigation pane, choose **Custom AZs**.
 - c. Choose **Create custom AZ**.

The **Create custom AZ** page appears.

RDS > Custom AZs > Create custom AZ


Create custom AZ

 **Your currently selected Region is us-east-1**
For the best performance, select the AWS Region closest to your on-premises VMware vSphere cluster.

Custom AZ details

Custom AZ name

Custom AZ name must be unique. Constraints: 3 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

 **VPN no longer required for custom AZs**
VPN details are no longer required to create a custom AZ. This change simplifies the creation of a custom AZ while ensuring a secure connection between your vSphere cluster and the AWS region. Starting on March 30, 2021, we will remove VPN details from all custom AZs. [Learn more](#)

- d. In **Custom AZ name**, enter a name for the custom AZ.
- e. Choose **Create custom AZ**.

Amazon RDS on VMware begins the custom AZ creation process.

You can repeat this step to create additional custom AZs in the same AWS Region.

6. In your VMware environment, deploy the Installer OVA to start an Installer virtual machine (VM).

As part of the installation, you choose the networks for Cluster Control Network, Internet Network, Application Network, and Management Network. The Internet Network and Application Network must have DHCP enabled.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Select storage
- 7 Select networks**
- 8 Ready to complete

Select networks
Select a destination network for each source network.

Source Network	Destination Network
Cluster Control Network	Internet
Internet Network	Internet
Application Network	Application
Management Network	VM Network

4 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL **BACK** **NEXT**

7. Power on the installer VM. The installer VM gets two IP addresses dynamically assigned on both the Internet Network and Application Network. You must be able to reach at least one of these IP addresses to continue with the installation. Note the IP address that you can reach as `installer-ip`.
8. Launch the Installer by opening a browser and connecting to the following URL.

```
https://installer-ip/ui
```

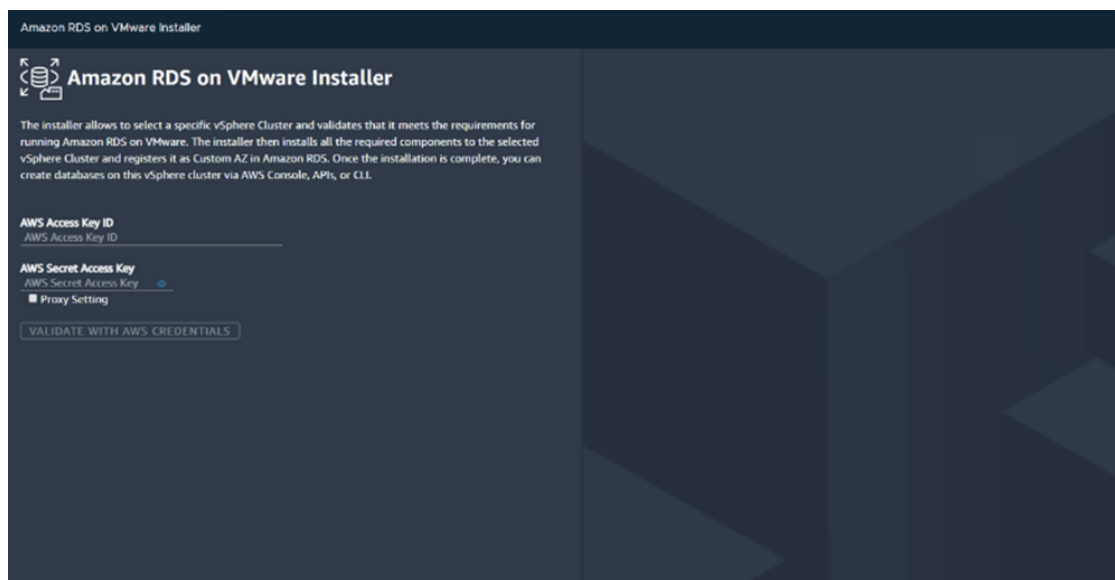
Replace `installer-ip` with the IP address of the Installer VM you noted earlier.

You launch the Installer by connecting to the Installer VM over HTTPS. When you connect to the Installer, the Installer presents a self-signed certificate that may not be trusted by your browser.

If the certificate is not trusted by your browser, you can choose to add an exception because you're connecting to the Installer VM that you just deployed in your VMware data center.

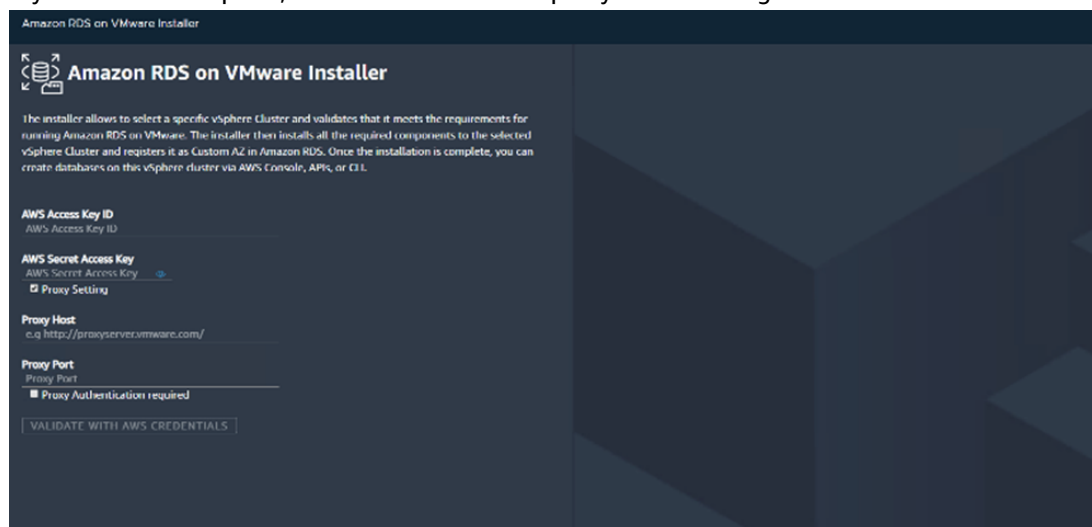
Or you can follow the steps in [Import the Installer VM certificate \(p. 31\)](#) to add the certificate to your browser before launching the installer.

The opening page of the Installer appears.



9. On the opening page, enter the following information:
- **AWS Access Key ID** – The access key for your AWS Identity and Access Management (IAM) user.
 - **AWS Secret Access Key** – The secret key for your IAM user.
 - **Proxy Setting** – Enable this option if you want all external HTTP and HTTPS traffic (for example, traffic to AWS services such as Amazon CloudWatch and Amazon S3) from RDS on VMware to use a proxy server.

If you enable this option, the Installer shows the proxy server settings.



Enter the following information:

- **Proxy Host** – The URL of the proxy host.
 - **Proxy Port** – The port used by the proxy host.
 - **Proxy Authentication required** – Enable this option if you aren't using a transparent proxy, and enter the proxy user, password, and public key in PEM format.
10. Choose **VALIDATE WITH AWS CREDENTIALS**.

If validation fails, create your **AWS Access Key ID** and **AWS Secret Access Key** by following the instructions in [Managing access keys for your AWS account](#) in the *AWS General Reference*.

11. Choose **AWS Configuration** and, for **Select Region**, choose the AWS Region that contains your custom AZ.

The screenshot shows the 'RDS on VMware Installer' window. On the left is a sidebar with a list of steps: 1 AWS Configuration, 2 Network Configuration, 3 vCenter Configuration, 4 Placement Details, 5 Validation Status, 6 Summary, and 7 Installation Status. Step 1 is highlighted. The main area is titled 'AWS Configuration' and contains a 'Select Region' dropdown menu with the text 'Select Region' and a downward arrow. At the bottom right of the window are two buttons: 'CANCEL' and 'NEXT'.

If you can't connect to the AWS Region, make sure that you completed all prerequisites described in [Complete the prerequisites \(p. 14\)](#).

