User Guide

AWS GovCloud (US)

AWS GovCloud (US): User Guide

Table of Contents

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.

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) consist of isolated AWS Regions designed to allow U.S. government agencies and customers move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements, including Federal Risk and Authorization Management Program (FedRAMP) High, Department of Defense Security Requirements Guide (DoD SRG) Impact Levels 4 and 5, and Criminal Justice Information Services (CJIS). To assist customers in managing their obligations under U.S. export control regimes such as the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR), AWS GovCloud (US) Regions are logically and physically administered exclusively by AWS personnel that are U.S. citizens only. In this guide, the term AWS GovCloud (US) Regions refer to both AWS GovCloud (US-West) and AWS GovCloud (US-East) Regions.

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 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.
- For more information about meeting US Government compliance requirements please, see AWSAWS GovCloud (US).
- For a list of AWS or AWS GovCloud (US)–related resources, see Related Resources.

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 Authorization Management Program (FedRAMP) High, Department of Defense Security Requirements Guide (DoD SRG) Impact Level 5, and Criminal Justice Services (CJIS). To assist customers in managing their obligations under U.S. export control regimes such as the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR), AWS GovCloud (US) are logically and physically administered exclusively by U.S. citizens

- AWS GovCloud (US) uses FIPS 140-2 approved cryptographic modules for all AWS service API endpoints, unless otherwise indicated in the Service Endpoints section.
- 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.
- 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. The standard AWS practice of using two AWS Regions in a partition remains. In this case, using both AWS AWS GovCloud (US) Regions for architecture is preferred. 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.

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).

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 detailed information about each service in the AWS GovCloud (US) Regions, see Using AWS GovCloud (US) Regions.

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

AWS GovCloud (US) users can use the same FIDO security tokens or virtual authenticator apps as commercial users. However, if instead opting for a TOTP hardware token for MFA, AWS GovCloud (US) users need to use a special device. This is due to the separate authentication stack. For more information, see the list of AWS GovCloud (US)-supported MFA devices on the Multi-Factor Authentication page.

Customer can validate AWS GovCloud (US) account ID from standard Region account by completing the following steps:

1. Login to standard Region account.
2. Click on "Account ID Name" in top right-hand corner of screen.
3. Click on "Account".
4. Scroll down to the "Sign up for AWS AWS GovCloud (US)" button.
5. Click on the "Sign up for AWS AWS GovCloud (US)" button.

A note will be displayed stating the following:

```
Our records show that you already have a GovCloud (US) account. If you lost the
 password please contact our customer support team. Thank you.
Your account is ready to use.
GovCloud (US) Account ID: XXXXXXXXXXXX (this is the customer's GovCloud account ID)
```

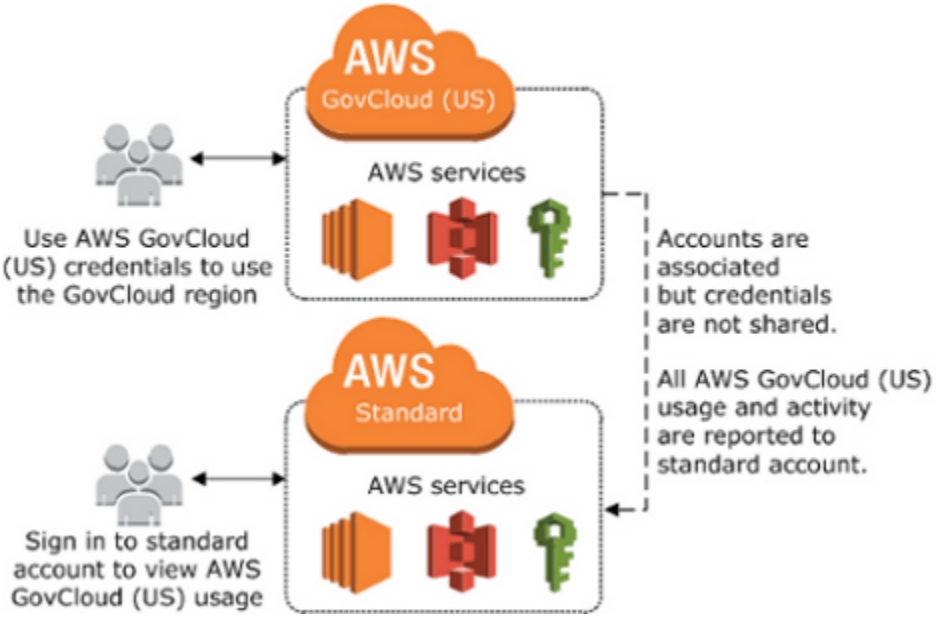
AWS GovCloud (US) Billing and Payment

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:



AWS GovCloud (US) account relationship to standard AWS account

AWS Cost and Usage Reports

The AWS Cost and Usage Reports (AWS CUR) contains a comprehensive set of cost and usage data. You can use Cost and Usage Reports to publish your AWS billing reports to an Amazon Simple Storage Service (Amazon S3) bucket that you own. The CURs contains AWS cost and usage data for both commercial and GovCloud partitions.

Access cost and usage reports in GovCloud partition

Currently, billing information for GovCloud accounts and regions are only available in the commercial partition. For organizations that require users to exclusively use AWS GovCloud (US) regions, you can copy CURs stored in an Amazon S3 bucket(s) in commercial region(s) into an AWS GovCloud (US) Amazon S3 bucket. See Move data in and out of AWS GovCloud (US) with Amazon S3.

Savings plans

Savings plans for GovCloud account and regions need to be purchased in the Standard commercial account. These plans purchased in the Standard account apply to usage in GovCloud regions. See How Amazon Elastic Compute Cloud Differs for AWS GovCloud (US). In addition, GovCloud accounts inherit discount sharing configuration from their associated commercial accounts. See Activating shared Reserved Instances and Savings Plans discounts.

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

AWS GovCloud (US) Sign Up

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).

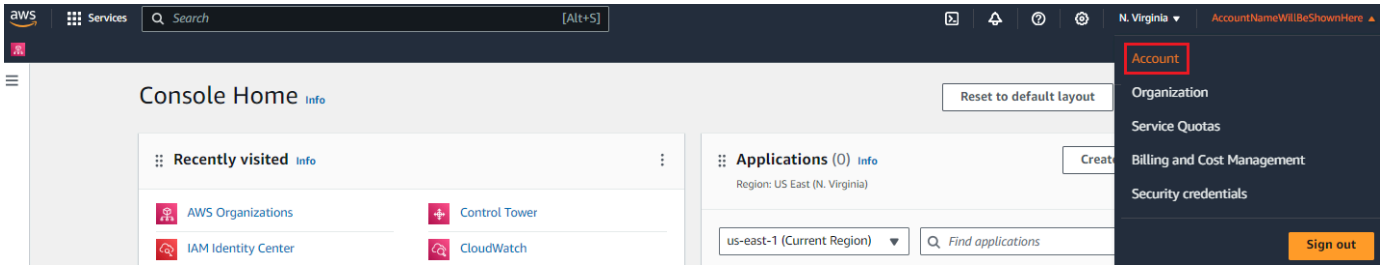
- The account holder must be a U.S. entity incorporated to do business in the United States and is based on U.S. soil.
- The account holder must be a U.S. Person defined as a U.S. Citizen or active Green Card holder.
- The account holder must be able to handle International Traffic and Arms Regulation (ITAR) export controlled data.
- In addition, AWS uses automated controls to prevent the creation of fraudulent accounts. This may cause new account creations to be denied. If you believe your request was denied in error, please contact AWS Customer Support for additional assistance in account creation.

There are two options for creating an AWS GovCloud (US) account as a direct consumer.

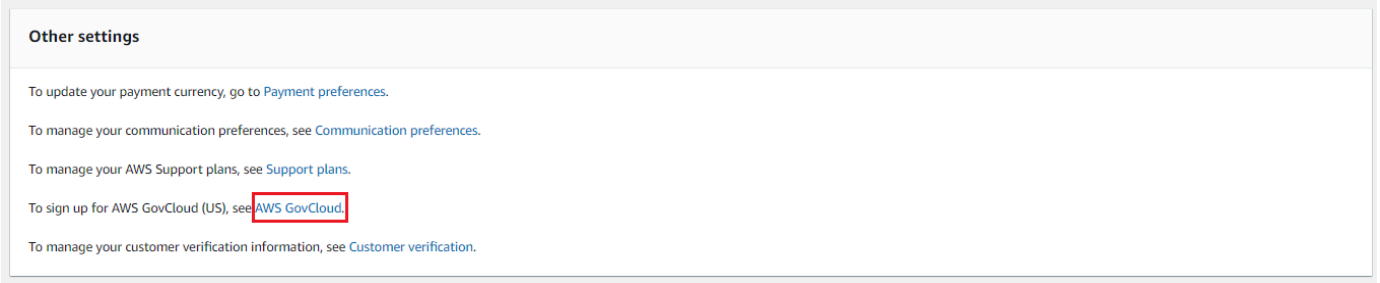
Option 1: Creating an AWS GovCloud (US) from a standalone AWS account

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 **Account** page at the top right of the AWS Management Console.



4. On the **Account** page, scroll down to the **Other settings** section. Choose the **AWS GovCloud** link. If you do not see this link, ensure you logged in with the root credentials otherwise, create a support ticket.



5. This will navigate you to the AWS GovCloud (US) Sign Up Portal where you are asked to accept the AWS GovCloud (US) legal agreement and provide additional information, so we can verify your eligibility for an AWS GovCloud (US) account.

Option 2: 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 organization within the AWS US Standard Regions to manage accounts in those Regions. You will need to create a separate AWS organization in AWS GovCloud (US) to manage accounts in the AWS GovCloud (US) partition.

1. Follow the steps above to create a standalone AWS GovCloud (US) account that is mapped to your AWS Organizations management account.
2. Call the AWS Organizations CreateGovCloudAccount API from the AWS Standard account that is the management account of your Organization. This will create two accounts, one in the AWS Standard Region Organization and an associated AWS GovCloud (US) Account. This API will create roles for accessing the new AWS Standard account from the Standard Organization and will create roles in the AWS GovCloud (US) account that is mapped to your management account for accessing the new AWS GovCloud (US) account.
3. The API call will return success but is executed asynchronously and may take a few minutes to complete. For more information, visit the AWS Organizations documentation.

   In order to get the account numbers being created, please run the describe-create-account-status command.

   Example

   describe-create-account-status --create-account-request-id [value].

   aws organizations describe-create-account-status --create-account-request-id car-examplecreateaccountrequestid111

   See here for more information.
4. Once complete, you can log in to your AWS GovCloud (US) management account and switch role into the new AWS GovCloud (US) account.
5. After creating the standalone account in the AWS GovCloud (US), you can invite it to an organization in the AWS GovCloud (US) only.

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.

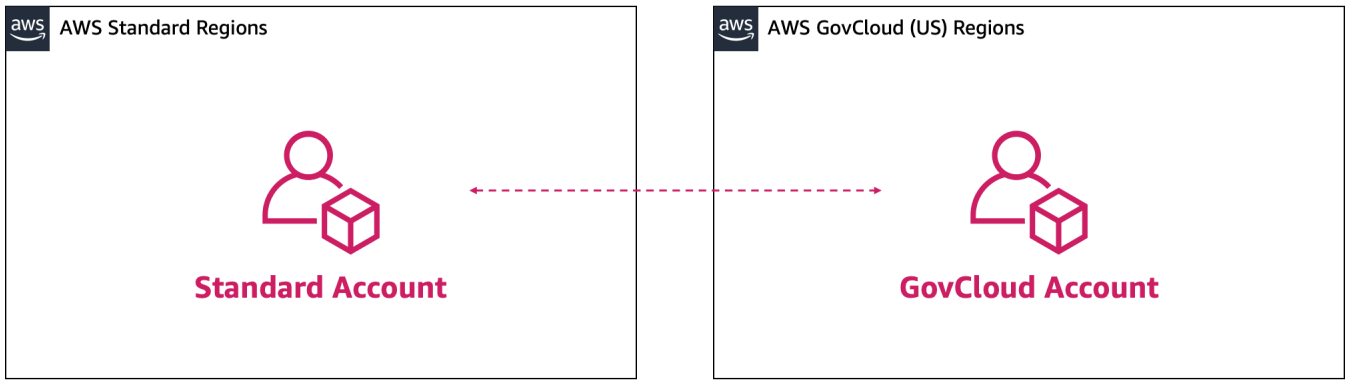
Close Account

For instructions on how to close an AWS GovCloud (US) account, see the section called “Closing an AWS GovCloud (US) account”.

AWS Standard Account Linking

AWS GovCloud (US) accounts are associated 1:1 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

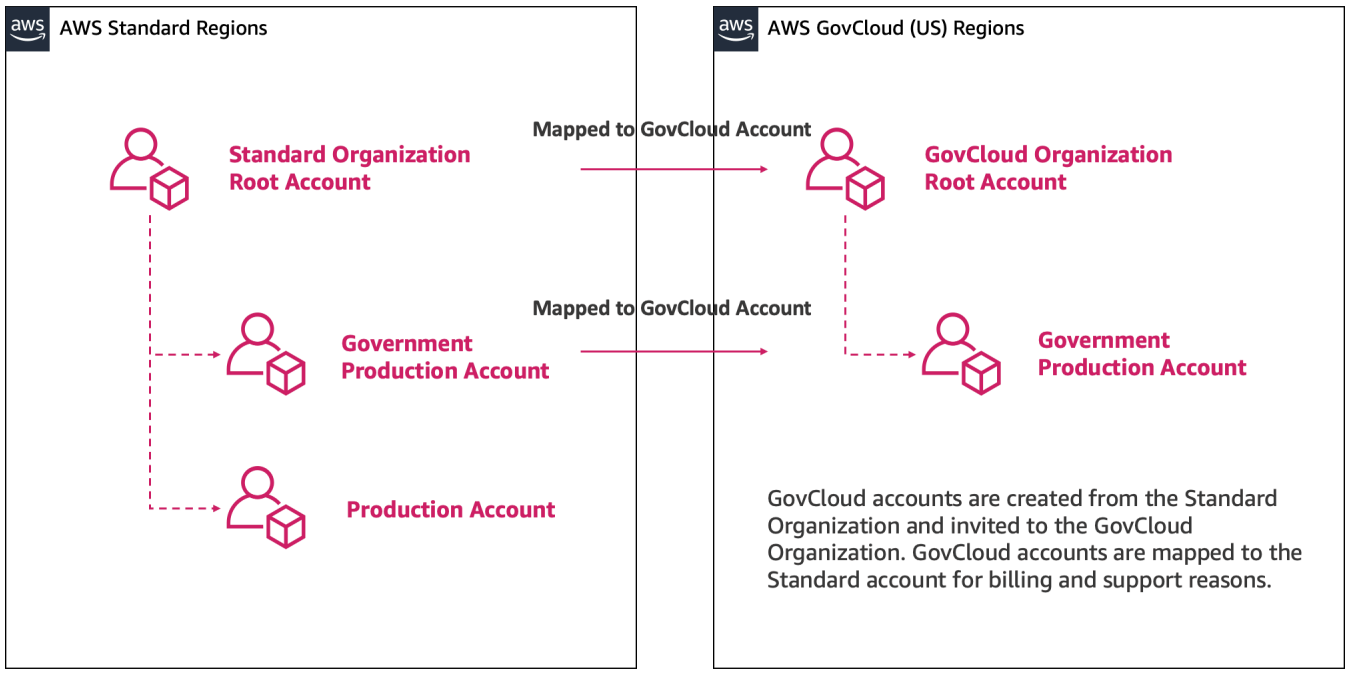
> **Important**
>
> We recommend creating a new AWS account that will only be used for AWS GovCloud (US) sign up and billing (i.e. do not deploy any AWS workloads into AWS standard account). A dedicated AWS account for the new AWS GovCloud (US) account will enable you to transfer the AWS GovCloud (US) 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. Your AWS Organization in your standard AWS account is separate from the AWS Organizations in your AWS GovCloud (US) should you choose to create one, even though the accounts are linked. You must manage each separately. Only the standard AWS account will be managed by the existing Organization.

You can create a new AWS Organizations within the AWS GovCloud (US) partition by creating a set of new accounts, creating a new AWS Organizations 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 Organization, one in each partition.



Signing in to AWS GovCloud (US)

The AWS Management Console provides a web-based user interface that you can use to create and manage your AWS resources. For example, you can start and stop Amazon EC2 instances, create Amazon DynamoDB tables, create Amazon S3 buckets, and so on.

Before you can use the AWS Management Console, you must sign in to your AWS GovCloud (US) account. There are two different types of users in AWS GovCloud (US). You are either the account owner (root user) or you are an IAM user. The root user is created when the AWS GovCloud (US) account is created. IAM users are created by the root user or an IAM administrator within the AWS GovCloud (US) account.

If you do not remember your credentials or have trouble signing in using your credentials, see Troubleshooting AWS GovCloud (US) sign-in or account issues.

Topics

Sign in as the root user

The AWS Management Console for AWS GovCloud (US) only supports signing in as an IAM user. Signing in to the AWS Management Console for AWS GovCloud (US) as the AWS GovCloud (US) account root user or as the associated standard AWS account root user is not supported.

For more information, see AWS Identity and Access Management.

For more information about the AWS GovCloud (US) account root user, see AWS GovCloud (US) account root user .

Sign in as an IAM user

Before you sign in to an AWS GovCloud (US) account as an IAM user, be sure that you have the following required information. If you do not have this information, contact the administrator for the AWS GovCloud (US) account.

Requirements

- One of the following:
  - The account alias.
  - The 12-digit AWS GovCloud (US) account ID.
- The user name for your IAM user.
- The password for your IAM user.

If you are a root user or IAM administrator and need to provide the AWS GovCloud (US) account ID or AWS GovCloud (US) account alias to an IAM user, see Your AWS GovCloud (US) account ID and its alias.

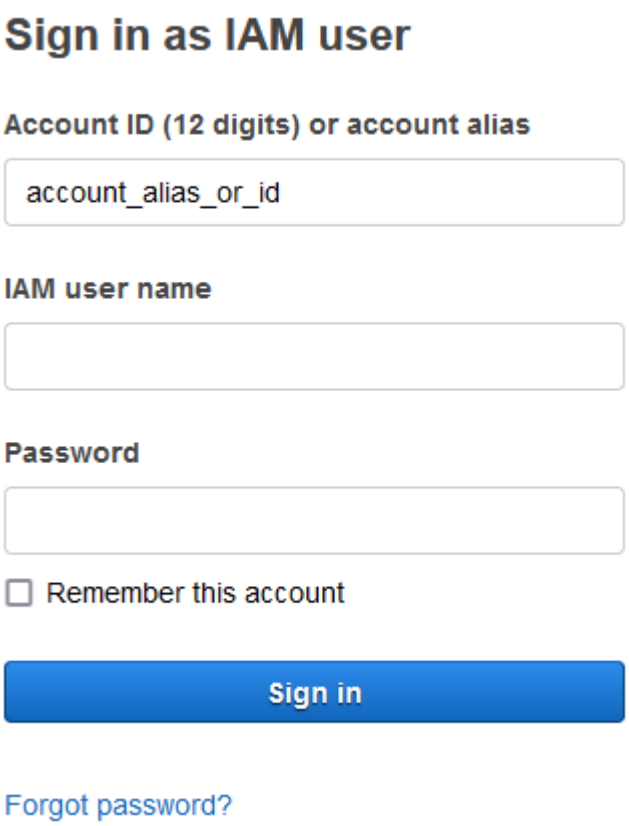
If you are an IAM user, you can log in using either a sign-in URL or the main sign-in page.

To sign in to an AWS GovCloud (US) account as an IAM user using an IAM user sign-in URL

1. Open a browser and enter the following sign-in URL, replacing account_alias_or_id with the account alias or account ID provided by your administrator.

   ```
   https://account_alias_or_id.signin.amazonaws-us-gov.com
   ```

2. Enter your IAM user name and password and choose **Sign in**.



To sign in to an AWS GovCloud (US) account as an IAM user using the main sign-in page

1. Open https://console.amazonaws-us-gov.com.

If you have signed in previously using this browser, your browser might remember the account alias or account ID for the AWS GovCloud (US) account.

2. Enter account alias or account ID, IAM user name and password and choose **Sign in**.

Your AWS GovCloud (US) account ID and its alias

To sign in to an AWS GovCloud (US) account as an IAM user, you must have an account alias or an account ID for the AWS GovCloud (US) account. If you are signed in to the AWS Management Console or have configured the AWS CLI or an AWS SDK with your account credentials, you can find the account alias or account ID for the AWS GovCloud (US) account. If you cannot sign in, ask your administrator for the information that you need to sign in.

> **Note**
>
> Account aliases are not secrets, and they will appear in your public-facing sign-in page URL. Do not include any sensitive information in your account alias.

Topics

Finding your AWS GovCloud (US) account ID

You can find the account ID for your AWS GovCloud (US) account using the following methods.

> **Note**
>
> AWS Support can't help you recover this information.

Finding your AWS GovCloud (US) account ID using the AWS Management Console for AWS GovCloud (US)

You can retrieve your AWS GovCloud (US) account ID by Signing in to AWS GovCloud (US). In the navigation bar, choose **Support**, and then **Support Center**. Your currently signed-in 12-digit account number (ID) appears in the **Support Center** navigation pane.

Finding your AWS GovCloud (US) account ID using the standard AWS Management Console

You can retrieve your AWS GovCloud (US) account ID by signing in to the standard AWS Management Console as the root user of the associated standard AWS account. In the navigation bar, choose your account name on the top right of the window, and then choose **Account**. On the **Account Settings** page, under **AWS GovCloud (US)**, choose 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 ID.

Finding your AWS GovCloud (US) account ID using the AWS CLI

With AWS GovCloud (US) account credentials use the following command to view your user ID, account ID, and your user ARN:

- aws sts get-caller-identity

If your AWS GovCloud (US) account was created using the CreateGovCloudAccount API, use the following command view your AWS GovCloud (US) account ID and its associated standard AWS account ID. This call must be made from the standard AWS Organizations management account or by a member account that is a delegated administrator for an AWS service.

- aws organizations list-create-account-status

Finding your AWS GovCloud (US) account ID using the API

With AWS GovCloud (US) account credentials, use the following API to view your user ID, account ID, and your user ARN:

- GetCallerIdentity

If your AWS GovCloud (US) account was created using the CreateGovCloudAccount API, use the following command view your AWS GovCloud (US) account ID and its associated standard AWS account ID. This call must be made from the standard AWS Organizations management account or by a member account that is a delegated administrator for an AWS service.

- ListCreateAccountStatus

Finding your associated standard AWS account ID

> **Note**
>
> AWS Support can't help you recover this information.

Finding your associated standard AWS account ID using the AWS Management Console for AWS GovCloud (US)

You can retrieve your associated standard AWS account ID by signing into your AWS GovCloud (US) account.

In the navigation bar, choose **Support**, and then **Support Center**. In the **Support Center** navigation pane, choose **Your support cases** and open the most recently created support case by choosing its **Case ID** or **Subject**. In the **Case details**, look for the email address listed in the **Opened by** field. If your account email address has not changed since opening the case, this will be your account email

address. Sign in as the root user of your standard AWS account using this email and follow Finding your AWS account ID in the *AWS Identity and Access Management User Guide*guide.

> **Note**
>
> If you have never opened a support case or believe the email address has since changed, create a support case for account and billing and resolve it immediately. Review the case's **Open by** field to see the associated account email.

Finding your associated standard AWS account ID using the AWS CLI

If your AWS GovCloud (US) account was created using CreateGovCloudAccount API, use the following command view your AWS GovCloud (US) account ID and its associated standard AWS account ID. This call must be made from the standard AWS Organizations management account or by a member account that is a delegated administrator for an AWS service.

- aws organizations list-create-account-status

Finding your associated standard AWS account ID using the API

If your AWS GovCloud (US) account was created using the CreateGovCloudAccount API, use the following command view your AWS GovCloud (US) account ID and its associated standard AWS account ID. This call must be made from the standard AWS Organizations management account or by a member account that is a delegated administrator for an AWS service.

- ListCreateAccountStatus

About account aliases

If you want the URL for your sign-in page to contain your company name (or other friendly identifier) instead of your AWS GovCloud (US) account ID, you can create an account alias. This section provides information about AWS account aliases and lists the API operations that you use to create an alias.

Your sign-in page URL has the following format, by default.

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

If you create an AWS account alias for your AWS GovCloud (US) ID, your sign-in page URL looks like the following example.

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

The original URL containing your AWS GovCloud (US) ID remains active and can be used after you create your AWS account alias.

> **Tip**
>
> To create a bookmark for your account sign-in page in your web browser, you should manually type the sign-in URL in the bookmark entry. Don't use your web browser's "bookmark this page" feature.

Creating, deleting, and listing an AWS account alias

You can use the AWS Management Console, the IAM API, or the command line interface to create or delete your AWS GovCloud (US) account alias.

Considerations

- Your AWS GovCloud (US) account can have only one alias. If you create a new alias for your AWS GovCloud (US) account, the new alias overwrites the previous alias, and the URL containing the previous alias stops working.
- The account alias must be unique across all Amazon Web Services products. It must contain only digits, lowercase letters, and hyphens. For more information on limitations on AWS account entities, see IAM and AWS STS quotas, name requirements, and character limits.
- Changes to your AWS GovCloud (US) account alias or the associated standard AWS account alias will not overwrite the other alias. They can each be customized without interference of the other. See Creating, deleting, and listing an AWS account alias in the *AWS Identity and Access Management User Guide*to learn more about customizing the associated standard AWS account alias.

Creating, editing, and deleting aliases (console)

You can create, edit, and delete an account alias from the AWS Management Console for AWS GovCloud (US).

To create, edit, or remove an account alias (console)

1. Sign in to the AWS Management Console for AWS GovCloud (US) and open the IAM console at https://console.amazonaws-us-gov.com/iam/.
2. In the navigation pane, choose **Dashboard**.
3. In the **AWS account** section, find **Account Alias**, and choose **Create**. If an alias already exists, then choose **Edit**.
4. Type the name you want to use for your alias, then choose **Save changes**.
5. To remove the alias, next to **Account Alias** choose **Delete**, and then choose **Delete**. The sign-in URL reverts to using your AWS account ID.

Creating, deleting, and listing aliases (AWS CLI)

> **Note**
>
> You must use AWS GovCloud (US) credentials.

To create an alias for your AWS Management Console for AWS GovCloud (US) sign-in page URL, run the following command:

- aws iam create-account-alias

To delete an AWS account ID alias, run the following command:

- aws iam delete-account-alias

To display your AWS account ID alias, run the following command:

- aws iam list-account-aliases

Creating, deleting, and listing aliases (AWS API)

> **Note**
>
> You must use AWS GovCloud (US) credentials.

To create an alias for your AWS Management Console for AWS GovCloud (US) sign-in page URL, call the following operation:

- aws CreateAccountAlias

To delete an alias for your AWS Management Console for AWS GovCloud (US) sign-in page URL, call the following operation:

- aws DeleteAccountAlias

To display your AWS account ID alias, call the following operation:

- aws ListAccountAliases

Troubleshooting AWS GovCloud (US) sign-in or account issues

Use the information here to help you troubleshoot sign-in and other AWS GovCloud (US) account issues. For step-by-step directions to sign in to an AWS account, see Sign in as the root user

If you are having trouble signing in to your associated standard AWS account, see Troubleshooting sign-in issues in the *AWS Sign-In User Guide* instead.

> **Note**
>
> For security purposes, AWS doesn't have access to view, provide, or change your credentials.

Topics

- I need to change the credit card for my AWS GovCloud (US) account
- I need to report fraudulent AWS GovCloud (US) account activity
- I need to close my AWS GovCloud (US) account activity

My AWS GovCloud (US) credentials aren't working

When you can't sign in to the AWS Management Console for AWS GovCloud (US), try to remember how you previously accessed AWS.

If you don't remember signing in using a password at all

You might have previously accessed AWS without using AWS credentials. This is common for enterprise single sign-on through IAM Identity Center. Accessing AWS this way means that you use your corporate credentials to access AWS accounts or applications without entering your credentials.

- **AWS access portal** – If an administrator allows you to use credentials from outside AWS to access AWS, you need the URL for your portal. Check your email, browser favorites, or browser history for a URL that includes `awsapps.com/start` or `signin.aws/platform/login`.

  For example, your custom URL might include an ID or a domain such as `https://d-1234567890.awsapps.com/start`. If you can't find your portal link, contact your administrator. AWS Support can't help you recover this information.

If you remember signing in using a password

You might be on the wrong page. Try signing in on a different page:

- **Root user sign-in page** – Signing in to the AWS Management Console for AWS GovCloud (US) as the root user is not supported. To learn more about the root user in AWS GovCloud (US), see AWS GovCloud (US) account root user in the *AWS GovCloud (US) User Guide*.
- **IAM user sign-in page** – If you or someone else created an IAM user within a single AWS GovCloud (US) account, you must know that account ID or alias. Enter your account ID or alias, user name, and password in to the AWS Management Console for AWS GovCloud (US). To learn how to access the IAM user sign-in page, see Sign in as the root user. If you forgot your IAM user password, see I lost or forgot my AWS GovCloud (US) IAM user name or password for information on resetting your IAM user password. If you forgot your account number, search your email, browser favorites, or browser history for a URL that includes

`signin.amazonaws-us-gov.com/`. Your account ID or alias will precede this URL, such as `account_alias_or_id.signin.amazonaws-us-gov.com`. The account ID can also follow the `account=` or `account%3D` text in the URL. If you can't find your account ID or alias, see I need my AWS GovCloud (US) account ID or account alias .

- **AWS access portal** – If an administrator set up an AWS IAM Identity Center identity source for AWS, you must sign in using your user name and password. In this case, you need the URL for your portal. Check your email, secure password storage, browser favorites, or browser history for a URL that includes `start.us-gov-home.awsapps.com` or `s signin-fips.amazonaws-us-gov.com/platform/login`. For example, your custom URL might include an ID or a domain such as `https://start.us-gov-home.awsapps.com/directory/d-1234567890`. If you can't find your portal link, contact your administrator. AWS Support can't help you recover this information.

For more assistance on troubleshooting your sign-in issues, see What do I do if I'm having trouble signing in to or accessing my AWS account?

I need my AWS GovCloud (US) account ID or account alias

If you are an IAM user and you are not signed in, you must ask your administrator for the AWS account ID or AWS account alias. You need this information, plus your IAM user name and password, to sign in to an AWS account. To learn more about where to find your account ID and alias, see Your AWS GovCloud (US) account ID and its alias in the *AWS GovCloud (US) User Guide*.

> **Note**
>
> AWS Support can't help you recover this information.

I lost or forgot my AWS GovCloud (US) IAM user name or password

If you are an IAM user, your administrator provides your credentials. If you forget your password, you must ask your administrator to reset your password. To learn how an administrator can manage your password, see Managing passwords for IAM users.

If you are an administrator of the AWS GovCloud (US) account and have forgot your password to the AWS Management Console for AWS GovCloud (US), please contact another administrator in the account to assist with restoring your access. If there are no other users with administrative access to your account, you will need root credentials for your AWS GovCloud (US) account to restore

console access. To learn how to restore administrative console access with the root user, see AWS GovCloud (US) account root user in the *AWS GovCloud (US) User Guide*.

I lost or forgot the access keys for my AWS GovCloud (US) IAM user name

If you are an IAM user and you forget your access keys, you will need new access keys. If you have permission to create your own access keys, you can find instructions for creating a new one at Managing access keys (console). If you do not have the required permissions, you must ask your administrator to create new access keys. If you are still using your old keys, ask your administrator not to delete the old keys. To learn how an administrator can manage your access keys, see Managing access keys for IAM users.

You should follow the AWS best practice of periodically changing your password and AWS access keys. In AWS, you change access keys by rotating them. This means that you create a new one, configure your applications to use the new key, and then delete the old one. You are allowed to have two access key pairs active at the same time for just this reason. For more information, see Rotating access keys.

I lost or forgot the access keys for my AWS GovCloud (US) root user

If you forget your AWS GovCloud (US) account root access keys, you can request new access keys, see AWS GovCloud (US) account root user in the *AWS GovCloud (US) User Guide*.

I forgot the root user password for my standard AWS account

If you are a root user and you have lost or forgot the password for your associated standard AWS account, you can reset your password. You must know the email address used to create the associated standard AWS account and you must have access to the email account. For more information, see Resetting lost or forgotten passwords or access keys for AWS.

I don't know the email for my standard AWS account or AWS GovCloud (US) account

Your AWS GovCloud (US) account email address is the same as email address configured in its assocated standard AWS account. Changing the standard AWS account email will result in a change to the AWS GovCloud (US)) account email.

If you are not sure of the email address associated with your AWS GovCloud (US) account, sign in to your AWS GovCloud (US) account. In the navigation bar, choose **Support**, and then **Support Center**. In the **Support Center** navigation pane, choose **Your support cases** and open the most recently

created support case by choosing its **Case ID** or **Subject**. In the **Case details**, look for the email address listed in the **Opened by** field. If your account email address has not changed since opening the case, this will be your account email address.

> **Note**
>
> If you have never opened a support case or believe the email address has since changed, Create a support case for account and billing and resolve it immediately. Review this cases **Open by** field to see the associated account email.

If you can't sign in to your AWS GovCloud (US) account to find your email address, see I don't have access to the email for my AWS account in the AWS Sign-In User Guide.

I don't have access to the email for my standard AWS account or AWS GovCloud (US) account

If you know the email address, but no longer have access to the email, see I don't have access to the email for my AWS account in the *AWS Sign-In User Guide*.

I need to change the credit card for my AWS GovCloud (US) account

To change the credit card for your AWS GovCloud (US) account, you must have access to its associated standard AWS account. See I need to change the credit card for my AWS account in the *AWS Account Management Reference Guide*.

I need to report fraudulent AWS GovCloud (US) account activity

If you suspect fraudulent activity using your AWS GovCloud (US) account and would like to make a report, see How do I report abuse of AWS resources.

I need to close my AWS GovCloud (US) account activity

See Closing an AWS GovCloud (US) account in the *AWS GovCloud (US) User Guide*.

AWS GovCloud (US) account root user

When you first create a standard AWS account (not an AWS GovCloud (US) account), you begin with one identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user. You can sign in as the root user using the email address and password that you used to create the account.

When you finish the AWS GovCloud (US) Sign Up process and your AWS GovCloud (US) account is created, the AWS GovCloud (US) account root user is also created at that time. Unlike the conclusion of the standard AWS account sign up process, you cannot sign-in to the AWS Management Console for AWS GovCloud (US) using your account email address and password. Depending on the method you used to sign up, you are provided initial console access to your AWS GovCloud (US) account via either an Administrator IAM user or the `OrganizationAccountAccessRole` IAM role.

While AWS GovCloud (US) account root user console access is not supported, programmatic access keys are supported. Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK).

Anyone who has root user access keys for your AWS GovCloud (US) account has unrestricted access to all the resources in your account.

In this guide you will find...

- How to identify if your AWS GovCloud (US) account has root access keys
- Step-by-step directions to request your AWS GovCloud (US) account root user access keys
- Information that will help you complete task that require the AWS GovCloud (US) account root user

> **Important**
>
> We strongly recommend that you do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the best practice of using the root user only to create your first IAM user. Then securely lock away the root user access keys and use them to perform only a few account and service management tasks. To view the tasks that require root user access keys, see Tasks in AWS GovCloud (US) Regions that require root user access keys

Topics

- Tasks in AWS GovCloud (US) Regions that require root user access keys
- Restore IAM Administrator access to the AWS Management Console for AWS GovCloud (US)
- Edit or delete an Amazon S3 bucket policy for a bucket where I accidentally denied everyone access
- Remediation of AWS Security Hub findings
- Rotate my AWS GovCloud (US) account root user access keys
- Deleting my AWS GovCloud (US) account root user access keys
- Securing my AWS GovCloud (US) account root user access keys
- Transferring the root user owner

Does my AWS GovCloud (US) account have existing root access keys?

As an AWS GovCloud (US) account administrator, you may want to know if there are root access keys in your AWS GovCloud (US) account.

Method 1

You can generate and download a credential report that lists all users in your account and the status of their various credentials, including passwords, access keys, and MFA device from your AWS GovCloud (US) account.

To get your credential report, see Getting credential reports for your AWS account in the *AWS Identity and Access Management User Guide*.

In the credential report CSV, the following columns will allow you to identify if you have root access keys in your account and if they are active.

- **user** – Identify the `root_account` row.
- **access_key_1_active** – When the root user has an access key and the access key's status is Active, this value is `TRUE`. Otherwise it is `FALSE`.
- **access_key_1_last_rotated** – The date and time, in ISO 8601 date-time format, when the root user's access key was created or last changed. If the root user does not have an active access key, the value in this field is `N/A` (not applicable).
- **access_key_2_active** – When the root user has a second access key and the second key's status is Active, this value is `TRUE`. Otherwise it is `FALSE`.

- **access_key_2_last_rotated** – The date and time, ISO 8601 date-time format, when the root user's second access key was created or last changed. If the root user does not have a second active access key, the value in this field is `N/A` (not applicable).

In this example, the root user has an active root access key in the account because the `access_key_1_last_rotated` field is not marked `N/A` and the `access_key_1_active` field is marked `TRUE`. You can also see there is not a second access key associated with the root user because `access_key_2_last_rotated` field is marked `N/A`. Since there is not a second access key `access_key_2_active` field is marked `FALSE`.

	A	B
1	user	<root_account>
2	arn	arn:aws-us-gov:iam::123456789012:root
3	user_creation_time	2018-09-18T12:40:35+00:00
4	password_enabled	not_supported
5	password_last_used	no_information
6	password_last_changed	not_supported
7	password_next_rotation	not_supported
8	mfa_active	FALSE
9	access_key_1_active	TRUE
10	access_key_1_last_rotated	2022-08-27T14:06:52+00:00
11	access_key_1_last_used_date	2022-09-30T21:28:00+00:00
12	access_key_1_last_used_region	us-gov-west-1
13	access_key_1_last_used_service	iam
14	access_key_2_active	FALSE
15	access_key_2_last_rotated	N/A
16	access_key_2_last_used_date	N/A
17	access_key_2_last_used_region	N/A
18	access_key_2_last_used_service	N/A
19	cert_1_active	FALSE
20	cert_1_last_rotated	N/A
21	cert_2_active	FALSE
22	cert_2_last_rotated	N/A

For info on removing root user access keys, see Deleting my AWS GovCloud (US) account root user access keys.

Method 2

If AWS Security Hub is enabled on your account, the following Security Hub controls have a Failed compliance status when root access keys exist in your AWS GovCloud (US) account.

- CIS AWS Foundations Benchmark standard: 1.12 – Ensure no root user access key exists
- Payment Card Industry Data Security Standard (PCI DSS): [PCI.IAM.1] IAM root user access key should not exist
- AWS Foundational Security Best Practices standard: [IAM.4] IAM root user access key should not exist

For more information on AWS Security Hub, see the AWS Security Hub User Guide.

To remediate these findings, see Deleting my AWS GovCloud (US) account root user access keys.

Requesting root access keys for an AWS GovCloud (US) account

AWS GovCloud (US) account root user access keys can be requested from AWS Support. Once your request is processed and approved, any existing AWS GovCloud (US) account root user access keys in your AWS GovCloud (US) account will be deleted, followed by the creation of a single new access key. This new access key will stored as an encrypted secret with AWS Secrets Manager and AWS KMS in the **US East (N. Virginia)** Region. This secret is made available exclusively to the root user of the standard AWS account associated with your AWS GovCloud (US) account.

AWS managed account for this process: **536883072436**.

Use the following guide to request and retrieve a new AWS GovCloud (US) account root user access key.

> **Important**
>
> This process is for AWS GovCloud (US) customers who have already signed up for an AWS GovCloud (US) account and completed all onboarding steps. If you are having issues with onboarding into AWS GovCloud (US), see AWS GovCloud (US) Sign Up or contact AWS Support.

Prerequisites

This task **requires root access** to the standard AWS account associated with your AWS GovCloud (US) account.

> **Important**
>
> The AWS GovCloud (US) account root user access keys provides unrestricted access to your AWS GovCloud (US) account. For security purposes AWS Support will only process request for AWS GovCloud (US) root credentials when the requester is the root user of the standard AWS account associated with your AWS GovCloud (US) account.

If your AWS GovCloud (US) account is in an AWS GovCloud (US) Organization and has a service control policy (SCP) applied to the AWS GovCloud (US) account that disallows actions as the root user or prevents the creation of root access keys, your AWS GovCloud (US) Organization management account will need to adjust the SCP before you can request AWS GovCloud (US) account root access keys. Specifically they will need to allow the following actions from the root user:

- CreateAccessKey
- DeleteAccessKey
- ListAccessKeys

For AWS GovCloud (US) Organization Management Account Administrators

The following SCP meets the minimum requirements to process a request for AWS GovCloud (US) account root user access keys while disallowing all other actions from the AWS GovCloud (US) account root user.

This is useful in the situation where a member account may have forgot or lost their existing AWS GovCloud (US) account root user access keys and you would like to prevent them from being used to take actions against account resources until AWS Support can process your request for new AWS GovCloud (US) account root user access keys.

> **Note**
>
> When a member account needs to perform administrative task as the root user after retrieving their new AWS GovCloud (US) account root access keys from AWS Support, they

may be blocked from completing the task. Move the member account to another OU with a less restrictive SCP applied or remove the policy completely to enable them to complete Tasks in AWS GovCloud (US) Regions that require root user access keys.
This SCP will not affect the AWS GovCloud (US) Organizations Management account should you move that account into an OU with this SCP applied. To learn more, see Tasks and entities not restricted by SCPs in the *AWS Organizations User Guide*.

```
{
                        "Version": "2012-10-17",
                        "Statement": [{
                            "Sid": "AccessKeyManagementOnly",
                            "Effect": "Deny",
                            "NotAction": [
                                "iam:DeleteAccessKey",
                                "iam:CreateAccessKey",
                                "iam:ListAccessKeys"
                            ],
                            "Resource": [
                                "*"
                            ],
                            "Condition": {
                                "StringLike": {
                                    "aws:PrincipalArn": [
                                        "arn:aws-us-gov:iam::*:root"
                                    ]
                                }
                            }
                        },
                        {
                            "Sid": "RootUserAccessKeyManagementOnly",
                            "Effect": "Deny",
                            "Action": [
                                "iam:DeleteAccessKey",
                                "iam:CreateAccessKey",
                                "iam:ListAccessKeys"
                            ],
                            "Resource": [
                                "arn:aws-us-gov:iam::*:user/*"
                            ],
                            "Condition": {
                                "StringLike": {
```

```
                            "aws:PrincipalArn": [
                                "arn:aws-us-gov:iam::*:root"
                            ]
                        }
                    }
                }
            ]
        }
```

Step 1: Gather required information

Gather the following required information so you have it on hand when you open a support case in Step 2:

1. **Company Name** – This is the full legal name of a Company or Public Sector Organization associated with this account. If this AWS GovCloud (US) account is not associated with a Company or Public Sector Organization, provide Individual Account Owner as the Company Name.
2. **Account Email** – If you are not aware of your account email, see I don't know the email for my standard AWS account or AWS GovCloud (US) account in the *AWS GovCloud (US) User Guide*. If you need to change your account email, see How do I change the email address that's associated with my AWS account?
3. **Address** – This is the mailing address for your Company, Public Sector Organization, or the Individual Account Holder.
4. **AWS GovCloud (US) Account ID** – If you are not aware of your AWS GovCloud (US) account ID, see Finding your AWS GovCloud (US) account ID in the *AWS GovCloud (US) User Guide*.
5. **Account Owner** – This is the full legal name (First, Middle, Last Name) of the account owner who is requesting AWS GovCloud (US) account root user access keys. Account owner is the individual creating the support case that meets the requirements outlined in the template found in Step 2.

