User Guide

AWS Top Secret Regions

Version 1.0.202411260521

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Top Secret Regions: User Guide

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

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

Table of Contents

What is AWS Top Secret Regions? ... 1
What is in this Guide? ... 1
What Can I Do? ... 2
Supported Services ... 2
Getting Started ... 5
Signing Up ... 5
Close Account ... 9
Using the Console ... 10
How the Console Differs for AWS Top Secret Regions ... 11
To open the console ... 11
Tracking AWS Spending ... 11
See an Overview of this Month's Spending ... 12
See Line-Item Reports ... 12
See Bills from Previous Months ... 13
Changing Your Account Email ... 14
Amazon Linux ... 16
Amazon Linux 2023 ... 16
Certificates Included in Amazon Linux 2023 ... 16
How to update an imported Amazon Linux 2023 AMI to work in the Region ... 17
On-Premises and Docker Images Not Included ... 18
Troubleshooting Amazon Linux 2023 ... 19
More Information ... 19
Amazon Linux 2 ... 19
Tools and Certificates Included in Amazon Linux 2 ... 20
How to Update to the Latest Amazon Linux 2 ... 20
How to update an imported Amazon Linux 2 AMI to work in the Region ... 21
On-Premises and Docker Images Not Included ... 22
Troubleshooting Amazon Linux 2 ... 22
More Information ... 23
Windows AMIs ... 24
Tools and Certificates Included in Windows AMIs ... 24
How Windows AMIs Differ for AWS Top Secret Regions ... 24
How to Install Windows Components from Installation Media ... 25
More Information ... 26

AWS Deep Learning AMIs ... 27
How Deep Learning AMI Differs for AWS Top Secret Regions ... 27
More Information ... 28
AWS CLI and Tools ... 29
AWS CLI ... 29
AWS Tools for Windows PowerShell ... 30
AWS SDKs ... 32
AWS SDK for C++ ... 32
AWS SDK for Go ... 33
AWS SDK for Java ... 33
AWS SDK for JavaScript ... 33
AWS SDK for JavaScript in Node.js ... 34
AWS SDK for Kotlin ... 34
AWS SDK for .NET ... 34
AWS SDK for PHP ... 35
AWS SDK for Python (Boto) ... 35
AWS SDK for Ruby ... 36
AWS SDK for Rust ... 36
AWS CDK ... 38
Configure AWS account and region ... 38
Install and configure Node.js ... 39
Install the AWS CDK ... 40
Configure Docker ... 40
Working with the AWS CDK in Python ... 40
Working with the AWS CDK in Java or C# ... 41
Using the AWS CDK Toolkit (CLI) ... 41
Bootstrapping (CDK v1) ... 41
Bootstrapping (CDK v2) ... 41
Synthesizing, deploying, and destroying your app ... 42
Certificates ... 44
Certificate Authority Rotation ... 45
Testing Your Certificate Configuration ... 45
Downloading the Test Scripts ... 45
AWS CLI ... 45
Java ... 45
JavaScript ... 46

PHP ... 46
Python ... 46
Ruby ... 46
Windows PowerShell ... 46
Using Amazon Linux 2 ... 47
Using AWS Windows AMIs ... 47
Verifying Your Windows AMI Certificates ... 47
Getting the Version of Your Windows AMI ... 47
Creating a Certificate Bundle ... 48
Create a New Certificate Bundle ... 48
Add a New CA Certificate to a Bundle ... 49
Use a Certificate Bundle from Linux on Windows ... 49
Creating a New Java Keystore on Linux ... 50
Manually Updating Your SDK and Tool Trust Stores ... 50
AWS CLI ... 50
AWS SDK for Java ... 51
AWS SDK for JavaScript in Node.js ... 52
AWS SDK for PHP ... 53
AWS SDK for Python (Boto) ... 53
AWS SDK for Ruby ... 54
AWS SDK for .NET and AWS Tools for Windows PowerShell ... 54
Customer Compliance Guide ... 55
Endpoints ... 56
AWS Top Secret - East Endpoints ... 56
AWS Top Secret - West Endpoints ... 68
ARNs ... 77
Services ... 79
AWS Account Management ... 83
Region Availability ... 83
How Account Management Differs for AWS Top Secret Regions ... 83
Documentation for Account Management ... 84
API Gateway ... 84
Region Availability ... 83
How API Gateway Differs for AWS Top Secret Regions ... 85
How Command Line and API Access Differs for AWS Top Secret Regions ... 86
Documentation for API Gateway ... 86

AWS AppConfig ... 88
Region Availability ... 83
How AWS AppConfig Differs for AWS Top Secret Regions ... 88
How Command Line and API Access Differs for AWS Top Secret Regions ... 88
Documentation for AWS AppConfig ... 89
Application Auto Scaling ... 90
Region Availability ... 83
How Application Auto Scaling Differs for AWS Top Secret Regions ... 90
How Command Line and API Access Differs for AWS Top Secret Regions ... 91
Documentation for Application Auto Scaling ... 92
Amazon Athena ... 93
How Athena Differs for AWS Top Secret Regions ... 93
How Command Line and API Access Differs for AWS Top Secret Regions ... 98
Documentation for Athena ... 99
Amazon Aurora ... 100
Region Availability ... 83
How Aurora Differs for AWS Top Secret Regions ... 100
How Command Line and API Access Differs for AWS Top Secret Regions ... 103
Documentation for Aurora ... 103
AWS Billing and Cost Management ... 104
Region Availability ... 83
How Billing and Cost Management Differs for AWS Top Secret Regions ... 104
Documentation for Billing and Cost Management ... 105
Cloud Control API ... 106
Region Availability ... 83
How Cloud Control API Differs for AWS Top Secret Regions ... 106
How Command Line and API Access Differs for AWS Top Secret Regions ... 107
Documentation for Cloud Control API ... 107
AWS CloudFormation ... 108
Region Availability ... 83
How AWS CloudFormation Differs for AWS Top Secret Regions ... 108
How the AWS CloudFormation Helper Scripts Differ for AWS Top Secret Regions ... 110
How Command Line and API Access Differs for AWS Top Secret Regions ... 112
Documentation for AWS CloudFormation ... 113
AWS CloudTrail ... 114
Region Availability ... 83

How CloudTrail Differs for AWS Top Secret Regions ... 114
Services Supported within CloudTrail ... 115
How Command Line and API Access Differs for AWS Top Secret Regions ... 115
Documentation for CloudTrail ... 115
Amazon CloudWatch ... 117
Region Availability ... 83
How CloudWatch Differs for AWS Top Secret Regions ... 88
How Command Line and API Access Differs for AWS Top Secret Regions ... 88
Documentation for CloudWatch ... 89
Amazon CloudWatch Logs ... 120
Region Availability ... 83
How CloudWatch Logs Differs for AWS Top Secret Regions ... 120
How Command Line and API Access Differs for AWS Top Secret Regions ... 121
Documentation for CloudWatch Logs ... 121
AWS CodeDeploy ... 122
Region Availability ... 83
How CodeDeploy Differs for AWS Top Secret Regions ... 122
How Command Line and API Access Differs for AWS Top Secret Regions ... 123
Documentation for CodeDeploy ... 123
Amazon Comprehend ... 125
Region Availability ... 83
How Amazon Comprehend Differs for AWS Top Secret Regions ... 125
How Command Line and API Access Differs for AWS Top Secret Regions ... 126
Documentation for Amazon Comprehend ... 126
AWS Config ... 127
Region Availability ... 83
How AWS Config Differs for AWS Top Secret Regions ... 127
How Command Line and API Access Differs for AWS Top Secret Regions ... 129
Documentation for AWS Config ... 129
AWS Database Migration Service ... 130
Region Availability ... 83
How AWS DMS Differs for AWS Top Secret Regions ... 130
How Command Line and API Access Differs for AWS Top Secret Regions ... 133
Documentation for AWS DMS ... 133
DataSync ... 134
Region Availability ... 83

How DataSync Differs for AWS Top Secret Regions 134
How Command Line and API Access Differs for AWS Top Secret Regions 135
Documentation for DataSync 135
..... 136
How Amazon DCV Differs for AWS Top Secret Regions 136
Documentation for Amazon DCV 137
AWS Direct Connect 138
Region Availability 83
How AWS Direct Connect Differs for AWS Top Secret Regions 138
How Command Line and API Access Differs for AWS Top Secret Regions 139
Documentation for AWS Direct Connect 140
AWS Directory Service 141
Region Availability 83
How AWS Directory Service Differs for AWS Top Secret Regions 141
How Command Line and API Access Differs for AWS Top Secret Regions 142
Documentation for AWS Directory Service 143
Amazon DynamoDB 144
Region Availability 83
How DynamoDB Differs for AWS Top Secret Regions 144
How Command Line and API Access Differs for AWS Top Secret Regions 145
Documentation for DynamoDB 145
Amazon EBS 146
Region Availability 83
How Amazon EBS Differs for AWS Top Secret Regions 146
Documentation for Amazon EBS 147
EBS direct APIs 148
Region Availability 83
How EBS direct APIs Differs for AWS Top Secret Regions 148
How Command Line and API Access Differs for AWS Top Secret Regions 148
Documentation for EBS direct APIs 149
Amazon EC2 150
Region Availability 83
How Amazon EC2 Differs for AWS Top Secret Regions 150
How VM Import/Export Differs for AWS Top Secret Regions 154
How Command Line and API Access Differs for AWS Top Secret Regions 155
Documentation for Amazon EC2 147

Amazon EC2 Auto Scaling ... 156
Region Availability ... 83
How Auto Scaling Differs for AWS Top Secret Regions ... 90
How Command Line and API Access Differs for AWS Top Secret Regions ... 91
Documentation for Auto Scaling ... 92
Amazon EC2 Image Builder ... 159
Region Availability for Image Builder ... 159
How Image Builder Differs for AWS Top Secret Regions ... 159
How Command Line and API Access Differs for AWS Top Secret Regions ... 160
Documentation for Image Builder ... 160
Amazon ECR ... 161
Region Availability ... 83
How Amazon ECR Differs for AWS Top Secret Regions ... 161
How Command Line and API Access Differs for AWS Top Secret Regions ... 162
Documentation for Amazon ECR ... 162
Amazon ECS ... 163
Region Availability ... 83
How Amazon ECS Differs for AWS Top Secret Regions ... 163
How Command Line and API Access Differs for AWS Top Secret Regions ... 165
Documentation for Amazon ECS ... 165
Amazon EFS ... 166
Region Availability ... 83
How Amazon EFS Differs for AWS Top Secret Regions ... 166
How Command Line and API Access Differs for AWS Top Secret Regions ... 167
Documentation for Amazon EFS ... 167
Amazon EKS ... 168
Amazon EKS ADC User Guide Supplement ... 168
Region Availability ... 83
How Amazon EKS Differs for AWS Top Secret Regions ... 169
How Command Line and API Access Differs for AWS Top Secret Regions ... 170
Elastic Load Balancing ... 171
Region Availability ... 83
How Elastic Load Balancing Differs for AWS Top Secret Regions ... 171
How Command Line and API Access Differs for AWS Top Secret Regions ... 173
Documentation for Elastic Load Balancing ... 173
Amazon EMR ... 175

Region Availability ... 83
How Amazon EMR Differs for AWS Top Secret Regions ... 175
Documentation for Amazon EMR ... 186
Amazon ElastiCache ... 188
Region Availability ... 83
How ElastiCache Differs for AWS Top Secret Regions ... 188
How Command Line and API Access Differs for AWS Top Secret Regions ... 191
Documentation for ElastiCache ... 192
AWS Elemental MediaPackage ... 193
Region Availability ... 83
How MediaPackage Differs for AWS Top Secret Regions ... 193
How Command Line and API Access Differs for AWS Top Secret Regions ... 194
Documentation for MediaPackage ... 194
AWS Elemental MediaLive ... 195
Region Availability ... 83
How MediaLive Differs for AWS Top Secret Regions ... 195
How Command Line and API Access Differs for AWS Top Secret Regions ... 196
Documentation for MediaLive ... 196
Amazon EventBridge ... 197
Region Availability ... 83
How Amazon EventBridge Differs for AWS Top Secret Regions ... 197
How Command Line and API Access Differs for AWS Top Secret Regions ... 198
Documentation for Amazon EventBridge ... 198
Amazon FSx ... 199
Region Availability ... 83
How Amazon FSx Differs for AWS Top Secret Regions ... 199
How Command Line and API Access Differs for AWS Top Secret Regions ... 200
Documentation for Amazon FSx ... 200
Amazon S3 Glacier ... 202
Region Availability ... 83
How S3 Glacier Differs for AWS Top Secret Regions ... 202
How Command Line and API Access Differs for AWS Top Secret Regions ... 202
Documentation for S3 Glacier ... 203
AWS Glue ... 204
Region Availability ... 83
How AWS Glue Differs for AWS Top Secret Regions ... 204

How Command Line and API Access Differs for AWS Top Secret Regions 205
Documentation for AWS Glue 205
GuardDuty 206
Region Availability 83
How Amazon GuardDuty Differs for AWS Top Secret Regions 206
How Command Line and API Access Differs for AWS Top Secret Regions 208
Documentation for Amazon GuardDuty 208
AWS Health 209
Region Availability 83
How AWS Health Differs for AWS Top Secret Regions 209
How Command Line and API Access Differs for AWS Top Secret Regions 210
Documentation for AWS Health 210
AWS Identity and Access Management 211
Region Availability 83
How IAM Differs for AWS Top Secret Regions 211
How Command Line and API Access Differs for AWS Top Secret Regions 213
Documentation for IAM 214
AWS Key Management Service 215
Region Availability 83
How AWS KMS Differs for AWS Top Secret Regions 215
How Command Line and API Access Differs for AWS Top Secret Regions 216
Documentation for AWS KMS 216
Amazon Kinesis Data Streams 217
Region Availability 83
How Kinesis Differs for AWS Top Secret Regions 217
How Command Line and API Access Differs for AWS Top Secret Regions 218
Documentation for Kinesis 218
Amazon Data Firehose 219
Region Availability 83
How Firehose Differs for AWS Top Secret Regions 219
How Command Line and API Access Differs for AWS Top Secret Regions 220
Documentation for Firehose 220
AWS Lambda 221
Region Availability 83
How Lambda Differs for AWS Top Secret Regions 221
How Command Line and API Access Differs for AWS Top Secret Regions 223

Documentation for Lambda ... 223
AWS License Manager ... 225
Region Availability for License Manager ... 225
How License Manager Differs for AWS Top Secret Regions ... 225
How Command Line and API Access Differs for AWS Top Secret Regions ... 226
Documentation for License Manager ... 226
AWS Marketplace ... 227
Region Availability ... 83
How AWS Marketplace Differs for AWS Top Secret Regions ... 227
Documentation for AWS Marketplace ... 228
AWS Modular Data Center Rack ... 229
How MDC Rack Differs for AWS Top Secret Regions ... 229
Documentation for MDC Rack ... 229
Neptune ... 230
Region Availability ... 83
How Neptune Differs for AWS Top Secret Regions ... 230
How Command Line and API Access Differs for AWS Top Secret Regions ... 231
Documentation for Neptune ... 231
Amazon OpenSearch Service ... 232
Region Availability ... 83
How OpenSearch Service Differs for AWS Top Secret Regions ... 232
How Command Line and API Access Differs for AWS Top Secret Regions ... 233
Documentation for OpenSearch Service ... 233
AWS Outposts ... 234
Region Availability ... 83
How AWS Outposts Differs for AWS Top Secret Regions ... 234
How Command Line and API Access Differs for AWS Top Secret Regions ... 234
Documentation for AWS Outposts ... 235
AWS ParallelCluster ... 236
Region Availability ... 83
How AWS ParallelCluster Differs for AWS Top Secret Regions ... 236
How the pcluster CLI Differs for AWS Top Secret Regions ... 238
Documentation for AWS ParallelCluster ... 238
AWS Pricing Calculator ... 240
Region Availability ... 83
How AWS Pricing Calculator Differs for AWS Top Secret Regions ... 88

Documentation for AWS Pricing Calculator ... 89
Amazon Redshift ... 242
Region Availability ... 83
How Amazon Redshift Differs for AWS Top Secret Regions ... 242
How Command Line and API Access Differs for AWS Top Secret Regions ... 245
Documentation for Amazon Redshift ... 245
Amazon RDS ... 247
Region Availability ... 83
How Amazon RDS Differs for AWS Top Secret Regions ... 100
How Command Line and API Access Differs for AWS Top Secret Regions ... 103
Documentation for Amazon RDS ... 103
AWS Resource Groups ... 252
Region Availability ... 83
How Resource Groups Differs for AWS Top Secret Regions ... 252
How Command Line and API Access Differs for AWS Top Secret Regions ... 252
Documentation for Resource Groups ... 253
AWS Resource Access Manager ... 254
Region Availability ... 83
How AWS RAM differs for AWS Top Secret Regions ... 254
How Command Line and API Access Differs for AWS Top Secret Regions ... 254
Documentation for AWS RAM ... 238
AWS Resource Groups Tagging API ... 256
How AWS Resource Groups Tagging API Differs for AWS Top Secret Regions ... 256
How Command Line and API Access Differs for AWS Top Secret Regions ... 256
Documentation for AWS Resource Groups Tagging API ... 257
Amazon Route 53 ... 258
Region Availability ... 83
How Route 53 Differs for AWS Top Secret Regions ... 258
How Command Line and API Access Differs for AWS Top Secret Regions ... 260
Documentation for Route 53 ... 261
ARC ... 262
Region Availability ... 83
How ARC Differs for AWS Top Secret Regions ... 262
How Command Line and API Access Differs for AWS Top Secret Regions ... 263
Documentation for ARC ... 263
SageMaker ... 264

Region Availability ... 83
How SageMaker Differs for AWS Top Secret Regions ... 264
How Command Line and API Access Differs for AWS Top Secret Regions ... 265
Documentation for SageMaker ... 265
AWS SAM ... 267
Region Availability ... 83
How AWS SAM Differs for AWS Top Secret Regions ... 267
How Command Line and API Access Differs for AWS Top Secret Regions ... 267
Documentation for AWS SAM ... 268
AWS Secrets Manager ... 269
Region Availability ... 83
How Secrets Manager Differs for AWS Top Secret Regions ... 269
How Command Line and API Access Differs for AWS Top Secret Regions ... 270
Documentation for Secrets Manager ... 270
AWS Security Hub ... 271
How Security Hub Differs for AWS Top Secret Regions ... 271
How Command Line and API Access Differs for AWS Top Secret Regions ... 272
Documentation for Security Hub ... 272
Amazon S3 ... 273
Region Availability ... 83
How Amazon S3 Differs for AWS Top Secret Regions ... 273
How Command Line and API Access Differs for AWS Top Secret Regions ... 276
Documentation for Amazon S3 ... 277
Amazon SNS ... 278
Region Availability ... 83
How Amazon SNS Differs for AWS Top Secret Regions ... 278
How Command Line and API Access Differs for AWS Top Secret Regions ... 285
Documentation for Amazon SNS ... 285
Amazon SQS ... 286
Region Availability ... 83
How Amazon SQS Differs for AWS Top Secret Regions ... 286
How Command Line and API Access Differs for AWS Top Secret Regions ... 290
Documentation for Amazon SQS ... 290
Amazon SWF ... 292
Region Availability ... 83
How Amazon SWF Differs for AWS Top Secret Regions ... 292

How Command Line and API Access Differs for AWS Top Secret Regions 292
Documentation for Amazon SWF 293
AWS Snowball Edge 294
Region Availability 83
How Snowball Edge Differs for AWS Top Secret - East 294
How Command Line and API Access Differs for AWS Top Secret - East 295
How Snowball Edge Differs for AWS Top Secret - West 295
How Command Line and API Access Differs for AWS Top Secret - West 295
Documentation for Snowball Edge 297
AWS Step Functions 298
Region Availability 83
How Step Functions Differs for AWS Top Secret Regions 298
How Command Line and API Access Differs for AWS Top Secret Regions 299
Documentation for Step Functions 299
AWS Storage Gateway 300
How Storage Gateway Differs for AWS Top Secret Regions 300
How Command Line and API Access Differs for AWS Top Secret Regions 300
Documentation for Storage Gateway 301
AWS Support 302
AWS Support Center 302
AWS Top Secret Regions Business Support 302
AWS Top Secret Regions Enterprise Support 303
Service Health Dashboard 303
AWS Trusted Advisor 303
Region Availability 83
How AWS Support Differs for AWS Top Secret Regions 303
Documentation for AWS Support 304
AWS Systems Manager 305
Region Availability 83
How Systems Manager Differs for AWS Top Secret Regions 305
How Command Line and API Access Differs for AWS Top Secret Regions 312
Documentation for Systems Manager 313
Amazon Textract 314
Region Availability 83
How Amazon Textract Differs for AWS Top Secret Regions 314
How Command Line and API Access Differs for AWS Top Secret Regions 315

Documentation for Amazon Textract ... 315
Amazon Transcribe ... 316
Region Availability ... 83
How Amazon Transcribe Differs for AWS Top Secret Regions ... 316
How Command Line and API Access Differs for AWS Top Secret Regions ... 317
Documentation for Amazon Transcribe ... 317
AWS Transit Gateway ... 318
Region Availability ... 83
How AWS Transit Gateway Differs for AWS Top Secret Regions ... 318
Documentation for AWS Transit Gateway ... 238
Amazon Translate ... 320
Region Availability ... 83
How Amazon Translate Differs for AWS Top Secret Regions ... 320
How Command Line and API Access Differs for AWS Top Secret Regions ... 321
Documentation for Amazon Translate ... 321
AWS Trusted Advisor ... 322
Region Availability ... 83
How AWS Trusted Advisor Differs for AWS Top Secret Regions ... 303
How Command Line and API Access Differs for AWS Top Secret Regions ... 323
Documentation for AWS Trusted Advisor ... 304
Amazon VPC ... 324
Region Availability ... 83
How Amazon VPC Differs for AWS Top Secret Regions ... 318
How Command Line and API Access Differs for AWS Top Secret Regions ... 155
Documentation for Amazon VPC ... 147
AWS VPN ... 327
Region Availability ... 83
How AWS VPN Differs for AWS Top Secret Regions ... 327
How Command Line and API Access Differs for AWS Top Secret Regions ... 155
Documentation for AWS VPN ... 147
Amazon WorkSpaces ... 330
Region Availability ... 83
How WorkSpaces Differs for AWS Top Secret Regions ... 330
How to Add the Required IAM Role Needed to Register a Directory for WorkSpaces in AWS Top Secret Regions ... 332
Downloading WorkSpaces Clients in AWS Top Secret Regions ... 333

How Command Line and API Access Differs for AWS Top Secret Regions 334
Documentation for WorkSpaces 334
Document History 335
Documentation Notice 458
AWS Glossary 459

What is AWS Top Secret Regions?

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

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

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

Topics

- What is in this Guide?
- What Can I Do with AWS Top Secret Regions?

What is in this Guide?

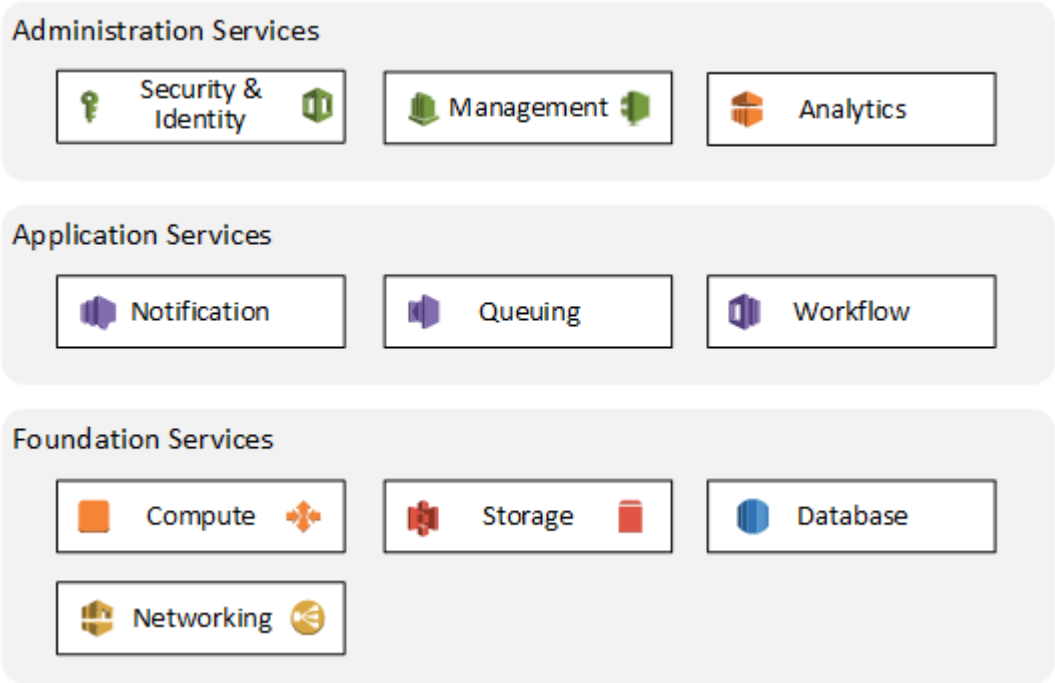
This guide provides instructions for setting up your account and identifies differences between the public Amazon Web Services (AWS) cloud offerings and the operational environment for AWS Top Secret Regions.

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

What Can I Do with AWS Top Secret Regions?

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

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



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

Supported Services

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

Compute

- Amazon Elastic Compute Cloud
- AWS Transit Gateway
- Amazon EC2 Auto Scaling
- Elastic Load Balancing

Storage

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

Database

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

Networking & Content Delivery

- AWS Transit Gateway
- AWS Direct Connect
- Elastic Load Balancing

Management Tools

- Amazon CloudWatch
- AWS CloudFormation
- AWS CloudTrail
- AWS Resource Groups Tagging API
- AWS CLI and Tools for AWS Top Secret Regions

Security, Identity, & Compliance

- AWS Identity and Access Management
- AWS Key Management Service

Analytics

- Amazon EMR
- Amazon Kinesis Data Streams
- Amazon Redshift

Application Services

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

Other Resources

- AWS Billing and Cost Management
- AWS Support

Getting Started with AWS Top Secret Regions

To use AWS Top Secret Regions, you must sign up to create an account that is specific to AWS Top Secret Regions. In other words, you can't use AWS accounts that were created for use in other AWS regions within AWS Top Secret Regions. Similarly, you cannot use AWS accounts that were created for AWS Top Secret Regions in other AWS regions.

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

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

Topics

- Signing Up
- Close Account
- Using the AWS Management Console
- Tracking AWS Spending
- Changing Your Account Email Address

Signing Up

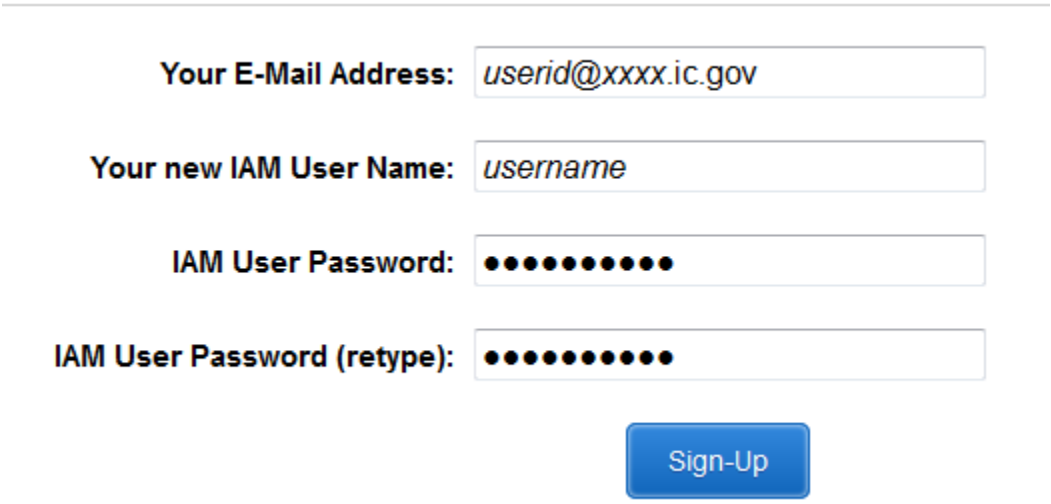
Only members of an IC agency's AWS Top Secret Regions account provisioning team can create AWS Top Secret Regions accounts for workload owners in that agency.

The provisioning team members take an approved request from the valid TO/CLIN and use the information to create a AWS Top Secret Regions account on the workload owner's behalf. The provisioning team member provides the email address and creates an IAM user name and a password. The email address must be JWICS routable and the password must contain a minimum of 10 characters.

In addition, the provisioning team member enters contact and payment information for the account provided to them from the valid TO/CLIN.

