AWS GovCloud (US): User Guide
Copyright © 2018 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Welcome ................................................................................................................................. 1  
What Is AWS GovCloud (US)? ................................................................................................ 2  
Differences with Standard AWS Accounts ............................................................................ 2  
Billing and Payment ............................................................................................................... 4  
Supported Services ............................................................................................................... 4  
Getting Started .................................................................................................................... 7  
Signing Up ............................................................................................................................ 7  
Onboarding (Direct Customers) ............................................................................................. 8  
Configuring Your Account .................................................................................................... 8  
Verifying AWS CloudTrail Is Enabled .................................................................................. 9  
Onboarding (Resellers or Reseller Customers) ..................................................................... 10  
Enabling Multi-Factor Authentication (MFA) ..................................................................... 14  
Signing Up for Customer Support ....................................................................................... 15  
Setting Up AWS GovCloud (US) .......................................................................................... 17  
CloudFront with Your Resources ........................................................................................ 17  
Credentials ........................................................................................................................ 17  
Tips for Setting Up CloudFront ......................................................................................... 18  
AWS WAF ........................................................................................................................... 18  
Route 53 with Your Resources ............................................................................................ 18  
Route 53 Zone Apex Support with a Load Balancer ............................................................ 19  
Step 1: Sign Up for AWS GovCloud (US) .......................................................................... 20  
Step 2: Create Your Resources in the AWS GovCloud (US) Region .................................. 20  
Step 3: Create a CloudFront Custom Origin Web Distribution ......................................... 21  
Step 4: Configure a New Route 53 Alias Resource Record Set ......................................... 23  
Step 5: Test that Your Website Is Accessible ...................................................................... 24  
Amazon SES ...................................................................................................................... 24  
Using AWS GovCloud (US) ................................................................................................. 26  
Amazon Resource Names ..................................................................................................... 26  
ARN Format ........................................................................................................................ 27  
Example ARNs .................................................................................................................... 27  
Paths in ARNs ..................................................................................................................... 35  
Endpoints ............................................................................................................................ 36  
Maintaining ITAR Compliance ............................................................................................ 39  
Accessing the AWS GovCloud (US) Region ....................................................................... 39  
Controlling Access ............................................................................................................. 40  
Command Line and API Access ......................................................................................... 40  
Resource Limits ................................................................................................................ 40  
Penetration Testing ............................................................................................................ 41  
Service Health Dashboard ................................................................................................. 42  
Services in the AWS GovCloud (US) Region ....................................................................... 43  
Amazon API Gateway ......................................................................................................... 44  
ITAR Boundary .................................................................................................................... 44  
Auto Scaling ....................................................................................................................... 45  
ITAR Boundary .................................................................................................................... 45  
AWS Certificate Manager .................................................................................................... 45  
ITAR Boundary .................................................................................................................... 45  
AWS CloudFormation ......................................................................................................... 46  
ITAR Boundary .................................................................................................................... 46  
AWS CloudHSM Classic ....................................................................................................... 46  
ITAR Boundary .................................................................................................................... 46  
AWS CloudTrail .................................................................................................................. 47  
Services Supported within CloudTrail ................................................................................ 48  
ITAR Boundary .................................................................................................................... 49  
Amazon CloudWatch .......................................................................................................... 49
Welcome

The *AWS GovCloud (US) User Guide* provides information about setting up your AWS GovCloud (US) account, identifies the differences between the AWS GovCloud (US) Region and other AWS regions, and defines usage guidelines for processing ITAR-regulated data within the AWS GovCloud (US) Region. In this guide, we assume you are familiar with Amazon Web Services (AWS).

For more information about AWS GovCloud (US), see *What Is AWS GovCloud (US)?* (p. 2).

For a list of AWS or AWS GovCloud (US) related resources, see *Related Resources* (p. 85).
What Is AWS GovCloud (US)?

AWS GovCloud (US) is an isolated AWS region designed to allow U.S. government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) Region adheres to U.S. International Traffic in Arms Regulations (ITAR) requirements.

You can run workloads that contain all categories of Controlled Unclassified Information (CUI) data and government-oriented, publicly available data in the AWS GovCloud (US) Region. The AWS GovCloud (US) Region supports the management of regulated data by offering the following features:

- Restricting physical and logical administrative access to U.S. citizens only.
- Providing FIPS 140-2 endpoints. (For details on each service, see the AWS GovCloud (US) Endpoints (p. 36) section.)

Depending on your requirements, you can also run unclassified workloads in the AWS GovCloud (US) Region and use the unique capabilities of this region.

Note

AWS manages physical and logical access controls for the AWS boundary. However, the overall security of your workloads is a shared responsibility, where you are responsible for controlling user access to content in your AWS GovCloud (US) account.

The AWS GovCloud (US) User Guide provides details on setting up your AWS GovCloud (US) account, identifies the differences between the AWS GovCloud (US) Region and other AWS regions, and defines usage guidelines for processing ITAR-regulated data within the AWS GovCloud (US) Region. This guide assumes that you are familiar with Amazon Web Services (AWS).

Additional resources:

- For pricing information, see AWS GovCloud (US) Region Pricing.
- For information about the differences between the AWS GovCloud (US) Region and other AWS regions, see AWS GovCloud (US) Region Compared to Standard AWS Regions (p. 2).
- For more information about ITAR compliance, see Maintaining U.S. International Traffic in Arms Regulations (ITAR) Compliance (p. 39).
- For a list of AWS or AWS GovCloud (US)–related resources, see Related Resources (p. 85).

AWS GovCloud (US) Region Compared to Standard AWS Regions

AWS GovCloud (US) is a gated community for workloads with direct or indirect ties to U.S. government functions or services. As a result, AWS GovCloud (US) offers the following features that are not available in the standard AWS regions:

- The AWS GovCloud (US) Region uses FIPS 140-2 approved cryptographic modules for all AWS service API endpoints, unless otherwise indicated in the AWS GovCloud (US) Endpoints (p. 36) section.
- The AWS GovCloud (US) Region maintains an ITAR-compliant infrastructure and is appropriate for all types of Controlled Unclassified Information (CUI) and unclassified data. For more details, see Maintaining U.S. International Traffic in Arms Regulations (ITAR) Compliance (p. 39).
- The AWS GovCloud (US) Region is physically isolated and has logical network isolation from all other regions.
• For administrative purposes, AWS restricts all physical and logical access to the AWS GovCloud (US) Region and all potential access to restricted customer data. AWS allows only vetted U.S. citizens with distinct access controls separate from other AWS regions to administer the AWS GovCloud (US) Region. Any customer data fields that are defined as outside of the ITAR boundary (such as S3 bucket names) are explicitly documented in the service-specific section as not permitted to contain ITAR-regulated data.

• The AWS GovCloud (US) Region authentication is completely isolated from Amazon.com.

The AWS GovCloud (US) Region also has high-level differences compared to the standard AWS regions. These differences are important when you evaluate and use the AWS GovCloud (US) Region. The following list outlines the differences:

Sign up
During the signup process, each customer is vetted to ensure they are a U.S. entity (such as a government body, contracting company, or educational organization) and cannot be prohibited or restricted by the U.S. government from exporting or providing services.

Endpoints
The AWS GovCloud (US) Region uses endpoints that are specific to the AWS GovCloud (US) Region and that are accessible only to AWS GovCloud (US) customers. For a list of these endpoints, see AWS GovCloud (US) Endpoints (p. 36).

Credentials
You can access the AWS GovCloud (US) Region only with AWS GovCloud (US) credentials (AWS GovCloud (US) account access key and AWS GovCloud (US) IAM user credentials). You cannot access the AWS GovCloud (US) Region with standard AWS credentials. Likewise, you cannot access standard AWS regions using AWS GovCloud (US) credentials. Access credentials for the AWS GovCloud (US) Region are isolated from the standard AWS regions.

AWS Management Console for the AWS GovCloud (US) Region
You sign in to the AWS GovCloud (US) console by using an IAM user name and password. This requirement is different from the standard AWS Management Console, where you can sign in by using your account credentials (email address and password). You cannot use your AWS GovCloud (US) account access keys to sign in to the AWS GovCloud (US) console. For more information about creating an IAM user, see Getting Started with AWS GovCloud (US) (p. 7).

Billing, account activity, and usage reports
An AWS GovCloud (US) account is always associated to a single standard AWS account for billing and payment purposes. All AWS GovCloud (US) billing is billed or invoiced to the associated standard AWS account. You can view the AWS GovCloud (US) account activity and usage reports through the associated standard AWS account only.

Services
The AWS GovCloud (US) Region currently supports only the services that are listed in Supported Services (p. 4). As additional services are deployed to the AWS GovCloud (US) Region, this list will be updated.

Services in the AWS GovCloud (US) Region might have different capabilities compared to services in standard AWS regions. For example, in AWS GovCloud (US), you must launch all Amazon EC2 instances in an Amazon Virtual Private Cloud (Amazon VPC). For detailed information about each service in the AWS GovCloud (US) Region, see Using AWS GovCloud (US) (p. 26).

For all AWS GovCloud (US) accounts created after December 15, 2014, AWS CloudTrail will be automatically enabled with logging turned on. Amazon SNS notifications, however, must be set up independently. If you prefer not to have CloudTrail enabled, you can use the CloudTrail console in the AWS Management Console for the AWS GovCloud (US) Region to disable it or turn off logging.
Multi-factor authentication

Due to the separate authentication stack, the hardware MFA tokens used with standard AWS accounts are not compatible with AWS GovCloud (US) accounts. AWS GovCloud (US) only supports MFA devices listed on the Multi-Factor Authentication page.

AWS GovCloud (US) Billing and Payment

All AWS GovCloud (US) activity, usage, and payments are managed through a standard AWS account. When you sign up for AWS GovCloud (US), your AWS GovCloud (US) account is associated with your standard AWS account. You can associate only one AWS GovCloud (US) account to one standard AWS account. If you require multiple AWS GovCloud (US) accounts, you must create a standard AWS account for each AWS GovCloud (US) account.

To view account activity and usage reports for the AWS GovCloud (US) account, you must sign in to the standard AWS account (using credentials from that account). You cannot view usage and activity from the AWS Management Console for the AWS GovCloud (US) Region.

If you use AWS services in other regions with the standard AWS account, your account activity and usage reports are combined. If you want to separate billing and usage between the two accounts, create a new standard AWS account that you use only to associate with your AWS GovCloud (US) account.

The following diagram outlines the relationship between AWS GovCloud (US) and standard AWS accounts:

![AWS GovCloud (US) account relationship to standard AWS account](image)

Supported Services

The AWS GovCloud (US) Region currently supports AWS services in the following list. For more information about requesting a service that is not currently supported, contact your AWS GovCloud (US) Region business representative.

For a complete list of all regions and their supported services, see Products and Services by Region.
Supported Services

Compute
- Amazon Elastic Compute Cloud (Amazon EC2) (p. 58)
- Amazon EC2 Auto Scaling (p. 45)
- AWS Elastic Beanstalk (p. 57)
- AWS Lambda (p. 71)
- Elastic Load Balancing (p. 64)
- Amazon Elastic Container Registry (p. 60)
- Amazon Elastic Container Service (p. 61)

Developer Tools
- AWS CodeDeploy (p. 51)

Storage & Content Delivery
- Amazon Simple Storage Service (Amazon S3) (p. 76)
- Amazon Elastic Block Store (Amazon EBS) (p. 57)
- Amazon Glacier (p. 67)
- AWS Snowball (p. 69)

Database
- Amazon Relational Database Service (Amazon RDS) (p. 75)
- Amazon DynamoDB (p. 56)
- Amazon ElastiCache (p. 65)

Networking
- Amazon Virtual Private Cloud (Amazon VPC) (p. 79)
- AWS Direct Connect (p. 54)

Management Tools
- Amazon CloudWatch (p. 49)
- Amazon CloudWatch Events (p. 50)
- Amazon EC2 Systems Manager (p. 64)
- AWS CloudFormation (p. 46)
- AWS CloudTrail (p. 47)
- AWS Config (p. 53)
- AWS Management Console for the AWS GovCloud (US) Region (p. 80)

Security, Identity & Compliance
- AWS Certificate Manager (p. 45)
- AWS CloudHSM Classic (p. 46)
- AWS Identity and Access Management (IAM) (p. 68)
- AWS Key Management Service (AWS KMS) (p. 70)
- AWS Multi-Factor Authentication (MFA) (p. 14)

Analytics
- Amazon Elasticsearch Service (p. 61)
- Amazon EMR (Amazon EMR) (p. 66)
- Amazon Kinesis Data Streams (p. 70)
- Amazon Redshift (p. 73)

Application Services
- Amazon API Gateway (p. 44)
- Amazon Simple Notification Service (Amazon SNS) (p. 77)
- Amazon Simple Queue Service (Amazon SQS) (p. 78)
- Amazon Simple Workflow Service (Amazon SWF) (p. 79)
Supported Services

**Support**
- Signing Up for AWS GovCloud (US) Customer Support (p. 15)
- Service Health Dashboard
- AWS Trusted Advisor (p. 81)

**Migration**
- AWS Server Migration Service (AWS SMS) (p. 62)
- AWS Database Migration Service (p. 54)

**Machine Learning**
- Amazon Polly (p. 72)
- Amazon Rekognition (p. 75)

**Additional Software & Services**
- AWS Marketplace (p. 71)
Getting Started with AWS GovCloud (US)

To sign up for AWS GovCloud (US) and to access the AWS Management Console for the AWS GovCloud (US) Region, you follow procedures that are different from those for other AWS regions.

The following topics describe how to sign up and get set up with AWS GovCloud (US).

Topics
- Signing Up for AWS GovCloud (US) (p. 7)
- Onboarding to AWS GovCloud (US) (Direct Customers) (p. 8)
- Onboarding to AWS GovCloud (US) (Resellers or Reseller Customers) (p. 10)
- Enabling Multi-Factor Authentication (MFA) (p. 14)
- Signing Up for AWS GovCloud (US) Customer Support (p. 15)

Signing Up for AWS GovCloud (US)

AWS GovCloud (US) follows specific U.S. regulatory requirements. You can only obtain AWS GovCloud (US) accounts if you are an individual or entity that qualifies as a U.S. Person under applicable regulations. In addition to the AWS Customer Agreement, you must also sign an AWS GovCloud (US) Region Addendum.

To enable access to the AWS GovCloud (US) Region, you must first have a standard AWS account for billing and customer support purposes.

Note
It is a best practice to create a new AWS account that you will use only for AWS GovCloud (US) access. This allows you to do the following:

- Transfer the AWS GovCloud (US) account to another party.
- Ensure the root user of the standard AWS account, which is the parent account of the AWS GovCloud (US) account, is a U.S. Person.
- Fully close the AWS GovCloud (US) account without affecting your other AWS workloads.
- Software vendors who want to be listed in the AWS GovCloud (US) region should sign up as Direct Customer whether they are resellers or not.

To sign up for AWS GovCloud (US)

1. Determine if you are a direct customer, reseller, or reseller customer.

You are a direct customer if your organization is paying or will pay your bills directly to AWS, and you are not reselling AWS services to an end user. You can sign up for an AWS GovCloud (US) account from your standard AWS account.

You are a reseller if your organization is reselling AWS services.

You are a reseller customer if you are paying a third party for AWS services.
2. If you are a direct customer or a reseller, create a standard AWS account by clicking Sign Up on the AWS home page.

   ![Sign Up Button](image)

   If you are a reseller customer, contact your reseller to open a standard account and request AWS GovCloud (US) access.

3. If you are a direct customer:
   1. Sign in to the standard AWS Management Console as a root user for your AWS account.
   2. Navigate to the Account Settings page.
   3. Choose Sign up for AWS GovCloud (US), and then follow the instructions.

   If you do not see a Sign up for AWS GovCloud (US) button, your account does not meet the criteria for self-enrollment. To request enrollment, follow the reseller steps in the next section.

   ![GovCloud (US) Sign Up Button](image)

   If you are a reseller:
   1. Go to the AWS GovCloud (US) Contact Us page.
   2. Complete the form to start the sign-up process.

---

### Onboarding to AWS GovCloud (US) (Direct Customers)

If you are a direct customer, there are few things you should do to make it easier to sign in and use the AWS GovCloud (US) console. We automatically enable AWS CloudTrail for AWS GovCloud (US) accounts, but you should also verify that CloudTrail is enabled to store logs.

### Configuring Your Account

The steps in this section describe how to sign in and create an account alias and access keys.

#### To sign in to the AWS GovCloud (US) console

1. Open the AWS GovCloud (US) console.
2. Sign in using your account number and administrator credentials. For your user name, type Administrator. You will need to specify your account number.
Verifying AWS CloudTrail Is Enabled

**Note**
If you did not save your AWS GovCloud (US) sign-in link, which includes your account number, you can retrieve your account number by signing in to the standard AWS Management Console with your root credentials, opening the **Accounts** page, and choosing the **Sign up for AWS GovCloud (US)** button. You will be directed to a page that indicates you already have access and displays your account number.

**To create an account alias**
Creating an account alias is optional, but strongly recommended. If you do not create an account alias, be sure to save your AWS GovCloud (US) sign-in link because your AWS GovCloud (US) account number is different from your AWS account number.

1. Sign in to the AWS GovCloud (US) console and open the IAM console at https://console.amazonaws-us-gov.com/iam.
2. Next to the IAM users sign-in link, choose **Customize**.
3. Type an alias for your account.

IAM users can now use either the account alias or account number when signing in to the AWS GovCloud (US) console.

**To create and download access keys**
The password for your AWS GovCloud (US) administrator IAM user cannot be reset by the root user of your AWS account. Creating access keys for your AWS GovCloud (US) administrator user is helpful because they can be used to reset your administrator password from the command line.

1. Sign in to the AWS GovCloud (US) console and open the IAM console at https://console.amazonaws-us-gov.com/iam.
2. In the navigation pane, choose **Users**, and select the IAM user account for which you would like to generate access keys.
3. On the **Security Credentials** tab, choose **Create Access Key**.
4. To download the access key, choose **Download Credentials** and save them locally.

**Verifying AWS CloudTrail Is Enabled**
As part of the automated AWS GovCloud (US) activation process, the CloudTrail service should be enabled for each account and an Amazon S3 bucket should be created to store CloudTrail logs. In the event of any interruptions in the automation process, you can manually enable CloudTrail.

**To verify the S3 bucket was created for CloudTrail log storage**
1. Sign in to the AWS GovCloud (US) console and open the Amazon S3 console at https://console.amazonaws-us-gov.com/s3.
2. If a bucket already exists, skip to the next procedure to ensure CloudTrail is enabled.
3. Choose **Create Bucket**.
4. Type a name for your bucket.

Bucket names must be unique. S3 buckets created during the automated process follow the naming convention "cloudtrail-xxxxxxxxxxxxxx" where xxxxxxxxxxxxxx is replaced by the AWS GovCloud (US) account number. If you want to use a different bucket name, you can delete this bucket, create a new bucket, and then follow the steps in the next section to enable CloudTrail.
To verify CloudTrail is enabled

1. Sign in to the AWS GovCloud (US) console and open the CloudTrail console at https://console.amazonaws-us-gov.com/cloudtrail.
2. Choose Get Started Now.
3. On the Turn on CloudTrail page next to Create a new S3 bucket, choose No.
4. From the S3 bucket drop-down list, choose the S3 bucket you created in the previous procedure.
5. Choose Turn On.