Step 2: Create a support case

In this step, you create a support case to the Accounts and Billing support team to request root credentials for your AWS GovCloud (US) account.

1. Sign in to your standard AWS account associated with your AWS GovCloud (US) account as the root user. To learn about signing in as the root user, see Sign in as the root user in the *AWS Sign-In User Guide*.

   If you are having issues signing in to your standard AWS account as the root user, see Troubleshooting AWS sign-in or account issues in the *AWS Sign-In User Guide*.
2. Navigate to Support Center by choosing the **?** icon in the navigation bar and then choose **Support Center** from the dropdown.
3. Choose **Create case** from the Open support cases section.
4. Choose **Account and billing**.
5. Use the dropdown box to choose **Account**. For **Category** choose **AWS GovCloud (US) – Request Root Credentials**, and then choose **Next step: Additional information**.
6. For **Subject** enter **AWS GovCloud (US) – Request Root Credentials**.
7. In the **Description** box, copy and paste the following template:

```
   Company Name: [Company Name From Step 1]
   Account Email: [Account Email  From Step 1]
   Address: [Address  From Step 1]
   AWS GovCloud (US) Account ID: [AWS GovCloud (US) Account ID From Step 1]

   I [Full Legal Name: First, Middle, Last Name of the Account Owner] hereby
   acknowledge the applicable requirements contained in the AWS GovCloud (US)
   Addendum to the AWS Customer Agreement (the "AWS GovCloud (US) Addendum")
   that apply to and governs the use of the AWS services in the AWS GovCloud (US)
   Region by the above referenced company. In accordance with the terms of the
   AWS GovCloud (US) Addendum, I represent and warrant that: I am a U.S. person;
   not subject to export restrictions under U.S. export control laws and
regulations
   (e.g., I am not on the denied or debarred party list or otherwise subject
   to sanctions); and have full authority to request AWS release to me
   account credentials relating to the subject AWS GovCloud (US) account listed
above.

   By typing my name below, I certify the above statements to be true and correct
   to the best of my knowledge, and that this information can be used for the
   purpose of processing new root credentials for the AWS GovCloud (US)
   account listed above.

   Name: [Full Legal Name: First, Middle, Last Name of the Account Owner]
```

```
Title: [Your title related to the Company Name identified above]
Date: [Enter the date]
```

8. Using the information collected in Step 1 fill out the required fields indicated by [brackets] in the template.

> **Important**
>
> AWS Support will not process your request should the following be identified in your support case:
>
> - An incomplete template was provided.
> - There is missing information in the required fields.
> - The AWS GovCloud (US) Account ID field has an AWS GovCloud (US) account ID not associated with the standard AWS account that is creating this support case.
> - The Account Email field has an email that is not associated with the standard AWS account that creates this support case.
> - Multiple AWS GovCloud (US) account IDs were provided. Each AWS GovCloud (US) account requested will need its own support case from the associated standard AWS account as the root user.

The following image shows an example of a completed ticket:

Subject

AWS GovCloud (US) - Request Root Credentials

Maximum 250 characters (206 remaining)

Description

Don't share any sensitive information in case correspondences, such as credentials, credit cards, signed URLs, or personally identifiable information.

Learn more.

Company Name: Example Company
Account Email: email@example.com
Address: 1960 W CHELSEA AVE STE 2006R ALLENTOWN PA 18104
AWS GovCloud (US) Account ID: 123456789012

I John Lee Doe hereby acknowledge the applicable requirements contained in the AWS GovCloud (US) Addendum to the AWS Customer Agreement (the "GovCloud Addendum") that apply to and governs the use of the AWS Services in the AWS GovCloud (US) region by the above referenced company. In accordance with the terms of the AWS GovCloud (US) Addendum, I represent and warrant that: I am a U.S. person; not subject to export restrictions under U.S. export control laws and regulations (e.g., I am not on the denied or debarred party list or otherwise subject to sanctions); and have full authority to request AWS release to me account credentials relating to the subject AWS GovCloud (US) account listed above.

By typing my name below, I certify the above statements to be true and correct to the best of my knowledge, and that this information can be used for the purpose of processing new root credentials for the AWS GovCloud (US) account listed above.

Name: John Lee Doe
Title: Executive Director of Information Technology
Date: October 14, 2022

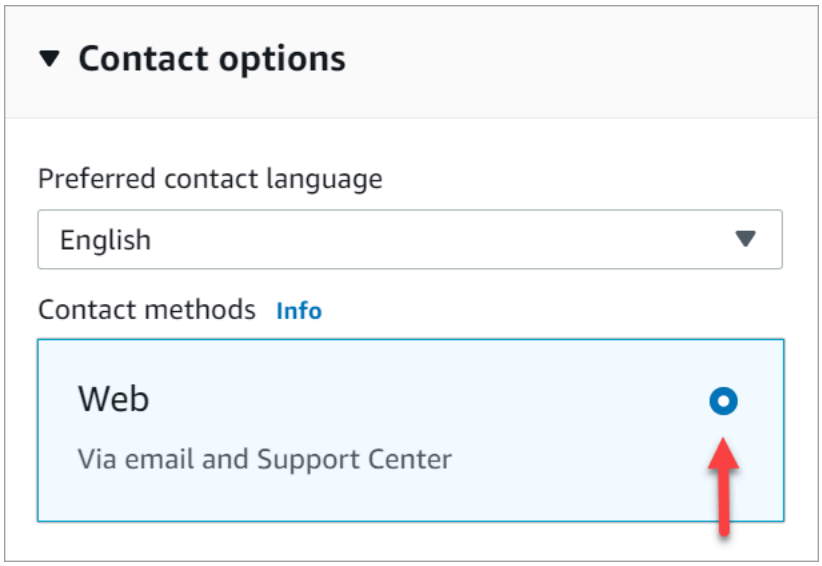
Maximum 5000 characters (3791 remaining)

Attach files

You can attach up to 3 files. Each file can be up to 5 MB.

9. Choose **Next step**.

10. Choose **Contact us**, choose your **Preferred contact language**, and then choose **Web** as the contact method, if it's not selected by default.



11. Choose **Submit**.
12. AWS Support will work with our internal service teams on your request and follow up with any additional questions.

    Once approved and processed, AWS Support will follow-up on the support case to provide the required information you need to continue onto Step 3.

Step 3: Retrieving your AWS GovCloud (US) account root user access keys

In this step, you will retrieve your new AWS GovCloud (US) account root user access keys.

1. Sign in to your standard AWS account associated with your AWS GovCloud (US) account as the root user. To learn about signing in as the root user, see Sign in as the root user in the *AWS Sign-In User Guide*.

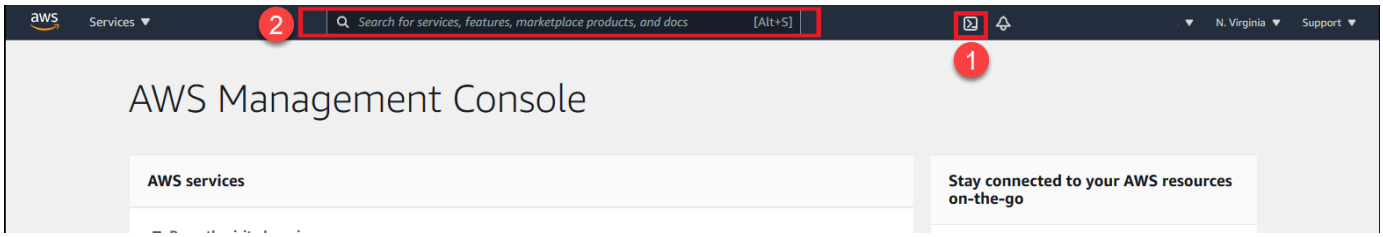
   If you are having issues signing in to your standard AWS account as the root user, see Troubleshooting AWS sign-in or account issues in the *AWS Sign-In User Guide*.
2. Navigate to Support Center by choosing the **?** icon in the navigation bar and then choose **Support Center** from the dropdown.
3. In the **Support Center** navigation pane, choose **Your support cases**.
4. Open your support case created in Step 2 by choosing the **Case ID** or **Subject**.
5. Find the latest **Correspondence** from AWS Support.

6. Use keyboard shortcuts or context (right-click) menu to copy the AWS CLI command provided by AWS Support, which looks like this:

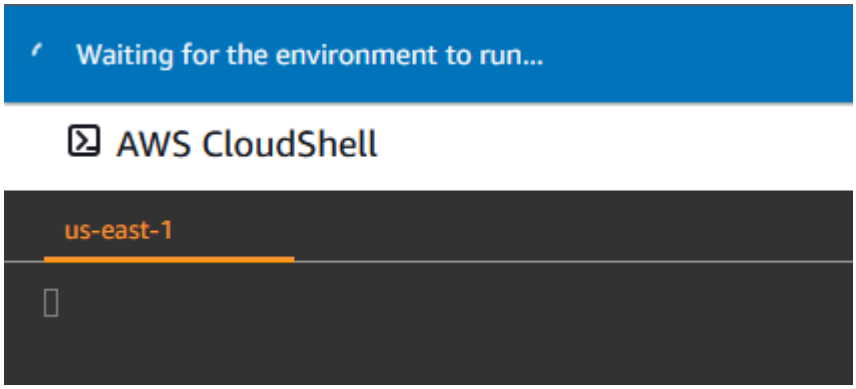
```
$ aws secretsmanager get-secret-value
--secret-id arn:aws:secretsmanager:us-east-1:536883072436:secret:abcDEfgHiJKLMno-abcDeF
--region us-east-1 --version-stage AWSCURRENT --output text --query 'SecretString'
```

7. With the command copied, launch AWS CloudShell. You can launch CloudShell from the AWS Management Console using either one of the following two methods:

   - Choose the AWS CloudShell icon on the console navigation bar.
   - Start typing *cloudshell* in the **Find Services** box and then choose the **CloudShell** option.



8. Your environment will take a few seconds to get started. Once ready you will see `[cloudshell-user@ip-xxx.xxx.xxx.xxx ~] $`.



9. Paste the command into the AWS CloudShell terminal, then press enter. Your AWS GovCloud (US) root access keys will be output to the terminal.

   Example

```
$ aws secretsmanager get-secret-value
--secret-id arn:aws:secretsmanager:us-east-1:536883072436:secret:abcDEfgHiJKLMno-
abcDeF --region us-east-1
--version-stage AWSCURRENT --output text --query 'SecretString'
 {"SecretAccessKey":
"wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY", "AccessKeyId": "AKIAIOSFODNN7EXAMPLE"}
```

   Note

   See the Troubleshooting section below should you experience any errors running the get-secret-value command.

10. Save your AWS GovCloud (US) account root user access keys in a safe location. To learn more, see Securing my AWS GovCloud (US) account root user access keys in this guide.
11. Configure AWS GovCloud (US) account root user access keys in the AWS CLI (AWS CloudShell) to complete Tasks in AWS GovCloud (US) Regions that require root user access keys.

    Important

    The `aws secretsmanager get-secret-value` command will fail any additional execution attempts after a single successful execution. If you closed the browser or cleared the terminal before saving your access key and secret access key, you will need to start this process over from the beginning. AWS Support will not be able to re-enable access to the previous secret from the original support case.

Troubleshooting

These are some of the most common issues you may face while retrieving your AWS GovCloud (US) account root user access keys.

Issue: DecryptionFailure

```
$ aws secretsmanager get-secret-value --secret-id arn:aws:secretsmanager:us-
east-1:536883072436:secret:abcDEfgHiJKLMno-abcDeF
--region us-east-1 --version-stage AWSCURRENT --output text --query 'SecretString'
An error occurred (DecryptionFailure) when calling the GetSecretValue operation:
Secrets Manager can't decrypt the secret value: arn:aws:kms:us-
east-1:536883072436:key/73947a77-ddbe-4dc7-bd8f-3fe0bc840778 is disabled.
(Service: AWSKMS; Status Code: 400; Error Code: DisabledException; Request
 ID: cdc4b7ed-e171-4cef-975a-ad829d4123e8; Proxy: null)
```

Cause

Your AWS GovCloud (US) account root user access key have been successfully retrieved once.

Solution

If you lost or forgot your AWS GovCloud (US) account root user access keys from Step 3, you will need to start from Step 1 and submit a new support case. AWS Support will not be able to re-enable access to the access keys generated in the original support case.

Issue: AccessDeniedException

```
$ aws secretsmanager get-secret-value --secret-id arn:aws:secretsmanager:us-
east-1:536883072436:secret:abcDEfgHiJKLMno-abcDeF
--region us-east-1 --version-stage AWSCURRENT --output text --query 'SecretString'
An error occurred (AccessDeniedException) when calling the GetSecretValue operation:
 User: arn:aws:iam::123456789012:user/admin
is not authorized to perform: secretsmanager:GetSecretValue on resource:
 arn:aws:secretsmanager:us-east-1:536883072436:secret:abcDEfgHiJKLMno-abcDeF
because no resource-based policy allows the secretsmanager:GetSecretValue action
```

Cause

An IAM identity that was not the root user of the standard AWS account associated with your AWS GovCloud (US) account was used to run this command. For security purposes AWS will only allow

the retrieval of your new AWS GovCloud (US) account root user access keys from the root user of the standard AWS account associated with your AWS GovCloud (US) account.

Solution

The AWS CLI in AWS CloudShell by default will assume the credentials of the user who is signed into the AWS Management Console. Sign in to the standard AWS account associated with your AWS GovCloud (US) account as the root user and run the provided command in AWS CloudShell.

> **Note**
>
> If you are signed in as the root user of the standard AWS account associated with your AWS GovCloud (US) account and you receive this error, your AWS CloudShell environment may have been altered from its default state. You can return AWS CloudShell to its default settings by deleting your home directory.

Configure AWS GovCloud (US) account root user access keys in the AWS CLI (AWS CloudShell)

Before completing Tasks in AWS GovCloud (US) Regions that require root user access keys, you will need to configure the AWS CLI with your AWS GovCloud (US) account root user access keys. If you do not have AWS GovCloud (US) account root user access keys, see Requesting root access keys for an AWS GovCloud (US) account.

If you have just completed the steps to retrieve your AWS GovCloud (US) account root user access keys, you can continue to use AWS CloudShell in your standard AWS account as the AWS CLI is preinstalled. Alternatively, you can download the AWS CLI for local use.

A collection of settings in the AWS CLI is called a profile. By default, the AWS CLI uses the default profile. We recommend the creation and use of an additional named profile for storing these root access keys by specifying the `--profile` option and assigning a name.

The following example creates a profile named `govcloudroot`. This profile will be used in other examples throughout this guide.

```
$ aws configure --profile govcloudroot
        AWS Access Key ID [None]: AKIAI44QH8DHBEXAMPLE
        AWS Secret Access Key [None]: je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
        Default Region name [None]: us-gov-west-1
```

```
        Default output format [None]: json
```

Note

If using AWS CloudShell you must specify the >region in each command using the `--region` option.

Example

```
$ aws sts get-caller-identity --profile govcloudroot --region us-gov-west-1
    {
        "UserId": "123456789012",
        "Account": "123456789012",
        "Arn": "arn:aws-us-gov:iam::123456789012:root"
    }
```

AWS CLI security with AWS GovCloud (US) account root user access keys

The credentials used by the AWS CLI are stored in plaintext files and are **not** encrypted. The `$HOME/.aws/credentials` file stores long-term credentials required to access your AWS resources. These include your access key ID and secret access key.

AWS CLI security with AWS GovCloud (US) account root user access keys

Once you have completed Tasks in AWS GovCloud (US) Regions that require root user access keys, delete your AWS GovCloud (US) account root user access keys.

If you would like to retain your AWS GovCloud (US) account root user access keys, it is recommended to remove them from your AWS CLI credentials file. Store your access keys in a safe location until the next time you need them. To remove your root access keys from the credentials file, you can use the following methods.

- Directly edit the **credentials** files in a text editor. For more information, see Where are configuration settings stored?
- Run the following commands to remove your AWS GovCloud (US) account root user access keys from the **govcloudroot** profile.

```
$ aws configure set aws_access_key_id "" --profile govcloudroot
```

```
                                        $ aws configure set aws_secret_access_key ""
--profile govcloudroot
```

Tasks in AWS GovCloud (US) Regions that require root user access keys

We recommend that you use an IAM user with appropriate permissions to perform tasks and access AWS resources. However, you can perform the tasks listed below only when you use the AWS GovCloud (US) account root user access keys. Configure AWS GovCloud (US) account root user access keys in the AWS CLI (AWS CloudShell) before starting these tasks.

Tasks

- Restore IAM Administrator access to the AWS Management Console for AWS GovCloud (US)
- Edit or delete an Amazon S3 bucket policy for a bucket where I accidentally denied everyone access
- Remediation of AWS Security Hub findings
- Rotate my AWS GovCloud (US) account root user access keys
- Deleting my AWS GovCloud (US) account root user access keys
- Securing my AWS GovCloud (US) account root user access keys
- Transferring the root user owner

Restore IAM Administrator access to the AWS Management Console for AWS GovCloud (US)

The most common use of AWS GovCloud (US) account root user access keys is to restore administrator access to the AWS GovCloud (US) console. In this section, you will learn how to restore AWS Management Console access for the `Administrator` IAM user in your AWS GovCloud (US) account using your AWS GovCloud (US) account root user access keys.

Any additional IAM administrative task not requiring AWS GovCloud (US) account root user access keys are recommended to be completed in the AWS GovCloud (US) console as the `Administrator` IAM user.

To learn how to sign in to the AWS GovCloud (US) console as an IAM user, see Sign in as an IAM user in the *AWS GovCloud (US) User Guide*.

Important

Before completing Tasks in AWS GovCloud (US) Regions that require root user access keys, you will need to configure the AWS CLI with your AWS GovCloud (US) account root user access keys. To learn how, see Configure AWS GovCloud (US) account root user access keys in the AWS CLI (AWS CloudShell).

Creating an Administrator IAM user and Administrators IAM group

Copy and paste the following AWS CLI commands into the terminal window to...

- Create the `Administrators` IAM group.
- Attach the AWS managed `AdministratorAccess` policy to `Administrators` IAM group.
- Create the `Administrator` IAM user.
- Add the `Administrator` IAM user to the `Administrators` IAM group.

```
$ aws iam create-group --group-name Administrators --profile govcloudroot --region us-
gov-west-1
                            $ aws iam attach-group-policy --group-name Administrators
 --policy-arn arn:aws-us-gov:iam::aws:policy/AdministratorAccess --profile govcloudroot
 --region us-gov-west-1
                            $ aws iam create-user --user-name Administrator --profile
 govcloudroot --region us-gov-west-1
                            $ aws iam add-user-to-group --user-name Administrator --
group Administrators --profile govcloudroot --region us-gov-west-1
```

Setting a new Administrator IAM user password

With the `Administrator` IAM user created you can now set a new password to access the AWS GovCloud (US) console. It is recommended you set a temporary password when using the AWS CLI and require the password to be changed once you sign in to the AWS GovCloud (US) console.

Copy and paste the following AWS CLI command into your terminal window to set a new temporary password for the `Administrator` IAM user. Sign in to the AWS GovCloud (US) console with the temporary password to set your new password for the `Administrator` IAM user.

```
$ aws iam create-login-profile --user-name Administrator --password-reset-required
```

```
                          --profile govcloudroot --region us-gov-west-1 --password
NewTempPasswordHere
```

Note

PasswordPolicyViolation errors may occur depending on the password policy applied to your account.
The default password policy enforces the following conditions:

- Minimum password length of 8 characters and a maximum length of 128 characters
- Minimum of three of the following mix of character types: uppercase, lowercase, numbers, and non-alphanumeric character (`! @ # $ % ^ & * ( ) _ + - = [ ] { } | '`)
- Not be identical to your AWS account name or email address

Use the following command to review your account password policy.

```
$ aws iam get-account-password-policy --profile govcloudroot --region us-gov-
west-1
```

To learn more about account password policies, see Setting an account password policy for IAM users in the *AWS Identity and Access Management Access Analyzer User Guide*.

Disabling an MFA device associated with the Administrator IAM user password

Use these commands to disassociate an MFA device from the `Administrator` IAM user and deactivate it. If the device is virtual, use the ARN of the virtual device as the serial number.

1. List MFA devices associated with the Administrator user. Note the `SerialNumber`.

   ```
   $ aws iam list-mfa-devices --user-name Administrator --profile govcloudroot --
   region us-gov-west-1
   ```

2. Disassociate the MFA device from the Administrator IAM user and deactivate it. Serial number from the last step will be used in the `--serial-number` option.

```
aws iam deactivate-mfa-device --user-name Administrator --profile govcloudroot --
region us-gov-west-1 --serial-number SerialNumberFromPreviousStepHere
```

Edit or delete an Amazon S3 bucket policy for a bucket where I accidentally denied everyone access

During development or implementation of a new Amazon S3 bucket policy, you may accidentally deny access to the bucket for all IAM users in your AWS GovCloud (US) account. Use the following commands with your AWS GovCloud (US) account root user access keys to retrieve, replace, or delete the policy.

> **Important**
>
> Before completing Tasks in AWS GovCloud (US) Regions that require root user access keys, you will need to configure the AWS CLI with your AWS GovCloud (US) account root user access keys. To learn how, see Configure AWS GovCloud (US) account root user access keys in the AWS CLI (AWS CloudShell).

aws s3api get-bucket-policy

```
aws s3api get-bucket-policy --profile govcloudroot --region us-gov-west-1 --bucket my-
bucket
```

aws s3api put-bucket-policy

```
aws s3api put-bucket-policy --profile govcloudroot --region us-gov-west-1
--bucket my-bucket --policy file://policy.json
```

> **Note**
>
> To learn how to work with files on your operating system in the AWS CLI, see Loading AWS CLI parameters from a file.

aws s3api delete-bucket-policy

```
aws s3api delete-bucket-policy --profile govcloudroot --region us-gov-west-1 --bucket
 my-bucket
```

Remediation of AWS Security Hub findings

The following AWS Security Hub findings can be remediated by deleting all root access keys in the AWS GovCloud (US) account. To learn how, see Deleting my AWS GovCloud (US) account root user access keys.

- CIS AWS Foundations Benchmark standard: 1.12 – Ensure no root user access key exists
- Payment Card Industry Data Security Standard (PCI DSS): [PCI.IAM.1] IAM root user access key should not exist
- AWS Foundational Security Best Practices standard: [IAM.4] IAM root user access key should not exist

Rotate my AWS GovCloud (US) account root user access keys

It is recommended to not have AWS GovCloud (US) root access keys in your account. If you must keep one available, rotate (change) the access key regularly. You can rotate access keys from the AWS Command Line Interface using an active AAWS GovCloud (US) account root user access key.

> **Important**
>
> Before completing Tasks in AWS GovCloud (US) Regions that require root user access keys, you will need to configure the AWS CLI with your AWS GovCloud (US) account root user access keys. To learn how, see Configure AWS GovCloud (US) account root user access keys in the AWS CLI (AWS CloudShell).

Rotating root access keys without interrupting your applications (AWS CLI)

1. While the first access key is still active, create a second access key, which is active by default. Run the following command:

   ```
   $ aws iam create-access-key --profile govcloudroot --region us-gov-west-1
   ```

> **Note**
>
> At this point, the AWS GovCloud (US) root user has two active access keys.

2. Update all applications and tools to use the new access key. This includes the AWS CLI you are currently using. Update to the new access keys by running the following command:

```
$ aws configure --profile govcloudroot
    AWS Access Key ID [None]: AKIAI44QH8DHBEXAMPLE
    AWS Secret Access Key [None]: je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
    Default Region name [None]: us-gov-west-1
    Default output format [None]: json
```

3. Determine whether the first access key is still in use by using this command:

```
$ aws iam get-access-key-last-used --profile govcloudroot --region us-gov-west-1 --
access-key-id FirstAccessKeyIdHere
```

> **Note**
>
> One approach is to wait several days and then check the old access key for any use before proceeding.

4. Even if step 3 indicates no use of the old key, we recommend that you do not immediately delete the first access key. Instead, change the state of the first access key to Inactive using this command:

```
$ aws iam update-access-key --status Inactive --profile govcloudroot --region us-
gov-west-1 --access-key-id FirstAccessKeyIdHere
```

5. Use only the new access key to confirm that your applications are working. Any applications and tools that still use the original access key will stop working at this point because they no longer have access to AWS resources. If you find such an application or tool, you can switch its state back to Active to reenable the first access key. Then return to step 2 and update this application to use the new key.
6. After you wait some period of time to ensure that all applications and tools have been updated, you can delete the first access key with this command:

```
$ aws iam delete-access-key --profile govcloudroot --region us-gov-west-1 --access-key-id FirstAccessKeyIdHere
```

Deleting my AWS GovCloud (US) account root user access keys

It is recommended to not have AWS GovCloud (US)) root access keys in your account. Use the following commands with your AWS GovCloud (US) account root user access keys to delete any additional root user access keys and itself.

> **Important**
>
> Before completing Tasks in AWS GovCloud (US) Regions that require root user access keys, you will need to configure the AWS CLI with your AWS GovCloud (US) account root user access keys. To learn how, see Configure AWS GovCloud (US) account root user access keys in the AWS CLI (AWS CloudShell).

1. List all root access keys with the following command:

```
$ aws iam list-access-keys --profile govcloudroot --region us-gov-west-1
```

2. List the root access key in use with the following command:

```
$ aws configure get aws_access_key_id --profile govcloudroot
```

3. (Optional) If there was a second root access key returned in the `list-access-keys` command that does not match the access key provided in the `configure get aws_access_key_id` command, delete that access key first. This will be the access key that is not currently in use by the AWS CLI. To delete that access key run the following command:

```
$ aws iam delete-access-key --profile govcloudroot --region us-gov-west-1 --access-key-id UnusedAccessKeyIdHere
```

> **Note**
>
> You can verify the unused access key was deleted by running the `list-access-keys` command again.

4. Delete the root user access key that is currently in use.

```
$ aws iam delete-access-key --profile govcloudroot --region us-gov-west-1 --access-key-id ConfiguredAccessKeyIdHere
```

Securing my AWS GovCloud (US) account root user access keys

Safeguard your AWS GovCloud (US) account root user access keys the same way you would protect other sensitive personal information. We don't recommend generating access keys for your root user, because they allow full access to all your resources for all AWS services. The root user in AWS GovCloud (US) does not support MFA. Don’t use your root user for everyday tasks. Use the root user to complete the tasks that only the root user can perform. For the complete list of these tasks, see Tasks in AWS GovCloud (US) Regions that require root user access keys in this guide. Listed here are best practices to secure your AWS GovCloud (US) account root access keys.

- If you don't already have an access key for your AWS account root user, don't create one unless you absolutely need to. Instead, use an IAM user that has administrative permissions.
- If you do have an access key for your root user, delete it. You can request another at any time by following the Requesting root access keys for an AWS GovCloud (US) account workflow in this guide.
- If you must keep one available, rotate (change) the access key regularly. To rotate your AWS GovCloud (US) account root user access keys, see Rotate my AWS GovCloud (US) account root user access keys.

Transferring the root user owner

The associated standard AWS account root user is the AWS GovCloud (US) account owner. To transfer ownership of your AWS GovCloud (US) account, you will transfer ownership of the related standard AWS account root user, see How do I transfer my AWS account to another person or business?

The method to provide the new owner access to the AWS GovCloud (US) account should be coordinated prior to the transfer of ownership and in accordance to the agreements between the individuals or organizations making the transfer.

If the previous owner has transferred the standard AWS account root user to you without providing access to the related AWS GovCloud (US) account, you can request root access keys for the AWS GovCloud (US) account from AWS Support, see Requesting root access keys for an AWS GovCloud (US) account.

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 linked standard AWS 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.
3. On the **My Security Credentials** tab, choose **Create Access Key**.
4. To download the access key, choose **Download Credentials** and save them locally.

> **Important**
>
> If you configure an IAM password expiration policy that requires administrator reset, and your Administrator password expires, access keys with appropriate privileges can be used to reset your administrator password from the command line. If you do not have additional administrator users created or access keys for your Administrator account, you will need to contact support to regain access to your account.

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 *xxxxxxxxxxxx* 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. If CloudTrail is enabled, the **Dashboard** page opens, and the **Trails** section shows your trail.
3. If CloudTrail is not enabled, choose **Create a trail**. For more information about creating a trail using the console, see Creating a trail in the console (advanced event selectors) in the *AWS CloudTrail User Guide*.

   > **Note**
   >
   > For the **Storage location**, choose **Use existing S3 bucket**, and specify the S3 bucket you created in the previous procedure.

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

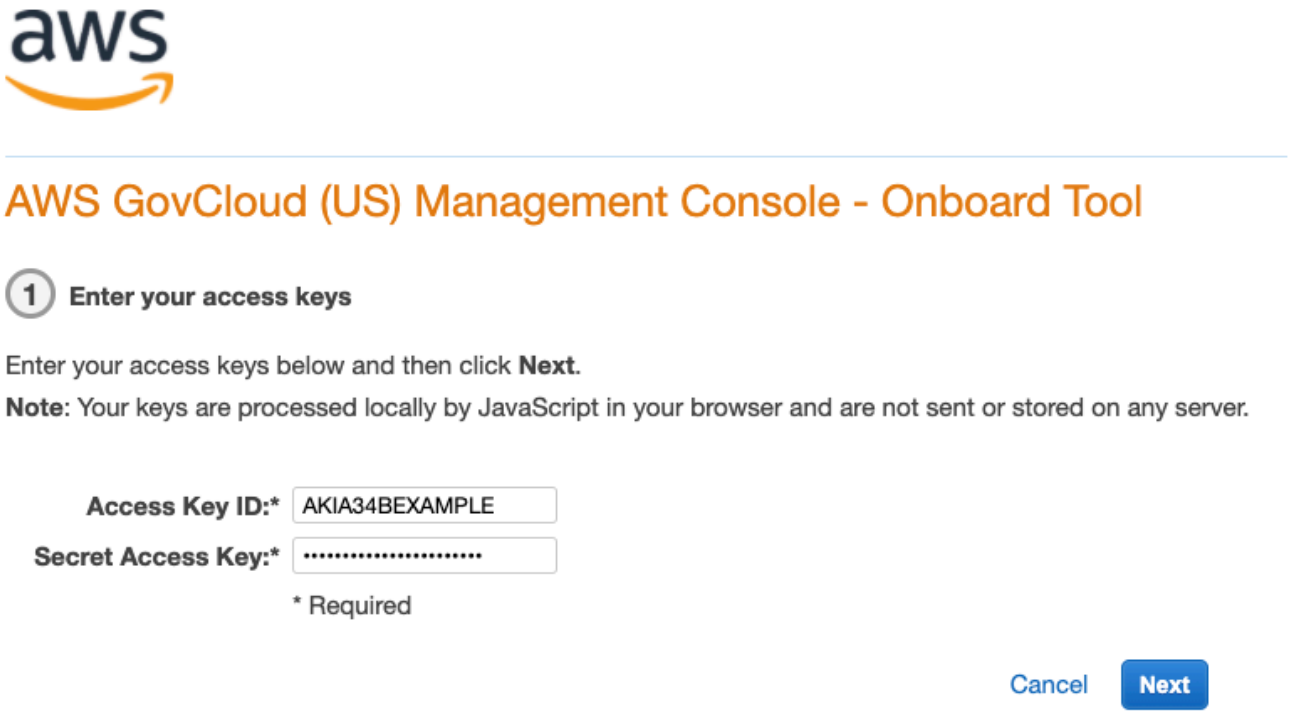
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws-us-gov:s3:::s3_bucket_name",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:aws-us-
gov:cloudtrail:region:account_id:trail/trail_name"
                }
            }
        },
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "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",
                    "aws:SourceArn": "arn:aws-us-
gov:cloudtrail:region:account_id:trail/trail_name"
                }
            }
        }
    ]
}
```

Onboarding to AWS GovCloud (US) as a Solution Provider reselling in AWS GovCloud (US)

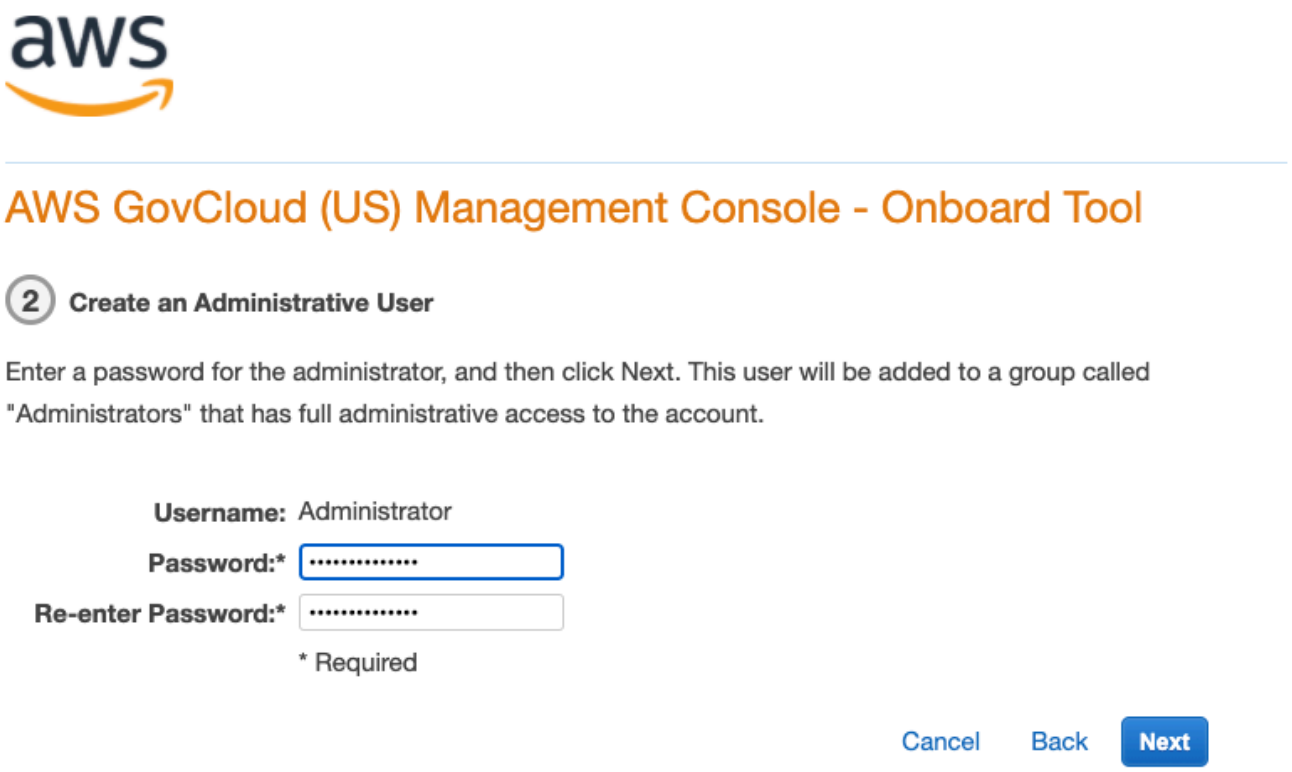
If you are serving as a Solution Provider and reselling in AWS GovCloud (US), you must create an IAM user to sign in to the AWS Management Console for the AWS GovCloud (US) Region. If you received your account credentials through a Solution Provider, please contact your Solution Provider to sign up.

To create your first administrative IAM user

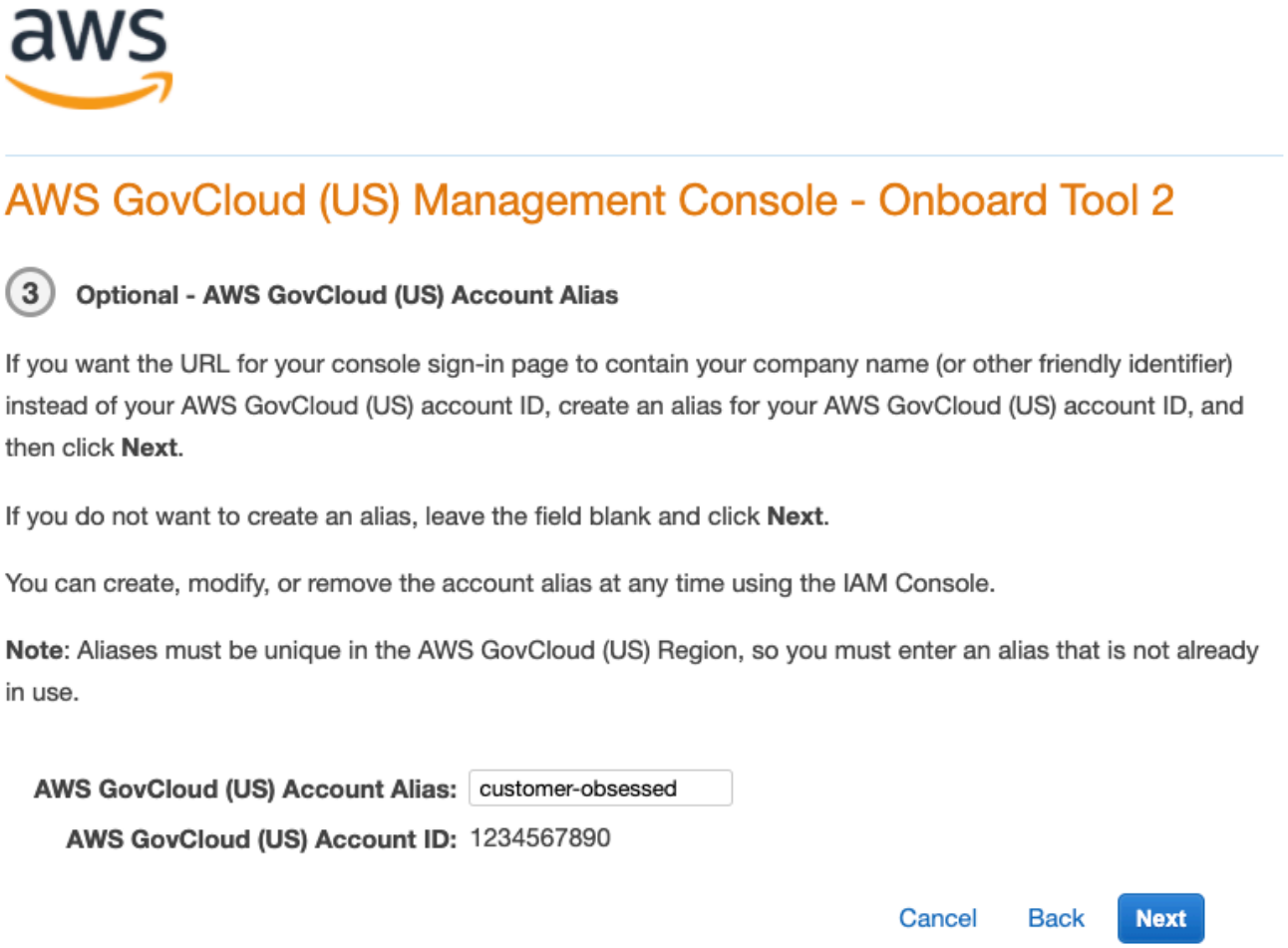
1. Access the AWS GovCloud (US) console onboard tool web application..
2. Type your access key ID and secret access key, and then choose **Next**.



3. Type a password for the administrator, and then choose **Next**.

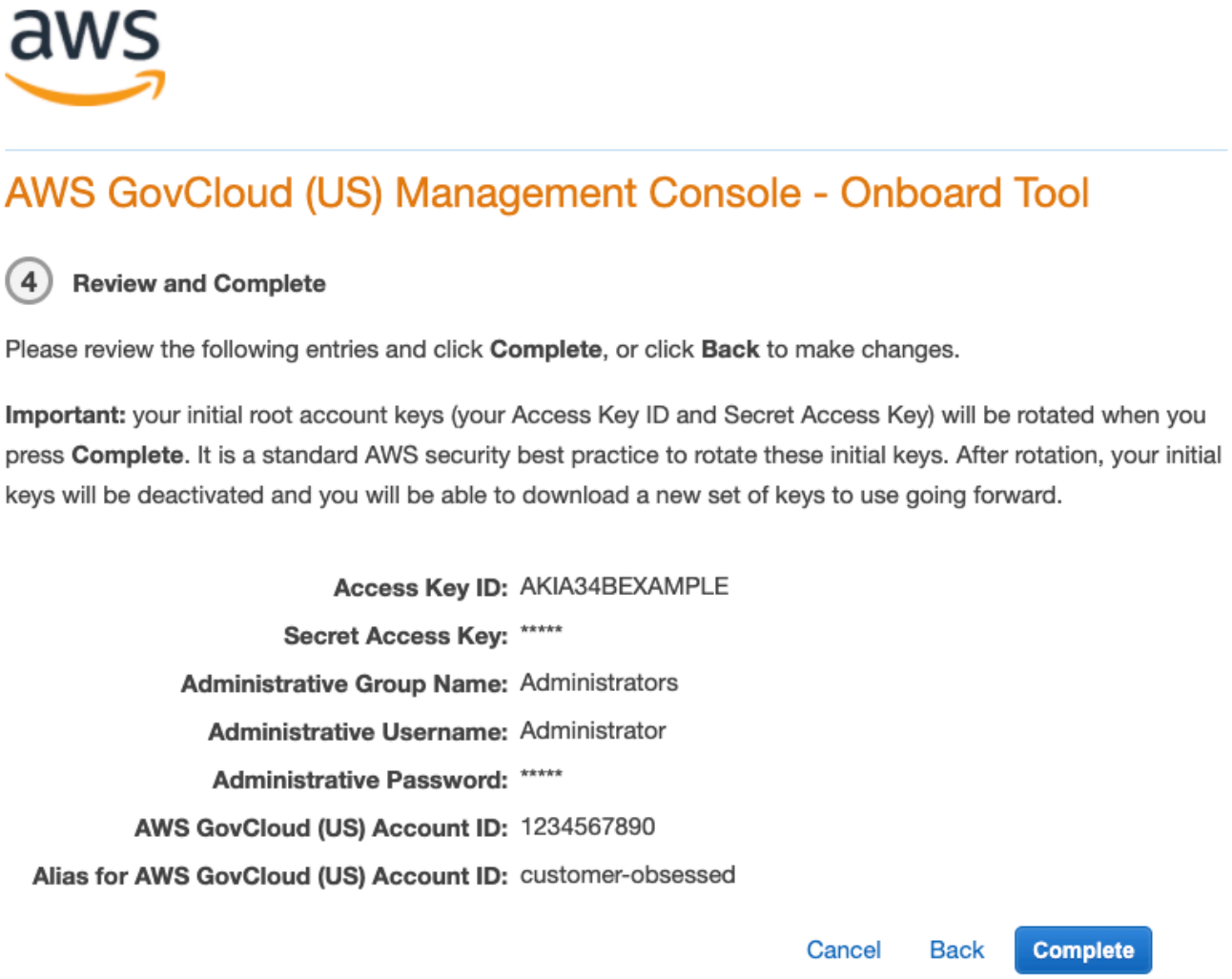


4. (Optional) If you want to create an account alias, type a name (all lowercase) for your account, and then choose **Next**.



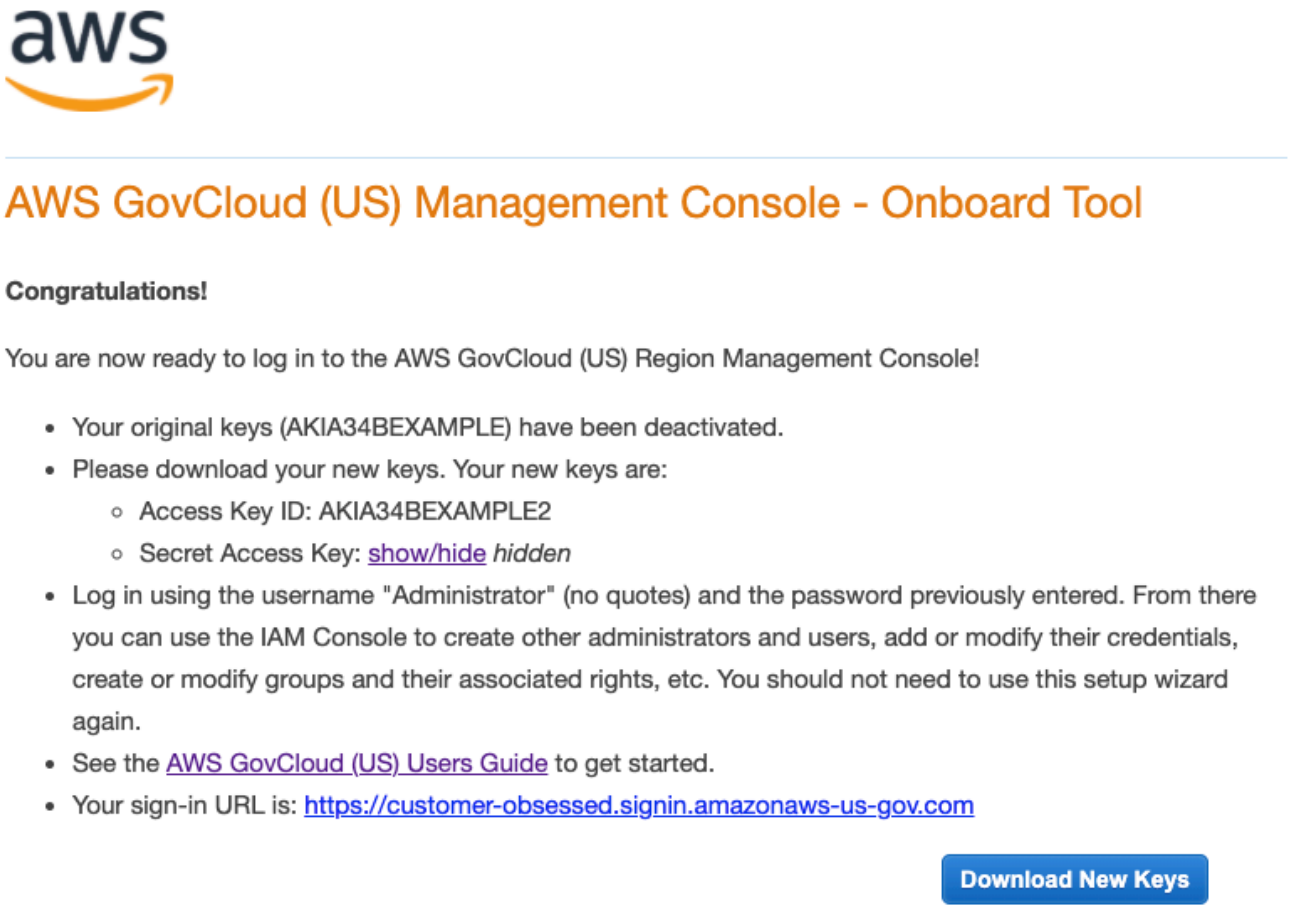
An account alias provides an easy-to-remember link for signing in to the console. For more information about account aliases, see Your AWS Account ID and Its Alias in the *IAM User Guide*.

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*.

Configure Your Account using AWS CLI

The AWS Management Console for the AWS GovCloud (US) Region provides an easy-to-use graphical interface to manage your AWS resources, similar to the AWS Management Console for the standard Regions. In the AWS GovCloud (US) region, you must create an IAM user and use this user name and password to sign in to the console. You cannot use the AWS GovCloud (US)

access keys to log into the console. You also cannot use your sign-in credentials for the standard AWS Management Console to access the AWS GovCloud (US) console. The AWS Management Console for the AWS GovCloud (US) Region is a completely separate console from the standard AWS Management Console.

Follow the directions below to create an administrator user name and password that will allow you to login to the console. You can create additional IAM accounts for all of your users once you sign in.

> **Note**
>
> If you are not an AWS GovCloud (US) Customer, please visit AWS GovCloud (US) Region Overview to find out about the AWS GovCloud (US) Region and then fill out the contact us form (https://aws.amazon.com/govcloud-us/contact/) to request an AWS GovCloud (US) Account.

Configure the AWS CLI

To get started, you will need install the AWS CLI on your local machine. To learn how to install the AWS CLI, visit the AWS CLI documentation. Next, you will need to configure your local CLI to use your new AWS GovCloud (US) (US) account. To do so, run the following command. This command will prompt for the Access Keys and Secret Keys that are provided in the onboarding email.

> **Note**
>
> You can replace `--profile "govcloud"` with a name that is convenient for you.