12. On the **AWS Configuration** page, choose **RETRIEVE AZS** to populate the list of custom AZs in the selected AWS Region. Next, choose your custom AZ from **Select Custom AZs**.

RDS on VMware Installer

1 AWS Configuration

2 Network Configuration

3 vCenter Configuration

4 Placement Details

5 Validation Status

6 Summary

7 Installation Status

AWS Configuration

Select Region

us-east-2

RETREIVE AZS

✓ Connection to AWS site is successful.

Select Custom AZs

deployer-92

Select Custom AZs

Lab-172.24.24.120-05Oct2019

deployer-92

rackspace-4oct2019

test-deployer-213-5Oct

test-deployer-nimbus

CANCEL

NEXT

13. Choose **NEXT** to open the **Network Configurations** page.

The screenshot shows the 'RDS on VMware Installer' window with the 'Network Configuration' step selected in the left sidebar. The main area contains five configuration fields: 'ESXi Management Static IP Address' (0.0.0.0), 'DNS Server' (DNS), 'ESXi Management Netmask' (Netmask), 'ESXi Management Default Gateway' (Gateway), and 'NTP Server' (NTP Server). At the bottom right are 'CANCEL', 'BACK', and 'NEXT' buttons.

Field	Value
ESXi Management Static IP Address	0.0.0.0
DNS Server	DNS
ESXi Management Netmask	Netmask
ESXi Management Default Gateway	Gateway
NTP Server	NTP Server

Enter the following information:

- **ESXi Management Static IP Address** – The IP address of your ESXi Management Network
- **DNS Server** – The IP address of the DNS server for the vCenter Server that is authoritative for your vCenter Server's private DNS zone
- **ESXi Management Netmask** – The IP address of the subnet mask of the Management Network
- **ESXi Management Default Gateway** – The IP address of the gateway (router) for the Management Network
- **NTP Server** – The DNS name or IPv4 address of the Network Time Protocol (NTP) server to which your ESXi hosts sync

14. Choose **NEXT** to open the **vCenter Configuration** page.

The screenshot shows the 'vCenter Configuration' window of the 'RDS on VMware Installer'. On the left is a sidebar with a list of steps: 1 AWS Configuration, 2 Network Configuration, 3 vCenter Configuration (highlighted), 4 Placement Details, 5 Validation Status, 6 Summary, and 7 Installation Status. The main area contains three input fields: 'FQDN' with placeholder text 'FQDN', 'Administrator Username' with placeholder text 'Administrator Username', and 'Administrator Password' with placeholder text 'Administrator Password' and a toggle icon. Below these fields is a 'TEST CONNECTION' button. At the bottom right are three buttons: 'CANCEL', 'BACK', and 'NEXT'.

Enter the following information:

- **FQDN** – The vCenter fully qualified domain name
- **Administrator Username** – The administrative user name for the specified vCenter FQDN

Enter the username in the format `user@domain`, for example `admin@vsphere.local`.

- **Administrator Password** – The password for the specified administrative user

15. On the **vCenter Configuration** page, choose **TEST CONNECTION**.

If you can't connect, make sure that you completed all of the prerequisites described in [Complete the prerequisites \(p. 14\)](#). You can also choose **DOWNLOAD SUPPORT BUNDLE** to download log files that can help you diagnose connection problems.

16. Choose **NEXT** to open the **Placement** page.

RDS on VMware Installer

1 AWS Configuration

2 Network Configuration

3 vCenter Configuration

4 Placement Details

5 Validation Status

6 Summary

7 Installation Status

Placement Details

Select Datacenter
Select Datacenter

Select Cluster
Select Cluster

Select Datastore
Select Datastore

Select Resource Pool
Select Resource Pool

CANCEL BACK VALIDATE

Choose the following items:

- **Select Datacenter** – The virtual data center
- **Select Cluster** – The vSphere cluster
- **Select Datastore** – The datastore
- **Select Resource Pool** – The resource pool

17. Choose **VALIDATE** to open the **Validation Status** page, and check the status for each item.

If there is a problem with one or more items, correct the problem before proceeding. Choose **BACK**, and then choose **VALIDATE** again to check the validation status.

18. When all of the items are ready for installation, choose **NEXT** to open the **Summary** page.

RDS on VMware Installer

- 1 AWS Configuration
- 2 Network Configuration
- 3 vCenter Configuration
- 4 Placement Details
- 5 Validation Status
- 6 Summary**
- 7 Installation Status

Summary

AWS Configuration

Region	us-east-2
Custom AZ	

Network Configuration

ESXi Management Static IP Address	
DNS Server	
ESXi Management Netmask	
ESXi Management Default Gateway	
NTP Server	

vCenter Configuration

FQDN	
Host IP	
Administrator Username	

Placement Details

Datacenter	
Cluster	
Datastore	
Resource Pool	

CANCEL **BACK** **INSTALL**

Verify the onboarding information.

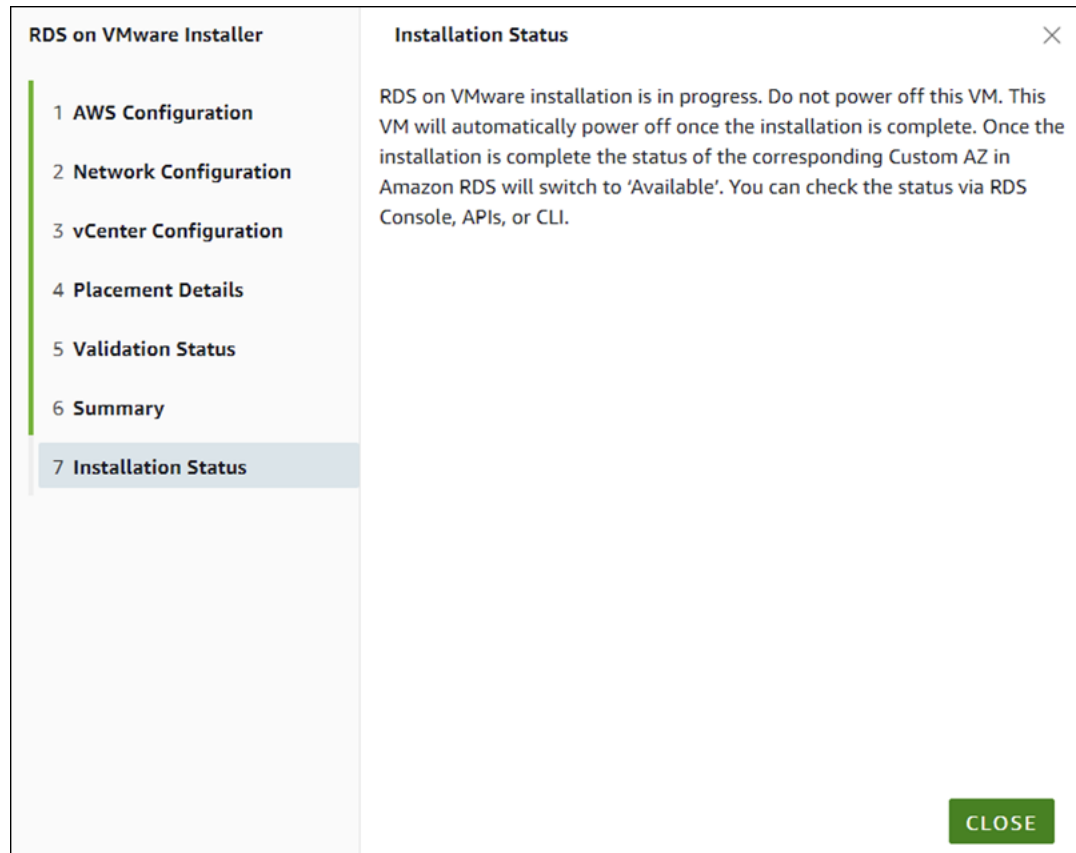
If an item isn't correct, go back to a previous page and correct it.

