aws

User Guide

# AWS Secret Region

# AWS Secret Region: User Guide



This documentation is a copy of the public AWS documentation. For supplemental information that is specific to AWS Secret Region such as feature and service availability, see the AWS Secret Region User Guide. Published: June 26, 2024.

# Table of Contents

# What is AWS Secret Region?

AWS Secret Region is a private community cloud that provides on-demand computing resources and services. For example, you can create a server on-demand with AWS that you can connect to, configure, secure, and run just as you would a physical server. Your virtual server runs on an infrastructure managed by AWS, and you pay for your virtual server only while it runs, with no up-front purchase costs or ongoing maintenance costs. In addition, your virtual server can do things no physical server can, such as automatically scaling into multiple servers when the workload for your application increases.

> **Note**
>
> AWS Secret Region operates as an air-gapped cloud computing region with no connectivity to the Internet and no connectivity to public Amazon or AWS network resources. While AWS Secret Region is completely separate and distinct from other AWS regions, each service available within AWS Secret Region provides features and capabilities that are essentially the same as the public AWS offering.

> **Note**
>
> AWS Secret Region documentation may be made available prior to service availability in the AWS Secret Region. Please see marketing for available services and features.

**Topics**



# What is in this Guide?

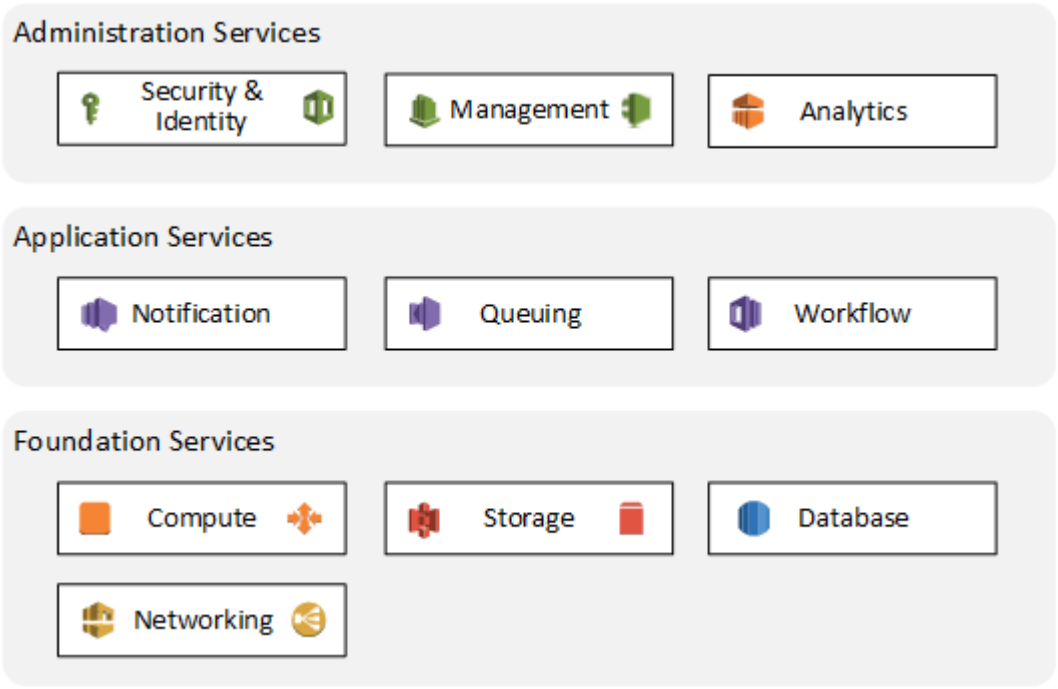
This guide provides instructions for setting up your account and identifies differences between the public Amazon Web Services (AWS) cloud offerings and the operational environment for AWS Secret Regions.

This guide is designed to complement the suite of public AWS documentation. Where the content of this guide differs from other AWS documentation, this guide should be interpreted as the relevant information for AWS Secret Region. For example, in the AWS documentation, when you see references to *Internet* or *Internet gateway*, these refer to your own private network.

# What Can I Do with AWS Secret Region?

You can run nearly anything on AWS Secret Region that you would run on physical hardware, such as websites, applications, databases, and data analysis. The services AWS Secret Region provides are designed to work together so that you can build complete solutions.

The following diagram shows just a few of the categories of functionality offered by AWS Secret Region.




In each category, there are one or more services. With so many offerings, you can design a solution that is tailored to your needs.

## Supported Services

AWS Secret Region currently supports the following services. To learn more about each service, including implementation differences for AWS Secret Region, see the corresponding links. For a complete listing of services supported by AWS Secret Region, see Services in AWS Secret Region .

### Compute

- Amazon Elastic Compute Cloud
- Amazon Virtual Private Cloud
- Amazon EC2 Auto Scaling
- Elastic Load Balancing

### Storage

- Amazon Simple Storage Service
- Amazon Elastic Block Store
- Amazon S3 Glacier

### Database

- Amazon Relational Database Service
- Amazon DynamoDB
- Amazon ElastiCache
- Amazon Redshift

### Networking & Content Delivery

- Amazon Virtual Private Cloud
- AWS Direct Connect
- Elastic Load Balancing

### Management Tools

- Amazon CloudWatch
- AWS CloudFormation
- AWS CloudTrail
- AWS CLI and Tools for AWS Secret Region

### Security, Identity, & Compliance

- AWS Identity and Access Management

- AWS Key Management Service

### Analytics

- Amazon EMR
- Amazon Kinesis Data Streams
- Amazon Redshift

### Application Services

- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Simple Workflow Service

### Other Resources

- AWS Billing and Cost Management
- AWS Support

# Getting Started with AWS Secret Region

To use the AWS Secret Region, you must sign up to create a high side account on the Secret network. In other words, you can't use AWS accounts that were created for use in other public AWS Regions on the low side in the AWS Secret Region on the high side. Similarly, you cannot use high side AWS accounts that were created for the AWS Secret Region in other low side public AWS Regions.

The AWS Secret Region is an IC cloud service offering in the IC Information Technology Enterprise (IC ITE). The IC Chief Information Officer (CIO) has imposed some limited governance on the use of AWS Secret Region services. To comply, as a prospective workload owner for the AWS Secret Region, you must first have a valid TO/CLIN on a contract sponsored by the government. Once you have established a TO/CLIN, you can notify your government agency's provisioning team so they can create an AWS account for you in the AWS Secret Region.

After your account is created, you can start working with the AWS Secret Region. It is important to note that customers cannot accumulate charges prior to having a valid TO/CLIN.

**Topics**



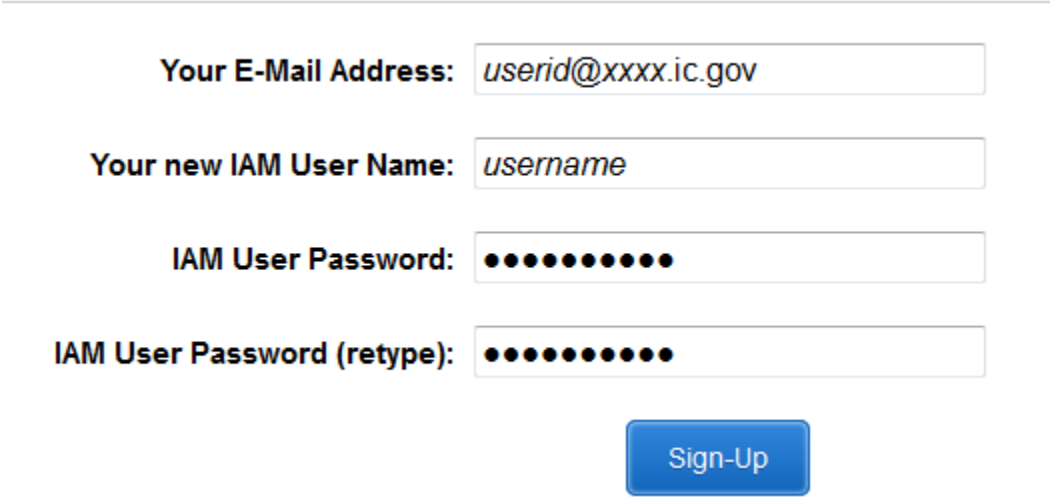
# Signing Up

Only members of an IC agency's account provisioning team can create AWS Secret Region accounts for workload owners in that agency.

The provisioning team members take an approved request on the Secret network and uses the information to create an AWS Secret Region account on the workload owner's behalf. The provisioning team member provides the email address and creates an IAM user name and a password. The email address must be JWICS routable and the password must contain a minimum of 10 characters.

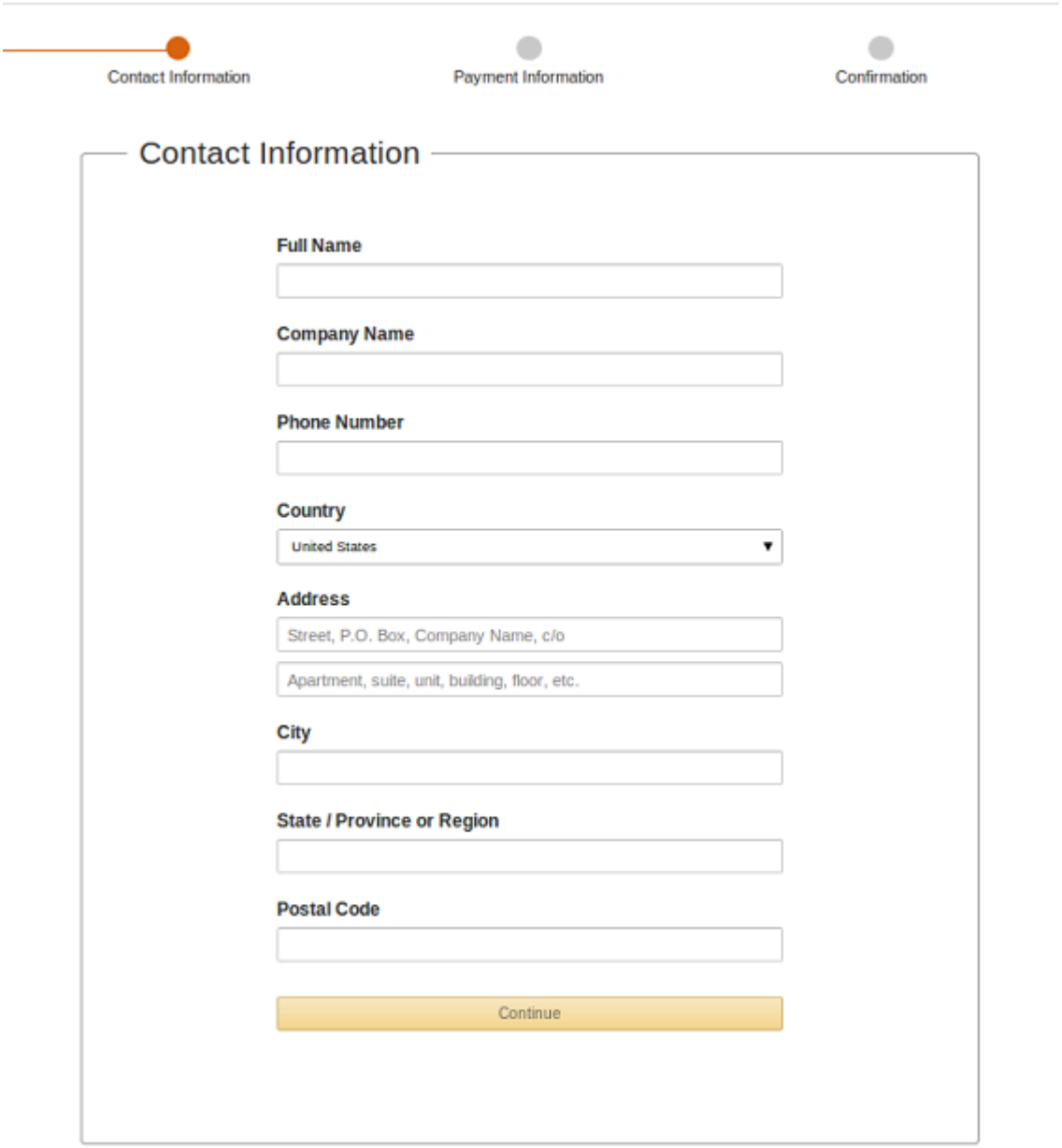
**Once your request has been approved by the agency provisioning team, you can create an account for the AWS Secret Region by doing the following:**

1. Navigate to the page https://signin.sc2shome.sgov.gov/signup?request_type=register.
2. On the account sign-up page, enter your email address, an IAM user name and password, and then click **Sign-Up**.

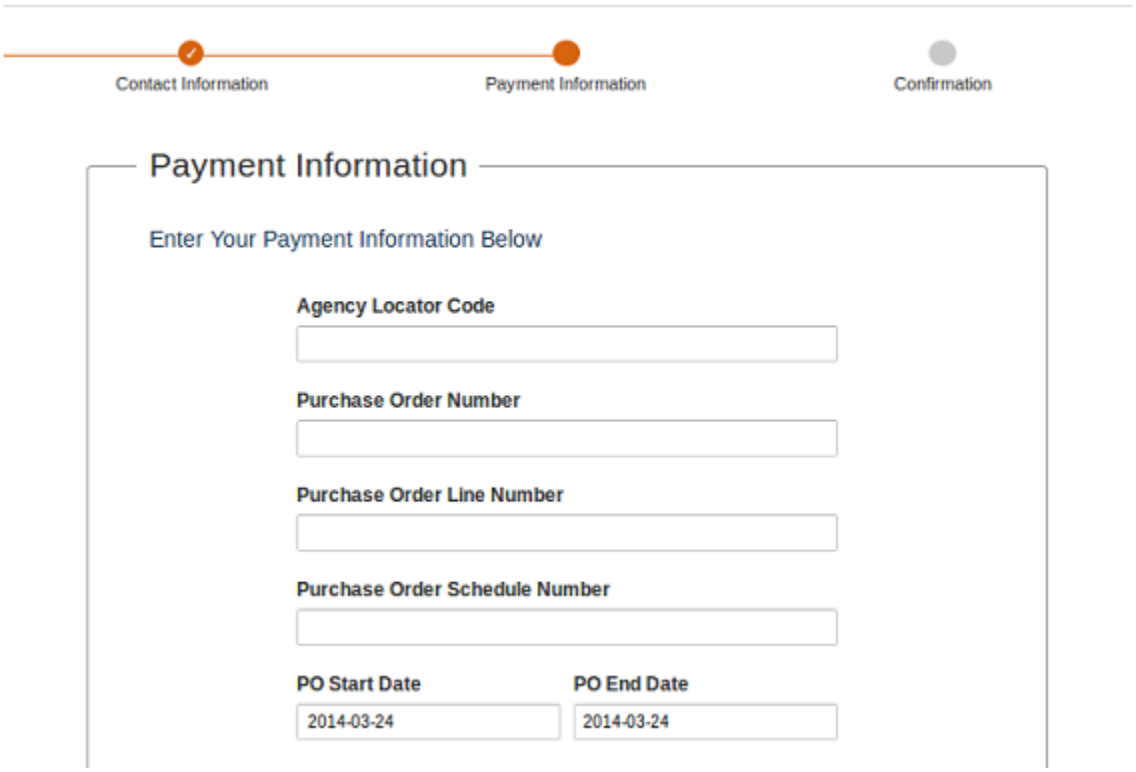



> **Note**
>
> If you later need to change the email address for an account, you use the Security Credentials page in the console. For more information, see Changing Your Account Email Address.

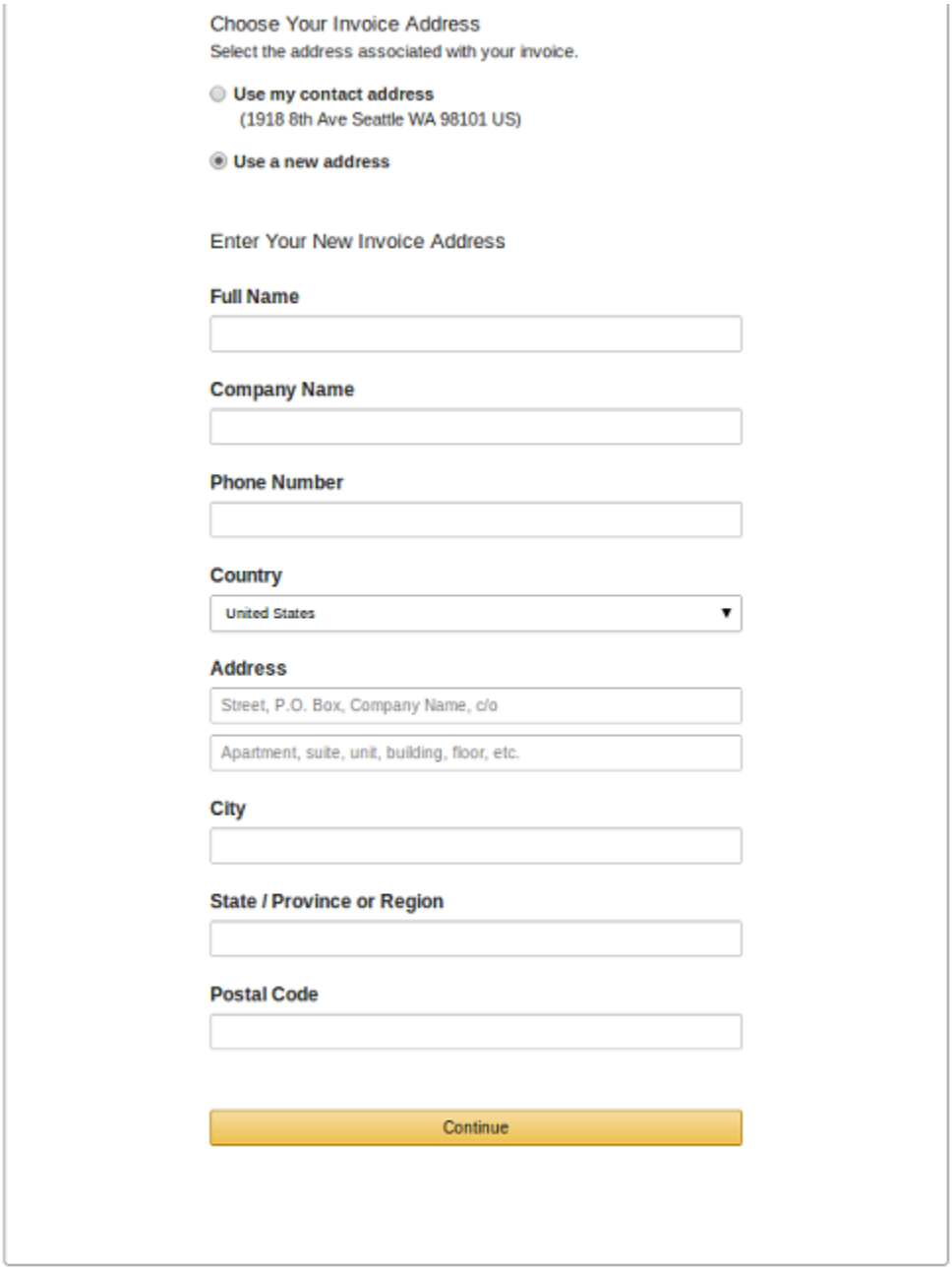
3. On the **Contact Information** page, enter your contact information and then click **Continue**.




4. On the **Payment Information** page, enter your payment information.




5. If your invoice address is different than your contact address, select **Use a new address** and enter your invoice address.




6. Click **Continue** to finish creating your account.

# Close Account

Use the AWS Management Console to close your AWS account. The steps below provide a high-level overview.

If you close the account that you're using for the AWS Firewall Manager administrator, AWS and Firewall Manager handle the closure as follows:

AWS revokes the account's administrative access from the service and deactivates any policies that were managed by the administrator account. The protections that were provided by these policies are stopped across the organization.

- Before closing your account, back up and then delete your policy data and other account resources. You will no longer have access to them after you close the account.
- For more information, see Closing an account.

You can close your AWS account using the following procedure.

**To close your AWS account**

1. Sign in to the account that you want to close. Note that if the AWS Identity and Access Management (IAM) user or role you sign in with does not have Administrator access, you can't close an account.
2. On the navigation bar in the upper-right corner, choose your account name (or alias), and then choose **My Account**.
3. On the **Account Settings** page, scroll to the end of the page to the **Close Account** section. Read and ensure that you understand the text next to the check box. After you close an AWS account, you can no longer use it to access AWS services.
4. Select the check box to accept the terms, and then choose **Close Account**.
5. In the confirmation box, choose **Close Account**.

# Using the AWS Management Console

The AWS Management Console is a web interface that you can use to interact with AWS services and perform many tasks, such as working with Amazon S3 buckets, launching and connecting to Amazon EC2 instances, setting CloudWatch alarms, and so on.

The IC CIO has deemed that all authentication requests to AWS Secret Region must use IC public key infrastructure (PKI) credentials. AWS does not natively support IC PKI, but does support federated enterprise authentication mechanisms. The AWS Secret Region Program Management Office has developed the AWS Secret Region Access Portal (CAP) to federate the IC's Identity, Authentication, and Authorization (IAA) services into the AWS Secret Region Identity and Access Management (IAM) services.

## How the Console Differs for AWS Secret Region

The implementation of the Console is different for AWS Secret Region in the following ways:

- Resource Groups, Tag Editor, and AWS Console mobile app are not available.
- Unified Search only supports service and feature searches.
- Console Home widgets are unavailable.
- myApplications is unavailable.

## To open the console

1. Go to https://cap.cia.sgov.gov/.
2. Locate the AWS Secret Region account you want to access.
3. Click the terminal icon next to the AWS Secret Region role that you want to assume for that account.

   You will be redirected to the console.
4. When you have finished, sign out by clicking your name in the navigation bar and then clicking **Sign Out**.

For more information about the console, see Getting Started with the AWS Management Console.

# Tracking AWS Spending

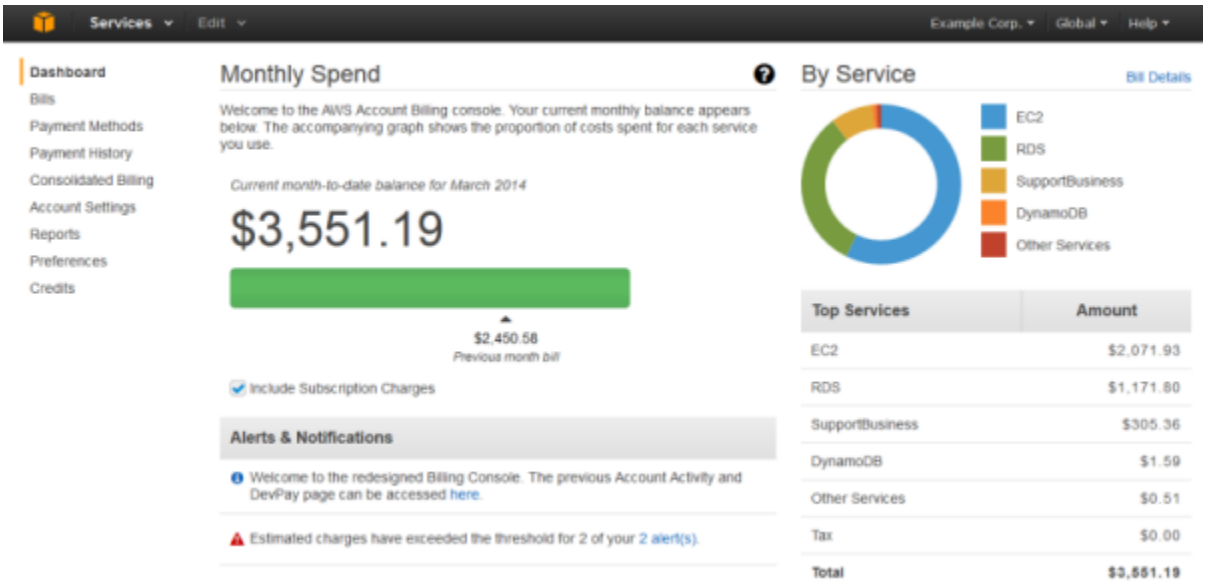
You can see your estimated AWS spending for the current month in one of two ways: as an overview in bar graph form, or as a detailed CSV report delivered daily to an Amazon S3 bucket. You can also see your past months' invoices and download them as PDF files.

**Topics**

- See an Overview of this Month's Spending
- See Line-Item Reports
- See Bills from Previous Months

## See an Overview of this Month's Spending

The Billing and Cost Management dashboard displays a high-level bar graph of your estimated spending for the current month and your total spending for the previous month, so that you can make at-a-glance comparisons:




### To see an overview of this month's spending

1. Sign in to the AWS Management Console at https://console.sc2shome.sgov.gov/.
2. Click your account name in the top navigation bar ("Example Corp." in the preceding illustration).
3. Click **Billing and Cost Management**.

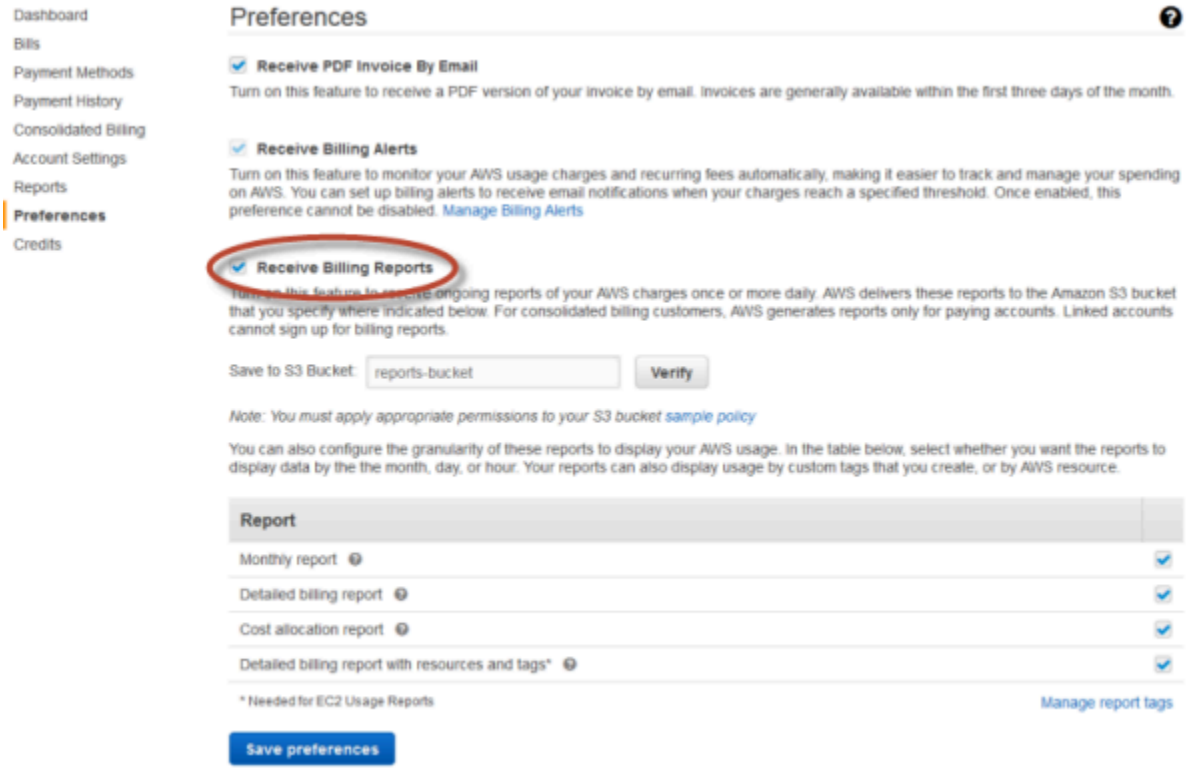
## See Line-Item Reports

You can sign up to receive detailed, line-item reports for every hour of your AWS spending for the current month. AWS publishes these reports to an Amazon S3 bucket that you designate at least once a day, and at the end of each month, publishes a final report. For information, see Understand Your Usage with Detailed Billing Reports in the AWS Billing User Guide.

### To sign up for Billing and Cost Management reports

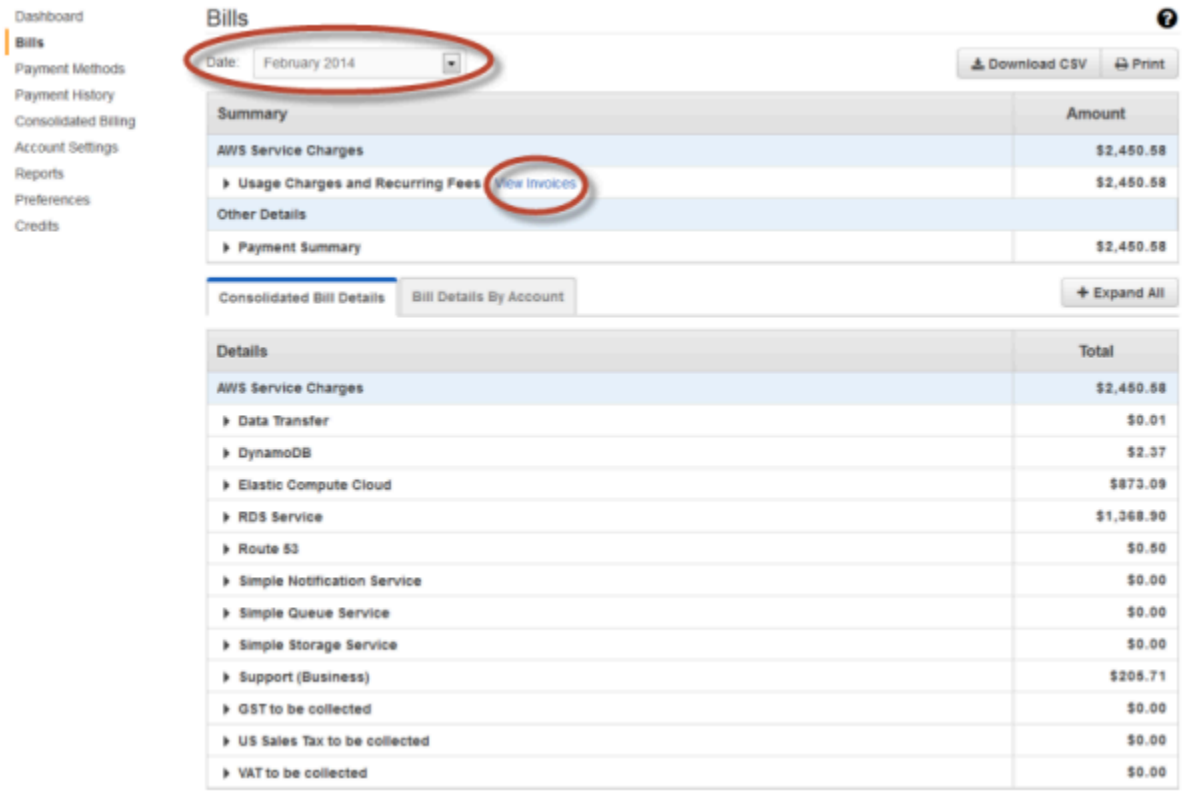
1. Sign in to the AWS Management Console at https://console.sc2shome.sgov.gov/.
2. Click your account name in the top navigation bar.

3. Click **Billing and Cost Management**.
4. Click **Preferences** in the left navigation pane.
5. Follow the instructions in the **Receive Billing Reports** section.




## See Bills from Previous Months

You can see bills from previous months on the **Bills** page of the Billing and Cost Management console. Your bill lists charges for each service in AWS you used, as well as other charges for your account, such as taxes or subscriptions for reserved instances or AWS Support. If your account is the paying account for a Consolidated Billing account family, you can also see the details for each linked account list separately.




**To view the Billing and Cost Management Bills page and download a PDF of your bill:**

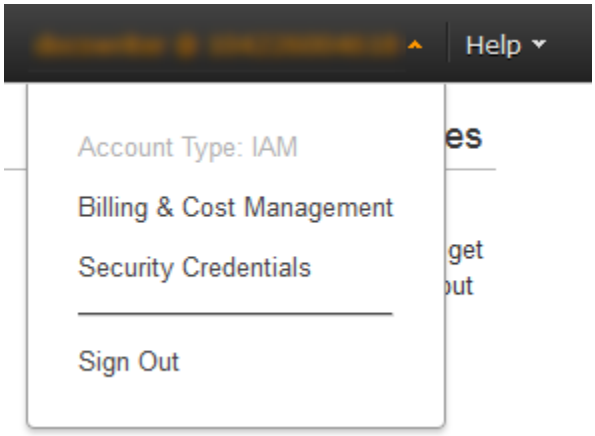
1. Sign in to the AWS Management Console at https://console.sc2shome.sgov.gov/
2. Click your account name in the top navigation bar.
3. Click **Billing and Cost Management**.
4. Click **Bills** in the left navigation pane.
5. Select the month you want to see in the **Date** list.
6. Click **View invoices** to download PDFs of previous bills.

# Changing Your Account Email Address

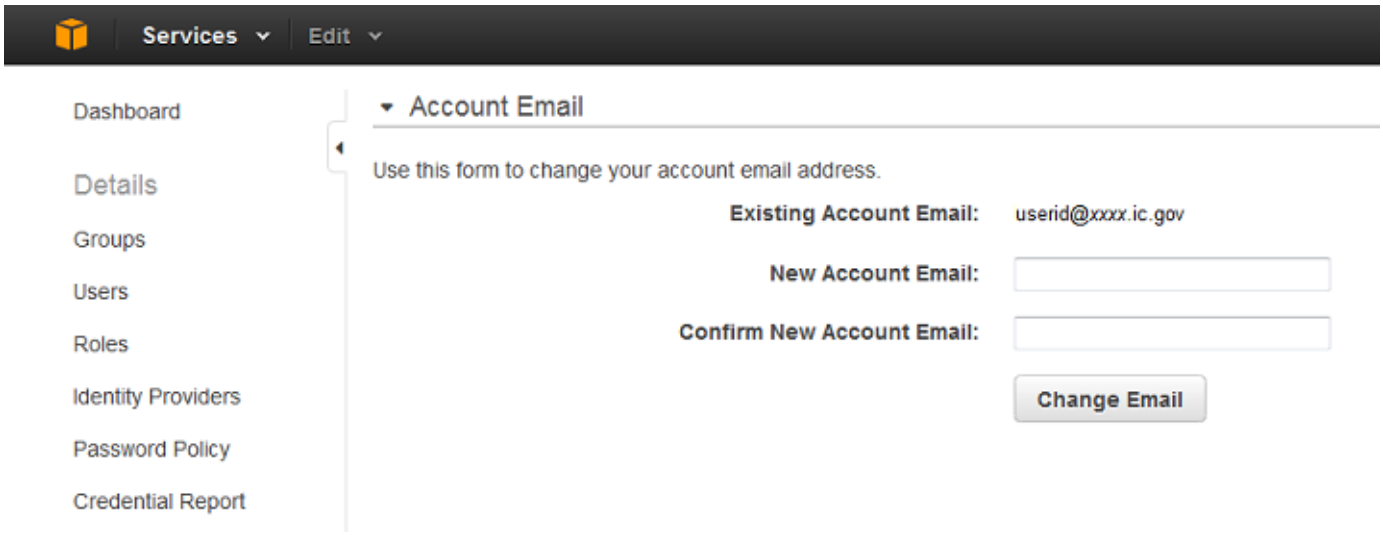
When your account is initially created in AWS Secret Region, it is associated with an email address. Later, if you need to change this email address, you use the following procedure.

**To change the email address for your account**

1. Sign into the AWS Management Console at https://console.sc2shome.sgov.gov/.
2. In the navigation bar, click your name, and then click **Security Credentials**.




3. In the **Account Email** section, enter your new account email address, and then click **Change Email**.




**To change the email address for your account for IAM roles**

1. Sign into the AWS Management Console at https://console.sc2shome.sgov.gov/.
2. Go to the Security Credentials console at https://console.sc2shome.sgov.gov/iam/home?#/my_password.
3. In the **Account Email** section, enter your new account email address and then choose **Change Email**.

# Amazon Linux 2 AMI for AWS Secret Region

Amazon Linux 2 is the next generation of Amazon Linux, a Linux server operating system from Amazon Web Services (AWS). It provides a secure, stable, and high-performance execution environment to develop and run cloud and enterprise applications. With Amazon Linux 2, you get an application environment that offers long-term support with access to the latest innovations in the Linux ecosystem.

**Topics**



## Tools and Certificates Included in Amazon Linux 2

When you use Amazon Linux 2, the following tools and certificates are already installed and configured:

- AWS Command Line Interface (AWS CLI)
- CA certificates

By using the latest version of Amazon Linux 2, you can ensure that you have the latest `ca-certificates` for AWS Secret Region. Amazon Linux 2 adds these certificates to the root CA bundle, so any tools that already use this bundle should successfully find the correct `ca-certificates` to verify SSL connections, including the AWS CLI and any AWS SDKs, such as Boto3.

## How to Update to the Latest Amazon Linux 2

Amazon Linux 2 provides long-term support that includes security updates and bug fixes for 5 years. You can use these steps to update your Amazon Linux 2 instance with the latest packages.

1. Log in to your Amazon Linux 2 instance.
2. Run the following commands.

```
sudo yum --disablerepo='*' --enablerepo='amzn2-*' update -y
sudo reboot
```

> **Note**
>
> Use the following command to only update the specific in-region configuration packages.
>
> ```
> sudo yum update '*-us-isob-east-1'
> ```

3. Run the `aws configure` command and make sure to set the default region to `us-isob-east-1`.

```
aws configure
```

Your Amazon Linux 2 instance is now up to date.

## How to update an imported Amazon Linux 2 AMI to work in the Region

If an instance is using an AMI copied from another Region, it will not contain the Region-specific packages and will not have the correct configuration for the `ca-certificates`, the AWS CLI, and SDK configurations. You can use these steps to update your Amazon Linux 2 instance with the latest Region-specific packages.

1. Log in to your Amazon Linux 2 instance.
2. To install Region-specific packages and configurations on an Amazon Linux 2 AMI copied from the low side, create a temporary `tmp-amzn2-iso` repo.

```
( cat << 'EOF'
[amzn2-iso]
name=Amazon Linux 2 isolated Region repository
```

```
mirrorlist=http://amazonlinux.$awsregion.$awsdomain/$releasever/core-$awsregion/
latest/$basearch/mirror.list
priority=9
gpgcheck=0
enabled=1
metadata_expire=300
mirrorlist_expire=300
report_instanceid=yes
EOF
) | sudo tee /etc/yum.repos.d/tmp-amzn2-iso.repo
```

3. Install the Region-specific packages.

```
sudo yum --disablerepo='*' --enablerepo='amzn2-iso' install '*-us-isob-east-1'
```

4. Remove the temporary `amzn2-iso` repo

```
sudo rm /etc/yum.repos.d/tmp-amzn2-iso.repo
```

5. Now you can run a `yum update` command to install any updates and security patches.

   To install all updates:

```
sudo yum --disablerepo='*' --enablerepo='amzn2-*' update -y
```

   To install just security updates.

```
sudo yum --disablerepo='*' --enablerepo='amzn2-*' --security -y update
```

Your Amazon Linux 2 instance is now configured to work in the Region. If you want to create an AMI based on this instance, clean up the yum cache and cloud init files:

```
sudo rm -rf /var/cache/yum/*
sudo rm -rf /var/lib/cloud/*
```

Use the Amazon EC2 console to create an AMI.

# Install Python3 based Botocore on Amazon Linux 2

Use the following procedure to enable and install Python3 based Botocore on Amazon Linux 2.

**To install Python3 based botocore**

1. Enable the AWS CLI by running the following command.

```
$ sudo amazon-linux-extras enable awscli1
```

2. Install the AWS CLI by running the following commands.

```
$ sudo yum clean all
```

```
$ sudo yum update awscli
```

3. To verify installation of the AWS CLI, run the following command.

```
$ aws --version
aws-cli/1.27.51 Python/3.7.16 Linux/5.10.147-133.644.amzn2.x86_64 botocore/1.29.51
```

4. Install boto3 for Python3 using the following command.

```
$ sudo yum install python3-boto3
```

# On-Premises and Docker Images Not Included

Amazon Linux 2 on-premises virtual and Docker images are currently unavailable in `us-isob-east-1`.

# Troubleshooting Amazon Linux 2

If you're having trouble with Amazon Linux 2, this section has some initial steps to help you troubleshoot. For more information, see the Amazon Linux 2 Security Center.

## AWS CLI Doesn't Work

If the AWS CLI doesn't work, try the following steps.

1. Run the `aws configure` command and verify that the region is set to `us-isob-east-1`.
2. If necessary, update to the latest Amazon Linux 2 AMI.

# SSL Certificate Verification Fails

If you experience SSL connection failures, try these steps.

1. See Testing Your Certificate Configuration to verify that your certificates are configured properly.
2. Update to the latest in-region `ca-certificates` package with the following command.

```
yum update ca-certificates-us-isob-east-1
```

3. If necessary, update to the latest Amazon Linux 2 AMI.

# Amazon Linux AMI for AWS Secret Region

The Amazon Linux AMI is a supported and maintained Linux image provided by Amazon Web Services for use on Amazon EC2. It includes packages for easy integration with AWS, including launch configuration tools and many popular AWS libraries and tools.

**Topics**



## Tools and Certificates Included in the Amazon Linux AMI

When you use the Amazon Linux AMI, the following tools and certificates are already installed and configured:

- AWS Command Line Interface (AWS CLI)
- Amazon EC2 AMI tools
- AWS SDK for Python (Boto) (The Boto 3 version is not included)
- CA certificates
- CA certificates for Java

## How the Amazon Linux AMI Differs for AWS Secret Region

The implementation of the Amazon Linux AMI is different for AWS Secret Region in the following ways:

- The Clam AntiVirus (ClamAV) package does not include virus definitions. If you want to use ClamAV, you will need to download definitions.
- The get_reference_source command to download source code for Amazon Linux is not available. Instead, you can use the **yumdownloader** to download an RPM.

# How to Update to the Latest Amazon Linux AMI (Quick Steps)

The Amazon Linux AMI is a rolling release that is periodically updated with new features and fixes. As long are you are not locking your AMI to a specific version, you can use these quick steps to update your AMI to the latest version.

1. Sign in to the Amazon Linux AMI.
2. Run the following commands:

```
sudo yum --disablerepo='*' --enablerepo='amzn-*' update -y
sudo sed -ri 's/^enabled=0$/enabled=1/' /etc/yum.repos.d/amzn-nosrc.repo
sudo yum install '*-config-us-isob-east-1'
sudo reboot
```

3. Run the `aws configure` command and make sure the default region is set to `us-isob-east-1`.

```
aws configure
```

Your Amazon Linux AMI instance is now up-to-date.

To update your Amazon Linux AMI again in the future, perform the following steps:

1. Run the following command:

```
sudo yum update
```

2. Run the following command to install any new config packages:

```
sudo yum install '*-config-us-isob-east-1'
```

# How to Update to the Latest Amazon Linux AMI

If you're not able to perform the previous quick steps to update your Amazon Linux AMI, you can try the steps in this section.

1. Run the following command to check whether the amzn-nosrc repository is enabled:

```
grep '^enabled=' /etc/yum.repos.d/amzn-nosrc.repo
```

If the repository is disabled, running `yum update` does not completely update the AMI.

2. If `enabled=1` does not appear in as the command output, run the following command to enable the repository:

```
sudo sed -ri 's/^enabled=0$/enabled=1/' /etc/yum.repos.d/amzn-nosrc.repo
```

3. Run yum update:

```
sudo yum update
```

4. Run the following command to install any new config packages:

```
sudo yum install '*-config-us-isob-east-1'
```

5. Sign out and sign in again to the Amazon Linux AMI.

   Packages to configure the AWS CLI and Amazon EC2 AMI tools make changes to /etc/profile.d/*, which do not take effect until you sign in.

6. Run the `aws configure` command and verify that the region is set to `us-isob-east-1`.

```
aws configure
AWS Access Key ID [None]: your-aws-access-key-id
AWS Secret Access Key [None]: your-aws-secret-key
Default region name [None]: us-isob-east-1
Default output format [None]: text
```

# Troubleshooting the Amazon Linux AMI

If you are having trouble with an Amazon Linux AMI, this section has some initial steps to help you troubleshoot. For more information, see the Amazon Linux AMI Security Center.

## AWS CLI Does Not Work

If the AWS CLI does not work, try the following steps:

1. Run the `aws configure` command and verify the region is set to `us-isob-east-1`.

2. If necessary, update to the latest Amazon Linux AMI.

## aws ec2 Commands Do Not Work

If you see errors, like the following, the AWS CLI might be looking for a newer Amazon EC2 API version than is deployed:

```
$ aws ec2 describe-images
```

```
A client error (NoSuchVersion) occurred when calling the DescribeImages operation: The requested version (2014-10-01) of service AmazonEC2 does not exist.
```

- To work around this issue, try running the following command:

```
sudo rm -f /usr/lib/python2.6/site-packages/botocore/data/aws/ec2/2014-10-01.*
```

# More Information

- Amazon Linux AMI Security Center
- Amazon Linux AMI

# AWS Windows AMIs for AWS Secret Region

Amazon Web Services provides a set of AMIs that contain software configurations specific to the Microsoft Windows platform. These Windows AMIs include launch configuration tools and many popular AWS libraries and tools.

**Topics**



## Tools and Certificates Included in Windows AMIs

When you use a Windows AMI, the following tools and certificates are already installed and configured:

- Windows PowerShell
- AWS Tools for Windows PowerShell (for Windows AMIs dated October 2015 or later)
- EC2Config service
- CA certificates

## How Windows AMIs Differ for AWS Secret Region

The implementation of the Windows AMIs for AWS Secret Region is different in the following ways:

- The nature of our isolated Regions can present challenges to importing specific root and enterprise CA certificates that are necessary for secure access to Amazon Web Services Regional services. For security purposes, these additional certificates are installed in the Windows AMIs provided by Amazon Web Services.
- For some scenarios, you may be required to configure custom endpoints or install service agents.

# How to Install Windows Components from Installation Media

Typically, you use installation media to add or configure optional Windows Server operating system components. Windows AMIs include many optional components, but if you need to install a component from installation media, you can use the following Amazon EBS snapshots:

| Installation Media | Snapshot ID |
|---|---|
| Installation media for Windows Sever 2008 SP2 32-bit | snap-070f460c161353b85 |
| Installation media for Windows Sever 2008 SP2 64-bit | snap-0848721b249de28e9 |
| Installation media for Windows Sever 2008 R2 SP1 | snap-03744ab1a34e6a8b7 |
| Installation media for Windows Sever 2012 | snap-09a1256025eedc922 |
| Installation media for Windows Sever 2012 R2 | snap-0092a3575193a38bd |
| Installation media for Windows Sever 2016 | snap-07cdae799da291bd9 |
| Installation media for Windows Sever 2019 | snap-0052b7d5c0bcc00f2 |

To use the console to add a Windows component snapshot to a new instance:

- When you launch a new instance, on the **Add Storage** page, add an **EBS** volume and select one of the previous installation media snapshots.