```
# 1. Configure the cli
aws configure --profile "govcloud"

# 2. Check if the credentials are functioning
aws iam list-users --profile "govcloud"
```

Now that we have the CLI configured with our new AWS GovCloud (US) account, we can configure IAM users for accessing the environment.

Create an IAM User to Access the Console

To get started, we will create an IAM Group to manage administrator access to the AWS GovCloud (US) account. Then, we will create an IAM user, add them to the group, and configure a password for accessing the environment. Using the profile we configured above, run the following commands on the CLI.

```
# 1. Create an “Administrators” IAM Group so that we can centrally manage Administrator
 IAM permissions for many users.
aws iam create-group \
    --group-name "Administrators" \
    --profile "govcloud"

# 2. Attach the AdministratorAccess policy to the group
aws iam attach-group-policy \
    --group-name "Administrators" \
    --policy-arn "arn:aws-us-gov:iam::aws:policy/AdministratorAccess" \
    --profile "govcloud"

# 3. Create a new IAM User
aws iam create-user \
    --user-name "username" \
    --profile "govcloud"

# 4. Enable the IAM User to sign in to the AWS Console
aws iam create-login-profile \
    --user-name "username" \
    --password "password" \
    --no-password-reset-required \
    --profile "govcloud"

# 5. Add the User to the Administrators IAM Group
aws iam add-user-to-group \
    --group-name "Administrators" \
    --user-name "username" \
    --profile "govcloud"

# 6. Create Access Keys for accessing AWS via the CLI and SDK
aws iam create-access-key \
    --user-name "username" \
    --profile "govcloud"
```

Logging in to the Console

1. Open the AWS GovCloud (US) console.
2. Sign in using your account number and the user name and password you created above.
3. Once you are signed in, navigate to the IAM console..
4. You should now see 2 users listed. Administrator and the user name you created above. The Administrator credentials were the ones provided during sign up.
5. Confirm your new user has been added to the Administrators group and has the AdministratorAccess policy associated with the Administrators group.
6. You can now safely delete the administrator IAM user or deactivate the Access Credentials.

Customizing the Sign In URL

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 AWS GovCloud (US) console and open the IAM console.
2. Next to the IAM users sign-in link, choose Customize.
3. Type an alias for your account.
4. IAM users can now use either the account alias or account number when signing in to the AWS AWS GovCloud (US) console.

Audit Logging

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.

Enabling Multi-Factor Authentication (MFA) for users

For increased security, we recommend that you configure multi-factor authentication (MFA) to help protect your AWS GovCloud (US) resources. MFA adds extra security because it requires users to

enter a unique authentication code from an approved authentication device when they access AWS websites or services.

AWS GovCloud (US) allows you to assign a hardware-based token device, a virtual MFA device, or a FIDO security key with FIPS-validated options to an IAM user or to your GovCloud administrator. A virtual or hardware token-based 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.

FIDO2 is an open authentication standard and an extension of FIDO U2F, based on public key cryptography, which enables strong, phishing-resistant authentication. To learn more about the FIDO2 standard, see FIDO Alliance. Based on your security and compliance needs, you can use both FIPS and non-FIPS FIDO security keys. You can also specify what kinds of authenticators your users can register in your IAM policies based on your preferred certification type and level. For more information about FIDO certifications, see Device certifications.

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 supported for IAM users. There is no root user in AWS GovCloud (US). For more information, see AWS Management Console documentation.
2. Get an MFA 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, supported by AWS, such as OTP token. This device has its unique token seeds shared securely with AWS. Token seeds are secret keys generated at the time of token production. Tokens purchased from other sources will not function with IAM.
   - 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.
   - A FIDO2 security key creates a new key pair for use with only AWS. FIDO-certified hardware security keys are provided by third-party providers such as Yubico, which include FIPS-validated options like YubiKey FIPS devices. For a full list, see FIDO devices supported by AWS. To use a FIDO2 security key, your browser must support FIDO2. For a list, see Browsers that support FIDO2.

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:

   - Hardware TOTP token: Enabling a hardware TOTP token (console)
   - Virtual MFA device: Enabling a Virtual Multi-Factor Authentication (MFA) Device
   - FIDO security key: Enabling a FIDO security key (console)
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)AWS 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. All AWS Support engineers in the AWS Region (`aws` partition) can access support cases from the AWS GovCloud (US) Region. Customers 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.

> **Important**
>
> Do not enter any export-controlled data in your support cases.

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 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.

For more information about the differences with AWS Support in the AWS GovCloud (US) Regions, see AWS Support.

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

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 is not available in AWS GovCloud (US), but you can use CloudFront in the standard Regions and point to your AWS GovCloud (US) resources.

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

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 AWS GovCloud (US) Sign Up 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.
- 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 AWS GovCloud (US) Sign Up 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 with public hosted zones, 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 create alias records in a public hosted zone that 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

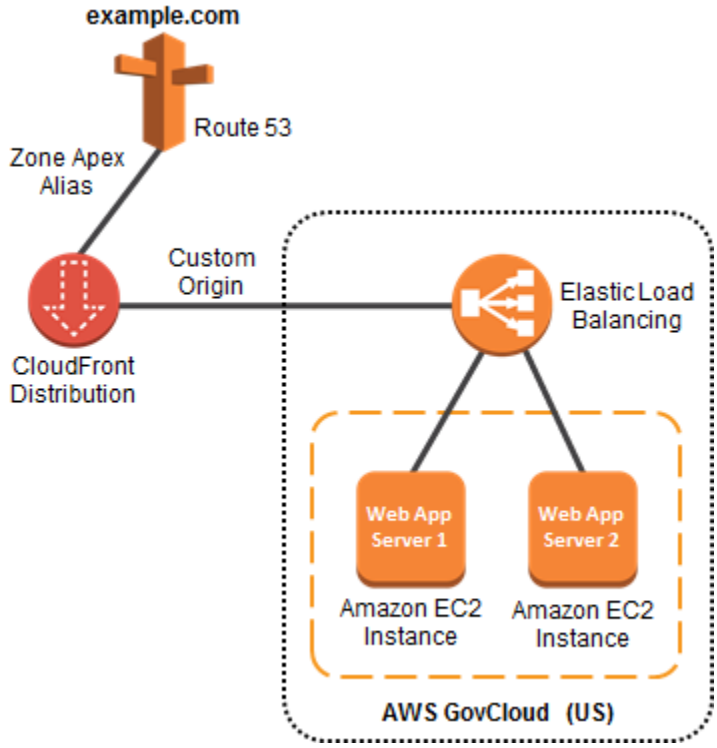
Additionally, Route 53 supports the alias resource record set, which lets you map your zone apex (e.g. example.com) DNS name to your load balancer DNS name. IP addresses associated with Elastic Load Balancing can change at any time due to scaling or software updates. Route 53 responds to each request 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:

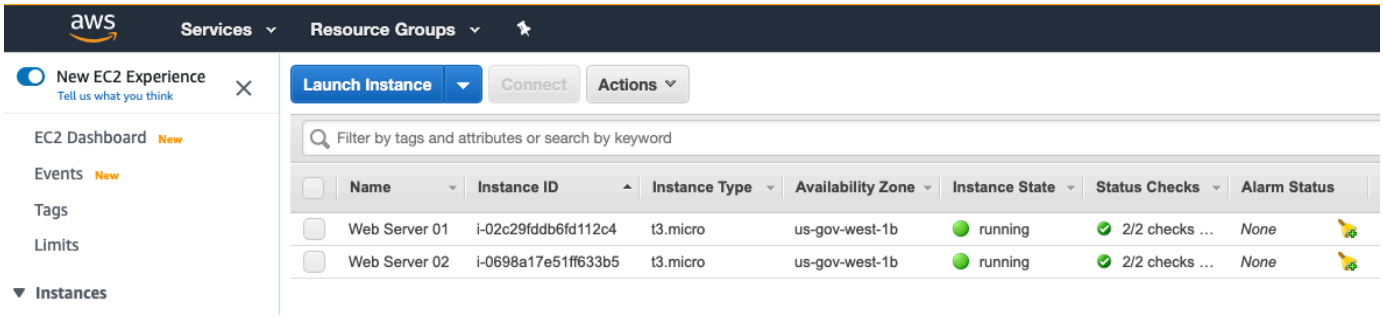


Step 1: Sign Up for AWS GovCloud (US)

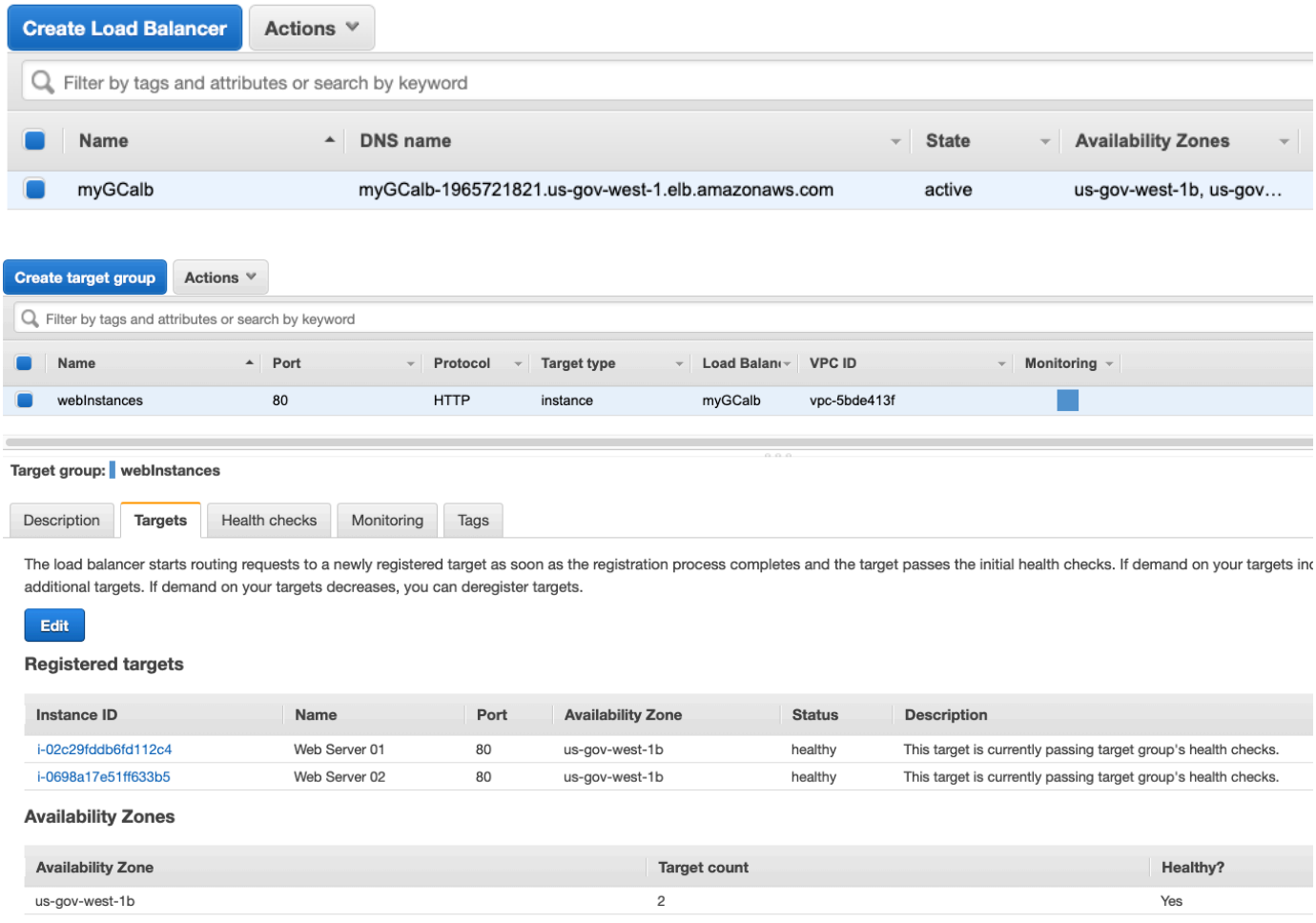
- To use AWS services in the AWS GovCloud (US) Regions, you must have an AWS GovCloud (US) account. If you don't have an account, see AWS GovCloud (US) Sign Up for more information.

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.

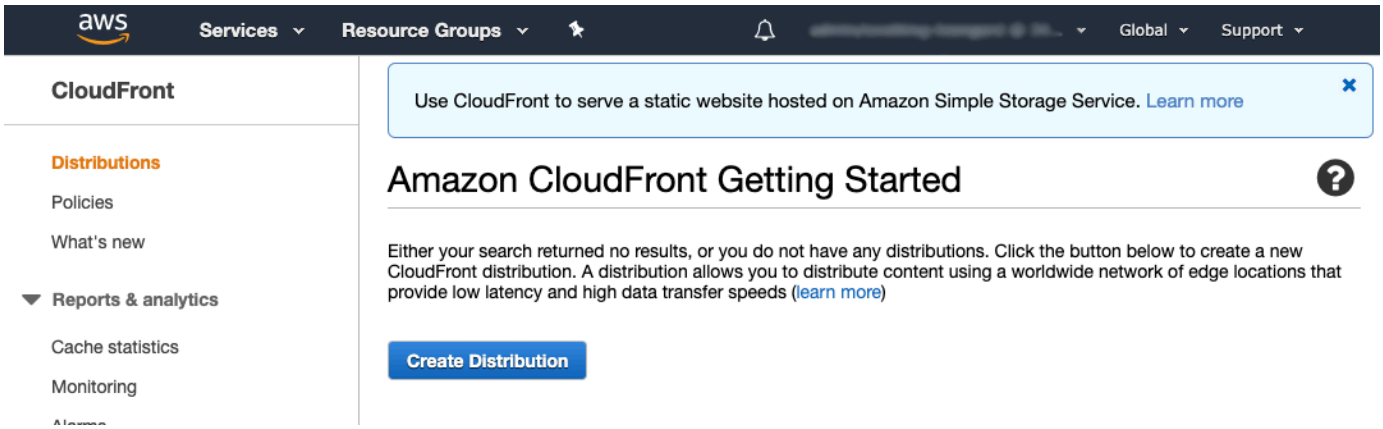


3. Test access to your website by entering the load balancer DNS name in a web browser. You can verify the load balancer is balancing traffic between the two instances by waiting at least one minute between requests.

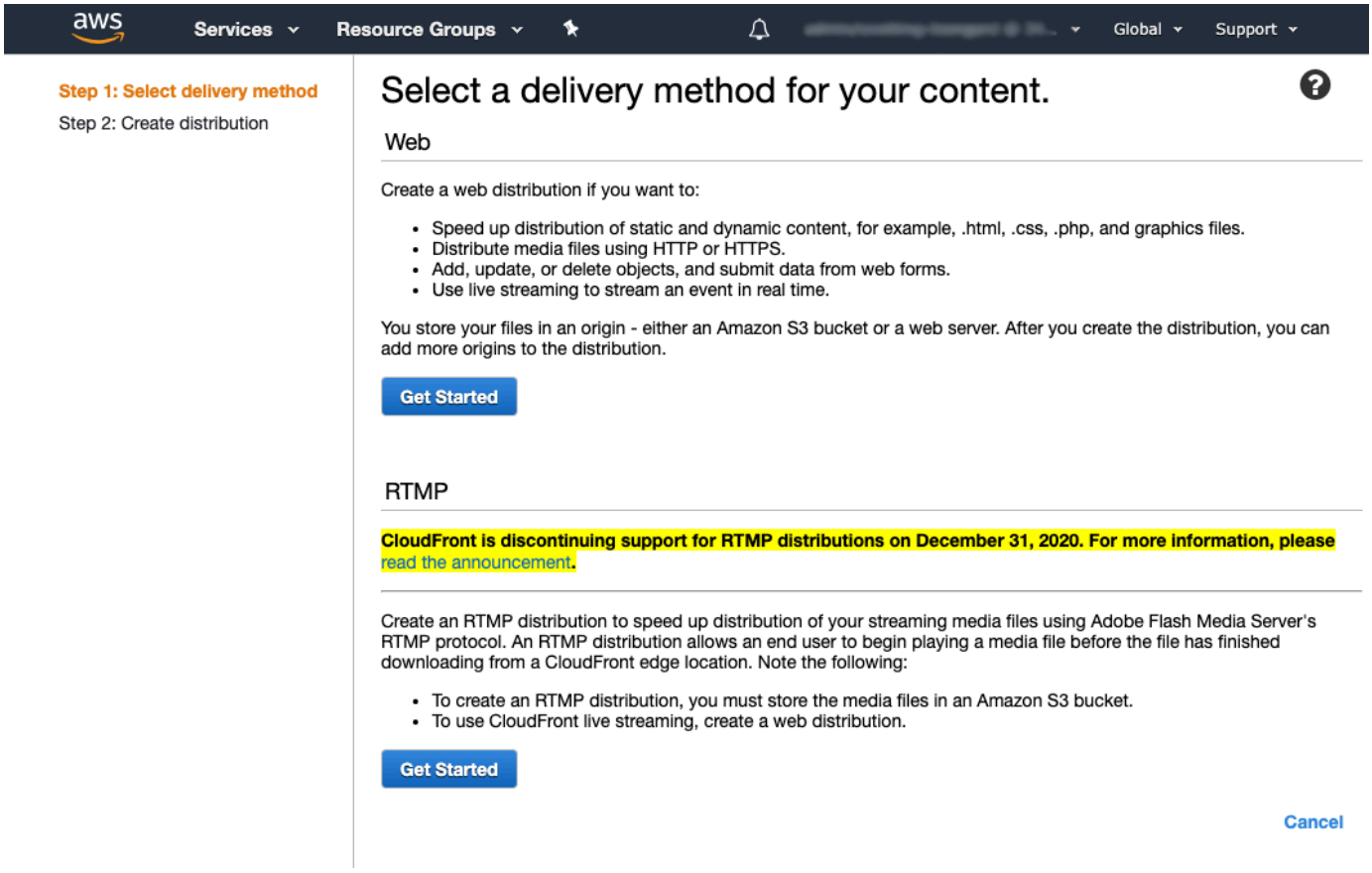
Step 3: Create a CloudFront Custom Origin Web Distribution

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.

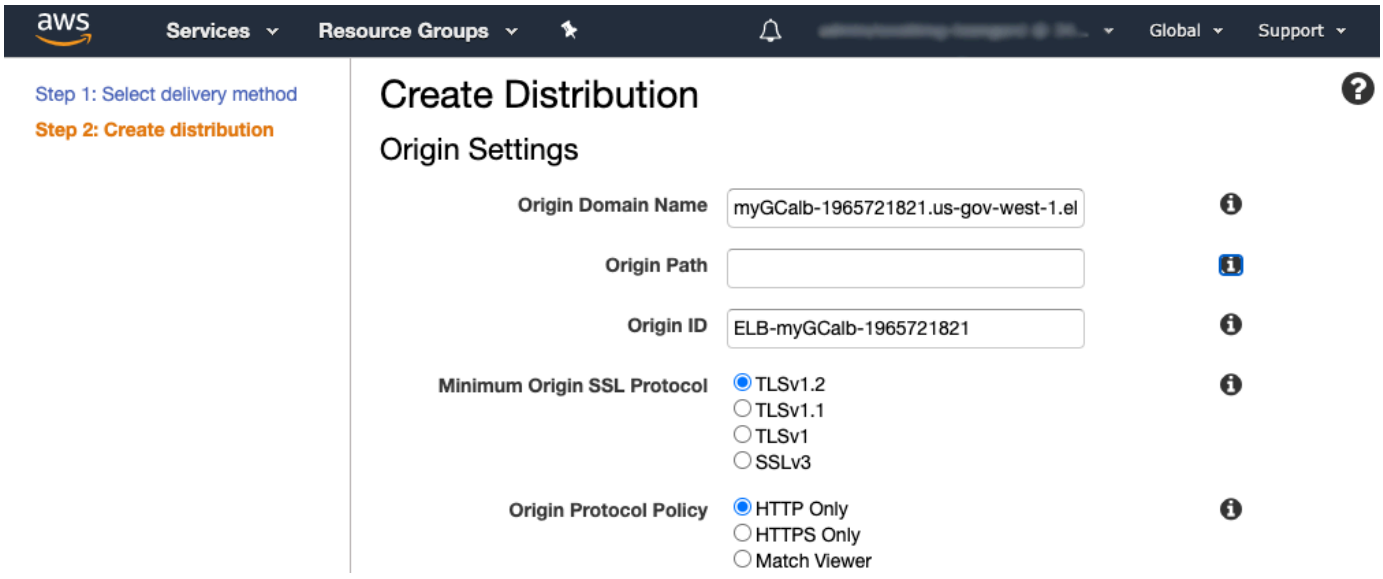
1. Sign in to the CloudFront console with your standard AWS account, and choose **Create Distribution**.



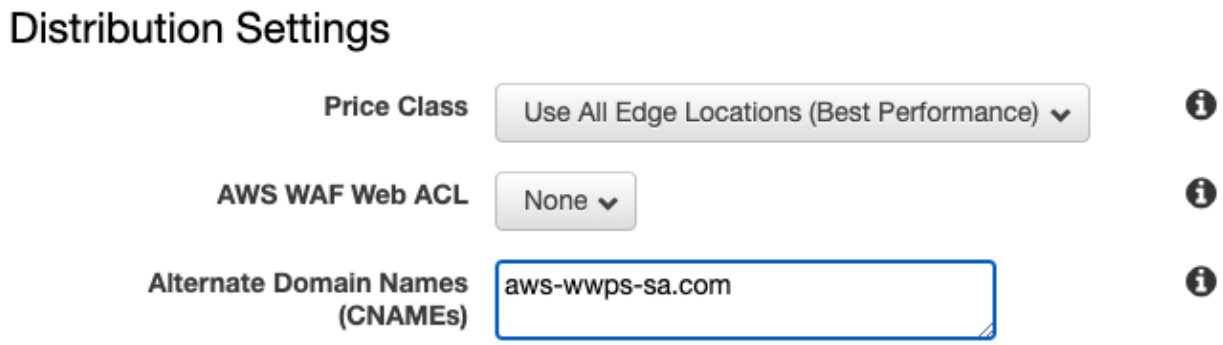
2. Select the **Get Started** under **Web** distribution delivery method, and then choose **Continue**.



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

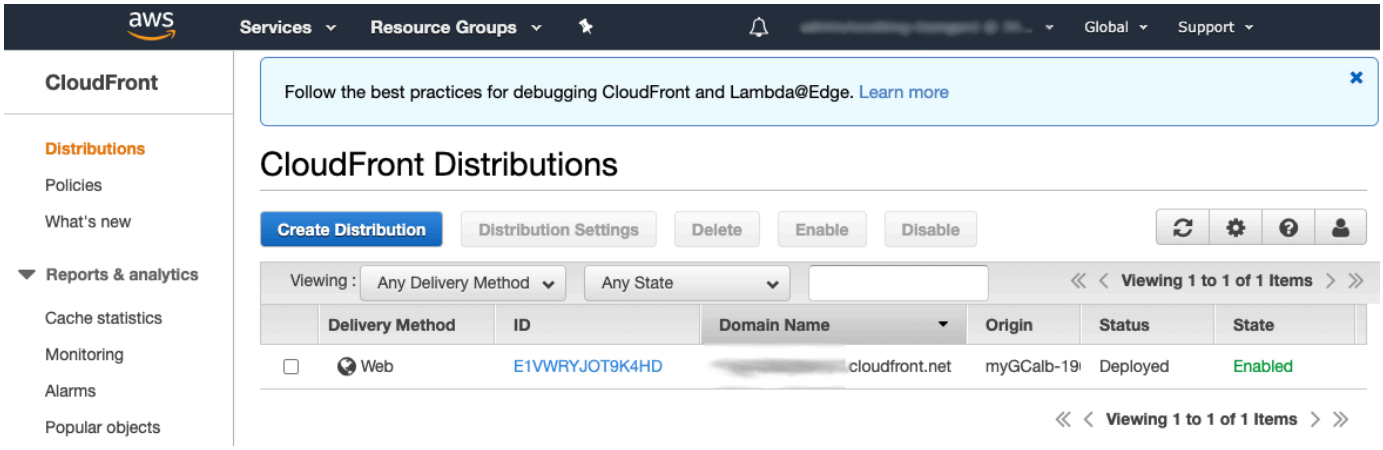


4. In **Alternate Domain Names (CNAMEs)**, add the zone apex name. Note you must attach a trusted certificate that validates your authorization to use the domain name.



5. Choose **Create Distribution**.

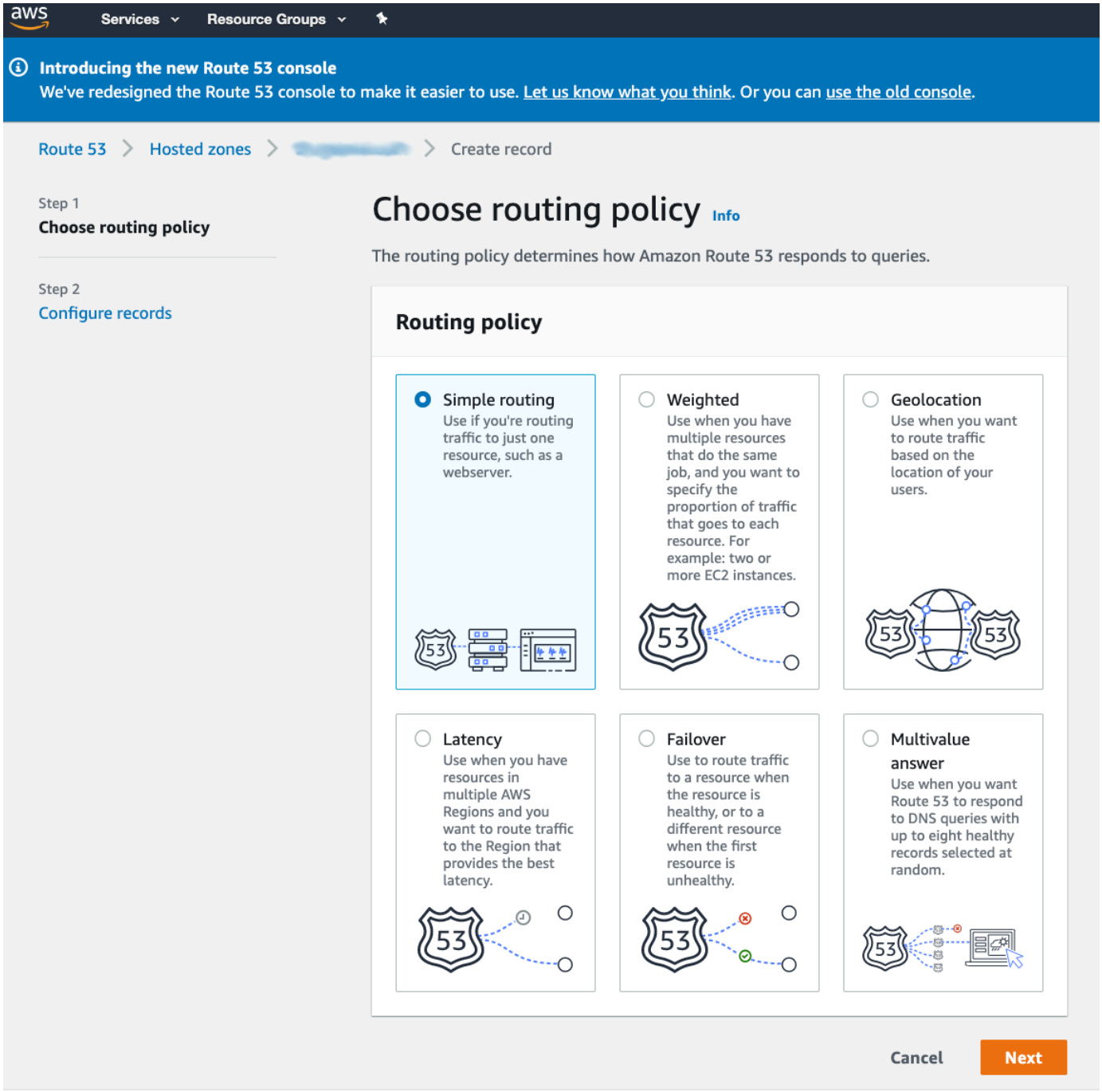
6. After the status for the new distribution changes to **Deployed**, make a note of the domain name. You will use this domain name when you set up Route 53 in the next step.



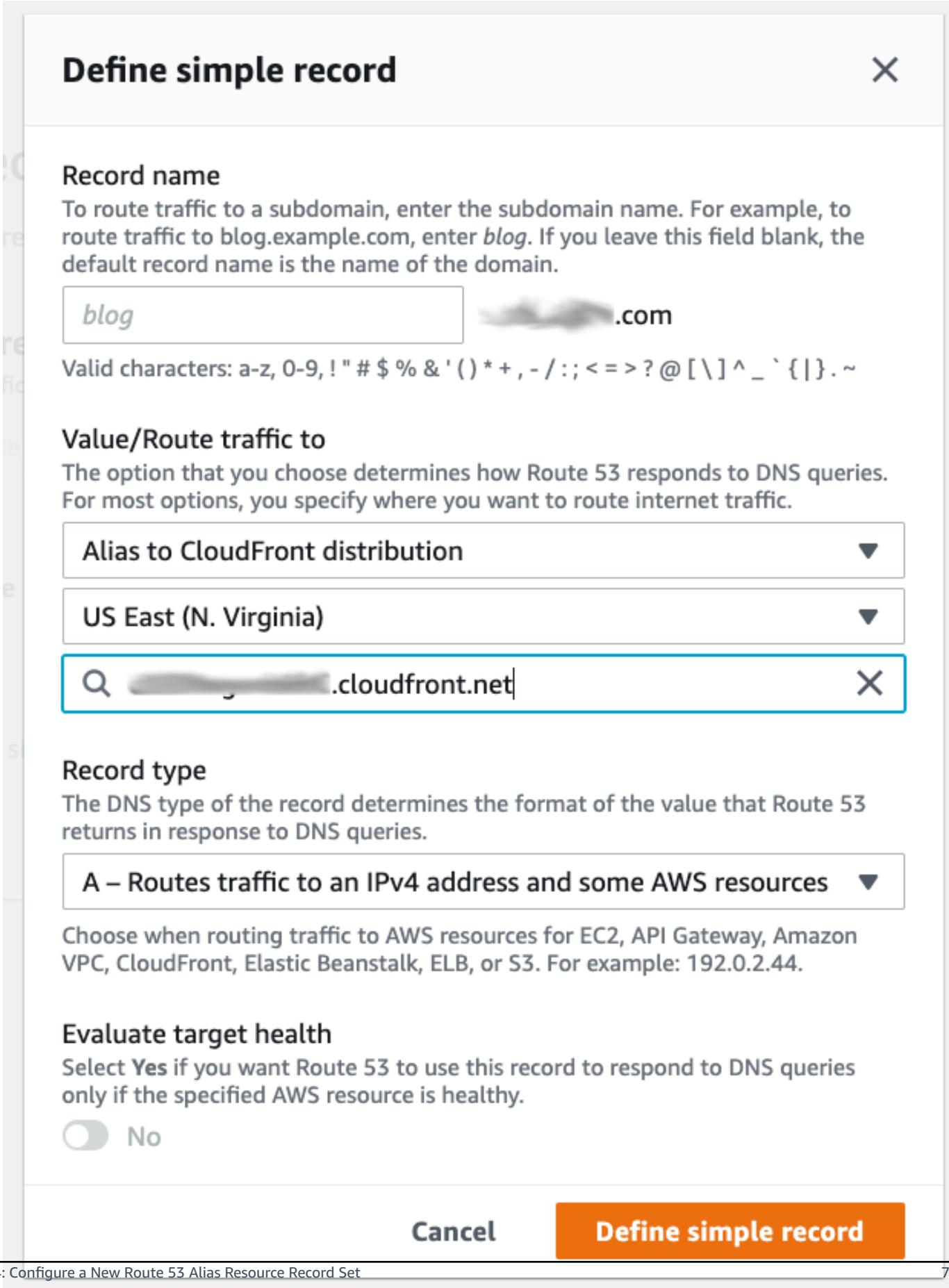
For information about how CloudFront processes and forwards requests to a customer origin server, such as an AWS GovCloud (US) load balancer, see the CloudFront documentation.

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.



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
Record name
To route traffic to a subdomain, enter the subdomain name. For example, to route traffic to blog.example.com, enter blog. If you leave this field blank, the default record name is the name of the domain.
blog
.com
Valid characters: a-z, 0-9, ! " # $ % & ' ( ) * + , - / : ; < = > ? @ [\ ] ^ _ ` { | } . ~
Value/Route traffic to
The option that you choose determines how Route 53 responds to DNS queries. For most options, you specify where you want to route internet traffic.
Alias to CloudFront distribution
US East (N. Virginia)
.cloudfront.net
Record type
The DNS type of the record determines the format of the value that Route 53 returns in response to DNS queries.
A – Routes traffic to an IPv4 address and some AWS resources
Choose when routing traffic to AWS resources for EC2, API Gateway, Amazon VPC, CloudFront, Elastic Beanstalk, ELB, or S3. For example: 192.0.2.44.
Evaluate target health
Select Yes if you want Route 53 to use this record to respond to DNS queries only if the specified AWS resource is healthy.
No
Cancel
Define simple record

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. For CLI and SDK calls, the Region names are us-gov-west-1 and us-gov-east-1.

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

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 you to specify a Region:

- For the AWS GovCloud (US-West) Region, use `us-gov-west-1`.
- For AWS GovCloud (US-East) Region, use `us-gov-east-1`.

For additional information about ARNs, see Amazon Resource Names (ARNs) in the *AWS General Reference*.

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. These HTTPS endpoints are referred to as the control plane used to configure AWS services.

If you require FIPS 140-2 compliance you should use the FIPS Endpoints linked in the following section. For more information about FIPS 140-2, see "Cryptographic Module Validation Program" on the NIST Computer Security Resource Center website.

If you require the use of FIPS 140-2 validated modules for TLS termination performed on the data plane of the Application Load Balancer HTTPS Listeners, have your account team reach out to the Elastic Load Balancing team.

FIPS-140-2 validated modules in the data plane of Amazon Relational Database Service (Amazon RDS) SSL can be configured for certain database engines. For more information about RDS SSL, see the Amazon RDS User Guide.

FIPS Endpoints for the AWS GovCloud (US) Regions

For a list of all GovCloud AWS FIPS endpoints, see *AWS GovCloud (US)* in FIPS Endpoints by Service.

Endpoints for AWS Services

For a list of AWS endpoints, see View the service endpoints in the *AWS General Reference*.

Regions for AWS Services

For a list of AWS Regions, see Regional endpoints in the *AWS General Reference*.

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.

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.

AWS Service	AWS GovCloud (US-West) VPC Endpoints	AWS GovCloud (US-East) VPC Endpoints
Application Auto Scaling	com.amazonaws.us-gov-west-1.application-autoscaling	com.amazonaws.us-gov-east-1.application-autoscaling
AWS Auto Scaling	com.amazonaws.us-gov-west-1.autoscaling-plans	com.amazonaws.us-gov-east-1.autoscaling-plans
AWS Application Migration Service	com.amazonaws.us-gov-west-1.mgn	com.amazonaws.us-gov-east-1.mgn

AWS Service	AWS GovCloud (US-West) VPC Endpoints	AWS GovCloud (US-East) VPC Endpoints
AWS Backup	com.amazonaws.us-gov-west-1.backup com.amazonaws.us-gov-west-1.backup-gateway	com.amazonaws.us-gov-east-1.backup com.amazonaws.us-gov-east-1.backup-gateway
AWS Batch	com.amazonaws.us-gov-west-1.batch	com.amazonaws.us-gov-east-1.batch
AWS CloudHSM	com.amazonaws.us-gov-west-1.cloudhsmv2	com.amazonaws.us-gov-east-1.cloudhsmv2
AWS CodeBuild	com.amazonaws.us-gov-west-1.codebuild com.amazonaws.us-gov-west-1.codebuild-fips	com.amazonaws.us-gov-east-1.codebuild com.amazonaws.us-gov-east-1.codebuild-fips
AWS CodeStar Connections	com.amazonaws.us-gov-east-1.codestar-connections	codestar-connections.us-gov-east-1.amazonaws.com
AWS CloudFormation	com.amazonaws.us-gov-west-1.cloudformation	com.amazonaws.us-gov-east-1.cloudformation
AWS CloudTrail	com.amazonaws.us-gov-west-1.cloudtrail	com.amazonaws.us-gov-east-1.cloudtrail
AWS CodeCommit	com.amazonaws.us-gov-west-1.codecommit com.amazonaws.us-gov-west-1.codecommit-fips	com.amazonaws.us-gov-east-1.codecommit com.amazonaws.us-gov-east-1.codecommit-fips
AWS CodePipeline	com.amazonaws.us-gov-west-1.codepipeline	Not applicable

AWS Service	AWS GovCloud (US-West) VPC Endpoints	AWS GovCloud (US-East) VPC Endpoints
AWS Config	com.amazonaws.us-gov-west-1.config	com.amazonaws.us-gov-east-1.config
AWS Database Migration Service	com.amazonaws.us-gov-west-1.dms	com.amazonaws.us-gov-east-1.dms
AWS DataSync	com.amazonaws.us-gov-west-1.datasync	com.amazonaws.us-gov-east-1.datasync
AWS Direct Connect	com.amazonaws.us-gov-west-1.directconnect	com.amazonaws.us-gov-east-1.directconnect
AWS Directory Service	com.amazonaws.us-gov-west-1.ds	com.amazonaws.us-gov-east-1.ds
AWS Elastic Beanstalk	com.amazonaws.us-gov-west-1.elasticbeanstalk com.amazonaws.us-gov-west-1.elasticbeanstalk-health	com.amazonaws.us-gov-east-1.elasticbeanstalk com.amazonaws.us-gov-east-1.elasticbeanstalk-health
AWS Elastic Disaster Recovery	com.amazonaws.us-gov-west-1.drs	com.amazonaws.us-gov-east-1.drs
AWS Fault Injection Service	com.amazonaws.us-gov-west-1.fis	com.amazonaws.us-gov-east-1.fis
AWS Glue	com.amazonaws.us-gov-west-1.glue	com.amazonaws.us-gov-east-1.glue
AWS Glue DataBrew	com.amazonaws.us-gov-west-1.databrew	Not applicable
AWS IAM Access Analyzer	com.amazonaws.us-gov-west-1.access-analyzer	com.amazonaws.us-gov-east-1.access-analyzer

AWS Service	AWS GovCloud (US-West) VPC Endpoints	AWS GovCloud (US-East) VPC Endpoints
AWS IoT Greengrass	com.amazonaws.us-gov-west-1.greengrass	com.amazonaws.us-gov-east-1.greengrass
AWS IoT SiteWise	com.amazonaws.us-gov-west-1.iotsitewise.api com.amazonaws.us-gov-west-1.iotsitewise.data	Not applicable
AWS IoT TwinMaker	com.amazonaws.us-gov-west-1.iottwinmaker.api com.amazonaws.us-gov-west-1.iottwinmaker.data	Not applicable
AWS Key Management Service	com.amazonaws.us-gov-west-1.kms com.amazonaws.us-gov-west-1.kms-fips	com.amazonaws.us-gov-east-1.kms com.amazonaws.us-gov-east-1.kms-fips
AWS Lake Formation	com.amazonaws.us-gov-west-1.lakeformation	Not applicable
AWS Lambda	com.amazonaws.us-gov-west-1.lambda	com.amazonaws.us-gov-east-1.lambda
AWS License Manager	com.amazonaws.us-gov-west-1.license-manager com.amazonaws.us-gov-west-1.license-manager-fips	com.amazonaws.us-gov-east-1.license-manager com.amazonaws.us-gov-east-1.license-manager-fips

AWS Service	AWS GovCloud (US-West) VPC Endpoints	AWS GovCloud (US-East) VPC Endpoints
AWS Mainframe Modernization	com.amazonaws.us-gov-west-1.m2 m2.us-gov-west-1.amazonaws.com	com.amazonaws.us-gov-east-1.m2 m2.us-gov-east-1.amazonaws.com
AWS Resilience Hub	resiliencehub.us-gov-west-1.amazonaws.com	resiliencehub.us-gov-east-1.amazonaws.com
AWS SDK for SAP ABAP	com.amazonaws.us-gov-west-1.awssdk-sapabap com.amazonaws.us-gov-west-1.sapabap	com.amazonaws.us-gov-east-1.awssdk-sapabap com.amazonaws.us-gov-east-1.sapabap
AWS Secrets Manager	com.amazonaws.us-gov-west-1.secretsmanager	com.amazonaws.us-gov-east-1.secretsmanager
AWS Security Hub	com.amazonaws.us-gov-west-1.securityhub	com.amazonaws.us-gov-east-1.securityhub
AWS Security Token Service	com.amazonaws.us-gov-west-1.sts	com.amazonaws.us-gov-east-1.sts
AWS Server Migration Service	com.amazonaws.us-gov-west-1.sms com.amazonaws.us-gov-west-1.sms-fips	com.amazonaws.us-gov-east-1.sms com.amazonaws.us-gov-east-1.sms-fips
AWS Service Catalog	com.amazonaws.us-gov-west-1.servicecatalog	com.amazonaws.us-gov-east-1.servicecatalog
AWS Service Catalog AppRegistry	com.amazonaws.us-gov-west-1.servicecatalog-appregistry	com.amazonaws.us-gov-east-1.servicecatalog-appregistry

AWS Service	AWS GovCloud (US-West) VPC Endpoints	AWS GovCloud (US-East) VPC Endpoints
AWS SimSpace Weaver	com.amazonaws.us-gov-west-1.simspaceweaver	com.amazonaws.us-gov-east-1.simspaceweaver
AWS Storage Gateway	com.amazonaws.us-gov-west-1.storagegateway	com.amazonaws.us-gov-east-1.storagegateway
AWS Systems Manager	com.amazonaws.us-gov-west-1.ssm com.amazonaws.us-gov-west-1.ssmmessages	com.amazonaws.us-gov-east-1.ssm com.amazonaws.us-gov-east-1.ssmmessages
AWS Transfer Family	com.amazonaws.us-gov-west-1.transfer	com.amazonaws.us-gov-east-1.transfer
AWS X-Ray	com.amazonaws.us-gov-west-1.xray	com.amazonaws.us-gov-east-1.xray
Amazon API Gateway	com.amazonaws.us-gov-west-1.execute-api	com.amazonaws.us-gov-east-1.execute-api
Amazon AppStream 2.0	com.amazonaws.us-gov-west-1.appstream.api com.amazonaws.us-gov-west-1.appstream.streaming	com.amazonaws.us-gov-east-1.appstream.api com.amazonaws.us-gov-east-1.appstream.streaming
Amazon Athena	com.amazonaws.us-gov-west-1.athena	com.amazonaws.us-gov-east-1.athena
Amazon Bedrock	bedrock.gov-us-west-1.amazonaws.com	bedrock-runtime.gov-us-west-1.amazonaws.com
Amazon Cloud Directory	com.amazonaws.us-gov-west-1.clouddirectory	Not applicable

AWS Service	AWS GovCloud (US-West) VPC Endpoints	AWS GovCloud (US-East) VPC Endpoints
Amazon CloudWatch Logs	com.amazonaws.us-gov-west-1.logs	com.amazonaws.us-gov-east-1.logs
Amazon Comprehend	com.amazonaws.us-gov-west-1.comprehend	Not applicable
Amazon Comprehend Medical	com.amazonaws.us-gov-west-1.comprehendmedical	Not applicable
Amazon DynamoDB	com.amazonaws.us-gov-west-1.dynamodb	com.amazonaws.us-gov-east-1.dynamodb
Amazon EC2 Auto Scaling	com.amazonaws.us-gov-west-1.autoscaling	com.amazonaws.us-gov-east-1.autoscaling
Amazon ElastiCache	com.amazonaws.us-gov-west-1.elasticache	com.amazonaws.us-gov-east-1.elasticache
Amazon Elastic Compute Cloud	com.amazonaws.us-gov-west-1.ec2 com.amazonaws.us-gov-west-1.ec2messages	com.amazonaws.us-gov-east-1.ec2 com.amazonaws.us-gov-east-1.ec2messages
Amazon Elastic Container Registry	com.amazonaws.us-gov-west-1.ecr.api com.amazonaws.us-gov-west-1.ecr.dkr	com.amazonaws.us-gov-east-1.ecr.api com.amazonaws.us-gov-east-1.ecr.dkr

AWS Service	AWS GovCloud (US-West) VPC Endpoints	AWS GovCloud (US-East) VPC Endpoints
Amazon Elastic Container Service	com.amazonaws.us-gov-west-1.ecs com.amazonaws.us-gov-west-1.ecs-agent com.amazonaws.us-gov-west-1.ecs-telemetry	com.amazonaws.us-gov-east-1.ecs com.amazonaws.us-gov-east-1.ecs-agent com.amazonaws.us-gov-east-1.ecs-telemetry
Amazon Elastic File System	com.amazonaws.us-gov-west-1.elasticfilesystem com.amazonaws.us-gov-west-1.elasticfilesystem-fips	com.amazonaws.us-gov-east-1.elasticfilesystem com.amazonaws.us-gov-east-1.elasticfilesystem-fips
Amazon EMR	com.amazonaws.us-gov-west-1.elasticmapreduce	com.amazonaws.us-gov-east-1.elasticmapreduce
Amazon FSx	com.amazonaws.us-gov-west-1.fsx com.amazonaws.us-gov-west-1.fsx-fips	com.amazonaws.us-gov-east-1.fsx com.amazonaws.us-gov-east-1.fsx-fips
Amazon Inspector	com.amazonaws.us-gov-west-1.inspector2 inspector2.us-gov-west-1.amazonaws.com	com.amazonaws.us-gov-east-1.inspector2 inspector2.us-gov-east-1.amazonaws.com
Amazon Kendra	com.amazonaws.us-gov-west-1.kendra	Not applicable
Amazon Keyspaces (for Apache Cassandra)	com.amazonaws.us-gov-west-1.cassandra	com.amazonaws.us-gov-east-1.cassandra

AWS Service	AWS GovCloud (US-West) VPC Endpoints	AWS GovCloud (US-East) VPC Endpoints
Amazon Data Firehose	com.amazonaws.us-gov-west-1.kinesis-firehose	com.amazonaws.us-gov-east-1.kinesis-firehose
Amazon Kinesis Data Streams	com.amazonaws.us-gov-west-1.kinesis-streams	com.amazonaws.us-gov-east-1.kinesis-streams
"Amazon Location Service	com.amazonaws.us-gov-west-1.geo	
Amazon QuickSight	quicksight.us-gov-west-1.amazonaws.com	Not applicable
Amazon Redshift	com.amazonaws.us-gov-west-1.redshift com.amazonaws.us-gov-west-1.redshift-data	com.amazonaws.us-gov-east-1.redshift com.amazonaws.us-gov-east-1.redshift-data
Amazon Rekognition	com.amazonaws.us-gov-west-1.rekognition com.amazonaws.us-gov-west-1.rekognition-fips	Not applicable
Amazon Relational Database Service	com.amazonaws.us-gov-west-1.rds	com.amazonaws.us-gov-east-1.rds
Amazon Route 53 Application Recovery Controller	PDT/us-gov-west-1: arc-zonal-shift.us-gov-west-1.amazonaws.com	OSU/us-gov-east-1: arc-zonal-shift.us-gov-east-1.amazonaws.com

AWS Service	AWS GovCloud (US-West) VPC Endpoints	AWS GovCloud (US-East) VPC Endpoints
Amazon SageMaker	com.amazonaws.us-gov-west-1.sagemaker.api com.amazonaws.us-gov-west-1.sagemaker.runtime aws.sagemaker.us-gov-west-1.notebook	Not Applicable
Amazon Simple Notification Service	com.amazonaws.us-gov-west-1.sns	com.amazonaws.us-gov-east-1.sns
Amazon Simple Queue Service	com.amazonaws.us-gov-west-1.sqs	com.amazonaws.us-gov-east-1.sqs
Amazon Simple Storage Service	com.amazonaws.us-gov-west-1.s3	com.amazonaws.us-gov-east-1.s3
Amazon SWF	com.amazonaws.us-gov-west-1.swf	com.amazonaws.us-gov-east-1.swf
Amazon Textract	com.amazonaws.us-gov-west-1.textract	com.amazonaws.us-gov-east-1.textract
Amazon Timestream	com.amazonaws.us-gov-west-1.timestream	Not Applicable
Amazon Transcribe	com.amazonaws.us-gov-west-1.transcribe	com.amazonaws.us-gov-east-1.transcribe
Amazon WorkSpaces	com.amazonaws.us-gov-west-1.workspaces	Not applicable
EBS direct APIs	com.amazonaws.us-gov-west-1.ebs	com.amazonaws.us-gov-east-1.ebs

AWS Service	AWS GovCloud (US-West) VPC Endpoints	AWS GovCloud (US-East) VPC Endpoints
EC2 Image Builder	com.amazonaws.us-gov-west-1.imagebuilder	com.amazonaws.us-gov-east-1.imagebuilder
Elastic Load Balancing	com.amazonaws.us-gov-west-1.elasticloadbalancing	com.amazonaws.us-gov-east-1.elasticloadbalancing
Git CodeCommit	com.amazonaws.us-gov-west-1.git-codecommit com.amazonaws.us-gov-west-1.git-codecommit-fips	com.amazonaws.us-gov-east-1.git-codecommit com.amazonaws.us-gov-east-1.git-codecommit-fips
S3 on Outposts	com.amazonaws.us-gov-west-1.s3-outposts	com.amazonaws.us-gov-east-1.s3-outposts
Service Quotas	com.amazonaws.us-gov-west-1.servicequotas	com.amazonaws.us-gov-east-1.servicequotas

Note

All the information provided in this page is manually updated. If you are looking for the most current version of the list, it can be found in the console or by using the AWS CLI command **"aws ec2 describe-vpc-endpoint-services --region us-gov-east-1 or --region us-gov-west-1"** as appropriate.

Compliance

AWS GovCloud (US) gives government customers and their partners the flexibility to architect secure cloud solutions that comply with the FedRAMP High baseline; the DOJ's Criminal Justice Information Systems (CJIS) Security Policy; U.S. International Traffic in Arms Regulations (ITAR); Export Administration Regulations (EAR); Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) for Impact Levels 2, 4 and 5; FIPS 140-2; IRS-1075; and other compliance regimes.

FedRAMP

The US Federal Government is dedicated to delivering its services to the American people in the most innovative, secure, and cost-efficient fashion. Cloud computing plays a key part in how the federal government can achieve operational efficiencies and innovate on demand to advance their mission across the nation. That is why many federal agencies today are using AWS cloud services to process, store, and transmit federal government data. For more information, see https://aws.amazon.com/compliance/fedramp

DoD CC SRG

A growing number of military customers are adopting AWS services to process, store, and transmit US Department of Defense (DoD) data. AWS enables defense organizations and their business associates to create secure environments to process, maintain, and store DoD data. For more information, see https://aws.amazon.com/compliance/dod

CMMC

The Cybersecurity Maturity Model Certification (CMMC) program enhances cyber protection standards for companies in the DIB. It is designed to protect sensitive unclassified information that is shared by the DoD with its contractors and subcontractors. The program incorporates a set of cybersecurity requirements into acquisition programs and provides the DoD increased assurance that contractors and subcontractors are meeting these requirements. For more information, see https://aws.amazon.com/compliance/cmmc

ITAR

AWS GovCloud (US) supports compliance with United States International Traffic in Arms Regulations (ITAR). As a part of managing a comprehensive ITAR compliance program, companies that are subject to ITAR export regulations must control unintended exports by restricting access to protected data to US Persons, and by restricting physical location of protected data to the US. AWS GovCloud (US) provides an environment that is physically located in the US, and access by AWS personnel is limited to US Persons, thereby allowing qualified companies to use AWS to transmit, process, and store protected articles and data subject to ITAR restrictions. For more information, see https://aws.amazon.com/compliance/itar

CJIS

The CJIS Security Policy outlines the "appropriate controls to protect the full lifecycle of CJI (Criminal Justice Information), whether at rest or in transit," irrespective of the underlying information technology model. For more information, see https://aws.amazon.com/compliance/cjis

IRS 1075

Internal Revenue Service Publication 1075 (IRS Pub 1075) provides guidance for US government agencies and their agents to protect Federal Tax Information (FTI). While the IRS does not publish an official designation or certification for compliance with Pub 1075, AWS supports organizations to protect FTI managed in AWS by aligning our implementations of NIST 800-53 and FedRAMP security controls with the respective IRS Pub 1075 security requirements. For more information, see https://aws.amazon.com/compliance/irs-1075

FIPS

The Federal Information Processing Standard (FIPS) Publication 140-2 is a US and Canadian government standard that specifies the security requirements for cryptographic modules that protect sensitive information. For more information, see https://aws.amazon.com/compliance/fips

ATO on AWS

The Authority to Operate (ATO) on AWS Program helps AWS Partners meet their customers' authorization needs, whether it be architecting, configuring, deploying, or integrating tools and controls. AWS supports businesses globally that need to meet security, privacy, and compliance requirements for healthcare, privacy, national security, and financial sectors. ATO on AWS supports workloads for government organizations such as FedRAMP, FISMA, the RMF, and CMMC in the U.S. For more information, see https://aws.amazon.com/partners/programs/ato

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.

Export Controlled Data in AWS GovCloud (US) Services

If you maintain export-controlled data in the AWS GovCloud (US) Regions, you are responsible for using services in the AWS GovCloud (US) Regions in a manner that is consistent with your obligations under applicable laws and regulations, including export control regulations. For more information about maintaining export controlled data in AWS GovCloud (US) Regions for each service, see the service-specific information in Services in AWS GovCloud (US) Regions.

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).
- 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 SDK**s 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/.

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. AWS GovCloud (US) Sign Up discusses how you create your first IAM administrative user.

Because of the shared responsibility model, customers are responsible for determining who should or should not access the AWS GovCloud (US) console, in accordance with the customer compliance requirements.

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, users need programmatic access.

Users need programmatic access if they want to interact with AWS outside of the AWS Management Console. The way to grant programmatic access depends on the type of user that's accessing AWS.

To grant users programmatic access, choose one of the following options.

Which user needs programmatic access?	To	By
Workforce identity (Users managed in IAM Identity Center)	Use temporary credentials to sign programmatic requests to the AWS CLI, AWS SDKs, or AWS APIs.	Following the instructions for the interface that you want to use. • For the AWS CLI, see Configuring the AWS CLI to use AWS IAM Identity Center in the *AWS Command Line Interface User Guide*. • For AWS SDKs, tools, and AWS APIs, see IAM Identity Center authentication in the *AWS SDKs and Tools Reference Guide*.
IAM	Use temporary credentials to sign programmatic requests to the AWS CLI, AWS SDKs, or AWS APIs.	Following the instructions in Using temporary credentials with AWS resources in the *IAM User Guide*.

Which user needs programmatic access?	To	By
IAM	(Not recommended) Use long-term credentials to sign programmatic requests to the AWS CLI, AWS SDKs, or AWS APIs.	Following the instructions for the interface that you want to use. • For the AWS CLI, see Authenticating using IAM user credentials in the *AWS Command Line Interface User Guide*. • For AWS SDKs and tools, see Authenticate using long-term credentials in the *AWS SDKs and Tools Reference Guide*. • For AWS APIs, see Managing access keys for IAM users in the *IAM User Guide*.

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.