This will set a bucket policy that allows the CloudTrail service to store logs in the S3 bucket. If the automated process created an S3 bucket and enabled CloudTrail, the following policy was applied:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws-us-gov:iam::608710470296:root"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws-us-gov:s3:::s3_bucket_name"
    },
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws-us-gov:iam::608710470296:root"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws-us-gov:s3:::s3_bucket_name/AWSLogs/account_id/**",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```

Onboarding to AWS GovCloud (US) (Resellers or Reseller Customers)

If you are a reseller or a reseller customer, you must create an IAM user to sign in to the AWS Management Console for the AWS GovCloud (US) Region.

**Note**
You cannot use the credentials that you received from your AWS GovCloud (US) Region business representative to access the console.

**To create your first administrative IAM user**

1. Download and run the AWS GovCloud (US) console onboard tool.
2. Type your access key ID and secret access key, and then choose Next.
3. Type a password for the administrator, and then choose Next.

4. (Optional) If you want to create an account alias, type a name (all lowercase) for your account, and then choose Next.
An account alias provides an easy-to-remember link for signing in to the console. For more information about account aliases, see Your AWS Account ID and Its Alias in the IAM User Guide.

5. Review your information, and then choose Complete.
You can choose Back to edit any information.

6. Review your new AWS GovCloud (US) credentials. Your original keys have been deactivated.
7. Choose **Download New Keys** and then save them in a secure location. If you do not download them, you will not be able to retrieve them in the future.

8. To access the AWS GovCloud (US) console, choose the link to your account's sign-in URL.

You now have your first IAM user administrator, which you can use to sign in to the AWS GovCloud (US) console. The administrator has full access to manage your AWS GovCloud (US) resources. For example, as the administrator, you can use the AWS GovCloud (US) console to create additional IAM users. You can then manage users and their permissions by assigning them to groups. For more information, see [IAM Users and Groups](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_groups.html) in **IAM User Guide**.

### Enabling Multi-Factor Authentication (MFA)

For increased security, we recommend that you configure multi-factor authentication (MFA) to help protect your AWS GovCloud (US) resources. MFA adds extra security because it requires users to enter a unique authentication code from an approved authentication device when they access AWS websites or services.

AWS GovCloud (US) offers security token-based MFA. You must assign an MFA device (hardware or virtual) to the IAM user or the AWS root account. The device generates a six-digit numeric code based on a time-synchronized, one-time password algorithm. The user must enter a valid code from the device on a second web page during sign-in. Each MFA device assigned to a user must be unique. A user cannot authenticate by entering a code from another user's device.

The following high-level procedure describes how to set up and use MFA in AWS GovCloud (US) and provides links to related information.

1. Get an MFA token device. You can enable only one MFA device per IAM user. The device can be used by the specified user only.
A hardware-based token device, such as one of the AWS-supported hardware token devices listed under the "Hardware Key Fob MFA Device for AWS GovCloud (US)" section of the Multi-Factor Authentication page.

A virtual token device, which is a software application that is compliant with RFC 6238, a standards-based, time-based one-time password (TOTP) algorithm. You can install the application on a mobile device, such as a tablet or smartphone. For a list of apps you can use as virtual MFA devices, see the "Virtual MFA Applications" section of the Multi-Factor Authentication page.

2. Enable the MFA device. There are two steps to enabling a device. First, you create an MFA device entity in IAM. Second, you associate the MFA device entity with the IAM user. You can perform these tasks in the AWS Management Console, the AWS CLI, AWS Tools for Windows PowerShell, or the IAM API.

   For information about enabling MFA devices, see the following topics:
   - Physical MFA device: Enabling a Hardware MFA Device (AWS Management Console)
   - Virtual MFA device: Enabling a Virtual Multi-Factor Authentication (MFA) Device

3. Use the MFA device when you sign in to or access AWS resources.

   For more information, see Using MFA Devices with Your IAM Sign-in Page and Enabling a Virtual Multi-Factor Authentication (MFA) Device.

## Signing Up for AWS GovCloud (US) Customer Support

AWS Support is available for the AWS GovCloud (US) Region. As an AWS GovCloud (US) customer, you can access the AWS Support engineers 24 hours a day by phone, email, and chat. In cases where export controls are a concern, AWS routes cases to ITAR-vetted and trained support engineers who understand the sensitivity around export controls. AWS GovCloud (US) protected resources are accessible only by ITAR-vetted and trained support engineers. However, non-vetted personnel can assist with basic support cases that do not contain protected resources. For more information see AWS GovCloud (US) Region Support.

To sign up for AWS Customer Support for the AWS GovCloud (US) Region, go to the customer support sign up page. You sign up for support by using the standard AWS root account credentials that are associated with your AWS GovCloud (US) account. You can sign up for Business Level support or submit a request for Enterprise Level support by completing the Enterprise Support form.

**Note**

Your premium support options are associated with your standard AWS account but also apply to your AWS GovCloud (US) account. If you already have support on your standard AWS account, you aren’t required to sign up for support again.

To open a new case, sign in to the Support Center with your standard AWS root account credentials. If you are opening a case for your AWS GovCloud (US) account, include a note that this case is for your AWS GovCloud (US) account, and include your AWS GovCloud (US) account ID. Do not enter any ITAR-regulated data in the case.

### Customer Support Differences for the AWS GovCloud (US) Region

- The Customer Support Center is available only through the standard AWS account that is associated with your AWS GovCloud (US) account.
- Some Premium Support features, such as some AWS Trusted Advisor (p. 81) checks, are not available for your AWS GovCloud (US) account.
• The AWS GovCloud (US) Region does not have a dedicated forum area.
• AWS accounts with an associated AWS GovCloud (US) account are prohibited from uploading attachments in Support Center.
Setting Up AWS GovCloud (US) with AWS Services Outside of the AWS GovCloud (US) Region

The following sections describe how to set up services as part of your AWS GovCloud (US) architecture.

Topics
- Setting Up Amazon CloudFront with Your AWS GovCloud (US) Resources (p. 17)
- Setting Up Amazon Route 53 with Your AWS GovCloud (US) Resources (p. 18)
- Setting Up Amazon Route 53 Zone Apex Support with an AWS GovCloud (US) Elastic Load Balancing Load Balancer (p. 19)
- Setting Up Amazon Simple Email Service in Your AWS GovCloud (US) Architecture (p. 24)

Setting Up Amazon CloudFront with Your AWS GovCloud (US) Resources

Amazon CloudFront is a web service that uses a global network of edge locations to deliver content to end users with low latency and high data transfer speeds. CloudFront is an AWS global service that you can leverage with your AWS GovCloud (US) resources. Requests for your content are routed to the nearest edge location, so content is delivered with the best possible performance. CloudFront is optimized to work with other Amazon Web Services, like Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing, and Amazon Route 53.

CloudFront also works seamlessly with any non-AWS origin server, which stores the original, definitive versions of your files. Due to the isolation of the AWS GovCloud (US) Region, using CloudFront with your AWS GovCloud (US) resources is analogous to using CloudFront with a non-AWS origin server.

Topics
- Credentials (p. 17)
- Tips for Setting Up CloudFront (p. 18)
- AWS WAF (p. 18)

Credentials

If you use CloudFront with AWS GovCloud (US), be sure that you use the correct credentials:

- To use CloudFront with your AWS GovCloud (US) resources, you must have an AWS GovCloud (US) account. If you don’t have an account, see Signing Up for AWS GovCloud (US) (p. 7) for more information.
- To set up CloudFront, sign in to the CloudFront console by using your standard AWS credentials. You cannot use your AWS GovCloud (US) account credentials to sign in to the standard AWS Management Console.
Tips for Setting Up CloudFront

As you set up CloudFront to serve your AWS GovCloud (US) content, keep the following in mind:

- You will be setting up CloudFront to distribute content from a custom origin server.
- Because you will be using a custom origin server, you do not have the option to restrict bucket access using a CloudFront Origin Access Identity.
- If you want to restrict viewer access and use signed URLs, you must:
  - Use your standard AWS account and one of its CloudFront key pairs to create the signed URLs. As with other AWS regions, you use the CloudFront key pair with your code or third-party console to create the signed URLs.
  - You can further restrict access to your content by blocking requests not originating from CloudFront IP addresses. You can use bucket policies to accomplish this for original content stored in AWS GovCloud (US) Amazon S3 buckets. A list of IP addresses is maintained on a best-effort basis at https://forums.aws.amazon.com/ann.jspa?annID=2051. For more information, see AWS IP Address Ranges.
  - If you want CloudFront to log all viewer requests for files in your distribution, select an Amazon S3 bucket in an AWS standard region as a destination for the log files.
  - Since CloudFront is not within the AWS GovCloud (US) Region, CloudFront is not within the ITAR boundary. If you want to use CloudFront to distribute your ITAR-regulated content, encrypt your content in transit.
  - Integrated support for CloudFront Live Streaming is not available for origins located in the AWS GovCloud (US) Region.
  - Streaming prerecorded media using Adobe's Real-Time Messaging Protocol (RTMP) is not supported with CloudFront for custom origins.
  - For detailed information about CloudFront, see the CloudFront documentation.

AWS WAF

To help protect your websites and web applications from attacks, you can integrate CloudFront with AWS WAF, a web application firewall. With AWS WAF, you can filter traffic based on conditions you specify, such as the IP addresses from which requests originate or values that appear in headers or query strings. CloudFront responds to HTTP and HTTPS requests with either the requested content or an HTTP 403 status code (Forbidden). You can also configure CloudFront to return a custom error page when a request is blocked.

For more information about AWS WAF, see the AWS WAF Developer Guide. For information about how to add the ID for an AWS WAF web access control list (web ACL) to a CloudFront distribution, see the Values that You Specify When You Create or Update a Web Distribution topic in the Amazon CloudFront Developer Guide.

Setting Up Amazon Route 53 with Your AWS GovCloud (US) Resources

Amazon Route 53 is a highly available and scalable Domain Name System (DNS) web service. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications by translating human readable names like www.example.com into the numeric IP addresses like 192.168.0.1 that computers use to connect to each other.

Route 53’s DNS implementation connects user requests to infrastructure running in Amazon Web Services (AWS), such as an Amazon Elastic Compute Cloud (Amazon EC2) instance, an Elastic Load
Balancing balancer, an Amazon CloudFront distribution, or an Amazon Simple Storage Service (Amazon S3) bucket.

Route 53 can also be used to route users to infrastructure outside of AWS or to resources in the AWS GovCloud (US) Region.

To use Route 53 with your AWS GovCloud (US) resources, you must have an AWS GovCloud (US) account. If you don't have an account, see Signing Up for AWS GovCloud (US) (p. 7) for more information.

To set up Route 53, go to the Route 53 console by using your standard AWS credentials. You cannot use your AWS GovCloud (US) account credentials to sign in to the standard AWS Management Console.

As you set up Route 53 to serve your AWS GovCloud (US) content, keep the following in mind:

• You must log in to the Route 53 console using your standard AWS credentials. Do not use your AWS GovCloud (US) credentials.
• You will set up Route 53 to route end users to your AWS GovCloud (US) resources.
• Route 53 is not within the AWS GovCloud (US) Region so Route 53 is not within the ITAR boundary. Route 53 domain names, subdomain names, hostnames, aliases, cnames, and other record data fields are not permitted to contain ITAR-regulated data.
• You can't directly associate a commercial Route 53 public or private hosted zone with an AWS GovCloud (US) account.
• For detailed information about Route 53, see the Amazon Route 53 Developer Guide.

Setting Up Amazon Route 53 Zone Apex Support with an AWS GovCloud (US) Elastic Load Balancing Load Balancer

Amazon Route 53 is a highly available and scalable Domain Name System (DNS) web service. It is designed to provide an extremely reliable and cost effective way to route end users to Internet applications by translating human readable names like www.example-company.com into numeric IP addresses like 192.168.0.1 that computers use to connect to each other.

Route 53’s DNS implementation connects user requests to infrastructure running inside (and outside) of Amazon Web Services (AWS). For example, if you have multiple web servers running on Amazon Elastic Compute Cloud (Amazon EC2) instances behind an Elastic Load Balancing load balancer, Route 53 will route all traffic addressed to your website (e.g. www.example.com) to the load balancer DNS name (e.g. elb1234.elb.amazonaws.com).

Additionally, Route 53 supports the alias resource record set, which lets you map your zone apex (e.g. example.com) DNS name to your load balancer DNS name. IP addresses associated with Elastic Load Balancing can change at any time due to scaling or software updates. Route 53 responds to each request for an alias resource record set with one IP address for the load balancer. If a load balancer has more than one IP address, Elastic Load Balancing selects one of the IP addresses in a round-robin fashion and returns it to Route 53; Route 53 then responds to the request with that IP address.

Alias resource record sets are virtual records that work like CNAME records. But they differ from CNAME records in that they are not visible to resolvers. Resolvers only see the A record and the resulting IP address of the target record. As such, unlike CNAME records, alias resource record sets are available to configure a zone apex (also known as a root domain or naked domain) in a dynamic environment.

This section provides a solution for Route 53 zone apex alias support by setting up an Amazon CloudFront distribution between Route 53 and an AWS GovCloud (US) Elastic Load Balancing load balancer.
balancer. The solution demonstrates how to configure Route 53 with a zone apex alias resource record set that maps to a CloudFront web distribution DNS name. The CloudFront distribution in turn points to the AWS GovCloud (US) load balancer DNS name as a custom origin.

An additional benefit of this approach is that CloudFront can help improve the performance of your website, including both static and dynamic content. For more information about CloudFront, see the CloudFront documentation.

The following figure shows the various AWS services used to demonstrate this solution:

**Step 1: Sign Up for AWS GovCloud (US)**

- To use AWS services in the AWS GovCloud (US) Region, you must have an AWS GovCloud (US) account. If you don't have an account, see Signing Up for AWS GovCloud (US) (p. 7) for more information.

**Step 2: Create Your Resources in the AWS GovCloud (US) Region**

1. Create two web application Amazon EC2 servers via the AWS GovCloud (US) console and confirm that they are in a running state. Configuring the web servers on the Amazon EC2 instances is outside of the scope of this section.
2. Create an Elastic Load Balancing load balancer and add the two instances created in the previous step to the load balancer. Confirm that the instances are in service and note the DNS name of the newly created load balancer.

3. Test access to your website by entering the load balancer DNS name in a web browser. You can verify the load balancer is balancing traffic between the two instances by waiting at least one minute between requests.

Step 3: Create a CloudFront Custom Origin Web Distribution

Because AWS GovCloud (US) is not currently integrated into the CloudFront service, you must create a CloudFront distribution using your standard AWS account.

1. Sign in to the CloudFront console with your standard AWS account, and choose Create Distribution.
Step 3: Create a CloudFront Custom Origin Web Distribution

2. Select the **Web** distribution delivery method, and then choose **Continue**.

3. In **Origin Domain Name**, type the AWS GovCloud (US) load balancer DNS name to create a custom origin.

4. In **Alternate Domain Names (CNAMEs)**, add the zone apex name.
5. Choose **Create Distribution**.

6. After the status for the new distribution changes to **Deployed**, make a note of the domain name. You will use this domain name when you set up Route 53 in the next step.

For information about how CloudFront processes and forwards requests to a customer origin server, such as an AWS GovCloud (US) load balancer, see the [CloudFront documentation](https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/).

**Step 4: Configure a New Route 53 Alias Resource Record Set**

1. Using your standard AWS account from the previous step, sign in to the Route 53 console.
2. Create a new alias resource record set for your root domain name. For **Alias**, choose **Yes**. From the **Alias Target** drop-down list, select the CloudFront distribution name you created earlier.
Step 5: Test that Your Website Is Accessible

• Enter your root domain in a web browser to verify that your website is accessible.

Congratulations! You have successfully pointed your zone apex at your Elastic Load Balancing load balancer in the AWS GovCloud (US) Region.

For more information about Route 53, see the Route 53 documentation.

Setting Up Amazon Simple Email Service in Your AWS GovCloud (US) Architecture

Amazon Simple Email Service (Amazon SES) is a cost-effective outbound-only email-sending service built on the reliable and scalable infrastructure originally developed to serve the Amazon.com customer base. With Amazon SES, you can send transactional email, marketing messages, or any other type of high-quality content, and you only pay for what you use.

Amazon SES offers a number of functions beyond simply sending email. Along with high deliverability, Amazon SES provides easy, real-time access to your sending statistics and built-in notifications for bounces and complaints to help you fine-tune your email-sending strategy.

To use Amazon SES in your AWS GovCloud (US) architecture, you must have both an AWS account and an AWS GovCloud (US) account. If you do not have an AWS GovCloud (US) account, see Signing Up for AWS GovCloud (US) (p. 7).

To set up Amazon SES, sign in to the Amazon SES console using your standard AWS credentials. You cannot use your AWS GovCloud (US) account credentials to sign into the standard AWS Management Console.

As you set up Amazon SES to use within your AWS GovCloud (US) architecture, keep the following in mind:
• Amazon SES is not within the ITAR boundary and ITAR data cannot be sent using Amazon SES.
• You must sign in to the Amazon SES console using your standard AWS credentials. Do not use your AWS GovCloud (US) credentials.
• When making API calls to the Amazon SES endpoint from the AWS GovCloud (US) Region, you must use your standard AWS account credentials. Do not use your AWS GovCloud (US) credentials.

<table>
<thead>
<tr>
<th>Region name</th>
<th>Region</th>
<th>API (HTTPS) endpoint</th>
<th>SMTP endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>us-east-1</td>
<td>email.us-east-1.amazonaws.com</td>
<td>email-smtp.us-east-1.amazonaws.com</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>us-west-2</td>
<td>email.us-west-2.amazonaws.com</td>
<td>email-smtp.us-west-2.amazonaws.com</td>
</tr>
</tbody>
</table>

• Amazon SES access is "sandboxed" by default. With sandbox access, you can only send email to the Amazon SES mailbox simulator and to email addresses or domains that you have verified. After you test your setup and want to go into production, you must request production access.
Using AWS GovCloud (US)

If you have used other AWS regions, you should be aware of specific differences in the AWS GovCloud (US) Region. For example, Amazon Resource Names (ARNs) and endpoints are different in the AWS GovCloud (US) Region.

In addition to the specific differences, the following topics describe how to maintain compliance with International Traffic in Arms Regulations (ITAR), how to access AWS GovCloud (US), and how to control access to your AWS GovCloud (US) account.

