# Table of Contents

What Is Amazon RDS on VMware? ................................................................. 1  
Features of Amazon RDS on VMware .............................................................. 1  
Accessing Amazon RDS on VMware .............................................................. 2  
How Amazon RDS on VMware Works  
  Onboarding ......................................................... 2  
  Connecting .......................................................... 3  
  Provisioning and Managing ......................................................... 3  
  Backing Up and Restoring ...................................................... 4  
Terminology ......................................................................................... 4  
  VMware Terminology ......................................................... 4  
  Amazon RDS on VMware Terminology ......................................... 4  
RDS Feature Support ........................................................................... 5  
Setting Up .......................................................................................... 8  
  Sign Up for AWS ..................................................... 8  
  Create and Configure an IAM User .............................................. 8  
  Create an IAM User .................................................... 8  
  Create Access Keys ...................................................... 10  
SSL/TLS Certificate Requirements ....................................................... 10  
Getting Started ............................................................................... 11  
  Complete the Prerequisites ...................................................... 12  
  Onboard Your vSphere Cluster .................................................. 17  
    Import the Installer VM Certificate ........................................ 28  
Working with Amazon RDS on VMware .................................................. 31  
  Installing the Media .......................................................... 31  
    Supported Media ....................................................... 31  
    Install the Media ......................................................... 32  
    Troubleshooting .......................................................... 36  
  Choosing the DB Instance Class ...................................................... 37  
    DB Instance Class Types ............................................... 37  
    Terminology ................................................................................ 38  
    Specifications ........................................................................... 38  
  Creating a DB Instance .......................................................... 39  
    Available Settings ......................................................... 43  
  Creating Additional Custom AZs ..................................................... 44  
  Managing On-Premises DB Instances ................................................ 46  
Troubleshooting .................................................................................. 47  
  Can't Connect to the RDS Connector .............................................. 47  
  Custom AZ Is Unregistered or Creating ......................................... 47  
  Custom AZ Is Disconnected ..................................................... 48  
  Can't Create a New Custom AZ ................................................... 48  
  Edge Router Can't Ping the ESXi Edge Gateway  
  Error in the OVF Template ......................................................... 48  
Document History ............................................................................. 50  
  Earlier Updates .............................................................................. 50  
AWS glossary ................................................................................... 51
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 VPN tunnel connecting 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. 2)
- How Amazon RDS on VMware Works (p. 2)
- Terminology (p. 4)
- Support for RDS Features in Amazon RDS on VMware (p. 5)

To start work with Amazon RDS on VMware, see Setting Up Amazon RDS on VMware (p. 8).

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 (except for Microsoft SQL Server DB instances)
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 a dedicated virtual private network (VPN) tunnel.

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 VPN 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 MySQL, PostgreSQL, and Microsoft SQL Server.

You also create an Application Network in your vSphere cluster. Your applications, users, and 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.

![Diagram of VMware vSphere cluster](image)

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. 4)
- RDS Edge Router (p. 5)
- RDS Connector (p. 5)
- RDS Cluster Control Network (p. 5)
- Application Network (p. 5)
- VPN Originator IP (p. 5)

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. In addition, it establishes an outbound VPN connection to a single-tenant DMZ or demilitarized zone (sometimes referred to as a perimeter network or screened subnet) in AWS. This DMZ is specific to your deployment.

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.

VPN Originator IP

The VPN originator IP is an external IP address for outgoing traffic from the vSphere cluster to the Amazon RDS website. This external IP address is used during the configuration of a vSphere cluster. Amazon RDS on VMware uses the VPN originator IP address at that point to create a VPN tunnel between the vSphere cluster and the Amazon RDS website.