If the summary information is correct, choose **INSTALL** to complete the installation.

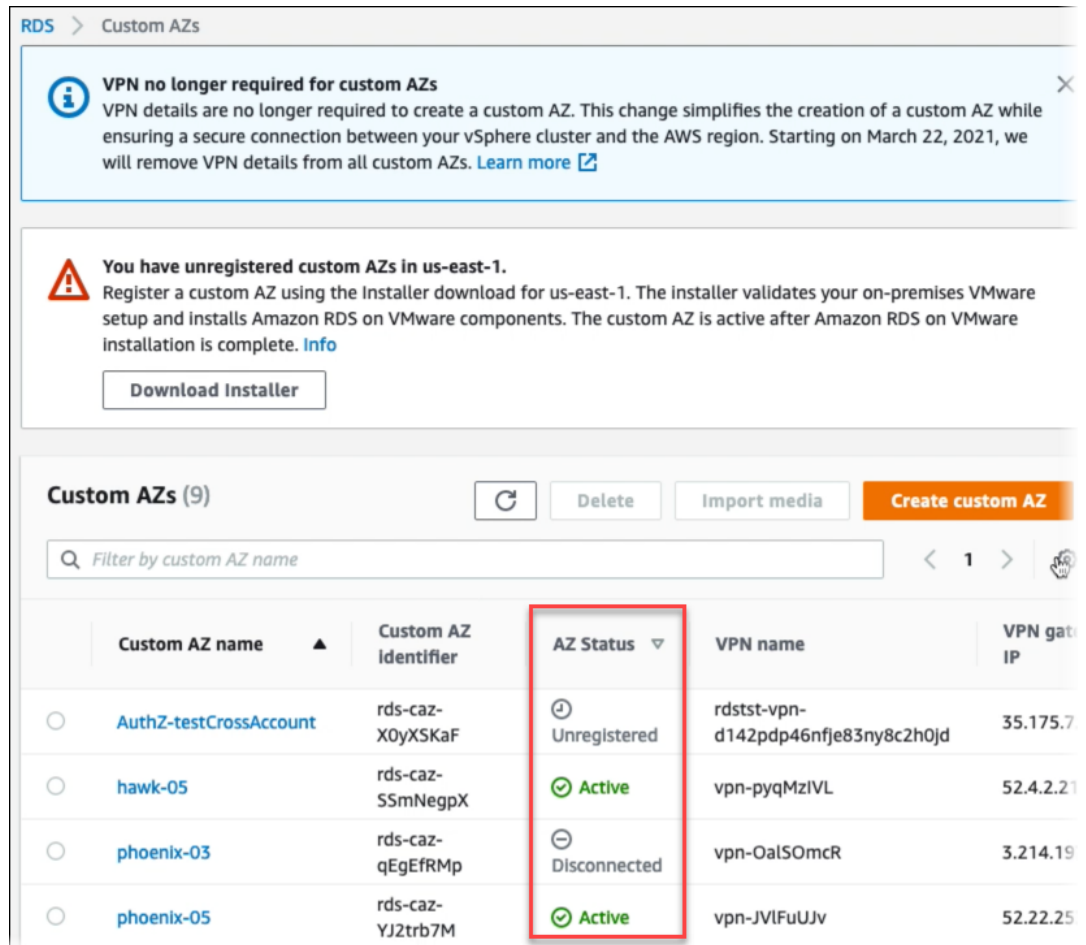
19. On the **Installation Status** page, read the message and choose **CLOSE**.

Important

The installation isn't complete until the status of the custom AZ is **Active**. Move on to the next steps to check the status of the custom AZ.



20. In the Amazon RDS console, check the status of your custom AZs.
- In the upper-right corner of the console, choose the AWS Region that contains your custom AZs.
 - In the navigation pane, choose **Custom AZs**.
 - View the **Status** column.



The screenshot shows the Amazon RDS Custom AZs console. At the top, there's a notification about VPN no longer being required for custom AZs. Below that, a warning states that there are unregistered custom AZs in us-east-1 and provides a 'Download Installer' button. The main section, 'Custom AZs (9)', contains a table with columns: Custom AZ name, Custom AZ identifier, AZ Status, VPN name, and VPN gateway IP. The table lists four custom AZs: 'AuthZ-testCrossAccount' (Unregistered), 'hawk-05' (Active), 'phoenix-03' (Disconnected), and 'phoenix-05' (Active). The 'AZ Status' column is highlighted with a red box.

Custom AZ name	Custom AZ identifier	AZ Status	VPN name	VPN gateway IP
AuthZ-testCrossAccount	rds-caz-X0yXSKaF	Unregistered	rdstst-vpn-d142pdp46nfje83ny8c2h0jd	35.175.7
hawk-05	rds-caz-SSmNegpX	Active	vpn-pyqMziVL	52.4.2.21
phoenix-03	rds-caz-qEgEfRMp	Disconnected	vpn-OalSOmcR	3.214.19
phoenix-05	rds-caz-YJ2trb7M	Active	vpn-JVIFuUJv	52.22.25

If a custom AZ isn't registered yet with your vSphere cluster, the status is **Unregistered**. Register these custom AZs.

If a custom AZ is registered with your vSphere cluster, the status is **Active**.

If a custom AZ is disconnected from Amazon RDS, the status is **Disconnected**. For more information about restoring connectivity with such a custom AZ, see [Custom AZ is disconnected \(p. 55\)](#).

21. After a custom AZ is registered, you can create one or more DB instances in the custom AZ.

For more information, see [Creating an on-premises DB instance \(p. 43\)](#).

Import the Installer VM certificate

You can extract the self-signed certificate generated at bootstrap time on the installer VM from vCenter. You then convert the certificate to binary format that you can import as a Trusted CA on the browser. Doing so makes the connection in between the browser and the RDS Installer secure.

Note

The process described in this section should work for most operating systems and browsers. However, each operating system and browser has its own way of storing and managing certificates. We described the sequence of steps for Windows 10, Chrome Version 77.0.3865.90, and Microsoft Edge 44.18362.387.0. We also tested this process for Mac OS and Chrome.

Performing this process avoids the **Connection Not Secure** alert in the browser when accessing the Installer because the application uses self-signed certificates.

The process requires the Managed Object Browser (MOB) to find the certificate of the Installer. Make sure that you have the MOB accessible. The MOB provides a way to explore the vSphere object model. However, it's not enabled in production systems on vSphere 6.5 and higher. To enable it, see the [VMware documentation](#).

To import the Installer VM certificate

1. Power on the Installer VM for Amazon RDS on VMware.
2. Get the VM Object Reference certificate by navigating the MOB.
 - a. Go to `https://vCenter FQDN/mob`.
 - b. Choose **Content**.
 - c. Choose **SearchIndex**.
 - d. Choose **FindAllByIp**.

The **Method Invocation Result** page looks similar to the following.

Method Invocation Result: ManagedObjectReference[]		
NAME	TYPE	VALUE
name	string	"Return value"
val	ManagedObjectReference[]	vm-41 (vdme-deployer-1.0.0.33091-14836180_OVF10)

Note the return value, which is the VM object reference. On the preceding page, the VM Object reference value is `vm-41`.

3. Get the VM Installer certificate using the VM object reference.
 - a. Go to this location: `http://vCenter-FQDN/mob/?moid=VM_object_reference&doPath=config.extraConfig["guestinfo.RDSInstaller.certific`


Replace `VM_object_reference` with the value that you retrieved in the previous step. In the sample page, it was `vm-41`.

A page similar to the following opens.