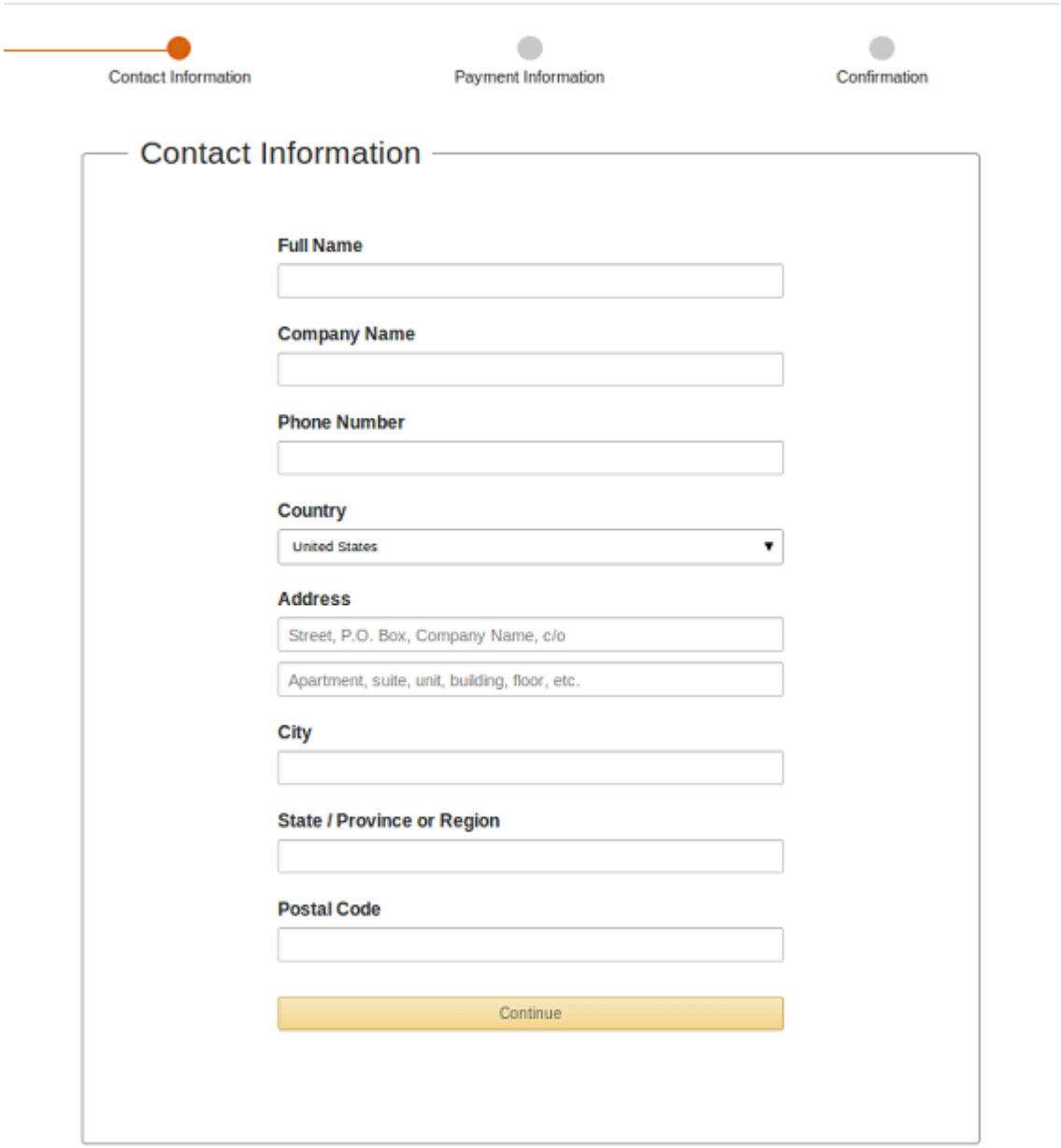
To sign up to create an account for AWS Top Secret Regions

1. Navigate to the page https://signin.c2shome.ic.gov/signup?request_type=register.
2. On the account sign-up page, enter your email address, an IAM user name and password, and then click **Sign-Up**.

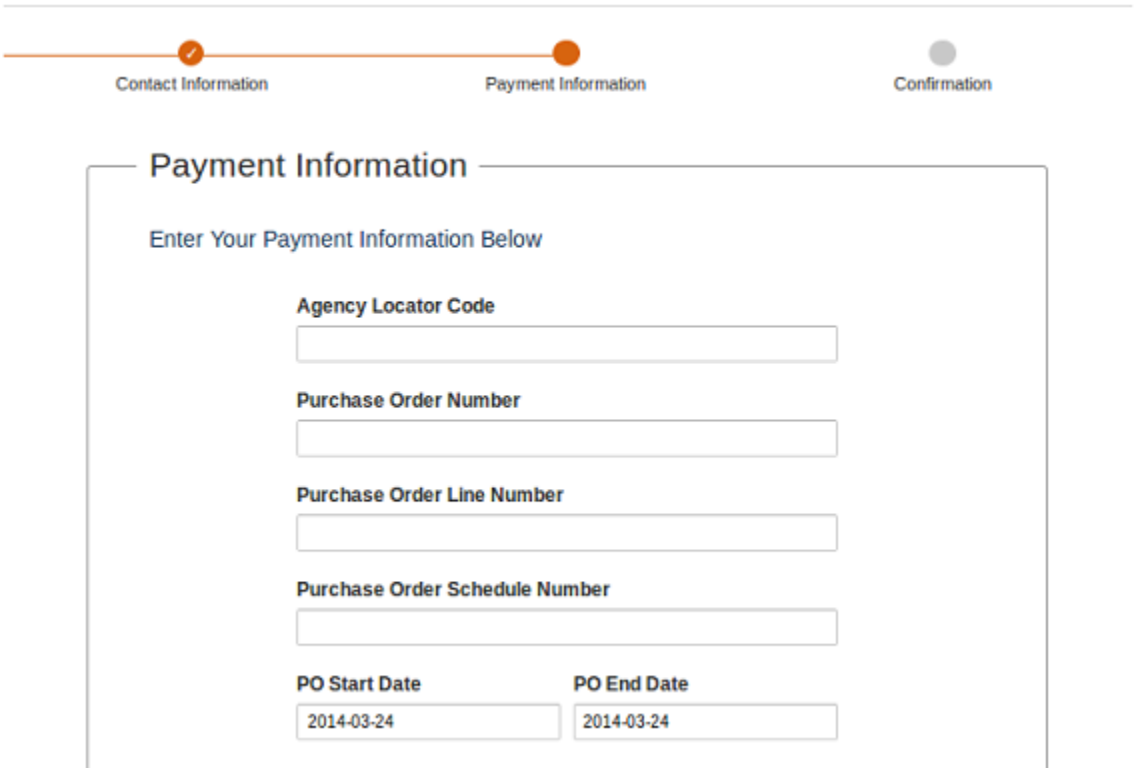


> **Note**
>
> If you later need to change the email address for an account, you use the Security Credentials page in the console. For more information, see Changing Your Account Email Address.

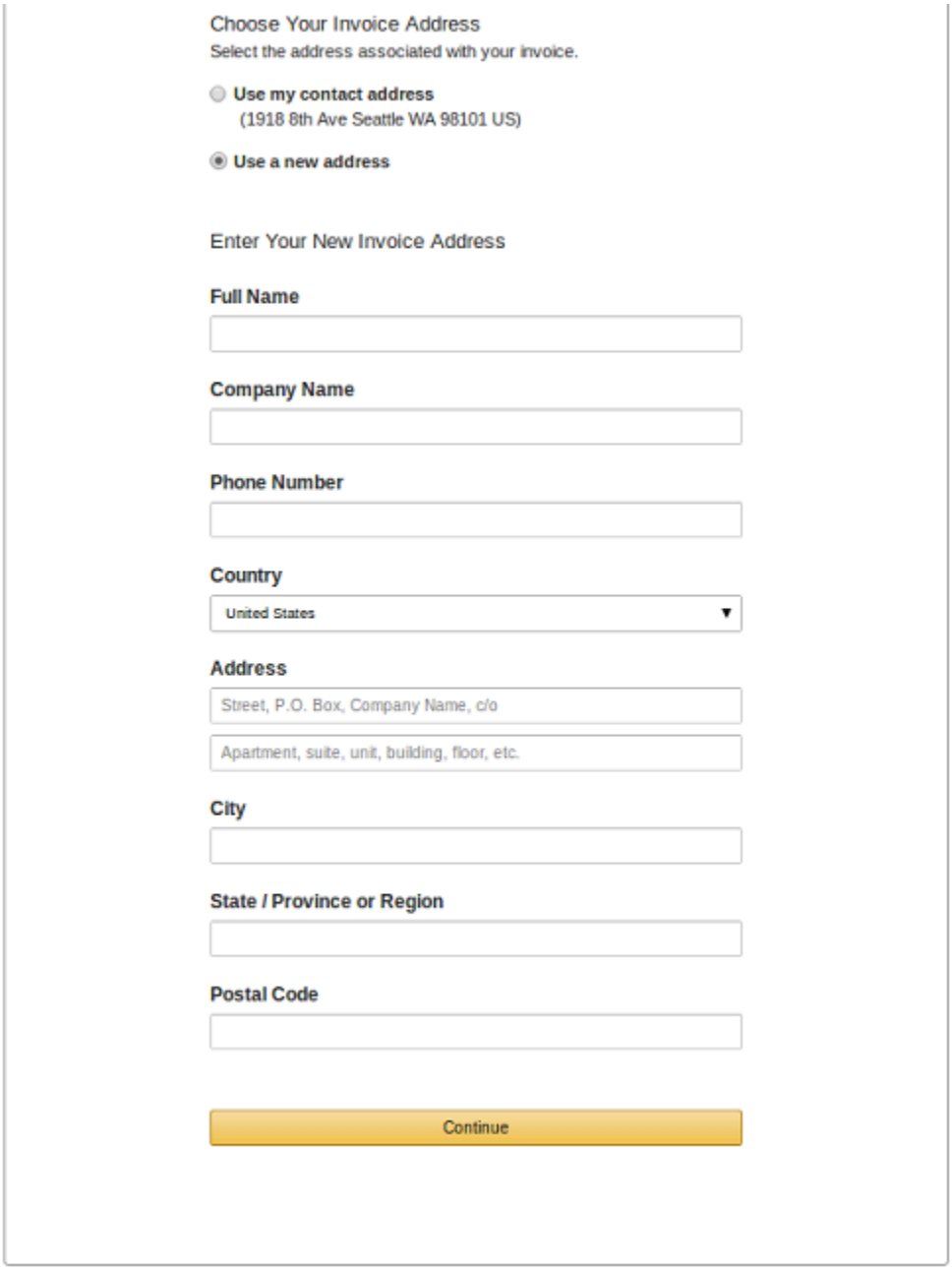
3. On the **Contact Information** page, enter your contact information and then click **Continue**.



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



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



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

Close Account

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

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

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

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

You can close your AWS account using the following procedure.

To close your AWS account

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

Using the AWS Management Console

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

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

How the Console Differs for AWS Top Secret Regions

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

- Resource Groups, Tag Editor, and AWS Console mobile app are not available.
- Unified Search only supports service and feature searches.
- The only widgets currently available in Console Home are the Welcome to AWS, Recently visited, AWS Health, and the Favorites widget.
- myApplications is unavailable.

To open the console

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

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

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

Tracking AWS Spending

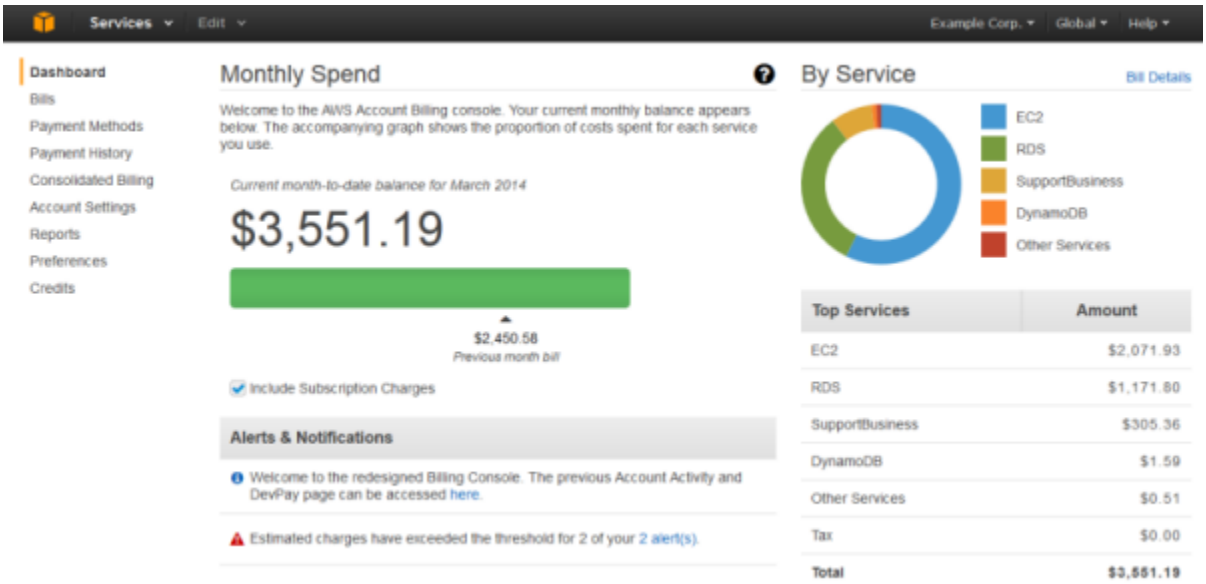
You can see your estimated AWS spending for the current month in one of two ways: as an overview in bar graph form, or as a detailed CSV report delivered daily to an Amazon S3 bucket. You can also see your past months' invoices and download them as PDF files.

Topics

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

See an Overview of this Month's Spending

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



To see an overview of this month's spending

1. Sign in to the AWS Management Console at https://console.c2shome.ic.gov/.
2. Click your account name in the top navigation bar ("Example Corp." in the preceding illustration).
3. Click **Billing and Cost Management**.

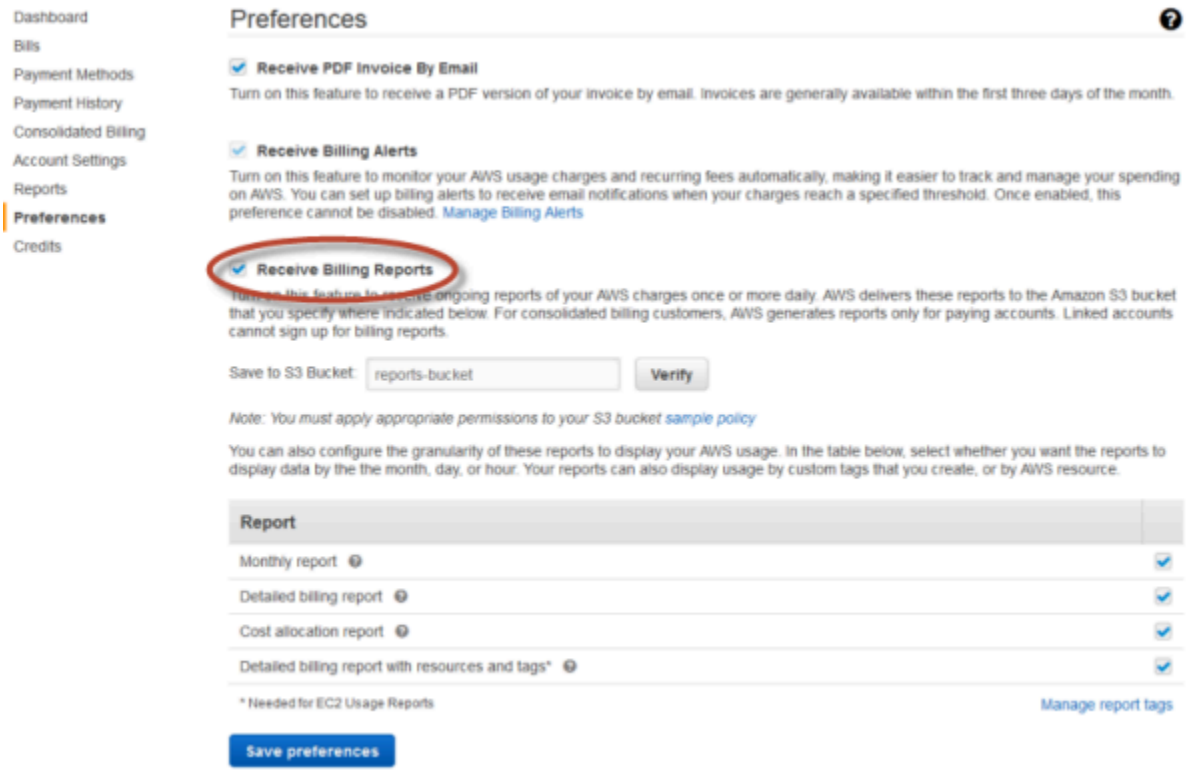
See Line-Item Reports

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

To sign up for Billing and Cost Management reports

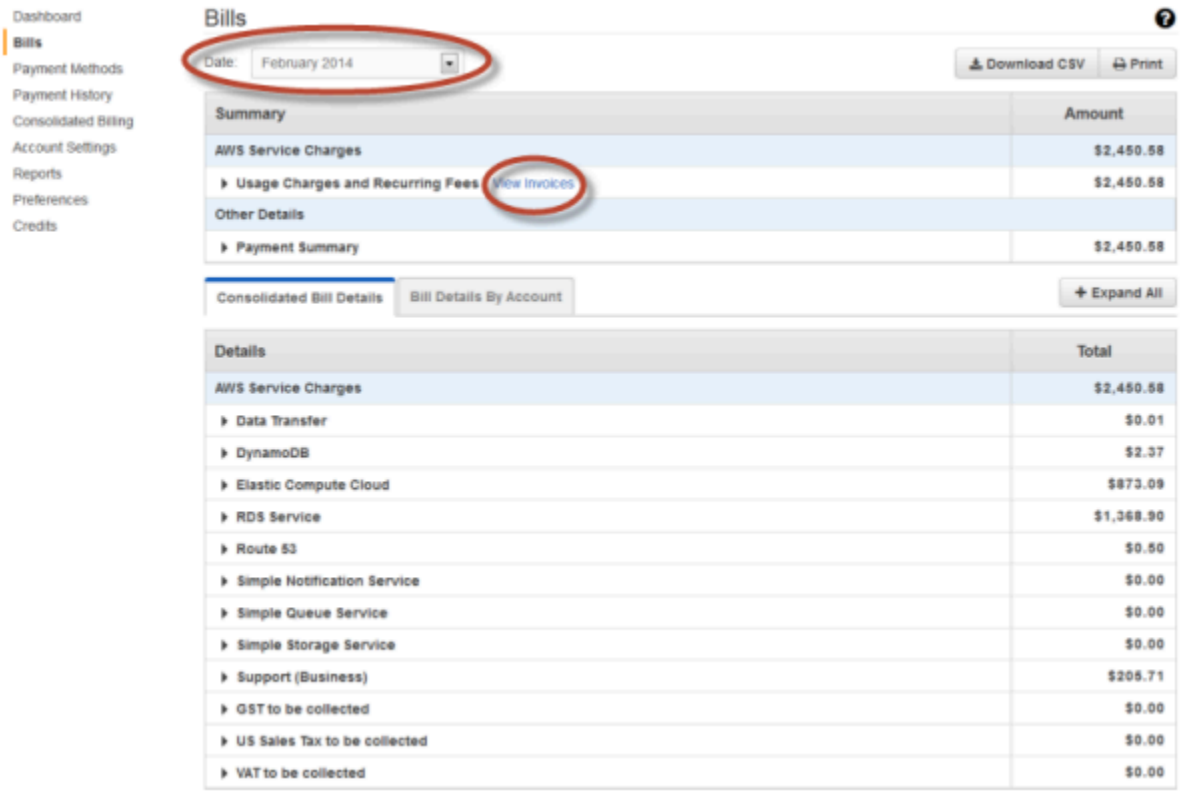
1. Sign in to the AWS Management Console at https://console.c2shome.ic.gov/.
2. Click your account name in the top navigation bar.

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



See Bills from Previous Months

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



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

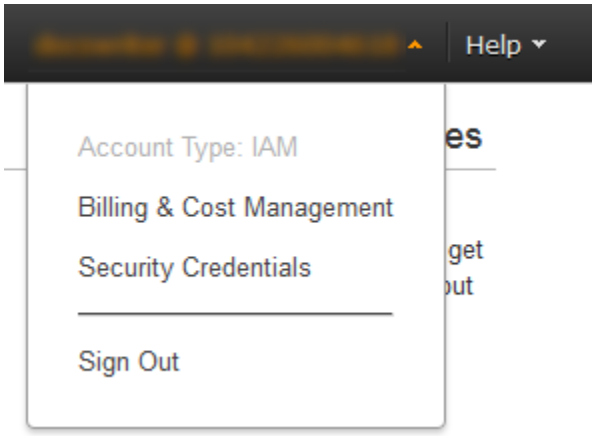
1. Sign in to the AWS Management Console at https://console.c2shome.ic.gov/
2. Click your account name in the top navigation bar.
3. Click **Billing and Cost Management**.
4. Click **Bills** in the left navigation pane.
5. Select the month you want to see in the **Date** list.
6. Click **View invoices** to download PDFs of previous bills.

Changing Your Account Email Address

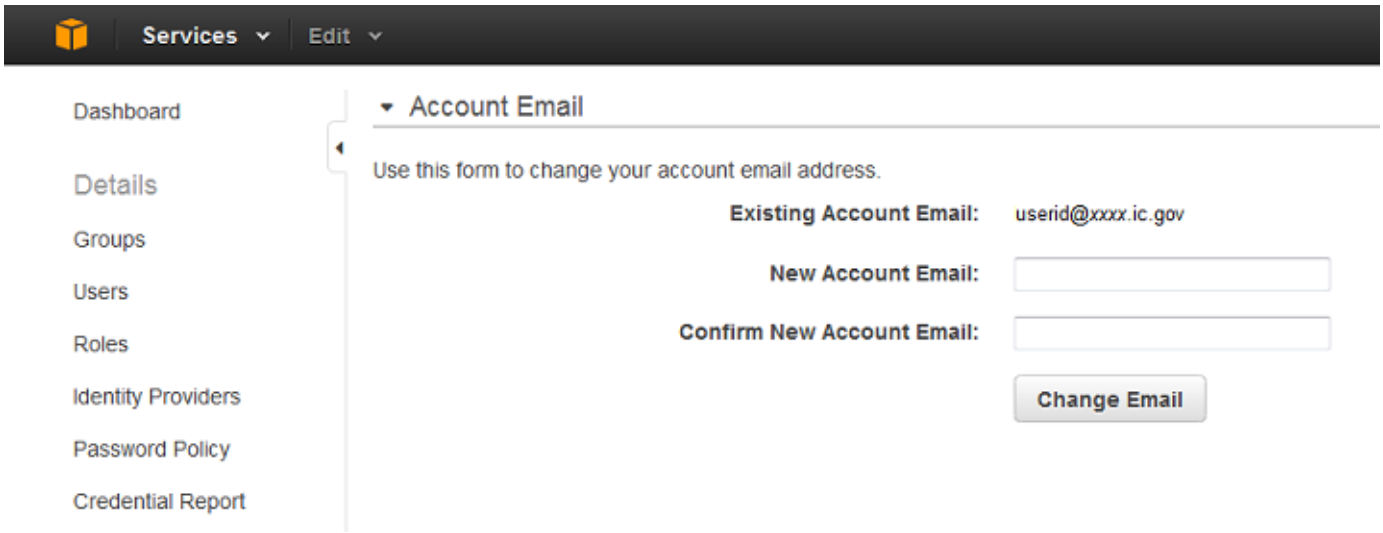
When your account is initially created in AWS Top Secret Regions, it is associated with an email address. Later, if you need to change this email address, you use the following procedure.

To change the email address for your account for IAM users

1. Sign into the AWS Management Console at https://console.c2shome.ic.gov/.
2. In the navigation bar, click your name, and then click **Security Credentials**.



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



To change the email address for your account for IAM roles

1. Sign into the AWS Management Console at https://console.c2shome.ic.gov/.
2. Go to the Security Credentials console at https://console.c2shome.ic.gov/iam/home?#/my_password.
3. In the **Account Email** section, enter your new account email address and then choose **Change Email**.

Amazon Linux for AWS Top Secret Regions

Amazon Linux AMIs are supported and maintained Linux images provided by Amazon Web Services for use on Amazon EC2. They include packages for easy integration with AWS, including launch configuration tools and many popular AWS libraries and tools.

Topics

- Amazon Linux 2023 for AWS Top Secret Regions
- Amazon Linux 2 AMI for AWS Top Secret Regions

Amazon Linux 2023 for AWS Top Secret Regions

Amazon Linux 2023 is the latest generation of Amazon Linux, a Linux server operating system from Amazon Web Services (AWS). It provides a secure, stable, and high-performance execution environment to develop and run cloud and enterprise applications. With Amazon Linux 2023, you get an application environment that offers long-term support with access to the latest innovations in the Linux ecosystem.

> **Note**
>
> The following code samples include references to `us-iso-east-1`. Replace this with `us-iso-west-1` if working in AWS Top Secret - West.

Topics

- Certificates Included in Amazon Linux 2023
- How to update an imported Amazon Linux 2023 AMI to work in the Region
- On-Premises and Docker Images Not Included
- Troubleshooting Amazon Linux 2023
- More Information

Certificates Included in Amazon Linux 2023

By using the latest version of the default Amazon Linux 2023 highside AMI, you can ensure that you have the correct `ca-certificates` package for AWS Top Secret Regions. Amazon Linux 2023

adds these certificates to the root CA bundle, so any tools that already use this bundle should successfully find the correct certificates to verify SSL connections, including the AWS CLI and any AWS SDKs, such as Boto3.

The `ca-certificates` packages for AWS Top Secret Regions use the partition name in AL2023, not the region name as in previous versions of Amazon Linux. The list below maps the partitions to regions and names for the corresponding `ca-certificates` package:

Partition	Region	Package name
iso	us-iso-east-1 and us-iso-west-1	ca-certificates-iso
isob	us-isob-east-1 and us-isob-west-1	ca-certificates-isob
isof	us-isof-south-1 and us-isof-east-1	ca-certificates-isof
isoe	eu-isoe-west-1	ca-certificates-isoe

How to update an imported Amazon Linux 2023 AMI to work in the Region

If an instance is using an AMI copied from another Region, it will not contain the Region-specific packages and will not have the correct configuration for the `ca-certificates`, the AWS CLI, and SDK configurations. You can use these steps to update your Amazon Linux 2023 instance with the latest Region-specific packages.

1. Log in to your Amazon Linux 2023 instance.
2. To install Region-specific packages and configurations on an Amazon Linux 2023 AMI copied from the low side, create a temporary `amzn2023-iso` repo.

```
( cat << 'EOF'
[amzn2023-iso]
name=Amazon Linux 2023 isolated Region repository
mirrorlist=http://al2023-repos-$awsregion-de612dc2.s3.$awsregion.$awsdomain/core-
iso/mirrors/$releasever/$basearch/mirror.list
```

```
priority=10
enabled=1
repo_gpgcheck=0
type=rpm
gpgcheck=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-amazon-linux-2023
EOF
) | sudo tee /etc/yum.repos.d/amzn2023-iso.repo
```

3. Install the Region-specific packages.

```
sudo dnf install amazon-linux-repo-iso ca-certificates-iso
```

4. Remove the temporary `amzn2023-iso` repo

```
sudo rm /etc/yum.repos.d/amzn2023-iso.repo
```

5. The Amazon S3 dualstack endpoint is not supported in AWS Top Secret Regions regions. To configure dnf to work properly in AWS Top Secret Regions regions, edit the `/etc/dnf/vars/dualstack` file, and remove the `.dualstack` string (i.e. make it an empty file). Alternatively, the file can be emptied by running:

```
echo -n "" > sudo tee /etc/dnf/vars/dualstack
```

Your Amazon Linux 2023 instance is now configured to work in the Region. You can install any updates and security patches following the same procedure outlined for AL2023 in standard regions. See Updating AL2023 in the AL2023 User Guide.

If you want to create an AMI based on this instance, first clean up the yum cache and cloud init files:

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

Then, use the Amazon EC2 console to create an AMI.

On-Premises and Docker Images Not Included

Amazon Linux 2023 on-premises virtual and Docker images are currently unavailable in AWS Top Secret Regions.

Troubleshooting Amazon Linux 2023

If you are having trouble with an Amazon Linux 2023 AMI, this section has some initial steps to help you troubleshoot. For more information, see AL2023 User Guide.

AWS CLI Doesn't Work

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

1. Run the `aws configure` command and verify that the region is set to *`us-iso-east-1`*.
2. If necessary, update to the latest Amazon Linux 2023 AMI.

SSL Certificate Verification Fails

If you experience SSL connection failures, try these steps.

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

```
dnf update ca-certificates-iso
```

3. If necessary, update to the latest Amazon Linux 2023 AMI.

More Information

For general usage information, including details on updating instances and installing security updates on AL2023, see AL2023 User Guide.

Amazon Linux 2 AMI for AWS Top Secret Regions

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

> **Note**
>
> The following code samples include references to `us-iso-east-1`. Replace this with `us-iso-west-1` if working in AWS Top Secret - West.

Topics

- Tools and Certificates Included in Amazon Linux 2
- How to Update to the Latest Amazon Linux 2
- How to update an imported Amazon Linux 2 AMI to work in the Region
- On-Premises and Docker Images Not Included
- Troubleshooting Amazon Linux 2
- More Information

Tools and Certificates Included in Amazon Linux 2

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

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

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

How to Update to the Latest Amazon Linux 2

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

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

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

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

3. Run the `aws configure` command and make sure to set the default Region to *us-iso-east-1*.

   ```
   aws configure
   ```

Your Amazon Linux 2 instance is now up to date.

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

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

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

   ```
   ( cat << 'EOF'
   [amzn2-iso]
   name=Amazon Linux 2 isolated Region repository
   mirrorlist=http://amazonlinux.$awsregion.$awsdomain/$releasever/core-$awsregion/
   latest/$basearch/mirror.list
   priority=9
   gpgcheck=0
   enabled=1
   metadata_expire=300
   ```

```
mirrorlist_expire=300
report_instanceid=yes
EOF
) | sudo tee /etc/yum.repos.d/tmp-amzn2-iso.repo
```

3. Install the Region-specific packages.

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

4. Remove the temporary `amzn2-iso` repo

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

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

   To install all updates:

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

   To install just security updates.

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

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

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

Use the Amazon EC2 console to create an AMI.

On-Premises and Docker Images Not Included

Amazon Linux 2 on-premises virtual and Docker images are currently unavailable in AWS Top Secret Regions.

Troubleshooting Amazon Linux 2

If you are having trouble with an Amazon Linux 2 AMI, this section has some initial steps to help you troubleshoot. For more information, see Amazon Linux 2 User Guide.

AWS CLI Doesn't Work

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

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

SSL Certificate Verification Fails

If you experience SSL connection failures, try these steps.

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

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

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

More Information

For general usage information, including details on updating instances and installing security updates on Amazon Linux 2, see Amazon Linux 2 User Guide.