Topics
• Amazon Resource Names (ARNs) in AWS GovCloud (US) (p. 26)
• AWS GovCloud (US) Endpoints (p. 36)
• Maintaining U.S. International Traffic in Arms Regulations (ITAR) Compliance (p. 39)
• Accessing the AWS GovCloud (US) Region (p. 39)
• Controlling Access to Your AWS GovCloud (US) Account (p. 40)
• Command Line and API Access (p. 40)
• Resource Limits (p. 41)
• Penetration Testing (p. 41)
• Service Health Dashboard (p. 42)

Amazon Resource Names (ARNs) in AWS GovCloud (US)

Amazon Resource Names (ARNs) uniquely identify AWS resources. We require an ARN when you need to specify a resource unambiguously across all of AWS, such as in IAM policies, Amazon S3 bucket names, and API calls. In the AWS GovCloud (US) Region, ARNs have an identifier that is different from the one in other AWS regions. For all other regions, ARNs begin with:

```
arn:aws
```

In the AWS GovCloud (US) Region, ARNs begin with:

```
arn:aws-us-gov
```

If an ARN requires a region, for the AWS GovCloud (US) Region, the region should be identified as `us-gov-west-1`.

Topics
• ARN Format (p. 27)
• Example ARNs (p. 27)
• Paths in ARNs (p. 35)
ARN Format

Here are some example ARNs:

```
<!-- IAM user name -->
arn:aws-us-gov:iam::123456789012:David

<!-- Amazon EC2 instances -->

<!-- Amazon S3 bucket (and all objects in it)--> 
arn:aws-us-gov:s3:::my_corporate_bucket/*
```

The following are the general formats for ARNs. The specific components and values used depend on the AWS service.

```
arn:aws-us-gov:service:region:account:resource
arn:aws-us-gov:service:region:account:resourcetype/resource
```

- **service**
  
  The service namespace that identifies the AWS product (for example, Amazon S3 or IAM). For a list of namespaces, see AWS Service Namespaces in the Amazon Web Services General Reference.

- **region**
  
  The region in which the resource reside. The ARNs for some resources do not require a region, so this component might be omitted. For the AWS GovCloud (US) Region, the region is us-gov-west-1.

- **account**
  
  The ID of the AWS account that owns the resource, without the hyphens (for example, 123456789012). The ARNs for some resources don’t require an account number, so this component might be omitted.

- **resource, resourcetype:resource, or resourcetype/resource**
  
  The content of this part of the ARN varies by service. It often includes an indicator of the type of resource—for example, IAM user—followed by a slash (/) or a colon (:), followed by the resource name itself. Some services allow paths for resource names, as described in Paths in ARNs (p. 35).

Example ARNs

The following sections provide syntax and examples of the ARNs for different services. For more information about using ARNs in a specific AWS service, see the documentation for that service.

**Topics**

- Amazon API Gateway (p. 28)
- Amazon EC2 Auto Scaling (p. 28)
- AWS Certificate Manager (p. 29)
- Amazon CloudWatch Events (p. 29)
- AWS CodeDeploy (p. 29)
- AWS Config (p. 29)
• AWS Database Migration Service (p. 30)
• Amazon DynamoDB (p. 30)
• AWS Elastic Beanstalk (p. 30)
• Amazon Elastic Compute Cloud (p. 31)
• Amazon Elastic Container Registry (p. 31)
• Amazon Elastic Container Service (p. 31)
• Amazon Elasticsearch Service (p. 32)
• AWS Identity and Access Management (p. 32)
• Amazon Kinesis Data Streams (p. 33)
• AWS Lambda (p. 33)
• Amazon Polly (p. 34)
• Amazon Rekognition (p. 34)
• Amazon Simple Notification Service (p. 34)
• Amazon Simple Queue Service (p. 34)
• Amazon Simple Storage Service (p. 35)
• Amazon Simple Workflow Service (p. 35)

Amazon API Gateway

Syntax:

```
arn:aws-us-gov:apigateway:region::resource-path
```

Example:

```
arn:aws-us-gov:apigateway:us-gov-west-1::/restapis/a123456789012bc3de45678901f23a45/*
```

```
arn:aws-us-gov:apigateway:us-gov-west-1::a123456789012bc3de45678901f23a45:/test/mydemoresource/*
```

```
arn:aws-us-gov:apigateway*:a123456789012bc3de45678901f23a45://petstorewalkthrough/pets
```

```
```

Amazon EC2 Auto Scaling

Syntax:

```
```
Example:

```
```

**AWS Certificate Manager**

Syntax:

```
```

Example:

```
```

**Amazon CloudWatch Events**

Syntax:

```
arn:aws-us-gov:events:us-gov-west-1:*:*
```

```
arn:aws-us-gov:events:us-gov-west-1:123456789012:*
```

```
```

**AWS CodeDeploy**

Syntax:

```
arn:aws-us-gov:codedeploy:account-id:application/applicationname
```

```
arn:aws-us-gov:codedeploy:account-id:deploymentgroup/deployment-group-name
```

```
arn:aws-us-gov:codedeploy:account-id:deploymentconfig/deployment-configuration-name
```

```
arn:aws-us-gov:codedeploy:account-id:instance/instanceid
```

```
arn:aws-us-gov:codedeploy:*
```

```
arn:aws-us-gov:codedeploy:account-id:*
```

**AWS Config**

Syntax:
Example ARNs

**AWS Database Migration Service**

**Syntax:**

```
```

**Example:**

```
```

**Amazon DynamoDB**

**Syntax:**

```
```

**Example:**

```
```

**AWS Elastic Beanstalk**

**Syntax:**

```
```

```
```

```
```

```
```

```
```

```
arn:aws-us-gov:elasticbeanstalk:region::solutionstack/solutionstackname
```

**Examples:**
Example ARNs

**Amazon Elastic Compute Cloud**

Syntax:

- `arn:aws-us-gov:ec2:region:account:placement-group/placement-group-name`
- `arn:aws-us-gov:ec2:region::snapshot/snapshot-id`

Examples:


**Amazon Elastic Container Registry**

Syntax:

- `arn:aws-us-gov:ecr:region:accountid:repository/repository-name`

Examples:


**Amazon Elastic Container Service**

Syntax:

Example ARNs

**Amazon Elasticsearch Service**

**Syntax:**


**Examples:**


**AWS Identity and Access Management**

**Syntax:**

- `arn:aws-us-gov:iam::account:root`
AWS GovCloud (US) User Guide
Example ARNs

<table>
<thead>
<tr>
<th>ARN Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>arn:aws-us-gov:iam::account:user/username</code></td>
<td>Account user ARN</td>
</tr>
<tr>
<td><code>arn:aws-us-gov:iam::account:group/groupname</code></td>
<td>Account group ARN</td>
</tr>
<tr>
<td><code>arn:aws-us-gov:iam::account:role/rolename</code></td>
<td>Account role ARN</td>
</tr>
<tr>
<td><code>arn:aws-us-gov:iam::account:instance-profile/instanceprofilename</code></td>
<td>Account instance profile ARN</td>
</tr>
<tr>
<td><code>arn:aws-us-gov:sts::account:federated-user/username</code></td>
<td>Account federated user ARN</td>
</tr>
<tr>
<td><code>arn:aws-us-gov:iam::account:mfa/virtualdevicename</code></td>
<td>Account MFA ARN</td>
</tr>
<tr>
<td><code>arn:aws-us-gov:iam::account:server-certificate/certificatename</code></td>
<td>Account server certificate ARN</td>
</tr>
</tbody>
</table>

Examples:

```
arn:aws-us-gov:iam::123456789012:root
arn:aws-us-gov:iam::123456789012:user/Bob
arn:aws-us-gov:iam::123456789012:user/division_abc/subdivision_xyz/Bob
arn:aws-us-gov:iam::123456789012:group/Developers
arn:aws-us-gov:iam::123456789012:group/division_abc/subdivision_xyz/product_A/Developers
arn:aws-us-gov:iam::123456789012:role/S3Access
arn:aws-us-gov:iam::123456789012:role/application_abc/component_xyz/S3Access
arn:aws-us-gov:iam::123456789012:instance-profile/Webserver
arn:aws-us-gov:sts::123456789012:federated-user/Bob
arn:aws-us-gov:iam::123456789012:mfa/BobJonesMFA
arn:aws-us-gov:iam::123456789012:server-certificate/ProdServerCert
arn:aws-us-gov:iam::123456789012:server-certificate/division_abc/subdivision_xyz/ProdServerCert
```

Amazon Kinesis Data Streams

Syntax:

```
```

Examples:

```
```

AWS Lambda

Syntax:

```
arn:aws-us-gov:lambda:account-id:function:function-name
```

```
arn:aws-us-gov:lambda:account-id:function:function-name:alias-name
```

```
```

```
```

Examples:

```
```

```
```

33
### Example ARNs

<table>
<thead>
<tr>
<th>Example ARNs</th>
<th>Syntax</th>
</tr>
</thead>
</table>

#### Amazon Polly

**Syntax:**

- `arn:aws-us-gov:polly:region:account-id:lexicon/LexiconName`

**Examples:**


#### Amazon Rekognition

**Syntax:**

- `arn:aws-us-gov:rekognition:region:account-id:*`

**Examples:**


#### Amazon Simple Notification Service

**Syntax:**


**Examples:**

- `arn:aws-us-gov:sns:us-gov-west-1:123456789012:my_corporate_topic:02034b43-fefa-4e07-a5eb-3be56f8c54ce`

#### Amazon Simple Queue Service

**Syntax:**


**Example:**

Amazon Simple Storage Service

Syntax:

- arn:aws-us-gov:s3:::bucketname
- arn:aws-us-gov:s3:::bucketname/objectpath

Amazon S3 does not require an account number or region in ARNs.

Examples:

- arn:aws-us-gov:s3:::my_corporate_bucket
- arn:aws-us-gov:s3:::my_corporate_bucket/*
- arn:aws-us-gov:s3:::my_corporate_bucket/Development/*

Amazon Simple Workflow Service

Syntax:


Examples:

- arn:aws-us-gov:swf:us-gov-west-1:123456789012:domain/department1

Paths in ARNs

Some services let you specify a path for the resource name. For example, in Amazon S3, the resource identifier is an object name that can include slashes (/) to form a path. Similarly, IAM user names and group names can include paths.

Paths can include wildcard characters such as an asterisk (*). For example, to specify all IAM users whose user name includes the prefix product_1234, you can use a wildcard like this:

- arn:aws-us-gov:iam::123456789012:user/Development/product_1234/*

To specify all IAM users or IAM groups in the AWS account, use a wildcard after the user/ or group/part of the ARN, respectively.

- arn:aws-us-gov:iam::123456789012:user/*
- arn:aws-us-gov:iam::123456789012:group/*

The following example shows ARNs for an Amazon S3 bucket in which the resource name includes a path:

- arn:aws-us-gov:s3:::my_corporate_bucket/*
- arn:aws-us-gov:s3:::my_corporate_bucket/Development/*

You cannot use a wildcard in the resource type, such as the term user in an IAM ARN. The following is not allowed:

- arn:aws-us-gov:iam::123456789012:u*
AWS GovCloud (US) Endpoints

If you access AWS GovCloud (US) by using the command line interface (CLI) or programmatically by using the APIs, you need the AWS GovCloud (US) Region endpoints. The following table lists each AWS service available in GovCloud (US) and its corresponding endpoints.

<table>
<thead>
<tr>
<th>AWS Service</th>
<th>AWS GovCloud (US) Endpoint</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon API Gateway*</td>
<td>apigateway.us-gov-west-1.amazonaws.com**</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Amazon EC2 Auto Scaling</td>
<td>autoscaling.us-gov-west-1.amazonaws.com</td>
<td>HTTP and HTTPS</td>
</tr>
<tr>
<td>AWS Certificate Manager</td>
<td>acm.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>AWS CloudFormation</td>
<td>cloudformation.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>AWS CloudHSM Classic</td>
<td>cloudhsm.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>AWS CloudTrail</td>
<td>cloudtrail.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Amazon CloudWatch</td>
<td>monitoring.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Amazon CloudWatch Events</td>
<td>events.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Amazon CloudWatch Logs</td>
<td>logs.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>AWS CodeDeploy</td>
<td>codedeploy.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>AWS Config</td>
<td>config.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>AWS Config Rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWS Direct Connect</td>
<td>directconnect.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>AWS Database Migration Service (DMS)</td>
<td>dms.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Amazon DynamoDB</td>
<td>dynamodb.us-gov-west-1.amazonaws.com</td>
<td>HTTP and HTTPS</td>
</tr>
<tr>
<td>Amazon DynamoDB Streams</td>
<td>streams.dynamodb.us-gov-west-1.amazonaws.com</td>
<td>HTTP and HTTPS</td>
</tr>
<tr>
<td>AWS Elastic Beanstalk</td>
<td>elasticbeanstalk.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Amazon Elastic Block Store (Amazon EBS)</td>
<td>ec2.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Amazon Elastic Compute Cloud (Amazon EC2)</td>
<td>ec2.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>

For more information, see Amazon Resource Names (ARNs) and AWS Service Namespaces.
<table>
<thead>
<tr>
<th>AWS Service</th>
<th>AWS GovCloud (US) Endpoint</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon EC2 Systems Manager</td>
<td>ssm.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Amazon Elastic Container Registry</td>
<td>ecr.us-gov-west-1.amazonaws.com **</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Amazon Elastic Container Service</td>
<td>ecs.us-gov-west-1.amazonaws.com **</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Elastic Load Balancing</td>
<td>elasticloadbalancing.us-gov-west-1.amazonaws.com</td>
<td>HTTP and HTTPS</td>
</tr>
<tr>
<td>Amazon ElastiCache</td>
<td>elasticache.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Amazon Elasticsearch Service</td>
<td>es.us-gov-west-1.amazonaws.com **</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Amazon EMR (Amazon EMR)</td>
<td>elasticmapreduce.us-gov-west-1.amazonaws.com</td>
<td>HTTP and HTTPS</td>
</tr>
<tr>
<td>Amazon Glacier</td>
<td>glacier.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>AWS Identity and Access Management (IAM)</td>
<td>iam.us-gov.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>AWS Key Management Service (AWS KMS)</td>
<td>kms-fips.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Amazon Kinesis Data Streams</td>
<td>kinesis.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>AWS Lambda</td>
<td>lambda.us-gov-west-1.amazonaws.com **</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Amazon Polly</td>
<td>polly.us-gov-west-1.amazonaws.com **</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Amazon Redshift</td>
<td>redshift.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Amazon Rekognition</td>
<td>rekognition.us-gov-west-1.amazonaws.com **</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Amazon Relational Database Service (Amazon RDS)</td>
<td>rds.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>AWS Server Migration Service (AWS SMS)</td>
<td>sms.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Amazon Simple Storage Service (Amazon S3)</td>
<td>s3-us-gov-west-1.amazonaws.com **</td>
<td>HTTP and HTTPS</td>
</tr>
<tr>
<td>Amazon Simple Storage Service (Amazon S3) (FIPS 140-2)</td>
<td>s3-fips-us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Amazon Simple Storage Service (Amazon S3) (website)</td>
<td>s3-website-us-gov-west-1.amazonaws.com</td>
<td>HTTP</td>
</tr>
</tbody>
</table>
### Endpoints

<table>
<thead>
<tr>
<th>AWS Service</th>
<th>AWS GovCloud (US) Endpoint</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Simple Notification Service (Amazon SNS)</td>
<td>sns.us-gov-west-1.amazonaws.com</td>
<td>HTTP and HTTPS</td>
</tr>
<tr>
<td>Amazon Simple Queue Service (Amazon SQS)</td>
<td>sqs.us-gov-west-1.amazonaws.com</td>
<td>HTTP and HTTPS</td>
</tr>
<tr>
<td>Amazon Simple Workflow Service (Amazon SWF)</td>
<td>swf.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>AWS Security Token Service (AWS STS)</td>
<td>sts.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>AWS Snowball</td>
<td>snowball.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Amazon Virtual Private Cloud (Amazon VPC)</td>
<td>ec2.us-gov-west-1.amazonaws.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td>AWS Management Console for the AWS GovCloud (US) Region</td>
<td>console.amazonaws-us-gov.com</td>
<td>HTTPS</td>
</tr>
<tr>
<td></td>
<td>signin.amazonaws-us-gov.com</td>
<td></td>
</tr>
<tr>
<td>AWS Management Console with Federation</td>
<td>signin.amazonaws-us-gov.com/federation</td>
<td>HTTPS</td>
</tr>
<tr>
<td>AWS Management Console with SAML</td>
<td>signin.amazonaws-us-gov.com/saml</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>

**Note**

* Amazon API Gateway edge-optimized API and edge-optimized custom domain name are not supported.
* Amazon Route 53 hosted Zone ID for the regional endpoint in the AWS GovCloud (US) region is Z1K6XKP9SAGWDV.
** AWS GovCloud (US) uses FIPS 140-2 validated cryptographic modules to support compliance with FIPS 140-2 in all our HTTPS endpoints except:
  * The non-FIPS alternative for Amazon S3: s3-us-gov-west-1.amazonaws.com
  * The AWS Key Management Service endpoint kms.us-gov-west-1.amazonaws.com is active, but does not support FIPS 140-2 for TLS connections.
  * The Amazon Elastic Container Registry endpoint does not yet support FIPS 140-2.
  * The Amazon Elastic Container Service endpoint does not yet support FIPS 140-2.
  * The Amazon Elasticsearch Service endpoint does not yet support FIPS 140-2.
  * The AWS Lambda endpoint does not yet support FIPS 140-2.
  * The Amazon Polly endpoint does not yet support FIPS 140-2.
  * The Amazon API Gateway endpoint does not yet support FIPS 140-2.
  * The Amazon Rekognition endpoint does not yet support FIPS 140-2.

When using the endpoints, note the following:

* If you use the AWS CLI or SDK for Python with Amazon SQS, you can also use the following legacy endpoint: us-gov-west-1.queue.amazonaws.com
Maintaining ITAR Compliance

If you store and process ITAR-regulated data in the AWS GovCloud (US) Region, you must conform to the following ITAR requirements, in addition to any other ITAR or export control restrictions that may be applicable to you:

- You are an individual or entity that qualifies as a U.S. Person under the applicable regulations.
- You have and will maintain a valid Directorate of Defense Trade Controls (DDTC) registration.
- You have full export privileges under U.S. export control laws and regulations and are not a denied or debarred party or otherwise subject to sanctions.
- If your export control privileges are revoked, suspended, or terminated, or you otherwise become subject to sanctions or are barred from maintaining export-controlled data, you will immediately remove ITAR and other export-controlled data from the AWS services.
- You must maintain an effective compliance program to ensure compliance with applicable U.S. export control laws and regulations, including ITAR, if applicable.

Note
Even if you don’t process any ITAR-regulated data, the owner of the AWS GovCloud (US) account must be a U.S. person. AWS doesn’t require IAM users or users of applications that run in the AWS GovCloud (US) Region to be U.S. persons. As part of the shared responsibility model, you are responsible for restricting access to your IAM users and to your application in accordance with regulations that apply to you.

ITAR Boundary for AWS GovCloud (US) Services

If you maintain ITAR-regulated data in the AWS GovCloud (US) Region, you must comply with the ITAR restrictions for each AWS service in the AWS GovCloud (US) Region. For more information about the ITAR boundaries for each service, see the service-specific information in Services in the AWS GovCloud (US) Region (p. 43).