To use the command line to add a Windows component snapshot to an existing instance:

1. Create an Amazon EBS volume from one of the previous installation media snapshots by using New-EC2Volume or aws ec2 create-volume:

**Windows PowerShell**

```
New-EC2Volume –AvailabilityZone same_as_your_windows_instance –
SnapshotId desired_snapshot_id
```

**AWS CLI**

```
aws ec2 create-volume --availability-zone same_as_your_windows_instance --
snapshot desired_snapshot_id
```

2. Attach the volume to your Windows instance by using Add-EC2Volume or aws ec2 attach-volume where the device can be xvdf through xvdp:

**Windows PowerShell**

```
Add-EC2Volume –InstanceId instance_id –VolumeId volume_id --device xvdg
```

**AWS CLI**

```
aws ec2 attach-volume volume_id --instance instance_id --device xvdg
```

3. In a few minutes, the volume will appear in Windows Explorer and you can configure the Windows Components Wizard to point to the new volume.

# More Information

- Amazon EC2 User Guide
- AWS Tools for Windows PowerShell User Guide
- AWS Tools for PowerShell Cmdlet Reference

# AWS Deep Learning AMI for AWS Secret Region

> **Note**
>
> This AMI includes drivers, software, or toolkits developed, owned, or provided by NVIDIA Corporation. You agree to use these NVIDIA drivers, software, or toolkits only on Amazon EC2 instances that include NVIDIA hardware.

Amazon Web Services provides AWS Deep Learning AMI (DLAMI) as your one-stop shop for deep learning in the cloud. This customized machine instance is available for a variety of instance types, from a small CPU-only instance to the latest high-powered multi-GPU instances.

**Topics**



## How Deep Learning AMI Differs for AWS Secret Region

The version of the Deep Learning AMI for AWS Secret Region is different in the following ways:

- The following Deep Learning AMIs are available in AWS Secret Region:
  - Deep Learning AMI (Amazon Linux)
  - Deep Learning Base AMI (Amazon Linux)
- The following Deep Learning AMIs are not available in AWS Secret Region:
  - Deep Learning AMI (Ubuntu)
  - Deep Learning Base AMI (Ubuntu)
  - Deep Learning AMI with Source Code (CUDA 8, Ubuntu)
  - Deep Learning AMI with Source Code (CUDA 9, Ubuntu)
  - Deep Learning AMI (Windows Server 2016)
  - Deep Learning AMI (Windows Server 2012 R2)
  - Deep Learning AMI with Source Code (CUDA 8, Amazon Linux)
  - Deep Learning AMI with Source Code (CUDA 9, Amazon Linux)

- Not all GPU instance types are available in AWS Secret Region. For more information, including a list of all supported instance types, see Amazon EC2 Instances. Furthermore, note that the recommended instance types for DLAMI in AWS Secret Region are p3.2xlarge, p3.8xlarge, p3.16xlarge, g3.4xlarge, or g3.8xlarge.
- Some of the Deep Learning Framework Tutorials and test scripts will not work. The tutorials and examples come from open source framework repos and many of them rely on connectivity to the public internet for downloading public datasets. These will not work in AWS Secret Region. This includes the TensorBoard, TFServing, and MMS tutorials. However, these applications can be configured to work without the public internet.
- The Deep Learning AMIs are not recommended to be used with `t2.micro` instance types due to its low memory and compute specifications.

# More Information

- AWS Deep Learning AMI Developer Guide

# AWS CLI and Tools for AWS Secret Region

AWS provides several command line tools to help you build and manage your applications. This topic describes how the implementation of the AWS command line tools are different for AWS Secret Region.

The AWS SDKs and Tools Reference Guide contains information on the configuration, settings, authentication, and other foundational concepts common amongst AWS SDKs and Tools.

**Topics**



## AWS CLI

The AWS Command Line Interface (AWS CLI) is a cross-service command line tool to manage your AWS services. The AWS CLI is supported on Windows, Linux, OS X, or Unix.

> **Note**
>
> If you're using Amazon Linux 2 AMI or the Amazon Linux AMI, the AWS CLI is already installed and configured.

To use the AWS CLI for AWS Secret Region, you must:

- Replace your _endpoints.json file with the version that is specific to the us-isob-east-1 region. (Windows only)
- Set the default region to us-isob-east-1.
- If you are using a custom certificate bundle, you must set the `AWS_CA_BUNDLE` environment variable to the appropriate path.

On Windows, you can use the following Windows PowerShell commands to create a certificate bundle and set the `AWS_CA_BUNDLE` environment variable:

1. Concatenate the certificate files into a single certificate bundle. The certificate files must be ordered starting with the child certificate.

```
PS C:\> @( "cert2", "cert1", "root-cert" ) | %{get-content $_ } | add-content "C:
\Program Files\Amazon\AWSCLI\aws_dca_bundle.crt"
```

2. Set the AWS_CA_BUNDLE environment variable.

```
PS C:\> [Environment]::SetEnvironmentVariable("AWS_CA_BUNDLE", "C:\Program Files
\Amazon\AWSCLI\aws_dca_bundle.crt", "Machine")
```

3. Because you are setting an environment variable, close and reopen the command prompt.

For more information, see the Readme file included with the AWS CLI installer.

## AWS Tools for Windows PowerShell

The AWS Tools for Windows PowerShell enable you to manage your AWS resources with the same Microsoft Windows PowerShell tools you use to manage your Windows environment. The installer includes the AWS SDK for .NET, AWS Tools for Windows PowerShell, and the AWS Toolkit for Visual Studio.

> **Note**
>
> If you are using a Windows AMI dated October 2015 (2015.10.*) or later, the AWS Tools for Windows PowerShell are already installed and configured.

To use the Tools for Windows PowerShell for AWS Secret Region, you must:

- Use the custom endpoints file (AWSSDK.endpoints.xml), which is configured for the us-isob-east-1 region.
- Set tool credentials. You can add `Set-DefaultAWSRegion us-isob-east-1` to your profile or specify the `-Region us-isob-east-1` parameter for all cmdlets.

If you are signing requests and creating objects manually (instead of using the PowerShell cmdlets), you must set the AuthenticationRegion property in AWS Secret Region. The following

commands show an example of how you could return a list S3 buckets. (Alternatively, it would be easier to just use the Get-S3Bucket cmdlet.)

```
$AWSregion = "us-isob-east-1"
$AWSserviceURL="https://s3.$AWSRegion.sc2s.sgov.gov"
$config=New-Object Amazon.S3.AmazonS3Config
$config.ServiceURL = $AWSserviceURL
$config.SignatureVersion = 4
# Set the AuthenticationRegion property because the region cannot be determined from
 the service endpoint.
$config.AuthenticationRegion = $AWSregion
$s3Client = New-Object Amazon.S3.AmazonS3Client ($config)
$response = $s3Client.ListBuckets()
$response.Buckets | Write-Output
```

For more information, see the Readme file included with the Tools for Windows PowerShell installer.

# AWS SDKs for AWS Secret Region

AWS provides several Software Development Kits (SDKs) to help you build and manage your applications. This topic describes how the implementation of the AWS SDKs are different for AWS Secret Region.

The AWS SDKs and Tools Reference Guide contains information on the configuration, settings, authentication, and other foundational concepts common amongst AWS SDKs and Tools.

**Topics**



## AWS SDK for C++

To use the AWS SDK for C++ for C2S, you must:

- Include a configuration snippet in your applications to use the us-iso-east-1 Region.
- Configure service clients to set either `caFile` (if your application has a single certificate file) or `caPath` (if your application has a directory with multiple certificates) in your Client Configuration.

For more information, see the Readme file in the SDK for C++.

## AWS SDK for Go

To use the SDK for Go for AWS Secret Region, you must:

- Set the `AWS_CA_BUNDLE` environment variable to the path of a certificate bundle file the SDK will use for in-region requests. Alternatively, you can also enable a custom CA Bundle in code creating a session with the option `CustomCABundle`, setting this option field to a `io.Reader` of the custom CA bundle file.
- To install the SDK for Go, download the archive at SDK for Go and extract the zip into your `GOPATH`.

For more information, see the Developer Guide and the API Reference.

## AWS SDK for Java

To use the SDK for Java for AWS Secret Region, you must:

- Configure the Java runtime to trust the in-region root certificate.
- Add customized JAR files to your classpath.
- Configure any SDK for Java clients to use the us-isob-east-1 region.

For more information, see the Readme file in the SDK for Java.

## AWS SDK for JavaScript

To install the SDK for JavaScript for AWS Secret Region:

- Copy the 'browser/aws-sdk.min.js' file to a location accessible by your application and reference it with a script tag, for example:

```
<script src="path/to/aws-sdk.min.js" type="text/javascript"></script>
```

To configure the SDK for JavaScript for AWS Secret Region, you must:

- Include a configuration snippet in your applications to use the us-isob-east-1 region.

For more information, see the Readme file in the SDK for JavaScript.

# AWS SDK for JavaScript in Node.js

To install the SDK for JavaScript in Node.js for AWS Secret Region:

- Run the following command:

```
npm install node/aws-sdk.npm.tgz
```

To configure the SDK for JavaScript in Node.js for AWS Secret Region, you must:

- Include a configuration snippet in your applications to use the us-isob-east-1 region.
- If you are using the SDK in the Node.js environment, you must also register custom SSL certificate bundles for Node.js to use.

For more information, see the Readme file in the SDK for JavaScript in Node.js.

# AWS SDK for .NET

To use the AWS SDK for .NET for AWS Secret Region, you must:

- Use the custom endpoints file (AWSSDK.endpoints.xml), which is configured for the us-isob-east-1 region.
- Set tool credentials.
- Configure service clients to use the us-isob-east-1 region in app.config or when you instantiate the client.

The installer includes the AWS SDK for .NET, AWS Tools for Windows PowerShell, and the AWS Toolkit for Visual Studio.

For more information, see the Readme file in the AWS SDK for .NET.

# AWS SDK for PHP

To use the SDK for PHP for AWS Secret Region, you must:

- Use the configuration file for the us-isob-east-1 region. (config.us-isob-east-1.php)

- If you cannot use the certificate bundle provided by the operating system, set the `openssl.cafile` PHP ini configuration setting configuration file to the path of the to the certificate bundle.

> **Note**
>
> You must use version 3 of SDK for PHP.

For more information, see the Readme file in the SDK for PHP.

## AWS SDK for Python (Boto)

> **Note**
>
> If you're using Amazon Linux 2 AMI, see Install Python3 based Botocore on Amazon Linux 2. If you're using the Amazon Linux AMI, the AWS SDK for Python (Boto) is already installed and configured. (The Boto 3 version isn't included.)

To use the SDK for Python for AWS Secret Region, you must:

- Use the boto configuration file, which sets the signature version to v4.
- Specify the path to your certificate bundle by using the `ca_certificates_file` setting.
- Use the endpoints file (endpoints.json), which is configured for the us-isob-east-1 region.
- Create connections using the `connect_to_region` method of each service module, so that you can specify the us-isob-east-1 region.

For more information, see the Readme file in the SDK for Python.

## AWS SDK for Ruby

To use the SDK for Ruby Version 1 for AWS Secret Region, you must:

- Specify a valid SSL certificate bundle with `:ssl_ca_file` or `:ssl_ca_path`.

- Require the `aws-sdk-v1-compat` gem to make the `aws-sdk` gem compatible with the us-isob-east-1 region.

To use the SDK for Ruby Version 2 for AWS Secret Region, you must:

- Specify a valid SSL certificate bundle with `:ssl_ca_bundle` or `:ssl_ca_directory`.

To use the SDK for Ruby Version 3 for AWS Secret Region, you must:

- Specify a valid SSL certificate bundle with `:ssl_ca_bundle` or `:ssl_ca_directory`.

To install the SDK for Ruby, download the archive at AWS SDK for Ruby and install all four gems bundled together in the archive. You can't install the SDK for Ruby by performing a `gem install aws-sdk` as described in Getting Started with the AWS SDK for Ruby.

For more information, see the Readme file in the SDK for Ruby.

# AWS CDK for AWS Secret Region

The AWS Cloud Development Kit (AWS CDK) is a software development framework to define cloud infrastructure as code and provision it through AWS CloudFormation.

In one of five supported programming languages, you can use the AWS CDK to customize, share, and reuse constructs within your organization or community, just like any other software library. This enables you to build constructs that help you or others get started faster and incorporate best practices by default.

This topic contains information about using the AWS CDK v1 in AWS Secret Region. For more information about the AWS CDK, see:

- AWS CDK Developer Guide
- AWS Construct Library API Reference

**Topics**



## Configure AWS account and region

Unless you are using the Amazon EC2 Instance Metadata Service (IMDS), you must provide your credentials and an AWS Region to use the AWS CDK.

If you have the the section called “AWS CLI” installed and set up to work in AWS Secret Region, the easiest way to satisfy this requirement is to issue the following command:

```
aws configure
```

Provide your AWS access key ID, secret access key, and default region when prompted.

You may also manually create or edit the `~/.aws/config` and `~/.aws/credentials` (Mac OS X or Linux) or `%USERPROFILE%\.aws\config` and `%USERPROFILE%\.aws\credentials` (Windows) files to contain credentials and a default region, in the following format.

In `~/.aws/config` or `%USERPROFILE%\.aws\config`:

```
[default] region=us-iso-east-1
```

In `~/.aws/credentials` or `%USERPROFILE%\.aws\credentials`:

```
[default] aws_access_key_id=AKIAIOSFODNN7EXAMPLE
 aws_secret_access_key=je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
```

Finally, you can set the environment variables `AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY`, and `AWS_DEFAULT_REGION` to appropriate values.

## Install and configure Node.js

Node.js, version 14.15+, is a prerequisite for and must be installed in an environment to use AWS CDK.

There are no repositories in region from which to obtain Node.js. Customers must use their own method to bring Node.js into the in-region environment.

## Install the AWS CDK Toolkit (CLI)

> **Tip**
>
> Use this link to download the AWS CDK Toolkit (CLI)

You must install Node.js to use the AWS CDK Toolkit, even if you will not be developing CDK apps in TypeScript or JavaScript. After installing Node.js, follow these instructions to install the AWS CDK Toolkit globally.

1. Download and unzip `cdk-cli.zip` using the link above, taking note of the location of the unzipped `node_modules` folder.
2. Run **npm install -g *PATH_TO_UNZIPPED_NODE_MODULES*/aws-cdk**.
3. Run **cdk --version** to verify correct installation and version of the AWS CDK Toolkit.

TypeScript or JavaScript developers may prefer to install the AWS CDK Toolkit in their projects. To do this, follow these steps.

1. Download and unzip `cdk-cli.zip`, taking note of the location of the unzipped `node_modules` folder.
2. From your project directory, run **npm install *PATH_TO_UNZIPPED_NODE_MODULES*/aws-cdk**.
3. Run **npx cdk --version** to verify correct installation and version of the AWS CDK Toolkit. You can also check the `project.json` file for the dependency on the `aws-cdk` package.

To use the AWS CDK Toolkit without installing it, follow these steps.

1. Download and unzip `cdk-cli.zip`, taking note of the location of the unzipped `node_modules` folder.
2. Invoke the AWS CDK Toolkit with a command like ***PATH_TO_UNZIPPED_NODE_MODULES*/aws-cdk/bin/cdk**.

## Bootstrapping (CDK v2)

Bootstrapping for CDK v2 is more complicated because of the need for additional resources, including roles. You will need to export and edit the bootstrap template (an AWS CloudFormation YAML file) so it complies with your policies, after which you can deploy it.

To export the bootstrap template to an editable file, issue:

```
cdk bootstrap --show-template > bootstrap-template.yaml
```

Now edit the template in accordance with your policies.

> **Important**
>
> Remove the `ImageTagMutability` and `ImageScanningConfiguration` properties from the template, as they are presently unsupported.

To deploy the template after editing, issue:

```
cdk bootstrap --public-access-block-configuration false --template bootstrap-
template.yaml
```

If you removed roles from the bootstrap template and instead want to use AWS CLI credentials (the default in CDK v1), specify the `CliCredentialStackSynthesizer` class as your stacks' `synthesizer` property when instantiating them, as shown in the following Python example.

```
from aws_cdk import App, CliCredentialsStackSynthesizer, Stack
from aws_cdk.aws_s3 import Bucket
from constructs import Construct

app = App()

class DemoStack(Stack):
    def __init__(self, scope: Construct, construct_id: str, **kwargs) -> None:
        super().__init__(scope, construct_id, **kwargs)

        Bucket(self, "demo-s3-bucket")

app_stack = DemoStack(app, "demo", synthesizer=CliCredentialsStackSynthesizer())

app.synth()
```

You can also use a DefaultStackSynthesizer to further customize the synthesis properties of your stacks.

Bootstrapping only needs to be done once per AWS account.

# Install AWS CDK libraries

## TypeScript and JavaScript (Node.js)

> **Tip**
>
> Download AWS CDK (v1) libraries for Node.js

1. Download and unzip `cdk-libs-nodejs.zip` from the link above, taking note of the location of the unzipped `node_modules` folder.

2. Inside your project directory, run **npm install *PATH_TO_UNZIPPED_NODE_MODULES*/@aws-cdk/aws-*SERVICE***
3. Check your `project.json` file to make sure the library was added to your project's dependencies.

## Java

> **Tip**
>
> Download AWS CDK (v1) libraries for Java

1. Download and unzip `cdk-libs-java.zip` from the link above.
2. Add the JAR files from the `cdk-libs-java` folder for the AWS services you want to use to your Java project's classpath.

## Python

> **Tip**
>
> Download AWS CDK (v1) libraries for Python

1. Download and unzip `cdk-libs-python.zip` from the link above, taking note of the location of the unzipped `cdk-libs-python` folder.
2. Activate your project's virtual environment, then run **pip install *PATH_TO_UNZIPPED_CDK_LIBS_PYTHON*/aws_cdk.aws_*SERVICE*- *VERSION*-py3-none-any.whl** for each AWS service you want to use in your project.

Alternatively, add your project's requirements to `requirements.txt`, then install them all at once. Ensure you have the `wheel` packaging tool installed by issuing **pip install wheel**.

1. Download and unzip `cdk-libs-python.zip`, taking note of the location of the unzipped `cdk-libs-python` folder.

2. Add *PATH_TO_UNZIPPED_CDK_LIBS_PYTHON*/aws_cdk.aws_*SERVICE*- *VERSION*-py3-none-any.whl to `requirements.txt` for each AWS service you want to use in your project.
3. Create a local directory (in your project or elsewhere) to hold the wheels for these requirements.
4. In your project's directory, run `pip wheel --wheel-dir=`*LOCAL_WHEEL_DIRECTORY* `-r requirements.txt` to build wheels to the local wheel directory.
5. Activate your project's virtual environment, then run `pip install --no-index --find-links=`*LOCAL_WHEEL_DIRECTORY* `-r requirements.txt` to install those requirements using the local wheel directory.

## C# (.NET)

> **Tip**
>
> Download AWS CDK (v1) libraries for .NET

1. Download and unzip `cdk-libs-dotnet.zip` from the link above, taking note of the location of the unzipped `cdk-libs-dotnet` folder.
2. From your project's `src` directory, run **dotnet --restore** ***PATH_TO_UNZIPPED_CDK_LIBS_DOTNET*****\amazon.cdk.*****SERVICE*** for each library your project requires.

# Digital Certificates for AWS Secret Region

A digital certificate is a document used to identify an entity (person, computer system, or organization) and exchange information securely over a computer network using a public key infrastructure (PKI). AWS certificates are signed by a trusted entity called a certificate authority (CA) that provides a chain of trust. The identities of the communicating parties can be authenticated using public key cryptography.

In the default configuration of the AWS Software Development Kits (SDKs) and tools, client connections with AWS services will return a warning if authentication of the AWS endpoint certificate is not successful. AWS verifies the authenticity of client connections through the AWS signature version 4 signing process.

When initially installed and configured, the AWS SDKs and tools require the addition of region-specific CA public keys to the trust store that validates connections in the us-isob-east-1 region. Certificates used by the AWS services in the us-isob-east-1 region are issued by a CA specific to the region. This CA is not available in the default trust stores disseminated by the operating system, web browser, and programming language providers on the Internet. However, some of the AWS SDKs and tools are already configured with the new certificates on recent versions of the Amazon Linux AMI and AWS Windows AMIs included in the us-isob-east-1 region.

**Topics**

# Certificate Authority Rotation

The current certificate authority, CA3, which has signed the certificates used by AWS services in the us-isob-east-1 region, is being deprecated in favor of a new certificate authority, CA4. AWS will begin migration of API endpoints and websites to CA4 on April 1, 2016.

If your AWS SDKs and tools are configured to **only** use CA3 certificates, you will receive security-related errors when AWS services migrate to certificates signed by the new CA. To avoid service disruptions, you must add the CA4 public keys to your trust store when connecting to AWS endpoints in the us-isob-east-1 region.

# Testing Your Certificate Configuration

If you access AWS services programmatically, you can download scripts to test whether the programming language you are using is configured to use certificates issued from CA4. The scripts perform an HTTPS GET against a known site that uses the correct certificates. The test endpoint is identified in the script.

If the test succeeds, you will see a success message, a true message, or a list of results. If the test fails, you will see a failed message, an exception, or a stack trace.

## Downloading the Test Scripts

The test scripts for the supported programming languages are available in the following zip file.

Download the Test Scripts

## AWS CLI

To test your AWS CLI configuration, run the following command. You should see the current region name and endpoint returned.

```
$ aws ec2 describe-regions
```

## Java

To test your Java configuration, run the following:

```
$ javac ShaTest.java
```

```
$ java ShaTest
```

## JavaScript

To test your JavaScript configuration, run the following. This script assumes your certificate bundle is in /etc/pki/tls/cert.pem. If your system using a different location, you will need to update the path.

```
$ node shaTest.js
```

## PHP

To test your PHP configuration, run the following. To run this script, you must be running PHP 5.5 or later and aws.phar must be in the same directory as the script.

```
$ php shaTest.php
```

## Python

To test your Python configuration, run the following. To run this script, you must have the AWS SDK for Python (Boto) installed.

```
$ python shaTest.py
```

## Ruby

To test your Ruby configuration, run the following:

```
$ ruby shaTest.rb
```

## Windows PowerShell

To test your PowerShell configuration, run the following command. You should see a list of AMIs returned.

```
PS C:\> Get-EC2Image -Region us-isob-east-1
```

# Using Amazon Linux 2

By using the latest version of Amazon Linux 2, you can ensure that you have the latest `ca-certificates` for AWS Secret Region. Amazon Linux 2 adds these certificates to the root CA bundle, so any tools that already use this bundle should successfully find the correct `ca-certificates` to verify SSL connections, including the AWS CLI and any AWS SDKs, such as Boto3.

If you're having problems connecting to SSL endpoints using these certificates, see SSL Certificate Verification Fails in the Amazon Linux 2 troubleshooting section.

# Using the Amazon Linux AMI

If the certificate test scripts fail, the easiest way to start using the new certificates is to use the Amazon Linux AMI version 2015.09.1 or later. The CA3 certificate and the new CA4 certificate are already available, and some of the tools are already configured. The following tools are already configured in the Amazon Linux AMI to use the CA3 and CA4 certificates:

- AWS CLI
- Amazon EC2 CLI tools
- AWS SDK for Java
- AWS SDK for Python (Boto)

The CA3 and CA4 certificates are available in the aws-cli-ca-certs-us-isob-east-1 and ca-certificates-java-config-us-isob-east-1 packages. See /etc/pki /us-isob-east-1/certs/ for the .pem and .jks files. The AWS CLI, SDK for Java, and SDK for Python are already configured to use these files.

## Verifying Your Amazon Linux AMI Certificates

To verify you have the latest certificates, run the following command:

```
rpm -q aws-cli-ca-certs-us-isob-east-1 ca-certificates-java-config-us-isob-east-1
```

You should see the following or later version:

```
aws-cli-ca-certs-us-isob-east-1-1.1-1.noarch
```

```
ca-certificates-java-config-us-isob-east-1-1.1-1.noarch
```

If you do not have the latest certificates, you may see something like this instead:

```
aws-cli-ca-certs-us-isob-east-1-1.0-1.noarch
ca-certificates-java-config-us-isob-east-1-1.0-1.noarch
```

## Getting the Version of Your Amazon Linux AMI

To get the latest certificates, you must use the Amazon Linux AMI version 2015.09 or later. You can determine your Amazon Linux AMI version by running the following:

```
cat /etc/system-release-cpe
```

If you have version 2015.09, you will see the following:

```
cpe:/o:amazon:linux:2015.09:ga
```

## Updating Older Versions of Your Amazon Linux AMI with the Latest Certificates

If you are using a version of the Amazon Linux AMI earlier than 2015.09, you'll first need to update to 2015.09 to get the new certificates. You can do that by following the upgrade and troubleshooting instructions at Amazon Linux AMI for AWS Secret Region.

## Updating 2015.09.0 Versions of Your Amazon Linux AMI with the Latest Certificates

If you are using the Amazon Linux AMI version 2015.09**.0** and you do not yet have the new certificates, you can get the latest certificates by using the following `yum update` commands:

```
sudo yum clean all
sudo yum --disablerepo='*' --enablerepo='amzn-*' update aws-cli-ca-certs-us-isob-east-1
 ca-certificates-java-config-us-isob-east-1
```

To verify you have the latest certificates, run the previous `rpm -q` command.

For more information, see Amazon Linux AMI for AWS Secret Region.

# Using AWS Windows AMIs

If the certificate test scripts fail, the easiest way to start using the new certificates is to use a Windows AMI dated October 2015 or later. The CA3 certificate and the new CA4 certificate are already available, and some of the tools are already configured. The following tools are already configured in the Windows AMIs to use the CA3 and CA4 certificates:

- AWS SDK for .NET
- AWS Tools for Windows PowerShell

## Verifying Your Windows AMI Certificates

To verify you have the latest certificates, run the following Windows PowerShell command. You should see a list of AMIs returned.

```
PS C:\> Get-EC2Image -Region us-isob-east-1
```

## Getting the Version of Your Windows AMI

To determine the version of your Windows AMI, check the date in the AWS Management Console.

For more information, see AWS Windows AMIs for AWS Secret Region.

# Creating a Certificate Bundle

If the certificate test scripts fail and you are not able to use the Amazon Linux AMI or a Windows AMI, you will likely need to create a certificate bundle that includes both the CA3 and CA4 certificates.

> **Note**
>
> As described earlier, if you are using the Amazon Linux AMI, the CA3 and CA4 certificates are already available in the aws-cli-ca-certs-us-isob-east-1 and ca-certificates-java-config-us-isob-east-1 packages. See /etc/pki /us-isob-east-1/certs/ for the .pem and .jks files.

# Create a New Certificate Bundle

To create a new certificate bundle, you can use the follow steps.

Linux

1. Create a directory with a pem subdirectory, such as ca-certificates/pem.
2. Retrieve CA certificates in .pem format you want to include in the certificate bundle and copy them to the pem directory.

```
curl -s -O https://www ... /cert1.pem
curl -s -O https://www ... /cert2.pem
curl -s -O https://www ... /root-cert.pem
```

3. In the ca-certificates directory, concatenate certificates together into a bundle.

```
cat pem/* > ca-bundle.pem
```

4. Use openssl or curl to test your certificate bundle against an endpoint.

```
openssl s_client -connect www. ... :443 -CAfile ./ca-bundle.pem
```

   The last line of output should be:

   ```
   Verify return code: 0 (ok)
   ```

   If you see something like the following instead, the certificate bundle you created doesn't contain all of the required CA certificates to trust the test endpoint:

   ```
   Verify return code: 19 (self signed certificate in certificate chain)
   ```

   You can also verify by using curl with the `--cacert` argument.

Windows PowerShell

- ```
  PS C:\> @( "cert2.cer", "cert1.cer" "root-cert.cer") | %{get-content $_ } | add-
  content "C:\Program Files\Amazon\AWSCLI\aws_dca_bundle.crt"
  ```
  ```

## Add a New CA Certificate to a Bundle

If you already have a certificate bundle, you might be able to add a CA4 certificate to it.

Linux

1. Locate the certificate bundle you want to modify (for example, ca-bundle.pem).
2. Make a backup of the old bundle.

```
cp ca-bundle.pem ca-bundle.pem.bak
```

3. Append a new .pem file to the bundle.

```
cat new-ca-certificate >> ca-bundle.pem
```

## Use a Certificate Bundle from Linux on Windows

If necessary, you might be able to use a certificate bundle from Linux on Windows. Windows can read CA certificates encoded in .pem files.

Linux

1. Create a .cer file from the .pem file.

```
cp ca-bundle.pem ca-bundle.cer
```

2. Copy ca-bundle.cer to your Windows system.
3. To add ca-bundle.cer to the Windows trust store, right-click the file, and then select the option to install the certificate bundle.

# Creating a New Java Keystore on Linux

If you need to create a new Java keystore on Linux, follow the steps in this section.

1. Make sure the keytool is installed. If you are using the Amazon Linux AMI, it is sufficient to install Java.

```
sudo yum install java
```

2. Use keytool to create a .jks keystore. For example, you can use the following script to create a keystore with a password of `password` from all files in the pem directory using the .pem's file name as the alias.

```
for file in pem/*.pem; do
  alias=$(basename $file .pem)
  keytool -import -trustcacerts -noprompt -file $file -alias $alias -keystore ca-bundle.jks -storepass password
done
```

3. List the keystore entries to verify they were added.

```
keytool -list -keystore ca-bundle.jks -storepass password
```

# Manually Updating Your SDK and Tool Trust Stores

If the certificate test scripts fail and you are not able to use the Amazon Linux AMI or a Windows AMI, you will likely need to update your system by adding the new certificate authority public keys to the trust store.

## AWS CLI

To use the AWS CLI, you must specify the certificate bundle using an environment variable.

Linux

1. Copy the certificate bundle to /etc/pki/us-isob-east-1/certs/ or another location.
2. Specify the location in the AWS_CA_BUNDLE environment variable:

```
$ export AWS_CA_BUNDLE=/etc/pki/us-isob-east-1/certs/ca-bundle.pem
```

Windows

1. Copy the certificate bundle to C:\Program Files\Amazon\AWSCLI\ or another location.
2. Specify the location in the AWS_CA_BUNDLE environment variable. You can use the following PowerShell command to set the environment variable:

```
PS C:\> [Environment]::SetEnvironmentVariable("AWS_CA_BUNDLE", "C:\Program Files
\Amazon\AWSCLI\aws_dca_bundle.crt", "Machine")
```

## AWS SDK for Java

To use the new certificates for the AWS SDK for Java, you will need to update your Java runtime to trust the certificate bundle.

Linux

1. Make sure keytool is installed.
2. Run the following command to import the certificate bundle.

```
keytool -import -trustcacerts -file /etc/pki/us-isob-east-1/certs/ca-bundle.pem -
alias alias -keystore /etc/pki/us-isob-east-1/certs/ca-bundle.jks -storepass password
```

Windows

1. Open a command prompt as administrator.
2. Change to the Java bin directory.

```
cd "C:\Program Files (x86)\Java\jreversion\bin"
```

3. Run the following command to import the certificate bundle.

```
keytool -importcert -trustcacerts -file path\aws_dca_bundle.crt -alias alias -
keystore ..\lib\security\cacerts -storepass changeit
```

## AWS SDK for JavaScript in Node.js

To use the new certificates for the AWS SDK for JavaScript in Node.js, you must also register the certificate bundles for Node.js to use. You can do this by registering a custom agent with the following JavaScript code:

```
var fs = require('fs'), https = require('https');
```

The following code adds PKI certificate authorities required to access AWS endpoints that are not included in the system certificate bundle included with Node.js.

```
var certs = [
  fs.readFileSync('path/ca-bundle.pem')
];

AWS.config.update({
  httpOptions: {
    agent: new https.Agent({rejectUnauthorized: true, ca: certs});
  }
});
```

If necessary, you can also specify each certificate where each entry is a single certificate.

```
var certs = [
  fs.readFileSync('path/cert2.pem'),
  fs.readFileSync('path/cert1.pem'),
  fs.readFileSync('path/root-cert.pem')
];

AWS.config.update({
  httpOptions: {
    agent: new https.Agent({rejectUnauthorized: true, ca: certs});
  }
});
```

## AWS SDK for PHP

By default, the AWS SDK for PHP will use the certificate bundle that is configured when PHP is compiled. It is recommended that you use the operating system certificate bundle provided by your organization. If the certificate bundle is not correctly configured on your system, download the certificates and modify the `openssl.cafile` PHP ini configuration setting so that it is set to the path of the certificate bundle.

> **Note**
>
> You must use version 3 of the AWS SDK for PHP.

## AWS SDK for Python (Boto)

To use the AWS SDK for Python (Boto), you must specify the path to the certificate bundle in the boto config file. A boto config file is a text file formatted like an .ini configuration file. It specifies values for options that control the behavior of the boto library.

On startup for Linux, the boto library looks for configuration files in the following locations and in the following order:

- `/etc/boto.cfg` for site-wide settings that all users on this machine will use.
- `~/.aws/credentials` (if a profile is specified) for credentials shared between SDKs.
- `~/.boto` (if a profile is specified) for user-specific settings.
- `~/.aws/credentials` for credentials shared between SDKs.
- `~/.boto` for user-specific settings.

On Windows, create a text file that has any name (such as boto.config). It's recommended that you put this file in your user folder. Then set a user environment variable named `BOTO_CONFIG` to the full path of that file.

You can specify the path to your certificate bundle by using the `ca_certificates_file` setting. The following shows an example of the `[Boto]` section of a boto config file on Amazon Linux AMI:

```
$ cat ~/.boto
[Boto]
ca_certificates_file = /etc/pki/us-isob-east-1/certs/ca-bundle.pem
endpoints_path = /home/ec2-user/boto/endpoints.json
```

## AWS SDK for Ruby

The AWS SDK for Ruby requires you to provide a valid certificate bundle. By default, it will attempt to use the certificate bundle provided by the OpenSSL installation in Ruby. You will likely need to specify one of the following configuration variables:

- `:ssl_ca_bundle`, the string path to a valid certificate bundle file.
- `:ssl_ca_directory`, the string path to a directory with an expanded certificate bundle.

The public release of the aws-sdk-core gem is included in the SDK for Ruby archive. To make this gem compatible with the us-isob-east-1 region, you must require the aws-sdk-v2-compat gem.

```
require 'aws-sdk-v2-compat' # this auto includes 'aws-sdk-core'

# configure cert bundle
Aws.config[:ssl_ca_bundle] = 'path/ca-bundle.crt'
```

## AWS SDK for .NET and AWS Tools for Windows PowerShell

The AWS SDK for .NET and AWS Tools for Windows PowerShell use the operating system certificate bundle. Depending on your organization, these certificates might be managed with Active Directory and Group Policy. The certificates would need to be added to the trusted root certification authorities store.

# Customer Compliance Guide

The Customer Compliance Guide (CCG) helps customers better understand what it takes to securely configure a wide array of AWS Services. The document is organized into services, controls, and implementation guidance and offers customers the ability to filter to their specific system architecture. This provides customers greater awareness of what security configurations can be made to strengthen their compliance posture.

This CCG is an informative resource for customers leveraging the shared responsibility model in navigating their security compliance needs. The CCG is derived from AWS public documentation and is designed to provide a consolidated view of AWS security practices based on the configurable options for a service and the related compliance topics and control requirements. Customers may use this CCG to facilitate an understanding of AWS's current product offerings and practices as of the date of issue of this CCG.

The CCG is not designed to address all aspects of a given compliance framework or all possible configurable options for a service. Customers are responsible for determining compliance requirements and validating control implementation in accordance with their organization's policies, requirements and objectives. The security practices described in this CCG may not represent the best course of action for every organization. Additionally, these resources have been created for the unclassified services offered in commercial regions. There may be differences in high side functionality. If you find any information that is not applicable to your high side environment, please feel free to reach out and let us know!

Customer Compliance Guides - AWS Secret Region

# Endpoints in AWS Secret Region

If you access services in AWS Secret Region by using the command line interface (CLI) or programmatically by using the APIs, you need to know the endpoints. The following table details each AWS service available in AWS Secret Region and their corresponding endpoints.

FIPs endpoints are subject to availability, please refer to the services difference documentation.

| AWS Service | US ISOB East (Ohio) Endpoint | Protocol |
|---|---|---|
| API Gateway | apigateway.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| API Gateway Dataplane | execute-api.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| AWS AppConfig | appconfig.us-isob-east-1.sc2s.sgov.gov<br><br>appconfig-fips.us-isob-east-1.sc2s.sgov.gov | HTTPS<br><br>HTTPS |
| AWS Config | config.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| AWS Config Rules | config.us-isob-east-1.sc2s.sgov.gov | |
| AWS Console Home | us-isob-east-1.console.sc2shome.sgov.gov/console/home?region=us-isob-east-1 | HTTPS |
| AWS Diode Messaging | diode-messaging.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| AWS Diode Messaging Proxy | diode-messaging-proxy.us-isob-east-1.sc2s.sgov.gov | HTTPS |

| AWS Service | US ISOB East (Ohio) Endpoint | Protocol |
|---|---|---|
| AWS Diode Service | diode.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| AWS Documentation | docs.sc2shome.sgov.gov | HTTPS |
| AWS Elemental MediaLive | medialive.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| AWS Elemental MediaPackage | mediapackage.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| AWS Glue Frontend Service | glue.us-isob-east-1.sc2s.sgov.gov | |
| AWS Health APIs And Notifications | health.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| AWS Health Dashboard | phd.sc2shome.sgov.gov | HTTP and HTTPS |
| AWS License Manager | license-manager.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| AWS Management Console | us-isob-east-1.console.sc2shome.sgov.gov | HTTPS |
| AWS Marketplace Metering Service | metering.marketplace.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| AWS Outposts | outposts.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| AWS Price List Service | api.pricing.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| AWS Resource Groups Tagging API | tagging.us-isob-east-1.sc2s.sgov.gov | HTTPS |

| AWS Service | US ISOB East (Ohio) Endpoint | Protocol |
| --- | --- | --- |
| AWS S3 Control | s3-control.us-isob-east-1.sc2s.sgov.gov<br>s3-control.dualstack.us-isob-east-1.sc2s.sgov.gov<br>s3-control-fips.dualstack.us-isob-east-1.sc2s.sgov.gov<br>s3-control-fips.us-isob-east-1.sc2s.sgov.gov | HTTPS<br>HTTPS<br>HTTPS<br>HTTPS |
| AWS S3 Outposts | s3-outposts.us-isob-east-1.sc2s.sgov.gov<br>s3-outposts-fips.us-isob-east-1.sc2s.sgov.gov | HTTPS<br>HTTPS |
| AWS SCM UI Argo Portal | awsscmuiportal.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| AWS Secrets Manager | secretsmanager.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| AWS Snowball Edge | snowball.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| AWS Step Functions | states.us-isob-east-1.sc2s.sgov.gov<br>sync-states.us-isob-east-1.sc2s.sgov.gov | HTTPS<br>HTTPS |
| AWS Support Center Console | console.sc2shome.sgov.gov/support | HTTPS |

| AWS Service | US ISOB East (Ohio) Endpoint | Protocol |
| --- | --- | --- |
| AWS Systems Manager (SSM) | ssm.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| AWS Systems Manager Session Manager | ssmmessages.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| AWSExternalTaxonomyATATService | aws.atat.service.us-isob-east-1.sc2s.sgov.gov | |
| AWSGarnetBIService | garnetbi.us-isob-east-1.sc2s.sgov.gov | |
| AWSSignUpPortal | aws-signup-portal.us-isob-east-1.sc2s.sgov.gov | HTTP and HTTPS |
| Amazon Budgets | budgets.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Amazon Data Lifecycle Manager | dlm.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Amazon EKS | eks.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Amazon Elastic Container Registry | ecr.us-isob-east-1.sc2s.sgov.gov<br>api.ecr.us-isob-east-1.sc2s.sgov.gov | HTTPS<br>HTTPS |
| Amazon Elastic Container Service | ecs.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Amazon Linux Security Center | alas.s3.us-isob-east-1.sc2s.sgov.gov | HTTPS |

| AWS Service | US ISOB East (Ohio) Endpoint | Protocol |
| --- | --- | --- |
| Amazon OpenSearch Service | es.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Amazon RDS for MariaDB | rds.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Amazon RDS for MySQL | rds.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Amazon RDS for Oracle | rds.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Amazon RDS for PostgreSQL | rds.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Amazon RDS for SQL Server | rds.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Amazon Recycle Bin | rbin.us-isob-east-1.sc2s.sgov.gov<br>rbin-fips.us-isob-east-1.sc2s.sgov.gov | HTTPS<br>HTTPS |
| Amazon SageMaker | api.sagemaker.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Amazon SageMaker Runtime (Realtime Endpoint Inference) | runtime.sagemaker.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| AppConfigData | appconfigdata.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Application Auto Scaling | application-autoscaling.us-isob-east-1.sc2s.sgov.gov | HTTP and HTTPS |

| AWS Service | US ISOB East (Ohio) Endpoint | Protocol |
|---|---|---|
| Aurora Control Plane | aurora-cp.us-isob-east-1.sc2s.sgov.gov | |
| Aurora MySQL | rds.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Aurora PostgreSQL | rds.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Cloud Control API | cloudcontrolapi.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| CloudFormation | cloudformation.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| CloudTrail | cloudtrail.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| CloudWatch | monitoring.us-isob-east-1.sc2s.sgov.gov | HTTP and HTTPS |
| CloudWatch Events | events.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| CloudWatch Logs | logs.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| CloudWatch Synthetics | synthetics.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| CodeDeploy | codedeploy.us-isob-east-1.sc2s.sgov.gov | HTTPS |

| AWS Service | US ISOB East (Ohio) Endpoint | Protocol |
|---|---|---|
| DS Console | us-isob-east-1.console.sc2shome.sgov.gov/directoryservicev2/home?region=us-isob-east-1 | HTTPS |
| Database Migration Service | dms.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Diode Console | diodeconsole.us-isob-east-1.sc2s.sgov.gov | |
| Direct Connect | directconnect.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Directory Service | ds.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Directory Service - AD Connector | ds.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Directory Service - Managed AD | ds.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| DynamoDB | dynamodb.us-isob-east-1.sc2s.sgov.gov | HTTP and HTTPS |
| DynamoDB Streams | streams.dynamodb.us-isob-east-1.sc2s.sgov.gov | HTTP and HTTPS |
| EBS Console | us-isob-east-1.console.sc2shome.sgov.gov/ec2/home?region=us-isob-east-1 | HTTPS |
| EBS Direct APIs | ebs.us-isob-east-1.sc2s.sgov.gov | HTTPS |

| AWS Service | US ISOB East (Ohio) Endpoint | Protocol |
|---|---|---|
| EC2 Auto Scaling | autoscaling.us-isob-east-1.sc2s.sgov.gov | HTTP and HTTPS |
| EC2 Dedicated Host Reservations | ec2hostel.us-isob-east-1.sc2s.sgov.gov | |
| EC2 Image Builder | imagebuilder.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| EC2 Launch v2 | ec2launchv2.us-isob-east-1.sc2s.sgov.gov | |
| EC2 Managed Prefix List Service | ec2.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| EC2 Message Delivery Service | ec2messages.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| EC2CustomerMaintenanceEventService | ec2cms.us-isob-east-1.sc2s.sgov.gov | HTTP and HTTPS |
| EC2VPCEndpointService | ec2-vpce-service.us-isob-east-1.sc2s.sgov.gov | |
| EKS Console | us-isob-east-1.console.sc2shome.sgov.gov/eks/home?region=us-isob-east-1 | |
| ElastiCache | elasticache.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Elastic Block Store (EBS) | ec2.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Elastic Compute Cloud (EC2) | ec2.us-isob-east-1.sc2s.sgov.gov | HTTP and HTTPS |

| AWS Service | US ISOB East (Ohio) Endpoint | Protocol |
| --- | --- | --- |
| Elastic File System (EFS) | elasticfilesystem.us-isob-east-1.sc2s.sgov.gov<br>elasticfilesystem-fips.us-isob-east-1.sc2s.sgov.gov | HTTPS<br>HTTPS |
| Elastic Load Balancing (ELB) | elasticloadbalancing.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Elastic Load Balancing - Gateway Load Balancer | elb-agw.us-isob-east-1.sc2s.sgov.gov | HTTP and HTTPS |
| Elastic MapReduce (EMR) | elasticmapreduce.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| EventBridge | events.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Glacier | glacier.us-isob-east-1.sc2s.sgov.gov | HTTP and HTTPS |
| IAM Console | console.sc2shome.sgov.gov/iam/home?region=us-isob-east-1 | |
| Identity & Access Management (IAM) | iam.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Import/Export Snowball | snowball.us-isob-east-1.sc2s.sgov.gov | |
| Key Management Service (KMS) | kms.us-isob-east-1.sc2s.sgov.gov<br>kms-fips.us-isob-east-1.sc2s.sgov.gov | HTTPS<br>HTTPS |

| AWS Service | US ISOB East (Ohio) Endpoint | Protocol |
| --- | --- | --- |
| Kinesis Data Firehose Console | kinesisfirehose-console.us-isob-east-1.sc2s.sgov.gov | |
| Kinesis Firehose | firehose.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Kinesis Streams | kinesis.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Kinesis Streams Console | us-isob-east-1.console.sc2shome.sgov.gov/kinesis/home?region=us-isob-east-1 | HTTPS |
| Lambda | lambda.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Marketplace | marketplace.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Recycle Bin Console | us-isob-east-1.console.sc2shome.sgov.gov/rbin/home?region=us-isob-east-1 | HTTPS |
| Redshift | redshift.us-isob-east-1.sc2s.sgov.gov<br><br>redshift-fips.us-isob-east-1.sc2s.sgov.gov | HTTPS<br><br>HTTPS |
| Relational Database Service (RDS) Core Control Plane | rds.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Resource Access Manager (RAM) | ram.us-isob-east-1.sc2s.sgov.gov | HTTPS |

| AWS Service | US ISOB East (Ohio) Endpoint | Protocol |
| --- | --- | --- |
| Resource Groups | resource-groups.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Route 53 Private DNS for VPCs | route53.sc2s.sgov.gov | HTTPS |
| Route 53 Public Control Plane | route53.sc2s.sgov.gov | HTTPS |
| Route 53 Public DNS | route53.sc2s.sgov.gov | HTTPS |
| Route 53 Resolver Endpoints | route53resolver.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Route53 Application Recovery Controller - Zonal Shift | arc-zonal-shift.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| S3 Access Points | s3-accesspoint.us-isob-east-1.sc2s.sgov.gov<br>s3-accesspoint-fips.dualstack.us-isob-east-1.sc2s.sgov.gov<br>s3-accesspoint-fips.us-isob-east-1.sc2s.sgov.gov<br>s3-accesspoint.dualstack.us-isob-east-1.sc2s.sgov.gov | HTTPS<br>HTTPS<br>HTTPS<br>HTTPS |
| SageMaker Console | console.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| SageMakerMetricsService | metrics.sagemaker.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Security Token Service (STS) | sts.us-isob-east-1.sc2s.sgov.gov | HTTPS |

| AWS Service | US ISOB East (Ohio) Endpoint | Protocol |
|---|---|---|
| Services Health Dashboard | status.sc2shome.sgov.gov | HTTPS |
| Sign-In Portal | signin.sc2shome.sgov.gov | HTTPS |
| Simple Notification Service (SNS) | sns.us-isob-east-1.sc2s.sgov.gov | HTTP and HTTPS |
| Simple Queue Service (SQS) | sqs.us-isob-east-1.sc2s.sgov.gov | HTTP and HTTPS |
| Simple Storage Service (S3) | s3.us-isob-east-1.sc2s.sgov.gov | HTTP and HTTPS |
| Simple Workflow Service (SWF) | swf.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Site-to-Site VPN | ec2.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Storage Gateway | storagegateway.us-isob-east-1.sc2s.sgov.gov<br>storagegateway-fips.us-isob-east-1.sc2s.sgov.gov | HTTPS<br>HTTPS |
| Support | support.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Transit Gateway | ec2.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| Unified Console | unified-console.us-isob-east-1.sc2s.sgov.gov | |
| Unified Settings Console | upc.us-isob-east-1.sc2s.sgov.gov | HTTPS |

| AWS Service | US ISOB East (Ohio) Endpoint | Protocol |
| --- | --- | --- |
| VPC Console | us-isob-east-1.console.sc2shome.sgov.gov/vpc/home?region=us-isob-east-1 | HTTPS |
| VPC Flow Logs | ec2.us-isob-east-1.sc2s.sgov.gov | HTTPS |
| WorkSpaces | workspaces.us-isob-east-1.sc2s.sgov.gov | HTTPS |

# Amazon Resource Names in AWS Secret Region

Amazon Resource Names (ARNs) uniquely identify AWS resources. You use an ARN when you need to unambiguously specify a resource, such as in IAM policies, Amazon S3 bucket names, and API calls. In AWS Secret Region, ARNs have a different identifier than in other AWS regions. For other regions, ARNs begin with:

```
arn:aws:
```

In AWS Secret Region, ARNs begin with:

```
arn:aws-iso-b:
```

If an ARN that you are using requires you to specify a region, use `us-isob-east-1`.

For more information about ARNs and namespaces, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the *AWS General Reference*.

# Services in AWS Secret Region

Services in AWS Secret Region are distinct from the public AWS services. Some features and new functionality available in the public AWS services might not be available in the current release of AWS Secret Region.

This section describes the services available in AWS Secret Region. Each topic describes any significant differences between the AWS Secret Region implementation and the public implementation of the service. The following AWS Secret Region implementation details apply to all the AWS services that you might work with:

- You must sign up for an account that is specific to AWS Secret Region. For more information, see Getting Started with AWS Secret Region .
- The one-year AWS Free Tier is not available.

**Topics**

- Amazon DynamoDB
- Amazon Elastic Block Store
- EBS direct APIs
- Amazon Elastic Compute Cloud
- Amazon EC2 Auto Scaling
- Amazon EC2 Image Builder
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- Amazon EFS
- Amazon EKS
- Elastic Load Balancing
- Amazon EMR
- Amazon ElastiCache
- Amazon EventBridge
- Amazon Data Firehose
- Amazon S3 Glacier
- AWS Health
- AWS Identity and Access Management
- AWS Key Management Service
- Amazon Kinesis Data Streams
- AWS Lambda
- AWS License Manager
- AWS Marketplace
- AWS Elemental MediaPackage
- AWS Elemental MediaLive
- Amazon OpenSearch Service
- AWS Outposts
- AWS ParallelCluster
- AWS Pricing Calculator

- Amazon Redshift
- Amazon Relational Database Service
- AWS Resource Access Manager
- AWS Resource Groups
- AWS Resource Groups Tagging API
- Amazon Route 53
- Amazon SageMaker
- AWS Serverless Application Model
- AWS Secrets Manager
- AWS Security Hub
- Amazon Simple Storage Service
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Simple Workflow Service
- AWS Snowball Edge
- AWS Step Functions
- AWS Storage Gateway
- AWS Support
- AWS Systems Manager
- AWS Transit Gateway
- AWS Trusted Advisor
- Amazon Virtual Private Cloud
- AWS Virtual Private Network
- Amazon WorkSpaces

# AWS Account Management

An AWS account is the basic container for all the AWS resources you create as an AWS customer. For example, an Amazon Simple Storage Service (Amazon S3) bucket, an Amazon Relational Database Service (Amazon RDS) database, and an Amazon Elastic Compute Cloud (Amazon EC2) instance are all resources. Every resource is uniquely identified by an Amazon Resource Name (ARN)

that includes the account ID of the account that contains, or owns, the resource. An AWS account is also the basic security boundary for your AWS resources. Resources that you create in your account are available to users who have credentials for your account.

**Topics**



## How Account Management Differs for AWS Secret Region

The implementation of Account Management is different for AWS Secret Region in the following ways:

- The process to sign up for a new AWS account is different than in commercial regions. For more information, see Signing Up.
- AWS Organizations is currently not available in AWS Secret Region.
- There is no concept of a "root" or "account" user or credentials. All AWS Secret Region users are IAM users, including the user who created the account.
- Accounts and credentials for the India regions will not work in the AWS Secret Region.
- AWS Account Management APIs are not available.
- AWS Secret Region does not support adding opt in regions.
- AWS Secret Region does not support adding multi-factor authentication (MFA) to IAM users or to the account. This includes both hardware and virtual MFA devices. The console does not include MFA options.
- Amazon Resource Names (ARNs) and endpoints have different values.

## Documentation for Account Management

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Account Management differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Account Management Reference Guide

- Managing your AWS account

# AWS AppConfig

Use AWS AppConfig, a capability of AWS Systems Manager, to create, manage, and quickly deploy application configurations. You can use AWS AppConfig with applications hosted on Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS Lambda, containers, mobile applications, or IoT devices.

**Topics**

- How AWS AppConfig Differs for AWS Secret Region
- How Command Line and API Access Differs for AWS Secret Region
- Documentation for AWS AppConfig

## How AWS AppConfig Differs for AWS Secret Region

The implementation of AWS AppConfig is different for AWS Secret Region in the following ways:

- AWS Codepipeline resources are currently not available in AWS Secret Region.
- AWS AppConfig Lambda extensions are not supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with AWS AppConfig and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to AWS AppConfig by using the command line or APIs, use the following endpoint:

- https://monitoring.us-isob-east-1.sc2s.sgov.gov

# Documentation for AWS AppConfig

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how AWS AppConfig differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS AppConfig User Guide
- AWS AppConfig API Reference
- AWS AppConfig section of AWS CLI Reference
- AWS AppConfig section of the AWS CLI Command Reference

# Application Auto Scaling

Application Auto Scaling is a web service for developers and system administrators who need a solution for automatically scaling their scalable resources for individual AWS services beyond Amazon EC2. For information about scaling Amazon EC2 instances in AWS Secret Region, see the section called "Amazon EC2 Auto Scaling" in this guide.

> **Note**
>
> You can access the Application Auto Scaling service by calling AWS CLI commands and AWS SDK API operations. There is no graphical user interface available.

**Topics**



## How Application Auto Scaling Differs for AWS Secret Region

The implementation of Application Auto Scaling is different for AWS Secret Region in the following ways:

- Only the following resources are supported for Application Auto Scaling in AWS Secret Region:
  - Amazon DynamoDB tables and global secondary indexes
  - Amazon EMR clusters
  - SageMaker endpoint variants
- Application Auto Scaling notifications are not currently supported in the AWS Personal Health Dashboard.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Application Auto Scaling and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Application Auto Scaling by using the command line or APIs, use the following endpoint:

- https://autoscaling.us-isob-east-1.sc2s.sgov.gov
- https://application-autoscaling.us-isob-east-1.sc2s.sgov.gov

## Documentation for Application Auto Scaling

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Application Auto Scaling differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Application Auto Scaling User Guide
- application-autoscaling section of AWS CLI Reference
- Application Auto Scaling API Reference

# Amazon API Gateway

Amazon API Gateway (API Gateway) is an AWS service that enables developers to create, publish, maintain, monitor, and secure APIs at any scale. You can create APIs that access AWS or other web services, as well as data stored in the AWS Cloud.

**Topics**



## How API Gateway Differs for AWS Secret Region

The implementation of API Gateway is different for AWS Secret Region in the following ways:

- AWS Certificate Manager (ACM) is not available. When creating a custom domain name for an API, you must upload the required certificate to API Gateway instead of ACM. For more information, see Set Up a Regional Custom Domain Name Certificate Without ACM Using AWS CLI.
- AWS WAF is not available for API Gateway APIs.
- X-Ray tracing is not available.
- Amazon Cognito authorizers are not available.
- Java and Ruby SDK generation is not available.
- Edge-optimized APIs and Integration with AWS Config are not available.
- API Gateway cannot communicate with endpoints outside of the region.
- API Gateway resources cannot be tagged using AWS CloudFormation.
- Stage variables are not encrypted.
- WebSocket APIs are not available.
- Mutual TLS authentication is not available.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.
- HTTP APIs are not available.

- To create a Regional REST API using AWS CloudFormation, set either `Properties.EndpointConfiguration.Types` to `["REGIONAL"]` or `Properties.Parameters.endpointConfigurationTypes` to `"REGIONAL"`.
- The following region-specific API Gateway account ID is automatically added to your Amazon VPC endpoint service as AllowedPrincipals for private integrations in AWS Secret Region:

| Region | Account ID |
| --- | --- |
| • us-isob-east-1 | • 856506949525 |

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with API Gateway and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to API Gateway by using the command line or APIs, use the following endpoint:

- https://apigateway.us-isob-east-1.sc2s.sgov.gov

To connect to API Gateway APIs, use the following endpoint:

- https://*api-id*.execute-api.us-isob-east-1

## Documentation for API Gateway

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how API Gateway differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not

be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- API Gateway Developer Guide
- API Gateway section of AWS CLI Reference
- API Gateway API Reference

# Amazon Aurora

Amazon Aurora (Aurora) is a fully managed relational database engine that's compatible with MySQL and PostgreSQL. With some workloads, Aurora can deliver up to five times the throughput of MySQL and up to three times the throughput of PostgreSQL without requiring changes to most of your existing applications. Aurora includes a high-performance storage subsystem. Its MySQL- and PostgreSQL-compatible database engines are customized to take advantage of that fast distributed storage. The underlying storage grows automatically as needed, up to 128 tebibytes (TiB). Aurora also automates and standardizes database clustering and replication, which are typically among the most challenging aspects of database configuration and administration.

**Topics**



## How Aurora Differs for AWS Secret Region

The implementation of Aurora is different for AWS Secret Region in the following ways:

The following features are currently not implemented, supported, or fully tested for the corresponding Aurora database engine.

**Features Not Available for Aurora MySQL**

- Blue/Green Deployments.
- Secrets Manager integration.
- RDS Proxy.
- Performance Insights.
- Enhanced monitoring.
- Aurora Serverless clusters.
- Multi-master clusters.
- Backtrack.
- Database Activity Streams.

- Recommendations.
- Parallel query clusters.
- Features that involve using multiple AWS Regions, including cross-Region snapshot copying, cross-Region replication, and Aurora Global Database.
- Calling Lambda functions.
- Aurora machine learning integration.
- Only db.t3 (burstable) and db.r5 instance classes are available.
- Amazon DevOps Guru for RDS.
- Amazon RDS Extended Support

**Features Not Available for Aurora PostgreSQL**

- Blue/Green Deployments.
- Secrets Manager integration.
- RDS Proxy.
- Performance Insights.
- Enhanced monitoring.
- Aurora Serverless clusters.
- Backtrack.
- Database Activity Streams.
- Recommendations.
- Features that involve using multiple AWS Regions, including cross-Region snapshot copying, cross-Region replication, and Aurora Global Database.
- Cross-account cluster cloning.
- Cluster cache management.
- Only db.t3 (burstable) and db.r5 instance classes are available.
- Babelfish.
- Amazon DevOps Guru for RDS.
- Saving or exporting data from Aurora to an Amazon S3 bucket.
- Aurora machine learning integration.

- Amazon RDS Extended Support

### General Differences

- Engine version support is different from the commercial Regions. To list the supported engine versions for a specific DB engine, run the following CLI command:

  ```
  aws rds describe-db-engine-versions --engine engine --query "*[].
  {Engine:Engine,EngineVersion:EngineVersion}" --output text
  ```

  For example, to list the supported engine versions for Aurora PostgreSQL, run the following CLI command:

  ```
  aws rds describe-db-engine-versions --engine aurora-postgresql --query "*[].
  {Engine:Engine,EngineVersion:EngineVersion}" --output text
  ```

- To connect to a Aurora MySQL or Aurora PostgreSQL DB instance with SSL, you must download the public key from https://s3.us-isob-east-1.sc2s.sgov.gov/rds-downloads/rds-combined-ca-bundle.pem. For more information, see Using SSL/TLS to Encrypt a Connection to a DB Cluster.
- Since AWS Secret Region uses a unique certificate authority (CA), Aurora is not subject to the SSL certificate rotation guidance described in SSL Certificate Rotation. Aurora DB instances for AWS Secret Region are already using the region-specific certificate identified by `rds-ca-2015` in DescribeCertificates API calls.
- Since AWS Secret Region operates as a single air-gapped region, cross-region features are not supported, such as DB snapshot copying across regions, read replication across multiple regions, and Aurora Global Database.
- Only selected DB instance types are available for use with Aurora. You can use any of the db.r5 instance types that Aurora usually supports. You can't use the db.r4, db.r3, db.t3, or db.t2 instance types.
- Enhanced Monitoring for Aurora is not supported.
- AWS Secret Region uses the following time block from which the default backup windows are assigned.

| Region | Time Block |
| --- | --- |
| us-isob-east-1 | 03:00-11:00 UTC |

- The AWS service principal for Aurora is `rds.sc2s.sgov.gov`.
- Amazon EC2 launches instances into a VPC instead of using the EC2-Classic platform. For more information, see Amazon EC2 and Amazon Virtual Private Cloud (VPC).
- Since AWS Secret Region is a VPC-only region, Aurora DB instances must use existing VPC security groups. Aurora APIs, such as CreateDBSecurityGroup and AWS::RDS::DBSecurityGroup do not apply in AWS Secret Region. Instead, create VPC security groups directly in Amazon EC2 using CreateSecurityGroup.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Aurora and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Aurora by using the command line or APIs, use the following endpoint:

- https://rds.us-isob-east-1.sc2s.sgov.gov

## Documentation for Aurora

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Aurora differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Aurora
  - Aurora MySQL

- Aurora PostgreSQL
- Amazon RDS section of AWS CLI Reference
- Amazon RDS API Reference

# AWS Billing and Cost Management

AWS Billing and Cost Management is where you set up the basic information about how you pay and receive your AWS bill. Billing and Cost Management also provides tools you can use to track and monitor your AWS costs and ensure that you are using AWS efficiently. For an introduction on how to track your spending, see Tracking AWS Spending.

**Topics**



## How Billing and Cost Management Differs for AWS Secret Region

The implementation of Billing and Cost Management is different for AWS Secret Region in the following ways:

- When you create your account, you specify your agency's standard invoicing system to pay for services.
- Each month, AWS sends an invoice in accordance with your agency's invoicing instructions. These instructions are delineated in a task order that is issued by the authorized contract representative. For more information, see Get Your Monthly Bill and View Your AWS Charges.
- If you want to deposit reports into an Amazon S3 bucket, in your policy, you must specify `812475063476` and `575243304591` (instead of `386209384616`) for the account ID. For more information, see Deposit Reports into an Amazon S3 Bucket.
- RI discounts sharing is enabled for all accounts in AWS Secret Region and cannot be disabled.
- The billing alerts feature is not available.
- The AWS Cost Explorer API is not available.
- When opting in to Cost Explorer, only the current month's data is available.
- Access to AWS Cost Explorer in the console is provided by the `aws-portal:ViewBilling` permission. Granular permissions provided by `ce:*` actions are not supported in AWS Secret Region.
- The AWS Price List API needs to be SigV4 signed. For details, see Signing AWS API requests. This isn't required for commercial Regions.

- Savings Plans are not supported in AWS Secret Region.

## AWS Budgets

AWS Budgets enable you to plan your service usage, service costs, and your RI utilization. You can also track how close your plan is to your budgeted amount or to the free tier limits. Budgets provide you with a quick way to see your usage-to-date and current estimated charges from AWS and to see how much your predicted usage accrues in charges by the end of the month.

### How AWS Budgets Differs for AWS Secret Region

The implementation of AWS Budgets is different for AWS Secret Region in the following ways:

- Reserved Instance (RI) Utilization reports are not available.

## Documentation for Billing and Cost Management

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Billing and Cost Management differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Billing User Guide
- Managing Your Costs with AWS Budgets

# AWS Cloud Control API

Use AWS Cloud Control API to create, read, update, delete, and list (CRUD-L) your cloud resources that belong to a wide range of AWS services. With the Cloud Control API standardized set of application programming interfaces (APIs), you can perform CRUD-L operations on any supported resources in your AWS account. Using Cloud Control API, you won't have to generate code or scripts specific to each individual service responsible for those resources.

**Topics**



## How Cloud Control API Differs for AWS Secret Region

The implementation of Cloud Control API is different for AWS Secret Region in the following ways:

- Cloud Control API supports any AWS resources published on the CloudFormation registry that are either fully mutable or immutable. For more information on listing supported resource types, see Determining if a resource type supports Cloud Control API.
- Cloud Control API operations in the AWS Secret Region have all capabilities that are available in the commercial AWS Regions.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Cloud Control API and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

Cloud Control API has a service-specific command line interface. For more information about the , see AWS CLI.

To connect to Cloud Control API by using the command line or APIs, use the following endpoint:

- https://ccapi.us-isob-east-1.sc2s.sgov.gov

## Documentation for Cloud Control API

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Cloud Control API differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Cloud Control API User Guide
- AWS Cloud Control API API Reference
- Cloud Control API section of AWS CLI Reference

# AWS CloudFormation

AWS CloudFormation enables you to create and provision infrastructure deployments predictably and repeatedly. It helps you leverage AWS products such as Amazon EC2, Amazon EBS, Amazon SNS, Elastic Load Balancing, and Auto Scaling to build highly reliable, highly scalable, cost-effective applications without worrying about creating and configuring the underlying infrastructure. With AWS CloudFormation, you use a template file to create and delete a collection of resources together as a single unit (a stack).

**Topics**



## How AWS CloudFormation Differs for AWS Secret Region

The implementation of AWS CloudFormation is different for AWS Secret Region in the following ways:

- AWS CloudFormation in AWS Secret Region does not support AWS CloudFormation IaC generator (infrastructure as code generator).
- AWS Secret Region supports a subset of AWS services. You might need to modify AWS CloudFormation sample templates and template snippets.
- AWS CloudFormation in AWS Secret Region does not support AWS Config.
- AWS CloudFormation in AWS Secret Region does not support managing AWS CloudFormation events using Amazon EventBridge.
- AWS CloudFormation StackSets are not available in AWS Secret Region.
- Macros are not available in AWS Secret Region.
- AWS CloudFormation does not support the limit for resources in concurrent stack operations.
- AWS CloudFormation does not support the limit of concurrent stack instance operations, by region, for StackSets.
- AWS CloudFormation may not support all resources in the AWS Secret Region.

To determine which resources are supported in a Region, you can programmatically query the AWS CloudFormation registry using the following commands:

```
aws cloudformation list-types --region us-isob-east-1 --visibility PUBLIC --
provisioning-type FULLY_MUTABLE --deprecated-status LIVE --type RESOURCE
```

```
aws cloudformation list-types --region us-isob-east-1 --visibility PUBLIC --
provisioning-type IMMUTABLE --deprecated-status LIVE --type RESOURCE
```

```
aws cloudformation list-types --region us-isob-east-1 --visibility PUBLIC --
provisioning-type NON_PROVISIONABLE --deprecated-status LIVE --type RESOURCE
```

- You cannot use an IAM service role for AWS CloudFormation stack operations.
- Amazon Resource Names (ARNs) and endpoints have different values. The value for a Principle: Service: key in a AWS CloudFormation Template is also different.

  In AWS Secret Region it would look like this:

```
"Statement": [
 {
  "Effect": "Allow",
  "Principal": {
   "Service": [ "ec2.sc2s.sgov.gov " ]
  },
  "Action": [ "sts:AssumeRole" ]
 }
]
```

- The force delete stack option is not available in AWS Secret Region.
- `ServiceTimeout`, an optional property for custom resource requests, is not supported in AWS Secret Region.
- Amazon EC2 launches instances and Amazon RDS DB instances into a VPC instead of using the EC2-Classic platform. For more information, see Amazon EC2 and Amazon Virtual Private Cloud (VPC).
- Only signature version 4 signing is supported.

# How the AWS CloudFormation Helper Scripts Differ for AWS Secret Region

The AWS CloudFormation helper scripts are different for AWS Secret Region in the following ways:

- Instead of a single package, the helper scripts for AWS Secret Region are contained in two packages: `aws-cfn-bootstrap` and `aws-cfn-bootstrap-config-us-isob-east-1`. The `aws-cfn-bootstrap` package contains the code for the helper scripts and `aws-cfn-bootstrap-config-us-isob-east-1` contains configuration information for the helper scripts to work in the region.
- Because the helper scripts are updated periodically, be sure you include the following commands in the `UserData` property of your templates:

  ```
  "yum install -y aws-cfn-bootstrap\n",
  "yum install -y aws-cfn-bootstrap-config-us-isob-east-1\n",
  ```

  The `yum install` command installs the package if it isn't already installed. If the package is installed, `yum install` will update it to the latest version.
- You should periodically update the `aws-cfn-bootstrap-config-us-isob-east-1` package.
- If you use the helper scripts source code to work on another version of Linux, you'll have to create the helper scripts trust store bundle manually or install the `aws-cfn-bootstrap-config-us-isob-east-1` package.
- The cfn-init and cfn-signal helper scripts require credentials in order to use them. Associate an IAM role with the Amazon EC2 instance that you are configuring and use the role's credentials to call `cfn-init` or `cfn-signal`. For `cfn-init`, the role requires permission to the cloudformation:DescribeStackResource action. For `cfn-signal`, the role requires permission to the cloudformation:SignalResource action.

  > **Note**
  >
  > For `cfn-init` and `cfn-signal`, you **must** specify the `--role` and `--url` options.

  For the credential options (`--access-key` and `--secret-key` or `--credential-file`), you do not have to explicitly set these options if the instance role is the same as the role set with the `--role` option.

The following shows an example of how to use the `cfn-init` and `cfn-signal` scripts:

```
"#!/bin/bash\n",
"/opt/aws/bin/cfn-init -v",
" --region ", {"Ref": "AWS::Region"},
" --role='role_goes_here'",
" --url='https://cloudformation.us-isob-east-1.sc2s.sgov.gov'",
" --stack ", {"Ref": "AWS::StackName"},
" --resource CfnInitInstance \n",
" # Signal the status from cfn-init\n",
"/opt/aws/bin/cfn-signal -e $? ",
" --region ", {"Ref": "AWS::Region"},
" --role='role_goes_here'",
" --url='https://cloudformation.us-isob-east-1.sc2s.sgov.gov'",
" --stack ", {"Ref": "AWS::StackName"},
" --resource CfnInitInstance ", "\n"]]}}
```

- For the cfn-hup and `cfn-auto-loader` helper scripts, you **must** specify the role and URL. This is similar to `cfn-init` and `cfn-signal`.

  The following shows an example of how to use the `cfn-hup` and `cfn-auto-reloader` scripts:

```
"/etc/cfn/cfn-hup.conf" : {
  "content" : { "Fn::Join" : ["", [
  "[main]\n",
    "stack=", { "Ref" : "AWS::StackId" }, "\n",
    "region=", { "Ref" : "AWS::Region" }, "\n",
    "url=https://cloudformation.us-isob-east-1.sc2s.sgov.gov\n",
    "role=", { "Ref" : "InstanceRole" }, "\n"
  ]]},
  "mode"    : "000400",
  "owner"   : "root",
  "group"   : "root"
},
"/etc/cfn/hooks.d/cfn-auto-reloader.conf" : {
  "content": { "Fn::Join" : ["", [
    "[cfn-auto-reloader-hook]\n",
    "triggers=post.update\n",
    "path=Resources.ContainerInstances.Metadata.AWS::CloudFormation::Init\n",
    "action=/opt/aws/bin/cfn-init -v ",
    "  --stack ", { "Ref" : "AWS::StackName" },
    "  --resource LaunchConfig ",
```

```
    "  --role ", { "Ref" : "InstanceRole" },
    "  --url https://cloudformation.us-isob-east-1.sc2s.sgov.gov",
    "  --region ", { "Ref" : "AWS::Region" }, "\n",
    "runas=root\n"
  ]]}
}
```

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with AWS CloudFormation and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to AWS CloudFormation by using the command line or APIs, use the following endpoint:

- https://cloudformation.us-isob-east-1.sc2s.sgov.gov

## Documentation for AWS CloudFormation

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how AWS CloudFormation differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS CloudFormation User Guide
- AWS CloudFormation section of AWS CLI Reference
- AWS CloudFormation API Reference
- AWS CloudFormation Sample Templates

# AWS CloudTrail

AWS CloudTrail is a service that records AWS API calls for your account and delivers log files to you. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service.

**Topics**



## How CloudTrail Differs for AWS Secret Region

The implementation of CloudTrail is different for AWS Secret Region in the following ways:

- If you need to manually edit the Amazon S3 bucket policy, Amazon SNS topic policy, or the CMK key policy, use the following service principal name:

```
"Principal": {"Service": "cloudtrail.amazonaws.com"}
```

> **Note**
>
> If the policy specifies the individual CloudTrail account ID for the AWS Secret Region region (`"Principal": { "AWS": ["arn:aws-iso-b:iam::343267119537:root"]}`), you can continue to use this permission type. However, as a best practice, update the policy to use the CloudTrail service principal name.

- AWS Organizations trails are not available.
- Downloading events from the **Insights** page on the AWS Management Console is not supported.
- CloudTrail Lake is not available.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## Services Supported within CloudTrail

CloudTrail supports logging for the services supported in the AWS Secret Region that are integrated with CloudTrail. You can find the specifics for each supported service in that service's guide. For more information, see AWS service topics for CloudTrail in the *AWS CloudTrail User Guide*.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with CloudTrail and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to CloudTrail by using the command line or APIs, use the following endpoint:

- https://cloudtrail.us-isob-east-1.sc2s.sgov.gov

## Documentation for CloudTrail

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how CloudTrail differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS CloudTrail User Guide
- CloudTrail section of AWS CLI Reference
- AWS CloudTrail API Reference

# Amazon CloudWatch

Amazon CloudWatch monitors your AWS resources and the applications you run in AWS Secret Region in real time. You can use CloudWatch to collect and track metrics, which are the variables you want to measure for your resources and applications. CloudWatch alarms send notifications or automatically make changes to the resources you are monitoring based on rules that you define.

**Topics**



## How CloudWatch Differs for AWS Secret Region

The implementation of CloudWatch is different for AWS Secret Region in the following ways:

- Dashboard sharing is not available.
- Metrics Insights is not available.
- Horizontal and vertical annotations are not available on graphs.
- Designating CloudWatch dashboards as favorite dashboards is not available.
- Console functionality (delete/edit model) for anomaly detection is not available.
- CW; Synthetics does not support the following features:
  - X-Ray tracing
  - AWS PrivateLink
  - scheduling with cron
  - The `Names` filter parameter for the **DescribeCanaries** and **DescribeCanariesLastRun** operations.
- Using AWS CloudFormation to add or remove tags on CloudWatch alarms is not supported.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

# How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with CloudWatch and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to CloudWatch by using the command line or APIs, use the following endpoint:

- https://monitoring.us-isob-east-1.sc2s.sgov.gov

## Documentation for CloudWatch

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how CloudWatch differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon CloudWatch User Guide
- Amazon CloudWatch API Reference
- CloudWatch section of AWS CLI Reference
- Amazon CloudWatch CLI Reference

# Amazon CloudWatch Logs

You can use Amazon CloudWatch Logs to monitor, store, and access your log files from EC2 instances and other sources.

**Topics**



## How CloudWatch Logs Differs for AWS Secret Region

The implementation of CloudWatch Logs is different for AWS Secret Region in the following ways:

- Export is not supported for SSE-KMS encrypted buckets.
- If you use the `awslogs` package, be sure that the region is set to us-isob-east-1. For more information, see Quick Start: Install and Configure the CloudWatch Logs Agent on a Running EC2 Instance.
- When encrypting log groups, using encryption context with the ARN of the log group is not available.
- Creating a subscription to stream logs data to Amazon OpenSearch Service is not supported.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with CloudWatch Logs and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to CloudWatch Logs by using the command line or APIs, use the following endpoint:

- https://logs.us-isob-east-1.sc2s.sgov.gov

## Documentation for CloudWatch Logs

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how CloudWatch Logs differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon CloudWatch Logs User Guide
- Amazon CloudWatch Logs API Reference
- CloudWatch Logs section of AWS CLI Reference

# AWS CodeDeploy

AWS CodeDeploy is a deployment service that automates application deployments to Amazon EC2 instances or on-premises instances running in your own facility.

**Topics**



## How CodeDeploy Differs for AWS Secret Region

The implementation of CodeDeploy is different for AWS Secret Region in the following ways:

- The CodeDeploy Resource Kit Bucket Name in AWS Secret Region is: `aws-codedeploy-us-isob-east-1`.
- The CodeDeploy service principal in AWS Secret Region is: `codedeploy.amazonaws.com`.
- CodeDeploy integration with GitHub is not supported.
- CodeDeploy integration with Elastic Load Balancing Application Load Balancers is not supported.
- The CodeDeploy "Getting Started" Wizard is currently not supported in AWS Secret Region.
- In AWS Secret Region, the CodeDeploy Windows Agent requires a certificate bundle containing CAs in at the following location C:\ProgramData\Amazon\CodeDeploy\certs\ca-bundle.crt. You will need to maintain the copy of this file on Windows hosts for continued successful operation of Windows instances. For more information see Digital Certificates for AWS Secret Region .
- On-premises deployments are not supported.
- Tag-based authorization is not supported.
- The notification rules are not currently supported in AWS Secret Region.
- Amazon ECS cluster configuration for CodeDeploy deployments is not supported through the Amazon ECS console in AWS Secret Region but only through the CLI.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.
- Automatically updating outdated instances is not supported.
- Amazon ECS capacity providers are not supported.

- To use CodeDeploy with Amazon Virtual Private Cloud, you must use CodeDeploy agent 1.3.1 or later in the AWS Secret Region.
- API calls to the CodeDeploy endpoint `com.amazonaws.us-isob-east-1.codedeploy` from within a VPC are not supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with CodeDeploy and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to CodeDeploy by using the command line or APIs, use the following endpoint:

- https://codedeploy.us-isob-east-1.sc2s.sgov.gov

## Documentation for CodeDeploy

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how CodeDeploy differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS CodeDeploy User Guide
- AWS CodeDeploy Resource Kit
- AWS CodeDeploy API Reference
- AWS CodeDeploy section of AWS CLI Reference

# AWS Config

AWS Config provides a detailed view of the resources associated with your AWS account, including how they are configured, how they are related to one another, and how the configurations and their relationships have changed over time.

**Topics**



## How AWS Config Differs for AWS Secret Region

The implementation of AWS Config is different for AWS Secret Region in the following ways:

- For a list of resource types supported in AWS Secret Region, see Resource Coverage by Region Availability.
- For a list of AWS Config managed rules supported in AWS Secret Region, see List of AWS Config Managed Rules by Region Availability.
- AWS Config recording of third-party resources is only supported in the AWS Secret Region through the AWS SDK or the AWS Command Line Interface (AWS CLI).
- AWS Config advanced queries are not supported in the AWS Secret Region.
- AWS Config multi-account multi-region data aggregation is not supported in the AWS Secret Region.
- AWS Config conformance packs are not supported in the AWS Secret Region.
- AWS Config deployment of AWS Config rules across an AWS Organization is not supported in the AWS Secret Region.
- AWS Config remediation actions for resources evaluated by AWS Config rules are not supported in the AWS Secret Region.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with AWS Config and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to AWS Config by using the command line or APIs, use the following endpoint:

- https://config.us-isob-east-1.sc2s.sgov.gov

### Documentation for AWS Config

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how AWS Config differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Config Developer Guide
- AWS Config API Reference
- AWS Config section of AWS CLI Reference

## AWS Database Migration Service

AWS Database Migration Service (AWS DMS) is a web service you can use to migrate data to and from most widely used commercial and open-source databases such as Oracle, PostgreSQL, MySQL, and Amazon Redshift.

**Topics**

- How AWS DMS Differs for AWS Secret Region
- How Command Line and API Access Differs for AWS Secret Region
- Documentation for AWS DMS

# How AWS DMS Differs for AWS Secret Region

The implementation of AWS DMS is different for AWS Secret Region in the following ways:

- The download locations for the AWS Schema Conversion Tool are different in AWS Secret Region. The downloads can be found here:
  - Microsoft Windows
  - Fedora Linux (rpm)
  - Ubuntu Linux (deb)
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.
- AWS Snowball Edge is deployed to AWS Secret Region. A description for how to download and install AWS Snowball Edge appears as part of step 2 of Step-by-step procedures for migrating data using AWS DMS with AWSAWS Snowball Edge in the *AWS Data Migration Service User Guide*. Or you can download and install the AWS Snowball Edge client from AWS Snowball Edge resources.
- For the LCK region, AWS DMS 3.4.7 supports the following new or changed behavior and resolved issues:
  - You can now use a date format from the table definition to parse a data string into a date object when using Amazon S3 as a source.
  - New table statistics counters are now available: `AppliedInserts`, `AppliedDdls`, `AppliedDeletes`, and `AppliedUpdates`.
  - You can now choose the default mapping type when using OpenSearch as a target.
  - The new `TrimSpaceInChar` endpoint setting for Oracle, PostgreSQL, and SQLServer sources allows you to specify whether to trim data on CHAR and NCHAR data types.
  - The new `ExpectedBucketOwner` endpoint setting for Amazon S3 prevents sniping when using S3 as a source or target.
  - For RDS SQL Server, Azure SQL Server, and self-managed SQL Server — DMS now provides automated setup of MS-CDC on all tables selected for a migration task that are with or without a PRIMARY KEY, or with a unique index considering the enablement priority for MS-REPLICATION on self-managed SQL Server tables with PRIMARY KEY.
  - Added support for replication of Oracle Partition and sub-partition DDL Operations during Oracle homogenous migrations.

- Fixed an issue where a data validation task crashes with a composite primary key while using Oracle as a source and target.
- Fixed an issue with correctly casting a varying character type to a boolean while the target column was pre-created as a boolean when using Redshift as a target.
- Fixed an issue that was causing data truncation for `varchar` data types migrated as `varchar(255)` due to a known ODBC issue when using PostgreSQL as a target.
- Fixed an issue where Parallel Hint for the DELETE operation wasn't respected with `BatchApplyEnabled` set to `true` and `BatchApplyPreserveTransaction` set to `false` when using Oracle as a target.
- The new `AddTrailingPaddingCharacter` endpoint setting for an Amazon S3 adds padding on string data when using S3 as a target.
- The new `max_statement_timeout_seconds` task setting extends the default timeout of endpoint queries. This setting is currently used by MySQL endpoint metadata queries.
- When using PostgreSQL as a target, fixed an issue where a CDC task wasn't properly utilizing the error handling task settings.
- Fixed an issue where DMS was unable to correctly identify Redis mode for a Redis Enterprise instance.
- Extended the support of `includeOpForFullLoad` extra connection attribute (ECA) for the S3 target parquet format.
- Introduced a new PostgreSQL endpoint setting `migrateBooleanAsBoolean`. When this setting is set to `true` for a PostgreSQL to Redshift migration, a boolean will be migrated as varchar(1). When it is set to `false`, a boolean is migrated as varchar(15), which is the default behavior.
- When using SQL Server source, fixed a migration issue with `datetime` datatype. This fix addresses the issue of inserting `Null` when precision is in milliseconds.
- For PostgresSQL source with PGLOGICAL, fixed a migration issue when using pglogical and removing a field from the source table during the CDC phase, where the value after the removed field wasn't migrated to the target table.
- Fixed a SQL Server Loopback migration issue with Bidirectional replication getting repeated records.
- Added a new ECA `mapBooleanAsBoolean` for PostgresSQL as a source. Using this extra connection attribute , you can override default data type mapping of a PostgresSQL Boolean to a RedShift Boolean data type.

- Fixed a migration issue when using SQL Server as source that addresses the ALTER DECIMAL/NUMERIC SCALE not replicating to targets.
- Fixed connection issue with SQL Server 2005.
- As of October 17, 2022, DMS 3.4.7 now supports Generation 6 Amazon EC2 instance classes for replication instances.

For the LCK region, AWS DMS doesn't support the following new features and enhancements introduced in AWS Database Migration Service (AWS DMS) version 3.4.7:

- Babelfish as a target.
- IBM Db2 z/OS databases as a source for full load only.
- SQL Server read replica as a source.
- EventBridge DMS events.
- VPC source and target endpoints.
- New PostgreSQL version 14.x supported as a source and as a target.
- Aurora Serverless v2 as a target.
- New IBM Db2 for LUW versions 11.5.6 and 11.5.7 as a source.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with AWS DMS and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to AWS DMS by using the command line or APIs, use the following endpoint:

- https://dms.us-isob-east-1.sc2s.sgov.gov

# Documentation for AWS DMS

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how AWS DMS differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Database Migration Service User Guide
- AWS Database Migration Service API Reference
- AWS Database Migration Service section of AWS CLI Reference

# AWS Direct Connect

AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 10-gigabit Ethernet fiber optic cable. One end of the cable is connected to a network partner device or a customer device in each location, the other to an AWS Direct Connect Router. With this connection in place, you can create virtual interfaces directly to AWS Secret Region and Amazon Virtual Private Cloud.

**Topics**



## How AWS Direct Connect Differs for AWS Secret Region

The implementation of AWS Direct Connect is different for AWS Secret Region in the following ways:

- The Resiliency Toolkit is not supported.
- Amazon CloudWatch metrics are not available.
- IPv6 is not supported.
- Port-hours are billed after the connection between the AWS router and your router is established, or 365 days after you ordered the port, whichever comes first.
- MAC Security (MACsec) is not supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to configure AWS Direct Connect and other AWS services through the command line. For more information about the AWS CLI, see AWS CLI.

> **Note**
>
> If you are using the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux AMI for AWS Secret Region.

The following are example AWS CLI directconnect commands:

- Describe locations

```
aws directconnect describe-locations
```

- Create connection

```
aws directconnect create-connection --location location --bandwidth 1Gbps|10Gbps --
connection-name name
```

- Confirm connection

```
aws directconnect confirm-connection --connection-id dxcon-ID
```

- Describe connections

```
aws directconnect describe-connections
```

- Create private virtual interface

```
aws directconnect create-private-virtual-interface --connection-id dxcon-ID
--new-private-virtual-interface '{"virtualInterfaceName": "name", "vlan": integer,
"asn": integer, "authKey": "string",
"amazonAddress": "XXX.XXX.XXX.XXX/YY", "customerAddress": "XXX.XXX.XXX.XXX/YY",
"virtualGatewayId": "vgw-ID"}'
```

- Create public virtual interface

```
aws directconnect create-public-virtual-interface --connection-id dxcon-ID
--new-public-virtual-interface '{"virtualInterfaceName": "name", "vlan": integer,
"asn": integer, "authKey": "string",
"amazonAddress": "XXX.XXX.XXX.XXX/YY", "customerAddress": "XXX.XXX.XXX.XXX/YY",
"routeFilterPrefixes":[{"cidr": "XXX.XXX.XXX.XXX/YY"}, {"cidr": "XXX.XXX.XXX.XXX/
YY"}]}'
```

To connect to AWS Direct Connect by using the command line or APIs, use the following endpoint:

- https://directconnect.us-isob-east-1.sc2s.sgov.gov

# Documentation for AWS Direct Connect

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how AWS Direct Connect differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Direct Connect User Guide
- AWS Direct Connect section of AWS CLI Reference
- AWS Direct Connect API Reference

# AWS Directory Service

AWS Directory Service provides multiple ways to use Microsoft Active Directory (AD) with other AWS services. Directories store information about users, groups, and devices, and administrators use them to manage access to information and resources. AWS Directory Service provides multiple directory choices for customers who want to use existing Microsoft AD or Lightweight Directory Access Protocol (LDAP)–aware applications in the cloud. It also offers those same choices to developers who need a directory to manage users, groups, devices, and access.

**Topics**



## How AWS Directory Service Differs for AWS Secret Region

The implementation of AWS Directory Service is different for AWS Secret Region in the following ways:

- Only AWS Managed Microsoft AD and AD Connector directory types are supported by AWS Directory Service.
- The following directory types are not currently supported:
  - Simple AD
  - Amazon Cloud Directory
- The following AWS Managed Microsoft AD features are not currently supported:
  - Directory sharing with other AWS accounts
  - Log Forwarding to CloudWatch Logs
  - Directory security settings
  - Multi-region replication
- The following AWS apps and services are not currently supported by AWS Directory Service:
  - Amazon WorkDocs
  - Amazon WorkMail
  - Amazon QuickSight
  - Amazon Chime

  - Amazon Connect
  - AWS IAM Identity Center (SSO)
  - AWS PrivateLink
- The following AD Connector feature is not currently supported:
  - Application access URL
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with AWS Directory Service and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to AWS Directory Service by using the command line or APIs, use the following endpoint:

- https://ds.us-isob-east-1.sc2s.sgov.gov
- The CreateAlias action is not supported.

## Documentation for AWS Directory Service

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how AWS Directory Service differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Directory Service Administration Guide

- AWS Directory Service API Reference
- AWS Directory Service section of AWS CLI Reference

# Amazon DynamoDB

Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale. It is a fully managed cloud database and supports both document and key-value store models.

**Topics**



## How DynamoDB Differs for AWS Secret Region

The implementation of DynamoDB is different for AWS Secret Region in the following ways:

- DynamoDB cross-region features are not available.
- Integration with AWS services that are not in the AWS Secret Region region is not possible. This includes Amazon Cognito and AWS Data Pipeline.
- The following features are not available: DynamoDB Accelerator (DAX), CloudWatch Contributor Insights for DynamoDB, NoSQL Workbench, Kinesis Data Streams integration for change capture, PartiQL API actions, and resource-based policies.
- Restores are limited to 4 concurrent operations.
- AWS PrivateLink is not supported for DynamoDB.
- Global Tables are not available in AWS Secret Region.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## Download DynamoDB Local and DynamoDB Storage Backend for Titan

The following tools are available for DynamoDB:

| Package | Location | Documentation |
| --- | --- | --- |
| Local version of DynamoDB | https://s3.us-isob-east-1.sc2s.sgov.gov/dynamodb-customer-facing-tools/dynamodb_local_latest.zip | Running DynamoDB on Your Computer |
| DynamoDB Storage Backend for Titan | https://s3.us-isob-east-1.sc2s.sgov.gov/dynamodb-customer-facing-tools/titan-titan10.zip | Amazon DynamoDB Storage Backend for Titan |

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with DynamoDB and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to DynamoDB by using the command line or APIs, use the following endpoint:

- https://dynamodb.us-isob-east-1.sc2s.sgov.gov

## Documentation for DynamoDB

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how DynamoDB differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon DynamoDB Developer Guide
- DynamoDB section of AWS CLI Reference

- Amazon DynamoDB API Reference

# Amazon Elastic Block Store

Amazon Elastic Block Store (Amazon EBS) provides persistent block storage for use with Amazon EC2 instances. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, providing high availability and durability. Amazon EBS volumes provide the consistent and low-latency performance needed to run your workloads. With Amazon EBS, you can scale your usage up or down within minutes – all while paying a low price for only what you provision.

**Topics**



## How Amazon EBS Differs for AWS Secret Region

The implementation of Amazon EBS is different for AWS Secret Region in the following ways:

- Since AWS Secret Region operates as a single air-gapped region, cross-region features are not supported, such as snapshot copying across regions.
- To create replicas of your Microsoft licensed images and retain your license settings, you can use the Amazon EC2 CLI or Amazon EC2 API to copy a snapshot. The copied snapshot behaves the same as other snapshots: it can be used to create new Amazon EBS volumes that can then be attached to an EC2 instance. For more information, see Copying an Amazon EBS Snapshot.
- Amazon EC2 launches instances into a VPC instead of using the EC2-Classic platform. For more information, see Amazon EC2 and Amazon Virtual Private Cloud (VPC).
- The Provisioned IOPS SSD (io2) EBS volume type is not available in AWS Secret Region.
- The Fast Snapshot Restore (FSR) feature is not available in AWS Secret Region.
- Amazon Data Lifecycle Manager does not support the following features in AWS Secret Region:
  - Amazon EBS snapshot archiving
  - Excluding specific data (non-root) volumes from multi-volume snapshot sets
  - Cross-Region snapshot and AMI copying
  - Fast snapshot restore
  - Amazon EBS local snapshots on Outposts

- You cannot encrypt a previously unencrypted volume using the console. To encrypt a volume, you must use the AWS CLI or AWS SDKs, or you must create a new volume that is encrypted. For more information, see Amazon EBS encryption or Copy an Amazon EBS snapshot in the *Amazon EC2 User Guide*.
- Amazon EBS Snapshots Archive is not available in AWS Secret Region.
- You can't exclude data (non-root) volumes from multi-volume snapshot sets in AWS Secret Region.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## Documentation for Amazon EBS

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Amazon EBS differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon EC2 User Guide

# EBS direct APIs

You can use the EBS direct APIs to create Amazon EBS snapshots, write data directly to your snapshots, read data on your snapshots, and identify the differences or changes between two snapshots. This can be done without having to create new volumes from snapshots, and without using Amazon EC2 instances to compare the differences.

You can create incremental snapshots directly from data on-premises into Amazon EBS volumes and the cloud to use for quick disaster recovery. With the ability to write and read snapshots, you can write your on-premises data to an Amazon EBS snapshot during a disaster. Then after recovery, you can restore it back to AWS or on-premises from the snapshot.

**Topics**



## How EBS direct APIs Differs for AWS Secret Region

EBS direct APIs is different for AWS Secret Region in the following ways:

- AWS CloudTrail data events are not supported in AWS Secret Region.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with EBS direct APIs and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to EBS direct APIs by using the command line or APIs, use the following endpoint:

- https://ebs.us-isob-east-1.sc2s.sgov.gov

## Documentation for EBS direct APIs

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how EBS direct APIs differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- EBS direct APIs User Guide
- EBS direct APIs section of AWS CLI Reference
- EBS direct APIs API reference
- AWS Tools for Windows PowerShell User Guide
- AWS Tools for PowerShell Cmdlet Reference

# Amazon Elastic Compute Cloud

Amazon Elastic Compute Cloud (Amazon EC2) is a service that provides resizable compute capacity in the cloud. It's designed to make web-scale computing easier for developers. Amazon EC2 presents a true virtual computing environment, allowing you to use web service interfaces to launch instances with a variety of operating systems, load them with your custom application environment, manage your network's access permissions, and run your image using as many or few systems as you want.

**Topics**



## How Amazon EC2 Differs for AWS Secret Region

The implementation of Amazon EC2 is different for AWS Secret Region in the following ways:

- Capacity Reservation Fleet is not supported with the Amazon EC2 console. It is supported with the AWS CLI and SDKs only.
- Amazon EC2 Instance Connect Endpoint is not available in AWS Secret Region.
- The EC2 Reserved Instance Marketplace is not available in AWS Secret Region.
- Tags in instance metadata are not available in the Amazon EC2 console in AWS Secret Region.
- EC2 Fleet can't launch On-Demand Instances into targeted Capacity Reservations in AWS Secret Region.
- Custom time windows for scheduled events are currently not available in AWS Secret Region.
- The AWS service principal for Amazon EC2 is `ec2.amazonaws.com`, but the former service principal of `ec2.sc2s.sgov.gov` is still supported for backward compatibility.
- EC2 Serial Console is currently not available in AWS Secret Region.
- Using AWS Systems Manager parameters instead of AMI IDs in launch templates is not available in AWS Secret Region.
- For a list of supported Amazon EC2 instance types, please see Instance Types.

- Savings Plans are currently not available in AWS Secret Region.
- Spot Instances are not available.
- The attribute-based instance type selection feature for Amazon EC2 Fleet and Spot Fleet is not available.
- For GPU instancesFor GPU instances, you should use the NVIDIA drivers that NVIDIA publishes in their AWS Marketplace. You can find NVIDIA AMIs and corresponding driver versions by searching for NVIDIA in the commercial AWS Marketplace.
- To enable enhanced networking on other Linux distributions, you must compile and install the `ixgbevf` module on your instance. The following `ixgbevf` versions are available for download:

| Module | Readme |
| --- | --- |
| ixgbevf-2.16.4.tar.gz | readme-ixgbevf-2.16.4.txt |
| ixgbevf-3.0.2.tar.gz | readme-ixgbevf-3.0.2.txt |
| ixgbevf-3.0.3.tar.gz | readme-ixgbevf-3.0.3.txt |
| ixgbevf-3.1.1.tar.gz | readme-ixgbevf-3.1.1.txt |
| ixgbevf-3.1.2.tar.gz | readme-ixgbevf-3.1.2.txt |
| ixgbevf-3.2.2.tar.gz | readme-ixgbevf-3.2.2.txt |

  For more information, see Enabling Enhanced Networking with the Intel 82599 VF Interface on Other Linux Distributions.
- For Windows instances, the maximum transmission unit (MTU) of a network connection is 1500 bytes. For Linux instances, the maximum supported MTU is 9001 bytes. For more information, see Network Maximum Transmission Unit (MTU) for Your EC2 Instance.
- Within AWS Secret Region, Availability Zones are not independently mapped to identifiers for each account, and are fixed in nature. All customer accounts utilize the same Availability Zone mapping, and require no action on the customer's part to ensure this.
- For differences about Amazon Linux 2, see Amazon Linux 2 AMI for AWS Secret Region.
- For differences about the Amazon Linux AMI, see Amazon Linux AMI for AWS Secret Region.
- For differences about Windows AMIs, see AWS Windows AMIs for AWS Secret Region.

- For instance identity documents, you should use the following AWS public certificate to verify the PKCS7 signature:

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQD3i0Bw4z2PPzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xNzA5MjYyMTQxNThaFw00
MzA5MjcyMTQxNThaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCRthrx/VKsMiIhfgdz
qZp5LJB4XlAvfLI1jqIlRcnn2d0lrjTVqIw3Je+Zd4PRM+2/FfcnRNarM8sOcaxL
a6U9yPGfSpDVXzPWfUDF9IGGSTDUmacnpiLEXUcPSMCQJEeJoZrtBN3hVN0vnYeP
2UCwX9Ur4sHnVApm7TNg/jfTQQIVAJ2sjeTo86vIFNYehnrIC9etWVIJAoGBAIr3
aiRQ73pH0JcnJMC1pTN6QagnGZh3opmWxgYKJAlKDHZMkmPDELSPiCP+MbPrwyW6
+QKEISiM+HhleDqGo1VLryiTAmzAwV3RQJkcEYT2ZF8495mb0iRB/86M7PtGTLGH
sIlhQ2gt0FYYuyxEHAnPjScDCgGDkP7+q95nMmv+A4GEAAKBgBQdbRN9VeLueQm0
+Aau8fWvHCMTxQ6ayFtBSuA/mQwLUhrMazevIsCntIqE5+9tr7J4Jy9wMsfLxAcx
H/7M3KfiBS04yOVrtYo44WphXSOjLWw0q/C2FEcm4rM4srxRO6nYyVMBT/Zhqo7d
4/E1zfnuArGS9WQoXQpuu+ecQY4LMAkGByqGSM44BAMDLwAwLAIUaUM4RH3s08TA
2JytfsWLlMq9JbUCFEdDBqON332KkwjLEo/y2xe2VH8t
-----END CERTIFICATE-----
```

- The Provisioned IOPS SSD (io2) EBS volume type is not available in AWS Secret Region.
- AWS Nitro Enclaves is not available in AWS Secret Region.
- Amazon Resource Names (ARNs) and endpoints have different values.
- AWS Compute Optimizer is not available in AWS Secret Region.
- Amazon Data Lifecycle Manager does not support the following features in AWS Secret Region:
  - Amazon EBS snapshot archiving
  - Excluding specific data (non-root) volumes from multi-volume snapshot sets
  - Cross-Region snapshot and AMI copying
  - Fast snapshot restore
  - Amazon EBS local snapshots on Outposts
- Dedicated Host resource groups are not available in AWS Secret Region.
- Dedicated Host sharing is not available in AWS Secret Region.
- Dedicated Hosts can support only one instance size in AWS Secret Region.
- Dedicated Host recovery is not available in AWS Secret Region.

