# Table of Contents

Welcome ........................................................................................................................................... 1  
What Is AWS GovCloud (US)? ........................................................................................................... 2  
Differences with Standard AWS Accounts ......................................................................................... 2  
Billing and Payment ........................................................................................................................... 4  
Getting Started ................................................................................................................................. 5  
Signing Up .......................................................................................................................................... 5  
Creating an AWS GovCloud (US) account through a Reseller or Solution Provider ................. 9  
Onboarding (Direct Customers) ......................................................................................................... 9  
Configuring Your Account ................................................................................................................. 9  
Verifying AWS CloudTrail Is Enabled ............................................................................................... 10  
Onboarding to AWS GovCloud (US) as a Solution Provider reselling in AWS GovCloud (US) ........ 11  
Enabling Multi-Factor Authentication (MFA) .................................................................................. 16  
Signing Up for Customer Support .................................................................................................... 17  
Setting Up AWS GovCloud (US) ....................................................................................................... 19  
CloudFront with Your Resources .................................................................................................... 19  
Credentials ....................................................................................................................................... 19  
Tips for Setting Up CloudFront .................................................................................................... 20  
Route 53 with Your Resources ......................................................................................................... 20  
Route 53 Zone Apex Support with a Load Balancer ........................................................................ 21  
Step 1: Sign Up for AWS GovCloud (US) ......................................................................................... 22  
Step 2: Create Your Resources in the AWS GovCloud (US) Region ............................................... 22  
Step 3: Create a CloudFront Custom Origin Web Distribution .................................................... 25  
Step 4: Configure a New Route 53 Alias Resource Record Set ...................................................... 28  
Step 5: Test that Your Website Is Accessible .................................................................................... 30  
Using AWS GovCloud (US) Regions ............................................................................................... 32  
Amazon Resource Names .................................................................................................................. 32  
ARN Format ....................................................................................................................................... 34  
Example ARNs ..................................................................................................................................... 35  
Amazon Athena ................................................................................................................................. 36  
Amazon AppStream 2.0 .................................................................................................................... 36  
AWS Artifact ...................................................................................................................................... 36  
Amazon Aurora ................................................................................................................................. 37  
Amazon EC2 Auto Scaling ................................................................................................................ 37  
AWS Batch ......................................................................................................................................... 37  
AWS Backup ...................................................................................................................................... 37  
AWS Certificate Manager .................................................................................................................. 38  
AWS Certificate Manager Private Certificate Authority ................................................................. 38  
Amazon Cloud Directory .................................................................................................................. 39  
Amazon CloudWatch Events ............................................................................................................. 39  
AWS CodeBuild ............................................................................................................................... 39  
AWS CodeCommit ............................................................................................................................ 40  
AWS CodeDeploy ............................................................................................................................. 40  
AWS CodePipeline ........................................................................................................................... 40  
Amazon Cognito ............................................................................................................................... 41  
Amazon Comprehend ....................................................................................................................... 41  
Amazon Comprehend Medical ......................................................................................................... 41  
AWS Config ....................................................................................................................................... 41  
AWS DataSync ................................................................................................................................. 42  
AWS Database Migration Service ..................................................................................................... 42  
AWS Directory Service ..................................................................................................................... 42  
Amazon DocumentDB (with MongoDB compatibility) ..................................................................... 42  
Amazon DynamoDB ........................................................................................................................ 43  
AWS Elastic Beanstalk .................................................................................................................... 43  
Amazon Elastic Compute Cloud ...................................................................................................... 44
ITAR Boundary ............................................................................................................. 116
Amazon Cognito ............................................................................................................. 116
  How Amazon Cognito Differs for AWS GovCloud (US) ............................................. 117
Documentation for Amazon Cognito ............................................................................ 117
ITAR Boundary ............................................................................................................. 117
Amazon Comprehend Medical ....................................................................................... 118
  How Amazon Comprehend Medical Differs for AWS GovCloud (US) .................... 118
Documentation for Amazon Comprehend Medical ..................................................... 118
ITAR Boundary ............................................................................................................. 118
AWS Config ................................................................................................................. 119
  How AWS Config Differs for AWS GovCloud (US) .................................................. 119
Documentation for AWS Config .................................................................................. 119
ITAR Boundary ............................................................................................................. 119
AWS Direct Connect .................................................................................................... 120
  How AWS Direct Connect Differs for AWS GovCloud (US) .................................... 120
Documentation for AWS Direct Connect ................................................................... 120
ITAR Boundary ............................................................................................................. 120
  Setting Up AWS Direct Connect with a VPN Connection ........................................ 121
AWS Directory Service ................................................................................................. 121
  How AWS Directory Service Differs for AWS GovCloud (US) ................................ 122
Documentation for AWS Directory Service ................................................................. 122
ITAR Boundary ............................................................................................................. 122
AWS Database Migration Service ................................................................................ 123
  How AWS Database Migration Service Differs for AWS GovCloud (US) ............... 123
Documentation for AWS Database Migration Service ............................................... 123
ITAR Boundary ............................................................................................................. 123
AWS Deep Learning AMIs ......................................................................................... 124
  How AWS Deep Learning AMI Differs for AWS GovCloud (US) ............................ 124
Documentation for AWS Deep Learning AMI .............................................................. 124
ITAR Boundary ............................................................................................................. 124
Amazon DocumentDB (with MongoDB compatibility) ............................................... 124
  How Amazon DocumentDB Differs for AWS GovCloud (US) ................................. 125
Documentation for Amazon DocumentDB ................................................................. 125
ITAR Boundary ............................................................................................................. 125
Amazon DynamoDB ..................................................................................................... 126
  How Amazon DynamoDB Differs for AWS GovCloud (US) ..................................... 126
Documentation for Amazon DynamoDB ...................................................................... 126
ITAR Boundary ............................................................................................................. 126
AWS Elastic Beanstalk ............................................................................................... 127
  How AWS Elastic Beanstalk Differs for AWS GovCloud (US) ............................... 127
Documentation for AWS Elastic Beanstalk ................................................................. 127
ITAR Boundary ............................................................................................................. 127
Amazon EBS ................................................................................................................... 128
  How Amazon Elastic Block Store Differs for AWS GovCloud (US) ......................... 128
Documentation for Amazon Elastic Block Store ......................................................... 128
ITAR Boundary ............................................................................................................. 128
Amazon EC2 ................................................................................................................ 129
  How Amazon Elastic Compute Cloud Differs for AWS GovCloud (US) ................. 129
Determining if Your Account Has a Default Amazon VPC ........................................ 130
Documentation for Amazon EC2 ................................................................................. 131
ITAR Boundary ............................................................................................................. 131
Amazon EC2 VM Import/Export ............................................................................... 131
  How Amazon EC2 VM Import/Export Differs for AWS GovCloud (US) ............... 132
Documentation for Amazon EC2 VM Import/Export ................................................ 132
ITAR Best Practices .................................................................................................... 132
Amazon EC2 Image Builder ....................................................................................... 132
  How Amazon EC2 Image Builder Differs for AWS GovCloud (US) ....................... 132
How AWS Storage Gateway Differs for AWS GovCloud (US) ......................................................... 189
Documentation for AWS Storage Gateway .................................................................................... 190
ITAR Boundary ................................................................................................................................. 190
AWS Storage Gateway AMI Information .......................................................................................... 190
Amazon SWF ...................................................................................................................................... 190
How Amazon Simple Workflow Service Differs for AWS GovCloud (US) ........................................... 191
Documentation for Amazon Simple Workflow Service ....................................................................... 191
ITAR Boundary ................................................................................................................................. 191
AWS Systems Manager ...................................................................................................................... 191
How AWS Systems Manager Differs for AWS GovCloud (US) ............................................................. 192
Documentation for AWS Systems Manager ....................................................................................... 192
ITAR Boundary ..................................................................................................................................... 192
Amazon Textract ................................................................................................................................. 192
How Amazon Textract Differs for AWS GovCloud (US) ...................................................................... 192
Documentation for Amazon Textract .................................................................................................. 195
ITAR Boundary ...................................................................................................................................... 195
AWS Transfer Family ........................................................................................................................... 193
How AWS Transfer Family Differs for AWS GovCloud (US) ................................................................. 193
Documentation for AWS Transfer Family .......................................................................................... 193
ITAR Boundary ..................................................................................................................................... 193
Amazon Transcribe ............................................................................................................................. 194
How Amazon Transcribe Differs for AWS GovCloud (US) ................................................................... 194
Documentation for Amazon Transcribe .............................................................................................. 194
ITAR Boundary ..................................................................................................................................... 194
Amazon Translate ............................................................................................................................... 194
How Amazon Translate Differs for AWS GovCloud (US) .................................................................... 195
Documentation for Amazon Translate .................................................................................................. 195
ITAR Boundary ..................................................................................................................................... 195
AWS Trusted Advisor ......................................................................................................................... 195
How AWS Trusted Advisor Differs for AWS GovCloud (US) ................................................................. 195
Documentation for AWS Trusted Advisor .......................................................................................... 201
ITAR Boundary ..................................................................................................................................... 201
Amazon VPC ....................................................................................................................................... 201
How Amazon Virtual Private Cloud Differs for AWS GovCloud (US) ................................................... 201
Documentation for Amazon Virtual Private Cloud .............................................................................. 201
ITAR Boundary ..................................................................................................................................... 201
AWS Site-to-Site VPN .......................................................................................................................... 202
How Site-to-Site VPN Differs for AWS GovCloud (US) ..................................................................... 202
Documentation for AWS Site-to-Site VPN ......................................................................................... 202
ITAR Boundary ..................................................................................................................................... 202
AWS WAF .......................................................................................................................................... 203
How AWS WAF Differs for AWS GovCloud (US) ................................................................................ 203
Documentation for AWS WAF ............................................................................................................ 203
ITAR Boundary ..................................................................................................................................... 203
Amazon WorkSpaces ............................................................................................................................ 204
How Amazon WorkSpaces Differs for AWS GovCloud (US) ................................................................. 204
Documentation for Amazon WorkSpaces ............................................................................................. 204
ITAR Boundary ..................................................................................................................................... 204
AWS X-Ray ......................................................................................................................................... 205
How AWS X-Ray Differs for AWS GovCloud (US) .............................................................................. 205
Documentation for AWS X-Ray ........................................................................................................... 205
ITAR Boundary ..................................................................................................................................... 205
Troubleshooting ................................................................................................................................. 206
Client.UnsupportedOperation: Instances can only be launched within Amazon VPC in this region ................................................................................................................................. 206
Related Resources ............................................................................................................................... 207
New to AWS ......................................................................................................................................... 207
Experienced with AWS .......................................................................................................................... 208
Welcome

The *AWS GovCloud (US) User Guide* provides information about setting up your AWS GovCloud (US) account, identifies the differences between AWS GovCloud (US) Regions and other standard AWS Regions, defines usage guidelines for processing export-controlled data within AWS GovCloud (US), and setting up and using AWS Services in the AWS GovCloud (US) Regions. In this guide, the term AWS GovCloud (US) Regions refer to both AWS GovCloud (US-West) and AWS GovCloud (US-East) Regions. In this guide, we assume you are familiar with Amazon Web Services (AWS).

For a list of AWS or AWS GovCloud (US) related resources, see Related Resources (p. 207).

More information related to the releases in AWS GovCloud (US) can be found at What’s new with AWS GovCloud (US).
What Is AWS GovCloud (US)?

AWS GovCloud (US) are isolated AWS Regions designed to allow U.S. government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements, including Federal Risk and Management Program (FedRAMP) High Department of Defense Security Requirements Guide (DoD SRG) Impact Level 5, and Criminal Justice Services (CJIS). The AWS GovCloud (US) 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 AWS GovCloud (US). For a list of compliance frameworks, see AWS GovCloud (US) Security. AWS GovCloud (US) supports the management of regulated data by offering the following features:

- Restricting physical and logical administrative access to AWS personnel that are U.S. citizens only.
- Providing FIPS 140-2 endpoints. (For details on each service, see the Service Endpoints (p. 62) section.)

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

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 AWS GovCloud (US) Regions and other AWS Regions, and defines usage guidelines for processing ITAR-regulated data within the AWS GovCloud (US). This guide assumes that you are familiar with Amazon Web Services (AWS).

Additional resources:
- For pricing information, see AWS GovCloud (US) Pricing.
- For information about the differences between AWS GovCloud (US) Regions and other AWS Regions, see AWS GovCloud (US) Compared to Standard AWS Regions (p. 2).
- For more information about meeting US Government compliance requirements please, see AWS GovCloud (US).
- For a list of AWS or AWS GovCloud (US)–related resources, see Related Resources (p. 207).

AWS GovCloud (US) Compared to Standard AWS Regions

AWS GovCloud (US) are isolated AWS Regions designed to allow U.S. government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements, including Federal Risk and Management Program (FedRAMP) High, Department of Defense Security Requirements Guide (DoD SRG) Impact Level 5, and Criminal Justice Services (CJIS). The AWS GovCloud (US) adheres to U.S. International Traffic in Arms Regulations (ITAR) requirements.

- AWS GovCloud (US) uses FIPS 140-2 approved cryptographic modules for all AWS service API endpoints, unless otherwise indicated in the Service Endpoints (p. 62) section.
AWS GovCloud (US) User Guide
Differences with Standard AWS Accounts

AWS GovCloud (US) 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. 79).

The AWS GovCloud (US) Regions are physically isolated and have logical network isolation from all other AWS Regions.

AWS restricts all physical and logical access for those staff supporting AWS GovCloud (US) to US Citizens. AWS allows only vetted U.S. citizens with distinct access controls separate from other AWS Regions to administer AWS GovCloud (US). 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 export-controlled data.

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

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

Sign up

During the sign-up process, each customer is reviewed to determine if they are a U.S. entity (such as a government body, contracting company, or educational organization) where account credentials will be managed by a U.S. Person.

Endpoints

AWS GovCloud (US) uses endpoints that are specific to AWS GovCloud (US) and are publicly available from the Internet but are accessible only to AWS GovCloud (US) customers. For a list of these endpoints, see Service Endpoints (p. 62).

Credentials

You can access AWS GovCloud (US) only with AWS GovCloud (US) credentials (AWS GovCloud (US) account access key and AWS GovCloud (US) IAM user credentials). You cannot access AWS GovCloud (US) with standard AWS credentials. Likewise, you cannot access standard AWS Regions using AWS GovCloud (US) credentials.

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 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. 5).

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 AWS standard account only.

Services

Services in the AWS GovCloud (US) Regions 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) Regions, see Using AWS GovCloud (US) Regions (p. 32).

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 AWS GovCloud (US) 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. For more information about Billing and Cost Management, see the AWS Billing and Cost Management documentation.

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 AWS 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:
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) Regions, 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. 5)
- Onboarding to AWS GovCloud (US) (Direct Customers) (p. 9)
- Onboarding to AWS GovCloud (US) as a Solution Provider reselling in AWS GovCloud (US) (p. 11)
- Enabling Multi-Factor Authentication (MFA) (p. 16)
- Signing Up for AWS GovCloud (US) Customer Support (p. 17)

Signing Up for AWS GovCloud (US)

In order to sign up for an AWS GovCloud (US) account, you need to be an individual or entity that meets the requirement of AWS GovCloud (US).

- The account holder must be a U.S. entity incorporated to do business in the United States and is based on U.S. soil.
- The account holder must be a U.S. Person defined as a U.S. Citizen or active Green Card holder.
- The account holder must be able to handle International Traffic and Arms Regulation (ITAR) export controlled data.

AWS GovCloud (US) accounts are associated with standard AWS accounts for billing, service and support purposes. Customers are required to have an existing standard account before signing up for an AWS GovCloud (US) account. We recommend creating a new AWS account that will only be used for AWS GovCloud (US) sign up and billing (i.e. do not deploy any AWS workloads into AWS standard account). A dedicated AWS account for the new AWS GovCloud (US) account will enable you to transfer the AWS GovCloud (US) account to another party in the future and fully close the AWS GovCloud (US) accounts without affecting your other AWS workloads.
If you are using AWS Organizations to manage accounts within AWS standard regions, you can create the new standard account from AWS Organizations console or using the AWS Organizations API. You can create AWS GovCloud (US) accounts from your standard Organization but aren't able to manage AWS GovCloud (US) accounts from your existing Organization within the standard regions, only the account that is mapped to the AWS GovCloud (US) account. You can create a new AWS Organizations within the AWS GovCloud (US) partition by creating a set of new accounts, creating a new AWS Organization root within one of the new accounts, and inviting the other AWS GovCloud (US) accounts to the new AWS Organization. Follow the steps for inviting accounts to an organization here. This will result in separate AWS Organizations one in each partition.
AWS Standard Regions

Standard Organization
Root Account

Governments
Product

Products
Creating an AWS GovCloud (US) from a standalone AWS account

If you are a direct customer of AWS and do not purchase AWS through an AWS Solution Provider or an AWS Reseller, follow the steps below. If you are using AWS Organizations to manage accounts, we recommend using the AWS Organizations API.

1. Create a new AWS standard account by signing up for a new account.
2. Log in to the new AWS Account with the root credentials. If you do not have the root credentials, create a support ticket to recover the credentials.
3. Navigate to the "My Account" page at the top right of the AWS Console.
4. At the bottom of the "My Account" page, there will be a GovCloud (US) section. If you do not see this section, ensure you logged in with the root credentials otherwise, create a support ticket. Click “Sign up for AWS GovCloud (US).”
5. This will navigate you to the AWS GovCloud (US) Sign Up Portal where it will ask you to accept the AWS GovCloud (US) legal agreement and provide additional information, so we can verify your eligibility for an AWS GovCloud (US) account.

Creating an AWS GovCloud (US) with AWS Organizations

AWS Organizations helps you centrally govern your environment as you grow and scale your workloads on AWS. AWS Organizations manages a set of accounts within each partition and can help create accounts across partitions. For example, you can create an AWS Organizations within the AWS US Standard regions to manage accounts in those regions. You will need to create a separate AWS Organizations in AWS GovCloud (US) to manage accounts in the AWS GovCloud (US) partition.
Creating an AWS GovCloud (US) account through a Reseller or Solution Provider

Contact your AWS Solution Provider or AWS Reseller to sign up for an AWS GovCloud (US) account.

Solution Providers or Resellers

If you are a Solution Provider and wish to resell Authorized Services in the AWS GovCloud (US) Regions please contact your AWS business representative by going to the AWS GovCloud (US) Contact Us page and completing the form to start the sign-up process.

AWS Marketplace

Software vendors who want to be listed in the AWS Marketplace for AWS GovCloud (US) must have a direct agreement with AWS. Software vendors who want to be listed in the AWS GovCloud (US) Region should sign up as a Direct Customer whether they are resellers or not.

Onboarding to AWS GovCloud (US) (Direct Customers)

AWS Direct Customers can follow the steps outlined in Configuring Your Account to set up their GovCloud accounts and ensure CloudTrail is enabled.

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 IAM administrator user credentials. For your user name, type Administrator.
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 user 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 GovCloud account root user. 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.
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-xxxxxxxxxxxx" where xxxxxxxxxxx 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:

   ```json
   {
   "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) as a Solution Provider reselling in AWS GovCloud (US)

If you are serving as a Solution Provider and reselling in AWS GovCloud (US), you must create an IAM user to sign in to the AWS Management Console for the AWS GovCloud (US) Region. If you received your account credentials through a Solution Provider, please contact your Solution Provider to sign up.

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 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 IAM 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 can assign a virtual or hardware MFA device to an IAM user or to your GovCloud administrator IAM user. 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. MFA devices are only supported for IAM users and not the root account. For more information, see AWS Management Console documentation.

2. Get an MFA token device. You can enable only one MFA device per 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 in the "Hardware Key Fob MFA Device for AWS GovCloud (US)" column of the MFA Form Factors table on 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.

3. 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, 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

4. 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) Regions. 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 U.S. citizens are needed, AWS can route cases to U.S. citizen support engineers. Customers can also choose to use general support resources for basic support cases that do not contain sensitive (that is, export controlled) data. 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 account root user credentials that were used to sign up for 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 AWS GovCloud (US) Region Support Center with your AWS GovCloud (US) credentials. Do not enter any export controlled data in the case.
Customer Support Differences for the AWS GovCloud (US) Regions

- The AWS Trusted Advisor is available in AWS GovCloud (US). Attachments are not allowed.
- Some Premium Support features, such as some AWS Trusted Advisor (p. 195) checks, are not available for your AWS GovCloud (US) account.
- The Service Health Dashboard for the AWS GovCloud (US) Region can be found at http://status.aws.amazon.com/govcloud.
- The AWS GovCloud (US) Regions do not have a dedicated forum area.
- The endpoint to access AWS Support is: https://support.us-gov-west-1.amazonaws.com.
Setting Up AWS GovCloud (US) with AWS Services Outside of the AWS GovCloud (US) Regions

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) or Resources (p. 19)
- Setting Up Amazon Route 53 with Your AWS GovCloud (US) Resources (p. 20)
- Setting Up Amazon Route 53 Zone Apex Support with an AWS GovCloud (US) Elastic Load Balancing Load Balancer (p. 21)

Setting Up Amazon CloudFront with Your AWS GovCloud (US) or 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) Regions, using CloudFront with your AWS GovCloud (US) resources is analogous to using CloudFront with a non-AWS origin server.

Topics
- Credentials (p. 19)
- Tips for Setting Up CloudFront (p. 20)

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. 5) 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.
- It is important to note that CloudFront is located outside of the AWS GovCloud (US) boundary and customers should not enter or store ITAR-controlled data in the service.
**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 AWS GovCloud (US) Regions, CloudFront is not within the ITAR boundary. If you want to use CloudFront to distribute your export-controlled data, encrypt your content in transit.
- Integrated support for CloudFront Live Streaming is not available for origins located in the AWS GovCloud (US) Regions.
- 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.

**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 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) Regions.

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. 5) 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-West) or AWS GovCloud (US-East) 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-West) or AWS GovCloud (US-East) credentials.

• You will set up Route 53 to route end users to your AWS GovCloud (US-West) or AWS GovCloud (US-East) resources.

• Route 53 is not within the AWS GovCloud (US) Regions 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 export-controlled data.

• To use Route 53 public DNS to respond to internet DNS queries for resources that you created using a GovCloud account, you must create a public hosted zone using a global AWS account, and create records in the hosted zone that specify the GovCloud resources.

If you want to use the Route 53 console to route traffic to resources in the GovCloud Region, such as an ELB load balancer or an S3 bucket, you can't choose the resource from the Alias Target list. You must enter the applicable domain name in the Alias Target field. For information about which value to specify for each type of resource and where to get that value, see Values for Alias Records documentation in the Amazon Route 53 Developer Guide.

• To use Route 53 private DNS to respond to DNS queries from VPCs in GovCloud, you must create a private hosted zone using a GovCloud 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

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. 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) Regions, you must have an AWS GovCloud (US) account. If you don’t have an account, see Signing Up for AWS GovCloud (US) (p. 5) 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 a new target group. Confirm that the instances are healthy and registered. 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.

Hello World / GovCloud Web Server 01

Backend instance ip: 160.
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. Since the CloudFront service is hosted outside the AWS GovCloud (US) Regions, customers should ensure any content hosted in the CloudFront service does not contain export-controlled information.

1. Sign in to the CloudFront console with your standard AWS account, and choose Create Distribution.

2. Select the Get Started under 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. Note you must attach a trusted certificate that validates your authorization to use the domain 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.
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. Under your root domain, create a new record.
3. Under the routing policy, select Simple routing and click Next.

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.
Introducing the new Route 53 console
We've redesigned the Route 53 console to make it easier to use. Let us know what you think. On

Step 1
Choose routing policy

Step 2
Configure records

Choose routing policy

The routing policy determines how Amazon Route 53 will distribute traffic to resources.

Routing policy

- **Simple routing**
  Use if you're routing traffic to just one resource, such as a webserver.

- **Weighted**
  Use when you have multiple resources that do the same job, and you want to specify the proportion of traffic that goes to each resource. For example, two or more EC2 instances.

- **Latency**
  Use when you have resources in multiple AWS Regions and you want to route traffic to the Region that provides the best latency.

- **Failover**
  Use to route traffic to a resource until the resource is healthy, or to route traffic to a different resource when the first resource is unhealthy.
4. Choose Define simple record. In the “Value/Route traffic to” drop down, select “Alias to CloudFront distribution”. Click in the “Choose Distribution” search box and select the distribution created in the prior step.

![Define simple record](image)

5. On the overview, click on Create records.

**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) Regions.

For more information about Route 53, see the Route 53 documentation.
Using AWS GovCloud (US) Regions

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

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 GovCloud (US) Regions (p. 32)
- Paths in ARNs (p. 62)
- Service Endpoints (p. 62)
- VPC Endpoints (p. 75)
- Maintaining U.S. International Traffic in Arms Regulations (ITAR) Compliance (p. 79)
- Accessing the AWS GovCloud (US) Regions (p. 79)
- Controlling Access to Your AWS GovCloud (US) Account (p. 80)
- Command Line and API Access (p. 80)
- Resource Limits (p. 81)
- Penetration Testing (p. 81)
- Service Health Dashboard (p. 81)
- Closing an AWS GovCloud (US) Account (p. 81)

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

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 AWS GovCloud (US) Regions, ARNs have an identifier that is different from the one in other standard AWS Regions. For all other standard regions, ARNs begin with:

```
arn:aws
```

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

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

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

Topics
- ARN Format (p. 34)
- Example ARNs (p. 35)
- Amazon Athena (p. 36)
• Amazon AppStream 2.0 (p. 36)
• AWS Artifact (p. 36)
• Amazon Aurora (p. 37)
• Amazon EC2 Auto Scaling (p. 37)
• AWS Batch (p. 37)
• AWS Backup (p. 37)
• AWS Certificate Manager (p. 38)
• AWS Certificate Manager Private Certificate Authority (p. 38)
• Amazon Cloud Directory (p. 39)
• Amazon CloudWatch Events (p. 39)
• AWS CodeBuild (p. 39)
• AWS CodeCommit (p. 40)
• AWS CodeDeploy (p. 40)
• AWS CodePipeline (p. 40)
• Amazon Cognito (p. 41)
• Amazon Comprehend (p. 41)
• Amazon Comprehend Medical (p. 41)
• AWS Config (p. 41)
• AWS DataSync (p. 42)
• AWS Database Migration Service (p. 42)
• AWS Directory Service (p. 42)
• Amazon DocumentDB (with MongoDB compatibility) (p. 42)
• Amazon DynamoDB (p. 43)
• AWS Elastic Beanstalk (p. 43)
• Amazon Elastic Compute Cloud (p. 44)
• Amazon Elastic Compute Cloud Image Builder (p. 44)
• Amazon Elastic Container Registry (p. 44)
• Amazon Elastic Container Service (p. 44)
• Amazon Elastic File System (p. 45)
• Amazon Elastic Kubernetes Service (p. 45)
• Amazon Elasticsearch Service (p. 46)
• Amazon EventBridge (p. 46)
• AWS Glue (p. 46)
• Amazon GuardDuty (p. 47)
• AWS Health (p. 47)
• AWS Identity and Access Management (p. 47)
• Amazon Inspector (p. 48)
• AWS IoT Core (p. 49)
• AWS IoT Device Defender (p. 49)
• AWS IoT Device Management (p. 50)
• AWS IoT Greengrass (p. 50)
• Amazon Kinesis Data Firehose (p. 51)
• Amazon Kinesis Data Analytics (p. 51)
• Amazon Kinesis Data Streams (p. 52)
• AWS Lambda (p. 52)
• AWS Elemental MediaConvert (p. 52)
• Amazon Managed Streaming for Apache Kafka (MSK) (p. 53)
• Amazon Neptune (p. 53)
• AWS Organizations (p. 53)
• AWS Outposts (p. 53)
• Amazon Pinpoint (p. 54)
• Amazon Polly (p. 54)
• Amazon QuickSight (p. 54)
• AWS Resource Access Manager (p. 55)
• Amazon RDS (p. 55)
• Amazon Rekognition (p. 55)
• AWS Resource Groups (p. 56)
• Amazon Route 53 (p. 56)
• Amazon SageMaker (p. 56)
• AWS Security Hub (p. 56)
• AWS Secrets Manager (p. 57)
• AWS Serverless Application Repository (p. 57)
• AWS Service Catalog (p. 58)
• Amazon Simple Email Service (p. 58)
• Amazon Simple Notification Service (p. 58)
• Amazon Simple Queue Service (p. 58)
• Amazon Simple Storage Service (p. 59)
• Amazon Simple Workflow Service (p. 59)
• AWS Step Functions (p. 59)
• AWS Storage Gateway (p. 60)
• AWS Systems Manager (p. 60)
• AWS Transfer Family (p. 60)
• AWS WAF (p. 61)
• Amazon WorkSpaces (p. 61)
• AWS X-Ray (p. 61)

**ARN Format**

Here are some example ARNs:

```plaintext
<!-- 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
```
**partition**

The service namespace that identifies the AWS partition (for example, for AWS GovCloud (US) it is aws-us-gov. For a list of namespaces, see [AWS Service Namespaces](https://docs.aws.amazon.com/en_us/general/latest/gr/aws-service-namespaces.html) in the *Amazon Web Services General Reference*.

**service**

The service namespace that identifies the AWS product (for example, Amazon S3 or IAM). For a list of namespaces, see [AWS Service Namespaces](https://docs.aws.amazon.com/en_us/general/latest/gr/aws-service-namespaces.html) 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-West) Region, the region is us-gov-west-1. For the AWS GovCloud (US-East) Region, the region is us-gov-east-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](https://docs.aws.amazon.com/en_us/general/latest/gr/aws-arns-and-namespaces.html#arn-structure) (p. 62).

### Example ARNs

The following sections provide syntax and examples of the ARNs for AWS GovCloud (US-West) and AWS GovCloud (US-East) 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. 35)

### Amazon API Gateway

**Syntax:**

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

**Examples:**

```
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
```

```
arn:aws-us-gov:apigateway:us-gov-east-1::/restapis/a123456789012bc3de45678901f23a45/*
arn:aws-us-gov:apigateway:us-gov-east-1::a123456789012bc3de45678901f23a45:/test/mydemoresource/*
arn:aws-us-gov:apigateway::a123456789012bc3de45678901f23a45:/*/petstorewalkthrough/pets
```
Amazon Athena

Syntax:

```
```

Example

```
```

```
```

Amazon AppStream 2.0

Syntax:

```
```

Examples:

```
```

```
```

```
```

```
```

AWS Artifact

Syntax:

```
arn:aws-us-gov:artifact:::agreement:/agreement_arn
arn:aws-us-gov:artifact::account-id:customer-agreement:/
arn:aws-us-gov:artifact:::report-package/:/report_package_arn:/SOC:/
arn:aws-us-gov:iam::*:role/service-role/AWSArtifactAccountSync
arn:aws-us-gov:iam::aws:policy/service-role/AWSArtifactAccountSync
```

Examples:

```
arn:aws-us-gov:artifact:::agreement/*
arn:aws-us-gov:artifact::agreement/AWS Business Associate Addendum
arn:aws-us-gov:artifact::123456789012:customer-agreement/*
arn:aws-us-gov:artifact::report-package/Certifications and Attestations/SOC/*
arn:aws-us-gov:artifact::report-package/Alignment Documents/Laws and Regulations/Form W-9
arn:aws-us-gov:iam::*:role/service-role/AWSArtifactAccountSync
arn:aws-us-gov:iam::aws:policy/service-role/AWSArtifactAccountSync
```
Amazon Aurora

Syntax:

```
arn:aws-us-gov:rds:region:account number:resourcetype:name
```

Examples:

```
```

Amazon EC2 Auto Scaling

Syntax:

```
```

```
```

Examples:

```
```

```
```

AWS Batch

Syntax:

```
arn:aws-us-gov:batch:region:accound-id:job-queue/JobQueueName
```

```
arn:aws-us-gov:batch:region:accound-id:jobdefinitionname/JobDefinitionName:revision
```

Examples:

```
```

```
```

AWS Backup

Syntax:

```
arn:aws-us-gov:backup:region:*
```

Examples:
AWS Certificate Manager

Syntax:

```
```

Examples:

```
```

```
```

AWS Certificate Manager Private Certificate Authority

Syntax:

```
```

Example:

```
Example:

| Example: | Arn: Aws-us-gov:acm-pca::template/SubordinateCACertificate_PathLen0/V1 |

### Amazon Cloud Directory

**Syntax:**


**Examples:**

| Examples: | Arn: Aws-us-gov:clouddirectory:us-west-1:123456789012:directory/ariqk1hd-ujdtmcirjhevpi/schema/deviceregistryschema/1.0/xyz |

### Amazon CloudWatch Events

**Syntax:**

| Syntax: | Arn: Aws-us-gov:events:region:*:* |

**Examples:**

| Examples: | Arn: Aws-us-gov:events:us-gov-west-1:*:* |

| Examples: | Arn: Aws-us-gov:events:us-gov-east-1:*:* |

### AWS CodeBuild

**Syntax:**

| Syntax: | Arn: Aws-us-gov:codebuild:* |
**AWS CodeCommit**

Syntax:

```
arn:aws-us-gov:codecommit:*  
arn:aws-us-gov:codecommit:region:account:repository name
```

Example:

```
```

**AWS CodeDeploy**

Syntax:

```
```

Examples:

```
arn:aws-us-gov:codedeploy:*  
arn:aws-us-gov:codedeploy:us-gov-west-1:123456789012:*  
arn:aws-us-gov:codedeploy:us-gov-west-1:123456789012:deploymentgroup/deployment-group-name  
```

**AWS CodePipeline**

Syntax:

```
```

Examples:

```
arn:aws-us-gov:codepipeline:*  
arn:aws-us-gov:codepipeline:us-gov-west-1:123456789012:*  
arn:aws-us-gov:codepipeline:us-gov-west-1:123456789012:pipeline-name  
arn:aws-us-gov:codepipeline:us-gov-west-1:123456789012:pipeline-name/stage-name
```
Amazon Cognito

Syntax:

```
```

Example:

```
```

Amazon Comprehend

Syntax:

```
ar:nwa-us-gov:comprehend:region:account-id:comprehend tool/file or resource id
```

Example:

```
```

Amazon Comprehend Medical

Syntax:

```
ar:nwa-us-gov:comprehendmedical:region:account-id:comprehend medical tool/file or resource id
```

Example:

```
```

AWS Config

Syntax:

```
ar:nwa-us-gov:config:region:account-id:config-rule/config-rule-name
```

Examples:

```
```
AWS DataSync

Syntax:


Examples:

`arn:aws-us-gov:datasync:us-gov-west-1:209870788375:agent/agent-09bf4d0be979c1154`

`arn:aws-us-gov:datasync:us-gov-east-1:209870788375:agent/agent-09bf4d0be979c1154`

AWS Database Migration Service

Syntax:


Examples:


AWS Directory Service

Syntax:

`arn:aws-us-gov:ds:region:account-id:directory/directoryId`

Examples:


Amazon DocumentDB (with MongoDB compatibility)

Syntax:


aws:rds:region:account-id:cluster-snapshot:resource_id

aws:rds:region:account-id:subgrp:resource_id

Examples:

aws:rds:us-east-1:123456789012:db:sample-db-instance
aws:rds:us-east-1:123456789012:cluster:sample-db-cluster
aws:rds:us-east-1:123456789012:cluster-pg:sample-db-cluster-parameter-group
aws:rds:us-east-1:123456789012:secgrp:sample-public-secgrp
aws:rds:us-east-1:123456789012:cluster-snapshot:sample-db-cluster-snapshot
aws:rds:us-east-1:123456789012:subgrp:sample-subnet-10