Accessing the AWS GovCloud (US) Region

When you access the AWS GovCloud (US) Region, use your AWS GovCloud (US) credentials. Although your AWS GovCloud (US) account is associated with your standard AWS account, each account has distinct credentials, where users from one account cannot access AWS resources from the other account. In other words, when you use the AWS GovCloud (US) Region, you must use credentials that were created
in that region. Similarly, when you use the standard AWS regions, you must use credentials that were created in those regions.

You can use any of the following methods to access and manage resources in the AWS GovCloud (US) Region:

- The AWS Management Console for the AWS GovCloud (US) Region provides an easy-to-use graphical interface to manage your compute, storage, and other cloud resources. Most AWS products can be used with the console, and the console supports the majority of functionality for each service. You can sign in to the console only as an IAM user. For more information, see Onboarding to AWS GovCloud (US) (Resellers or Reseller Customers) (p. 10).

- The AWS command line interface (CLI) allows you to control AWS services from a command line and automate commands through scripts. For more information about accessing the CLI for each service, see AWS Command Line Tools in the AWS General Reference.

- The AWS SDKs offer SDKs for Java, .NET, PHP, Android, iOS, and Ruby. The Sample Code & Libraries Catalog also provides a listing of code, SDKs, sample applications, and other tools available for use.

- The Toolkits for developers provide programming libraries that help you quickly deploy your applications to AWS for Java or .NET. For more information, see AWS Toolkit for Eclipse or AWS Toolkit for Visual Studio.

- You can construct REST or Query API calls to AWS services. For API syntax and examples, see the API references for each service at https://aws.amazon.com/documentation/.

- The AWS ElasticWolf Client Console can be used to manage AWS resources in all regions.

Controlling Access to Your AWS GovCloud (US) Account

Your AWS GovCloud (US) account credentials grant full access to your AWS GovCloud (US) account. We recommend that you don't share your account credentials. Instead, use AWS Identity and Access Management (IAM) to grant users access to AWS GovCloud (US). With IAM, you can control who can perform which actions on a specific resource. Signing Up for AWS GovCloud (US) (p. 7) discusses how you create your first IAM administrative user.

For more information, see What Is IAM? in Using IAM.

For suggestions about how to secure your account with IAM, see IAM Best Practices in Using IAM.

Command Line and API Access

You can use the command line interface (CLI), Query API, or REST interfaces to access AWS GovCloud (US) services. You can also use a language-specific software development kit (SDK). For more information about the CLI and SDK tools, see Tools for Amazon Web Services.

For the CLI and APIs, you are required to use access and secret access keys. You can create keys for each individual user by creating IAM users. For more information, see Working with Users and Groups in Using IAM.

After you have installed your preferred tool, you can access AWS GovCloud (US) by specifying the AWS GovCloud (US) endpoint for the AWS service that you want to access.

For information about setting regions using the AWS SDKs, see Available Region Endpoints for the AWS SDKs in the AWS Developer Center.
If you use the CLI, you can either specify the AWS GovCloud (US) endpoint every time you enter a command, or you can set an environment variable that specifies the endpoint. For more information, see the CLI documentation for the service.

**Resource Limits**

By default, AWS maintains limits for certain resources in your AWS GovCloud (US) account. For example, accounts have a limit on the number of Amazon EC2 instances that can be launched. You can see your current limits and request limit increases on the Limits Page in the Amazon EC2 console. When you request a limit increase, specify your AWS GovCloud (US) account ID and select the AWS GovCloud (US) Region from the region drop-down list.

For more information, see [AWS Service Limits](#).

**Penetration Testing**

Penetration testing can be indistinguishable from activity that is prohibited by AWS, such as certain security violations and network abuse. As a result, AWS has established a policy that you must submit a request for permission to conduct penetration testing on your AWS GovCloud (US) instances.

You are required to sign in by using the standard AWS root account credentials that are associated with your AWS GovCloud (US) account. You can request up to three months of penetration testing by specifying the start and end times. The form also includes our testing terms and policies. After you submit the form, AWS reviews your request and will respond in approximately one to two business days.

If you do not have standard AWS root account credentials, submit your request by sending an email to aws-security-cust-pen-test@amazon.com with the following information:

- Account name:
- Account number:
- Email address:
- Additional email address to cc:
  - **Account owner must be specified on cc.**
- IPs to be scanned:
- Target or source:
- Instance IDs:
  - **Be aware that testing to or from m1.small or t1.micro instances is prohibited.**
  - **These instances must be specified.**
- Source IPs:
- Region:
- Time zone:
- Start date/time:
- End date/time:
- Additional comments:

For more information, see [Penetration Testing](#).
Service Health Dashboard

AWS GovCloud (US) includes a dashboard that displays up-to-the-minute information about service availability in the region. To get current status information, or subscribe to an RSS feed to be notified of interruptions to each individual service, see the Service Health Dashboard.
Services in the AWS GovCloud (US) Region

The following sections describe the differences between the AWS GovCloud (US) Region and the standard AWS regions. They include links to documentation and describe the ITAR boundaries (where you can and can’t enter or process ITAR-regulated data) for each service. ITAR-regulated data is permitted in most configuration data fields. However, some of the data fields, such as Amazon S3 bucket names or Amazon EC2 tags, cannot contain ITAR-regulated data. Also, some services, such as Amazon SNS, cannot process ITAR-regulated data at all.

Topics
- Amazon API Gateway (p. 44)
- Amazon EC2 Auto Scaling (p. 45)
- AWS Certificate Manager (p. 45)
- AWS CloudFormation (p. 46)
- AWS CloudHSM Classic (p. 46)
- AWS CloudTrail (p. 47)
- Amazon CloudWatch (p. 49)
- Amazon CloudWatch Events (p. 50)
- Amazon CloudWatch Logs (p. 51)
- AWS CodeDeploy (p. 51)
- AWS Config (p. 53)
- AWS Database Migration Service (p. 54)
- AWS Direct Connect (p. 54)
- Amazon DynamoDB (p. 56)
- AWS Elastic Beanstalk (p. 57)
- Amazon Elastic Block Store (Amazon EBS) (p. 57)
- Amazon Elastic Compute Cloud (Amazon EC2) (p. 58)
- Amazon Elastic Container Registry (p. 60)
- Amazon Elastic Container Service (p. 61)
- Amazon Elasticsearch Service (p. 61)
- AWS Server Migration Service (AWS SMS) (p. 62)
- Importing Virtual Machines into the AWS GovCloud (US) Region (p. 63)
- Amazon EC2 Systems Manager (p. 64)
- Elastic Load Balancing (p. 64)
- Amazon ElastiCache (p. 65)
- Amazon EMR (Amazon EMR) (p. 66)
- Amazon Glacier (p. 67)
Amazon API Gateway

The following list describes the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

• At this time, the service endpoint does not support FIPS 140-2.
• Amazon API Gateway edge-optimized API and edge-optimized custom domain name are not supported.
• Amazon Route 53 Hosted Zone ID for the regional endpoint in the AWS GovCloud (US) region is Z1K6XKP9SAGWDV.

For more information about Amazon API Gateway, see the Amazon API Gateway documentation.

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Customers’ APIs are permitted to process ITAR data</td>
<td>API Gateway’s configuration metadata is not permitted to contain ITAR-regulated data*, including:</td>
</tr>
<tr>
<td></td>
<td>• API Name</td>
</tr>
<tr>
<td></td>
<td>• API Description</td>
</tr>
</tbody>
</table>

* Depending on the specific ITAR controls and policies in place.
## ITAR Boundary

#### Amazon EC2 Auto Scaling

For more information about Amazon EC2 Auto Scaling, see the [Amazon EC2 Auto Scaling documentation](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/itars-supported.html).

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Not applicable</td>
<td>• Auto Scaling is not permitted to contain ITAR-regulated data.</td>
</tr>
<tr>
<td></td>
<td>• For example, do not enter ITAR-regulated data in the following fields:</td>
</tr>
<tr>
<td></td>
<td>• Capacity group tag names</td>
</tr>
<tr>
<td></td>
<td>• Capacity group tag name values</td>
</tr>
<tr>
<td></td>
<td>• Capacity group names</td>
</tr>
<tr>
<td></td>
<td>• Amazon EC2 Security Group names</td>
</tr>
<tr>
<td></td>
<td>• Scaling policies</td>
</tr>
<tr>
<td></td>
<td>• Launch notifications</td>
</tr>
<tr>
<td></td>
<td>• Notification topics</td>
</tr>
<tr>
<td></td>
<td>• Policy documents</td>
</tr>
</tbody>
</table>

#### AWS Certificate Manager

For more information about AWS Certificate Manager, see the [AWS Certificate Manager documentation](https://docs.aws.amazon.com/AWSSM/latest/UserGuide/itars-supported.html).

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Not applicable</td>
<td>• Authorizer Name</td>
</tr>
</tbody>
</table>

* However customers can send ITAR-regulated data through the customers’ deployed APIs, with the caveat that downstream systems need to be compliant (e.g. caching cannot be enabled on the API for any ITAR-regulated data)
AWS CloudFormation

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

- Use SSL (HTTPS) when you make calls to the service in the AWS GovCloud (US) Region. In other regions, you can use HTTP or HTTPS.

For more information about AWS CloudFormation, see the AWS CloudFormation documentation.

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not applicable</td>
<td>No ITAR-regulated data may be entered, stored, or processed by AWS Certificate Manager. For example, domain names specified for certificates are not permitted to contain ITAR-regulated data. For example, do not enter ITAR-regulated data into the DomainName or SubjectAlternativeNames fields when requesting a certificate.</td>
</tr>
</tbody>
</table>

AWS CloudHSM Classic

For more information about AWS CloudHSM Classic, see the AWS CloudHSM Classic User Guide.

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR
compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• AWS CloudHSM Classic secret access keys are protected as ITAR-regulated data.</td>
<td>• AWS CloudHSM Classic metadata is not permitted to contain ITAR-regulated data. This includes all configuration data that you enter when creating and maintaining your AWS CloudHSM Classic config and partitions. Audit and syslogs should not contain ITAR-regulated data.</td>
</tr>
</tbody>
</table>

**AWS CloudTrail**

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

- For all AWS GovCloud (US) accounts created after 12/15/2014, AWS CloudTrail event log delivery to Amazon S3 is enabled automatically. However, you must set up Amazon SNS notifications. You can turn off logging through the AWS CloudTrail console for the AWS GovCloud (US) Region.
- Since AWS GovCloud (US) operates as a single isolated region, the capability to receive CloudTrail log files from multiple regions does not apply.
- If you are using AWS Direct Connect, you must enable CloudTrail in your AWS account (not your AWS GovCloud (US) account) and enable logging.
- The Amazon S3 and Amazon SNS policy statements must refer to the ARN for the AWS GovCloud (US) Region. For more information, see Amazon Resource Names (ARNs) in AWS GovCloud (US) (p. 26).
- To enable CloudTrail to write log files to your bucket in the AWS GovCloud (US) Region, you can use the following policy.