- License-included AMIs that are offered by AWS or that are available on AWS Marketplace can't be used with Dedicated Hosts.
- Amazon EBS Multi-Attach is not available in AWS Secret Region.
- Amazon EBS local snapshots on Outposts is not available in AWS Secret Region.
- The minimum size for Throughput Optimized HDD (st1) and Cold HDD (sc1) volumes is 500 GiB.
- Fast snapshot restore is not available in AWS Secret Region.
- Wavelength Zones are not available in AWS Secret Region.
- Local Zones are not available in AWS Secret Region.
- ARM-64 AMIs are not available in AWS Secret Region.
- Elastic GPUs are not available in AWS Secret Region.
- Elastic Inference Accelerators are not available in AWS Secret Region.
- Bring your own IP addresses (BYOIP) is not available in AWS Secret Region.
- You can't reschedule scheduled maintenance events in AWS Secret Region.
- On-demand instance hibernation is not available in AWS Secret Region.
- Security group rule IDs are not available in the Amazon EC2 Console.
- Seamless domain join is not enabled in AWS Secret Region.
- On-demand instance quotas are based on number of vCPUs in AWS Secret Region.
- The transfer Elastic IP address feature is not available in AWS Secret Region.
- AMD Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP) is not available in AWS Secret Region.
- Attached EBS status checks are not available in AWS Secret Region.
- VSS application-consistent snapshot is not available in AWS Secret Region.
- Amazon EC2 instance topology is not available in AWS Secret Region.
- Launching an instance with an AWS Marketplace AMI is not supported in AWS Secret Region. Therefore, the **AWS Marketplace AMIs** tab is not available in the AMI Catalog in AWS Secret Region.
- AMI's that have the ImdsSupport property set to `V2.0` will not currently enable IMDSv2 when launching instances via the RunInstances API. Customers should rather configure IMDSv2 via the relevant RunInstances parameters or via a Launch Template.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## How VM Import/Export Differs for AWS Secret Region

Virtual machine (VM) Import/Export is different for AWS Secret Region in the following ways:

- You can use the AWS VM Import tools to import VM images from your local environment and convert them into Amazon EC2 instances. For more information, see Importing a VM into Amazon EC2.
- You can import Microsoft Windows VMs that use the Bring Your Own License (BYOL) model. First, create a case in AWS Support Center and request to be whitelisted for Windows BYOL. Import the Windows VM using the instructions for Importing a Virtual Machine Using the Amazon EC2 CLI.
- `ImportInstance` is not supported in AWS Secret Region.
- UEFI boot mode is not supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Amazon EC2 and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

Amazon EC2 has a service-specific command line interface. For more information about the Amazon EC2 CLI Tools, see AWS CLI.

To connect to Amazon EC2 by using the command line or APIs, use the following endpoint:

- https://ec2.us-isob-east-1.sc2s.sgov.gov

## Documentation for Amazon EC2

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Amazon EC2 differs for AWS Secret Region, as described

in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon Elastic Compute Cloud Documentation

# Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling allows you to scale your Amazon EC2 capacity up or down automatically according to conditions you define. With Amazon EC2 Auto Scaling, you can ensure that the number of Amazon EC2 instances you're using increases seamlessly to maintain performance during demand spikes, and decreases automatically to minimize costs during demand lulls. Auto Scaling is particularly well suited for applications that experience hourly, daily, or weekly variability in usage. Auto Scaling is enabled by Amazon CloudWatch and available at no additional charge beyond CloudWatch fees.

**Topics**



## How Auto Scaling Differs for AWS Secret Region

The implementation of Auto Scaling is different for AWS Secret Region in the following ways:

- For Auto Scaling groups with multiple instance types, you can only launch On-Demand Instances. However, Reserved Instances are supported. These On-Demand Instances must match certain attributes, such as instance type and Region, in order to benefit from the billing discount. Savings Plans are not currently supported in AWS Secret Region.
- Amazon EC2 Auto Scaling does not support launching Spot Instances.
- The attribute-based instance type selection feature is not available.
- Specifying `lowest-price` for the `OnDemandAllocationStrategy` property of a mixed instances group is currently not supported.
- Amazon EC2 launches instances into a VPC instead of using the EC2-Classic platform. For more information, see Amazon EC2 and Amazon Virtual Private Cloud (VPC).
- Amazon EC2 provides other restrictions. For more information, see Amazon Elastic Compute Cloud .
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.
- You cannot create a predictive scaling policy in AWS Secret Region.

- Retrieving the target lifecycle state through instance metadata is not available in AWS Secret Region.
- The metric math feature for target tracking scaling policies is not available.
- Amazon EC2 Auto Scaling does not currently support the AttachTrafficSources, DetachTrafficSources, and DescribeTrafficSources API operations.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Auto Scaling and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Auto Scaling by using the command line or APIs, use the following endpoint:

- https://autoscaling.us-isob-east-1.sc2s.sgov.gov

## Documentation for Auto Scaling

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Auto Scaling differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon EC2 Auto Scaling User Guide
- Auto Scaling section of AWS CLI Reference
- Amazon EC2 Auto Scaling API Reference

# Amazon EC2 Image Builder

Amazon EC2 Image Builder (Image Builder) is a fully managed AWS service that makes it easier to automate the creation, management, and deployment of customized, secure, and up-to-date server images that are pre-installed and pre-configured with software and settings to meet specific IT standards.

**Topics**



## How Image Builder Differs for AWS Secret Region

The implementation of Image Builder is different for AWS Secret Region in the following ways:

- Amazon Resource Names (ARNs) and endpoints have different values.
- The AWS Task Orchestrator and Executor (AWSTOE) component management tool's UpdateOS Action Module won't work for Windows unless you configure your own WSUS Server and modify the image to point to that.
- For all Linux distributions except for Amazon Linux 2, you must configure your image to use repository mirrors that are available on the network.
- Image Builder doesn't support third party managed Linux base images, except for RHEL, for example SUSE, Ubuntu, CentOs, or others. However, you can supply your own custom AMIs for those operating system platforms.
- Image Builder doesn't support Virtual machine (VM) import/export in AWS Secret Region.
- Image Builder doesn't support AWS PrivateLink in AWS Secret Region.
- Image Builder doesn't support AWS CloudFormation for container images in AWS Secret Region.
- Image Builder doesn't support managed container images in AWS Secret Region.
- Image Builder doesn't support common vulnerability (CVE) findings in AWS Secret Region.
- Image Builder doesn't support CIS Hardened Images or the CIS Hardening component from the Center for Internet Security in AWS Secret Region.
- Image Builder doesn't support image lifecycle policies in AWS Secret Region.
- Image Builder doesn't support image workflows in AWS Secret Region.

# How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Image Builder and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Image Builder by using the command line or APIs, use the following endpoint:

- https://imagebuilder.us-isob-east-1.sc2s.sgov.gov

## Documentation for Image Builder

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Image Builder differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Image Builder User Guide
- Image Builder section of AWS CLI Reference
- Image Builder API Reference

# Amazon Elastic Container Registry

Amazon Elastic Container Registry (Amazon ECR) is a fully managed container registry offering high-performance hosting, so you can reliably deploy application images and artifacts anywhere.

**Topics**



## How Amazon ECR Differs for AWS Secret Region

The implementation of Amazon ECR is different for AWS Secret Region in the following ways:

- Amazon ECR lifecycle policies are not supported.
- Pushing Open Container Initiative (OCI) artifacts, including Helm charts, is not supported.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.
- Amazon ECR image scanning is not supported. This includes both basic and enhanced scanning.
- Pull through cache rules are not supported.
- Tagging an Amazon ECR repository is not supported.
- Cross-region and cross-account replication is not supported.
- Amazon ECR doesn't emit any events to Amazon EventBridge in AWS Secret Region.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Amazon ECR and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Amazon ECR by using the command line or APIs, use the following endpoint:

- https://ecr.us-isob-east-1.sc2s.sgov.gov

## Documentation for Amazon ECR

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Amazon ECR differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon Elastic Container Registry User Guide
- Amazon ECR section of AWS CLI Reference
- Amazon Elastic Container Registry API Reference

# Amazon Elastic Container Service

Amazon Elastic Container Service (Amazon ECS) is a highly scalable, fast, container management service that makes it easy to run, stop, and manage Docker containers.

**Topics**



## How Amazon ECS Differs for AWS Secret Region

The implementation of Amazon ECS is different for AWS Secret Region in the following ways:

- All layers and containers specified must be in Amazon ECR or another registry in the region.
- When registering a task definition, if you are using a task execution IAM role, then the task definition role must already be created. The AWS Management Console cannot create this role on your behalf. For more information on creating the task execution role, see Amazon ECS Task Execution IAM Role in the *Amazon Elastic Container Service Developer Guide*.
- The `ECS_BACKEND_HOST` parameter must be specified using the correct endpoint in `/etc/ecs/ecs.config`. After this change is made the Amazon ECS container agent must be restarted.

```
echo "ECS_BACKEND_HOST=https://ecs.us-isob-east-1.sc2s.sgov.gov">> /etc/ecs/
ecs.config
```

- If your container instance was not launched using an Amazon ECS-optimized AMI, see Installing the Amazon ECS Container Agent in the *Amazon Elastic Container Service Developer Guide* for details on installing the Amazon ECS container agent.
- The **Clusters** section of the console has a **Get Started** button for creating a simple task in a cluster. The **Image** field is prepopulated with `httpd:2.4` to use version 2.4 of the Apache HTTP server Docker image. Because there are no public registries in the region, this will not work. If you have a compatible image in a registry for which you have access, you can use *`repository-url/image:tag`* or *`repository-url/image@digest`* to specify that image.
- Interface VPC endpoints(AWS PrivateLink) for Amazon ECS are not supported.
- The UpdateContainerAgent API action is not supported.
- Attaching Amazon Elastic Inference accelerators to your containers is not supported.

- Amazon ECS cluster auto scaling is not supported.
- ECS Anywhere is not supported.
- AWS Copilot is not supported.
- Tagging Amazon ECS resources is not available.
- Fargate Spot is not available in AWS Secret Region.
- The ECS CLI is not supported.
- Amazon ECS resources are not supported CloudWatch targets.
- Private Registry Authentication is not supported.
- Amazon ECS Exec Suite not supported against Fargate Containers.
- You must explicitly specify the AWS service endpoint in the Fluent Bit output definition using the endpoint option supported by all AWS plugins. For more information, see Using the AWS for Fluent Bit image in the *Amazon Elastic Container Service Developer Guide*.
- Amazon ECS Deployment Circuit Breaker is not supported in the AWS Secret Region.
- Scheduled tasks are not supported for Amazon ECS tasks.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.
- Amazon ECS limit increases aren't available through AWS Service Quotas
- Amazon ECS Service Connect is not available in AWS Secret Region.
- Task definition deletion is not supported.
- The `splunk` log driver is not supported in the AWS Secret Region.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Amazon ECS and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Amazon ECS by using the command line or APIs, use the following endpoint:

- https://ecs.us-isob-east-1.sc2s.sgov.gov

## Documentation for Amazon ECS

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Amazon ECS differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon Elastic Container Service Developer Guide
- Amazon ECS section of AWS CLI Reference
- Amazon Elastic Container Service API Reference

# Amazon EFS

Amazon EFS provides a simple, serverless, elastic, set-and-forget elastic file system that automatically grows and shrinks as you add and remove files with no need for management or provisioning. You can use Amazon EFS with Amazon EC2, Lambda, Amazon ECS, Amazon EKS and other Amazon compute instances. You can mount an Amazon EFS file system in your virtual private cloud (VPC), through the Network File System versions 4.0 and 4.1 (NFSv4) protocol. We recommend using a current generation Linux NFSv4.1 client, such as those found in the latest Amazon Linux, Amazon Linux 2, Red Hat, Ubuntu, and macOS Big Sur AMIs, in conjunction with the Amazon EFS mount helper.

**Topics**



## How Amazon EFS Differs for AWS Secret Region

The implementation of Amazon EFS is different for AWS Secret Region in the following ways:

- 17-character format resource IDs for file system and mount target resource types are not available.
- The default selection for Amazon EFS Lifecycle Management is **None** when creating a new file system.
- Using AWS Backup to backup Amazon EFS file systems is not available.
- Using AWS DataSync to transfer data into or out of Amazon EFS file systems is not available.
- Using AWS Transfer Family to transfer data into or out of Amazon EFS file systems is not available.
- Amazon EFS One Zone storage classes are not available.
- EFS file system policies are not available when creating an EFS file system using AWS CloudFormation.
- EFS backup policies are not available when creating an EFS file system using AWS CloudFormation.
- EFS Access Points are not supported in AWS CloudFormation in this Region.

- Using Amazon Elastic Kubernetes Service with Amazon EFS is not available in this Region.
- Amazon Resource Names (ARNs) and endpoints have different values.
- EFS Replication is not available.
- Replicating to an existing file system is not supported.
- The EFS Archive storage class and the Transition into Archive lifecycle policy are not supported.
- The EFS console refers to One Zone as a storage class instead of a file system type.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Amazon EFS and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Amazon EFS by using the command line or APIs, use the following endpoint:

- https://efs.us-isob-east-1.sc2s.sgov.gov

## Documentation for Amazon EFS

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Amazon EFS differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon Elastic File System User Guide
- Amazon EFS section of AWS CLI Reference

# Amazon EKS

Amazon Elastic Kubernetes Service (Amazon EKS) is a fully-managed, certified Kubernetes conformant service that simplifies the process of building, securing, operating, and maintaining Kubernetes clusters on AWS. Amazon EKS integrates with core AWS services such as CloudWatch, Auto Scaling Groups, and IAM to provide a seamless experience for monitoring, scaling and load balancing your containerized applications.

**Topics**



## How Amazon EKS Differs for AWS Secret Region

The implementation of Amazon EKS is different for AWS Secret Region in the following ways:

- Amazon EKS Pod Identities aren't available.
- Amazon EKS Anywhere isn't available.
- Amazon Resource Names (ARNs) and endpoints have different values.
- The latest Amazon EKS supported Kubernetes version might not be available. We recommend that you review Kubernetes versions regularly to see which versions are available.
- Amazon EKS Extended Support for Kubernetes Versions isn't available.
- You can't use AWS PrivateLink to create a private connection between your VPC and Amazon EKS.
- AWS Fargate on EKS isn't available.
- Spot instances aren't available for managed node groups.
- ARM, Bottlerocket, and Windows AMIs aren't available.
- Amazon Linux 2023 isn’t available.
- The Amazon FSx for Lustre CSI driver isn't available.
- The CSI snapshot controller is only available as a self-managed installation.
- `IPv6` support isn't available.
- IP prefix assignment can't be used with the Amazon VPC CNI plugin.
- The following features of the AWS Load Balancer Controller aren't available: Load Balancer listener tagging, SSL policy, AWS WAF and AWS WAFv2, and AWS Shield.

- The AWS App Mesh Kubernetes controller isn't available.
- Amazon EKS limit increases aren't available through AWS Service Quotas.
- AWS Certificate Manager private Kubernetes integration isn't available.
- Only signature version 4 signing is supported.
- Clusters running Kubernetes version 1.27 or higher can use Kubernetes Secrets Store CSI driver with AWS Secrets Manager.
- Amazon EKS on AWS Outposts isn't supported.
- The Amazon CloudWatch Observability Operator isn't available.
- CloudWatch Container Insights isn't available.
- Amazon Managed Service for Prometheus isn't available.
- The AWS Distro for OpenTelemetry (ADOT) Operator isn't available.
- Amazon GuardDuty isn't available.
- The Amazon EKS Connector isn't available.
- Mountpoint for Amazon S3 CSI Driver is only available as a self-managed installation.
- Amazon EKS Upgrade insights aren't available.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Amazon EKS and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Amazon EKS by using the command line or APIs, use the following endpoint:

- https://eks.us-isob-east-1.sc2s.sgov.gov

# Elastic Load Balancing

Elastic Load Balancing automatically distributes incoming application traffic across multiple Amazon EC2 instances. It enables you to achieve greater fault tolerance in your applications, seamlessly providing the amount of load balancing capacity needed in response to incoming application traffic. Elastic Load Balancing detects unhealthy instances within a pool and automatically reroutes traffic to healthy instances until the unhealthy instances have been restored.

**Topics**



## How Elastic Load Balancing Differs for AWS Secret Region

The implementation of Elastic Load Balancing is different for AWS Secret Region in the following ways:

- Application Load Balancers and Classic Load Balancers in AWS Secret Region do not support desync mitigation mode.
- Application Load Balancers in AWS Secret Region do not support Cognito user authentication in listener rules.
- AWS WAF (Web Application Firewall) is not available in AWS Secret Region for Application Load Balancers.
- Application cookie stickiness is not available in AWS Secret Region for Application Load Balancers.
- Application Load Balancers in AWS Secret Region do not support the least outstanding requests algorithm.
- Application Load Balancers in AWS Secret Region do not support registering IP addresses as targets. You can register instance IDs as targets.
- Because Amazon Route 53 is not available in AWS Secret Region, Elastic Load Balancing doesn't support Route 53 features. You can use CNAME to associate your custom domain name with your load balancer name.

- Elastic Load Balancing does not support Internet Protocol version 6 (IPv6) in AWS Secret Region. Elastic Load Balancing provides a public DNS name for your load balancer that returns Internet Protocol version 4 (IPv4) records.
- Amazon EC2 launches instances into a VPC instead of using the EC2-Classic platform. For more information, see Amazon EC2 and Amazon Virtual Private Cloud (VPC).
- Elastic Load Balancing uses the following account ID. For information about when it is used, see Attach a Policy to Your Amazon S3 Bucket.

| Region | Elastic Load Balancing Account ID |
|---|---|
| us-isob-east-1 | 740734521339 |

- Route 53 Hosted Zone ID information:

| Region | Route 53 Hosted Zone ID |
|---|---|
| us-isob-east-1 | Network Load Balancers: Z1JGH2CK5AI3TN |
| us-isob-east-1 | Application Load Balancers/Classic Load Balancers: Z07958632NF8C8QMGH5OQ |

- AWS Secret Region uses a private CA and the IDP endpoints need to be within the AWS Secret Region WAN and not open internet.
- Network Load Balancers in AWS Secret Region do not support custom private IPv4 addresses.
- Network Load Balancers in AWS Secret Region do not support configuring Application Load Balancers as targets.
- Elastic Load Balancing does not support standalone creation of target groups with protocol version HTTP/2 or gRPC in AWS Secret Region. These target groups can only be created while launching a new Application Load Balancer.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Elastic Load Balancing and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Elastic Load Balancing by using the command line or APIs, use the following endpoint:

- https://elasticloadbalancing.us-isob-east-1.sc2s.sgov.gov

## Documentation for Elastic Load Balancing

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Elastic Load Balancing differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Elastic Load Balancing User Guide
- User Guide for Classic Load Balancers
- User Guide for Application Load Balancers
- User Guide for Network Load Balancers
- User Guide for Gateway Load Balancers
- Elastic Load Balancing section of AWS CLI Reference
- Elastic Load Balancing API Reference version 2012-06-01

# Amazon EMR

Amazon EMR helps you analyze and process vast amounts of data by distributing the computational work across a cluster of virtual servers running in the AWS cloud. The cluster is managed using an open-source framework called Hadoop. Amazon EMR lets you focus on processing and analyzing your data without having to worry about time-consuming set up, management, and tuning of Hadoop clusters or the compute capacity they rely on.

**Topics**



## How Amazon EMR Differs for AWS Secret Region

The implementation of Amazon EMR is different for AWS Secret Region in the following ways:

**6.x available versions**

The following 6.x release versions are available in AWS Secret Region:

- 6.15.0
- 6.12.0
- 6.11.0
- 6.10.0
- 6.9.0
- 6.6.0
- 6.3.0
- 6.2.0
- 6.0.0

**5.x available versions**

The following 5.x release versions are available in AWS Secret Region:

- 5.36.2

- 5.36.1
- 5.36.0
- 5.33.0
- 5.32.0
- 5.31.0
- 5.30.1
- 5.29.0
- 5.28.1
- 5.27.0, 5.27.1
- 5.25.0
- 5.21.0, 5.21.2
- 5.19.0, 5.19.1
- 5.15.0, 5.15.1
- 5.13.0, 5.13.1

### Supported instance types

The following Amazon EC2 instance types are available for Amazon EMR in AWS Secret Region. We recommend that you upgrade your processes and workloads to use current generation instance types.

| Instance class | Instance types |
| --- | --- |
| **General Purpose - Current Generation** | m5.xlarge, m5.2xlarge, m5.4xlarge, m5.8xlarge, m5.12xlarge, m5.16xlarge, m5.24xlarge, m5d.xlarge, m5d.2xlarge, m5d.4xlarge, m5d.8xlarge, m5d.12xlarge, m5d.16xlarge, m5d.24xlarge, m6g.xlarge, m6g.2xlarge, m6g.4xlarge, m6g.8xlarge, m6g.12xlarge, m6g.16xlarge, m6gd.xlarge, m6gd.2xlarge, m6gd.4xlarge, m6gd.8xlarge, m6gd.12xlarge, m6gd.16xlarge, m6i.xlarge, m6i.2xlarge, m6i.4xlarge, m6i.8xlarge, m6i.12xlarge, m6i.16xlarge, m6i.24xlarge, m6i.32xlarge |
| **General Purpose - Previous Generation** | m4.large, m4.xlarge, m4.2xlarge, m4.4xlarge, m4.10xlarge, m4.16xlarge |

| Instance class | Instance types |
| --- | --- |
| **Compute Optimized - Current Generation** | c5.xlarge, c5.2xlarge, c5.4xlarge, c5.9xlarge, c5.12xlarge, c5.18xlarge, c5.24xlarge, c5d.xlarge, c5d.2xlarge, c5d.4xlarge, c5d.9xlarge, c5d.12xlarge, c5d.18xlarge, c5d.24xlarge, c5n.xlarge, c5n.2xlarge, c5n.4xlarge, c5n.9xlarge, c5n.18xlarge, c6g.xlarge, c6g.2xlarge, c6g.4xlarge, c6g.8xlarge, c6g.12xlarge, c6g.16xlarge, c6i.xlarge, c6i.2xlarge, c6i.4xlarge, c6i.8xlarge, c6i.12xlarge, c6i.16xlarge, c6i.24xlarge, c6i.32xlarge |
| **Compute Optimized - Previous Generation** | c4.large, c4.xlarge, c4.2xlarge, c4.4xlarge, c4.8xlarge |
| **Accelerated Computing - Current Generation** | g3.4xlarge, g3.8xlarge, g3.16xlarge, g4dn.xlarge, g4dn.2xlarge, g4dn.4xlarge, g4dn.8xlarge, g4dn.12xlarge, g4dn.16xlarge, g5.xlarge, g5.2xlarge, g5.4xlarge, g5.8xlarge, g5.12xlarge, g5.16xlarge, g5.24xlarge, g5.48xlarge, p3.2xlarge, p3.8xlarge, p3.16xlarge |
| **Memory Optimized - Current Generation** | r5.xlarge, r5.2xlarge, r5.4xlarge, r5.8xlarge, r5.12xlarge, r5.16xlarge, r5.24xlarge, r5d.xlarge, r5d.2xlarge, r5d.4xlarge, r5d.8xlarge, r5d.12xlarge, r5d.16xlarge, r5d.24xlarge, r5n.xlarge, r5n.2xlarge, r5n.4xlarge, r5n.8xlarge, r5n.12xlarge, r5n.16xlarge, r5n.24xlarge, r6g.xlarge, r6g.2xlarge, r6g.4xlarge, r6g.8xlarge, r6g.12xlarge, r6g.16xlarge, r6i.xlarge, r6i.2xlarge, r6i.4xlarge, r6i.8xlarge, r6i.12xlarge, r6i.16xlarge, r6i.24xlarge, r6i.32xlarge, x1.16xlarge, x1.32xlarge |
| **Memory Optimized - Previous Generation** | r3.xlarge, r3.2xlarge, r3.4xlarge, r3.8xlarge, r4.xlarge, r4.2xlarge, r4.4xlarge, r4.8xlarge, r4.16xlarge |
| **Storage Optimized - Current Generation** | d2.xlarge, d2.2xlarge, d2.4xlarge, d2.8xlarge, d3.xlarge, d3.2xlarge, d3.4xlarge, d3.8xlarge, i3.xlarge, i3.2xlarge, i3.4xlarge, i3.8xlarge, i3.16xlarge, i3en.xlarge, i3en.2xlarge, i3en.3xlarge, i3en.6xlarge, i3en.12xlarge, i3en.24xlarge |

- Automatic Amazon Linux updates, as discussed in the Amazon EMR Management Guide , are not enabled in AWS Secret Region.
- The issue discussed in CVE-2021-44228 is relevant to Apache log4j- core versions between 2.0 and 2.14.1 when processing inputs from untrusted sources. EMR clusters launched with EMR 5 releases up to 5.34 and EMR 6 releases up to EMR 6.5 include open source frameworks such as Apache Hive, Flink, HUDI, Presto, and Trino, which use these versions of Apache Log4j. However, many customers use the open source frameworks installed on their EMR clusters to process and log inputs from untrusted sources. Therefore, AWS recommends that you apply the "EMR Bootstrap Action Solution for Log4j CVE-2021-44228" as described in the topic, Approach to mitigate CVE-2021-44228. This solution also addresses CVE-2021-45046.

> **Note**
>
> In the AWS Secret Region, starting with Amazon EMR 5.36 and Amazon EMR 6.6, applications that use Log4j 1.x and Log4j 2.x will be upgraded to use Log4j 1.2.17 (or higher) and Log4j 2.17.1 (or higher) respectively, and will not require using the bootstrap actions provided above to mitigate the CVE issues.

For each EMR release available in your region that has an associated bootstrap action script, you will find a link below. If you are not using the latest revision for an EMR minor release (for example, 6.3.0), use the script associated with the latest revision (for example, 6.3.1), and then apply the solution discussed in Approach to mitigate CVE-2021-44228.

**CVE-2021-44228 & CVE-2021-45046 - AWS Secret Region - Bootstrap Scripts for EMR Releases**

| Amazon EMR release version | Script location | Script release date |
|---|---|---|
| 6.3.1 | `s3://us-isob-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-6.3.1-v1.sh` | December 13, 2021 |
| 6.2.1 | `s3://us-isob-east-1.elasticmapreduce` | December 13, 2021 |

| Amazon EMR release version | Script location | Script release date |
|---|---|---|
| | `/bootstrap-actions/log4j/patch-log4j-emr-6.2.1-v1.sh` | |
| 6.0.1 | `s3://us-isob-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-6.0.1-v1.sh` | December 14, 2021 |
| 5.33.1 | `s3://us-isob-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.33.1-v1.sh` | December 12, 2021 |
| 5.32.1 | `s3://us-isob-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.32.1-v1.sh` | December 13, 2021 |
| 5.31.1 | `s3://us-isob-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.31.1-v1.sh` | December 13, 2021 |
| 5.30.2 | `s3://us-isob-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.30.2-v1.sh` | December 14, 2021 |

| Amazon EMR release version | Script location | Script release date |
|---|---|---|
| 5.29.0 | `s3://us-isob-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.29.0-v1.sh` | December 14, 2021 |
| 5.28.1 | `s3://us-isob-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.28.1-v1.sh` | December 15, 2021 |
| 5.27.1 | `s3://us-isob-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.27.1-v1.sh` | December 15, 2021 |
| 5.25.0 | `s3://us-isob-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.25.0-v1.sh` | December 15, 2021 |
| 5.21.2 | `s3://us-isob-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.21.2-v1.sh` | December 15, 2021 |

| Amazon EMR release version | Script location | Script release date |
|---|---|---|
| 5.19.1 | `s3://us-isob-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.19.1-v1.sh` | December 15, 2021 |
| 5.15.1 | `s3://us-isob-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.15.1-v1.sh` | December 15, 2021 |
| 5.13.1 | `s3://us-isob-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.13.1-v1.sh` | December 15, 2021 |
| 5.12.3 | `s3://us-isob-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.12.3-v1.sh` | December 15, 2021 |
| 5.11.4 | `s3://us-isob-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.11.4-v1.sh` | December 15, 2021 |

| Amazon EMR release version | Script location | Script release date |
|---|---|---|
| 5.9.1 | `s3://us-isob-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.9.1-v1.sh` | December 15, 2021 |
| 5.8.3 | `s3://us-isob-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.8.3-v1.sh` | December 15, 2021 |
| 5.7.1 | `s3://us-isob-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.7.1-v1.sh` | December 15, 2021 |

| EMR release version | Associated bootstrap script as of December 2021 |
|---|---|
| 6.3.0 | 6.3.1 |
| 6.2.0 | 6.2.1 |
| 6.0.0 | 6.0.1 |
| 5.33.0 | 5.33.1 |
| 5.32.0 | 5.32.1 |
| 5.31.0 | 5.31.1 |
| 5.30.0 or 5.30.1 | 5.30.2 |

| EMR release version | Associated bootstrap script as of December 2021 |
| --- | --- |
| 5.29.0 | 5.29.0 |
| 5.28.0 | 5.28.1 |
| 5.27.0 | 5.27.1 |
| 5.24.0 | 5.24.1 |
| 5.23.0 | 5.23.1 |
| 5.21.0 or 5.21.1 | 5.21.2 |
| 5.20.0 | 5.20.1 |
| 5.19.0 | 5.19.1 |
| 5.18.0 | 5.18.1 |
| 5.17.0 or 5.17.1 | 5.17.2 |
| 5.16.0 | 5.16.1 |
| 5.15.0 | 5.15.1 |
| 5.14.0 or 5.14.1 | 5.14.2 |
| 5.13.0 | 5.13.1 |
| 5.12.0, 5.12.1, 5.12.2 | 5.12.3 |
| 5.11.0, 5.11.1, 5.11.2, 5.11.3 | 5.11.4 |
| 5.9.0 | 5.9.1 |
| 5.8.0, 5.8.1, 5.8.2 | 5.8.3 |
| 5.7.0 | 5.7.1 |

- Hunk is not available.

- MapR is not available.
- Debugging is not available.
- Amazon EC2 launches instances into a VPC instead of using the EC2-Classic platform. For more information, see Amazon EC2 and Amazon Virtual Private Cloud (VPC).
- Tez UI and YARN timeline server persistent application history interfaces are not available.
- EMR Notebooks is not available.
- Managed scaling is not available.
- The allocation strategy option for instance fleets is not available.
- The old Amazon EMR management console is the default console for AWS Secret Region.
- Docker containers are not available.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## How Command Line and API Access Differs for AWS Secret Region

Amazon EMR has a service-specific command line interface. For more information about the Amazon EMR Ruby Client, see AWS CLI.

To connect to Amazon EMR by using the command line or APIs, use the following endpoint:

- https://elasticmapreduce.us-isob-east-1.sc2s.sgov.gov

## Documentation for Amazon EMR

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Amazon EMR differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon EMR Management Guide
- Amazon EMR Release Guide
- Amazon EMR API Reference

# Amazon ElastiCache

Amazon ElastiCache is a web service that makes it easy to set up, manage, and scale distributed in-memory cache environments in the cloud. It provides a high performance, resizable, and cost-effective in-memory cache, while removing the complexity associated with deploying and managing a distributed cache environment.

**Topics**



## How ElastiCache Differs for AWS Secret Region

The implementation of ElastiCache is different for AWS Secret Region in the following ways:

- Reader endpoints are not available in AWS Secret Region.
- The following ElastiCache Cluster Clients are available:

| Cluster Client | Location | Documentation |
|---|---|---|
| Java | http://elasticache-downloads.s3-website.us-isob-east-1.sc2s.sgov.gov/ClusterClient/Java/AmazonElastiCacheClusterClient.zip | Using Auto Discovery |
| .NET | http://elasticache-downloads.s3-website.us-isob-east-1.sc2s.sgov.gov/ClusterClient/.NET/Amazon.ElastiCacheCluster.zip | Installing the ElastiCache Cluster Client for .NET |
| PHP 7.0 | http://elasticache-downloads.s3-website.us-isob-east-1.sc2s.sgov.gov/ClusterClient/PHP-7.0/latest-64bit | Installing the ElastiCache Cluster Client for PHP |

| Cluster Client | Location | Documentation |
| --- | --- | --- |
| PHP 5.6 | http://elasticache-downloads.s3-website.us-isob-east-1.sc2s.sgov.gov/ClusterClient/PHP-5.6/latest-64bit | Installing the ElastiCache Cluster Client for PHP |
| PHP 5.5 | http://elasticache-downloads.s3-website.us-isob-east-1.sc2s.sgov.gov/ClusterClient/PHP-5.5/latest-64bit<br><br>http://elasticache-downloads.s3-website.us-isob-east-1.sc2s.sgov.gov/ClusterClient/PHP-5.5/latest-32bit | Installing the ElastiCache Cluster Client for PHP |
| PHP 5.4 | http://elasticache-downloads.s3-website.us-isob-east-1.sc2s.sgov.gov/ClusterClient/PHP-5.4/latest-64bit<br><br>http://elasticache-downloads.s3-website.us-isob-east-1.sc2s.sgov.gov/ClusterClient/PHP-5.4/latest-32bit | Installing the ElastiCache Cluster Client for PHP |
| PHP 5.3 | http://elasticache-downloads.s3-website.us-isob-east-1.sc2s.sgov.gov/ClusterClient/PHP-5.3/latest-64bit<br><br>http://elasticache-downloads.s3-website.us-isob-east-1.sc2s.sgov.gov/ClusterClient/PHP-5.3/latest-32bit | Installing the ElastiCache Cluster Client for PHP |

- The following are the supported Amazon EC2 instance types for ElastiCache:

| Instance Family | Instance Types |
| --- | --- |
| General purpose | `cache.m4.large` \| `cache.m4.xlarge` \| `cache.m4.2xlarge` \| `cache.m4.4xlarge` \| `cache.m4.10xlarge` |
| | `cache.m5.large` \| `cache.m5.xlarge` \| `cache.m5.2xlarge` \| `cache.m5.4xlarge` \| `cache.m5.12xlarge` \| `cache.m5.24xlarge` |
| Memory optimized | `cache.t2.micro` \| `cache.t2.small` \| `cache.t2.medium` |
| | `cache.t3.micro` \| `cache.t3.small` \| `cache.t3.medium` |
| | `cache.r5.large` \| `cache.r5.xlarge` \| `cache.r5.2xlarge` \| `cache.r5.4xlarge` \| `cache.r5.12xlarge` \| `cache.r5.24xlarge` |

- Amazon EC2 launches instances into a VPC instead of using the EC2-Classic platform. For more information, see Amazon EC2 and Amazon Virtual Private Cloud (VPC).
- The following compliance programs are not supported:
  - ElastiCache for Redis FedRAMP Compliance
  - HIPAA Compliance
  - ElastiCache for Redis PCI DSS Compliance
- In-transit encryption is now available in AWS Secret Region.
- Global Datastores are not available in AWS Secret Region.
- Data tiering is not available in AWS Secret Region.
- PrivateLink feature is not available in AWS Secret Region.
- Role-Based Access Control (RBAC) is not supported in AWS Secret Region.
- Redis engine version 6.0 is not available, but supported Redis engine 6.2 includes all cumulative updates.
- Redis engine version 7.0 is not supported in AWS Secret Region.
- IAM Authentication is not supported in AWS Secret Region.
- Tagging is not available for Replication Groups.
- Amazon Resource Names (ARNs) and endpoints have different values.

- Only signature version 4 signing is supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with ElastiCache and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to ElastiCache by using the command line or APIs, use the following endpoint:

- https://elasticache.us-isob-east-1.sc2s.sgov.gov

## Documentation for ElastiCache

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how ElastiCache differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon ElastiCache User Guide
- Amazon ElastiCache API Reference

# Amazon EventBridge

Amazon EventBridge (formerly CloudWatch Events) is a serverless event bus service that makes it easy to connect your applications with data from a variety of sources. EventBridge delivers a stream of real-time data from your own applications, and AWS services and routes that data to targets such as Lambda. You can set up routing rules to determine where to send your data to build application architectures that react in real time to all of your data sources. EventBridge allows you to build event driven architectures, which are loosely coupled and distributed."

**Topics**



## How Amazon EventBridge Differs for AWS Secret Region

The implementation of Amazon EventBridge is different for AWS Secret Region in the following ways:

- API destinations are not supported.
- Archive and replay are not supported.
- AWS CloudFormation support is only available for EventBus, EventBusPolicy and Rule.
- Cross-Region event destinations are not supported.
- Cross-Region event sources are not supported.
- Sending events between event buses in the same account and Region is not supported.
- Dead-letter queues (DLQs) are not supported.
- Encryption using AWS KMS is not supported.
- Managed rules are not supported.
- Setting up partner event sources to receive events from Software-as-a-Service (SaaS) Partner applications and services is not supported.
- Amazon EventBridge Schema Registry is not supported in AWS Secret Region.
- Tags are not supported.
- EventBridge Pipes is not supported.
- The EventBridge Scheduler service is not supported.

# How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Amazon EventBridge and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Amazon EventBridge by using the command line or APIs, use the following endpoint:

- https://eventbridge.us-isob-east-1.sc2s.sgov.gov

## Documentation for Amazon EventBridge

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Amazon EventBridge differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon EventBridge User Guide
- Amazon EventBridge API Reference
- Amazon EventBridge section of AWS CLI Reference

# Amazon Data Firehose

Amazon Data Firehose is a fully managed service that delivers real-time streaming data to destinations such as Amazon Simple Storage Service (Amazon S3), Amazon OpenSearch Service (OpenSearch Service), Amazon Redshift, and others.

**Topics**



## How Firehose Differs for AWS Secret Region

The implementation of Firehose is different for AWS Secret Region in the following ways:

- Dynamic partitioning is NOT supported.
- Splunk isn't available as a destination.
- Third-party HTTP endpoint partners are not available as destinations.
- Writing to Firehose using CloudWatch Logs via subscription filters is not supported.
- Writing to Firehose using CloudWatch Events is not supported.
- Writing to Firehose using AWS IoT is not supported.
- Writing to Firehose using Kinesis Agent is not supported.
- Monitoring Firehose with the following CloudWatch metrics is not supported:
  - BytesPerSecondLimit
  - PutRequestsPerSecondLimit
  - RecordsPerSecondLimit
- When you are granting access to Amazon Data Firehose while using an Amazon Redshift destination, if your Amazon Redshift cluster is in a virtual private cloud (VPC), make sure to unblock the following Firehose IP addresses in the CIDR for:
  - : 7.23.112.0/27
  - : 7.26.175.0/27
  - : 7.23.xxx.0/27
- Record format conversion is not available.

# How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Firehose and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Firehose by using the command line or APIs, use the following endpoint:

- https://firehose.us-isob-east-1.sc2s.sgov.gov

## Documentation for Firehose

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Firehose differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon Data Firehose Developer Guide
- Amazon Data Firehose API Reference
- Firehose section of AWS CLI Reference

# Amazon S3 Glacier

S3 Glacier is a storage service optimized for infrequently used data, or "cold data." The service provides durable and extremely low-cost storage with security features for data archiving and backup.

**Topics**



## How S3 Glacier Differs for AWS Secret Region

The implementation of S3 Glacier is different for AWS Secret Region in the following ways:

- S3 Glacier Select is not available in AWS Secret Region.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with S3 Glacier and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to S3 Glacier by using the command line or APIs, use the following endpoint:

- https://glacier.us-isob-east-1.sc2s.sgov.gov

# Documentation for S3 Glacier

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how S3 Glacier differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon S3 Glacier Developer Guide
- S3 Glacier section of AWS CLI Reference

# AWS Health

AWS Health provides ongoing visibility into the state of your AWS resources, services, and accounts. The service gives you awareness and remediation guidance for resource performance or availability issues that may affect your applications that run on AWS. AWS Health provides relevant and timely information to help you manage events in progress, as well as be aware of and prepare for planned activities. The service delivers alerts and notifications triggered by changes in the health of AWS resources, so you get near-instant event visibility and guidance to help accelerate troubleshooting.

**Topics**



## How AWS Health Differs for AWS Secret Region

The implementation of AWS Health is different for AWS Secret Region in the following ways:

- AWS Health does not support tagging resources.
- The organizational view feature is currently not supported.
- You can navigate to the AWS Health Dashboard - Service health page to view the health of all AWS services without signing in to your AWS account.
- If you sign in to your AWS account, you can find events specific to your account and services in the **AWS Health Dashboard - Your account health**.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with AWS Health and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to AWS Health by using the command line or APIs, use the following endpoint:

- https://health.us-isob-east-1.sc2s.sgov.gov

## Documentation for AWS Health

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how AWS Health differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Health User Guide
- AWS Health API Reference
- AWS Health section of AWS CLI Reference

# AWS Identity and Access Management

AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources in AWS Secret Region. With IAM, you can create users and groups and grant or deny them permissions to access AWS resources in AWS Secret Region. By using the AWS Security Token Service, you can delegate access across AWS accounts using temporary, limited credentials.

**Topics**



## How IAM Differs for AWS Secret Region

The implementation of IAM is different for AWS Secret Region in the following ways:

- There is no concept of a "root" or "account" user or credentials. All AWS Secret Region users are IAM users, including the user who created the account.
- AWS Secret Region does not support adding multi-factor authentication (MFA) to IAM users or to the account. This includes both hardware and virtual MFA devices. The console does not include MFA options.
- For web identity federation, OpenID Connect (OIDC) identity providers (IdPs) Google, Facebook, or Amazon Cognito are not supported as built-in providers in AWS Secret Region. Also, all OIDC IdPs configured in AWS Secret Region require the certificate thumbprint to verify the IdP server certificate.
- The IAM control plane for the AWS Secret Region is located in the Secret-US-East Region. Each AWS Region has a completely independent instance of the IAM data plane. For more information, see Resilience in AWS Identity and Access Management.
- When you create a policy in the console, the **Visual editor** tab and the **JSON** tab supported in other regions are not yet available. Instead you can choose from the following options:
  - Copy an AWS Managed policy
  - Use the policy generator
  - Create a new policy using JSON
- You cannot upload and associate an X.509 certification with an individual IAM user. However, you can upload a server certificate to be associated with an account.

- AWS Secret Region supports two additional permissions that can be used in an IAM policy: `iam:GetAccountEmailAddress` and `iam:UpdateAccountEmailAddress`. If you grant a user the `GetAccountEmailAddress` permission, then the user can see the email address associated with the account. If you grant the `UpdateAccountEmailAddress` permission, then the user can change the email address associated with the account. If you grant your administrators permissions by using `iam:*` in a policy, then we recommend that you explicitly deny these two permissions to ensure that users cannot change your main account email address.