```
#Example Call
aws s3 ls --endpoint-url https://s3-fips.us-gov-west-1.amazonaws.com --region us-gov-
west-1
```

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 (US) 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.

Use the following AWS GovCloud (US) account closure procedure that is most applicable to your business needs.

Close an AWS GovCloud (US) standalone or member account

You can close an AWS GovCloud (US) standalone or member account by initiating closure of its associated standard account.

To close an AWS GovCloud (US) standalone or member account

1. Sign in to the AWS GovCloud (US) account.
2. Find and terminate all active resources currently running in the AWS GovCloud (US) account (both Regions if applicable).

   Important

   Before terminating your resources, back up your data where appropriate. After your account has been closed, you will no longer have access to the data or AWS services.

3. After you've terminated all active resources from your AWS GovCloud (US) account, delete all IAM users, and rotate and delete the access keys from the AWS GovCloud (US) account.
4. Close the standard AWS account using the **Close account** option available in the standard account Management Console. After the standard AWS account closure, your AWS GovCloud (US) account will close within the next billing cycle.

   If you run into issues with billing/access to the AWS GovCloud (US) Management Console after this time, please submit an AWS Support case using your standard AWS account, referencing the issue and the AWS GovCloud (US) account ID.

Notes

- Closing your standard AWS account will not automatically terminate all your active resources in the AWS GovCloud (US) account. You might continue to incur charges for usage of any active resources in the AWS GovCloud (US) account until it is closed within the next billing cycle after your standard AWS account closure. To prevent this, make sure that all the resources in your AWS GovCloud (US) account are terminated before closing the standard AWS account.
- Closed AWS GovCloud (US) member accounts are not automatically removed from the AWS GovCloud (US) organization after the post-closure period and they remain visible in the AWS GovCloud (US) organization in suspended status. You must remove the AWS

GovCloud (US) member accounts from your AWS GovCloud (US) organization if you wish to delete your AWS GovCloud (US) organization.

Close an AWS GovCloud (US) management account

You can only close an AWS GovCloud (US) management account after you've deleted the organization associated with it. After deleting the organization, your management account will change to a standalone AWS GovCloud (US) account. At this point, you can initiate the closing of the standalone AWS GovCloud (US) account by closing its associated standard AWS account.

To close an AWS GovCloud (US) management account

1. Remove and close all the AWS GovCloud (US) member accounts from the AWS GovCloud (US) management account. For more information, see Removing a member account from your organization.

   Note

   Removing an AWS GovCloud (US) member account does not close the account, instead it removes the member account from the AWS GovCloud (US) organization and the member account becomes a standalone AWS account. If you wish to close the removed member accounts, follow the instructions in the previous section Close an AWS GovCloud (US) standalone or member account.

2. Sign in to the AWS GovCloud (US) management account and delete the AWS GovCloud (US) organization. For more information, see Deleting an organization.
3. Find and terminate all active resources, delete all IAM users, and rotate and delete the access keys of the AWS GovCloud (US) management account.
4. Close the standard management account associated with the AWS GovCloud (US) management account using the **Close account** option available in the standard account's Management Console. After the standard management account has been closed, your AWS GovCloud (US) management account will close within the next billing cycle. For more information, see Closing a member account in your organization.

Reopening an AWS GovCloud (US) account

Within the post-closure period, which are the 90 days after your account is closed, you can reopen your standard AWS account and AWS GovCloud (US) account by contacting AWS Support. For more information, see Accessing your AWS account during the post-closure period in the *AWS Account Management Guide*.

Important

Re-opening your AWS GovCloud (US) account will only restore data/resources that were not terminated. If you terminated resources to avoid incurring charges during the closure process, they will not be restored. To ensure access to important data that might be needed upon re-opening, it is recommended that you backup that data prior to terminating AWS GovCloud (US) resources.

After the post-closure period, you cannot reopen your standard AWS account or AWS GovCloud (US) account.

Services in AWS GovCloud (US) Regions

The following sections describe the differences between the AWS GovCloud (US) Regions and the standard AWS Region US East (N. Virginia). They include links to documentation and describe the export-controlled content (where you can and can't enter or process export-controlled data) for each service.

Topics

- AWS Compute Optimizer
- AWS Config
- AWS Control Tower
- AWS Database Migration Service
- AWS DataSync
- AWS Deep Learning AMIs
- AWS Direct Connect
- AWS Directory Service
- AWS Elastic Beanstalk
- AWS Elastic Disaster Recovery
- AWS Elemental MediaConvert
- AWS Fargate
- AWS Fault Injection Service
- AWS Firewall Manager
- AWS Glue
- AWS Health
- AWS IAM Identity Center
- AWS Identity and Access Management
- AWS IoT Core
- AWS IoT Device Defender
- AWS IoT Device Management
- AWS IoT Events
- AWS IoT Greengrass Version 1
- AWS IoT Greengrass Version 2
- AWS IoT SiteWise
- AWS IoT TwinMaker
- AWS Key Management Service
- AWS Lake Formation
- AWS Lambda

- AWS License Manager
- AWS Managed Services - AMS Accelerate
- AWS Management Console for the AWS GovCloud (US) Region
- AWS Mainframe Modernization
- AWS Marketplace
- AWS Modular Data Center
- AWS Network Firewall
- AWS Organizations
- AWS Outposts
- AWS ParallelCluster
- AWS Resilience Hub
- AWS Resource Access Manager
- AWS Resource Groups
- AWS RoboMaker
- AWS SDK for SAP ABAP
- AWS Secrets Manager
- AWS Security Hub
- Service Catalog
- AWS Serverless Application Repository
- AWS Server Migration Service
- AWS SimSpace Weaver
- AWS Site-to-Site VPN
- AWS Snow Family
- AWS Step Functions
- AWS Storage Gateway
- AWS Support
- AWS Systems Manager
- AWS Transfer Family
- AWS Trusted Advisor

- AWS Verified Access
- AWS WAF
- AWS Well-Architected Tool
- AWS WickrGov
- AWS X-Ray
- Amazon API Gateway
- Amazon AppStream 2.0
- Amazon Athena
- Amazon Aurora with MySQL and PostgreSQL compatibility
- Amazon Bedrock
- Amazon Chime SDK
- Amazon Cloud Directory
- Amazon CloudWatch
- Amazon CloudWatch Events
- Amazon CloudWatch Logs
- Amazon Cognito
- Amazon Comprehend
- Amazon Comprehend Medical
- Amazon Connect
- Amazon Detective
- Amazon DocumentDB (with MongoDB compatibility)
- Amazon DynamoDB
- Amazon EBS
- Amazon EC2
- Amazon EC2 Auto Scaling
- Amazon EC2 Image Builder
- Amazon EC2 VM Import/Export
- Amazon ECR
- Amazon ECS
- Amazon Elastic File System

- Amazon Elastic Kubernetes Service
- Amazon ElastiCache
- Amazon EMR
- Amazon EventBridge
- Amazon FSx
- Amazon GuardDuty
- Amazon Inspector Classic
- Amazon Inspector
- Amazon Kendra
- Amazon Keyspaces (for Apache Cassandra)
- Amazon Managed Service for Apache Flink
- Amazon Data Firehose
- Amazon Kinesis Data Streams
- Amazon Lex
- Amazon Location Service
- Amazon Managed Blockchain
- Amazon Managed Streaming for Apache Kafka (MSK)
- Amazon MQ
- Amazon Neptune
- Amazon OpenSearch Service
- Amazon Pinpoint
- Amazon Polly
- Amazon QuickSight
- Amazon RDS
- Amazon Redshift
- Amazon Rekognition
- Amazon Route 53
- Amazon Route 53 Application Recovery Controller
- Amazon S3
- Amazon S3 Glacier

- Amazon S3 on Outposts
- Amazon SageMaker
- Amazon SES
- Amazon SNS
- Amazon SQS
- Amazon SWF
- Amazon Textract
- Amazon Timestream
- Amazon Transcribe
- Amazon Translate
- Amazon VPC
- Amazon WorkSpaces
- Elastic Load Balancing
- Red Hat OpenShift Service on AWS
- Research and Engineering Studio on AWS
- Service Quotas
- VMware Cloud on AWS

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)

- Application Auto Scaling notifications are not currently supported in the AWS 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 Neptune clusters
  - ElastiCache for Redis clusters (replication groups)

- 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 Neptune clusters
  - ElastiCache for Redis clusters (replication groups)
  - 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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Auto Scaling is not permitted to contain export-controlled data.
- For example, do not enter export-controlled data in the following fields:
  - Scaling policy names
  - Scaling policy configuration

AWS AppConfig

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

How AWS AppConfig Differs for AWS GovCloud (US)

AWS CodePipeline resources are not currently supported for AWS AppConfig in the AWS GovCloud (US-East) Region.

Documentation for AWS AppConfig

AWS AppConfig documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Any AWS AppConfig resource names (Application, Environment, ConfigurationProfile, Deployment Strategy, etc.)
  - Validator JSON Schema
  - Location URIs or Validator ARNs
  - Any AWS AppConfig resource descriptions

AWS Application Migration Service

AWS Application Migration Service (MGN) is a highly automated lift-and-shift (rehost) solution that simplifies, expedites, and reduces the cost of migrating applications to AWS. It allows companies to lift-and-shift a large number of physical, virtual, or cloud servers without compatibility issues, performance disruption, or long cutover windows. MGN replicates source servers into your AWS account. When you're ready, it automatically converts and launches your servers on AWS so you

can quickly benefit from the cost savings, productivity, resilience, and agility of the Cloud. Once your applications are running on AWS, you can leverage AWS services and capabilities to quickly and easily replatform or refactor those applications – which makes lift-and-shift a fast route to modernization.

How AWS Application Migration Service differs for AWS GovCloud (US)

The following post-launch actions are not supported by Application Migration Service in AWS GovCloud (US):

- App2Container for Replatforming
- Enable Refactor Spaces

Documentation for AWS Application Migration Service

Application Migration Service documentation

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- No export-controlled data is entered, stored, or processed by Application Migration Service.

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Function name
- Description
- DLQ data (can be exported through Amazon SNS and Amazon SQS)
- Memory
- Timeout
- Runtime
- Role name for service principals
- Aliases

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 Differs 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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Auto Scaling is not permitted to contain export-controlled data.
- For example, do not enter export-controlled data in the following fields:
  - Scaling plan names
  - Scaling policy names
  - Scaling policy configurations

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

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)

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

Documentation for AWS Backup

AWS Backup documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Do not enter export-controlled data in the following AWS Backup fields:
  - Resource tag
  - Plan name
  - Rule name
  - Selection name
  - Vault name

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal

course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Job Definitions API attributes
- Job Queues API attributes
- Compute Environments API attributes
- Job API attributes
- Tags

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- No export-controlled data may be entered, stored, or processed by AWS Certificate Manager. For example, domain names specified for certificates are not permitted to contain export-controlled data. For example, do not enter export-controlled data into the **DomainName** or **SubjectAlternativeNames** fields when requesting a certificate.

AWS Private Certificate Authority

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

How AWS Private CA Differs for AWS GovCloud (US)

- Online Certificate Status Protocol (OCSP) is not supported in the AWS GovCloud (US) Regions.

Documentation for AWS Private CA

AWS Private Certificate Authority documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- No export-controlled data may be entered, stored, or processed by AWS Private Certificate Authority. For example, domain names specified for certificates are not permitted to contain export-controlled data. For example, do not enter export-controlled data into the **DomainName** or **SubjectAlternativeNames** fields when requesting a certificate.

AWS Client VPN

AWS Client VPN is a managed client-based AWS VPN service that enables you to securely access AWS resources and resources in your on-premises network. With AWS Client VPN, you can access your resources from any location using an OpenVPN-based VPN client.

How Client VPN Differs for AWS GovCloud (US)

- AWS Client VPN endpoints in AWS GovCloud (US) operate using FIPS 140-2 validated cryptographic modules. AWS VPN connections created in AWS GovCloud (US) 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 Client VPN

AWS Client VPN documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- AWS Client VPN metadata is not permitted to contain export-controlled data. This metadata includes all of the configuration data that you enter when setting up and maintaining your Client VPN Endpoints.

  For example, do not enter export-controlled data into user input fields such as the following:

  - Display Name
  - Topic Policy
  - Topic Delivery Policy
  - Topic ARN
  - Endpoint

AWS Cloud Control API

AWS Cloud Control API, a set of common application programming interfaces (APIs) that is designed to make it easy for developers to manage their cloud infrastructure in a consistent manner and leverage the latest AWS capabilities faster. Using AWS Cloud Control API, developers can manage the lifecycle of hundreds of AWS resources and over a dozen third-party resources with five consistent APIs instead of using distinct service-specific APIs. With this launch, AWS Partner Network (APN) Partners can now automate how their solutions integrate with existing

and future AWS services through a one-time integration, instead of spending weeks of custom development work as new resources become available.

How AWS Cloud Control API Differs for AWS GovCloud (US)

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

Documentation for AWSCloud Control API

AWSCloud Control API documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- No export-controlled data may be entered, stored, or processed by AWS Cloud Control API. For example, AWS Cloud Control API metadata is not permitted to contain export-controlled data. This metadata includes all the configuration data that you enter when creating and maintaining your resources using AWS Cloud Control API.

AWS Cloud Map

AWS Cloud Map is a fully managed service that you can use to create and maintain a map of the backend services and resources that your applications depend on.

How AWS Cloud Map Differs for AWS GovCloud (US)

- Public DNS namespaces are not supported in the AWS GovCloud (US) Regions.

Documentation for AWS Cloud Map

AWS Cloud Map documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

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)

- KmsKeyID property is not available.
- AWS CloudFormation doesn't support the following resources:
  - `AWS::IAM::GroupPolicy`
  - `AWS::IAM::RolePolicy`
  - `AWS::IAM::UserPolicy`
  - `AWS::Organizations::Account`

> **Note**
>
> ResourceTypes for AWS CloudFormation can vary per Region. Ensure the ResourceTypes needed are available in AWS GovCloud (US-West) and AWS GovCloud (US-East) which can be found here within the Resource Specification table.

Documentation for AWS CloudFormation

AWS CloudFormation documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- No export-controlled data may be entered, stored, or processed by AWS CloudFormation. For example, AWS CloudFormation metadata is not permitted to contain export-controlled data. This metadata includes all the configuration data that you enter when creating and maintaining your AWS CloudFormation templates.

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- AWS CloudHSM metadata is not permitted to contain export-controlled data. This includes all configuration data that you enter when creating and maintaining your AWS CloudHSM config. Audit and syslogs should not contain export-controlled data.

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- AWS CloudHSM Classic metadata is not permitted to contain export-controlled 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 export-controlled data.

AWS CloudShell

AWS CloudShell is a browser-based, pre-authenticated shell that you can launch directly from the AWS Management Console. You can run AWS CLI commands against AWS services using your preferred shell (Bash, PowerShell, or Z shell). And you can do this without needing to download or install command line tools.

How AWS CloudShell Differs for AWS GovCloud (US)

Currently, AWS CloudShell does not support Docker in the AWS GovCloud (US) Regions.

Documentation for AWS CloudShell

CloudShell documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- No data will leave the AWS GovCloud (US) Regions for this service.

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:

- As of November 22, 2021, AWS CloudTrail changed how trails capture global service events. Now, events created by CloudFront, IAM, and AWS STS are recorded in the AWS Region in which they were created, the AWS GovCloud (US-West) Region, us-gov-west-1. This makes CloudTrail's treatment of these services consistent with that of other AWS global services.

  To continue receiving global service events outside of AWS GovCloud (US-West), be sure to convert *single-Region trails* using global service events outside of AWS GovCloud (US-West) into *multi-Region trails*. For more information about using the CLI to update or create trails for global service events, see Using update-trail.

  In contrast, the **Event history** in the CloudTrail console and the **aws cloudtrail lookup-events** command will show these events in the Region where they occurred.
- 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.
- The following CloudTrail Lake features are currently not available in the AWS GovCloud (US) Regions:
  - CloudTrail Lake integrations
  - CloudTrail Lake event data stores for AWS Config configuration items, AWS Audit Manager evidence, and non-AWS events.
- 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",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:aws-us-
gov:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        },
        {
            "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",
                    "aws:SourceArn": "arn:aws-us-
gov:cloudtrail:region:myAccountID:trail/trailName"
                }
```

```
            }
        }
    ]
}
```

For more information, see Amazon S3 bucket policy and Amazon SNS topic policy for CloudTrail.

> **Note**
>
> This note applies to bucket policies that use a CloudTrail account ID as the Principal. 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

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

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- CloudTrail logs do not contain export-controlled data.
- CloudTrail configuration data may not contain export-controlled data.

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 environment types are not available in the AWS GovCloud (US) Regions.
- The `2xlarge` compute type is not available in the AWS GovCloud (US) Regions.
- The ability to pause a running build and then use AWS Systems Manager Session Manager to connect to the build container is not available in the AWS GovCloud (US) Regions.
- The public builds feature of CodeBuild is not available in the AWS GovCloud (US) Regions.
- Windows managed and custom images are not available in the AWS GovCloud (US) Regions.
- Batch Configuration is not available in the AWS GovCloud (US) Regions.

Documentation for AWS CodeBuild

AWS CodeBuild documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

AWS CodeStar Connections

You can use the connections feature in the Developer Tools console to connect AWS resources to external code repositories. This feature has its own API, the AWS CodeStar Connections API reference. Each connection is a resource that you can give to AWS services to connect to a third-party repository, such as BitBucket. For example, you can add a connection in CodePipeline so that it starts your pipeline when a code change is made to your third-party code repository. Each connection is named and associated with a unique Amazon Resource Name (ARN) that is used to reference the connection.

How AWS CodeStar Connections Differs for AWS GovCloud (US) Regions

- AWS CodeStar Connections is only available in the AWS GovCloud (US-East) Region.
- Since AWS GovCloud (US) operates as isolated Regions, you cannot share or use connections resources with other services outside of the Regions. For example, you cannot use a connection in AWS GovCloud (US-East) with a pipeline in CodePipeline that is not in the AWS GovCloud (US-East) Region.

Documentation for AWS CodeStar Connections

AWS CodeStar Connections documentation

Export-Controlled Content

For AWS services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

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 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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- 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.
- ECS capacity providers are not supported.
- Automatically updating outdated instances is not supported.
- CodeDeploy does not have a VPC endpoint powered by PrivateLink.

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:

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

AWS CloudFormation Template Location

Location of AWS CloudFormation template for launching Amazon EC2 instance configured for CodeDeploy deployments:

```
https://s3-us-gov-west-1.amazonaws.com/aws-codedeploy-us-gov-west-1/templates/latest/
CodeDeploy_SampleCF_Template.json
```

Links for Downloading CodeDeploy Installer and Updater (Windows Server)

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

- Installer:

  ```
  https://aws-codedeploy-us-gov-west-1.s3-us-gov-west-1.amazonaws.com/latest/
  codedeploy-agent.msi
  ```

- Updater:

```
https://aws-codedeploy-us-gov-west-1.s3-us-gov-west-1.amazonaws.com/latest/
codedeploy-agent-updater.msi
```

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

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- **Application Details:**
  - Name
- **Deployment Groups:**
  - Deployment group name
  - Service Role name
  - EC2 Auto Scaling group names
  - EC2 instance tag key
  - EC2 instance tag group name
  - On-premise Instances tag key
  - On-premise Instances tag group
  - Load Balancer ALB target group
  - Load Balancer NLB target group
  - Deployment trigger name
  - Deployment trigger SNS Topic
  - Deployment CloudWatch alarms
- **Deployment Configuration:**
  - Deployment configuration name
  - Deployment description

AWS CodePipeline

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. The following actions are only available in AWS GovCloud (US-East):
  - AWS CodeStar Source Connection (Bitbucket Cloud)
  - AWS CodeStar Source Connection (GitHub)
  - AWS CodeStar Source Connection (GitHub Enterprise Server)
  - AWS CodeStar Source Connection (GitLab.com)
- 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 OpsWorks
  - Amazon Alexa
  - AWS AppConfig (Supported in CLI, not supported in console)
  - AWS CloudFormation StackSets
- 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 .
- All users and service roles must exist in the AWS GovCloud (US) Region.
- Cross-region actions such as multi-region deployment are not supported.

Documentation for AWS CodePipeline

AWS CodePipeline documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Pipeline Name
- Stage Name
- Action Name
- CodeCommit Branch Name
- GitHub Branch Name

AWS Compute Optimizer

AWS Compute Optimizer recommends optimal AWS compute resources for your workloads to reduce costs and improve performance. Compute Optimizer uses machine learning to analyze your historical utilization metrics to help you choose the optimal AWS resource configuration.

How AWS Compute Optimizer Differs for AWS GovCloud (US)

Compute Optimizer only supports FIPS enabled endpoints in AWS GovCloud (US). To call Compute Optimizer APIs in AWS GovCloud (US), set the environment variable `AWS_USE_FIPS_ENDPOINT` to `true` for the AWS CLI and SDK.

The following AWS Compute Optimizer features aren't available in AWS GovCloud (US):

- Estimated monthly savings, savings opportunity, Reserved Instances (RI) coverage, and RI utilization information for Amazon Elastic Compute Cloud (Amazon EC2) instances and Amazon EC2 Auto Scaling groups.
- The savings opportunity summary displayed in the Compute Optimizer dashboard.
- External metrics ingestion.
- Enhanced infrastructure metrics.
- Recommendations for Amazon ECS services on AWS Fargate.

Documentation for AWS Compute Optimizer

Compute Optimizer documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- No data will leave the AWS GovCloud (US) Regions for this service.

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)

The implementation of AWS Config is different for AWS GovCloud (US) in the following ways:

- AWS Config recording of third-party resources or custom resource types are not supported in AWS GovCloud (US).
- For a list of rules supported in AWS GovCloud (US-East), see List of AWS Config Managed Rules by Region Availability | AWS GovCloud (US-East).
- For a list of rules supported in AWS GovCloud (US-West), see List of AWS Config Managed Rules by Region Availability | AWS GovCloud (US-West).

Documentation for AWS Config

AWS Config documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- AWS Config metadata is not permitted to contain export-controlled data. This includes the naming and configuration data that you enter when creating and managing your AWS Config settings.

  For example, do not enter export-controlled data into user input fields such as the following:

  - Annotations for rule evaluations
  - Resource identifier
  - S3 bucket name
  - SNS topic name
  - Tag key

AWS Control Tower

AWS Control Tower offers a straightforward way to set up and govern an AWS multi-account environment, following prescriptive best practices. AWS Control Tower orchestrates the capabilities of several other AWS services, including AWS Organizations, AWS Service Catalog, and IAM Identity Center, to build a landing zone in less than an hour. Resources are set up and managed on your behalf.

You can utilize AWS Control Tower with workloads that require FedRAMP High categorization level in the AWS GovCloud (US) Regions. AWS Control Tower is in scope for numerous compliance programs and standards, including HIPAA (Health Insurance Portability and Accountability Act), PCI DSS (Payment Card Industry – Data Security Standard), ISO (International Organization for Standardization), SOC 1, 2, and 3 (System and Organization Controls). To learn more, visit the AWS Control Tower homepage or see the *AWS Control Tower User Guide*.

How AWS Control Tower Differs for AWS GovCloud (US)

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

Overview of differences

- As in the commercial Region, you must use AWS Control Tower with all features enabled for AWS Organizations in AWS GovCloud (US) Regions. However, the consolidated billing feature set is not available in AWS GovCloud (US) Regions.
- You must meet the U.S. regulatory requirements as described in Signing Up for AWS GovCloud (US).
- Organizations that you create in the AWS GovCloud (US) Regions are independent from organizations created in commercial AWS Regions.
- Creating accounts from within AWS Control Tower operates differently in the AWS GovCloud (US) Regions compared to commercial AWS Regions:
  - You start creating AWS GovCloud (US) accounts by calling the CreateGovCloudAccount action from the management account of the landing zone in the commercial Region. Calling account creation APIs from the AWS GovCloud (US) Regions is not supported.
  - When you call the `CreateGovCloudAccount` API action, you create *two accounts*: a standalone account in the AWS GovCloud (US) Regions, and an associated account in the commercial Region for billing and support purposes. The account in the commercial Region

automatically becomes a member of the organization whose credentials made the request. Both accounts are associated with the same email address.

  - After you create the standalone account in the AWS GovCloud (US) Regions, you can invite it to an organization in the AWS GovCloud (US) Regions only.
  - Accounts created in other AWS Regions cannot be members of an organization in the AWS GovCloud (US) Regions.
- To learn what AWS services are currently available for trusted access with AWS Control Tower, check the list in the AWS Control Tower console from the AWS GovCloud (US) Regions.
- Landing Zone APIs are not available in AWS GovCloud (US) Regions.

For more information about AWS Control Tower, see the AWS Control Tower Documentation.

Feature-level differences

- **Inability to create accounts in AWS GovCloud (US)**

  AWS Control Tower does not support the ability to create accounts within AWS GovCloud (US). The AWS Organizations **CreateGovCloudAccount** API is available in the Commercial Region (US East (N. Virginia)) only. Therefore, AWS Control Tower cannot programmatically create accounts with Account Factory, nor during Landing Zone setup. This difference affects setup regarding the creation of the Audit account and the Log Archive account.
- **Must enroll existing AWS GovCloud (US) accounts for Audit and Log Archive**

  AWS Control Tower in AWS GovCloud (US) requires you to bring your own, existing Audit and Log Archive accounts during Landing Zone setup. These accounts must exist in your AWS GovCloud (US) organization before you enroll them. AWS Control Tower supports single account enrollment only, for Account Factory.
- **Changes for Account Factory**

  The **Create account** feature in Account Factory is removed in AWS GovCloud (US) Regions. During the **Create account** workflow, you will see an error if the member account does not already exist in AWS GovCloud (US).
- **Home Region**

  You are redirected to the appropriate AWS GovCloud (US) home Region (AWS GovCloud (US-West) or AWS GovCloud (US-East)) when running AWS Control Tower in the AWS GovCloud (US) console.