AWS Windows AMIs for AWS Top Secret Regions

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

Topics

- Tools and Certificates Included in Windows AMIs
- How Windows AMIs Differ for AWS Top Secret Regions
- How to Install Windows Components from Installation Media
- More Information

Tools and Certificates Included in Windows AMIs

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

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

How Windows AMIs Differ for AWS Top Secret Regions

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

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

How to Install Windows Components from Installation Media

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

> **Note**
>
> These Amazon EBS snapshots are only available in AWS Top Secret - East

Installation Media	Snapshot ID AWS Top Secret - East
Installation media for Windows Server 2008 SP2 64-bit	`snap-9619caff`
Installation media for Windows Server 2008 R2 SP1	`snap-fb18cb92`
Installation media for Windows Server 2012	`snap-f61ecd9f`
Installation media for Windows Server 2012 R2	`snap-3305b75a`
Installation media for Windows Server 2016	`snap-0c183f927586caa36`
Installation media for Windows Server 2019	`snap-098a607556c5da023`

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

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

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

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

Windows PowerShell

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

AWS CLI

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

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

   Windows PowerShell

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

   AWS CLI

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

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

More Information

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

AWS Deep Learning AMIs for AWS Top Secret Regions

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

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

Topics

- How Deep Learning AMI Differs for AWS Top Secret Regions
- More Information

How Deep Learning AMI Differs for AWS Top Secret Regions

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

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

- While the Deep Learning AMIs are supported across all GPU instance types, not all GPU instance types are available in AWS Top Secret Regions. For more information, including a list of all supported instance types, see Amazon EC2 Instances.
- Some of the Deep Learning Framework Tutorials and test scripts will not work. Most of the tutorials come from open source framework repos and rely on connectivity to the public internet for downloading public datasets. These will not work in AWS Top Secret Regions. This includes the TensorBoard, TFServing, and MMS tutorials.
- The AWS Deep Learning AMIs Developer Guide has links to the marketplace and lists all versions of the Deep Learning AMIs. As noted above, only 2 versions are available in AWS Top Secret Regions.
- The Deep Learning AMIs are not recommended to be used with `t2.micro` instance types due to its low memory and compute specifications.

More Information

- AWS Deep Learning AMIs Developer Guide

AWS CLI and Tools for AWS Top Secret Regions

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

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

> **Note**
>
> The following code samples include references to `us-iso-east-1`. Replace this with `us-iso-west-1` if working in AWS Top Secret - West.

Topics

- AWS CLI
- AWS Tools for Windows PowerShell

AWS CLI

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

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

To use the AWS CLI for AWS Top Secret Regions, you must:

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

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

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

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

2. Set the `AWS_CA_BUNDLE` environment variable.

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

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

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

AWS Tools for Windows PowerShell

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

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

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

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

If you are signing requests and creating objects manually (instead of using the PowerShell cmdlets), you must set the AuthenticationRegion property in AWS Top Secret Regions. The following commands show an example of how you could return a list S3 buckets. (Alternatively, it would be easier to just use the Get-S3Bucket cmdlet.)

```
$AWSregion = "us-iso-east-1"
$AWSserviceURL="https://s3.$AWSRegion.c2s.ic.gov"
$config=New-Object Amazon.S3.AmazonS3Config
$config.ServiceURL = $AWSserviceURL
$config.SignatureVersion = 4
# Set the AuthenticationRegion property because the region cannot be determined from
 the service endpoint.
$config.AuthenticationRegion = $AWSregion
$s3Client = New-Object Amazon.S3.AmazonS3Client ($config)
$response = $s3Client.ListBuckets()
$response.Buckets | Write-Output
```

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

AWS SDKs for AWS Top Secret Regions

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

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

> **Note**
>
> The following code samples include references to `us-iso-east-1`. Replace this with `us-iso-west-1` if working in AWS Top Secret - West.

Topics

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for JavaScript in Node.js
- AWS SDK for Kotlin
- AWS SDK for .NET
- AWS SDK for PHP
- AWS SDK for Python (Boto)
- AWS SDK for Ruby
- AWS SDK for Rust

AWS SDK for C++

To use the AWS SDK for C++ for AWS Top Secret Regions, you must:

- Include a configuration snippet in your applications to use the us-iso-east-1 Region.

- Configure service clients to set either `caFile` (if your application has a single certificate file) or `caPath` (if your application has a directory with multiple certificates) in your Client Configuration.

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

AWS SDK for Go

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

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

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

AWS SDK for Java

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

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

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

AWS SDK for JavaScript

To install the SDK for JavaScript for AWS Top Secret Regions:

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

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

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

- Include a configuration snippet in your applications to use the us-iso-east-1 Region.

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

AWS SDK for JavaScript in Node.js

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

- Run the following command:

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

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

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

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

AWS SDK for Kotlin

To use the SDK for Kotlin for AWS Top Secret Regions, you must:

- Configure the JVM to trust the in-Region root certificate.
- Extract the SDK for Kotlin files to your local Maven repository.
- Configure your SDK for Kotlin clients to use the us-iso-east-1 Region.

AWS SDK for .NET

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

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

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

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

AWS SDK for PHP

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

- Use the configuration file for the us-iso-east-1 Region. (config.us-iso-east-1.php)
- If you cannot use the certificate bundle provided by the operating system, set the `openssl.cafile` PHP ini configuration setting configuration file to the path of the to the certificate bundle.

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

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

AWS SDK for Python (Boto)

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

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

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

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

AWS SDK for Ruby

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

- Specify a valid SSL certificate bundle with `:ssl_ca_file` or `:ssl_ca_path`.
- Require the `aws-sdk-v1-compat` gem to make the `aws-sdk` gem compatible with the us-iso-east-1 region.

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

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

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

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

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

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

AWS SDK for Rust

To use the SDK for Rust for AWS Top Secret Regions, you must:

- Set the region to the us-iso-east-1 Region.
- Override the default HTTP client with one configured to trust the in-region root certificate.

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

AWS CDK for AWS Top Secret Regions

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

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

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

- AWS CDK Developer Guide
- AWS Construct Library API Reference

> **Note**
>
> The following code samples include references to `us-iso-east-1`. Replace this with `us-iso-west-1` if working in AWS Top Secret - West.

Topics

- Configure AWS account and region
- Install and configure Node.js
- Install the AWS CDK
- Configure Docker
- Working with the AWS CDK in Python
- Working with the AWS CDK in Java or C#
- Using the AWS CDK Toolkit (CLI)

Configure AWS account and region

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

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

```
aws configure
```

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

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

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

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

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

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

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

Install and configure Node.js

To install Node.js on Amazon Linux 2, ensure that you have Git installed, then install Node Version Manager (NVM) and configure Node Package Manager (NPM) to use ADV's NPM registry.

```
NODE_VERSION="v14.15.0"

curl https://s3.us-iso-east-1.c2s.ic.gov/adv-src/nvm/install.sh | /bin/bash
. ~/.bash_profile

nvm install $NODE_VERSION
nvm use $NODE_VERSION
nvm alias default $NODE_VERSION
npm config set registry http://npm.appdev.proj.coe.ic.gov
```

Install the AWS CDK

Install the AWS CDK Toolkit globally using the following NPM command.

```
npm install -g aws-cdk
```

Run the following command to verify correct installation and print the version number of the AWS CDK.

```
cdk --version
```

Configure Docker

The AWS CDK can leverage Docker to locally build and test serverless applications. Follow the instructions to set up Docker on Amazon Linux 2.

Working with the AWS CDK in Python

To define cloud infrastructure in Python using the AWS CDK, you will need Python 3.6 or later and configure **pip** to use ADV's Python package repository.

To install Python 3 on Amazon Linux 2, run the following command.

```
sudo yum install python3 -y
```

Create a **pip** configuration file at ~/.pip/pip.conf (Mac OS X or Linux) or %APPDATA%\pip\pip.ini (Windows).

```
[global]
index = http://pypi.appdev.proj.coe.ic.gov/simple/
index-url = http://pypi.appdev.proj.coe.ic.gov/simple/
trusted-host = pypi.appdev.proj.coe.ic.gov
```

To create a new Python AWS CDK application, run the following commands.

```
mkdir my_test_app
cd my_test_app

cdk init sample-app --language python
```

```
source .venv/bin/activate
pip install -r requirements.txt
```

Working with the AWS CDK in Java or C#

For Java and C# support, configure each language's package manager (Maven or NuGet) to point to a repository that has the AWS CDK packages, and is hosted by ADV.

Using the AWS CDK Toolkit (CLI)

This section covers bootstrapping your AWS environment for deploying AWS CDK applications along with the commands to synthesize and deploy apps. For complete information on working with the AWS CDK Toolkit command line interface, see AWS CDK Toolkit.

Bootstrapping (CDK v1)

You must bootstrap the AWS environment so you can deploy AWS CDK applications into it. This differs depending on whether you are using CDK v1 or v2. For v1, simply issue:

```
cdk bootstrap --public-access-block-configuration false
```

Bootstrapping only needs to be done once per AWS account.

Bootstrapping (CDK v2)

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

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

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

Now edit the template in accordance with your policies.

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

To deploy the template after editing, issue:

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

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

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

app = App()

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

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

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

app.synth()
```

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

Bootstrapping only needs to be done once per AWS account.

Synthesizing, deploying, and destroying your app

To view the AWS CloudFormation template generated by the AWS CDK app, issue:

```
cdk synth
```

To deploy your AWS CDK app:

```
cdk deploy
```

To destroy your AWS CDK app and all the resources it defines:

```
cdk destroy
```

Digital Certificates for AWS Top Secret Regions

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

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

When initially installed and configured, the AWS SDKs and tools require the addition of region-specific CA public keys to the trust store that validates connections in the AWS Top Secret Regions. Certificates used by the AWS services in the AWS Top Secret Regions are issued by a CA specific to the region. This CA isn't available in the default trust stores disseminated by the operating system, web browser, and programming language providers on the Internet. However, some of the AWS SDKs and tools are already configured with the new certificates on recent versions of Amazon Linux 2, the Amazon Linux AMI, and AWS Windows AMIs included in the AWS Top Secret Regions.

> **Note**
>
> The following code samples include references to `us-iso-east-1`. Replace this with `us-iso-west-1` if working in AWS Top Secret - West.

Topics

- Certificate Authority Rotation
- Testing Your Certificate Configuration
- Using Amazon Linux 2
- Using AWS Windows AMIs
- Creating a Certificate Bundle
- Creating a New Java Keystore on Linux
- Manually Updating Your SDK and Tool Trust Stores

Certificate Authority Rotation

The current certificate authority, CA4, which has signed the certificates used by AWS services in the AWS Top Secret Regions, is migrating to the new certificate authority, CA5. AWS will begin migration of API endpoints and websites to CA5 in early February 2018.

If your AWS SDKs and tools are configured to **only** use CA4 certificates, you will receive security-related errors when AWS services migrate to certificates signed by the new CA. To avoid service disruptions, you must add the CA5 public keys to your trust store when connecting to AWS endpoints in the AWS Top Secret Regions.

Testing Your Certificate Configuration

If you access AWS services programmatically, you can download scripts to test whether the programming language you are using is configured to use certificates issued from CA5. The scripts perform an HTTPS GET against a known site that uses the correct certificates. The test endpoint is identified in the script.

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

Downloading the Test Scripts

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

Download the Test Scripts

AWS CLI

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

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

Java

To test your Java configuration, run the following:

```
$ javac ShaTest.java
```

```
$ java ShaTest
```

JavaScript

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

```
$ node shaTest.js
```

PHP

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

```
$ php shaTest.php
```

Python

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

```
$ python shaTest.py
```

Ruby

To test your Ruby configuration, run the following:

```
$ ruby shaTest.rb
```

Windows PowerShell

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

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

Using Amazon Linux 2

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

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

Using AWS Windows AMIs

If the certificate test scripts fail, the easiest way to start using the new certificates is to use the latest Windows AMI. The CA4 certificate and the new CA5 certificate are already available, and some of the tools are already configured. The following tools are already configured in the Windows AMIs to use the CA4 and CA5 certificates:

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

Verifying Your Windows AMI Certificates

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

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

Getting the Version of Your Windows AMI

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

For more information, see AWS Windows AMIs for AWS Top Secret Regions.

Creating a Certificate Bundle

If the certificate test scripts fail and you are not able to use the Amazon Linux AMI or a Windows AMI, you will likely need to create a certificate bundle that includes both the CA4 and CA5 certificates.

> **Note**
>
> As described earlier, if you are using the Amazon Linux AMI, the CA4 and CA5 certificates are already available in the aws-cli-ca-certs-*us-iso-east-1* and ca-certificates-java-config-*us-iso-east-1* packages. See /etc/pki /*us-iso-east-1*/certs/ for the .pem and .jks files.

Create a New Certificate Bundle

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

Linux

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

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

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

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

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

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

   The last line of output should be:

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

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

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

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

Windows PowerShell

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

Add a New CA Certificate to a Bundle

If you already have a certificate bundle, you might be able to add a CA5 certificate to it.

Linux

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

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

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

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

Use a Certificate Bundle from Linux on Windows

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

Linux

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

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

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

Creating a New Java Keystore on Linux

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

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

```
sudo yum install java
```

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

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

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

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

Manually Updating Your SDK and Tool Trust Stores

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

AWS CLI

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

Linux

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

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

Windows

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

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

AWS SDK for Java

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

Linux

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

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

Windows

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

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

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

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

AWS SDK for JavaScript in Node.js

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

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

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

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

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

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

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

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

AWS SDK for PHP

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

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

AWS SDK for Python (Boto)

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

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

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

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

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

```
$ cat ~/.boto
[Boto]
```

```
ca_certificates_file = /etc/pki/us-iso-east-1/certs/ca-bundle.pem
endpoints_path = /home/ec2-user/boto/endpoints.json
```

AWS SDK for Ruby

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

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

The public release of the aws-sdk-core gem is included in the SDK for Ruby archive. To make this gem compatible with the AWS Top Secret Regions, you must require the aws-sdk-v2-compat gem.

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

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

AWS SDK for .NET and AWS Tools for Windows PowerShell

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

Customer Compliance Guide

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

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

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

Customer Compliance Guides - AWS Top Secret Regions

Endpoints in AWS Top Secret Regions

If you access services in AWS Top Secret Regions by using the command line interface (CLI) or programmatically by using the APIs, you need to know the endpoints.

For a complete list of endpoints in AWS Top Secret Regions, see the following topics:

- AWS Top Secret - East Endpoints
- AWS Top Secret - West Endpoints

AWS Top Secret - East Endpoints

- The endpoint domain for AWS Top Secret Regions is `c2s.ic.gov`.
- The Region value should be `us-iso-east-1` for an endpoint in AWS Top Secret - East.
- FIPs endpoints are subject to availability, please refer to the services difference documentation.

AWS Service	US ISO East Endpoint	Protocol
API Gateway	apigateway.us-iso-east-1.c2s.ic.gov	HTTPS
API Gateway Dataplane	execute-api.us-iso-east-1.c2s.ic.gov	HTTPS
API Gateway V2	apigateway.us-iso-east-1.c2s.ic.gov	HTTPS
AWS AppConfig	appconfig.us-iso-east-1.c2s.ic.gov appconfig-fips.us-iso-east-1.c2s.ic.gov	HTTPS HTTPS
AWS Config	config.us-iso-east-1.c2s.ic.gov	HTTPS
AWS Config Rules	config.us-iso-east-1.c2s.ic.gov	

AWS Service	US ISO East Endpoint	Protocol
AWS Console Home	us-iso-east-1.console.c2shome.ic.gov/console/home?region=us-iso-east-1	HTTPS
AWS DataSync	datasync.us-iso-east-1.c2s.ic.gov datasync-fips.us-iso-east-1.c2s.ic.gov	HTTPS HTTPS
AWS Diode Service	diode.us-iso-east-1.c2s.ic.gov	HTTPS
AWS Documentation	docs.c2shome.ic.gov	HTTPS
AWS Elemental MediaLive	medialive.us-iso-east-1.c2s.ic.gov	HTTPS
AWS Elemental MediaPackage	mediapackage.us-iso-east-1.c2s.ic.gov	HTTPS
AWS Glue	glue.us-iso-east-1.c2s.ic.gov	HTTPS
AWS Glue DataCatalog Service	datacatalog.us-iso-east-1.c2s.ic.gov	
AWS Glue Frontend Service	glue.us-iso-east-1.c2s.ic.gov	
AWS Health APIs And Notifications	health.us-iso-east-1.c2s.ic.gov	HTTPS
AWS Health Dashboard	phd.c2shome.ic.gov	HTTP and HTTPS
AWS License Manager	license-manager.us-iso-east-1.c2s.ic.gov	HTTPS
AWS Management Console	us-iso-east-1.console.c2shome.ic.gov	HTTPS

AWS Service	US ISO East Endpoint	Protocol
AWS Outposts	outposts.us-iso-east-1.c2s.ic.gov	HTTPS
AWS Price List Service	api.pricing.us-iso-east-1.c2s.ic.gov	HTTPS
AWS Resource Groups Tagging API	tagging.us-iso-east-1.c2s.ic.gov	HTTPS
AWS S3 Control	s3-control.us-iso-east-1.c2s.ic.gov s3-control-fips.us-iso-east-1.c2s.ic.gov s3-control-fips.dualstack.us-iso-east-1.c2s.ic.gov s3-control.dualstack.us-iso-east-1.c2s.ic.gov	HTTPS HTTPS HTTPS HTTPS
AWS S3 Outposts	s3-outposts.us-iso-east-1.c2s.ic.gov s3-outposts-fips.us-iso-east-1.c2s.ic.gov	HTTPS HTTPS
AWS SCM UI Argo Portal	aws-dc.argo.ocean-wave.c2s-a2z.ic.gov	HTTPS
AWS Secrets Manager	secretsmanager.us-iso-east-1.c2s.ic.gov	HTTPS
AWS Snowball Edge	snowball.us-iso-east-1.c2s.ic.gov	HTTPS
AWS Step Functions	states.us-iso-east-1.c2s.ic.gov	HTTPS

AWS Service	US ISO East Endpoint	Protocol
AWS Support Center Console	console.c2shome.ic.gov/support	HTTPS
AWS Systems Manager (SSM)	ssm.us-iso-east-1.c2s.ic.gov	HTTPS
AWS Systems Manager Session Manager	ssmmessages.us-iso-east-1.c2s.ic.gov	HTTPS
AWS Zelkova Service	zelkova.us-iso-east-1.c2s.ic.gov	HTTPS
AWSSignUpPortal	signup.c2shome.ic.gov	HTTP and HTTPS
Amazon API Gateway Websocket Connection API	execute-api.us-iso-east-1.c2s.ic.gov	HTTPS
Amazon CloudWatch Observability Access Manager	oam.us-iso-east-1.c2s.ic.gov	HTTPS
Amazon DCV	nice-dcv.us-iso-east-1.c2s.ic.gov	
Amazon Data Lifecycle Manager	dlm.us-iso-east-1.c2s.ic.gov	HTTPS
Amazon EKS	eks.us-iso-east-1.c2s.ic.gov	HTTPS
Amazon Elastic Container Registry	ecr.us-iso-east-1.c2s.ic.gov	HTTPS
	api.ecr.us-iso-east-1.c2s.ic.gov	HTTPS
Amazon Elastic Container Service	ecs.us-iso-east-1.c2s.ic.gov	HTTPS
Amazon FSx	fsx.us-iso-east-1.c2s.ic.gov	HTTPS
	fsx-fips.us-iso-east-1.c2s.ic.gov	HTTPS

AWS Service	US ISO East Endpoint	Protocol
Amazon FSx for Lustre	fsx.us-iso-east-1.c2s.ic.gov fsx-fips.us-iso-east-1.c2s.ic.gov	HTTPS HTTPS
Amazon FSx for NetApp ONTAP	fsx.us-iso-east-1.c2s.ic.gov fsx-fips.us-iso-east-1.c2s.ic.gov	HTTPS HTTPS
Amazon FSx for Windows File Server	fsx.us-iso-east-1.c2s.ic.gov fsx-fips.us-iso-east-1.c2s.ic.gov	HTTPS HTTPS
Amazon GuardDuty	guardduty.us-iso-east-1.c2s.ic.gov	HTTPS
Amazon Linux Security Center	alas.s3.us-iso-east-1.c2s.ic.gov	HTTPS
Amazon Neptune	rds.us-iso-east-1.c2s.ic.gov	HTTP and HTTPS
Amazon OpenSearch Service	es.us-iso-east-1.c2s.ic.gov	HTTPS
Amazon RDS for MariaDB	rds.us-iso-east-1.c2s.ic.gov	HTTPS
Amazon RDS for MySQL	rds.us-iso-east-1.c2s.ic.gov	HTTPS
Amazon RDS for Oracle	rds.us-iso-east-1.c2s.ic.gov	HTTPS
Amazon RDS for PostgreSQL	rds.us-iso-east-1.c2s.ic.gov	HTTPS
Amazon RDS for SQL Server	rds.us-iso-east-1.c2s.ic.gov	HTTPS
Amazon Recycle Bin	rbin.us-iso-east-1.c2s.ic.gov rbin-fips.us-iso-east-1.c2s.ic.gov	HTTPS HTTPS

AWS Service	US ISO East Endpoint	Protocol
Amazon S3 Replication Time Control	rtc.us-iso-east-1.c2s.ic.gov	
Amazon SageMaker	api.sagemaker.us-iso-east-1.c2s.ic.gov	HTTPS
Amazon SageMaker Neo	api.sagemaker.us-iso-east-1.c2s.ic.gov	
Amazon SageMaker Runtime (Realtime Endpoint Inference)	runtime.sagemaker.us-iso-east-1.c2s.ic.gov	HTTPS
Amazon Textract	textract.us-iso-east-1.c2s.ic.gov	HTTPS
Amazon Transcribe Streaming Service	transcribestreaming.us-iso-east-1.c2s.ic.gov	HTTPS
AppConfigData	appconfigdata.us-iso-east-1.c2s.ic.gov	HTTPS
Application Auto Scaling	application-autoscaling.us-iso-east-1.c2s.ic.gov	HTTP and HTTPS
Athena	athena.us-iso-east-1.c2s.ic.gov	HTTPS
Aurora MySQL	rds.us-iso-east-1.c2s.ic.gov	HTTPS
Aurora PostgreSQL	rds.us-iso-east-1.c2s.ic.gov	HTTPS
Capacity Reservation Service Linked Group	capacity-reservation-integration.us-iso-east-1.c2s.ic.gov	
Cloud Control API	cloudcontrolapi.us-iso-east-1.c2s.ic.gov	HTTPS

AWS Service	US ISO East Endpoint	Protocol
CloudFormation	cloudformation.us-iso-east-1.c2s.ic.gov	HTTPS
CloudTrail	cloudtrail.us-iso-east-1.c2s.ic.gov cloudtrail-fips.us-iso-east-1.c2s.ic.gov	HTTPS HTTPS
CloudWatch	monitoring.us-iso-east-1.c2s.ic.gov	HTTP and HTTPS
CloudWatch Events	events.us-iso-east-1.c2s.ic.gov	HTTPS
CloudWatch Logs	logs.us-iso-east-1.c2s.ic.gov	HTTPS
CloudWatch Logs Cross-Account Observability	cloudwatchlogs-crossaccountobservability.us-iso-east-1.c2s.ic.gov	
CloudWatch Synthetics	synthetics.us-iso-east-1.c2s.ic.gov	HTTPS
CodeDeploy	codedeploy.us-iso-east-1.c2s.ic.gov	HTTPS
Comprehend	comprehend.us-iso-east-1.c2s.ic.gov	HTTPS
DS Console	us-iso-east-1.console.c2shome.ic.gov/directoryservicev2/home?region=us-iso-east-1	HTTPS
Database Migration Service	dms.us-iso-east-1.c2s.ic.gov	HTTPS

AWS Service	US ISO East Endpoint	Protocol
Diode Console	us-iso-east-1.console.c2shome.ic.gov/diodev2/home?region=us-iso-east-1	
Direct Connect	directconnect.us-iso-east-1.c2s.ic.gov	HTTPS
Directory Service	ds.us-iso-east-1.c2s.ic.gov	HTTPS
	ds-fips.us-iso-east-1.c2s.ic.gov	HTTPS
Directory Service - AD Connector	ds.us-iso-east-1.c2s.ic.gov	HTTPS
Directory Service - Managed AD	ds.us-iso-east-1.c2s.ic.gov	HTTPS
DynamoDB	dynamodb.us-iso-east-1.c2s.ic.gov	HTTP and HTTPS
DynamoDB Streams	streams.dynamodb.us-iso-east-1.c2s.ic.gov	HTTP and HTTPS
EBS Console	us-iso-east-1.console.c2shome.ic.gov/ec2/home?region=us-iso-east-1	HTTPS
EBS Direct APIs	ebs.us-iso-east-1.c2s.ic.gov	HTTPS
EC2 Auto Scaling	autoscaling.us-iso-east-1.c2s.ic.gov	HTTP and HTTPS
EC2 Image Builder	imagebuilder.us-iso-east-1.c2s.ic.gov	HTTPS
EC2 Managed Prefix List Service	ec2.us-iso-east-1.c2s.ic.gov	HTTPS

AWS Service	US ISO East Endpoint	Protocol
EC2 Message Delivery Service	ec2messages.us-iso-east-1.c2s.ic.gov	HTTPS
EC2 Placement Groups Service	ec2-pgs.us-iso-east-1.c2s.ic.gov	
EC2CustomerMaintenanceEventService	ec2cms.us-iso-east-1.c2s.ic.gov	HTTP and HTTPS
EKS Console	us-iso-east-1.console.c2shome.ic.gov/eks/home?region=us-iso-east-1	
ElastiCache	elasticache.us-iso-east-1.c2s.ic.gov	HTTPS
Elastic Block Store (EBS)	ec2.us-iso-east-1.c2s.ic.gov	HTTPS
Elastic Compute Cloud (EC2)	ec2.us-iso-east-1.c2s.ic.gov	HTTP and HTTPS
Elastic File System (EFS)	elasticfilesystem.us-iso-east-1.c2s.ic.gov elasticfilesystem-fips.us-iso-east-1.c2s.ic.gov	HTTPS HTTPS
Elastic Load Balancing (ELB)	elasticloadbalancing.us-iso-east-1.c2s.ic.gov	HTTP and HTTPS
Elastic MapReduce (EMR)	elasticmapreduce.us-iso-east-1.c2s.ic.gov	HTTPS
EventBridge	events.us-iso-east-1.c2s.ic.gov	HTTPS
IAM Console	console.c2shome.ic.gov/iam/home?region=us-iso-east-1	

AWS Service	US ISO East Endpoint	Protocol
Identity & Access Management (IAM)	iam.us-iso-east-1.c2s.ic.gov	HTTPS
Import/Export Snowball	snowball.us-iso-east-1.c2s.ic.gov	
Key Management Service (KMS)	kms.us-iso-east-1.c2s.ic.gov kms-fips.us-iso-east-1.c2s.ic.gov	HTTPS HTTPS
Kinesis Data Firehose Console	kinesisfirehose-console.us-iso-east-1.c2s.ic.gov	
Kinesis Firehose	firehose.us-iso-east-1.c2s.ic.gov	HTTPS
Kinesis Streams	kinesis.us-iso-east-1.c2s.ic.gov	HTTPS
Kinesis Streams Console	us-iso-east-1.console.c2shome.ic.gov/kinesis/home?region=us-iso-east-1	HTTPS
Lambda	lambda.us-iso-east-1.c2s.ic.gov	HTTPS
Marketplace	marketplace.c2shome.ic.gov	HTTPS
Recycle Bin Console	us-iso-east-1.console.c2shome.ic.gov/rbin/home?region=us-iso-east-1	HTTPS
Redshift	redshift.us-iso-east-1.c2s.ic.gov	HTTPS
Relational Database Service (RDS) Core Control Plane	rds.us-iso-east-1.c2s.ic.gov	HTTPS

AWS Service	US ISO East Endpoint	Protocol
Resource Access Manager (RAM)	ram.us-iso-east-1.c2s.ic.gov	HTTPS
Resource Groups	resource-groups.us-iso-east-1.c2s.ic.gov	HTTPS
Route 53 Private DNS for VPCs	route53.c2s.ic.gov	HTTPS
Route 53 Public Control Plane	route53.c2s.ic.gov	HTTPS
Route 53 Public DNS	route53.c2s.ic.gov	HTTPS
Route 53 Resolver Endpoints	route53resolver.us-iso-east-1.c2s.ic.gov	HTTPS
Route53 Application Recovery Controller - Zonal Shift	arc-zonal-shift.us-iso-east-1.c2s.ic.gov	HTTPS
S3 Access Points	s3-accesspoint.us-iso-east-1.c2s.ic.gov s3-accesspoint-fips.dualstack.us-iso-east-1.c2s.ic.gov s3-accesspoint-fips.us-iso-east-1.c2s.ic.gov s3-accesspoint.dualstack.us-iso-east-1.c2s.ic.gov	HTTPS HTTPS HTTPS HTTPS
S3 Glacier service using Vaults ***For new use cases, use S3 storage classes***	glacier.us-iso-east-1.c2s.ic.gov	HTTP and HTTPS
SageMaker Console	us-iso-east-1.console.c2shome.ic.gov/sagemaker/home?region=us-iso-east-1	HTTPS

AWS Service	US ISO East Endpoint	Protocol
Security Token Service (STS)	sts.us-iso-east-1.c2s.ic.gov	HTTPS
Services Health Dashboard	status.c2shome.ic.gov	HTTPS
Sign-In Portal	signin.c2shome.ic.gov	HTTPS
Simple Notification Service (SNS)	sns.us-iso-east-1.c2s.ic.gov	HTTP and HTTPS
Simple Queue Service (SQS)	sqs.us-iso-east-1.c2s.ic.gov	HTTP and HTTPS
Simple Storage Service (S3)	s3.us-iso-east-1.c2s.ic.gov s3-fips.us-iso-east-1.c2s.ic.gov	HTTP and HTTPS HTTPS
Simple Workflow Service (SWF)	swf.us-iso-east-1.c2s.ic.gov	HTTPS
Site-to-Site VPN	ec2.us-iso-east-1.c2s.ic.gov	HTTPS
Support	support.us-iso-east-1.c2s.ic.gov	HTTPS
Transcribe	transcribe.us-iso-east-1.c2s.ic.gov	HTTPS
Transit Gateway	ec2.us-iso-east-1.c2s.ic.gov	HTTPS
Translate	translate.us-iso-east-1.c2s.ic.gov	HTTPS
Unified Settings Console	us-iso-east-1.console.c2shome.ic.gov/settings/home?region=us-iso-east-1	HTTPS

AWS Service	US ISO East Endpoint	Protocol
VPC Console	us-iso-east-1.console.c2shome.ic.gov/vpc/home?region=us-iso-east-1	HTTPS
VPC Flow Logs	ec2.us-iso-east-1.c2s.ic.gov	HTTPS
WorkSpaces	workspaces.us-iso-east-1.c2s.ic.gov	HTTPS

AWS Top Secret - West Endpoints

- The endpoint domain for AWS Top Secret Regions is `c2s.ic.gov`.
- The Region value should be `us-iso-west-1` for an endpoint in AWS Top Secret - West.
- FIPs endpoints are subject to availability, please refer to the services difference documentation.

AWS Service	US ISO WEST Endpoint	Protocol
API Gateway	apigateway.us-iso-west-1.c2s.ic.gov	HTTPS
API Gateway V2	apigateway.us-iso-west-1.c2s.ic.gov	HTTPS
AWS AppConfig	appconfig.us-iso-west-1.c2s.ic.gov appconfig-fips.us-iso-west-1.c2s.ic.gov	HTTPS HTTPS
AWS Config	config.us-iso-west-1.c2s.ic.gov	HTTPS
AWS Config Rules	config.us-iso-west-1.c2s.ic.gov	

AWS Service	US ISO WEST Endpoint	Protocol
AWS Console Home	us-iso-west-1.console.c2shome.ic.gov/console/home?region=us-iso-west-1	HTTPS
AWS DataSync	datasync.us-iso-west-1.c2s.ic.gov datasync-fips.us-iso-west-1.c2s.ic.gov	HTTPS HTTPS
AWS Diode Service	diode.us-iso-west-1.c2s.ic.gov	HTTPS
AWS Health Dashboard	phd.c2shome.ic.gov	HTTP and HTTPS
AWS License Manager	license-manager.us-iso-west-1.c2s.ic.gov	HTTPS
AWS Management Console	us-iso-west-1.console.c2shome.ic.gov	HTTPS
AWS Resource Groups Tagging API	tagging.us-iso-west-1.c2s.ic.gov	HTTPS
AWS S3 Control	s3-control.us-iso-west-1.c2s.ic.gov s3-control.dualstack.us-iso-west-1.c2s.ic.gov s3-control-fips.us-iso-west-1.c2s.ic.gov s3-control-fips.dualstack.us-iso-west-1.c2s.ic.gov	HTTPS HTTPS HTTPS HTTPS
AWS Secrets Manager	secretsmanager.us-iso-west-1.c2s.ic.gov	HTTPS

AWS Service	US ISO WEST Endpoint	Protocol
AWS Snowball Edge	snowball.us-iso-west-1.c2s.ic.gov	HTTPS
AWS Step Functions	states.us-iso-west-1.c2s.ic.gov	HTTPS
AWS Systems Manager (SSM)	ssm.us-iso-west-1.c2s.ic.gov	HTTPS
AWS Systems Manager Session Manager	ssmmessages.us-iso-west-1.c2s.ic.gov	HTTPS
AWS Zelkova Service	zelkova.us-iso-west-1.c2s.ic.gov	HTTPS
Amazon DCV	nice-dcv.us-iso-west-1.c2s.ic.gov	
Amazon Data Lifecycle Manager	dlm.us-iso-west-1.c2s.ic.gov	HTTPS
Amazon EKS	eks.us-iso-west-1.c2s.ic.gov	HTTPS
Amazon Elastic Container Registry	ecr.us-iso-west-1.c2s.ic.gov	HTTPS
	api.ecr.us-iso-west-1.c2s.ic.gov	HTTPS
Amazon Elastic Container Service	ecs.us-iso-west-1.c2s.ic.gov	HTTPS
Amazon OpenSearch Service	es.us-iso-west-1.c2s.ic.gov	HTTPS
Amazon RDS for MariaDB	rds.us-iso-west-1.c2s.ic.gov	HTTPS
Amazon RDS for MySQL	rds.us-iso-west-1.c2s.ic.gov	HTTPS
Amazon RDS for Oracle	rds.us-iso-west-1.c2s.ic.gov	HTTPS
Amazon RDS for PostgreSQL	rds.us-iso-west-1.c2s.ic.gov	HTTPS

AWS Service	US ISO WEST Endpoint	Protocol
Amazon RDS for SQL Server	rds.us-iso-west-1.c2s.ic.gov	HTTPS
Amazon Recycle Bin	rbin.us-iso-west-1.c2s.ic.gov rbin-fips.us-iso-west-1.c2s.ic.gov	HTTPS HTTPS
Amazon S3 Replication Time Control	rtc.us-iso-west-1.c2s.ic.gov	
AppConfigData	appconfigdata.us-iso-west-1.c2s.ic.gov	HTTPS
Application Auto Scaling	application-autoscaling.us-iso-west-1.c2s.ic.gov	HTTP and HTTPS
Aurora MySQL	rds.us-iso-west-1.c2s.ic.gov	HTTPS
Aurora PostgreSQL	rds.us-iso-west-1.c2s.ic.gov	HTTPS
Cloud Control API	cloudcontrolapi.us-iso-west-1.c2s.ic.gov	HTTPS
CloudFormation	cloudformation.us-iso-west-1.c2s.ic.gov	HTTPS
CloudTrail	cloudtrail.us-iso-west-1.c2s.ic.gov cloudtrail-fips.us-iso-west-1.c2s.ic.gov	HTTPS HTTPS
CloudWatch	monitoring.us-iso-west-1.c2s.ic.gov	HTTP and HTTPS
CloudWatch Events	events.us-iso-west-1.c2s.ic.gov	HTTPS

AWS Service	US ISO WEST Endpoint	Protocol
CloudWatch Logs	logs.us-iso-west-1.c2s.ic.gov	HTTPS
CloudWatch Synthetics	synthetics.us-iso-west-1.c2s.ic.gov	HTTPS
CodeDeploy	codedeploy.us-iso-west-1.c2s.ic.gov	HTTPS
DS Console	us-iso-west-1.console.c2shome.ic.gov/directoryservicev2/home?region=us-iso-west-1	HTTPS
Database Migration Service	dms.us-iso-west-1.c2s.ic.gov	HTTPS
Direct Connect	directconnect.us-iso-west-1.c2s.ic.gov	HTTPS
Directory Service	ds.us-iso-west-1.c2s.ic.gov ds-fips.us-iso-west-1.c2s.ic.gov	HTTPS HTTPS
Directory Service - AD Connector	ds.us-iso-west-1.c2s.ic.gov	HTTPS
Directory Service - Managed AD	ds.us-iso-west-1.c2s.ic.gov	HTTPS
DynamoDB	dynamodb.us-iso-west-1.c2s.ic.gov	HTTP and HTTPS
DynamoDB Streams	streams.dynamodb.us-iso-west-1.c2s.ic.gov	HTTP and HTTPS
EBS Console	us-iso-west-1.console.c2shome.ic.gov/ec2/home?region=us-iso-west-1	HTTPS

AWS Service	US ISO WEST Endpoint	Protocol
EBS Direct APIs	ebs.us-iso-west-1.c2s.ic.gov	HTTPS
EC2 Auto Scaling	autoscaling.us-iso-west-1.c2s.ic.gov	HTTP and HTTPS
EC2 Image Builder	imagebuilder.us-iso-west-1.c2s.ic.gov	HTTPS
EC2 Managed Prefix List Service	ec2.us-iso-west-1.c2s.ic.gov	HTTPS
EC2 Message Delivery Service	ec2messages.us-iso-west-1.c2s.ic.gov	HTTPS
EC2 Placement Groups Service	ec2-pgs.us-iso-west-1.c2s.ic.gov	
EC2CustomerMaintenanceEventService	ec2cms.us-iso-west-1.c2s.ic.gov	HTTP and HTTPS
EKS Console	us-iso-west-1.console.c2shome.ic.gov/eks/home?region=us-iso-west-1	
ElastiCache	elasticache.us-iso-west-1.c2s.ic.gov	HTTPS
Elastic Block Store (EBS)	ec2.us-iso-west-1.c2s.ic.gov	HTTPS
Elastic Compute Cloud (EC2)	ec2.us-iso-west-1.c2s.ic.gov	HTTP and HTTPS
Elastic File System (EFS)	elasticfilesystem.us-iso-west-1.c2s.ic.gov elasticfilesystem-fips.us-iso-west-1.c2s.ic.gov	HTTPS HTTPS

AWS Service	US ISO WEST Endpoint	Protocol
Elastic Load Balancing (ELB)	elasticloadbalancing.us-iso-west-1.c2s.ic.gov	HTTPS
Elastic MapReduce (EMR)	elasticmapreduce.us-iso-west-1.c2s.ic.gov	HTTPS
EventBridge	events.us-iso-west-1.c2s.ic.gov	HTTPS
IPv6	ipv6.us-iso-west-1.c2s.ic.gov	
Identity & Access Management (IAM)	iam.us-iso-east-1.c2s.ic.gov	HTTPS
Import/Export Snowball	snowball.us-iso-west-1.c2s.ic.gov	
Key Management Service (KMS)	kms.us-iso-west-1.c2s.ic.gov kms-fips.us-iso-west-1.c2s.ic.gov	HTTPS HTTPS
Kinesis Data Firehose Console	kinesisfirehose-console.us-iso-west-1.c2s.ic.gov	
Kinesis Firehose	firehose.us-iso-west-1.c2s.ic.gov	HTTPS
Kinesis Streams	kinesis.us-iso-west-1.c2s.ic.gov	HTTPS
Kinesis Streams Console	us-iso-west-1.console.c2shome.ic.gov/kinesis/home?region=us-iso-west-1	HTTPS
Lambda	lambda.us-iso-west-1.c2s.ic.gov	HTTPS

AWS Service	US ISO WEST Endpoint	Protocol
Recycle Bin Console	us-iso-west-1.console.c2shome.ic.gov/rbin/home?region=us-iso-west-1	HTTPS
Redshift	redshift.us-iso-west-1.c2s.ic.gov	HTTPS
Relational Database Service (RDS) Core Control Plane	rds.us-iso-west-1.c2s.ic.gov	HTTPS
Resource Access Manager (RAM)	ram.us-iso-west-1.c2s.ic.gov	HTTPS
Resource Groups	resource-groups.us-iso-west-1.c2s.ic.gov	HTTPS
Route 53 Private DNS for VPCs	route53.c2s.ic.gov	HTTPS
Route 53 Public Control Plane	route53.c2s.ic.gov	HTTPS
Route 53 Public DNS	route53.c2s.ic.gov	HTTPS
Route 53 Resolver Endpoints	route53resolver.us-iso-west-1.c2s.ic.gov	HTTPS
Route53 Application Recovery Controller - Zonal Shift	arc-zonal-shift.us-iso-west-1.c2s.ic.gov	HTTPS

AWS Service	US ISO WEST Endpoint	Protocol
S3 Access Points	s3-accesspoint.us-iso-west-1.c2s.ic.gov s3-accesspoint-fips.dualstack.us-iso-west-1.c2s.ic.gov s3-accesspoint-fips.us-iso-west-1.c2s.ic.gov s3-accesspoint.dualstack.us-iso-west-1.c2s.ic.gov	HTTPS HTTPS HTTPS HTTPS
S3 Glacier service using Vaults ***For new use cases, use S3 storage classes***	glacier.us-iso-west-1.c2s.ic.gov	HTTP and HTTPS
Security Token Service (STS)	sts.us-iso-west-1.c2s.ic.gov	HTTPS
Services Health Dashboard	status.c2shome.ic.gov	HTTPS
Sign-In Portal	us-iso-west-1.signin.c2shome.ic.gov	HTTPS
Simple Notification Service (SNS)	sns.us-iso-west-1.c2s.ic.gov	HTTP and HTTPS
Simple Queue Service (SQS)	sqs.us-iso-west-1.c2s.ic.gov	HTTP and HTTPS
Simple Storage Service (S3)	s3.us-iso-west-1.c2s.ic.gov s3-fips.us-iso-west-1.c2s.ic.gov	HTTP and HTTPS HTTPS
Simple Workflow Service (SWF)	swf.us-iso-west-1.c2s.ic.gov	HTTPS
Site-to-Site VPN	ec2.us-iso-west-1.c2s.ic.gov	HTTPS

AWS Service	US ISO WEST Endpoint	Protocol
Support	support.us-iso-east-1.c2s.ic.gov	HTTPS
Transit Gateway	ec2.us-iso-west-1.c2s.ic.gov	HTTPS
Unified Settings Console	us-iso-west-1.console.c2shome.ic.gov/settings/home?region=us-iso-west-1	HTTPS
VPC Console	us-iso-west-1.console.c2shome.ic.gov/vpc/home?region=us-iso-west-1	HTTPS
VPC Flow Logs	ec2.us-iso-west-1.c2s.ic.gov	HTTPS
WorkSpaces	workspaces.us-iso-west-1.c2s.ic.gov	HTTPS

Amazon Resource Names in AWS Top Secret Regions

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