  The following shows an example policy that prevents users from changing the account email address:

  ```
  {
    "Version": "2012-10-17",
    "Statement": {
      "Effect": "Deny",
      "Action": "iam:UpdateAccountEmailAddress",
      "Resource": "*"
    }
  }
  ```

- Data about when an IAM entity (user, group, or role) last accessed an AWS service through permissions granted by an IAM policy is not available. For more information, see Service Last Accessed Data.
- Information about when a role was last used is not available. For more information, see View Role Access.
- You cannot use IAM tags to add metadata to the following IAM resources:
  - IAM SAML identity providers
  - Instance profiles
  - OpenID Connect (OIDC) identity providers
  - Policies
  - Server certificates
  - Virtual MFA devices

  For more information, see Tagging IAM Resources.
- Only some AWS services support service-linked roles in AWS Secret Region. For information about which services support using service-linked roles, see AWS Services That Work with IAM and look for the services that have **Yes** in the **Service-Linked Role** column. To learn whether the

service supports service-linked roles in a specific region, choose the **Yes** link to view the service-linked role documentation for that service.

- Amazon Resource Names (ARNs) and endpoints have different values.
- The identifier for a service principal includes the service name, and is usually in the following format:

  `service-name.amazonaws.com`

  However, some services might use the following format instead of or in addition to the usual format:

  `service-name.sc2s.sgov.gov`
- Only signature version 4 signing is supported.
- IAM Roles Anywhere is not supported in the AWS Secret Region. To learn more, see Providing access for non AWS workloads in the *IAM User Guide*.

- **IAM Access Analyzer**
  - **Policy generation** – Policy generation is not supported in AWS Secret Region. To learn more, see Generate policies based on access activity in the *IAM User Guide*.
  - **Policy validation** – IAM Access Analyzer policy validation checks are not available in AWS Secret Region. For more information, see IAM Access Analyzer policy validation.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with IAM and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to IAM by using the command line or APIs, use the following endpoint:

- https://iam.us-isob-east-1.sc2s.sgov.gov

# Documentation for IAM

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how IAM differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- IAM User Guide
- Using Temporary Security Credentials
- IAM section of AWS CLI Reference
- IAM API Reference
- AWS Security Token Service API Reference

# AWS Key Management Service

AWS Key Management Service (AWS KMS) is an encryption and key management service scaled for the cloud. AWS KMS keys and functionality are used by other AWS services, and you can use them to protect data in your own applications that use AWS.

**Topics**



## How AWS KMS Differs for AWS Secret Region

The implementation of AWS KMS is different for AWS Secret Region in the following ways:

- Many AWS services integrate with AWS KMS to protect their resources. For information about how AWS services in AWS Secret Region use AWS KMS, see the AWS Secret Region documentation for the AWS service.
- The AWS KMS Custom Key Stores feature is not available in AWS Secret Region. You cannot create AWS CloudHSM key stores or external key stores in AWS Secret Region.
- AWS KMS supports Transport Layer Security (TLS) 1.2—1.3 for endpoints in AWS Secret Region.
- AWS KMS supports Transport Layer Security (TLS) 1.2—1.3 for FIPS endpoints in AWS Secret Region.
- Multi-Region keys are not available in the AWS Secret Region. You cannot create multi-Region primary keys or multi-Region replica keys in any AWS Secret Region.
- The AWS KMS console feature that lets you filter KMS keys based on their tags is not supported.
- AWS KMS CloudFormation resources are limited in this Region. You cannot use an AWS CloudFormation template to create or manage asymmetric KMS keys, HMAC KMS keys, or multi-Region KMS keys (primary or replica). To use an AWS CloudFormation template to create a symmetric encryption (`SYMMETRIC_DEFAULT`) KMS key, you must specify a key policy.
- Amazon Resource Names (ARNs) and endpoints have different values.
- AWS KMS does not support the `KeyUsage` value of `KEY_AGREEMENT` for asymmetric keys in AWS Secret Region.
- AWS KMS does not support the DeriveSharedSecret operation in AWS Secret Region.

# How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with AWS KMS and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to AWS KMS by using the command line or APIs, use the following endpoint:

- https://kms.us-isob-east-1.sc2s.sgov.gov

## Documentation for AWS KMS

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how AWS KMS differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Key Management Service Developer Guide
- AWS Key Management Service API Reference
- AWS KMS section of AWS CLI Reference
- AWS Encryption SDK Developer Guide

# Amazon Kinesis Data Streams

Amazon Kinesis Data Streams is a managed service that scales elastically for real-time processing of streaming data at a massive scale. The service collects large streams of data records that can then be consumed in real time by multiple data-processing applications that can be run on Amazon EC2 instances.

**Topics**



## How Kinesis Differs for AWS Secret Region

The implementation of Kinesis is different for AWS Secret Region in the following ways:

- To help you build Amazon Kinesis Data Streams applications, you can download the following library:
  - Kinesis Client Library - Java
- Kinesis Data Streams On Demand does not support 1 GB/s increase in write capacity and 2GB/s read capacity.
- Only **Extended data retention** (retention of up to seven days) is supported. **Long-term data retention** (retention of more than seven days and up to 365 days) is not supported.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Kinesis and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Kinesis by using the command line or APIs, use the following endpoint:

- https://kinesis.us-isob-east-1.sc2s.sgov.gov

## Documentation for Kinesis

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Kinesis differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon Kinesis Developer Guide
- Kinesis section of AWS CLI Reference
- Amazon Kinesis API Reference

# AWS Lambda

AWS Lambda is is a compute service that lets you run code without provisioning or managing servers. Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second.

**Topics**



## How Lambda Differs for AWS Secret Region

The implementation of Lambda is different for AWS Secret Region in the following ways:

- The following event sources are not available in AWS Secret Region.
  - AWS IoT Button
  - Amazon Alexa Skills Kit
  - Amazon Alexa Smart Home
  - Amazon CloudFront
  - AWS CodeCommit
  - For the Amazon S3 event source, the following S3 Glacier event types are not available:
    - Restore from S3 Glacier initiated
    - Restore from S3 Glacier completed
  - Amazon Cognito Sync Trigger
  - Amazon DocumentDB
- The following event source mapping parameters are not available in AWS Secret Region:
  - FilterCriteria
  - ScalingConfig
  - TumblingWindowInSeconds
- The FunctionEventInvokeConfig parameter and the `PutFunctionEventInvokeConfig`, `UpdateFunctionEventInvokeConfig`, `DeleteFunctionEventInvokeConfig`,

`GetFunctionEventInvokeConfig`, and `ListFunctionEventInvokeConfigs` actions are not available in AWS Secret Region.

- Provisioned concurrency is available in AWS Secret Region, but Application Auto Scaling for provisioned concurrency is not available in AWS Secret Region.
- Event destinations are not available in AWS Secret Region.
- AWS Lambda Function URLs is not available in AWS Secret Region.
- Lambda support for container image is available in AWS Secret Region but Amazon ECR public gallery is not available in AWS Secret Region.
- Lambda does not support batch sizes greater than 10 for Lambda SQS triggers.
- Runtime management configuration is not available in AWS Secret Region.
- Lambda SnapStart is not available in AWS Secret Region.
- The Node.js 20 (`nodejs20.x`) runtime is not available in AWS Secret Region.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.
- Outbound IPv6 traffic is not supported in AWS Secret Region.
- Lambda doesn't support Lambda@Edge in AWS Secret Region.
- The Java 21 (`java21`) runtime is not available in AWS Secret Region.
- Multi-VPC connectivity for Amazon Managed Streaming for Apache Kafka event source mappings is not available in AWS Secret Region.
- The Amazon Linux 2023 (`provided.al2023`) runtime is not available in AWS Secret Region.
- Lambda Advanced Logging Controls are not available in AWS Secret Region.
- The Python 3.12 (`python3.12`) runtime is not available in AWS Secret Region.
- The Future runtime launch dates are not applicable in AWS Secret Region.
- The .NET 8 (`dotnet8`) runtime is not available in AWS Secret Region.
- The Ruby 3.3 (`ruby3.3`) runtime is not available in AWS Secret Region.
- Lambda Kinesis trigger cross-account access is not available in AWS Secret Region.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Lambda and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Lambda by using the command line or APIs, use the following endpoint:

- https://lambda.us-isob-east-1.sc2s.sgov.gov

### Documentation for Lambda

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Lambda differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Lambda Developer Guide
- AWS Lambda section of AWS CLI Reference

## AWS License Manager

AWS License Manager is a service for administrators who need a solution for managing, discovering, and reporting software license usage. Administrators can use License Manager to help prevent licensing violations, such as using more licenses than an agreement stipulates.

**Topics**

- How License Manager Differs for AWS Secret Region
- How Command Line and API Access Differs for AWS Secret Region
- Documentation for License Manager

### How License Manager Differs for AWS Secret Region

The implementation of License Manager is different for AWS Secret Region in the following ways:

- Cross-account license management is not supported in AWS Secret Region. This includes license sharing and automated discovery.
- Host resource groups are not supported in AWS Secret Region.
- AWS PrivateLink is not supported in AWS Secret Region.
- Managed entitlements are not supported in AWS Secret Region.
- Report generators are not supported in AWS Secret Region.
- User-based subscriptions are not supported in AWS Secret Region.
- Linux subscriptions are not supported in AWS Secret Region.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with License Manager and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to License Manager by using the command line or APIs, use the following endpoint:

- https://license-manager.us-isob-east-1.sc2s.sgov.gov

## Documentation for License Manager

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how License Manager differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- License Manager User Guide

- License Manager API Reference
- License Manager section of AWS CLI Reference

# AWS Marketplace

AWS Marketplace is a curated digital catalog that you can use to find, buy, deploy, and manage third-party software that you need to build solutions and run your operations. AWS Marketplace includes many software listings from categories such as security, networking, storage, IoT, business intelligence, database, and DevOps. AWS Marketplace also simplifies software licensing and procurement with flexible pricing options and multiple deployment methods.

**Topics**



## How AWS Marketplace Differs for AWS Secret Region

The implementation of AWS Marketplace is different for AWS Secret Region in the following ways:

- AWS Secret Region only supports Amazon Machine Image (AMI) and CloudFormation product types. Container, SaaS, SageMaker, professional services, and data products are not supported.
- The AWS Marketplace console is available at https://marketplace.sc2shome.sgov.gov/ . You can also subscribe through the AWS Marketplace or Amazon EC2 consoles.
- Private image builds are not available.
- Private marketplaces are not available.
- Private offers are available. However, private offers must be coordinated with the AWS Marketplace operations team; they are not available in the user interface.
- Procurement system integration is not available.
- Product reviews are not available.
- AWS Marketplace CLI and APIs are not available. However, you can use the Amazon EC2 and AWS CloudFormation CLIs to manipulate resources you subscribe to from AWS Marketplace.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## Documentation for AWS Marketplace

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how AWS Marketplace differs for AWS Secret Region, as

described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Marketplace Buyer Guide

# AWS Elemental MediaPackage

AWS Elemental MediaPackage is a just-in-time video packaging and origination service that delivers highly secure, scalable, and reliable video streams to a wide variety of playback devices. MediaPackage enriches audience experience with live and catch-up TV features.

**Topics**



## How MediaPackage Differs for AWS Secret Region

The implementation of MediaPackage is different for AWS Secret Region in the following ways:

- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.
- Amazon CloudFront distribution creation isn't available.
- Content delivery network (CDN) authorization isn't available.
- Content encryption digital rights management (DRM) isn't available. Encryption options are available in the console and API but will not work if enabled.
- CloudWatch events aren't available.
- Video on demand (VOD) isn't available.
- SPEKE isn't available.
- The MediaPackage VOD API isn't available.
- MediaPackage V2 features aren't available.
- The following Live APIs aren't available:
  - CreateOriginEndpoint.Authorization, CreateOriginEndpoint.CmafEncryption, CreateOriginEndpoint.DashEncryption, CreateOriginEndpoint.HLSEncryption, CreateOriginEndpoint.MssEncryption, CreateOriginEndpoint.SpekeKeyProvider, UpdateOriginEndpoint.Authorization, UpdateOriginEndpoint.CmafEncryption, UpdateOriginEndpoint.DashEncryption, UpdateOriginEndpoint.HLSEncryption, UpdateOriginEndpoint.MssEncryption, UpdateOriginEndpoint.SpekeKeyProvider

# How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with MediaPackage and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

MediaPackage has a service-specific command line interface. For more information about the , see AWS CLI.

To connect to MediaPackage by using the command line or APIs, use the following endpoint:

- https://mediapackage.us-isob-east-1.sc2s.sgov.gov

## Documentation for MediaPackage

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how MediaPackage differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Elemental MediaPackage User Guide
- AWS Elemental MediaPackage section of AWS CLI Reference
- AWS Elemental MediaPackage API Reference

# AWS Elemental MediaLive

AWS Elemental MediaLive is a real-time video service that lets you create live outputs for broadcast and streaming delivery. You use MediaLive to transform live video content from one format and package into other formats and packages. You typically need to transform the content in order to provide a format and package that a playback device can handle. Playback devices include smartphones and set-top boxes attached to televisions.

**Topics**



## How MediaLive Differs for AWS Secret Region

The implementation of MediaLive is different for AWS Secret Region in the following ways:

- AWS CloudFormation – You can't create MediaLive templates in AWS CloudFormation.
- CDI inputs – You can't create CDI inputs, even though this type appears in the API and on the console.
- Elemental Link inputs – AWS Elemental Link devices are not supported as inputs. You can't create an Elemental Link input.
- MediaConnect inputs – You can't create MediaConnect inputs, even though this type appears in the API and on the console. However, as soon as AWS Elemental MediaConnect is available in AWS Secret Region, MediaConnect inputs will be supported.
- MediaStore – AWS Elemental MediaStore is not supported as an upstream system for inputs, as a destination for output groups, or as the source for various assets that MediaLive uses.
- Multiplex output groups – You can't create multiplex output groups, even though this type appears in the API and on the console.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

# How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with MediaLive and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to MediaLive by using the command line or APIs, use the following endpoint:

- https://medialive.us-isob-east-1.sc2s.sgov.gov

## Documentation for MediaLive

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how MediaLive differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Elemental MediaLive User Guide
- AWS Elemental MediaLive API Reference
- MediaLive section of AWS CLI Reference

# Amazon OpenSearch Service

Amazon OpenSearch Service is a managed service that makes it easy to deploy, operate, and scale OpenSearch and legacy Elasticsearch OSS clusters in the AWS Cloud.

**Topics**



## How OpenSearch Service Differs for AWS Secret Region

The implementation of OpenSearch Service is different for AWS Secret Region in the following ways:

- The following OpenSearch versions are supported: 1.0, 1.1, 1.2, 1.3, 2.3, 2.5, 2.7, 2.9, 2.11
- Fewer instance types are available.
- Amazon Cognito for OpenSearch Dashboards (previously Kibana) is not supported.
- Multi-AZ domains are limited to two Availability Zones.
- Custom endpoints are not supported.
- Asynchronous search and Auto-Tune are not available.
- Amazon OpenSearch Ingestion is not supported.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with OpenSearch Service and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to OpenSearch Service by using the command line or APIs, use the following endpoint:

- https://opensearch.us-isob-east-1.sc2s.sgov.gov

## Documentation for OpenSearch Service

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how OpenSearch Service differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon OpenSearch Service Developer Guide
- Amazon OpenSearch Service section of the AWS CLI Reference

# AWS Outposts

AWS Outposts is a fully managed service that extends AWS infrastructure, services, APIs, and tools to customer premises. By providing local access to AWS managed infrastructure, AWS Outposts enables customers to build and run applications on premises using the same programming interfaces as in AWS Regions, while using local compute and storage resources for lower latency and local data processing needs.

**Topics**



## How AWS Outposts Differs for AWS Secret Region

The implementation of AWS Outposts is different for AWS Secret Region in the following ways:

- AWS Outposts servers is not available in AWS Secret Region.
- The AWS services that you can run on AWS Outposts depends on service availability in AWS Secret Region compared to other Regions.
- You cannot share Outpost resources through AWS Resource Access Manager or AWS Organizations in AWS Secret Region.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with AWS Outposts and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

# Documentation for AWS Outposts

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how AWS Outposts differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Outposts User Guide
- AWS Outposts API Reference
- AWS Outposts in the Amazon EC2 API Reference
- AWS Outposts section of AWS CLI Reference

# AWS ParallelCluster

AWS ParallelCluster is an AWS supported open source cluster management tool that helps you to deploy and manage high performance computing (HPC) clusters in the AWS Cloud.

**Topics**



## How AWS ParallelCluster Differs for AWS Secret Regions

The implementation of AWS ParallelCluster is different for AWS Secret Regions in the following ways:

- AWS ParallelCluster doesn't support use of the following AWS services and resources:
  - AWS Batch
  - Amazon FSx
  - EC2 Image Builder
  - AWS Secrets Manager
  - NICE DCV
  - Amazon File Cache
  - Amazon EC2 Capacity Blocks for ML
- AWS ParallelCluster only supports clusters that use Amazon Linux 2 x86_64 architecture.
- The AWS ParallelCluster API isn't available.
- The AWS ParallelCluster UI isn't available.
- Only the gp2 (default), `io1`, `sc1`, and `st1` Amazon Elastic Block Store volume types are available. All other Amazon EBS volume types aren't available. Set the size for the supported volume:

```
HeadNode:
  LocalStorage:
    RootVolume:
      Size: integer
```

```
      VolumeType: string
```

```
SlurmQueues:
  Name:
  ComputeSettings:
    LocalStorage:
      RootVolume:
        Size: integer
        VolumeType: string
```

- The following AWS ParallelCluster configuration properties and options aren't supported:
  - All Build Image configuration properties and options. The following example shows the `Dcv` setting to exclude from a cluster configuration:
  - NICE DCV properties and options.

    ```
    Dcv:
      Enabled: boolean
      Port: integer
      AllowedIps: string
    ```

  - All `awsbatch` (AWS Batch) configuration properties and options (Scheduler: awsbatch).
  - All configuration properties and options associated with `FsxLustre`, `FsxOntap`, `FsxOpenZfs`, and `Amazon FileCache` storage types. The following example shows the `StorageType` settings to exclude from a cluster configuration:

    ```
    SharedStorage:
      StorageType: FsxLustre, FsxOntap, FsxOpenZfs, FileCache
    ```

## How the pcluster CLI Differs for AWS Secret Regions

The implementation of the pcluster CLI is different for AWS Secret Regions in the following ways:

- The pcluster CLI can only be installed by using a stand-alone installer.
- The following pcluster commands aren't supported:
  - `pcluster build-image`
  - `pcluster delete-image`
  - `pcluster export-image-logs`

- `pcluster get-image-log-events`
- `pcluster get-image-stack-events`
- `pcluster list-images`
- `pcluster dcv-connect`

- The following AWS ParallelCluster configuration properties and options aren't supported for `pcluster configure`, `pcluster create-cluster`, and `pcluster update-cluster`:
  - All Build Image configuration properties and options.
  - NICE DCV properties and options.

    ```
    Dcv:
      Enabled: boolean
      Port: integer
      AllowedIps: string
    ```

  - All `awsbatch` (AWS Batch) configuration properties and options (Scheduler: awsbatch).
  - All configuration properties and options associated with `FsxLustre`, `FsxOntap`, `FsxOpenZfs`, and `Amazon FileCache` storage types. The following example shows the `StorageType` settings to exclude from a cluster configuration:

    ```
    SharedStorage:
      StorageType: FsxLustre, FsxOntap, FsxOpenZfs, FileCache
    ```

## Documentation for AWS ParallelCluster

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how AWS ParallelCluster differs for AWS Secret Regions, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Regions. There are other differences, such as links, endpoints, and screen-shots.

- AWS ParallelCluster User Guide

# AWS Pricing Calculator

You can use AWS Pricing Calculator to explore AWS services and create an estimate for the cost of your AWS use cases. You can model your solutions before building them, explore the price points and calculations behind your estimate, and find the available instance types and contract terms that meet your needs. This enables you to make informed decisions about using AWS. You can plan your AWS costs and usage or price out setting up a new set of instances and services.

AWS Pricing Calculator is useful both for people who have never used AWS and for those who want to reorganize or expand their AWS usage. You don't need any experience with the cloud or AWS to use AWS Pricing Calculator.

**Topics**



## How AWS Pricing Calculator Differs for AWS Secret Region

The implementation of AWS Pricing Calculator is different for AWS Secret Region in the following ways:

- The Windows Server and SQL Server calculator is not available in AWS Secret Region.

## Documentation for AWS Pricing Calculator

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how AWS Pricing Calculator differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Pricing Calculator User Guide

# Amazon Redshift

Amazon Redshift is a fast, fully managed, petabyte-scale data warehouse service that makes it simple and cost-effective to efficiently analyze all your data using your existing business intelligence tools. It is optimized for datasets ranging from a few hundred gigabytes to a petabyte or more.

**Topics**



## How Amazon Redshift Differs for AWS Secret Region

The implementation of Amazon Redshift is different for AWS Secret Region in the following ways:

- The following features are not available:
  - Concurrency scaling
  - Redshift-managed VPC endpoints
  - Amazon Redshift scheduler
  - Cross-Region snapshot copy
  - Amazon Redshift Data API
  - Integrating with an AWS Partner
  - Cluster relocation
  - Data sharing
  - Amazon Redshift Spectrum
  - Amazon Redshift Advisor
  - Amazon Redshift query editor

- All Amazon Redshift clusters must be launched in an Amazon VPC.
- Since AWS Secret Region operates as a single air-gapped region, snapshot copy is not supported.

- If you want Amazon Redshift to write logs to an Amazon S3 bucket, the bucket must have a policy that uses `702190854255` for the Amazon Redshift Account ID. For more information, see Managing Log Files in the *Amazon Redshift Management Guide*.

  The following shows an example of a bucket policy that enables audit logging for AWS Secret Region, where *`BucketName`* is a placeholder for your bucket name:

```
{
    "Statement": [
        {
            "Sid": "Put bucket policy needed for audit logging",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws-iso-b:iam::702190854255:user/logs"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws-iso-b:s3:::BucketName/*"
        },
        {
            "Sid": "Get bucket policy needed for audit logging ",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws-iso-b:iam::702190854255:user/logs"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws-iso-b:s3:::BucketName"
        }
    ]
}
```

- To connect to Amazon Redshift with SSL, you must download the public key from https://s3.us-isob-east-1.sc2s.sgov.gov/redshift-downloads/redshift-ssl-ca-cert.pem. For more information, see Configure Security Options for Connections.
- If you want to set up a JDBC or ODBC connection, you can download and install the appropriate driver from the following locations:

| Driver | Driver Location | Documentation |
| --- | --- | --- |
| JDBC 4.2-compatible | https://redshift-downloads.s3.us-isob-east-1.sc2s.sgov.gov/drivers/jd | Configure a JDBC Connection |

| Driver | Driver Location | Documentation |
| --- | --- | --- |
| | bc/2.1.0.11/redshift-jdbc42-2.1.0.11.jar | |
| ODBC driver on Windows | https://redshift-downloads.s3.us-isob-east-1.sc2s.sgov.gov/drivers/odbc/2.0.0.1/AmazonRedshiftODBC64-2.0.0.1.msi | Install and Configure the Amazon Redshift ODBC Driver on Microsoft Windows Operating Systems |
| ODBC driver on Linux | https://redshift-downloads.s3.us-isob-east-1.sc2s.sgov.gov/drivers/odbc/2.0.0.1/AmazonRedshiftODBC64-2.0.0.1.x86_64.rpm | Install the Amazon Redshift ODBC Driver on Linux Operating Systems |
| ODBC driver on Mac OS X | https://redshift-downloads.us-isob-east-1.sc2s.sgov.gov/drivers/odbc/1.4.62.1000/AmazonRedshiftODBC-1.4.62.1000.dmg | Install the Amazon Redshift ODBC Driver on Mac OS X |

- If you want to perform the tutorials in the Amazon Redshift documentation, you must download the sample data from the following locations:

| Sample Data | Bucket Location | Documentation |
| --- | --- | --- |
| Tickit | s3://awssampledbusisobeast1/tickit/ | Step 5: Load Sample Data from Amazon S3 |
| Resize | s3://awssampledbusisobeast1/resize/ | Step 5: Copy Post-Snapshot Data from the Source to the Target Cluster |
| Ssbgz | s3://awssampledbusisobeast1/ssbgz/ | Step 1: Create a Test Data Set |
| Load | s3://awssampledbusisobeast1/load/ | Step 5: Run the COPY Commands |

- You cannot use an on-premises hardware security module (HSM) to generate and manage your Amazon Redshift cluster key. For more information about HSM, see Hardware Security Modules.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Amazon Redshift and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Amazon Redshift by using the command line or APIs, use the following endpoint:

- https://redshift.us-isob-east-1.sc2s.sgov.gov

## Documentation for Amazon Redshift

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Amazon Redshift differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon Redshift Getting Started Guide
- Amazon Redshift Management Guide
- Amazon Redshift Database Developer Guide
- Amazon Redshift section of AWS CLI Reference
- Amazon Redshift API Reference

# Amazon Relational Database Service

Amazon Relational Database Service (Amazon RDS) is a service that makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while managing time-consuming database administration tasks.

- The following database engines are supported on Amazon RDS:
  - MySQL
  - MariaDB
  - PostgreSQL
  - Oracle
  - Microsoft SQL Server

**Topics**



## How Amazon RDS Differs for AWS Secret Region

The implementation of Amazon RDS is different for AWS Secret Region in the following ways:

**Oracle**

- The Bring Your Own License (BYOL) model is the only supported license model for Oracle on Amazon RDS.
- Amazon EFS integration is not available for Oracle in AWS Secret Region.

**MariaDB, MySQL, and PostgreSQL**

- RDS Proxy is not available.
- To connect to a MySQL or PostgreSQL DB instance with SSL, you must download the public key from https://s3.us-isob-east-1.sc2s.sgov.gov/rds-downloads/rds-combined-ca-bundle.pem. For more information, see Using SSL with a MySQL DB Instance or Using SSL with a PostgreSQL DB Instance.

- Amazon RDS Extended Support isn't available.

### Microsoft SQL Server

- SQL Server Web and Express editions aren't available.
- For SQL Server Enterprise Edition, all supported DB engine versions are available on the db.m5 and db.r5 DB instance classes.
- For SQL Server Standard Edition, all supported DB engine versions are available on the db.m5, db.r5 and db.t3 DB instance classes.
- Native backup and restore is supported for SQL Server, but only full backups and restores. Differential backups and restores, and log restores aren't supported. Backup compression isn't supported.
- Publishing database logs to Amazon CloudWatch Logs is not supported.
- The SQL Server Analysis Services option is not available.
- The SQL Server Integration Services option is not available.
- The SQL Server Reporting Services option is not available.
- Read replicas for SQL Server are not supported.
- RDS Proxy is not available.

### General Differences

- Engine version support is different from the commercial Regions. To list the supported engine versions for a specific DB engine, run the following CLI command:

  ```
  aws rds describe-db-engine-versions --engine engine --query "*[].
  {Engine:Engine,EngineVersion:EngineVersion}" --output text
  ```

  For example, to list the supported engine versions for RDS for MySQL, run the following CLI command:

  ```
  aws rds describe-db-engine-versions --engine mysql --query "*[].
  {Engine:Engine,EngineVersion:EngineVersion}" --output text
  ```

- Since AWS Secret Region uses a unique certificate authority (CA), update your DB instances for AWS Secret Region to use the Region-specific certificate identified by `rds-ca-2021` in

DescribeCertificates calls as soon as possible. The remaining instructions described in the SSL Certificate Rotation topic are the same, except for the certificate identifier.

- Since AWS Secret Region operates as a single air-gapped Region, cross-Region features are not supported, such as DB snapshot-copying across Regions and read replication across multiple Regions.
- Performance Insights for Amazon RDS isn't supported.
- The list of available DB instance classes is at Database Instance Classes.
- AWS Secret Region uses the following time block from which the default backups windows are assigned.

| Region | Time Block |
| --- | --- |
| us-isob-east-1 | 03:00-11:00 UTC |

- The AWS service principal for Amazon RDS is `rds.sc2s.sgov.gov`.
- Amazon EC2 launches instances into a VPC instead of using the EC2-Classic platform. For more information, see Amazon EC2 and Amazon Virtual Private Cloud (VPC).
- Since AWS Secret Region is a VPC-only Region, Amazon RDS DB instances must use existing VPC security groups. Amazon RDS APIs, such as CreateDBSecurityGroup and AWS::RDS::DBSecurityGroup do not apply in AWS Secret Region. Instead, create VPC security groups directly in Amazon EC2 using CreateSecurityGroup.
- Amazon RDS cannot create an encrypted copy of a snapshot of an unencrypted DB instance.
- Database activity streams aren't supported.
- Encryption at rest isn't supported for the db.t2.micro, db.t2.small and db.t2.medium instance classes.
- The RDS PostgreSQL S3 import feature is only supported for version 10.11 and later 10 versions, version 11.7 and later 11 versions, and all 12.1 or later versions.
- Storage autoscaling isn't supported.
- S3 export isn't supported.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.
- Size-flexible reserved DB instances aren't supported.
- Kerberos authentication is only supported for RDS for MySQL DB instances.

- Kerberos authentication isn't supported in the RDS console.
- The Blue/Green Deployments feature isn't available.
- The Secrets Manager integration feature isn't available.
- Some older minor DB engine versions don't support the latest generation DB instance classes.
- Amazon RDS Custom is not available in AWS Secret Region.
- Copying an option group isn't available.
- Events in the security patching event category aren't available.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Amazon RDS and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Amazon RDS by using the command line or APIs, use the following endpoint:

- https://rds.us-isob-east-1.sc2s.sgov.gov

## Documentation for Amazon RDS

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Amazon RDS differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- MySQL on Amazon RDS
- MariaDB on Amazon RDS
- Oracle on Amazon RDS

- PostgreSQL on Amazon RDS
- Microsoft SQL Server on Amazon RDS
- Amazon RDS section of AWS CLI Reference
- Amazon RDS API Reference

# AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) is a service that lets you share resources that you own with any AWS account.

**Topics**



## How AWS RAM differs for AWS Secret Region

The implementation of AWS RAM is different for AWS Secret Region in the following ways:

- AWS Organizations is currently not available in AWS Secret Region. Therefore, you cannot share resources with an organization or organizational units (OUs) in AWS Organizations.
- AWS RAM on AWS Outposts is not yet supported.
- The AWS RAM implementation in AWS Secret Region supports resource sharing for only some AWS services and resource types. To confirm which shareable resource types that appear in the **Resource type** column are supported in AWS Secret Region, do any of the following:
  - In the AWS RAM management console, open the Permissions Library page. You can share only those resource types that appear in the **Resource type** column.
  - In the AWS CLI, use the `list-resource-types` command.
  - In an AWS SDK, use the `ListResourceTypes` API operation.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with AWS RAM and other AWS services through the command line. For more information, see AWS CLI .

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region .

To connect to AWS RAM by using the command line or APIs, use the following endpoint:

- https://ram.us-isob-east-1.sc2s.sgov.gov

## Documentation for AWS RAM

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how AWS RAM differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS RAM for AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Resource Access Manager User Guide
- AWS RAM section of AWS CLI Reference
- AWS Resource Access Manager API Reference

# AWS Resource Groups

AWS Resource Groups provides the ability to group your AWS resources so that you manage multiple resources as a single entity. Resource groups can be one of two types:

- **Tag-based** – All resources in the account that have the specified tag key and value are members of the group.
- **AWS CloudFormation stack-based** – All resources that are created as part of the specified AWS CloudFormation stack are members of the group.

**Topics**



## How Resource Groups Differs for AWS Secret Region

The implementation of Resource Groups is different for AWS Secret Region in the following ways:

- Groups can include resources of only those types where the associated AWS service is also supported in the AWS Secret Region.
- Service-linked resource groups are not supported. This means that you can't attach a service configuration to the resource group in the AWS Secret Region.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.
- Group lifecycle events are not supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Resource Groups and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Resource Groups by using the command line or APIs, use the following endpoint:

- https://resourcegroups.us-isob-east-1.sc2s.sgov.gov

## Documentation for Resource Groups

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Resource Groups differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Resource Groups User Guide
- AWS Resource Groups API Reference

# AWS Resource Groups Tagging API

AWS Resource Groups Tagging API provides API operations for tagging AWS resources. A tag is a label that you can attach to your AWS resources. A tag consists of a key and a value, both of which you define.

### Topics

- How Resource Groups Tagging API Differs for AWS Secret Region
- How Command Line and API Access Differs for AWS Secret Region
- Documentation for Resource Groups Tagging API

## How Resource Groups Tagging API Differs for AWS Secret Region

The implementation of Resource Groups Tagging API is different for AWS Secret Region in the following ways:

- You can tag only resources for AWS services that are available in the AWS Secret Region Region.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Resource Groups Tagging API and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Resource Groups Tagging API by using the command line or APIs, use the following endpoint:

- https://resourcegroupstaggingapi.us-isob-east-1.sc2s.sgov.gov

## Documentation for Resource Groups Tagging API

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Resource Groups Tagging API differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Resource Groups Tagging API API Reference

# Amazon Route 53

Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed to give developers an extremely reliable and cost effective way to route end users to applications in AWS Secret Region by translating names like www.example.com into the numeric IP addresses like 192.0.2.1 that computers use to connect to each other. You can also use Route 53 to configure DNS health checks to route traffic to healthy endpoints or to independently monitor the health of your application and its endpoints.

**Topics**



## How Route 53 Differs for AWS Secret Region

The implementation of Route 53 is different for AWS Secret Region in the following ways:

- The AWS console for Route 53 is supported, with the following exceptions:
  - The dashboard is not included.
  - The domain registration console is not included.
  - The traffic flow console is not included.
- Registering domain names is not supported.
- DNSSEC is not supported.
- Traffic flow is not supported.
- Route 53 Resolver Firewall is not supported.
- Route 53 alias records are supported as follows:
  - You can alias to another record in the same hosted zone.
  - You can alias to Elastic Load Balancing load balancers.
  - You can alias to a VPC endpoint.
  - You can alias to a Network Load Balancer but only by using the AWS CLI and SDK.
  - You can't alias to other AWS resources, such as S3 buckets.
- You can't create records that use geolocation, geoproximity, latency, or IP-based routing policies. This applies both to public and private hosted zones.

- Latency-based health checks are not supported. This feature is controlled by the **Evaluate target health** field.
- DNS query logging is not supported.
- IPv6 endpoint types are not supported.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.
- AWS-managed prefix lists are not available.
- Route 53 Profiles are not available.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Route 53 and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Route 53 by using the command line or APIs, use the following endpoint:

- https://route53.sc2s.sgov.gov

If you're using the AWS CLI to access Route 53, include the `region` parameter, for example:

```
$ aws route53 list-hosted-zones --region us-isob-east-1 --endpoint-url
https://route53.sc2s.sgov.gov
```

You can omit the `region` parameter from CLI commands if you specify the default region name in your config file:

```
region = us-isob-east-1
```

In addition, if you have the latest version of the AWS CLI, you can omit the `endpoint-url` parameter.

# Documentation for Route 53

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Route 53 differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon Route 53 Developer Guide
- Amazon Route 53 API Reference
- Route 53 section of AWS CLI Reference

# Amazon SageMaker

Amazon SageMaker is an AWS service that enables developers to build, train, and deploy machine learning models in a managed environment.

**Topics**



## How SageMaker Differs for AWS Secret Region

The implementation of SageMaker is different for AWS Secret Region in the following ways:

- Only the following features are available in the AWS Secret Region.
  - Notebook instances – Only example notebooks that are confirmed to work in AWS Secret Region are available through the notebook instances.
  - Training – Fast file input mode is not supported.
  - Hosting – The following features are not supported:
    - Auto scaling
    - The following endpoint parameters for large model inference are not supported:
      - VolumeSizeInGB
      - ContainerStartupHealthCheckTimeoutInSeconds
      - ModelDataDownloadTimeoutInSeconds
      - Asynchronous Inference
      - Serverless Inference
  - Batch transform
  - SageMaker Neo – Only PyTorch version 1.12 and TensorFlow version 2.9 are supported.
  - SageMaker Ground Truth – The following features are not supported:
    - Amazon Mechanical Turk workforce.
    - The automated segmentation (auto-segmentation) tool is not included when you create an image semantic segmentation labeling job.
    - Amazon CloudWatch Logs. CloudWatch Logs logs for labeling jobs do not include worker metrics.

  - AWS Deep Learning Containers.
  - Model tuning (HPO).
  - SageMaker Search – Search does not return results for SageMaker features that are not available in AWS Secret Region.
- Internet Explorer is not supported on the SageMaker Console
- Only TensorFlow versions 1.12, 1.13 and 1.14 are supported.
- Only Reinforcement Learning TensorFlow Ray 0.6.5 and Coach 0.11.1 are supported.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with SageMaker and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to SageMaker by using the command line or APIs, use the following endpoint:

- https://sagemaker.us-isob-east-1.sc2s.sgov.gov

## Documentation for SageMaker

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how SageMaker differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon SageMaker Developer Guide
- SageMaker API Reference

- SageMaker section of AWS CLI Reference

# AWS Serverless Application Model

The AWS Serverless Application Model (AWS SAM) is an open-source framework that enables you to build serverless applications on AWS. It provides you with a template specification to define your serverless application, and a command line interface (CLI) tool.

**Topics**



## How AWS SAM Differs for AWS Secret Region

The implementation of AWS SAM is different for AWS Secret Region in the following ways:

- The installation links for the AWS SAM CLI are not directly available to hosts in the region. You must manually copy the AWS SAM CLI installation files to a host in the region in order to install the AWS SAM CLI.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with AWS SAM and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

# Documentation for AWS SAM

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how AWS SAM differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Serverless Application Model Developer Guide
- AWS SAM Specification

# AWS Secrets Manager

AWS provides the service AWS Secrets Manager for easier management of secrets. *Secrets* can be database credentials, passwords, third-party API keys, and even arbitrary text. You can store and control access to these secrets centrally by using the Secrets Manager console, the Secrets Manager command line interface (CLI), or the Secrets Manager API and SDKs.

**Topics**



## How Secrets Manager Differs for AWS Secret Region

The implementation of Secrets Manager is different for AWS Secret Region in the following ways:

- Multi-Region secrets are not supported.
- AAAA IPv6 records for the Secrets Manager endpoint are not supported.
- The PrivateLink VPC Endpoint service name is `com.amazonaws.<region string>.secretsmanager`
- FIPS endpoints are not supported.
- Secret Rotation in the console for Amazon DocumentDB credentials is not supported.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.
- AWS Config managed rules for Secrets Manager are not supported.
- Secrets Manager API BatchGetSecretValue is not supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Secrets Manager and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Secrets Manager by using the command line or APIs, use the following endpoint:

- https://secretsmanager.us-isob-east-1.sc2s.sgov.gov

## Documentation for Secrets Manager

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Secrets Manager differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Secrets Manager User Guide
- AWS Secrets Manager API Reference
- Secrets Manager section of AWS CLI Reference

# AWS Security Hub

AWS Security Hub (Security Hub) is an AWS service that provides you with a comprehensive view of your security state in AWS and helps you assess your AWS environment against security industry standards and best practices.

Security Hub collects security data across AWS accounts, integrated AWS services, and supported third-party products and helps you analyze your security trends and identify the highest priority security issues.

To help you manage your security state, Security Hub supports multiple security standards, such as AWS Foundational Security Best Practices, Center for Internet Security (CIS) AWS Foundations Benchmark, and Payment Card Industry Data Security Standard (PCI DSS). Each standard includes several security controls, each of which represents a security best practice. Security Hub runs checks against security controls and generates control findings to help you assess your compliance against security best practices.

Security Hub also offers automation rules and an integration with Amazon EventBridge to help you triage and remediate security issues.

**Topics**



## How Security Hub Differs for AWS Secret Region

The implementation of Security Hub is different for AWS Secret Region in the following ways:

- The integration between Security Hub and AWS Organizations isn't available. Features that depends on this integration, including central configuration, aren't available.
- The AWS Resource Tagging Standard and the controls that apply exclusively to this standard aren't available.
- To receive Security Hub announcements through Amazon Simple Notification Service (Amazon SNS), use the following SNS topic ARN: `arn:aws-iso-b:sns:us-isob-east-1:047235868427:SecurityHubAnnouncements`

- The security controls in the following section aren't available. For a list of all Security Hub controls, see the Security Hub controls reference.

## Controls that are unavailable in AWS Secret Region

- ACM.1
- ACM.2
- ACM.3
- Account.1
- Account.2
- APIGateway.1
- APIGateway.2
- APIGateway.3
- APIGateway.4
- APIGateway.5
- APIGateway.8
- APIGateway.9
- AppSync.2
- AppSync.4
- AppSync.5
- Athena.2
- Athena.3
- AutoScaling.2
- AutoScaling.3
- AutoScaling.6
- AutoScaling.9
- AutoScaling.10
- Backup.1
- Backup.2
- Backup.3
- Backup.4

- Backup.5
- CloudFormation.2
- CloudFront.1
- CloudFront.3
- CloudFront.4
- CloudFront.5
- CloudFront.6
- CloudFront.7
- CloudFront.8
- CloudFront.9
- CloudFront.10
- CloudFront.12
- CloudFront.13
- CloudFront.14
- CloudWatch.17
- CloudTrail.9
- CodeArtifact.1
- CodeBuild.1
- CodeBuild.2
- CodeBuild.3
- CodeBuild.4
- DataFirehose.1
- Detective.1
- DMS.1
- DMS.2
- DMS.3
- DMS.4
- DMS.5
- DMS.6
- DMS.7

- DMS.8
- DMS.9
- DMS.10
- DMS.11
- DMS.12
- DocumentDB.1
- DocumentDB.2
- DocumentDB.3
- DocumentDB.4
- DocumentDB.5
- DynamoDB.3
- DynamoDB.4
- DynamoDB.5
- DynamoDB.6
- DynamoDB.7
- EC2.4
- EC2.14
- EC2.19
- EC2.21
- EC2.22
- EC2.23
- EC2.24
- EC2.25
- EC2.28
- EC2.33
- EC2.34
- EC2.35
- EC2.36
- EC2.37
- EC2.38

- EC2.39
- EC2.40
- EC2.41
- EC2.42
- EC2.43
- EC2.44
- EC2.45
- EC2.46
- EC2.47
- EC2.48
- EC2.49
- EC2.50
- EC2.51
- EC2.52
- EC2.53
- EC2.54
- ECR.1
- ECR.2
- ECR.3
- ECR.4
- ECS.1
- ECS.2
- ECS.3
- ECS.4
- ECS.5
- ECS.8
- ECS.9
- ECS.10
- ECS.12
- ECS.13

- ECS.14
- ECS.15
- EFS.2
- EFS.3
- EFS.4
- EFS.5
- EFS.6
- EKS.2
- EKS.3
- EKS.6
- EKS.7
- EKS.8
- ELB.1
- ELB.2
- ELB.4
- ELB.5
- ELB.6
- ELB.7
- ELB.8
- ELB.10
- ELB.12
- ELB.13
- ELB.14
- ELB.16
- ElastiCache.2
- ElastiCache.3
- ElastiCache.4
- ElastiCache.5
- ElastiCache.6
- ElastiCache.7

- ElasticBeanstalk.1
- ElasticBeanstalk.2
- ElasticBeanstalk.3
- EMR.1
- EMR.2
- ES.5
- ES.6
- ES.7
- ES.8
- ES.9
- EventBridge.2
- EventBridge.3
- EventBridge.4
- FSx.1
- FSx.2
- GlobalAccelerator.1
- Glue.1
- GuardDuty.1
- GuardDuty.2
- GuardDuty.3
- GuardDuty.4
- IAM.18
- IAM.23
- IAM.24
- IAM.25
- IAM.26
- IAM.27
- IAM.28
- IoT.1
- IoT.2

- IoT.3
- IoT.4
- IoT.5
- IoT.6
- Kinesis.1
- Kinesis.2
- KMS.2
- KMS.3
- Lambda.5
- Lambda.6
- Macie.1
- Macie.2
- MQ.2
- MQ.3
- MQ.4
- MQ.5
- MQ.6
- MSK.1
- MSK.2
- Neptune.1
- Neptune.2
- Neptune.3
- Neptune.4
- Neptune.5
- Neptune.6
- Neptune.7
- Neptune.8
- Neptune.9
- NetworkFirewall.1
- NetworkFirewall.2

- NetworkFirewall.3
- NetworkFirewall.4
- NetworkFirewall.5
- NetworkFirewall.6
- NetworkFirewall.7
- NetworkFirewall.8
- NetworkFirewall.9
- Opensearch.1
- Opensearch.2
- Opensearch.3
- Opensearch.4
- Opensearch.5
- Opensearch.6
- Opensearch.7
- Opensearch.8
- Opensearch.9
- Opensearch.10
- Opensearch.11
- PCA.1
- RDS.16
- RDS.17
- RDS.18
- RDS.19
- RDS.20
- RDS.21
- RDS.22
- RDS.23
- RDS.24
- RDS.25
- RDS.26

- RDS.27
- RDS.28
- RDS.29
- RDS.30
- RDS.31
- RDS.32
- RDS.33
- RDS.34
- RDS.35
- Redshift.3
- Redshift.4
- Redshift.8
- Redshift.9
- Redshift.11
- Redshift.12
- Redshift.13
- Redshift.14
- Redshift.15
- Route53.1
- Route53.2
- S3.1
- S3.7
- S3.8
- S3.10
- S3.11
- S3.12
- S3.13
- S3.15
- S3.19
- S3.20

- S3.22
- S3.23
- SageMaker.1
- SageMaker.2
- SageMaker.3
- SageMaker.4
- SES.1
- SES.2
- SecretsManager.1
- SecretsManager.2
- SecretsManager.5
- ServiceCatalog.1
- SNS.3
- SQS.1
- SQS.2
- SSM.1
- SSM.2
- SSM.3
- StepFunctions.1
- StepFunctions.2
- Transfer.1
- Transfer.2
- WAF.1
- WAF.2
- WAF.3
- WAF.4
- WAF.6
- WAF.7
- WAF.8
- WAF.10

- WAF.11
- WAF.12

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Security Hub and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Security Hub by using the command line or APIs, use the following endpoint:

- https://securityhub.us-isob-east-1.sc2s.sgov.gov

## Documentation for Security Hub

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Security Hub differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Security Hub User Guide
- AWS Security Hub API Reference
- Security Hub section of AWS CLI Reference

# Amazon Simple Storage Service

Amazon Simple Storage Service (Amazon S3) is storage for the cloud. It provides a simple web service interface you can use to store and retrieve any amount of data, at any time, from anywhere on the network. It gives any developer access to the same highly scalable, reliable, secure, fast, inexpensive infrastructure solution that Amazon uses in its public cloud.