Amazon DynamoDB

Syntax:


Examples:


AWS Elastic Beanstalk

Syntax:

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

Examples:

arn:aws-us-gov:elasticbeanstalk:us-west-2:123456789012:platform/MyFlatPlatform/1.0
arn:aws-us-gov:elasticbeanstalk:us-west-2::solutionstack/32bit Amazon Linux running Tomcat 7

Examples:
Amazon Elastic Compute Cloud

Syntax:

```plaintext
arn:aws-us-gov:ec2:region:account:placement-group:placement-group-name
```

Examples:

```plaintext

```

Amazon Elastic Compute Cloud Image Builder

Syntax:

```plaintext
```

Examples:

```plaintext
arn:aws-us-gov:imagebuilder:us-gov-west-1:123456789012:component:my-component/1.2.3/1
```

Amazon Elastic Container Registry

Syntax:

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

Examples:

```plaintext
arn:aws-us-gov:ecr:us-gov-west-1:123456789012:repository/my-repository

arn:aws-us-gov:ecr:us-gov-east-1:123456789012:repository/my-repository
```

Amazon Elastic Container Service

Syntax:
### Amazon Elastic File System

**Syntax:**

```yaml
```

**Examples:**

```yaml
arn:aws-us-gov:elasticfilesystem:us-gov-west-1:012345678901:file-system/fs-f00df00d
```

### Amazon Elastic Kubernetes Service

**Syntax:**

```yaml
```

**Examples:**

```yaml
arn:aws-us-gov:eks:us-gov-west-1:123456789012:nodegroup/my-cluster/my-nodegroup/e0b84a29-dacb-052c-33e9-1b6b4595d1aa
```
Amazon Elasticsearch Service

Syntax:


Examples:


Amazon EventBridge

Syntax:

arn:aws-us-gov:events:region:*:*

Examples:

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

arn:aws-us-gov:events:us-gov-east-1:*:*
arn:aws-us-gov:events:us-gov-east-1:123456789012:*

AWS Glue

Syntax:

arn:aws-us-gov:glue:region:account-id:typeresource_path

Examples:

arn:aws-us-gov:glue:us-gov-west-1:123456789012:database/db1
Amazon GuardDuty

Syntax:

```
```

Examples:

```
arn:aws-us-gov:guardduty:us-gov-west-1:detector/12abc34d567e8fa901bc2d34e56789f0
arn:aws-us-gov:guardduty:us-gov-west-1:123456789012:ipset/0cb0141ab9fbde177613ab9436212e90
arn:aws-us-gov:guardduty:us-gov-west-1:123456789012:threatintelset/12a34567890bc1de2345f67ab8901234
```

AWS Health

Syntax:

```
arn:aws-us-gov:health:region::event/SERVICE/EVENT_TYPE/EVENT_ID
```

Examples:

```
```

AWS Identity and Access Management

Syntax:

```
arn:aws-us-gov:iam:region:account-id:user/username
arn:aws-us-gov:iam:region:account-id:role/rolename
arn:aws-us-gov:sts:region:account-id:federated-user/username
```
Examples:

```
```

Amazon Inspector

Syntax:

```
```

Examples:

```
arn:aws-us-gov:inspector:us-gov-west-1:123456789012:target/0-SbqF87sd/template/0-ltAhR4vg/run/0-IABgH9tK
arn:aws-us-gov:inspector:us-gov-east-1:123456789012:target/0-SbqF87sd/template/0-ltAhR4vg/run/0-IABgH9tK
```
AWS GovCloud (US) User Guide
AWS IoT Core

----------


AWS IoT Core

Syntax:

```
arn:aws-us-gov:iot:region:account-id:index/index-id
arn:aws-us-gov:iot:region:account-id:index/index-name
arn:aws-us-gov:iot:region:account-id:role/role-name
arn:aws-us-gov:iot:region:account-id:rule/rule-name
arn:aws-us-gov:iot:region:account-id:thinggroup/thing-group-name
arn:aws-us-gov:iot:region:account-id:thingtype/thing-type-name
```

Examples:

```
arn:aws-us-gov:iot:us-gov-west-1:123456789012:authorizer/my_authorizer_function_name
arn:aws-us-gov:iot:us-gov-west-1:123456789012:index/my_index_id
arn:aws-us-gov:iot:us-gov-west-1:123456789012:role/role_name
arn:aws-us-gov:iot:us-gov-west-1:123456789012:rolealias/role_alias_name
arn:aws-us-gov:iot:us-gov-west-1:123456789012:rule/my_rule_name
arn:aws-us-gov:iot:us-gov-west-1:123456789012:thing/my_thing_name
arn:aws-us-gov:iot:us-gov-west-1:123456789012:thinggroup/my_thing_group_name
arn:aws-us-gov:iot:us-gov-west-1:123456789012:thingtype/my_thing_type_name
```

AWS IoT Device Defender

Syntax:

```
arn:aws-us-gov:iot:region:account-id:index/index-id
arn:aws-us-gov:iot:region:account-id:index/index-name
arn:aws-us-gov:iot:region:account-id:role/role-name
arn:aws-us-gov:iot:region:account-id:rule/rule-name
arn:aws-us-gov:iot:region:account-id:thinggroup/thing-group-name
arn:aws-us-gov:iot:region:account-id:thingtype/thing-type-name
```

Examples:

```
arn:aws-us-gov:iot:us-gov-west-1:123456789012:authorizer/my_authorizer_function_name
```
AWS IoT Device Management

Syntax:

<table>
<thead>
<tr>
<th>ARN Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>arn:aws-us-gov:iot:region:account-id:index/index-id</td>
</tr>
<tr>
<td>arn:aws-us-gov:iot:region:account-id:index/index-name</td>
</tr>
<tr>
<td>arn:aws-us-gov:iot:region:account-id:role/role-name</td>
</tr>
<tr>
<td>arn:aws-us-gov:iot:region:account-id:rule/rule-name</td>
</tr>
<tr>
<td>arn:aws-us-gov:iot:region:account-id:thinggroup/thing-group-name</td>
</tr>
<tr>
<td>arn:aws-us-gov:iot:region:account-id:thingtype/thing-type-name</td>
</tr>
</tbody>
</table>

Examples:

<table>
<thead>
<tr>
<th>ARN Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>arn:aws-us-gov:iot:us-gov-west-1:123456789012:authorizer/my_authorizer_function_name</td>
</tr>
<tr>
<td>arn:aws-us-gov:iot:us-gov-west-1:123456789012:index/my_index_id</td>
</tr>
<tr>
<td>arn:aws-us-gov:iot:us-gov-west-1:123456789012:index/my_index_name</td>
</tr>
<tr>
<td>arn:aws-us-gov:iot:us-gov-west-1:123456789012:role/my_role_name</td>
</tr>
<tr>
<td>arn:aws-us-gov:iot:us-gov-west-1:123456789012:rolealias/my_role_alias_name</td>
</tr>
<tr>
<td>arn:aws-us-gov:iot:us-gov-west-1:123456789012:rule/my_rule_name</td>
</tr>
<tr>
<td>arn:aws-us-gov:iot:us-gov-west-1:123456789012:thing/my_thing_name</td>
</tr>
<tr>
<td>arn:aws-us-gov:iot:us-gov-west-1:123456789012:thinggroup/my_thing_group_name</td>
</tr>
<tr>
<td>arn:aws-us-gov:iot:us-gov-west-1:123456789012:thingtype/my_thing_type_name</td>
</tr>
</tbody>
</table>

* Please note the ARN syntax is the same for AWS IoT

AWS IoT Greengrass

Syntax:

<table>
<thead>
<tr>
<th>ARN Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>arn:aws-us-gov:greengrass:region:account-id:greengrass/groups/group-id</td>
</tr>
<tr>
<td>arn:aws-us-gov:greengrass:region:account-id:greengrass/groups/group-id/certificateauthorities/certificate-fingerprint</td>
</tr>
<tr>
<td>arn:aws-us-gov:greengrass:region:account-id:greengrass/groups/group-id/deployments/deployment-id</td>
</tr>
<tr>
<td>arn:aws-us-gov:greengrass:region:account-id:greengrass/groups/group-id/versions/group-version-id</td>
</tr>
</tbody>
</table>

50
Amazon Kinesis Data Firehose

Syntax:

```
```

Examples:

```
```

Amazon Kinesis Data Analytics

Syntax:

```
```

Examples:

```
```
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:

```

```

AWS Elemental MediaConvert

Syntax:

```
arn:aws-us-gov:mediaconvert:region:account-id:jobTemplates/jobTemplateName
arn:aws-us-gov:mediaconvert:region:account-id:presets/presetName
arn:aws-us-gov:mediaconvert:region:account-id:queues/queueName
```

Examples:

```
```
Amazon Managed Streaming for Apache Kafka (MSK)

Syntax:

```
arn:aws-us-gov:service:region:account-id:cluster/cluster-name/ID
```

```
arn:aws-us-gov:service:region:account-id:configuration/config-name/ID
```

Examples:

```
arn:aws-us-gov:kafka:us-gov-east-1:123456789012:cluster/TestCluster-03/abcd1234-ab12-7e7e-9999-1234abcd5678-1
```

Amazon Neptune

Syntax:

```
```

Examples:

```
arn:aws-us-gov:neptune:us-gov-west-1:123456789012
```

AWS Organizations

Syntax:

```
arn:aws-us-gov:organizations:master-account-id:organization/o-organization-id
arn:aws-us-gov:organizations:master-account-id:account/o-organization-id/account-id
arn:aws-us-gov:organizations:master-account-id:ou/o-organization-id/ou-organizational-unit-id
arn:aws-us-gov:organizations:master-account-id:handshake/o-organization-id/handshake-type/handshake-id
```

Examples:

```
arn:aws-us-gov:organizations::123456789012:organization/o-a1b2c3d4e5example
arn:aws-us-gov:organizations::123456789012:root/o-a1b2c3d4e5/r-f6g7h8i9j0example
arn:aws-us-gov:organizations::123456789012:account/o-a1b2c3d4e5/123456789012
arn:aws-us-gov:organizations::123456789012:ou/o-a1b2c3d4e5/ou-k9l8m7n6o5example
arn:aws-us-gov:organizations::123456789012:policy/o-a1b2c3d4e5/service_control_policy/p-p4q3r2s1t0example
arn:aws-us-gov:organizations::123456789012:handshake/o-a1b2c3d4e5/invite/h-u2v4w5x8y0example
```

AWS Outposts

Syntax:
Amazon Pinpoint

Syntax:

```
```

Examples:

```
```

Amazon Pinpoint

Syntax:

```
arn:aws-us-gov:mobletargeting:region:account-id:apps/projectId
d
```


```
arn:aws-us-gov:mobletargeting:region:account-id:apps/projectId/campaigns
d
```

```
arn:aws-us-gov:mobletargeting:region:account-id:apps/projectId/journeys/journeyId
d
```

```
arn:aws-us-gov:mobletargeting:region:account-id:templates/templateName/EMAIL
d
```

Examples:

```
```

```
```

```
```

```
arn:aws-us-gov:mobletargeting:us-gov-west-1:123456789012:templates/MyTemplate/EMAIL
d
```

Amazon Polly

Syntax:

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

Examples:

```
```

Amazon QuickSight

Syntax:

```
```

Examples:

```
```
AWS Resource Access Manager

Syntax:

\[ \text{arn:aws-us-gov:ram:region:account-id:resource} \]

Examples:

\[ \text{arn:aws-us-gov:ram:us-gov-west-1:123456789012:resource-share/fds5ung6-44e98-d0bh-6cf4-c00e09177huf} \]
\[ \text{arn:aws-us-gov:ram:us-gov-east-1:123456789012:resource-share/fds5ung6-44e98-d0bh-6cf4-c00e09177huf} \]

Amazon RDS

Syntax:

\[ \text{arn:aws-us-gov:rds:region:account-number:resourcetype:name} \]

Examples:

\[ \text{arn:aws-us-gov:rds:us-gov-west-1:123456789012:db:my-mysql-instance-1} \]
\[ \text{arn:aws-us-gov:rds:us-gov-east-1:123456789012:db:my-mysql-instance-1} \]

Amazon Rekognition

Syntax:

\[ \text{arn:aws-us-gov:rekognition:region:account-id:collection/collection-id} \]
\[ \text{arn:aws-us-gov:rekognition:region:account-id:*} \]

Examples:

\[ \text{arn:aws-us-gov:rekognition:us-gov-west-1:123456789012:mycollection/mycollection-id} \]
\[ \text{arn:aws-us-gov:rekognition:us-gov-west-1:123456789012:mycollection} \]
\[ \text{arn:aws-us-gov:rekognition:us-gov-east-1:123456789012:mycollection/mycollection-id} \]
\[ \text{arn:aws-us-gov:rekognition:us-gov-west-1:123456789012:mycollection} \]
AWS Resource Groups

Syntax:

```
arn:aws-us-gov:resource-groups:region:account-id:group/group-name
```

Examples:

```
```

Amazon Route 53

Syntax:

```
arn:aws:route53:::hostedzone/hostedzoneId
arn:aws:route53:::change/changeId
```

Examples:

```
arn:aws:route53:::hostedzone/Z148QEXAMPLE8V
arn:aws:route53:::change/C2RDJ5EXAMPLE2
arn:aws:route53:::change/*
```

Amazon SageMaker

Syntax:

```
arn:aws-us-gov:sagemaker:region:account-id:notebook-instance/notebookInstanceName
arn:aws-us-gov:sagemaker:region:account-id:notebook-instance-lifecycle-config/notebookInstanceLifecycleConfigName
arn:aws-us-gov:sagemaker:region:account-id:training-job/trainingJobName
arn:aws-us-gov:sagemaker:region:account-id:model/modelName
arn:aws-us-gov:sagemaker:region:account-id:endpointName
arn:aws-us-gov:sagemaker:region:account-id:endpoint-config/endpointConfigName
arn:aws-us-gov:sagemaker:region:account-id:hyper-parameter-tuning-job/hyperParameterTuningJobName
```

Examples:

```
```

AWS Security Hub

Syntax:
AWS GovCloud (US) User Guide

AWS Secrets Manager

Syntax:

Examples:

AWS Serverless Application Repository

Syntax:

Example:
AWS Service Catalog

Syntax:

```
arn:aws-us-gov:servicecatalog:region:account:stack/Provisioned Product Name/Provisioned Product ID
```

Example:

```
```

Amazon Simple Email Service

Syntax:

```
```

Example:

```
arn:aws-us-gov:email:us-gov-west-1:123456789012:identity/sender@example.com
```

Amazon Simple Notification Service

Syntax:

```
arn:aws-us-gov:sns:region:account:topicname
```

Examples:

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

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

Amazon Simple Queue Service

Syntax:

```
arn:aws-us-gov:sqs:region:account:queuename
```

Examples:
Amazon Simple Storage Service

Syntax:

```plaintext
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:

```plaintext
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:

```plaintext
```

Examples:

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

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

AWS Step Functions

Syntax:

```plaintext
```

Examples:

```plaintext

```

59
**AWS Storage Gateway**

**Syntax:**

```
```

**Examples:**

```
arn:aws:storagegateway:us-gov-west-1:123456789012:share/share-7E52E414
arn:aws:storagegateway:us-gov-west-1:123456789012:gateway/gateway-id/volume/vol-004b446472f121a0a
arn:aws:storagegateway:us-gov-west-1:123456789012:gateway/sgw-C0ED0222/device/mytarget
```

**AWS Systems Manager**

**Syntax:**

```
arn:aws-us-gov:ssm:us-gov-west-1:*
arn:aws-us-gov:ssm:region:account-id:
```

**AWS Transfer Family**

**Syntax:**

```
arn:aws-us-gov:transfer:region:account-id:user/server-id/username
```

**Examples:**
AWS WAF

Syntax:

```
```

Examples:

```
arn:aws-us-gov:waf-regional:us-east-1:123456789012:rule/41b5b052-1e4a-426b-8149-3595b6342c2
arn:aws-us-gov:waf-regional:us-east-1:123456789012:ipset/3f74bd8c-f046-4970-a1a7-41aa52e05480
arn:aws-us-gov:waf-regional:us-east-1:123456789012:bytematchset/d131bc0b-57be-4536-af1d-4894fd28acc4
```

Amazon WorkSpaces

Syntax:

```
arn:aws:workspaces:region:account_id:workspace/workspace_identifier
```

Examples:

```
```

AWS X-Ray

Syntax:

```
arn:aws-us-gov:xray:region:account_id:sampling-rule/rule-name
arn:aws-us-gov:xray:region:account_id:group/group-name/id
```

Examples:

```
```
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*`

For more information, see Amazon Resource Names (ARNs) and AWS Service Namespaces.

Service Endpoints

If you access AWS GovCloud (US-West) or AWS GovCloud (US-East) by using the command line interface (CLI) or programmatically by using the APIs, you need the AWS GovCloud (US-West) or AWS GovCloud (US-East) region endpoints. AWS GovCloud (US-West) and AWS GovCloud (US-East) uses FIPS 140-2 validated cryptographic modules to support compliance with FIPS 140-2 in all our HTTPS endpoints unless otherwise noted. For more information about FIPS 140-2, see "Cryptographic Module Validation Program" on the NIST Computer Security Resource Center website.

When using the endpoints, note the following:

- Amazon S3 has the following website endpoint:

<table>
<thead>
<tr>
<th>Website Endpoint</th>
<th>Route 53 Hosted Zone ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>s3-website.us-gov-west-1.amazonaws.com</td>
<td>Z31GFT0UA1I2HV</td>
</tr>
<tr>
<td>s3-website.us-gov-east-1.amazonaws.com</td>
<td>Z2NFVFYYW2VKV1</td>
</tr>
</tbody>
</table>

For a list of all AWS endpoints, see Regions and Endpoints in the AWS General Reference.
Endpoints for the AWS GovCloud (US) Regions

The following table lists each AWS service available in the AWS GovCloud (US) Regions and the corresponding endpoints.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon AppStream 2.0</td>
<td><strong>FIPS</strong>: appstream2-fips.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS</strong>: Not Applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS</strong>: appstream2.us-gov-west-1.amazonaws.com</td>
<td><strong>Non-FIPS</strong>: Not Applicable</td>
<td></td>
</tr>
<tr>
<td>Amazon API Gateway*</td>
<td><strong>FIPS</strong>: apigateway-fips.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS</strong>: apigateway-fips.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS</strong>: apigateway.us-gov-west-1.amazonaws.com</td>
<td><strong>Non-FIPS</strong>: apigateway.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td>AWS Artifact</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td></td>
</tr>
<tr>
<td>Amazon Athena</td>
<td><strong>FIPS</strong>: athena-fips.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS</strong>: athena-fips.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS</strong>: athena.us-gov-west-1.amazonaws.com</td>
<td><strong>Non-FIPS</strong>: athena.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td>Amazon Aurora</td>
<td><strong>FIPS</strong>: rds.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS</strong>: rds.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS</strong>: Not applicable</td>
<td><strong>Non-FIPS</strong>: Not applicable</td>
<td></td>
</tr>
<tr>
<td>AWS Auto Scaling</td>
<td><strong>FIPS</strong>: autoscaling-plans.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS</strong>: autoscaling-plans.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS</strong>: Not applicable</td>
<td><strong>Non-FIPS</strong>: Not applicable</td>
<td></td>
</tr>
<tr>
<td>Application Auto Scaling</td>
<td><strong>FIPS</strong>: application-autoscaling.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS</strong>: application-autoscaling.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS</strong>: Not applicable</td>
<td><strong>Non-FIPS</strong>: Not applicable</td>
<td></td>
</tr>
<tr>
<td>Amazon EC2 Auto Scaling</td>
<td><strong>FIPS</strong>: autoscaling.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS</strong>: autoscaling.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS</strong>: Not applicable</td>
<td><strong>Non-FIPS</strong>: Not applicable</td>
<td></td>
</tr>
<tr>
<td>AWS Batch</td>
<td><strong>FIPS</strong>: batch.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS</strong>: batch.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS</strong>: Not applicable</td>
<td><strong>Non-FIPS</strong>: Not applicable</td>
<td></td>
</tr>
<tr>
<td>AWS Backup</td>
<td><strong>FIPS</strong>: backup-fips.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS</strong>: backup-fips.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS</strong>: backup.us-gov-west-1.amazonaws.com</td>
<td><strong>Non-FIPS</strong>: backup.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Private Certificate Authority</td>
<td>FIPS: Not applicable</td>
<td>FIPS: acm.pca.us-gov-east-1.amazonaws.com</td>
<td>FIPS: Not applicable</td>
</tr>
<tr>
<td>Amazon Cloud Directory</td>
<td>FIPS: clouddirectory.us-gov-west-1.amazonaws.com</td>
<td>Not applicable</td>
<td>Non-FIPS: Not Applicable</td>
</tr>
<tr>
<td>AWS CloudHSM</td>
<td>FIPS: Not applicable</td>
<td>FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
</tr>
<tr>
<td>AWS CloudHSM Classic</td>
<td>FIPS: Not applicable</td>
<td>Not applicable</td>
<td>Non-FIPS: Not applicable</td>
</tr>
<tr>
<td>Amazon CloudWatch Events</td>
<td>FIPS: events.us-gov-west-1.amazonaws.com</td>
<td>FIPS: events.us-gov-east-1.amazonaws.com</td>
<td>Non-FIPS: Not applicable</td>
</tr>
<tr>
<td>Amazon CloudWatch Logs</td>
<td>FIPS: logs.us-gov-west-1.amazonaws.com</td>
<td>FIPS: logs.us-gov-east-1.amazonaws.com</td>
<td>Non-FIPS: Not applicable</td>
</tr>
<tr>
<td>Amazon Comprehend Medical</td>
<td>FIPS: comprehendmedical-fips.us-gov-west-1.amazonaws.com</td>
<td>FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
</tr>
</tbody>
</table>
### AWS GovCloud (US) User Guide

#### Service Endpoints

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS CodeBuild</td>
<td><strong>FIPS:</strong> codebuild-fips.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS:</strong> codebuild-fips.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS:</strong> codebuild.us-gov-west-1.amazonaws.com</td>
<td><strong>Non-FIPS:</strong> codebuild.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td>AWS CodeCommit</td>
<td><strong>FIPS:</strong> codecommit-fips.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS:</strong> codecommit-fips.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>FIPS:</strong> git-codecommit-fips.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS:</strong> codecommit-us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS:</strong> codecommit.us-gov-west-1.amazonaws.com</td>
<td><strong>Non-FIPS:</strong> codecommit.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td>AWS CodeDeploy</td>
<td><strong>FIPS:</strong> codedeploy-fips.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS:</strong> codedeploy-fips.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS:</strong> codedeploy.us-gov-west-1.amazonaws.com</td>
<td><strong>Non-FIPS:</strong> codedeploy.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td>AWS CodePipeline</td>
<td><strong>FIPS:</strong> codepipeline-fips.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS:</strong> Not applicable</td>
<td><strong>FIPS:</strong> Not applicable</td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS:</strong> codepipeline.us-gov-west-1.amazonaws.com</td>
<td><strong>Non-FIPS:</strong> Not applicable</td>
<td><strong>Non-FIPS:</strong> Not applicable</td>
</tr>
<tr>
<td>Amazon Cognito</td>
<td><strong>User Pools:</strong></td>
<td><strong>FIPS:</strong> Not applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>FIPS:</strong> cognito-idp-fips.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS:</strong> Not applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS:</strong> cognito-idp.us-gov-west-1.amazonaws.com</td>
<td><strong>Non-FIPS:</strong> Not applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Identity Pools:</strong></td>
<td><strong>FIPS:</strong> Not applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>FIPS:</strong> cognito-identity.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS:</strong> Not applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS:</strong> Not applicable</td>
<td><strong>Non-FIPS:</strong> Not applicable</td>
<td></td>
</tr>
<tr>
<td>Amazon Comprehend</td>
<td><strong>FIPS:</strong> comprehend-fips.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS:</strong> Not applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS:</strong> comprehend.us-gov-west-1.amazonaws.com</td>
<td><strong>Non-FIPS:</strong> Not applicable</td>
<td></td>
</tr>
<tr>
<td>AWS Config</td>
<td><strong>FIPS:</strong> config.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS:</strong> config.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS:</strong> Not applicable</td>
<td><strong>Non-FIPS:</strong> Not applicable</td>
<td></td>
</tr>
<tr>
<td>AWS Config Rules</td>
<td><strong>FIPS:</strong> config.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS:</strong> config.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS:</strong> Not applicable</td>
<td><strong>Non-FIPS:</strong> Not applicable</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>---------------------------------------------------</td>
<td>---------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td>Amazon DocumentDB (with MongoDB compatibility)</td>
<td>FIPS: rds.us-gov-west-1.amazonaws.com</td>
<td>FIPS: Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td>AWS Direct Connect</td>
<td>FIPS: Not applicable</td>
<td>FIPS: Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td>Amazon DynamoDB Streams</td>
<td>FIPS: streams.dynamodb.us-gov-west-1.amazonaws.com</td>
<td>FIPS: Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td>Amazon Elastic Block Store (Amazon EBS)</td>
<td>FIPS: ec2.us-gov-west-1.amazonaws.com</td>
<td>FIPS: ec2.us-gov-east-1.amazonaws.com</td>
<td>Protocol</td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td>EBS direct APIs</td>
<td>FIPS: ebs.us-gov-west-1.amazonaws.com</td>
<td>FIPS: ebs.us-gov-east-1.amazonaws.com</td>
<td>Protocol</td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td>Amazon Elastic Compute Cloud (Amazon EC2)</td>
<td>FIPS: ec2.us-gov-west-1.amazonaws.com</td>
<td>FIPS: ec2.us-gov-east-1.amazonaws.com</td>
<td>Protocol</td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------</td>
<td>---------------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Amazon Elastic Compute Cloud Image Builder</td>
<td>FIPS: imagebuilder.us-gov-west-1.amazonaws.com</td>
<td>FIPS: Not applicable</td>
<td>FIPS: Not applicable</td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td></td>
</tr>
<tr>
<td>AWS Elemental MediaConvert</td>
<td>FIPS: mediaconvert.us-gov-west-1.amazonaws.com</td>
<td></td>
<td>Not applicable</td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Amazon EventBridge</td>
<td>FIPS: events.us-gov-west-1.amazonaws.com</td>
<td>FIPS: events.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td></td>
</tr>
<tr>
<td>Amazon S3 Glacier</td>
<td>FIPS: glacier.us-gov-west-1.amazonaws.com</td>
<td>FIPS: glacier.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td></td>
</tr>
<tr>
<td>AWS Glue</td>
<td>FIPS: glue-fips.us-gov-west-1.amazonaws.com</td>
<td>FIPS: glue-fips.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td>Amazon GuardDuty</td>
<td>FIPS: guardduty.us-gov-west-1.amazonaws.com</td>
<td>FIPS: guardduty.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Not applicable</td>
<td></td>
</tr>
<tr>
<td>AWS Health*</td>
<td>FIPS: health-fips.us-gov-west-1.amazonaws.com</td>
<td>Not applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWS Identity and Access</td>
<td>FIPS: iam.us-gov.amazonaws.com</td>
<td>FIPS: iam.us-gov.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td>Management (IAM)</td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td></td>
</tr>
<tr>
<td>AWS IoT Core</td>
<td>FIPS: Not applicable</td>
<td>FIPS: Not applicable</td>
<td></td>
</tr>
<tr>
<td>AWS IoT Greengrass</td>
<td>FIPS:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Control plane operations:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>greengrass.us-gov-west-1.amazonaws.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Discovery operations:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>greengrass-ats.iot.us-gov-west-1.amazonaws.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AWS IoT device operations:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>prefix-ats.iot.us-gov-west-1.amazonaws.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-FIPS:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Control plane operations:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>greengrass.us-gov-west-1.amazonaws.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Discovery operations:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>greengrass-ats.iot.us-gov-west-1.amazonaws.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• AWS IoT device operations:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>prefix-ats.iot.us-gov-west-1.amazonaws.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>---------------------------------------------------</td>
<td>---------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>AWS IoT Device Management</td>
<td>FIPS: Not applicable</td>
<td>FIPS: Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td>AWS IoT Device Defender</td>
<td>FIPS: Not applicable</td>
<td>FIPS: Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td>Amazon Kinesis Data Streams</td>
<td>FIPS: kinesis.us-gov-west-1.amazonaws.com</td>
<td>FIPS: kinesis.us-gov-east-1.amazonaws.com</td>
<td>Protocol</td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td>AWS Lake Formation</td>
<td>FIPS: lakeformation-fips.us-gov-west-1.amazonaws.com</td>
<td>FIPS: Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td>Amazon Managed Streaming for Apache Kafka (MSK)</td>
<td>FIPS: Not Applicable</td>
<td>FIPS: Not Applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td><strong>AWS Service</strong></td>
<td><strong>AWS GovCloud (US-West) Endpoints (FIPS, Non-FIPS)</strong></td>
<td><strong>AWS GovCloud (US-East) Endpoints (FIPS, Non-FIPS)</strong></td>
<td><strong>Protocol</strong></td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>------------------------------------------------------</td>
<td>------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>AWS Marketplace Metering</td>
<td><strong>FIPS:</strong> Not Applicable</td>
<td><strong>FIPS:</strong> Not Applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS:</strong> metering.marketplace.us-gov-west-1.amazonaws.com</td>
<td><strong>Non-FIPS:</strong> metering.marketplace.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td>Amazon Neptune</td>
<td><strong>FIPS:</strong> rds.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS:</strong> rds.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS:</strong> Not applicable</td>
<td><strong>Non-FIPS:</strong> Not applicable</td>
<td></td>
</tr>
<tr>
<td>AWS Organizations</td>
<td><strong>FIPS:</strong> organizations.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS:</strong> Not Applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS:</strong> Not Applicable</td>
<td><strong>Non-FIPS:</strong> Not Applicable</td>
<td></td>
</tr>
<tr>
<td>AWS Outposts</td>
<td><strong>FIPS:</strong> outposts.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS:</strong> outposts.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS:</strong> Not Applicable</td>
<td><strong>Non-FIPS:</strong> Not Applicable</td>
<td></td>
</tr>
<tr>
<td>AWS Personal Health Dashboard</td>
<td><strong>FIPS:</strong> Not Applicable</td>
<td><strong>FIPS:</strong> Not Applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS:</strong> phd.amazonaws-us-gov.com</td>
<td><strong>Non-FIPS:</strong> phd.amazonaws-us-gov.com</td>
<td></td>
</tr>
<tr>
<td>Amazon Pinpoint</td>
<td><strong>FIPS:</strong> pinpoint-fips.us-gov-west-1.amazonaws.com</td>
<td></td>
<td>Not applicable</td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS:</strong> pinpoint.us-gov-west-1.amazonaws.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amazon Polly</td>
<td><strong>FIPS:</strong> polly-fips.us-gov-west-1.amazonaws.com</td>
<td></td>
<td>Not applicable</td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS:</strong> polly.us-gov-west-1.amazonaws.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amazon QuickSight</td>
<td><strong>FIPS:</strong> fips-us-gov-west-1.quicksight.amazonaws-us-gov.com</td>
<td></td>
<td>Not applicable</td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Service endpoint:</strong> quicksight.us-gov-west-1.amazonaws.com;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Website endpoint:</strong> <a href="https://us-gov-west-1.quicksight.amazonaws-us-gov.com/">https://us-gov-west-1.quicksight.amazonaws-us-gov.com/</a>;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWS Resource Access Manager</td>
<td><strong>FIPS:</strong> Not Applicable</td>
<td><strong>FIPS:</strong> Not Applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS:</strong> ram.us-gov-west-1.amazonaws.com</td>
<td><strong>Non-FIPS:</strong> ram.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>AWS Resource Groups</td>
<td>FIPS: Not Applicable</td>
<td>FIPS: Not Applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td>Amazon Redshift</td>
<td>FIPS: redshift.us-gov-west-1.amazonaws.com</td>
<td>FIPS: redshift.us-gov-east-1.amazonaws.com</td>
<td>Protocol</td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td>Amazon Rekognition</td>
<td>FIPS: rekognition-fips.us-gov-west-1.amazonaws.com</td>
<td>Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: rekognition.us-gov-west-1.amazonaws.com</td>
<td>Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td>Amazon Relational Database Service (Amazon RDS)</td>
<td>FIPS: rds.us-gov-west-1.amazonaws.com</td>
<td>FIPS: rds.us-gov-east-1.amazonaws.com</td>
<td>Protocol</td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td>Amazon Route 53</td>
<td>FIPS: route53.us-gov.amazonaws.com</td>
<td>FIPS: Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td>Amazon SageMaker</td>
<td>FIPS: api.sagemaker.us-gov-west-1.amazonaws.com</td>
<td>Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: runtime.sagemaker.us-gov-west-1.amazonaws.com</td>
<td>Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td>Protocol</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>AWS Service Catalog</td>
<td><strong>FIPS</strong>: servicecatalog-fips.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS</strong>: servicecatalog-fips.us-gov-east-1.amazonaws.com</td>
<td><strong>FIPS</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS</strong>: servicecatalog.us-gov-west-1.amazonaws.com</td>
<td><strong>Non-FIPS</strong>: servicecatalog.us-gov-east-1.amazonaws.com</td>
<td><strong>Non-FIPS</strong></td>
</tr>
<tr>
<td>Amazon SES</td>
<td><strong>FIPS</strong>: email-fips.us-gov-west-1.amazonaws.com</td>
<td></td>
<td>Not applicable</td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS</strong>: email.us-gov-west-1.amazonaws.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>FIPS SMTP</strong>: email-smtp-fips.us-gov-west-1.amazonaws.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS SMTP</strong>: email-smtp.us-gov-west-1.amazonaws.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWS Server Migration Service (AWS SMS)</td>
<td><strong>FIPS</strong>: sms-fips.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS</strong>: sms-fips.us-gov-east-1.amazonaws.com</td>
<td><strong>FIPS</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS</strong>: sms.us-gov-west-1.amazonaws.com</td>
<td><strong>Non-FIPS</strong>: sms.us-gov-east-1.amazonaws.com</td>
<td><strong>Non-FIPS</strong></td>
</tr>
<tr>
<td>Amazon Simple Storage Service (Amazon S3)</td>
<td><strong>FIPS</strong>: s3-fips.us-gov-west-1.amazonaws.com, s3.dualstack.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS</strong>: s3-fips.us-gov-east-1.amazonaws.com, s3.dualstack.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS</strong>: s3.us-gov-west-1.amazonaws.com</td>
<td><strong>Non-FIPS</strong>: s3.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td>Amazon Simple Storage Service (Amazon S3) (website)</td>
<td><strong>FIPS</strong>: Not applicable</td>
<td><strong>FIPS</strong>: Not applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS</strong>: s3-website.us-gov-west-1.amazonaws.com</td>
<td><strong>Non-FIPS</strong>: s3-website.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td>Amazon Simple Storage Service (Amazon S3) Access Points</td>
<td><strong>FIPS</strong>:s3-accesspoint-fips.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS</strong>: s3-accesspoint-fips.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS</strong>:s3-accesspoint.us-gov-west-1.amazonaws.com</td>
<td><strong>Non-FIPS</strong>:s3-accesspoint.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td>Amazon Simple Notification Service (Amazon SNS)</td>
<td><strong>FIPS</strong>:sns.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS</strong>: sns.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS</strong>:Not applicable</td>
<td><strong>Non-FIPS</strong>:Not applicable</td>
<td></td>
</tr>
<tr>
<td>Amazon Simple Queue Service (Amazon SQS)</td>
<td><strong>FIPS</strong>: sqs.us-gov-west-1.amazonaws.com</td>
<td><strong>FIPS</strong>: sqs.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Non-FIPS</strong>: Not applicable</td>
<td><strong>Non-FIPS</strong>: Not applicable</td>
<td></td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| Amazon Simple Workflow Service (Amazon SWF) | FIPS: swf.us-gov-west-1.amazonaws.com  
Non-FIPS: Not applicable                      | FIPS: swf.us-gov-east-1.amazonaws.com                                             |          |
| AWS Security Token Service (AWS STS)     | FIPS: sts.us-gov-west-1.amazonaws.com  
Non-FIPS: Not applicable                      | FIPS: sts.us-gov-east-1.amazonaws.com                                             |          |
| AWS Snow Family               | FIPS: Not applicable  
Non-FIPS: snowball.us-gov-west-1.amazonaws.com                                 | Not applicable                                                                 |          |
| AWS Step Functions            | FIPS: states.us-gov-west-1.amazonaws.com  
Non-FIPS: Not applicable                      | FIPS: states-fips.us-gov-east-1.amazonaws.com                                     |          |
| AWS Storage Gateway           | FIPS: storagegateway-fips.us-gov-west-1.amazonaws.com  
Non-FIPS: storagegateway.us-gov-west-1.amazonaws.com  | FIPS: storagegateway-fips.us-gov-east-1.amazonaws.com  
Non-FIPS: storagegateway.us-gov-east-1.amazonaws.com |          |
| AWS Support                   | FIPS: support.us-gov-west-1.amazonaws.com  
Non-FIPS: Not applicable                      | FIPS: support.us-gov-east-1.amazonaws.com                                         |          |
| AWS Systems Manager           | FIPS: ssm.us-gov-west-1.amazonaws.com  
Non-FIPS: Not applicable                      | FIPS: ssm.us-gov-east-1.amazonaws.com                                             |          |
| Amazon Textract               | FIPS: textract-fips.us-gov-west-1.amazonaws.com  
Non-FIPS: textract.us-gov-east-1.amazonaws.com |          |
| AWS Transfer Family           | FIPS: transfer-fips.us-gov-west-1.amazonaws.com  
Non-FIPS: transfer.us-gov-west-1.amazonaws.com                      | FIPS: transfer-fips.us-gov-east-1.amazonaws.com  
Non-FIPS: transfer.us-gov-east-1.amazonaws.com |          |
| Amazon Transcribe             | FIPS: fips.transcribe.us-gov-west-1.amazonaws.com  
Non-FIPS: transcribe.us-gov-west-1.amazonaws.com                      | FIPS: fips.transcribe.us-gov-east-1.amazonaws.com  
Non-FIPS: transcribe.us-gov-east-1.amazonaws.com |          |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Translate</td>
<td>FIPS: translate-fips.us-gov-west-1.amazonaws.com</td>
<td>FIPS: translate-fips.us-gov-west-1.amazonaws.com</td>
<td>Not applicable</td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: translate.us-gov-west-1.amazonaws.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amazon Virtual Private Cloud (Amazon VPC)</td>
<td>FIPS: ec2.us-gov-west-1.amazonaws.com</td>
<td>FIPS: ec2.us-gov-east-1.amazonaws.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td></td>
</tr>
<tr>
<td>AWS Management Console for the AWS GovCloud (US)</td>
<td>FIPS: Not applicable</td>
<td>FIPS: Not applicable</td>
<td></td>
</tr>
<tr>
<td>AWS Management Console with Federation</td>
<td>FIPS: Not applicable</td>
<td>FIPS: Not applicable</td>
<td></td>
</tr>
<tr>
<td>AWS Management Console with SAML</td>
<td>FIPS: Not applicable</td>
<td>FIPS: Not applicable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: Not applicable</td>
<td>Non-FIPS: Not applicable</td>
<td></td>
</tr>
<tr>
<td>AWS WAF</td>
<td>FIPS: waf-regional-fips.us-gov-west-1.amazonaws.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: waf-regional.us-gov-west-1.amazonaws.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWS WAF v2</td>
<td>FIPS:wafv2-fips.us-gov-west-1.amazonaws.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: wafv2.us-gov-west-1.amazonaws.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amazon WorkSpaces</td>
<td>FIPS: workspaces-fips.us-gov-west-1.amazonaws.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-FIPS: workspaces.us-gov-west-1.amazonaws.com</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
For information about giving federated users single sign-on access to the AWS Management Console, see Giving Federated Users Direct Access to the AWS Management Console.