[Home](#)

Data Object Type: OptionValue
Parent Managed Object ID: **vm-41**
Property Path: **config.extraConfig["guestinfo.RDSInstaller.certificate"]**

Properties

NAME	TYPE	VALUE
key	string	"guestinfo.RDSInstaller.certificate"
value	string	"-----BEGIN CERTIFICATE-----  -----END CERTIFICATE-----"

- b. Copy and paste this certificate to create a text file called `RDSinstCert.cer`.
4. Use a tool to convert the captured certificate to the CRT binary format. For example, you can use `openssl`, which is available on Windows, Mac, and Linux.

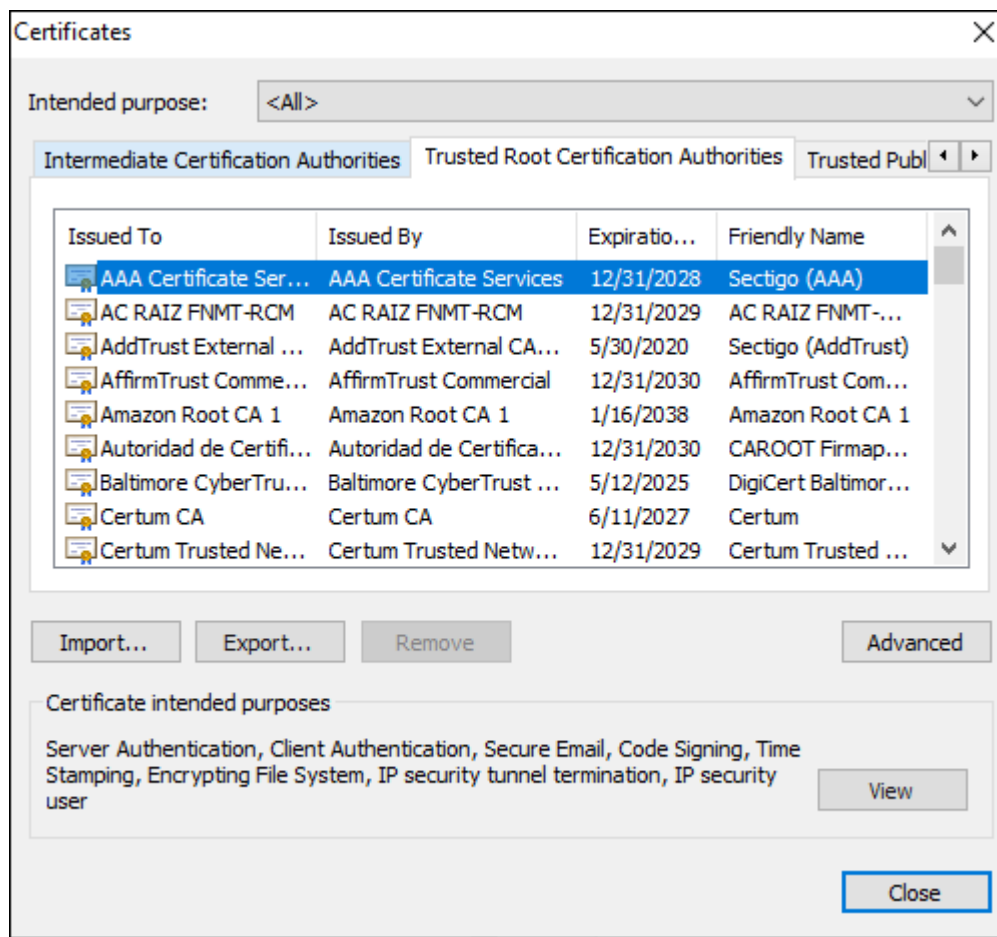
The following example shows the conversion with `openssl`.

```
openssl x509 -outform der -in RDSinstCert.cer -out RDSinstCert.crt
```

5. Import the certificate with your browser.

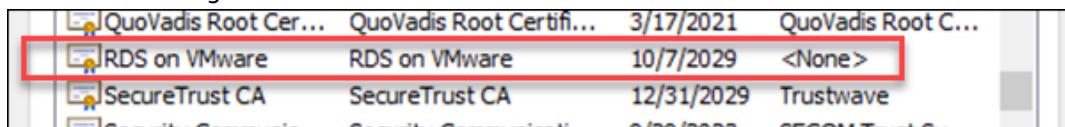
The following steps import the certificate with Chrome on Windows. On Windows, this method also works with Edge and Firefox, but Firefox must be configured to use the Windows certificate store instead of the Mozilla store. On Mac, you must use the Mac system keychain.

- a. Go to **Manage Certificates** Chrome settings, and import the certificate on the **Trusted Root Certification Authorities** folder, as shown following.



- b. On the **Security Warning** page, accept the installation of the certificate.

After the certificate is installed, it is listed in the **Trusted Root Certification Authorities** folder, as shown following.



6. Restart the browser and launch the Installer by following the instructions in step 8 in [Onboard your vSphere cluster](#) (p. 20).

The security alert shouldn't appear.

Working with Amazon RDS on VMware

Working with an Amazon RDS on VMware DB instance is similar to working with any Amazon RDS DB instance. To run your DB instances, you can provision on-premises DB instance classes for Amazon RDS on VMware that work in your vSphere cluster.

Topics

- [Installing the media for Microsoft SQL Server \(p. 35\)](#)
- [Choosing the on-premises DB instance class \(p. 42\)](#)
- [Creating an on-premises DB instance \(p. 43\)](#)
- [Creating additional custom AZs in an AWS Region \(p. 49\)](#)
- [Creating read replicas \(p. 50\)](#)
- [Managing your on-premises DB instances \(p. 53\)](#)

Installing the media for Microsoft SQL Server

If you are using Microsoft SQL Server, an on-premises customer provided license is required. In this case, make sure that you install your operating system media and database media before you create Amazon RDS DB instances.

Important

MySQL and PostgreSQL don't require you to install media. If you plan to use one of these DB engines, you can move on to [Choosing the on-premises DB instance class \(p. 42\)](#).

Supported media

Currently, the following media are supported:

• OS Installation Media

- Windows Server 2016 (x64) - DVD (English)

Released: 10/12/2016

File name: en_windows_server_2016_x64_dvd_9327751.iso

- Windows Server 2016 (Updated January 2017) (x64) - DVD (English)

Released: 1/12/2017

File name: en_windows_server_2016_x64_dvd_9718492.iso

- Windows Server 2016 (Updated February 2018) (x64) - DVD (English)

Released: 2/15/2018

File name: en_windows_server_2016_updated_feb_2018_x64_dvd_11636692.iso

- **Engine Installation Media**

- SQL Server 2016 Enterprise (x64) - DVD (English)

Released: 6/1/2016

File name: en_sql_server_2016_enterprise_x64_dvd_8701793.iso

- SQL Server 2016 Enterprise with Service Pack 1 (x64) - DVD (English)

Released: 11/16/2016

File name: en_sql_server_2016_enterprise_with_service_pack_1_x64_dvd_9542382.iso

- SQL Server 2016 Enterprise with Service Pack 2 (x64) - DVD (English)

Released: 5/22/2018

File name: en_sql_server_2016_enterprise_with_service_pack_2_x64_dvd_12124051.iso

Install the media

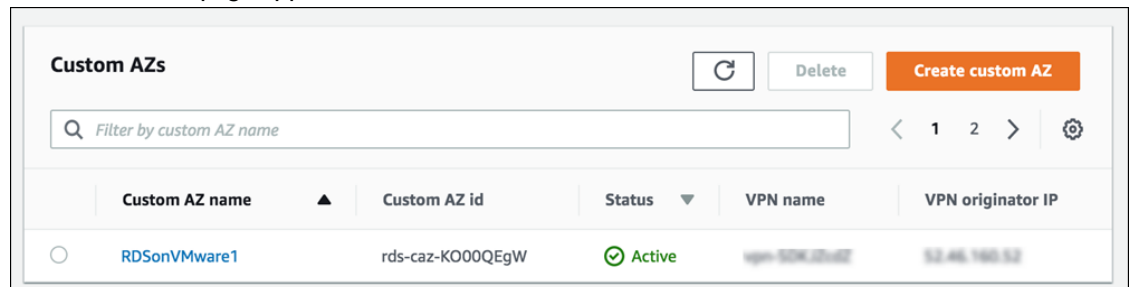
You can install the media using the AWS Management Console, the AWS CLI, or the RDS API.