**Topics**



## How Amazon S3 Differs for AWS Secret Region

The implementation of Amazon S3 is different for AWS Secret Region in the following ways:

- When you upload or copy an object to Amazon S3, your data will always be encrypted.
- Objects are encrypted using one of the following encryption types:
  - Server-side encryption with Amazon S3-managed encryption keys (SSE-S3)
  - Server-side encryption with AWS KMS encryption keys (SSE-KMS)
  - Server-side encryption with customer-provided encryption keys (SSE-C)
  - Dual-layer server-side encryption with AWS KMS encryption keys (DSSE-KMS)
- The encryption type that is selected depends on different factors:

| Operation | Server-Side Encryption |
| --- | --- |
| Upload an object to Amazon S3 without specifying the SSE-S3, SSE-KMS, DSSE-KMS, or SSE-C options. | If the bucket is configured for default encryption, the object is encrypted as per the bucket configuration (SSE-S3, SSE-KMS, DSSE-KMS). Otherwise, the object is encrypted with SSE-S3. |
| Upload an object to Amazon S3 and specify SSE-SS3 option. | The object is encrypted with SSE-S3. |

| Operation | Server-Side Encryption |
| --- | --- |
| Upload an object to Amazon S3 and specify the SSE-KMS option. | The object is encrypted with SSE-KMS. |
| Upload an object to Amazon S3 and specify the DSSE-KMS option. | The object is encrypted with DSSE-KMS. |
| Upload an object to Amazon S3 and specify the SSE-C option. | The object is encrypted with SSE-C. |
| Copy an object within Amazon S3 and attempt to change an SSE-S3, SSE-KMS, DSSE-KMS, or SSE-C protected object to use no encryption. | The object is copied and if the bucket is configured for default encryption, the object is encrypted as per the bucket configuration (SSE-S3, SSE-KMS, or DSSE-KMS). Otherwise, the object is encrypted with SSE-S3. |
| Copy an object within Amazon S3 and attempt to change from SSE-S3, SSE-KMS, DSSE-KMS, or SSE-C encryption to SSE-S3, SSE-KMS, DSSE-KMS, or SSE-C encryption. | The object is copied using the requested encryption type. |

- Object copy operations are permitted within AWS Secret Region; however, cross-region copy operations are not supported because AWS Secret Region operates as a single air-gapped region. For more information, see Copying Objects.
- Amazon S3 Replication is available in AWS Secret Region.
- Amazon S3 objects are associated with the following storage classes:
  - DEEP_ARCHIVE
  - GLACIER
  - GLACIER_IR
  - INTELLIGENT_TIERING
  - ONEZONE_IA
  - STANDARD
  - STANDARD_IA

  For more information, see Storage Classes.

- Objects restored from Glacier storage class are billed at the Standard storage rates, not RRS.
- If you are using Amazon S3 event notifications, the Reduced Redundancy Storage (RRS) object lost event is not available. For more information, see Configuring Amazon S3 Event Notifications.
- Static website hosting using Amazon S3 is available to users in AWS Secret Region. The special case of apex domain website hosting is unsupported because it requires the Route 53 service, which is not available in AWS Secret Region. For more information about static website hosting, see Hosting a Static Website on Amazon S3.
- The AWS Import/Export service is not available.
- Amazon S3 Transfer Acceleration is not available in AWS Secret Region.
- Amazon CloudFront is not available in AWS Secret Region, so content distribution techniques using CloudFront are not available in Amazon S3.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.
- Amazon S3 Storage Lens is not available in AWS Secret Region.
- AWS PrivateLink for Amazon S3 is not available in AWS Secret Region.
- Amazon S3 Object Lambda Access Points are not available in AWS Secret Region.
- Amazon S3 Replication Time Control (S3 RTC) is not available in AWS Secret Region.
- Amazon S3 does not support notifications for the event type of `S3 Intelligent-Tiering automatic archival events` in AWS Secret Region.
- Sending AWS X-Ray trace headers through Amazon S3 is not supported in AWS Secret Region.
- Amazon S3 does not support S3 Intelligent-Tiering archive access Tiers (Archive Access tier and Deep Archive Access tier) in AWS Secret Region.
- In AWS Secret Region, Amazon S3 Inventory does not have the Object Access Control List and Object Owner as available object metadata fields in inventory reports.
- Standard retrievals for restore requests that are made through S3 Batch Operations have the same restore times as other Standard retrieval requests for AWS Secret Region.
- Generating a manifest is only supported for Amazon S3 Batch Replication jobs in AWS Secret Region.
- Amazon S3 does not support FIPS or FIPS Dualstack service endpoints in AWS Secret Region.

# How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Amazon S3 and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Amazon S3 by using the command line or APIs, use the following endpoint:

- https://s3.us-isob-east-1.sc2s.sgov.gov

## Documentation for Amazon S3

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Amazon S3 differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon Simple Storage Service User Guide
- Amazon Simple Storage Service User Guide
- Amazon Simple Storage Service User Guide
- Amazon S3 section of AWS CLI Reference
- Amazon Simple Storage Service API Reference

# Amazon Simple Notification Service

Amazon Simple Notification Service (Amazon SNS) is a fast, flexible, fully managed push messaging service. Amazon SNS makes it simple and cost-effective to push to devices and distributed services. Amazon SNS can also deliver notifications by email and it can push to Amazon SQS queues or to any HTTP(S) endpoint in AWS Secret Region.

**Topics**



## How Amazon SNS Differs for AWS Secret Region

The implementation of Amazon SNS is different for AWS Secret Region in the following ways:

- Since AWS Secret Region operates as a single air-gapped region, Amazon SNS cannot communicate to endpoints outside of the region.
- In AWS Secret Region, Amazon SNS does not support SMS or mobile push notifications.
- Amazon SNS signs all notification deliveries using a private-public key pair based on certificates. The public key is available at https://sns.us-isob-east-1.sc2s.sgov.gov/SimpleNotificationService.pem.
- If you subscribe an HTTPS endpoint to a topic, that endpoint must have a server certificate signed by a trusted certificate authority (CA). Amazon SNS will deliver messages only to HTTPS endpoints that have a signed certificate from a trusted CA recognized by Amazon SNS. For a list of CAs, see Certificate Authorities (CA) Recognized by Amazon SNS for HTTPS in AWS Secret Region. For more information, see Sending Messages to HTTP/HTTPS Endpoints.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.
- In AWS Secret Region, Amazon SNS does not support FIFO topics.
- In AWS Secret Region, Amazon SNS does not support Kinesis Firehose delivery stream endpoints.
- Message Data Protection is not supported.
- Active tracing is not supported.

- Payload-based message filtering is not supported.
- Amazon SNS message archiving and replay is not supported.
- Custom data identifiers are not supported.

## Publishing a message from a VPC

To publish to an Amazon SNS topic in AWS Secret Region, you need to use a different AWS CloudFormation template than described in Publishing an Amazon SNS message from Amazon VPC in the *Amazon Simple Notification Service Developer Guide*. Rather than download an AWS CloudFormation template from GitHub, copy and paste the following template into a text-only file, and then upload it to AWS CloudFormation:

```
AWSTemplateFormatVersion: 2010-09-09
Description: CloudFormation Template for SNS VPC Endpoints Tutorial
Parameters:
  KeyName:
    Description: Name of an existing EC2 KeyPair to enable SSH access to the instance
    Type: 'AWS::EC2::KeyPair::KeyName'
    ConstraintDescription: must be the name of an existing EC2 KeyPair.
  SSHLocation:
    Description: The IP address range that can be used to SSH to the EC2 instance
    Type: String
    MinLength: '9'
    MaxLength: '18'
    Default: 0.0.0.0/0
    AllowedPattern: '(\d{1,3})\.(\d{1,3})\.(\d{1,3})\.(\d{1,3})/(\d{1,2})'
    ConstraintDescription: must be a valid IP CIDR range of the form x.x.x.x/x.
Mappings:
  RegionMap:
    us-east-1:
      AMI: ami-428aa838
    us-east-2:
      AMI: ami-710e2414
    us-west-1:
      AMI: ami-4a787a2a
    us-west-2:
      AMI: ami-7f43f307
    ap-northeast-1:
      AMI: ami-c2680fa4
    ap-northeast-2:
      AMI: ami-3e04a450
```

```
    ap-southeast-1:
      AMI: ami-4f89f533
    ap-southeast-2:
      AMI: ami-38708c5a
    ap-south-1:
      AMI: ami-3b2f7954
    ca-central-1:
      AMI: ami-7549cc11
    eu-central-1:
      AMI: ami-1b2bb774
    eu-west-1:
      AMI: ami-db1688a2
    eu-west-2:
      AMI: ami-6d263d09
    eu-west-3:
      AMI: ami-5ce55321
    sa-east-1:
      AMI: ami-f1337e9d
    us-isob-east-1:
      AMI: ami-02e97847c224981ce
Resources:
  VPC:
    Type: 'AWS::EC2::VPC'
    Properties:
      CidrBlock: 10.0.0.0/16
      EnableDnsSupport: 'true'
      EnableDnsHostnames: 'true'
      Tags:
        - Key: Name
          Value: VPCE-Tutorial-VPC
  Subnet:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref VPC
      CidrBlock: 10.0.0.0/24
      Tags:
        - Key: Name
          Value: VPCE-Tutorial-Subnet
  InternetGateway:
    Type: 'AWS::EC2::InternetGateway'
    Properties:
      Tags:
        - Key: Name
          Value: VPCE-Tutorial-InternetGateway
```

```
  VPCGatewayAttachment:
    Type: 'AWS::EC2::VPCGatewayAttachment'
    Properties:
      VpcId: !Ref VPC
      InternetGatewayId: !Ref InternetGateway
  RouteTable:
    Type: 'AWS::EC2::RouteTable'
    Properties:
      VpcId: !Ref VPC
      Tags:
        - Key: Name
          Value: VPCE-Tutorial-RouteTable
  SubnetRouteTableAssociation:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref RouteTable
      SubnetId: !Ref Subnet
  InternetGatewayRoute:
    Type: 'AWS::EC2::Route'
    Properties:
      RouteTableId: !Ref RouteTable
      GatewayId: !Ref InternetGateway
      DestinationCidrBlock: 0.0.0.0/0
  SecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupName: Tutorial Security Group
      GroupDescription: Security group for SNS VPC endpoing tutorial
      VpcId: !Ref VPC
      SecurityGroupIngress:
        - IpProtocol: '-1'
          CidrIp: 10.0.0.0/16
        - IpProtocol: tcp
          FromPort: '22'
          ToPort: '22'
          CidrIp: !Ref SSHLocation
      SecurityGroupEgress:
        - IpProtocol: '-1'
          CidrIp: 10.0.0.0/16
      Tags:
        - Key: Name
          Value: VPCE-Tutorial-SecurityGroup
  EC2Instance:
    Type: 'AWS::EC2::Instance'
```

```
    Properties:
      KeyName: !Ref KeyName
      InstanceType: t2.micro
      ImageId: !FindInMap
        - RegionMap
        - !Ref 'AWS::Region'
        - AMI
      NetworkInterfaces:
        - AssociatePublicIpAddress: 'true'
          DeviceIndex: '0'
          GroupSet:
            - !Ref SecurityGroup
          SubnetId: !Ref Subnet
      IamInstanceProfile: !Ref EC2InstanceProfile
      Tags:
        - Key: Name
          Value: VPCE-Tutorial-EC2Instance
  EC2InstanceProfile:
    Type: 'AWS::IAM::InstanceProfile'
    Properties:
      Roles:
        - !Ref EC2InstanceRole
      InstanceProfileName: EC2InstanceProfile
  EC2InstanceRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: VPCE-Tutorial-EC2InstanceRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: ec2.amazonaws.com
            Action: 'sts:AssumeRole'
      ManagedPolicyArns:
        - 'arn:aws-iso-b:iam::aws:policy/AmazonSNSFullAccess'
  LambdaExecutionRole:
    Type: 'AWS::IAM::Role'
    Properties:
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
        - Effect: Allow
          Principal:
```

```
            Service: lambda.amazonaws.com
          Action: 'sts:AssumeRole'
      ManagedPolicyArns:
        - 'arn:aws-iso-b:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole'
  LambdaFunction1:
    Type: 'AWS::Lambda::Function'
    Properties:
      Code:
        ZipFile: |
          from __future__ import print_function
          print('Loading function')
          def lambda_handler(event, context):
            message = event['Records'][0]['Sns']['Message']
            print("From SNS: " + message)
            return message
      Description: SNS VPC endpoint tutorial lambda function 1
      FunctionName: VPCE-Tutorial-Lambda-1
      Handler: index.lambda_handler
      Role: !GetAtt
        - LambdaExecutionRole
        - Arn
      Runtime: python2.7
      Timeout: '3'
  LambdaPermission1:
    Type: 'AWS::Lambda::Permission'
    Properties:
      Action: 'lambda:InvokeFunction'
      FunctionName: !Ref LambdaFunction1
      Principal: sns.amazonaws.com
      SourceArn: !Ref SNSTopic
  LambdaLogGroup1:
    Type: 'AWS::Logs::LogGroup'
    Properties:
      LogGroupName: !Sub "/aws/lambda/${LambdaFunction1}"
      RetentionInDays: '7'
  LambdaFunction2:
    Type: 'AWS::Lambda::Function'
    Properties:
      Code:
        ZipFile: |
          from __future__ import print_function
          print('Loading function')
          def lambda_handler(event, context):
            message = event['Records'][0]['Sns']['Message']
```

```
            print("From SNS: " + message)
            return message
      Description: SNS VPC endpoint tutorial lambda function 2
      FunctionName: VPCE-Tutorial-Lambda-2
      Handler: index.lambda_handler
      Role: !GetAtt
        - LambdaExecutionRole
        - Arn
      Runtime: python2.7
      Timeout: '3'
  LambdaPermission2:
    Type: 'AWS::Lambda::Permission'
    Properties:
      Action: 'lambda:InvokeFunction'
      FunctionName: !Ref LambdaFunction2
      Principal: sns.amazonaws.com
      SourceArn: !Ref SNSTopic
  LambdaLogGroup2:
    Type: 'AWS::Logs::LogGroup'
    Properties:
      LogGroupName: !Sub "/aws/lambda/${LambdaFunction2}"
      RetentionInDays: '7'
  SNSTopic:
    Type: 'AWS::SNS::Topic'
    Properties:
      DisplayName: VPCE-Tutorial-Topic
      TopicName: VPCE-Tutorial-Topic
      Subscription:
        - Endpoint: !GetAtt
            - LambdaFunction1
            - Arn
          Protocol: lambda
        - Endpoint: !GetAtt
            - LambdaFunction2
            - Arn
          Protocol: lambda
```

To use this template, follow the Publishing an Amazon SNS message from Amazon VPC, but change the first few steps under "Step 2: Create the AWS resources" to the following:

1. Sign in to the AWS CloudFormation Console.
2. Choose **Create stack**.

3. Under **Specify template**, choose **Upload a template file** and choose the text-only file where you saved the above template.
4. Choose **Next** and then resume following the standard procedure at step 5, where you specify stack details.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Amazon SNS and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Amazon SNS by using the command line or APIs, use the following endpoint:

- https://sns.us-isob-east-1.sc2s.sgov.gov

## Documentation for Amazon SNS

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Amazon SNS differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon Simple Notification Service Developer Guide
- Amazon SNS section of AWS CLI Reference
- Amazon Simple Notification Service API Reference

# Amazon Simple Queue Service

Amazon Simple Queue Service (Amazon SQS) is a fast, reliable, scalable, fully managed queue service. Amazon SQS makes it simple and cost-effective to decouple the components of a cloud application. You can use Amazon SQS to transmit any volume of data, at any level of throughput, without losing messages or requiring other services to be always available.

**Topics**



## How Amazon SQS Differs for AWS Secret Region

The implementation of Amazon SQS is different for AWS Secret Region in the following ways:

- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.
- AWS JSON protocol is not supported.
- Amazon SQS Extended Client Library for Python is not supported.

### Publishing a message from a VPC

To send messages to an Amazon SQS queue in AWS Secret Region, you need to use a different AWS CloudFormation template than described in Tutorial: Sending a message to an Amazon SQS queue from Amazon Virtual Private Cloud in the *Amazon Simple Queue Service Developer Guide*. Rather than download an AWS CloudFormation template from GitHub, copy and paste the following template into a text-only file, and then upload it to AWS CloudFormation:

```
AWSTemplateFormatVersion: 2010-09-09
  Description: CloudFormation Template for SQS VPC Endpoints Tutorial
  Parameters:
    KeyName:
      Description: Name of an existing EC2 KeyPair to enable SSH access to the instance
      Type: 'AWS::EC2::KeyPair::KeyName'
      ConstraintDescription: must be the name of an existing EC2 KeyPair.
    SSHLocation:
```

```
      Description: The IP address range that can be used to SSH to the EC2 instance
      Type: String
      MinLength: '9'
      MaxLength: '18'
      Default: 0.0.0.0/0
      AllowedPattern: '(\d{1,3})\.(\d{1,3})\.(\d{1,3})\.(\d{1,3})/(\d{1,2})'
      ConstraintDescription: must be a valid IP CIDR range of the form x.x.x.x/x.
  Conditions:
    IsT3Supported: !Equals [!Ref 'AWS::Region', eu-north-1]
  Resources:
    VPC:
      Type: 'AWS::EC2::VPC'
      Properties:
        CidrBlock: 10.0.0.0/16
        EnableDnsSupport: 'true'
        EnableDnsHostnames: 'true'
        Tags:
          - Key: Name
            Value: SQS-VPCE-Tutorial-VPC
    Subnet:
      Type: 'AWS::EC2::Subnet'
      Properties:
        VpcId: !Ref VPC
        CidrBlock: 10.0.0.0/24
        Tags:
          - Key: Name
            Value: SQS-VPCE-Tutorial-Subnet
    InternetGateway:
      Type: 'AWS::EC2::InternetGateway'
      Properties:
        Tags:
          - Key: Name
            Value: SQS-VPCE-Tutorial-InternetGateway
    VPCGatewayAttachment:
      Type: 'AWS::EC2::VPCGatewayAttachment'
      Properties:
        VpcId: !Ref VPC
        InternetGatewayId: !Ref InternetGateway
    RouteTable:
      Type: 'AWS::EC2::RouteTable'
      Properties:
        VpcId: !Ref VPC
        Tags:
          - Key: Name
```

```
          Value: SQS-VPCE-Tutorial-RouteTable
    SubnetRouteTableAssociation:
      Type: 'AWS::EC2::SubnetRouteTableAssociation'
      Properties:
        RouteTableId: !Ref RouteTable
        SubnetId: !Ref Subnet
    InternetGatewayRoute:
      Type: 'AWS::EC2::Route'
      Properties:
        RouteTableId: !Ref RouteTable
        GatewayId: !Ref InternetGateway
        DestinationCidrBlock: 0.0.0.0/0
    SecurityGroup:
      Type: 'AWS::EC2::SecurityGroup'
      Properties:
        GroupName: SQS VPCE Tutorial Security Group
        GroupDescription: Security group for SQS VPC endpoint tutorial
        VpcId: !Ref VPC
        SecurityGroupIngress:
          - IpProtocol: '-1'
            CidrIp: 10.0.0.0/16
          - IpProtocol: tcp
            FromPort: '22'
            ToPort: '22'
            CidrIp: !Ref SSHLocation
        SecurityGroupEgress:
          - IpProtocol: '-1'
            CidrIp: 10.0.0.0/16
        Tags:
          - Key: Name
            Value: SQS-VPCE-Tutorial-SecurityGroup
    EC2Instance:
      Type: 'AWS::EC2::Instance'
      Properties:
        KeyName: !Ref KeyName
        InstanceType: !If [IsT3Supported, t3.micro, t2.micro]
        ImageId: ami-a98c77d2
        NetworkInterfaces:
          - AssociatePublicIpAddress: 'true'
            DeviceIndex: '0'
            GroupSet:
              - !Ref SecurityGroup
            SubnetId: !Ref Subnet
        IamInstanceProfile: !Ref EC2InstanceProfile
```

```
      Tags:
        - Key: Name
          Value: SQS-VPCE-Tutorial-EC2Instance
  EC2InstanceProfile:
    Type: 'AWS::IAM::InstanceProfile'
    Properties:
      Roles:
        - !Ref EC2InstanceRole
      InstanceProfileName: !Sub 'EC2InstanceProfile-${AWS::Region}'
  EC2InstanceRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: !Sub 'SQS-VPCE-Tutorial-EC2InstanceRole-${AWS::Region}'
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: ec2.sc2s.sgov.gov
            Action: 'sts:AssumeRole'
      ManagedPolicyArns:
        - 'arn:aws-iso-b:iam::aws:policy/AmazonSQSFullAccess'
  CFQueue:
    Type: 'AWS::SQS::Queue'
    Properties:
      VisibilityTimeout: 60
```

To use this template, follow the Tutorial: Sending a message to an Amazon SQS queue from Amazon Virtual Private Cloud procedure, but change the first few steps under "Step 2: Create the AWS resources" to the following:

1. Sign in to the AWS CloudFormation Console.
2. Choose **Create stack**.
3. Under **Specify template**, choose **Upload a template file** and choose the text-only file where you saved the above template.
4. Choose **Next** and then resume following the standard procedure at step 5, where you specify stack details.

# How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Amazon SQS and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Amazon SQS by using the command line or APIs, use the following endpoint:

- https://sqs.us-isob-east-1.sc2s.sgov.gov

## Documentation for Amazon SQS

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Amazon SQS differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon Simple Queue Service Developer Guide "Getting Started" section
- Amazon Simple Queue Service Developer Guide
- Amazon SQS section of AWS CLI Reference
- Amazon Simple Queue Service API Reference

# Amazon Simple Workflow Service

Amazon Simple Workflow Service (Amazon SWF) is a task coordination and state management service for cloud applications. The Amazon SWF APIs, libraries, and control engine give developers the tools to coordinate, audit, and scale applications across multiple machines—in the AWS cloud and other data centers. With Amazon SWF, you can stop writing complex glue-code and state machinery and invest more in the business logic that makes your applications unique.

**Topics**



## How Amazon SWF Differs for AWS Secret Region

The implementation of Amazon SWF is different for AWS Secret Region in the following ways:

- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Amazon SWF and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Amazon SWF by using the command line or APIs, use the following endpoint:

- https://swf.us-isob-east-1.sc2s.sgov.gov

# Documentation for Amazon SWF

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Amazon SWF differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon Simple Workflow Service Developer Guide
- Amazon SWF section of AWS CLI Reference
- Amazon Simple Workflow Service API Reference
- AWS Flow Framework for Java Developer Guide
- AWS Flow Framework for Java API Reference
- AWS Flow Framework for Ruby Developer Guide
- AWS Flow Framework for Ruby API Reference

# AWS Snowball Edge

The AWS Snowball Edge is a type of Snowball device with on-board storage and compute power for select AWS capabilities. Snowball Edge can undertake local processing and edge-computing workloads in addition to transferring data between your local environment and the AWS Cloud.

**Topics**



## How Snowball Edge Differs for AWS Secret Region

The implementation of Snowball Edge is different for AWS Secret Region in the following ways:

- For differences on managing Amazon EC2-compatible instances on your device, see Amazon Elastic Compute Cloud. AWS Snow Family EC2-compatible instances allow customers to use and manage Amazon EC2-compatible instances using a subset of EC2 APIs and a subset of AMIs.
- The only shipping carrier for AWS Secret Region is Fedex. This carrier is approved to handle and transport AWS Secret Region Snowball and Snowball Edge devices.
- For Compute using Amazon EC2-compatible instances you need to have one or more supported AMIs in your AWS account before you can add any AMIs to your job creation request otherwise you will see "You have no compatible AMIs". If you believe your AMI is supported but it is not showing please open a case with AWS Secret Region AWS Support, provide your account number, your AMI IDs, and we will review why your AMIs are not appearing.
- Snowcone is not available in AWS Secret Region because AWS DataSync is not available in the AWS Secret Region.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.
- The high performance NFS data transfer feature is not available on AWS Secret Region Snowball Edge Storage Optimized devices because AWS DataSync is not available in the AWS Secret Region.
- The AWS Snow Family Job Management Service CreateReturnShippingLabel and DescribeReturnShippingLabel API actions are not available for AWS Secret Region Snow Family jobs. In the event you require a shipping label in order to return your AWS Secret Region Snow

Family device, open a case with AWS Secret Region Support, provide your AWS Snow Family Job ID, and AWS Snow Family Snowball Edge device Serial Number. AWS will then provide you with a shipping label.

- AWS Snow Device Management service is not available in AWS Secret Region because AWS IoT Greengrass is not available in AWS Secret Region.
- AWS Snow Family Large Data Migration Manager is not available in AWS Secret Region.
- Amazon EKS Anywhere on Snow is not available in AWS Secret Region.
- Amazon S3 Compatible Storage is not available on Snowball Edge Compute Optimized with AMD EPYC Gen1, HDD, and optional GPU in AWS Secret Region.
- Snowball Edge devices in the AWS Secret Region do not have an embedded GPS module.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Snowball Edge and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Snowball Edge by using the command line or APIs, use the following endpoint:

- https://snowball.us-isob-east-1.sc2s.sgov.gov

## Documentation for Snowball Edge

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Snowball Edge differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Snowball Edge Developer Guide

- AWS Snowball API Reference
- AWS Snowball section of AWS CLI Reference

# AWS Step Functions

AWS Step Functions is a web service that enables you to coordinate the components of distributed applications and microservices using visual workflows.

**Topics**



## How Step Functions Differs for AWS Secret Region

The implementation of Step Functions is different for AWS Secret Region in the following ways:

- Step Functions Local .jar file is not available in AWS Secret Region.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.
- Synchronous Express Workflows are not available.
- Support for AWS X-Ray tracing is not available.
- Support for and from the AWS Serverless Application Model is not available.
- Support to call third-party APIs is not available.
- Support to use the TestState API is not available.
- The Step Functions Data Science SDK is not supported.
- Integration with AWS services available as of December 23, 2023 are supported in AWS Secret Region if these services are available in the Region.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Step Functions and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Step Functions by using the command line or APIs, use the following endpoint:

- https://states.us-isob-east-1.sc2s.sgov.gov

## Documentation for Step Functions

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Step Functions differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Step Functions Developer Guide
- AWS Step Functions API Reference
- AWS Step Functions section of AWS CLI Reference

# AWS Storage Gateway

AWS Storage Gateway is a service that connects an on-premises software appliance with cloud-based storage to provide seamless and secure integration between your on-premises IT environment and the AWS storage infrastructure in the AWS Cloud.

**Topics**



## How Storage Gateway Differs for AWS Secret Region

The implementation of Storage Gateway is different for AWS Secret Region in the following ways:

- The AWS Storage Gateway hardware appliance is not available in AWS Secret Region.
- Amazon FSx File Gateway is not currently supported in AWS Secret Region.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Storage Gateway and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Storage Gateway by using the command line or APIs, use the following endpoints:

- https://storagegateway.us-isob-east-1.sc2s.sgov.gov
- https://storagegateway-fips.us-isob-east-1.sc2s.sgov.gov

# Documentation for Storage Gateway

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Storage Gateway differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Storage Gateway - Amazon S3 File Gateway User Guide
- AWS Storage Gateway - Tape Gateway User Guide
- AWS Storage Gateway - Volume Gateway User Guide
- AWS Storage Gateway - API Reference

# AWS Support

AWS Support for AWS Secret Region offers support options ranging from online help to personal support.

**Topics**



## AWS Support Center

AWS Support Center is your location for AWS Technical Support, which includes access to technical FAQs, service status page, and AWS Support. AWS Support Center is available in the AWS Management Console, with federated access support and enhanced case-management workflows. For more information, see AWS Support Center.

> **Note**
>
> AWS Support Center currently does not integrate with the Classification Management Tool. You must manually add classification markings when using AWS Support Center.

## AWS Secret Region Business Support

AWS Secret Region Business Support is a one-on-one, fast-response support channel that is staffed around the clock by experienced technical support engineers. Business support is available to all customers in AWS Secret Region at no additional charge. For more information, see AWS Support.

## AWS Secret Region Enterprise Support

The optional AWS Secret Region Enterprise Support offering builds on AWS Secret Region Business Support by adding features such as direct access to a Technical Account Manager (TAM). There are charges for Enterprise support. For more information, see AWS Support.

## Service Health Dashboard

AWS Secret Region includes a Service Health Dashboard (SHD) that provides access to current status and historical data about every AWS service in AWS Secret Region. If there's a problem with a service, you'll be able to expand the appropriate line in the Details section and learn more. You can also subscribe to the RSS feed for any service. You can access the SHD from the marketing site or at http://status.sc2shome.sgov.gov/.

## AWS Trusted Advisor

AWS Trusted Advisor is a service in the console that inspects your AWS environment and identifies ways to save money, improve system performance and reliability, or close security gaps. For more information, see Meet AWS Trusted Advisor.

## How AWS Support Differs for AWS Secret Region

The implementation of AWS Support is different for AWS Secret Region in the following ways:

- The **How can we help?** search bar in the AWS Support Center is not available.
- Some Trusted Advisor features are not available. See AWS Trusted Advisor.
- Only signature version 4 signing is supported.

## Documentation for AWS Support

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how AWS Support differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Support User Guide
- AWS Support section of AWS CLI Reference

- AWS Support API Reference

To connect to AWS Support by using the command line or APIs, use the following endpoint:

- https://support.us-isob-east-1.sc2s.sgov.gov

# AWS Systems Manager

AWS Systems Manager gives you visibility into and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and you can use Systems Manager to automate operational tasks across your AWS resources. Systems Manager is comprised of individual capabilities, which are grouped into five categories: *Operations Management*, *Application Management*, *Actions & Change*, *Instances & Nodes*, and *Shared Resources*.

**Topics**



## How Systems Manager Differs for AWS Secret Region

The implementation of Systems Manager is different for AWS Secret Region in the following ways:

- The following Systems Manager capabilities are not yet available for AWS Secret Region:
  - Application Manager
  - Change Calendar
  - Change Manager
  - Distributor
  - Explorer
  - Fleet Manager
  - Incident Manager
  - OpsCenter
  - Quick Setup
- The following Systems Manager features are not available for AWS Secret Region:
  - In the Parameter Store capability, the shared parameters feature is not available.
  - In the Session Manager capability, the Block public sharing for SSM documents feature is not available.
  - Support for specifying a resource group as a target.
  - The ability to delete the Systems Manager service-linked role is not supported.

- In the Automation capability, the Document Builder feature is not available.
- In the Automation capability, the `aws:executeScript` action is not yet available for running Python or PowerShell scripts as part of a custom Automation workflow.
- Not all Automation runbooks and SSM Command documents are available for AWS Secret Region.

- The URLs to download the Session Manager plugin for the AWS CLI are as follows:

| Operating System | Session Manager Plugin URL |
| --- | --- |
| Windows Server | `https://s3.us-isob-east-1.sc2s.sgov.gov/session-manager-downloads/plugin/latest/windows/SessionManagerPluginSetup.exe` |
| macOS | `https://s3.us-isob-east-1.sc2s.sgov.gov/session-manager-downloads/plugin/latest/mac/sessionmanager-bundle.zip` |
| Linux | **x86_64:**<br>`https://s3.us-isob-east-1.sc2s.sgov.gov/session-manager-downloads/plugin/latest/linux_64bit/session-manager-plugin.rpm`<br>**x86:**<br>`https://s3.us-isob-east-1.sc2s.sgov.gov/session-manager-downloads/plugin/latest/linux_32bit/session-manager-plugin.rpm`<br>**ARM64:** |

| Operating System | Session Manager Plugin URL |
| --- | --- |
| | `https://s3.us-isob-east-1.sc2s.sgov.gov/session-manager-downloads/plugin/latest/linux_arm64/session-manager-plugin.rpm` |
| Ubuntu Server | **x86_64:**<br><br>`https://s3.us-isob-east-1.sc2s.sgov.gov/session-manager-downloads/plugin/latest/ubuntu_64bit/session-manager-plugin.deb`<br><br>**x86:**<br><br>`https://s3.us-isob-east-1.sc2s.sgov.gov/session-manager-downloads/plugin/latest/ubuntu_32bit/session-manager-plugin.deb`<br><br>**ARM64:**<br><br>`https://s3.us-isob-east-1.sc2s.sgov.gov/session-manager-downloads/plugin/latest/ubuntu_arm64/session-manager-plugin.deb` |

- The process for installing SSM Agent on managed instances includes the following differences for AWS Secret Region:
  - The URLs to download the installers from are specific to AWS Secret Region.
  - On version 2.3.714.0 and earlier versions of SSM Agent, a custom file must be created to specify the endpoint values for the agent to use.
  - SSM Agent must be restarted after creating the custom file.

When following the instructions to install SSM Agent on Linux and Windows operating systems, see the following table for the sources of installation files to use.

| Operating System | SSM Agent Installer URL |
| --- | --- |
| Amazon Linux and Amazon Linux 2 | **Intel (x86_64) 64-bit instances:**<br>`https://s3.us-isob-east-1.sc2s.sgov.gov/amazon-ssm-us-isob-east-1/latest/linux_amd64/amazon-ssm-agent.rpm`<br>**ARM (arm64) 64-bit instances:**<br>`https://s3.us-isob-east-1.sc2s.sgov.gov/amazon-ssm-us-isob-east-1/latest/linux_arm64/amazon-ssm-agent.rpm`<br>**Intel (x86) 32-bit instances:**<br>`https://s3.us-isob-east-1.sc2s.sgov.gov/amazon-ssm-us-isob-east-1/latest/linux_386/amazon-ssm-agent.rpm` |
| Ubuntu Server | `https://s3.us-isob-east-1.sc2s.sgov.gov/amazon-ssm-us-isob-east-1/latest/debian_amd64/amazon-ssm-agent.deb sudo dpkg -i amazon-ssm-agent.deb` |

| Operating System | SSM Agent Installer URL |
| --- | --- |
| Red Hat Enterprise Linux (RHEL) | **Intel (x86_64) 64-bit instances:**<br>`https://s3.us-isob-east-1.s c2s.sgov.gov/amazon-ssm-us- isob-east-1/latest/linux_am d64/amazon-ssm-agent.rpm`<br>**ARM (arm64) 64-bit instances::**<br>`https://s3.us-isob-east-1.s c2s.sgov.gov/amazon-ssm-us- isob-east-1/latest/linux_ar m64/amazon-ssm-agent.rpm`<br>**Intel (x86) 32-bit instances:**<br>`https://s3.us-isob-east-1.s c2s.sgov.gov/amazon-ssm-us- isob-east-1/latest/linux_386/ amazon-ssm-agent.rpm` |
| CentOS | **64-bit instances:**<br>`https://s3.us-isob-east-1.s c2s.sgov.gov/amazon-ssm-us- isob-east-1/latest/linux_am d64/amazon-ssm-agent.rpm`<br>**32-bit instances:**<br>`https://s3.us-isob-east-1.s c2s.sgov.gov/amazon-ssm-us- isob-east-1/latest/linux_386/ amazon-ssm-agent.rpm` |

| Operating System | SSM Agent Installer URL |
| --- | --- |
| SUSE Linux Enterprise Server (SLES) | **64-bit instances:**<br>`https://s3.us-isob-east-1.sc2s.sgov.gov/amazon-ssm-us-isob-east-1/latest/linux_amd64/amazon-ssm-agent.rpm sudo rpm --install amazon-ssm-agent.rpm` |
| Raspbian | `https://s3.us-isob-east-1.sc2s.sgov.gov/amazon-ssm-us-isob-east-1/latest/debian_arm/amazon-ssm-agent.deb` |
| Windows Server | `https://s3.us-isob-east-1.sc2s.sgov.gov/amazon-ssm-us-isob-east-1/latest/windows_amd64/AmazonSSMAgentSetup.exe` |

**Customize endpoints (SSM Agent versions 2.3.714.0 and earlier)**

If you are running SSM Agent version 2.3.714.0 or earlier, follow these steps to specify the custom endpoints for SSM Agent. These steps are not required for versions of the agent later than 2.3.714.0.

> **Tip**
>
> For all operating system types, you can locate the SSM Agent version number on the **Managed Instances** page in the Systems Manager console.

1. Open the file `amazon-ssm-agent.json.template` from the appropriate location.

   **All Unix-based operating systems and Raspbian:**

   `/etc/amazon/ssm/amazon-ssm-agent.json.template`

**Windows Server:**

`C:\Program Files\Amazon\SSM\amazon-ssm-agent.json.template`

2. For the following elements in the file, enter the endpoints as specified in the **Endpoint** column.

| Element | Endpoint |
| --- | --- |
| Mds | `ec2messages.us-isob-east-1.sc2s.sgov.gov` |
| Ssm | `ssm.us-isob-east-1.sc2s.sgov.gov` |
| Mgs | `ssmmessages.us-isob-east-1.sc2s.sgov.gov` |
| S3 | `s3.us-isob-east-1.sc2s.sgov.gov` |
| Kms | `kms.us-isob-east-1.sc2s.sgov.gov` |

3. Save the file as `amazon-ssm-agent.json`.
4. Restart SSM Agent.

- A table in the topic About minimum S3 Bucket permissions for SSM Agent lists two Amazon Simple Storage Service (S3) buckets that can provide access to the distribution service used by version 2.2.45.0 and later of SSM Agent. (This service is used to run the document `AWS-ConfigureAWSPackage`).

  In AWS Secret Region, the bucket that SSM Agent requires access to is the one in the format `arn:aws:s3:::aws-ssm-distributor-file-`*`region`*`/*` .
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

# How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Systems Manager and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Systems Manager by using the command line or APIs, use the following endpoint:

- https://ssm.us-isob-east-1.sc2s.sgov.gov

## Documentation for Systems Manager

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Systems Manager differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Systems Manager User Guide
- AWS Systems Manager API Reference
- Systems Manager section of AWS CLI Reference

# AWS Transit Gateway

A *transit gateway* is a network transit hub that you can use to interconnect your virtual private clouds (VPCs) and on-premises networks.

**Topics**



## How AWS Transit Gateway Differs for AWS Secret Region

The implementation of AWS Transit Gateway is different for AWS Secret Region in the following ways:

- IGMP multicast is not supported.
- Transit Gateway Connect is not supported in AWS Secret Region.
- Connect peers are not supported in AWS Secret Region.
- Transit Gateway Network Manager is not supported in AWS Secret Region.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with AWS Transit Gateway and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to AWS Transit Gateway by using the command line or APIs, use the following endpoint:

- https://ec2.us-isob-east-1.sc2s.sgov.gov

# Documentation for AWS Transit Gateway

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how AWS Transit Gateway differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon VPC Transit Gateways
- Amazon EC2 section of AWS CLI Reference
- Amazon EC2 API Reference

# AWS Trusted Advisor

AWS Trusted Advisor helps you provision your resources by following best practices. Trusted Advisor inspects your AWS environment and finds opportunities to save money, improve system performance and reliability, or help close security gaps.

**Topics**



## How AWS Trusted Advisor Differs for AWS Secret Region

The implementation of AWS Trusted Advisor is different for AWS Secret Region in the following ways:

- The organizational view feature is not supported.
- Not all checks are supported in AWS Secret Region. For a list of available checks, see the Trusted Advisor check reference.
- Trusted Advisor does not support sending weekly notification emails for checks at this time.
- Monitoring Trusted Advisor checks with Amazon CloudWatch Events is not supported.
- The AWS Security Hub integration feature is not supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with AWS Trusted Advisor and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

> **Note**
>
> To call the Trusted Advisor API, use the same endpoint as AWS Support.

To connect to AWS Trusted Advisor by using the command line or APIs, use the following endpoint:

- https://support.us-isob-east-1.sc2s.sgov.gov

## Documentation for AWS Trusted Advisor

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how AWS Trusted Advisor differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Support User Guide
- AWS Support API Reference
- Trusted Advisor section of AWS CLI Reference

# Amazon Virtual Private Cloud

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Secret Region cloud where you can launch resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

**Topics**



## How Amazon VPC Differs for AWS Secret Region

The implementation of Amazon VPC is different for AWS Secret Region in the following ways:

- Tag on create and vanity DNS are not supported with AWS PrivateLink.
- AWS Site-to-Site VPN integration with Global Accelerator is not available.
- You can't assign a private DNS name to a VPC endpoint service.
- You can't add a tag when you create a VPC, network interface, or Elastic IP address using the Amazon VPC console.
- Internet gateways do not connect to the public Internet.
- You can view and use AWS-managed prefix lists with security groups only.
- Traffic Mirroring is not supported.
- Reachability Analyzer is not supported.
- Network Access Analyzer is not supported.
- Amazon VPC IP Address Manager (IPAM) is not supported.
- You can enable IPv6 to support traffic flow within a single VPC and between multiple VPCs. AWS Site-to-Site VPN, transit gateways, and AWS Direct Connect do not support IPv6.
- IPv6 only subnets are not supported.
- The following IPv6 ranges are supported:
  - us-isob-east-1 – 2600:1f19::/36
- The transfer Elastic IP address feature is not available.

- DNS64 and NAT64 are not available.
- Security group referencing support for transit gateways and transit gateway attachments is not available.
- When creating a DHCP option set, the IPv6 Preferred Lease Time option is not available.
- VPC Flow Logs cannot be sent to Amazon Data Firehose.
- If you send VPC flow logs to Amazon S3, the `Parquet`, `Hive-compatible S3 prefixes` and `Hourly partitions` log file options are not available.
- Fields related to Amazon ECS that were released in VPC Flow Logs version 7 are not available.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with Amazon VPC and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to Amazon VPC by using the command line or APIs, use the following endpoint:

- https://ec2.us-isob-east-1.sc2s.sgov.gov

## Documentation for Amazon VPC

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Amazon VPC differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon VPC Getting Started Guide

- Amazon VPC User Guide
- AWS Site-to-Site VPN Network Administrator Guide
- Amazon EC2 section of AWS CLI Reference
- Amazon EC2 API Reference

# AWS Virtual Private Network

AWS Virtual Private Network lets you establish a secure and private tunnel from your network or device to the AWS Cloud. You can extend your existing on-premises network into a VPC, or connect to other AWS resources from a client. AWS VPN offers two types of private connectivity that feature the high availability and robust security necessary for your data.

**Topics**



## How AWS VPN Differs for AWS Secret Region

The implementation of AWS VPN is different for AWS Secret Region in the following ways:

- AWS Site-to-Site VPN integration with Global Accelerator is not available.
- Configurable Security Algorithms and Timer Settings is not supported.
- Certificate authentication and customer gateway modification are not supported.
- The following APIs do not support resource-level permissions: CreateVpnConnection, DeleteVpnConnection, CreateVpnGateway, DeleteVpnGateway, CreateCustomerGateway, DeleteCustomerGateway, AttachVpnGateway, DetachVpnGateway, CreateVpnConnectionRoute, DeleteVpnConnectionRoute, and ModifyVpnTunnelCertificate.
- VPN single tunnel and VPN tunnel endpoint replacement notifications are not available.
- IPv6 is not supported.
- You cannot initiate Internet Key Exchange (IKE) negotiations for your VPN connections from AWS.
- The following algorithms are not supported:
  - Encryption: AES128-GCM-16, AES256-GCM-16
  - Integrity: SHA2-384, SHA2-512
  - Diffie-Hellman groups: 19, 20, 21
- The following APIs are not supported: GetVpnConnectionDeviceTypes and GetVpnConnectionDeviceSampleConfiguration.
- Sample configuration files using IKEv2 are not available.

- AWS Site-to-Site VPN private IP VPN with AWS Direct Connect is not available.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.
- AWS Site-to-Site VPN logging feature is not available.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with AWS VPN and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to AWS VPN by using the command line or APIs, use the following endpoint:

- https://ec2.us-isob-east-1.sc2s.sgov.gov

## Documentation for AWS VPN

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how AWS VPN differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- AWS Client VPN Administrator Guide
- AWS Client VPN User Guide
- Amazon EC2 API Reference
- AWS Site-to-Site VPN Network Administrator Guide
- AWS Site-to-Site VPN User Guide
- Amazon EC2 API Reference

# Amazon WorkSpaces

Amazon WorkSpaces is a managed, secure cloud desktop service. You can use Amazon WorkSpaces to provision either Windows or Linux desktops in just a few minutes and quickly scale to provide thousands of desktops to workers across the globe. You can pay either monthly or hourly, just for the WorkSpaces you launch, which helps you save money when compared to traditional desktops and on-premises VDI solutions. Amazon WorkSpaces helps you eliminate the complexity in managing hardware inventory, OS versions and patches, and Virtual Desktop Infrastructure (VDI), which helps simplify your desktop delivery strategy. With Amazon WorkSpaces, your users get a fast, responsive desktop of their choice that they can access anywhere, anytime, from any supported device.

**Topics**



## How WorkSpaces Differs for AWS Secret Region

The implementation of WorkSpaces is different for AWS Secret Region in the following ways:

- The AWS service principal for Amazon WorkSpaces is `workspaces.amazonaws.com`.
- Graphics and GraphicsPro WorkSpaces are not available in the AWS Secret Region.
- Bring Your Own License (BYOL) is not available in the AWS Secret Region.
- The Web Access client is not available in the AWS Secret Region.
- Amazon WorkSpaces Application Manager (Amazon WAM) is not available in the AWS Secret Region.
- Redirection across AWS Regions (cross-Region redirection) is not supported in the AWS Secret Region.
- Simple AD is not available in the AWS Secret Region.
- Amazon WorkDocs is not available in the AWS Secret Region.

- In order to register a WorkSpaces Directory, the IAM Role `workspaces_DefaultRole` needs to be created and added for your account. See How to Add the Required IAM Role Needed to Register a Directory for WorkSpaces in the AWS Secret Region for details on how to do this.
- To register a directory for use with WorkSpaces, the directory must be located in the `us-isob-1b` or the `us-isob-1c` Availability Zone. WorkSpaces is not available in the `us-isob-1a` Availability Zone.
- The WorkSpaces client `.msi` file is downloaded from Amazon S3 in the AWS Secret Region. See Downloading WorkSpaces Clients in the AWS Secret Region for details.
- CloudWatch Logging of Successful Login Events is not available.
- Because public internet access to public update servers (including the Microsoft Update Server) is unavailable in the AWS Secret Region, customers need to distribute software updates (not changes to the configuration) to update the Windows OS (using SCCM or a WSUS server), and individual applications running on Amazon WorkSpaces.
- Custom branding is not available in AWS Secret Region.
- WorkSpace Client Diagnostic Log Uploads are not available in the AWS Secret Region.
- CreateUpdatedWorkspaceImage is not available in AWS Secret Region.
- WorkSpaces Web is not available in AWS Secret Region.
- The "Remember me" feature for self-service permissions is not available in AWS Secret Region.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only signature version 4 signing is supported.

## How to Add the Required IAM Role Needed to Register a Directory for WorkSpaces in the AWS Secret Region

1. From the AWS Console, go to IAM.
2. Under **Roles**, click **Create role**.
3. Under **Choose the service that will use this role**, select **EC2**.
4. Click **Next: Tags**.
5. Click **Next: Review**.
6. In the **Role Name** field, enter `workspaces_DefaultRole` and enter a Role Description of your choice.
7. Click **Create role**.

8. In **Roles**, click the role you created: `workspaces_DefaultRole`.
9. Under the **Permissions** tab, click **Add inline policy**.
10. Under the **JSON** tab, paste this permission:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Action": [
"ec2:CreateNetworkInterface",
"ec2:DeleteNetworkInterface",
"ec2:DescribeNetworkInterfaces",
"ds:DescribeDomains"
],
"Effect": "Allow",
"Resource": "*"
}
]
}
```

11. Click **Review policy**.
12. In the **Name** field, enter `WorkSpacesServiceAccess`.
13. Click **Create policy**.
14. In **Roles**, click the role you created: `workspaces_DefaultRole`.
15. Under the **Trust relationships** tab, click **Edit trust relationship**.
16. In the **Policy Document field**, remove the existing text, and paste this trust policy:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"Service": "workspaces.amazonaws.com"
},
"Action": "sts:AssumeRole"
}
]
}
```

17. Click **Update Trust Policy**.

## Downloading WorkSpaces Clients in the AWS Secret Region

- The Windows Desktop Client for the AWS Secret Region can be downloaded by end users here.
- The Linux Client for AWS Secret Region (.deb) can be downloaded by end users here.

## How Command Line and API Access Differs for AWS Secret Region

You can use the AWS Command Line Interface (AWS CLI) to interact with WorkSpaces and other AWS services through the command line. For more information, see AWS CLI.