- **Verifying an account email address**

  An account in the commercial Region and the associated account in the AWS GovCloud (US) Region share an email adress. AWS Control Tower cannot verify account email addresses independently in AWS GovCloud (US) Regions.

- **Guardrail changes**

  All guardrails are present, but certain guardrails include functionality that has no effect in AWS GovCloud (US) Regions, based on other underlying differences. No error messages are reported for the differences in guardrail functionality. These guardrails include:

  - Disallow cross-region networking for Amazon EC2, Amazon CloudFront, and AWS Global Accelerator
  - Disallow delete actions on Amazon S3 buckets without MFA
  - Disallow changes to replication configuration for Amazon S3 buckets
  - Disallow creation of access keys for the root user
  - Disallow actions as a root user
  - Disallow the specified actions except in Regions with status Governed by AWS Control Tower

- **Marketplace**

  The Marketplace link in the left navigation of the AWS Control Tower console is not available in AWS GovCloud (US) Regions.

- **GDPR compliance**

  GDPR compliance is not required for services that reside only in the United States; therefore, it is not implemented in AWS Control Tower in AWS GovCloud (US) Regions.

- **Customizations for AWS Control Tower (CfCT) and Account Factory for Terraform (AFT) are unavailable for home Region AWS GovCloud (US-East)**

  AFT and CfCT are not available if the home Region is AWS GovCloud (US-East), but these capabilities are available if the home Region is AWS GovCloud (US-West). Customers can use AWS GovCloud (US-West) to customize both AWS GovCloud (US) Regions.

- **Control APIs unavailable in AWS GovCloud (US) Regions**

  The AWS Control Tower APIs for managing controls are not available in AWS GovCloud (US) Regions. However, the Service Catalog APIs for enrolling an existing account are available.

- **Security Hub controls**

Some controls in the Security Hub standard named **Service-Managed Standard: AWS Control Tower** are not supported in AWS GovCloud (US) Regions. For a complete list of these controls by Region, see Security Hub.

- **Proactive controls** are not available in AWS GovCloud (US) Regions.
- **Preventive and detective controls that support digital sovereignty**

  Preventive and detective controls, including enhanced Region deny capabilities, are available to help meet digital sovereignty requirements. These controls can assist in preventing undesired actions. They can detect resource changes for data residency, granular access restriction, encryption, and resiliency capabilities. View these controls under a digital sovereignty group in the AWS Control Tower console. For more information, see https://docs.aws.amazon.com/controltower/latest/userguide/digital-sovereignty-controls.html.
- **Support for FedRamp Levels 4 and 5**

  AWS Control Tower is authorized for Department of Defense Cloud Computing Security Requirements Guide Impact Levels 4 and 5 (DoD SRG IL4 and IL5) in the AWS GovCloud (US-East and US-West) Regions.

  This capability builds on the existing FedRamp High categorization level, as well as numerous compliance programs and standards, including HIPAA (Health Insurance Portability and Accountability Act), PCI DSS (Payment Card Industry – Data Security Standard), ISO (International Organization for Standardization), SOC 1, 2, and 3 (System and Organization for Standardization), SOC 1, 2, and 3 (System and Organization Controls). To learn more, visit the AWS Control Tower homepage or see the AWS Control Tower User Guide.

Creating your accounts

AWS Control Tower must be set up in the commercial Region before you can sign in to the AWS Control Tower management account to create AWS Control Tower accounts in AWS GovCloud (US).

When you create an account in the AWS GovCloud (US) Regions from AWS Control Tower, an associated account in the commercial Region is created for billing and support purposes, automatically. The account in the commercial Region and the account in the AWS GovCloud (US) Regions are linked.

The account in the commercial Region is a member of the organization whose credentials made the request, automatically, but the account in the AWS GovCloud (US) Regions is a standalone account until you invite it to an organization in that same Region.

Before creating accounts in the AWS GovCloud (US) Regions from AWS Control Tower, make sure that you meet specific U.S. regulatory requirements as described in Signing Up for AWS GovCloud (US).

For more information about getting started with AWS GovCloud (US) see AWS GovCloud (US) Sign Up.

To create an account in the AWS GovCloud (US) Regions from AWS Control Tower

1. From the management account of your organization in the commercial Region, sign in and authenticate to the AWS Control Tower console at https://console.aws.amazon.com/controltower
2. While signed into your management account in a commercial Region, with AWS CloudShell, or by means of a CLI script, you can call the the CreateGovCloudAccount API action.
3. Go to your AWS GovCloud (US) Region and invite the new standalone account to an organization.

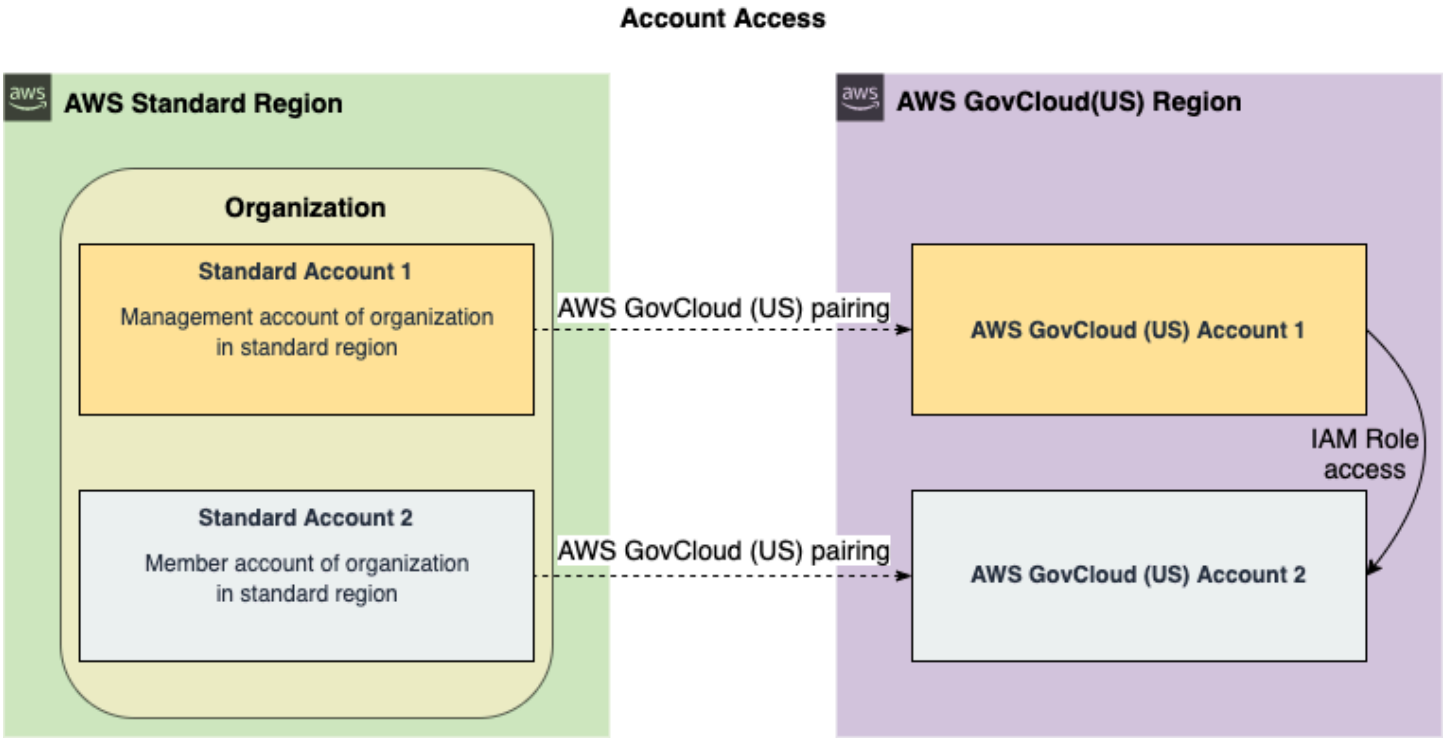
Accounts and roles are created as follows

- An account is created in the commercial Region and it automatically is a member of the organization whose credentials made the request.
- A role is created in the new account in the commercial Region, which the management account in this same Region can assume.
- The account in the AWS GovCloud (US) Regions 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 (US) Regions is a standalone account. It is not yet a member of an organization.
- The AWS GovCloud (US) account, which is linked to the management account in the commercial Region, can assume the role that is created during setup of that AWS GovCloud (US) account.

Inviting accounts to an organization

After creating a standalone account in the AWS GovCloud (US) Regions, you can invite it to an organization in the AWS GovCloud (US) Regions. You cannot invite accounts in the AWS GovCloud (US) Regions to organizations in other AWS Regions.

The following diagram shows how account access works, so that you can invite standalone accounts in the AWS GovCloud (US) Regions to an organization in the same Region.



Example: Account 1 invites Account 2 in the AWS GovCloud (US) Regions to an Organization

1. In this example, **AWS GovCloud (US) Account 1** is the AWS GovCloud (US) account that's associated with the management account of your organization in the commercial Region. **AWS GovCloud (US) Account 2** is going to become a member account in the organization of **AWS GovCloud (US) Account 1**.

   - Sign into **AWS GovCloud (US) Account 1**. Assume the administrative role of the AWS GovCloud (US) account you just created in the AWS GovCloud (US) Regions.
   - Send an invitation to **Account 2**. Sign out of **Account 1**.
   - Sign into and assume the IAM role that was created in **AWS GovCloud (US) Account 2**.
   - Accept the invitation.

2. Alternatively, another **AWS GovCloud (US) Account 2** user can sign into **Account 2** with the IAM user credentials you provided, then view and accept the invitation.

For more information, see the procedure described in Sending Invitations to AWS Accounts in the AWS Organizations User Guide to invite the account in the AWS GovCloud (US) Regions to the AWS GovCloud (US) organization.

Setting up your landing zone

Here's an overview and a recommended sequence of steps for setting up an AWS Control Tower landing zone in AWS GovCloud (US) Regions. It is slightly different than the process for commercial Regions, because of the way you must create accounts.

AWS Control Tower setup process overview

1. **In the commercial Region**: Create the two AWS accounts you'll require in AWS GovCloud (US), which will become log archive and audit accounts for your AWS GovCloud (US) organization.
2. **In the AWS GovCloud (US) home Region**: Create an organization in your AWS GovCloud (US) home Region, or choose which organization and Region you'll require for your AWS Control Tower landing zone. In AWS GovCloud (US) Regions, you can deploy AWS Control Tower in an existing AWS GovCloud (US) organization.
3. **In the AWS GovCloud (US) home Region**: Invite the two new accounts into your selected AWS GovCloud (US) organization. Go to those accounts and accept the invitations.
4. **In the AWS GovCloud (US) home Region**: Follow the procedure to set up AWS Control Tower in an existing organization. Specify the two existing accounts, which you've already created in the first step and just invited to your organization, as your audit and log archive accounts.
5. **In the AWS GovCloud (US) home Region**: Use AWS Control Tower to set up OUs in your landing zone, for your AWS Control Tower workloads in AWS GovCloud (US) Regions. (Use AWS Organizations to set up any other required organizations. AWS Control Tower supports one landing zone per organization.)
6. **In the commercial Region**: Create the necessary member accounts to run your AWS GovCloud (US) Regions workloads.
7. **In the AWS GovCloud (US) home Region**: Invite each account that you created in the previous step into its proper organization and OU, presumably into the organization in which you have already set up the AWS Control Tower landing zone.

After you've performed these tasks, it's a good idea to check the guardrails (also called controls) that are enabled on your OUs, and apply any optional controls that are applicable to your business requirements.

Documentation for AWS Control Tower

AWS Control Tower documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- AWS Control Tower metadata is not permitted to contain export-controlled data. This metadata includes all of the configuration data that you enter when creating and maintaining your AWS Control Tower landing zone and AWS accounts, including AWS account names and email addresses, or Organizational Unit names.

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)

- AWS DMS Schema Conversion is not available.

Documentation for AWS Database Migration Service

AWS Database Migration Service documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

AWS DataSync

DataSync is a data transfer service that makes it easy for you to automate moving data between on-premises storage and Amazon S3, Amazon Elastic File System (Amazon EFS), or Amazon FSx. 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. Deploy the DataSync agent on premises, connect it to a file system or storage array, select Amazon EFS, Amazon S3, or Amazon FSx 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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

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)

- Using the AWS Direct Connect Gateway connectivity from any AWS Direct Connect location can be established into either or both AWS GovCloud (US) locations. For more information, see https://aws.amazon.com/blogs/publicsector/aws-hybrid-connectivity-sharing-aws-direct-connect-aws-govcloud-us-commercial-regions/
- AWS Direct Connect Gateway is supported between an AWS GovCloud (US) account and a linked standard/commercial AWS account. From your AWS GovCloud (US) account, you can associate a virtual private gateway with an AWS Direct Connect gateway that exists in the linked commercial/standard AWS account.
- AWS Direct Connect Partners do not support Hosted connections to AWS GovCloud (US) Account IDs. When ordering connections through an AWS Direct Connect Partner for a hosted connection, use the commercial account ID.
- 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.
- When you create a public virtual interface on your AWS Direct Connect connection associated with any standard Region or AWS GovCloud (US) Region, a data path to AWS GovCloud (US) is made available. Public virtual interface on an AWS Direct Connect connections associated with an AWS China Region do not have a data path to AWS GovCloud (US).

- To access your VPC without using an Amazon VPC VPN (for non-export 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 export-controlled 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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- AWS Direct Connect metadata is not permitted to contain export-controlled data. This metadata includes all of the configuration data that you enter when creating and maintaining AWS Direct Connect, such as connection names.
- Do not enter export-controlled data in the following console fields:
  - Connection Name
  - VIF Name

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:
  - Amazon WorkDocs
  - Amazon WorkMail
  - Amazon Chime
  - AWS Management Console
  - Amazon Connect only in available in AWS GovCloud (US-West).
  - AWS IAM Identity Center
- 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
- Automatic DNS forwarding is not enabled by default and must be configured.

Documentation for AWS Directory Service

AWS Directory Service documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- AWS Directory Service metadata is not permitted to contain export-controlled data. This metadata includes all configuration data that you enter when creating and maintaining your AWS Directory Service directory except passwords.

  Do not enter export-controlled data in the following console fields:

  - Directory aliases
  - Directory description
  - Directory DNS name
  - Netbios name
  - Manual snapshot name
  - Resource tags
  - Description of schema extensions

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- The following AWS Elastic Beanstalk metadata fields:
  - Application Name
  - Environment Name
  - Option Settings

AWS Elastic Disaster Recovery

AWS Elastic Disaster Recovery minimizes downtime and data loss with fast, reliable recovery of on-premises and cloud-based applications using affordable storage, minimal compute, and point-in-time recovery.

How AWS Elastic Disaster Recovery Differs for AWS GovCloud (US)

- In AWS GovCloud (US) Regions, you must launch all Amazon EC2 instances for recovery, drill, failback and AWS Elastic Disaster Recovery service resources 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 or setting up the AWS Elastic Disaster Recovery staging area.
- Use SSL (HTTPS) or Federal Information Processing System (FIPS) protocols when you make calls to the service in the AWS GovCloud (US) Regions (us-gov-west-1, us-gov-east-1). In other AWS Regions, you can use HTTP or HTTPS.

- Cross-Partition failback features between commercial and AWS GovCloud (US) partitions are not supported. Cross-Region failback features within the AWS GovCloud (US) partition are available between AWS GovCloud (US) Regions (us-gov-west-1 and us-gov-east-1).
- AWS Elastic Disaster Recovery source servers can only be extended to other GovCloud AWS accounts when using multiple staging accounts.
- AWS Elastic Disaster Recovery trusted account features are only supported between other GovCloud AWS accounts.
- The Provisioned IOPS SSD (io2) EBS volume type is not available in the AWS GovCloud (US) Regions.
- AWS Elastic Disaster Recovery leverages the following AWS services in AWS GovCloud (US). Please refer to the individual service for GovCloud differentiators:
  - Amazon EC2
  - AWS Key Management Service
  - Amazon EBS
  - Amazon VPC
  - AWS Direct Connect
  - AWS Site-to-Site VPN
  - AWS Systems Manager
  - Cloudwatch

Documentation for AWS Elastic Disaster Recovery

AWS Elastic Disaster Recovery documentation.

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 the Amazon VPC User Guide.

If you don't want a default VPC for your AWS Elastic Disaster Recovery account in AWS GovCloud (US), 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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon EC2 metadata is not permitted to contain export-controlled data. This metadata includes all configuration data that you enter when creating and maintaining your AWS Elastic Disaster Recovery source servers.
- Do not enter export-controlled data in the following fields:
  - Source server names
  - Key and Value of Tags associated with your resources.
  - Name and Description of Security Groups and Security Group Rules
  - Refer to AWS Elastic Disaster Recovery leveraged AWS services for service-specific export-controlled data fields.

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

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)

- Amazon EKS on Fargate is not available in AWS GovCloud (US).

Documentation for AWS Fargate

Amazon ECS User Guide for AWS Fargate documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

AWS Fault Injection Service

AWS Fault Injection Service (AWS FIS) is a managed service that enables you to perform fault injection experiments on your AWS workloads. Fault injection is based on the principles of chaos engineering. These experiments stress an application by creating disruptive events so that you can observe how your application responds. You can then use this information to improve the performance and resiliency of your applications so that they behave as expected.

How AWS Fault Injection Service Differs for AWS GovCloud (US)

The AWS FIS Experiment Schedule feature is not available in AWS GovCloud (US).

Documentation for AWS Fault Injection Service

AWS Fault Injection Service documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

AWS Fault Injection Service metadata is not permitted to contain export-controlled data. This metadata includes:

- Experiment templates
- Experiment tags

AWS Firewall Manager

AWS Firewall Manager simplifies your administration and maintenance tasks across multiple accounts and resources for AWS WAF, AWS Shield Advanced, Amazon VPC security groups, and AWS Network Firewall. With Firewall Manager, you set up your AWS WAF firewall rules, Shield Advanced protections, Amazon VPC security groups, Network Firewall firewalls, and DNS Firewall rule group associations just once. The service automatically applies the rules and protections across your accounts and resources, even as you add new resources.

How AWS Firewall Manager Differs for AWS GovCloud (US)

- AWS Marketplace managed rule groups for AWS WAF cannot be used with Firewall Manager security policies 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) with Firewall Manager security policies. AWS Marketplace rule groups are provided for subscription by AWS Marketplace sellers and aren't available for use in AWS GovCloud (US) with Firewall Manager.
- Firewall Manager security policies for AWS WAF cannot be enabled on Amazon CloudFront distributions in AWS GovCloud (US).
- Firewall Manager does not support AWS Shield Advanced or AWS WAF Classic.

Documentation for AWS Firewall Manager

AWS Firewall Manager documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- AWS Firewall Manager metadata is not permitted to contain export-controlled data. For example, do not enter export-controlled data into user input fields such as the following:
  - Firewall Manager policy name
  - Resource Tag/Key values

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)

- The following AWS Glue features are available AWS GovCloud (US-West), but not in AWS GovCloud (US-East):
  - AWS Glue Databrew
  - Workflows
  - Interactive sessions
  - AWS Glue versions 3.0 and 4.0
  - Machine Learning
  - Sensitive Data Detection
- AWS Glue Studio notebooks is not available in AWS GovCloud (US).
- Flex Execution is not available in AWS GovCloud (US)
- For AWS Glue Studio, the Marketplace Connector feature is not available in AWS GovCloud (US)
- The Interactive Data Preview feature is not available in AWS GovCloud (US)

How AWS Glue Differs for AWS GovCloud (US)

- AWS Glue Databrew is available in AWS GovCloud (US-West), but not in AWS GovCloud (US-East).
- For AWS Glue Studio, the Marketplace Connector feature is not available in AWS GovCloud (US).
- Workflows are available in AWS GovCloud (US-West), but not in AWS GovCloud (US-East).
- Interactive sessions are available in AWS GovCloud (US-West), but not in AWS GovCloud (US-East).
- AWS Glue Studio notebooks are not available in AWS GovCloud (US).
- Flex Execution is not available in AWS GovCloud (US).

Documentation for AWS Glue

AWS Glue documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

AWS IAM Identity Center

IAM Identity Center provides one place where you can create or connect workforce users and centrally manage their access to all of their AWS accounts, Identity Center enabled applications, and applications that support Security Assertion Markup Language (SAML) 2.0. Workforce users benefit from a single sign-on experience and can use the access portal to find all of their assigned AWS accounts and applications in one place. IAM Identity Center integrates with AWS Organizations to enable you to manage workforce users' access and permissions across all of their assigned AWS accounts.

How IAM Identity Center Differs for AWS GovCloud (US)

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

- IAM Identity Center integrates with AWS Organizations to manage access across your AWS accounts, and therefore, IAM Identity Center is subject to any AWS Organizations GovCloud differences.
- To access the IAM Identity Center administrative console, the Software Development Kit (SDK), or the AWS Command Line Interface (CLI) use the Federal Information Processing Standards (FIPS) endpoints. For a list of all GovCloud AWS FIPS endpoints, see *AWS GovCloud (US)* in FIPS Endpoints by Service.
- The AWS access portal URL has an AWS GovCloud (US) URL pattern of `https://start.us-gov-home.awsapps.com/directory/<IdentityStoreId>` or `https://start.us-gov-home.awsapps.com/directory/<CustomAlias>`

You can find this URL on the **Settings** page in the IAM Identity Center console.

- The Amazon Resource Number (ARN) for your IAM Identity Center instance has an AWS GovCloud (US) pattern of `arn:aws-us-gov:sso:::instance/<SSOInstanceId>`

  You can find this ARN on the **Settings** page in the IAM Identity Center console.

- The ARNs for IAM Identity Center permission sets has an AWS GovCloud (US) pattern of `arn:aws-us-gov:sso:::permissionSet/<SSOInstanceID>/<PermissionSetID>`

  You can find these ARNs on the **Permission sets** tab under the **AWS accounts** page in the IAM Identity Center console.

- The email address `no-reply@us-gov-home.awsapps.com` is used for sending email-verification, password reset, and user invitation emails to GovCloud.

  The email address `no-reply@<identitystore_id>.us-gov-home.awsapps.com` is used for sending forgotten password emails.

- If you filter access to specific AWS domains by using a web content filtering solution such as next-generation firewalls (NGFW) or Secure Web Gateways (SWG), you must add the following domains to your web-content filtering solution allowlists. Doing so enables you to access your AWS access portal.
  - `start.us-gov-home.awsapps.com`
  - `start.[Region].us-gov-home.awsapps.com`
  - `oidc.[Region].amazonaws.com`
  - `*.sso.amazonaws.com`
  - `*.sso.[Region].amazonaws.com`
  - `*.sso-portal.[Region].amazonaws.com`
  - `aws-access-portal-website-prod-pdt-assets.s3.us-gov-west-1.amazonaws.com`
  - `aws-access-portal-website-prod-osu-assets.s3.us-gov-east-1.amazonaws.com`
  - `s3.us-gov-west-1.amazonaws.com/awsconsole-peregrine-portal-prod-pdt-assets`
  - `s3.us-gov-east-1.amazonaws.com/awsconsole-peregrine-portal-prod-osu-assets`
  - `[Region].signin-fips.amazonaws-us-gov.com`

- `*.cloudfront.net`
- `opfcaptcha-prod.s3.amazonaws.com`

Documentation for AWS IAM Identity Center

AWS IAM Identity Center documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Your IAM Identity Center Identity Store ID may leave the AWS GovCloud (US) Regions in the normal course of the service offerings.

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 must have an existing standard AWS account to create an AWS GovCloud (US) account. See AWS GovCloud (US) Sign Up to learn more. If you have AWS GovCloud (US) sign up issues, contact AWS Customer Support.
- When your AWS GovCloud (US) account is created, you are provided initial access to the AWS Management Console for AWS GovCloud (US) by an `Administrator` IAM user or an `OrganizationAccountAccessRole` IAM role, depending on the method used.

  You cannot access the AWS Management Console for AWS GovCloud (US) using the associated standard AWS account root user credentials.

- The AWS GovCloud (US) account root user is created at the same time the AWS GovCloud (US) account is created, but access to this user is not provided by default to AWS GovCloud (US) customers.
  - Sign in to the AWS Management Console for AWS GovCloud (US) as the AWS GovCloud (US) account root user is not supported.
  - AWS GovCloud (US) account root user access keys can be provided at the request of associated standard AWS account root user by contacting AWS Customer Support. See Requesting root access keys for an AWS GovCloud (US) account to get started.
  - There is one IAM control plane for all AWS GovCloud (US) Regions, which is located in the AWS GovCloud (US-West) Region. Each AWS Region has a completely independent instance of the IAM data plane. For more information, see Resilience in AWS Identity and Access Management.
  - Tasks that require the root user in AWS GovCloud (US) are limited. See Tasks in AWS GovCloud (US) Regions that require root user access keys.
  - Solution Providers reselling in AWS GovCloud (US) may receive AWS GovCloud (US) account root user access keys to be used for initial access to their account from an AWS business representative.
  - For more information, see AWS GovCloud (US) account root user .
- Access issues for IAM users that are administrators in your AWS GovCloud (US) can be resolved by another administrator in the account.

  If all administrators have forgotten or lost access to the AWS GovCloud (US) account, request AWS GovCloud (US) account root user access keys to Restore IAM Administrator access to the AWS Management Console for AWS GovCloud (US). See Requesting root access keys for an AWS GovCloud (US) account to get started.
- There is one IAM control plane for all AWS GovCloud (US) Regions, which is located in the AWS GovCloud (US-West) Region. Each AWS Region has a completely independent instance of the IAM data plane. For more information, see Resilience in AWS Identity and Access Management.
- When using the IAM or AWS STS service in AWS GovCloud (US), you must use AWS GovCloud (US) IAM/AWS STS endpoints. Use SSL (HTTPS) when you make calls to the IAM or AWS STS service in AWS GovCloud (US) Regions.
- 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 Multi-Factor Authentication (MFA) in AWS GovCloud (US) page.

  - You can use these MFA devices with your AWS GovCloud (US) administrator user or any IAM user in your account.
  - You cannot use these MFA devices with 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. export-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.
- When you create policies, use the AWS GovCloud (US) resource ARN prefix. For more information, see Amazon Resource Names (ARNs) in 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*.
- IAM Access Analyzer unused access findings and policy generation are not supported in AWS GovCloud (US). To learn more, see IAM Access Analyzer in the *IAM User Guide*.
- IAM Roles Anywhere is now supported in AWS GovCloud (US). To learn more, see Providing access for non AWS workloads in the *IAM User Guide*.
- When configuring SAML Applications for single sign on in AWS GovCloud (US), the SAML Audience and ACS links will be different than those used in the standard Regions.
  - Application ACS URL: https://signin.amazonaws-us-gov.com/saml
  - Application SAML audience: `urn:amazon:webservices:govcloud`

Documentation for AWS Identity and Access Management

AWS IAM documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- IAM metadata is not permitted to contain export-controlled data. This metadata includes all configuration data that you enter when creating and maintaining your IAM entities.
- Do not enter export-controlled data in the following fields:
  - Authentication codes, which are clear-text memcached
  - User names
  - Group names
  - Password policies
  - Policy names
  - Roles and role names
  - Policy documents

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.

Documentation for AWS IoT

AWS IoT Core documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Message topics and topic filters
- Thing names

- Thing types
- Thing group names
- Rule definitions (including SQL statements and actions)

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.
- AWS IoT Device Defender ML Detect feature is not available in GovCloud regions

Documentation for AWS IoT Device Defender

AWS IoT Device Defender documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Security Profile Name
- Behavior Name
- Audit Schedule Name
- Mitigation Action Name
- Audit Mitigation Action Task Id

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. For more information, see Common Amazon Cognito scenarios.
- AWS IoT Device Management Fleet Hub is not available. For more information, see What is Fleet Hub for AWS IoT Device Management?
- FreeRTOS over-the-air (OTA) updates using MQTT-based file delivery via a stream is not supported. For more information, see OTA Update Manager service and MQTT-based file delivery.

Documentation for AWS IoT Device Management

AWS IoT Device Management documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Message topics and topic filters
- Thing names
- Thing types
- Thing group names
- Rule definitions (including SQL statements and actions)

AWS IoT Events

AWS IoT Events enables you to monitor your equipment or device fleets for failures or changes in operation, and to trigger actions when such events occur. AWS IoT Events continuously watches IoT sensor data from devices, processes, applications, and other AWS services to identify significant events so you can take action.

AWS IoT Events is only supported in the AWS GovCloud (US-West) Region.

How AWS IoT Events Differs for AWS GovCloud (US)

- SSO integration not supported.
- Notification action is not supported.

Documentation for AWS IoT Events

AWS IoT Events documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Detector Model Name
- Alarm Model name
- Input Name
- Fields in run-time messages used as key-value in Detector Models or Alarm Models
- MessageId in BatchPutMessage calls
- SiteWise AssetId and PropertyId that are referenced in AlarmModel rules

AWS IoT Greengrass Version 1

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 V1 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.

Language or platform	Minimum version
Python 3.7	1.4.0
Java 8	1.3.1
Node.js 8.10	1.4.0
C, C++	1.1.0

- 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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                    "arn:aws-us-gov::s3:::us-gov-west-1-greengrass-updates/*"

            ]
        }
    ]
}
```

- 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 more information, see Service Endpoints. 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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Message topics and topic filters
- Customer-defined names and IDs of Greengrass resources:
  - Connectors
  - Cores
  - Devices
  - Functions
  - Groups
  - Loggers
  - Resources (local and machine learning)
  - Subscriptions

AWS IoT Greengrass Version 2

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 V2 Differs for AWS GovCloud (US)

- Secret manager v2.0.5 is the minimum supported version in the AWS GovCloud (US) Regions.

Documentation for AWS IoT Greengrass V2

AWS IoT Greengrass documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Message topics and topic filters
- Customer-defined names and IDs of Greengrass resources:
  - CoreDevices
  - Components
  - Deployments

AWS IoT SiteWise

AWS IoT SiteWise is a managed service that you can use to collect, model, analyze, and visualize data from industrial equipment at scale. With AWS IoT SiteWise Monitor, you can quickly create web applications for non-technical users to view and analyze your industrial data in real time. With AWS IoT SiteWise gateways, you can view and process your data on your local devices.

AWS IoT SiteWise is only supported in the AWS GovCloud (US-West) Region.

How AWS IoT SiteWise Differs for AWS GovCloud (US)

- The alarm configuration and notification features in AWS IoT SiteWise Monitor portals are currently not supported.
- The following endpoints are not supported:
  - The endpoint for the control plane API operations that you use to manage asset models and assets: `model.iotsitewise.region.amazonaws.com`.
  - The endpoint for the control plane API operations that you use to manage tags, storage configurations, and account configurations: `iotsitewise.region.amazonaws.com`.
  - The endpoint for the control plane API operations that you use to manage gateways: `edge.iotsitewise.region.amazonaws.com`.

  For more information, see Service Endpoints.

Documentation for AWS IoT SiteWise

AWS IoT SiteWise documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Data source names
- Metric definitions
- Transform definitions
- Amazon S3 bucket names for the exporting data to Amazon S3 feature
- IAM roles for the exporting data to Amazon S3 feature
- AWS KMS keys

AWS IoT TwinMaker

AWS IoT TwinMaker is used to build operational digital twins of physical and digital systems. AWS IoT TwinMaker creates digital visualizations using measurements and analysis from a variety of real-world sensors, cameras, and enterprise applications to help you keep track of your physical factory, building, or industrial plant.

AWS IoT TwinMaker is available in 6 Classic regions (us-east-1, us-west-2, eu-west-1, ap-southeast-1, eu-central-1, ap-southeast-2). AWS IoT TwinMaker is available in one GovCloud region: us-gov-west-1.

How AWS IoT TwinMaker Differs for AWS GovCloud (US)

The following differences exist between AWS IoT TwinMaker in AWS GovCloud (US) and standard regions:

- AWS IoT TwinMaker only supports the self-managed Grafana configuration option. Amazon Managed Grafana (AMG) is not available in the GovCloud PDT (us-gov-west-1) region.

- AWS IoT TwinMaker has an Edge Video feature which depends on Kinesis Video Streams (KVS). KVS is not supported in GovCloud PDT.
- The `com.amazon.iotsitewise.connector.edgevideo` component type is not supported.
- The `com.amazon.kvs.video` component type is not supported.
- The metadata bulk import and export operations are not available in the GovCloud PDT (us-gov-west-1) region.

Documentation for AWS IoT TwinMaker

AWS IoT TwinMaker documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Workspace ID
- ComponentType name
- Component Name
- Scene ID
- Property name
- Entity name

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)

- AWS KMS supports Transport Layer Security (TLS) 1.2—1.3 for endpoints in AWS GovCloud (US).

- AWS KMS supports Transport Layer Security (TLS) 1.2—1.3 for FIPS endpoints in AWS GovCloud (US). AWS KMS does not support hybrid post-quantum TLS for FIPS endpoints.
- External key store proxies in the AWS GovCloud (US) Region must support HTTP/1.1 or later and TLS 1.2 or later with at least one of these cipher suites: TLS_AES_256_GCM_SHA384 (TLS 1.3), TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (TLS 1.2), TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (TLS 1.2). The AWS GovCloud (US) Region does not support the TLS_CHACHA20_POLY1305_SHA256 cipher suite. For more information, see the open-source external key store proxy API specification that AWS KMS publishes.

Documentation for AWS Key Management Service

AWS Key Management Service Developer Guide.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- AWS KMS metadata is not permitted to contain export-controlled data. Do not enter export-controlled data in the following fields:
  - Alias
  - Descriptions
  - Key policy documents, including key administrators and key users
  - Resource tags: Key
  - Resource tags: Value
- The Encryption Context is outside the Export-Controlled Content.
- AWS KMS generated metadata will not contain export-controlled data:
  - Key ID
  - Key ARN

AWS Lake Formation

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:

- Granting Lake Formation permissions to Amazon Athena users who authenticate through the JDBC or ODBC driver using a SAML identity provider is not supported.
- AWS Lake Formation blueprints are available in AWS GovCloud (US-West) only.
- AWS Lake Formation governed tables are not available.

Documentation for AWS Lake Formation

AWS Lake Formation documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer

compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- No data will leave the AWS GovCloud (US) Regions for this service.

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)

- AWS Lambda Function URLs is not available.
- Lambda ARM architecture support is not available.
- Code signing for AWS Lambda is not available.
- Lambda SnapStart is not available.
- Runtime management configuration is not available.
- The DocumentDB event sources are not available.
- Outbound IPv6 traffic is not supported.
- The Amazon Linux 2023 (`provided.al2023`) runtime is not available.
- The Node.js 20 managed runtime (`nodejs20.x`) is not available.
- The Java 21 managed runtime (`java21`) is not available.
- Multi-VPC connectivity for Managed Streaming for Apache Kafka event source mappings is not available.
- The Python 3.12 managed runtime (`python3.12`) is not available.
- Lambda integration with Application Composer is not available.
- The Future runtime launch dates are not applicable.
- Lambda Advanced Logging Controls are not available.
- The .NET 8 (`dotnet8`) runtime is not available.

Documentation for AWS Lambda

AWS Lambda documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Do not enter export-controlled data in the following console fields:
  - Function name
  - Description
  - DLQ data (can be exported through Amazon SNS and Amazon SQS)
  - Memory
  - Timeout
  - Runtime
  - Role name for service principals
  - Aliases
  - LayerName
  - Layer Description
  - Layer Compatible Architectures
  - Layer Compatible Runtimes
  - EphemeralStorage Size
  - PackageType
  - State
  - StateReason

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)

- Sharing licenses between AWS standard accounts and AWS GovCloud (US) accounts is not supported.
- The user-based subscriptions feature is not available.
- The license type conversion feature is not available.

Documentation for AWS License Manager

AWS License Manager documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

AWS Managed Services - AMS Accelerate

AMS Accelerate is a service for configuring and managing your AWS infrastructure. For more information, see the service description.

How AMS Accelerate Differs for AWS GovCloud (US)

Some services available in other AWS Regions are not available or have limitations in AWS GovCloud (US) Regions.

- Not supported in AWS GovCloud (US) Regions:
  - Amazon Macie
  - Self-service reporting
  - Enable AMS to use your own CloudTrail trail
  - Customized findings responses for AWS Config rules
  - Cost optimization with AMS Resource Scheduler
  - Customer-provided tags
- Different in AWS GovCloud (US) Regions:
  - Outbound Service notifications are not sent to AWS account primary emails. Reports go to smaller, more targeted lists.
  - Accelerate Compliance and conformance is limited by the AWS Config managed rules available in your AWS Region.
- Differences in other AWS services. Some examples:
  - Not all AWS Config managed rules are available in all Regions. The Developer Guide lists all managed rules, and the applicable Regions for each rule.
  - GuardDuty: For information about the differences in AWS GovCloud (US) Regions, see Amazon GuardDuty.

Documentation for AMS Accelerate

For information, see the AMS Accelerate documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Resource names
- Tags
- Communications between customers and AMS Accelerate, such as service requests and incident reports.

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. You cannot enable an MFA device for your AWS GovCloud (US) account root user email, but can enable for IAM users. 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.
- 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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Your user name is not permitted to contain export-controlled data.
- All console data fields inherit the export restrictions for the specific service that is being accessed. See each service for details.

AWS Mainframe Modernization

AWS Mainframe Modernization helps you modernize your mainframe applications to AWS managed runtime environments. It provides tools and resources to help you plan and implement migration and modernization. You can analyze your existing mainframe applications, develop or update them using COBOL or PL/I, and implement an automated pipeline for continuous integration and continuous delivery (CI/CD) of the applications. You can choose between automated refactoring and replatforming patterns, depending on your clients' needs. If you are a consultant helping a client migrate their mainframe workloads, you can use Mainframe Modernization tools for all phases of the migration and modernization journey, from initial planning to post-migration cloud operations.

You can use Mainframe Modernization to help you efficiently create and manage the runtime environment on AWS for your mainframe applications, as well as to manage and monitor your modernized applications.

How AWS Mainframe Modernization Differs for AWS GovCloud (US)

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

Documentation for AWS Mainframe Modernization

Mainframe Modernization documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- No data will leave the AWS GovCloud (US) Regions for this service.

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.
- 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 Service Catalog is currently not available.

Documentation for AWS Marketplace

- AWS Marketplace documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

AWS Modular Data Center

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

AWS MDC is a simple and cost-effective service for defense and intelligence agencies to deploy AWS managed data centers anywhere in the world to run low-latency applications. AWS MDC is self-contained, which means that it's a physical, environmentally controlled enclosure that holds as many as five racks of AWS Outposts or AWS Snowball Edge devices. It can also be scaled further through deployment of additional modules. AWS MDC reduces the time and resources required to deploy data centers in remote environments with limited infrastructure. Customers can proactively monitor and manage their modular data centers using a management system that comes with every MDC. Each modular data center is equipped with Building Management System (BMS) sensors to monitor the environmental conditions of the MDC, including temperature, humidity, ventilation, HVAC performance, and power quality. The BMS also monitors safety systems, such as smoke detection, fire alarm, and the Access Control System (ACS) / Intrusion Detection System (IDS).

How AWS Modular Data Center Differs for AWS GovCloud (US)

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

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- AWS suggests that customers do not enter export-controlled information in the AWS MDC order consultation form use case field.

AWS Network Firewall

AWS Network Firewall is a stateful, managed, network firewall and intrusion detection and prevention service for your virtual private cloud (VPC) that you created in Amazon Virtual Private Cloud (Amazon VPC).

How AWS Network Firewall Differs for AWS GovCloud (US)

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

Documentation for AWS Network Firewall

AWS Network Firewall documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- No data will leave the AWS GovCloud (US) Regions for this service.

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 following Organizations API operations work only when you specify the AWS GovCloud (US-West) Region:

- DeletePolicy
- DisablePolicyType
- EnablePolicyType
- Any operation that references the organization root, such as ListRoots.

- Organization policies – You can use only the following policy types in a GovCloud organization:
  - Service control policies
  - Tag policies

    As a rule, you can create tag policies that reference only those resource types whose services are supported in the AWS GovCloud (US) Regions. However, you can use the following additional resource types in a tag policy even though the associated service is not yet supported in the AWS GovCloud (US) Regions:

    - `chime:meeting`
    - `codepipeline:pipeline`

    Tag policy compliance reporting works only in the AWS GovCloud (US-West) Region.

    The following tagging API operations work only when you specify the AWS GovCloud (US-West) Region:

    - DescribeReportCreation
    - GetComplianceSummary
    - GetResources
    - StartReportCreation

  You can't create or use AI services opt-out policies at this time.

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.

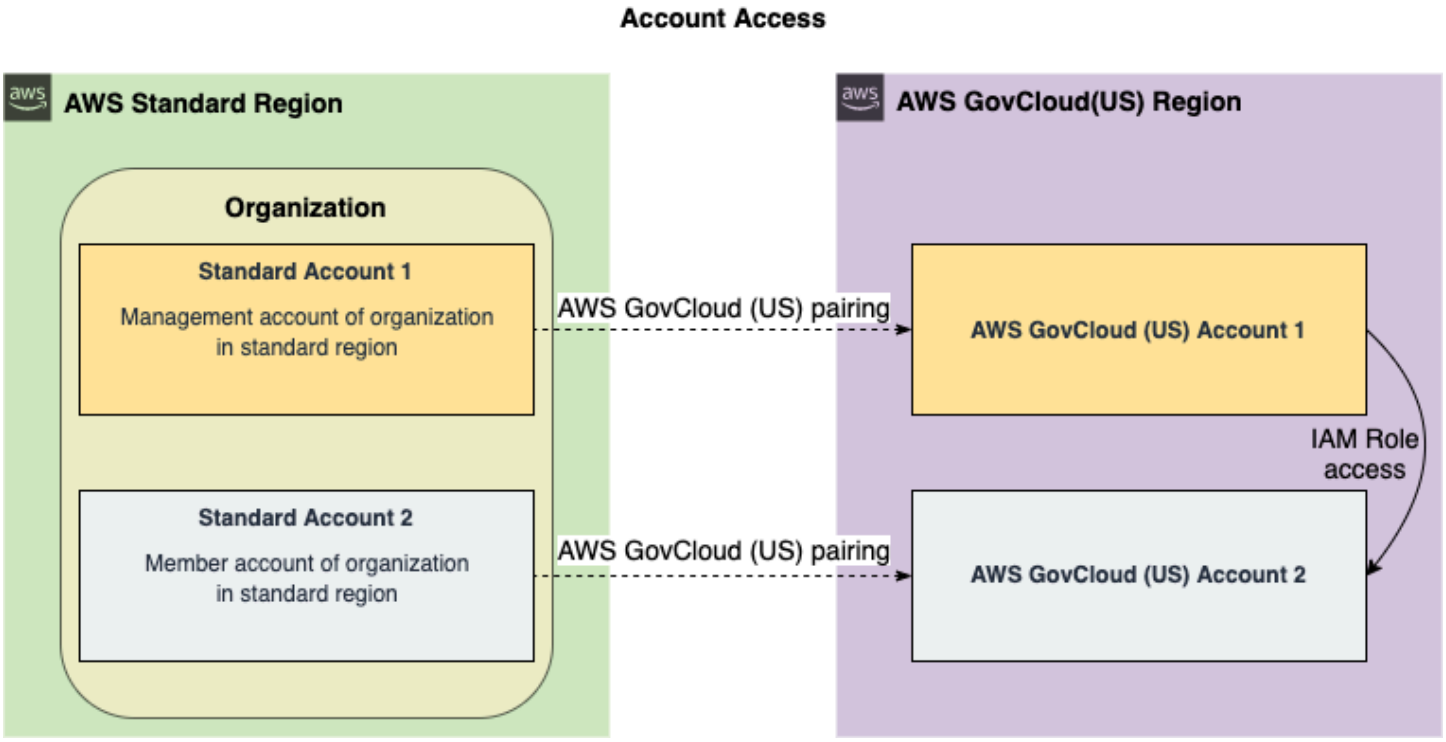
Accounts and roles are created as follows

- 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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

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)

- Application Load Balancer is not supported.
- Amazon RDS is not supported.
- Amazon EMR is not supported.
- ElastiCache is not supported.
- Route 53 resolver is not supported.

Documentation for AWS Outposts

AWS Outposts documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- AWS Outposts metadata is not permitted to contain export-controlled data. This metadata includes all configuration data that you enter when setting up and maintaining your topics.

  For example, do not enter export-controlled data in the following fields:

  - Outpost Name
  - Outpost Description
  - Site Address
  - Site Name
  - Site Description
  - Site Notes

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

AWS Resilience Hub

AWS Resilience Hub gives you a central place to define, validate, and track the resiliency of your AWS application. AWS Resilience Hub helps you to protect your applications from disruptions, and reduce recovery costs to optimize business continuity to help meet compliance and regulatory requirements.

How AWS Resilience Hub Differs for AWS GovCloud (US)

- When you are using AWS Resilience Hub from AWS GovCloud (US) Regions, you can't import resources that are located in non-AWS GovCloud (US) Regions.
- When you are using AWS Resilience Hub from AWS standard Regions, you can't import resources that are located in AWS GovCloud (US) Regions.

Documentation for AWS Resilience Hub

AWS Resilience Hub documentation.

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Resource Share name cannot contain export-controlled data.

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)

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

- Group lifecycle events are not supported.

Documentation for AWS Resource Groups

AWS Resource Groups documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Name

AWS RoboMaker

AWS RoboMaker is a cloud-based simulation service that enables robotics developers to run, scale, and automate simulation without managing any infrastructure. This enables robotics developers to cost-effectively scale and automate simulation workloads, run large-scale and parallel simulations with a single API call. Using the AWS RoboMaker simulation service, you can speed application testing. AWS RoboMaker is also capable of automated testing within a continuous integration and continuous delivery (CI/CD) pipeline, training reinforcement models with high volumes of interative

trials, and connecting multiple concurrent simulations to your fleet management software for testing. When combined with AWS machine learning, monitoring, and analytics services, robots can stream data, navigate, communicate, comprehend, and learn.

How AWS RoboMaker Differs for AWS GovCloud (US)

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

RoboMaker Development Environment (based on Cloud9 IDE) is not supported, therefore, the following APIs are not supported and will throw a `4xx` exception if used in the AWS GovCloud (US-West) Region.

- DescribeEnvironments
- ListEnvironments
- DescribeEnvironmentStatus
- CreateEnvironmentEC2
- DeleteEnvironment

Simulation WorldForge is not supported, therefore, the following APIs are not supported and will throw a `4xx` exception if used in the AWS GovCloud (US-West) Region.

- CreateWorldGenerationJob
- DescribeWorldGenerationJob
- ListWorldGenerationJobs
- CancelWorldGenerationJob
- CreateWorldExportJob
- DescribeWorldExportJob
- ListWorldExportJobs
- CancelWorldExportJob
- CreateWorldTemplate
- DeleteWorldTemplate
- DescribeWorldTemplate
- GetWorldTemplateBody
- ListWorldTemplates

- UpdateWorldTemplate
- BatchDeleteWorlds
- DescribeWorld
- ListWorlds

Documentation for AWS RoboMaker

AWS RoboMaker documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

Permissions required for a simulation job

When you create a simulation job, it must have an IAM role with the permissions below.

- Replace `my-input-bucket` with the name of the bucket containing the robot and simulation application bundles.
- Replace `my-output-bucket` to point to the bucket were AWS RoboMaker will write output files.
- Replace `account#` with your account number.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Action": "s3:ListBucket",
          "Resource": [
```

```
                "arn:aws:s3:::my-input-bucket"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": [
                "arn:aws:s3:::my-input-bucket/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": "s3:Put*",
            "Resource": [
                "arn:aws:s3:::my-output-bucket/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DescribeLogStreams"
            ],
            "Resource": [
                "arn:aws:logs:*:account#:log-group:/aws/robomaker/SimulationJobs*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ecr:BatchGetImage",
                "ecr:GetAuthorizationToken",
                "ecr:BatchCheckLayerAvailability",
                "ecr:GetDownloadUrlForLayer"
            ],
            "Resource": "arn:partition:ecr:region:account#:repository/repository_name",
            "Effect": "Allow"
        }
    ]
```

```
}
```