```
arn:aws:
```

In AWS Top Secret Regions, ARNs begin with:

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

If an ARN that you are using requires you to specify a region, use:

- AWS Top Secret - East - `us-iso-east-1`
- AWS Top Secret - West - `us-iso-west-1`

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

Services in AWS Top Secret Regions

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

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

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

Topics

- AWS Account Management
- Amazon API Gateway
- AWS AppConfig
- Application Auto Scaling
- Amazon Athena
- Amazon Aurora
- AWS Billing and Cost Management
- AWS Cloud Control API
- AWS CloudFormation
- AWS CloudTrail
- Amazon CloudWatch
- Amazon CloudWatch Logs
- AWS CodeDeploy
- Amazon Comprehend
- AWS Config
- AWS Database Migration Service

- AWS DataSync
- Amazon DCV
- AWS Direct Connect
- AWS Directory Service
- Amazon DynamoDB
- Amazon Elastic Block Store
- EBS direct APIs
- Amazon Elastic Compute Cloud
- Amazon EC2 Auto Scaling
- Amazon EC2 Image Builder
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- Amazon EFS
- Amazon EKS
- Elastic Load Balancing
- Amazon EMR
- Amazon ElastiCache
- AWS Elemental MediaPackage
- AWS Elemental MediaLive
- Amazon EventBridge
- Amazon FSx
- Amazon S3 Glacier
- AWS Glue
- Amazon GuardDuty
- AWS Health
- AWS Identity and Access Management
- AWS Key Management Service
- Amazon Kinesis Data Streams
- Amazon Data Firehose
- AWS Lambda

- AWS License Manager
- AWS Marketplace
- AWS Modular Data Center Rack
- Amazon Neptune
- Amazon OpenSearch Service
- AWS Outposts
- AWS ParallelCluster
- AWS Pricing Calculator
- Amazon Redshift
- Amazon Relational Database Service
- AWS Resource Groups
- AWS Resource Access Manager
- AWS Resource Groups Tagging API
- Amazon Route 53
- Amazon Application Recovery Controller (ARC)
- Amazon SageMaker
- AWS Serverless Application Model
- AWS Secrets Manager
- AWS Security Hub
- Amazon Simple Storage Service
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Simple Workflow Service
- AWS Snowball Edge
- AWS Step Functions
- AWS Storage Gateway
- AWS Support
- AWS Systems Manager
- Amazon Textract
- Amazon Transcribe

- AWS Transit Gateway
- Amazon Translate
- AWS Trusted Advisor
- Amazon Virtual Private Cloud
- AWS Virtual Private Network
- Amazon WorkSpaces

AWS Account Management

An AWS account is the basic container for all the AWS resources you create as an AWS customer. For example, an Amazon Simple Storage Service (Amazon S3) bucket, an Amazon Relational Database Service (Amazon RDS) database, and an Amazon Elastic Compute Cloud (Amazon EC2) instance are all resources. Every resource is uniquely identified by an Amazon Resource Name (ARN) that includes the account ID of the account that contains, or owns, the resource. An AWS account is also the basic security boundary for your AWS resources. Resources that you create in your account are available to users who have credentials for your account.

Topics

- Region Availability
- How Account Management Differs for AWS Top Secret Regions
- Documentation for Account Management

Region Availability

AWS Account Management is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Account Management Differs for AWS Top Secret Regions

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

- The process to sign up for a new AWS account is different than in commercial regions. For more information, see Signing Up.
- AWS Organizations is currently not available in AWS Top Secret Regions.
- There is no concept of a "root" or "account" user or credentials. All AWS Top Secret Regions users are IAM users, including the user who created the account.
- Accounts and credentials for the India regions will not work in the AWS Top Secret Regions.
- AWS Account Management APIs are not available.
- AWS Top Secret Regions does not support adding opt in regions.

- AWS Top Secret Regions does not support adding multi-factor authentication (MFA) to IAM users or to the account. This includes both hardware and virtual MFA devices. The console does not include MFA options.
- Amazon Resource Names (ARNs) and endpoints have different values.

Documentation for Account Management

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

- AWS Account Management Reference Guide
- Managing your AWS account

Amazon API Gateway

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

Topics

- Region Availability
- How API Gateway Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for API Gateway

Region Availability

Amazon API Gateway is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How API Gateway Differs for AWS Top Secret Regions

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

- AWS Certificate Manager (ACM) is not available. When creating a custom domain name for an API, you must upload the required certificate to API Gateway instead of ACM. For more information, see Set Up a Regional Custom Domain Name Certificate Without ACM Using AWS CLI.
- AWS WAF is not available for API Gateway APIs.
- X-Ray tracing is not available.
- Amazon Cognito authorizers are not available.
- Java and Ruby SDK generation is not available.
- Edge-optimized APIs and Integration with AWS Config are not available.
- API Gateway cannot communicate with integration endpoints outside of AWS Top Secret - East and AWS Top Secret - West.
- API Gateway resources cannot be tagged using AWS CloudFormation.
- CloudTrail events for ApiGatewayV2 resources (such as operations on WebSocket APIs) are only available in the S3 bucket. They will not show up in the CloudTrail console or CLI.
- Stage variables are not encrypted.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.
- HTTP APIs are not available.
- Mutual TLS authentication is not available.
- Multi-level base path mapping is not yet available in AWS Top Secret Regions.
- WebSocket APIs are available, but custom domain names for WebSocket APIs aren't available in AWS Top Secret - East and AWS Top Secret - West.
- To create a REST API using AWS CloudFormation, you must use a Regional endpoint. Set either `Properties.EndpointConfiguration.Types` to `["REGIONAL"]` or `Properties.Parameters.endpointConfigurationTypes` to `"REGIONAL"`.
- Private API automatic creation of DNS records is not available.
- The VPC endpoints `execute-api.us-iso-east-1.c2s.ic.gov` and `apigateway.us-iso-east-1.c2s.ic.gov` are not available in the AWS Top Secret - East Region.

- The following region-specific API Gateway account IDs are automatically added to your Amazon VPC endpoint service as AllowedPrincipals for private integrations in AWS Top Secret Regions:

Region	Account ID
• us-iso-east-1 • us-iso-west-1	• 078191414070 • 287306548648

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to API Gateway by using the command line or APIs, use the appropriate endpoint.

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

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

Documentation for API Gateway

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

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

AWS AppConfig

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

Topics

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

Region Availability

AWS AppConfig is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How AWS AppConfig Differs for AWS Top Secret Regions

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

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

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to AWS AppConfig by using the command line or APIs, use the appropriate endpoint.

Documentation for AWS AppConfig

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

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

Application Auto Scaling

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

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

Topics

- Region Availability
- How Application Auto Scaling Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Application Auto Scaling

Region Availability

Application Auto Scaling is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Application Auto Scaling Differs for AWS Top Secret Regions

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

- Only the following resources are supported for Application Auto Scaling in the AWS Top Secret - East Region:
  - Aurora replicas
  - Amazon DynamoDB tables and global secondary indexes

  - Amazon ECS services
  - Amazon EMR clusters
  - SageMaker endpoint variants
- Only the following resources are supported for Application Auto Scaling in the AWS Top Secret - West Region:
  - Amazon DynamoDB tables and global secondary indexes
  - Amazon ECS services
  - Amazon EMR clusters
- Application Auto Scaling is not supported for AWS PrivateLink in the AWS Top Secret - West Region.
- Application Auto Scaling notifications are not currently supported in the AWS Personal Health Dashboard.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.
- Predictive scaling is not supported in AWS Top Secret Regions.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

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

- https://autoscaling.us-iso-east-1.c2s.ic.gov
- https://application-autoscaling.us-iso-east-1.c2s.ic.gov

Documentation for Application Auto Scaling

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

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

Amazon Athena

Amazon Athena is an interactive query service that lets you use standard SQL to analyze data directly in Amazon S3. You can point Athena at your data in Amazon S3 and run ad-hoc queries and get results in seconds. Athena is serverless, so there is no infrastructure to set up or manage. Athena scales automatically—executing queries in parallel—so results are fast, even with large datasets and complex queries.

Topics

- How Athena Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Athena

How Athena Differs for AWS Top Secret Regions

The implementation of Athena is different for AWS Top Secret Regions in the following ways:

- The query results reuse feature is not supported.
- AWS Lake Formation fine-grained access control is not supported.
- Querying data that is registered with AWS Lake Formation is not supported.
- Amazon Athena for Apache Spark and Spark notebooks are not supported.
- IPv6 dual stack support is not available.
- Self-service quota increases are not available. To request a service limit increase, a ticket must be filed.
- Only the latest version of Athena engine version 3 is supported. Earlier versions are not supported.
- Because the AWS Serverless Application Repository is not available, federated connectors must be configured manually in AWS Lambda. For connector templates, see `s3://athena-query-federation-us-iso-east-1/aws-athena-query-federation-master/`.

  For more information about federated connectors, see the following resources:

  - Amazon Athena Query Federation
  - Deploy DynamoDB Connector without AWS Serverless Application Repository or AWS CloudFormation Permissions

- Deploy the Athena PostgreSQL Connector without using AWS SAM
- The following data source connectors for Amazon Athena are not supported:
  - Azure Data Lake Storage (ADLS) Gen2
  - Azure Synapse
  - Amazon DocumentDB
  - Google BigQuery
  - Google Cloud Storage
  - MSK
  - Neptune
  - Snowflake
  - Timestream
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

JDBC driver download links

Use the links in this section to download JDBC drivers for Athena.

JDBC 3.x driver download

To download the Amazon Athena 3.x JDBC driver, visit the following links.

JDBC 3.x driver uber jar

The following download packages the driver and all its dependencies in the same `.jar` file. This download is commonly used for third-party SQL clients.

3.3.0 uber jar

JDBC 3.x driver lean jar

The following download is a `.zip` file that contains the lean `.jar` for the driver and separate `.jar` files for the driver's dependencies. This download is commonly used for custom applications that might have dependencies that conflict with the dependencies that the driver uses. This download is useful if you want to choose which of the driver dependencies to include with the lean jar, and which to exclude if your custom application already contains one or more of them.

3.3.0 lean jar

JDBC 3.x License

The following link contains the license agreement for the JDBC 3.x driver.

License

Previous versions of the Athena JDBC 3.x driver

We highly recommended that you use the latest version of the JDBC 3.x driver. The latest version of the driver contains the most recent improvements and fixes. Use an older version only if your application experiences incompatibilities with the latest version.

JDBC driver uber jar

The following download packages the driver and all its dependencies in the same `.jar` file. This download is commonly used for third-party SQL clients.

- 3.2.2 uber jar
- 3.2.1 uber jar
- 3.2.0 uber jar
- 3.1.0 uber jar
- 3.0.0 uber jar

JDBC driver lean jar

The following download is a `.zip` file that contains the lean `.jar` for the driver and separate `.jar` files for the driver's dependencies. This download is commonly used for custom applications that might have dependencies that conflict with the dependencies that the driver uses. This download is useful if you want to choose which of the driver dependencies to include with the lean jar, and which to exclude if your custom application already contains one or more of them.

- 3.2.2 lean jar
- 3.2.1 lean jar
- 3.2.0 lean jar
- 3.1.0 lean jar
- 3.0.0 lean jar

JDBC 2.x driver and documentation download links

Use the following links to download the JDBC 2.x drivers and documentation for Athena.

JDBC 2.x driver with AWS SDK

The JDBC driver version 2.1.5 complies with the JDBC API 4.2 data standard and requires JDK 8.0 or later.

Use the following link to download the JDBC 4.2 driver `.jar` file.

- AthenaJDBC42-2.1.5.1000.jar

The following `.zip` file download contains the `.jar` file for JDBC 4.2 and includes the AWS SDK and the accompanying documentation, release notes, licenses, and agreements.

- SimbaAthenaJDBC-2.1.5.1000.zip

JDBC 2.x driver without AWS SDK

The JDBC driver version 2.1.5 complies with the JDBC API 4.2 data standard and requires JDK 8.0 or later.

Use the following link to download the JDBC 4.2 driver `.jar` file without the AWS SDK.

- AthenaJDBC42-2.1.5.1001.jar

The following `.zip` file download contains the `.jar` file for JDBC 4.2 and the accompanying documentation, release notes, licenses, and agreements. It does not include the AWS SDK.

- SimbaAthenaJDBC-2.1.5.1001.zip

ODBC driver download links

Use the links in this section to download ODBC drivers for Athena.

ODBC 2.x driver download

To download the Amazon Athena 2.x ODBC driver, visit the links in this section.

Linux

Driver version	Download link
ODBC 2.0.3.0 for Linux 64-bit	Linux 64 bit ODBC driver 2.0.3.0

macOS (ARM)

Driver version	Download link
ODBC 2.0.3.0 for macOS 64-bit (ARM)	macOS 64 bit ODBC driver 2.0.3.0 (ARM)

macOS (Intel)

Driver version	Download link
ODBC 2.0.3.0 for macOS 64-bit (Intel)	macOS 64 bit ODBC driver 2.0.3.0 (Intel)

Windows

Driver version	Download link
ODBC 2.0.3.0 for Windows 64-bit	Windows 64 bit ODBC driver 2.0.3.0

ODBC 1.x driver and documentation download links

Use the following links to download the ODBC 1.x drivers and documentation for Athena.

Windows

Driver version	Download link
ODBC 1.2.3.1000 for Windows 32-bit	Windows 32 bit ODBC driver 1.2.3.1000
ODBC 1.2.3.1000 for Windows 64-bit	Windows 64 bit ODBC driver 1.2.3.1000

Linux

Driver version	Download link
ODBC 1.2.3.1000 for Linux 32-bit	Linux 32 bit ODBC driver 1.2.3.1000
ODBC 1.2.3.1000 for Linux 64-bit	Linux 64 bit ODBC driver 1.2.3.1000

OSX

Driver version	Download link
ODBC 1.2.3.1000 for OSX	OSX ODBC driver 1.2.3.1000

Documentation

Content	Download link
Documentation for ODBC 1.2.3.1000	ODBC driver installation and configuration guide version 1.2.3.1000
Release Notes for ODBC 1.2.3.1000	ODBC driver release notes version 1.2.3.1000

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Athena by using the command line or APIs, use the appropriate endpoint.

Documentation for Athena

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

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

Amazon Aurora

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

Topics

- Region Availability
- How Aurora Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Aurora

Region Availability

Amazon Aurora is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Aurora Differs for AWS Top Secret Regions

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

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

Features Not Available for Aurora MySQL

- Aurora DB cluster storage configurations
- Blue/Green Deployments
- AWS Secrets Manager integration

- RDS Proxy
- Performance Insights
- Aurora Serverless clusters
- Backtrack
- Database Activity Streams
- Recommendations
- Parallel query clusters
- Calling Lambda functions
- Aurora machine learning integration
- Aurora custom endpoints
- Copy-on-write protocol for Aurora cloning
- GTID-based replication
- Amazon RDS Extended Support

Features Not Available for Aurora PostgreSQL

- Aurora DB cluster storage configurations
- Blue/Green Deployments
- AWS Secrets Manager integration
- RDS Proxy
- Performance Insights
- Aurora Serverless clusters
- Database Activity Streams
- Recommendations
- Cross-account cluster cloning
- Cluster cache management
- Aurora machine learning integration
- Aurora custom endpoints
- Copy-on-write protocol for Aurora cloning
- Kerberos authentication
- Amazon RDS Extended Support

General Differences

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

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

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

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

- To connect to a Aurora MySQL or Aurora PostgreSQL DB instance with SSL, you must download the public key from https://s3.us-iso-east-1.c2s.ic.gov/rds-downloads/rds-combined-ca-bundle.pem. For more information, see Using SSL/TLS to Encrypt a Connection to a DB Cluster.
- Since AWS Top Secret Regions uses a unique certificate authority (CA), update your DB instances for AWS Top Secret Regions to use the Region-specific certificate identified by `rds-ca-2021` in DescribeCertificates calls as soon as possible. The remaining instructions described in the SSL Certificate Rotation topic are the same, except for the certificate identifier.
- The list of available DB instance classes is at Amazon Aurora Pricing.
- AWS Top Secret Regions uses the following time block from which the default backup windows are assigned.

Region	Time Block
us-iso-east-1	03:00–11:00 UTC

- The AWS service principal for Aurora is `rds.c2s.ic.gov`.
- Amazon EC2 launches instances into a VPC instead of using the EC2-Classic platform. For more information, see Amazon EC2 and Amazon Virtual Private Cloud (VPC).
- Since AWS Top Secret Regions is a VPC-only region, Aurora DB instances must use existing VPC security groups. Aurora APIs, such as CreateDBSecurityGroup and AWS::RDS::DBSecurityGroup do not apply in AWS Top Secret Regions. Instead, create VPC security groups directly in Amazon EC2 using CreateSecurityGroup.
- Amazon Resource Names (ARNs) and endpoints have different values.

- Only Signature Version 4 signing is supported.
- Size-flexible reserved DB instances aren't supported.
- An Aurora cluster that is a read replica can't be promoted to read-write capability using the RDS console. To promote such a cluster, use the AWS CLI or RDS API.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Aurora by using the command line or APIs, use the appropriate endpoint.

Documentation for Aurora

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

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

AWS Billing and Cost Management

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

Topics

- Region Availability
- How Billing and Cost Management Differs for AWS Top Secret Regions
- Documentation for Billing and Cost Management

Region Availability

AWS Billing and Cost Management is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Billing and Cost Management Differs for AWS Top Secret Regions

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

- When you create your account, you specify your agency's standard invoicing system to pay for services.
- Each month, AWS sends an invoice in accordance with your agency's invoicing instructions. These instructions are delineated in a task order that is issued by the authorized contract representative. For more information, see Get Your Monthly Bill and View Your AWS Charges.
- If you want to deposit reports into an Amazon S3 bucket, in your policy, you must specify `120873416848` (instead of `386209384616`) for the account ID . For more information, see Example 8: Deposit Reports into an Amazon S3 Bucket.
- RI discounts sharing is enabled for all accounts in AWS Top Secret Regions and cannot be disabled.
- The AWS Cost and Usage Reports feature is not available in AWS Top Secret Regions.

- Savings Plans are not supported in AWS Top Secret Regions.
- The AWS Cost Explorer API is not available in AWS Top Secret Regions.
- When opting in to Cost Explorer, only the current month's data is available.
- Access to AWS Cost Explorer in the console is provided by the `aws-portal:ViewBilling` permission. Granular permissions provided by `ce:*` actions are not supported in AWS Top Secret Regions.
- AWS Marketplace purchases aren't displayed on Billing and Cost Management features.
- Multi-year data, resource-level, and hourly granularity features in Cost Explorer are not available in AWS Top Secret Regions.
- Cost Explorer returns full month data when you choose `monthly granularity` in AWS Top Secret Regions. To receive partial month data, use `daily granularity`.

Documentation for Billing and Cost Management

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

- AWS Billing User Guide

AWS Cloud Control API

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

Topics

- Region Availability
- How Cloud Control API Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Cloud Control API

Region Availability

AWS Cloud Control API is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Cloud Control API Differs for AWS Top Secret Regions

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

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

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

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

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

Documentation for Cloud Control API

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

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

AWS CloudFormation

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

Topics

- Region Availability
- How AWS CloudFormation Differs for AWS Top Secret Regions
- How the AWS CloudFormation Helper Scripts Differ for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for AWS CloudFormation

Region Availability

AWS CloudFormation is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How AWS CloudFormation Differs for AWS Top Secret Regions

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

- AWS CloudFormation in AWS Top Secret Regions does not support AWS CloudFormation IaC generator (infrastructure as code generator).
- The AWS CloudFormation service principal in AWS Top Secret Regions is `cloudformation.amazonaws.com`.
- AWS Top Secret Regions supports a subset of AWS services. You might need to modify AWS CloudFormation sample templates and template snippets.
- AWS CloudFormation in AWS Top Secret Regions does not support AWS Config.

- AWS CloudFormation in AWS Top Secret Regions does not support managing AWS CloudFormation events using Amazon EventBridge.
- AWS CloudFormation StackSets are not available in AWS Top Secret Regions.
- Macros are not available in AWS Top Secret Regions.
- AWS CloudFormation cannot tag API Gateway resources.
- AWS CloudFormation does not support the limit for resources in concurrent stack operations.
- AWS CloudFormation does not support the limit of concurrent stack instance operations, by region, for StackSets.
- AWS CloudFormation may not support all resources in AWS Top Secret Regions.

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

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

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

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

- Amazon Resource Names (ARNs) and endpoints have different values. The value for a Principle: Service: key in a AWS CloudFormation Template is also different.

  In AWS Top Secret Regions it would look like this:

```
"Statement": [
        {
          "Effect": "Allow",
          "Principal": {
          "Service": [ "ec2.c2s.ic.gov " ]
          },
          "Action": [ "sts:AssumeRole" ]
        }
        ]
```

- The force delete stack option is not available in AWS Top Secret Regions.
- `ServiceTimeout`, an optional property for custom resource requests, is not supported in AWS Top Secret Regions.
- The following AWS CloudFormation Hook features are not yet available:
  - Guard Hooks that check if your resources follow rules that are created using AWS CloudFormation Guard.
  - Lambda Hooks that forwards requests for resource evaluation to an AWS Lambda function.
  - Hook support for resource evaluation during create, update, or delete operations for resources managed by the Cloud Control API.
  - Hook support for template evaluation during create, update, or delete stack operations.
  - Hook support for change set evaluation.
- Amazon EC2 launches instances and Amazon RDS DB instances into a VPC instead of using the EC2-Classic platform. For more information, see Amazon EC2 and Amazon Virtual Private Cloud (VPC).
- Only Signature Version 4 signing is supported.

How the AWS CloudFormation Helper Scripts Differ for AWS Top Secret Regions

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

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

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

The `yum install` command installs the package if it isn't already installed. If the package is installed, `yum install` will update it to the latest version.

- You should periodically update the `aws-cfn-bootstrap-config-us-iso-east-1` package.
- If you use the helper scripts source code to work on another version of Linux, you'll have to create the helper scripts trust store bundle manually or install the `aws-cfn-bootstrap-config-us-iso-east-1` package.
- The cfn-init and cfn-signal helper scripts require credentials in order to use them. Associate an IAM role with the Amazon EC2 instance that you are configuring and use the role's credentials to call `cfn-init` or `cfn-signal`. For `cfn-init`, the role requires permission to the cloudformation:DescribeStackResource action. For `cfn-signal`, the role requires permission to the cloudformation:SignalResource action.

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

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

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

```
"#!/bin/bash\n",
"/opt/aws/bin/cfn-init -v",
" --region ", {"Ref": "AWS::Region"},
" --role='role_goes_here'",
" --url='https://cloudformation.us-iso-east-1.c2s.ic.gov'",
" --stack ", {"Ref": "AWS::StackName"},
" --resource CfnInitInstance \n",
" # Signal the status from cfn-init\n",
"/opt/aws/bin/cfn-signal -e $? ",
" --region ", {"Ref": "AWS::Region"},
" --role='role_goes_here'",
" --url='https://cloudformation.us-iso-east-1.c2s.ic.gov'",
" --stack ", {"Ref": "AWS::StackName"},
" --resource CfnInitInstance ", "\n"]]}}
```

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

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

```
"/etc/cfn/cfn-hup.conf" : {
  "content" : { "Fn::Join" : ["", [
  "[main]\n",
    "stack=", { "Ref" : "AWS::StackId" }, "\n",
    "region=", { "Ref" : "AWS::Region" }, "\n",
    "url=https://cloudformation.us-iso-east-1.c2s.ic.gov\n",
    "role=", { "Ref" : "InstanceRole" }, "\n"
  ]]},
  "mode"    : "000400",
  "owner"   : "root",
  "group"   : "root"
},
"/etc/cfn/hooks.d/cfn-auto-reloader.conf" : {
  "content": { "Fn::Join" : ["", [
    "[cfn-auto-reloader-hook]\n",
    "triggers=post.update\n",
    "path=Resources.ContainerInstances.Metadata.AWS::CloudFormation::Init\n",
    "action=/opt/aws/bin/cfn-init -v ",
    "  --stack ", { "Ref" : "AWS::StackName" },
    "  --resource LaunchConfig ",
    "  --role ", { "Ref" : "InstanceRole" },
    "  --url https://cloudformation.us-iso-east-1.c2s.ic.gov",
    "  --region ", { "Ref" : "AWS::Region" }, "\n",
    "runas=root\n"
  ]]}
}
```

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to AWS CloudFormation by using the command line or APIs, use the appropriate endpoint.

Documentation for AWS CloudFormation

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

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

AWS CloudTrail

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

Topics

- Region Availability
- How CloudTrail Differs for AWS Top Secret Regions
- Services Supported within CloudTrail
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for CloudTrail

Region Availability

AWS CloudTrail is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How CloudTrail Differs for AWS Top Secret Regions

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

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

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

> **Note**
>
> If the policy specifies the individual CloudTrail account ID for the AWS Top Secret Regions region (`"Principal": { "AWS": ["arn:aws-iso:iam::343267119537:root"]}`), you can continue to use this permission type.

However, as a best practice, update the policy to use the CloudTrail service principal name.

- AWS Organizations trails are not available.
- CloudTrail Lake is not available.
- CloudTrail network activity events (in preview) is not available.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

Services Supported within CloudTrail

CloudTrail supports logging for the services supported in the AWS Top Secret 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*.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to CloudTrail by using the command line or APIs, use the appropriate endpoint.

Documentation for CloudTrail

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

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

Amazon CloudWatch

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

Topics

- Region Availability
- How CloudWatch Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for CloudWatch

Region Availability

Amazon CloudWatch is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How CloudWatch Differs for AWS Top Secret Regions

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

- Transaction Search is not available.
- In the AWS Top Secret - West Region, the CloudWatch agent is not available. In AWS Top Secret - East Region, the CloudWatch agent is available.
- CloudWatch Synthetics is available with the following differences:

  In the AWS Top Secret - West Region, CloudWatch Synthetics does not support X-Ray tracing or AWS PrivateLink

  In the AWS Top Secret - East Region, CloudWatch Synthetics does not support the following features:

  - X-Ray tracing
  - AWS PrivateLink

  - scheduling with cron
  - The `Names` filter parameter for the **DescribeCanaries** and **DescribeCanariesLastRun** operations.
- The AWS PrivateLink endpoint for CloudWatch in the AWS Top Secret - East Region is `com.amazonaws.us-iso-east-1.monitoring`. The AWS PrivateLink endpoint in the AWS Top Secret - West Region is `gov.ic.c2s.us-iso-west-1.monitoring`.
- Dashboard sharing is not available.
- Horizontal and vertical annotations are not available on graphs.
- Designating CloudWatch dashboards as favorite dashboards is not available.
- Console functionality (delete/edit model) for anomaly detection is not available.
- In the AWS Top Secret - West Region, CloudWatch Synthetics is not available.

  In AWS Top Secret - East Region, CloudWatch Synthetics is available, but does not support the following features:

  - X-Ray tracing
  - AWS PrivateLink
  - scheduling with cron
  - The `Names` filter parameter for the **DescribeCanaries** and **DescribeCanariesLastRun** operations.
- Logging GetMetricData and GetMetricWidgetImage data events to CloudTrail is not supported.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to CloudWatch by using the command line or APIs, use the appropriate endpoint.

Documentation for CloudWatch

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

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

Amazon CloudWatch Logs

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

Topics

- Region Availability
- How CloudWatch Logs Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for CloudWatch Logs

Region Availability

Amazon CloudWatch Logs is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How CloudWatch Logs Differs for AWS Top Secret Regions

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

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

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to CloudWatch Logs by using the command line or APIs, use the appropriate endpoint.

Documentation for CloudWatch Logs

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

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

AWS CodeDeploy

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

Topics

- Region Availability
- How CodeDeploy Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for CodeDeploy

Region Availability

AWS CodeDeploy is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How CodeDeploy Differs for AWS Top Secret Regions

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

- The CodeDeploy Resource Kit Bucket Name in AWS Top Secret - East is: `aws-codedeploy-us-iso-east-1`.
- The CodeDeploy Resource Kit Bucket Name in AWS Top Secret - West is: `aws-codedeploy-us-iso-west-1`.
- The AWS service principal for CodeDeploy is `codedeploy.amazonaws.com`, but the former service principal of `codedeploy.c2s.ic.gov` is still supported for backward compatibility.
- Amazon ECS deployments are not supported.
- CodeDeploy integration with AWS CloudFormation is not supported.
- CodeDeploy integration with GitHub is not supported.
- CodeDeploy integration with Elastic Load Balancing Application Load Balancers is not supported.
- The CodeDeploy "Getting Started" Wizard is currently not supported in AWS Top Secret Regions.

- In AWS Top Secret Regions, the CodeDeploy Windows Agent requires a certificate bundle containing CAs in at the following location C:\ProgramData\Amazon\CodeDeploy\certs\ca-bundle.crt. You will need to maintain the copy of this file on Windows hosts for continued successful operation of Windows instances. For more information see Digital Certificates for AWS Top Secret Regions .
- On-premises deployments are not supported.
- Tag-based authorization is not supported.
- The notification rules are not currently supported in AWS Top Secret Regions.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.
- Automatically updating outdated instances is not supported.
- ECS capacity providers are not supported.
- To use CodeDeploy with Amazon Virtual Private Cloud, you must use CodeDeploy agent 1.3.1 or later.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to CodeDeploy by using the command line or APIs, use the appropriate endpoint.

Documentation for CodeDeploy

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

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

Amazon Comprehend

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.

Topics

- Region Availability
- How Amazon Comprehend Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Amazon Comprehend

Region Availability

Amazon Comprehend is available in the following AWS Top Secret Regions:

- AWS Top Secret - East

How Amazon Comprehend Differs for AWS Top Secret Regions

The implementation of Amazon Comprehend is different for AWS Top Secret Regions in the following ways:

- Amazon Comprehend Medical is not supported.
- Comprehend events are only available to AWS Top Secret Regions customers. You can request access to the API reference from your AWS contact for the AWS Top Secret Regions operational environment:
  - Comprehend Events API Reference
- The following APIs are not supported:
  - ContainsPiiEntities
  - Any Comprehend Medical APIs

- The following Data Types are not supported:
  - Any Comprehend Medical Data Types
- Amazon Resource Names (ARNs) and endpoints have different values.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Amazon Comprehend by using the command line or APIs, use the appropriate endpoint.

Documentation for Amazon Comprehend

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

- Amazon Comprehend Developer Guide

AWS Config

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

Topics

- Region Availability
- How AWS Config Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for AWS Config

Region Availability

AWS Config is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How AWS Config Differs for AWS Top Secret Regions

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

- The AWS service principal for AWS Config is `config.amazonaws.com`, but the former service principal of `config.c2s.ic.gov` is still supported for backward compatibility.
- For a list of resource types supported in AWS Top Secret Regions, see Resource Coverage by Region Availability.
- For a list of AWS Config managed rules supported in AWS Top Secret Regions, see List of AWS Config Managed Rules by Region Availability.
- AWS Config recording of third-party resources is only supported in the AWS Top Secret Regions through the AWS SDK or the AWS Command Line Interface (AWS CLI).
- AWS Config advanced queries are not supported in the AWS Top Secret Regions.
- AWS Config multi-account multi-region data aggregation is not supported in the AWS Top Secret Regions.

- AWS Config conformance packs are not supported in the AWS Top Secret Regions.
- AWS Config deployment of AWS Config rules across an AWS Organization is not supported in the AWS Top Secret Regions.
- AWS Config remediation actions for resources evaluated by AWS Config rules are not supported in the AWS Top Secret Regions.
- AWS Config custom policy rules created using AWS CloudFormation Guard might require additional permissions to allow debug logging in the AWS Top Secret Regions. If you are not using a service-linked role, you will need to add the following policy to your customer managed role.

```
...
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigCreateLogStreamStatement",
      "Effect": "Allow",
      "Action": [
          "logs:CreateLogStream",
          "logs:CreateLogGroup"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/config/*"
    },
    {
      "Sid": "AWSConfigPutLogEventsStatement",
      "Effect": "Allow",
      "Action": "logs:PutLogEvents",
      "Resource": "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
    }
  ]
}
...
```

(Recommended) Use the service-linked role

It is recommended that you use the AWS Config service-linked role. A service-linked role adds all the necessary permissions for AWS Config to run as expected.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to AWS Config by using the command line or APIs, use the appropriate endpoint.

Documentation for AWS Config

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

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

AWS Database Migration Service

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

Topics

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

Region Availability

AWS Database Migration Service is available in the following AWS Top Secret Regions:

- AWS Top Secret - East

How AWS DMS Differs for AWS Top Secret Regions

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

- The download locations for the AWS Schema Conversion Tool are different in AWS Top Secret Regions. The downloads can be found here:
  - Microsoft Windows
  - Fedora Linux (rpm)
  - Ubuntu Linux (deb)
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.
- AWS Snowball Edge is deployed to AWS Top Secret Regions. A description for how to download and install AWS Snowball Edge appears as part of step 2 of Step-by-step procedures for migrating data using AWS DMS with AWSAWS Snowball Edge in the *AWS Data Migration Service User Guide*. Or you can download and install the AWS Snowball Edge client from AWS Snowball Edge resources.

- For the APA/DCA region, AWS DMS 3.4.7 supports the following new or changed behavior and resolved issues:
  - You can now use a date format from the table definition to parse a data string into a date object when using Amazon S3 as a source.
  - New table statistics counters are now available: `AppliedInserts`, `AppliedDdls`, `AppliedDeletes`, and `AppliedUpdates`.
  - You can now choose the default mapping type when using OpenSearch as a target.
  - The new `TrimSpaceInChar` endpoint setting for Oracle, PostgreSQL, and SQLServer sources allows you to specify whether to trim data on CHAR and NCHAR data types.
  - The new `ExpectedBucketOwner` endpoint setting for Amazon S3 prevents sniping when using S3 as a source or target.
  - For RDS SQL Server, Azure SQL Server, and self-managed SQL Server — DMS now provides automated setup of MS-CDC on all tables selected for a migration task that are with or without a PRIMARY KEY, or with a unique index considering the enablement priority for MS-REPLICATION on self-managed SQL Server tables with PRIMARY KEY.
  - Added support for replication of Oracle Partition and sub-partition DDL Operations during Oracle homogenous migrations.
  - Fixed an issue where a data validation task crashes with a composite primary key while using Oracle as a source and target.
  - Fixed an issue with correctly casting a varying character type to a boolean while the target column was pre-created as a boolean when using Redshift as a target.
  - Fixed an issue that was causing data truncation for `varchar` data types migrated as `varchar(255)` due to a known ODBC issue when using PostgreSQL as a target.
  - Fixed an issue where Parallel Hint for the DELETE operation wasn't respected with `BatchApplyEnabled` set to `true` and `BatchApplyPreserveTransaction` set to `false` when using Oracle as a target.
  - The new `AddTrailingPaddingCharacter` endpoint setting for an Amazon S3 adds padding on string data when using S3 as a target.
  - The new `max_statement_timeout_seconds` task setting extends the default timeout of endpoint queries. This setting is currently used by MySQL endpoint metadata queries.
  - When using PostgreSQL as a target, fixed an issue where a CDC task wasn't properly utilizing the error handling task settings.

- Fixed an issue where DMS was unable to correctly identify Redis mode for a Redis Enterprise instance.
- Extended the support of `includeOpForFullLoad` extra connection attribute (ECA) for the S3 target parquet format.
- Introduced a new PostgreSQL endpoint setting `migrateBooleanAsBoolean`. When this setting is set to `true` for a PostgreSQL to Redshift migration, a boolean will be migrated as varchar(1). When it is set to `false`, a boolean is migrated as varchar(15), which is the default behavior.
- When using SQL Server source, fixed a migration issue with `datetime` datatype. This fix addresses the issue of inserting `Null` when precision is in milliseconds.
- For PostgresSQL source with PGLOGICAL, fixed a migration issue when using pglogical and removing a field from the source table during the CDC phase, where the value after the removed field wasn't migrated to the target table.
- Fixed a SQL Server Loopback migration issue with Bidirectional replication getting repeated records.
- Added a new ECA `mapBooleanAsBoolean` for PostgresSQL as a source. Using this extra connection attribute , you can override default data type mapping of a PostgresSQL Boolean to a RedShift Boolean data type.
- Fixed a migration issue when using SQL Server as source that addresses the ALTER DECIMAL/NUMERIC SCALE not replicating to targets.
- Fixed connection issue with SQL Server 2005.
- As of October 17, 2022, DMS 3.4.7 now supports Generation 6 Amazon EC2 instance classes for replication instances.

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

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

- New IBM Db2 for LUW versions 11.5.6 and 11.5.7 as a source.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

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

- https://dms.us-iso-east-1.c2s.ic.gov
- https://dms.us-iso-west-1.c2s.ic.gov

Documentation for AWS DMS

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

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

AWS DataSync

AWS DataSync is an online data movement and discovery service that simplifies data migration and helps you quickly, easily, and securely move your file or object data to, from, and between AWS storage services.

Topics

- Region Availability
- How DataSync Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for DataSync

Region Availability

DataSync is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How DataSync Differs for AWS Top Secret Regions

The implementation of DataSync is different for AWS Top Secret Regions in the following ways:

- You currently can't use the task mode option in the AWS Top Secret Regions.
- You can transfer between AWS Top Secret - East and AWS Top Secret - West only by using an Amazon EC2 agent. Transferring across these Regions without an agent isn’t available.
- You can’t transfer data to or from Microsoft Azure Blob Storage.
- You can’t transfer data to or from an AWS Snowcone because that device isn’t available in the AWS Top Secret Regions.
- You can't transfer data between Amazon S3 and Amazon S3 on Outposts because S3 on Outposts isn’t available in the AWS Top Secret Regions.
- AWS Support can’t access your DataSync agent.
- In the AWS Top Secret - East Region, you can transfer data to or from Amazon FSx for Windows File Server and FSx for Lustre. However, you can't transfer to or from FSx for ONTAP or FSx for OpenZFS because those file systems aren't available in the AWS Top Secret Regions.

- In the AWS Top Secret - West Region, you can't transfer data to or from Amazon FSx because those file systems aren't available in that Region.
- You can't use AWS DataSync Discovery in the AWS Top Secret Regions.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to DataSync by using the command line or APIs, use the appropriate endpoint.

Documentation for DataSync

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

- AWS DataSync User Guide
- DataSync section of AWS CLI Reference

Amazon DCV

Amazon DCV is a remote visualization technology that you can use to connect securely to graphic-intensive 3D applications hosted on remote servers. With Amazon DCV, you can bring high-performance processing capabilities to remote users through secure client sessions.

Topics

- How Amazon DCV Differs for AWS Top Secret Regions
- Documentation for Amazon DCV

How Amazon DCV Differs for AWS Top Secret Regions

The implementation of Amazon DCV is different for AWS Top Secret Regions in the following ways:

- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

General Differences

- There is no public facing website for Amazon DCV in the ADC regions. Instead, all artifacts live in a public facing bucket `amazon-dcv-download-us-iso-east-1`. Each artifact has an associated checksum object for verification.

  To review what artifacts are available in your specific region, please authenticate in a terminal and execute:

  ```
  aws --region us-iso-east-1 s3 ls --recursive s3://amazon-dcv-download-us-iso-east-1/
   --recursive
  ```

  You can also view the contents of the bucket by going to:

  ```
  https://amazon-dcv-download-us-iso-east-1.s3.us-iso-east-1.c2s.ic.gov/
  ```

- Operating systems in this partition are RHEL7, RHEL8, RHEL9, AmazonLinux2, and Windows.

Documentation for Amazon DCV

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

- Amazon DCV

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 AWS Top Secret Regions and Amazon Virtual Private Cloud.

Topics

- Region Availability
- How AWS Direct Connect Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for AWS Direct Connect

Region Availability

AWS Direct Connect is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How AWS Direct Connect Differs for AWS Top Secret Regions

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

- Both 10Gbps and 100Gbps connections are supported through the APIs in the AWS Top Secret - West Region.
- AWS Direct Connect allows for automated requests of 10Gbps connections through the console or API. Requests for connections of other sizes (1Gbps or 100Gbps) can be made to the AWS Top Secret Regions Project Management Office by filing a AWS Top Secret Regions Jira ticket.
- If you do not complete the cross connect within 365 days, the authority granted by the LOA-CFA expires.
- The Jumbo MTU size is 8801.
- An AWS Direct Connect gateway only supports VPC associations from within the AWS Top Secret Regions.

- Port-hours are billed once the connection between the AWS router and your router is established, or 365 days after you ordered the port, whichever comes first.
- Amazon CloudWatch metrics are not available in AWS Top Secret Regions.
- For TGW we will not support IPv6.
- MAC Security (MACsec) is not supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

The following are example AWS CLI directconnect commands:

- Describe locations

```
aws directconnect describe-locations
```

- Create connection

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

- Confirm connection

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

- Describe connections

```
aws directconnect describe-connections
```

- Create private virtual interface

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

- Create public virtual interface

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

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

Documentation for AWS Direct Connect

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

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

AWS Directory Service

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

Topics

- Region Availability
- How AWS Directory Service Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for AWS Directory Service

Region Availability

AWS Directory Service is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How AWS Directory Service Differs for AWS Top Secret Regions

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

- Only AWS Managed Microsoft AD and AD Connector directory types are supported by AWS Directory Service.
- The following directory types are not currently supported:
  - Simple AD
  - Amazon Cloud Directory
- The following AWS Managed Microsoft AD features are not currently supported:
  - Support for client-side LDAPS
  - Directory sharing with other AWS accounts

  - Directory security settings
  - Multi-region replication
- The following AD Connector features are not currently supported:
  - Support for client-side LDAPS
  - Support for smart card authentication
- The following AWS apps and services are not currently supported by AWS Directory Service:
  - Amazon WorkDocs
  - Amazon WorkMail
  - Amazon QuickSight
  - Amazon Chime
  - Amazon Connect
  - AWS IAM Identity Center (SSO)
  - AWS PrivateLink
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.
- The AWS Directory Service Data API are not supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

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

- https://ds.us-iso-east-1.c2s.ic.gov
- The CreateAlias action is not supported.

Documentation for AWS Directory Service

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

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

Amazon DynamoDB

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

Topics

- Region Availability
- How DynamoDB Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for DynamoDB

Region Availability

Amazon DynamoDB is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How DynamoDB Differs for AWS Top Secret Regions

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

- The following tools are available for DynamoDB:

Package	Location	Documentation
Local version of DynamoDB	https://s3.us-iso-east-1.c2s.ic.gov/dynamodb-customer-facing-tools/dynamodb_local_latest.zip	Running DynamoDB on Your Computer
DynamoDB Storage Backend for Titan	https://s3.us-iso-east-1.c2s.ic.gov/dynamodb-customer-facing-tools/titan-titan10.zip	Amazon DynamoDB Storage Backend for Titan

- Restores are limited to 4 concurrent operations.

- The following features are not available: DynamoDB Accelerator (DAX), CloudWatch Contributor Insights for DynamoDB, NoSQL Workbench, PartiQL API actions, resource-based policies, and attribute-based access policies.
- AWS PrivateLink is not supported for DynamoDB.
- Zero-ETL integration with DynamoDB and Amazon Redshift is not available.
- Warm throughput is not available.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to DynamoDB by using the command line or APIs, use the appropriate endpoint.

Documentation for DynamoDB

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

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

Amazon Elastic Block Store

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

Topics

- Region Availability
- How Amazon EBS Differs for AWS Top Secret Regions
- Documentation for Amazon EBS

Region Availability

Amazon Elastic Block Store is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Amazon EBS Differs for AWS Top Secret Regions

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

- You cannot encrypt a previously unencrypted volume using the console. To encrypt a volume, you must use the AWS CLI or AWS SDKs, or you must create a new volume that is encrypted. For more information, see Changing the Encryption State of Your Data or Copying an Amazon EBS Snapshot.
- You can copy snapshots between the AWS Top Secret Regions only. You can't copy snapshots from the AWS Top Secret Regions to any other AWS Region.
- To create replicas of your Microsoft licensed images and retain your license settings, you can use the Amazon EC2 CLI or Amazon EC2 API to copy a snapshot. The copied snapshot behaves the same as other snapshots: it can be used to create new Amazon EBS volumes that can then be attached to an EC2 instance. For more information, see Copying an Amazon EBS Snapshot.

- Amazon EC2 launches instances into a VPC instead of using the EC2-Classic platform. For more information, see Amazon EC2 and Amazon Virtual Private Cloud (VPC).
- The Provisioned IOPS SSD (io2) EBS volume type is not available in AWS Top Secret Regions.
- The Fast Snapshot Restore (FSR) feature is not available in AWS Top Secret Regions.
- Amazon Data Lifecycle Manager does not support the following features in AWS Top Secret Regions:
  - Amazon EBS snapshot archiving
  - Excluding specific data (non-root) volumes from multi-volume snapshot sets
  - Fast snapshot restore

  Amazon Data Lifecycle Manager supports Amazon EBS local snapshots on Outposts in AWS Top Secret - East only.
- The Multi-Attach feature is not available in AWS Top Secret Regions.
- Amazon EBS Snapshots Archive is not available in AWS Top Secret Regions.
- You can't exclude data (non-root) volumes from multi-volume snapshot sets in AWS Top Secret Regions.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

Documentation for Amazon EBS

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

- Amazon EC2 User Guide

EBS direct APIs

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

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

Topics

- Region Availability
- How EBS direct APIs Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for EBS direct APIs

Region Availability

EBS direct APIs is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How EBS direct APIs Differs for AWS Top Secret Regions

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

- AWS CloudTrail data events are not supported in AWS Top Secret Regions.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

EBS direct APIs has a service-specific command line interface. For more information about the EBS direct APIs CLI Tools, see AWS CLI.

To connect to EBS direct APIs by using the command line or APIs, use the appropriate endpoint.

Documentation for EBS direct APIs

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

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

Amazon Elastic Compute Cloud

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

Topics

- Region Availability
- How Amazon EC2 Differs for AWS Top Secret Regions
- How VM Import/Export Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Amazon EC2

Region Availability

Amazon Elastic Compute Cloud is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Amazon EC2 Differs for AWS Top Secret Regions

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

- Capacity Reservation sharing is not supported with the Amazon EC2 console in the AWS Top Secret - West Region. It is supported only with the AWS CLI and SDKs in this Region.
- Capacity Reservation Fleet is not supported with the Amazon EC2 console. It is supported with the AWS CLI and SDKs only.
- Amazon EC2 Instance Connect Endpoint is not available in AWS Top Secret Regions.
- The EC2 Reserved Instance Marketplace is not available in AWS Top Secret Regions.
- EC2 Fleet can't launch On-Demand Instances into targeted Capacity Reservations in AWS Top Secret Regions.

- Custom time windows for scheduled events are currently not available in AWS Top Secret Regions.
- The AWS service principal for Amazon EC2 is `ec2.amazonaws.com`, but the former service principal of `ec2.c2s.ic.gov` is still supported for backward compatibility.
- EC2 Serial Console is currently not available in AWS Top Secret Regions.
- Using AWS Systems Manager parameters instead of AMI IDs in launch templates is not available in AWS Top Secret Regions.
- Savings Plans are currently not available in AWS Top Secret Regions.
- Spot Instances are not available.
- The attribute-based instance type selection feature for Amazon EC2 Fleet and Spot Fleet is not available.
- For EC2 Fleet, you can only create an `instant` fleet type and only launch On-Demand Instances in the fleet. You cannot delete an `instant` fleet.
- There are limits on the number of instances that you can run. For more information, see Amazon EC2 FAQs. To request a limit increase, see "To request a limit increase" at AWS Service Limits.
- Amazon EC2 launches instances into a VPC instead of using the EC2-Classic platform. For more information, see Amazon EC2 and Amazon Virtual Private Cloud (VPC).
- For GPU instances, you should use the NVIDIA drivers that NVIDIA publishes in their AWS Marketplace. You can find NVIDIA AMIs and corresponding driver versions by searching for NVIDIA in the commercial AWS Marketplace.
- To enable enhanced networking on other Linux distributions, you must compile and install the `ixgbevf` module on your instance. The following `ixgbevf` versions are available for download:

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

Module	Readme
ixgbevf-3.2.2.tar.gz	readme-ixgbevf-3.2.2.txt

For more information, see Enabling Enhanced Networking with the Intel 82599 VF Interface on Other Linux Distributions.

- For Windows instances, the maximum transmission unit (MTU) of a network connection is 1500 bytes. For Linux instances, the maximum supported MTU is 8868 bytes instead of 9001 bytes. However, the path MTU has been reduced to 8801 bytes in the region to enable Enhanced Networking on instances that support them. For more information, see Network Maximum Transmission Unit (MTU) for Your EC2 Instance.
- Within AWS Top Secret Regions, Availability Zones are not independently mapped to identifiers for each account, and are fixed in nature. All customer accounts utilize the same Availability Zone mapping, and require no action on the customer's part to ensure this.
- For differences about Amazon Linux 2, see Amazon Linux 2 AMI for AWS Top Secret Regions.
- For differences about the Amazon Linux AMI, see Amazon Linux for AWS Top Secret Regions.
- For differences about Windows AMIs, see AWS Windows AMIs for AWS Top Secret Regions.
- Installation of EC2Launch v2 from SSM Distributor and migration to the latest version of EC2Launch v2 with an SSM RunCommand document are not supported.
- For instance identity documents, you should use the following AWS public certificate to verify the PKCS7 signature:


```
-----BEGIN CERTIFICATE-----
MIIC7TCCAqwCCQCZtqOU7PplNzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xNDEyMTgxNTU3MDBaFw00
MDEyMTgxNTU3MDBaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbYwggErBgcqhkjOOAQBMIIBHgKBgQCW7NsbpQ/fG1IPAR1D
jSL+37fZxKsDNhNTtRazeWZ8i3rkj0UKviGNc5znkofEeXBRYGOy2VMj9s/LDNwe
5EWUSM1NFATxEnNj0a6Mpe6+fdULvu0dRRgzFrzPwz+N+7W6FTIsPKOvoCiL9Wo2
jH/+runj7eh3hdawCRgMs/551QIVAOPmSEbw7CQb+qN9H4GaJZ9hJCAVAoGAE8bV
wflcFuiVzEMaKYs/PL6J8FnJmpUOQD+/toZEUlJb/rCsGuwffaLrKRWERvhB9g4V
Sq8gbJxD+VivhtBBjEFX46UYSuUCpsDe5S33IMav2M0Vh6TzpJNJuNBMwgFGsGoU
gdQIbLQYoFYjY5wO3stcSGukhKDAlfOy/3j9yH8DgYQAAoGAX11N+iYCpzdXLd4L
Koeu8hWG2NaemcMWSPNcvWkDcytk/zZ63scB48hWVjUm6Cr87MKYO9EbKSVxY+gm
zqxGNBdU09BNHH4mJlDRU5iXQ+N2NU4G4T8Zib7sdBQmjmcwzuTCcapCOfTtZbD/
```

```
PcxNaq9XQlUCZpa7R8HON+7jBkowCQYHKoZIzjgEAwMwADAtAhUAjbApf4fhNIBo
vSUJU5klxlzFGT0CFGKWETFYVQBg0mqppz2/0rVqvLCy
-----END CERTIFICATE-----
```

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

```
-----BEGIN CERTIFICATE-----
 MIIBxjCCAXACCQDu2vZ7sK1CPzANBgkqhkiG9w0BAQUFADBqMQswCQYDVQQGEwJV
 UzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMHU2VhdHRsZTEYMBYGA1UE
 ChMPQW1hem9uLmNvbSBJbmMuMRowGAYDVQQDExFlYzIuYW1hem9uYXdzLmNvbTAe
 Fw0xNDEyMTgxNTUyMTFaFw0yNDEyMTcxNTUyMTFaMGoxCzAJBgNVBAYTAlVTMRMw
 EQYDVQQIEwpXYXNoaW5ndG9uMRAwDgYDVQQHEwdTZWF0dGxlMRgwFgYDVQQKEw9B
 bWF6b24uY29tIEluYy4xGjAYBgNVBAMTEWVjMi5hbWF6b25hd3MuY29tMFwwDQYJ
 KoZIhvcNAQEBBQADSwAwSAJBAMZakpMvmY5+4Li9K/siSU6q81o8kTUj8PAOxdGe
 VBybF2O50UtuWKZhFGVKbyB+mI4Enl6RC+voVsM1aufW/CMCAwEAATANBgkqhkiG
 9w0BAQUFAANBAAL8vGNcCalUywMVpAswlDisMg2BUK7h0Rj0ceKwEfZXcfZAWhYu
 JfZgObWF9A0QVFcnSPQNekmicK+Q3VEq6ts=
-----END CERTIFICATE-----
```

- The Provisioned IOPS SSD (io2) EBS volume type is not available in AWS Top Secret Regions.
- AWS Nitro Enclaves is not available in AWS Top Secret Regions.
- On-Demand Instance hibernation is not available in AWS Top Secret Regions.
- Amazon EC2 Images does not currently support *create-restore-image-task*, *create-store-image-task* or *describe-store-image-task* in the AWS Top Secret - West Region.
- Seamless domain join is not enabled in AWS Top Secret Regions.
- On-demand instance quotas are based on number of vCPUs in AWS Top Secret Regions.
- The transfer Elastic IP address feature is not available in AWS Top Secret Regions.
- AMD Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP) is not available in AWS Top Secret Regions.
- Attached EBS status checks are not available in AWS Top Secret Regions.
- Amazon EC2 instance topology is not available in AWS Top Secret Regions.
- Launching an instance with an AWS Marketplace AMI is not supported in AWS Top Secret - West. Therefore, the **AWS Marketplace AMIs** tab is not available in the AMI Catalog in AWS Top Secret - West.
- When you use the 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 Top Secret - East (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 Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.
- The Capacity Reservation management capabilities of split, move, and modify instance eligibility are not available in AWS Top Secret Regions.
- You can't modify, reset, or view the address attributes of an Elastic IP address.
- The only Capacity Reservation metric dimension available in AWS Top Secret Regions is `CapacityReservationID`.
- Prefix delegation for Amazon EC2 network interfaces is not supported in AWS Top Secret Regions.

How VM Import/Export Differs for AWS Top Secret Regions

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

- You can use the AWS VM Import tools to import VM images from your local environment and convert them into Amazon EC2 instances. For more information, see Importing a VM into Amazon EC2.
- The following instance types are supported for VM import. The version must be 1.7.1.1 or later.

Instance Family	Instance Types
General purpose	`m3.xlarge` | `m3.2xlarge`
Storage optimized	`hs1.8xlarge`

  For more information about VM import prerequisites, see VM Import/Export Prerequisites.
- You can import Microsoft Windows VMs that use the Bring Your Own License (BYOL) model. First, create a case in AWS Support Center and request to be whitelisted for Windows BYOL. Import the Windows VM using the instructions for Importing a Virtual Machine Using the Amazon EC2 CLI.
- UEFI boot mode is not supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

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

To connect to Amazon EC2 by using the command line or APIs, use the appropriate endpoint.

Documentation for Amazon EC2

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Amazon EC2 differs for AWS Top Secret Regions, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Top Secret Regions. There are other differences, such as links, endpoints, and screenshots.

- Amazon Elastic Compute Cloud Documentation

Amazon EC2 Auto Scaling

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

Topics

- Region Availability
- How Auto Scaling Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Auto Scaling

Region Availability

Amazon EC2 Auto Scaling is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Auto Scaling Differs for AWS Top Secret Regions

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

- The AWS service principal for Amazon EC2 Auto Scaling is `autoscaling.amazonaws.com`, but the former service principal of `autoscaling.c2s.ic.gov` is still supported for backward compatibility.
- For Auto Scaling groups with multiple instance types, you can only launch On-Demand Instances. However, Reserved Instances are supported. These On-Demand Instances must match certain attributes, such as instance type and Region, in order to benefit from the billing discount. Savings Plans are not currently supported in AWS Top Secret Regions.
- Amazon EC2 Auto Scaling does not support launching Spot Instances.

- The attribute-based instance type selection feature is not available.
- Specifying `lowest-price` for the `OnDemandAllocationStrategy` property of a mixed instances group is currently not supported.
- Amazon EC2 launches instances into a VPC instead of using the EC2-Classic platform. For more information, see Amazon EC2 and Amazon Virtual Private Cloud (VPC).
- Amazon EC2 provides other restrictions. For more information, see Amazon Elastic Compute Cloud
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.
- You cannot create a predictive scaling policy in AWS Top Secret Regions.
- Retrieving the target lifecycle state through instance metadata is not available in AWS Top Secret Regions.
- The metric math feature for target tracking scaling policies is not available.
- Amazon EC2 Auto Scaling does not currently support the AttachTrafficSources, DetachTrafficSources, and DescribeTrafficSources API operations.
- EBS health check monitoring is not available in AWS Top Secret Regions.
- Zonal shift is not available in AWS Top Secret Regions.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Auto Scaling by using the command line or APIs, use the appropriate endpoint.

Documentation for Auto Scaling

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

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

Amazon EC2 Image Builder

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

Topics

- Region Availability for Image Builder
- How Image Builder Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Image Builder

Region Availability for Image Builder

Image Builder is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Image Builder Differs for AWS Top Secret Regions

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

- Amazon Resource Names (ARNs) and endpoints have different values.
- The AWS Task Orchestrator and Executor (AWSTOE) component management tool's UpdateOS Action Module won't work for Windows unless you configure your own WSUS Server and modify the image to point to that.
- For all Linux distributions except for Amazon Linux 2, you must configure your image to use repository mirrors that are available on the network.
- Image Builder doesn't support third party managed Linux base images, except for RHEL, for example SUSE, Ubuntu, CentOs, or others. However, you can supply your own custom AMIs for those operating system platforms.
- Image Builder doesn't support AWS PrivateLink in AWS Top Secret Regions.

- Image Builder doesn't support AWS CloudFormation for container images in AWS Top Secret Regions.
- Image Builder doesn't support managed container images in AWS Top Secret Regions.
- Image Builder doesn't support CIS Hardened Images or the CIS Hardening component products from the Center for Internet Security in AWS Top Secret Regions.
- Image Builder doesn't support common vulnerability (CVE) findings in AWS Top Secret Regions.
- Image Builder doesn't support image lifecycle policies in AWS Top Secret Regions.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Image Builder by using the command line or APIs, use the appropriate endpoint.

Documentation for Image Builder

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

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

Amazon Elastic Container Registry

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

Topics

- Region Availability
- How Amazon ECR Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Amazon ECR

Region Availability

Amazon Elastic Container Registry is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Amazon ECR Differs for AWS Top Secret Regions

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

- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.
- Dual-layer server-side encryption with AWS KMS (DSSE-KMS) is available.
- Improved basic scanning isn't available.
- Amazon ECR image scanning is not supported. This includes both basic and enhanced scanning.
- Pull through cache rules are not supported.
- Tagging an Amazon ECR repository is not supported.
- Cross-region and cross-account replication is not supported.
- Amazon ECR doesn't emit any events to Amazon EventBridge in AWS Top Secret Regions.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Amazon ECR by using the command line or APIs, use the appropriate endpoint.

Documentation for Amazon ECR

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

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

Amazon Elastic Container Service

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

Topics

- Region Availability
- How Amazon ECS Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Amazon ECS

Region Availability

Amazon Elastic Container Service is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Amazon ECS Differs for AWS Top Secret Regions

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

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