**Note**
- AWS Health is a non-fips endpoint (https://aws.amazon.com/compliance/fips/). We were cleared to not use fips because we do not share customer data (Health events are considered AWS data). FIPS endpoints have mandated encryptions applied to them.
- 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.
- Amazon S3 dual-stack endpoints support requests to S3 buckets over IPv6 and IPv4. For more information, see Using Dual-Stack Endpoints.

## VPC Endpoints

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network. Interface with a private IP address from the IP address range of your subnet that serves as an entry point for traffic destined to a supported service. Interface endpoints are powered by AWS PrivateLink, a technology that enables you to privately access services by using private IP addresses. AWS PrivateLink restricts all network traffic between your VPC and services to the Amazon network. You do not need an internet gateway, a NAT device, or a virtual private gateway.

A gateway endpoint is a gateway that you specify as a target for a route in your route table for traffic destined to a supported AWS service.

### VPC Endpoints for the AWS GovCloud (US) Regions

The following table lists each AWS service available in the AWS GovCloud (US) Regions and the corresponding VPC endpoints.

<table>
<thead>
<tr>
<th>AWS Service</th>
<th>AWS GovCloud (US-West) VPC Endpoints</th>
<th>AWS GovCloud (US-East) VPC Endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Auto Scaling</td>
<td>com.amazonaws.us-gov-west-1.application-autoscaling</td>
<td>com.amazonaws.us-gov-east-1.application-autoscaling</td>
</tr>
<tr>
<td>AWS Auto Scaling</td>
<td>com.amazonaws.us-gov-west-1.autoscaling-plans</td>
<td>com.amazonaws.us-gov-east-1.autoscaling-plans</td>
</tr>
<tr>
<td>Amazon AppStream 2.0</td>
<td>com.amazonaws.us-gov-west-1.appstream.api</td>
<td>Not applicable</td>
</tr>
<tr>
<td></td>
<td>com.amazonaws.us-gov-west-1.appstream.streaming</td>
<td></td>
</tr>
</tbody>
</table>
### AWS GovCloud (US) User Guide

**VPC Endpoints**

<table>
<thead>
<tr>
<th>AWS Service</th>
<th>AWS GovCloud (US-West) VPC Endpoints</th>
<th>AWS GovCloud (US-East) VPC Endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Athena</td>
<td>com.amazonaws.us-gov-west-1.athena</td>
<td>com.amazonaws.us-gov-east-1.athena</td>
</tr>
<tr>
<td>Amazon EC2 Auto Scaling</td>
<td>com.amazonaws.us-gov-west-1.autoscaling</td>
<td>com.amazonaws.us-gov-east-1.autoscaling</td>
</tr>
<tr>
<td>Amazon Cloud Directory</td>
<td>com.amazonaws.us-gov-west-1.clouddirectory</td>
<td>Not applicable</td>
</tr>
<tr>
<td>AWS CloudFormation</td>
<td>com.amazonaws.us-gov-west-1.cloudformation</td>
<td>com.amazonaws.us-gov-east-1.cloudformation</td>
</tr>
<tr>
<td>AWS CloudTrail</td>
<td>com.amazonaws.us-gov-west-1.cloudtrail</td>
<td>com.amazonaws.us-gov-east-1.cloudtrail</td>
</tr>
<tr>
<td>AWS CodeCommit</td>
<td>com.amazonaws.us-gov-west-1.codecommit</td>
<td>com.amazonaws.us-gov-east-1.codecommit</td>
</tr>
<tr>
<td>AWS CodeCommit</td>
<td>com.amazonaws.us-gov-west-1.codecommit-fips</td>
<td>com.amazonaws.us-gov-east-1.codecommit-fips</td>
</tr>
<tr>
<td>AWS Config</td>
<td>com.amazonaws.us-gov-west-1.config</td>
<td>com.amazonaws.us-gov-east-1.config</td>
</tr>
<tr>
<td>AWS CodePipeline</td>
<td>com.amazonaws.us-gov-west-1.codepipeline</td>
<td>Not applicable</td>
</tr>
<tr>
<td>AWS DataSync</td>
<td>com.amazonaws.us-gov-west-1.datasync</td>
<td>com.amazonaws.us-gov-east-1.datasync</td>
</tr>
<tr>
<td>AWS Direct Connect</td>
<td>com.amazonaws.us-gov-west-1.directconnect</td>
<td>com.amazonaws.us-gov-east-1.directconnect</td>
</tr>
<tr>
<td>Amazon DynamoDB</td>
<td>com.amazonaws.us-gov-west-1.dynamodb</td>
<td>com.amazonaws.us-gov-east-1.dynamodb</td>
</tr>
<tr>
<td>Amazon EC2</td>
<td>com.amazonaws.us-gov-west-1.ec2</td>
<td>com.amazonaws.us-gov-east-1.ec2</td>
</tr>
<tr>
<td>Amazon EC2</td>
<td>com.amazonaws.us-gov-west-1.ec2messages</td>
<td>com.amazonaws.us-gov-east-1.ec2messages</td>
</tr>
<tr>
<td>EBS direct APIs</td>
<td>com.amazonaws.us-gov-west-1.ebs</td>
<td>com.amazonaws.us-gov-east-1.ebs</td>
</tr>
<tr>
<td>Amazon ECR</td>
<td>com.amazonaws.us-gov-west-1.ecr.api</td>
<td>com.amazonaws.us-gov-east-1.ecr.api</td>
</tr>
<tr>
<td>Amazon ECR</td>
<td>com.amazonaws.us-gov-west-1.ecr.dkr</td>
<td>com.amazonaws.us-gov-east-1.ecr.dkr</td>
</tr>
<tr>
<td>AWS Service</td>
<td>AWS GovCloud (US-West) VPC Endpoints</td>
<td>AWS GovCloud (US-East) VPC Endpoints</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Amazon ECS</td>
<td>com.amazonaws.us-gov-west-1.ecs</td>
<td>com.amazonaws.us-gov-east-1.ecs</td>
</tr>
<tr>
<td></td>
<td>com.amazonaws.us-gov-west-1.ecs-agent</td>
<td>com.amazonaws.us-gov-east-1.ecs-agent</td>
</tr>
<tr>
<td></td>
<td>com.amazonaws.us-gov-west-1.ecs-telemetry</td>
<td>com.amazonaws.us-gov-east-1.ecs-telemetry</td>
</tr>
<tr>
<td>AWS Elastic Beanstalk</td>
<td>com.amazonaws.us-gov-west-1.elasticbeanstalk</td>
<td>com.amazonaws.us-gov-east-1.elasticbeanstalk</td>
</tr>
<tr>
<td></td>
<td>com.amazonaws.us-gov-west-1.elasticbeanstalk-health</td>
<td>com.amazonaws.us-gov-east-1.elasticbeanstalk-health</td>
</tr>
<tr>
<td>Amazon Elastic File System</td>
<td>com.amazonaws.us-gov-west-1.elasticfilesystem</td>
<td>com.amazonaws.us-gov-east-1.elasticfilesystem</td>
</tr>
<tr>
<td></td>
<td>com.amazonaws.us-gov-west-1.elasticfilesystem-fips</td>
<td>com.amazonaws.us-gov-east-1.elasticfilesystem-fips</td>
</tr>
<tr>
<td>Elastic Load Balancing</td>
<td>com.amazonaws.us-gov-west-1.elasticloadbalancing</td>
<td>com.amazonaws.us-gov-east-1.elasticloadbalancing</td>
</tr>
<tr>
<td>Amazon EMR</td>
<td>com.amazonaws.us-gov-west-1.elasticmapreduce</td>
<td>com.amazonaws.us-gov-east-1.elasticmapreduce</td>
</tr>
<tr>
<td>Git CodeCommit</td>
<td>com.amazonaws.us-gov-west-1.git-codecommit</td>
<td>com.amazonaws.us-gov-east-1.git-codecommit</td>
</tr>
<tr>
<td></td>
<td>com.amazonaws.us-gov-west-1.git-codecommit-fips</td>
<td>com.amazonaws.us-gov-east-1.git-codecommit-fips</td>
</tr>
<tr>
<td>EC2 Image Builder</td>
<td>com.amazonaws.us-gov-west-1.imagebuilder</td>
<td>com.amazonaws.us-gov-east-1.imagebuilder</td>
</tr>
<tr>
<td>Amazon Kinesis Data Firehose</td>
<td>com.amazonaws.us-gov-west-1.kinesis-firehose</td>
<td>com.amazonaws.us-gov-east-1.kinesis-firehose</td>
</tr>
<tr>
<td>Amazon Kinesis Data Streams</td>
<td>com.amazonaws.us-gov-west-1.kinesis-streams</td>
<td>com.amazonaws.us-gov-east-1.kinesis-streams</td>
</tr>
<tr>
<td>AWS KMS</td>
<td>com.amazonaws.us-gov-west-1.kms</td>
<td>com.amazonaws.us-gov-east-1.kms</td>
</tr>
<tr>
<td>AWS Lake Formation</td>
<td>com.amazonaws.us-gov-west-1.lakeformation</td>
<td>Not applicable</td>
</tr>
<tr>
<td>AWS License Manager</td>
<td>com.amazonaws.us-gov-west-1.license-manager</td>
<td>com.amazonaws.us-gov-east-1.license-manager</td>
</tr>
<tr>
<td></td>
<td>com.amazonaws.us-gov-west-1.license-manager-fips</td>
<td>com.amazonaws.us-gov-east-1.license-manager-fips</td>
</tr>
<tr>
<td>Amazon QuickSight</td>
<td>quicksight.us-gov-west-1.amazonaws.com</td>
<td>Not applicable</td>
</tr>
<tr>
<td>AWS Service</td>
<td>AWS GovCloud (US-West) VPC Endpoints</td>
<td>AWS GovCloud (US-East) VPC Endpoints</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Amazon Rekognition</td>
<td>com.amazonaws.us-gov-west-1.rekognition</td>
<td>Not applicable</td>
</tr>
<tr>
<td></td>
<td>com.amazonaws.us-gov-west-1.rekognition-fips</td>
<td></td>
</tr>
<tr>
<td>Amazon RDS</td>
<td>com.amazonaws.us-gov-west-1.rds</td>
<td>com.amazonaws.us-gov-east-1.rds</td>
</tr>
<tr>
<td>Amazon S3</td>
<td>com.amazonaws.us-gov-west-1.s3</td>
<td>com.amazonaws.us-gov-east-1.s3</td>
</tr>
<tr>
<td>SageMaker</td>
<td>com.amazonaws.us-gov-west-1.sagemaker.api</td>
<td>Not Applicable</td>
</tr>
<tr>
<td></td>
<td>com.amazonaws.us-gov-west-1.sagemaker.runtime</td>
<td></td>
</tr>
<tr>
<td></td>
<td>aws.sagemaker.us-gov-west-1.notebook</td>
<td></td>
</tr>
<tr>
<td>AWS Secrets Manager</td>
<td>com.amazonaws.us-gov-west-1.secretsmanager</td>
<td>com.amazonaws.us-gov-east-1.secretsmanager</td>
</tr>
<tr>
<td>AWS Service Catalog</td>
<td>com.amazonaws.us-gov-west-1.servicecatalog</td>
<td>com.amazonaws.us-gov-west-1.servicecatalog</td>
</tr>
<tr>
<td>AWS Server Migration Service</td>
<td>com.amazonaws.us-gov-west-1.sms</td>
<td>com.amazonaws.us-gov-east-1.sms</td>
</tr>
<tr>
<td></td>
<td>com.amazonaws.us-gov-west-1.sms-fips</td>
<td>com.amazonaws.us-gov-east-1.sms-fips</td>
</tr>
<tr>
<td>Amazon SNS</td>
<td>com.amazonaws.us-gov-west-1.sns</td>
<td>com.amazonaws.us-gov-east-1.sns</td>
</tr>
<tr>
<td>Amazon SQS</td>
<td>com.amazonaws.us-gov-west-1.sqs</td>
<td>com.amazonaws.us-gov-east-1.sqs</td>
</tr>
<tr>
<td>AWS Systems Manager</td>
<td>com.amazonaws.us-gov-west-1.ssm</td>
<td>com.amazonaws.us-gov-east-1.ssm</td>
</tr>
<tr>
<td></td>
<td>com.amazonaws.us-gov-west-1.ssmmessages</td>
<td>com.amazonaws.us-gov-east-1.ssmmessages</td>
</tr>
<tr>
<td>Amazon Transcribe</td>
<td>com.amazonaws.us-gov-west-1.transcribe</td>
<td>com.amazonaws.us-gov-east-1.transcribe</td>
</tr>
<tr>
<td>AWS Transfer Family</td>
<td>com.amazonaws.us-gov-west-1.transfer</td>
<td>com.amazonaws.us-gov-east-1.transfer</td>
</tr>
<tr>
<td>AWS Storage Gateway</td>
<td>com.amazonaws.us-gov-west-1.storagegateway</td>
<td>com.amazonaws.us-gov-east-1.storagegateway</td>
</tr>
<tr>
<td>Amazon WorkSpaces</td>
<td>com.amazonaws.us-gov-west-1.workspaces</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>
Maintaining U.S. International Traffic in Arms Regulations (ITAR) Compliance

If you store and process ITAR-regulated data in the AWS GovCloud (US) Regions, 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 AWS GovCloud (US) 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) Regions, you must comply with the ITAR restrictions for each AWS services in the AWS GovCloud (US) Regions. For more information about the ITAR boundaries for each service, see the service-specific information in Services in AWS GovCloud (US) Regions (p. 83).

Accessing the AWS GovCloud (US) Regions

When you access the AWS GovCloud (US) Regions, 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.

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

- 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) as a Solution Provider reselling in AWS GovCloud (US) (p. 11).

- 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 a variety of languages. Some service operations that require computation of an md5 content hash, such as S3, may be unavailable or require additional code. The Sample Code and Libraries Catalog also provides a listing of code, SDKs, sample applications, and other tools available for use. For SDKs that leverage cryptography other than OpenSSL, such as Go, make sure you are following best practices for meeting compliance. Go leverages a built-in cryptography library that is not FIPS 140-2 validated.

- 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://docs.aws.amazon.com/.

- 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. 5)** 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) Region **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

AWS customers are permitted to perform penetration testing on certain services by following the AWS Customer Support Policy for Penetration Testing. Please refer to the Policy before planning and performing penetration testing activities.

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.

Closing an AWS GovCloud (US) Account

The following instructions describe the process to close an AWS GovCloud (US) account. Because AWS account management functions are not available in the AWS GovCloud (US) Management Console, closing an AWS GovCloud account may require additional steps.

Note
There is no 'Close Account' option available in the AWS GovCloud (US) Management Console as there is in the standard AWS account Management Console.

Users can either close both the standard AWS account and the AWS GovCloud account that it's linked to or close just the AWS GovCloud account.

Closing both Standard and AWS GovCloud accounts:

- If you wish to close both your AWS Standard account and its' associated AWS GovCloud (US) account, you can use the 'Close Account' option available in the standard account console.
- The GovCloud account will close within the next billing cycle (similar to the standard AWS account). If you run into issues with billing/access to the GovCloud console after this time, please submit a Support Case via the standard account, referencing the issue and the GovCloud Account ID.

Closing the AWS GovCloud account only:

- To close the GovCloud account, you must first terminate all resources currently running in the AWS GovCloud (US) account (both regions if applicable).
- Delete all IAM users.
- Rotate and delete the Access Keys for the GovCloud account.
Note
The IAM permission stack to access the AWS GovCloud (US) Management Console will still exist, but users will no longer be able to log into the console or create AWS resources. The standard account access/resources will remain the same.
Services in AWS GovCloud (US) Regions

The following sections describe the differences between the AWS GovCloud (US) Regions 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.

Topics
- Amazon API Gateway (p. 85)
- Amazon AppStream 2.0 (p. 86)
- AWS Artifact (p. 88)
- Amazon Athena (p. 89)
- Amazon Aurora with MySQL and PostgreSQL compatibility (p. 89)
- AWS Auto Scaling (p. 91)
- Application Auto Scaling (p. 92)
- Amazon EC2 Auto Scaling (p. 93)
- AWS Batch (p. 94)
- AWS Backup Agent for SAP HANA (p. 95)
- AWS Backup (p. 95)
- AWS Certificate Manager (p. 96)
- AWS Certificate Manager Private Certificate Authority (p. 97)
- Amazon Cloud Directory (p. 97)
- AWS CloudFormation (p. 98)
- Amazon Comprehend (p. 99)
- AWS DataSync (p. 100)
- AWS CloudHSM (p. 101)
- AWS CloudHSM Classic (p. 101)
- AWS CloudTrail (p. 102)
- Amazon CloudWatch (p. 108)
- Amazon CloudWatch Events (p. 109)
- Amazon CloudWatch Logs (p. 110)
- AWS CodeBuild (p. 111)
- AWS CodeCommit (p. 111)
- AWS CodeDeploy (p. 112)
- AWS CodePipeline (p. 115)
- Amazon Cognito (p. 116)
- Amazon Comprehend Medical (p. 118)
- AWS Config (p. 119)
- AWS Direct Connect (p. 120)
- AWS Directory Service (p. 121)
- AWS Database Migration Service (p. 123)
• AWS Deep Learning AMIs (p. 124)
• Amazon DocumentDB (with MongoDB compatibility) (p. 124)
• Amazon DynamoDB (p. 126)
• AWS Elastic Beanstalk (p. 127)
• Amazon EBS (p. 128)
• Amazon EC2 (p. 129)
• Importing Virtual Machines into AWS GovCloud (US) Regions (p. 131)
• Amazon EC2 Image Builder (p. 132)
• Amazon ECR (p. 133)
• Amazon ECS (p. 134)
• Amazon Elastic File System (p. 134)
• Amazon Elastic Kubernetes Service (p. 135)
• Amazon Elasticsearch Service (p. 136)
• Elastic Load Balancing (p. 137)
• Amazon ElastiCache (p. 138)
• Amazon EMR (p. 139)
• Amazon EventBridge (p. 140)
• AWS Fargate (p. 141)
• Amazon S3 Glacier (p. 142)
• AWS Glue (p. 143)
• Amazon GuardDuty (p. 143)
• AWS Health (p. 144)
• AWS Identity and Access Management (p. 145)
• Amazon Inspector (p. 147)
• AWS IoT Core (p. 147)
• AWS IoT Device Defender (p. 148)
• AWS IoT Device Management (p. 149)
• AWS IoT Greengrass (p. 150)
• Amazon Kinesis Data Analytics (p. 152)
• Amazon Kinesis Data Firehose (p. 152)
• Amazon Kinesis Data Streams (p. 153)
• AWS Key Management Service (p. 154)
• AWS Lake Formation (p. 155)
• AWS Lambda (p. 156)
• AWS License Manager (p. 156)
• AWS Management Console for the AWS GovCloud (US) Region (p. 157)
• AWS Marketplace (p. 158)
• Amazon Managed Streaming for Apache Kafka (MSK) (p. 159)
• AWS Elemental MediaConvert (p. 160)
• Amazon Neptune (p. 161)
• AWS Organizations (p. 162)
• AWS Outposts (p. 165)
• AWS ParallelCluster (p. 166)
• Amazon Pinpoint (p. 167)
• Amazon Polly (p. 168)
Amazon API Gateway

Amazon API Gateway is a fully managed service that makes it easy for developers to publish, maintain, monitor, and secure APIs at any scale. Create an API to access data, business logic, or functionality from your back-end services, such as applications running on Amazon Elastic Compute Cloud (Amazon EC2), code running on AWS Lambda, or any web application.

How Amazon API Gateway Differs for AWS GovCloud (US)

- 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 Z1K6XKP95AGWDV.
- HTTP API private integrations aren’t supported in AWS GovCloud (US-East).
- HTTP API private integrations with AWS Cloud Map aren’t supported in AWS GovCloud (US-West).
- All API Gateway APIs created in GovCloud regions are FIPS-compliant by default. In commercial regions that require FIPS compliance, contact API Gateway.

The following region-specific API Gateway accounts are used for private integrations in GovCloud:

<table>
<thead>
<tr>
<th>Region</th>
<th>Account ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>us-gov-west-1</td>
<td>291049978687</td>
</tr>
<tr>
<td>us-gov-east-1</td>
<td>044865953448</td>
</tr>
</tbody>
</table>

**ITAR Boundary**

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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><em>Customers’ APIs are permitted to process ITAR data.</em></td>
<td>API Gateway’s configuration metadata is not permitted to contain ITAR-regulated data*, including:</td>
</tr>
<tr>
<td></td>
<td><em>API Name</em></td>
</tr>
<tr>
<td></td>
<td><em>API Description</em></td>
</tr>
<tr>
<td></td>
<td><em>Authorizer Name</em></td>
</tr>
<tr>
<td></td>
<td><em>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).</em></td>
</tr>
</tbody>
</table>

**Amazon AppStream 2.0**

This service is currently available in AWS GovCloud (US-West) only.

Amazon AppStream 2.0 is a fully managed application streaming service that provides users with instant access to their desktop applications from anywhere. AppStream 2.0 manages the AWS resources required
to host and run your applications, scales automatically, and provides access to your users on demand. AppStream 2.0 provides users access to the applications they need on the device of their choice, with a responsive, fluid user experience that is indistinguishable from natively installed applications.

**How Amazon AppStream 2.0 Differs for AWS GovCloud (US)**

- The Graphics Design instance type is currently not supported in AWS GovCloud (US-West).
- Copying AppStream 2.0 images between AWS GovCloud (US-West) and another AWS Region is not supported.
- The AppStream 2.0 user pool is not supported.
- The following CloudFormation resources are not available in AWS GovCloud (US-West):
  - AWS::AppStream::User
  - AWS::AppStream::StackUserAssociation
- The AppStream 2.0 CopyImage API action is not supported for copying AppStream 2.0 images between AWS GovCloud (US-West) and another AWS Region.
- The following AppStream 2.0 API actions are not supported in AWS GovCloud (US-West):
  - BatchAssociateUserStack
  - BatchDisassociateUserStack
  - DescribeUserStackAssociations, when USERPOOL is specified for the AuthenticationType parameter. USERPOOL is the only supported value for this parameter.
  - CreateUser
  - DeleteUser
  - DescribeUsers
  - DisableUser
  - EnableUser

**Documentation for Amazon AppStream 2.0**

Amazon AppStream 2.0 documentation.

**ITAR Boundary**

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 stored and processed within Amazon AppStream 2.0 can contain ITAR-regulated data.</td>
<td>Amazon AppStream 2.0 metadata is not permitted to contain ITAR-regulated data. This metadata includes all configuration data that you enter when creating and maintaining AppStream 2.0 image builders, images, fleets, and stacks. Do not enter ITAR-regulated data in the following console fields or when using the AppStream 2.0</td>
</tr>
</tbody>
</table>
ITAR-Regulated Data Permitted | ITAR-Regulated Data Not Permitted
--- | ---
| API actions or AWS Command Line Interface (AWS CLI) commands: |  |
| • Names and descriptions for Amazon AppStream 2.0 image builders, images, fleets and stacks. |  |
| • Resource tags. |  |
| • If importing ITAR-regulated images, do not use pre-signed URLs for the CLI argument. |  |

AWS Artifact

AWS Artifact provides on-demand downloads of AWS security and compliance documents, such as AWS ISO certifications, Payment Card Industry (PCI), and Service Organization Control (SOC) reports. You can submit the security and compliance documents (also known as audit artifacts) to your auditors or regulators to demonstrate the security and compliance of the AWS infrastructure and services that you use. You can also use AWS Artifact to review, accept, and track the status of AWS agreements such as the Business Associate Addendum (BAA). With AWS Artifact, you can accept agreements with AWS and designate AWS accounts that can legally process restricted information.

How AWS Artifact Differs for AWS GovCloud (US)

This service has no differences between AWS GovCloud (US) Regions and the standard AWS Regions.

Documentation for AWS Artifact

AWS Artifact documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>
</tbody>
</table>
Amazon Athena

Amazon Athena is an interactive query service that makes it easy to analyze data directly in Amazon Simple Storage Service (Amazon S3) using standard SQL. With a few actions in the AWS Management Console, you can point Athena at your data stored in Amazon S3 and begin using standard SQL to run ad-hoc queries and get results in seconds. Athena is serverless, so there is no infrastructure to set up or manage, and you pay only for the queries you run. Athena scales automatically—executing queries in parallel—so results are fast, even with large datasets and complex queries.

How Athena Differs for AWS GovCloud (US)

This service has no differences between AWS GovCloud (US) Regions and the standard AWS Regions.

Documentation for Amazon Athena

Amazon Athena documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 Athena can contain ITAR-regulated data.</td>
<td>Amazon Athena metadata is not permitted to contain ITAR-regulated data. This metadata includes:</td>
</tr>
<tr>
<td></td>
<td>• Database Name</td>
</tr>
<tr>
<td></td>
<td>• Table Name</td>
</tr>
<tr>
<td></td>
<td>• Partitions</td>
</tr>
<tr>
<td></td>
<td>• Query Names</td>
</tr>
</tbody>
</table>

Amazon Aurora with MySQL and PostgreSQL compatibility

Amazon Aurora (Aurora) is a fully managed relational database engine that's compatible with MySQL and PostgreSQL. You already know how MySQL and PostgreSQL combine the speed and reliability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases. The code, tools, and applications you use today with your existing MySQL and PostgreSQL databases can be used with Aurora. With some workloads, Aurora can deliver up to five times the throughput of MySQL and up to three times the throughput of PostgreSQL without requiring changes to most of your existing applications.
How Amazon Aurora Differs for AWS GovCloud (US)

- **Backtracking** is not available.
- Publishing Amazon Aurora MySQL Logs to Amazon CloudWatch Logs is not supported.
- Creation of cross-Region read replicas from other AWS Regions to the AWS GovCloud (US) Regions or from AWS GovCloud (US) Regions to other AWS Regions isn't supported.
- Copying of DB Snapshots from other AWS Regions to the AWS GovCloud (US) Regions or from AWS GovCloud (US) Regions to other AWS Regions isn't supported.
- Amazon RDS Performance Insights isn't available in the AWS GovCloud (US) Regions.
- Instance types and engine versions might vary in the AWS GovCloud (US) Regions. To determine instance and engine availability, see the RDS Management Console or CLI tools.
- Database activity streams are not supported in AWS GovCloud (US).
- Intermediate SSL certificates must be used to connect to the AWS GovCloud (US) Regions using SSL. For more information related to Intermediate certificates, see Using SSL/TLS to Encrypt a Connection.

The following Amazon Aurora editions are supported in AWS GovCloud (US) Regions:

- Amazon Aurora MySQL-compatible edition
- Amazon Aurora PostgreSQL-compatible edition

Documentation for Amazon Aurora

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

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>
<tr>
<td>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.</td>
<td>Do not enter ITAR-regulated data in the following fields:</td>
</tr>
<tr>
<td>Database Cluster Identifier</td>
<td></td>
</tr>
<tr>
<td>Database instance identifier</td>
<td></td>
</tr>
<tr>
<td>Master user name</td>
<td></td>
</tr>
<tr>
<td>Database name</td>
<td></td>
</tr>
<tr>
<td>Database snapshot name</td>
<td></td>
</tr>
<tr>
<td>Database security group name</td>
<td></td>
</tr>
<tr>
<td>Database security group description</td>
<td></td>
</tr>
</tbody>
</table>
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-West) 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-West) 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 Service Endpoints (p. 62).

AWS Auto Scaling

With AWS Auto Scaling, you can quickly discover the scalable AWS resources for your application and set up dynamic scaling. It uses Amazon EC2 Auto Scaling to scale your EC2 instances and Application Auto Scaling to scale resources from other services. The AWS Management Console provides a web interface for AWS Auto Scaling.

How AWS Auto Scaling Differences for AWS GovCloud (US)

- Predictive scaling is not available in the AWS GovCloud (US) Regions.
- The following CloudFormation resource is not available in the AWS GovCloud (US) Regions:
  - AWS::AutoScalingPlans::ScalingPlan
Documentation for AWS Auto Scaling

For more information about anything in the above list, see the documentation for the specific service at AWS documentation.

For information about scaling Amazon EC2 instances in AWS GovCloud (US), see Amazon EC2 Auto Scaling in this guide.

For more information about AWS Auto Scaling and Application Auto Scaling, see AWS Auto Scaling documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>• This service boundary exists entirely within the GovCloud regions and all export-controlled Content entered, processed, and created within Service will exist in the GovCloud regions.</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>• Scaling plan names</td>
</tr>
<tr>
<td></td>
<td>• Scaling policy names</td>
</tr>
<tr>
<td></td>
<td>• Scaling policy configurations</td>
</tr>
</tbody>
</table>

Application Auto Scaling

Application Auto Scaling is a web service for developers and system administrators who need a solution for automatically scaling their scalable resources for individual AWS services beyond Amazon EC2.

How Application Auto Scaling Differs for AWS GovCloud (US)

• Using Amazon EventBridge with Application Auto Scaling events (Scaled to Max) in the AWS GovCloud (US) Regions is not currently supported.
• Application Auto Scaling notifications are not currently supported in the AWS Personal Health Dashboard in the AWS GovCloud (US) Regions.
• The following resources are not currently supported for Application Auto Scaling in the AWS GovCloud (US-West) Region:
  • Amazon Keyspaces (for Apache Cassandra) tables
  • Spot Fleet requests
  • Custom resources
• The following resources are not currently supported for Application Auto Scaling in the AWS GovCloud (US-East) Region:
  • AppStream 2.0 fleets
• Amazon Comprehend document classification and entity recognizer endpoints
• Amazon Keyspaces (for Apache Cassandra) tables
• SageMaker endpoint variants
• Spot Fleet requests
• Custom resources

Documentation for Application Auto Scaling

For more information about anything in the above list, see the documentation for the specific service at AWS documentation.

For information about scaling Amazon EC2 instances in AWS GovCloud (US), see Amazon EC2 Auto Scaling in this guide.

For more information about AWS Auto Scaling and Application Auto Scaling, see AWS Auto Scaling documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>• This service boundary exists entirely within the GovCloud regions and all export-controlled Content entered, processed, and created within Service will exist in the GovCloud regions.</td>
<td>• Auto Scaling is not permitted to contain ITAR-regulated data.</td>
</tr>
<tr>
<td>• For example, do not enter ITAR-regulated data in the following fields:</td>
<td>• Auto Scaling is not permitted to contain ITAR-regulated data.</td>
</tr>
<tr>
<td>• Scaling policy names</td>
<td>• Auto Scaling is not permitted to contain ITAR-regulated data.</td>
</tr>
<tr>
<td>• Scaling policy configuration</td>
<td>• Auto Scaling is not permitted to contain ITAR-regulated data.</td>
</tr>
</tbody>
</table>

Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling helps you ensure that you have the correct number of Amazon EC2 instances available to handle the load for your application. You create collections of EC2 instances, called Auto Scaling groups. You can specify the minimum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes below this size. You can specify the maximum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes above this size.