**Warning**

If the bucket already has one or more policies attached, add the statements for CloudTrail access to that policy or policies. We recommend that you evaluate the resulting set of permissions to be sure they are appropriate for the users who will be accessing the bucket.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20131101",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws-us-gov:s3:::myBucketName"
        },
        {
            "Sid": "AWSCloudTrailWrite20131101",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws-us-gov:s3:::myBucketName/[optional] prefix/AWSLogs/myAccountID/**",
```
"Condition": {
    "StringEquals": {
        "s3:x-amz-acl": "bucket-owner-full-control"
    }
}

For more information, see Amazon S3 Bucket Policy and Permissions for SNS Notifications.

**Note**

In the AWS GovCloud (US) Region, do not add CloudTrail account IDs of non-isolated regions to your policy templates, or an "Invalid principal in policy" error will occur. Similarly, if you are in a non-isolated region, do not add the CloudTrail account ID for AWS GovCloud (US) to your policy templates.

For more information about CloudTrail, see the CloudTrail documentation.

## Services Supported within CloudTrail

The following services are supported within CloudTrail in the AWS GovCloud (US) Region:

<table>
<thead>
<tr>
<th>AWS Service</th>
<th>Support Start Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Elasticsearch Service</td>
<td>02/15/2018</td>
</tr>
<tr>
<td>Amazon API Gateway</td>
<td>08/01/2017</td>
</tr>
<tr>
<td>Amazon EC2 Auto Scaling</td>
<td>12/16/2014</td>
</tr>
<tr>
<td>AWS CloudFormation</td>
<td>12/16/2014</td>
</tr>
<tr>
<td>AWS CloudHSM Classic</td>
<td>08/05/2015</td>
</tr>
<tr>
<td>AWS CloudTrail</td>
<td>12/16/2014</td>
</tr>
<tr>
<td>Amazon CloudWatch</td>
<td>12/16/2014</td>
</tr>
<tr>
<td>Amazon CloudWatch Events</td>
<td>04/07/2017</td>
</tr>
<tr>
<td>Amazon CloudWatch Logs</td>
<td>11/19/2015</td>
</tr>
<tr>
<td>AWS CodeDeploy</td>
<td>03/31/2017</td>
</tr>
<tr>
<td>AWS Database Migration Service (AWS DMS)</td>
<td>10/28/2015</td>
</tr>
<tr>
<td>AWS Direct Connect</td>
<td>10/28/2015</td>
</tr>
<tr>
<td>Amazon DynamoDB</td>
<td>05/28/2015</td>
</tr>
<tr>
<td>AWS Elastic Beanstalk</td>
<td>12/16/2014</td>
</tr>
<tr>
<td>Amazon Elastic Block Store (Amazon EBS)</td>
<td>12/16/2014</td>
</tr>
<tr>
<td>Amazon Elastic Compute Cloud (Amazon EC2)</td>
<td>12/16/2014</td>
</tr>
<tr>
<td>Elastic Load Balancing</td>
<td>12/16/2014</td>
</tr>
<tr>
<td>ElastiCache</td>
<td>01/29/2015</td>
</tr>
<tr>
<td>AWS Service</td>
<td>Support Start Date</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Amazon EMR (Amazon EMR)</td>
<td>12/16/2014</td>
</tr>
<tr>
<td>Amazon Glacier</td>
<td>12/30/2014</td>
</tr>
<tr>
<td>AWS Identity and Access Management (IAM)</td>
<td>12/16/2014</td>
</tr>
<tr>
<td>AWS Key Management Service (AWS KMS)</td>
<td>04/29/2015</td>
</tr>
<tr>
<td>Amazon Kinesis</td>
<td>12/21/2016</td>
</tr>
<tr>
<td>AWS Lambda</td>
<td>05/18/2017</td>
</tr>
<tr>
<td>Amazon Redshift</td>
<td>12/16/2014</td>
</tr>
<tr>
<td>Amazon RDS</td>
<td>01/22/2015</td>
</tr>
<tr>
<td>AWS Security Token Service (AWS STS)</td>
<td>12/16/2014</td>
</tr>
<tr>
<td>AWS Server Migration Service (AWS SMS)</td>
<td>06/21/2017</td>
</tr>
<tr>
<td>Amazon Simple Storage Service (Amazon S3)</td>
<td>10/01/2015</td>
</tr>
<tr>
<td>Amazon Simple Notification Service (Amazon SNS)</td>
<td>12/16/2014</td>
</tr>
<tr>
<td>Amazon Simple Queue Service (Amazon SQS)</td>
<td>12/16/2014</td>
</tr>
<tr>
<td>Amazon Simple Workflow Service (Amazon SWF)</td>
<td>12/16/2014</td>
</tr>
<tr>
<td>AWS Systems Manager (SSM)</td>
<td>05/23/2017</td>
</tr>
<tr>
<td>Amazon Virtual Private Cloud (Amazon VPC)</td>
<td>12/16/2014</td>
</tr>
</tbody>
</table>

**ITAR Boundary**

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Not applicable</td>
<td>• CloudTrail logs do not contain ITAR-regulated data.</td>
</tr>
<tr>
<td></td>
<td>• CloudTrail configuration data may not contain ITAR-regulated data.</td>
</tr>
</tbody>
</table>

**Amazon CloudWatch**

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

- Use SSL (HTTPS) when you make calls to the service in the AWS GovCloud (US) Region. In other regions, you can use HTTP or HTTPS.
For more information about CloudWatch, see the CloudWatch documentation.

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not applicable</td>
<td>No ITAR-regulated data may be entered, stored, or processed by CloudWatch. For example, CloudWatch metadata is not permitted to contain ITAR-regulated data. This metadata includes all the configuration data that you enter when creating and maintaining your CloudWatch alarms. For example, do not enter ITAR-regulated data in the following fields: Monitor configuration names, Descriptions, Trigger names, Metric names.</td>
</tr>
</tbody>
</table>

Amazon CloudWatch Events

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

- Use SSL (HTTPS) when you make calls to the service in the AWS GovCloud (US) Region. In other regions, you can use HTTP or HTTPS.

For more information about CloudWatch Events, see the CloudWatch Events documentation.

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not applicable</td>
<td>No ITAR-regulated data may be entered, stored, or processed by CloudWatch Events. For example, CloudWatch Events metadata is not permitted to contain ITAR-regulated data. This metadata includes all the configuration data that you enter</td>
</tr>
</tbody>
</table>
Amazon CloudWatch Logs

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

- Use SSL (HTTPS) when you make calls to the service in the AWS GovCloud (US) Region. In other regions, you can use HTTP or HTTPS.

For more information about CloudWatch Logs, see the CloudWatch Logs documentation.

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not applicable</td>
<td>No ITAR-regulated data may be entered, stored, or processed by CloudWatch Logs. For example, CloudWatch Logs metadata is not permitted to contain ITAR-regulated data.</td>
</tr>
<tr>
<td></td>
<td>For example, do not enter ITAR-regulated data in the following fields:</td>
</tr>
<tr>
<td></td>
<td>- Monitor configuration names</td>
</tr>
<tr>
<td></td>
<td>- Descriptions</td>
</tr>
<tr>
<td></td>
<td>- Trigger names</td>
</tr>
<tr>
<td></td>
<td>- Metric names</td>
</tr>
<tr>
<td></td>
<td>- Log group tags</td>
</tr>
</tbody>
</table>

AWS CodeDeploy

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:
• Use SSL (HTTPS) when you make calls to the service in the AWS GovCloud (US) Region. In other regions, you can use HTTP or HTTPS.

• Several procedures in the AWS CodeDeploy User Guide require the customer to substitute the name of a region-specific Amazon S3 bucket or bucket ARN. These procedures are for tasks such as restricting bucket access and downloading installation files, samples, and templates. In the AWS GovCloud (US) Region, the formats for accessing these resources do not follow the same patterns as for other regions. For information on the values to use for AWS GovCloud (US), see the following section.

AWS CodeDeploy Resources for AWS GovCloud (US)

Use the values presented here to complete AWS CodeDeploy procedures in the AWS GovCloud (US) Region.

AWS CodeDeploy Amazon S3 Resources Bucket

Name of the Amazon S3 bucket containing AWS CodeDeploy files:

aws-codedeploy-us-gov-west-1

AWS CodeDeploy Amazon S3 Bucket ARN

ARN of the Amazon S3 bucket containing AWS CodeDeploy files:

arn:aws:s3:::aws-codedeploy-us-gov-west-1

wget Download Command

wget command for downloading the AWS CodeDeploy agent on Linux and Ubuntu instances:

wget https://aws-codedeploy-us-gov-west-1.s3-us-gov-west-1.amazonaws.com/latest/install

Sample Application Locations

Location of sample AWS CodeDeploy applications:

• Amazon Linux, Red Hat Enterprise Linux, and Ubuntu Server instances:

  https://s3-us-gov-west-1.amazonaws.com/aws-codedeploy-us-gov-west-1/samples/latest/SampleApp_Linux.zip

• Windows Server instances:


AWS CloudFormation Template Location

Location of AWS CloudFormation template for launching Amazon EC2 instance configured for AWS CodeDeploy deployments:
Links for Downloading AWS CodeDeploy Installer and Updater (Windows Server)

Links for downloading AWS CodeDeploy installer and updater for Windows Server instances:

- Installer:


- Updater:


For more information about AWS CodeDeploy, see the AWS CodeDeploy documentation.

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>All deployments managed in AWS CodeDeploy support ITAR-regulated data.</td>
<td>The following AWS CodeDeploy metadata fields are not permitted to contain ITAR-regulated data:</td>
</tr>
<tr>
<td></td>
<td>• Application name</td>
</tr>
<tr>
<td></td>
<td>• Deployment group name</td>
</tr>
<tr>
<td></td>
<td>• Deployment description</td>
</tr>
<tr>
<td></td>
<td>• Deployment configuration name</td>
</tr>
<tr>
<td></td>
<td>• Trigger name</td>
</tr>
<tr>
<td></td>
<td>• Alarm name</td>
</tr>
</tbody>
</table>

AWS Config

AWS Config and AWS Config Rules are supported in the AWS GovCloud (US) Region. For more information about AWS Config, see the AWS Config documentation.

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR
compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• AWS Config data is outside of the ITAR boundary.</td>
<td></td>
</tr>
<tr>
<td>• AWS Config does not include any ITAR-regulated data.</td>
<td></td>
</tr>
<tr>
<td>• AWS Config metadata is not permitted to contain ITAR-regulated data. This includes the naming and configuration data that you enter when creating and managing your AWS Config settings. For example, do not enter ITAR-regulated data into user input fields such as the following:</td>
<td></td>
</tr>
<tr>
<td>• Annotations for rule evaluations</td>
<td></td>
</tr>
<tr>
<td>• Resource identifier</td>
<td></td>
</tr>
<tr>
<td>• S3 bucket name</td>
<td></td>
</tr>
<tr>
<td>• SNS topic name</td>
<td></td>
</tr>
<tr>
<td>• Tag key</td>
<td></td>
</tr>
</tbody>
</table>

**AWS Database Migration Service**

For more information about AWS Database Migration Service, see the [AWS Database Migration Service documentation](#).

**ITAR Boundary**

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>All data entered, stored, and processed in the source and destination database platforms in the AWS GovCloud (US) Region can contain ITAR-regulated data.</td>
<td></td>
</tr>
<tr>
<td>Not applicable.</td>
<td></td>
</tr>
</tbody>
</table>

**AWS Direct Connect**

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

- To set up an AWS Direct Connect connection to the AWS GovCloud (US) Region, you must use the [AWS GovCloud (US) console](#) and the AWS GovCloud (US) credentials associated with your AWS GovCloud (US) account. For instructions about how to provision and configure AWS Direct Connect, see the [AWS Direct Connect User Guide](#).
- Alternatively, you can set up an AWS Direct Connect connection in a different region and connect to the AWS GovCloud (US) using a public virtual interface and a VPN connection. For more information, see [Setting Up AWS Direct Connect with a VPN Connection](#).
• When you create a public virtual interface on your AWS Direct Connect connection, a data path to AWS GovCloud (US) is made available.

• To access your VPC without using an Amazon VPC VPN (for non-ITAR uses), create an AWS Direct Connect private virtual interface in the AWS GovCloud (US) Region (us-gov-west-1) only.

• Use the Amazon VPC section of the AWS GovCloud (US) console to set up hardware VPN access to the AWS GovCloud (US) Region over a public virtual interface.

• If you are processing ITAR-regulated workloads, you must configure your AWS Direct Connect connection with a VPN to encrypt data in transit. For detailed instructions about how to create your VPC and VPN, see Adding a Hardware Virtual Private Gateway to Your VPC in the Amazon VPC User Guide. For instructions about how to configure your on-premises VPN hardware, see the Amazon VPC Network Administrator Guide.

For more information about AWS Direct Connect, see the AWS Direct Connect documentation.

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• If you are transferring any type of ITAR-regulated data through the AWS Direct Connect connection, you must encrypt the data that is being transferred by using a VPN tunnel.</td>
<td>• AWS Direct Connect metadata is not permitted to contain ITAR-regulated data. This metadata includes all of the configuration data that you enter when creating and maintaining AWS Direct Connect, such as connection names.</td>
</tr>
<tr>
<td></td>
<td>• Do not enter ITAR-regulated data in the following console fields:</td>
</tr>
<tr>
<td></td>
<td>• Connection Name</td>
</tr>
<tr>
<td></td>
<td>• VIF Name</td>
</tr>
</tbody>
</table>

Setting Up AWS Direct Connect with a VPN Connection

You can create an AWS Direct Connect connection in a different region and use a VPN on top of the connection to encrypt all data in transit from your AWS GovCloud (US) virtual private cloud (VPC) to your own network.

Step 1: Create a AWS Direct Connect Connection and Virtual Interface

To provision a connection and public virtual interface, follow the steps in the Getting Started with AWS Direct Connect with AWS Direct Connect section of the AWS Direct Connect user guide and ensure that you do the following:

• Submit a connection request at a location in any other supported region.
• Create a public virtual interface (not a private virtual interface).
Step 2: Enable the Virtual Public Interface for AWS GovCloud (US) Access

In order to enable your virtual public interface for AWS GovCloud (US), create a customer support case via Support Center on the standard AWS Management Console. Note: You cannot use your AWS GovCloud (US) credentials to log in. You must use your standard AWS credentials. If you do not have access to the standard AWS Management Console and Support Center, please contact your AWS Business Representative to enable your virtual interface.

Step 3: Verify Your Virtual Public Interface

After you have established virtual public interfaces to the AWS GovCloud (US) Region, verify your virtual public interface connection to the AWS GovCloud (US) Region by running a traceroute from your on-premises router and verifying that the AWS Direct Connect identifier is in the network trace.

Step 4: Set Up Your VPN Over Your Public Virtual Interface

Create your AWS GovCloud (US) VPC and VPN. For detailed instructions on how to create your VPC and VPN, see Adding a Hardware Virtual Private Gateway to Your VPC in the Amazon Virtual Private Cloud User Guide. For instructions on how to configure your on-premises VPN hardware, see Amazon Virtual Private Cloud Network Administrator Guide.

Amazon DynamoDB

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

- **Import Table** is not available in the DynamoDB console.
- **Export Table** is not available in the DynamoDB console.

For more information about DynamoDB, see the DynamoDB documentation.

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• All data entered, stored and processed in DynamoDB database tables can contain ITAR-regulated data.</td>
<td>• DynamoDB metadata is not permitted to contain ITAR-regulated data. This metadata includes all the configuration data that you enter when creating and maintaining your DynamoDB tables, such as table names, hash attribute names, and range attribute names.</td>
</tr>
<tr>
<td>• Do not enter ITAR-regulated data in the following fields:</td>
<td>• Table names</td>
</tr>
<tr>
<td>• Table names</td>
<td>• Hash attribute names</td>
</tr>
<tr>
<td>• Hash attribute names</td>
<td></td>
</tr>
</tbody>
</table>

56
If you are processing ITAR-regulated data with this service, use the SSL (HTTPS) endpoint to maintain ITAR compliance. For a list of endpoints, see AWS GovCloud (US) Endpoints (p. 36).

AWS Elastic Beanstalk

For more information about AWS Elastic Beanstalk, see the AWS Elastic Beanstalk documentation.

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
</table>
| All code uploaded to AWS Elastic Beanstalk can contain ITAR-regulated data. | The following AWS Elastic Beanstalk metadata fields are not permitted to contain ITAR-regulated data:
  | • Application Name  
  | • Environment Name  
  | • Option Settings |

Amazon Elastic Block Store (Amazon EBS)

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

- The copy snapshot commands can be used, but only allow you to copy snapshots available to your account within the AWS GovCloud (US) Region. If you specify a source or destination region to copy to or from, the commands will return an error.
- Use SSL (HTTPS) when you make calls to the service in the AWS GovCloud (US) Region. In other regions, you can use HTTP or HTTPS.

For more information about Amazon EBS, see Amazon Elastic Block Store in the Amazon Elastic Compute Cloud User Guide.

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance.
compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• All data entered, stored, and processed in Amazon EBS volumes can contain ITAR-regulated data</td>
<td>• Amazon EBS metadata is not permitted to contain ITAR-regulated data. This metadata includes all configuration data that you enter when creating and maintaining your Amazon EBS volumes.</td>
</tr>
<tr>
<td></td>
<td>• Do not enter ITAR-regulated data in the following fields:</td>
</tr>
<tr>
<td></td>
<td>• Volume names</td>
</tr>
<tr>
<td></td>
<td>• Snapshot names</td>
</tr>
<tr>
<td></td>
<td>• Image names</td>
</tr>
<tr>
<td></td>
<td>• Image descriptions</td>
</tr>
</tbody>
</table>

Amazon Elastic Compute Cloud (Amazon EC2)

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

• Spot instances and select Amazon EC2 instance types are not available in the AWS GovCloud (US) Region.
• The public IP ranges for AWS GovCloud (US) Region Amazon EC2 instances are 52.222.0.0/17 and 96.127.0.0/17.
• Reserved Instance resale is not available in the AWS GovCloud (US) Region.
• AMI copy and snapshot copy do not support migrating AMIs and snapshots from another AWS region into the AWS GovCloud (US) region. For information about how to migrate your AMIs from another AWS region into the AWS GovCloud (US) Region, see Importing Virtual Machines into the AWS GovCloud (US) Region (p. 63).
• When using the Amazon EC2 AMI tools, the AWS GovCloud (US) Region uses a non-default public key certificate to encrypt AMI manifests. The `ec2-bundle-image`, `ec2-bundle-vol`, `ec2-migrate-bundle`, and `ec2-migrate-manifest` commands require the `--ec2cert $EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-gov.pem` option in the AWS GovCloud (US) Region.
• By default, enhanced networking is not enabled on Windows Server 2012 R2 AMIs. For more information, see Enabling Enhanced Networking on Windows Instances in a VPC.
• In the AWS GovCloud (US) Region, you must launch all Amazon EC2 instances in an Amazon Virtual Private Cloud (Amazon VPC). In some cases, your account might have a default VPC; otherwise, you must create a VPC before launching instances. For more information, see Determining if Your Account Has a Default Amazon VPC (p. 59).
• When you launch an instance in the AWS GovCloud (US) Region using the CLI `ec2-run-instances` command or API `RunInstances` action, you must specify the `subnet` parameter.
• Use SSL (HTTPS) when you make calls to the service in the AWS GovCloud (US) Region. In other regions, you can use HTTP or HTTPS.
• Use SSL (HTTPS) when generating key pairs using `ec2-create-keypair` and `CreateKeyPair` commands.
• To import your own set of key pairs, follow the directions in Importing Your Own Key Pair to Amazon EC2.
• When using VM Import:
  • If your account is set up as default VPC, then your default VPC will be the target for your import.
Determining if Your Account Has a Default Amazon VPC

In the AWS GovCloud (US) Region, you must launch all Amazon EC2 instances in an Amazon Virtual Private Cloud (Amazon VPC). In some cases, your account might have a default VPC, where you launch all your Amazon EC2 instances. If your account doesn't have a default VPC, you must create a VPC before you can launch Amazon EC2 instances. For more information, see What is Amazon VPC? in Amazon VPC User Guide.

1. Sign in to the AWS Management Console for the AWS GovCloud (US) Region.
2. Navigate to the dashboard of the Amazon EC2 console.
3. In the Account Attributes section, view the Supported Platforms.
   - If you see only EC2-VPC, as shown in the following figure, your account has a VPC by default.

```
Supported Platforms
   EC2-VPC

Default VPC
   vpc-1a2b3c4d
```

- If you see both EC2-Classical and EC2-VPC, as shown in the following figure, your account doesn't have a default VPC. You must create a VPC before you launch Amazon EC2 or Amazon RDS instances.

```
Supported Platforms
   EC2-Classic
   EC2-VPC
```

If you don't want a default VPC for your AWS GovCloud (US) account, you can delete the default VPC and default subnets. The default VPC and subnets will not be recreated. However, you still need to create a VPC before launching instances.
If you deleted your default VPC, you can create a new one. For more information, see Creating a Default VPC.

If your account doesn’t have a default VPC but you want a default VPC, you can submit a request by completing the AWS GovCloud (US) Contact Us form. In the form, include your AWS GovCloud (US) account ID and indicate that you want to enable your account for a default VPC.

**ITAR Boundary**

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• All data entered, stored, and processed within an Amazon EC2 instance and ephemeral drives can contain ITAR-regulated data.</td>
<td>• Amazon EC2 metadata is not permitted to contain ITAR-regulated data. This metadata includes all configuration data that you enter when creating and maintaining your instances.</td>
</tr>
<tr>
<td>• Key Pairs created using HTTPS.</td>
<td>• Do not enter ITAR-regulated data in the following fields:</td>
</tr>
<tr>
<td>• Imported Key Pairs.</td>
<td>• Instance names</td>
</tr>
<tr>
<td></td>
<td>• AMI descriptions</td>
</tr>
<tr>
<td></td>
<td>• Resource tags</td>
</tr>
<tr>
<td></td>
<td>• Key pairs created using HTTP.</td>
</tr>
<tr>
<td></td>
<td>• When using VM Import, you may not enter any ITAR-regulated data as part of CLI arguments, paths, or OS disk images. Any data that is ITAR-regulated should be encrypted and placed in partitions other than root and boot.</td>
</tr>
<tr>
<td></td>
<td>• If importing ITAR-regulated images, do not use pre-signed URLs for the CLI argument -- manifest-url.</td>
</tr>
</tbody>
</table>

**Amazon Elastic Container Registry**

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

- At this time, the service endpoint does not support FIPS 140-2.

For more information about Amazon Elastic Container Registry, see the Amazon Elastic Container Registry documentation.

**ITAR Boundary**

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:
Amazon Elastic Container Service

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

- At this time, the service endpoint does not support FIPS 140-2.

For more information about Amazon Elastic Container Service, see the Amazon Elastic Container Service documentation.

**ITAR Boundary**

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• All data entered, stored, and processed within an Amazon EC2 instance and ephemeral drives can contain ITAR-regulated data.</td>
<td>Do not enter ITAR-regulated data in the following fields:</td>
</tr>
<tr>
<td></td>
<td>• Cluster name</td>
</tr>
<tr>
<td></td>
<td>• Service name</td>
</tr>
<tr>
<td></td>
<td>• Attribute name</td>
</tr>
<tr>
<td></td>
<td>• Attribute value</td>
</tr>
<tr>
<td></td>
<td>• Task definitions</td>
</tr>
<tr>
<td></td>
<td>• Task group</td>
</tr>
<tr>
<td></td>
<td>• Task overrides</td>
</tr>
<tr>
<td></td>
<td>• Task started by</td>
</tr>
<tr>
<td></td>
<td>• Placement constraints</td>
</tr>
</tbody>
</table>

Amazon Elasticsearch Service

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

- The Amazon Elasticsearch Service endpoint does not yet support FIPS 140-2.
ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• All documents entered, stored, and processed in an Elasticsearch cluster can contain ITAR-regulated data.</td>
<td>• Amazon Elasticsearch Service metadata is not permitted to contain ITAR-regulated data. This metadata includes all configuration data that you specify when creating and maintaining your Elasticsearch clusters and indices, such as index names, alias names, tags, snapshot names, and repository names.</td>
</tr>
<tr>
<td></td>
<td>• Do not enter ITAR-regulated data in the following fields:</td>
</tr>
<tr>
<td></td>
<td>• Domain name</td>
</tr>
<tr>
<td></td>
<td>• Index names</td>
</tr>
<tr>
<td></td>
<td>• Type names</td>
</tr>
<tr>
<td></td>
<td>• Document IDs</td>
</tr>
<tr>
<td></td>
<td>• Snapshot names</td>
</tr>
<tr>
<td></td>
<td>• Resource tags</td>
</tr>
<tr>
<td></td>
<td>• Repository names</td>
</tr>
<tr>
<td></td>
<td>• Alias names</td>
</tr>
<tr>
<td></td>
<td>• CloudWatch log group names</td>
</tr>
</tbody>
</table>

AWS Server Migration Service (AWS SMS)

To use the Server Migration Connector with the AWS GovCloud (US) Region, follow these steps on your Server Migration Connector VM. The following procedure permanently converts your connector virtual appliance to an AWS GovCloud (US) connector.

1. Install the Server Migration Connector as described in Getting Started with AWS Server Migration Service.
2. Open the connector's virtual machine console and log in as ec2-user with the password ec2pass. Supply a new password if prompted.
3. Run the following command:

```
sudo enable-govcloud
```
4. In a web browser, access the connector VM at its IP address (https://ip-address-of-connector/). In the setup wizard, under AWS Region, AWS GovCloud (US) Region should now be the only region listed.

For more information about AWS SMS, see the AWS SMS User Guide.
ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• All data entered, stored, and processed on an encrypted, non-root, non-boot partition in a virtual machine can contain ITAR-regulated data.</td>
<td>• Virtual machine metadata is not permitted to contain ITAR-regulated data. For example, text displayed outside of a virtual machine console in vSphere Client, SCVMM, or Hyper-V Manager is not permitted to contain ITAR-regulated data.</td>
</tr>
<tr>
<td>• Do not enter ITAR-regulated data in the following fields:</td>
<td>• Do not enter ITAR-regulated data in the following fields:</td>
</tr>
<tr>
<td>• VM names or paths</td>
<td>• VM names or paths</td>
</tr>
<tr>
<td>• Virtual machine disk file paths</td>
<td>• Virtual machine disk file paths</td>
</tr>
<tr>
<td>• IP addresses or host names of VMs, ESXi hosts, vCenter, Hyper-V hosts, or SCVMM</td>
<td>• IP addresses or host names of VMs, ESXi hosts, vCenter, Hyper-V hosts, or SCVMM</td>
</tr>
<tr>
<td>• User name of any service account or Active Directory user created for Service Migration Connector to log into vCenter, SCVMM, or Hyper-V</td>
<td>• User name of any service account or Active Directory user created for Service Migration Connector to log into vCenter, SCVMM, or Hyper-V</td>
</tr>
<tr>
<td>• Do not enter ITAR-regulated data into the root or boot partition of any virtual machine being imported using the AWS Server Migration Service</td>
<td>• Do not enter ITAR-regulated data into the root or boot partition of any virtual machine being imported using the AWS Server Migration Service</td>
</tr>
</tbody>
</table>

Importing Virtual Machines into the AWS GovCloud (US) Region

With Amazon EC2 VM Import/Export, you can import virtual machine images from your environment to Amazon EC2 instances or as images. This capability is available at no charge beyond standard usage charges for Amazon EC2 and Amazon S3. AWS GovCloud (US) supports all image types (RAW, VHD, VMDK, and OVA) and operating systems listed in the Amazon EC2 VM Import documentation.

**Note**
The AWS Management Portal for vCenter, which enables you to manage your AWS resources using VMware vCenter, is not compatible with the AWS GovCloud (US) Region.

**Note**
AWS Server Migration Service is a significant enhancement of Amazon EC2 VM Import/Export. The AWS SMS provides automated, live incremental server replication and AWS Console support. For customers using VM Import/Export for migration, we recommend using AWS Server Migration Service.

ITAR Best Practices

You should never enter ITAR-regulated data in CLI arguments or paths. As a best practice, ITAR-regulated data should be encrypted and placed in partitions other than root and boot. If you have questions, contact us.
Amazon EC2 Systems Manager

For more information about Amazon EC2 Systems Manager, see the Amazon EC2 Systems Manager documentation.

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>All EC2 Systems Manager Document content and Parameter Store values can contain ITAR-regulated data.</td>
<td>The following EC2 Systems Manager metadata fields are not permitted to contain ITAR-regulated data:</td>
</tr>
<tr>
<td></td>
<td>• Document names</td>
</tr>
<tr>
<td></td>
<td>• Parameter Store parameter names</td>
</tr>
<tr>
<td></td>
<td>• Patch group names (that is, the value of the Patch Group tag)</td>
</tr>
</tbody>
</table>

Elastic Load Balancing

Elastic Load Balancing supports three types of load balancers: Application Load Balancer, Network Load Balancer, and Classic Load Balancer. All three types of load balancers are supported in AWS GovCloud (US).

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

- Your load balancer must run in a virtual private cloud (VPC).
- Because Elastic Load Balancing must run in a VPC, Classic Load Balancer does not provide IPv6 capability that is offered in standard AWS regions when running outside of a VPC. Application Load Balancer supports IPv6 in VPCs in all regions including AWS GovCloud (US).
- ITAR data must be encrypted in transit outside of the ITAR boundary. Because Elastic Load Balancing uses global DNS servers, ITAR traffic across Elastic Load Balancing must be encrypted.
- You can use SSL certificates on your Classic and Application load balancers only. Network Load Balancers don't support SSL/TLS termination yet. For more information, see Replace the SSL Certificate for Your Load Balancer. The Elastic Load Balancing SSL termination is not FIPS 140-2 compliant.
- You can also use Network Load Balancer to pass TCP traffic and terminate SSL on your web server.
- Elastic Load Balancing uses the following account ID. For information about when it is used, see Attach a Policy to Your Amazon S3 Bucket.

<table>
<thead>
<tr>
<th>Region</th>
<th>Elastic Load Balancing Account ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>us-gov-west-1</td>
<td>048591011584</td>
</tr>
</tbody>
</table>

64
For more information about Elastic Load Balancing, see the Elastic Load Balancing documentation.

**ITAR Boundary**

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• All data transmitted through Elastic Load Balancing must be encrypted if it contains ITAR-regulated data. Encryption must be used both between clients and the load balancer and between the load balancer and registered instances. It is strongly recommended that Backend Authentication is enabled to enforce public key authentication of the registered instance.</td>
<td>• All customer parameters provided as input to Elastic Load Balancing (via console, APIs, or other mechanism) are not permitted to contain ITAR-regulated data. Examples include the names of load balancers and the names of load balancer policies. • Do not enter ITAR-regulated data in the following fields: • Resource tags</td>
</tr>
</tbody>
</table>

If you are processing ITAR-regulated data with this service, use the SSL (HTTPS) endpoint to maintain ITAR compliance. For a list of endpoints, see AWS GovCloud (US) Endpoints (p. 36).

**Amazon ElastiCache**

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

• All ElastiCache instances must be launched in an Amazon VPC.
• ElastiCache clusters have a preferred weekly maintenance window. For information about the time blocks, see Cache Engine Version Management.

For more information about ElastiCache, see the ElastiCache documentation.

**ITAR Boundary**

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• You may store and process ITAR-regulated data in ElastiCache cache clusters only if the data is encrypted on the client side.</td>
<td>• Unencrypted data stored in a cache cluster may not contain ITAR-regulated data. • ElastiCache metadata is not permitted to contain ITAR-regulated data. This metadata includes all the configuration data that you</td>
</tr>
</tbody>
</table>
If you are processing ITAR-regulated data with ElastiCache, follow these guidelines in order to maintain ITAR compliance:

- To secure ITAR-regulated data in your VPC, set up access control lists (ACLs) to control traffic entering and exiting your VPC. If you have multiple databases configured with different ports, set up ACLs on all the ports.
  - For example, if you’re running an application server on an Amazon EC2 instance that connects to an ElastiCache cluster, a non-U.S. person could reconfigure the DNS to redirect ITAR-regulated data out of the VPC and into any server that could possibly be outside of the AWS GovCloud (US) Region.
  - To prevent this type of attack and to maintain ITAR compliance, use network ACLs to prevent network traffic from exiting the VPC on the database port. For more information, see Network ACLs in the Amazon VPC User Guide.
- For each cluster that contains ITAR-regulated data, ensure that only specific CIDR ranges and Amazon EC2 security groups can access the database instance, especially when an Internet gateway is attached to the VPC. Only allow connections that are from the AWS GovCloud (US) Region or other ITAR-controlled environments to ITAR-controlled clusters.

ElastiCache requires the use of the SSL (HTTPS) endpoint for service API calls. For a list of endpoints, see AWS GovCloud (US) Endpoints (p. 36).

Amazon EMR (Amazon EMR)

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

- MapR distributions are currently not supported in the AWS GovCloud (US) Region.
- In the AWS GovCloud (US) Region, you launch all Amazon EMR job flows in Amazon Virtual Private Cloud (Amazon VPC). For information about configuring an Amazon VPC that can run a job flow, see Select an Amazon VPC and Subnet for the Cluster.
- Launching a job flow by using Spot instances is not currently supported in the AWS GovCloud (US) Region.
- Launching a job flow with debugging is not currently supported in the AWS GovCloud (US) Region.
For more information about Amazon EMR, see the Amazon EMR documentation.

**ITAR Boundary**

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• All input and output data that is entered, stored, and processed in Amazon EMR can contain ITAR-regulated data.</td>
<td>• Amazon EMR metadata is not permitted to contain ITAR-regulated data. This metadata includes all configuration data that you enter when creating and maintaining your job flows.</td>
</tr>
<tr>
<td></td>
<td>• Do not enter ITAR-regulated data in Amazon EMR when doing the following:</td>
</tr>
<tr>
<td></td>
<td>• Naming a job flow</td>
</tr>
<tr>
<td></td>
<td>• Specifying a file location</td>
</tr>
<tr>
<td></td>
<td>• Naming a bootstrap action</td>
</tr>
<tr>
<td></td>
<td>• Providing arguments</td>
</tr>
<tr>
<td></td>
<td>• Resource tags</td>
</tr>
<tr>
<td></td>
<td>• ITAR-regulated data should not be printed to your logs. (Amazon EMR metadata and logs are not permitted to contain ITAR-regulated data.)</td>
</tr>
</tbody>
</table>

If you are processing ITAR-regulated data with this service, use the SSL (HTTPS) endpoint to maintain ITAR compliance. For a list of endpoints, see AWS GovCloud (US) Endpoints (p. 36).

**Amazon Glacier**

For more information about Amazon Glacier, see the Amazon Glacier documentation.

**ITAR Boundary**

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• All data entered and stored in Amazon Glacier archives can contain ITAR-regulated data.</td>
<td>• Amazon Glacier metadata is not permitted to contain ITAR-regulated data. This metadata includes all configuration data that you enter when creating and maintaining your Amazon Glacier vaults names.</td>
</tr>
<tr>
<td></td>
<td>• Do not enter ITAR-regulated data in the following fields:</td>
</tr>
</tbody>
</table>


AWS Identity and Access Management (IAM)

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

- IAM users that you create in the AWS GovCloud (US) Region are specific to the AWS GovCloud (US) Region and do not exist in other AWS regions.
- Due to the separate authentication stack, the hardware MFA tokens used with standard AWS regions are not compatible with AWS GovCloud (US) accounts. AWS GovCloud (US) only supports MFA devices listed under the “Compatibility with AWS GovCloud (US)” row on the Multi-Factor Authentication page.
- You can’t create a role to delegate access between an AWS GovCloud (US) account and an AWS account.
- IAM roles can be used to protect ITAR data, but you cannot enter ITAR-regulated data into the roles and role names, and you cannot assign a non-US person to a role that can access ITAR data.
- If you create policies, use the correct AWS GovCloud (US) ARN prefix. For more information, see Amazon Resource Names (ARNs) in AWS GovCloud (US) (p. 26).
- Use SSL (HTTPS) when you make calls to the service in the AWS GovCloud (US) Region.
- When you use a SAML provider in the AWS GovCloud (US) Region, use the following URL for the XML document that contains relying party information and certificates: https://signin.amazonaws-us-gov.com/static/saml-metadata.xml. For more information, see Configuring a Relying Party and Adding Claims in IAM User Guide.
- SSH public keys are used only in conjunction with AWS CodeCommit, which is currently not available in the AWS GovCloud (US) Region.
- The AWS GovCloud (US) Region does not report the last time, last service, or last region in which an access key was used. The IAM console does not display the Last Used column and you can’t use the aws iam get-access-key-last-used command.
- The credential report will not include data for when an access key was last used and which service was most recently accessed with an access key.
- You can attach or replace an IAM role on your existing Amazon EC2 instances in the AWS GovCloud (US) Region. To enable IAM roles for your existing EC2 instances, follow the example described in this AWS Security Blog post.

For more information about IAM, see the IAM documentation.

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• IAM passwords are protected as ITAR-regulated data.</td>
<td>• IAM metadata is not permitted to contain ITAR-regulated data. This metadata includes all</td>
</tr>
</tbody>
</table>
AWS Snowball

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

- Users can only select AWS GovCloud (US) as the import or export destination region. The AWS GovCloud (US) Region selection is available only when signed in to AWS GovCloud (US).
- When you create jobs in the AWS GovCloud (US) Region, you can use the following device types:
  - 50 TB Snowball (with 42 TB of usable space)
  - 80 TB Snowball (with 72 TB of usable space)
  - 100 TB Snowball Edge (with 82 TB of usable space)
- Compute functionality (AWS Lambda powered by AWS Greengrass) for the AWS Snowball Edge is not supported.

For more information about Snowball, see the [AWS Snowball documentation](#).

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>- All data downloaded to the Snowball appliance can contain ITAR-regulated data.</td>
<td>- Snowball metadata is not permitted to contain ITAR-regulated data. This includes the naming and configuration data that you enter when creating and managing your Snowball import or export job. For example, do not enter ITAR-regulated data into user input fields describing your job, such as import job name, Amazon S3 bucket name, or Amazon SNS topic name. Snowball generated metadata will not contain ITAR-regulated data.</td>
</tr>
</tbody>
</table>
AWS Key Management Service (AWS KMS)

For more information about AWS KMS, see the AWS Key Management Service Developer Guide.

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• All data encrypted with an AWS KMS key contains ITAR-regulated data</td>
<td>• AWS KMS metadata is not permitted to contain ITAR-regulated data. Do not enter ITAR-regulated data in the following fields:</td>
</tr>
<tr>
<td></td>
<td>• Alias</td>
</tr>
<tr>
<td></td>
<td>• Descriptions</td>
</tr>
<tr>
<td></td>
<td>• Key policy documents, including key administrators and key users</td>
</tr>
<tr>
<td></td>
<td>• The Encryption Context is outside the ITAR boundary.</td>
</tr>
<tr>
<td></td>
<td>• AWS KMS generated metadata will not contain ITAR-regulated data:</td>
</tr>
<tr>
<td></td>
<td>• Key ID</td>
</tr>
<tr>
<td></td>
<td>• Key ARN</td>
</tr>
</tbody>
</table>

Amazon Kinesis Data Streams

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

• You can use Amazon Kinesis Data Streams, but Amazon Kinesis Data Firehose and Amazon Kinesis Data Analytics aren’t available in the AWS GovCloud (US) Region.

For more information about Amazon Kinesis Data Streams, see the Amazon Kinesis documentation.

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• All data entered, stored and processed in Amazon Kinesis Data Streams can contain ITAR-regulated data.</td>
<td>• Do not enter ITAR-regulated data in the following fields:</td>
</tr>
<tr>
<td></td>
<td>• Stream names</td>
</tr>
</tbody>
</table>
If you are processing ITAR-regulated data with this service, use the SSL (HTTPS) endpoint to maintain ITAR compliance. For a list of endpoints, see AWS GovCloud (US) Endpoints (p. 36).

AWS Lambda

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

- At this time, the service endpoint does not support FIPS 140-2.

For more information about AWS Lambda, see the AWS Lambda documentation.

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Customer’s code</td>
<td>Do not enter ITAR-regulated data in the following console fields:</td>
</tr>
<tr>
<td>• Environment variable</td>
<td>• Function name</td>
</tr>
<tr>
<td>• Role</td>
<td>• Description</td>
</tr>
<tr>
<td>• VPC</td>
<td>• DLQ data (can be exported through Amazon SNS and Amazon SQS)</td>
</tr>
<tr>
<td>• KMS key</td>
<td>• Memory</td>
</tr>
<tr>
<td></td>
<td>• Timeout</td>
</tr>
<tr>
<td></td>
<td>• Runtime</td>
</tr>
<tr>
<td></td>
<td>• Role name for service principals</td>
</tr>
<tr>
<td></td>
<td>• Aliases</td>
</tr>
</tbody>
</table>

AWS Marketplace

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

- Full catalog of solutions is currently not available for use in region but we are actively working with AWS Marketplace Sellers to offer their solutions in region.

- Cloud Formation and multi-AMI solutions are available in region.

- SaaS Subscription and SaaS Contract are not currently available in region.

- Product Support Connection is not currently available in region.
• One-click launch of AMIs from the AWS Marketplace website is not supported.

• Integration with Service Catalog is currently not available.

For more information about AWS Marketplace, see the AWS Marketplace documentation. For the Sellers Guide for the AWS Marketplace, see the AWS Marketplace Seller Guide documentation

### ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• AWS does not attest to compliance of Independent Software Vendor (ISV) solutions implemented on AWS services regarding any state, federal, regulatory or industry-specific security controls, baselines, laws, standards or regimes - including ITAR. Pursuant to AWS GovCloud (US) Terms and Conditions, it is the customer's responsibility to use the software appropriately and in accordance with applicable requirements, including ITAR.</td>
<td>None</td>
</tr>
<tr>
<td>• ISVs may communicate whether their solution meets compliance requirements when they market their offering. Customers are responsible for verifying that their software meets applicable requirements.</td>
<td></td>
</tr>
<tr>
<td>• All AWS Marketplace software in AWS GovCloud (US) is operated on the same infrastructure as other AWS GovCloud (US) resources. This results in the software being deployed to Amazon EC2 and other AWS services managed by US Citizens to help customers maintain compliance with applicable requirements, including ITAR.</td>
<td></td>
</tr>
</tbody>
</table>

### Amazon Polly

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

• At this time, the service endpoint does not support FIPS 140-2.

For more information about Amazon Polly, see the Amazon Polly documentation.

### ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR
compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input Text</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Lexicons</td>
<td></td>
</tr>
</tbody>
</table>

### Amazon Redshift

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

- In the AWS GovCloud (US) Region, all Amazon Redshift clusters must be launched in an Amazon VPC.
- Snapshot copy is not available in the AWS GovCloud (US) Region.
- To connect to Amazon Redshift with SSL, you must download the Amazon Redshift certificate bundle from https://s3-us-gov-west-1.amazonaws.com/redshift-downloads/redshift-ca-bundle-ugw1.crt. For more information, see Configure Security Options for Connections.
- If you want Amazon Redshift to write logs to an Amazon S3 bucket, the bucket must have a policy that uses `665727464434` for the Amazon Redshift Account ID. For more information, see Managing Log Files in the Amazon Redshift Cluster Management Guide.

The following shows an example of a bucket policy that enables audit logging for the AWS GovCloud (US) Region, where `BucketName` is a placeholder for your bucket name:

```json
{
    "Statement": [
        {
            "Sid": "Put bucket policy needed for audit logging",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws-us-gov:iam::665727464434:user/logs"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws-us-gov:s3:::BucketName/*"
        },
        {
            "Sid": "Get bucket policy needed for audit logging",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws-us-gov:iam::665727464434:user/logs"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws-us-gov:s3:::BucketName"
        }
    ]
}
```

For more information about Amazon Redshift, see the Amazon Redshift documentation.

### ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR
compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Amazon Redshift master passwords are protected as ITAR-regulated data.</td>
<td>• Amazon Redshift metadata is not permitted to contain ITAR-regulated data. This metadata includes all configuration data that you enter when creating and maintaining your Amazon Redshift clusters except the master password.</td>
</tr>
<tr>
<td>• All data stored and processed in Amazon Redshift clusters can contain ITAR-regulated data. You cannot transfer ITAR-regulated data in and out of Amazon Redshift using the API or CLI. You must use database tools for data transfer of ITAR-regulated data.</td>
<td>• Do not enter ITAR-regulated data in the following fields:</td>
</tr>
<tr>
<td>• Database instance identified</td>
<td>• Database instance identified</td>
</tr>
<tr>
<td>• Master user name</td>
<td>• Master user name</td>
</tr>
<tr>
<td>• Database name</td>
<td>• Database name</td>
</tr>
<tr>
<td>• Database snapshot name</td>
<td>• Database snapshot name</td>
</tr>
<tr>
<td>• Database security group name</td>
<td>• Database security group name</td>
</tr>
<tr>
<td>• Database security group description</td>
<td>• Database security group description</td>
</tr>
<tr>
<td>• Database parameter group name</td>
<td>• Database parameter group name</td>
</tr>
<tr>
<td>• Database parameter group description</td>
<td>• Database parameter group description</td>
</tr>
<tr>
<td>• Option group name</td>
<td>• Option group name</td>
</tr>
<tr>
<td>• Option group description</td>
<td>• Option group description</td>
</tr>
<tr>
<td>• Database subnet group name</td>
<td>• Database subnet group name</td>
</tr>
<tr>
<td>• Database subnet group description</td>
<td>• Database subnet group description</td>
</tr>
<tr>
<td>• Event subscription name</td>
<td>• Event subscription name</td>
</tr>
<tr>
<td>• Resource tags</td>
<td>• Resource tags</td>
</tr>
</tbody>
</table>

If you are processing ITAR-regulated data with Amazon Redshift, follow these guidelines in order to maintain ITAR compliance:

• When you use the console or the AWS APIs, the only data field that is protected as ITAR-regulated data is the Amazon Redshift Master Password.
• After you create your database, change the master password of your Amazon Redshift cluster by directly using the database client.
• You can enter ITAR-regulated data into any data fields by using your database client-side tools. Do not pass ITAR-regulated data by using the web service APIs that are provided by Amazon Redshift.
• To secure ITAR-regulated data in your VPC, set up access control lists (ACLs) to control traffic entering and exiting your VPC. If you have multiple databases configured with different ports, set up ACLs on all the ports.
• For example, if you’re running an application server on an Amazon EC2 instance that connects to an Amazon Redshift cluster, a non-U.S. person could reconfigure the DNS to redirect ITAR-regulated data out of the VPC and into any server that could possibly be outside of the AWS GovCloud (US) Region.

To prevent this type of attack and to maintain ITAR compliance, use network ACLs to prevent network traffic from exiting the VPC on the database port. For more information, see Network ACLs in the Amazon VPC User Guide.

• For each cluster that contains ITAR-regulated data, ensure that only specific CIDR ranges and Amazon EC2 security groups can access the cluster, especially when an Internet gateway is attached to the VPC. Only allow connections that are from the AWS GovCloud (US) Region or other ITAR-controlled environments to ITAR-controlled clusters.
If you are processing ITAR-regulated data with this service, use the SSL (HTTPS) endpoint to maintain ITAR compliance. For a list of endpoints, see AWS GovCloud (US) Endpoints (p. 36).

Amazon Rekognition

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

- Celebrity Recognition is not available in AWS GovCloud (US).
- Amazon Rekognition does not support FIPS 140-2.

For more information about Amazon Rekognition, see the Amazon Rekognition documentation.

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection identifiers</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Image bytes</td>
<td></td>
</tr>
<tr>
<td>External Image Identifiers</td>
<td></td>
</tr>
<tr>
<td>Face identifiers</td>
<td></td>
</tr>
</tbody>
</table>

Amazon Relational Database Service (Amazon RDS)

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon RDS master passwords are protected as ITAR-regulated data.</td>
<td>Amazon RDS metadata is not permitted to contain ITAR-regulated data. This metadata includes all configuration data that you enter when creating and maintaining your Amazon RDS instances except the master password.</td>
</tr>
</tbody>
</table>
| All data stored and processed in Amazon RDS database tables can contain ITAR-regulated data. You cannot transfer ITAR-regulated data in and out of your Amazon RDS instance using the API or CLI. You must use database tools for data transfer of ITAR-regulated data. | Do not enter ITAR-regulated data in the following fields:
If you are processing ITAR-regulated data with Amazon RDS, follow these guidelines in order to maintain ITAR compliance:

- When you use the console or the AWS APIs, the only data field that is protected as ITAR-regulated data is the Amazon RDS Master Password.
- After you create your database, change the master password of your Amazon RDS instance by directly using the database client.
- You can enter ITAR-regulated data into any data fields by using your database client-side tools. Do not pass ITAR-regulated data by using the web service APIs that are provided by Amazon RDS.
- To secure ITAR-regulated data in your VPC, set up access control lists (ACLs) to control traffic entering and exiting your VPC. If you have multiple databases configured with different ports, set up ACLs on all the ports.
  - For example, if you're running an application server on an Amazon EC2 instance that connects to an Amazon RDS database instance, a non-U.S. person could reconfigure the DNS to redirect ITAR-regulated data out of the VPC and into any server that might be outside of the AWS GovCloud (US) Region.
  
  To prevent this type of attack and to maintain ITAR compliance, use network ACLs to prevent network traffic from exiting the VPC on the database port. For more information, see Network ACLs in the Amazon VPC User Guide.

- For each database instance that contains ITAR-regulated data, ensure that only specific CIDR ranges and Amazon EC2 security groups can access the database instance, especially when an Internet gateway is attached to the VPC. Only allow connections that are from the AWS GovCloud (US) Region or other ITAR-controlled environments to ITAR-controlled database instances.

If you are processing ITAR-regulated data with this service, use the SSL (HTTPS) endpoint to maintain ITAR compliance. For a list of endpoints, see AWS GovCloud (US) Endpoints (p. 36).

Amazon Simple Storage Service (Amazon S3)

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Database instance identifier</td>
<td>• Database instance identifier</td>
</tr>
<tr>
<td>• Master user name</td>
<td>• Master user name</td>
</tr>
<tr>
<td>• Database name</td>
<td>• Database name</td>
</tr>
<tr>
<td>• Database snapshot name</td>
<td>• Database snapshot name</td>
</tr>
<tr>
<td>• Database security group name</td>
<td>• Database security group name</td>
</tr>
<tr>
<td>• Database security group description</td>
<td>• Database security group description</td>
</tr>
<tr>
<td>• Database parameter group name</td>
<td>• Database parameter group name</td>
</tr>
<tr>
<td>• Database parameter group description</td>
<td>• Database parameter group description</td>
</tr>
<tr>
<td>• Option group name</td>
<td>• Option group name</td>
</tr>
<tr>
<td>• Option group description</td>
<td>• Option group description</td>
</tr>
<tr>
<td>• Database subnet group name</td>
<td>• Database subnet group name</td>
</tr>
<tr>
<td>• Database subnet group description</td>
<td>• Database subnet group description</td>
</tr>
<tr>
<td>• Event subscription name</td>
<td>• Event subscription name</td>
</tr>
<tr>
<td>• Resource tags</td>
<td>• Resource tags</td>
</tr>
</tbody>
</table>
• You cannot do a direct copy of the contents of an Amazon S3 bucket in the AWS GovCloud (US) Region to or from another AWS region.
• Cross-region replication is not supported in the AWS GovCloud (US) Region.
• If you use Amazon S3 policies, use the AWS GovCloud (US) ARN identifier. For more information, see Amazon Resource Names (ARNs) in AWS GovCloud (US) (p. 26).
• In the AWS GovCloud (US) Region, Amazon S3 has three endpoints. If you are processing ITAR-regulated data, use one of the SSL endpoints. If you have FIPS requirements, use the FIPS 140-2 endpoint (https://s3-fips-us-gov-west-1.amazonaws.com). You can access VPC endpoints for Amazon S3 over both the FIPS and non-FIPS endpoints. For a list of AWS GovCloud (US) endpoints, see AWS GovCloud (US) Endpoints (p. 36).
• Amazon S3 bucket names are unique to the AWS GovCloud (US) Region. Bucket names in the AWS GovCloud (US) Region are not shared across other AWS regions.
• Amazon S3 Transfer Acceleration is not available in the AWS GovCloud (US) Region.

For more information about Amazon S3, see the Amazon Simple Storage Service documentation.

**ITAR Boundary**

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• All data entered and stored in Amazon S3 buckets can contain ITAR-regulated data.</td>
<td>• Amazon S3 metadata is not permitted to contain ITAR-regulated data. This metadata includes all configuration data that you enter when creating and maintaining your Amazon S3 buckets, such as bucket names.</td>
</tr>
<tr>
<td>• Do not enter ITAR-regulated data in the following fields:</td>
<td>• Resource tags</td>
</tr>
<tr>
<td>• Resource tags</td>
<td></td>
</tr>
</tbody>
</table>

**Amazon Simple Notification Service (Amazon SNS)**

For more information about Amazon SNS, see the Amazon Simple Notification Service documentation.

**ITAR Boundary**

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• You may enter ITAR-regulated data in the following field when meeting the notification endpoints conditions below:</td>
<td>• ITAR-regulated data may not be entered, stored, or processed in Amazon SNS notification</td>
</tr>
</tbody>
</table>
### ITAR-Regulated Data Permitted

- Notification Message
- ITAR-regulated data may be entered, stored, and processed in the Amazon SNS notification when the following notification endpoints are being used:

**Notification Endpoints**
- Amazon SQS queues in AWS GovCloud (US) – may receive notifications containing ITAR-regulated data
- HTTPS URL endpoint in AWS GovCloud (US) – may receive notifications containing ITAR-regulated data if the service is allowed to accept ITAR regulated data (see the service for details)
- HTTPS URL endpoint outside of AWS GovCloud (US) – may receive notifications containing ITAR-regulated data if the customer has set up the endpoint URL in compliance with ITAR regulations

### ITAR-Regulated Data Not Permitted

messages when the following notification endpoints are being used:

**Notification Endpoints**
- Mobile push notifications – not permitted to contain ITAR-regulated data
- Email – not permitted to contain ITAR regulated data
- Amazon SQS queues outside of AWS GovCloud (US) – not permitted to contain ITAR-regulated data
- HTTP URL endpoint – not permitted to contain ITAR-regulated data
- Amazon SNS metadata is not permitted to contain ITAR-regulated data. This metadata includes all configuration data that you enter when setting up and maintaining your topics.

For example, do not enter ITAR-regulated data in the following fields:
- Topic Name
- Display Name
- Topic Policy
- Topic Delivery Policy
- Topic ARN
- Endpoint
- Subject
- Application Name

---

### Amazon Simple Queue Service (Amazon SQS)

For more information about Amazon SQS, see the [Amazon Simple Queue Service documentation](#).

### ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon SQS message contents</td>
<td>Amazon SQS metadata is not permitted to contain ITAR-regulated data. This metadata includes all configuration data that you enter when setting up and maintaining your queues. For example, do not enter ITAR-regulated data in the following fields:</td>
</tr>
</tbody>
</table>

---

78
Amazon Simple Workflow Service (Amazon SWF)

For more information about Amazon SWF, see the Amazon Simple Workflow Service documentation.

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not applicable</td>
<td>No ITAR-regulated data can be entered, stored, or processed in Amazon SWF.</td>
</tr>
<tr>
<td></td>
<td>Amazon SWF metadata is not permitted to contain ITAR-regulated data. This metadata includes all of the configuration data that you enter when setting up and maintaining your workflows.</td>
</tr>
<tr>
<td></td>
<td>For example, do not enter ITAR-regulated data in the following fields:</td>
</tr>
<tr>
<td></td>
<td>• Workflow type name</td>
</tr>
<tr>
<td></td>
<td>• Workflow type version</td>
</tr>
<tr>
<td></td>
<td>• Activity type name</td>
</tr>
<tr>
<td></td>
<td>• Activity type version</td>
</tr>
<tr>
<td></td>
<td>• Execution workflow ID</td>
</tr>
<tr>
<td></td>
<td>• Activity task ID</td>
</tr>
<tr>
<td></td>
<td>• The input, result, or details arguments to workflow executions</td>
</tr>
<tr>
<td></td>
<td>• The input, result, or details arguments to activity tasks</td>
</tr>
</tbody>
</table>

Amazon Virtual Private Cloud (Amazon VPC)

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

- You must launch Amazon EC2 instances, Amazon RDS instances, or Amazon EMR instances in an Amazon VPC. In some cases, your account might have a default VPC. For more information, see Determining if Your Account Has a Default Amazon VPC (p. 59).
• Use SSL (HTTPS) when you make calls to the service in the AWS GovCloud (US) Region. In other regions, you can use HTTP or HTTPS.
• Inter-region Amazon VPC peering connections are not supported.

For more information, see the Amazon Virtual Private Cloud documentation.

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• All data entered, stored, and processed in Amazon VPC can contain ITAR-regulated data.</td>
<td>• Amazon VPC metadata is not permitted to contain ITAR-regulated data. This metadata includes all of the configuration data that you enter when setting up and maintaining your VPCs.</td>
</tr>
<tr>
<td>• You can transmit ITAR-regulated data in clear text across the network within your Amazon VPC.</td>
<td>• If you are using VPC Flow Logs, the following field is not permitted to contain ITAR-regulated data:</td>
</tr>
<tr>
<td>• You can transmit ITAR-regulated data in clear text across your Amazon VPC VPN tunnels, assuming the destination endpoint is ITAR compliant.</td>
<td>• Destination log group name</td>
</tr>
</tbody>
</table>

AWS Management Console for the AWS GovCloud (US) Region

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

• You access the AWS GovCloud (US) console by using a different URL than the standard AWS Management Console.
• You can only access the console by using an IAM user name and password, not with the AWS GovCloud (US) root account.
• The console includes only the services that are available in the AWS GovCloud (US) Region.
• You are automatically signed out from the console after 4 hours.
• Hardware Multi-factor Authentication (MFA) tokens are not available for the console.
• The console does not permit navigation to any regions other than the AWS GovCloud (US) Region.
• You can sign in to the AWS GovCloud (US) console and the standard AWS Management Console concurrently.
• You cannot automatically create a support ticket from the AWS GovCloud (US) console.

ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:
ITAR-Regulated Data Permitted | ITAR-Regulated Data Not Permitted
---|---
- Console passwords are protected as ITAR-regulated data.
- All console data fields inherit the ITAR restrictions for the specific service that is being accessed. See each service for details.
- Your user name is not permitted to contain ITAR-regulated data.
- All console data fields inherit the ITAR restrictions for the specific service that is being accessed. See each service for details.

AWS Trusted Advisor

The following list details the differences for using this service in the AWS GovCloud (US) Region compared to other AWS regions:

- Email notifications are not yet enabled in Trusted Advisor in the AWS GovCloud (US) Region.
- All 23 checks are available to all AWS GovCloud (US) customers today.

The following table lists the Trusted Advisor checks that are available in the AWS GovCloud (US) Region and the required support level:

<table>
<thead>
<tr>
<th>Category</th>
<th>Check</th>
<th>Enabled in AWS GovCloud (US)</th>
<th>Support Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost Optimization</td>
<td>Unassociated Elastic IP Address</td>
<td>Yes</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Security</td>
<td>Security Groups - Specific Ports Unrestricted</td>
<td>Yes</td>
<td>Basic</td>
</tr>
<tr>
<td></td>
<td>Security Groups - Unrestricted Access</td>
<td>Yes</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Amazon S3 Bucket Permissions</td>
<td>Yes</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>IAM Password Policy</td>
<td>Yes</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>AWS CloudTrail Logging</td>
<td>Yes</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>ELB Listener Security</td>
<td>Yes</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Fault Tolerance</td>
<td>ELB Security Groups</td>
<td>Yes</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Amazon EBS Snapshots</td>
<td>Yes</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Amazon EC2 Availability Zone Balance</td>
<td>Yes</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Load Balancer Optimization</td>
<td>Yes</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Category</td>
<td>Check</td>
<td>Enabled in AWS GovCloud (US)</td>
<td>Support Level</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------</td>
<td>-----------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td></td>
<td>VPN Tunnel Redundancy</td>
<td>Yes</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Auto Scaling Group Resources</td>
<td>Yes</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Auto Scaling Group Health Check</td>
<td>Yes</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Amazon S3 Bucket Logging</td>
<td>Yes</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>ELB Connection Draining</td>
<td>Yes</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>ELB Cross-Zone Load Balancing</td>
<td>Yes</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Performance</td>
<td>High Utilization Amazon EC2 Instances</td>
<td>Yes</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Service Limits</td>
<td>Yes</td>
<td>Basic</td>
</tr>
<tr>
<td></td>
<td>Amazon EBS Provisioned IOPS (SSD) Volume Attachment Configuration</td>
<td>Yes</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Large Number of Rules in an EC2 Security Group</td>
<td>Yes</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Large Number of EC2 Security Group Rules Applied to an Instance</td>
<td>Yes</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Overutilized Amazon EBS Magnetic Volumes</td>
<td>Yes</td>
<td>Business and Enterprise</td>
</tr>
</tbody>
</table>

The following table lists the Trusted Advisor checks that are not available in the AWS GovCloud (US) Region:

<table>
<thead>
<tr>
<th>Category</th>
<th>Check</th>
<th>Enabled in AWS GovCloud (US)</th>
<th>Support Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost Optimization</td>