Console

To install media in a custom AZ

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the top-right corner of the console, choose the AWS Region that contains the custom AZ in which you want to create the DB instance.
3. In the navigation pane, choose **Custom AZs**.

The **Custom AZs** page appears.



4. Choose the name of the custom AZ on which you want to install media to show the custom AZ details.

The details page for the custom AZ appears.

[RDS](#) > [Custom AZs](#) > RDSonVMware1

RDSonVMware1

Delete

Summary

Custom AZ name	Custom AZ identifier	Custom AZ status
RDSonVMware1	rds-caz-MNaQXHre	✓ Active
VPN name	VPN id	VPN originator IP
XXXXXXXXXX	XXXXXXXXXX-XXXX-XXXX	10.0.0.100

Install media

Remove

Import

↺

< 1 > ⚙

Media id	Status	Engine	Engine version
You do not have any imported media.			

5. In the **Install media** section, choose **Import**.

The **Import media** page appears.


Import media

Engine options

Choose the DB engine, edition, and version that corresponds to your on-premises media.

Engine type

☒ Microsoft SQL Server



Microsoft SQL Server

Edition

☒ SQL Server Enterprise Edition

Comprehensive high-end capabilities for mission-critical applications with demanding database workloads and business intelligence requirements.

Version

SQL Server 2016 13.00.5337.0.v1

Importation settings

Input the paths to your OS and installation media from your on-premises datastore. If no media exists, upload the media to a directory in your datastore before proceeding.

OS installation path [Info](#)

ex. WindowsISO/en_windows_server_2016_x64_dvd_9327751.iso

The absolute path of the OS media uploaded to your on-premises datastore.

Engine installation path [Info](#)

ex. SQLServerISO/en_sql_server_2016_enterprise_x64_dvd_8701793.iso

The absolute path of the DB engine media uploaded to your on-premises datastore. The version of the engine media must match the engine version you selected above.

[Cancel](#) [Import media](#)

6. In the **Engine options** section, choose the DB engine, the edition, and the version.
7. In the **Importation settings** section, complete the settings:
 - **OS installation path** – The absolute path to the operating system media on your VMware cluster datastore

- **Engine installation path** – The absolute path to the DB engine media on your VMware cluster datastore

Important

The edition and version of the media referenced in the **Engine installation path** must match the DB engine edition and version that you chose in the previous step. For information about supported media, see [Supported media \(p. 35\)](#).

Both paths must be present on the same datastore that was specified in the Installer during onboarding. Don't include the datastore name in the path. The following are examples of valid paths:

- **OS installation path** – WindowsISO/en_windows_server_2016_x64_dvd_9327751.iso
- **Engine installation path** – SQLServerISO/en_sql_server_2016_enterprise_x64_dvd_8701793.iso

8. Choose **Import media**.

You can monitor the status of the import on the details page for the custom AZ.

The screenshot shows the AWS Management Console interface for a custom Availability Zone named 'RDSONVMware1'. The 'Summary' section displays the custom AZ name, identifier, and status (Active). The 'Install media' section shows a table of installed media. The 'Status' column is highlighted with a red box, showing two entries: 'Available' (with a green checkmark) and 'Importing' (with a clock icon).

Media id	Status	Engine	Engine version
ZYFNGGLZvrNBPaky	Available	sqlserver-ee	13.00.5337.0.v1
kPWOn34GMhaKgmX0	Importing	sqlserver-ee	13.00.5337.0.v1

AWS CLI

To install media by using the AWS CLI, call the [import-installation-media](#) command with the options following. All of the options are required.

- **--custom-availability-zone-id** – The identifier of the custom Availability Zone (AZ) to import the installation media to
- **--engine** – The name of the database engine to be used for this instance
- **--engine-installation-media-path** – The absolute path to the DB engine media on your VMware cluster datastore

Important

The edition and version of the media specified in the **--engine-installation-media-path** must match the DB engine edition and version specified in the **--engine** option. The path must be present on the same datastore that was specified in the installer during onboarding. Don't include the datastore name in the path.

- **--engine-version** – The version number of the database engine to use

- `--os-installation-media-path` – The absolute path to the operating system media on your VMware cluster datastore

Important

The path must be present on the same datastore that was specified in the installer during onboarding. Do not include the datastore name in the path.

For information about supported media, see [Supported media \(p. 35\)](#).

Example

The following example imports the installation media for a `sqlserver-ee` engine.

For Linux, OS X, or Unix:

```
aws rds import-installation-media \
  --custom-availability-zone-id mycustomaz_identifier \
  --engine sqlserver-ee \
  --engine-version 13.00.5292.0.v1 \
  --engine-installation-media-path SQLServerISO/
en_sql_server_2016_enterprise_x64_dvd_8701793.iso \
  --os-installation-media-path WindowsISO/en_windows_server_2016_x64_dvd_9327751.iso
```

For Windows:

```
aws rds import-installation-media ^
  --custom-availability-zone-id mycustomaz_identifier ^
  --engine sqlserver-ee ^
  --engine-version 13.00.5292.0.v1 ^
  --engine-installation-media-path SQLServerISO/
en_sql_server_2016_enterprise_x64_dvd_8701793.iso ^
  --os-installation-media-path WindowsISO/en_windows_server_2016_x64_dvd_9327751.iso
```

Replace the placeholders with appropriate values.

RDS API

To install media by using the Amazon RDS API, call the [ImportInstallationMedia](#) operation with the parameters following. All of the parameters are required.

- `CustomAvailabilityZoneId` – The identifier of the custom Availability Zone (AZ) to import the installation media to
- `Engine` – The name of the database engine to be used for this instance
- `EngineInstallationMediaPath` – The path to the installation media for the specified DB engine
- `EngineVersion` – The version number of the database engine to use
- `OSInstallationMediaPath` – The path to the installation media for the operating system associated with the specified DB engine

Troubleshooting media installation issues for Microsoft SQL Server

Use the following sections to troubleshoot problems that you have with installing the media for Microsoft SQL Server.

Topics

- [Media not found \(p. 41\)](#)
- [Media not supported \(p. 41\)](#)
- [Custom AZ disconnected \(p. 41\)](#)

Media not found

In this case, the media wasn't found in the specified location, and the following errors can be returned.

```
OS media not found at provided location
Engine media not found at provided location
```

The cause for this issue is almost always one of the following:

- The specified path for the media is incorrect.
- The datastore is included in the path.
- The media path isn't in the datastore that was specified during onboarding.

To solve the issue, make sure that the path is correct and that the datastore isn't included in the path. Also, make sure that the media is in the datastore that was specified in the installer during onboarding.

For information about onboarding, see [Getting started with Amazon RDS on VMware \(p. 13\)](#).

Media not supported

In this case, the specified media isn't supported by Amazon RDS on VMware, and the following errors can be returned:

```
OS media validation failed
Engine media validation failed
```

To solve the issue, specify supported installation media. For information about supported media, see [Supported media \(p. 35\)](#).

Custom AZ disconnected

In this case, the custom AZ that you attempted to attach installation media to can't currently be reached.

To solve the issue, see [Custom AZ is disconnected \(p. 55\)](#).

Choosing the on-premises DB instance class

The DB instance class determines the computation and memory capacity of an Amazon RDS DB instance. Determine which DB instance class most closely matches your VMware cluster. You specify the DB instance class when you create your on-premises DB instance.

On-premises DB instance class types

Amazon RDS on VMware supports three types of on-premises DB instance classes: General, Compute Optimized, and Memory Optimized.