How Amazon EC2 Auto Scaling Differs for AWS GovCloud (US)

• Amazon EC2 provides other restrictions. For more information, see Amazon Elastic Compute Cloud documentation.
• You can access Amazon EC2 Auto Scaling using the Amazon EC2 Auto Scaling API and command line interface (CLI) as well as the Amazon EC2 console.
Documentation for Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>• This service boundary exists entirely within the GovCloud regions and all export-controlled Content entered, processed, and created within Service will exist in the GovCloud regions.</td>
<td>• Auto Scaling is not permitted to contain ITAR-regulated data.</td>
</tr>
<tr>
<td>• For example, do not enter ITAR-regulated data in the following fields:</td>
<td>• Capacity group tag names</td>
</tr>
<tr>
<td>• Capacity group tag name values</td>
<td>• Capacity group names</td>
</tr>
<tr>
<td>• Capacity group names</td>
<td>• Amazon EC2 Security Group names</td>
</tr>
<tr>
<td>• Scaling policies</td>
<td>• Launch notifications</td>
</tr>
<tr>
<td>• Notification topics</td>
<td>• Policy documents</td>
</tr>
</tbody>
</table>

AWS Batch

AWS Batch enables you to run batch computing workloads on the AWS Cloud. Batch computing is a common way for developers, scientists, and engineers to access large amounts of compute resources, and AWS Batch removes the undifferentiated heavy lifting of configuring and managing the required infrastructure, similar to traditional batch computing software. This service can efficiently provision resources in response to jobs submitted in order to eliminate capacity constraints, reduce compute costs, and deliver results quickly.

How AWS Batch Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

Documentation for AWS Batch

AWS Batch documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in the AWS GovCloud (US) Region. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in the AWS GovCloud (US) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:
AWS Backint Agent for SAP HANA

AWS Backint Agent for SAP HANA (AWS Backint Agent) is an SAP-certified backup and restore application for SAP HANA workloads running on Amazon EC2 instances in the cloud. AWS Backint Agent runs as a standalone application that integrates with your existing workflows to back up your SAP HANA database to Amazon S3 and to restore it using SAP HANA Cockpit, SAP HANA Studio, and SQL commands. AWS Backint Agent supports full, incremental, and differential backup of SAP HANA databases.

How AWS Backint Agent for SAP HANA Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) Region and the standard AWS Regions.

Documentation for AWS Backint Agent for SAP HANA

AWS Backint Agent for SAP HANA documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 EC2 instance and ephemeral drives provisioned by AWS can contain ITAR-controlled data.</td>
<td>Do not enter ITAR-regulated data in the following:</td>
</tr>
<tr>
<td></td>
<td>• Job Definitions API attributes</td>
</tr>
<tr>
<td></td>
<td>• Job Queues API attributes</td>
</tr>
<tr>
<td></td>
<td>• Compute Environments API attributes</td>
</tr>
<tr>
<td></td>
<td>• Job API attributes</td>
</tr>
<tr>
<td></td>
<td>• Tags</td>
</tr>
</tbody>
</table>

AWS Backup

AWS Backup is a fully managed backup service that makes it easy to centralize and automate the backup of data across AWS services in the cloud and on premises. Using AWS Backup, you can configure backup
policies and monitor backup activity for your AWS resources in one place. AWS Backup automates and consolidates backup tasks that were previously performed service-by-service, and removes the need to create custom scripts and manual processes. With just a few clicks on the AWS Backup console, you can create backup policies that automate backup schedules and retention management.

How AWS Backup Differs for AWS GovCloud (US)

• The Cross-account Management feature is not available in AWS GovCloud (US) Region.

Documentation for AWS Backup

AWS Backup documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>• ITAR-regulated data may be backed up and managed using AWS Backup.</td>
<td>• Do not enter ITAR-regulated data in resource tag, plan names, rule names, selection names, or vault names.</td>
</tr>
</tbody>
</table>

AWS Certificate Manager

AWS Certificate Manager (ACM) makes it easy to provision, manage, and deploy SSL/TLS certificates on AWS managed resources.

How AWS Certificate Manager Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

Documentation for AWS Certificate Manager

AWS Certificate Manager documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, this section does not apply to you. The following information identifies the ITAR boundary for this service:
AWS Certificate Manager Private Certificate Authority

AWS Certificate Manager Private Certificate Authority (ACM PCA) is a managed private CA service with which you can easily and security manage your CA infrastructure and your private certificates.

How ACM PCA Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

Documentation for ACM PCA

AWS Certificate Manager Private Certificate Authority documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in the AWS GovCloud (US) Region. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled 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>• This service boundary exists entirely within the GovCloud regions and all export-controlled Content entered, processed, and created within Service will exist in the GovCloud regions.</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>

Amazon Cloud Directory

This service is currently available in AWS GovCloud (US-West) only.

Amazon Cloud Directory is a high-performance, serverless, hierarchical data store. Cloud Directory is a highly scalable multi-tenant service that makes it easy for customers to organize and manage all their
multi-dimensional data such as users, groups, locations, and devices and the rich relationships between them. Amazon Cloud Directory automatically scales to hundreds of millions of objects and provides an extensible schema that can be shared with multiple applications. As a serverless data store, Cloud Directory eliminates time-consuming and expensive administrative tasks, such as scaling infrastructure and managing servers. Cloud Directory is targeted for use cases such as human resources applications, course catalogs, device registry and network topology. Additionally, customer applications that need fine-grained permissions (Authorization) are well suited to leverage capabilities in Cloud Directory.

How Amazon Cloud Directory Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

Documentation for Amazon Cloud Directory

Amazon Cloud Directory documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in the AWS GovCloud (US) Region. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled 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 stored in Amazon Cloud Directory can contain ITAR-regulated data.</td>
<td>Amazon Cloud Directory metadata is not permitted to contain ITAR-regulated data. This metadata includes configuration data that you enter when creating and maintaining your Cloud Directory. Do not enter ITAR-regulated data in the following fields:</td>
</tr>
<tr>
<td></td>
<td>• Schema name</td>
</tr>
<tr>
<td></td>
<td>• Directory name</td>
</tr>
</tbody>
</table>

AWS CloudFormation

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

How AWS CloudFormation Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.
Documentation for AWS CloudFormation

AWS CloudFormation documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>• The user data section of AWS CloudFormation templates can refer to scripts containing ITAR-regulated. The scripts containing ITAR-regulated data must be stored in an AWS GovCloud (US) Amazon S3 bucket.</td>
<td>• No ITAR-regulated data may be entered, stored, or processed by AWS CloudFormation. For example, AWS CloudFormation metadata is not permitted to contain ITAR-regulated data. This metadata includes all the configuration data that you enter when creating and maintaining your AWS CloudFormation templates.</td>
</tr>
<tr>
<td>• ITAR-regulated data may be stored and processed on the instances launched using AWS CloudFormation.</td>
<td></td>
</tr>
</tbody>
</table>

Amazon Comprehend

This service is currently available in AWS GovCloud (US-West) only.

Amazon Comprehend uses natural language processing (NLP) to extract insights about the content of documents without the need of any special preprocessing. Amazon Comprehend processes any text files in UTF-8 format. It develops insights by recognizing the entities, key phrases, language, sentiments, and other common elements in a document. Use Amazon Comprehend to create new products based on understanding the structure of documents. With Amazon Comprehend you can search social networking feeds for mentions of products, scan an entire document repository for key phrases, or determine the topics contained in a set of documents. To extract insights from clinical documents such as doctor’s notes or clinical trial reports, use Amazon Comprehend Medical.

How Amazon Comprehend Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

Documentation for Amazon Comprehend

Amazon Comprehend documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in the AWS GovCloud (US-West) Region. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in the AWS GovCloud (US-West) Region, this section does not apply to you. The following information identifies the ITAR boundary for this service:
AWS DataSync

AWS DataSync is a data transfer service that makes it easy for you to automate moving data between on-premises storage and Amazon S3 or Amazon Elastic File System (Amazon EFS). DataSync automatically handles many of the tasks related to data transfers that can slow down migrations or burden your IT operations, including running your own instances, handling encryption, managing scripts, network optimization, and data integrity validation. You can use DataSync to transfer data at speeds up to 10 times faster than open-source tools. DataSync uses an on-premises software agent to connect to your existing storage or file systems using the Network File System (NFS) protocol, so you don’t have to write scripts or modify your applications to work with AWS APIs. You can use DataSync to copy data over AWS Direct Connect or internet links to AWS. The service enables one-time data migrations, recurring data processing workflows, and automated replication for data protection and recovery. Getting started with DataSync is easy: Deploy the DataSync agent on premises, connect it to a file system or storage array, select Amazon EFS or S3 as your AWS storage, and start moving data. You pay only for the data you copy.

How AWS DataSync Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

Documentation for AWS DataSync

AWS DataSync documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in the AWS GovCloud (US) Region. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled 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>• ITAR-regulated data may be stored and processed on the resources provisioned using AWS DataSync so long as those services are utilized in an ITAR-compliant fashion.</td>
<td>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</td>
</tr>
</tbody>
</table>
AWS CloudHSM

AWS CloudHSM offers secure cryptographic key storage for customers by providing managed hardware security modules in the AWS Cloud.

How AWS CloudHSM Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

Documentation for AWS CloudHSM

AWS CloudHSM documentation.

ITAR Boundary

AWS CloudHSM offers secure cryptographic key storage for customers by providing managed hardware security modules in the AWS Cloud.

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 secret access keys are protected as ITAR-regulated data.</td>
<td>• AWS CloudHSM metadata is not permitted to contain ITAR-regulated data. This includes all configuration data that you enter when creating and maintaining your AWS CloudHSM config. Audit and syslogs should not contain ITAR-regulated data.</td>
</tr>
</tbody>
</table>

AWS CloudHSM Root Certificate

If you choose to verify the identity of an HSM, be sure to use the root certificate for the AWS GovCloud (US) region rather than the root certificate that is available for commercial regions. You can download the certificate from AWS-US-GOV_CloudHSM_Root_G1.zip. Verification is an optional step that you can perform after you create an HSM. For more information about AWS CloudHSM, see the AWS CloudHSM User Guide. For more information about AWS CloudHSM Classic, see the AWS CloudHSM Classic User Guide.

AWS CloudHSM Classic

AWS CloudHSM Classic helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated HSM appliances within the AWS cloud. AWS and AWS Marketplace partners offer a variety of solutions for protecting sensitive data within the AWS platform, but additional protection is necessary for some applications and data that are subject to strict contractual or regulatory requirements for managing cryptographic keys.
How AWS CloudHSM Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

Documentation for AWS CloudHSM

AWS CloudHSM Classic documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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

With AWS CloudTrail, you can monitor your AWS deployments in the cloud by getting a history of AWS API calls for your account, including API calls made via the AWS Management Console, the AWS SDKs, the command line tools, and higher-level AWS services. You can also identify which users and accounts called AWS APIs for services that support CloudTrail, the source IP address the calls were made from, and when the calls occurred. You can integrate CloudTrail into applications using the API, automate trail creation for your organization, check the status of your trails, and control how administrators turn CloudTrail logging on and off.

How AWS CloudTrail Differs for AWS GovCloud (US)

The following list details the differences for using this service in AWS GovCloud (US) Regions 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.
• If you are using AWS Direct Connect, you must enable CloudTrail in your standard 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 AWS GovCloud (US) Regions. For more information, see Amazon Resource Names (ARNs) in GovCloud (US) Regions (p. 32).
• To enable CloudTrail to write log files to your bucket in AWS GovCloud (US) Regions, 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.

```
{
  "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 AWS GovCloud (US) Regions, 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.

Documentation for AWS CloudTrail

AWS CloudTrail documentation.

Services Supported within CloudTrail

The following services are supported in the AWS GovCloud (US-West) Region:

<table>
<thead>
<tr>
<th>AWS Service</th>
<th>Support Start Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Certificate Manager</td>
<td>03/25/2016</td>
</tr>
<tr>
<td>AWS Certificate Manager Private Certificate Authority</td>
<td>06/06/2019</td>
</tr>
<tr>
<td>API Gateway</td>
<td>07/09/2015</td>
</tr>
<tr>
<td>AWS Service</td>
<td>Support Start Date</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Amazon Athena</td>
<td>05/19/2017</td>
</tr>
<tr>
<td>Application Auto Scaling</td>
<td>10/31/2016</td>
</tr>
<tr>
<td>Amazon Cloud Directory</td>
<td>01/26/2017</td>
</tr>
<tr>
<td>AWS CloudFormation</td>
<td>04/02/2014</td>
</tr>
<tr>
<td>AWS CloudHSM</td>
<td>01/08/2014</td>
</tr>
<tr>
<td>AWS CloudTrail</td>
<td>11/13/2015</td>
</tr>
<tr>
<td>AWS CodeBuild</td>
<td>12/01/2013</td>
</tr>
<tr>
<td>AWS CodeCommit</td>
<td>01/11/2016</td>
</tr>
<tr>
<td>AWS CodeDeploy</td>
<td>12/16/2014</td>
</tr>
<tr>
<td>AWS CodePipeline</td>
<td>07/09/2015</td>
</tr>
<tr>
<td>Amazon Comprehend</td>
<td>01/17/2018</td>
</tr>
<tr>
<td>AWS Config</td>
<td>02/10/2015</td>
</tr>
<tr>
<td>AWS DataSync</td>
<td>11/26/2018</td>
</tr>
<tr>
<td>AWS Direct Connect</td>
<td>03/08/2014</td>
</tr>
<tr>
<td>AWS Database Migration Service</td>
<td>02/04/2016</td>
</tr>
<tr>
<td>AWS Directory Service</td>
<td>05/14/2015</td>
</tr>
<tr>
<td>Amazon DynamoDB</td>
<td>05/28/2015</td>
</tr>
<tr>
<td>Amazon Elastic Compute Cloud</td>
<td>11/13/2013</td>
</tr>
<tr>
<td>Amazon Elastic Container Registry</td>
<td>12/21/2015</td>
</tr>
<tr>
<td>Amazon Elastic Container Service</td>
<td>04/09/2015</td>
</tr>
<tr>
<td>Amazon ElastiCache</td>
<td>09/15/2014</td>
</tr>
<tr>
<td>AWS Elastic Beanstalk</td>
<td>03/31/2014</td>
</tr>
<tr>
<td>Amazon Elastic File System</td>
<td>06/28/2016</td>
</tr>
<tr>
<td>Elastic Load Balancing</td>
<td>04/04/2014</td>
</tr>
<tr>
<td>Amazon Elastic Map Reduce (EMR)</td>
<td>04/04/2014</td>
</tr>
<tr>
<td>Amazon Elasticsearch Service</td>
<td>10/01/2015</td>
</tr>
<tr>
<td>Amazon CloudWatch Events</td>
<td>01/16/2016</td>
</tr>
<tr>
<td>Amazon Kinesis Data Firehose</td>
<td>03/17/2016</td>
</tr>
<tr>
<td>Amazon S3 Glacier</td>
<td>12/11/2014</td>
</tr>
<tr>
<td>AWS Glue</td>
<td>11/07/2017</td>
</tr>
<tr>
<td>AWS IoT Greengrass</td>
<td>10/29/2018</td>
</tr>
</tbody>
</table>
## Services Supported within CloudTrail

<table>
<thead>
<tr>
<th>AWS Service</th>
<th>Support Start Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon GuardDuty</td>
<td>02/12/2018</td>
</tr>
<tr>
<td>AWS Health</td>
<td>11/21/2016</td>
</tr>
<tr>
<td>AWS Identity and Access Management</td>
<td>11/13/2013</td>
</tr>
<tr>
<td>Amazon Inspector</td>
<td>04/20/2016</td>
</tr>
<tr>
<td>AWS IoT</td>
<td>04/11/2016</td>
</tr>
<tr>
<td>Amazon Kinesis</td>
<td>04/25/2016</td>
</tr>
<tr>
<td>AWS Key Management Service</td>
<td>11/12/2014</td>
</tr>
<tr>
<td>AWS Lambda</td>
<td>04/09/2015</td>
</tr>
<tr>
<td>AWS License Manager</td>
<td>03/01/2019</td>
</tr>
<tr>
<td>Amazon CloudWatch Logs</td>
<td>03/10/2016</td>
</tr>
<tr>
<td>AWS Elemental MediaConvert</td>
<td>11/27/2017</td>
</tr>
<tr>
<td>AWS Marketplace Marketing Service</td>
<td>08/22/2018</td>
</tr>
<tr>
<td>Amazon CloudWatch</td>
<td>04/30/2014</td>
</tr>
<tr>
<td>AWS Organizations</td>
<td>02/27/2017</td>
</tr>
<tr>
<td>Amazon Polly</td>
<td>11/30/2016</td>
</tr>
<tr>
<td>AWS Resource Access Manager</td>
<td>11/20/2018</td>
</tr>
<tr>
<td>Amazon Relational Database Service</td>
<td>11/13/2013</td>
</tr>
<tr>
<td>Amazon Redshift</td>
<td>06/10/2013</td>
</tr>
<tr>
<td>Amazon Rekognition</td>
<td>04/06/2018</td>
</tr>
<tr>
<td>AWS Resource Groups</td>
<td>06/29/2018</td>
</tr>
<tr>
<td>Amazon Route 53</td>
<td>02/11/2015</td>
</tr>
<tr>
<td>Amazon Route 53 Resolver</td>
<td>02/11/2015</td>
</tr>
<tr>
<td>Amazon Simple Storage Service</td>
<td>09/01/2015</td>
</tr>
<tr>
<td>Amazon SageMaker</td>
<td>01/11/2018</td>
</tr>
<tr>
<td>AWS Secrets Manager</td>
<td>04/05/2018</td>
</tr>
<tr>
<td>AWS Serverless Application Repository</td>
<td>02/20/2018</td>
</tr>
<tr>
<td>AWS Service Catalog</td>
<td>07/06/2016</td>
</tr>
<tr>
<td>AWS Server Migration Service</td>
<td>11/14/2016</td>
</tr>
<tr>
<td>AWS Snowball</td>
<td>01/25/2019</td>
</tr>
<tr>
<td>Amazon Simple Notification Service</td>
<td>10/09/2014</td>
</tr>
<tr>
<td>Amazon Simple Queue Service</td>
<td>07/16/2014</td>
</tr>
<tr>
<td>AWS Service</td>
<td>Support Start Date</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>AWS Systems Manager</td>
<td>11/13/2013</td>
</tr>
<tr>
<td>AWS Step Functions</td>
<td>12/01/2016</td>
</tr>
<tr>
<td>AWS Storage Gateway</td>
<td>12/16/2014</td>
</tr>
<tr>
<td>AWS Security Token Service</td>
<td>11/13/2013</td>
</tr>
<tr>
<td>Amazon Simple Workflow Service</td>
<td>05/13/2013</td>
</tr>
<tr>
<td>AWS Resource Groups Tagging API</td>
<td>06/29/2018</td>
</tr>
<tr>
<td>Amazon Transcribe</td>
<td>06/28/2018</td>
</tr>
<tr>
<td>Amazon Translate</td>
<td>04/04/2018</td>
</tr>
<tr>
<td>AWS WAF</td>
<td>04/28/2016</td>
</tr>
<tr>
<td>Amazon WorkSpaces</td>
<td>04/09/2015</td>
</tr>
<tr>
<td>AWS X-Ray</td>
<td>04/25/2018</td>
</tr>
</tbody>
</table>

The following services are supported in the AWS GovCloud (US-East) Region:

<table>
<thead>
<tr>
<th>AWS Service</th>
<th>Support Start Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Certificate Manager</td>
<td>03/25/2016</td>
</tr>
<tr>
<td>AWS Certificate Manager Private Certificate Authority</td>
<td>06/06/2019</td>
</tr>
<tr>
<td>API Gateway</td>
<td>07/09/2015</td>
</tr>
<tr>
<td>Amazon Athena</td>
<td>05/19/2017</td>
</tr>
<tr>
<td>Application Auto Scaling</td>
<td>10/31/2016</td>
</tr>
<tr>
<td>AWS CloudFormation</td>
<td>04/02/2014</td>
</tr>
<tr>
<td>AWS CloudHSM</td>
<td>01/08/2015</td>
</tr>
<tr>
<td>AWS CloudTrail</td>
<td>11/13/2013</td>
</tr>
<tr>
<td>AWS CodeBuild</td>
<td>12/01/2016</td>
</tr>
<tr>
<td>AWS CodeCommit</td>
<td>01/11/2017</td>
</tr>
<tr>
<td>AWS CodeDeploy</td>
<td>12/16/2014</td>
</tr>
<tr>
<td>AWS Config</td>
<td>02/10/2015</td>
</tr>
<tr>
<td>AWS Direct Connect</td>
<td>03/08/2014</td>
</tr>
<tr>
<td>AWS Database Migration Service</td>
<td>02/04/2016</td>
</tr>
<tr>
<td>AWS Directory Service</td>
<td>05/14/2015</td>
</tr>
<tr>
<td>Amazon DynamoDB</td>
<td>05/28/2015</td>
</tr>
<tr>
<td>Amazon Elastic Compute Cloud</td>
<td>11/13/2013</td>
</tr>
</tbody>
</table>
## Services Supported within CloudTrail

<table>
<thead>
<tr>
<th>AWS Service</th>
<th>Support Start Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Elastic Container Registry</td>
<td>12/21/2015</td>
</tr>
<tr>
<td>Amazon Elastic Container Service</td>
<td>04/09/2015</td>
</tr>
<tr>
<td>Amazon ElastiCache</td>
<td>09/15/2014</td>
</tr>
<tr>
<td>AWS Elastic Beanstalk</td>
<td>03/31/2014</td>
</tr>
<tr>
<td>Elastic Load Balancing</td>
<td>04/04/2014</td>
</tr>
<tr>
<td>Amazon Elastic Map Reduce (EMR)</td>
<td>04/04/2014</td>
</tr>
<tr>
<td>Amazon Elasticsearch Service</td>
<td>10/01/2015</td>
</tr>
<tr>
<td>Amazon CloudWatch Events</td>
<td>01/16/2016</td>
</tr>
<tr>
<td>Amazon Kinesis Data Firehose</td>
<td>03/17/2016</td>
</tr>
<tr>
<td>Amazon S3 Glacier</td>
<td>12/11/2014</td>
</tr>
<tr>
<td>AWS Glue</td>
<td>11/07/2017</td>
</tr>
<tr>
<td>AWS Identity and Access Management</td>
<td>11/13/2013</td>
</tr>
<tr>
<td>Amazon Inspector</td>
<td>04/20/2016</td>
</tr>
<tr>
<td>Amazon Kinesis</td>
<td>04/25/2014</td>
</tr>
<tr>
<td>AWS Key Management Service</td>
<td>11/12/2014</td>
</tr>
<tr>
<td>AWS Lambda</td>
<td>04/09/2015</td>
</tr>
<tr>
<td>AWS License Manager</td>
<td>03/01/2019</td>
</tr>
<tr>
<td>Amazon CloudWatch Logs</td>
<td>03/10/2019</td>
</tr>
<tr>
<td>AWS Marketplace Marketing Service</td>
<td>08/22/2016</td>
</tr>
<tr>
<td>Amazon CloudWatch</td>
<td>04/30/2018</td>
</tr>
<tr>
<td>AWS Resource Access Manager</td>
<td>11/20/2018</td>
</tr>
<tr>
<td>Amazon Relational Database Service</td>
<td>11/13/2013</td>
</tr>
<tr>
<td>Amazon Redshift</td>
<td>06/10/2014</td>
</tr>
<tr>
<td>AWS Resource Groups</td>
<td>06/29/2018</td>
</tr>
<tr>
<td>Amazon Route 53 Resolver</td>
<td>02/11/2015</td>
</tr>
<tr>
<td>Amazon Simple Storage Service</td>
<td>09/01/2015</td>
</tr>
<tr>
<td>AWS Secrets Manager</td>
<td>04/05/2018</td>
</tr>
<tr>
<td>AWS Serverless Application Repository</td>
<td>02/20/2018</td>
</tr>
<tr>
<td>AWS Server Migration Service</td>
<td>11/14/2016</td>
</tr>
<tr>
<td>AWS Snowball</td>
<td>01/25/2019</td>
</tr>
<tr>
<td>Amazon Simple Notification Service</td>
<td>10/09/2014</td>
</tr>
<tr>
<td>AWS Service</td>
<td>Support Start Date</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Amazon Simple Queue Service</td>
<td>07/16/2014</td>
</tr>
<tr>
<td>AWS Systems Manager</td>
<td>11/13/2013</td>
</tr>
<tr>
<td>AWS Step Functions</td>
<td>12/01/2016</td>
</tr>
<tr>
<td>AWS Security Token Service</td>
<td>11/13/2013</td>
</tr>
<tr>
<td>Amazon Simple Workflow Service</td>
<td>05/13/2014</td>
</tr>
<tr>
<td>AWS Resource Groups Tagging API</td>
<td>06/29/2018</td>
</tr>
<tr>
<td>Amazon Transcribe</td>
<td>06/28/2018</td>
</tr>
</tbody>
</table>

**ITAR Boundary**

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>• This service boundary exists entirely within the GovCloud regions and all export-controlled Content entered, processed, and created within Service will exist in the GovCloud regions.</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**

Use CloudWatch Events to send system events from AWS resources to AWS Lambda functions, Amazon SNS topics, streams in Amazon Kinesis, and other target types.

**How Amazon CloudWatch Differs for AWS GovCloud (US)**

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

**Documentation for Amazon CloudWatch**

Amazon CloudWatch documentation.

**ITAR Boundary**

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you
must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>• This service boundary exists entirely within the GovCloud regions and all export-controlled Content entered, processed, and created within Service will exist in the GovCloud regions.</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:</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>
</tbody>
</table>

Amazon CloudWatch Events

Use CloudWatch Events to send system events from AWS resources to AWS Lambda functions, Amazon SNS topics, streams in Amazon Kinesis, and other target types.

How Amazon CloudWatch Events Differs for AWS GovCloud (US)

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

Documentation for Amazon CloudWatch Events

Amazon CloudWatch Events documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>• This service boundary exists entirely within the GovCloud regions and all export-controlled Content entered, processed, and created within Service will exist in the GovCloud regions.</td>
<td>No ITAR-regulated data may be entered, stored, or processed by CloudWatch Events. For example,</td>
</tr>
</tbody>
</table>
Amazon CloudWatch Logs

Use CloudWatch Logs to monitor, store, and access your log files from Amazon EC2 instances, AWS CloudTrail, or other sources.

How Amazon CloudWatch Logs Differs for AWS GovCloud (US)

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

Documentation for Amazon CloudWatch Logs

Amazon CloudWatch Logs documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>- This service boundary exists entirely within the GovCloud regions and all export-controlled Content entered, processed, and created within Service will exist in the GovCloud regions.</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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content entered, processed, and created within Service will exist in the GovCloud regions.</td>
<td>CloudWatch Events 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 Events alarms.</td>
</tr>
<tr>
<td></td>
<td>For example, do not enter ITAR-regulated data in the following field:</td>
</tr>
<tr>
<td></td>
<td>- Rule names</td>
</tr>
<tr>
<td></td>
<td>- Rule descriptions</td>
</tr>
<tr>
<td></td>
<td>- Event patterns</td>
</tr>
<tr>
<td></td>
<td>- Data input to APIs</td>
</tr>
</tbody>
</table>
AWS CodeBuild

AWS CodeBuild is a fully managed continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy. With CodeBuild, you don't need to provision, manage, and scale your own build servers. CodeBuild scales continuously and processes multiple builds concurrently, so your builds are not left waiting in a queue. You can get started quickly by using prepackaged build environments, or you can create custom build environments that use your own build tools. With CodeBuild, you are charged by the minute for the compute resources you use.

How AWS CodeBuild Differs for AWS GovCloud (US)

- The Linux GPU and Arm environment types are not available in the AWS GovCloud (US) Regions.
- The 2xlarge compute type is not available in the AWS GovCloud (US) Regions.

Documentation for AWS CodeBuild

AWS CodeBuild documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in the AWS GovCloud (US) Region. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled 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 CodeBuild support ITAR-regulated data.</td>
<td>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</td>
</tr>
</tbody>
</table>

AWS CodeCommit

AWS CodeCommit is a fully-managed source control service that hosts secure Git-based repositories. It makes it easy for teams to collaborate on code in a secure and highly scalable ecosystem. CodeCommit
AWS GovCloud (US) User Guide
How AWS CodeCommit Differs for AWS GovCloud (US)

eliminates the need to operate your own source control system or worry about scaling its infrastructure. You can use CodeCommit to securely store anything from source code to binaries, and it works seamlessly with your existing Git tools.

How AWS CodeCommit Differs for AWS GovCloud (US)

• The old console experience is not available in the AWS GovCloud (US) Regions. The documentation reflects the new console experience.
• Since AWS GovCloud (US) operates as isolated regions, you cannot share or use CodeCommit repositories and resources with other services outside of the regions. For example, you cannot use a CodeCommit repository in AWS GovCloud (US-West) as the source for a pipeline in CodePipeline that is not in the AWS GovCloud (US-West) Region.
• All policy statements must refer to the GovCloud ARNs for the AWS GovCloud (US) Regions. For example, policies for Amazon SNS notifications, CloudWatch Events rules, and trigger resources must use the AWS GovCloud (US) ARNs for those services. For more information, see Amazon Resource Names (ARNs) in AWS GovCloud.
• All IAM users and service roles must exist in the AWS GovCloud (US) Regions.

Documentation for AWS CodeCommit

AWS CodeCommit documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in the AWS GovCloud (US) Region. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled 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 CodeCommit support ITAR-regulated data.</td>
<td>The following CodeCommit metadata fields are not permitted to contain ITAR-regulated data:</td>
</tr>
</tbody>
</table>
| | • Repository name  
| | • Repository description  
| | • Branch name  
| | • Trigger name  
| | • SNS topic name  
| | • AWS Lambda topic name |

AWS CodeDeploy

AWS CodeDeploy is a deployment service that enables developers to automate the deployment of applications to instances and to update the applications as required.
How AWS CodeDeploy Differs for AWS GovCloud (US)

- The new AWS CodeDeploy console is not available in the AWS GovCloud (US) Regions
- Use SSL (HTTPS) when you make calls to the service in AWS GovCloud (US) Regions. In other regions, you can use HTTP or HTTPS.
- Several procedures in the 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 AWS GovCloud (US) Regions, the formats for accessing these resources do not follow the same patterns as for other regions.

Documentation for AWS CodeDeploy

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

**CodeDeploy Amazon S3 Resources Bucket**

Name of the Amazon S3 bucket containing CodeDeploy files:

```
aws-codedeploy-us-gov-west-1
```

**CodeDeploy Amazon S3 Bucket ARN**

ARN of the Amazon S3 bucket containing CodeDeploy files:

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

**wget Download Command**

wget command for downloading the 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 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 CodeDeploy deployments:
Links for Downloading CodeDeploy Installer and Updater (Windows Server)

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

- **Installer:**
  

- **Updater:**
  

For more information about AWS CodeDeploy, see the [AWS CodeDeploy documentation](https://aws.amazon.com/codeploy/).

**ITAR Boundary**

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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, including your application revision, managed in AWS CodeDeploy support ITAR-regulated data.</td>
<td>The following CodeDeploy metadata fields are not permitted to contain ITAR-regulated data:</td>
</tr>
<tr>
<td></td>
<td><strong>Application Details:</strong></td>
</tr>
<tr>
<td></td>
<td>• Name</td>
</tr>
<tr>
<td></td>
<td><strong>Deployment Groups:</strong></td>
</tr>
<tr>
<td></td>
<td>• Deployment group name</td>
</tr>
<tr>
<td></td>
<td>• Service Role name</td>
</tr>
<tr>
<td></td>
<td>• EC2 Auto Scaling group names</td>
</tr>
<tr>
<td></td>
<td>• EC2 instance tag key</td>
</tr>
<tr>
<td></td>
<td>• EC2 instance tag group name</td>
</tr>
<tr>
<td></td>
<td>• On-premise Instances tag key</td>
</tr>
<tr>
<td></td>
<td>• On-premise Instances tag group</td>
</tr>
<tr>
<td></td>
<td>• Load Balancer ALB target group</td>
</tr>
<tr>
<td></td>
<td>• Load Balancer NLB target group</td>
</tr>
<tr>
<td></td>
<td>• Deployment trigger name</td>
</tr>
<tr>
<td></td>
<td>• Deployment trigger SNS Topic</td>
</tr>
</tbody>
</table>
AWS CodePipeline

This service is currently available in AWS GovCloud (US-West) only.

AWS CodePipeline is a continuous delivery service you can use to model, visualize, and automate the steps required to release your software. You can quickly model and configure the different stages of a software release process. CodePipeline automates the steps required to release your software changes continuously.

How AWS CodePipeline Differs for AWS GovCloud (US)

The following actions/provider types are not supported:

- Custom actions
- Source Actions:
  - Amazon ECR
  - AWS CodeStar Source Connection (Bitbucket)
  - AWS CodeStar Source Connection (GitHub)
  - AWS CodeStar Source Connection (GitHub Enterprise Server)
  - GitHub
- Build Actions:
  - Jenkins
  - For the CodeBuild action, enabling batch builds is not supported. For the CodeBuild action type, the action configuration does not contain the following parameters : BatchEnabled, CombineArtifacts.
- Test Actions:
  - Device Farm
  - Jenkins
- Deploy Actions:
  - AWS Elastic Beanstalk
  - AWS OpsWorks
  - AWS Service Catalog
  - Amazon Alexa
  - AWS AppConfig
- Invoke Actions:
  - AWS Step Functions
- Since AWS GovCloud (US) operates as isolated regions, you cannot share or use CodePipeline resources with other services outside of the regions. For example, you cannot use a CodeCommit repository in
AWS GovCloud (US-West) as the source for a pipeline in CodePipeline that is not in the AWS GovCloud (US-West) Region.

- All policy statements must refer to the GovCloud ARNs for the AWS GovCloud (US) Region. For example, policies for AWS Artifact buckets, CloudWatch Events rules, and trigger resources must use the AWS GovCloud (US) ARNs for those services. For more information, see Amazon Resource Names (ARNs) in GovCloud (US) Regions (p. 32).
- All IAM users and service roles must exist in the AWS GovCloud (US) Region.
- For the CodeCommit source action, the full clone feature is supported. However, the default CodePipeline service role policy does not contain the necessary codecommit:GetRepository permission for the full clone feature. To use the feature, update your new or existing CodePipeline service role policy with the following policy statement:

```json
{
    "Action": [
        "codecommit:GetRepository"
    ],
    "Resource": "*",
    "Effect": "Allow"
}
```

Documentation for AWS CodePipeline

AWS CodePipeline documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in the AWS GovCloud (US) Region. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled 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 CodePipeline support ITAR-regulated data.</td>
<td>CodePipeline metadata fields are not permitted to contain ITAR-regulated data. For example, do not enter ITAR-regulated data in the following fields:</td>
</tr>
<tr>
<td></td>
<td>Pipeline Name</td>
</tr>
<tr>
<td></td>
<td>Stage Name</td>
</tr>
<tr>
<td></td>
<td>Action Name</td>
</tr>
<tr>
<td></td>
<td>CodeCommit Branch Name</td>
</tr>
<tr>
<td></td>
<td>GitHub Branch Name</td>
</tr>
</tbody>
</table>

Amazon Cognito

Amazon Cognito provides authentication, authorization, and user management for your web and mobile apps. Your users can sign in directly with a user name and password, or through a third party such as Facebook, Amazon, Google or Apple. The two main components of Amazon Cognito are user pools and identity pools. User pools are user directories that provide sign-up and sign-in options for your app users. Identity pools enable you to grant your users access to other AWS services. You can use identity pools and user pools separately or together.
How Amazon Cognito Differs for AWS GovCloud (US)

Below listed are the differences between the AWS GovCloud (US) and the standard AWS Regions.

- Advanced Security Features of User Pools is not supported in the AWS GovCloud (US).
- Pinpoint integration with User Pools is not supported in the AWS GovCloud (US).
- Custom domains for User Pools is not supported in the AWS GovCloud (US).

The IAM roles you configure to be used with Cognito identity pools must have a trust policy that allows Cognito to use them. In AWS GovCloud, those policies use the cognito-identity-us-gov.amazonaws.com name for Cognito identity pools, as shown in the example policy below.