> **Note**
>
> If you are using Amazon Linux 2 or the Amazon Linux AMI, the AWS CLI is already installed and configured. For more information, see Amazon Linux 2 AMI for AWS Secret Region or Amazon Linux AMI for AWS Secret Region.

To connect to WorkSpaces by using the command line or APIs, use the following endpoint:

- https://workspaces.us-isob-east-1.sc2s.sgov.gov

## Documentation for WorkSpaces

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how WorkSpaces differs for AWS Secret Region, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Secret Region. There are other differences, such as links, endpoints, and screenshots.

- Amazon WorkSpaces Admin Guide
- Amazon WorkSpaces User Guide
- Amazon WorkSpaces API Reference
- Amazon WorkSpaces section of AWS CLI Reference

# Document History

The following table describes the document history for *AWS Secret Region User Guide*.

> **Note**
>
> For new Features and updates of AWS Services already in AWS Secret Region, please refer to the AWS Secret Region Marketing page.

**Latest significant documentation updates can be referenced in below table:**

| Change | Description | Date |
|---|---|---|
| Amazon EventBridge | EventBridge Pipes is not supported. The EventBridge Scheduler service is not supported. | June 19, 2024 |
| AWS CloudFormation | The AWS CloudFormation AWS::LanguageExtensions transform is available in AWS Secret Region. | June 19, 2024 |
| AWS Config | Added a link to a list of supported AWS Config managed rules by Region availability. | June 19, 2024 |
| AWS KMS | AWS KMS does not support the `KeyUsage` value of `KEY_AGREEMENT` for asymmetric keys in AWS Secret Region. | June 19, 2024 |
| AWS KMS | AWS KMS does not support the DeriveSharedSecret | June 19, 2024 |

| | | |
|---|---|---|
| | operation in AWS Secret Region. | |
| Amazon EMR | Version 5.36.2 is now available in AWS Secret Region. | June 12, 2024 |
| Amazon EC2 | Amazon Linux 2023 is now available. | June 12, 2024 |
| AWS Lambda | `ReportBatchItemFailures` and `ParallelizationFactor` event source mapping parameters are now available. | June 12, 2024 |
| Amazon S3 | Date-based partitioning of Amazon S3 Server Access Logs is now supported in AWS Secret Region. | June 5, 2024 |
| Amazon Route 53 | Dual-stack endpoint types are now supported. | June 5, 2024 |
| Amazon Route 53 | DNS over HTTPS is now supported. | June 5, 2024 |
| AWS Config | AWS Config custom rules created with Guard are now supported. | June 5, 2024 |
| AWS Lambda | Lambda now supports increased ephemeral storage in AWS Secret Region. | June 5, 2024 |
| Amazon S3 | Amazon S3 now supports the `GetObjectAttributes` API operation in AWS Secret Region. | May 29, 2024 |

| | | |
|---|---|---|
| AWS KMS | Importing asymmetric and HMAC keys is now supported in AWS Secret Region. | May 29, 2024 |
| Security Hub | Security Hub is now available in AWS Secret Region. | May 22, 2024 |
| Amazon WorkSpaces | The "Remember me" feature for self-service permissions is not available in AWS Secret Region. | May 22, 2024 |
| Amazon RDS | Amazon RDS Extended Support isn't available. | May 22, 2024 |
| Amazon RDS | Events in the security patching event category aren't available. | May 22, 2024 |
| AWS CloudFormation | The force delete stack option is not available in AWS Secret Region. | May 22, 2024 |
| Amazon Redshift | RA3.xplus node types are now available in AWS Secret Region. | May 15, 2024 |
| Lambda | Lambda Kinesis trigger cross-account access is not available in AWS Secret Region. | May 8, 2024 |
| Amazon S3 | Generating a manifest is only supported for Amazon S3 Batch Replication jobs in AWS Secret Region. | May 8, 2024 |

| | | |
|---|---|---|
| Amazon S3 | Amazon S3 Batch Operations and Amazon S3 Batch Replication are now available in AWS Secret Region. | May 8, 2024 |
| Amazon RDS | Copying an option group isn't available. | May 8, 2024 |
| Amazon EC2 | The DescribeInstanceEventNotificationAttributes, RegisterInstanceEventNotificationAttributes, and DeregisterInstanceEventNotificationAttributes APIs are now available in . | May 8, 2024 |
| Amazon OpenSearch Service | Custom dictionaries are now supported. | May 1, 2024 |
| AWS Management Console | Unified Search only supports service and feature searches. Console Home widgets are unavailable. myApplications is unavailable. | May 1, 2024 |
| Amazon Simple Queue Service | The SQS dead-letter queue redrive feature is now supported for this region. | April 24, 2024 |
| Amazon Route 53 | Route 53 Profiles are not available. | April 24, 2024 |
| AWS CDK | Added bootstrapping instructions. | April 24, 2024 |

| | | |
|---|---|---|
| License Manager | Updated the differences to include subscription products that are not available in AWS Secret Region. | April 17, 2024 |
| Amazon RDS | All SQL Server options are now supported. | April 17, 2024 |
| AWS Lambda | The Ruby 3.3 (`ruby3.3`) runtime is not available in AWS Secret Region. | April 17, 2024 |
| Amazon Data Firehose | Inaugural launch into AWS Secret Region. | April 10, 2024 |
| Application Auto Scaling | SageMaker endpoint variants are now supported. | April 3, 2024 |
| Amazon S3 | Amazon S3 now supports notifications for the event types of `S3 Lifecycle expiration events` , `S3 Lifecycle transition events`, `Object ACL PUT events`, `Object tagging events`, and the `s3:ObjectRestore:Delete` event in AWS Secret Region. | April 3, 2024 |
| Amazon EMR | Version 6.15.0 is now available in AWS Secret Region. | April 3, 2024 |

| | | |
|---|---|---|
| AWS Snowball Edge | Amazon S3 Compatible Storage is not available on Snowball Edge Compute Optimized with AMD EPYC Gen1, HDD, and optional GPU in AWS Secret Region. | April 3, 2024 |
| Amazon S3 | Amazon S3 on Outposts is now supported in AWS Secret Region. | March 27, 2024 |
| Amazon EKS | Corrected the list of features of the AWS Load Balancer Controller that aren't available. | March 27, 2024 |
| AWS Elemental MediaPackage | MediaPackage V2 features aren't available in AWS Secret Region. | March 27, 2024 |
| AWS Elemental MediaLive | Inaugural launch into AWS Secret Region. | March 27, 2024 |
| AWS Outposts | Amazon S3 on Outposts is now supported in AWS Secret Region. | March 27, 2024 |
| AWS Transit Gateway | Appliance mode is now supported. | March 27, 2024 |
| Amazon VPC | You can view and use AWS-managed prefix lists with security groups only. | March 20, 2024 |
| Amazon RDS | There's no longer a maximum number of databases supported on a Microsoft SQL Server DB instance. | March 20, 2024 |

| | | |
|---|---|---|
| Amazon OpenSearch Service | OpenSearch version 2.11 is now supported. | March 20, 2024 |
| Amazon DynamoDB | Resource-based policies are not available. | March 20, 2024 |
| Amazon DynamoDB | Global Tables are not available in AWS Secret Region. | March 20, 2024 |
| Amazon DynamoDB | AWS PrivateLink is not supported for DynamoDB. | March 20, 2024 |
| AWS Snowball Edge | AWS Snowball Edge Storage Optimized 210TB is now available in AWS Secret Region. | March 20, 2024 |
| AWS Snowball Edge | AWS Snowball with Tape Gateway is not available in AWS Secret Region. | March 20, 2024 |
| AWS CloudFormation | Stack drift detection is available in . | March 20, 2024 |
| Amazon WorkSpaces | Added download link for Linux Client. | March 13, 2024 |
| Amazon VPC | When creating a DHCP option set, the IPv6 Preferred Lease Time option is not available. | March 13, 2024 |
| Amazon EKS | Amazon Linux 2023 isn't available. | March 13, 2024 |
| AWS Storage Gateway | AWS Storage Gateway is now available in AWS Secret Region | March 13, 2024 |

| | | |
|---|---|---|
| Amazon EKS | The Amazon EFS Cloud Storage Interface (CSI) driver is now available. | March 6, 2024 |
| AWS Step Functions | Integration with AWS services available as of December 23, 2023 are supported in if these services are available in the Region. | March 6, 2024 |
| Amazon ECS | Extensible Ephemeral Storage on AWS Fargate is supported , EphemeralStorageReservation and Ephemeral StorageUtilization metrics are available in CloudWatch Container Insights in AWS Secret Region. | February 28, 2024 |
| AWS Lambda | The .NET 8 (`dotnet8`) runtime is not available in AWS Secret Region. | February 28, 2024 |
| Amazon CloudWatch | Using AWS CloudFormation to add or remove tags on CloudWatch alarms is not supported. | February 21, 2024 |
| AWS Step Functions | Added support for AWS PrivateLink, so you can start a workflow from your Amazon Virtual Private Cloud without traversing the public internet. | February 21, 2024 |
| AWS Systems Manager | Patch Manager now supports Windows or Mac Operating Systems. | February 21, 2024 |

| | | |
|---|---|---|
| AWS Systems Manager | In the Parameter Store capability, the shared parameters feature is not available. | February 21, 2024 |
| Amazon Simple Queue Service | Amazon SQS Extended Client Library for Python is not supported. | February 14, 2024 |
| AWS CloudTrail | Downloading events from the **Insights** page on the AWS Management Console is not supported. | February 14, 2024 |
| AWS Transit Gateway | Amazon CloudWatch metrics per attachment are now supported in AWS Secret Region. | February 14, 2024 |
| AWS CloudFormation | AWS CloudFormation in AWS Secret Region does not support AWS CloudFormation IaC generator (infrastructure as code generator). | February 7, 2024 |
| AWS Config | AWS Config service-linked roles (such as `AWSServiceRoleForConfig`) are now supported. | February 7, 2024 |
| AWS Lambda | The Python 3.11 (`python3.11`) runtime is now available in AWS Secret Region. | February 7, 2024 |
| Amazon WorkSpaces | Non-Windows desktop clients are now supported in the AWS Secret Region. | January 31, 2024 |

| | | |
|---|---|---|
| Amazon EFS | File systems using Elastic throughput can drive a maximum of 90,000 read IOPS for infrequently accessed data. | January 31, 2024 |
| AWS CloudTrail | You can now configure advanced event selectors for trails by using the AWS Management Console. | January 31, 2024 |
| AWS Identity and Access Management | The aws:RequestedRegion global condition key is now supported. | January 31, 2024 |
| AWS Step Functions | Support for using the `Map` state in Distributed mode and setting up large-scale parallel workloads are now available. | January 31, 2024 |
| Amazon WorkSpaces | Self-Service WorkSpaces Client is now available. | January 24, 2024 |
| Amazon EC2 Auto Scaling | Amazon EC2 Auto Scaling now supports configuring an instance refresh to set its status to failed and roll back when it detects that a specified CloudWatch alarm has gone into the `ALARM` state. | January 24, 2024 |
| Amazon Simple Queue Service | Attribute-based access control (ABAC) is now supported. | January 17, 2024 |
| Amazon Route 53 | Route 53 Resolver Firewall is not supported. | January 17, 2024 |

| | | |
|---|---|---|
| AWS Billing and Cost Management | When opting in to Cost Explorer, only the current month's data is available. Access to AWS Cost Explorer in the console is provided by the `aws-portal:ViewBilling` permission. Granular permissions provided by `ce:*` actions are not supported in AWS Secret Region. | January 17, 2024 |
| AWS Lambda | The Future runtime launch dates are not applicable in AWS Secret Region. | January 17, 2024 |
| AWS ParallelCluster | Amazon EC2 Capacity Blocks for ML is not supported | January 17, 2024 |
| Amazon WorkSpaces | WorkSpaces Web is not available in AWS Secret Region. | January 10, 2024 |
| Amazon S3 | Amazon S3 does not support the `GetObjectAttributes` API operation in AWS Secret Region. | January 10, 2024 |
| Amazon Redshift | Amazon Redshift query editor is not available in AWS Secret Region. | January 10, 2024 |
| Amazon EKS | Amazon EKS Upgrade insights aren't available. | January 10, 2024 |
| Amazon EC2 Auto Scaling | Amazon EC2 Auto Scaling now supports instance maintenance policies in AWS Secret Region. | January 10, 2024 |

| | | |
|---|---|---|
| Amazon EC2 | UEFI boot mode is not supported. | January 10, 2024 |
| AWS Config | AWS Config recording of third-party resources is now supported. | January 10, 2024 |
| Amazon SageMaker | SageMaker Search – Search does not return results for SageMaker features that are not available in AWS Secret Region. | December 27, 2023 |
| Amazon SageMaker | Model tuning (HPO) is now supported. | December 27, 2023 |
| Amazon SageMaker | Asynchronous Inference and Serverless Inference are not supported. | December 27, 2023 |
| Amazon Route 53 | DNS over HTTPS is not supported. | December 27, 2023 |
| Amazon Kinesis Data Streams | Only **Extended data retention** (retention of up to seven days) is supported . **Long-term data retention** (retention of more than seven days and up to 365 days) is not supported. | December 27, 2023 |
| Amazon OpenSearch Service | OpenSearch version 2.9 is now supported. | December 20, 2023 |
| Amazon OpenSearch Service | Cross-cluster search, cross-clu ster replication, and remote reindex are now supported. | December 20, 2023 |

| | | |
|---|---|---|
| Amazon EKS | Amazon EKS Pod Identities aren't available. | December 20, 2023 |
| Amazon EC2 Image Builder | Image Builder doesn't support image lifecycle policies and image workflows in . | December 20, 2023 |
| Amazon EC2 | Launching an instance with an AWS Marketplace AMI is not supported in AWS Secret Region. | December 20, 2023 |
| Amazon CloudWatch | Contributor Insights with CloudWatch is now supported . | December 20, 2023 |
| AWS Lambda | The Python 3.12 (`python3.12`) runtime is not available in AWS Secret Region. | December 20, 2023 |
| Amazon EFS | Replicating to an existing file system is not supported | December 13, 2023 |
| AWS CloudFormation | The AWS CloudFormation registry now available. | December 13, 2023 |
| AWS Lambda | The asynchronous invocation metrics, `AsyncEventsReceived`, `AsyncEventAge`, and `AsyncEventsDropped` are now available in AWS Secret Region. | December 13, 2023 |
| AWS Step Functions | Remove a bullet about Support for accessing cross-account resources is not available. | December 13, 2023 |

| | | |
|---|---|---|
| AWS Step Functions | Support to call third-party APIs is not available. | December 13, 2023 |
| Amazon S3 | Amazon S3 Object Lock is now available in AWS Secret Region. | December 6, 2023 |
| Amazon EKS | Mountpoint for Amazon S3 CSI Driver is only available as a self-managed installation. | December 6, 2023 |
| Amazon DynamoDB | DynamoDB operation logging to CloudTrail now includes more than just control plane activities. | December 6, 2023 |
| AWS CloudTrail | When logging CloudTrail data events, Amazon DynamoDB API activity on streams is now available. | December 6, 2023 |
| AWS Lambda | Lambda Advanced Logging Controls are not available in AWS Secret Region. | December 6, 2023 |
| AWS Secrets Manager | Secrets Manager API BatchGetSecretValue is not supported. | December 6, 2023 |
| Amazon VPC | Security group referenci ng support for transit gateways and transit gateway attachments is not available. | November 22, 2023 |

| | | |
|---|---|---|
| Amazon VPC | You can now assign a primary private IPv4 address to the NAT gateway. You can also associate secondary private IPv4 addresses and secondary Elastic IP addresses to a NAT gateway. | November 22, 2023 |
| Amazon S3 | Amazon S3 does not support date-based partitioning in S3 Server Access Logs in AWS Secret Region. | November 22, 2023 |
| Amazon EKS | Added that the CSI snapshot controller is only available as a self-managed installation. Added missing statement that Amazon Managed Service for Prometheus isn't available . Added additional links, reorganized the order to match the user guide better, and other cleanup. | November 22, 2023 |
| Amazon EFS | The Elastic Throughput mode is now available. | November 22, 2023 |
| Amazon EC2 Auto Scaling | Amazon EC2 Auto Scaling does not currently support instance maintenance policies in AWS Secret Region. | November 22, 2023 |
| Amazon EC2 | Amazon EC2 instance topology is not available in AWS Secret Region. | November 22, 2023 |

| | | |
|---|---|---|
| AWS CloudFormation | Interface VPC endpoints (AWS PrivateLink) for AWS CloudFormation are now available in the Secret-US-East. | November 22, 2023 |
| AWS Lambda | Multi-VPC connectivity for Amazon Managed Streaming for Apache Kafka event source mappings is not available in AWS Secret Region. | November 22, 2023 |
| AWS Lambda | The Java 21 (`java21`) runtime is not available in AWS Secret Region. | November 22, 2023 |
| Elastic Load Balancing | Application Load Balancers in AWS Secret Region now support weighted target groups. | November 15, 2023 |
| Amazon S3 | Amazon S3 Lifecycle rules based on object size is now available in AWS Secret Region. | November 15, 2023 |
| Amazon OpenSearch Service | OpenSearch version 2.7 is now supported. | November 15, 2023 |
| Amazon EKS | Added missing statements that Amazon EKS Anywhere, Amazon CloudWatch Observability Operator, and AWS Distro for OpenTelem etry (ADOT) Operator aren't available. | November 15, 2023 |

| | | |
|---|---|---|
| AWS Health | Added support for AWS Health Dashboard - Service health | November 15, 2023 |
| AWS Lambda | The Amazon Linux 2023 (`provided.al2023`) runtime is not available in AWS Secret Region. | November 15, 2023 |
| AWS Lambda | The Node.js 20 (`nodejs20.x`) runtime is not available in AWS Secret Region. | November 15, 2023 |
| Amazon EMR | Updated and reformatted list of supported instance types. | November 8, 2023 |
| AWS CloudTrail | You can only configure advanced event selectors for trails by using the AWS CLI. Configuration using the AWS Management Console is not supported. | November 8, 2023 |
| Cloud Control API | New service launch. | November 1, 2023 |
| Amazon SNS | Custom data identifiers are not supported. | November 1, 2023 |
| Amazon EKS | Amazon EKS Extended Support for Kubernetes Versions isn't available. | November 1, 2023 |
| Amazon EKS | Fully private cluster functionality is now available. | November 1, 2023 |
| Amazon SNS | Amazon SNS message archiving and replay is not supported. | October 25, 2023 |

| | | |
|---|---|---|
| Amazon EC2 Auto Scaling | You can now use an instance reuse policy to return instances to a warm pool when your Auto Scaling group scales in (terminates instances ). | October 25, 2023 |
| Amazon EC2 | VSS application-consistent snapshot is not available in AWS Secret Region. | October 25, 2023 |
| Amazon DynamoDB | `ReturnValuesOnCond itionCheckFailure` is now available. | October 25, 2023 |
| AWS Lambda | Lambda doesn't support Lambda@Edge in AWS Secret Region. | October 25, 2023 |
| AWS Step Functions | Support for creating state machine versions and aliases is now available. | October 25, 2023 |
| Amazon SageMaker | Amazon SageMaker available in AWS Secret Region. | October 18, 2023 |
| Amazon EMR | Version 5.36.1 now available in AWS Secret Region. | October 18, 2023 |
| Amazon ECS | CloudWatch Container Insights is now supported. | October 18, 2023 |
| AWS Lambda | Outbound IPv6 traffic is not supported in AWS Secret Region. | October 18, 2023 |

| | | |
|---|---|---|
| Amazon VPC | You cannot assign a primary private IPv4 address to the NAT gateway; one is chosen for you at random from the CIDR in the subnet. You cannot associate secondary private IPv4 addresses or secondary Elastic IP addresses to a NAT gateway. | October 11, 2023 |
| Amazon ECS | CloudWatch Container Insights is now supported. | October 11, 2023 |
| Amazon EC2 | Amazon Linux 2023 is not available. | October 11, 2023 |
| Amazon EC2 | Attached EBS status checks are not available in AWS Secret Region. | October 11, 2023 |
| Amazon EC2 | Simplified auto recovery feature is now available in AWS Secret Region. | October 11, 2023 |
| Amazon WorkSpaces | WorkSpaces Streaming Protocol (WSP) is now available in the AWS Secret Region. | October 4, 2023 |
| Amazon SNS | Payload-based message filtering is not supported. | October 4, 2023 |
| Amazon S3 | Amazon S3 now sends Event Notifications to Amazon EventBridge in AWS Secret Region | October 4, 2023 |

| | | |
|---|---|---|
| Amazon EKS | The Amazon EBS CSI driver is now also available as an Amazon EKS managed add-on. | October 4, 2023 |
| Amazon EC2 | The DescribeInstanceEventNotificationAttributes, RegisterInstanceEventNotificationAttributes, and DeregisterInstanceEventNotificationAttributes APIs are not available in AWS Secret Region. | October 4, 2023 |
| AWS CloudFormation | AWS::ApiGateway::VpcLink resource now supported. | October 4, 2023 |
| AWS KMS | The Hybrid Post-Quantum TLS feature is now available in AWS Secret Region. TLS 1.3 is now available in AWS Secret Region. | October 4, 2023 |
| Amazon RDS | The maximum number of databases supported on a Microsoft SQL Server DB instance is 30 for all instance classes. | September 27, 2023 |
| Amazon OpenSearch Service | Audit Logs are now available. | September 27, 2023 |
| Amazon OpenSearch Service | OpenSearch version 2.5 is now supported. | September 27, 2023 |

| | | |
|---|---|---|
| AWS KMS | The feature that allows you to import key material into an AWS KMS key only supports importing symmetric key material in AWS Secret Region. The key material must be a 256-bit symmetric encryption key. Importing asymmetric and HMAC keys is not supported in AWS Secret Region. | September 27, 2023 |
| AWS KMS | The `kms:ScheduleKeyDeletionPendingWindowInDays` condition key, which enables you to further constrain the values that principals can specify in the PendingWindowInDays parameter of a ScheduleKeyDeletion request, is now supported. | September 27, 2023 |
| AWS Step Functions | The Step Functions Workflow Studio is now available. | September 27, 2023 |
| Amazon OpenSearch Service | Amazon Cognito for OpenSearch Dashboards (previously Kibana) is not supported. | September 20, 2023 |
| Amazon EC2 Auto Scaling | The gp3 EBS volume type cann now be specified in the block device mappings for launch configurations. | September 20, 2023 |

| | | |
|---|---|---|
| AWS Identity and Access Management | Web identity federation (authenticating using well-known web-based identity providers) is now available in AWS Secret Region. | September 13, 2023 |
| Amazon SNS | Attribute-based access controls (ABAC) for Amazon SNS resources is now supported. | September 6, 2023 |
| AWS Lambda | Lambda now supports the ability to integrate with Amazon Elastic File System (EFS) natively. | September 6, 2023 |
| AWS Step Functions | Integration with AWS services available as of June 16, 2023 are supported in AWS Secret Region if these services are available in the Region. | September 6, 2023 |
| Aurora | Updated Amazon S3 integrati on features and available instance classes. | August 30, 2023 |
| Amazon EKS | Clusters running Kubernete s v1.27 or higher can use Kubernetes Secrets Store CSI driver with AWS Secrets Manager. | August 30, 2023 |
| Amazon ECR | Encryption with customer master keys (CMKs) is now supported. | August 30, 2023 |

| | | |
|---|---|---|
| Amazon EC2 | `ExportImage` and the Replace Root Volume feature is now supported. | August 30, 2023 |
| AWS Billing and Cost Management | RI discounts sharing is enabled for all accounts in AWS Secret Region and cannot be disabled. The AWS Cost and Usage Reports feature is now available. | August 30, 2023 |
| Aurora | Export to Amazon S3 is supported only for DB snapshots | August 23, 2023 |
| Amazon SNS | Amazon SNS now supports message batching. | August 23, 2023 |
| Amazon RDS | Amazon EFS integration is not available for Oracle in AWS Secret Region. | August 23, 2023 |
| Amazon RDS | Amazon RDS Custom is not available in AWS Secret Region. | August 23, 2023 |
| Amazon OpenSearch Service | OpenSearch version 2.3 is now supported. | August 23, 2023 |
| AWS VPN | AWS Site-to-Site VPN logging feature is not available. | August 23, 2023 |
| Amazon EMR | Version 6.12.0 now available in AWS Secret Region. | August 16, 2023 |
| Amazon DynamoDB | Export to Amazon S3 is now available. | August 16, 2023 |

| | | |
|---|---|---|
| AWS Lambda | TumblingWindowInSeconds and ParallelizationFactor are not available in AWS Secret Region. | August 16, 2023 |
| AWS Outposts | AWS Outposts for racks is now available. | August 16, 2023 |
| AWS Transit Gateway | Appliance mode is not supported. | August 16, 2023 |
| Amazon WorkSpaces | Windows Server 2016 based bundles are now available in the AWS Secret Region. | August 9, 2023 |
| Amazon VPC | You can view and use AWS-managed prefix lists with security groups only. You cannot create, manage, or use customer-managed prefix lists. | August 9, 2023 |
| Amazon S3 | Standard retrievals for restore requests that are made through S3 Batch Operation s have the same restore times as other Standard retrieval requests for AWS Secret Region. | August 9, 2023 |
| Amazon S3 | Server-side encryption with AWS KMS encryption keys (SSE-KMS) | August 9, 2023 |
| Amazon EKS | Corrected some links throughout document. | August 9, 2023 |

| | | |
|---|---|---|
| Amazon EC2 Auto Scaling | Amazon EC2 Auto Scaling does not currently support configuring an instance refresh to set its status to failed and roll back when it detects that a specified CloudWatch alarm has gone into the `ALARM` state. | August 9, 2023 |
| AWS Secrets Manager | AWS Config managed rules for Secrets Manager are not supported. | August 9, 2023 |
| Lambda | Provisioned concurrency is available in AWS Secret Region, but Application Auto Scaling for provisioned concurrency is not available in AWS Secret Region. | August 2, 2023 |
| Amazon Route 53 | AWS-managed prefix lists are not available. | August 2, 2023 |
| Lambda | The Python 3.11 (`python3.11`) runtime is not available in AWS Secret Region. | July 26, 2023 |
| Amazon RDS | SQL Server Web and Express editions aren't available. | July 26, 2023 |
| Amazon EC2 | General Purpose SSD (gp3) volumes are available in AWS Secret Region. | July 26, 2023 |
| Amazon EBS | The General Purpose SSD (gp3) volume type is available in AWS Secret Region. | July 26, 2023 |

| | | |
|---|---|---|
| Amazon Simple Queue Service | AWS JSON protocol is not supported. | July 19, 2023 |
| Amazon S3 | In AWS Secret Region, Amazon S3 Inventory does not have the Object Access Control List and Object Owner as available object metadata fields in inventory reports. | July 19, 2023 |
| Amazon Linux 2 | Added instructions to install Python3 based Botocore on Amazon Linux 2 | July 19, 2023 |
| Amazon EKS | Fully private cluster functionality isn't available. | July 19, 2023 |
| AWS ParallelCluster | AWS ParallelCluster now supports AWS Secrets Manager | July 19, 2023 |
| Amazon RDS | Read replicas for Amazon RDS for Oracle aren't supported. | July 12, 2023 |
| Amazon EMR | Version 6.11.0 now available in AWS Secret Region. | July 12, 2023 |
| Amazon EC2 Auto Scaling | Instance refresh rollback features are now available in AWS Secret Region. | July 12, 2023 |
| AWS Step Functions | Support for creating state machine versions and aliases is not available. | July 12, 2023 |

| | | |
|---|---|---|
| Lambda | The Java 17 (`java17`), Ruby 3.2 (`ruby3.2`), and Python 3.10 runtimes are now available in AWS Secret Region. | July 5, 2023 |
| Amazon EKS | Amazon EKS AWS CloudFormation resources and `Eksctl` are now available. | July 5, 2023 |
| Amazon DynamoDB | `ReturnValuesOnConditionCheckFailure`, an optional parameter that returns the item attributes for an operation that fails a condition check, is not available. | July 5, 2023 |
| Amazon S3 | Amazon S3 Bucket Keys for SSE-KMS are now available in AWS Secret Region. | June 28, 2023 |
| Amazon EC2 | Capacity Reservation Fleet is not supported with the Amazon EC2 console. It is supported with the AWS CLI and SDKs only. | June 28, 2023 |
| AWS Config | Moved the list of supported resource types to Resource Coverage by Region Availability. | June 28, 2023 |
| AWS Systems Manager | Patch Manager is now available. | June 28, 2023 |

| | | |
|---|---|---|
| Amazon S3 | Amazon S3 Inventory reports are now available in Apache optimized row columnar (ORC) or Apache Parquet (Parquet) formats in AWS Secret Region. | June 21, 2023 |
| Amazon ECS | The `splunk` log driver is not supported in the AWS Secret Region. | June 21, 2023 |
| AWS Snowball Edge | AWS Snowball Edge Storage Optimized 210TB is not available in AWS Secret Region. | June 21, 2023 |
| Amazon EC2 | Amazon EC2 Instance Connect Endpoint is not available in AWS Secret Region. | June 14, 2023 |
| AWS Account Management | Account Management page added to this guide. | June 14, 2023 |
| AWS Step Functions | Express Workflows are now available. | June 14, 2023 |
| Lambda | The Ruby 3.2 (`ruby3.2`) runtime is not available. | June 7, 2023 |
| Amazon S3 | Amazon S3 on Outposts is not supported in AWS Secret Region. | June 7, 2023 |
| Amazon ECS | Extensible Ephemeral Storage on AWS Fargate is not supported in the AWS Secret Region. | June 7, 2023 |

| | | |
|---|---|---|
| AWS Config | AWS Config Updates to supported resource types. | June 7, 2023 |
| AWS KMS | The `kms:ScheduleKeyDeletionPendingWindowInDays` condition key, which enables you to further constrain the values that principals can specify in the PendingWindowInDays parameter of a ScheduleKeyDeletion request, is not supported in AWS Secret Region. | June 7, 2023 |
| AWS Resource Access Manager | AWS RAM on AWS Outposts is not yet supported. | June 7, 2023 |
| Application Auto Scaling | Reworked the differences section. | May 31, 2023 |
| Amazon VPC | DNS64 and NAT64 are not available | May 31, 2023 |
| AWS Step Functions | The Amazon EMR service integration is now available. | May 31, 2023 |
| Amazon WorkSpaces | CreateUpdatedWorkspaceImage is not available in AWS Secret Region. | May 24, 2023 |
| Amazon EC2 Auto Scaling | Amazon EC2 Auto Scaling does not currently support the AttachTrafficSources, DetachTrafficSources, and DescribeTrafficSources API operations. | May 24, 2023 |

| | | |
|---|---|---|
| Amazon EBS | Recycle Bin is now available. | May 24, 2023 |
| Amazon WorkSpaces | CreateWorkspaceImage API is now available in the AWS Secret Region. | May 17, 2023 |
| Amazon RDS | Updated the availability of SQL Server editions and DB engine versions. | May 17, 2023 |
| AWS Snowball Edge | Snowball Edge devices in the AWS Secret Region do not have an embedded GPS module. | May 17, 2023 |
| AWS Billing and Cost Management | Savings Plans are not supported in AWS Secret Region. | May 17, 2023 |
| AWS Directory Service | AWS PrivateLink is not currently supported by AWS Directory Service. | May 17, 2023 |
| AWS Systems Manager | Updated the windows download link. | May 17, 2023 |
| Image Builder | Image Builder doesn't support AWS CloudFormation for container images in AWS Secret Region. | May 10, 2023 |
| Amazon S3 | Amazon S3 Bucket Access Points, Amazon S3 Access Points aliases, and Amazon S3 Block Public Access are now available. | May 10, 2023 |
| Amazon EMR | Version 6.10.0 now available in AWS Secret Region. | May 10, 2023 |

| | | |
|---|---|---|
| Amazon EC2 | ED25519 keys are now supported when using the Amazon EC2 console. | May 10, 2023 |
| Amazon CloudWatch Logs | Creating a subscription to stream logs data to Amazon OpenSearch Service is not supported. | May 10, 2023 |
| AWS Step Functions | Removed a note about Lambda availability in the differences list. | May 10, 2023 |
| AWS Transit Gateway | Multicast is now supported. | May 10, 2023 |
| Lambda | The Java 17 (`java17`) runtime is not available. | May 3, 2023 |
| Amazon OpenSearch Service | Amazon OpenSearch Ingestion is not supported. | May 3, 2023 |
| Amazon Kinesis Data Streams | Kinesis Data Streams On Demand does not support 1 GB/s increase in write capacity and 2GB/s read capacity. | May 3, 2023 |
| Amazon EC2 | AMD Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP) is not available. | May 3, 2023 |
| AWS CloudTrail | CloudTrail Lake is not available. | May 3, 2023 |
| AWS Systems Manager | Patch Manager does not support Windows or Mac Operating Systems. | May 3, 2023 |

| | | |
|---|---|---|
| Amazon DynamoDB | Restores are limited to 4 concurrent operations. | April 26, 2023 |
| AWS Snowball Edge | AWS Snowball Edge Compute Optimized is now available in AWS Secret Region. | April 26, 2023 |
| AWS Direct Connect | AWS Direct Connect gateways are now supported in AWS Secret Region. | April 26, 2023 |
| AWS Directory Service | Added additional features not supported in AWS Secret Region. | April 26, 2023 |
| Lambda | The Python 3.10 runtime is not available in AWS Secret Region. | April 19, 2023 |
| Amazon Redshift | Updated links for redshift drivers. | April 19, 2023 |
| Amazon RDS | Kerberos authentication isn't supported in the RDS console. | April 19, 2023 |
| Amazon EFS | The Elastic Throughput mode is not available. | April 19, 2023 |
| Amazon CloudWatch | Composite alarm action suppression with AWS CloudFormation is now supported. | April 12, 2023 |

| | | |
|---|---|---|
| AWS Snowball Edge | For Compute using EC2-compatible instances you need to have one or more supported AMIs in your AWS account before you can add any AMIs to your job creation request otherwise you will see "You have no compatible AMIs". | April 12, 2023 |
| Image Builder | Added difference for CVE findings, and updated wording for some of the exi sting content. | April 6, 2023 |
| Elastic Load Balancing | Elastic Load Balancing does not support standalone creation of target groups with protocol version HTTP/2 or gRPC in AWS Secret Region. | April 5, 2023 |
| Customer Compliance Guide | Customer Compliance Guide is now available. | April 5, 2023 |
| Amazon RDS | Kerberos authentication is only supported for RDS for MySQL DB instances. | April 5, 2023 |
| Amazon EKS | Amazon GuardDuty isn't available. | April 5, 2023 |
| Amazon EC2 | UEFI boot mode on Intel- and AMD-based instances is available in AWS Secret Region. | April 5, 2023 |

| | | |
|---|---|---|
| Amazon EC2 | Capacity Reservation sharing is available in AWS Secret Region. | April 5, 2023 |
| Amazon EC2 | Capacity Reservation resource groups are available in AWS Secret Region. | April 5, 2023 |
| Amazon RDS | Updated MS SQL Server features in AWS Secret Region. | March 29, 2023 |
| Amazon ElastiCache | Reader endpoints are not available in AWS Secret Region. | March 29, 2023 |
| Amazon EMR | The old Amazon EMR management console is the default console for AWS Secret Region. | March 29, 2023 |
| Amazon EMR | Version 6.9.0 now available in AWS Secret Region. | March 29, 2023 |
| AWS Snowball Edge | Snowball Edge cluster feature is now available in AWS Secret Region. | March 29, 2023 |
| AWS ParallelCluster | AWS ParallelCluster is now available in AWS Secret Region. | March 29, 2023 |
| Amazon EKS | Added link to Kubernetes versions in documentation. | March 22, 2023 |
| Amazon EC2 Auto Scaling | The metric math feature for target tracking scaling policies is not available. | March 22, 2023 |

| | | |
|---|---|---|
| AWS KMS | List of HMAC keys types that cannot be created/managed with a CFN template in AWS Secret Region. | March 22, 2023 |
| Amazon OpenSearch Service | AWS::OpenSearchService::Domain CloudFormation is now supported. | March 15, 2023 |
| Amazon EKS | Amazon EKS Advanced Configuration is now available. | March 15, 2023 |
| Amazon EC2 | EC2 Image Builder is now available in AWS Secret Region. | March 15, 2023 |
| Amazon EC2 | Stop Protection feature is now available in AWS Secret Region. | March 15, 2023 |
| Amazon CloudWatch | AWS Systems Manager is now available in AWS Secret Region. | March 15, 2023 |
| AWS KMS | HMAC KMS keys are now available in AWS Secret Region. | March 15, 2023 |
| Lambda | Added DocumentDB as an event source (link). | March 8, 2023 |
| Amazon Route 53 | IPv6 and dual-stack Route 53 endpoint types are not supported. | March 8, 2023 |
| AWS Serverless Application Model | Updated multi-destination connectors region availability. | March 8, 2023 |

| | | |
|---|---|---|
| Amazon ECS | Task definition deletion is not supported. | March 1, 2023 |
| AWS Snowball Edge | AWS Lambda compute functionality is now available in AWS Secret Region. | March 1, 2023 |
| AWS Config | AWS Config Updates to supported resource types. | March 1, 2023 |
| AWS Serverless Application Model | Multi-destination connectors for AWS SAM is not available. | March 1, 2023 |
| Lambda | ReportBatchItemFailures is not available in AWS Secret Region. | February 22, 2023 |
| Amazon ECR | Amazon ECR multi-architecture images are supported. | February 22, 2023 |
| AWS Snowball Edge | Amazon EKS Anywhere on Snow is not available in AWS Secret Region. | February 22, 2023 |
| AWS DMS | Added AWS DMS 3.4.7 list of changes. | February 22, 2023 |
| Amazon Route 53 | IPv6 and dual-stack Route 53 endpoint types are now supported. | February 15, 2023 |

| | | |
|---|---|---|
| Amazon EC2 Auto Scaling | The instance refresh rollback features are not available AWS Secret Region; Setting up an instance refresh to ignore or terminate instances that are in `Standby` state or protected from scale in is not supported in AWS Secret Region. | February 15, 2023 |
| Lambda | The asynchronous invocation metrics, `AsyncEventsReceived`, `AsyncEventAge`, and `AsyncEventsDropped` are not available in AWS Secret Region. | February 8, 2023 |
| Elastic Load Balancing | Updated the User Guide links for Application and Gateway Load Balancers. | February 8, 2023 |
| Amazon Route 53 | IPv6 and dual-stack Route 53 endpoint types are not supported and IPv6 is not supported as a Route 53 rule target. | February 8, 2023 |
| AWS Direct Connect | AWS Direct Connect does not require redundant conenctions and virtual interfaces in each availability zone. | February 8, 2023 |

| | | |
|---|---|---|
| Lambda | Some EventInvokeConfig functions and parameters are not available in AWS Secret Region;Maximum concurrency for Amazon SQS event sources (ScalingConfig) is not available in AWS Secret Region;Lambda SnapStart is not available in AWS Secret Region. | February 1, 2023 |
| Aurora | Blue/Green Deployments and Secret Manager integration are not available for Aurora MySQL and Aurora PostgreSQL. | February 1, 2023 |
| Amazon S3 | Restore requests, at a rate of up to 1,000 transactions per second, is now supported in AWS Secret Region; Amazon S3 does not support S3 Intelligent-Tiering archive access Tiers (Archive Access tier and Deep Archive Access tier) in AWS Secret Region. | February 1, 2023 |
| Amazon RDS | Blue/Green deployments and Secrets Manager integration are not supported. | February 1, 2023 |
| AWS Elemental MediaPackage | New service launch. | February 1, 2023 |
| Lambda | Runtime management configuration is not available in AWS Secret Region. | January 25, 2023 |

| | | |
|---|---|---|
| Amazon EFS | One day lifecycle policies are not supported. | January 25, 2023 |
| Amazon EC2 | Amazon Data Lifecycle Manager is now available in AWS Secret Region and AMI aliasing in launch templates is not available. | January 25, 2023 |
| Amazon EBS | Amazon Data Lifecycle Manager is now available in AWS Secret Region. | January 25, 2023 |
| AWS CloudTrail | The IAM condition keys aws:SourceArn and aws:SourceAccount are now supported in resource policies for resources that you associate with a trail. | January 25, 2023 |
| AWS VPN | The following APIs: GetVpnConnectionDeviceTypes and GetVpnConnectionDeviceSampleConfiguration and Sample configuration files using IKEv2 are not supported. | January 25, 2023 |
| Amazon EC2 | Simplified Auto Recovery is not available in AWS Secret Region at this moment. | January 18, 2023 |
| AWS Resource Groups | Group lifecycle events are not supported. | January 18, 2023 |

| | | |
|---|---|---|
| Image Builder | Image Builder doesn't support CIS Hardened Images or the CIS Hardening component in AWS Secret Region. | January 13, 2023 |
| Elastic Load Balancing | TLS support is now available on Network Load Balancers. | January 11, 2023 |
| AWS VPN | The following APIs: GetVpnConnectionDeviceTypes and GetVpnConnectionDeviceSampleConfiguration and Sample configuration files using IKEv2 are now supported. | January 11, 2023 |
| Amazon EKS | You can't use AWS PrivateLink to create a private connection between your Amazon VPC and Amazon EKS. | January 4, 2023 |
| Amazon EFS | One day lifecycle policies are not supported. | January 4, 2023 |
| Amazon EC2 | `ExportImage` is not supported in AWS Secret Region. | January 4, 2023 |
| Amazon EC2 | `ExportImage` is not supported in AWS Secret Region. | January 4, 2023 |
| Amazon CloudWatch Logs | AWS PrivateLink support for CloudWatch Logs is now available. | January 4, 2023 |
| AWS Config | AWS Config Updates to supported resource types. | December 28, 2022 |

| | | |
|---|---|---|
| Amazon EFS | The updated Amazon EFS console that simplifies file system creation and management is available; Creating an Amazon EFS file system automatically using the service preferred settings is available. | December 21, 2022 |
| AWS Billing and Cost Management | The AWS Price List API needs to be SigV4 signed. | December 21, 2022 |
| Amazon OpenSearch Service | OpenSearch version 1.3 is now supported. | December 14, 2022 |
| Amazon EKS | Amazon EKS add-ons - Advanced Configuration isn't available. | December 14, 2022 |
| Amazon ECR | Interface VPC endpoints(AWS PrivateLink) for Amazon ECR are supported. | December 14, 2022 |
| Amazon ECR | Retrieving the Amazon ECS-optimized AMI metadata using the Systems Manager Parameter Store parameter is now supported. Amazon ECS Deployment Circuit Breaker is not supported in AWS Secret Region. Scheduled tasks is not supported for Amazon ECS tasks. | December 14, 2022 |

| | | |
|---|---|---|
| AWS Step Functions | Support for using the `Map` state in Distributed mode, set up large-scale parallel workloads, and accessing cross-account resources is not available. | December 14, 2022 |
| Amazon S3 | Amazon S3 Replication Time Control (S3 RTC) is not available in AWS Secret Region. | December 7, 2022 |
| Amazon EFS | Elastic Throughput mode is not available. | December 7, 2022 |
| Amazon ECR | Amazon ECS Service Connect is not available in AWS Secret Region. | December 7, 2022 |
| AWS KMS | External key stores, a new type of custom key store, are not supported in AWS Secret Region. | November 29, 2022 |
| Amazon Simple Queue Service | Attribute-based access control (ABAC) is not supported. | November 23, 2022 |
| Amazon S3 | Restore requests, at a rate of up to 1,000 transactions per second, is not supported in AWS Secret Regions. | November 23, 2022 |
| Amazon SNS | Active tracing is not supported. | November 16, 2022 |

| | | |
|---|---|---|
| Amazon ElastiCache | IAM Authentication and Redis engine version 7.0 are not supported in AWS Secret Region. | November 16, 2022 |
| Amazon ECR | Container Insights are not supported for Amazon ECS Fargate | November 16, 2022 |
| Amazon EC2 | The former service principal of `ec2.sc2s.sgov.gov` is still supported for backward compatibility. | November 16, 2022 |
| Amazon VPC | The transfer Elastic IP address feature is not available. | November 2, 2022 |
| Amazon OpenSearch Service | The UltraWarm feature is now available. | November 2, 2022 |
| Amazon EventBridge | Amazon EventBridge is now availabl in AWS Secret Region | November 2, 2022 |
| Amazon EC2 Auto Scaling | Specifying a default instance warmup for an Auto Scaling group is now available in AWS Secret Region. | November 2, 2022 |
| Amazon EC2 | Tags in instance metadata are now available in AWS Secret Region, but are not available in the Amazon EC2 console in AWS Secret Region. The transfer Elastic IP address feature is not available. | November 2, 2022 |

| | | |
|---|---|---|
| AWS Config | AWS Config Custom Policy rules with Guard, organizational deployment, remediation actions and monitoring config with EventBridge or CloudWatch are not supported in AWS Secret Region. | November 2, 2022 |
| Lambda | The FilterCriteria parameter is not available in AWS Secret Region. | October 26, 2022 |
| Amazon WorkSpaces | WorkSpace Client Diagnostic Log Uploads are not available in the AWS Secret Region. | October 26, 2022 |
| Amazon Linux 2 | Removed the more information section. | October 26, 2022 |
| AWS Systems Manager | A list of Systems Manager plugin download links were added. | October 26, 2022 |
| AWS Snowball Edge | The enhanced Snowball Edge Compute Optimized with 104 vCPUs, 416GB RAM, and 28TB SSD NVMe Storage is not available in AWS Secret Region. | October 25, 2022 |
| Amazon RDS | Read replicas for SQL Server are not supported. | October 19, 2022 |
| AWS Direct Connect | AWS Direct Connect CNSSP11 Protected Dedicated Circuits are now supported. | October 19, 2022 |

| | | |
|---|---|---|
| Elastic Load Balancing | Elastic Load Balancers in AWS Secret Region now support an endpoint for PrivateLink. | October 12, 2022 |
| Amazon ECR | The following task definitio n sizes are now supported: 8 vCPU, 16 vCPU. | October 5, 2022 |
| Amazon OpenSearch Service | Custom endpoints are not supported. | September 28, 2022 |
| Amazon EC2 | The Simplified automatic recovery feature is now available in AWS Secret Region. | September 28, 2022 |
| Amazon OpenSearch Service | OpenSearch version 1.2 is now supported. | September 21, 2022 |
| Amazon ECR | The following task definitio n sizes are not supported: 8 vCPU, 16 vCPU. | September 21, 2022 |
| AWS Config | AWS Config Rules and remediation are now supported. | September 21, 2022 |
| Windows AMIs | Changes to Windows AMI implementation section. | September 14, 2022 |
| Amazon Route 53 | Resolver endpoints are now available. | September 14, 2022 |
| AWS KMS | Attribute-based access control (ABAC), the ability to control access to an AWS KMS key based on its aliases and tags, is now supported in the AWS Secret Region. | September 14, 2022 |

| | | |
|---|---|---|
| AWS Resource Groups | Resource Groups launched in AWS Secret Region. | September 14, 2022 |
| Aurora | Added a CLI command to identify supported engine versions. | September 7, 2022 |
| Amazon S3 | Glacier Instant Retrieval now available in AWS Secret Region | September 7, 2022 |
| Amazon RDS | Removed MySQL 5.1 unsupported version and added CLI command to list supported engine versions. | September 7, 2022 |
| Amazon EKS | AWS for Fluent Bit is now available. | September 7, 2022 |
| Amazon EC2 | The Optimize CPU Options feature is now available in AWS Secret Region. | September 7, 2022 |
| AWS Systems Manager | Not all Automation runbooks and SSM Command documents are available for AWS Secret Region. | September 7, 2022 |
| Amazon WorkSpaces | Graphics and GraphicsPro WorkSpaces and Bring Your Own License are not available in the AWS Secret Region. | August 31, 2022 |
| Amazon ECR | Amazon ECS Fargate Ephemeral Storage feature is not available in AWS Secret Region. | August 31, 2022 |