The following are the on-premises DB instance classes available:

- **db.mv11** – Current-generation general DB instance classes that provide a balance of compute and memory resources for a variety of workloads.
- **db.cv11** – Current-generation DB instance classes optimized for compute-intensive workloads.
- **db.rv11** – Current-generation DB instance classes optimized for memory-intensive applications.

Terminology for DB instance class hardware specifications

The following terminology is used to describe hardware specifications for DB instance classes:

- **vCPU** – The number of virtual central processing units (CPUs)
- **Memory (GiB)** – The RAM memory, in gibibytes, allocated to the DB instance

Specifications for all available on-premises DB instance classes

The following table provides details of the on-premises Amazon RDS DB instance classes.

Instance Class	vCPU	Memory (GiB)
db.mv11 – Current Generation General		
db.mv11.medium	1	4
db.mv11.large	2	8
db.mv11.xlarge	4	16
db.mv11.2xlarge	8	32
db.mv11.4xlarge	16	64
db.mv11.12xlarge	48	192
db.mv11.24xlarge	96	384
db.cv11 – Current Generation Compute Optimized		
db.cv11.small	1	1

Instance Class	vCPU	Memory (GiB)
db.cv11.medium	1	2
db.cv11.large	2	4
db.cv11.xlarge	4	8
db.cv11.2xlarge	8	16
db.cv11.4xlarge	16	32
db.cv11.9xlarge	36	72
db.cv11.18xlarge	72	144
db.rv11 – Current Generation Memory Optimized		
db.rv11.large	2	16
db.rv11.xlarge	4	32
db.rv11.2xlarge	8	64
db.rv11.4xlarge	16	128
db.rv11.12xlarge	48	384
db.rv11.24xlarge	96	768

Creating an on-premises DB instance

The basic building block of Amazon RDS is the DB instance. The DB instance is where you create your on-premises databases.

Before you can create on-premises DB instances, you must complete the following prerequisites:

- Set up your AWS account. For instructions, see [Setting up Amazon RDS on VMware \(p. 10\)](#).
- Create at least one custom Availability Zone (custom AZ), and register the custom AZ with the vSphere cluster. For instructions, see [Getting started with Amazon RDS on VMware \(p. 13\)](#).

If the status of the custom AZ in which you want to create a DB instance is **Disconnected**, see [Custom AZ is disconnected \(p. 55\)](#).

- If you are working with a DB engine that requires an on-premises customer provided license (such as Microsoft SQL Server), install your operating system and database media. For SQL Server, you must do this before you can create Amazon RDS DB instances. For instructions, see [Installing the media for Microsoft SQL Server \(p. 35\)](#). Installing media is not required for MySQL or PostgreSQL.
- Determine which DB instance class most closely matches your VMware cluster. For instructions, see [Choosing the on-premises DB instance class \(p. 42\)](#).

Amazon RDS on VMware supports the following DB engines and versions:

- Amazon RDS for Microsoft SQL Server 2016 SP2 Enterprise Edition
- Amazon RDS for MySQL version 5.7
- Amazon RDS for PostgreSQL version 10.9-R1 and 10.10-R1

You can create an on-premises DB instance using the AWS Management Console, the AWS CLI, or the RDS API.

Console

To create an on-premises DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the top-right corner of the console, choose the AWS Region that contains the custom AZ in which you want to create the DB instance.
3. In the navigation pane, choose **Databases**.
4. Choose **Create database**.

The **Create database** page opens.

Create database

Database location
Choose a location to meet your use case. [Info](#)

☐ **Amazon Cloud**
Use Amazon's cloud to store and provision a database instance with RDS.

☒ **On-premises**
Use a custom AZ to create a DB instance with an on-premises VMware cluster.

Availability Zone

Custom Availability Zone [Info](#)

caz-EVBOBGjc ▼

i After the DB instance is created, you can't change the availability zone selection.

5. In the **Database location** section, choose **On-premises**.
6. In the **Availability zone** section, choose **Custom Availability Zone**.
7. In the **Engine options** section, choose the type of DB engine in **Engine type**, and then, for some DB engines, choose the DB engine version in **Version**.

Engine options

Engine type

☒ MySQL



☐ PostgreSQL



☐ Microsoft SQL Server



MySQL

MySQL is the most popular open source database in the world. MySQL on RDS offers the rich features of the MySQL community edition with the flexibility to easily scale compute resources or storage capacity for your database.

- Supports database size up to 32 TiB.
- Supports General Purpose, Memory Optimized, and Burstable Performance instance classes.
- Supports automated backup and point-in-time recovery.
- Supports up to 5 Read Replicas per instance, within a single Region or cross-region.

Version [Info](#)

mysql 5.7.21




Known Issues/Limitations


Review the [Known Issues/Limitations](#) to learn about potential compatibility issues with specific database versions.


If you chose a DB engine that requires an on-premises customer provided license (such as Microsoft SQL Server), you might need to choose the DB engine edition for **Edition**.

Engine options

Engine type

☐ MySQL

☐ PostgreSQL

☒ Microsoft SQL Server

Microsoft SQL Server

Edition

☒ SQL Server Enterprise Edition
Comprehensive high-end capabilities for mission-critical applications with demanding database workloads and business intelligence requirements.

Version [Info](#)

SQL Server 2016 14.00.1000.169.v1

License

bring-your-own-license

Important

For DB engines that require an on-premises customer-provided license, operating system and database media must be installed in the custom AZ. Also, the edition and version of the media must match your selections. If the media is not installed, a warning message appears. For information about installing media, see [Installing the media for Microsoft SQL Server](#) (p. 35).

8. In the **Settings** section, complete the **DB instance identifier**, **Master username**, and **Master password** settings.

For more information about settings, see [Available settings](#) (p. 48).

9. In the **DB instance size** section, choose the **DB instance class**.
10. In the **Connectivity** section, enter the number for the **Database port**.
11. In the **Additional configuration** section, complete the remaining settings.
12. Choose **Create database**.

AWS CLI

To create an on-premises DB instance by using the AWS CLI, call the [create-db-instance](#) command with the options following.

- `--availability-zone` (Required)
- `--db-instance-class` (Required)
- `--db-instance-identifier` (Required)
- `--engine` (Required)
- `--backup-retention-period`
- `--db-name`
- `--engine-version`

- `--master-username`
- `--master-user-password`
- `--port`
- `--preferred-backup-window`

For more information about these options, see [Available settings \(p. 48\)](#).

Example

The following example creates an on-premises PostgreSQL DB instance named `mydbinstance`.

For Linux, OS X, or Unix:

```
aws rds create-db-instance \  
  --db-instance-identifier mydbinstance \  
  --db-instance-class db.mv11.medium \  
  --engine postgres \  
  --availability-zone mycustomaz_identifier \  
  --master-username masterawsuser \  
  --master-user-password masteruserpassword
```

For Windows:

```
aws rds create-db-instance ^  
  --db-instance-identifier mydbinstance ^  
  --db-instance-class db.mv11.medium ^  
  --engine postgres ^  
  --availability-zone mycustomaz_identifier ^  
  --master-username masterawsuser ^  
  --master-user-password masteruserpassword
```

Replace the placeholders with appropriate values. For *mycustomaz_identifier*, specify the unique identifier for the custom AZ that you want to create the DB instance in.

RDS API

To create an on-premises DB instance by using the Amazon RDS API, call the [CreateDBInstance](#) operation with the parameters following.

For `AvailabilityZone`, specify the unique identifier for the custom AZ that you want to create the DB instance in.

- `AvailabilityZone` (Required)
- `DBInstanceClass` (Required)
- `DBInstanceIdentifier` (Required)
- `Engine` (Required)
- `BackupRetentionPeriod`
- `DBName`
- `EngineVersion`
- `MasterUsername`
- `MasterUserPassword`
- `Port`
- `PreferredBackupWindow`

For more information about these parameters, see [Available settings \(p. 48\)](#).

Available settings

For details about the available settings that you can modify during DB instance creation, see the table following.