```json
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Federated": "cognito-identity-us-gov.amazonaws.com"
      },
      "Action": "sts:AssumeRoleWithWebIdentity",
      "Condition": {
        "StringEquals": {
          "cognito-identity-us-gov.amazonaws.com:aud": "us-east-1:12345678-corner-cafe-123456790ab"
        },
        "ForAnyValue: StringLike": {
          "cognito-identity-us-gov.amazonaws.com:amr": "unauthenticated"
        }
      }
    }
  ]
}
```

Documentation for Amazon Cognito

Amazon Cognito documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>• Passwords and software token MFA seeds.</td>
<td>• Amazon Cognito metadata may be moved or stored outside of the AWS GovCloud (US) Region, or, in rare cases, accessed by certain AWS support personnel and system administrators who are not U.S. citizens.</td>
</tr>
</tbody>
</table>
Amazon Comprehend Medical

This service is currently available in AWS GovCloud (US-West) only.

Amazon Comprehend Medical detects useful information in unstructured clinical text. As much as 75 percent of all health record data is found in unstructured text such as physician's notes, discharge summaries, test results, and case notes. Amazon Comprehend Medical uses Natural Language Processing (NLP) models to sort through enormous quantities of data for valuable information gained through advances in machine learning.

How Amazon Comprehend Medical Differs for AWS GovCloud (US)

Below listed are the differences between the AWS GovCloud (US) and the standard AWS Regions.

Differences in Feature Availability:

- Ontology Linking features are not available.
- Service is only available in AWS GovCloud (US-West).

Differences in Quotas/Limits:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transactions per second (TPS) for the DetectEntities-v2 and DetectEntities operations</td>
<td>2</td>
</tr>
<tr>
<td>Transactions per second (TPS) for the DetectPHI operation</td>
<td>5</td>
</tr>
<tr>
<td>Transactions per second (TPS) for the StartEntitiesDetectionV2Job, StartPHIDetectionJob, StopEntitiesDetectionV2Job, StopPHIDetectionJob, ListEntitiesDetectionV2Jobs, ListPHIDetectionJobs, DescribeEntitiesDetectionV2Job, and DescribePHIDetectionJob operations</td>
<td>2</td>
</tr>
</tbody>
</table>

Documentation for Amazon Comprehend Medical

Amazon Comprehend Medical documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you
must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 text and documents processed by Amazon Comprehend Medical can contain ITAR-regulated data.</td>
<td>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</td>
</tr>
</tbody>
</table>

AWS Config

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

AWS Config and AWS Config Rules are supported in the AWS GovCloud (US) Region.

How AWS Config Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

Documentation for AWS Config

AWS Config documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>
| • AWS Config data is outside of the ITAR boundary.  
  • AWS Config does not include any ITAR-regulated data. | • 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:  
  • Annotations for rule evaluations  
  • Resource identifier  
  • S3 bucket name |
AWS Direct Connect

AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 1 gigabit or 10 gigabit Ethernet fiber-optic cable. One end of the cable is connected to your router, the other to an AWS Direct Connect router. With this connection in place, you can create virtual interfaces directly to the AWS cloud and Amazon Virtual Private Cloud, bypassing Internet service providers in your network path.

How AWS Direct Connect Differs for AWS GovCloud (US)

- To set up an AWS Direct Connect connection to AWS GovCloud (US) Regions, 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 AWS GovCloud (US) Regions using a public virtual interface and a VPN connection. For more information, see Setting Up AWS Direct Connect with a VPN Connection (p. 121).
- 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 AWS GovCloud (US) Regions (us-gov-west-1) only, or create an AWS Direct Connect gateway and use any AWS Direct Connect connection from any AWS Direct Connect location.
- An AWS Direct Connect gateway is supported between an AWS GovCloud (US) account and a linked public AWS account. From your AWS GovCloud (US) account, you can associate a virtual private gateway with an AWS Direct Connect gateway that’s in the linked account.
- Use the Amazon VPC section of the AWS GovCloud (US) console to set up hardware VPN access to AWS GovCloud (US) Regions 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 AWS Site-to-Site VPN Network Administrator Guide.

Documentation for AWS Direct Connect

AWS Direct Connect documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any

---

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNS topic name</td>
<td>Tag key</td>
</tr>
</tbody>
</table>

---

AWS GovCloud (US) User Guide

AWS Direct Connect

ITAR Boundary
ITAR-controlled data in AWS GovCloud (US) Regions, 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.</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-West) 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: Verify Your Virtual Public Interface**

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

**Step 3: Set Up Your VPN Over Your Public Virtual Interface**

Create your AWS GovCloud (US-West) 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.

AWS Directory Service

AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud.
AWS Managed Microsoft AD is built on actual Microsoft Active Directory and does not require you to synchronize or replicate data from your existing Active Directory to the cloud. You can use standard Active Directory administration tools and take advantage of built-in Active Directory features, such as Group Policy and single sign-on (SSO). With AWS Managed Microsoft AD, you can easily join Amazon EC2 and Amazon RDS for SQL Server instances to your domain, and use AWS Enterprise IT applications such as Amazon WorkSpaces with Active Directory users and groups.

How AWS Directory Service Differs for AWS GovCloud (US)

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

- Only AWS Managed Microsoft AD and AD Connector directory types are supported by AWS Directory Service.
- The following directory types are not supported:
  - Simple AD
  - Amazon Cloud Directory
- The following AWS apps and services are not currently supported by AWS Directory Service:
  - RDS for SQL Server
  - Amazon WorkDocs
  - Amazon WorkMail
  - Amazon QuickSight
  - Amazon Chime
  - Amazon Connect
  - AWS Management Console
  - AWS Single Sign-On
- Only signature version 4 signing is supported.
- You can use the AWS Command Line Interface (AWS CLI) to interact with AWS Directory Service and other AWS services through the command line. For more information, see AWS CLI documentation.

  **Note**
  
  If you are using the Amazon Linux AMI, the AWS CLI is already installed and configured.

- To connect to AWS Directory Service by using the command line or APIs, use the following endpoints:
  - https://ds-fips.us-gov-west-1.amazonaws.com
  - https://ds.us-gov-west-1.amazonaws.com
  - https://ds-fips.us-gov-east-1.amazonaws.com
  - https://ds.us-gov-east-1.amazonaws.com

Documentation for AWS Directory Service

AWS Directory Service documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, this section does not apply to you. The following information identifies the ITAR boundary for this service:
AWS Database Migration Service

AWS Database Migration Service is a web service you can use to migrate data from your database that is on-premises, on an Amazon Relational Database Service (Amazon RDS) DB instance, or in a database on an Amazon Elastic Compute Cloud (Amazon EC2) instance to a database on an AWS service. These services can include a database on Amazon RDS or a database on an Amazon EC2 instance. You can also migrate a database from an AWS service to an on-premises database. You can migrate data between heterogeneous or homogenous database engines.

How AWS Database Migration Service Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

Documentation for AWS Database Migration Service

AWS Database Migration Service documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 customer-defined configurations. This metadata includes all configuration data in console fields,</td>
<td>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields,</td>
</tr>
</tbody>
</table>
AWS Deep Learning AMIs

The AWS Deep Learning AMIs equip machine learning practitioners and researchers with the infrastructure and tools to accelerate deep learning in the cloud at any scale. You can quickly launch Amazon EC2 instances on Amazon Linux or Ubuntu, preinstalled with popular deep learning frameworks. Examples include Apache MXNet and Gluon, TensorFlow, the Microsoft Cognitive Toolkit (CNTK), Caffe, Caffe2, Theano, Torch and Keras. You can use these frameworks to train sophisticated, custom AI models; experiment with new algorithms; or to learn new skills and techniques.

How AWS Deep Learning AMI Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

Documentation for AWS Deep Learning AMI

AWS Deep Learning AMIs documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 GovCloud (US) Regions can contain ITAR-regulated data.</td>
<td>descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</td>
</tr>
</tbody>
</table>

Amazon DocumentDB (with MongoDB compatibility)

Amazon DocumentDB (with MongoDB compatibility) is a fast, scalable, highly available, and fully managed document database service that supports MongoDB workloads. As a document database, Amazon DocumentDB makes it easy to store, query, and index JSON data.
Amazon DocumentDB is a non-relational database service designed from the ground-up to give you the performance, scalability, and availability you need when operating mission-critical MongoDB workloads at scale. In Amazon DocumentDB, the storage and compute are decoupled, allowing each to scale independently. You can increase the read capacity to millions of requests per second by adding up to 15 low latency read replicas in minutes, regardless of the size of your data.

**How Amazon DocumentDB Differs for AWS GovCloud (US)**

- Copying [cluster snapshots](#) from other AWS Regions to the AWS GovCloud (US) Regions or from AWS GovCloud (US) Regions to other regions is not supported.

**Documentation for Amazon DocumentDB**

Amazon DocumentDB documentation.

**ITAR Boundary**

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 DocumentDB master passwords are protected as ITAR-regulated data. All data stored and processed in Amazon DocumentDB database collections can contain ITAR-regulated data. You cannot transfer ITAR-regulated data in and out of your Amazon DocumentDB cluster using the API or CLI. You must use database tools for data transfer of ITAR-regulated data.</td>
<td>Amazon DocumentDB metadata is not permitted to contain ITAR-regulated data. This metadata includes all configuration data that you enter when creating and maintaining your Amazon DocumentDB cluster except the master password. Do not enter ITAR-regulated data in the following fields:</td>
</tr>
</tbody>
</table>
| | • Cluster Identifier  
| | • Instance identifier  
| | • Master user name  
| | • Database name  
| | • Snapshot name  
| | • Security group name  
| | • Security group description  
| | • Cluster parameter group name  
| | • Cluster parameter group description  
| | • Subnet group name  
| | • Subnet group description  
| | • Resource tags |

If you are processing ITAR-regulated data with Amazon DocumentDB, 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 DocumentDB Master Password.

• After you create your cluster, change the master password of your Amazon DocumentDB cluster by directly using the AWS Management Console or AWS CLI.

• 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 DocumentDB.

• 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 DocumentDB cluster, 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-West) 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 cluster, especially when an Internet gateway is attached to the VPC. Only allow connections that are from the AWS GovCloud (US-West) 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 Service Endpoints.

Amazon DynamoDB

Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. You can use Amazon DynamoDB to create a database table that can store and retrieve any amount of data, and serve any level of request traffic. Amazon DynamoDB automatically spreads the data and traffic for the table over a sufficient number of servers to handle the request capacity specified by the customer and the amount of data stored, while maintaining consistent and fast performance.

How Amazon DynamoDB Differs for AWS GovCloud (US)

• Import Table is not available in the DynamoDB console.

• Export Table is not available in the DynamoDB console.

Documentation for Amazon DynamoDB

Amazon DynamoDB documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any
ITAR-controlled data in AWS GovCloud (US) Regions, 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. • Do not enter ITAR-regulated data in the following fields: • Table names • Hash attribute names • Range attribute names • 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 Service Endpoints (p. 62).

AWS Elastic Beanstalk

With AWS Elastic Beanstalk, you can quickly deploy and manage applications in the AWS Cloud without worrying about the infrastructure that runs those applications. AWS Elastic Beanstalk reduces management complexity without restricting choice or control. You simply upload your application, and AWS Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring.

How AWS Elastic Beanstalk Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

Documentation for AWS Elastic Beanstalk

AWS Elastic Beanstalk documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 code uploaded to AWS Elastic Beanstalk can contain ITAR-regulated data.</td>
<td>The following AWS Elastic Beanstalk metadata fields are not permitted to contain ITAR-regulated data:</td>
</tr>
</tbody>
</table>
Amazon EBS

Amazon Elastic Block Store (Amazon EBS) provides block level storage volumes for use with EC2 instances. EBS volumes are highly available and reliable storage volumes that can be attached to any running instance that is in the same Availability Zone. EBS volumes that are attached to an EC2 instance are exposed as storage volumes that persist independently from the life of the instance. With Amazon EBS, you pay only for what you use.

How Amazon Elastic Block Store Differs for AWS GovCloud (US)

- The copy snapshot commands can be used, but only allow you to copy snapshots available to your account within AWS GovCloud (US) Regions. 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 AWS GovCloud (US) Regions. In other AWS Regions, you can use HTTP or HTTPS.
- The Provisioned IOPS SSD (io2) EBS volume type is not available in the AWS GovCloud (US) Regions.

Documentation for Amazon Elastic Block Store

For more information related to EBS Data LifeCycle Manager (DLM), see Amazon EBS Snapshot Lifecycle.

For Amazon EBS User Guide, see Amazon Elastic Block Store documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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. • Do not enter ITAR-regulated data in the following fields: • Volume names • Snapshot names</td>
</tr>
</tbody>
</table>
Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizeable computing capacity—literally, servers in Amazon's data centers—that you use to build and host your software systems.

How Amazon Elastic Compute Cloud Differs for AWS GovCloud (US)

- **EC2 Instance Connect** will not work in AWS GovCloud (US) if your Linux instance has SELinux enabled in enforcing mode. The process for enabling or disabling SELinux varies across Linux distributions. For information about how to check the status of SELinux on your instance, or to enable or disable SELinux, see the relevant operating system guide for your instance.
- Reserved Instance resale is not available in the AWS GovCloud (US) Regions.
- AMI copy and snapshot copy do not support migrating AMIs and snapshots from another AWS Region into AWS GovCloud (US) Regions. For information about how to migrate your AMIs from another AWS Region into AWS GovCloud (US) Regions, see Importing Virtual Machines into AWS GovCloud (US) Regions (p. 131).
- When using the Amazon EC2 AMI tools, AWS GovCloud (US) Regions 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 AWS GovCloud (US) Regions.
- 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 AWS GovCloud (US) Regions, 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. 130).
- When you launch an instance in AWS GovCloud (US) Regions 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 AWS GovCloud (US) Regions. In other AWS 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.
  - If your account is not set up as default VPC, then you will need to specify an Availability Zone and subnet. To specify a subnet to use when you create the import task, use the --subnet subnet_id option and --availability_zone option (specifying the Availability Zone corresponding to the subnet ID) with the ec2-import-instance command.
- When using VM Export:
  - The Amazon EC2 instance must have been previously imported using VM Import.
The Amazon S3 bucket for the destination image must exist and must have WRITE and READ_ACP permissions granted to the AWS GovCloud (US) account with canonical ID: af913ca13efe7a94b88392711f6cfc8aa07c9d1454d4f190a624b126733a5602.

To export an instance, you can use the `ec2-create-instance-export-task` command. For more information, see Exporting Amazon EC2 Instances.

Microsoft System Center Virtual Machine Manager (SCVMM) is not yet supported in AWS GovCloud (US) Regions.

AWS Management Portal for vCenter is not compatible with AWS GovCloud (US) Regions.

Savings Plans cannot be purchased from AWS GovCloud (US) accounts but can be purchased in any standard account and these plans purchased in the Standard account can apply to usage in AWS GovCloud (US) Regions.

The Provisioned IOPS SSD (io2) EBS volume type is not available in the AWS GovCloud (US) Regions.

EC2 CPU Optimization is currently API-only in the AWS GovCloud (US) Regions.

AWS Nitro Enclaves is not available in the AWS GovCloud (US) Regions.

### Determining if Your Account Has a Default Amazon VPC

In AWS GovCloud (US) Regions, 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](image)

   ![Default VPC vpc-1a2b3c4d](image)

   - If you see both EC2-Classic 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](image)

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-West) account ID and indicate that you want to enable your account for a default VPC.

Documentation for Amazon EC2

Amazon Elastic Compute Cloud documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>

Importing Virtual Machines into AWS GovCloud (US) Regions

VM Import/Export enables you to import virtual machine (VM) images from your existing virtualization environment to Amazon EC2, and then export them back. This enables you to migrate applications and workloads to Amazon EC2, copy your VM image catalog to Amazon EC2, or create a repository of VM images for backup and disaster recovery.

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 below documentation.

**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.

### How Amazon EC2 VM Import/Export Differs for AWS GovCloud (US)

The [AWS Management Portal for vCenter](https://aws.amazon.com/vmware/), which enables you to manage your AWS resources using VMware vCenter, is not compatible with AWS GovCloud (US) Regions.

### Documentation for Amazon EC2 VM Import/Export


### 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 Image Builder

Amazon Elastic Compute Cloud Image Builder is a fully managed AWS service that makes it easier to automate the creation, management and deployment of customized, secure and up-to-date “golden” server images that are pre-installed and pre-configured with software and settings to meet specific IT standards. You can use the AWS Management Console, AWS CLI or APIs to create “golden” images in your AWS account. The images you build are created in your account and you can configure them for operating system patches on an ongoing basis.

### How Amazon EC2 Image Builder Differs for AWS GovCloud (US)

This service has no differences between AWS GovCloud (US) Regions and the standard AWS Regions.

### Documentation for Amazon EC2 Image Builder

For more information about Amazon EC2 Image Builder, see the [Amazon EC2 Image Builder documentation](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/imagebuilder.html).

### ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, this section does not apply to you. The following information identifies the ITAR boundary for this service:
Amazon ECR

Amazon Elastic Container Registry (Amazon ECR) is a fully managed Docker container registry that makes it easy for developers to store, manage, and deploy Docker container images.

How Amazon Elastic Container Registry Differs for AWS GovCloud (US)

- Amazon ECR integration with AWS PrivateLink to use an interface VPC endpoint is not supported in AWS GovCloud (US-East). Amazon ECR VPC endpoint documentation.
- Amazon ECR image lifecycle policies are not supported in AWS GovCloud (US-East). Amazon ECR Lifecycle documentation.

Documentation for Amazon Elastic Container Registry

Amazon Elastic Container Registry documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 layer and image data</td>
<td>Do not enter ITAR-regulated data in the following fields:</td>
</tr>
<tr>
<td></td>
<td>• Repository name</td>
</tr>
<tr>
<td></td>
<td>• Image tag</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>• All data contained within a component can contain ITAR-regulated data.</td>
<td>EC2 Image Builder metadata is not permitted to contain ITAR-regulated data. This metadata includes all configuration data that you enter when creating and maintaining your images, components, image recipes, distribution configurations and infrastructure configurations. Do not enter ITAR-regulated data in the following console fields:</td>
</tr>
<tr>
<td></td>
<td>• Names</td>
</tr>
<tr>
<td></td>
<td>• Description</td>
</tr>
<tr>
<td></td>
<td>• Resource tags</td>
</tr>
</tbody>
</table>
Amazon ECS

Amazon Elastic Container Service (Amazon ECS) is a highly scalable, fast, container management service that makes it easy to run, stop, and manage Docker containers on a cluster of Amazon EC2 instances.

How Amazon Elastic Container Service Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

Documentation for Amazon Elastic Container Service

Amazon Elastic Container Service documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 Elastic File System

Amazon EFS provides file storage for use with Amazon EC2 instances. The service is designed to be highly scalable, highly available, and highly durable. The service manages all the file storage infrastructure for you, meaning that you can avoid the complexity of deploying, patching, and maintaining complex file system configurations.
How Amazon Elastic File System Differs for AWS GovCloud (US)

- The new EFS management console user interface is not supported in the AWS GovCloud (US).
- The option to create an EFS file system using the service recommended settings is not supported in the AWS GovCloud (US).
- The ability to access CloudWatch metrics and alarms in the Amazon EFS console is not supported in the AWS GovCloud (US).

Documentation for Amazon Elastic File System

Amazon Elastic File System documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 can contain ITAR-regulated data.</td>
<td>Do not enter ITAR-regulated data into the following fields:</td>
</tr>
<tr>
<td></td>
<td>• Resource Tags</td>
</tr>
</tbody>
</table>

Amazon Elastic Kubernetes Service

Amazon Elastic Kubernetes Service (Amazon EKS) is a managed service that makes it easy for you to run Kubernetes on AWS without needing to stand up or maintain your own Kubernetes control plane. Kubernetes is an open-source system for automating the deployment, scaling, and management of containerized applications.

How Amazon EKS Differs for AWS GovCloud (US)

- Amazon EKS on Fargate is not available in AWS GovCloud (US).
- Public DNS resolution of EKS cluster private endpoint is not available in AWS GovCloud (US).

Documentation for Amazon EKS

Amazon EKS documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you
must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 data entered, stored, and processed within Amazon EKS in GovCloud can contain ITAR-regulated data. | • Do not enter ITAR-regulated data in the following fields:  
  • Cluster name  
  • Fargate profile name  
  • Node group name |

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 Service Endpoints (p. 62).

Amazon Elasticsearch Service

Amazon Elasticsearch Service (Amazon ES) is a managed service that makes it easy to deploy, operate, and scale Elasticsearch, a popular open-source search and analytics engine. Amazon ES also offers security options, high availability, data durability, and direct access to the Elasticsearch API.

How Amazon Elasticsearch Service Differs for AWS GovCloud (US)

• Amazon Cognito authentication for Kibana is not supported in the AWS GovCloud (US) Regions.
• In AWS GovCloud (US) East, AWS ElasticSearch only supports 2 availability zone deployments. 3 availability zone deployments are available in AWS GovCloud (US) West.

Documentation for Amazon Elasticsearch Service

Amazon Elasticsearch Service documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>
</tbody>
</table>
Elastic Load Balancing

Elastic Load Balancing automatically distributes your incoming application traffic across multiple targets, such as EC2 instances. It monitors the health of registered targets and routes traffic only to the healthy targets.

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) Regions.

How Elastic Load Balancing Differs for AWS GovCloud (US)

- 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) Regions.
- 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 TLS/SSL certificates on your Classic, Application and Network load balancers. 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.

Documentation for Elastic Load Balancing

Elastic Load Balancing documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, this section does not apply to you. The following information identifies the ITAR boundary for this service:
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 Service Endpoints (p. 62).

Amazon ElastiCache

Amazon ElastiCache makes it easy to set up, manage, and scale distributed in-memory cache environments in the AWS Cloud. It provides a high performance, resizable, and cost-effective in-memory cache, while removing complexity associated with deploying and managing a distributed cache environment. ElastiCache works with both the Redis and Memcached engines; to see which works best for you, see the Comparing Memcached and Redis topic in either user guide.

How Amazon ElastiCache Differs for AWS GovCloud (US)

• 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.

Documentation for Amazon ElastiCache

Amazon ElastiCache documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 is not permitted to contain ITAR-regulated data.</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 AWS GovCloud (US) Regions.
- 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 AWS GovCloud (US) Regions 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 Service Endpoints (p. 62).

Amazon EMR

Amazon EMR is a web service that makes it easy to process large amounts of data efficiently. Amazon EMR uses Hadoop processing combined with several AWS products to do such tasks as web indexing, data mining, log file analysis, machine learning, scientific simulation, and data warehousing.

For information related to Release history, refer to Amazon EMR Release Information.

How Amazon EMR Differs for AWS GovCloud (US)

- MapR distributions are currently not supported in AWS GovCloud (US) Regions.
In AWS GovCloud (US) Regions, 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 with debugging is not currently supported in AWS GovCloud (US) Regions.
- Instance fleets are currently not supported in AWS GovCloud (US) Regions.

Documentation for Amazon EMR

Amazon EMR documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 Service Endpoints (p. 62).

Amazon EventBridge

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

Existing CloudWatch Events users can access their existing default bus, rules, and events in the new EventBridge console and in the CloudWatch Events console. EventBridge uses the same CloudWatch Events API, so all of your existing CloudWatch Events API usage remains the same.
How Amazon EventBridge Differs for AWS GovCloud (US)

- Use SSL (HTTPS) when you make calls to the service in AWS GovCloud (US) Regions. In other AWS Regions, you can use HTTP or HTTPS.
- Amazon EventBridge Schema Registry is not supported in AWS GovCloud (US) Regions
- Setting up partner event sources to receive events from Software-as-a-Service (SaaS) Partner applications and services is not supported in AWS GovCloud (US) Regions
- Support for Dead Letter Queues (DLQs) is not supported in AWS GovCloud (US) Regions

Documentation for Amazon EventBridge

Amazon EventBridge documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in the AWS GovCloud (US) Region. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled 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>• This service boundary exists entirely within the GovCloud regions and all export-controlled Content entered, processed, and created within Service will exist in the GovCloud regions.</td>
<td>• No ITAR-regulated data may be entered, stored, or processed by Amazon EventBridge. For example, EventBridge metadata is not permitted to contain ITAR-regulated data. This metadata includes all the configuration data that you enter when creating and maintaining your EventBridge alarms.</td>
</tr>
<tr>
<td></td>
<td>• For example, do not enter ITAR-regulated data in the following field:</td>
</tr>
<tr>
<td></td>
<td>• Rule names</td>
</tr>
<tr>
<td></td>
<td>• Rule description</td>
</tr>
<tr>
<td></td>
<td>• Event patterns</td>
</tr>
<tr>
<td></td>
<td>• Data input to APIs</td>
</tr>
</tbody>
</table>

AWS Fargate

AWS Fargate is a compute engine for Amazon ECS that lets you run containers in production without deploying or managing servers. Fargate lets you focus on designing and building your applications instead of managing the infrastructure that runs them.

How AWS Fargate Differs for AWS GovCloud (US)

This service has no differences between AWS GovCloud (US) Regions and the standard AWS Regions.
ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 Fargate can contain ITAR-regulated data.</td>
<td>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</td>
</tr>
</tbody>
</table>

Amazon S3 Glacier

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

How Amazon S3 Glacier Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 S3 Glacier archives can contain ITAR-regulated data.</td>
<td>• S3 Glacier metadata is not permitted to contain ITAR-regulated data. This metadata includes all configuration data that you enter when creating and maintaining your S3 Glacier vaults names.</td>
</tr>
<tr>
<td></td>
<td>• Do not enter ITAR-regulated data in the following fields:</td>
</tr>
</tbody>
</table>
AWS Glue

AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. You can create and run an ETL job with a few clicks in the AWS Management Console. You simply point AWS Glue to your data stored on AWS, and AWS Glue discovers your data and stores the associated metadata (e.g. table definition and schema) in the AWS Glue Data Catalog. Once cataloged, your data is immediately searchable, queryable, and available for ETL.

How AWS Glue Differs for AWS GovCloud (US)

This service has no differences between AWS GovCloud (US) Regions and the standard AWS Regions.

Documentation for AWS Glue

AWS Glue documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 is ITAR permitted.</td>
<td>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</td>
</tr>
</tbody>
</table>

Amazon GuardDuty

Amazon GuardDuty is a continuous security monitoring service. Amazon GuardDuty can help to identify unexpected and potentially unauthorized or malicious activity in your AWS environment.

How Amazon GuardDuty Differs for AWS GovCloud (US)

• Using AWS CloudFormation to set up Amazon GuardDuty resources in AWS GovCloud (US) is not currently supported.
• The Enable GuardDuty StackSet feature to enable Amazon GuardDuty in multiple accounts at the same time is currently unavailable due to the lack of AWS CloudFormation support currently in AWS GovCloud (US). To bypass this limitation, use the Python scripts described in the Amazon GuardDuty documentation.

• Cross-region data transfer is not supported.

• Member invite notifications through Personal Health Dashboard and email is not supported.

Documentation for Amazon GuardDuty

Amazon GuardDuty documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 GuardDuty can contain ITAR-regulated data.</td>
<td>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</td>
</tr>
</tbody>
</table>

AWS Health

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

All customers can use the Personal Health Dashboard (PHD), powered by the AWS Health API. The dashboard requires no setup, and it’s ready to use for authenticated AWS users.

Additionally, AWS Support customers who have a Business or Enterprise support plan can use the AWS Health API to integrate with in-house and third-party systems.

How AWS Health Differs for AWS GovCloud (US)

• The organizational view feature is currently not supported in the AWS GovCloud (US) Regions.

Documentation for AWS Health

AWS Health documentation.
ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>• This service boundary exists entirely within the GovCloud regions and all export-controlled Content entered, processed, and created within Service will exist in the GovCloud regions.</td>
<td>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</td>
</tr>
</tbody>
</table>

AWS Identity and Access Management

AWS Identity and Access Management (IAM) is a web service for securely controlling access to AWS services. With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users and applications can access.

How IAM Differs for AWS GovCloud (US)

• You created your AWS GovCloud (US) account using your standard AWS account root user credentials. To sign in as that root user, you must use the standard AWS endpoint. When you created your account, AWS provided you with the credentials for your GovCloud administrator IAM user or your AWS GovCloud (US) account root user. To sign in with these credentials, use the AWS GovCloud (US) endpoint. Keep in mind that you cannot access the AWS GovCloud (US) console using your root user credentials.

• IAM users that you create in AWS GovCloud (US) are specific to AWS GovCloud (US) and do not exist in other standard AWS Regions.

• AWS GovCloud (US) supports MFA devices listed in the Compatibility with AWS GovCloud (US) table row on the AWS Multi-Factor Authentication page. You can use these MFA devices with your AWS GovCloud (US) administrator IAM user or any IAM user in your account. You cannot enable an MFA device for your AWS GovCloud (US) account root user.

• You cannot create a role to delegate access between an AWS GovCloud (US) account and a standard AWS account.

• Customers with export-controlled data (e.g., ITAR-controlled technical data) in their environment may consider using IAM roles as part of their export control compliance program. It is the customer’s responsibility to properly architect its AWS GovCloud (US) account if there will be export controlled data in its environment in order to comply with export control laws.

• If you create policies, use the correct AWS GovCloud (US) ARN prefix. For more information, see Amazon Resource Names (ARNs) in GovCloud (US) Regions (p. 32).

• Use SSL (HTTPS) when you make calls to the service in AWS GovCloud (US) Regions.

• When you use a SAML provider in AWS GovCloud (US) Regions, 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 CodeCommit, which is currently not available in AWS GovCloud (US-East).

• The credential report includes information about your AWS GovCloud (US) account root user. Root user access key activity can occur if someone uses your root user access keys. If a user in your AWS GovCloud (US) contacts AWS Support because they cannot sign in, AWS Support verifies their identity and notifies the AWS GovCloud (US) account owner. AWS Support then creates an AWS GovCloud (US) root user access key and secret key in your account. The AWS Support team delivers these credentials to the verified user, and works with them to reset their credentials. This user can then run AWS API operations or CLI commands using those access keys. If you see root user activity in your credential report that you do not recognize, you can do one of the following:
  • Use the AWS GovCloud (US) root user access keys to call AWS API operations or CLI commands and manage your root user access keys. You can then make any root user access keys inactive, or delete them entirely.
  • If you do not have access to any AWS GovCloud (US) root user access keys, you can contact AWS Support. After you prove your account ownership, AWS Support will deliver new AWS GovCloud (US) root user access keys to you. You can then delete any (or all) root user access keys as described above.
  • You can attach or replace an IAM role on your existing Amazon EC2 instances in AWS GovCloud (US). To enable IAM roles for your existing Amazon EC2 instances, follow the example described in this AWS Security Blog post.
  • You can now establish a private connection between your Amazon VPC and AWS STS in the AWS GovCloud (US-West) region. For more information, see the Using AWS STS Interface VPC Endpoints in the IAM User Guide.
  • Information about when a role was last used is not available. For more information, see the View Role Access.

Documentation for AWS Identity and Access Management

AWS IAM documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 configuration data that you enter when creating and maintaining your IAM entities.</td>
</tr>
<tr>
<td>• Secret access keys are protected as ITAR-regulated data.</td>
<td>• Do not enter ITAR-regulated data in the following fields:</td>
</tr>
<tr>
<td>• Virtual MFA seeds are protected as ITAR-regulated data.</td>
<td>• Authentication codes, which are clear text memcached</td>
</tr>
<tr>
<td></td>
<td>• User names</td>
</tr>
<tr>
<td></td>
<td>• Group names</td>
</tr>
</tbody>
</table>
Amazon Inspector

Amazon Inspector is a security vulnerability assessment service that helps improve the security and compliance of your AWS resources. Amazon Inspector automatically assesses resources for vulnerabilities or deviations from best practices, and then produces a detailed list of security findings prioritized by level of severity. Amazon Inspector includes a knowledge base of hundreds of rules mapped to common security standards and vulnerability definitions that are regularly updated by AWS security researchers.

How Amazon Inspector Differs for AWS GovCloud (US)

- Network Assessment rules package is not deployed in AWS GovCloud (US) Regions.

Documentation for Amazon Inspector

Amazon Inspector documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, this section does not apply to you. The following information identifies the ITAR boundary for this service:

- All data entered, stored, and processed in Amazon Inspector can contain ITAR-regulated data.

AWS IoT Core

AWS IoT enables secure, bi-directional communication between Internet-connected things (such as sensors, actuators, embedded devices, or smart appliances) and the AWS Cloud over MQTT and HTTP.
How AWS IoT Differs for AWS GovCloud (US)

• Use of Amazon Cognito Identities to grant permissions to users of your AWS IoT applications, via your