| | | |
|---|---|---|
| Amazon EC2 | Amazon EC2 Images now supports create-restore-image-task, create-store-image-task or describe-store-image-task in AWS Secret Region. | August 31, 2022 |
| Amazon WorkSpaces | Graphics, GraphicsPro, Graphics.g4dn, and GraphicsPro.g4dn WorkSpaces are not available in the AWS Secret Region. | August 24, 2022 |
| Amazon OpenSearch Service | The following OpenSearch versions are supported: 1.0, 1.1 | August 24, 2022 |
| Amazon EMR | The document was reworked to improve the customer experience. | August 24, 2022 |
| Amazon S3 | Amazon S3 Object Ownership now available in AWS Secret Region | August 17, 2022 |
| Amazon EBS | You can't exclude data (non-root) volumes from multi-volume snapshot sets in AWS Secret Region. | August 17, 2022 |
| AWS Lambda | Lambda doesn't support increased ephemeral storage in AWS Secret Region. Functions still have 512 MB of ephemeral storage available at /tmp in the file system. | August 10, 2022 |

| | | |
|---|---|---|
| AWS Lambda | Lambda doesn't support the ability to integrate with Amazon Elastic File System (EFS) natively in AWS Secret Region. | August 10, 2022 |
| Elastic Load Balancing | Application Load Balancers in AWS Secret Region do not support weighted target groups. | August 3, 2022 |
| Amazon WorkSpaces | CreateWorkspaceImage API is not available in AWS Secret Region. | August 3, 2022 |
| Amazon EMR | Automatic Amazon Linux updates, as discussed in the Amazon EMR Management Guide , are not enabled in AWS Secret Region. | August 3, 2022 |
| Amazon EC2 | On-demand instance quotas are based on number of vCPUs in AWS Secret Region. | July 27, 2022 |
| Amazon EMR | Amazon EMR version 6.6.0 is now supported and instance types were updated. | July 20, 2022 |
| Amazon ECR | Amazon ECS limit increases aren't available through AWS Service Quotas | July 20, 2022 |
| Amazon CloudWatch | Composite alarm action suppression with AWS CloudFormation is not supported. | July 20, 2022 |

| | | |
|---|---|---|
| Aurora | The underlying storage for Aurora grows automatically as needed, up to 128 tebibytes (TiB) instead of 64 tebibytes. | July 13, 2022 |
| Amazon WorkSpaces | Linux WorkSpaces are now available. Custom branding and Graphics Workspaces are not available in AWS Secret Region. | July 13, 2022 |
| Amazon EKS | ARM, Bottlerocket, and Windows AMIs aren't available in AWS Secret Region. | July 13, 2022 |
| AWS Lambda | Lambda doesn't support base images that conform to the Open Container Initiative (OCI) Specification formats in AWS Secret Region. | July 13, 2022 |
| Amazon ElastiCache | Redis engine version 6.0 is not available, but supported Redis engine 6.2 includes all cumulative updates. | July 6, 2022 |
| Amazon ElastiCache | Role-Based Access Control (RBAC) is not supported in AWS Secret Region. | July 6, 2022 |
| AWS Identity and Access Management | IAM Roles Anywhere is not supported in the AWS Secret Region. | July 6, 2022 |
| Systems Manager | In the Session Manager capability, the Block public sharing for SSM documents feature is not available. | June 29, 2022 |

| | | |
|---|---|---|
| Amazon EKS | Amazon EKS 1.22 is available in AWS Secret Region. | June 29, 2022 |
| Amazon EFS | Amazon EFS Intelligent Tiering now available. | June 29, 2022 |
| Amazon CloudWatch | Choosing custom colors for metrics in the console now available. | June 29, 2022 |
| AWS Lambda | Lambda does not support batch sizes greater than 10 for Lambda SQS triggers. | June 29, 2022 |
| AWS Lambda | For EventSourceMapping Configuration, the MaximumBatchingWindowInSeconds parameter is not available in AWS Secret Region. | June 29, 2022 |
| Amazon EC2 | The Optimize CPU Options feature is not available in in AWS Secret Region. | June 22, 2022 |
| Amazon CloudWatch | Anomaly detection now available. | June 22, 2022 |
| AWS Snowball Edge | T100 Storage Optimized device deprecated in AWS Secret Region. | June 22, 2022 |
| AWS VPN | AWS Site-to-Site VPN private IP VPN with AWS Direct Connect is not available. | June 22, 2022 |

| | | |
|---|---|---|
| Amazon S3 | Amazon S3 event notifications for the event type of `s3:ObjectRestore:Completed` no longer only emitted on a best-effort basis in AWS Secret Region. | June 15, 2022 |
| Amazon ECR | You must explicitly specify the AWS service endpoint in the Fluent Bit output definition using the endpoint option supported by all AWS plugins. | June 15, 2022 |
| Amazon EC2 | The Stop Protection feature is not available in in AWS Secret Region. | June 15, 2022 |
| Amazon EC2 | The Replace Root Volume feature is not available in in AWS Secret Region. | June 15, 2022 |
| Amazon EC2 | The Simplified automatic recovery feature is not available in AWS Secret Region. | June 15, 2022 |
| Aurora | Logical replication available in AWS Secret Region. | June 8, 2022 |
| Amazon WorkSpaces | WorkSpaces inaugural launch into the AWS Secret Region. | June 8, 2022 |
| Amazon EFS | Sub-millisecond read latency now available. | June 8, 2022 |

| | | |
|---|---|---|
| Amazon CloudWatch | CloudWatch Synthetics does not support the `Names` filter parameter for the `DescribeCanaries` operation. | June 8, 2022 |
| Amazon OpenSearch Service | Fine-grained access control is supported. | June 1, 2022 |
| Amazon CloudWatch | CloudWatch Metrics Insights is not available. | May 25, 2022 |
| AWS Snowball Edge | AWS Snow Family Large Data Migration Manager is not available in AWS Secret Region. | May 25, 2022 |
| Amazon EC2 | AMI deprecation is available in AWS Secret Region. | May 18, 2022 |
| Amazon RDS | SQL Server Audit option now available. | May 11, 2022 |
| Amazon RDS | Native backup and restore is supported for SQL Server, but only full backups and restores. Differential backups and restores, and log restores aren't supported. Backup compression isn't supported. | May 11, 2022 |
| Amazon EBS | Amazon EBS CreateSnapshots is available in AWS Secret Region. | May 11, 2022 |
| AWS CloudTrail | CloudTrail can now send events to Amazon CloudWatch Events. | May 11, 2022 |

| | | |
|---|---|---|
| Amazon EFS | Amazon EFS inaugural launch into AWS Secret Region.. | May 4, 2022 |
| AWS Health | You can navigate to the Service Health Dashboard page to view the health of all AWS services without signing in to your AWS account. | May 4, 2022 |
| AWS Health | If you sign in to your AWS account, you can find events specific to your account and services in the Personal Health Dashboard. | May 4, 2022 |
| Amazon VPC | Security group rule IDs are now available in the Amazon Virtual Private Cloud Console. | April 27, 2022 |
| Amazon SNS | Message Data Protection is not supported. | April 27, 2022 |
| Amazon EC2 Auto Scaling | Specifying a default instance warmup for an Auto Scaling group is not available in AWS Secret Region. | April 27, 2022 |
| Amazon EKS | The Amazon EBS CSI driver is only available as a self-mana ged add-on. | April 20, 2022 |

| | | |
|---|---|---|
| AWS KMS | HMAC KMS keys, which generate and verify hash-based message authentic ation codes, are not available in the AWS Secret Region. AWS KMS does not support the `GenerateMac` and `VerifyMac` APIs in the AWS Secret Region. | April 20, 2022 |
| AWS Resource Access Manager | Inaugural launch of AWS RAM in AWS Secret Region. | April 20, 2022 |
| Amazon Elastic Container Service | Amazon ECS Exec Suite not supported against Fargate Containers | April 13, 2022 |
| Amazon ECR | Interface VPC endpoints(AWS PrivateLink) for Amazon ECR are not supported. | April 13, 2022 |
| Amazon ECR | Interface VPC endpoints(AWS PrivateLink) for Amazon ECS are not supported. | April 13, 2022 |
| AWS Snowball Edge | AWS Snow Device Management service is not available in AWS Secret Region because AWS IoT Greengrass is not available in AWS Secret Region | April 13, 2022 |
| AWS KMS | Update AWS KMS Transport Layer Security (TLS) for FIPS endpoint information in AWS Secret Region. | April 13, 2022 |

| | | |
|---|---|---|
| AWS Lambda | AWS Lambda Function URLs is not available in AWS Secret Region. | April 13, 2022 |
| AWS Lambda | The `dotnet6` runtime is not available in AWS Secret Region. | April 13, 2022 |
| Aurora | Inaugural launch into AWS Secret Region. | April 6, 2022 |
| Amazon EKS | Inaugural launch into AWS Secret Region. | April 6, 2022 |
| Amazon OpenSearch Service | The new `AWS::OpenSearchService::Domain` CloudFormation resource is not supported. | March 23, 2022 |
| Amazon CloudWatch Logs | CloudWatch Logs Insights is now available | March 23, 2022 |
| Amazon OpenSearch Service | OpenSearch Service rebrand. | March 16, 2022 |
| Amazon EC2 Auto Scaling | Remove "Currently, specifying a Lambda function as a custom termination policy for an Auto Scaling group is available only if..." | March 16, 2022 |
| Amazon EC2 Auto Scaling | Retrieving the target lifecycle state through instance metadata is not available in AWS Secret Region. | March 16, 2022 |
| Changing Your Account Email | Added section on changing IAM role email account. | March 9, 2022 |

| | | |
|---|---|---|
| Amazon EC2 | The `lastLaunchedTime` AMI attribute is not available in AWS Secret Region. | March 9, 2022 |
| Image Builder | Initial launch for EC2 Image Builder in MVP Regions. | March 2, 2022 |
| Amazon EBS | Amazon EBS Snapshots Archive is not available in AWS Secret Region. | March 2, 2022 |
| Amazon EBS | You can create multi-volume snapshots of instances using the Amazon EC2 API, AWS CLI, or AWS SDKs only. | March 2, 2022 |
| AWS Snowball Edge | Snowcone is not available in AWS Secret Region because AWS DataSync is not available in the AWS Secret Region. | March 2, 2022 |
| AWS Step Functions | Update to step functions. | March 2, 2022 |
| Amazon EC2 | The EC2 Reserved Instance Marketplace is not available in AWS Secret Region. | February 23, 2022 |
| Amazon EC2 | Seamless domain join is not enabled in AWS Secret Region. | February 23, 2022 |
| AWS KMS | AWS KMS supports versions 1.0—1.2 of Transport Layer Security (TLS) for endpoints in AWS Secret Region. | February 23, 2022 |
| AWS Trusted Advisor | The AWS Security Hub integration feature is not supported. | February 23, 2022 |

| | | |
|---|---|---|
| Amazon S3 | Amazon S3 strong read-after-write consistency now available in AWS Secret Region. | February 16, 2022 |
| Amazon S3 | Amazon S3 Batch Replication is not available in AWS for Secret Regions. | February 16, 2022 |
| Amazon ECR | Amazon ECR doesn't emit any events to Amazon EventBridge in this Region. | February 16, 2022 |
| Amazon EC2 Auto Scaling | You currently cannot use an instance reuse policy to return instances to a warm pool when your Auto Scaling group scales in (terminates instances). | February 16, 2022 |
| Amazon EC2 Auto Scaling | The warm pools feature is now available in AWS Secret Region. | February 16, 2022 |
| Amazon EC2 Auto Scaling | Currently, specifying a Lambda function as a custom termination policy for an Auto Scaling group is available only if you use the AWS CLI or an SDK. This option is not available from the console. | February 16, 2022 |
| Amazon SNS | In AWS Secret Region, Attribute-based access controls (ABAC) for Amazon SNS resources is not supported. | February 9, 2022 |

| | | |
|---|---|---|
| Amazon Simple Queue Service | In AWS Secret Region, tagging SQS resources is supported. | February 2, 2022 |
| AWS KMS | AWS KMS CloudFormation resources are limited in this Region. You cannot use an AWS CloudFormation template to create or manage asymmetric KMS keys or multi-Region KMS keys (primary or replica). | February 2, 2022 |
| Amazon EBS | Recycle Bin for EBS snapshots is not available. | January 26, 2022 |
| AWS Snowball Edge | The high performance NFS data transfer feature is not available on AWS Secret Region Snowball Edge Storage Optimized devices because AWS DataSync is not available in the AWS Secret Region. | January 26, 2022 |
| AWS Snowball Edge | Snowball Edge cluster feature is not available in AWS Secret Region. | January 26, 2022 |
| AWS Snowball Edge | Remove bullet: "AWS Systems Manager AMIs are currently not available in AWS Secret Region." | January 26, 2022 |
| Amazon EC2 | Tags in instance metadata are currently not available in AWS Secret Region. | January 19, 2022 |

| | | |
|---|---|---|
| AWS Snowball Edge | AWS Snowball with Tape Gateway is not available in AWS Secret Region as AWS Storage Gateway is not available in AWS Secret Region. | January 19, 2022 |
| Amazon Simple Queue Service | The SQS dead-letter queue redrive feature is not supported for this region. | January 5, 2022 |
| Amazon Route 53 | Reviewed and updated the document. | January 5, 2022 |
| Amazon EMR | Added content related to Log4j vulnerabilities. | January 5, 2022 |
| Elastic Load Balancing | Application Load Balancers and Classic Load Balancers in AWS Secret Region do not support desync mitigation mode. | December 20, 2021 |
| Elastic Load Balancing | Network Load Balancers in AWS Secret Region do not support TLS listeners. You can use TCP or UDP listeners. | December 20, 2021 |
| Amazon ElastiCache | PrivateLink feature is not available in AWS Secret Region. | December 20, 2021 |
| Amazon EC2 | Amazon EC2 Images does not currently support `create-restore-image-task`, `create-store-image-task` or `describe-store-image-task` in AWS Secret Region. | December 20, 2021 |

| | | |
|---|---|---|
| Amazon DynamoDB | Updated local versions of Amazon DynamoDB link location. | December 20, 2021 |
| AWS DMS | Replaced snowball edge para. Remove Apple Mac bullet. | December 20, 2021 |
| Amazon S3 | Amazon S3 Object Ownership is not available in AWS Secret Region | December 15, 2021 |
| Amazon S3 | Amazon S3 Lifecycle rules based on object size is not available in AWS for AWS Secret Region. | December 15, 2021 |
| Amazon Elastic Container Service | Private Registry Authentic ation is not supported. | December 15, 2021 |
| Amazon VPC | Amazon VPC IP Address Manager (IPAM) is not available. | December 8, 2021 |
| Amazon Redshift | RA3.xplus node types not available. | December 8, 2021 |
| Amazon RDS | Encryption at rest isn't supported for the db.t2.micro, db.t2.small and db.t2.medium instance classes. | December 8, 2021 |
| Amazon SNS | In AWS Secret Region, Amazon SNS does not support message batching. | November 22, 2021 |

| | | |
|---|---|---|
| Amazon ElastiCache | Redis engine 6.2 data-tiering, at-rest encryption and in-transit encryption are not available in AWS Secret Region. | November 22, 2021 |
| AWS CloudTrail | The IAM condition keys `aws:SourceArn` and `aws:SourceAccount` are not supported in resource policies for resources that you associate with a trail, such as those for Amazon S3 buckets, AWS KMS keys, or Amazon SNS topics. | November 22, 2021 |
| AWS DMS | Removed multiple bullets in 'How AWS DMS differs section'. | November 22, 2021 |
| Amazon CloudWatch | AWS PrivateLink support for CloudWatch is now available. | November 17, 2021 |
| AWS Billing and Cost Management | The AWS Cost Explorer API is not available. | November 17, 2021 |
| AWS Config | AWS Config does not support monitoring AWS Config rules with Amazon CloudWatch Events in AWS Secret Region. | November 17, 2021 |
| Amazon RDS | Some older minor DB engine versions don't support the latest generation DB instance classes. | November 10, 2021 |
| Amazon Linux 2 | Added section on updating AMIs to work in the Region. | November 10, 2021 |

| | | |
|---|---|---|
| Amazon Linux 2 | Removed bullet: AWS SDK for Python (Boto3) as already being installed & configured. | November 10, 2021 |
| Amazon EBS | AWS CloudTrail data events are not supported in . | November 3, 2021 |
| AWS CodeDeploy | API calls to the CodeDeploy endpoint `com.amazonaws.us-isob-east-1.codedeploy` from within a VPC are not supported. | November 3, 2021 |
| AWS CodeDeploy | To use CodeDeploy with Amazon Virtual Private Cloud, you must use CodeDeploy agent 1.3.1 or later in the AWS Secret Region. | November 3, 2021 |
| Amazon RDS | Performance Insights for Amazon RDS isn't supported. | October 27, 2021 |
| Amazon EC2 Auto Scaling | The attribute-based instance type selection feature is not available. | October 27, 2021 |
| Amazon EC2 Auto Scaling | Specifying `lowest-price` for the `OnDemandAllocationStrategy` property of a mixed instances group is currently not supported. | October 27, 2021 |
| Amazon EC2 | The attribute-based instance type selection feature for Amazon EC2 Fleet and Spot Fleet is not available. | October 27, 2021 |

| | | |
|---|---|---|
| Amazon Elastic Container Service | Amazon ECS resources are not supported CloudWatch targets. | October 20, 2021 |
| Amazon EBS | Amazon EBS Direct APIs are now available in . | October 20, 2021 |
| Amazon EBS | Amazon EBS Direct APIs are now available in AWS Secret Region. | October 20, 2021 |
| AWS CloudTrail | When logging CloudTrail data events, Amazon DynamoDB API activity on streams is currently not available. | October 20, 2021 |
| Elastic Load Balancing | Network Load Balancers in AWS Secret Region do not support configuring Applicati on Load Balancers as targets. | October 13, 2021 |
| Amazon VPC | Security group rule IDs are currently available in the AWS Command Line Interface but are not available in the Amazon Virtual Private Cloud Console. | October 13, 2021 |
| AWS Identity and Access Management | Removed the bullet "You cannot simulate permissio ns boundaries on IAM entities using the IAM Policy Simulator." | October 13, 2021 |
| AWS Step Functions | The Step Functions Workflow Studio and all AWS SDK service integrations are not available. | October 6, 2021 |

| | | |
|---|---|---|
| AWS Support | The AWS Support section of this guide was moved under the Services heading. | October 6, 2021 |
| AWS Trusted Advisor | Monitoring Trusted Advisor checks with Amazon CloudWatch Events is not supported and Trusted Advisor does not support sending weekly notification emails for checks at this time. | October 6, 2021 |
| AWS Serverless Application Model | New page for AWS SAM. | October 4, 2021 |
| Aurora | Enhanced monitoring and Performance Insights are now supported. | September 29, 2021 |
| AWS Trusted Advisor | Added a new page to this guide. | September 22, 2021 |
| AWS VPN | The following APIs are not supported: GetVpnConnectionDeviceTypes and GetVpnConnectionDeviceSampleConfiguration and Sample configuration files using IKEv2 are not available. | September 22, 2021 |
| Amazon Elastic Container Service | Updated the RDS Certificate Authority information. | September 15, 2021 |
| Amazon Elastic Compute Cloud | ED25519 keys are supported in the AWS CLI, but are not supported when using the Amazon EC2 console. | September 8, 2021 |

| | | |
|---|---|---|
| Amazon CloudWatch Logs | AWS PrivateLink support for CloudWatch Logs is not available | September 8, 2021 |
| Amazon OpenSearch Service | Updated terminology for OpenSearch Service rebrand. | September 7, 2021 |
| Application Auto Scaling | ElastiCache for Redis clusters (replication groups) are not supported. | September 1, 2021 |
| Amazon CloudWatch | AWS PrivateLink support for CloudWatch is not available. | September 1, 2021 |
| Elastic Load Balancing | Application Load Balancers in AWS Secret Region now support Lambda functions as a target. | August 25, 2021 |
| Amazon Redshift | Amazon Redshift console query editor is now available. | August 25, 2021 |
| Amazon Elastic Compute Cloud | ED25519 keys are currently not supported. | August 25, 2021 |
| API Gateway | Inaugural launch into AWS Secret Region. | August 25, 2021 |
| AWS AppConfig | AWS AppConfig is now available in AWS Secret Region | August 25, 2021 |
| Amazon VPC | Traffic Mirroring and VPC Reachability Analyzer are not supported. | August 18, 2021 |
| AWS Billing and Cost Management | Reviewed and updated the entire differences section. | August 18, 2021 |

| | | |
|---|---|---|
| Amazon S3 | Amazon S3 Access Points aliases are not available in AWS Secret Region. | August 4, 2021 |
| Amazon OpenSearch Service | Updated multiple items in the differences section. | August 4, 2021 |
| AWS Resource Groups Tagging API | Resource Groups Tagging API launched in AWS Secret RegionRegion. | August 4, 2021 |
| Amazon SNS | Tagging Amazon SNS resources is not supported. | July 28, 2021 |
| Amazon EC2 Auto Scaling | Removed bullet: "Describing scaling activities for deleted Auto Scaling groups using version 2 of the AWS CLI is currently not supported." | July 28, 2021 |
| AWS Billing and Cost Management | The billing alerts feature is not available. | July 28, 2021 |
| AWS Lambda | Event destinations are not available in AWS Secret Region | July 28, 2021 |
| Amazon Elastic Compute Cloud | Custom time windows for scheduled events are currently not available. | July 21, 2021 |
| AWS Marketplace | The AWS Marketplace section of AWS is available in AWS Secret Region. | July 21, 2021 |
| AWS Pricing Calculator | AWS Pricing Calculator now available. | July 21, 2021 |

| | | |
|---|---|---|
| Amazon Redshift | Added a list of features that are not available. | July 7, 2021 |
| Amazon CloudWatch | Added three bullets related to CloudWatch Synthetics. | July 7, 2021 |
| License Manager | License Manager is now available in AWS Secret Region. | June 30, 2021 |
| Amazon Elastic Compute Cloud | Updated the service principal information. | June 30, 2021 |
| Amazon CloudWatch | Composite alarms are now available. | June 30, 2021 |
| AWS Direct Connect | AWS Direct Connect CNSSP11 Protected Dedicated Circuits are not supported. | June 30, 2021 |
| Amazon Simple Queue Service | Added the section titled "Publishing a message from a VPC". | June 23, 2021 |
| Amazon Elastic Compute Cloud | AMI deprecation is currently not available. | June 23, 2021 |
| AWS KMS | Multi-Region keys are not available in the AWS Secret Region and the VPC Endpoint feature in AWS KMS is available in AWS Secret Region | June 16, 2021 |
| Amazon S3 | Support for BitTorrent is now available. | June 9, 2021 |
| Amazon Redshift | Amazon Redshift Spectrum is not available. | June 9, 2021 |

| | | |
|---|---|---|
| Amazon Elastic Container Service | The ECS Anywhere is not supported. | June 9, 2021 |
| Amazon Elastic Container Service | Updated the RDS ca from `rds-ca-2015` to `rds-ca-2017` . | June 9, 2021 |
| Amazon EC2 Auto Scaling | The gp3 EBS volume type cannot be specified in the block device mappings for launch configurations. | June 9, 2021 |
| Amazon EC2 Auto Scaling | Removed bullet "You can create scheduled actions in UTC only. Specifying your time zone is currently not supported." | June 2, 2021 |
| Amazon RDS | Several unsupported features: Adding bullets for limitations in the region. | May 26, 2021 |
| Amazon Elastic Compute Cloud | Security Group Rule IDs are not supported in the console. | May 26, 2021 |
| Amazon EMR | Amazon EMR release version 6.3.0 is available in AWS Secret Region. | May 26, 2021 |
| AWS Identity and Access Management | Added bullet for the identifier for a service principal. | May 26, 2021 |
| AWS Step Functions | The Amazon EventBridge service integration is not available. | May 26, 2021 |

| | | |
|---|---|---|
| Amazon Elastic Compute Cloud | Updated multiple bullets in section 'How Amazon EC2 Differs for AWS Secret Region'. | May 19, 2021 |
| Amazon EMR | Amazon EMR release version 5.27.1 is available in AWS Secret Region. | May 19, 2021 |
| Amazon EC2 Auto Scaling | Describing scaling activitie s for deleted Auto Scaling groups using version 2 of the AWS CLI is currently not supported. | May 19, 2021 |
| AWS Snowball Edge | Removed bullets- 1.AWS Secret Region doesn't support monthly metering for either Snowball or Snowball Edge. 2.In AWS Secret Region, the 1 year or 3 year commitmen t upfront charge model is not supported. If this is required, work with your AWS account team. | May 19, 2021 |
| Amazon RDS | RDS Proxy is not available for MariaDB, MySQL, and PostgreSQL. | May 12, 2021 |
| Amazon VPC | Security Group Rule IDs are not supported in the console. | May 5, 2021 |
| Amazon RDS | Size-flexible reserved DB instances aren't supported. | May 5, 2021 |

| | | |
|---|---|---|
| Amazon Elastic Compute Cloud | Root volume replacement for running instances is not available. | May 5, 2021 |
| Amazon EMR | The release versions 5.33.0 is available in AWS Secret Region. | May 5, 2021 |
| Amazon EC2 Auto Scaling | You cannot create a predictiv e scaling policy in AWS Secret Region. | May 5, 2021 |
| AWS Transit Gateway | Multicast, including IGMP multicast is not supported in AWS Secret Region. | May 5, 2021 |
| Elastic Load Balancing | Network Load Balancers in AWS Secret Region do not support custom private IPv4 addresses. | April 28, 2021 |
| Amazon EC2 Auto Scaling | Removed bullet "Instance refresh checkpoints are currently not available in AWS Secret Region." | April 28, 2021 |
| AWS Config | Reworked the differences section. | April 28, 2021 |
| AWS Identity and Access Management | Added bullet for permission boundary support in policy simulation. | April 28, 2021 |
| Amazon RDS | Deleted Sharing a DB snapshot with other accounts is not supported. | April 21, 2021 |

| | | |
|---|---|---|
| Amazon EC2 Auto Scaling | The warm pools feature is currently not available in AWS Secret Region. | April 21, 2021 |
| AWS Billing and Cost Management | Update details in deposit reports into an Amazon S3 bucket. | April 21, 2021 |
| AWS Identity and Access Management | Removed bullet for permissio n boundary support in policy simulation. | April 21, 2021 |
| AWS Identity and Access Management | IAM Access Analyzer policy generation checks are not available in AWS Secret Region. | April 21, 2021 |
| Amazon Elastic Container Service | The ECS CLI is not supported. | April 14, 2021 |
| Amazon EC2 Auto Scaling | Removed multiple bullets and added Instance refresh checkpoints are currently not available. | April 14, 2021 |
| AWS Transit Gateway | Initial release | April 14, 2021 |
| AWS VPN | Configurable Security Algorithms, Timer Settings, certificate authentication, and customer gateway modificat ion are not supported. | April 14, 2021 |
| Amazon Elastic Compute Cloud | EC2 Serial Console is currently not available in C2S. | April 7, 2021 |

| | | |
|---|---|---|
| Amazon ElastiCache | Engine version Redis 6.x is not available in AWS Secret Region. Global Datastores are not available in AWS Secret Region. | April 7, 2021 |
| Amazon EMR | IMDSv2 (instance metadata service) is supported in EMR versions 5.32.0 and later, and 6.2.0 and later. There is no support for IMDSv2 for EMR versions 5.27.1 and 5.23.1. | April 7, 2021 |
| Systems Manager | Added multiple bullets to the document. | March 31, 2021 |
| Amazon Simple Queue Service | Tagging SQS resources is not supported. | March 31, 2021 |
| Amazon SNS | Added new section- Publishin g a message from a VPC. | March 31, 2021 |
| Amazon Route 53 | Reviewed and updated the document. | March 31, 2021 |
| Amazon Kinesis Data Streams | Reviewed and improved the document. | March 31, 2021 |
| Amazon EMR | Reviewed and updated the document. | March 31, 2021 |

| | | |
|---|---|---|
| Amazon DynamoDB | Added bullets - The following features are not available : DynamoDB Accelerator (DAX), Export to S3, CloudWatch Contributor Insights for DynamoDB, NoSQL Workbench, Kinesis Data Streams integration for change capture, and PartiQL API actions. DynamoDB operation logging to CloudTrail includes control plane activities only. | March 31, 2021 |
| Amazon CloudWatch | Removed download link and updated Contributor Insights to not available. | March 31, 2021 |
| AWS Snowball Edge | In AWS Secret Region, AWS services Snowball Edge Storage Optimized (for data transfer) with either the T100 or T98 Snowball Edge Storage Optimized device and Snowball Edge Storage Optimized (with EC2-compatible compute functionality) jobs with only the T98 Snowball Edge Storage Optimized device. | March 31, 2021 |
| AWS CloudTrail | Reviewed and updated the document. | March 31, 2021 |
| AWS Config | Updates to resource types and supported features. | March 31, 2021 |

| | | |
|---|---|---|
| AWS Direct Connect | MAC Security (MACsec) is not supported. | March 31, 2021 |
| AWS KMS | The AWS KMS console feature that lets you filter KMS keys based on their tags is not supported in AWS Secret Region. | March 31, 2021 |
| AWS Snowball | AWS Snowball is no longer available in AWS Secret Region. | March 31, 2021 |
| Amazon S3 | Amazon S3 Object Lambda Access Points are not available in AWS Secret Region. | March 24, 2021 |
| Amazon Elastic Compute Cloud | UEFI boot mode on Intel- and AMD-based instances is not available. | March 24, 2021 |
| Amazon EBS | Added multiple items in the differences section. | March 24, 2021 |
| Amazon DynamoDB | Removed bullets On-demand backup and restore for DynamoDB is not yet available and Point-in-time recovery for DynamoDB is not yet available | March 24, 2021 |
| Amazon CloudWatch | Dashboard sharing is not available. | March 24, 2021 |

| | | |
|---|---|---|
| AWS Snowball Edge | Removed bullet AWS OpsHub for Snow Family is not available in AWS Secret Region. | March 24, 2021 |
| AWS CodeDeploy | Amazon ECS capacity providers are not supported. | March 24, 2021 |
| AWS Identity and Access Management | IAM Access Analyzer policy validation checks are not available in AWS Secret Region. | March 24, 2021 |
| AWS Lambda | Removed bullets to the section that defined how Lambda differs in AWS Secret Region. | March 24, 2021 |
| AWS Step Functions | Added multiple bullets defining differences in the region. | March 24, 2021 |
| Amazon S3 | Added five bullets to the bottom of the list of differenc es. | March 17, 2021 |
| Amazon OpenSearch Service | Reworded and updated multiple items in the differenc es section. | March 17, 2021 |
| Amazon EC2 Auto Scaling | You can create scheduled actions in UTC only. Specifyin g your time zone is currently not supported. | March 17, 2021 |
| Amazon CloudWatch Logs | CloudWatch Logs Insights is not available. | March 17, 2021 |

| | | |
|---|---|---|
| AWS CodeDeploy | Automatically updating outdated instances is not supported. | March 17, 2021 |
| AWS DMS | Added five bullets to the bottom of the section on how DMS Differs for AWS Secret Region. | March 17, 2021 |
| AWS Direct Connect | Added multiple bullets to the section that defines how AWS Direct Connect differs in AWS Secret Region. | March 17, 2021 |
| Amazon S3 | S3 Replication, including Cross-Region & Same-Region replication, not available. | March 10, 2021 |
| Amazon RDS | Deleted stray TDE bullet. | March 10, 2021 |
| Amazon RDS | S3 export not supported. | March 10, 2021 |
| Amazon Elastic Container Service | Numerous updates by ECS tech writer - please re-read chpater. | March 10, 2021 |
| Amazon CloudWatch | Composite alarms not available. | March 10, 2021 |
| AWS Health | Organizational view feature not supported. | March 10, 2021 |
| Amazon ECR | Cross-region and cross-account replication is not supported. | March 3, 2021 |

| | | |
|---|---|---|
| AWS Identity and Access Management | Added a list of IAM resources that cannot use IAM tags and removed a bullet stating that you cannot use IAM tags to control permissions in AWS. | March 3, 2021 |
| Amazon Route 53 | Inaugural launch into AWS Secret Region. | February 25, 2021 |
| Amazon Elastic Container Registry | OCI artifacts not supported. | February 24, 2021 |
| Elastic Load Balancing | ALB's don't support: Cognito user authentication in listener rules, Lambda functions as a target, the least outstanding requests algorithm, Application cookie stickiness, AWS WAF (Web Application Firewall). Updated Route 53 Hosted Zone ID table. | February 17, 2021 |
| Amazon Elastic Container Service | AWS Fargate Spot not available. | February 17, 2021 |
| Amazon EMR | Release versions 5.30.0 and 6.1.0 not available. | February 17, 2021 |
| Amazon EC2 Auto Scaling | Launch template can't be specified from the console if it has multiple network interfaces. | February 17, 2021 |
| Elastic Load Balancing | NLBs in AWS Secret Region don't support changing source IP preservation defaults. | February 10, 2021 |

| | | |
|---|---|---|
| Amazon VPC | Elastic IP address tagging only by using the allocate-address AWS CLI command. | February 10, 2021 |
| Amazon RDS | Transparent Data Encryption (TDE) now supported; but no other SQL Server options are supported. | February 10, 2021 |
| Amazon Kinesis Data Streams | Long term retention for data streams not supported. | February 10, 2021 |
| Amazon RDS | Performance Insights not supported. Oracle TDE not supported. | February 3, 2021 |
| Amazon Elastic Container Service | AWS Fargate now available. | February 3, 2021 |
| Amazon Elastic Compute Cloud | Tagging AMIs and their snapshots on AMI creation now supported. | February 3, 2021 |
| Amazon CloudWatch | Percentile statistics & High-definition metrics now available via console. | February 3, 2021 |
| AWS KMS | Added link to Services section of AWS Secret Region for AWS KMS integration. | February 3, 2021 |
| AWS VPN | Internet Key Exchange negotiations can't be initiated for VPN connections. Noted algorithms not supported. IPv6 not supported. | February 3, 2021 |

| | | |
|---|---|---|
| Amazon RDS | Noted which versions of PostgreSQL S3 import feature are supported. | January 27, 2021 |
| Amazon EC2 Auto Scaling | Auto Scaling group max instance types is 20. | January 27, 2021 |
| Amazon Elastic Container Service | Tagging Amazon ECS resources not available. | January 13, 2021 |
| Amazon RDS | IAM database authentic ation for RDS DB engines is supported. | December 16, 2020 |
| Amazon Elastic Compute Cloud | AMIs and their snapshots on AMI creation cannot be tagged. | December 16, 2020 |
| AWS CloudFormation | AWS::Kinesis::StreamConsume r resource now supported. | December 16, 2020 |
| AWS KMS | The ability to control access to an AWS KMS key based on its aliases and tags is not supported. | December 16, 2020 |
| Amazon RDS | SQL Server builds no longer restricted to the R4 instance type. | November 24, 2020 |
| Amazon RDS | Storage autoscaling not supported. | November 24, 2020 |
| Amazon RDS | IAM database authentic ation for RDS DB engines not supported. | November 24, 2020 |
| Amazon RDS | PostgreSQL S3 import feature not supported. | November 24, 2020 |

| | | |
|---|---|---|
| Amazon RDS | Encryption at rest not supported for db.t2.medium DB instance class. | November 24, 2020 |
| Amazon ElastiCache | At-rest encryption & in-transit encryption not supported. | November 24, 2020 |
| Amazon Elastic Compute Cloud | Noted that instant fleet types cannot be deleted. | November 18, 2020 |
| Amazon RDS | Release 11.2.0.4 of Oracle Database now available. | November 11, 2020 |
| Amazon OpenSearch Service | Inaugural launch into AWS Secret Region. | November 11, 2020 |
| AWS CodeDeploy | Inaugural launch into AWS Secret Region. | November 11, 2020 |
| AWS DMS | AWS Health Dashboard (PHD) notifications are now available. | November 11, 2020 |
| Amazon RDS | Oracle Gen5 instances are available. | November 4, 2020 |
| Amazon Elastic Compute Cloud | AWS Nitro Enclaves not available. | November 4, 2020 |
| AWS VPN | For either default VPC or EC2-Classic, the RevokeSecurityGroupEgress command now includes the security group rules that were not revoked in the output. | November 4, 2020 |
| AWS VPN | Single Tunnel & Tunnel Replacement notifications not available. | November 4, 2020 |

| | | |
|---|---|---|
| Amazon RDS | Oracle Gen5 instances and release 11.2.0.4 not available. | October 28, 2020 |
| Amazon Elastic Container Registry | Tagging an Amazon ECR repository not available. | October 28, 2020 |
| Amazon Elastic Container Service | Noted restrictions to use version 2.4 of the Apache HTTP server Docker image. | October 21, 2020 |
| Amazon Elastic Container Registry | Image scanning, Multi-architecture images, and Encryption with CMKs are not available. | October 21, 2020 |
| Amazon CloudWatch | Percentile statistics now available. | October 21, 2020 |
| Application Auto Scaling | Noted Amazon Comprehend document classification and entity recognizer endpoints resources not supported. | October 7, 2020 |
| AWS VPN | Tag on create now supports resource types: customer gateway, virtual private gateway, and VPN connection. | October 7, 2020 |
| Application Auto Scaling | Managed Streaming for Apache Kafka (MSK) cluster storage not supported. | September 30, 2020 |
| Amazon RDS | S3 export is only supported for MySQL. | September 30, 2020 |
| AWS DMS | AWS Health Dashboard (PHD) notifications are not available. | September 30, 2020 |

| | | |
|---|---|---|
| Elastic Load Balancing | Network Load Balancers do not support the TLS or UDP listener types (only TCP listener type). | September 16, 2020 |
| Elastic Load Balancing | IDP endpoints need to be within the AWS Secret Region WAN and not open internet. | September 2, 2020 |
| Amazon S3 | Noted bucket owner condition s & restrictions regarding account IDs. | September 2, 2020 |
| Amazon RDS | Database activity streams aren't supported. | September 2, 2020 |
| Amazon Elastic Compute Cloud | Provisioned IOPS SSD (io2) EBS volume type not available. | September 2, 2020 |
| Amazon EBS | Provisioned IOPS SSD (io2) EBS volume type not available. | September 2, 2020 |
| Systems Manager | Noted S3 bucket specifics and format required for SSM Agent. | August 26, 2020 |
| Amazon VPC | Noted managed prefix lists can't be created, but can be viewed. | August 26, 2020 |
| Amazon EC2 Auto Scaling | Disable scaling policies not available from the console. | August 26, 2020 |
| Amazon VPC | Noted tag can't be added when creating a VPC or network interface using the VPC Console. | August 19, 2020 |

| | | |
|---|---|---|
| Amazon EC2 Auto Scaling | Instance refreshes not available from the console. | August 12, 2020 |
| Amazon Elastic Compute Cloud | Notated EC2Launch v2 from SSM Distributor restrictions with a SSM RunCommand document not supported. | August 5, 2020 |
| AWS VPN | Noted resource types that do not support tagging on creation. | August 5, 2020 |
| AWS VPN | Noted APIs that do not support resource-level permissions. | August 5, 2020 |
| Amazon RDS | Publishing database logs to Amazon CloudWatch Logs now supported for MariaDB and MySQL. | July 29, 2020 |
| Amazon ElastiCache | Exporting ElastiCache snapshots to S3 buckets now supported. | July 29, 2020 |
| Amazon EMR | Notated features that are not available in EMR version 5.30.1. | July 29, 2020 |
| Amazon VPC | Tag on create & vanity DNS not supported on AWS PrivateLink. | July 22, 2020 |
| Amazon EMR | All Hadoop versions supported. Tez UI and YARN timeline history not available . Docker containers not available. | July 22, 2020 |

| | | |
|---|---|---|
| Amazon Redshift | New download links for new versions of drivers. | July 15, 2020 |
| Amazon EMR | Clusters with multi-master nodes now supported via console. | July 8, 2020 |
| AWS KMS | VPC endpoint policies not supported in AWS Secret Region. | July 8, 2020 |
| Amazon EMR | Release version 5.30.0 not available in AWS Secret Region. | July 1, 2020 |
| Amazon EC2 Auto Scaling | Instance refreshes are not available. | June 24, 2020 |
| Application Auto Scaling | Amazon EMR clusters now supported. | June 17, 2020 |
| Amazon ElastiCache | R5, M5, & T3 Amazon EC2 instance famlies now supported. | June 17, 2020 |
| Amazon EMR | Automatic Scaling in Amazon EMR now supported via console. | June 17, 2020 |
| Amazon Elastic Compute Cloud | On-Demand Capacity Reservations now available. | June 3, 2020 |
| Amazon CloudWatch | Automatic dashboards now available. | June 3, 2020 |
| AWS Lambda | Lambda service now avaible in AWS Secret Region. | June 3, 2020 |

| | | |
|---|---|---|
| Amazon RDS | Oracle S3 integration now supported via console. | May 6, 2020 |
| Windows AMIs | Changes to EC2Launch and EC2Config. | April 22, 2020 |
| Amazon RDS | Publishing database logs to Amazon CloudWatch Logs is not supported for MariaDB and MySQL. | April 22, 2020 |
| Amazon CloudWatch Logs | Encryption context with the ARN of log groups is not available. | April 22, 2020 |
| AWS Snowball Edge | Multiple AWS Secret Region non-supported features and differences called out. | April 22, 2020 |
| AWS Identity and Access Management | Restrictions on simulating permissions boundaries. | April 22, 2020 |
| Amazon EC2 Auto Scaling | Reserved instances are supported. | April 15, 2020 |
| Amazon RDS | Amazon S3 integration is supported with Oracle using the AWS CLI only. | April 8, 2020 |
| AWS Marketplace | Initial launch of AWS Marketplace in AWS Secret Region. | June 1, 2016 |

| Change | Description | Date |
|---|---|---|
| AWS Systems Manager |   | February 2020 |

| Change | Description | Date |
| --- | --- | --- |
| | New AWS Systems Manager console is now available in C2S. See AWS Systems Manager. | |
| Amazon Elastic Container Registry and Amazon Elastic Container Service | NEW OR COMING SOON<br><br>Amazon ECR and Amazon ECS are now available in AWS Secret Region. See Amazon Elastic Container Registry and Amazon Elastic Container Service. | August 2019 |
| Amazon EMR | NEW OR COMING SOON<br><br>M5 and C5 instance types now available for Amazon EMR. See Amazon EMR. | July 2019 |
| AWS Snowball Edge | July 2019 | |
| Application Auto Scaling | NEW OR COMING SOON<br><br>Application Auto Scaling is now available in AWS Secret Region. See Application Auto Scaling. | June 2019 |
| AWS Key Management Service | NEW OR COMING SOON<br><br>New AWS KMS management console is now available in AWS Secret Region. See Getting Started. | June 2019 |
| Amazon DynamoDB | NEW OR COMING SOON<br><br>DynamoDB Encryption at Rest is now supported. See DynamoDB Encryption at Rest. | April 2019 |

| Change | Description | Date |
| --- | --- | --- |
| Amazon Elastic Compute Cloud | NEW OR COMING SOON<br>• Enabled support for C5, C5d, M5, M5d, R5, R5d instance types. For more information, see Amazon EC2 Instance Types.<br>• Enabled support for T2 Unlimited and T3 instance types. For more information, see Amazon EC2 Instance Types.<br>• Enabled support for Service-Linked Roles for EC2 Auto Scaling. For more information, see Service-Linked Roles for Amazon EC2 Auto Scaling. | March 2019 |
| Amazon RDS | NEW OR COMING SOON<br>Amazon RDS Enables Stopping and Starting of Multi-AZ Database Instances via AWS CLI. See Amazon Relational Database Service. | January 2019 |
| Amazon Elastic Compute Cloud | NEW OR COMING SOON<br>Enabled support for Attaching, Detaching, and Replacing an IAM role to an instance. For more information, see Amazon EC2 IAM Roles. | January 2019 |
| Amazon Linux 2 | NEW OR COMING SOON<br>Added information about how Amazon Linux 2 differs. See Amazon Linux 2 AMI for AWS Secret Region. | December 2018 |
| Amazon Virtual Private Cloud | Creating a Default Subnet is now supported. | September 2018 |

| Change | Description | Date |
| --- | --- | --- |
| Amazon Elastic Compute Cloud | Added support for Auto Recovery for Dedicated Instances. | September 2018 |
| AWS Step Functions | Initial release for AWS Secret Region. See AWS Step Functions. | August 2018 |
| AWS Database Migration Service | Initial release for AWS Secret Region. See AWS Database Migration Service. | August 2018 |
| AWS Schema Conversion Tool | Initial release for AWS Secret Region. See AWS Schema Conversion Tool. | August 2018 |
| Kinesis Data Streams | Enhanced Fan-out and HTTP/2 reads for Kinesis Data Streams. See Reading Data from Amazon Kinesis Data Streams. | August 2018 |
| Amazon RDS | Enabled Microsoft SQL Server as a supported database engine on Amazon RDS. See Microsoft SQL Server on Amazon RDS. | August 2018 |
| Amazon S3 | Enabled ONEZONE_IA as an available storage class. See Storage Classes. | August 2018 |
| Amazon Virtual Private Cloud | Enabled support for Amazon VPC Adding IPv4 CIDR Blocks to a VPC. | July 2018 |
| Amazon Virtual Private Cloud | Enabled support for Amazon VPC NAT Gateway. | July 2018 |
| Amazon CloudWatch Events | Initial release for AWS Secret Region. Added topic describing differences. | July 2018 |
| Amazon DynamoDB | Enabled support for DynamoDB Streams. | June 2018 |

| Change | Description | Date |
| --- | --- | --- |
| AWS Identity and Access Management | You cannot use the maximum session duration setting for a role to allow users assuming the role to request a longer 12-hour role session. API and CLI users are limited to a 1-hour maximum role session duration. | May 2018 |
| AWS Health | Initial release for AWS Secret Region. Added topic describing differences. See the section called "AWS Health". | May 2018 |
| AWS CloudTrail | Enabled support for logging data events. See the section called "AWS CloudTrail". | April 2018 |
| AWS Key Management Service | Enabled support for FIPS 140-2 validated hardware security modules (HSM) and supports FIPS 140-2 validated endpoints. See the section called "AWS Key Management Service". | April 2018 |
| Amazon Virtual Private Cloud | Enabled support for creating a default VPC using the CLI or API and adding security group rule descriptions using only the CLI. For more information, see Creating a default VPC and Security Groups for your VPC. | March 2018 |
| Initial publication | This is the first publication of *AWS Secret Region User Guide*. This guide provides instructions for setting up your account and identifies differences between the public AWS cloud offerings and the private AWS Secret Region operational environment. | September, 2017 |

# Not Applicable to AWS Secret Region

It appears that you clicked an AWS Documentation link that does not apply to AWS Secret Region.

We are continuously updating AWS Secret Region with additional services and documentation. For a list of services and documentation you can use today, see the following page:

- Services in AWS Secret Region

# AWS Glossary

For the latest AWS terminology, see the AWS glossary in the *AWS Glossary Reference*.