The policy must be attached to a role with the following trust policy.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Principal": { "Service": "robomaker.amazonaws.com" },
        "Action": "sts:AssumeRole",
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "account#" // Account where the simulation job
 resource is created
            },
            "StringEquals": {
                "aws:SourceArn": "arn:aws:robomaker:region:account#:simulation-job/*"
            }
        }
    }
}
```

Condition keys prevent an AWS service from being used as a confused deputy during transactions between services. See SourceAccount and SourceArn for additional information about condition keys.

AWS RoboMaker updates to AWS managed policies

View details about updates to AWS managed policies for AWS RoboMaker since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the AWS RoboMaker Document history page.

Change	Description	Date
AWSRoboMaker_FullAccess – New policy	AWS RoboMaker added a new policy to allow access to resources it needs to successfully run.	July 27, 2021

Change	Description	Date
	This policy gives AWS RoboMaker access to the Amazon ECR images or zip files that you've stored on Amazon S3 to create your robot and simulation applications. It also gives AWS RoboMaker the ability to access the Amazon EC2 it needs to run successfully.	
AWSRoboMakerReadOnlyAccess – New policy	AWS RoboMaker added a new policy to allow read only access to AWS RoboMaker resources.	January 11, 2022
AWS RoboMaker started tracking changes	AWS RoboMaker started tracking changes for its AWS managed policies.	July 27, 2021

Document history

The following table shows when features and deprecations were applied to the AWS RoboMaker service and documentation.

Change	Description	Date
IDE deprecation	Deprecated the AWS RoboMaker IDE	12/15/2022
Preinstalled RUG deprecation	Deprecated preinstalled Robot Operating Software (ROS), Ubuntu, and Gazebo base images and migrated	3/15/2022

Change	Description	Date
	AWS RoboMaker simulation jobs to container images.	
Application deployment deprecation	Deprecated application deployment for AWS RoboMaker.	1/31/2022
Cloud extensions deprecation	Deprecated cloud extensions for AWS RoboMaker.	1/31/2022
Samples deprecation	Deprecated self-driving reinforcement, navigation, person detection, and voice command samples for AWS RoboMaker.	5/15/2020
Support for tags	Added support for tags to many AWS RoboMaker resources.	1/24/2019
New service and guide	The initial release of AWS RoboMaker and the *AWS RoboMaker Developer Guide*.	11/07/2018

AWS SDK for SAP ABAP

AWS SDK for SAP ABAP provides an interface to the services offered by AWS in the ABAP language. Using the SDK, you can implement ABAP BADIs, reports, transactions, OData services, and other ABAP artifacts on AWS services.

How AWS SDK for SAP ABAP Differs for AWS GovCloud (US)

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

Documentation for AWS SDK for SAP ABAP

AWS SDK for SAP ABAP documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- No data will leave the AWS GovCloud (US) Regions for AWS SDK for SAP ABAP.
- The services used with the SDK can handle the export-controlled content differently. For more information, see Services in AWS GovCloud (US) Regions.

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

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)

Product integrations

Not all integrations with AWS Services and third-party partners are available in the AWS GovCloud (US) Region.

For a list of the supported integrations in the AWS GovCloud (US) Region, see Integrations that are supported in AWS GovCloud (US-East) and AWS GovCloud (US-West).

Controls

Not all security controls are supported in the AWS GovCloud (US) Region. For details, see the following lists in the *AWS Security Hub User Guide*.

- Controls that are not supported in AWS GovCloud (US-East)
- Controls that are not supported in AWS GovCloud (US-West)

Cross-Region aggregation

Cross-Region aggregation is supported with limitations in AWS GovCloud (US). In AWS GovCloud (US), cross-Region aggregation is supported only for findings, finding updates, and insights across AWS GovCloud (US). Specifically, you can only aggregate findings, finding updates, and insights between AWS GovCloud (US-East) and AWS GovCloud (US-West).

Documentation for Security Hub

AWS Security Hub documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

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 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.
- Stack Sets are not currently supported in AWS GovCloud (US) Regions.

Documentation for Service Catalog

AWS Service Catalog documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- No export-controlled data may be entered, stored, or processed by AWS Service Catalog. For example, AWS Service Catalog metadata is not permitted to contain export-controlled data. This metadata includes all the configuration data that you enter when creating and maintaining your Products, Actions, and Tag Options.

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal

course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

AWS Server Migration Service

> **Important**
>
> **Product update**
> On March 31, 2022, AWS discontinued AWS Server Migration Service (AWS SMS). We recommend AWS Application Migration Service as the primary migration service for lift-and-shift migrations in AWS GovCloud (US).

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Virtual machine metadata is not permitted to contain export-controlled data. For example, text displayed outside of a virtual machine console in vSphere Client, SCVMM, or Hyper-V Manager is not permitted to contain export-controlled data.
- Do not enter export-controlled 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 export-controlled data into the root or boot partition of any virtual machine being imported using the AWS Server Migration Service

AWS SimSpace Weaver

AWS SimSpace Weaver is a service that you can use to build and run large-scale spatial simulations in the AWS Cloud. For example, you can create crowd simulations, large real-world environments, and immersive and interactive experiences.

With SimSpace Weaver, you can distribute simulation workloads across multiple Amazon Elastic Compute Cloud (Amazon EC2) instances. SimSpace Weaver deploys the underlying AWS

infrastructure for you, and handles the simulation data management and network communication between the Amazon EC2 instances running your simulation.

How AWS SimSpace Weaver Differs for AWS GovCloud (US)

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

Documentation for AWS SimSpace Weaver

SimSpace Weaver documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Simulation name
- Log destination resource name
- Domain name
- Schema file path
- App binary name
- App binary file path
- Resource tags

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- AWS Site-to-Site VPN metadata is not permitted to contain export-controlled 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 export-controlled data into user input fields such as the following:

  - Display Name
  - Topic Policy
  - Topic Delivery Policy
  - Topic ARN
  - Endpoint

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).
- Snowcone is not available.
- Snowball with Tape Gateway is not available.
- AWS Snow Device Management service is not available.
- AWS Snow Family Large Data Migration Manager is not available.
- Amazon EKS Anywhere on Snow is not available.

Documentation for AWS Snow Family

AWS Snow Family documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Snow Family metadata is not permitted to contain export-controlled 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 export-controlled 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 export-controlled data.

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.
- Support to call third-party APIs is not available.
- Support to use the TestState API is not available.

Documentation for AWS Step Functions

AWS Step Functions documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- No data will leave the AWS GovCloud (US) Regions for this service.

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).
- TLS-enabled endpoint are available.
- AWS Storage Gateway Hardware Appliance is not supported for use with the AWS Storage Gateway service running in the AWS GovCloud (US) Region.

Documentation for AWS Storage Gateway

AWS Storage Gateway documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- AWS Storage Gateway metadata is not permitted to contain export-controlled 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 export-controlled 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.

Gateway Type	AMI ID
File Gateway	ami-0b5d2a6a us-gov-west-1

AWS Support

AWS Support offers a range of support plans that provide access to tools and technical help to support the success and operational health of your AWS solutions. For more information, see Signing Up for AWS GovCloud (US)AWS Support.

To create a new case, sign in to the AWS GovCloud (US) Region Support Center with your AWS GovCloud (US) credentials.

> **Important**
>
> Do not enter any export-controlled data in your support cases.

How AWS Support Differs for AWS GovCloud (US)

- AWS Trusted Advisor is available in AWS GovCloud (US), but some AWS Trusted Advisor checks and features are not available. For more information, see .
- 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.
- AWS Partner-Led Support is available in all AWS Regions however Diagnostic Tools and case management are not available in AWS GovCloud (US) Regions, ADCs.

Documentation for AWS Support

See the following topics:

- AWS Support User Guide
- AWS Support API Reference

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Support engineers in the AWS Region (`aws` partition) can access support cases from the AWS GovCloud (US) Region.
- Do not enter any export-controlled data in your support cases.

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)

- In the OpsCenter capability, markdown support in the OpsItem description field in the console is not available.
- AWS Systems Manager Application Manager cost management is not available.
- Support for viewing association histories is not available.
- 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
```

- AWS Systems Manager Change Manager is not available.
- Delegated administrator for AWS Systems Manager Explorer is not available.
- Quick Setup doesn't support cross account or cross Region configurations in AWS GovCloud (US) Regions.
- Quick Setup for Organizations is not available.
- Incident Manager is not available.

- Patch Policies feature is not available.

Documentation for AWS Systems Manager

AWS Systems Manager documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- The following AWS Systems Manager metadata fields are not permitted to contain export-controlled data:
  - Document names
  - Parameter Store parameter names
  - Patch group names (that is, the value of the Patch Group tag)

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) and Amazon Elastic File System (Amazon EFS) file systems 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).
- Applicability Statement 2 (AS2).

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 internal 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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- AWS Transfer Family metadata is not permitted to contain export-controlled data.

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 for Trusted Advisor check summaries aren't supported in the AWS GovCloud (US) Regions.
- The organizational view feature is currently not supported in the AWS GovCloud (US) Regions.
- For a list of supported checks in the AWS GovCloud (US) Regions, see Supported Trusted Advisor checks. You can also sign in to the Trusted Advisor console.
- Email notifications for Trusted Advisor Priority recommendation summaries aren't supported in the AWS GovCloud (US) Regions.
- Not all checks are automatically refreshed. For checks not automatically refreshed, customers can manually refresh via the Console or API.

Supported Trusted Advisor checks

The following tables list the Trusted Advisor checks that are available in the AWS GovCloud (US) Regions and the required support level.

Topics

Cost optimization

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

Check	Support level
Amazon EC2 Instances Stopped	Business and Enterprise
Amazon ECR Repository Without Lifecycle Policy Configured	Business and Enterprise
AWS Account Not Part of AWS Organizations	Business and Enterprise
Amazon RDS Idle DB Instances	Business and Enterprise
Amazon S3 Bucket Lifecycle Policy Configured	Business and Enterprise
Amazon S3 version enabled buckets without lifecycle policies configured	Business and Enterprise
Idle Load Balancers	Business and Enterprise
Low Utilization Amazon EC2 Instances	Business and Enterprise

Check	Support level
Unassociated Elastic IP Addresses	Business and Enterprise
Underutilized Amazon EBS Volumes	Business and Enterprise

Fault tolerance

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

Check	Support level
Amazon Aurora DB Instance Accessibility	Business and Enterprise
Amazon DynamoDB Table Not Included in Backup Plan	Business and Enterprise
Amazon EBS Not Included in AWS Backup Plan	Business and Enterprise
Amazon EBS Snapshots	Business and Enterprise
Amazon EC2 Auto Scaling Group does not have ELB Health check Enabled	Business and Enterprise
Amazon EC2 Availability Zone Balance	Business and Enterprise
Amazon EC2 Detailed Monitoring Not Enabled	Business and Enterprise
Amazon ECS service using a single AZ	Business and Enterprise
Amazon ECS Multi-AZ placement strategy	Business and Enterprise
Amazon ElastiCache Multi-AZ Clusters	Business and Enterprise
Amazon ElastiCache Redis clusters Automatic Backup	Business and Enterprise
AWS Lambda Functions without a dead-letter queue configured	Business and Enterprise

Check	Support level
Amazon MemoryDB Multi-AZ Clusters	Business and Enterprise
Amazon Redshift cluster automated snapshots	Business and Enterprise
Amazon RDS not in AWS Backup Plan	Business and Enterprise
Amazon RDS Backups	Business and Enterprise
Amazon RDS DB Instance Enhanced Monitoring Not Enabled	Business and Enterprise
Amazon RDS Multi-AZ	Business and Enterprise
Amazon RDS Multi-AZ Standby Instance Not Enabled	Business and Enterprise
Amazon S3 Bucket Logging	Business and Enterprise
Amazon S3 Bucket Replication Not Enabled	Business and Enterprise
Amazon S3 Bucket Versioning	Business and Enterprise
Auto Scaling Group Resources	Business and Enterprise
AWS Site-to-Site VPN has at least one Tunnel in DOWN Status	Business and Enterprise
Auto Scaling Group Health Check	Business and Enterprise
ELB Connection Draining	Business and Enterprise
ELB Cross-Zone Load Balancing	Business and Enterprise
Load Balancer Optimization	Business and Enterprise
VPN Tunnel Redundancy	Business and Enterprise
ActiveMQ Availability Zone Redundancy	Business and Enterprise
RabbitMQ Availability Zone Redundancy	Business and Enterprise

Operational Excellence

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

Check	Support level
Amazon API Gateway Not Logging Execution Logs	Business and Enterprise
Amazon API Gateway REST APIs Without X-Ray Tracing Enabled	Business and Enterprise
Amazon EC2 Instance Not Managed by AWS Systems Manager	Business and Enterprise
Amazon ECR Repository With Tag Immutability Disabled	Business and Enterprise
Amazon ECS clusters with Container Insights disabled	Business and Enterprise
Amazon S3 does not have Event Notifications enabled	Business and Enterprise
Amazon VPC Without Flow Logs	Business and Enterprise
AWS CloudFormation Stack Notification	Business and Enterprise
AWS CloudTrail data events logging for objects in an S3 bucket	Business and Enterprise
AWS CodeBuild Project Logging	Business and Enterprise
AWS Elastic Beanstalk Enhanced Health Reporting Is Not Configured	Business and Enterprise
AWS Elastic Beanstalk with Managed Platform Updates disabled	Business and Enterprise

Check	Support level
AWS Fargate platform version is not latest	Business and Enterprise
AWS Systems Manager State Manager Association in Non-compliant Status	Business and Enterprise
Application Load Balancers and Classic Load Balancers Without Access Logs Enabled	Business and Enterprise
CloudTrail trails is not configured with Amazon CloudWatch Logs	Business and Enterprise
Elastic Load Balancing Deletion Protection Not Enabled for Load Balancers	Business and Enterprise
RDS Cluster Deletion Protection Check	Business and Enterprise
RDS DB Instance Automatic Minor Version Upgrade Check	Business and Enterprise

Performance

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

Check	Support level
Amazon DynamoDB Auto Scaling Not Enabled	Business and Enterprise
Amazon EBS Optimization Not Enabled	Business and Enterprise
Amazon EBS Provisioned IOPS (SSD) Volume Attachment Configuration	Business and Enterprise
Amazon EC2 to EBS Throughput Optimization	Business and Enterprise
Amazon EC2 Virtualization Type is Paravirtual	Business and Enterprise

Check	Support level
High Utilization Amazon EC2 Instances	Business and Enterprise
Large Number of EC2 Security Group Rules Applied to an Instance	Business and Enterprise
Large Number of Rules in an EC2 Security Group	Business and Enterprise
Overutilized Amazon EBS Magnetic Volumes	Business and Enterprise
AWS Lambda Functions without Concurrency Limit configured	Business and Enterprise

Security

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

Check	Support level
Amazon CloudWatch Log Group retention period less than 365 days	All support levels
Amazon EBS Public Snapshots	All support levels
Amazon RDS Security Group Access Risk	Business and Enterprise
Amazon RDS Public Snapshots	All support levels
Amazon S3 Bucket Permissions	All support levels
AWS Backup Vault Without Resource-Based Policy to Prevent Deletion of Recovery Points	Business and Enterprise
AWS CloudTrail Logging	Business and Enterprise
ELB Security Groups	Business and Enterprise

Check	Support level
ELB Listener Security	Business and Enterprise
IAM Access Key Rotation	All support levels
IAM Use	All support levels
IAM Password Policy	Business and Enterprise
Security Groups – Specific Ports Unrestricted	All support levels
Security Groups – Unrestricted Access	Business and Enterprise

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.

Check	Support level
Amazon DynamoDB Throughput	All support levels
Auto Scaling Groups	All support levels
Auto Scaling Launch Configurations	All support levels
AWS CloudFormation Stacks	All support levels
DynamoDB Read Capacity	All support levels
DynamoDB Write Capacity	All support levels
EBS Active Snapshots	All support levels
EBS Cold HDD (sc1) Volume Storage	All support levels
EBS General Purpose SSD (gp2) Volume Storage	All support levels

Check	Support level
EBS General Purpose SSD (gp3) Volume Storage	All support levels
EBS Magnetic (standard) Volume Storage	All support levels
EBS Provisioned IOPS (SSD) Volume Aggregate IOPS	All support levels
EBS Provisioned IOPS SSD (io1) Volume Storage	All support levels
EBS Throughput Optimized HDD (st1) Volume Storage	All support levels
EC2 Reserved Instance Leases	All support levels
ELB Classic Load Balancers	All support levels
ELB Network Load Balancers	All support levels
ELB Application Load Balancers	All support levels
IAM Group	All support levels
IAM Instance Profiles	All support levels
IAM Policies	All support levels
IAM Roles	All support levels
IAM Server Certificates	All support levels
IAM Users	All support levels
Kinesis Shards per Region	All support levels
RDS Cluster Parameter Groups	All support levels
RDS Cluster Roles	All support levels

Check	Support level
RDS Clusters	All support levels
RDS DB Instances	All support levels
RDS DB Parameter Groups	All support levels
RDS DB Security Groups	All support levels
RDS DB Manual Snapshots	All support levels
RDS Event Subscriptions	All support levels
RDS Max Auths per Security Group	All support levels
RDS Option Groups	All support levels
RDS Read Replicas per Master	All support levels
RDS Reserved Instances	All support levels
RDS Subnet Groups	All support levels
RDS Subnets per Subnet Group	All support levels
RDS Total Storage Quota	All support levels
VPC	All support levels
VPC Elastic IP Address	All support levels
VPC Internet Gateways	All support levels

Documentation for AWS Trusted Advisor

See the following topics:

- AWS Trusted Advisor in the AWS Support User Guide
- For more information about Trusted Advisor features, see AWS Trusted Advisor.

- For a complete list of Trusted Advisor checks, see the AWS Trusted Advisor best practice checklist.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

AWS Verified Access

AWS Verified Access provides secure access to corporate applications without a VPN connection. It evaluates each request in real time and determines whether the user has access to the application.

How AWS Verified Access Differs for AWS GovCloud (US)

- 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 Verified Access

Verified Access documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Any metadata that you provide when setting up and maintaining your Verified Access resources, including all configuration data that you enter.

AWS WAF

AWS WAF is a web application firewall that lets you monitor web requests that are forwarded to resources, such as AWS API Gateway and AWS Application Load Balancers. 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.

For list of services that AWS WAF supports, please visit the service page.

How AWS WAF Differs for AWS GovCloud (US)

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

- Managed rule groups that are provided for subscription by AWS Marketplace third party sellers are not available for use in AWS GovCloud (US). The only managed rule groups that are available in AWS GovCloud (US) are the AWS managed rule groups that are provided with AWS WAF. 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.

Documentation for AWS WAF

AWS WAF documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- No export-controlled data may be entered, stored, or processed by AWS WAF. For example, AWS WAF metadata is not permitted to contain export-controlled data.

  For example, do not enter export-controlled data in the following fields:

- Web ACL name
- CloudWatch metric name
- Condition
- Rule name
- String filters and regex pattern set

AWS Well-Architected Tool

AWS Well-Architected Tool (AWS WA Tool) is a service in the cloud that provides a consistent process for measuring your architecture using AWS best practices. AWS WA Tool helps you throughout the product lifecycle by:

- Assisting with documenting the decisions that you make
- Providing recommendations for improving your workload based on best practices
- Guiding you in making your workloads more reliable, secure, efficient, and cost-effective

You can use AWS WA Tool to document and measure your workload using the best practices from the AWS Well-Architected Framework. These best practices were developed by AWS Solutions Architects based on their years of experience building solutions across a wide variety of businesses. The framework provides a consistent approach for measuring architectures and provides guidance for implementing designs that scale with your needs over time.

How AWS Well-Architected Tool Differs for AWS GovCloud (US)

AWS Service Catalog AppRegistry integration with Well-Architected using service-managed attribute groups – The ability to reference Well-Architected metadata in AppRegistry using service-managed attribute groups is not available in AWS GovCloud (US) Regions.

Profiles – Profiles is not available in AWS GovCloud (US) Regions.

Documentation for AWS Well-Architected Tool

AWS WA Tool documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- AWS account IDs associated with workload
- Workload name
- Milestone name
- Review owner

AWS WickrGov

AWS WickrGov is an end-to-end encrypted service that helps organizations collaborate across messaging, calling, file sharing, and screen sharing. Users of AWS WickrGov can also federate with other AWS WickrGov users outside their network.

How AWS WickrGov Differs for AWS GovCloud (US)

- WickrGov is only available in the AWS GovCloud (US-West) Region.
- Federation available only between WickrGov networks in the AWS GovCloud (US-West) Region.
- RDS-Proxy is not available or used in WickrGov.
- Client name will appear changed to AWS WickrGov and utilizes a new AWS WickrGov logo with blue background and white slashes.

Documentation for AWS WickrGov

AWS WickrGov documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer

compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Email addresses of provisioned users within a network leave the AWS GovCloud (US) Regions in the normal course of service use. Do not enter export-controlled information into the email field when provisioning users.
- Network names are visible to the AWS WickrGov service team as part of normal service function. Do not enter export-controlled or sensitive information into the network name field when creating a network.

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.

Documentation for AWS X-Ray

AWS X-Ray documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

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 Z1K6XKP9SAGWDV.
- 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.
- API Gateway mTLS endpoints do not currently support ECDSA server certificates.
- `TLS-CHACHA20-POLY1305-SHA256` is not supported.

The following region-specific API Gateway account IDs are automatically added to your Amazon VPC endpoint service as AllowedPrincipals for private integrations in AWS GovCloud (US):

Region	Account ID
• us-gov-west-1 • us-gov-east-1	• 291049978687 • 044865953448

Documentation for Amazon API Gateway

Amazon API Gateway documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- API Gateway's configuration metadata is not permitted to contain export-controlled data*, including:
  - API Name
  - API Description
  - Authorizer Name

* However customers can send export-controlled data through the customers' deployed APIs, with the caveat that downstream systems need to be compliant (for example, caching cannot be enabled on the API for any export-controlled data).

Amazon AppStream 2.0

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 and Graphics Pro instance types are not supported in the AWS GovCloud (US-East) Region.
- The Windows Server 2012 image is not supported in the AWS GovCloud (US-East) Region.
- Copying AppStream 2.0 images from the AWS GovCloud (US) Regions to other AWS Regions is not supported.
- The AppStream 2.0 user pool is not supported.

- The following CloudFormation resources are not available in AWS GovCloud (US):
  - AWS::AppStream::User
  - AWS::AppStream::StackUserAssociation
- The following AppStream 2.0 API actions are not supported in AWS GovCloud (US):
  - 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.

Configure the Relay State of Your Federation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon AppStream 2.0 metadata is not permitted to contain export-controlled 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 export-controlled data in the following console fields or when using the AppStream 2.0 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 export-controlled images, do not use pre-signed URLs for the CLI argument.

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)

- Granting AWS 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 Amazon Athena

Amazon Athena documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon Athena metadata is not permitted to contain export-controlled data. This metadata includes:
  - Database Name
  - Table Name
  - Partitions
  - Query Names
  - Query Strings

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)

- RDS Proxy 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.
- Aurora PostgresSQL cross-Region read replicas is not available in AWS GovCloud (US) Regions.
- 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.
- 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.
- Exporting to Amazon S3 and loading data from Amazon S3 are not available.
- Backtracking is not available.
- Aurora Serverless v1 is not available.
- Aurora multi-master clusters feature is not available.
- Aurora MySQL binlog replication from other AWS Regions to the AWS GovCloud (US) Regions or from AWS GovCloud (US) Regions to other AWS Regions isn't supported.
- Since the AWS GovCloud (US) Regions use a unique certificate authority (CA), update your DB clusters for the AWS GovCloud (US) Regions to use the Region-specific certificate identified

by `rds-ca-rsa4096-g1` in DescribeCertificates calls as soon as possible. The remaining instructions described in the Rotating your SSL/TLS certificate topic are the same, except for the certificate identifier.

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon RDS metadata is not permitted to contain export-controlled data. This metadata includes all configuration data that you enter when creating and maintaining your Amazon RDS instances except the master password.
- Do not enter export-controlled data in the following fields:
  - Database Cluster Identifier
  - Database instance identifier
  - Master user name
  - Database name
  - Database snapshot name
  - Database security group name
  - Database security group description
  - Database cluster parameter group name
  - Database cluster parameter group description
  - Database subnet group name

- Database subnet group description
- Event subscription name
- Resource tags

If you are processing export-controlled data with Amazon RDS, follow these guidelines in order to maintain export compliance:

- When you use the console or the AWS APIs, the only data field that is protected as export-controlled 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 export-controlled data into any data fields by using your database client-side tools. Do not pass export-controlled data by using the web service APIs that are provided by Amazon RDS.
- To secure export-controlled 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 export-controlled 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 export 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 export-controlled 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 export-controlled environments to export-controlled database instances.

If you are processing export-controlled data with this service, use the SSL (HTTPS) endpoint to maintain export compliance. For more information, see Service Endpoints.

Amazon Bedrock

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

Amazon Bedrock provides a broad set of capabilities you need to build generative AI applications, simplifying development while maintaining privacy and security. You can easily experiment with Foundation Models (FMs) and privately customize them. Since Amazon Bedrock is serverless, you don't have to manage any infrastructure, and you can securely integrate and deploy generative AI capabilities into your applications.

How Amazon Bedrock Differs for AWS GovCloud (US)

- Only Amazon Titan Express is available in AWS GovCloud (US-West) only.
- Support for continued pre-training model, model evaluation, Agents, and Knowledge base is not yet available.
- Provisioned throughput options of 1-month and 6-month term is not available. (No-commit option for customized models is available)

Documentation for Amazon Bedrock

Amazon Bedrock documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

The following customer-defined metadata may leave the AWS GovCloud (US) Regions only when the customer asks AWS to investigate a reported issue:

- Custom model metadata
- Provisioned throughput metadata for the no-commit option

Amazon Chime SDK

With the Amazon Chime SDK, you can quickly add voice, video, and screen sharing into your websites and mobile applications. Built-in machine learning provides noise and echo reduction to improve audio quality, and background replacement and blur to help improve visual privacy. Innovate faster by using the Amazon Chime SDK communication building blocks for secure customer communications that scale up or down to meet demand.

How Amazon Chime SDK Differs for AWS GovCloud (US)

- WebRTC media sessions (meetings-chime)
  - Sessions can be hosted in AWS GovCloud (US) Regions only
  - The nearest AWS Region can be discovered via https://nearest-us-gov-media-region.l.chime.aws
  - Live transcription only uses Amazon Transcribe in the AWS GovCloud (US-West) Region
  - Live transcription does not support Amazon Transcribe Medical
- The following Amazon Chime SDK features are not supported:
  - Media Pipelines (media-pipelines-chime)
  - PSTN Audio (service.chime)
  - SIP Trunking (service.chime)
  - Messaging (messaging-chime)
  - Identity (identity-chime)
  - Console
- Amazon Chime SDK in AWS GovCloud (US) is in a separate AWS partition from other AWS Regions. Therefore, it does not support cross-partition integration with other AWS services, such as Amazon CloudWatch, Amazon EventBridge, Amazon Simple Notification Service, Amazon Simple Queue Service and Amazon Transcribe.

Documentation for Amazon Chime SDK

Amazon Chime SDK documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

Amazon Chime SDK metadata is not permitted to contain export-controlled data. This metadata includes all configuration data that you enter or parameters that you supply in API requests.

Do not enter export-controlled data in the following fields:

- External Meeting Id
- External User Id
- Tags

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon Cloud Directory metadata is not permitted to contain export-controlled data. This metadata includes configuration data that you enter when creating and maintaining your Cloud Directory.
- Do not enter export-controlled data in the following fields:
  - Schema name
  - Directory name

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)

- The GetMetricWidgetImage API is not available.
- Dashboard sharing is not available.
- CloudWatch real user monitoring (RUM) is not available.
- You cannot create CloudWatch alarms for Trusted Advisor metrics in AWS GovCloud (US).
- Amazon CloudWatch cross-account observability is not available in AWS GovCloud (US).

Documentation for Amazon CloudWatch

Amazon CloudWatch documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal

course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Alarm Name and Description
- Alarm configuration
- Alarm tags
- Metric Name
- Metric Namespace
- Metric Dimensions

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- No export-controlled data may be entered, stored, or processed by CloudWatch Events. For example, CloudWatch Events metadata is not permitted to contain export-controlled data. This metadata includes all the configuration data that you enter when creating and maintaining your CloudWatch Events alarms.

For example, do not enter export-controlled data in the following fields:

- Rule names
- Rule descriptions
- Event patterns
- Data input to APIs

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.
- The `logGroupNamePattern` parameter is not supported for use in the describe-log-groups AWS CLI command or the DescribeLogGroups API.

Documentation for Amazon CloudWatch Logs

Amazon CloudWatch Logs documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- CloudWatch Log Group Names
- CloudWatch Log Stream Names
- Log group tags

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.

- Amazon Cognito isn't currently available in AWS GovCloud (US-East).
- Advanced security features in user pools aren't supported in AWS GovCloud (US).
- Amazon Pinpoint integration with user pools isn't suported in AWS GovCloud (US).
- Access token customization and pre token generation Lambda trigger event versions greater than 1 aren't supported in AWS GovCloud (US).
- Amazon Cognito in AWS GovCloud (US) uses FIPS endpoints only.
  - The API service endpoint is `cognito-idp-fips.us-gov-west-1.amazonaws.com`
  - Hosted UI endpoints have a URL path in the format *`<your_user_pool_domain>`*`.auth-fips.us-gov-west-1.amazoncognito.com`
- Custom domains for user pools aren't supported in AWS GovCloud (US).

The IAM roles that you assign to users with Amazon Cognito identity pools must have a trust policy that allows Amazon Cognito to generate temporary sessions. In AWS GovCloud (US), your trust policies must grant `AssumeRoleWithWebIdentity` permission to the `cognito-identity-us-gov.amazonaws.com` service principal. The following example trust policy allows the identity pool `us-gov-west-1:12345678-corner-cafe-123456790ab` to grant IAM credentials to unauthenticated guest users.

```
{
   "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-gov-west-1:12345678-
corner-cafe-123456790ab"
            },
            "ForAnyValue:StringLike":{
               " cognito-identity-us-gov.amazonaws.com:amr":"unauthenticated"
            }
         }
      }
   ]
}
```

Documentation for Amazon Cognito

Amazon Cognito documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- 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.

  For example, user pool domains, custom attribute names, resource server identifiers and custom scopes may be included as part of the public Cognito sign-in and sign-up functionality.

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)

- In AWS GovCloud (US) Regions, AWS DOES NOT use or store AI Content processed by this AI Service to develop and improve that Service or technologies of AWS or its affiliates. Opt-out policies are not currently applicable to these Regions.

Documentation for Amazon Comprehend

Amazon Comprehend documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

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 Quotas/Limits:

Resource	Default
Transactions per second (TPS) for the `DetectEntities-v2` and `DetectEntities` operations	2
Transactions per second (TPS) for the `DetectPHI` operation	5
Transactions per second (TPS) for the `StartEntitiesDetectionV2Job` , `StartPHIDetectionJob` , `StopEntitiesDetectionV2Job` , `StopPHIDetectionJob` , `ListEntitiesDetectionV2Jobs` , `ListPHIDetectionJobs` , `DescribeEntitiesDetectionV2Job` , and `DescribePHIDetectionJob` operations	2

Documentation for Amazon Comprehend Medical

Amazon Comprehend Medical documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

Amazon Connect

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

Amazon Connect is an easy to use omnichannel cloud contact center that helps you provide superior customer service at a lower cost. It provides a seamless experience across voice and chat for your customers and agents. This includes one set of tools for skills-based routing, powerful real-time and historical analytics, and intuitive management tools – all with pay-as-you-go pricing, which means Amazon Connect simplifies contact center operations, improves agent efficiency, and lowers costs. You can set up a contact center in minutes that can scale to support millions of customers from the office or as a virtual contact center.

How Amazon Connect Differs for AWS GovCloud (US)

Amazon Connect in AWS GovCloud (US) differs from other commercial Regions in the following ways:

- Amazon Connect instances in AWS GovCloud (US) use the domain ***.govcloud.connect.aws**
- It supports only the latest Contact Control Panel (CCP) for both voice and chat contacts for agents. The earlier CCP is not supported.
- It supports only the latest contact search experience, as described in What's new in contact search.
- Amazon Connect in AWS GovCloud (US) is in a separate partition from all commercial Regions. Therefore it does not support cross-partition integration with other AWS services – such as Amazon Lex, Amazon Lambda, Amazon Kinesis, Amazon S3, Amazon CloudWatch, amongst others – that are available in commercial Regions.
- The following Amazon Connect features are not supported.
  - Contact Lens for Amazon Connect
  - Amazon Connect Customer Profiles
  - Amazon Q in Connect
  - Amazon Connect Voice ID
  - Amazon Connect Live Media Streaming
  - Amazon Connect Chat integration with Apple Business Chat
  - Amazon Connect Forecasting, Capacity Planning and Scheduling
  - Amazon Connect Cases

- Amazon Connect Outbound Campaigns
- Granular access controls for real-time metrics

Documentation for Amazon Connect

Amazon Connect documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon Connect instance and resource configuration metadata is not permitted to contain export-controlled data. This metadata includes all configuration data (for example, name, alias, description, tags) that you enter when creating and maintaining your Amazon Connect instance and resources within an instance, such as users, queues, routing profiles, contact flows, or scheduled report names.

Amazon Detective

Amazon Detective makes it easy to analyze, investigate, and quickly identify the root cause of security findings or suspicious activities. Detective automatically collects log data from your AWS resources. It then uses machine learning, statistical analysis, and graph theory to help you visualize and conduct faster and more efficient security investigations.

How Detective Differs for AWS GovCloud (US)

- In GovCloud Regions, Detective does not validate the email address for member accounts, and does not send invitation emails to member accounts.
- When accounts are terminated in AWS, Detective cannot automatically remove them from the behavior graph.

Documentation for Amazon Detective

Detective documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- 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.

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon DocumentDB metadata is not permitted to contain export-controlled 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 export-controlled data in the following fields:

  - 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 export-controlled data with Amazon DocumentDB, follow these guidelines in order to maintain export compliance:

- When you use the console or the AWS APIs, the only data field that is protected as export-controlled 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 export-controlled data into any data fields by using your database client-side tools. Do not pass export-controlled data by using the web service APIs that are provided by Amazon DocumentDB.
- To secure export-controlled 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 export-controlled 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 export 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 export-controlled 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 export-controlled environments to export-controlled clusters.

If you are processing export-controlled data with this service, use the SSL (HTTPS) endpoint to maintain export compliance. For more information, 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)

- **Export Table** is not available in the DynamoDB console.
- DynamoDB Accelerator(DAX) is not available.

Documentation for Amazon DynamoDB

Amazon DynamoDB documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- DynamoDB metadata is not permitted to contain export-controlled 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 export-controlled data in the following fields:
  - Table names
  - Hash attribute names
  - Range attribute names
  - Resource tags

If you are processing export-controlled data with this service, use the SSL (HTTPS) endpoint to maintain export compliance. For more information, see Service Endpoints.

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.
- Amazon EBS Multi-Attach is not available.

Documentation for Amazon Elastic Block Store

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

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

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon EBS metadata is not permitted to contain export-controlled data. This metadata includes all configuration data that you enter when creating and maintaining your Amazon EBS volumes.
- Do not enter export-controlled data in the following fields:
  - Volume names
  - Snapshot names
  - Image names
  - Image descriptions

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 Amazon EC2 VM Import/Export.
- 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.
- 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 **–z *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.
- The AWS Certificate Manager (ACM) for Nitro Enclaves AMI is not available from the AWS Marketplace. ACM for Nitro Enclaves must be installed from the Amazon Linux Extras repository.
- The Nitro Enclaves Developer AMI is not available from the AWS Marketplace.
- Spot Instance data feed is not available.
- Attestation documents used by Nitro Enclaves are signed by the AWS Nitro Attestation Public Key Infrastructure (PKI). You can verify that the attestation documents are signed by the Nitro Attestation PKI. For more information, see Verifying the root of trust in the *AWS Nitro Enclaves User Guide*.
  - The root certificate for the Nitro Attestation PKI is unique for each partition. The root certificate for the `aws-us-gov` partition is as follows:

```
-----BEGIN CERTIFICATE-----
MIICIDCCAaWgAwIBAgIQP+wUYfyWFFRko9PR00zhZzAKBggqhkjOPQQDAzBQMQsw
CQYDVQQGEwJVUzEPMA0GA1UECgwGQW1hem9uMQwwCgYDVQQLDANBV1MxIjAgBgNV
BAMMGWF3cy11cy1nb3Yubml0cm8tZW5jbGF2ZXMwIBcNMjAwOTEwMTIwMzQ2WhgP
MjA1MDA5MTAxMzAzNDZaMFAxCzAJBgNVBAYTAlVTMQ8wDQYDVQQKDAZBbWF6b24x
DDAKBgNVBAsMA0FXUzEiMCAGA1UEAwwZYXdzLXVzLWdvdi5uaXRyby1lbmNsYXZl
```

```
czB2MBAGByqGSM49AgEGBSuBBAAiA2IABCzkRJcZVx7Sg2yXXkl0Nqj9o1ECZNAh
0L8/90ATZXAaS1rxA1ti1F3wE86PGsh2UiQIYXiMu81l5kO7775gPuLsgYcGMO/J
0t08BHI8s3+JmjxTlA+/UyAqEmj7fD5CbKNCMEAwDwYDVR0TAQH/BAUwAwEB/zAd
BgNVHQ4EFgQUUKIzFk2FAlhihuQexsqOxZ5ZjF0wDgYDVR0PAQH/BAQDAgGGMAoG
CCqGSM49BAMDA2kAMGYCMQD9bO9epcf5kMSdsHcyNJXs4bo07wvTIOwnxN41t5eE
SDyXtUei++RebAbI9Viap2gCMQC7PVZ6Kpg0+N9k+DDpksoJv7gx6YwCqKsmTfU/
WigyQlpyJUrWapqk0afDA4lef14=
-----END CERTIFICATE-----
```

- The Nitro Attestation PKI root certificate for the `aws-us-gov` partition has a subject as follows:

  `CN=aws-us-gov.nitro-enclaves, C=US, O=Amazon, OU=AWS`

- The `lastLaunchedTime` AMI attribute is not available.
- The CLI function get-console-screenshot is not available.
- Get instance screenshot is not available in AWS GovCloud (US).
- When you use the new launch instance wizard in the console to launch an instance with an AWS Marketplace AMI, we don't automatically subscribe you to the AMI in AWS GovCloud (US). (in other AWS Regions we automatically subscribe you). Instead, when you choose the AMI, choose **Subscribe with Marketplace** to open the AWS Marketplace website and subscribe there.
- Amazon EC2 instance topology is not available.