  own identity provider or other popular identity providers, is not supported.
• The AWS IoT Core endpoint does not yet support FIPS 140-2.

Documentation for AWS IoT

AWS IoT Core documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-
controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you
must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any
ITAR-controlled data in AWS GovCloud (US) Regions, 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>• Message payloads</td>
<td>• Message topics and topic filters</td>
</tr>
<tr>
<td>• Device shadows (both keys and values)</td>
<td>• Thing names</td>
</tr>
<tr>
<td>• Thing registry data (except thing names, thing types, and thing group names)</td>
<td>• Thing types</td>
</tr>
<tr>
<td></td>
<td>• Thing group names</td>
</tr>
<tr>
<td></td>
<td>• Rule definitions (including SQL statements and actions)</td>
</tr>
</tbody>
</table>

AWS IoT Device Defender

AWS IoT Device Defender is a fully managed service that helps you secure your fleet of IoT devices. You
can use AWS IoT Device Defender to audit your IoT resources like policies, certificates, IAM roles and
Amazon Cognito IDs against security best practices, monitor connected devices to detect abnormal
behavior, and mitigate security risks. By using AWS IoT Device Defender, you can enforce consistent
security policies across your AWS IoT device fleet and respond quickly when devices are compromised.

How AWS IoT Device Defender Differs for AWS GovCloud (US)

• Cognito related checks in Device Defender Audit are not available.
• Role alias related and key quality related checks in Device Defender Audit are not available.

Documentation for AWS IoT Device Defender

AWS IoT Device Defender documentation.
ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>• Security Profile data (other than Security Profile and Behavior names)</td>
<td>• Security Profile Name</td>
</tr>
<tr>
<td>• Schedule Audit data (other than Scheduled Audit name)</td>
<td>• Behavior Name</td>
</tr>
<tr>
<td>• Mitigation action data (other than Mitigation Action name and Audit Mitigation Action Task Id)</td>
<td>• Audit Schedule Name</td>
</tr>
<tr>
<td></td>
<td>• Mitigation Action Name</td>
</tr>
<tr>
<td></td>
<td>• Audit Mitigation Action Task Id</td>
</tr>
</tbody>
</table>

AWS IoT Device Management

AWS IoT Device Management is a cloud-based device management service that makes it easy for customers to securely manage IoT devices throughout their lifecycle. Customers can use AWS IoT Device Management to onboard device information and configuration, organize their device inventory, monitor their fleet of devices, and remotely manage devices deployed across many locations. This remote management includes over-the-air (OTA) updates to device software.

How AWS IoT Device Management Differs for AWS GovCloud (US)

• Use of Amazon Cognito Identities to grant permissions to users of your AWS IoT applications, via your own identity provider or other popular identity providers, is not supported.

• The AWS IoT Device Management endpoint does not yet support FIPS 140-2.

Documentation for AWS IoT Device Management

AWS IoT Device Management documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>• Message payloads</td>
<td>• Message topics and topic filters</td>
</tr>
<tr>
<td>ITAR-Regulated Data Permitted</td>
<td>ITAR-Regulated Data Not Permitted</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>• Device shadows (both keys and values)</td>
<td>• Thing names</td>
</tr>
<tr>
<td>• Thing registry data (except thing names and thing attribute keys)</td>
<td>• Thing types</td>
</tr>
<tr>
<td></td>
<td>• Thing group names</td>
</tr>
<tr>
<td></td>
<td>• Rule definitions (including SQL statements and actions)</td>
</tr>
</tbody>
</table>

AWS IoT Greengrass

AWS IoT Greengrass seamlessly extends AWS to edge devices so they can act locally on the data they generate, while still using the cloud for management, analytics, and durable storage. With AWS IoT Greengrass, connected devices can run AWS Lambda functions, execute predictions based on machine learning models, keep device data in sync, and communicate with other devices securely even when not connected to the Internet.

How AWS IoT Greengrass Differs for AWS GovCloud (US)

- AWS IoT Greengrass Core software v1.9.2 is the minimum supported version.
- The following minimum versions of the AWS IoT Greengrass Core SDK are supported.

<table>
<thead>
<tr>
<th>Language or platform</th>
<th>Minimum version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Python 3.7</td>
<td>1.4.0</td>
</tr>
<tr>
<td>Java 8</td>
<td>1.3.1</td>
</tr>
<tr>
<td>Node.js 8.10</td>
<td>1.4.0</td>
</tr>
<tr>
<td>C, C++</td>
<td>1.1.0</td>
</tr>
</tbody>
</table>

- The following connectors are supported in AWS GovCloud (US-East):
  - Cloudwatch Metrics, v4
  - Device Defender, v3
  - Docker Application Deployment, v6
  - Kinesis Firehose, v5
  - SNS, v4
  - Modbus-RTU Protocol Adapter, v3
  - Raspberry Pi GPIO, v4
  - Serial Stream, v3
- The following connectors are supported in AWS GovCloud (US-West):
  - Modbus-RTU Protocol Adapter, v2
  - Raspberry Pi GPIO, v2
  - Serial Stream, v2
- For over-the-air (OTA) updates, the IAM role used to presign the Amazon S3 URL (that links to the Greengrass software update) must allow access in the appropriate AWS Region.

The following example policy includes the minimum required permissions that must be attached to the role for AWS GovCloud (US-West) Region support.
• AWS IoT Greengrass operations use three endpoints that have different support for FIPS 140-2.
  • The endpoint for Greengrass control plane operations provides FIPS access only.
  • The endpoint for Greengrass discovery operations does not yet support FIPS. This endpoint provides non-FIPS access only.
  • The endpoint for AWS IoT device operations does not yet support FIPS. This endpoint provides non-FIPS access only.

For a list of AWS GovCloud (US) endpoints, see the section called “Service Endpoints” (p. 62). Only Amazon Trust Services (ATS) server authentication is supported, so you must use ATS-signed root CA certificates and ATS endpoints. For more information, see Server Authentication in the AWS IoT Developer Guide.

• The default limit for the maximum number of transactions per second (TPS) on the AWS IoT Greengrass API is 10 TPS. For more information, see AWS IoT Greengrass Limits in the Amazon Web Services General Reference.

---

### Documentation for AWS IoT Greengrass

AWS IoT Greengrass documentation.

#### ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in the AWS GovCloud (US-West) Region. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in the AWS GovCloud (US-West) 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>• Message payloads</td>
<td>• Message topics and topic filters</td>
</tr>
<tr>
<td>• Device shadows (both keys and values)</td>
<td>• Customer-defined names and IDs of Greengrass resources:</td>
</tr>
<tr>
<td>• Thing registry data (except thing names and thing attribute keys)</td>
<td>• Connectors</td>
</tr>
<tr>
<td></td>
<td>• Cores</td>
</tr>
<tr>
<td></td>
<td>• Devices</td>
</tr>
<tr>
<td></td>
<td>• Functions</td>
</tr>
<tr>
<td></td>
<td>• Groups</td>
</tr>
</tbody>
</table>
Amazon Kinesis Data Analytics

Amazon Kinesis Data Analytics is the easiest way to analyze streaming data, gain actionable insights, and respond to your business and customer needs in real time. Amazon Kinesis Data Analytics reduces the complexity of building, managing, and integrating streaming applications with other AWS services. SQL users can easily query streaming data or build entire streaming applications using templates and an interactive SQL editor. Java developers can quickly build sophisticated streaming applications using open source Java libraries and AWS integrations to transform and analyze data in real-time.

Amazon Kinesis Data Analytics takes care of everything required to run your real-time applications continuously and scales automatically to match the volume and throughput of your incoming data. With Amazon Kinesis Data Analytics, you only pay for the resources your streaming applications consume. There is no minimum fee or setup cost.

How Amazon Kinesis Data Analytics Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) Region and the standard AWS Regions.

Documentation for Amazon Kinesis Data Analytics

Amazon Kinesis Data Analytics documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 Analytics can contain ITAR-regulated data.</td>
<td>• Do not enter ITAR-regulated data in the following fields:</td>
</tr>
<tr>
<td></td>
<td>• Application 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 Service Endpoints (p. 62).

Amazon Kinesis Data Firehose

Amazon Kinesis Data Firehose is a fully managed service for delivering real-time streaming data to destinations such as Amazon Simple Storage Service (Amazon S3), Amazon Redshift, Amazon

152
Elasticsearch Service (Amazon ES), and Splunk. Kinesis Data Firehose is part of the Kinesis streaming data platform, along with Kinesis Data Streams, Kinesis Video Streams, and Amazon Kinesis Data Analytics. With Kinesis Data Firehose, you don’t need to write applications or manage resources. You configure your data producers to send data to Kinesis Data Firehose, and it automatically delivers the data to the destination that you specified. You can also configure Kinesis Data Firehose to transform your data before delivering it.

How Amazon Kinesis Data Firehose Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

Documentation for Amazon Kinesis Data Firehose

Amazon Kinesis Data Firehose documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 Firehose 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 Service Endpoints (p. 62).

Amazon Kinesis Data Streams

Amazon Kinesis makes it easy to collect, process, and analyze video and data streams in real time.

How Amazon Kinesis Data Streams Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

Documentation for Amazon Kinesis Data Streams

Amazon Kinesis Data Streams documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you
must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 Service Endpoints (p. 62).

### AWS Key Management Service

AWS Key Management Service (KMS) is an encryption and key management service scaled for the cloud. KMS keys and functionality are used by other AWS services, and you can use them to protect data in your own applications that use AWS.

### How AWS KMS Differs for AWS GovCloud (US)

This service has no differences between AWS GovCloud (US) Regions and the standard AWS Regions.

### Documentation for AWS Key Management Service

AWS Key Management Service Developer Guide.

### ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>
</tbody>
</table>
AWS Lake Formation

This service is currently available in AWS GovCloud (US-West) only.

AWS Lake Formation is a service that makes it easy to set up a secure data lake in days. A data lake is a centralized, curated, and secured repository that stores all your data, both in its original form and prepared for analysis. A data lake enables you to break down data silos and combine different types of analytics to gain insights and guide better business decisions.

Lake Formation simplifies and automates many of the complex manual steps that are usually required to create data lakes. These steps include collecting, cleansing, moving, and cataloging data, and securely making that data available for analytics and machine learning. You point Lake Formation at your data sources, and Lake Formation crawls those sources and moves the data into your new Amazon Simple Storage Service (Amazon S3) data lake.

Lake Formation provides its own permissions model that augments the AWS Identity and Access Management (IAM) permissions model. This centrally defined permissions model enables fine-grained access to data stored in data lakes through a simple grant/revoke mechanism.

Lake Formation permissions are enforced at the table and column level across the full portfolio of AWS analytics and machine learning services.

How AWS Lake Formation Differs for AWS GovCloud (US)

The AWS GovCloud (US) Region implementation of Lake Formation is unique in the following ways:

- Amazon QuickSight integration with Lake Formation is not supported.
- Granting Lake Formation permissions to Amazon Athena users who authenticate through the JDBC or ODBC driver using a SAML identity provider is not supported.

Documentation for AWS Lake Formation

AWS Lake Formation documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in the AWS GovCloud (US) Region. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled 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>ITAR-regulated data may be backed up and managed using Lake Formation.</td>
<td>Do not enter ITAR-regulated data in resource tag, plan names, rule names, selection names, or vault names.</td>
</tr>
</tbody>
</table>
AWS Lambda

With AWS Lambda, you can run code without provisioning or managing servers. You pay only for the compute time that you consume—there’s no charge when your code isn’t running. You can run code for virtually any type of application or backend service—all with zero administration. Just upload your code and Lambda takes care of everything required to run and scale your code with high availability. You can set up your code to automatically trigger from other AWS services or call it directly from any web or mobile app.

How AWS Lambda Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

Documentation for AWS Lambda

AWS Lambda documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 License Manager

AWS License Manager makes it easier to manage licenses in AWS and on-premises servers from software vendors such as Microsoft, SAP, Oracle, and IBM. AWS License Manager lets administrators create customized licensing rules that emulate the terms of their licensing agreements, and then enforces these rules when an instance of EC2 gets launched. Administrators can use these rules to limit licensing violations, such as using more licenses than an agreement stipulates or reassigning licenses to different servers on a short-term basis. The rules in AWS License Manager enable you to limit a licensing breach by physically stopping the instance from launching or by notifying administrators about the infringement.
Administrators gain control and visibility of all their licenses with the AWS License Manager dashboard and reduce the risk of non-compliance, misreporting, and additional costs due to licensing overages.

AWS License Manager integrates with AWS services to simplify the management of licenses across multiple AWS accounts, IT catalogs, and on-premises, through a single AWS account. License administrators can add rules in AWS Service Catalog, which allows them to create and manage catalogs of IT services that are approved for use on all their AWS accounts. Through seamless integration with AWS Systems Manager and AWS Organizations, administrators can manage licenses across all the AWS accounts in an organization and on-premises environments. AWS Marketplace buyers can also use AWS License Manager to track bring your own license (BYOL) software obtained from the Marketplace and keep a consolidated view of all their licenses.

How AWS License Manager Differs for AWS GovCloud (US)

- The AWS GovCloud regions will only have the Single Account discovery model enabled for customer use. This means that customers will be unable to onboard to Organizations and perform cross-account discovery.
- License sharing using Resource share will be unavailable.

Documentation for AWS License Manager

AWS License Manager documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in the AWS GovCloud (US-West) Region. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in the AWS GovCloud (US-West) 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>• This service boundary exists entirely within the GovCloud regions and all export-controlled Content entered, processed, and created within Service will exist in the GovCloud regions.</td>
<td>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</td>
</tr>
</tbody>
</table>

AWS Management Console for the AWS GovCloud (US) Region

The AWS Management Console is a graphical interface for accessing a wide range of AWS Cloud services and managing compute, storage, and other cloud resources. The console includes the Tag Editor tool for managing metadata that you add to your resources. You can then use those tags to create resource groups to manage your AWS resources collectively.
How AWS Management Console Differs for AWS GovCloud (US)

- You access the AWS GovCloud (US) console by using a different URL than the standard AWS Management Console.
- You can only access the AWS GovCloud (US) console by using an IAM user name and password, not with the GovCloud account root user email address and password. For information about the AWS GovCloud (US) differences in IAM, see AWS Identity and Access Management.
- The console includes only the services that are available in AWS GovCloud (US) Regions. To see a list of the supported services, see Services in the AWS GovCloud (US).
- You are automatically signed out from the console after 4 hours.
- Due to the separate authentication stack for AWS GovCloud (US), the hardware MFA devices used with standard AWS Regions are not compatible with AWS GovCloud (US) accounts. AWS GovCloud (US) supports only MFA devices listed in the Compatibility with AWS GovCloud (US) table row on the Multi-Factor Authentication page.
- You cannot enable an MFA device for your AWS GovCloud (US) account root user.
- The console does not permit navigation to any regions other than AWS GovCloud (US) Regions.
- 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.
- Resource Groups, Tag Editor, and AWS Console mobile app are not available.
- On the Console Navigation the following features are not available: Personal Health Dashboard (PHD) alerts, Language Selector, Feedback.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>• Console passwords are protected as ITAR-regulated data.</td>
<td>• Your user name is not permitted to contain ITAR-regulated data.</td>
</tr>
<tr>
<td>• All console data fields inherit the ITAR restrictions for the specific service that is being accessed. See each service for details.</td>
<td>• All console data fields inherit the ITAR restrictions for the specific service that is being accessed. See each service for details.</td>
</tr>
</tbody>
</table>

AWS Marketplace

AWS Marketplace is an online store where you can buy or sell software that runs on Amazon Web Services (AWS).

How AWS Marketplace Differs for AWS GovCloud (US)

- Full catalog of solutions is currently not available for use but we are actively working with AWS Marketplace sellers to offer their solutions.
• Product Support Connection is currently not available.
• Currently, container products and Amazon Machine Learning products are not supported in AWS GovCloud (US).
• Launch from the AWS Marketplace website is not supported with your GovCloud AWS account. To launch from the AWS Marketplace website, you must use a commercial AWS account.
• Integration with AWS Service Catalog is currently not available.

Documentation for AWS Marketplace

• AWS Marketplace documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</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 Managed Streaming for Apache Kafka (MSK)

Amazon Managed Streaming for Apache Kafka (Amazon MSK) is a fully managed service that enables you to build and run applications that use Apache Kafka to process streaming data. Amazon MSK
provides the control-plane operations, such as those for creating, updating, and deleting clusters. It lets you use Apache Kafka data-plane operations, such as those for producing and consuming data. It runs open-source versions of Apache Kafka. This means existing applications, tooling, and plugins from partners and the Apache Kafka community are supported without requiring changes to application code.

How Managed Streaming for Apache Kafka Differs for AWS GovCloud (US)

- Kinesis Data Firehose isn't available as a destination for broker logs in AWS GovCloud (US).

Documentation for Managed Streaming for Apache Kafka

Amazon Managed Streaming for Apache Kafka (MSK) documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 text and documents processed by Managed Streaming for Apache Kafka can contain ITAR-regulated data.</td>
<td>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</td>
</tr>
</tbody>
</table>

AWS Elemental MediaConvert

This service is currently available in AWS GovCloud (US-West) only.

AWS Elemental MediaConvert is a file-based video processing service that provides scalable video processing for content owners and distributors with media libraries of any size. MediaConvert offers advanced features that enable premium content experiences.

How AWS Elemental MediaConvert Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

Documentation for AWS Elemental MediaConvert

AWS Elemental MediaConvert documentation.
ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>• This service boundary exists entirely within the GovCloud regions and all export-controlled content entered, processed, and created within Service will exist in the GovCloud regions.</td>
<td>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</td>
</tr>
</tbody>
</table>

Amazon Neptune

Amazon Neptune is a fast, reliable, fully managed graph database service that makes it easy to build and run applications that work with highly connected datasets. The core of Neptune is a purpose-built, high-performance graph database engine. This engine is optimized for storing billions of relationships and querying the graph with milliseconds latency. Neptune supports the popular graph query languages Apache TinkerPop Gremlin and W3C’s SPARQL, enabling you to build queries that efficiently navigate highly connected datasets. Neptune powers graph use cases such as recommendation engines, fraud detection, knowledge graphs, drug discovery, and network security.

How Amazon Neptune Differs for AWS GovCloud (US)

This service has no differences between AWS GovCloud (US) Regions and the standard AWS Regions.

Documentation for Amazon Neptune

Amazon Neptune documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 text and documents processed by Amazon Neptune can contain ITAR-regulated data.</td>
<td>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</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 Service Endpoints (p. 62).

AWS Organizations

AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage. AWS Organizations includes account management and consolidated billing capabilities that enable you to better meet the budgetary, security, and compliance needs of your business.

How AWS Organizations Differs for AWS GovCloud (US)

- You must use AWS Organizations with all features enabled. The consolidated billing feature set is not available in this Region.
- You must meet the U.S. regulatory requirements as described in Signing Up for AWS GovCloud.
- Creating accounts from within AWS Organizations operates differently in the AWS GovCloud Region compared to commercial AWS Regions:
  - You start creating GovCloud accounts by calling the CreateGovCloudAccount action from the management account of the organization in the commercial Region. Calling account creation APIs from the AWS GovCloud Region is not supported.
  - When you call the CreateGovCloudAccount API action, you create two accounts: a standalone account in the AWS GovCloud Region, and an associated account in the commercial Region for billing and support purposes. The account in the commercial Region is automatically a member of the organization whose credentials made the request. Both accounts are associated with the same email address.
  - After creating the standalone account in the AWS GovCloud Region, you can invite it to an organization in the AWS GovCloud Region only.
  - Accounts created in other AWS Regions cannot be members of an organization in the AWS GovCloud Region.
  - Organizations that you create in the AWS GovCloud Region are independent from organizations created in commercial AWS Regions.
  - The CreateGovCloudAccount API action is not available from the AWS GovCloud Region.
  - To sign in to the AWS Organizations console in the AWS GovCloud Region, you must be signed in from a GovCloud account.
  - To learn what AWS services are currently available for trusted access with AWS Organizations, check the list in the AWS Organizations console from the AWS GovCloud Region.
  - The only policy type that you can use in a GovCloud organization is a service control policy. You can't create or use any of the management policy types at this time, including AI services opt-out policies, backup policies, or tag policies.

Creating Your Account

When you create accounts in the AWS GovCloud Region from AWS Organizations, an associated account in the commercial Region is automatically created for billing and support purposes. The account in the commercial Region and the account in the AWS GovCloud Region are linked. The account in the commercial Region is automatically a member of the organization whose credentials made the request, but the account in the AWS GovCloud Region is a standalone account until you invite it to an organization in that same Region.
Before creating accounts in the AWS GovCloud Region from AWS Organizations, make sure that you meet specific U.S. regulatory requirements as described in Signing Up for AWS GovCloud.

**To create an account in the AWS GovCloud Region from AWS Organizations**

1. From the management account of your organization in the commercial Region, sign in to the Organizations console at https://console.aws.amazon.com/organizations
2. From the Command Line Interface (CLI), Call the `CreateGovCloudAccount` API action.

**Accounts and roles are created as follows**

- An account is created in the commercial Region and it is automatically a member of the organization whose credentials made the request.
- A role is created in the new account in the commercial Region that the management account in this same Region can assume.
- The account in the AWS GovCloud Region is created and it links to the associated account that was created at the same time in the commercial Region.
- The account in the AWS GovCloud Region is a standalone account and is not yet a member of an organization.
- A role is created in the AWS GovCloud account that the GovCloud account that is linked to the management account in the commercial Region can assume.

**Inviting Accounts to an Organization**

After creating a standalone account in the AWS GovCloud Region, you can invite it to organizations in the AWS GovCloud Region. You cannot invite accounts in the AWS GovCloud Region to organizations in other AWS Regions.

The following diagram explains account access works so that you can invite standalone accounts in the AWS GovCloud Region to an organization in the same Region.
To invite an account in the AWS GovCloud Region to an Organization

1. From the GovCloud account that’s associated with the management account of your organization in the commercial Region, assume the role of the GovCloud account you just created in the AWS GovCloud Region.

   In the above example, start from GovCloud Account 1 and assume the role that was created in GovCloud Account 2.

2. Follow the procedure described in Sending Invitations to AWS Accounts in the AWS Organizations User Guide to invite the account in the AWS GovCloud Region to the organization.

To access the new account in the AWS GovCloud Region

1. Sign in to the GovCloud account that is mapped to your commercial organization's management account.

2. Assume the role into the newly-created GovCloud management account.
The role is automatically created when you create the account. By default, the role is named OrganizationAccountAccessRole but you can change it using the RoleName parameter when you call the CreateGovCloudAccount action.

Documentation for AWS Organizations

AWS Organizations documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in the AWS GovCloud (US) Region. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled 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>• This service boundary exists entirely within the GovCloud regions and all export-controlled Content entered, processed, and created within Service will exist in the GovCloud regions.</td>
<td>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</td>
</tr>
</tbody>
</table>

AWS Outposts

AWS Outposts is a fully managed service that extends AWS infrastructure, services, APIs, and tools to customer premises. By providing local access to AWS managed infrastructure, AWS Outposts enables customers to build and run applications on premises using the same programming interfaces as in AWS Regions, while using local compute and storage resources for lower latency and local data processing needs.

How AWS Outposts Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

Documentation for AWS Outposts

AWS Outposts documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, this section does not apply to you. For AWS Outposts, under the shared responsibility model, customers are responsible for physical security and access controls around the Outpost. The following information identifies the ITAR boundary for this service.
AWS ParallelCluster

AWS ParallelCluster is an AWS-supported open source cluster management tool that helps you to deploy and manage High Performance Computing (HPC) clusters in the AWS cloud. Built on the open source CfnCluster project, AWS ParallelCluster enables you to quickly build an HPC compute environment in AWS. It automatically sets up the required compute resources and shared filesystem. You can use AWS ParallelCluster with a variety of batch schedulers, such as AWS Batch, SGE, Torque, and Slurm. AWS ParallelCluster facilitates quick start proof of concept deployments and production deployments. You can also build higher level workflows, such as a genomics portal that automates an entire DNA sequencing workflow, on top of AWS ParallelCluster.

How AWS ParallelCluster Differs for AWS GovCloud (US)

This service has no differences between AWS GovCloud (US) Regions and the standard AWS Regions.

Documentation for AWS ParallelCluster

AWS ParallelCluster documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>• This service boundary exists entirely within the GovCloud regions and all export-controlled content entered, processed, and created within Service will exist in the GovCloud regions.</td>
<td>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging.</td>
</tr>
</tbody>
</table>
Amazon Pinpoint

This service is currently available in AWS GovCloud (US-West) only.

Amazon Pinpoint is an AWS service that you can use to engage with your customers across multiple messaging channels. You can use Amazon Pinpoint to send push notifications, emails, SMS text messages, and voice messages.

How Amazon Pinpoint Differs for AWS GovCloud (US)

- You can’t use the SendMessages operation in the Amazon Pinpoint API to send voice messages.
- The Machine learning modules section isn’t available in the Amazon Pinpoint console.
- The project overview page in the Amazon Pinpoint console doesn’t include the Application analytics chart.
- The following differences apply to the Analytics section of the Amazon Pinpoint console:
  - The Events, Funnel, and Demographics pages aren’t available.
  - The Analytics overview page doesn’t include the following charts: Daily active endpoints, Monthly active endpoints, New endpoints, 7-day retention rate, or Active targetable endpoints. Additionally, the Campaigns chart doesn’t include the Opt-out rate metric.
  - The Usage page doesn’t include a Filters section. Additionally, the User metrics section and the Sessions per endpoint, Sessions per user, and Average users month-to-date charts aren’t included.
  - The Revenue page doesn’t include a Filters section. Additionally, the Revenue per endpoint, Units sold per endpoint, and Purchases per endpoint charts aren’t included.
  - The Campaigns page doesn’t include the Active targetable endpoints chart. Additionally, the Campaigns chart doesn’t include an Opt-out rate metric.

- The following differences apply to the Segments section of the Amazon Pinpoint console:
  - When you create a dynamic segment, the Segment estimate section doesn’t include the numbers of Eligible endpoints or Total endpoints.
  - When you create a dynamic segment, the Filter by user option isn’t available. Additionally, you can’t filter the segment based on endpoint attributes. However, you can filter by endpoint activity (for example, you can filter the segment to only include endpoints that were active in the last 30 days).
  - When you choose a segment from the Segments page, the Segment details section doesn’t include the numbers of Eligible endpoints or Total endpoints.

- The following differences apply to the Campaigns section of the Amazon Pinpoint console:
  - When you create a campaign, the Choose a segment page doesn’t include the numbers of Eligible endpoints or Total endpoints.
  - When you create a campaign, you can’t configure the campaign to be sent when an event occurs.
  - When you choose a campaign from the Campaign page, the Segment details section doesn’t include the numbers of Eligible endpoints or Total endpoints.

- The following differences apply to the Journeys section of the Amazon Pinpoint console:
• When you create a journey, the **Total endpoints in segment** section doesn't display the number of endpoints in the segment that you selected.

• When you create a journey, you can only configure the **Journey entry** activity to add participants who are in a specific segment. You can't configure the **Journey entry** activity to add participants when they perform an activity (also known as an event).

• When you review the metrics for a **Journey entry** activity, the number of endpoints in the **Next entry group** section is not included.

• The following differences apply to the **Templates** section of the Amazon Pinpoint console:
  • When you create a template, you can't include endpoint or user attributes.
  • You can't create templates that include recommendations provided by Amazon Personalize.

## Documentation for Amazon Pinpoint

Amazon Pinpoint documentation.

### ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 Pinpoint database tables can contain ITAR-regulated data.</td>
<td>• Amazon Pinpoint metadata is not permitted to contain ITAR-regulated data. This metadata includes all the configuration data that you enter when creating and maintaining your Amazon Pinpoint tables, such as table names, hash attribute names, and range attribute names.</td>
</tr>
<tr>
<td></td>
<td>• Do not enter ITAR-regulated data in the following fields:</td>
</tr>
<tr>
<td></td>
<td>• Keyspace names</td>
</tr>
<tr>
<td></td>
<td>• Table names</td>
</tr>
<tr>
<td></td>
<td>• Column names</td>
</tr>
<tr>
<td></td>
<td>• 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 [Service Endpoints](#) (p. 62).

## Amazon Polly

This service is currently available in AWS GovCloud (US-West) only.

Amazon Polly is a Text-to-Speech (TTS) cloud service that converts text into lifelike speech. You can use Amazon Polly to develop applications that increase engagement and accessibility. Amazon Polly
supports multiple languages and includes a variety of lifelike voices, so you can build speech-enabled applications that work in multiple locations and use the ideal voice for your customers.

How Amazon Polly Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

Documentation for Amazon Polly

Amazon Polly documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</td>
</tr>
<tr>
<td>• Lexicons</td>
<td></td>
</tr>
</tbody>
</table>

Amazon QuickSight

This service is currently available in AWS GovCloud (US-West) only.

Amazon QuickSight is a fully managed, serverless business intelligence service for the AWS Cloud that makes it easy to securely extend data and insights to every user in your organization. Using this business analytics service, you can build visualizations, perform ad hoc analysis, and get business insights from your data. It can automatically discover AWS data sources and also works with your data sources. Amazon QuickSight enables organizations to scale to hundreds of thousands of users, and delivers responsive performance by using a robust in-memory engine (SPICE). QuickSight dashboards and authoring experiences can also be embedded in customer-facing applications to enable interactive, multi-tenant analytics that scale with the growth of the application user base without any servers.

How Amazon QuickSight Differs for AWS GovCloud (US)

As of 10/25/2020, Amazon QuickSight in AWS GovCloud (US) does not support

- Email based user provisioning (only federated IAM users supported)
- Email reports functionality
- Geospatial visualizations
- AWS Sagemaker integration
These features will be progressively added in the future

Use caution with exports to CSV, which can be created from analyses. The file can be exported to any drive location accessible to the user. You can disable exports to CSV for dashboards. We recommend that you avoid access ITAR-regulated data on mobile devices.

Exports to CSV/Excel

Documentation for Amazon QuickSight

Amazon QuickSight documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in the AWS GovCloud (US) Region. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled 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 ingested into Amazon QuickSight's SPICE engine can contain ITAR-regulated data.</td>
<td>• Avoid using ITAR-Regulated Data in names, descriptions, custom IDs, or tags used for any QuickSight object or entity, including but not limited to:</td>
</tr>
<tr>
<td>• All data data processed by Amazon QuickSight can contain ITAR-regulated data.</td>
<td>• QuickSight users</td>
</tr>
<tr>
<td>• QuickSight groups</td>
<td>• Connections to data sources</td>
</tr>
<tr>
<td>• Datasets</td>
<td>• Analyses</td>
</tr>
<tr>
<td>• Analyses</td>
<td>• Dashboards</td>
</tr>
<tr>
<td>• Datasets</td>
<td>• Embedded dashboards</td>
</tr>
<tr>
<td>• Analyses</td>
<td>• Templates</td>
</tr>
<tr>
<td>• Datasets</td>
<td>• Custom URL actions</td>
</tr>
<tr>
<td>• Analyses</td>
<td>• Parameters</td>
</tr>
<tr>
<td>• Datasets</td>
<td>• VPC connection names</td>
</tr>
<tr>
<td>• Analyses</td>
<td>• IAM policy assignments</td>
</tr>
<tr>
<td>• Datasets</td>
<td>• QuickSight &quot;account&quot; names (the name you give to your QuickSight subscription on your AWS account)</td>
</tr>
<tr>
<td>• Analyses</td>
<td>• Names of actual database objects and files in your on-prem data sources, if using these in Amazon QuickSight</td>
</tr>
<tr>
<td>• Datasets</td>
<td>• Use caution with exports to CSV, which can be created from analyses. The file can be exported to any drive location accessible to the user. You can disable exports to CSV for dashboards. We recommend that you avoid access ITAR-regulated data on mobile devices.</td>
</tr>
<tr>
<td>• Analyses</td>
<td>• We recommend that you avoid accessing ITAR-regulated data on mobile devices.</td>
</tr>
</tbody>
</table>
AWS Resource Access Manager

AWS Resource Access Manager (RAM) is a service that enables you to easily and securely share AWS resources with any AWS account or within your AWS Organization. You can share AWS Transit Gateways, Subnets, AWS License Manager configurations, and Amazon Route 53 Resolver rules resources with RAM. Many organizations use multiple accounts to create administrative or billing isolation, and to limit the impact of errors. RAM eliminates the need to create duplicate resources in multiple accounts, reducing the operational overhead of managing those resources in every single account you own. You can create resources centrally in a multi-account environment, and use RAM to share those resources across accounts in three simple steps: create a Resource Share, specify resources, and specify accounts. RAM is available to you at no additional charge.

How AWS Resource Access Manager Differs for AWS GovCloud (US)