Console Setting	CLI Option	RDS API Parameter	Description
Backup retention period	--backup-retention-period	BackupRetentionPeriod	The number of days that you want automatic backups of your DB instance to be retained. For any nontrivial DB instance, set this value to 1 or greater. Enable the Enable automatic backups option to set this value.
Backup window	--preferred-backup-window	PreferredBackupWindow	The time period during which Amazon RDS automatically takes a backup of your DB instance. Unless you have a specific time that you want to have your database backup, use the default of No Preference .
Custom Availability Zone	--availability-zone	AvailabilityZone	The custom AZ for your DB instance. For more information, see Custom Availability Zones (p. 6) .
Database name	--db-name	DBName	The name for the database on your DB instance. The requirements for the name vary by DB engine. If you don't provide a name, Amazon RDS doesn't create a database on the DB instance you are creating. You can create additional databases after the DB instance is created.
Database port	--port	Port	The port that you want to use to access the DB instance.
DB instance class	--db-instance-class	DBInstanceClass	The DB instance class that you want to use. For more information, see Choosing the on-premises DB instance class (p. 42) .
DB instance identifier	--db-instance-identifier	DBInstanceIdentifier	The name for your DB instance. This value is stored as a lowercase string.
Engine	--engine	Engine	The name of the database engine to be used for this instance. Currently, the following engines are supported: <ul style="list-style-type: none"> mysql postgres

Console Setting	CLI Option	RDS API Parameter	Description
			• sqlserver-ee
Master password	--master-user-password	MasterUserPassword	The password for your master user.
Master username	--master-username	MasterUsername	The name that you use as the master user name to log on to your DB Instance. For more information, including a list of the default privileges for the master user, see Master user account privileges in the <i>Amazon RDS User Guide</i> .
Version	--engine-version	EngineVersion	The version of database engine that you want to use.

Creating additional custom AZs in an AWS Region

During the onboarding process described in [Getting started with Amazon RDS on VMware \(p. 13\)](#), you created a custom Availability Zone (custom AZ) in an AWS Region. You can create additional custom AZs in the same AWS Region.

To create a custom AZ

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the top-right corner of the AWS Management Console, choose the AWS Region that you want to create the custom AZ in.
3. In the navigation pane, choose **Custom AZs**.
4. Choose **Create custom AZ**.

The **Create custom AZ** page appears.

RDS > Custom AZs > Create custom AZ

Create custom AZ

Your currently selected Region is us-east-1
For the best performance, select the AWS Region closest to your on-premises VMware vSphere cluster.

Custom AZ details

Custom AZ name

Custom AZ name must be unique. Constraints: 3 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

VPN no longer required for custom AZs
VPN details are no longer required to create a custom AZ. This change simplifies the creation of a custom AZ while ensuring a secure connection between your vSphere cluster and the AWS region. Starting on March 30, 2021, we will remove VPN details from all custom AZs. [Learn more](#)

5. In **Custom AZ name**, enter a name for the custom AZ.
6. Choose **Create custom AZ**.

Amazon RDS on VMware begins the custom AZ creation process.

Creating read replicas

Amazon RDS on VMware uses the MySQL and PostgreSQL DB engines' built-in replication functionality to create a special type of DB instance called a read replica from a source DB instance. Updates made to the source DB instance are asynchronously copied to the read replica. You can reduce the load on your source DB instance by routing read queries from your applications to the read replica. Using read replicas, you can elastically scale out beyond the capacity constraints of a single DB instance for read-heavy database workloads.

When you create a read replica, you first specify an existing DB instance as the source. Then Amazon RDS takes a snapshot of the source instance and creates a read-only instance from the snapshot. RDS then uses the asynchronous replication method for the DB engine to update the read replica whenever there is a change to the source DB instance. The read replica operates as a DB instance that allows only read-only connections. Applications connect to a read replica the same way they do to any DB instance. RDS replicates all databases in the source DB instance.

For more information on Amazon RDS read replicas, see [Working with read replicas](#).

Limitations

Read replicas on Amazon RDS on VMware have the following limitations:

- Read replicas are supported only for MySQL and PostgreSQL DB instance types.
- RDS on VMware read replicas are supported on PostgreSQL versions 10.9 and 10.10, and MySQL version 5.7.
- You can't create a read replica in a different AWS Region from the primary DB instance.
- Only one read replica per DB instance is supported.
- The primary DB instance and the read replica both exist on-premises.
- The read replica has the same compute and storage requirements as the primary DB instance. Make sure that your installation has enough capacity for both the primary and the replica.
- The read replica isn't automatically promoted if the primary DB instance fails. You must manually promote the read replica.

Creating a read replica

You can create a read replica from an existing MySQL or PostgreSQL DB instance using the AWS Management Console or AWS CLI.

Console

To create a read replica from a source MySQL or PostgreSQL DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the navigation pane, choose **Databases**.
3. Choose the MySQL or PostgreSQL DB instance that you want to use as the source for a read replica.
4. For **Actions**, choose **Create read replica**.
5. Choose the instance specifications that you want to use. We recommend that you use the same DB instance class and storage type as the source DB instance for the read replica.
6. For **Destination Custom AZ**, choose the custom Availability Zone where you want to create the read replica. This can be the same CAZ as the primary DB instance (the default value), or a different CAZ.
7. For **DB instance identifier**, enter a name for the read replica.
8. Choose the other settings that you want to use.
9. Choose **Create read replica**.

AWS CLI

To create a read replica from a source MySQL or PostgreSQL DB instance, use the AWS CLI command [create-db-instance-read-replica](#).

Example

For Linux, OS X, or Unix:

```
aws rds create-db-instance-read-replica \  
  --db-instance-identifier myreadreplica \  
  --source-db-instance-identifier mydbinstance \  
  --availability-zone mycaz
```

For Windows:

```
aws rds create-db-instance-read-replica ^  
  --db-instance-identifier myreadreplica ^
```

```
--source-db-instance-identifier mydbinstance ^  
--availability-zone mycaz
```

Promoting a read replica to be a standalone DB instance

You can promote a MySQL or PostgreSQL read replica into a standalone DB instance. When you promote a read replica, the DB instance is rebooted before it becomes available.

When you promote a read replica, the new DB instance that is created retains the backup retention period and backup window of the former read replica source. The promotion process can take several minutes or longer to complete, depending on the size of the read replica. After you promote the read replica to a new DB instance, it's just like any other DB instance. For example, you can create read replicas from the new DB instance and perform point-in-time restore operations. Because the promoted DB instance is no longer a read replica, you can't use it as a replication target.

Backup duration is a function of the number of changes to the database since the previous backup. If you plan to promote a read replica to a standalone instance, we recommend that you enable backups and complete at least one backup prior to promotion. In addition, you can't promote a read replica to a standalone instance when it has the `backing-up` status. If you have enabled backups on your read replica, configure the automated backup window so that daily backups don't interfere with read replica promotion.

Console

To promote a read replica to a DB instance

1. Sign in to the AWS Management Console and open the Amazon RDS console at <https://console.aws.amazon.com/rds/>.
2. In the Amazon RDS console, choose **Databases**.

The **Databases** pane appears. Each read replica shows **Replica** in the **Role** column.

3. Choose the read replica that you want to promote.
4. For **Actions**, choose **Promote**.
5. On the **Promote Read Replica** page, enter the backup retention period and the backup window for the new promoted DB instance.
6. When the settings are as you want them, choose **Continue**.
7. On the acknowledgment page, choose **Promote Read Replica**.

AWS CLI

To promote a read replica to a DB instance, use the AWS CLI `promote-read-replica` command.

Example

For Linux, OS X, or Unix:

```
aws rds promote-read-replica \  
--db-instance-identifier myreadreplica
```

For Windows:

```
aws rds promote-read-replica ^
```

```
--db-instance-identifier myreadreplica
```

Managing your on-premises DB instances

In general, you manage on-premises DB instances for Amazon RDS on VMware in the same way that you manage Amazon RDS DB instances in a cloud environment. For information about managing DB instances, see the [Amazon RDS User Guide](#).