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*.

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon EC2 metadata is not permitted to contain export-controlled data. This metadata includes all configuration data that you enter when creating and maintaining your instances.
- Do not enter export-controlled data in the following fields:
  - Instance names
  - AMI descriptions
  - Resource tags
- Key pairs created using HTTP.
- When using VM Import, you may not enter any export-controlled data as part of CLI arguments, paths, or OS disk images. Any data that is export-controlled should be encrypted and placed in partitions other than root and boot.
- If importing export-controlled images, do not use pre-signed URLs for the CLI argument **--manifest-url**.

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.
- `Hibernated` is not available as a pool state when creating or updating a warm pool.

Documentation for Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Auto Scaling is not permitted to contain export-controlled data.
- For example, do not enter export-controlled data in the following fields:
  - Capacity group tag names
  - Capacity group tag name values
  - Capacity group names
  - Amazon EC2 Security Group names
  - Scaling policies
  - Launch notifications
  - Notification topics
  - Policy documents

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)

The implementation of Amazon EC2 Image Builder is different for AWS GovCloud (US) Regions in the following ways:

- Image Builder doesn't support image lifecycle policies in AWS GovCloud (US) Regions.

Documentation for Amazon EC2 Image Builder

For more information about Amazon EC2 Image Builder, see the Amazon EC2 Image Builder documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- EC2 Image Builder metadata is not permitted to contain export-controlled 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 export-controlled data in the following console fields:

  - Names
  - Description
  - Resource tags

Amazon EC2 VM Import/Export

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, 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

Amazon EC2 VM Import/Export documentation.

Export Best Practices

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

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 cross-region and cross-account replication isn't supported.
- Amazon ECR pull through cache rules aren't supported.
- Amazon ECR public registries aren't supported.
- The Amazon ECR Public Gallery isn't hosted in AWS GovCloud (US) however, if external internet access is available, you should be able to reach and pull container images from the gallery.

Documentation for Amazon Elastic Container Registry

Amazon Elastic Container Registry documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Do not enter export-controlled data in the following fields:
  - Repository name
  - Image tag
  - Image manifest
  - Lifecycle policy
  - Repository policy

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)

- The Amazon ECS-optimized AMI variant of the Bottlerocket operating system is not available when launching Amazon ECS container instances.
- Amazon ECS Service Connect is not supported.

Documentation for Amazon Elastic Container Service

Amazon Elastic Container Service documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Do not enter export-controlled data in the following fields:
  - Cluster name
  - Service name
  - Attribute name
  - Attribute value
  - Task definitions
  - Task group
  - Task overrides
  - Task started by
  - Placement constraints

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)

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

Documentation for Amazon Elastic File System

Amazon Elastic File System documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Do not enter export-controlled data into the following fields:
  - Resource Tags

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 isn't available.
- Amazon Managed Service for Prometheus isn't available.

- Mountpoint for Amazon S3 CSI Driver is only available for AWS GovCloud (US) Regions as a self-managed installation.
- Amazon EKS Anywhere isn't available.
- Amazon EKS Upgrade insights aren't available.
- Amazon EKS Pod Identities aren't available.

Documentation for Amazon EKS

Amazon EKS documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Do not enter export-controlled data in the following fields:
  - Cluster name
  - Fargate profile name
  - Node group name

If you are processing export-controlled data with this service, use the SSL (HTTPS) endpoint to maintain export compliance. For more information, see Service Endpoints.

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.
- The r6gd node type and data-tiering are not available in AWS GovCloud (US).
- AWS Key Management Service for encryption at rest is not available in AWS GovCloud (US). Default (service managed) encryption is available.

Documentation for Amazon ElastiCache

Amazon ElastiCache documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Unencrypted data stored in a cache cluster may not contain export-controlled data.
- ElastiCache metadata is not permitted to contain export-controlled data. This metadata includes all the configuration data that you enter when creating and maintaining your ElastiCache clusters.
- Do not enter export-controlled data in the following fields:
  - Cluster instance identifier
  - Cluster name
  - Cluster snapshot name
  - Cluster security group name
  - Cluster security group description
  - Cluster parameter group name
  - Cluster parameter group description
  - Cluster subnet group name

- Cluster subnet group description
- Replication group name
- Replication group description

If you are processing export-controlled data with ElastiCache, follow these guidelines in order to maintain export compliance:

- To secure export-controlled 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 export-controlled 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 export 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 export-controlled 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 export-controlled environments to export-controlled clusters.

ElastiCache requires the use of the SSL (HTTPS) endpoint for service API calls. For more information, see Service Endpoints.

Amazon EMR

Amazon EMR is a cloud big data platform for running large-scale distributed data processing jobs, interactive SQL queries, and machine learning (ML) applications using open-source analytics frameworks such as Apache Spark, Apache Hive, and Presto.

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, 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 Set up a VPC to host clusters.
- Launching a job flow with debugging is not currently supported.
- Auto-termination for idle clusters using an auto-termination policy is not available.
- Amazon EMR on EKS on Fargate is not available.
- Amazon EMR with AWS Lake Formation is not available.

Documentation for Amazon EMR

Amazon EMR documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon EMR metadata is not permitted to contain export-controlled data. This metadata includes all configuration data that you enter when creating and maintaining your job flows.
- Do not enter export-controlled data in Amazon EMR when doing the following:
  - Naming a job flow
  - Specifying a file location
  - Naming a bootstrap action
  - Providing arguments
  - Resource tags
- Export-controlled data should not be printed to your logs. (Amazon EMR metadata and logs are not permitted to contain export-controlled data.)

If you are processing export-controlled data with this service, use the SSL (HTTPS) endpoint to maintain export compliance. For more information, see Service Endpoints.

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.
- Setting up partner event sources to receive events from Software-as-a-Service (SaaS) Partner applications and services is not supported.
- EventBridge scheduler is not available in AWS GovCloud (US).
- Amazon API Gateway is not supported as an event bus target.
- The following content filtering options for even matching are available only in the AWS GovCloud (US-West) region.
  - Suffix matching
  - Equals-ignore-case matching
  - Match any conditions across multiple separate fields using $ or ?
  - Increased numeric values ranges of -5.0e9 to +5.0e9, up from -1e9 to 1e9

Documentation for Amazon EventBridge

Amazon EventBridge documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- No data will leave the AWS GovCloud (US) Regions for this service.

Amazon FSx

Amazon FSx makes it easy and cost effective to launch and run popular file systems. With Amazon FSx, you can leverage the rich feature sets and fast performance of widely-used open source and commercially-licensed file systems, while avoiding time-consuming administrative tasks like hardware provisioning, software configuration, patching, and backups. It provides cost-efficient capacity and high levels of reliability, and it integrates with other AWS services so that you can manage and use the file systems in cloud-native ways. Amazon FSx let you choose between three widely-used file systems: NetApp ONTAP, Windows File Server, and Lustre.

How Amazon FSx Differs for AWS GovCloud (US)

- Amazon FSx for Lustre Persistent_2 is not available.
- Amazon FSx for OpenZFS is not available.
- Amazon File Cache is not available for Amazon FSx.

Documentation for Amazon FSx

Amazon FSx documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Resource Tags.
- ClientRequestTokens.
- FSx for Windows File Server file system configuration fields:
  - Self-managed Active Directory user names
  - Self-managed Active Directory domain names
  - Self-managed Active Directory organizational unit distinguished names
  - DNS aliases
- FSx for Lustre file system configuration fields:
  - S3 import and export data paths

Amazon GuardDuty

How Amazon GuardDuty differs for AWS GovCloud (US)

The following features are not supported in both the AWS GovCloud (US) Regions:

- Runtime Monitoring
- EKS Runtime Monitoring
- RDS Protection
- Malware Protection
- Cross-region data transfer
- Member accounts invitation notifications through AWS Health Dashboard and email

The following EKS audit log finding types are not available in the GovCloud Regions:

- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed! ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

Documentation for Amazon GuardDuty

Amazon GuardDuty documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

Amazon Inspector Classic

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 Classic Differs for AWS GovCloud (US)

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

Documentation for Amazon Inspector Classic

Amazon Inspector Classic documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

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.

> **Note**
>
> The Amazon Inspector plugin for Linux deep inspection is not FIPS compliant.

How Amazon Inspector Differs for AWS GovCloud (US)

- Lambda code scanning is not available.

Documentation for Amazon Inspector

Amazon Inspector documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal

course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- No data will leave the AWS GovCloud (US) Regions for this service.

Amazon Kendra

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

Amazon Kendra is an intelligent search service powered by machine learning. Amazon Kendra reimagines enterprise search for your websites and applications so your employees and customers can easily find the content they are looking for, even when it is scattered across multiple locations and content repositories within your organization.

How Amazon Kendra Differs for AWS GovCloud (US)

- Amazon Kendra in AWS GovCloud (US) only supports connectors for S3, Sharepoint (Online, 2013 and 2016), Confluence (server and cloud) and custom data source connector. Other data sources are not currently supported.
- IAM Identity Center Integration is not supported.
- Experience Builder is not supported.

Documentation for Amazon Kendra

Amazon Kendra documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- No data will leave the AWS GovCloud (US) Regions for this service.

Amazon Keyspaces (for Apache Cassandra)

Amazon Keyspaces (for Apache Cassandra) is a scalable, highly available, and managed Apache Cassandra–compatible database service. With Amazon Keyspaces, you don't have to provision, patch, or manage servers, and you don't have to install, maintain, or operate software.

Amazon Keyspaces is serverless, so you pay for only the resources that you use, and the service automatically scales tables up and down in response to application traffic. You can build applications that serve thousands of requests per second with virtually unlimited throughput and storage.

How Amazon Keyspaces Differs for AWS GovCloud (US)

- Amazon Keyspaces Multi-Region replication is not supported.
- Amazon Keyspaces integration with AWS CloudFormation is not supported.

This section describes the Amazon Keyspaces quotas and default values in AWS GovCloud (US) Regions that differ from Amazon Keyspaces quotas in other AWS Regions.

Quota	Description	Amazon Keyspaces default
Max read throughput per second	The maximum read throughput per second—read request units (RRUs) or read capacity units (RCUs)—that can be allocated to a table per Region. This default value is adjustable in the AWS Service Quotas console.	10,000
Max write throughput per second	The maximum write throughput per second—write request units (WRUs) or write capacity units (WCUs)—that can be allocated to a table per Region. This default	10,000

Quota	Description	Amazon Keyspaces default
	value is adjustable in the AWS Service Quotas console.	

For more information about quotas in AWS GovCloud (US) Regions, see Service Quotas in the AWS GovCloud (US) User Guide.

Documentation for Amazon Keyspaces

Amazon Keyspaces documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon Keyspaces metadata is not permitted to contain export-controlled data. This metadata includes all the configuration data that you enter when creating and maintaining your Amazon Keyspaces resources such as keyspaces and tables, for example resource names and tags.
- Do not enter export-controlled data in the following fields:
  - Keyspace names
  - Table names
  - Resource tags

Amazon Managed Service for Apache Flink

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 Managed Service for Apache Flink 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 Managed Service for Apache Flink, you only pay for the resources your streaming applications consume. There is no minimum fee or setup cost.

How Amazon Managed Service for Apache Flink Differs for AWS GovCloud (US)

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

Documentation for Amazon Managed Service for Apache Flink

Amazon Managed Service for Apache Flink documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Application names

If you are processing export-controlled data with this service, use the SSL (HTTPS) endpoint to maintain export compliance. For more information, see Service Endpoints.

Amazon 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 OpenSearch Service, 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 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 Data Firehose

Amazon Data Firehose documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Do not enter export-controlled data in the following fields:
  - Stream names

If you are processing export-controlled data with this service, use the SSL (HTTPS) endpoint to maintain export compliance. For more information, see Service Endpoints.

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Do not enter export-controlled data in the following fields:
  - Stream names

If you are processing export-controlled data with this service, use the SSL (HTTPS) endpoint to maintain export compliance. For more information, see Service Endpoints.

Amazon Lex

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

Amazon Lex is an AWS service for building conversational interfaces for applications using voice and text. With Amazon Lex, the same conversational engine that powers Amazon Alexa is now available to any developer, enabling you to build sophisticated, natural language chatbots into your new and existing applications. Amazon Lex provides the deep functionality and flexibility of natural language understanding (NLU) and automatic speech recognition (ASR) so you can build highly engaging user experiences with lifelike, conversational interactions, and create new categories of products.

How Amazon Lex Differs for AWS GovCloud (US)

- Amazon Lex V2 is not available in AWS GovCloud (US). Only Amazon Lex V1 is available.
- Amazon Lex does not support channels, which enable bots to integrate with messaging platforms such as Facebook, Slack, and Twilio.
- The Amazon Lex console does not show utterances or missed utterances. The GetUtterancesView API action is not supported.
- The supported languages include only en-US and es-US.
- Amazon Lex does not support conversation logs, which store interactions to help you review the bot's performance and troubleshoot.

- In AWS GovCloud (US) Regions, AWS DOES NOT use or store AI Content processed by this AI Service to develop and improve that Service or technologies of AWS or its affiliates. Opt-out policies are not currently applicable to these Regions.

Documentation for Amazon Lex

Amazon Lex documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- The following customer-defined metadata may leave the AWS GovCloud (US) Regions only when the customer asks AWS to investigate a reported issue:
  - Bot definitions
  - Intent definitions
  - Slot definitions
  - Session attributes that customers use for the Get customer input block in the Amazon Connect console, such as `x-amz-lex:start-silence-threshold-ms` or `x-amz-lex:end-silence-threshold-ms`. For all session attributes, see Contact block: Get customer input in the Amazon Connect Administrator Guide.

Amazon Location Service

This service is currently available in AWS GovCloud (US-West) only, because Amazon Cognito is not available in AWS GovCloud (US-East).

Amazon Location Service lets you securely add location data to your application. Amazon Location provides access to location-based functionality and data providers through AWS resources. Amazon Location offers five types of AWS resources, depending on the type of functionality you need. Use the different resources together to create a full location-based application.

How Amazon Location Service Differs for AWS GovCloud (US)

- Granting access to resources using API keys is not supported.

Documentation for Amazon Location Service

Amazon Location documentation.

Export-Controlled Content

For AWS services architected within the AWS GovCloud (US) Regions, the following list explains which components of data may leave or remain within the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations.

- When you use the following geolocation data providers, you transmit request parameters (such as location searches) from Amazon Location features (Maps, Places, and Routes) to the geolocation provider for processing, which may be outside of the AWS Region in which your request was made.
  - Esri
  - Here
  - GrabMaps
- The exception is requests to the Open Data geolocation provider, which are processed by AWS in the AWS Region in which your request was made.
- Request parameters transmitted by using Amazon Location features Trackers and Geofences are processed by AWS in the AWS Region in which your request was made.

Amazon Managed Blockchain

Amazon Managed Blockchain is a fully managed service for creating and managing blockchain networks and network resources using open-source frameworks. Blockchain allows you to build applications where multiple parties can securely and transparently run transactions and share data without the need for a trusted, central authority.

You can use Managed Blockchain to create scalable blockchain resources and networks quickly and efficiently using the AWS Management Console, the AWS CLI, or the Managed Blockchain SDK.

> **Note**
>
> Only the Hyperledger Fabric framework on Amazon Managed Blockchain is currently supported in the AWS GovCloud (US-West) Region.

How Hyperledger Fabric on Amazon Managed Blockchain Differs for AWS GovCloud (US)

- This service does not support AWS CloudFormation for Members and Peers creation.

Documentation for Hyperledger Fabric on Amazon Managed Blockchain

Hyperledger Fabric on Managed Blockchain documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- No data will leave the AWS GovCloud (US) Regions for this service.

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)

- Firehose isn't available as a destination for broker logs in AWS GovCloud (US).
- Amazon Managed Streaming for Apache Kafka (MSK) Connect is not available in AWS GovCloud (US).
- Amazon Managed Streaming for Apache Kafka (MSK) Serverless is not available in AWS GovCloud (US).

Documentation for Managed Streaming for Apache Kafka

Amazon Managed Streaming for Apache Kafka (MSK) documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

Amazon MQ

Amazon MQ is a managed message broker service that makes it easy to migrate to a message broker in the cloud. A *message broker* allows software applications and components to communicate using various programming languages, operating systems, and formal messaging protocols. Currently, Amazon MQ supports Apache ActiveMQ and RabbitMQ engine types.

Amazon MQ works with your existing applications and services without the need to manage, operate, or maintain your own messaging system.

How Amazon MQ Differs for AWS GovCloud (US)

Amazon MQ in AWS GovCloud (US) differs from its counterpart in commercial Regions in the following key ways:

- The AWS Free Tier is not available in GovCloud, meaning users cannot access the free resources offered in commercial Regions.
- Amazon MQ in GovCloud Regions does not support cross-Region data replication.
- The instance types supported by Amazon MQ in GovCloud differ from those in commercial Regions. Users should consult the Amazon MQ pricing page for the specific instance types available in their Region.

Documentation for Amazon MQ

Amazon MQ documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon MQ metadata is not permitted to contain export-controlled data. For example, do not enter export-controlled data into user input fields such as the following:
  - Broker name
  - Configuration name
  - Resource tag/key value pairs

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)

- Neptune workbench with Jupyter notebooks is not available.
- Neptune Serverless is not available.

Documentation for Amazon Neptune

Amazon Neptune documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

If you are processing export-controlled data with this service, use the SSL (HTTPS) endpoint to maintain export compliance. For more information, see Service Endpoints.

Amazon OpenSearch Service

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

How Amazon OpenSearch Service Differs for AWS GovCloud (US)

- Amazon Cognito authentication for OpenSearch Dashboards is not supported in the AWS GovCloud (US-East) Region.
- OpenSearch serverless is not available in AWS GovCloud (US).
- OpenSearch ingestion is not available in AWS GovCloud (US).

Documentation for Amazon OpenSearch Service

Amazon OpenSearch Service documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon OpenSearch Service metadata is not permitted to contain export-controlled data. This metadata includes all configuration data that you specify when creating and maintaining your OpenSearch clusters and indices, such as index names, alias names, tags, snapshot names, and repository names.
- Do not enter export-controlled data in the following fields:
  - Domain name
  - Index names
  - Type names
  - Document IDs
  - Snapshot names
  - Resource tags
  - Repository names
  - Alias names
  - CloudWatch log group names

Amazon Pinpoint

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

There are two sets of APIs in Amazon Pinpoint. The Amazon Pinpoint API is currently available in AWS GovCloud (US-West) and the Amazon Pinpoint SMS and voice v2 API is currently available in AWS GovCloud (US-West) and AWS GovCloud (US-East).

How Amazon Pinpoint Differs for AWS GovCloud (US)

- Amazon Pinpoint API
  - 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 **Analytics** section of the Amazon Pinpoint console doesn't include the **Events** page.
  - When you create a campaign, you can't configure the campaign to be sent when an event occurs.
  - 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).
  - You can't create message templates that include recommendations provided by Amazon Personalize.
  - The In-App channel is unavailable.
  - Time zone estimation is not supported.
- Amazon Pinpoint SMS and voice v2 API
  - Text to voice messages are only supported in AWS GovCloud (US-West).

Documentation for Amazon Pinpoint

Amazon Pinpoint documentation, Amazon Pinpoint API documentaiton, Amazon Pinpoint SMS documentaiton and Amazon Pinpoint SMS and voice v2 API documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon Pinpoint metadata is not permitted to contain export-controlled 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.
- Do not enter export-controlled data in the following fields:
  - Keyspace names
  - Table names
  - Column names
  - Resource tags

If you are processing export-controlled data with this service, use the SSL (HTTPS) endpoint to maintain export compliance. For more information, see Service Endpoints.

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)

- In AWS GovCloud (US) Regions, AWS DOES NOT use or store AI Content processed by this AI Service to develop and improve that Service or technologies of AWS or its affiliates. Opt-out policies are not currently applicable to these Regions.

Documentation for Amazon Polly

Amazon Polly documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

Amazon QuickSight

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

Amazon QuickSight is a cloud-scale business intelligence (BI) service that you can use to deliver easy-to-understand insights to the people who you work with, wherever they are. Amazon QuickSight connects to your data in the cloud and combines data from many different sources. In a single data dashboard, Amazon QuickSight can include AWS data, third-party data, big data, spreadsheet data, SaaS data, B2B data, and more. As a fully managed cloud-based service, Amazon QuickSight provides enterprise-grade security, global availability, and built-in redundancy. It also provides the user-management tools that you need to scale from 10 users to 10,000, all with no infrastructure to deploy or manage.

Amazon QuickSight gives decision-makers the opportunity to explore and interpret information in an interactive visual environment. They have secure access to dashboards from any device on your network and from mobile devices.

How Amazon QuickSight Differs for AWS GovCloud (US)

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

- Email based user provisioning is not supported in AWS GovCloud (US).
- Using geospatial visualizations is not supported in AWS GovCloud (US).

- Using Amazon SageMaker integration is not supported in AWS GovCloud (US).
- Amazon QuickSight Q is not supported in AWS GovCloud (US).

Amazon QuickSight in AWS GovCloud (US) supports user authorization for federated users only. Amazon QuickSight directly supports authentication through AWS Identity and Access Management (IAM), AWS IAM Identity Center (IAM Identity Center), and AWS Directory Service for Microsoft Active Directory. For more information, see Identity federation in AWS.

If you're a Amazon QuickSight administrator, make sure to allow-list the following domains within your organization's network.

User type	Domain to allow-list
Native Amazon QuickSight and Active Directory users	awsapps.com and amazonaws-us-gov.com
IAM users	amazonaws-us-gov.com

Specialized configurations that allow users to authenticate with a different identity service can also work, even if not directly supported from inside Amazon QuickSight. For example, you can use Amazon Cognito as is described in the Embedded Analytics Tutorial. This authentication method works because it is compatible and transparent to Amazon QuickSight. For more information on Amazon QuickSight authentication, see Identity and Access Management in Amazon QuickSight.

Note

If you are using the Embedded Analytics Tutorial, you can point to AWS GovCloud (US) ARNs and URLs for your resources, but in the step for the static website that uses Amazon CloudFront and Amazon S3, you need to point to a classic AWS Region, for example US East (N. Virginia), for the tutorial to work. This is not necessary outside the tutorial. For more information and additional examples, see Developing with Amazon QuickSight in the Amazon QuickSight User Guide.

Documentation for Amazon QuickSight

Amazon QuickSight documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- No data will leave the AWS GovCloud (US) Regions for this service.

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 Proxy isn't available.
- Multi-AZ DB clusters aren't available. However, Multi-AZ DB instances are available.
- Amazon RDS Custom for SQL Server isn't available.
- Amazon RDS Kerberos authentication for PostgreSQL DB instances is not available.
- 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.

- Since the AWS GovCloud (US) Regions use a unique certificate authority (CA), update your DB instances for the AWS GovCloud (US) Regions to use the Region-specific certificate identified by `rds-ca-rsa4096-g1` in DescribeCertificates calls as soon as possible. The remaining instructions described in the Rotating your SSL/TLS certificate topic are the same, except for the certificate identifier.
- You cannot migrate from an Amazon RDS DB Instance for MySQL to Amazon Aurora by creating an Aurora Read Replica.

Documentation for Amazon Relational Database Service

Amazon RDS documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon RDS metadata is not permitted to contain export-controlled data. This metadata includes all configuration data that you enter when creating and maintaining your Amazon RDS instances except the master password.
- Do not enter export-controlled data in the following fields:
  - Database instance identifier
  - 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
- Event subscription name
- Resource tags

If you are processing export-controlled data with Amazon RDS, follow these guidelines in order to maintain export compliance:

- When you use the console or the AWS APIs, the only data field that is protected as export-controlled 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 export-controlled data into any data fields by using your database client-side tools. Do not pass export-controlled data by using the web service APIs that are provided by Amazon RDS.
- To secure export-controlled 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 export 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 export-controlled 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 export-controlled environments to export-controlled database instances.

If you are processing export-controlled data with this service, use the SSL (HTTPS) endpoint to maintain export compliance. For more information, see Service Endpoints.

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)

- In AWS GovCloud (US) Regions, all Amazon Redshift clusters must be launched in an Amazon VPC.
- 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/amazon-trust-ca-bundle.crt. For more information, see Configure Security Options for Connections.
- Advanced Query Accelerator (AQUA) is not available.
- The COPY EXPLICIT_IDS parameter is not available.
- Cluster relocation is not available.
- Amazon Redshift serverless is not available in AWS GovCloud (US).

Documentation for Amazon Redshift

Amazon Redshift documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon Redshift metadata is not permitted to contain export-controlled data. This metadata includes all configuration data that you enter when creating and maintaining your Amazon Redshift clusters except the master password.
- Do not enter export-controlled 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
- Event subscription name
- Resource tags

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

- When you use the console or the AWS APIs, the only data field that is protected as export-controlled 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 export-controlled data into any data fields by using your database client-side tools. Do not pass export-controlled data by using the web service APIs that are provided by Amazon Redshift.
- To secure export-controlled 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 export-controlled 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 export 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 export-controlled 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 export-controlled environments to export-controlled clusters.

If you are processing export-controlled data with this service, use the SSL (HTTPS) endpoint to maintain export compliance. For more information, see Service Endpoints.

Amazon Rekognition

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

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) for either Amazon Rekognition Image or Amazon Rekognition Stored Video.
- Amazon Rekognition Streaming Video is not available in AWS GovCloud (US).
- Amazon Rekognition Custom Labels is not available in AWS GovCloud (US).
- In AWS GovCloud (US) Regions, AWS DOES NOT use or store AI Content processed by this AI Service to develop and improve that Service or technologies of AWS or its affiliates. Opt-out policies are not currently applicable to these Regions.

Documentation for Amazon Rekognition

Amazon Rekognition documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal

course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

Amazon Route 53

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)

- Route 53 public hosted zones are not available.
- Geolocation and latency based routing are not available.

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.
- 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 allowlisting 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
- 18.253.168.0/25
- 18.253.167.0/25

Documentation for Amazon Route 53

Amazon Route 53 documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

Amazon Route 53 Application Recovery Controller

Zonal shift in Amazon Route 53 Application Recovery Controller (Route 53 ARC) enables you to quickly recover from Availability Zone (AZ) issues, by temporarily moving traffic for a resource away from an AZ. Starting a zonal shift helps your application recover quickly from a developer's bad code deployment or from an AWS infrastructure failure in a single AZ, reducing the impact and time lost from an issue in one AZ. You can start a zonal shift for any managed resource in your account in a Region. Network Load Balancers and Application Load Balancers that do not have cross-zone enabled are currently supported. Supported AWS resources are automatically registered with Route 53 ARC. Zonal shifts are temporary. You must specify an expiration when you start a zonal shift, of up to three days initially. If you want to still keep traffic away from an AZ, you can update the zonal shift and set a new expiration.

How Amazon Route 53 Application Recovery Controller differs for AWS GovCloud (US)

The AWS GovCloud (US-West) implementation of Route 53 ARC is unique in the following way:

- The routing control, readiness check, and zonal autoshift features of the Route 53 ARC service are not available in AWS GovCloud (US-West).

Documentation for Amazon Route 53 Application Recovery Controller

Route 53 ARC Developer Guide.

Export-controlled content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- All customer parameters provided as input to Route 53 ARC through the console, APIs, or other mechanisms, are not permitted to contain export-controlled data. Examples include comments entered by the user, and the resource name and Amazon Resource Name (ARN) for registered resources.

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 .

- In AWS GovCloud (US) Regions, Amazon S3 has three endpoints. If you are processing export-controlled 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).
- 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).
- S3 Replication Time Control (S3 RTC) is not available in AWS GovCloud (US).
- Amazon S3 Storage Lens is not available in AWS GovCloud (US) Regions.
- Amazon S3 Object Lambda Access Points are available in AWS GovCloud (US) Regions for SSL endpoints. FIPS endpoints are not available.
- Amazon S3 presigned URLs are only available via the CLI and SDKs.
- A bucket-style alias for your Amazon S3 Object Lambda access point is not available.
- In AWS GovCloud (US), Amazon S3 Inventory does not have the Object Access Control List and Object Owner as available object metadata fields in inventory reports.
- Amazon S3 Express One Zone is not available in AWS GovCloud (US) Regions.

Documentation for Amazon Simple Storage Service

Amazon Simple Storage Service documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon S3 metadata is not permitted to contain export-controlled data. This metadata includes all configuration data that you enter when creating and maintaining your Amazon S3 buckets, such as bucket names.
- Do not enter export-controlled data in the following fields:
  - Resource tags

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.

Documentation for Amazon S3 Glacier

Amazon S3 Glacier documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- S3 Glacier metadata is not permitted to contain export-controlled data. This metadata includes all configuration data that you enter when creating and maintaining your S3 Glacier vaults names.
- Do not enter export-controlled data in the following fields:
  - Resource tags: Key
  - Resource tags: Value

Amazon S3 on Outposts

Amazon S3 on Outposts delivers object storage to your on-premises AWS Outposts environment to help you meet your low latency, local data processing, and data residency needs. Using the Amazon S3 APIs and features, Amazon S3 on Outposts makes it easier to store, secure, tag, retrieve, report on, and control access to the data on your Outposts. AWS Outposts is a fully managed service that extends AWS infrastructure, services, and tools to virtually any data center, co-location space, or on-premises facility for a truly consistent hybrid experience.

How Amazon S3 on Outposts Differs for AWS GovCloud (US)

AWS CloudFormation is not supported.

Documentation for Amazon S3 on Outposts

S3 on Outposts documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon S3 on Outposts metadata is not permitted to contain export-controlled data. This metadata includes all configuration data that you enter when creating and maintaining your Amazon S3 on Outposts buckets, such as bucket names. For example, do not enter export-controlled data in the following fields:
  - Outpost Bucket Name
  - Outpost Object Name
  - Resource tags

Amazon SageMaker

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.

Topics

- How Amazon SageMaker Differs for AWS GovCloud (US)

- Documentation for Amazon SageMaker
- Export-Controlled Content

How Amazon SageMaker Differs for AWS GovCloud (US)

- The following instance types are not supported: t3.[medium, large, xlarge, 2xlarge] and p2.[xlarge, 8xlarge, 16xlarge].
- Only the following features are available. API calls to unavailable features will fail with a 4xx message indicating "The requested operation is not supported in the called region".
  - Notebook instances
  - Training
  - Hosting
  - Batch Transform
  - Processing
  - Neo
  - SageMaker Search
  - SageMaker Debugger and Profiler
  - Model Tuning
  - SageMaker Studio
    - Authentication using AWS Identity and Access Management is supported; authentication using IAM Identity Center is not supported
    - Scheduling a notebook job is not supported
    - AWS Glue interactive sessions is supported only in AWS GovCloud (US-West)
  - SageMaker Studio notebooks

Documentation for Amazon SageMaker

Amazon SageMaker documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal

course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon SageMaker metadata is not permitted to contain export-controlled data. This metadata includes all configuration data that you enter when creating and maintaining your NotebookInstances, NotebookInstanceLifecycleConfigs, Endpoints, Models, EndpointConfigs, TrainingJobs, HyperParameterTuningJobs, and BatchTransformJobs.

  Do not enter export-controlled 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

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 the AWS GovCloud (US) Region.

Documentation for Amazon SES

Amazon SES documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

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.
- Amazon Data Firehose subscriptions are not supported.
- Kinesis Firehose protocol option for the Amazon SNS topics is not available.
- Message Data Protection is not supported.

- Custom data identifiers are not supported.
- Amazon SNS message archiving and replay is not supported.

Documentation for Amazon Simple Notification Service

Amazon SNS documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Export-controlled 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 export-controlled data
  - Email – not permitted to contain export-controlled data
  - Amazon SQS queues outside of AWS GovCloud (US) Regions – not permitted to contain export-controlled data
  - HTTP URL endpoint – not permitted to contain export-controlled data
- Amazon SNS metadata is not permitted to contain export-controlled data. This metadata includes all configuration data that you enter when setting up and maintaining your topics.

  For example, do not enter export-controlled 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)

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

Documentation for Amazon Simple Queue Service

Amazon SQS documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon SQS metadata is not permitted to contain export-controlled data. This metadata includes all configuration data that you enter when setting up and maintaining your queues.

  For example, do not enter export-controlled data in the following fields:

  - Queue Name
  - Queue Configuration
  - Queue Policy Document
  - Queue Permissions

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.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- No export-controlled data can be entered, stored, or processed in Amazon SWF.
- Amazon SWF metadata is not permitted to contain export-controlled data. This metadata includes all of the configuration data that you enter when setting up and maintaining your workflows.

  For example, do not enter export-controlled data in the following fields:

  - Workflow type name
  - Workflow type version
  - Activity type name
  - Activity type version
  - Execution workflow ID
  - Activity task ID

- The `input`, `result`, or `details` arguments to workflow executions
- The `input`, `result`, or `details` arguments to activity tasks

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)

- In AWS GovCloud (US) Regions, AWS DOES NOT use or store AI Content processed by this AI Service to develop and improve that Service or technologies of AWS or its affiliates. Opt-out policies are not currently applicable to these Regions.

Documentation for Amazon Textract

Amazon Textract documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon Textract metadata is not permitted to contain export-controlled data.

Amazon Timestream

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

Timestream is a fast, scalable, and serverless time series database service for IoT and operational applications. With Timestream, you can store and analyze trillions of events per day up to 1,000 times faster than with relational databases—at as little as one-tenth of the cost.

Timestream saves you time and cost in managing the lifecycle of time series data by keeping recent data in memory and moving historical data to a cost-optimized storage tier, based upon user-defined policies.

With the purpose-built query engine in Timestream, you can access and analyze recent and historical data together, without needing to specify explicitly in the query whether the data resides in memory or in the cost-optimized storage tier.

Timestream helps ensure that your time series data is always encrypted, whether at rest or in transit. With Timestream, you can also specify an AWS KMS customer managed key for encrypting data in the magnetic store.

How Amazon Timestream Differs for AWS GovCloud (US)

The AWS GovCloud (US) Region implementation of Amazon Timestream is unique in the following ways.

- The query editor in the Timestream console does not allow you to save your queries for later usage or search from saved queries.
- Customers who rely upon FIFO support with SNS notifications from the scheduled query service for Timestream will not be able to create such a topic in GovCloud since the Region does not support FIFO topics. For more information, see Amazon SNS . This might cause notifications for scheduled queries to arrive out of order.

Documentation for Amazon Timestream

Timestream documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon Timestream metadata is not permitted to contain export-controlled data. This metadata includes all configuration data that you enter when creating and maintaining your Amazon Timestream instances except the master password.

- Do not enter export-controlled data in the following fields.
  - Master user name
  - Database name
  - Table name
  - Scheduled query, Query Name
  - Resource tags

If you are processing export-controlled data with Amazon Timestream, follow these guidelines in order to maintain export compliance.

- When you use the console or the AWS APIs, the only data field that is protected as export-controlled data is the Amazon Timestream master password.
- You can enter export-controlled data into any data fields by using your database client-side tools. Do not pass export-controlled data by using the web service APIs that are provided by Amazon Timestream.
- To secure export-controlled 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 Amazon Timestream, a non-U.S. person could reconfigure the DNS to redirect export-controlled 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 export 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 that contains export-controlled 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 export-controlled environments to export-controlled database instances.
- If you are processing export-controlled data with this service, use the SSL (HTTPS) endpoint to maintain export compliance. For more information, see Service Endpoints.

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)

- Automatic language identification is not available in the AWS GovCloud (US-East) Region.
- Call Analytics is not available in the AWS GovCloud (US) Regions.
- Automatic content redaction is not available in the AWS GovCloud (US-East) Region.
- In AWS GovCloud (US) Regions, AWS DOES NOT use or store AI Content processed by this AI Service to develop and improve that Service or technologies of AWS or its affiliates. Opt-out policies are not currently applicable to these Regions.

Documentation for Amazon Transcribe

Amazon Transcribe documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- No data will leave the AWS GovCloud (US) Regions for this service.

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)

- Async batch is not available in AWS GovCloud (US).
- Active Custom Translation is not available in AWS GovCloud (US).
- Parallel Data Operations are not available in AWS GovCloud (US).
- In AWS GovCloud (US) Regions, AWS DOES NOT use or store AI Content processed by this AI Service to develop and improve that Service or technologies of AWS or its affiliates. Opt-out policies are not currently applicable to these Regions.

Documentation for Amazon Translate

Amazon Translate documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

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.

> **Note**
>
> Not all Amazon VPC endpoints in AWS GovCloud (US) support Amazon VPC endpoint policies.

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 VPC.
- 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.
- Security group rule IDs are not available in the Amazon VPC console.
- You can't visualize your global network in geographic map view in Transit Gateway Network Manager console.
- The AWS-managed prefix list for Amazon CloudFront is not available.
- Reachability Analyzer is not supported.
- Network Access Analyzer is not supported.

Documentation for Amazon Virtual Private Cloud

Amazon VPC documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon VPC metadata is not permitted to contain export-controlled data. This metadata includes all of the configuration data that you enter when setting up and maintaining your VPCs. This applies to free-text entry fields for VPC resources, including but not limited to:
  - Name and Description of Security Groups and Security Group Rules.
  - Key and Value of DHCP option sets created in your VPC.
  - Client Token values used for Idempotency of your API calls.
  - Destination log group name of VPC Flow Logs.
  - Service name of a VPC Endpoint.
  - Key and Value of Tags associated with your resources.

Amazon WorkSpaces

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) does not support PCoIP WorkSpaces.
- The cross-Region redirection feature is not supported.
- The **Forgot Password** option and the **Welcome Email** feature are not supported in the AWS GovCloud (US) Regions. Users cannot reset their own passwords and users with new WorkSpaces will not receive a welcome email.

Documentation for Amazon WorkSpaces

Amazon WorkSpaces documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- Amazon WorkSpaces metadata is not permitted to contain export-controlled data. This metadata includes all configuration data that you enter when creating and maintaining your WorkSpaces.

  Do not enter export-controlled data in the following console fields:

  - AMI descriptions
  - Resource tags
  - If importing export-controlled images, do not use pre-signed URLs for the CLI argument
  - Key pairs created using HTTP

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 the following types of load balancers: Application Load Balancers, Network Load Balancers, Gateway Load Balancers, and Classic Load Balancers. All four types of load balancers are supported in AWS GovCloud (US) Regions.

> **Note**
>
> Some features of Elastic Load Balancing (ELB) TLS do not support FIPS 140-2 requirements by default. When using the Classic or Network Load Balancer, you can pass TCP traffic and terminate TLS on your target (e.g. web server), that is configured to support FIPS 140-2 requirements. Application Load Balancer (ALB) supports selecting FIPS algorithms.

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.
- Export data must be encrypted in transit outside of the export boundary. Because Elastic Load Balancing uses global DNS servers, export traffic across Elastic Load Balancing must be encrypted.
- Cognito authentication is not available in AWS GovCloud (US) Regions.

Documentation for Elastic Load Balancing

Elastic Load Balancing documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- All customer parameters provided as input to Elastic Load Balancing (via console, APIs, or other mechanism) are not permitted to contain export-controlled data. Examples include the names of load balancers and the names of load balancer policies.
- Do not enter export-controlled data in the following fields:
  - Resource tags

If you are processing export-controlled data with this service, use the SSL (HTTPS) endpoint to maintain export compliance. For more information, see Service Endpoints.

Red Hat OpenShift Service on AWS

Red Hat OpenShift Service on AWS (ROSA) is a managed service that you can use to build, scale, and deploy containerized applications with Red Hat OpenShift running on AWS infrastructure.

ROSA is jointly supported and operated by AWS and Red Hat. ROSA offers 24-hour site reliability engineering (SRE) support for cluster installation, management, and upgrades backed by Red Hat's 99.95% uptime service-level agreement.

> **Note**
>
> Red Hat OpenShift Service on AWS has achieved an agency Authority to Operate (ATO) at the FedRAMP High Baseline, but has not yet been granted a Provisional Authority to Operate (P-ATO) by the Joint Authorization Board (JAB).

How Red Hat OpenShift Service on AWS Differs for AWS GovCloud (US)

- You must have access to the Red Hat Hybrid Cloud Console on AWS GovCloud (US). To obtain access, complete the ROSA FedRAMP access request form.
- AWS Support does not yet have the ability to transfer support cases to Red Hat on behalf of customers.
- Red Hat support cases are managed through ServiceNow. ServiceNow has a Provisional Authority to Operate (P-ATO) at the FedRAMP High benchmark. Red Hat personnel that manage ROSA support cases through ServiceNow are U.S. persons. For more information, see ServiceNow's FedRAMP authorization details on the FedRAMP Marketplace.
  - Customers set up access to ServiceNow during the onboarding process.
- ROSA with hosted control planes (HCP) is not yet available in the AWS GovCloud (US) Regions. Only ROSA classic is supported.
- The ROSA console is not yet available in AWS GovCloud (US) Regions.
- Only ROSA clusters that use AWS PrivateLink can be deployed in AWS GovCloud (US).
- You must meet the U.S. regulatory requirements as described in AWS GovCloud (US) Sign Up.
- You must deploy ROSA into an existing VPC.
- ROSA only supports the use of AWS Security Token Service (AWS STS) temporary security credentials to allow the service to perform actions in the customer AWS account.
- ROSA only uses FIPS-validated modules to process cryptographic libraries.
- You must have a FIPS 140-2 compliant hardware token for use with the service.
- You need to configure the AWS CLI on your local machine to use your AWS GovCloud (US) account. This configuration is required to create ROSA clusters.

- ROSA entitlements cannot be shared between AWS standard accounts and AWS GovCloud (US) accounts using AWS License Manager.
- VPC sharing is not supported.

Enabling ROSA

To enable access to ROSA in the AWS GovCloud (US) Regions, the AWS GovCloud (US) account root user must complete the following steps.

> **Note**
>
> For AWS Organizations users, repeat these steps for each member account that requires access.

1. Create a Red Hat commercial account or use an existing one.
2. Create an AWS standard account. AWS recommends creating a new AWS standard account that will only be used for AWS GovCloud (US) sign-up and billing.
3. Log in to the AWS standard account.
4. Go to the ROSA console and enable ROSA.
5. Sign up for an AWS GovCloud (US) account. For more information, see AWS GovCloud (US) Sign Up.