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.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Supported</th>
<th>Notes</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB instance provisioning</td>
<td>Yes</td>
<td></td>
<td><a href="#">Creating an Amazon RDS DB Instance</a></td>
</tr>
<tr>
<td>Feature</td>
<td>Supported</td>
<td>Notes</td>
<td>More Information</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------</td>
<td>-------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>Modifying the master user password</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Renaming a DB instance</td>
<td>Yes</td>
<td></td>
<td>Renaming a DB Instance</td>
</tr>
<tr>
<td>Rebooting a DB instance</td>
<td>Yes</td>
<td></td>
<td>Rebooting a DB Instance</td>
</tr>
<tr>
<td>Stopping a DB instance</td>
<td>No</td>
<td></td>
<td>Stopping an Amazon RDS DB Instance Temporarily</td>
</tr>
<tr>
<td>Starting a DB instance</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multi-AZ deployments</td>
<td>No</td>
<td></td>
<td>High Availability (Multi-AZ) for Amazon RDS</td>
</tr>
<tr>
<td>DB parameter groups</td>
<td>No</td>
<td></td>
<td>Working with DB Parameter Groups</td>
</tr>
<tr>
<td>Read Replicas</td>
<td>No</td>
<td></td>
<td>Working with Read Replicas</td>
</tr>
<tr>
<td>Encryption at rest and compliance</td>
<td>No</td>
<td></td>
<td>Encrypting Amazon RDS Resources</td>
</tr>
<tr>
<td>certification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tagging Amazon RDS resources</td>
<td>Yes</td>
<td></td>
<td>Tagging Amazon RDS Resources</td>
</tr>
<tr>
<td>Option groups</td>
<td>No</td>
<td></td>
<td>Working with Option Groups</td>
</tr>
<tr>
<td>Modifying the maintenance window</td>
<td>No</td>
<td></td>
<td>Maintaining a DB Instance</td>
</tr>
<tr>
<td>Modifying the backup window</td>
<td>No</td>
<td></td>
<td>Working With Backups</td>
</tr>
<tr>
<td>DB instance scaling</td>
<td>Yes</td>
<td></td>
<td>Modify the on-premises DB instance class to scale the DB instance.</td>
</tr>
<tr>
<td>Manual and automatic DB snapshots</td>
<td>Yes</td>
<td></td>
<td>DB snapshots aren't stored in Amazon S3. DB snapshot copying and sharing aren't supported.</td>
</tr>
</tbody>
</table>

**Modifying an Amazon RDS DB Instance**

**Renaming a DB Instance**

**Rebooting a DB Instance**

**Stopping an Amazon RDS DB Instance Temporarily**

**Starting an Amazon RDS DB Instance That Was Previously Stopped**

**High Availability (Multi-AZ) for Amazon RDS**

**Working with DB Parameter Groups**

**Working with Read Replicas**

**Encrypting Amazon RDS Resources**

**Tagging Amazon RDS Resources**

**Working with Option Groups**

**Maintaining a DB Instance**

**Working With Backups**

**Modifying an Amazon RDS DB Instance**

**Choosing the On-Premises DB Instance Class (p. 37)**

**Creating a DB Snapshot**
### RDS Feature Support

<table>
<thead>
<tr>
<th>Feature</th>
<th>Supported</th>
<th>Notes</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restoring from a DB snapshot</td>
<td>Yes</td>
<td>—</td>
<td>Restoring from a DB Snapshot</td>
</tr>
<tr>
<td>Point-in-time recovery</td>
<td>Yes</td>
<td>Currently, this feature is supported for MySQL and PostgreSQL. It isn’t supported for Microsoft SQL Server.</td>
<td>Restoring a DB Instance to a Specified Time</td>
</tr>
<tr>
<td>Enhanced Monitoring</td>
<td>No</td>
<td>—</td>
<td>Enhanced Monitoring</td>
</tr>
<tr>
<td>Amazon CloudWatch monitoring</td>
<td>Yes</td>
<td>—</td>
<td>Monitoring with Amazon CloudWatch</td>
</tr>
<tr>
<td>Publishing database engine logs to Amazon CloudWatch Logs</td>
<td>No</td>
<td>—</td>
<td>Publishing Database Engine Logs to Amazon CloudWatch Logs</td>
</tr>
<tr>
<td>Event notification</td>
<td>No</td>
<td>—</td>
<td>Using Amazon RDS Event Notification</td>
</tr>
<tr>
<td>Amazon RDS Performance Insights</td>
<td>No</td>
<td>—</td>
<td>Using Amazon RDS Performance Insights</td>
</tr>
<tr>
<td>Stored procedures for Amazon RDS for MySQL</td>
<td>Yes</td>
<td>—</td>
<td>MySQL on Amazon RDS SQL Reference</td>
</tr>
<tr>
<td>Automatic minor engine version upgrade</td>
<td>No</td>
<td>—</td>
<td>Automatically Upgrading the Minor Engine Version</td>
</tr>
<tr>
<td>Replication with external databases (MySQL)</td>
<td>No</td>
<td>—</td>
<td>Replication with a MySQL or MariaDB Instance Running External to Amazon RDS</td>
</tr>
<tr>
<td>Importing backups from Amazon S3 (Microsoft SQL Server)</td>
<td>No</td>
<td>—</td>
<td>Importing and Exporting SQL Server Databases</td>
</tr>
</tbody>
</table>

### 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. 11).

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. 8)
- Create and Configure an IAM User (p. 8)
- SSL/TLS Certificate Requirements (p. 10)

Sign Up for AWS

If you have an AWS account already, skip to the next section, Create and Configure an IAM User (p. 8).