<td>Amazon EC2 Reserved Instance Optimization</td>
<td>No</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Low Utilization Amazon EC2 Instances</td>
<td>No</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Idle Load Balancers</td>
<td>No</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Underutilized Amazon EBS Volumes</td>
<td>No</td>
<td>Business and Enterprise</td>
</tr>
</tbody>
</table>
### ITAR Boundary

The ITAR boundary defines where customers are allowed to store ITAR-regulated data for this service in the AWS GovCloud (US) Region. You must comply with the boundaries in order to maintain ITAR compliance. If you do not have any ITAR-regulated data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Not applicable</td>
<td>• Not applicable</td>
</tr>
</tbody>
</table>

---

**AWS GovCloud (US) User Guide**

**ITAR Boundary**

**Category** | **Check** | **Enabled in AWS GovCloud (US)** | **Support Level** |
--- | --- | --- | --- |
Security | IAM Use | No | Basic |
| MFA on Root Account | No | Basic |
| Amazon RDS Security Group Access Risk | No | Business and Enterprise |
| Amazon Route 53 MX Resource Record Sets and Sender Policy Framework | No | Business and Enterprise |
Fault Tolerance | Amazon RDS Backups | No | Business and Enterprise |
| Amazon RDS Multi-AZ | No | Business and Enterprise |
| Amazon Route 53 Name Server Delegations | No | Business and Enterprise |
| Amazon Route 53 High TTL Resource Record Sets | No | Business and Enterprise |
| Amazon Route 53 Failover Resource Record Sets | No | Business and Enterprise |
| Amazon Route 53 Deleted Health Checks | No | Business and Enterprise |
Performance | Amazon Route 53 Alias Resource Record Sets | No | Business and Enterprise |
| Amazon CloudFront Content Delivery Optimization | No | Business and Enterprise |
| Amazon Route 53 Latency Resource Record Sets | No | Business and Enterprise |

For more information about Trusted Advisor, see [Meet AWS Trusted Advisor](#).
**Troubleshooting**

The following section discusses common issues you might encounter when you work in the AWS GovCloud (US) Region.

**Topics**
- Client.UnsupportedOperation: Instances can only be launched within Amazon VPC in this region (p. 84)

**Client.UnsupportedOperation: Instances can only be launched within Amazon VPC in this region**

**Service:** Amazon EC2

**Issue:** When I attempt to launch an instance by using the CLI or API, I get a "Client.UnsupportedOperation: Instances can only be launched within Amazon VPC in this region" error.

**Cause:** Your account might not have a VPC.

**Recommended Action:** Verify that your account has a VPC. If not, create a VPC and then use it to launch instances.

In some cases, your account might have a default VPC. For more information, see Determining if Your Account Has a Default Amazon VPC (p. 59). If you still receive this error when you run the `ec2-run-instances` command (or the `RunInstances` action) to launch an Amazon EC2 instance, you must specify the `subnet` parameter. Although the `subnet` parameter is optional in other regions, if you omit it in the AWS GovCloud (US) Region, you receive an error.
Related Resources

This topic lists additional resources related to AWS GovCloud (US).

New to AWS

The following table lists additional resources for users new to AWS:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development and Test on AWS</td>
<td>This paper describes how AWS adds value in the various phases of the software development cycle, with a specific focus on development and test.</td>
</tr>
<tr>
<td>Amazon VPC Network Connectivity Options</td>
<td>This paper describes connectivity options for integrating remote customer networks with Amazon VPC, as well as interconnecting multiple Amazon VPCs into a contiguous virtual network.</td>
</tr>
<tr>
<td>Microsoft SharePoint Server on AWS Reference Architecture</td>
<td>This paper discusses general concepts about how to run SharePoint on AWS. It provides detailed technical guidance for configuring, deploying, and running a SharePoint Server farm on AWS.</td>
</tr>
<tr>
<td>Operational Checklists for AWS</td>
<td>This paper provides two checklists, Basic and Enterprise, that you can use to evaluate your applications against a list of essential and recommended best practices.</td>
</tr>
<tr>
<td>Amazon's Corporate IT Deploys SharePoint 2010 to the AWS Cloud</td>
<td>This paper describes how and why Amazon's corporate IT organization deployed its corporate intranet (an enterprise mission-critical corporate IT application that involves highly sensitive data) running Microsoft SharePoint 2010 to the AWS cloud.</td>
</tr>
<tr>
<td>Extend Your IT Infrastructure with Amazon VPC</td>
<td>This paper highlights common use cases and best practices for Amazon VPC and related services.</td>
</tr>
<tr>
<td>Auditing Security Checklist for Use of AWS</td>
<td>This paper provides a checklist to help you design and execute a security assessment of your organization's use of AWS, which may be required by industry or regulatory standards.</td>
</tr>
<tr>
<td>Security at Scale: Governance on AWS</td>
<td>This paper discusses the security and governance features built in to AWS services to help you incorporate security benefits and best practices in building your integrated environment with AWS.</td>
</tr>
<tr>
<td>AWS Security Best Practices</td>
<td>This paper explains the AWS shared security model and provides an overview of various security topics. These topics include identifying, categorizing, and protecting your assets on AWS;</td>
</tr>
</tbody>
</table>
The following table lists additional resources for users experienced with AWS:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Identity Federation with Mobile Applications</td>
<td>This article discusses the web identity federation feature of AWS Security Token Service and a sample for use in the AWS Mobile SDKs.</td>
</tr>
<tr>
<td>High Availability for Amazon VPC NAT Instances: An Example</td>
<td>This article provides all required resources, including an easy-to-use script and instructions on how you can leverage bidirectional monitoring between two NAT instances, to implement a high availability (HA) failover solution for network address translation (NAT).</td>
</tr>
<tr>
<td>Securing Data at Rest with Encryption</td>
<td>This paper provides an overview of methods for encrypting your data at rest.</td>
</tr>
</tbody>
</table>

**Experienced with AWS**

The following table lists additional resources for users experienced with AWS:
The following table describes important changes to the documentation since the last release of the AWS GovCloud (US) User Guide.

- **Latest documentation update:** December 21, 2016

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date Changed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Kinesis Data Streams</td>
<td>Amazon Kinesis Data Streams is now supported in the AWS GovCloud (US) Region. See Amazon Kinesis Data Streams (p. 70).</td>
<td>December 21, 2016</td>
</tr>
<tr>
<td>Amazon EC2</td>
<td>Updated public IP range. See Amazon Elastic Compute Cloud (Amazon EC2) (p. 58).</td>
<td>June 21, 2016</td>
</tr>
<tr>
<td>AWS Config</td>
<td>AWS Config is now available in the AWS GovCloud (US) Region. See AWS Config (p. 53).</td>
<td>May 26, 2016</td>
</tr>
<tr>
<td>AWS Import/Export</td>
<td>AWS Snowball, a feature of AWS Import/Export, is now available in the AWS GovCloud (US) Region. See AWS Snowball (p. 69).</td>
<td>April 19, 2016</td>
</tr>
<tr>
<td>AWS CloudTrail</td>
<td>Updated information about creating multiple trails. See AWS CloudTrail (p. 47).</td>
<td>March 24, 2016</td>
</tr>
<tr>
<td>Importing VMs</td>
<td>Updated information about importing virtual machines into the AWS GovCloud (US) Region. See Importing Virtual Machines into the AWS GovCloud (US) Region (p. 63).</td>
<td>February 11, 2016</td>
</tr>
<tr>
<td>Signing up for AWS GovCloud (US)</td>
<td>Describes the new sign-up process for direct customers and resellers. See Signing Up for AWS GovCloud (US) (p. 7).</td>
<td>December 18, 2015</td>
</tr>
<tr>
<td>IAM</td>
<td>Updates to MFA for the AWS GovCloud (US) console.</td>
<td>December 18, 2015</td>
</tr>
<tr>
<td>Amazon S3</td>
<td>Updated text about VPC endpoints for Amazon S3. See Amazon Simple Storage Service (Amazon S3) (p. 76).</td>
<td>December 18, 2015</td>
</tr>
<tr>
<td>Amazon EBS</td>
<td>Updated text about copying snapshots. See Amazon Elastic Block Store (Amazon EBS) (p. 57).</td>
<td>December 18, 2015</td>
</tr>
<tr>
<td>CloudWatch Logs and CloudTrail</td>
<td>CloudWatch Logs is now supported within CloudTrail in the AWS GovCloud (US) Region. See AWS CloudTrail (p. 47).</td>
<td>November 19, 2015</td>
</tr>
<tr>
<td>AWS Direct Connect</td>
<td>Updated information about using AWS Direct Connect. See AWS Direct Connect (p. 54).</td>
<td>October 28, 2015</td>
</tr>
<tr>
<td>Amazon Glacier</td>
<td>Updated ITAR-regulated data for Amazon Glacier. See Amazon Glacier (p. 67).</td>
<td>October 28, 2015</td>
</tr>
<tr>
<td>VPC Flow Logs</td>
<td>VPC Flow Logs are now supported in AWS GovCloud (US). See Amazon Virtual Private Cloud (Amazon VPC) (p. 79).</td>
<td>October 27, 2015</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date Changed</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>CloudWatch Logs</td>
<td>CloudWatch Logs are now supported in AWS GovCloud (US). See Amazon CloudWatch (p. 49).</td>
<td>October 27, 2015</td>
</tr>
<tr>
<td>AWS WAF and Amazon CloudFront</td>
<td>Added information about using AWS WAF with CloudFront. See Setting Up Amazon CloudFront with Your AWS GovCloud (US) Resources (p. 17).</td>
<td>October 27, 2015</td>
</tr>
<tr>
<td>AWS CloudTrail</td>
<td>Added a policy example that enables CloudTrail to write log files to your bucket. See AWS CloudTrail (p. 47).</td>
<td>August 25, 2015</td>
</tr>
<tr>
<td>AWS CloudHSM Classic</td>
<td>AWS CloudHSM Classic is now available in the AWS GovCloud (US) Region. See AWS CloudHSM Classic (p. 46).</td>
<td>August 5, 2015</td>
</tr>
<tr>
<td>Penetration testing</td>
<td>Updated instructions for submitting a request. See Penetration Testing (p. 41).</td>
<td>August 5, 2015</td>
</tr>
<tr>
<td>IAM</td>
<td>Added information about SSH public keys. See AWS Identity and Access Management (IAM) (p. 68).</td>
<td>July 9, 2015</td>
</tr>
<tr>
<td>IAM and VM Import</td>
<td>Added information about using roles to delegate access. Added a note about ImportImage. See AWS Identity and Access Management (IAM) (p. 68) and Importing Virtual Machines into the AWS GovCloud (US) Region (p. 63).</td>
<td>June 12, 2015</td>
</tr>
<tr>
<td>DynamoDB and CloudTrail</td>
<td>DynamoDB is now supported within CloudTrail in the AWS GovCloud (US) Region. See AWS CloudTrail (p. 47).</td>
<td>May 28, 2015</td>
</tr>
<tr>
<td>AWS Key Management Service</td>
<td>AWS KMS is now available in the AWS GovCloud (US) Region. See AWS Key Management Service (AWS KMS) (p. 70).</td>
<td>May 7, 2015</td>
</tr>
<tr>
<td>Encryption</td>
<td>Encryption is now available for Amazon Elastic Block Store (Amazon EBS) (p. 57), Amazon EMR (Amazon EMR) (p. 66), and Amazon Simple Storage Service (Amazon S3) (p. 76).</td>
<td>May 7, 2015</td>
</tr>
<tr>
<td>AWS Direct Connect</td>
<td>Updated instructions for setting up AWS Direct Connect. See AWS Direct Connect (p. 54).</td>
<td>April 3, 2015</td>
</tr>
<tr>
<td>Amazon S3</td>
<td>Added info about cross-region replication. See Amazon Simple Storage Service (Amazon S3) (p. 76).</td>
<td>March 24, 2015</td>
</tr>
<tr>
<td>AWS Trusted Advisor</td>
<td>Added two new Trusted Advisor checks that are now supported (IAM Password Policy, ELB Connection Draining). See AWS Trusted Advisor (p. 81).</td>
<td>March 18, 2015</td>
</tr>
<tr>
<td>AWS Trusted Advisor</td>
<td>Added three new Trusted Advisor checks that are now supported (ELB Cross-Zone Load Balancing, ELB Listener Security, ELB Security Groups). See AWS Trusted Advisor (p. 81).</td>
<td>March 11, 2015</td>
</tr>
<tr>
<td>VM Export</td>
<td>Updated information about using VM Export. See Amazon Elastic Compute Cloud (Amazon EC2) (p. 58).</td>
<td>March 9, 2015</td>
</tr>
<tr>
<td>VM Import</td>
<td>Updated information about using VM Import. See Amazon Elastic Compute Cloud (Amazon EC2) (p. 58).</td>
<td>March 6, 2015</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date Changed</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Importing VMs</td>
<td>Updated information about importing virtual machines into the AWS GovCloud (US) Region. See Importing Virtual Machines into the AWS GovCloud (US) Region (p. 63).</td>
<td>February 11, 2015</td>
</tr>
<tr>
<td>Amazon ElastiCache</td>
<td>ElastiCache is now available in the AWS GovCloud (US) Region. See Amazon ElastiCache (p. 65).</td>
<td>January 29, 2015</td>
</tr>
<tr>
<td>AWS Trusted Advisor</td>
<td>Updated information about Trusted Advisor. See AWS Trusted Advisor (p. 81).</td>
<td>January 29, 2015</td>
</tr>
<tr>
<td>Amazon RDS and CloudTrail</td>
<td>Amazon RDS is now supported within CloudTrail in the AWS GovCloud (US) Region. See AWS CloudTrail (p. 47).</td>
<td>January 22, 2015</td>
</tr>
<tr>
<td>AWS Trusted Advisor</td>
<td>Trusted Advisor is now available in the AWS GovCloud (US) Region. See AWS Trusted Advisor (p. 81).</td>
<td>January 20, 2015</td>
</tr>
<tr>
<td>Amazon Glacier</td>
<td>Amazon Glacier is now available in the AWS GovCloud (US) Region. See Amazon Glacier (p. 67).</td>
<td>December 30, 2014</td>
</tr>
<tr>
<td>AWS CloudTrail</td>
<td>CloudTrail is now available in the AWS GovCloud (US) Region. See AWS CloudTrail (p. 47).</td>
<td>December 16, 2014</td>
</tr>
<tr>
<td>Importing VMs</td>
<td>Updated information about importing virtual machines into the AWS GovCloud (US) Region. See Importing Virtual Machines into the AWS GovCloud (US) Region (p. 63) and Amazon Elastic Compute Cloud (Amazon EC2) (p. 58).</td>
<td>December 15, 2014</td>
</tr>
<tr>
<td>Amazon Redshift</td>
<td>Amazon Redshift is now available in the AWS GovCloud (US) Region. See Amazon Redshift (p. 73).</td>
<td>November 18, 2014</td>
</tr>
<tr>
<td>Feedback links</td>
<td>Fixed links to provide feedback.</td>
<td>September 26, 2014</td>
</tr>
<tr>
<td>IP range</td>
<td>Another public IP range for Amazon EC2 instances has been added. See Amazon Elastic Compute Cloud (Amazon EC2) (p. 58).</td>
<td>August 27, 2014</td>
</tr>
<tr>
<td>IAM</td>
<td>Updates to MFA for changes in IAM console.</td>
<td>August 5, 2014</td>
</tr>
<tr>
<td>IAM</td>
<td>Added the URL for the XML document that contains relying party information and certificates when using a SAML provider. See AWS Identity and Access Management (IAM) (p. 68).</td>
<td>July 25, 2014</td>
</tr>
<tr>
<td>Amazon EC2</td>
<td>Updates to differences in Amazon EC2 AMI tools. See Amazon Elastic Compute Cloud (Amazon EC2) (p. 58).</td>
<td>July 15, 2014</td>
</tr>
<tr>
<td>Amazon SNS</td>
<td>Updates to Amazon SNS ITAR boundary. See Amazon Simple Notification Service (Amazon SNS) (p. 77).</td>
<td>July 2, 2014</td>
</tr>
<tr>
<td>Provisioned IOPS</td>
<td>Provisioned IOPS and tagging in the console are supported for Amazon RDS in the AWS GovCloud (US) Region. For information about using Amazon RDS in the AWS GovCloud (US) Region, see Amazon Relational Database Service (Amazon RDS) (p. 75).</td>
<td>May 28, 2014</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date Changed</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Accessing the console</td>
<td>Updates for the AWS GovCloud (US) Management Console onboard tool. See Onboarding to AWS GovCloud (US) (Resellers or Reseller Customers) (p. 10).</td>
<td>April 7, 2014</td>
</tr>
<tr>
<td>Provisioned IOPS</td>
<td>Provisioned IOPS is supported in the AWS GovCloud (US) Region. For information about using Amazon EC2 and Amazon EBS in the AWS GovCloud (US) Region, see Amazon Elastic Compute Cloud (Amazon EC2) (p. 58) and Amazon Elastic Block Store (Amazon EBS) (p. 57).</td>
<td>April 1, 2014</td>
</tr>
<tr>
<td>Amazon EC2</td>
<td>Updates to Amazon EC2 and troubleshooting. For information, see Amazon Elastic Compute Cloud (Amazon EC2) (p. 58) and Troubleshooting (p. 84).</td>
<td>March 19, 2014</td>
</tr>
<tr>
<td>Amazon SES</td>
<td>Added instructions on how to set up Amazon SES in your AWS GovCloud (US) architecture. See Setting Up Amazon Simple Email Service in Your AWS GovCloud (US) Architecture (p. 24).</td>
<td>March 4, 2014</td>
</tr>
<tr>
<td>Migrating AMIs</td>
<td>Added information about how to migrate your AMIs from another AWS region into the AWS GovCloud (US) Region. See Importing Virtual Machines into the AWS GovCloud (US) Region (p. 63).</td>
<td>March 4, 2014</td>
</tr>
<tr>
<td>Red Hat Linux</td>
<td>Red Hat Linux is now available in the AWS GovCloud (US) Region. For information about using Amazon EC2 in the AWS GovCloud (US) Region, see Amazon Elastic Compute Cloud (Amazon EC2) (p. 58).</td>
<td>March 4, 2014</td>
</tr>
<tr>
<td>SUSE Linux</td>
<td>SUSE Linux is now available in the AWS GovCloud (US) Region. For information about using Amazon EC2 in the AWS GovCloud (US) Region, see Amazon Elastic Compute Cloud (Amazon EC2) (p. 58).</td>
<td>January 17, 2014</td>
</tr>
<tr>
<td>Resources</td>
<td>Updated list of additional resources. See Related Resources (p. 85).</td>
<td>January 8, 2014</td>
</tr>
<tr>
<td></td>
<td>Added note about Amazon SNS Mobile Push Notifications. See Amazon Simple Notification Service (Amazon SNS) (p. 77).</td>
<td></td>
</tr>
<tr>
<td>DynamoDB</td>
<td>The DynamoDB console is available and no longer in beta in the AWS GovCloud (US) Region. See Amazon DynamoDB (p. 56).</td>
<td>December 30, 2013</td>
</tr>
<tr>
<td>Endpoints</td>
<td>Added AWS Management Console endpoints for federation and SAML. See AWS GovCloud (US) Endpoints (p. 36).</td>
<td>December 11, 2013</td>
</tr>
<tr>
<td>Amazon EC2</td>
<td>Added fix for instructions to create a key pair. See Amazon Elastic Compute Cloud (Amazon EC2) (p. 58).</td>
<td>November 20, 2013</td>
</tr>
<tr>
<td>Amazon EMR</td>
<td>The Amazon EMR console is now available in the AWS GovCloud (US) Region. See Amazon EMR (Amazon EMR) (p. 66).</td>
<td>November 12, 2013</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date Changed</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Elastic Load Balancing</td>
<td>Elastic Load Balancing is available and no longer in beta in the AWS GovCloud (US) Region. See Elastic Load Balancing (p. 64).</td>
<td>November 1, 2013</td>
</tr>
<tr>
<td>AWS Direct Connect</td>
<td>Incorporated changes for AWS Direct Connect console update.</td>
<td>October 31, 2013</td>
</tr>
<tr>
<td>AWS CloudFormation</td>
<td>The AWS CloudFormation console is now available in the AWS GovCloud (US) Region. See AWS CloudFormation (p. 46).</td>
<td>October 31, 2013</td>
</tr>
<tr>
<td>Kindle</td>
<td>Published a Kindle version.</td>
<td>October 22, 2013</td>
</tr>
<tr>
<td>AWS ElasticWolf Client Console</td>
<td>Added link to AWS ElasticWolf Client Console. See Accessing the AWS GovCloud (US) Region (p. 39).</td>
<td>October 18, 2013</td>
</tr>
<tr>
<td>Elastic Load Balancing</td>
<td>Updates to Elastic Load Balancing ITAR boundary. See Elastic Load Balancing (p. 64).</td>
<td>September 27, 2013</td>
</tr>
<tr>
<td>Virtual Multi-Factor Authentication (MFA)</td>
<td>Added a section about enabling virtual MFA.</td>
<td>August 28, 2013</td>
</tr>
<tr>
<td>Amazon Route 53 zone apex</td>
<td>Added a new section about setting up Route 53 zone apex. See Setting Up Amazon Route 53 Zone Apex Support with an AWS GovCloud (US) Elastic Load Balancing Load Balancer (p. 19).</td>
<td>August 9, 2013</td>
</tr>
<tr>
<td>AWS GovCloud (US) AWS Direct Connect</td>
<td>Added an example to Amazon Resource Names (ARNs) in AWS GovCloud (US) (p. 26).</td>
<td>July 24, 2013</td>
</tr>
<tr>
<td>Amazon CloudFront</td>
<td>Added information about setting up Amazon CloudFront and Amazon Route 53 for AWS GovCloud (US). See Setting Up Amazon CloudFront with Your AWS GovCloud (US) Resources (p. 17) and Setting Up Amazon Route 53 with Your AWS GovCloud (US) Resources (p. 18).</td>
<td>July 16, 2013</td>
</tr>
<tr>
<td>Amazon Virtual Private Cloud</td>
<td>Added information about AWS GovCloud (US) accounts having an Amazon VPC by default. See Amazon Elastic Compute Cloud (Amazon EC2) (p. 58).</td>
<td>May 28, 2013</td>
</tr>
<tr>
<td>Initial release</td>
<td>This is the first release of AWS GovCloud (US) User Guide.</td>
<td>April 10, 2013</td>
</tr>
</tbody>
</table>
AWS Glossary

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