   > **Note**
   >
   > Before creating accounts in the AWS GovCloud (US) Regions, make sure that you meet specific U.S. regulatory requirements as described in AWS GovCloud (US) Sign Up.

6. Link your AWS GovCloud account to your AWS standard account.
7. Complete the ROSA FedRAMP access request form to initiate onboarding to AWS GovCloud (US). Upon submission, this form will be processed by Red Hat. If Red Hat requires further information, you will receive a follow-up email, or you will receive instructions on how to access the service.

> **Note**
>
> You can use the Red Hat Hybrid Cloud Console on AWS GovCloud (US) to deploy ROSA to multiple AWS GovCloud (US) accounts.

Creating and deploying a ROSA classic cluster into the AWS GovCloud (US) Regions

After enabling ROSA for AWS GovCloud (US), you can create and deploy ROSA classic clusters into the AWS GovCloud (US) Regions.

Prerequisites

To deploy ROSA classic clusters into the AWS GovCloud (US) Regions, the following prerequisites must be met.

- You have access to the Red Hat Hybrid Cloud Console on AWS GovCloud (US).
- You have an AWS GovCloud (US) account linked to an AWS standard account.
- You configured the AWS CLI on your local machine to use your AWS GovCloud (US) account. For more information, see Configure your Account using AWS CLI.
- You created your own Amazon VPC architecture to deploy your clusters into. For more information, see Create Amazon VPC architecture for the cluster in the *ROSA User Guide*.
- You completed the prerequisite actions documented in Getting started with ROSA classic using AWS PrivateLink.

Log in to your AWS GovCloud (US) and Red Hat Hybrid Cloud Console on AWS GovCloud (US) accounts

Once the prerequisites have been met, follow these steps.

> **Note**
>
> If you cannot sign in to your AWS GovCloud (US) account or Red Hat Hybrid Cloud Console on AWS GovCloud (US) account, ask your administrator for the information that you need to sign in.

1. Sign in to your AWS GovCloud (US) account.
2. Go to the Red Hat Hybrid Cloud Console on AWS GovCloud (US) login page and sign in with your Red Hat account credentials.
3. The remaining procedure varies depending on whether you are creating clusters using the Red Hat Hybrid Cloud Console on AWS GovCloud (US) or ROSA CLI.
   - Console
     a. Choose **Create cluster with web interface**.
     b. Follow the console prompts to create the ROSA cluster.
   - ROSA CLI
     a. Choose **Create cluster with CLI**.
     b. Copy the following command.

```
rosa login --govcloud TOKEN
```

     c. Open a terminal session and run the command.

Create and deploy a ROSA classic cluster that uses AWS PrivateLink

Once logged in to your AWS GovCloud (US) and Red Hat Hybrid Cloud Console on AWS GovCloud (US) accounts, you can create a ROSA classic cluster that uses AWS PrivateLink and deploys into the AWS GovCloud (US) Regions.

The procedure is the same for deploying a ROSA classic cluster in AWS GovCloud (US) Regions and AWS standard Regions. For more information, see Getting started with ROSA using AWS PrivateLink in the *ROSA User Guide*.

Documentation for Red Hat OpenShift Service on AWS

ROSA documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer

compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This service can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

Research and Engineering Studio on AWS

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

Research and Engineering Studio on AWS (RES) is an AWS supported, open source product that enables IT administrators to provide a web portal for scientists and engineers to run technical computing workloads on AWS. RES provides a single pane of glass for users to launch secure virtual desktops to conduct scientific research, product design, engineering simulations, or data analysis workloads. Users can connect to the RES portal using their existing corporate credentials and work on individual or collaborative projects.

How Research and Engineering Studio on AWS Differs for AWS GovCloud (US)

The Research and Engineering Studio User Guide already includes special instructions for AWS GovCloud (US) where appropriate. The following list describes the instances where there are special instructions for AWS GovCloud (US).

- In the Deploy the product chapter:
  - Under Prerequisites:
    - You must follow the procedures under Create domain (GovCloud only).
  - Under Step 1: Create external resources:
    - We provide a different template for AWS GovCloud (US).
    - The `SubDomain` template parameter is required in AWS GovCloud (US).
    - Don't use the `PortalDomainName` template parameter.
  - Under Step 2: Launch the product:
    - We provide a different template for AWS GovCloud (US).
- In the Configuration guide chapter:

- In the Managing users and groups section:
  - Under Setting up SSO with Identity Center:
    - You must set up SSO in the AWS GovCloud (US) partition where you deployed RES.
- In the Create an ACM certificate section:
  - You must create a certificate in your AWS GovCloud (US) account.
  - For step 7: copy the CNAME key and value. From the commercial partition account, use the values to create a new record in the Public Hosted Zone. The status of the certificate should change to **Issued**.
- In the Administrator guide chapter:
  - In the eVDI section:
    - Under Software Stacks (AMIs):
      - To run the provided CentOS7 stack, you must subscribe to the AMI in AWS Marketplace with your linked standard account.
  - In the Cost monitoring and control section:
    - Associating RES projects to AWS Budgets isn't supported.

Documentation for Research and Engineering Studio on AWS

Research and Engineering Studio documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- This product can generate metadata from customer-defined configurations. AWS suggests customers do not enter export-controlled information in console fields, descriptions, resource names, and tagging information.

Service Quotas

Service Quotas enables you to view and manage your AWS service quotas from a central location. You can view the AWS default quotas, your account-level or applied quotas and request for quota increases. Through its integration with AWS CloudWatch, you can also view usage against quotas and configure alarms to get notified when approaching a quota threshold. Service Quotas offers both a console experience and programmatic access via the AWS SDK, and is available to all AWS customers at no additional cost.

How Service Quotas Differs for AWS GovCloud (US)

- The Quota request template is currently not supported in AWS GovCloud(US) Regions.

Documentation for Service Quotas

Service Quotas documentation.

Export-Controlled Content

For AWS Services architected within the AWS GovCloud (US) Regions, the following list explains how certain components of data may leave the AWS GovCloud (US) Regions in the normal course of the service offerings. The list can be used as a guide to help meet applicable customer compliance obligations. Data not included in the following list remains within the AWS GovCloud (US) Regions.

- The initial quota value established by AWS (default value) and the new quota value after a quota increase (applied value).
- Information related to open quota increase requests or requests that were closed in the last 90 days.
- Tags on any service quota with applied values.

VMware Cloud on AWS

VMware Cloud on AWS brings VMware's enterprise-class Software-Defined Data Center software to the AWS Cloud, and enables customers to run production applications in a managed service from VMware and AWS. For more information, see VMware Cloud on AWS.

Documentation for VMware Cloud on AWS

VMware Cloud on AWS documentation.

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

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. 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.

AWS GovCloud (US) Administrator Account Password Reset

If you've lost access to your AWS GovCloud (US) account, please review the following options:

- Troubleshooting AWS GovCloud (US) sign-in or account issues

- Restore IAM Administrator access to the AWS Management Console for AWS GovCloud (US)
- Requesting root access keys for an AWS GovCloud (US) account

Deactivating AWS GovCloud (US) MFA devices

If you are having trouble signing in with a multi-factor authentication (MFA) device as an IAM user, contact your administrator for help.

As an administrator, you can deactivate the device for another IAM user. This allows the user to sign in without using MFA. You might do this as a temporary solution while the MFA device is replaced, or if the device is temporarily unavailable. However, we recommend that you enable a new device for the user as soon as possible. To learn how to enable a new MFA device, see Enabling MFA devices for users in AWS.

Deactivating MFA devices (console)

To deactivate an MFA device for another IAM user (console)

1. Sign in to the AWS Management Console and open the IAM console at https://signin.amazonaws-us-gov.com/iam/
2. In the navigation pane, choose **Users**.
3. To deactivate the MFA device for a user, choose the name of the user whose MFA you want to remove.
4. Choose the **Security credentials** tab. Next to **Assigned MFA device**, choose **Manage**.
5. In the **Manage MFA device** wizard, choose **Remove**, and then choose **Remove**.

The device is removed from AWS. It cannot be used to sign in or authenticate requests until it is reactivated and associated with an AWS user.

Deactivating MFA devices (AWS CLI)

To deactivate an MFA device for an IAM user (AWS CLI) run this command:

```
aws iam deactivate-mfa-device
```

Example to deactivate an MFA device:

```
aws iam deactivate-mfa-device --user-name Bob --serial-number arn:aws-us-
gov:iam::210987654321:mfa/BobsMFADevice
```

This command deactivates the virtual MFA device with the ARN `arn:aws-us-gov:iam::210987654321:mfa/BobsMFADevice` that is associated with the user Bob.

Deactivating MFA devices (AWS API)

To deactivate an MFA device for an IAM user (AWS API)

- Call this operation: `DeactivateMFADevice`

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:

Resource	Description
Development and Test on AWS	This paper describes how AWS adds value in the various phases of the software developme nt cycle, with a specific focus on development and test.
Amazon VPC Network Connectivity Options	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.
Microsoft SharePoint Server on AWS Reference Architecture	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.
Amazon's Corporate IT Deploys SharePoint 2010 to the AWS Cloud	This paper describes how and why Amazon's corporate IT organization deployed its corporate intranet (an enterprise mission-c ritical corporate IT application that involves

Resource	Description
	highly sensitive data) running Microsoft SharePoint 2010 to the AWS cloud.
Extend Your IT Infrastructure with Amazon VPC	This paper highlights common use cases and best practices for Amazon VPC and related services.
Auditing Security Checklist for Use of AWS	This fundamental course dives into cloud-specific audit considerations and best practices , and is aligned to common security and compliance domains. It also includes a checklist to prepare you for auditing security in the cloud..
Security at Scale: Governance on AWS	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.
AWS Security Best Practices	The focus of this paper is the security pillar of the AWS Well-Architected Framework. It provides guidance to help you apply best practices, current recommendations in the design, delivery, and maintenance of secure AWS workloads.
AWS: Overview of Security Processes	Learn how to meet your security and compliance goals using AWS infrastructure and services.

Resource	Description
AWS: Risk and Compliance	This paper outlines the mechanisms that AWS has implemented to manage risk on the AWS side of the Shared Responsibility Model, and the tools that customers can leverage to gain assurance that these mechanisms are being implemented effectively.
AWS Compliance Whitepapers	This site has information and whitepapers related to compliance.

Experienced with AWS

The following table lists additional resources for users experienced with AWS:

Resource	Description
Web Identity Federation with Mobile Applications	This article discusses the web identity federation feature of AWS Security Token Service and a sample for use in the AWS Mobile SDKs.
High Availability for Amazon VPC NAT Instances: An Example	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).
Securing Data at Rest with Encryption	This paper provides an overview of methods for encrypting your data at rest.

Document History

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

Change	Description	Date
AWS Security Hub	Central configuration, custom control parameters, and finding enrichment are now available in AWS GovCloud (US) Regions.	February 8, 2024
Amazon QuickSight	Dashboard snapshot export API operations are now supported in AWS GovCloud (US). See How Amazon QuickSight Differs for AWS GovCloud (US).	January 24, 2024
Amazon EKS	Amazon EKS Extended Support for Kubernetes Versions is now available.	January 22, 2024
Amazon EKS	Amazon EKS Upgrade insights aren't available.	January 8, 2024
Amazon EKS	Amazon EKS Pod Identitie s aren't available in AWS GovCloud (US).	December 26, 2023
EC2 Image Builder	Update differences - Image lifecycle policies are not supported in AWS GovCloud (US) Regions.	December 12, 2023
AWS Application Migration Service	App2Container Replatfor ming and Refactor Spaces are	December 6, 2023

	not supported by Applicati on Migration Service in AWS GovCloud (US). See How AWS Application Migration Service differs for AWS GovCloud (US).	
AWS Elastic Disaster Recovery	AWS Elastic Disaster Recovery is now supported in AWS GovCloud (US) Regions.	December 6, 2023
Amazon EKS	Added missing statements that Amazon EKS Anywhere isn't available.	December 4, 2023
Amazon Pinpoint	Amazon Pinpoint SMS and voice v2 API is now supported in AWS GovCloud (US-West) and AWS GovCloud (US-East).	November 16, 2023
Research and Engineering Studio on AWS	Research and Engineering Studio on AWS (RES) is now supported in AWS GovCloud (US-West).	November 13, 2023
AWS Trusted Advisor	AWS Trusted Advisor now supports checks from AWS Config. See AWS Trusted Advisor.	October 26, 2023
AWS Mainframe Moderniza tion	Mainframe Modernization is now supported in AWS GovCloud (US) Regions.	October 2, 2023

AWS Lambda	The Python 3.11 (`python3.11`) runtime is now available in the AWS GovCloud (US-East) and AWS GovCloud (US-West) Regions.	September 28, 2023
Red Hat OpenShift Service on AWS	ROSA is now supported in AWS GovCloud (US) Regions.	September 16, 2023
AWS Security Hub	Consolidated controls view and consolidated control findings are now supported in AWS GovCloud (US) Regions.	September 6, 2023
Amazon GuardDuty	Lambda Protection is now supported in AWS GovCloud (US) Regions. The service-linked role now includes AWS Lambda actions to retrieve information about your Lambda functions and tags (`"lambda:GetFunctionConfiguration"` and `"lambda:ListTags"`)."	August 15, 2023
Amazon EventBridge	Dead Letter Queues (DLQs) are now supported in the AWS GovCloud (US) Region.	August 1, 2023
Amazon QuickSight	Dashboard snapshot export API operations are not supported in AWS GovCloud (US). See How Amazon QuickSight Differs for AWS GovCloud (US).	July 24, 2023

Amazon Location Service	Amazon Location Service is now supported in AWS GovCloud (US) Regions.	July 17, 2023
AWS SDK for SAP ABAP	AWS SDK for SAP ABAP is now supported in AWS GovCloud (US) Regions.	June 30, 2023
AWS Control Tower achieves FedRAMP high authorization	AWS Control Tower achieves FedRAMP high authoriza tion in AWS GovCloud (US) Regions.	June 20, 2023
???	now supports AWS Network Firewall and DNS Firewall policies in AWS GovCloud (US) Regions.	June 8, 2023
AWS Application Migration Service	Application Migration Service is now supported in AWS GovCloud (US) Regions.	June 1, 2023
AWS SimSpace Weaver	SimSpace Weaver is now supported in AWS GovCloud (US) Regions.	May 31, 2023
Amazon Pinpoint	The In-App channel is not supported in the AWS GovCloud (US-West) for Amazon Pinpoint. See How Amazon Pinpoint Differs for AWS GovCloud (US)	May 26, 2023
Amazon AppStream 2.0	Copying AppStream 2.0 images between the AWS GovCloud (US) Regions is now supported.	May 17, 2023

SageMaker	SageMaker Studio and SageMaker Studio notebooks are now supported.	May 15, 2023
Amazon WorkSpaces	Amazon WorkSpaces is now supported in AWS GovCloud (US-East).	May 3, 2023
Amazon Relational Database Service	Amazon RDS Proxy is now supported in AWS GovCloud (US) Regions.	May 1, 2023
Amazon Route 53 Application Recovery Controller	Amazon Route 53 Applicati on Recovery Controller is now supported in AWS GovCloud (US) Regions.	April 28, 2023
Amazon Bedrock	Amazon Bedrock is now supported in AWS GovCloud (US) Regions	April 28, 2023
AWS Verified Access	AWS Verified Access is now supported in AWS GovCloud (US) Regions.	April 28, 2023
Amazon WorkSpaces	The Web Access client for Amazon WorkSpaces is now supported in the AWS GovCloud (US-West) Region.	April 19, 2023
Amazon AppStream 2.0	Amazon AppStream 2.0 is now supported in AWS GovCloud (US-East).	April 5, 2023
WickrGov	AWS WickrGov is now supported in the AWS GovCloud (US-West) Region.	March 30, 2023

AWS CloudFormation	AWS CloudFormation now supports resource AWS::Organizations::ResourcePolicy in AWS GovCloud (US) Regions.	March 27, 2023
AWS IoT TwinMaker	AWS IoT TwinMaker is only supported in AWS GovCloud (US-West) Region.	March 25, 2023
Enable Amazon EventBridge on buckets	You can now enable EventBridge on Amazon S3 buckets to send events to Amazon EventBridge in AWS GovCloud (US) Regions.	March 22, 2023
AWS MDC	AWS Modular Data Center is now supported in AWS GovCloud (US-West).	February 13, 2023
Amazon Inspector	Amazon Inspector is now supported in AWS GovCloud (US) Regions.	January 31, 2023
SageMaker	Amazon SageMaker is now supported in AWS GovCloud (US-East).	January 25, 2023
Compute Optimizer	AWS Compute Optimizer is now supported in AWS GovCloud (US) Regions.	January 25, 2023
Amazon VPC	Amazon VPC IP Address Manager is now supported in the AWS GovCloud (US) Region.	December 8, 2022

AWS Organizations	AWS Organizations now supports tag policies in AWS GovCloud (US) Regions.	November 17, 2022
Timestream	Amazon Timestream is now supported in AWS GovCloud (US-West).	November 16, 2022
Amazon EventBridge	Additional content filtering options are now supported in the AWS GovCloud (US) Region.	November 14, 2022
AWS Control Tower	AWS Control Tower is now supported in AWS GovCloud (US) Regions.	October 19, 2022
Amazon Chime SDK	Amazon Chime SDK is now supported in AWS GovCloud (US) Regions.	October 6, 2022
Amazon Managed Blockchain	Hyperledger Fabric on Amazon Managed Blockchain is now supported in the AWS GovCloud (US-West) Region.	September 7, 2022
AWS WA Tool	AWS Well-Architected Tool is now supported in AWS GovCloud (US) Regions.	August 17, 2022
Amazon Keyspaces	Amazon Keyspaces (for Apache Cassandra) is now supported in AWS GovCloud (US) Regions.	August 4, 2022
IAM Identity Center	AWS SSO is now IAM Identity Center.	July 26, 2022

AWS Fault Injection Service	AWS Fault Injection Service is now supported in AWS GovCloud (US) Regions.	July 13, 2022
CloudShell	AWS CloudShell is now supported in AWS GovCloud (US) Regions.	June 29, 2022
Amazon Transcribe	Streaming Transcription is now available in AWS GovCloud (US) Regions.	June 9, 2022
AWS RoboMaker	AWS RoboMaker is now supported in AWS GovCloud (US-West) Region.	May 4, 2022
AWS IoT SiteWise	AWS IoT SiteWise endpoints now support FIPS 140-2.	April 20, 2022
AMS Accelerate	AMS Accelerate is now supported in AWS GovCloud (US) Regions.	February 9, 2022
IAM Identity Center	AWS IAM Identity Center is now supported in the AWS GovCloud (US) Regions.	January 5, 2022
S3 on Outposts	Amazon S3 on Outposts is now supported in AWS GovCloud (US) Regions.	December 22, 2021
Amazon Kendra	Amazon Kendra is now supported in AWS GovCloud (US-West).	October 14, 2021
AWSCloud Control API	AWS Cloud Control API is now supported in the AWS GovCloud (US) Region.	September 30, 2021

AWS IoT SiteWise	AWS IoT SiteWise is now supported in the AWS GovCloud (US-West) Region.	September 29, 2021
IAM Identity Center	AWS IAM Identity Center is now supported in the AWS GovCloud (US-West) Region.	September 22, 2021
AWS IoT Events	AWS IoT Events is now supported in the AWS GovCloud (US-West) Region.	September 22, 2021
AWS Cloud Map	AWS Cloud Map is now supported in the AWS GovCloud (US) Region.	September 8, 2021
AWS Private Certificate Authority	Online Certificate Status Protocol (OCSP) is not supported in the AWS GovCloud (US) Regions.	September 2, 2021
AWS Network Firewall	AWS Network Firewall is now supported in the AWS GovCloud (US) Region.	June 24, 2021

Previous history

Change	Description	Date Changed
Amazon MQ	Amazon MQ is now supported in the AWS GovCloud (US) Region. See Amazon MQ.	June 16, 2021
AWS Firewall Manager	AWS Firewall Manager is now supported in the AWS GovCloud (US) Region. See AWS Firewall Manager.	April 08, 2021
Service Quotas	Service Quotas is now supported in the AWS GovCloud (US) Region. See Service Quotas.	March 31, 2021

Change	Description	Date Changed
Amazon Detective	Amazon Detective is now supported in the AWS GovCloud (US) Region. See Amazon Detective.	March 24, 2021
AWS AppConfig	AWS AppConfig is now supported in the AWS GovCloud (US) Region. See AWS AppConfig.	February 26, 2021
Amazon Lex	Amazon Lex is now supported in the AWS GovCloud (US) Region. See Amazon Lex.	February 10, 2021
Amazon Connect	Amazon Connect is now supported in the AWS GovCloud (US) Region. See Amazon Connect.	February 09, 2021
Amazon FSx	Amazon FSx is now supported in the AWS GovCloud (US) Region. See Amazon FSx.	December 16, 2020
AWS IoT Greengrass V2	AWS IoT Greengrass V2 is now supported in the AWS GovCloud (US) Region. See AWS IoT Greengrass Version 2.	December 15, 2020
AWS Lake Formation	AWS Lake Formation is now supported in the AWS GovCloud (US) Region. See AWS Lake Formation.	November 11, 2020
Amazon EventBridge	Amazon EventBridgeis now supported in the AWS GovCloud (US) Region. See Amazon EventBridge.	November 4, 2020
Amazon QuickSight	Amazon QuickSight is now supported in the AWS GovCloud (US) Region. See Amazon QuickSight.	October 28, 2020
AWS Transfer Family	AWS Transfer Family is now supported in the AWS GovCloud (US) Region. See AWS Transfer Family.	September 30, 2020
Amazon Elastic Block Store EBS direct APIs	EBS direct APIs is now supported in the AWS GovCloud (US) Region. See Accessing the contents of an EBS snapshot.	September 15, 2020

Change	Description	Date Changed
Amazon SQS	Tagging Amazon SQS resources is now supported in all AWS GovCloud (US) Regions. See Amazon SQS.	September 15, 2020
Amazon Textract	Amazon Textract is now supported in the AWS GovCloud (US) Region. See Amazon Textract.	August 19, 2020
Amazon DocumentDB (with MongoDB compatibility)	Amazon DocumentDB is now supported in the AWS GovCloud (US) Region. See Amazon DocumentDB (with MongoDB compatibility).	June 29, 2020
Amazon Managed Service for Apache Flink	Amazon Managed Service for Apache Flink is now supported in the AWS GovCloud (US) Region. See Amazon Managed Service for Apache Flink.	June 24, 2020
AWS Backup	AWS Backup is now supported in the AWS GovCloud (US) Region. See AWS Backup.	June 24, 2020
Amazon Cognito	Amazon Cognito is now supported in the AWS GovCloud (US) Region. See Amazon Cognito.	May 13, 2020
Amazon EKS	Amazon Elastic Kubernetes Service is now supported in the AWS GovCloud (US) Region. See Amazon Elastic Kubernetes Service.	May 13, 2020
Amazon Comprehend Medical	Amazon Comprehend Medical is now supported in the AWS GovCloud (US) Region. See Amazon Comprehend Medical.	May 08, 2020
Amazon Managed Streaming for Apache Kafka (MSK)	Amazon Managed Streaming for Apache Kafka (MSK) is now supported in the AWS GovCloud (US) Region. See Amazon Managed Streaming for Apache Kafka (MSK).	May 06, 2020

Change	Description	Date Changed
Amazon SES	Amazon Simple Email Service is now supported in the AWS GovCloud (US) Region. See Amazon SES.	April 30, 2020
Amazon Pinpoint	Amazon Pinpoint is now supported in the AWS GovCloud (US) Region. See Amazon Pinpoint.	April 30, 2020
AWS Security Hub	AWS Security Hub is now supported in the AWS GovCloud (US) Region. See AWS Security Hub.	April 22, 2020
AWS CodePipeline	AWS CodePipeline is now supported in the AWS GovCloud (US) Region. See AWS CodePipeline.	April 08, 2020
AWS Outposts	AWS Outposts is now supported in the AWS GovCloud (US) Regions. See AWS Outposts.	March 25, 2020
AWS X-Ray	AWS X-Ray is now supported in the AWS GovCloud (US) Regions. See AWS X-Ray.	February 19, 2020
AWS Batch	AWS Batch is now supported in the AWS GovCloud (US) Regions. See AWS Batch.	January 29, 2020
Amazon EC2Image Builder	Amazon EC2 Image Builder is now supported in the AWS GovCloud (US-East) and AWS GovCloud (US-West) Regions. See Amazon EC2 Image Builder.	December 03, 2019
Amazon S3	Access points for S3 buckets. Customers can attach additional access-points to both existing and new buckets. See Amazon S3 .	December 03, 2019
AWS DataSync	AWS DataSync is now supported in the AWS GovCloud (US-East) Region. See AWS DataSync.	November 20, 2019
AWS Artifact	AWS Artifact is now supported in the AWS GovCloud (US-West) Region. See AWS Artifact.	October 9, 2019

Change	Description	Date Changed
Amazon AppStream 2.0	Amazon AppStream 2.0 is now supported in the AWS GovCloud (US-West) Region. See Amazon AppStream 2.0.	October 9, 2019
AWS Resource Groups	AWS Resource Groups is now supported in the AWS GovCloud (US) Region. See AWS Resource Groups.	September 25, 2019
AWS IoT Device Defender	AWS IoT Device Defender is now supported in the AWS GovCloud (US) Region. See AWS IoT Device Defender.	November 14, 2018
AWS Resource Access Manager	AWS Resource Access Manager is now supported in the AWS GovCloud (US-East) Region. See AWS Resource Access Manager.	August 28, 2019
Amazon Neptune	Amazon Neptune is now supported in the AWS GovCloud (US) Region. See Amazon Neptune.	August 14, 2019
AWS Health	AWS Health is now supported in the AWS GovCloud US. See AWS Health.	August 7, 2019
Firehose	Firehose is now supported in the AWS GovCloud (US-East) Region. See Amazon Data Firehose.	June 26, 2019
AWS IoT Greengrass	AWS IoT Greengrass is now supported in the AWS GovCloud (US-West) Region. See AWS IoT Greengrass Version 1 .	June 26, 2019
AWS Fargate	AWS Fargate is now supported in the AWS GovCloud (US) Regions. See AWS Fargate.	June 24th, 2019
AWS Secrets Manager	AWS Secrets Manager is now supported in the AWS GovCloud (US-West) Region. See AWS Secrets Manager.	June 11th, 2019
AWS DataSync	AWS DataSync is now supported in the AWS GovCloud (US-West) Region. See AWS DataSync.	June 11th, 2019

Change	Description	Date Changed
AWS Serverless Application Repository	AWS Serverless Application Repository is now supported in the AWS GovCloud (US-West) Region. See AWS Serverless Application Repository.	June 11th, 2019
AWS CodeBuild	AWS CodeBuild is now supported in the AWS GovCloud (US-West) Region. See AWS CodeBuild.	June 11th, 2019
Amazon Route 53	Amazon Route 53 is now supported in the AWS GovCloud (US-West) Region. See Amazon Route 53.	May 29, 2019
Amazon Athena	Amazon Athena is now supported in the AWS GovCloud (US) Regions. See Amazon Athena.	May 13, 2019
AWS WAF	AWS WAF is now supported in the AWS GovCloud (US-West) Region. See AWS WAF.	March 13, 2019
Amazon Comprehend	Amazon Comprehend is now supported in the AWS GovCloud (US-West) Region.	March 13, 2019
Updated the guide for the re-merge	Updated all the references from a single govCloud Region to multi-regions for GovCloud	February 6, 2019
Amazon Transcribe	Amazon Transcribe is now supported in the AWS GovCloud (US-West) Region	May 1, 2019
AWS Resource Access Manager	AWS Resource Access Manager is now supported in the AWS GovCloud (US-West) Region	April 25, 2019
AWS Organizations	AWS Organizations is now supported in the AWS GovCloud (US-West) Region.	April 18, 2019

Change	Description	Date Changed
AWS CodeCommit	AWS CodeCommit is now supported in the AWS GovCloud (US-West) Region.	April 17, 2019
AWS Service Catalog	AWS Service Catalog is now supported in the AWS GovCloud (US-West) Region.	March 20, 2019
AWS WAF	AWS WAF is now supported in the AWS GovCloud (US-West) Region. See AWS WAF.	March 13, 2019
Amazon Comprehend	Amazon Comprehend is now supported in the AWS GovCloud (US-West) Region.	March 13, 2019
AWS Glue	AWS Glue is now supported in the AWS GovCloud (US-West) Region. See AWS Glue.	February 6, 2019
Amazon Athena	Amazon Athena is now supported in the AWS GovCloud (US-West) Region.	February 6, 2019
Amazon WorkSpaces	Amazon WorkSpaces is now supported in the AWS GovCloud (US-West) Region. See Amazon WorkSpaces .	January 16, 2019
Amazon Data Firehose	Amazon Data Firehose is now supported in the AWS GovCloud (US-West) Region. See Amazon Data Firehose.	January 16, 2019
AWS Elemental MediaConvert	AWS Elemental MediaConvert is now supported in the AWS GovCloud (US-West) Region. See AWS Elemental MediaConvert.	December 19, 2018
Amazon Elastic File System	Amazon Elastic File System is now supported in the AWS GovCloud (US-West) Region. See Amazon Elastic File System .	December 12, 2018

Change	Description	Date Changed
AWS GovCloud (US-East) Region launch	The AWS GovCloud (US-East) Region was launched. For more information about AWS GovCloud (US-East), see AWS GovCloud (US-East) User Guide.	November 12, 2018
AWS Directory Service	AWS Directory Service is now supported in the AWS GovCloud (US-West) Region. See AWS Directory Service.	October 24, 2018
Amazon SageMaker	Amazon SageMaker is now supported in the AWS GovCloud (US-West) Region. See Amazon SageMaker.	September 27, 2018
AWS Auto Scaling	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. As part of this update, the Application Auto Scaling service has its own separate page. See Application Auto Scaling.	September 4, 2018
AWS IoT Device Management	AWS IoT Device Management is now supported in the AWS GovCloud (US-West) Region. See AWS IoT Device Management .	August 15, 2018
AWS IoT Core	AWS IoT Core is now supported in the AWS GovCloud (US-West) Region. See AWS IoT Core .	August 15, 2018
Amazon GuardDuty	Amazon GuardDuty is now supported in the AWS GovCloud (US-West) Region. See Amazon GuardDuty.	July 25, 2018
AWS Step Functions	AWS Step Functions is now supported in the AWS GovCloud (US-West) Region. See AWS Step Functions.	June 28, 2018
AWS Deep Learning AMIs	AWS Deep Learning AMIs are now supported in the AWS GovCloud (US-West) Region. See AWS Deep Learning AMIs.	June 21, 2018

Change	Description	Date Changed
Amazon Translate	Amazon Translate is now supported in the AWS GovCloud (US-West) Region. See Amazon Translate.	June 20, 2018
Amazon Aurora MySQL and Aurora PostgreSQL	Amazon Aurora MySQL is now supported in the AWS GovCloud (US-West) Region. See Amazon Aurora with MySQL and PostgreSQL compatibility.	June 14, 2018
Amazon Inspector	Amazon Inspector is now supported in the AWS GovCloud (US-West) Region. See Amazon Inspector Classic.	June 13, 2018
AWS CloudHSM Classic	AWS CloudHSM Classic is now supported in the AWS GovCloud (US-West) Region. See AWS CloudHSM Classic.	April 19, 2018
AWS CloudHSM	AWS CloudHSM is now supported in the AWS GovCloud (US-West) Region. See AWS CloudHSM.	April 19, 2018
AWS Storage Gateway	AWS Storage Gateway is now supported in the AWS GovCloud (US-West) Region. See AWS Storage Gateway.	March 28, 2018
Amazon Polly	Amazon Polly is now supported in the AWS GovCloud (US-West) Region. See Amazon Polly.	February 28, 2018
Amazon OpenSearch Service	Amazon OpenSearch Service is now supported in the AWS GovCloud (US-West) Region. See Amazon OpenSearch Service.	February 15, 2018
Amazon Elastic Container Registry	Amazon Elastic Container Registry is now supported in the AWS GovCloud (US-West) Region. See Amazon ECR.	January 24, 2018

Change	Description	Date Changed
Amazon Elastic Container Service	Amazon Elastic Container Service is now supported in the AWS GovCloud (US-West) Region. See Amazon ECS.	January 24, 2018
Amazon API Gateway	Amazon API Gateway is now supported in the AWS GovCloud (US-West) Region. See Amazon API Gateway.	August 1, 2017
AWS Marketplace	AWS Marketplace is now supported in the AWS GovCloud (US-West) Region. See AWS Marketplace.	July 31, 2017
Amazon Rekognition	Amazon Rekognition is now supported in the AWS GovCloud (US-West) Region. See Amazon Rekognition .	June 12, 2017
AWS Server Migration Service	AWS Server Migration Service is now supported in the AWS GovCloud (US-West) Region. See AWS Server Migration Service.	June 1, 2017
AWS Certificate Manager	AWS Certificate Manager is now supported in the AWS GovCloud (US-West) Region. See AWS Certificate Manager.	June 1, 2017
Amazon EC2 Systems Manager	Amazon EC2 Systems Manager is now supported in the AWS GovCloud (US-West) Region. See AWS Systems Manager.	May 23, 2017
AWS Lambda	AWS Lambda is now supported in the AWS GovCloud (US-West) Region. See AWS Lambda.	May 18, 2017
Amazon CloudWatch Events	Amazon CloudWatch Events is now supported in the AWS GovCloud (US-West) Region. See Amazon CloudWatch Events.	May 18, 2017
AWS CodeDeploy	AWS CodeDeploy is now supported in the AWS GovCloud (US-West) Region. See AWS CodeDeploy.	May 11, 2017

Change	Description	Date Changed
AWS Elastic Beanstalk	AWS Elastic Beanstalk is now supported in the AWS GovCloud (US-West) Region. See AWS Elastic Beanstalk.	May 10, 2017
Amazon Kinesis Data Streams	Amazon Kinesis Data Streams is now supported in the AWS GovCloud (US-West) Region. See Amazon Kinesis Data Streams.	December 21, 2016
Elastic Load Balancing	Updated information about Elastic Load Balancing. See Elastic Load Balancing.	August 2, 2016
Amazon EC2	Updated public IP range. See Amazon EC2 .	June 21, 2016
AWS Config	AWS Config is now available in the AWS GovCloud (US-West) Region. See AWS Config.	May 26, 2016
AWS Import/Export	AWS Snowball, a feature of AWS Import/Export, is now available in the AWS GovCloud (US-West) Region. See AWS Snow Family.	April 19, 2016
AWS CloudTrail	Updated information about creating multiple trails. See AWS CloudTrail.	March 24, 2016
Importing VMs	Updated information about importing virtual machines into the AWS GovCloud (US-West) Region. See Amazon EC2 VM Import/Export.	February 11, 2016
Signing up for AWS GovCloud (US)	Describes the new sign-up process for direct customers and resellers. See AWS GovCloud (US) Sign Up .	December 18, 2015
IAM	Updates to MFA for the AWS GovCloud (US) console.	December 18, 2015
Amazon S3	Updated text about VPC endpoints for Amazon S3. See Amazon S3 .	December 18, 2015

Change	Description	Date Changed
Amazon EBS	Updated text about copying snapshots. See Amazon EBS .	December 18, 2015
CloudWatch Logs and CloudTrail	CloudWatch Logs is now supported within CloudTrail in the AWS GovCloud (US-West) Region. See AWS CloudTrail.	November 19, 2015
AWS Direct Connect	Updated information about using AWS Direct Connect. See AWS Direct Connect.	October 28, 2015
S3 Glacier	Updated ITAR-regulated data for S3 Glacier. See Amazon S3 Glacier.	October 28, 2015
VPC Flow Logs	VPC Flow Logs are now supported in AWS GovCloud (US). See Amazon VPC .	October 27, 2015
CloudWatch Logs	CloudWatch Logs are now supported in AWS GovCloud (US). See Amazon CloudWatch.	October 27, 2015
AWS WAF and Amazon CloudFront	Added information about using AWS WAF with CloudFront. See Setting Up Amazon CloudFront with Your AWS GovCloud (US) or Resources.	October 27, 2015
AWS CloudTrail	Added a policy example that enables CloudTrail to write log files to your bucket. See AWS CloudTrail.	August 25, 2015
AWS CloudHSM Classic	AWS CloudHSM Classic is now available in the AWS GovCloud (US-West) Region. See AWS CloudHSM.	August 5, 2015
Penetration testing	Updated instructions for submitting a request. See Penetration Testing.	August 5, 2015
IAM	Added information about SSH public keys. See AWS Identity and Access Management.	July 9, 2015

Change	Description	Date Changed
IAM and VM Import	Added information about using roles to delegate access. Added a note about `ImportImage` . See AWS Identity and Access Management and Amazon EC2 VM Import/Export.	June 12, 2015
DynamoDB and CloudTrail	DynamoDB is now supported within CloudTrail in the AWS GovCloud (US-West) Region. See AWS CloudTrail.	May 28, 2015
AWS Key Management Service	AWS KMS is now available in the AWS GovCloud (US-West) Region. See AWS Key Management Service.	May 7, 2015
Encryption	Encryption is now available for Amazon EBS , Amazon EMR , and Amazon S3 .	May 7, 2015
AWS Direct Connect	Updated instructions for setting up AWS Direct Connect. See AWS Direct Connect.	April 3, 2015
Amazon S3	Added info about cross-region replication. See Amazon S3 .	March 24, 2015
AWS Trusted Advisor	Added two new Trusted Advisor checks that are now supported (IAM Password Policy, ELB Connection Draining). See AWS Trusted Advisor.	March 18, 2015
AWS Trusted Advisor	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.	March 11, 2015
VM Export	Updated information about using VM Export. See Amazon EC2 .	March 9, 2015
VM Import	Updated information about using VM Import. See Amazon EC2 .	March 6, 2015
Importing VMs	Updated information about importing virtual machines into the AWS GovCloud (US-West) Region. See Amazon EC2 VM Import/Export.	February 11, 2015

Change	Description	Date Changed
Amazon ElastiCache	ElastiCache is now available in the AWS GovCloud (US-West) Region. See Amazon ElastiCache.	January 29, 2015
AWS Trusted Advisor	Updated information about Trusted Advisor. See AWS Trusted Advisor.	January 29, 2015
Amazon RDS and CloudTrail	Amazon RDS is now supported within CloudTrail in the AWS GovCloud (US-West) Region. See AWS CloudTrail.	January 22, 2015
AWS Trusted Advisor	Trusted Advisor is now available in the AWS GovCloud (US-West) Region. See AWS Trusted Advisor.	January 20, 2015
Amazon S3 Glacier	S3 Glacier is now available in the AWS GovCloud (US-West) Region. See Amazon S3 Glacier.	December 30, 2014
AWS CloudTrail	CloudTrail is now available in the AWS GovCloud (US-West) Region. See AWS CloudTrail.	December 16, 2014
Importing VMs	Updated information about importing virtual machines into the AWS GovCloud (US-West) Region. See Amazon EC2 VM Import/Export and Amazon EC2 .	December 15, 2014
Amazon Redshift	Amazon Redshift is now available in the AWS GovCloud (US-West) Region. See Amazon Redshift.	November 18, 2014
Feedback links	Fixed links to provide feedback.	September 26, 2014
Service Health Dashboard	The Service Health Dashboard is supported in AWS GovCloud (US). See Service Health Dashboard.	August 27, 2014
IP range	Another public IP range for Amazon EC2 instances has been added. See Amazon EC2 .	August 27, 2014
IAM	Updates to MFA for changes in IAM console.	August 5, 2014

Change	Description	Date Changed
IAM	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.	July 25, 2014
Amazon EC2	Updates to differences in Amazon EC2 AMI tools. See Amazon EC2 .	July 15, 2014
Amazon SNS	Updates to Amazon SNS ITAR boundary. See Amazon SNS .	July 2, 2014
Provisioned IOPS	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 .	May 28, 2014
Accessing the console	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).	April 7, 2014
Provisioned IOPS	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 and Amazon EBS .	April 1, 2014
Amazon EC2	Updates to Amazon EC2 and troubleshooting. For informati on, see Amazon EC2 and Troubleshooting.	March 19, 2014
Migrating AMIs	Added information about how to migrate your AMIs from another AWS Region into the AWS GovCloud (US-West) Region. See Amazon EC2 VM Import/Export.	March 4, 2014
Red Hat Linux	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 .	March 4, 2014
SUSE Linux	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 .	January 17, 2014

Change	Description	Date Changed
Route 53	Elastic Load Balancing load balancers located in the AWS GovCloud (US-West) Region are now integrated into the Route 53 service. Updated text in Setting Up Amazon Route 53 Zone Apex Support with an AWS GovCloud (US) Elastic Load Balancing Load Balancer.	January 12, 2014
Resources	Updated list of additional resources. See Related Resources. Added note about Amazon SNS Mobile Push Notifications. See Amazon SNS .	January 8, 2014
DynamoDB	The DynamoDB console is available and no longer in beta in the AWS GovCloud (US-West) Region. See Amazon DynamoDB.	December 30, 2013
Endpoints	Added AWS Management Console endpoints for federation and SAML. See Service Endpoints.	December 11, 2013
Amazon EC2	Added fix for instructions to create a key pair. See Amazon EC2 .	November 20, 2013
Amazon EMR	The Amazon EMR console is now available in the AWS GovCloud (US-West) Region. See Amazon EMR .	November 12, 2013
Elastic Load Balancing	Elastic Load Balancing is available and no longer in beta in the AWS GovCloud (US-West) Region. See Elastic Load Balancing.	November 1, 2013
AWS Direct Connect	Incorporated changes for AWS Direct Connect console update.	October 31, 2013
AWS CloudFormation	The AWS CloudFormation console is now available in the AWS GovCloud (US-West) Region. See AWS CloudFormation.	October 31, 2013
Kindle	Published a Kindle version.	October 22, 2013

Change	Description	Date Changed
AWS ElasticWolf Client Console	Added link to AWS ElasticWolf Client Console. See Accessing the AWS GovCloud (US) Regions.	October 18, 2013
Elastic Load Balancing	Updates to Elastic Load Balancing ITAR boundary. See Elastic Load Balancing.	September 27, 2013
AWS CloudFormation	Added information about differences with the AWS CloudFormation console for AWS GovCloud (US). See AWS CloudFormation.	August 28, 2013
Virtual Multi-Factor Authentication (MFA)	Added a section about enabling virtual MFA.	August 28, 2013
Amazon Route 53 zone apex AWS GovCloud (US) AWS Direct Connect	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.	August 9, 2013
ARN	Added an example to Amazon Resource Names (ARNs) in GovCloud (US) Regions.	July 24, 2013
Amazon CloudFront Amazon Route 53	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 and Setting Up Amazon Route 53 with Your AWS GovCloud (US) Resources.	July 16, 2013

Change	Description	Date Changed
Amazon Virtual Private Cloud	Added information about AWS GovCloud (US) accounts having an Amazon VPC by default. See Amazon EC2 .	May 28, 2013
AWS Direct Connect	Added information about AWS Direct Connect for AWS GovCloud (US).	May 8, 2013
Initial release	This is the first release of *AWS GovCloud (US) User Guide*.	April 10, 2013

AWS Glossary

For the latest AWS terminology, see the AWS glossary in the *AWS Glossary Reference*.