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

To create a new AWS account
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. 8)
- Create Access Keys (p. 10)

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. Use your AWS account email address and password to sign in as the AWS account root user to the IAM console at https://console.aws.amazon.com/iam/.

   **Note**
   We strongly recommend that you adhere to the best practice of using the Administrator IAM user below 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.
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 Managing Access Keys for Your AWS Account, Installing the AWS Command Line Interface, 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 a Region (p. 44).

During onboarding, you configure the following networks.

<table>
<thead>
<tr>
<th>Network Name</th>
<th>Purpose</th>
<th>DHCP Server Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Control Network</td>
<td>New network for communication between Amazon RDS management virtual machines (VMs) and database VMs</td>
<td>No. Amazon RDS runs its own Dynamic Host Configuration Protocol (DHCP) server on this network.</td>
</tr>
<tr>
<td>Internet Network</td>
<td>New or existing network for outbound internet connectivity for Amazon RDS VMs and for establishing a VPN tunnel to the Amazon RDS service</td>
<td>Yes. This network must advertise a default route.</td>
</tr>
<tr>
<td>Application Network</td>
<td>New or existing network for communication between your applications and Amazon RDS database VMs</td>
<td>Yes. This network can advertise a default route, but the corresponding default route is not installed.</td>
</tr>
<tr>
<td>Management Network</td>
<td>Existing network for communication between Amazon RDS management VMs and ESXi hosts</td>
<td>No. You must provide a static IP address during onboarding.</td>
</tr>
</tbody>
</table>

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. 12)
2. Onboard Your vSphere Cluster (p. 17)

For more details about working with Amazon RDS on VMware, see Working with Amazon RDS on VMware (p. 31).

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. 8).
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.
      • **VPN Originator IP** – The external source IPv4 address of packets leaving your virtual data center.

      This address is used to configure an IP security (IPSec) VPN tunnel. This VPN tunnel goes from your vSphere cluster to an RDS DMZ or demilitarized zone (sometimes referred to as a perimeter network or screened subnet) in AWS. This DMZ is created specifically for that tunnel.

      **Note**
      This address must not change, and only vSphere clusters are supported.

   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.
- Outbound connectivity to the internet must have a fixed, public-facing IP (Originator IP for outbound VPN).
- 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 traffic for ISAKMP (UDP port 500), IPSec NAT Traversal (UDP port 4500), and Encapsulating Security Payload (IP protocol 50).
- 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 will be given an address by 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.
Complete the Prerequisites

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. 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.
• Verify the VPN Originator IP.

To do this, you can put a small Linux VM or a Windows VM on the Internet Network and then run the following command.

```
curl checkip.amazonaws.com
```

Or you can put a small Linux VM or a Windows VM on the Internet Network, open a web browser, and go to http://checkip.amazonaws.com/.

After determining the IP address, get the IP address for another VM on the Internet Network. Then make sure that you're getting the same IP address.

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.

9. 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.
10. 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.

```json
{
   "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 Policies in the AWS Identity and Access Management User Guide.

## Onboard Your vSphere Cluster

After you complete the steps in Complete the Prerequisites (p. 12), 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 top-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 top-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.

   d. In Custom AZ name, enter a name for the custom AZ.
e. In **VPN settings**, enter a name for the VPN for **VPN tunnel name** and enter the VPN Originator IP for **VPN originator IP**.

f. 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.

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. 28) 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

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.
If you can't connect to the AWS Region, make sure that you completed all prerequisites described in Complete the Prerequisites (p. 12).

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.
13. Choose **NEXT** to open the **Network Configurations** page.
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.
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. 12)**. 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.
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.
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.
   a. In the top-right corner of the console, choose the AWS Region that contains your custom AZs.
   b. In the navigation pane, choose **Custom AZs**.
   c. View the **Status** column.

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. 48).

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. 39).

### 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](image)

   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.certificate"]`

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

28
A page similar to the following opens.

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.

   ```bash
   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. 17).