• Sharing of Amazon Aurora DB clusters is not supported in AWS GovCloud (US) Regions.
• Sharing of AWS CodeBuild projects is not supported in AWS GovCloud (US) Regions.
• Sharing AWS CodeBuild Report groups is not supported in AWS GovCloud (US) Regions.
• Sharing of AWS App Mesh Meshes is not supported in AWS GovCloud (US) Regions.

Documentation for AWS Resource Access Manager

AWS Resource Access Manager documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 is ITAR permitted.</td>
<td>• Resource Share name cannot contain ITAR regulated data.</td>
</tr>
</tbody>
</table>

Amazon RDS

Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. It provides cost-efficient, resizable capacity for an industry-standard relational database and manages common database administration tasks.

How Amazon Relational Database Service Differs for AWS GovCloud (US)

• Amazon RDS Performance Insights isn't available in the AWS GovCloud (US) Regions.
• Creation of cross-Region read replicas from other AWS Regions to the AWS GovCloud (US) Regions or from AWS GovCloud (US) Regions to other AWS Regions isn't supported.

• Copying of DB Snapshots from other AWS Regions to the AWS GovCloud (US) Regions or from AWS GovCloud (US) Regions to other AWS Regions isn't supported.

• Oracle Management Agent versions 12.1 and 13.1 aren't available in the AWS GovCloud (US) Regions.

• Intermediate SSL certificates must be used to connect to the AWS GovCloud (US) Regions using SSL. For more information related to Intermediate certificates, see Using SSL/TLS to Encrypt a Connection.

• Instance types and engine versions might vary in the AWS GovCloud (US) Regions. To determine instance and engine availability, see the RDS Management Console or CLI tools.

• SQL Server Integration Services (SSIS), SQL Server Analysis Services (SSAS) and SQL Server Reporting Services (SSRS) for RDS SQL Server are not supported in AWS GovCloud (US) Regions.

Documentation for Amazon Relational Database Service

Amazon RDS documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>
<tr>
<td>• 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.</td>
<td>• Do not enter ITAR-regulated data in the following fields:</td>
</tr>
<tr>
<td></td>
<td>• Database instance identifier</td>
</tr>
<tr>
<td></td>
<td>• Master user name</td>
</tr>
<tr>
<td></td>
<td>• Database name</td>
</tr>
<tr>
<td></td>
<td>• Database snapshot name</td>
</tr>
<tr>
<td></td>
<td>• Database security group name</td>
</tr>
<tr>
<td></td>
<td>• Database security group description</td>
</tr>
<tr>
<td></td>
<td>• Database parameter group name</td>
</tr>
<tr>
<td></td>
<td>• Database parameter group description</td>
</tr>
<tr>
<td></td>
<td>• Option group name</td>
</tr>
<tr>
<td></td>
<td>• Option group description</td>
</tr>
<tr>
<td></td>
<td>• Database subnet group name</td>
</tr>
<tr>
<td></td>
<td>• Database subnet group description</td>
</tr>
<tr>
<td></td>
<td>• Event subscription name</td>
</tr>
<tr>
<td></td>
<td>• Resource tags</td>
</tr>
</tbody>
</table>
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.
- 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) Regions 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 Service Endpoints (p. 62).

Amazon Redshift

Amazon Redshift is a fast, fully managed, petabyte-scale data warehouse service that makes it simple and cost-effective to efficiently analyze all your data using your existing business intelligence tools. It is optimized for datasets ranging from a few hundred gigabytes to a petabyte or more and costs less than $1,000 per terabyte per year, a tenth the cost of most traditional data warehousing solutions.

How Amazon Redshift Differs for AWS GovCloud (US)

- The Amazon Redshift Data API is not available in the AWS GovCloud (US) Regions.
- In AWS GovCloud (US) Regions, Amazon Redshift Spectrum is available in AWS GovCloud (US-West) only.
- In AWS GovCloud (US) Regions, all Amazon Redshift clusters must be launched in an Amazon VPC.
- Snapshot copy is not available in the AWS GovCloud (US) Regions.
- 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 the Amazon Redshift account ID for the AWS Region. The account ID for AWS GovCloud (US-West) is 665727464434. The account ID for AWS GovCloud (US-East) is 876460406779. 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 AWS GovCloud (US) Regions, 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"
}
}

Documentation for Amazon Redshift

Amazon Redshift documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>
</tbody>
</table>
| • 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. | • Do not enter ITAR-regulated data in the following fields:  
| | • Database instance identified  
| | • Master user name  
| | • Database name  
| | • Database snapshot name  
| | • Database security group name  
| | • Database security group description  
| | • Database parameter group name  
| | • Database parameter group description  
| | • Option group name  
| | • Option group description  
| | • Database subnet group name  
| | • Database subnet group description |
ITAR-Regulated Data Permitted | ITAR-Regulated Data Not Permitted
---|---
- Event subscription name
- Resource tags

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) Regions.

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) Regions 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 Service Endpoints (p. 62).

Amazon Rekognition

Amazon Rekognition makes it easy to add image and video analysis to your applications. You just provide an image or video to the Rekognition API, and the service can identify objects, people, text, scenes, and activities. It can detect any inappropriate content as well. Amazon Rekognition also provides highly accurate facial analysis and facial recognition. You can detect, analyze, and compare faces for a wide variety of use cases, including user verification, cataloging, people counting, and public safety.

How Amazon Rekognition Differs for AWS GovCloud (US)

- Celebrity Recognition is not available in AWS GovCloud (US).

Documentation for Amazon Rekognition

Amazon Rekognition documentation.
ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>• This service can generate metadata from customer-defined configurations. This metadata</td>
</tr>
<tr>
<td>• Image bytes</td>
<td>includes all configuration data in console fields, descriptions, resource names, and tagging</td>
</tr>
<tr>
<td>• External Image Identifiers</td>
<td>information. AWS suggests customers do not enter export-controlled information in those</td>
</tr>
<tr>
<td>• Face identifiers</td>
<td>fields.</td>
</tr>
<tr>
<td>• Video bytes</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>

Amazon Route 53

Amazon Route 53 is a highly available and scalable Domain Name System (DNS) web service. In the AWS GovCloud (US), you can use Route 53 private DNS and health checking.

How Amazon Route 53 Differs for AWS GovCloud (US)

Private Hosted Zones

- You can create private hosted zones in the AWS GovCloud (US). In general, the functionality is the same as for private hosted zones in the global version of Route 53. However, you can create alias records only when the alias target is another record in the same hosted zone. To route traffic to another AWS resource, such as an ELB load balancer or an S3 bucket, you can use a CNAME record instead of an alias record unless you're creating a record at the zone apex.

Health Checking

- You can create health checks that monitor endpoints in the AWS GovCloud, and you can create health checks that monitor the status of other health checks.
- Route 53 doesn't support creating health checks that monitor the status of CloudWatch alarms in the AWS GovCloud.
- As in other AWS Regions, if you create a health check that monitors an endpoint in the AWS GovCloud, you must make the endpoint available on the public internet. Route 53 health checkers send health checking requests over the public internet.
- You can restrict access to your endpoints by whitelisting the IP addresses of Route 53 health checkers in the AWS GovCloud:
  - 160.1.56.0/25
  - 160.1.55.0/25
  - 160.1.55.128/25
  - 18.253.167.128/25
AWS GovCloud (US) User Guide
Documentation for Amazon Route 53

• 18.253.168.0/25
• 18.253.167.0/25

Documentation for Amazon Route 53

Amazon Route 53 documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in the AWS GovCloud (US) Region. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled 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 is ITAR permitted</td>
<td>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</td>
</tr>
</tbody>
</table>

Amazon S3

Amazon Simple Storage Service (Amazon S3) is storage for the internet. You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere on the web. You can accomplish these tasks using the simple and intuitive web interface of the AWS Management Console.

How Amazon Simple Storage Service Differs for AWS GovCloud (US)

• You cannot do a direct copy of the contents of an Amazon S3 bucket in the AWS GovCloud (US) Regions to or from another AWS Region.
• If you use Amazon S3 policies, use the AWS GovCloud (US) ARN identifier. For more information, see Amazon Resource Names (ARNs) in GovCloud (US) Regions (p. 32).
• In AWS GovCloud (US) Regions, Amazon S3 has three endpoints. If you are processing ITAR-regulated data, use one of the SSL endpoints. If you have FIPS requirements, use a FIPS 140-2 endpoint (https://s3-fips.us-gov-west-1.amazonaws.com or https://s3-fips.us-gov-east-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 Service Endpoints (p. 62).
• Amazon S3 bucket names are unique to the AWS GovCloud (US) Regions. Bucket names in the AWS GovCloud (US) Regions are not shared across other standard AWS Regions.
• MFA delete is not available in AWS GovCloud (US) Regions.
• Amazon S3 Transfer Acceleration is not available in AWS GovCloud (US).
ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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></td>
<td>• Do not enter ITAR-regulated data in the following fields:</td>
</tr>
<tr>
<td></td>
<td>• Resource tags</td>
</tr>
</tbody>
</table>

Amazon SageMaker

This service is currently available in AWS GovCloud (US-West) only.

Amazon SageMaker is a fully managed machine learning service. With Amazon SageMaker, data scientists and developers can quickly and easily build and train machine learning models, and then directly deploy them into a production-ready hosted environment. It provides an integrated Jupyter authoring notebook instance for easy access to your data sources for exploration and analysis, so you don't have to manage servers. It also provides common machine learning algorithms that are optimized to run efficiently against extremely large data in a distributed environment. With native support for bring-your-own-algorithms and frameworks, Amazon SageMaker provides flexible distributed training options that adjust to your specific workflows.

How Amazon SageMaker Differs for AWS GovCloud (US)

• The following instance types are not supported in the AWS GovCloud (US) Region: t3.[medium, large, xlarge, 2xlarge] and p2.[xlarge, 8xlarge, 16xlarge].
• The associated API calls for these services are available but will fail with a 4xx message indicating "The requested operation is not supported in the called region".

Documentation for Amazon SageMaker

Amazon SageMaker documentation.
ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 a Notebook Instance and ephemeral drives can contain ITAR-regulated data. All data processed during training, automatic model tuning, batch transformation, and endpoint invocation can contain ITAR-regulated data.</td>
<td>• Amazon SageMaker metadata is not permitted to contain ITAR-regulated data. This metadata includes all configuration data that you enter when creating and maintaining your NotebookInstances, NotebookInstanceLifecycleConfigs, Endpoints, Models, EndpointConfig, TrainingJobs, HyperParameterTuningJobs, and BatchTransformJobs.</td>
</tr>
</tbody>
</table>

Do not enter ITAR-regulated data in the following console fields:
• NotebookInstance Name
• NotebookInstanceLifecycleConfig Name
• Model Name
• Model Container Hostname
• Model Environment names and values
• Endpoint Name
• Endpoint Config Name
• Endpoint Config Production Variant names
• Endpoint Config
• TrainingJob Name
• BatchTransformJob Name
• Hyperparameter Names or values
• Input Channel Name
• Any resource tag or value.
• Names of any metrics emitted by algorithms.
• Names of any training or inference container environment variables.

AWS Resource Groups

In AWS, a resource is an entity that you can work with. Examples include an Amazon EC2 instance, an AWS CloudFormation stack, or an Amazon S3 bucket. If you work with multiple resources, you might find it useful to manage them as a group rather than move from one AWS service to another for each task. AWS Resource Groups make it easier to manage and automate tasks on large numbers of resources at one time. You can use resource groups to organize your AWS resources. A resource group is a collection of AWS resources that are all in the same AWS region, and that match criteria provided in a query. In Resource Groups, there are two types of queries on which you can build a group: tag-based and AWS CloudFormation stack-based queries. Resource Groups feature permissions are at the account level. In
Resource Groups, the only available resource is a group. Groups have unique Amazon Resource Names (ARNs) associated with them.

**How AWS Resource Groups Differs for AWS GovCloud (US)**

This service has no differences between AWS GovCloud (US) Regions and the standard AWS Regions.

**Documentation for AWS Resource Groups**

AWS Resource Groups documentation.

**ITAR Boundary**

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>• Description</td>
<td>Do not enter ITAR-regulated data in the following console fields:</td>
</tr>
<tr>
<td></td>
<td>• Name</td>
</tr>
</tbody>
</table>

**AWS Security Hub**

AWS Security Hub provides you with a comprehensive view of your security state in AWS and helps you check your environment against security industry standards and best practices. Security Hub collects security data from across AWS accounts, services, and supported third-party partner products and helps you analyze your security trends and identify the highest priority security issues.

**How Security Hub Differs for AWS GovCloud (US)**

**Integrations**

- Not all AWS Service and partner integrations are available in the AWS GovCloud (US) Region. If an integration is not available, it is not listed on the Integrations page.

**Standards and Controls**

- For the CIS AWS Foundations Standard, the following controls are not supported in the AWS GovCloud (US) Region.
  - 1.13 - Ensure MFA is enabled for the "root" account
  - 1.14 - Ensure hardware MFA is enabled for the "root" account

- For the Payment Card Industry Data Security Standard (PCI DSS), the following controls are not supported in the AWS GovCloud (US) Region.
  - [PCI.CodeBuild.1] CodeBuild GitHub or Bitbucket source repository URLs should use OAuth
• [PCI.CodeBuild.2] CodeBuild project environment variables should not contain clear text credentials
• [PCI.IAM.4] Hardware MFA should be enabled for the root user
• [PCI.IAM.5] Virtual MFA should be enabled for the root user
• The following controls are not supported in the AWS GovCloud (US-East) Region.
  • [PCI.GuardDuty.1] GuardDuty should be enabled
  • [PCI.SageMaker.1] SageMaker notebook instances should not have direct internet access

• For the AWS Foundational Security Best Practices standard, the following controls are not supported in the AWS GovCloud (US) Region.
  • [IAM.6] Hardware MFA should be enabled for the root user
  • [CodeBuild.1] CodeBuild GitHub or Bitbucket source repository URLs should use OAuth
  • [CodeBuild.2] CodeBuild project environment variables should not contain clear text credentials
  • The following controls are not supported in the AWS GovCloud (US-East) Region.
    • [GuardDuty.1] GuardDuty should be enabled
    • [SageMaker.1] Amazon SageMaker notebook instances should not have direct internet access

**Documentation for Security Hub**

AWS Security Hub documentation.

**ITAR Boundary**

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 text and documents processed by AWS Security Hub can contain ITAR-regulated data.</td>
<td>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</td>
</tr>
</tbody>
</table>

**AWS Secrets Manager**

AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text. Secrets Manager offers secret rotation with built-in integration for Amazon RDS, Amazon Redshift, and Amazon DocumentDB. Also, the service is extensible to other types of secrets, including API keys and OAuth tokens. In addition, Secrets Manager enables you to control access to secrets using fine-grained permissions and audit secret rotation centrally for resources in the AWS Cloud, third-party services, and on-premises.
How AWS Secrets Manager Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

Documentation for AWS Secrets Manager

AWS Secrets Manager documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in the AWS GovCloud (US) Region. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled 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>• ITAR-regulated data may be stored and processed on the resources provisioned using AWS Secrets Manager so long as those services are utilized in an ITAR-compliant fashion.</td>
<td>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</td>
</tr>
</tbody>
</table>

AWS Serverless Application Repository

The AWS Serverless Application Repository is a managed repository for serverless applications. It enables teams, organizations, and individual developers to find, deploy, publish, share, store, and easily assemble serverless architectures.

How AWS Serverless Application Repository Differs for AWS GovCloud (US)

• Applications that are publicly shared in other AWS Regions are not automatically available in AWS GovCloud (US) Regions. To make applications available in AWS GovCloud (US) Regions, you must publish and share them independently of other AWS Regions.

Documentation for AWS Serverless Application Repository

AWS Serverless Application Repository documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in the AWS GovCloud (US) Region. To maintain ITAR compliance, you
must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled 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>• ITAR-regulated data may be stored and processed on the resources provisioned using AWS Serverless Application Repository so long as those services are utilized in an ITAR-compliant fashion.</td>
<td>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</td>
</tr>
</tbody>
</table>

### AWS Service Catalog

AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures. AWS Service Catalog allows you to centrally manage commonly deployed IT services, and helps you achieve consistent governance and meet your compliance requirements, while enabling users to quickly deploy only the approved IT services they need.

### How AWS Service Catalog Differs for AWS GovCloud (US)

- In AWS GovCloud (US) Copy Product is only supported within AWS GovCloud (US) Regions in the GovCloud partition.
- Organizations and Stack Sets are not currently supported in AWS GovCloud (US) Regions.

### Documentation for AWS Service Catalog

AWS Service Catalog documentation.

### ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in the AWS GovCloud (US) Region. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled 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>• ITAR-regulated data may be stored and processed on the resources provisioned using AWS Service Catalog so long as those services are utilized in an ITAR-compliant fashion.</td>
<td>• No ITAR-regulated data may be entered, stored, or processed by AWS Service Catalog. For example, AWS Service Catalog metadata is not permitted to contain ITAR-regulated data. This metadata includes all the configuration data that you enter when creating and maintaining your Products, Actions, and Tag Options.</td>
</tr>
</tbody>
</table>
Amazon SES

This service is currently available in AWS GovCloud (US-West) only.

Amazon SES is an email platform that provides an easy, cost-effective way for you to send and receive email using your own email addresses and domains. For example, you can send marketing emails such as special offers, transactional emails such as order confirmations, and other types of correspondence such as newsletters. When you use Amazon SES to receive mail, you can develop software solutions such as email autoresponders, email unsubscribe systems, and applications that generate customer support tickets from incoming emails.

How Amazon SES Differs for AWS GovCloud (US)

• Amazon SES doesn’t support email receiving in AWS GovCloud (US) Region.

Documentation for Amazon SES

Amazon SES documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 text and documents processed by Amazon Simple Email Service can contain ITAR-regulated data.</td>
<td>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</td>
</tr>
</tbody>
</table>

AWS Snow Family

AWS Snow Family is a service for customers who want to transport terabytes or petabytes of data to and from AWS, or who want to access the storage and compute power of the AWS Cloud locally and cost effectively in places where connecting to the internet might not be an option.

How AWS Snow Family Differs for AWS GovCloud (US)

• Users can only select AWS GovCloud (US) Regions 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 AWS GovCloud (US) Regions, you can use the following device types:
• 50 TB Snow Family (with 42 TB of usable space)
• 80 TB Snow Family (with 72 TB of usable space)
• 100 TB Snow Family Edge (with 82 TB of usable space)
• Compute functionality (AWS Lambda powered by AWS IoT Greengrass) for the AWS Snow Family Edge is not supported.

Documentation for AWS Snow Family

AWS Snow Family documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 Snow Family device can contain ITAR-regulated data.</td>
<td>• Snow Family metadata is not permitted to contain ITAR-regulated data. This includes the naming and configuration data that you enter when creating and managing your Snow Family 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. Snow Family generated metadata will not contain ITAR-regulated data.</td>
</tr>
</tbody>
</table>

AWS Server Migration Service

AWS Server Migration Service (AWS SMS) combines data collection tools with automated server replication to speed the migration of on-premises servers to AWS.

To use the Server Migration Connector with AWS GovCloud (US) Regions, 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, the AWS GovCloud (US) Regions should now be the regions listed.
How AWS Server Migration Service Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

Documentation for AWS Server Migration Service

AWS SMS User Guide.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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. • Do not enter ITAR-regulated data in the following fields: • VM names or paths • Virtual machine disk file paths • IP addresses or host names of VMs, ESXi hosts, vCenter, Hyper-V hosts, or SCVMM • User name of any service account or Active Directory user created for Service Migration Connector to log into vCenter, SCVMM, or Hyper-V • 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>

Amazon SNS

Amazon Simple Notification Service (Amazon SNS) is a web service that enables applications, end-users, and devices to instantly send and receive notifications from the cloud.

How Amazon Simple Notification Service Differs for AWS GovCloud (US)

• You cannot use Amazon SNS to send SMS messages while using the AWS GovCloud (US-East) Region.
**Documentation for Amazon Simple Notification Service**

Amazon SNS documentation.

**ITAR Boundary**

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>
| • You may enter ITAR-regulated data in the following field when meeting the notification endpoints conditions below:  
  • 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) Regions – may receive notifications containing ITAR-regulated data  
  • HTTPS URL endpoint in AWS GovCloud (US) Regions – 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) Regions – may receive notifications containing ITAR-regulated data if the customer has set up the endpoint URL in compliance with ITAR regulations | • ITAR-regulated data may not be entered, stored, or processed in Amazon SNS notification 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) Regions – 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 SQS

Amazon Simple Queue Service (Amazon SQS) is a fully managed message queuing service that makes it easy to decouple and scale microservices, distributed systems, and serverless applications. Amazon SQS moves data between distributed application components and helps you decouple these components.

How Amazon Simple Queue Service Differs for AWS GovCloud (US)

- 1-Minute CloudWatch metrics are not currently supported in any AWS GovCloud (US) Region.

Documentation for Amazon Simple Queue Service

Amazon SQS documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>
<tr>
<td></td>
<td>• Queue Name</td>
</tr>
<tr>
<td></td>
<td>• Queue Configuration</td>
</tr>
<tr>
<td></td>
<td>• Queue Policy Document</td>
</tr>
<tr>
<td></td>
<td>• Queue Permissions</td>
</tr>
</tbody>
</table>

AWS Step Functions

AWS Step Functions makes it easy to coordinate the components of distributed applications as a series of steps in a visual workflow. You can quickly build and run state machines to execute the steps of your application in a reliable and scalable fashion.

How AWS Step Functions Differs for AWS GovCloud (US)

- US Commercial regions supports FIPS and Non-FIPS endpoints.
• US GovCloud East supports FIPS and Non-FIPS endpoints.
• US GovCloud West only supports FIPS endpoints.
• US Commercial regions only supports AWS PrivateLink for Non-FIPS endpoints.
• US GovCloud East region supports AWS PrivateLink for FIPS and Non-FIPS endpoints.
• US GovCloud West region only supports AWS PrivateLink for FIPS endpoints.

Documentation for AWS Step Functions

AWS Step Functions documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>• This service boundary exists entirely within the GovCloud regions and all export-controlled Content entered, processed, and created within Service will exist in the GovCloud regions.</td>
<td>• No ITAR-regulated data can be entered, stored, or processed in AWS Step Functions. • AWS Step Functions 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. • For example, do not enter ITAR-regulated data in the following fields:  • State machine name  • State machine definition  • Activity name  • Execution name</td>
</tr>
</tbody>
</table>

AWS Storage Gateway

AWS Storage Gateway is a service that connects an on-premises software appliance with cloud-based storage to provide seamless and secure integration between your on-premises IT environment and the AWS storage infrastructure in the cloud.

How AWS Storage Gateway Differs for AWS GovCloud (US)

• A file gateway created inside AWS GovCloud (US) cannot connect to a bucket outside of the AWS GovCloud (US) Regions.
• A file gateway created outside of AWS GovCloud (US) cannot connect to a bucket inside AWS GovCloud (US).
AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 data entered and stored in tapes and volumes can contain ITAR-regulated data. All data entered and stored in S3 using the file gateway can contain ITAR-regulated data, as described in Amazon S3. | AWS Storage Gateway metadata is not permitted to contain ITAR-regulated data. This metadata includes all configuration data that you enter when creating and maintaining your gateway in AWS Storage Gateway, including but not limited to:  
  • Storage Gateway name.  
  • Tape barcode.  
  • The name of the iSCSI initiator configured for CHAP.  
  Do not enter ITAR-regulated data into the following console fields:  
  • Resource tag: Key  
  • Resource tag: Value |

AWS Storage Gateway AMI Information

The following table lists the available AWS Storage Gateway AMIs in the AWS GovCloud (US) Regions.

<table>
<thead>
<tr>
<th>Gateway Type</th>
<th>AMI ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Gateway</td>
<td>ami-05d2a6a us-gov-west-1</td>
</tr>
</tbody>
</table>

Amazon SWF

Amazon Simple Workflow Service (Amazon SWF) makes it easy to build applications that coordinate work across distributed components. In Amazon SWF, a task represents a logical unit of work that is
performed by a component of your application. Coordinating tasks across the application involves managing intertask dependencies, scheduling, and concurrency in accordance with the logical flow of the application. Amazon SWF gives you full control over implementing tasks and coordinating them without worrying about underlying complexities such as tracking their progress and maintaining their state.

How Amazon Simple Workflow Service Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) and the standard AWS Regions.

Documentation for Amazon Simple Workflow Service

Amazon SWF documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>• This service boundary exists entirely within the GovCloud regions and all export-controlled Content entered, processed, and created within Service will exist in the GovCloud regions.</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>

AWS Systems Manager

Use AWS Systems Manager to organize, monitor, and automate management tasks on your AWS resources.
How AWS Systems Manager Differs for AWS GovCloud (US)

- AWS AppConfig, a component of AWS Systems Manager, is not supported in AWS GovCloud (US) Regions.
- Support for viewing association histories is not available in AWS GovCloud (US) Regions.
- The following AWS Systems Manager Automation actions for invoking APIs from other AWS services are not supported:
  - aws:executeAwsApi
  - aws:waitForAwsResourceProperty
  - aws:assertAwsResourceProperty
- SSM Agent for AWS GovCloud (US) can be downloaded from the following location:
  
  https://amazon-ssm-us-gov-east-1.s3.us-gov-east-1.amazonaws.com/latest/windows_amd64/AmazonSSMAgentSetup.exe

Documentation for AWS Systems Manager

AWS Systems Manager documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 AWS Systems Manager Document content and Parameter Store values can contain ITAR-regulated data.</td>
<td>The following AWS 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>

Amazon Textract

Amazon Textract makes it easy to add document text detection and analysis to your applications. The Amazon Textract Text Detection API can detect text in a variety of documents including financial reports, medical records, and tax forms. For documents with structured data, you can use the Amazon Textract Document Analysis API to extract text, forms and tables.

How Amazon Textract Differs for AWS GovCloud (US)

This service has no differences between the AWS GovCloud (US) Region and the standard AWS Regions.
AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 Textract can contain ITAR-regulated data.</td>
<td>• Amazon Textract metadata is not permitted to contain ITAR-regulated data.</td>
</tr>
</tbody>
</table>

AWS Transfer Family

AWS Transfer Family is a secure transfer service that enables you to transfer files into and out of Amazon Simple Storage Service (Amazon S3) storage over the following protocols:

• Secure Shell (SSH) File Transfer Protocol (SFTP) (AWS Transfer for SFTP).
• File Transfer Protocol Secure (FTPS) (AWS Transfer for FTPS).
• File Transfer Protocol (FTP) (AWS Transfer for FTP).

How AWS Transfer Family Differs for AWS GovCloud (US)

• PUBLIC and VPC_ENDPOINT endpoint types are not supported. Only VPC endpoint type is supported, for both internet and internet facing access. For more information, see Creating a server in a virtual private cloud in the AWS Transfer Family User Guide.
• If you are providing your end users access to your endpoint using a custom hostname, you need to map your endpoint’s IP addresses to the custom domain using Amazon Route 53 or any DNS provider. If you use a hostname registered with Route 53, there are some DNS limitations. For more information about using Route 53 for GovCloud endpoints, see Setting Up Amazon Route 53 with Your AWS GovCloud (US) Resources.

Documentation for AWS Transfer Family

AWS Transfer Family documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any...
ITAR-controlled data in AWS GovCloud (US) Regions, 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 transferred with AWS Transfer Family can contain ITAR-regulated data.</td>
<td>• AWS Transfer Family metadata is not permitted to contain ITAR-regulated data.</td>
</tr>
</tbody>
</table>

Amazon Transcribe

Amazon Transcribe uses advanced machine learning technologies to recognize speech in audio files and transcribe them into text. Use Amazon Transcribe to convert audio to text and to create applications that incorporate the content of audio files. For example, you can transcribe the audio track from a video recording to create closed captioning for the video.

How Amazon Transcribe Differs for AWS GovCloud (US)

• Streaming Transcription using Amazon Transcribe is not available in the AWS GovCloud (US) Region.
• Automatic content reaction is not available in the AWS GovCloud (US-East) Region.
• Automatic language identification is not available in the AWS GovCloud (US-East) Region.

Documentation for Amazon Transcribe

Amazon Transcribe documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 text and documents processed by Amazon Transcribe can contain ITAR-regulated data.</td>
<td>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</td>
</tr>
</tbody>
</table>

Amazon Translate

This service is currently available in AWS GovCloud (US-West) only.
Amazon Translate is a neural machine translation service for translating text to and from English across a breadth of supported languages. Powered by deep-learning technologies, Amazon Translate delivers fast, high-quality, and affordable language translation. It provides a managed, continually trained solution so you can easily translate company and user-authored content or build applications that require support across multiple languages. The machine translation engine has been trained on a wide variety of content across different domains to produce quality translations that serve any industry need.

How Amazon Translate Differs for AWS GovCloud (US)

- Automatic source language detection using Amazon Comprehend is not available in AWS GovCloud (US) Regions.
- The default throttling limits for AWS GovCloud (US) are set to 5000 Bytes per 10 seconds per language pair and 10 transactions per second per language pair. You can request an increase for any of the limits using the Amazon Translate service limits increase form.
- The following languages are not supported in the AWS GovCloud (US) Regions: Traditional Chinese, Czech, Italian, Japanese, Russian, and Turkish.

Documentation for Amazon Translate

Amazon Translate documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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 text and all language pairs (source language and target language) processed by Amazon Translate can contain ITAR-regulated data.</td>
<td>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</td>
</tr>
</tbody>
</table>

AWS Trusted Advisor

An online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment, Trusted Advisor provides real time guidance to help you provision your resources following AWS best practices.

How AWS Trusted Advisor Differs for AWS GovCloud (US)

- Email notifications are not yet enabled in Trusted Advisor in the AWS GovCloud (US) Regions.
The following tables list the Trusted Advisor checks that are available in the AWS GovCloud (US) Regions and the required support level:

**Cost optimization**

The following table lists the Trusted Advisor checks for cost optimization that are available in the AWS GovCloud (US) Regions.

<table>
<thead>
<tr>
<th>Check</th>
<th>Support level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon RDS Idle DB Instances</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Idle Load Balancers</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Low Utilization Amazon EC2 Instances</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Unassociated Elastic IP Addresses</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Underutilized Amazon EBS Volumes</td>
<td>Business and Enterprise</td>
</tr>
</tbody>
</table>

**Fault tolerance**

The following table lists the Trusted Advisor checks for fault tolerance that are available in the AWS GovCloud (US) Regions.

<table>
<thead>
<tr>
<th>Check</th>
<th>Support level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Aurora DB Instance Accessibility</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Amazon EBS Snapshots</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Amazon EC2 Availability Zone Balance</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Amazon RDS Backups</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Amazon RDS Multi-AZ</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Amazon S3 Bucket Logging</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Amazon S3 Bucket Versioning</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Auto Scaling Group Resources</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Auto Scaling Group Health Check</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>ELB Connection Draining</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>ELB Cross-Zone Load Balancing</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Load Balancer Optimization</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>VPN Tunnel Redundancy</td>
<td>Business and Enterprise</td>
</tr>
</tbody>
</table>

**Performance**

The following table lists the Trusted Advisor checks for performance that are available in the AWS GovCloud (US) Regions.
How AWS Trusted Advisor Differs for AWS GovCloud (US)

<table>
<thead>
<tr>
<th>Check</th>
<th>Support level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon EBS Provisioned IOPS (SSD) Volume Attachment Configuration</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Amazon EC2 to EBS Throughput Optimization</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>High Utilization Amazon EC2 Instances</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Large Number of EC2 Security Group Rules Applied to an Instance</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Large Number of Rules in an EC2 Security Group</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Overutilized Amazon EBS Magnetic Volumes</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Service Limits</td>
<td>All support levels</td>
</tr>
</tbody>
</table>

**Security**

The following table lists the Trusted Advisor checks for security that are available in the AWS GovCloud (US) Regions.

<table>
<thead>
<tr>
<th>Check</th>
<th>Support level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon EBS Public Snapshots</td>
<td>All support levels</td>
</tr>
<tr>
<td>Amazon RDS Security Group Access Risk</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Amazon RDS Public Snapshots</td>
<td>All support levels</td>
</tr>
<tr>
<td>Amazon S3 Bucket Permissions</td>
<td>All support levels</td>
</tr>
<tr>
<td>AWS CloudTrail Logging</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>ELB Security Groups</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>ELB Listener Security</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>IAM Access Key Rotation</td>
<td>All support levels</td>
</tr>
<tr>
<td>IAM Use</td>
<td>All support levels</td>
</tr>
<tr>
<td>IAM Password Policy</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Security Groups - Specific Ports Unrestricted</td>
<td>All support levels</td>
</tr>
<tr>
<td>Security Groups - Unrestricted Access</td>
<td>Business and Enterprise</td>
</tr>
</tbody>
</table>

**Service quotas**

The following table lists the checks for Trusted Advisor service quotas, formerly known as limits, that are available in the AWS GovCloud (US) Regions.