Note

Some management tasks that apply to Amazon RDS DB instances in a cloud environment don't apply to Amazon RDS on VMware DB instances. For example, with Amazon RDS on VMware, you manage storage locally on your vSphere cluster. Also, some restrictions apply to Amazon RDS on VMware DB instances. For information about the Amazon RDS features that are supported by Amazon RDS on VMware, see [Support for RDS features in Amazon RDS on VMware \(p. 6\)](#).

Because many RDS on VMware operations are dependent on a stable internet connection to AWS, some Amazon RDS operations are unavailable when the status of the custom AZ is **Disconnected**. For more information about restoring connectivity with a custom AZ, see [Custom AZ is disconnected \(p. 55\)](#).

Troubleshooting Amazon RDS on VMware

To help troubleshoot problems that you have with Amazon RDS on VMware, you can use the following sections.

Topics

- [Can't connect to the RDS connector \(p. 54\)](#)
- [Custom AZ is unregistered or creating \(p. 54\)](#)
- [Custom AZ is disconnected \(p. 55\)](#)
- [Can't create a new custom AZ \(p. 55\)](#)
- [Edge Router can't ping the ESXi Edge Gateway \(p. 55\)](#)
- [Error in the OVF template \(p. 56\)](#)
- [Proxy server connection problems or changes \(p. 56\)](#)

Can't connect to the RDS connector

In this case, you can't connect to the RDS connector on your vSphere cluster.

The cause for this issue is almost always that one or more of the following values in your .ovf file are incorrect:

- The host name
- IP addresses in the Management Network
- The custom Availability Zone (custom AZ) ID
- The certificate

To solve the issue when onboarding is not complete, deploy the RDS Edge Router image and correct the values in the .ovf file. If a certificate is incorrect, check the output in the `/var/output/log/application.log` file.

To solve the issue when onboarding is finished, complete the following steps:

1. Delete all of the management virtual machines (VMs) associated with onboarding.
2. Delete any roles created by the VMware Virtual DMZ Environment (VDME), if any.
3. Delete the custom AZ in Amazon RDS.
4. Complete the onboarding steps for a new custom AZ.

For more information, see [Onboard your vSphere cluster \(p. 20\)](#).

Custom AZ is unregistered or creating

If your custom AZ is unregistered or is in **Creating** status on the **Custom AZs** page, your custom AZ has yet to complete onboarding. The onboarding might still be in progress.

To solve the issue, make sure that your custom AZ ID is correct. Also, make sure that you selected the correct custom AZ. If you are onboarding a new custom AZ, you might have selected this new custom AZ by mistake instead of an already onboarded custom AZ.

Custom AZ is disconnected

If your custom AZ is disconnected, Amazon RDS can't reach your custom AZ. In this state, some Amazon RDS features are disabled on this specific custom AZ. In this state, the AWS Management Console shows the **Disconnected** status on the **Custom AZs** page.

RDS

> Custom AZs

Custom AZs

Delete

Modify

Create Custom AZ

filter Custom AZs

< 1 >

	AZ Name	AZ ID	Environment	Status	Created Time
<input type="radio"/>	customAZ001	1234567891	VMware	available	N/A
<input type="radio"/>	customAZ002	1234567892	VMware	Disconnected	N/A

Your custom AZ might not have internet access. Check the Distributed Port Group that is providing internet access to the custom AZ to verify whether it still has internet access. You can verify internet access by first deploying a VM attached to this Distributed Port Group. You can then run `curl checkip.amazonaws.com` or go to <http://checkip.amazonaws.com/> in a browser from within this VM.

To solve the issue, make sure that the Distributed Port Group provides internet access.

If you make any adjustments to your environment, wait up to 15 minutes for connectivity to be re-established. If your custom AZ remains offline after taking the steps described preceding, contact AWS Support.

Can't create a new custom AZ

In this case, you can't create a new custom AZ, and the following error can be returned.

```
Custom Availability Zones quota exceeded.
```

To solve the issue, delete your unused DB instances and unused custom AZs. If you can't create a new custom AZ after deleting unused DB instances and unused custom AZs, contact AWS Support.

For information about creating a new custom AZ, see [Creating additional custom AZs in an AWS Region](#) (p. 49).

Edge Router can't ping the ESXi Edge Gateway

In this case, the Edge Router can't ping the ESXi Edge Gateway.

To solve the issue, check the routing configuration from Edge Router console, and look for errors.

Error in the OVF template

In this case, there is an error in the OVF template.

If you haven't completed onboarding, modify the OVF template using the software package option to attempt to solve the issue.

If you have completed onboarding, complete the following steps to attempt to solve the issue:

- Delete all your management VMs.
- Remove any roles created by VDME.
- Delete the custom AZ in Amazon RDS.
- Create a new custom AZ.

For more information about the OVF template, see [Onboard your vSphere cluster \(p. 20\)](#).

For information about creating a new custom AZ, see [Creating additional custom AZs in an AWS Region \(p. 49\)](#).

Proxy server connection problems or changes

In this case, you can't reach the internet through a proxy server, or you want to change your proxy server settings.

To solve connectivity problems, contact AWS Support. To avoid connectivity problems, contact AWS Support before changing any proxy server settings.

Document history

The following table describes important changes in each release the *Amazon RDS on VMware User Guide* after October 2019. For notification about updates to this documentation, you can subscribe to an RSS feed. For information about Amazon Relational Database Service (Amazon RDS), see the [Amazon Relational Database Service User Guide](#).

update-history-change	update-history-description	update-history-date
RDS on VMware can now use HTTPS (p. 57)	RDS on VMware can now use HTTPS to connect with AWS. For more information, see How Amazon RDS on VMware works .	April 20, 2021
Point-in-time recovery (PITR) supported for Microsoft SQL Server DB instances (p. 57)	RDS on VMware now supports restoring SQL Server DB instances to a specified time. For more information, see Support for RDS features in Amazon RDS on VMware .	December 22, 2020
Cross-CAZ read replica support (p. 57)	RDS on VMware now supports creating a read replica for a MySQL or PostgreSQL DB instance in a different custom Availability Zone (CAZ) from the primary DB instance. For more information, see Creating read replicas .	November 12, 2020
Reserved DB instance support (p. 57)	You can now reserve RDS on VMware DB instances for a period of time. Reserved RDS on VMware DB instances provide a discount compared to on-demand DB instance pricing. For more information, see Support for RDS features in Amazon RDS on VMware .	October 26, 2020
Read replica support (p. 57)	RDS on VMware now supports creating read replicas for MySQL and PostgreSQL DB instances. For more information, see Creating read replicas .	June 18, 2020
DB engine upgrade supported for PostgreSQL DB instances (p. 57)	RDS on VMware now supports upgrading PostgreSQL DB instances from release from 10.9-R1 to release 10.10-R1. For more information, see Support for RDS features in Amazon RDS on VMware .	May 20, 2020

Proxy server support (p. 57)	RDS on VMware connects with AWS services, such as Amazon CloudWatch and Amazon S3, over HTTPS. RDS on VMware now supports using a proxy server for such external traffic. For more information about using a proxy server, see Complete the prerequisites and Onboard your vSphere cluster .	May 12, 2020
Disconnected status (p. 57)	RDS on VMware now displays the Disconnected status if Amazon RDS can't reach your custom AZ. For more information, see Custom AZ is disconnected .	February 12, 2020

Earlier Updates

The following table describes important changes to the *Amazon RDS on VMware User Guide* before November 2019.

Change	Description	Date changed
New guide	This is the first release of the <i>Amazon RDS on VMware User Guide</i> .	October 16, 2019

AWS glossary

For the latest AWS terminology, see the [AWS glossary](#) in the *AWS General Reference*.