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. 31)
- Choosing the On-Premises DB Instance Class (p. 37)
- Creating an On-Premises DB Instance (p. 39)
- Creating Additional Custom AZs in a Region (p. 44)
- Managing Your On-Premises DB Instances (p. 46)

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. 37).

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

For more information, see [https://my.visualstudio.com/Downloads?q=windows%20server%202016](https://my.visualstudio.com/Downloads?q=windows%20server%202016).
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.

• **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

For more information, see https://my.visualstudio.com/Downloads?q=sql%20server%202016.
5. In the Install media section, choose Import.

The Import media page appears.
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.
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.

---

**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. 31).

Example

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

For Linux, OS X, or Unix:

```bash
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:

```bash
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. 37)
- Media Not Supported (p. 37)
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. 11).

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. 31).

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. 48).

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.

<table>
<thead>
<tr>
<th>Instance Class</th>
<th>vCPU</th>
<th>Memory (GiB)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>db.mv11 – Current Generation General</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>db.mv11.medium</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>db.mv11.large</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>db.mv11.xlarge</td>
<td>4</td>
<td>16</td>
</tr>
<tr>
<td>db.mv11.2xlarge</td>
<td>8</td>
<td>32</td>
</tr>
<tr>
<td>db.mv11.4xlarge</td>
<td>16</td>
<td>64</td>
</tr>
<tr>
<td>db.mv11.12xlarge</td>
<td>48</td>
<td>192</td>
</tr>
<tr>
<td>db.mv11.24xlarge</td>
<td>96</td>
<td>384</td>
</tr>
<tr>
<td><strong>db.cv11 – Current Generation Compute Optimized</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>db.cv11.small</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>db.cv11.medium</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>db.cv11.large</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>db.cv11.xlarge</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>db.cv11.2xlarge</td>
<td>8</td>
<td>16</td>
</tr>
<tr>
<td>db.cv11.4xlarge</td>
<td>16</td>
<td>32</td>
</tr>
<tr>
<td>db.cv11.9xlarge</td>
<td>36</td>
<td>72</td>
</tr>
<tr>
<td>db.cv11.18xlarge</td>
<td>72</td>
<td>144</td>
</tr>
</tbody>
</table>
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. 8).
- 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. 11).
- If the status of the custom AZ in which you want to create a DB instance is Disconnected, see Custom AZ Is Disconnected (p. 48).
- 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. 31). 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. 37).

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

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/](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.

<table>
<thead>
<tr>
<th>Instance Class</th>
<th>vCPU</th>
<th>Memory (GiB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>db.rv11.large</td>
<td>2</td>
<td>16</td>
</tr>
<tr>
<td>db.rv11.xlarge</td>
<td>4</td>
<td>32</td>
</tr>
<tr>
<td>db.rv11.2xlarge</td>
<td>8</td>
<td>64</td>
</tr>
<tr>
<td>db.rv11.4xlarge</td>
<td>16</td>
<td>128</td>
</tr>
<tr>
<td>db.rv11.12xlarge</td>
<td>48</td>
<td>384</td>
</tr>
<tr>
<td>db.rv11.24xlarge</td>
<td>96</td>
<td>768</td>
</tr>
</tbody>
</table>
3. In the navigation pane, choose **Databases**.
4. Choose **Create database**.

The **Create database** page opens.

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**.
Creating a DB Instance

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**.

**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
8. In the Settings section, complete the DB instance identifier, Master username, and Master password settings. For more information about settings, see Settings (p. 43).

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 Settings (p. 43).

Example

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

For Linux, OS X, or Unix:

```bash
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:

```bash
aws rds create-db-instance ^
  --db-instance-identifier mydbinstance ^
  --db-instance-class db.mv11.medium ^
  --engine postgres ^
  --availability-zone mycustomaz_identifier ^
  --master-username masterawsuser ^
```
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 Settings (p. 43).

**Settings**

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

<table>
<thead>
<tr>
<th>Console Setting</th>
<th>CLI Option</th>
<th>RDS API Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup retention period</td>
<td>--backup-retention-</td>
<td>BackupRetentionPeriod</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>period</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup window</td>
<td>--preferred-</td>
<td>PreferredBackupWindow</td>
<td>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.</td>
</tr>
<tr>
<td>Console Setting</td>
<td>CLI Option</td>
<td>RDS API Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------</td>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For more information, see Custom Availability Zones (p. 4).</td>
</tr>
<tr>
<td>Database name</td>
<td>--db-name</td>
<td>DBName</td>
<td>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.</td>
</tr>
<tr>
<td>Database port</td>
<td>--port</td>
<td>Port</td>
<td>The port that you want to use to access the DB instance.</td>
</tr>
<tr>
<td>DB instance class</td>
<td>--db-instance-class</td>
<td>DBInstanceClass</td>
<td>The DB instance class that you want to use.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For more information, see Choosing the On-Premises DB Instance Class (p. 37).</td>
</tr>
<tr>
<td>DB instance identifier</td>
<td>--db-instance-identifier</td>
<td>DBInstanceIdentifier</td>
<td>The name for your DB instance. This value is stored as a lowercase string.</td>
</tr>
<tr>
<td>Engine</td>
<td>--engine</td>
<td>Engine</td>
<td>The name of the database engine to be used for this instance. Currently, the following engines are supported: mysql, postgres, sqlserver-ee</td>
</tr>
<tr>
<td>Master password</td>
<td>--master-user-password</td>
<td>MasterUserPassword</td>
<td>The password for your master user.</td>
</tr>
<tr>
<td>Master username</td>
<td>--master-username</td>
<td>MasterUsername</td>
<td>The name that you use as the master user name to log on to your DB Instance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For more information, including a list of the default privileges for the master user, see Master User Account Privileges in the Amazon RDS User Guide.</td>
</tr>
<tr>
<td>Version</td>
<td>--engine-version</td>
<td>EngineVersion</td>
<td>The version of database engine that you want to use.</td>
</tr>
</tbody>
</table>

Creating Additional Custom AZs in a Region

During the onboarding process described in Getting Started with Amazon RDS on VMware (p. 11), 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.

5. In Custom AZ name, enter a name for the custom AZ.
6. In VPN settings, enter a friendly name for the VPN in VPN tunnel name, and enter the Local Uplink IP in VPN originator IP.

Note
A Local Uplink IP is the external source IPv4 address of packets leaving your virtual data center. Multiple vSphere clusters in the same virtual data center can use the same Local Uplink IP or different Local Uplink IPs. However, you must create a new VPN connection for each vSphere cluster.
7. Choose **Create custom AZ**.

Amazon RDS on VMware begins the custom AZ creation process.

**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. 5)*. 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. 48)*.
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. 47)
- Custom AZ Is Unregistered or Creating (p. 47)
- Custom AZ Is Disconnected (p. 48)
- Can't Create a New Custom AZ (p. 48)
- Edge Router Can't Ping the ESXi Edge Gateway (p. 48)
- Error in the OVF Template (p. 49)

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 VPN originator IP address
- 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 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. 17).

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.
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.

The following cases might result in a disconnected custom AZ:

- 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/](http://checkip.amazonaws.com/) in a browser from within this VM.

- The custom AZ's VPN Originator IP might have changed. Make sure that this IP address matches the internet-facing IP address of your vSphere Cluster. You can verify this 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/](http://checkip.amazonaws.com/) in a browser from within this VM. The IP address returned is the cluster's internet-facing IP address. If this IP address doesn't match the Originator IP for this custom AZ, the custom AZ is disconnected.

To solve the issue, make sure that the Distributed Port Group provides internet access. Also, make sure that the custom AZ's VPN Originator IP matches the internet-facing IP address of your vSphere Cluster. You might need to change your egress routing to use this IP address.

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

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 a Region (p. 44).

**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. 17).

For information about creating a new custom AZ, see Creating Additional Custom AZs in a Region (p. 44).
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.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date Changed</th>
</tr>
</thead>
<tbody>
<tr>
<td>update-history-change</td>
<td>RDS on VMware now displays the <strong>Disconnected</strong> status if Amazon RDS can't reach your custom AZ. For more information, see Custom AZ Is Disconnected.</td>
<td>February 12, 2020</td>
</tr>
<tr>
<td>update-history-date</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Earlier Updates

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

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date Changed</th>
</tr>
</thead>
<tbody>
<tr>
<td>New guide</td>
<td>This is the first release of the Amazon RDS on VMware User Guide.</td>
<td>October 16, 2019</td>
</tr>
</tbody>
</table>
AWS glossary

For the latest AWS terminology, see the AWS glossary in the AWS General Reference.