<table>
<thead>
<tr>
<th>Check</th>
<th>Support level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Scaling Groups</td>
<td>All support levels</td>
</tr>
</tbody>
</table>
## How AWS Trusted Advisor Differs for AWS GovCloud (US)

<table>
<thead>
<tr>
<th>Check</th>
<th>Support level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Scaling Launch Configurations</td>
<td>All support levels</td>
</tr>
<tr>
<td>CloudFormation Stacks</td>
<td>All support levels</td>
</tr>
<tr>
<td>DynamoDB Read Capacity</td>
<td>All support levels</td>
</tr>
<tr>
<td>DynamoDB Write Capacity</td>
<td>All support levels</td>
</tr>
<tr>
<td>EBS Active Snapshots</td>
<td>All support levels</td>
</tr>
<tr>
<td>EBS Active Volumes</td>
<td>All support levels</td>
</tr>
<tr>
<td>EBS Cold HDD (sc1) Volume Storage</td>
<td>All support levels</td>
</tr>
<tr>
<td>EBS General Purpose SSD (gp2) Volume Storage</td>
<td>All support levels</td>
</tr>
<tr>
<td>EBS Magnetic (standard) Volume Storage</td>
<td>All support levels</td>
</tr>
<tr>
<td>EBS Provisioned IOPS (SSD) Volume Aggregate IOPS</td>
<td>All support levels</td>
</tr>
<tr>
<td>EBS Provisioned IOPS SSD (io1) Volume Storage</td>
<td>All support levels</td>
</tr>
<tr>
<td>EBS Throughput Optimized HDD (st1) Volume Storage</td>
<td>All support levels</td>
</tr>
<tr>
<td>EC2 Elastic IP Addresses</td>
<td>All support levels</td>
</tr>
<tr>
<td>EC2 Reserved Instance Leases</td>
<td>All support levels</td>
</tr>
<tr>
<td>ELB Active Load Balancers</td>
<td>All support levels</td>
</tr>
<tr>
<td>ELB Network Load Balancers</td>
<td>All support levels</td>
</tr>
<tr>
<td>ELB Application Load Balancers</td>
<td>All support levels</td>
</tr>
<tr>
<td>IAM Group</td>
<td>All support levels</td>
</tr>
<tr>
<td>IAM Instance Profiles</td>
<td>All support levels</td>
</tr>
<tr>
<td>IAM Policies</td>
<td>All support levels</td>
</tr>
<tr>
<td>IAM Roles</td>
<td>All support levels</td>
</tr>
<tr>
<td>IAM Server Certificates</td>
<td>All support levels</td>
</tr>
<tr>
<td>IAM Users</td>
<td>All support levels</td>
</tr>
<tr>
<td>Kinesis Shards per Region</td>
<td>All support levels</td>
</tr>
<tr>
<td>RDS Cluster Parameter Groups</td>
<td>All support levels</td>
</tr>
<tr>
<td>RDS Cluster Roles</td>
<td>All support levels</td>
</tr>
<tr>
<td>RDS Clusters</td>
<td>All support levels</td>
</tr>
<tr>
<td>RDS DB Instances</td>
<td>All support levels</td>
</tr>
<tr>
<td>RDS DB Parameter Groups</td>
<td>All support levels</td>
</tr>
<tr>
<td>RDS DB Security Groups</td>
<td>All support levels</td>
</tr>
</tbody>
</table>
### Check

<table>
<thead>
<tr>
<th>Check</th>
<th>Support level</th>
</tr>
</thead>
<tbody>
<tr>
<td>RDS DB Manual Snapshots</td>
<td>All support levels</td>
</tr>
<tr>
<td>RDS Event Subscriptions</td>
<td>All support levels</td>
</tr>
<tr>
<td>RDS Max Auths per Security Group</td>
<td>All support levels</td>
</tr>
<tr>
<td>RDS Option Groups</td>
<td>All support levels</td>
</tr>
<tr>
<td>RDS Read Replicas per Master</td>
<td>All support levels</td>
</tr>
<tr>
<td>RDS Reserved Instances</td>
<td>All support levels</td>
</tr>
<tr>
<td>RDS Subnet Groups</td>
<td>All support levels</td>
</tr>
<tr>
<td>RDS Subnets per Subnet Group</td>
<td>All support levels</td>
</tr>
<tr>
<td>RDS Total Storage Quota</td>
<td>All support levels</td>
</tr>
<tr>
<td>VPC</td>
<td>All support levels</td>
</tr>
<tr>
<td>VPC Elastic IP Address</td>
<td>All support levels</td>
</tr>
<tr>
<td>VPC Internet Gateways</td>
<td>All support levels</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Category</th>
<th>Check</th>
<th>Support Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost optimization</td>
<td>Amazon EC2 Reserved Instance Optimization</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Amazon EC2 Reserved Instance Lease Expiration</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Amazon Route 53 MX Resource Record Sets and Sender Policy Framework</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Amazon Route 53 Latency Resource Record Sets</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Fault tolerance</td>
<td>Amazon Route 53 Name Server Delegations</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Amazon Route 53 High TTL Resource Record Sets</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Amazon Route 53 Failover Resource Record Sets</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Amazon Route 53 Deleted Health Checks</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>AWS Direct Connect Connection Redundancy</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>AWS Direct Connect Location Redundancy</td>
<td>Business and Enterprise</td>
</tr>
</tbody>
</table>

199
<table>
<thead>
<tr>
<th>Category</th>
<th>Check</th>
<th>Support Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AWS Direct Connect Virtual Interface Redundancy</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>EC2 Config Service for EC2 Windows Instances</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>ENA Driver Version for EC2 Windows Instances</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>NVMe Driver Version for EC2 Windows Instances</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>PV Driver Version for EC2 Windows Instances</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Performance</td>
<td>Amazon Route 53 Alias Resource Record Sets</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Amazon CloudFront Alternate Domain Names</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Amazon CloudFront Content Delivery Optimization</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Amazon CloudFront Header Forwarding and Cache Hit Ratio</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td>Security</td>
<td>MFA on Root Account</td>
<td>All support levels</td>
</tr>
<tr>
<td></td>
<td>Amazon Route 53 MX Resource Record Sets and Sender Policy Framework</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Amazon CloudFront Custom SSL Certificates in the IAM Certificate Store</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Amazon CloudFront SSL Certificate on the Origin Server</td>
<td>Business and Enterprise</td>
</tr>
<tr>
<td></td>
<td>Exposed Access Keys</td>
<td>All support levels</td>
</tr>
<tr>
<td>Service quotas</td>
<td>SES Daily Sending Quota</td>
<td>All support levels</td>
</tr>
<tr>
<td></td>
<td>Route 53 Traffic Policies</td>
<td>All support levels</td>
</tr>
<tr>
<td></td>
<td>Route 53 Traffic Policy Instances</td>
<td>All support levels</td>
</tr>
<tr>
<td></td>
<td>Route 53 Reusable Delegation Sets</td>
<td>All support levels</td>
</tr>
<tr>
<td></td>
<td>Route 53 Max Health Checks</td>
<td>All support levels</td>
</tr>
<tr>
<td></td>
<td>Route 53 Hosted Zones</td>
<td>All support levels</td>
</tr>
<tr>
<td></td>
<td>EC2 On-Demand Instances</td>
<td>All support levels</td>
</tr>
<tr>
<td></td>
<td>EBS Active Volumes</td>
<td>All support levels</td>
</tr>
</tbody>
</table>
AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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>• This service boundary exists entirely within the GovCloud regions and all export-controlled Content entered, processed, and created within Service will exist in the GovCloud regions.</td>
<td>• This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields.</td>
</tr>
</tbody>
</table>

Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network that you’ve defined. This virtual network closely resembles a traditional network that you’d operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

How Amazon Virtual Private Cloud Differs for AWS GovCloud (US)

• 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. 130).
• Use SSL (HTTPS) when you make calls to the service in the AWS GovCloud (US) Region. In other AWS Regions, you can use HTTP or HTTPS.
• Traffic mirror sessions are visible to the owner of a traffic mirror target only if created using the same account. If a traffic mirror target is shared with other accounts, those other accounts may still create sessions with that target, but those sessions will not be visible to the target owner.
• You cannot create your own managed prefix lists. You can view AWS-managed prefix lists by using the DescribePrefixLists API or describe-prefix-lists AWS CLI command.

Documentation for Amazon Virtual Private Cloud

Amazon VPC documentation.
ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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></td>
<td>• Destination log group name</td>
</tr>
</tbody>
</table>

AWS Site-to-Site VPN

AWS Site-to-Site VPN enables you to securely connect your on-premises network or branch office site to your Amazon Virtual Private Cloud (Amazon VPC).

How Site-to-Site VPN Differs for AWS GovCloud (US)

• AWS Site-to-Site VPN integration with Global Accelerator (Accelerated VPN Connections) is not available in the AWS GovCloud (US) Region.
• The AWS Site-to-Site VPN endpoints in AWS GovCloud (US) operate using FIPS 140-2 validated cryptographic modules. Correspondingly, VPN connections created in GovCloud require a different set of algorithms to establish a tunnel. For more information about FIPS 140-2, see "Cryptographic Module Validation Program" on the NIST Computer Security Resource Center website.
• Use SSL (HTTPS) when you make calls to the service in the AWS GovCloud (US) Region. In other AWS Regions, you can use HTTP or HTTPS.

Documentation for AWS Site-to-Site VPN

AWS VPN documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, this section does not apply to you. The following information identifies the ITAR boundary for this service:
### AWS WAF

This service is currently available in AWS GovCloud (US-West) only.

AWS WAF is a web application firewall that lets you monitor web requests that are forwarded to Amazon CloudFront distributions, Application Load Balancers, or APIGateway APIs. You can also use AWS WAF to block or allow requests based on conditions that you specify, such as the IP addresses that requests originate from or values in the requests.

#### How AWS WAF Differs for AWS GovCloud (US)

AWS WAF for AWS GovCloud (US) doesn't support the following functionality:

- AWS Marketplace managed rule groups are not available in AWS GovCloud (US). Managed rule groups are collections of predefined, ready-to-use rules that AWS and AWS Marketplace sellers write and maintain for you. AWS managed rule groups are provided free of charge with AWS WAF and are available for use in AWS GovCloud (US). AWS Marketplace rule groups are provided for subscription by AWS Marketplace sellers and aren’t available for use in AWS GovCloud (US). For more information about managed rule groups in AWS WAF, see Managed rule groups in the AWS WAF, AWS Firewall Manager, and AWS Shield Advanced Developer Guide.

- Logging of web ACL traffic information is not available in AWS GovCloud (US). Logging provides detailed information about traffic that is analyzed by your web ACL. For information about logging in AWS WAF, see Logging Web ACL traffic information in the AWS WAF, AWS Firewall Manager, and AWS Shield Advanced Developer Guide.

#### Documentation for AWS WAF

AWS WAF documentation.

#### ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in the AWS GovCloud (US-West) Region. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any

### ITAR-Regulated Data Permitted vs. ITAR-Regulated Data Not Permitted

<table>
<thead>
<tr>
<th>ITAR-Regulated Data Permitted</th>
<th>ITAR-Regulated Data Not Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>- You can transmit ITAR-regulated data in clear text across AWS Site-to-Site VPN tunnels, assuming the destination endpoint is ITAR compliant.</td>
<td>- AWS Site-to-Site VPN 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 Site-to-Site VPNs. For example, do not enter ITAR-regulated data into user input fields such as the following:</td>
</tr>
<tr>
<td></td>
<td>- Display Name</td>
</tr>
<tr>
<td></td>
<td>- Topic Policy</td>
</tr>
<tr>
<td></td>
<td>- Topic Delivery Policy</td>
</tr>
<tr>
<td></td>
<td>- Topic ARN</td>
</tr>
<tr>
<td></td>
<td>- Endpoint</td>
</tr>
</tbody>
</table>
Amazon WorkSpaces

This service is currently available in AWS GovCloud (US-West) only.

Amazon WorkSpaces is a managed, secure cloud desktop service. You can use Amazon WorkSpaces to provision either Windows or Amazon Linux 2 desktops in just a few minutes and quickly scale to provide thousands of desktops to workers across the globe. You can pay either monthly or hourly, just for the WorkSpaces you launch, which helps you save money when compared to traditional desktops and on-premises virtual desktop infrastructure (VDI) solutions. Amazon WorkSpaces helps you eliminate the complexity in managing hardware inventory and OS versions and patches which helps simplify your desktop delivery strategy. With Amazon WorkSpaces, your users get a fast, responsive desktop of their choice that they can access anywhere, anytime, from any supported device.

How Amazon WorkSpaces Differs for AWS GovCloud (US)

• The Amazon WorkSpaces Application Manager console is not supported.
• The Web Access client (from browser) is not supported.
• The cross-Region redirection feature is not supported in AWS GovCloud (US).

Documentation for Amazon WorkSpaces

Amazon WorkSpaces documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in AWS GovCloud (US) Regions. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled data in AWS GovCloud (US) Regions, 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
--- | ---
• Amazon WorkSpaces passwords are protected as ITAR-regulated data through AWS Directory Service. | Amazon WorkSpaces metadata is not permitted to contain ITAR-regulated data. This metadata includes all configuration data that you enter when creating and maintaining your WorkSpaces. Do not enter ITAR-regulated data in the following console fields:
• AMI descriptions
• Resource tags
• If importing ITAR-regulated images, do not use pre-signed URLs for the CLI argument.
• Key pairs created using HTTP
• All data stored and processed within Amazon WorkSpaces can contain ITAR-regulated data. | AWS X-Ray

AWS X-Ray is a service that collects data about requests that your application serves, and provides tools you can use to view, filter, and gain insights into that data to identify issues and opportunities for optimization. For any traced request to your application, you can see detailed information not only about the request and response, but also about calls that your application makes to downstream AWS resources, microservices, databases and HTTP web APIs.

How AWS X-Ray Differs for AWS GovCloud (US)

Versions 3.1.0 or above of AWS X-Ray Daemon should be used in AWS GovCloud (US) Region.

Documentation for AWS X-Ray

AWS X-Ray documentation.

ITAR Boundary

AWS GovCloud (US) has an ITAR boundary, which defines where customers are allowed to store ITAR-controlled data for this service in the AWS GovCloud (US) Region. To maintain ITAR compliance, you must place ITAR-controlled data on the applicable part of the ITAR boundary. If you do not have any ITAR-controlled 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 |
--- | ---
• ITAR-regulated data may be stored and processed on the resources provisioned using AWS X-Ray so long as those services are utilized in an ITAR-compliant fashion. | • This service can generate metadata from customer-defined configurations. This metadata includes all configuration data in console fields, descriptions, resource names, and tagging information. AWS suggests customers do not enter export-controlled information in those fields. |
Troubleshooting

The following section discusses common issues you might encounter when you work in the AWS GovCloud (US-West) or AWS GovCloud (US-East) Regions.

Topics
- Client.UnsupportedOperation: Instances can only be launched within Amazon VPC in this region (p. 206)

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. 130). 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-West) Region, you receive an error.
Related Resources

This topic lists additional resources related to AWS GovCloud (US-West) and AWS GovCloud (US-East) regions.

All the pricing related information can be found at AWS Billing and Cost Management documentation.

For more information, see AWS GovCloud (US) Documentation.

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>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>
### Experienced with AWS

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>
# Document History

The following table describes important changes to the documentation since the last release of the *AWS GovCloud (US) User Guide*.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date Changed</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Lake Formation</td>
<td>AWS Lake Formation is now supported in the AWS GovCloud (US) Region. See [AWS Lake Formation](p. 155).</td>
<td>November 11, 2020</td>
</tr>
<tr>
<td>Amazon EventBridge</td>
<td>Amazon EventBridge is now supported in the AWS GovCloud (US) Region. See [Amazon EventBridge](p. 140).</td>
<td>November 4, 2020</td>
</tr>
<tr>
<td>Amazon QuickSight</td>
<td>Amazon QuickSight is now supported in the AWS GovCloud (US) Region. See [Amazon QuickSight](p. 169).</td>
<td>October 28, 2020</td>
</tr>
<tr>
<td>AWS Transfer Family</td>
<td>AWS Transfer Family is now supported in the AWS GovCloud (US) Region. See [AWS Transfer Family](p. 193).</td>
<td>September 30, 2020</td>
</tr>
<tr>
<td>Amazon Elastic Block Store EBS direct APIs</td>
<td>EBS direct APIs is now supported in the AWS GovCloud (US) Region. See [Accessing the contents of an EBS snapshot](p. 150).</td>
<td>September 15, 2020</td>
</tr>
<tr>
<td>Amazon SQS</td>
<td>Tagging Amazon SQS resources is now supported in all AWS GovCloud (US) Regions. See [Amazon SQS](p. 188).</td>
<td>September 15, 2020</td>
</tr>
<tr>
<td>Amazon Textract</td>
<td>Amazon Textract is now supported in the AWS GovCloud (US) Region. See [Amazon Textract](p. 192).</td>
<td>August 19, 2020</td>
</tr>
<tr>
<td>Amazon DocumentDB (with MongoDB compatibility)</td>
<td>Amazon DocumentDB is now supported in the AWS GovCloud (US) Region. See [Amazon DocumentDB (with MongoDB compatibility)](p. 124).</td>
<td>June 29, 2020</td>
</tr>
<tr>
<td>Amazon Kinesis Data Analytics</td>
<td>Amazon Kinesis Data Analytics is now supported in the AWS GovCloud (US) Region. See [Amazon Kinesis Data Analytics](p. 152).</td>
<td>June 24, 2020</td>
</tr>
<tr>
<td>AWS Backup</td>
<td>AWS Backup is now supported in the AWS GovCloud (US) Region. See [AWS Backup](p. 95).</td>
<td>June 24, 2020</td>
</tr>
<tr>
<td>Amazon Cognito</td>
<td>Amazon Cognito is now supported in the AWS GovCloud (US) Region. See [Amazon Cognito](p. 116).</td>
<td>May 13, 2020</td>
</tr>
<tr>
<td>Amazon EKS</td>
<td>Amazon Elastic Kubernetes Service is now supported in the AWS GovCloud (US) Region. See [Amazon Elastic Kubernetes Service](p. 135).</td>
<td>May 13, 2020</td>
</tr>
<tr>
<td>Amazon Comprehend Medical</td>
<td>Amazon Comprehend Medical is now supported in the AWS GovCloud (US) Region. See [Amazon Comprehend Medical](p. 118).</td>
<td>May 08, 2020</td>
</tr>
<tr>
<td>Amazon Managed Streaming for Apache Kafka (MSK)</td>
<td>Amazon Managed Streaming for Apache Kafka (MSK) is now supported in the AWS GovCloud (US) Region. See [Amazon Managed Streaming for Apache Kafka (MSK)](p. 159).</td>
<td>May 06, 2020</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date Changed</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Apache Kafka (MSK)</td>
<td>Amazon Simple Email Service is now supported in the AWS GovCloud (US) Region. See Amazon SES (p. 184).</td>
<td>April 30, 2020</td>
</tr>
<tr>
<td>Amazon SES</td>
<td>Amazon Pinpoint is now supported in the AWS GovCloud (US) Region. See Amazon Pinpoint (p. 167).</td>
<td>April 30, 2020</td>
</tr>
<tr>
<td>AWS CodePipeline</td>
<td>AWS CodePipeline is now supported in the AWS GovCloud (US) Region. See AWS CodePipeline (p. 115).</td>
<td>April 08, 2020</td>
</tr>
<tr>
<td>AWS Outposts</td>
<td>AWS Outposts is now supported in the AWS GovCloud (US) Regions. See AWS Outposts (p. 165).</td>
<td>March 25, 2020</td>
</tr>
<tr>
<td>AWS X-Ray</td>
<td>AWS X-Ray is now supported in the AWS GovCloud (US) Regions. See AWS X-Ray (p. 205).</td>
<td>February 19, 2020</td>
</tr>
<tr>
<td>AWS Batch</td>
<td>AWS Batch is now supported in the AWS GovCloud (US) Regions. See AWS Batch (p. 94).</td>
<td>January 29, 2020</td>
</tr>
<tr>
<td>Amazon EC2 Image Builder</td>
<td>Amazon EC2 Image Builder is now supported in the AWS GovCloud (US-East) and AWS GovCloud (US-West) Regions. See Amazon EC2 Image Builder (p. 132).</td>
<td>December 03, 2019</td>
</tr>
<tr>
<td>Amazon S3</td>
<td>Access points for S3 buckets. Customers can attach additional access-points to both existing and new buckets. See Amazon S3 (p. 177).</td>
<td>December 03, 2019</td>
</tr>
<tr>
<td>AWS DataSync</td>
<td>AWS DataSync is now supported in the AWS GovCloud (US-East) region. See AWS DataSync (p. 100).</td>
<td>November 20, 2019</td>
</tr>
<tr>
<td>AWS Artifact</td>
<td>AWS Artifact is now supported in the AWS GovCloud (US-West) region. See AWS Artifact (p. 88).</td>
<td>October 9, 2019</td>
</tr>
<tr>
<td>Amazon AppStream 2.0</td>
<td>Amazon AppStream 2.0 is now supported in the AWS GovCloud (US-West) region. See Amazon AppStream 2.0 (p. 86).</td>
<td>October 9, 2019</td>
</tr>
<tr>
<td>AWS Resource Groups</td>
<td>AWS Resource Groups is now supported in the AWS GovCloud (US) Region. See AWS Resource Groups (p. 179).</td>
<td>September 25, 2019</td>
</tr>
<tr>
<td>AWS IoT Device Defender</td>
<td>AWS IoT Device Defender is now supported in the AWS GovCloud (US) Region. See AWS IoT Device Defender (p. 148).</td>
<td>November 14, 2018</td>
</tr>
<tr>
<td>AWS Resource Access Manager</td>
<td>AWS Resource Access Manager is now supported in the AWS GovCloud (US-East) Region. See AWS Resource Access Manager (p. 171).</td>
<td>August 28, 2019</td>
</tr>
<tr>
<td>Amazon Neptune</td>
<td>Amazon Neptune is now supported in the AWS GovCloud (US) Region. See Amazon Neptune (p. 161).</td>
<td>August 14, 2019</td>
</tr>
<tr>
<td>AWS Health</td>
<td>AWS Health is now supported in the AWS GovCloud US. See AWS Health (p. 144).</td>
<td>August 7, 2019</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date Changed</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Kinesis Data Firehose</td>
<td>Kinesis Data Firehose is now supported in the AWS GovCloud (US-East) Region. See Amazon Kinesis Data Firehose (p. 152).</td>
<td>June 26, 2019</td>
</tr>
<tr>
<td>AWS IoT Greengrass</td>
<td>AWS IoT Greengrass is now supported in the AWS GovCloud (US-West) Region. See AWS IoT Greengrass (p. 150).</td>
<td>June 26, 2019</td>
</tr>
<tr>
<td>AWS Secrets Manager</td>
<td>AWS Fargate is now supported in the AWS GovCloud (US) Regions. See AWS Fargate (p. 141).</td>
<td>June 24th, 2019</td>
</tr>
<tr>
<td>AWS Secrets Manager</td>
<td>AWS Secrets Manager is now supported in the AWS GovCloud (US-West) Region. See AWS Secrets Manager (p. 181).</td>
<td>June 11th, 2019</td>
</tr>
<tr>
<td>AWS DataSync</td>
<td>AWS DataSync is now supported in the AWS GovCloud (US-West) Region. See AWS DataSync (p. 100).</td>
<td>June 11th, 2019</td>
</tr>
<tr>
<td>AWS Serverless Application Repository</td>
<td>AWS Serverless Application Repository is now supported in the AWS GovCloud (US-West) Region. See AWS Serverless Application Repository (p. 182).</td>
<td>June 11th, 2019</td>
</tr>
<tr>
<td>AWS CodeBuild</td>
<td>AWS CodeBuild is now supported in the AWS GovCloud (US-West) Region. See AWS CodeBuild (p. 111).</td>
<td>June 11th, 2019</td>
</tr>
<tr>
<td>Amazon Route 53</td>
<td>Amazon Route 53 is now supported in the AWS GovCloud (US-West) Region. See Amazon Route 53 (p. 176).</td>
<td>May 29, 2019</td>
</tr>
<tr>
<td>Amazon Athena</td>
<td>Amazon Athena is now supported in the AWS GovCloud (US) Regions. See Amazon Athena (p. 89).</td>
<td>May 13, 2019</td>
</tr>
<tr>
<td>AWS WAF</td>
<td>AWS WAF is now supported in the AWS GovCloud (US-West) Region. See AWS WAF (p. 203).</td>
<td>March 13, 2019</td>
</tr>
<tr>
<td>Amazon Comprehend</td>
<td>Amazon Comprehend is now supported in the AWS GovCloud (US-West) Region.</td>
<td>March 13, 2019</td>
</tr>
<tr>
<td>Updated the guide for the re-merge</td>
<td>Updated all the references from a single govCloud region to multi-regions for GovCloud</td>
<td>February 6, 2019</td>
</tr>
<tr>
<td>Amazon Transcribe</td>
<td>Amazon Transcribe is now supported in the AWS GovCloud (US-West) Region</td>
<td>May 1, 2019</td>
</tr>
<tr>
<td>AWS Resource Access Manager</td>
<td>AWS Resource Access Manager is now supported in the AWS GovCloud (US-West) Region</td>
<td>April 25, 2019</td>
</tr>
<tr>
<td>AWS Organizations</td>
<td>AWS Organizations is now supported in the AWS GovCloud (US-West) Region.</td>
<td>April 18, 2019</td>
</tr>
<tr>
<td>AWS CodeCommit</td>
<td>AWS CodeCommit is now supported in the AWS GovCloud (US-West) Region.</td>
<td>April 17, 2019</td>
</tr>
<tr>
<td>AWS Service Catalog</td>
<td>AWS Service Catalog is now supported in the AWS GovCloud (US-West) Region.</td>
<td>March 20, 2019</td>
</tr>
<tr>
<td>AWS WAF</td>
<td>AWS WAF is now supported in the AWS GovCloud (US-West) Region. See AWS WAF (p. 203).</td>
<td>March 13, 2019</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date Changed</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Amazon Comprehend</td>
<td>Amazon Comprehend is now supported in the AWS GovCloud (US-West) Region.</td>
<td>March 13, 2019</td>
</tr>
<tr>
<td>AWS Glue</td>
<td>AWS Glue is now supported in the AWS GovCloud (US-West) Region. See AWS Glue  (p. 143).</td>
<td>February 6, 2019</td>
</tr>
<tr>
<td>Amazon Athena</td>
<td>Amazon Athena is now supported in the AWS GovCloud (US-West) Region.</td>
<td>February 6, 2019</td>
</tr>
<tr>
<td>Amazon WorkSpaces</td>
<td>Amazon WorkSpaces is now supported in the AWS GovCloud (US-West) Region. See Amazon WorkSpaces  (p. 204).</td>
<td>January 16, 2019</td>
</tr>
<tr>
<td>Amazon Kinesis Data Firehose</td>
<td>Amazon Kinesis Data Firehose is now supported in the AWS GovCloud (US-West) Region. See Amazon Kinesis Data Firehose  (p. 152).</td>
<td>January 16, 2019</td>
</tr>
<tr>
<td>AWS Elemental MediaConvert</td>
<td>AWS Elemental MediaConvert is now supported in the AWS GovCloud (US-West) Region. See AWS Elemental MediaConvert (p. 160).</td>
<td>December 19, 2018</td>
</tr>
<tr>
<td>Amazon Elastic File System</td>
<td>Amazon Elastic File System is now supported in the AWS GovCloud (US-West) Region. See Amazon Elastic File System (p. 134).</td>
<td>December 12, 2018</td>
</tr>
<tr>
<td>AWS GovCloud (US-East) Region</td>
<td>The AWS GovCloud (US-East) Region was launched. For more information about AWS GovCloud (US-East), see AWS GovCloud (US-East) User Guide.</td>
<td>November 12, 2018</td>
</tr>
<tr>
<td>AWS Directory Service</td>
<td>AWS Directory Service is now supported in the AWS GovCloud (US-West) Region. See AWS Directory Service  (p. 121).</td>
<td>October 24, 2018</td>
</tr>
<tr>
<td>Amazon SageMaker</td>
<td>Amazon SageMaker is now supported in the AWS GovCloud (US-West) Region. See Amazon SageMaker  (p. 178).</td>
<td>September 27, 2018</td>
</tr>
<tr>
<td>AWS Auto Scaling</td>
<td>AWS Auto Scaling(scaling plans) is now supported in the AWS GovCloud (US-West) Region and AWS GovCloud (US-East) Regions. See AWS Auto Scaling  (p. 91). As part of this update, the Application Auto Scaling service has its own separate page. See Application Auto Scaling  (p. 92).</td>
<td>September 4, 2018</td>
</tr>
<tr>
<td>AWS IoT Device Management</td>
<td>AWS IoT Device Management is now supported in the AWS GovCloud (US-West) Region. See AWS IoT Device Management (p. 149).</td>
<td>August 15, 2018</td>
</tr>
<tr>
<td>AWS IoT Core</td>
<td>AWS IoT Core is now supported in the AWS GovCloud (US-West) Region. See AWS IoT Core  (p. 147).</td>
<td>August 15, 2018</td>
</tr>
<tr>
<td>Amazon GuardDuty</td>
<td>Amazon GuardDuty is now supported in the AWS GovCloud (US-West) Region. See Amazon GuardDuty (p. 143).</td>
<td>July 25, 2018</td>
</tr>
<tr>
<td>AWS Step Functions</td>
<td>AWS Step Functions is now supported in the AWS GovCloud (US-West) Region. See AWS Step Functions  (p. 188).</td>
<td>June 28, 2018</td>
</tr>
<tr>
<td>AWS Deep Learning AMIs</td>
<td>AWS Deep Learning AMIs are now supported in the AWS GovCloud (US-West) Region. See AWS Deep Learning AMIs (p. 124).</td>
<td>June 21, 2018</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date Changed</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Amazon Translate</td>
<td>Amazon Translate is now supported in the AWS GovCloud (US-West) Region. See Amazon Translate (p. 194).</td>
<td>June 20, 2018</td>
</tr>
<tr>
<td>Amazon Aurora MySQL and Aurora PostgreSQL</td>
<td>Amazon Aurora MySQL is now supported in the AWS GovCloud (US-West) Region. See Amazon Aurora with MySQL and PostgreSQL compatibility (p. 89).</td>
<td>June 14, 2018</td>
</tr>
<tr>
<td>Amazon Inspector</td>
<td>Amazon Inspector is now supported in the AWS GovCloud (US-West) Region. See Amazon Inspector (p. 147).</td>
<td>June 13, 2018</td>
</tr>
<tr>
<td>AWS CloudHSM Classic</td>
<td>AWS CloudHSM Classic is now supported in the AWS GovCloud (US-West) Region. See AWS CloudHSM Classic (p. 101).</td>
<td>April 19, 2018</td>
</tr>
<tr>
<td>AWS CloudHSM</td>
<td>AWS CloudHSM is now supported in the AWS GovCloud (US-West) Region. See AWS CloudHSM (p. 101).</td>
<td>April 19, 2018</td>
</tr>
<tr>
<td>AWS Storage Gateway</td>
<td>AWS Storage Gateway is now supported in the AWS GovCloud (US-West) Region. See AWS Storage Gateway (p. 189).</td>
<td>March 28, 2018</td>
</tr>
<tr>
<td>Amazon Polly</td>
<td>Amazon Polly is now supported in the AWS GovCloud (US-West) Region. See Amazon Polly (p. 168).</td>
<td>February 28, 2018</td>
</tr>
<tr>
<td>Amazon Elasticsearch Service</td>
<td>Amazon Elasticsearch Service is now supported in the AWS GovCloud (US-West) Region. See Amazon Elasticsearch Service (p. 136).</td>
<td>February 15, 2018</td>
</tr>
<tr>
<td>Amazon Elastic Container Registry</td>
<td>Amazon Elastic Container Registry is now supported in the AWS GovCloud (US-West) Region. See Amazon ECR (p. 133).</td>
<td>January 24, 2018</td>
</tr>
<tr>
<td>Amazon Elastic Container Service</td>
<td>Amazon Elastic Container Service is now supported in the AWS GovCloud (US-West) Region. See Amazon ECS (p. 134).</td>
<td>January 24, 2018</td>
</tr>
<tr>
<td>Amazon API Gateway</td>
<td>Amazon API Gateway is now supported in the AWS GovCloud (US-West) Region. See Amazon API Gateway (p. 85).</td>
<td>August 1, 2017</td>
</tr>
<tr>
<td>AWS Marketplace</td>
<td>AWS Marketplace is now supported in the AWS GovCloud (US-West) Region. See AWS Marketplace (p. 158).</td>
<td>July 31, 2017</td>
</tr>
<tr>
<td>Amazon Rekognition</td>
<td>Amazon Rekognition is now supported in the AWS GovCloud (US-West) Region. See Amazon Rekognition (p. 175).</td>
<td>June 12, 2017</td>
</tr>
<tr>
<td>AWS Server Migration Service</td>
<td>AWS Server Migration Service is now supported in the AWS GovCloud (US-West) Region. See AWS Server Migration Service (p. 185).</td>
<td>June 1, 2017</td>
</tr>
<tr>
<td>AWS Certificate Manager</td>
<td>AWS Certificate Manager is now supported in the AWS GovCloud (US-West) Region. See AWS Certificate Manager (p. 96).</td>
<td>June 1, 2017</td>
</tr>
<tr>
<td>Amazon EC2 Systems Manager</td>
<td>Amazon EC2 Systems Manager is now supported in the AWS GovCloud (US-West) Region. See AWS Systems Manager (p. 191).</td>
<td>May 23, 2017</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date Changed</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>AWS Lambda</td>
<td>AWS Lambda is now supported in the AWS GovCloud (US-West) Region. See AWS Lambda (p. 156).</td>
<td>May 18, 2017</td>
</tr>
<tr>
<td>Amazon CloudWatch Events</td>
<td>Amazon CloudWatch Events is now supported in the AWS GovCloud (US-West) Region. See Amazon CloudWatch Events (p. 109).</td>
<td>May 18, 2017</td>
</tr>
<tr>
<td>AWS CodeDeploy</td>
<td>AWS CodeDeploy is now supported in the AWS GovCloud (US-West) Region. See AWS CodeDeploy (p. 112).</td>
<td>May 11, 2017</td>
</tr>
<tr>
<td>Amazon Kinesis Data Streams</td>
<td>Amazon Kinesis Data Streams is now supported in the AWS GovCloud (US-West) Region. See Amazon Kinesis Data Streams (p. 153).</td>
<td>December 21, 2016</td>
</tr>
<tr>
<td>Amazon EC2</td>
<td>Updated public IP range. See Amazon EC2 (p. 129).</td>
<td>June 21, 2016</td>
</tr>
<tr>
<td>AWS Config</td>
<td>AWS Config is now available in the AWS GovCloud (US-West) Region. See AWS Config (p. 119).</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-West) Region. See AWS Snow Family (p. 184).</td>
<td>April 19, 2016</td>
</tr>
<tr>
<td>AWS CloudTrail</td>
<td>Updated information about creating multiple trails. See AWS CloudTrail (p. 102).</td>
<td>March 24, 2016</td>
</tr>
<tr>
<td>Importing VMs</td>
<td>Updated information about importing virtual machines into the AWS GovCloud (US-West) Region. See Importing Virtual Machines into AWS GovCloud (US) Regions (p. 131).</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. 5).</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 S3 (p. 177).</td>
<td>December 18, 2015</td>
</tr>
<tr>
<td>Amazon EBS</td>
<td>Updated text about copying snapshots. See Amazon EBS (p. 128).</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-West) Region. See AWS CloudTrail (p. 102).</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. 120).</td>
<td>October 28, 2015</td>
</tr>
<tr>
<td>S3 Glacier</td>
<td>Updated ITAR-regulated data for S3 Glacier. See Amazon S3 Glacier (p. 142).</td>
<td>October 28, 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>VPC Flow Logs</td>
<td>VPC Flow Logs are now supported in AWS GovCloud (US). See Amazon VPC (p. 201).</td>
<td>October 27, 2015</td>
</tr>
<tr>
<td>CloudWatch Logs</td>
<td>CloudWatch Logs are now supported in AWS GovCloud (US). See Amazon CloudWatch (p. 108).</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) or Resources (p. 19).</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. 102).</td>
<td>August 25, 2015</td>
</tr>
<tr>
<td>Penetration testing</td>
<td>Updated instructions for submitting a request. See Penetration Testing (p. 81).</td>
<td>August 5, 2015</td>
</tr>
<tr>
<td>IAM</td>
<td>Added information about SSH public keys. See AWS Identity and Access Management (p. 145).</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 (p. 145) and Importing Virtual Machines into AWS GovCloud (US) Regions (p. 131).</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-West) Region. See AWS CloudTrail (p. 102).</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-West) Region. See AWS Key Management Service (p. 154).</td>
<td>May 7, 2015</td>
</tr>
<tr>
<td>Encryption</td>
<td>Encryption is now available for Amazon EBS (p. 128), Amazon EMR (p. 139), and Amazon S3 (p. 177).</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. 120).</td>
<td>April 3, 2015</td>
</tr>
<tr>
<td>Amazon S3</td>
<td>Added info about cross-region replication. See Amazon S3 (p. 177).</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. 195).</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. 195).</td>
<td>March 11, 2015</td>
</tr>
<tr>
<td>VM Export</td>
<td>Updated information about using VM Export. See Amazon EC2 (p. 129).</td>
<td>March 9, 2015</td>
</tr>
<tr>
<td>VM Import</td>
<td>Updated information about using VM Import. See Amazon EC2 (p. 129).</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-West) Region. See Importing Virtual Machines into AWS GovCloud (US) Regions (p. 131).</td>
<td>February 11, 2015</td>
</tr>
<tr>
<td>Amazon ElastiCache</td>
<td>ElastiCache is now available in the AWS GovCloud (US-West) Region. See Amazon ElastiCache (p. 138).</td>
<td>January 29, 2015</td>
</tr>
<tr>
<td>AWS Trusted Advisor</td>
<td>Updated information about Trusted Advisor. See AWS Trusted Advisor (p. 195).</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-West) Region. See AWS CloudTrail (p. 102).</td>
<td>January 22, 2015</td>
</tr>
<tr>
<td>AWS Trusted Advisor</td>
<td>Trusted Advisor is now available in the AWS GovCloud (US-West) Region. See AWS Trusted Advisor (p. 195).</td>
<td>January 20, 2015</td>
</tr>
<tr>
<td>Amazon S3 Glacier</td>
<td>S3 Glacier is now available in the AWS GovCloud (US-West) Region. See Amazon S3 Glacier (p. 142).</td>
<td>December 30, 2014</td>
</tr>
<tr>
<td>AWS CloudTrail</td>
<td>CloudTrail is now available in the AWS GovCloud (US-West) Region. See AWS CloudTrail (p. 102).</td>
<td>December 16, 2014</td>
</tr>
<tr>
<td>Importing VMs</td>
<td>Updated information about importing virtual machines into the AWS GovCloud (US-West) Region. See Importing Virtual Machines into AWS GovCloud (US) Regions (p. 131) and Amazon EC2 (p. 129).</td>
<td>December 15, 2014</td>
</tr>
<tr>
<td>Amazon Redshift</td>
<td>Amazon Redshift is now available in the AWS GovCloud (US-West) Region. See Amazon Redshift (p. 173).</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 EC2 (p. 129).</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 (p. 145).</td>
<td>July 25, 2014</td>
</tr>
<tr>
<td>Amazon EC2</td>
<td>Updates to differences in Amazon EC2 AMI tools. See Amazon EC2 (p. 129).</td>
<td>July 15, 2014</td>
</tr>
<tr>
<td>Amazon SNS</td>
<td>Updates to Amazon SNS ITAR boundary. See Amazon SNS (p. 186).</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-West) Region. For information about using Amazon RDS in the AWS GovCloud (US-West) Region, see Amazon RDS (p. 171).</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) as a Solution Provider reselling in AWS GovCloud (US) (p. 11).</td>
<td>April 7, 2014</td>
</tr>
<tr>
<td>Provisioned IOPS</td>
<td>Provisioned IOPS is supported in the AWS GovCloud (US-West) Region. For information about using Amazon EC2 and Amazon EBS in the AWS GovCloud (US-West) Region, see Amazon EC2 (p. 129) and Amazon EBS (p. 128).</td>
<td>April 1, 2014</td>
</tr>
<tr>
<td>Amazon EC2</td>
<td>Updates to Amazon EC2 and troubleshooting. For information, see Amazon EC2 (p. 129) and Troubleshooting (p. 206).</td>
<td>March 19, 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-West) Region. See Importing Virtual Machines into AWS GovCloud (US) Regions (p. 131).</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-West) Region. For information about using Amazon EC2 in the AWS GovCloud (US-West) Region, see Amazon EC2 (p. 129).</td>
<td>March 4, 2014</td>
</tr>
<tr>
<td>SUSE Linux</td>
<td>SUSE Linux is now available in the AWS GovCloud (US-West) Region. For information about using Amazon EC2 in the AWS GovCloud (US-West) Region, see Amazon EC2 (p. 129).</td>
<td>January 17, 2014</td>
</tr>
<tr>
<td>Resources</td>
<td>Updated list of additional resources. See Related Resources (p. 207).</td>
<td>January 8, 2014</td>
</tr>
<tr>
<td></td>
<td>Added note about Amazon SNS Mobile Push Notifications. See Amazon SNS (p. 186).</td>
<td></td>
</tr>
<tr>
<td>DynamoDB</td>
<td>The DynamoDB console is available and no longer in beta in the AWS GovCloud (US-West) Region. See Amazon DynamoDB (p. 126).</td>
<td>December 30, 2013</td>
</tr>
<tr>
<td>Amazon EC2</td>
<td>Added fix for instructions to create a key pair. See Amazon EC2 (p. 129).</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-West) Region. See Amazon EMR (p. 139).</td>
<td>November 12, 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>Change</td>
<td>Description</td>
<td>Date Changed</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>AWS CloudFormation</td>
<td>The AWS CloudFormation console is now available in the AWS GovCloud (US-West) Region. See AWS CloudFormation (p. 98).</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) Regions (p. 79).</td>
<td>October 18, 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. 21).</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 GovCloud (US) Regions (p. 32).</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) or Resources (p. 19) and Setting Up Amazon Route 53 with Your AWS GovCloud (US) Resources (p. 20).</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 EC2 (p. 129).</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.