```
echo "ECS_BACKEND_HOST=https://ecs.us-iso-east-1.c2s.ic.gov">> /etc/ecs/ecs.config
```

- All layers and containers specified must be in Amazon ECR or another registry in the region.
- The Amazon ECS container agent needs to use the certificates from the host machine. This requires that the `/etc/pki` path must be mapped as a mount point into the container and the `SSL_CERT_DIR` environment variable must be set to `/etc/pki/tls/certs`. This can be done in the container definition by adding these to the mountPoint and environment parameters.

- If your container instance was not launched using an Amazon ECS-optimized AMI, see Installing the Amazon ECS container agent in the *Amazon Elastic Container Service Developer Guide* for details on installing the Amazon ECS container agent.
- The **Clusters** section of the console has a **Get Started** button for creating a simple task in a cluster. The **Image** field is prepopulated with `httpd:2.4` to use version 2.4 of the Apache HTTP server Docker image. Because there are no public registries in the region, this will not work. If you have a compatible image in a registry for which you have access, you can use *`repository-url/image:tag`* or *`repository-url/image@digest`* to specify that image.
- Interface VPC endpoints(AWS PrivateLink) for Amazon ECS are not supported.
- The UpdateContainerAgent API action is not supported.
- Attaching Amazon Elastic Inference accelerators to your containers is not supported.
- ECS Anywhere is not supported.
- AWS Copilot is not supported.
- Fargate Spot is not available in AWS Top Secret Regions.
- The ECS CLI is not supported.
- Attaching Amazon EBS volumes to Amazon ECS tasks is not supported.
- AWS does not own or operate the docker.io domain in this Region. Any examples referencing the default Docker repository shouldn't be used. Ensure you use a repository you own or whose owner you can verify.
- Amazon ECS resources are not supported CloudWatch targets.
- Private Registry Authentication is not supported.
- Amazon ECS Exec Suite not supported against Fargate Containers.
- In AWS Top Secret - East, you must explicitly specify the AWS service endpoint in the Fluent Bit output definition using the endpoint option supported by all AWS plugins. For more information, see Using the AWS for Fluent Bit image in the *Amazon Elastic Container Service Developer Guide*
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.
- Amazon ECS limit increases aren't available through AWS Service Quotas.
- Scheduled tasks are not supported for tasks that use the Fargate launch type.
- Scheduled tasks are not supported for tasks that use the EC2 launch type.
- Amazon ECS Service Connect is not supported.
- Task definition deletion is not supported.

- The `splunk` log driver is not supported.
- The `versionConsistency` container definition parameter is not supported.
- Official Amazon ECS agent update support is provided through regular Amazon ECS-optimized AMI releases. Standalone agent package releases through Amazon S3 or ecs-agent OCI artifacts are not currently supported.
- Availability Zone rebalancing is not supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Amazon ECS by using the command line or APIs, use the appropriate endpoint.

Documentation for Amazon ECS

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

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

Amazon EFS

Amazon EFS provides a simple, serverless, set-and-forget elastic file system. With Amazon EFS, you can create a file system, mount the file system on an Amazon EC2 instance, and then read and write data to and from your file system. You can mount an Amazon EFS file system in your virtual private cloud (VPC), through the Network File System versions 4.0 and 4.1 (NFSv4) protocol. We recommend using a current generation Linux NFSv4.1 client, such as those found in the latest Amazon Linux, Amazon Linux 2, Red Hat, Ubuntu, and macOS Big Sur AMIs, in conjunction with the Amazon EFS mount helper. It is built to scale on demand to petabytes without disrupting applications, growing and shrinking automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth.

Topics

- Region Availability
- How Amazon EFS Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Amazon EFS

Region Availability

Amazon EFS is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Amazon EFS Differs for AWS Top Secret Regions

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

- Amazon EFS is not available with AWS CloudFormation in AWS Top Secret - West.
- 17-character format resource IDs for file system and mount target resource types are not available in AWS Top Secret - East.
- The default selection for Amazon EFS Lifecycle Management is **None** when creating a new file system in AWS Top Secret - East.
- Using AWS Backup to backup Amazon EFS file systems is not available.

- Using AWS Transfer Family to transfer data into or out of Amazon EFS file systems is not available.
- Amazon EFS One Zone storage classes are not available.
- EFS file system policies, backup policies, and Access Points are not available when creating an EFS file system using AWS CloudFormation.
- The EFS Archive storage class and the Transition into Archive lifecycle policy are not supported.
- The EFS console refers to One Zone as a storage class instead of a file system type.
- Amazon EFS can only support 500 MiB/s throughput per client in AWS Top Secret - West.
- Amazon Resource Names (ARNs) and endpoints have different values.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Amazon EFS by using the command line or APIs, use the appropriate endpoint.

Documentation for Amazon EFS

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

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

Amazon EKS

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

Topics

- Amazon EKS ADC User Guide Supplement
- Region Availability
- How Amazon EKS Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions

Amazon EKS ADC User Guide Supplement

The Amazon EKS ADC User Guide Supplement provides additional information specifically for customers running workloads in ADC regions.

Review the Amazon EKS ADC User Guide Supplement.

This guide supplements the standard Amazon EKS documentation with details on:

- Availability of EKS (Amazon Elastic Kubernetes Service) features in the ADC Regions
- Supported Kubernetes versions
- Addon availability for EKS clusters in the ADC Regions
- Common issues and considerations when running Kubernetes in the ADC Regions

We recommend reviewing this ADC Supplement if you are deploying Kubernetes-based applications in the ADC Regions, as it contains crucial information not covered in the general Amazon EKS documentation.

Region Availability

Amazon Elastic Kubernetes Service is available in the following AWS Top Secret Regions:

- AWS Top Secret - East

- AWS Top Secret - West

How Amazon EKS Differs for AWS Top Secret Regions

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

- Dual-stack endpoints for EKS clusters aren't available.
- Dual-stack API endpoint for the Amazon EKS OIDC Issuer URL isn't available.
- Dual-stack API endpoint for the Amazon EKS API isn't available.
- Amazon EKS Anywhere isn't available.
- Amazon Resource Names (ARNs) and endpoints have different values.
- AWS Fargate on EKS isn't available.
- Spot instances aren't available for managed node groups.
- GPU instance (P and G) types aren't supported in AWS Top Secret - West.
- ARM, Bottlerocket, and Windows AMIs aren't available.
- Amazon Linux 2023 isn’t available.
- The Amazon FSx for Lustre CSI driver isn't available.
- The CSI snapshot controller is only available as a self-managed installation.
- `IPv6` support isn't available.
- The following features of the AWS Load Balancer Controller aren't available: Load Balancer listener tagging, SSL policy, AWS WAF and AWS WAFv2, and AWS Shield.
- Amazon EKS limit increases aren't available through AWS Service Quotas.
- AWS Certificate Manager private Kubernetes integration isn't available.
- Only Signature Version 4 signing is supported.
- Clusters running Kubernetes version `1.27` or higher can use Kubernetes Secrets Store CSI driver with AWS Secrets Manager.
- Amazon EKS on AWS Outposts isn't supported.
- The observability dashboard isn't available.
- The Amazon CloudWatch Observability Operator isn't available.
- CloudWatch Container Insights isn't available.
- Amazon Managed Service for Prometheus isn't available.
- The AWS Distro for OpenTelemetry (ADOT) Operator isn't available.

- Amazon GuardDuty isn't available in AWS Top Secret - West.
- The Amazon EKS Connector isn't available.
- Amazon EKS Upgrade insights aren't available.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Amazon EKS by using the command line or APIs, use the appropriate endpoint.

Elastic Load Balancing

Elastic Load Balancing automatically distributes incoming application traffic across multiple targets. Elastic Load Balancing enables you to achieve greater fault tolerance in your applications by seamlessly scaling your load balancer as incoming traffic changes over time. Elastic Load Balancing monitors the health of your targets, and routes traffic only to the healthy targets.

Topics

- Region Availability
- How Elastic Load Balancing Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Elastic Load Balancing

Region Availability

Elastic Load Balancing is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Elastic Load Balancing Differs for AWS Top Secret Regions

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

- Application Load Balancers and Classic Load Balancers in AWS Top Secret Regions do not support desync mitigation mode.
- Amazon EC2 launches instances into a VPC instead of using the EC2-Classic platform. For more information, see Amazon EC2 and Amazon Virtual Private Cloud (VPC).
- When using access logs, specify this AWS account ID to grant Elastic Load Balancing permission to write the access logs to your Amazon S3 bucket:

Region	Elastic Load Balancing Account ID
`us-iso-east-1`	770363063475

Region	Elastic Load Balancing Account ID
us-iso-west-1	121062877647

- Route 53 Hosted Zone ID information:

Region	Route 53 Hosted Zone ID
us-iso-east-1	Network Load Balancers: Z96M0JZ3VWHIO
us-iso-east-1	Application Load Balancers/Classic Load Balancers: Z1958BCSJLLOYB
us-iso-west-1	Network Load Balancers: Z0831180GI6H86MLGNIR
us-iso-west-1	Application Load Balancers/Classic Load Balancers: Z08048161KDY557ICL9WM

- When using user authentication with your Application Load Balancer, use the following endpoints to validate JWT headers:

Region	Elastic Load Balancing Account ID
us-iso-east-1	https://s3.us-iso-east-1.c2s.ic.gov/aws-elb-public-keys-prod-us-iso-east-1/
us-iso-west-1	https://s3.us-iso-west-1.c2s.ic.gov/aws-elb-public-keys-prod-us-iso-west-1/

- When using user authentication with your Application Load Balancer, AWS Top Secret Regions uses a private CA and the IDP endpoints must be within the AWS Top Secret Regions WAN and not the open internet.
- Application Load Balancers in AWS Top Secret Regions do not support Cognito user authentication in listener rules.
- Application Load Balancers in AWS Top Secret Regions do not support application cookie stickiness.
- Application Load Balancers in AWS Top Secret Regions do not support the least outstanding requests algorithm.

- Because AWS WAF (AWS WAF) is not available in AWS Top Secret Regions, Application Load Balancers in AWS Top Secret Regions cannot integrate with AWS WAF.
- Network Load Balancers in AWS Top Secret Regions do not support sticky sessions.
- Network Load Balancers in AWS Top Secret Regions do not support custom private IPv4 addresses.
- Network Load Balancers in AWS Top Secret Regions do not support attaching security groups.
- Elastic Load Balancing does not support standalone creation of target groups with protocol version HTTP/2 or gRPC in AWS Top Secret Regions. These target groups can only be created while launching a new Application Load Balancer.
- More than one SSL certificate per Listener is not supported in AWS Top Secret Regions.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

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

Documentation for Elastic Load Balancing

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

Overview

Elastic Load Balancing User Guide

Elastic Load Balancing v2

- User Guide for Application Load Balancers
- User Guide for Network Load Balancers
- User Guide for Gateway Load Balancers
- Elastic Load Balancing API Reference version 2015-12-01
- elbv2 section of the AWS CLI Command Reference

Elastic Load Balancing v1

- User Guide for Classic Load Balancers
- Elastic Load Balancing API Reference version 2012-06-01
- elb section of the AWS CLI Command Reference

Amazon EMR

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

Topics

- Region Availability
- How Amazon EMR Differs for AWS Top Secret Regions
- Documentation for Amazon EMR

Region Availability

Amazon EMR is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Amazon EMR Differs for AWS Top Secret Regions

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

The following Amazon EMR releases are available in the **AWS Top Secret - East Region**:

6.x supported versions

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

- 6.15.0
- 6.12.0
- 6.11.0
- 6.10.0
- 6.9.0
- 6.6.0

- 6.3.0
- 6.2.0
- 6.0.0

5.x supported versions

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

- 5.36.2
- 5.36.1
- 5.36.0
- 5.33.0
- 5.32.0
- 5.31.0
- 5.30.1
- 5.29.0
- 5.28.1
- 5.27.0, 5.27.1
- 5.25.0
- 5.21.0, 5.21.2
- 5.19.0, 5.19.1
- 5.15.0, 5.15.1
- 5.13.0, 5.13.1
- 5.9.0, 5.9.1
- 5.8.0, 5.8.3
- 5.7.0, 5.7.1
- 5.6.0, 5.6.1
- 5.5.0, 5.5.4
- 5.4.0, 5.4.1
- 5.3.0, 5.3.1, 5.3.2
- 5.2.0, 5.2.1, 5.2.3
- 5.1.0, 5.1.1

- 5.0.0, 5.0.3

4.x supported versions

The following 4.x release versions are available in AWS Top Secret - East Region:

- 4.9.1, 4.9.6
- 4.8.0, 4.8.2, 4.8.3, 4.8.4, 4.8.5
- 4.7.0, 4.7.1, 4.7.2, 4.7.4
- 4.6.0
- 4.5.0
- 4.4.0
- 4.3.0
- 4.2.0

3.x supported versions

The 3.x release series is not supported in AWS Top Secret - East Region.

The following Amazon EMR releases are available in the **AWS Top Secret - West Region**:

6.x supported versions

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

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

5.x supported versions

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

- 5.36.2
- 5.36.1
- 5.36.0
- 5.32.0

4.x supported versions

The 4.x release series is not supported in AWS Top Secret - West Region.

3.x supported versions

The 3.x release series is not supported in AWS Top Secret - West Region.

The following Amazon EC2 instance types are available for Amazon EMR in the AWS Top Secret - East and AWS Top Secret - West Regions. We recommend that you upgrade your processes and workloads to use current generation instance types.

Supported instance types - AWS Top Secret - West

Instance class	Instance types
General Purpose - Current Generation	m5.xlarge, m5.2xlarge, m5.4xlarge, m5.8xlarge, m5.12xlarge, m5.16xlarge, m5.24xlarge, m5d.xlarge, m5d.2xlarge, m5d.4xlarge, m5d.8xlarge, m5d.12xlarge, m5d.16xlarge, m5d.24xlarge, m6i.xlarge, m6i.2xlarge, m6i.4xlarge, m6i.8xlarge, m6i.12xlarge, m6i.16xlarge, m6i.24xlarge, m6i.32xlarge
Compute Optimized - Current Generation	c5.xlarge, c5.2xlarge, c5.4xlarge, c5.9xlarge, c5.12xlarge, c5.18xlarge, c5.24xlarge, c5d.xlarge, c5d.2xlarge, c5d.4xlarge, c5d.9xlarge, c5d.12xlarge, c5d.18xlarge, c5d.24xlarge, c5n.xlarge, c5n.2xlarge, c5n.4xlarge, c5n.9xlarge, c5n.18xlarge, c6i.xlarge, c6i.2xlarge, c6i.4xlarge, c6i.8xlarge, c6i.12xlarge, c6i.16xlarge, c6i.24xlarge, c6i.32xlarge
Memory Optimized - Current Generation	r5.xlarge, r5.2xlarge, r5.4xlarge, r5.8xlarge, r5.12xlarge, r5.16xlarge, r5.24xlarge, r5d.xlarge, r5d.2xlarge, r5d.4xlarge, r5d.8xlarge, r5d.12xlarge, r5d.16xlarge, r5d.24xlarge, r5dn.xlarge, r5dn.2xlarge, r5dn.4xlarge, r5dn.8xlarge, r5dn.12xlarge,

Instance class	Instance types
	r5dn.16xlarge, r5dn.24xlarge, r6i.xlarge, r6i.2xlarge, r6i.4xlarge, r6i.8xlarge, r6i.12xlarge, r6i.16xlarge, r6i.24xlarge, r6i.32xlarge
Storage Optimized - Current Generation	d2.xlarge, d2.2xlarge, d2.4xlarge, d2.8xlarge, i3.xlarge, i3.2xlarge, i3.4xlarge, i3.8xlarge, i3.16xlarge, i3en.xlarge, i3en.2xlarge, i3en.3xlarge, i3en.6xlarge, i3en.12xlarge, i3en.24xlarge

Supported instance types - AWS Top Secret - East

Instance class	Instance types
General Purpose - Current Generation	m5.xlarge, m5.2xlarge, m5.4xlarge, m5.8xlarge, m5.12xlarge, m5.16xlarge, m5.24xlarge, m5d.xlarge, m5d.2xlarge, m5d.4xlarge, m5d.8xlarge, m5d.12xlarge, m5d.16xlarge, m5d.24xlarge, m6g.xlarge, m6g.2xlarge, m6g.4xlarge, m6g.8xlarge, m6g.12xlarge, m6g.16xlarge, m6gd.xlarge, m6gd.2xlarge, m6gd.4xlarge, m6gd.8xlarge, m6gd.12xlarge, m6gd.16xlarge, m6i.xlarge, m6i.2xlarge, m6i.4xlarge, m6i.8xlarge, m6i.12xlarge, m6i.16xlarge, m6i.24xlarge, m6i.32xlarge
General Purpose - Previous Generation	m3.xlarge, m3.2xlarge, m4.large, m4.xlarge, m4.2xlarge, m4.4xlarge, m4.10xlarge, m4.16xlarge
Compute Optimized - Current Generation	c5.xlarge, c5.2xlarge, c5.4xlarge, c5.9xlarge, c5.12xlarge, c5.18xlarge, c5.24xlarge, c5d.xlarge, c5d.2xlarge, c5d.4xlarge, c5d.9xlarge, c5d.12xlarge, c5d.18xlarge, c5d.24xlarge, c5n.xlarge, c5n.2xlarge, c5n.4xlarge, c5n.9xlarge, c5n.18xlarge, c6g.xlarge, c6g.2xlarge, c6g.4xlarge, c6g.8xlarge, c6g.12xlarge, c6g.16xlarge, c6i.xlarge, c6i.2xlarge, c6i.4xlarge, c6i.8xlarge, c6i.12xlarge, c6i.16xlarge, c6i.24xlarge, c6i.32xlarge
Compute Optimized - Previous Generation	c4.large, c4.xlarge, c4.2xlarge, c4.4xlarge, c4.8xlarge

Instance class	Instance types
Accelerated Computing - Current Generation	g3.4xlarge, g3.8xlarge, g3.16xlarge, g4dn.xlarge, g4dn.2xlarge, g4dn.4xlarge, g4dn.8xlarge, g4dn.12xlarge, g4dn.16xlarge, p3.2xlarge, p3.8xlarge, p3.16xlarge
Memory Optimized - Current Generation	r5.xlarge, r5.2xlarge, r5.4xlarge, r5.8xlarge, r5.12xlarge, r5.16xlarge, r5.24xlarge, r5d.xlarge, r5d.2xlarge, r5d.4xlarge, r5d.8xlarge, r5d.12xlarge, r5d.16xlarge, r5d.24xlarge, r5dn.xlarge, r5dn.2xlarge, r5dn.4xlarge, r5dn.8xlarge, r5dn.12xlarge, r5dn.16xlarge, r5dn.24xlarge, r5n.xlarge, r5n.2xlarge, r5n.4xlarge, r5n.8xlarge, r5n.12xlarge, r5n.16xlarge, r5n.24xlarge, r6g.xlarge, r6g.2xlarge, r6g.4xlarge, r6g.8xlarge, r6g.12xlarge, r6g.16xlarge, r6gd.xlarge, r6gd.2xlarge, r6gd.4xlarge, r6gd.8xlarge, r6gd.12xlarge, r6gd.16xlarge, r6i.xlarge, r6i.2xlarge, r6i.4xlarge, r6i.8xlarge, r6i.12xlarge, r6i.16xlarge, r6i.24xlarge, r6i.32xlarge, r6id.xlarge, r6id.2xlarge, r6id.4xlarge, r6id.8xlarge, r6id.12xlarge, r6id.16xlarge, r6id.24xlarge, r6id.32xlarge, x1.16xlarge, x1.32xlarge
Memory Optimized - Previous Generation	r3.xlarge, r3.2xlarge, r3.4xlarge, r3.8xlarge, r4.xlarge, r4.2xlarge, r4.4xlarge, r4.8xlarge, r4.16xlarge
Storage Optimized - Current Generation	d2.xlarge, d2.2xlarge, d2.4xlarge, d2.8xlarge, d3.xlarge, d3.2xlarge, d3.4xlarge, d3.8xlarge, i3.xlarge, i3.2xlarge, i3.4xlarge, i3.8xlarge, i3.16xlarge, i3en.xlarge, i3en.2xlarge, i3en.3xlarge, i3en.6xlarge, i3en.12xlarge, i3en.24xlarge
Storage Optimized - Previous Generation	i2.xlarge, i2.2xlarge, i2.4xlarge, i2.8xlarge

- Automatic Amazon Linux updates, as discussed in the Amazon EMR Management Guide, are not enabled in AWS Top Secret Regions.
- The issue discussed in CVE-2021-44228 is relevant to Apache log4j- core versions between 2.0 and 2.14.1 when processing inputs from untrusted sources. EMR clusters launched with EMR 5 releases up to 5.34 and EMR 6 releases up to EMR 6.5 include open source frameworks such as Apache Hive, Flink, HUDI, Presto, and Trino, which use these versions of Apache Log4j. However,

many customers use the open source frameworks installed on their EMR clusters to process and log inputs from untrusted sources. Therefore, AWS recommends that you apply the "EMR Bootstrap Action Solution for Log4j CVE-2021-44228" as described in the topic, Approach to mitigate CVE-2021-44228. This solution also addresses CVE-2021-45046.

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

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

CVE-2021-44228 & CVE-2021-45046 - AWS Top Secret Regions - Bootstrap Scripts for EMR Releases

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

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

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

Amazon EMR release version	Script location	Script release date
5.19.1	`s3://us-iso-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.19.1-v1.sh`	December 15, 2021
5.15.1	`s3://us-iso-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.15.1-v1.sh`	December 15, 2021
5.13.1	`s3://us-iso-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.13.1-v1.sh`	December 15, 2021
5.9.1	`s3://us-iso-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.9.1-v1.sh`	December 15, 2021
5.8.3	`s3://us-iso-east-1.elasticmapreduce/bootstrap-actions/log4j/patch-log4j-emr-5.8.3-v1.sh`	December 15, 2021

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

EMR release version	Associated bootstrap script as of December 2021
6.3.0	6.3.1
6.2.0	6.2.1
6.0.0	6.0.1
5.33.0	5.33.1
5.32.0	5.32.1
5.31.0	5.31.1
5.30.0 or 5.30.1	5.30.2
5.29.0	5.29.0
5.28.0	5.28.1
5.27.0	5.27.1
5.25.0	5.25.0
5.21.0 or 5.21.2	5.21.2
5.19.0 or 5.19.1	5.19.1
5.15.0	5.15.1

EMR release version	Associated bootstrap script as of December 2021
5.13.0 or 5.13.1	5.13.1
5.9.0	5.9.1
5.8.0 or 5.8.3	5.8.3
5.7.0 or 5.7.1	5.7.1

- The Amazon EMR service principal in AWS Top Secret Regions is `elasticmapreduce.c2s.ic.gov`.
- EMRFS encryption is limited to user-specified and managed encryption keys until AWS Key Management Service is operational.
- Hunk is not available.
- MapR is not available.
- Debugging is not available.
- Amazon EC2 launches instances into a VPC instead of using the EC2-Classic platform. For more information, see Amazon EC2 and Amazon Virtual Private Cloud (VPC).
- Tez UI and YARN timeline server persistent application history interfaces are not available.
- EMR Notebooks is not available.
- Managed scaling is not available.
- The old Amazon EMR management console is the default console for AWS Top Secret Regions.
- The allocation strategy option for instance fleets is not available.
- Docker containers are not available.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

Documentation for Amazon EMR

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Amazon EMR differs for AWS Top Secret Regions, as described in this topic. Also, some features and new functionality described in this documentation

might not be available in the current release of AWS Top Secret Regions. There are other differences, such as links, endpoints, and screenshots.

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

Amazon ElastiCache

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

Topics

- Region Availability
- How ElastiCache Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for ElastiCache

Region Availability

Amazon ElastiCache is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How ElastiCache Differs for AWS Top Secret Regions

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

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

Cluster Client	Location	Documentation
Java	http://elasticache-downloads.s3-website.us-iso-east-1.c2s.ic.gov/ClusterClient/Java/AmazonElastiCacheClusterClient.zip	Using Auto Discovery
.NET	http://elasticache-downloads.s3-website.us-iso-east-1.c2s.ic.gov/	Installing the ElastiCache Cluster Client for .NET

Cluster Client	Location	Documentation
	ClusterClient/.NET/Amazon.ElastiCacheCluster.zip	
PHP 7.0	http://elasticache-downloads.s3-website.us-iso-east-1.c2s.ic.gov/ClusterClient/PHP-7.0/latest-64bit	Installing the ElastiCache Cluster Client for PHP
PHP 5.6	http://elasticache-downloads.s3-website.us-iso-east-1.c2s.ic.gov/ClusterClient/PHP-5.6/latest-64bit	Installing the ElastiCache Cluster Client for PHP
PHP 5.5	http://elasticache-downloads.s3-website.us-iso-east-1.c2s.ic.gov/ClusterClient/PHP-5.5/latest-64bit http://elasticache-downloads.s3-website.us-iso-east-1.c2s.ic.gov/ClusterClient/PHP-5.5/latest-32bit	Installing the ElastiCache Cluster Client for PHP
PHP 5.4	http://elasticache-downloads.s3-website.us-iso-east-1.c2s.ic.gov/ClusterClient/PHP-5.4/latest-64bit http://elasticache-downloads.s3-website.us-iso-east-1.c2s.ic.gov/ClusterClient/PHP-5.4/latest-32bit	Installing the ElastiCache Cluster Client for PHP
PHP 5.3	http://elasticache-downloads.s3-website.us-iso-east-1.c2s.ic.gov/ClusterClient/PHP-5.3/latest-64bit http://elasticache-downloads.s3-website.us-iso-east-1.c2s.ic.gov/ClusterClient/PHP-5.3/latest-32bit	Installing the ElastiCache Cluster Client for PHP

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

Instance Family	Instance Types
General purpose	`cache.m3.medium, cache.m3.large, cache.m3.xlarge, cache.m3.2xlarge`
	`cache.m4.large, cache.m4.xlarge, cache.m4.2xlarge, cache.m4.4xlarge, cache.m4.10xlarge`
	`cache.m5.large, cache.m5.xlarge, cache.m5.2xlarge, cache.m5.4xlarge, cache.m5.12xlarge, cache.m5.24xlarge`
	`cache.t3.micro, cache.t3.small, cache.t3.medium`
Memory optimized	`cache.r3.large, cache.r3.xlarge, cache.r3.2xlarge, cache.r3.4xlarge, cache.r3.8xlarge`
	`cache.r4.large, cache.r4.xlarge, cache.r4.2xlarge, cache.r4.4xlarge, cache.r4.8xlarge, cache.r4.16xlarge`
	`cache.r5.large, cache.r5.xlarge, cache.r5.2xlarge, cache.r5.4xlarge, cache.r5.12xlarge, cache.r5.24xlarge`

- Amazon EC2 launches instances into a VPC instead of using the EC2-Classic platform. For more information, see Amazon EC2 and Amazon Virtual Private Cloud (VPC).
- ElastiCache in AWS Top Secret Regions supports upgrades of Redis OSS clusters as of the 5.0.6 release.
- Seeding a New Cluster with an Externally Created Backup includes Canonical S3 IDs. The ID customers need to use for AWS Top Secret Regions is:
  - APA: `44ad3dbcae4632689ffcdce72dd15193b2697a2a2b9ded963e2d529e16276bb9`
  - DCA: `8b26fddf486af8825a9450bdebcf67163f94f8d0388f39bf073513bf959ecf80`
- The following compliance programs are not supported:
  - ElastiCache (Redis OSS) FedRAMP Compliance
  - HIPAA Compliance

- ElastiCache (Redis OSS) PCI DSS Compliance
- TestFailover API is not available in AWS Top Secret Regions
- At-rest encryption is now available in AWS Top Secret Regions. In-transit encryption is not available.
- Global Datastores are not available in AWS Top Secret Regions.
- Data tiering is not available in AWS Top Secret Regions.
- PrivateLink feature is not available in AWS Top Secret Regions.
- Role-Based Access Control (RBAC) is not supported in AWS Top Secret Regions.
- Increase Replica Count feature is not supported in AWS Top Secret Regions for AWS Management Console, AWS CLI, or ElastiCache API. In order to increase the Replica Count, we recommend creating a snapshot of your cluster and using that snapshot to create a new cluster with the desired configuration.
- Redis OSS engine version 6.2 is only available in AWS Top Secret - East.
- Redis OSS engine version 6.0 is not available, but supported Redis OSS engine version 6.2 includes all cumulative updates.
- ElastiCache (Redis OSS) version 7.1 is now supported in the AWS Top Secret - East.
- IAM Authentication is not supported in AWS Top Secret Regions.
- The Valkey 8 engine is not supported in AWS Top Secret Regions.
- You can test automatic failover on up to 5 shards (called node groups in the ElastiCache API and AWS CLI) in any rolling 24-hour period.
- Tagging is not available for Replication Groups.
- Memcached serverless is not available for ADC.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to ElastiCache by using the command line or APIs, use the appropriate endpoint.

Documentation for ElastiCache

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

- Amazon ElastiCache User Guide
- Amazon ElastiCache API Reference

AWS Elemental MediaPackage

AWS Elemental MediaPackage is a just-in-time video packaging and origination service that delivers highly secure, scalable, and reliable video streams to a wide variety of playback devices. MediaPackage enriches audience experience with live and catch-up TV features.

Topics

- Region Availability
- How MediaPackage Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for MediaPackage

Region Availability

AWS Elemental MediaPackage is available in the following AWS Top Secret Regions:

- AWS Top Secret - East

How MediaPackage Differs for AWS Top Secret Regions

The implementation of MediaPackage is different for AWS Top Secret Regions in the following ways:

- Amazon CloudFront distribution creation isn't available.
- Content delivery network (CDN) authorization isn't available.
- Content encryption digital rights management (DRM) isn't available. Encryption options are available in the console and API but will not work if enabled.
- CloudWatch events aren't available.
- Video on demand (VOD) isn't available.
- SPEKE isn't available.
- The MediaPackage VOD API isn't available.
- MediaPackage V2 features aren't available.
- The following Live APIs aren't available:

- CreateOriginEndpoint.Authorization, CreateOriginEndpoint.CmafEncryption, CreateOriginEndpoint.DashEncryption, CreateOriginEndpoint.HLSEncryption, CreateOriginEndpoint.MssEncryption, CreateOriginEndpoint.SpekeKeyProvider, UpdateOriginEndpoint.Authorization, UpdateOriginEndpoint.CmafEncryption, UpdateOriginEndpoint.DashEncryption, UpdateOriginEndpoint.HLSEncryption, UpdateOriginEndpoint.MssEncryption, UpdateOriginEndpoint.SpekeKeyProvider

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to MediaPackage by using the command line or APIs, use the appropriate endpoint.

Documentation for MediaPackage

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

- AWS Elemental MediaPackage User Guide
- AWS Elemental MediaPackage section of AWS CLI Reference
- AWS Elemental MediaPackage API Reference

AWS Elemental MediaLive

AWS Elemental MediaLive is a real-time video service that lets you create live outputs for broadcast and streaming delivery. You use MediaLive to transform live video content from one format and package into other formats and packages. You typically need to transform the content in order to provide a format and package that a playback device can handle. Playback devices include smartphones and set-top boxes attached to televisions.

Topics

- Region Availability
- How MediaLive Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for MediaLive

Region Availability

AWS Elemental MediaLive is available in the following AWS Top Secret Regions:

- AWS Top Secret - East

How MediaLive Differs for AWS Top Secret Regions

The implementation of MediaLive is different for AWS Top Secret Regions in the following ways:

- AWS CloudFormation – You can't create MediaLive templates in AWS CloudFormation.
- CDI inputs – You can't create CDI inputs, even though this type appears in the API and on the console.
- Elemental Link inputs – AWS Elemental Link devices are not supported as inputs. You can't create an Elemental Link input.
- MediaConnect inputs – You can't create MediaConnect inputs, even though this type appears in the API and on the console. However, as soon as AWS Elemental MediaConnect is available in AWS Top Secret Regions, MediaConnect inputs will be supported.
- MediaStore – AWS Elemental MediaStore is not supported as an upstream system for inputs, as a destination for output groups, or as the source for various assets that MediaLive uses.

- Multiplex output groups – You can't create multiplex output groups, even though this type appears in the API and on the console.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to MediaLive by using the command line or APIs, use the appropriate endpoint.

Documentation for MediaLive

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

- AWS Elemental MediaLive User Guide
- AWS Elemental MediaLive API Reference
- MediaLive section of AWS CLI Reference

Amazon EventBridge

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

Topics

- Region Availability
- How Amazon EventBridge Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Amazon EventBridge

Region Availability

Amazon EventBridge is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Amazon EventBridge Differs for AWS Top Secret Regions

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

- API destinations are not supported.
- Archive and replay are not supported.
- AWS CloudFormation support is only available for EventBus, EventBusPolicy and Rule.
- Sending events between event buses in the same account and Region is not supported.
- Encryption using AWS KMS is not supported.
- Managed rules are not supported.
- Setting up partner event sources to receive events from Software-as-a-Service (SaaS) Partner applications and services is not supported.

- Amazon EventBridge Schema Registry is not supported in AWS Top Secret Regions.
- Tags are not supported.
- EventBridge Pipes is not supported.
- The EventBridge Scheduler service is not supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Amazon EventBridge by using the command line or APIs, use the appropriate endpoint.

Documentation for Amazon EventBridge

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

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

Amazon FSx

Amazon FSx makes it easy and cost effective to launch, run, and scale feature-rich, high-performance file systems in the cloud. It supports a wide range of workloads with its reliability, security, scalability, and broad set of capabilities. Amazon FSx is built on the latest AWS compute, networking, and disk technologies to provide high performance and lower TCO. And as a fully managed service, it handles hardware provisioning, patching, and backups — freeing you up to focus on your applications, your end users, and your business.

Topics

- Region Availability
- How Amazon FSx Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Amazon FSx

Region Availability

Amazon FSx is available in the following AWS Top Secret Regions:

- AWS Top Secret - East

How Amazon FSx Differs for AWS Top Secret Regions

The implementation of Amazon FSx is different for AWS Top Secret Regions in the following ways:

- FSx for OpenZFS file systems are not available.
- Features not available for FSx for Lustre file systems:
  - Scratch_1 deployment type
  - Persistent_2 deployment type
  - Interface VPC endpoints powered by AWS PrivateLink
- Features not available for Amazon FSx for NetApp ONTAP file systems:
  - Second-generation file systems (Single-AZ 2 and Multi-AZ 2)
  - The ability to create a Multi-AZ file system in a Shared VPC from a participant account.
- Features not available for FSx for Windows File Server file systems:

- Public IP addresses are not supported. This means that FSx for Windows File Server file systems can only be accessed from peered networks that use IP addresses that are in the CIDR block associated with the VPC.
- Interface VPC endpoints powered by AWS PrivateLink
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

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

To connect to Amazon FSx by using the command line or APIs, use the appropriate endpoint.

Documentation for Amazon FSx

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

- Amazon FSx for Windows File Server User Guide
- Amazon FSx for Lustre User Guide
- Amazon FSx for NetApp ONTAP User Guide
- Amazon FSx API Reference

Amazon S3 Glacier

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

Topics

- Region Availability
- How S3 Glacier Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for S3 Glacier

Region Availability

S3 Glacier is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How S3 Glacier Differs for AWS Top Secret Regions

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

- S3 Glacier Select is not available in AWS Top Secret Regions.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to S3 Glacier by using the command line or APIs, use the appropriate endpoint.

Documentation for S3 Glacier

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

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

AWS Glue

AWS Glue is a fully managed ETL (extract, transform, and load) service that makes it simple and cost-effective to categorize your data, clean it, enrich it, and move it reliably between various data stores. AWS Glue consists of a central data repository known as the AWS Glue Data Catalog, an ETL engine that automatically generates Python code, and a flexible scheduler that handles dependency resolution, job monitoring, and retries. AWS Glue is serverless, so there's no infrastructure to set up or manage. Use the AWS Glue console to discover your data, transform it, and make it available for search and querying. You can also use the AWS Glue API operations to interface with AWS Glue.

Topics

- Region Availability
- How AWS Glue Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for AWS Glue

Region Availability

AWS Glue is available in the following AWS Top Secret Regions:

- AWS Top Secret - East

How AWS Glue Differs for AWS Top Secret Regions

The implementation of AWS Glue is different for AWS Top Secret Regions in the following ways:

- AWS Glue blueprints are not available.
- AWS Glue versions 0.9 and 1.0 are not supported. Customers must use AWS Glue version 2.0 or later.
- AWS Glue 3.0 is now available for AWS Glue and AWS Glue Studio.
- AWS Glue interactive sessions, and AWS Glue dev endpoints and notebooks are not supported. For job development, you must develop your scripts locally and use the CLI/API to run jobs.
- AWS Glue Schema Registry is not available.
- AWS Glue ETL workflows are not available.

- AWS Glue streaming ETL jobs are not available.
- AWS PrivateLink endpoints are not available.
- The following services are not available for integration with AWS Glue:
  - Amazon QuickSight
- Amazon Resource Names (ARNs) and endpoints have different values.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to AWS Glue by using the command line or APIs, use the appropriate endpoint.

Documentation for AWS Glue

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

- AWS Glue Developer Guide (and API reference)
- AWS Glue Command Line Reference

Amazon GuardDuty

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

Topics

- Region Availability
- How Amazon GuardDuty Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Amazon GuardDuty

Region Availability

Amazon GuardDuty is available in the following AWS Top Secret Regions:

- AWS Top Secret - East

How Amazon GuardDuty Differs for AWS Top Secret Regions

The implementation of Amazon GuardDuty is different for AWS Top Secret Regions in the following ways:

- The following retired finding types are supported in the AWS Top Secret Regions:
  - Persistence:IAMUser/NetworkPermissions
  - Persistence:IAMUser/ResourcePermissions
  - Persistence:IAMUser/UserPermissions
  - Recon:IAMUser/NetworkPermissions
  - Recon:IAMUser/ResourcePermissions
  - Recon:IAMUser/UserPermissions
  - ResourceConsumption:IAMUser/ComputeResources
  - Stealth:IAMUser/LoggingConfigurationModified
  - UnauthorizedAccess:IAMUser/ConsoleLogin
  - PrivilegeEscalation:IAMUser/AdministrativePermissions
- The following finding types are not supported in the AWS Top Secret Regions:

  - UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
  - UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS
  - Exfiltration:IAMUser/AnomalousBehavior
  - Impact:IAMUser/AnomalousBehavior
  - CredentialAccess:IAMUser/AnomalousBehavior
  - DefenseEvasion:IAMUser/AnomalousBehavior
  - InitialAccess:IAMUser/AnomalousBehavior
  - Persistence:IAMUser/AnomalousBehavior
  - PrivilegeEscalation:IAMUser/AnomalousBehavior
  - Discovery:IAMUser/AnomalousBehavior
- With the availability of S3 Protection, the following finding types are supported in the AWS Top Secret Regions:
  - Discovery:S3/MaliciousIPCaller
  - Discovery:S3/MaliciousIPCaller.Custom
  - Exfiltration:S3/MaliciousIPCaller
  - Impact:S3/MaliciousIPCaller
  - UnauthorizedAccess:S3/MaliciousIPCaller.Custom
  - UnauthorizedAccess:S3/TorIPCaller
  - Discovery:S3/TorIPCaller
  - PenTest:S3/KaliLinux
  - PenTest:S3/ParrotLinux
  - PenTest:S3/PentooLinux
- GuardDuty EKS Audit Log Monitoring, and its associated finding types and APIs are not supported in AWS Top Secret Regions.
- GuardDuty Runtime Monitoring, and its associated finding types and APIs are not supported in AWS Top Secret Regions.
- GuardDuty Malware Protection for EC2 (both GuardDuty-initiated and On-demand malware scan), and associated finding types and APIs are not supported in AWS Top Secret Regions.
- GuardDuty Malware Protection for S3, and its associated finding types and APIs are not supported in AWS Top Secret Regions.

- GuardDuty RDS Protection, and its associated finding types and APIs are not supported in AWS Top Secret Regions.
- Threat intel (geo location only) is not supported in AWS Top Secret Regions.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

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

To connect to Amazon GuardDuty by using the command line or APIs, use the appropriate endpoint.

Documentation for Amazon GuardDuty

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

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

AWS Health

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

Topics

- Region Availability
- How AWS Health Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for AWS Health

Region Availability

AWS Health is available in the following AWS Top Secret Regions:

- AWS Top Secret - East

How AWS Health Differs for AWS Top Secret Regions

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

- Planned Lifecycle Events doesn't support dynamic resource burndown.
- The organizational view feature is currently not supported.
- You can navigate to the AWS Health Dashboard - Service health page to view the health of all AWS services without signing in to your AWS account.
- If you sign in to your AWS account, you can find events specific to your account and services in the **AWS Health Dashboard - Your account health**.
- AWS Health does not support tagging resources.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to AWS Health by using the command line or APIs, use the appropriate endpoint.

Documentation for AWS Health

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

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

AWS Identity and Access Management

AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources in AWS Top Secret Regions. With IAM, you can create users and groups and grant or deny them permissions to access AWS resources in AWS Top Secret Regions. By using the AWS Security Token Service, you can delegate access across AWS accounts using temporary, limited credentials.

Topics

- Region Availability
- How IAM Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for IAM

Region Availability

AWS Identity and Access Management is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How IAM Differs for AWS Top Secret Regions

The implementation of IAM is different for AWS Top Secret Regions in the following ways:

- There is no concept of a "root" or "account" user or credentials. All AWS Top Secret Regions users are IAM users, including the user who created the account.
- AWS Top Secret Regions does not support adding multi-factor authentication (MFA) to IAM users or to the account. This includes both hardware and virtual MFA devices. The console does not include MFA options.
- For web identity federation, OpenID Connect (OIDC) identity providers (IdPs) Google, Facebook, or Amazon Cognito are not supported as built-in providers in AWS Top Secret Regions.
- There is one IAM control plane for all AWS Top Secret Regions, which is located in the AWS Top Secret - East Region. Each AWS Region has a completely independent instance of the IAM data plane. For more information, see Resilience in AWS Identity and Access Management.

- There is no AWS STS global endpoint in AWS Top Secret Regions. AWS provides Regional AWS STS endpoints.
- You cannot upload and associate an X.509 certification with an individual IAM user. However, you can upload a server certificate to be associated with an account.
- AWS Top Secret Regions supports two additional permissions that can be used in an IAM policy: `iam:GetAccountEmailAddress` and `iam:UpdateAccountEmailAddress`. If you grant a user the `GetAccountEmailAddress` permission, then the user can see the email address associated with the account. If you grant the `UpdateAccountEmailAddress` permission, then the user can change the email address associated with the account. If you grant your administrators permissions by using `iam:*` in a policy, then we recommend that you explicitly deny these two permissions to ensure that users cannot change your main account email address.

  The following shows an example policy that prevents users from changing the account email address:

  ```
  {
    "Version": "2012-10-17",
    "Statement": {
      "Effect": "Deny",
      "Action": "iam:UpdateAccountEmailAddress",
      "Resource": "*"
    }
  }
  ```

- Data about when an IAM entity (user, group, or role) last accessed an AWS service through permissions granted by an IAM policy is not available. For more information, see Service Last Accessed Data.
- Information about when a role was last used is not available. For more information, see View Role Access.
- You cannot use IAM tags to add metadata to the following IAM resources:
  - IAM SAML identity providers
  - Instance profiles
  - OpenID Connect (OIDC) identity providers
  - Policies
  - Server certificates
  - Virtual MFA devices

For more information, see Tagging IAM Resources.

- Only some AWS services support service-linked roles in AWS Top Secret Regions. For information about which services support using service-linked roles, see AWS Services That Work with IAM and look for the services that have **Yes** in the **Service-Linked Role** column. To learn whether the service supports service-linked roles in a specific region, choose the **Yes** link to view the service-linked role documentation for that service.
- The identifier for a service principal includes the service name, and is usually in the following format:

  ```
  service-name.amazonaws.com
  ```

  However, some services might use the following format instead of or in addition to the usual format:

  ```
  service-name.c2s.ic.gov
  ```

- IAM Roles Anywhere is not supported in the AWS Top Secret Regions. To learn more, see Providing access for non AWS workloads in the *IAM User Guide*.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.
- **IAM Access Analyzer**
  - **Policy generation** – Policy generation is not supported in AWS Top Secret Regions. To learn more, see Generate policies based on access activity in the *IAM User Guide*.
  - **Policy validation** – IAM Access Analyzer policy validation checks are not available in AWS Top Secret Regions. For more information, see IAM Access Analyzer policy validation.
- You cannot create AWS PrivateLink interface VPC endpoints for IAM in AWS Top Secret Regions.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to IAM by using the command line or APIs, use the appropriate endpoint.

Documentation for IAM

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

- IAM User Guide
- Using Temporary Security Credentials
- IAM section of AWS CLI Reference
- IAM API Reference
- AWS Security Token Service API Reference

AWS Key Management Service

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

Topics

- Region Availability
- How AWS KMS Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for AWS KMS

Region Availability

AWS Identity and Access Management is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How AWS KMS Differs for AWS Top Secret Regions

The implementation of AWS KMS is different for AWS Top Secret Regions in the following ways:

- Many AWS services integrate with AWS KMS to protect their resources. For information about how AWS services in AWS Top Secret Regions use AWS KMS, see the AWS Top Secret Regions documentation for the AWS service.
- The AWS KMS Custom Key Stores feature is not available in AWS Top Secret Regions. You cannot create AWS CloudHSM key stores or external key stores in AWS Top Secret Regions.
- AWS KMS supports Transport Layer Security (TLS) 1.2—1.3 for endpoints in AWS Top Secret Regions.
- AWS KMS supports Transport Layer Security (TLS) 1.2—1.3 for FIPS endpoints in AWS Top Secret Regions.
- The AWS KMS console feature that lets you filter KMS keys based on their tags is not supported in AWS Top Secret Regions.

- AWS KMS CloudFormation resources are limited in this Region. You cannot use an AWS CloudFormation template to create or manage asymmetric KMS keys, HMAC KMS keys, or multi-Region KMS keys (primary or replica). To use an AWS CloudFormation template to create a symmetric encryption (`SYMMETRIC_DEFAULT`) KMS key, you must specify a key policy.
- AWS KMS does not support the `KeyUsage` value of `KEY_AGREEMENT` for asymmetric keys in AWS Top Secret Regions.
- AWS KMS does not support the DeriveSharedSecret operation in AWS Top Secret Regions.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to AWS KMS by using the command line or APIs, use the appropriate endpoint.

Documentation for AWS KMS

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

- AWS Key Management Service Developer Guide
- AWS Key Management Service API Reference
- AWS KMS section of AWS CLI Reference
- AWS Encryption SDK Developer Guide

Amazon Kinesis Data Streams

Amazon Kinesis Data Streams is a managed service that scales elastically for real-time processing of streaming data at a massive scale. The service collects large streams of data records that can then be consumed in real time by multiple data-processing applications that can be run on Amazon EC2 instances.

Topics

- Region Availability
- How Kinesis Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Kinesis

Region Availability

Amazon Kinesis Data Streams is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Kinesis Differs for AWS Top Secret Regions

The implementation of Kinesis is different for AWS Top Secret Regions in the following ways:

- To help you build Amazon Kinesis Data Streams applications, you can download the following library:
  - Kinesis Client Library - Java
- Kinesis Data Streams On Demand does not support 1 GB/s increase in write capacity and 2GB/s read capacity.
- Kinesis Data Streams does not support Resource Policies.
- Only **Extended data retention** (retention of up to seven days) is supported. **Long-term data retention** (retention of more than seven days and up to 365 days) is not supported.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Kinesis by using the command line or APIs, use the appropriate endpoint.

Documentation for Kinesis

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

- Amazon Kinesis Developer Guide
- Kinesis section of AWS CLI Reference
- Amazon Kinesis API Reference

Amazon Data Firehose

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

Topics

- Region Availability
- How Firehose Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Firehose

Region Availability

Amazon Data Firehose is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Firehose Differs for AWS Top Secret Regions

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

- Dynamic partitioning is NOT supported.
- Snowflake isn't available as a destination.
- Apache Iceberg Tables isn’t available as a destination.
- Splunk isn't available as a destination.
- Third-party HTTP endpoint partners are not available as destinations.
- Writing to Firehose using CloudWatch Logs via subscription filters is not supported.
- Writing to Firehose using CloudWatch Events is not supported.
- Writing to Firehose using AWS IoT is not supported.
- Writing to Firehose using Kinesis Agent is not supported.
- Monitoring Firehose with the following CloudWatch metrics is not supported:
  - BytesPerSecondLimit

- PutRequestsPerSecondLimit
- RecordsPerSecondLimit
- When you are granting access to Amazon Data Firehose while using an Amazon Redshift destination, if your Amazon Redshift cluster is in a virtual private cloud (VPC), make sure to unblock the following Firehose IP addresses in the CIDR for:
  - AWS Top Secret - East: 7.23.112.0/27
  - AWS Top Secret - West: 7.26.175.0/27
- Record format conversion is not available.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Firehose by using the command line or APIs, use the appropriate endpoint.

Documentation for Firehose

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

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

AWS Lambda

AWS Lambda is is a compute service that lets you run code without provisioning or managing servers. Lambda executes your code only when needed and scales automatically, from a few requests per day to thousands per second.

Topics

- Region Availability
- How Lambda Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Lambda

Region Availability

AWS Lambda is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Lambda Differs for AWS Top Secret Regions

The implementation of Lambda is different for AWS Top Secret Regions in the following ways:

- The following event sources are not available in AWS Top Secret Regions:
  - AWS IoT Button
  - Amazon Alexa Skills Kit
  - Amazon Alexa Smart Home
  - Amazon CloudFront
  - AWS CodeCommit
  - For the Amazon S3 event source, the following S3 Glacier event types are not available:
    - Restore from S3 Glacier initiated
    - Restore from S3 Glacier completed
  - Amazon Cognito Sync Trigger
  - Amazon DocumentDB

- The following event source mapping parameters are not available in AWS Top Secret Regions:
  - ScalingConfig
  - TumblingWindowInSeconds
- The FunctionEventInvokeConfig parameter and the `PutFunctionEventInvokeConfig`, `UpdateFunctionEventInvokeConfig`, `DeleteFunctionEventInvokeConfig`, `GetFunctionEventInvokeConfig`, and `ListFunctionEventInvokeConfigs` actions are not available in AWS Top Secret Regions.
- Provisioned concurrency is available in AWS Top Secret Regions, but Application Auto Scaling for provisioned concurrency is not available in AWS Top Secret Regions.
- Lambda does not support batch sizes greater than 10 for Lambda SQS triggers.
- AWS Lambda Function URLs is not available in AWS Top Secret - East or AWS Top Secret - West.
- Lambda support for container image is available in AWS Top Secret Regions but Amazon ECR public gallery is not available in AWS Top Secret Regions.
- Runtime management configuration is not available in AWS Top Secret - East or AWS Top Secret - West.
- Lambda SnapStart is not available in AWS Top Secret Regions.
- The Node.js 20 (`nodejs20.x`) runtime is not available in AWS Top Secret Regions.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.
- Outbound IPv6 traffic is not supported in AWS Top Secret Regions.
- Lambda doesn't support Lambda@Edge in AWS Top Secret Regions.
- The Java 21 (`java21`) runtime is not available in AWS Top Secret Regions.
- Multi-VPC connectivity for Amazon Managed Streaming for Apache Kafka event source mappings is not available in AWS Top Secret Regions.
- The Amazon Linux 2023 (`provided.al2023`) runtime is not available in AWS Top Secret Regions.
- The Python 3.12 (`python3.12`) runtime is not available in AWS Top Secret Regions.
- The Future runtime launch dates are not applicable in AWS Top Secret Regions.
- The Ruby 3.3 (`ruby3.3`) runtime is not available in AWS Top Secret Regions.
- Lambda Kinesis trigger cross-account access is not available in AWS Top Secret Regions.
- The .NET 8 (`dotnet8`) runtime is not yet available in AWS Top Secret Regions. To give customers time to migrate from .NET 6 to .NET 8 after .NET 8 is released, Lambda will continue to

support .NET 6 in AWS Top Secret Regions for at least 6 months after the release of .NET 8. During that time, Lambda will apply patches to the .NET 6 operating system (OS), but not to the .NET 6 language runtime.

- Lambda recursive loop detection is not available in AWS Top Secret Regions.
- The Amazon CloudWatch Logs Live Tail integration in the Lambda console is not available in AWS Top Secret Regions.
- AWS KMS customer managed key encryption for .zip deployment packages is not available in AWS Top Secret Regions.
- The Python 3.13 (`python3.13`) runtime is not available in AWS Top Secret Regions.
- The Node.js 22 (`nodejs22.x`) runtime is not available in AWS Top Secret Regions.
- CloudWatch Application Signals for Lambda functions is not available in AWS Top Secret Regions.
- Event source mapping metrics are not available in AWS Top Secret Regions.
- Provisioned mode for event source mappings is not available in AWS Top Secret Regions.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Lambda by using the command line or APIs, use the appropriate endpoint.

Documentation for Lambda

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

- AWS Lambda Developer Guide
- AWS Lambda section of AWS CLI Reference

AWS License Manager

AWS License Manager is a service for administrators who need a solution for managing, discovering, and reporting software license usage. Administrators can use License Manager to help prevent licensing violations, such as using more licenses than an agreement stipulates.

Topics

- Region Availability for License Manager
- How License Manager Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for License Manager

Region Availability for License Manager

License Manager is available in the following AWS Top Secret Regions Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How License Manager Differs for AWS Top Secret Regions

The implementation of License Manager is different for AWS Top Secret Regions in the following ways:

- Cross-account license management is not supported in AWS Top Secret Regions. This includes license sharing and automated discovery.
- Host resource groups are not supported in AWS Top Secret Regions.
- AWS PrivateLink is not supported in AWS Top Secret Regions.
- Managed entitlements are not supported in AWS Top Secret Regions.
- Report generators are not supported in AWS Top Secret Regions.
- User-based subscriptions are not supported in AWS Top Secret Regions.
- Linux subscriptions are not supported in AWS Top Secret Regions.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to License Manager by using the command line or APIs, use the appropriate endpoint.

Documentation for License Manager

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

- License Manager User Guide
- License Manager API Reference
- License Manager section of AWS CLI Reference

AWS Marketplace

AWS Marketplace is a curated digital catalog that you can use to find, buy, deploy, and manage third-party software that you need to build solutions and run your operations. AWS Marketplace includes many software listings from categories such as security, networking, storage, IoT, business intelligence, database, and DevOps. AWS Marketplace also simplifies software licensing and procurement with flexible pricing options and multiple deployment methods.

Topics

- Region Availability
- How AWS Marketplace Differs for AWS Top Secret Regions
- Documentation for AWS Marketplace

Region Availability

AWS Marketplace is available in the following AWS Top Secret Regions:

- AWS Top Secret - East

How AWS Marketplace Differs for AWS Top Secret Regions

The implementation of AWS Marketplace is different for AWS Top Secret Regions in the following ways:

- AWS Top Secret Regions only supports Amazon Machine Image (AMI) and CloudFormation product types. Container, SaaS, SageMaker, professional services, and data products are not supported.
- The AWS Marketplace console is not available. You can subscribe to products from the AWS Marketplace website. The website is available at https://marketplace.c2shome.ic.gov/, or through the Amazon EC2 console.

  You can manage your existing subscriptions by choosing **Your Marketplace Software** from the AWS Marketplace website.
- Private image builds are not available.
- Private marketplaces are not available.

- Private offers are available. However, private offers must be coordinated with the AWS Marketplace operations team; they are not available in the user interface.
- Procurement system integration is not available.
- Product reviews are not available.
- AWS Marketplace CLI and APIs are not available. However, you can use the Amazon EC2 and AWS CloudFormation CLIs to manipulate resources you subscribe to from AWS Marketplace.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

Documentation for AWS Marketplace

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

- AWS Marketplace Buyer Guide

AWS Modular Data Center Rack

AWS Modular Data Center Rack is a managed service and deployment option that enables customers to deploy devices at scale. With MDC Rack, AWS installs racks of devices at your site based on the form factor selected by you during the ordering process. MDC Rack is a 42U rack, equipped with redundant top of rack switches (ToRs), management switch, management server, up to six devices, and a power shelf including 240/120-volt power distribution and redundant uninterruptible power supply (UPS). MDC Rack includes on-site rack hardware maintenance and AWS network equipment to support an (optional) AWS remotely managed network configuration.

Topics

- How MDC Rack Differs for AWS Top Secret Regions
- Documentation for MDC Rack

How MDC Rack Differs for AWS Top Secret Regions

The implementation of MDC Rack is different for AWS Top Secret Regions in the following ways:

- The AWS services that you can run on depends on service availability in AWS Top Secret Regions compared to other Regions.
- MDC Rack is shipped unclassified and the customer must have an Authority to Connect (ATC) before the rack can be connected to the AWS Top Secret Regions.

Documentation for MDC Rack

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

- MDC Rack User Guide

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 that is optimized for storing billions of relationships and querying the graph with milliseconds latency. Neptune supports the popular property-graph query languages Apache TinkerPop Gremlin and Neo4j's openCypher, as well as the W3C's SPARQL for RDF data.

Topics

- Region Availability
- How Neptune Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Neptune

Region Availability

Amazon Neptune is available in the following AWS Top Secret Regions:

- AWS Top Secret - East

How Neptune Differs for AWS Top Secret Regions

The implementation of Neptune is different for AWS Top Secret Regions in the following ways:

General Differences

- The Neptune workbench Jupyter notebooks are not supported.
- Cross-region replication, such as using DB snapshot copying, is not supported.
- Global databases are not supported.
- Neptune serverless is not supported.
- Graviton instances are not supported.
- Neptune Analytics is not supported.
- I/O-Optimized is not supported.
- The list of available DB instance classes is at Amazon Neptune Pricing.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Neptune by using the command line or APIs, use the appropriate endpoint.

Documentation for Neptune

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

- Neptune User Guide
- Neptune section of AWS CLI Reference

Amazon OpenSearch Service

Amazon OpenSearch Service is a managed service that makes it easy to deploy, operate, and scale OpenSearch and legacy Elasticsearch OSS clusters in the AWS Cloud.

Topics

- Region Availability
- How OpenSearch Service Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for OpenSearch Service

Region Availability

Amazon OpenSearch Service is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How OpenSearch Service Differs for AWS Top Secret Regions

The implementation of OpenSearch Service is different for AWS Top Secret Regions in the following ways:

- The following OpenSearch versions are supported: 1.0, 1.1, 1.2, 1.3, 2.3, 2.5, 2.7, 2.9, 2.11, 2.13
- Fewer instance types are available.
- Amazon Cognito for OpenSearch Dashboards (previously Kibana) is not supported.
- Asynchronous search and Auto-Tune are not available.
- Custom endpoints are not supported.
- Amazon OpenSearch Ingestion is not supported.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to OpenSearch Service by using the command line or APIs, use the appropriate endpoint.

Documentation for OpenSearch Service

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

- Amazon OpenSearch Service Developer Guide
- Amazon OpenSearch Service section of the AWS CLI Reference

AWS Outposts

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

Topics

- Region Availability
- How AWS Outposts Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for AWS Outposts

Region Availability

AWS Outposts is available in the following AWS Top Secret Regions:

- AWS Top Secret - East

How AWS Outposts Differs for AWS Top Secret Regions

The implementation of AWS Outposts is different for AWS Top Secret Regions in the following ways:

- The AWS services that you can run on AWS Outposts depends on service availability in AWS Top Secret Regions compared to other Regions.
- You cannot share Outpost resources through AWS Resource Access Manager or AWS Organizations in AWS Top Secret Regions.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to AWS Outposts by using the command line or APIs, use the appropriate endpoint.

Documentation for AWS Outposts

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

- AWS Outposts User Guide
- AWS Outposts API Reference
- AWS Outposts in the Amazon EC2 API Reference
- AWS Outposts section of AWS CLI Reference

AWS ParallelCluster

AWS ParallelCluster is an AWS supported open source cluster management tool that helps you to deploy and manage high performance computing (HPC) clusters in the AWS Cloud.

Topics

- Region Availability
- How AWS ParallelCluster Differs for AWS Top Secret Regions
- How the pcluster CLI Differs for AWS Top Secret Regions
- Documentation for AWS ParallelCluster

Region Availability

AWS ParallelCluster is available in the following AWS Top Secret Regions:

- AWS Top Secret - East

How AWS ParallelCluster Differs for AWS Top Secret Regions

The implementation of AWS ParallelCluster is different for AWS Top Secret Regions in the following ways:

- AWS ParallelCluster doesn’t support use of the following AWS services and resources:
  - AWS Batch
  - Amazon FSx for NetApp ONTAP
  - Amazon FSx for OpenZFS
  - Amazon File Cache
  - Amazon DCV
  - Amazon EC2 Capacity Blocks for ML
- Amazon FSx for Lustre is supported by AWS ParallelCluster 3.10.1 and newer.
- EC2 Image Builder is supported by AWS ParallelCluster 3.10.1 and newer.
- AWS ParallelCluster versions earlier than version 3.6.1 aren't supported.
- AWS ParallelCluster only supports clusters that use Amazon Linux 2 and Red Hat 8 on x86_64 architecture.

- The AWS ParallelCluster API isn't available.
- The AWS ParallelCluster UI isn't available.
- Attaching security groups on login nodes' network load balancer is not supported. Therefore, the network load balancer of login nodes doesn't have security groups.
- The AWS ParallelCluster AWS CloudFormation custom resource isn't available.
- Only the `gp2` (default), `io1`, `sc1`, and `st1` Amazon Elastic Block Store volume types are available. All other Amazon EBS volume types aren't available. The following example shows `VolumeType` in a cluster configuration where only the supported volume types can be set and where you can set the size for a supported volume:

```
HeadNode:
  LocalStorage:
    RootVolume:
      Size: integer
      VolumeType: string
```

```
SlurmQueues:
  Name:
  ComputeSettings:
    LocalStorage:
      RootVolume:
        Size: integer
        VolumeType: string
```

- The following AWS ParallelCluster configuration properties and options aren’t supported:
  - All Build Image configuration properties and options.
  - Amazon DCV properties and options. The following example shows the `Dcv` setting to exclude from a cluster configuration:

    ```
    Dcv:
      Enabled: boolean
      Port: integer
      AllowedIps: string
    ```

  - All `awsbatch` (AWS Batch) configuration properties and options (Scheduler: awsbatch).
  - All configuration properties and options associated with `FsxOntap`, `FsxOpenZfs`, and `Amazon FileCache` storage types. The following example shows the `StorageType` settings to exclude from a cluster configuration:

```
SharedStorage:
  StorageType: FsxOntap, FsxOpenZfs, FileCache
```

How the pcluster CLI Differs for AWS Top Secret Regions

The implementation of the pcluster CLI is different for AWS Top Secret Regions in the following ways:

- The pcluster CLI can only be installed by using a stand-alone installer.
- The following pcluster command isn't supported:
  - `pcluster dcv-connect`
- The following AWS ParallelCluster configuration properties and options aren't supported for `pcluster configure`, `pcluster create-cluster`, and `pcluster update-cluster`:
  - Amazon DCV properties and options. The following example shows the `Dcv` setting to exclude from a cluster configuration:

    ```
    Dcv:
      Enabled: boolean
      Port: integer
      AllowedIps: string
    ```

  - All `awsbatch` (AWS Batch) configuration properties and options (Scheduler: awsbatch).
  - All configuration properties and options associated with `FsxLustre`, `FsxOntap`, `FsxOpenZfs`, and `Amazon FileCache` storage types. The following example shows the `StorageType` settings to exclude from a cluster configuration:

    ```
    SharedStorage:
      StorageType: FsxLustre, FsxOntap, FsxOpenZfs, FileCache
    ```

Documentation for AWS ParallelCluster

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how AWS ParallelCluster differs for AWS Top Secret Regions, as described in this topic. Also, some features and new functionality described in this

documentation might not be available in the current release of AWS Top Secret Regions. There are other differences, such as links, endpoints, and screen-shots.

- AWS ParallelCluster User Guide

AWS Pricing Calculator

You can use AWS Pricing Calculator to explore AWS services and create an estimate for the cost of your AWS use cases. You can model your solutions before building them, explore the price points and calculations behind your estimate, and find the available instance types and contract terms that meet your needs. This enables you to make informed decisions about using AWS. You can plan your AWS costs and usage or price out setting up a new set of instances and services.

AWS Pricing Calculator is useful both for people who have never used AWS and for those who want to reorganize or expand their AWS usage. You don't need any experience with the cloud or AWS to use AWS Pricing Calculator.

Topics

- Region Availability
- How AWS Pricing Calculator Differs for AWS Top Secret Regions
- Documentation for AWS Pricing Calculator

Region Availability

AWS Pricing Calculator is available in the following AWS Top Secret Regions:

- AWS Top Secret - East

How AWS Pricing Calculator Differs for AWS Top Secret Regions

The implementation of AWS Pricing Calculator is different for AWS Top Secret Regions in the following ways:

- The Windows Server and SQL Server calculator is not available.

Documentation for AWS Pricing Calculator

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

- AWS Pricing Calculator User Guide

Amazon Redshift

Amazon Redshift is a fast, fully managed, petabyte-scale data warehouse service that makes it simple and cost-effective to efficiently analyze all your data using your existing business intelligence tools. It is optimized for datasets ranging from a few hundred gigabytes to a petabyte or more.

Topics

- Region Availability
- How Amazon Redshift Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Amazon Redshift

Region Availability

Amazon Redshift is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Amazon Redshift Differs for AWS Top Secret Regions

The implementation of Amazon Redshift is different for AWS Top Secret Regions in the following ways:

- The following features are not available:
  - Concurrency scaling
  - Redshift-managed VPC endpoints
  - Amazon Redshift scheduler
  - Cross-Region snapshot copy
  - Amazon Redshift Data API
  - Integrating with an AWS Partner
  - Cluster relocation
  - Data sharing

- Amazon Redshift Advisor
- Amazon Redshift query editor
- Zero-ETL integration with DynamoDB and Amazon Redshift is not available.

- RA3.16xlarge and RA3.4xlarge node types are available in AWS Top Secret - West and in AWS Top Secret - East, but not in AWS Top Secret - East (B).
- Amazon Redshift Managed Storage (RMS) is available in AWS Top Secret - West and in AWS Top Secret - East, but not in AWS Top Secret - East (B).
- DC1 instance families are available in AWS Top Secret - East, but not in AWS Top Secret - West.
- All Amazon Redshift clusters must be launched in an Amazon VPC.
- Amazon Redshift Spectrum is available in AWS Top Secret - East but not in AWS Top Secret - West.
- Snapshot copy is not supported.
- If you want Amazon Redshift to write logs to an Amazon S3 bucket, the bucket must have a policy that uses `947364790714` for the Amazon Redshift Account ID. For more information, see Managing Log Files in the *Amazon Redshift Management Guide*.

  The following shows an example of a bucket policy that enables audit logging for AWS Top Secret Regions, where *`BucketName`* is a placeholder for your bucket name:

```
{
    "Statement": [
        {
            "Sid": "Put bucket policy needed for audit logging",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws-iso:iam::947364790714:user/logs"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws-iso:s3:::BucketName/*"
        },
        {
            "Sid": "Get bucket policy needed for audit logging ",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws-iso:iam::947364790714:user/logs"
            },
            "Action": "s3:GetBucketAcl",
```

```
            "Resource": "arn:aws-iso:s3:::BucketName"
        }
    ]
}
```

- To connect to Amazon Redshift with SSL, you must download the public key from https://s3.us-iso-east-1.c2s.ic.gov/redshift-downloads/redshift-ssl-ca-cert.pem. For more information, see Configure Security Options for Connections.
- If you want to set up a JDBC or ODBC connection, you can download and install the appropriate driver from the following locations:

Driver	Driver Location	Documentation
JDBC 4.2-compatible	https://redshift-downloads.s3.us-iso-east-1.c2s.ic.gov/drivers/jdbc/2.1.0.11/redshift-jdbc42-2.1.0.11.jar	Configure a JDBC Connection
ODBC driver on Windows	https://redshift-downloads.s3.us-iso-east-1.c2s.ic.gov/drivers/odbc/2.0.0.1/AmazonRedshiftODBC64-2.0.0.1.msi	Install and Configure the Amazon Redshift ODBC Driver on Microsoft Windows Operating Systems
ODBC driver on Linux	https://redshift-downloads.s3.us-iso-east-1.c2s.ic.gov/drivers/odbc/2.0.0.1/AmazonRedshiftODBC64-2.0.0.1.x86_64.rpm	Install the Amazon Redshift ODBC Driver on Linux Operating Systems
ODBC driver on Mac OS X	https://redshift-downloads.s3.us-iso-east-1.c2s.ic.gov/drivers/odbc/1.4.62.1000/AmazonRedshiftODBC-1.4.62.1000.dmg	Install the Amazon Redshift ODBC Driver on Mac OS X

- If you want to perform the tutorials in the Amazon Redshift documentation, you must download the sample data from the following locations:

Sample Data	Bucket Location	Documentation
Tickit	s3://awssampledbusisoeast1/tickit/	Step 5: Load Sample Data from Amazon S3
Resize	s3://awssampledbusisoeast1/resize/	Step 5: Copy Post-Snapshot Data from the Source to the Target Cluster
Ssbgz	s3://awssampledbusisoeast1/ssbgz/	Step 1: Create a Test Data Set
Load	s3://awssampledbusisoeast1/load/	Step 5: Run the COPY Commands

- You cannot use an on-premises hardware security module (HSM) to generate and manage your Amazon Redshift cluster key. For more information about HSM, see Hardware Security Modules.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Amazon Redshift by using the command line or APIs, use the appropriate endpoint.

Documentation for Amazon Redshift

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Amazon Redshift differs for AWS Top Secret Regions, as

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

- Amazon Redshift Getting Started Guide
- Amazon Redshift Management Guide
- Amazon Redshift Database Developer Guide
- Amazon Redshift section of AWS CLI Reference
- Amazon Redshift API Reference

Amazon Relational Database Service

Amazon Relational Database Service (Amazon RDS) is a service that makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while managing time-consuming database administration tasks.

- The following database engines are supported on Amazon RDS:
  - MySQL
  - MariaDB
  - PostgreSQL
  - Oracle
  - Microsoft SQL Server

Amazon Aurora support is covered separately. For information on Aurora, see Amazon Aurora.

Topics

- Region Availability
- How Amazon RDS Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Amazon RDS

Region Availability

Amazon Relational Database Service is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Amazon RDS Differs for AWS Top Secret Regions

The implementation of Amazon RDS is different for AWS Top Secret Regions in the following ways:

Oracle

- The Bring Your Own License (BYOL) model is the only supported license model for Oracle on Amazon RDS.

MariaDB, MySQL, and PostgreSQL

- RDS Proxy is not available.
- Amazon RDS Extended Support isn't available.

Microsoft SQL Server

- SQL Server Web and Express editions aren't available.
- For SQL Server Enterprise Edition, all supported DB engine versions are available on the db.m5 and db.r5 DB instance classes.
- For SQL Server Standard Edition, all supported DB engine versions are available on the db.m5, db.r5, and db.t3 DB instance classes.
- Native backup and restore is supported for SQL Server, but only full backups and restores. Differential backups and restores, and log restores, aren't supported. Backup compression isn't supported.
- Publishing database logs to Amazon CloudWatch Logs is not supported.
- The SQL Server Analysis Services option is not available.
- The SQL Server Integration Services option is not available.
- The SQL Server Reporting Services option is not available.
- SQL Server on Amazon RDS doesn't support cross-Region features, such as DB snapshot-copying across Regions.
- Read replicas for SQL Server are not supported.
- RDS Proxy is not available.

General Differences

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

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

  For example, to list the supported engine versions for RDS for MySQL, run the following CLI command:

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

- Amazon RDS io2 Block Express storage isn't supported.
- Since AWS Top Secret Regions uses a unique certificate authority (CA), update your DB instances for AWS Top Secret Regions to use the Region-specific certificate identified by `rds-ca-2021` in DescribeCertificates calls as soon as possible. The remaining instructions described in the SSL Certificate Rotation topic are the same, except for the certificate identifier.
- Performance Insights for Amazon RDS isn't supported.
- The list of available DB instance classes is at Amazon RDS Pricing.
- AWS Top Secret Regions uses the following time block from which the default backups windows are assigned.

Region	Time Block
us-iso-east-1	03:00-11:00 UTC
us-iso-west-1	08:00–16:00 UTC

- The AWS service principal for Amazon RDS is `rds.c2s.ic.gov`.
- Amazon EC2 launches instances into a VPC instead of using the EC2-Classic platform. For more information, see Amazon EC2 and Amazon Virtual Private Cloud (VPC).
- Since AWS Top Secret Regions is a VPC-only Region, Amazon RDS DB instances must use existing VPC security groups. Amazon RDS APIs, such as CreateDBSecurityGroup and AWS::RDS::DBSecurityGroup do not apply in AWS Top Secret Regions. Instead, create VPC security groups directly in Amazon EC2 using CreateSecurityGroup.
- Database activity streams aren't supported.
- AWS Top Secret - East Encryption at rest isn't supported for the db.m2 instance class.
- The RDS PostgreSQL S3 import feature is only supported for version 10.11 and later 10 versions, version 11.7 and later 11 versions, and all 12.1 or later versions.
- S3 export isn't supported.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.
- Size-flexible reserved DB instances aren't supported.

- Kerberos authentication is only supported for RDS for MySQL DB instances.
- Kerberos authentication isn't supported in the RDS console.
- Some older minor DB engine versions don't support the latest generation DB instance classes.
- The Blue/Green Deployments feature isn't available.
- The Secrets Manager integration feature isn't available.
- Amazon RDS Custom is not available in AWS Top Secret Regions.
- Copying an option group isn't available.
- Events in the security patching event category aren't available.
- RDS VPC endpoints/PrivateLink are not available.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Amazon RDS by using the command line or APIs, use the appropriate endpoint.

Documentation for Amazon RDS

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

- MySQL on Amazon RDS
- MariaDB on Amazon RDS
- Oracle on Amazon RDS

- PostgreSQL on Amazon RDS
- Microsoft SQL Server on Amazon RDS
- Amazon RDS section of AWS CLI Reference
- Amazon RDS API Reference

AWS Resource Groups

AWS Resource Groups is the service that lets you manage and automate tasks on large numbers of resources at one time.

Topics

- Region Availability
- How Resource Groups Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Resource Groups

Region Availability

AWS Resource Groups is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Resource Groups Differs for AWS Top Secret Regions

The implementation of Resource Groups is different for AWS Top Secret Regions in the following ways:

- Group lifecycle events are not supported.
- Service Quotas are not supported.
- Tag Editor console is not supported.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

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

To connect to Resource Groups by using the command line or APIs, use the appropriate endpoint.

Documentation for Resource Groups

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

- AWS Resource Groups User Guide
- AWS Resource Groups API Reference
- AWS Resource Groups section of the AWS CLI Reference

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) is a service that lets you share resources that you own with any AWS account.

Topics

- Region Availability
- How AWS RAM differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for AWS RAM

Region Availability

AWS Resource Access Manager is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How AWS RAM differs for AWS Top Secret Regions

The implementation of AWS RAM is different for AWS Top Secret Regions in the following ways:

- AWS PrivateLink for AWS RAM is not supported.
- AWS Organizations is currently not available in AWS Top Secret Regions. Therefore, you cannot share resources with an organization or organizational units in AWS Organizations.
- The AWS RAM implementation in AWS Top Secret Regions does not support resource sharing for all services and resource types. To confirm which shareable resource types are supported in AWS Top Secret Regions, do either of the following:
  - Use the `list-resource-types`AWS CLI command.
  - Use the `ListResourceTypes` API action.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

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

- https://ram.us-iso-east-1.c2s.ic.gov

Documentation for AWS RAM

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

- AWS Resource Access Manager User Guide
- AWS RAM section of AWS CLI Reference
- AWS Resource Access Manager API Reference

AWS Resource Groups Tagging API

AWS Resource Groups Tagging API supports attaching tags to your AWS resources. A tag is a label that you assign to an AWS resource. A tag consists of a key and a value, both of which you define. For example, if you have two Amazon EC2 instances, you might assign both a tag with the key name "Environment". But you can set the value of "Environment" to "Testing" for one and to "Production" for the other.

Most AWS resources support tagging. Some resources support tagging only through that service's native tagging operations, and don't yet support this API. See the documentation for an individual service for information about that service's native tagging operations. Tagging can help you organize your resources and enables you to simplify resource management, access management and cost allocation.

Topics

- How AWS Resource Groups Tagging API Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for AWS Resource Groups Tagging API

How AWS Resource Groups Tagging API Differs for AWS Top Secret Regions

The implementation of AWS Resource Groups Tagging API is different for AWS Top Secret Regions in the following ways:

- Tag Editor console is not supported.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to AWS Resource Groups Tagging API by using the command line or APIs, use the appropriate endpoint.

Documentation for AWS Resource Groups Tagging API

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

- AWS Resource Groups Tagging API Reference Guide
- AWS Resource Groups Tagging API section of the AWS CLI Reference

Amazon Route 53

Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed to give developers an extremely reliable and cost effective way to route end users to applications in C2S by translating names like www.example.com into the numeric IP addresses like 192.0.2.1 that computers use to connect to each other. You can also use Route 53 to configure DNS health checks to route traffic to healthy endpoints or to independently monitor the health of your application and its endpoints.

Topics

- Region Availability
- How Route 53 Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Route 53

Region Availability

Amazon Route 53 is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Route 53 Differs for AWS Top Secret Regions

The implementation of Route 53 is different for AWS Top Secret Regions in the following ways:

- The AWS console for Route 53 is supported, with the following exceptions:
  - The dashboard is not included.
  - The domain registration console is not included.
  - The traffic flow console is not included.
  - The updated health checks console is not included.
- Registering domain names is not supported.
- DNSSEC is not supported.
- Traffic Flow is not supported.

- Route 53 Resolver Firewall is not supported.
- Route 53 alias records are supported as follows:
  - You can alias to another record in the same hosted zone.
  - You can alias to Elastic Load Balancing load balancers.
  - You can alias to a Network Load Balancer.
  - You can alias to a VPC endpoint.
  - You can alias to an Amazon API Gateway endpoint.
  - You can't alias to other AWS resources, such as S3 buckets.
- You can't create records that use geolocation, geoproximity, latency, or IP-based routing policies. This applies both to public and private hosted zones.
- DNS query logging is not supported.
- IPv6 endpoint types are not supported.
- Resolver query logging is not supported.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.
- AWS-managed prefix lists are not available.
- Route 53 Profiles are not available.
- Service Name Indication (SNI) support in DoH outbound endpoints is not supported.
- DNS record types HTTPS, SSHFP, SVCB, and TLSA are not available.

Health Checking

- Latency-based health checks are not supported. This feature is controlled by the **Evaluate target health** field.
- These IP address ranges are used by Route 53 health checkers in AWS Top Secret Regions. Add these ranges to the list of allowed IP address ranges if you're using Route 53 health checks to check the health of resources on your network:

  IPv4:

  - 140.64.202.0/25
  - 140.64.202.128/25
  - 140.64.203.0/25

IPv6:

- 2600:1f19:3cc:cc00::/56
- 2600:1f19:3cc:cd00::/56
- 2600:1f19:3cc:ce00::/56

Name servers

- These IP address ranges are used by Route 53 name servers in AWS Top Secret Regions. Add these ranges to the list of allowed IP address ranges if you're using R53; as the DNS service for one or more domains and you want to be able to use the `dig` or `nslookup` commands to query Route 53 name servers:
  - 140.66.8.0/23
  - 140.66.10.0/23
  - 140.66.12.0/23
  - 140.66.14.0/23

How Command Line and API Access Differs for AWS Top Secret Regions

You can use the AWS Command Line Interface (AWS CLI) to interact with Route 53 and other AWS services through the command line. For more information, see AWS CLI.

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

To connect to Route 53 by using the command line or APIs, use the following endpoint:

- https://route53.c2s.ic.gov

If you're using the AWS CLI to access Route 53, include the `region` parameter, for example:

```
$ aws route53 list-hosted-zones --region us-iso-east-1 --endpoint-url
https://route53.c2s.ic.gov
```

You can omit the `region` parameter from CLI commands if you specify the default region name in your config file:

`region = us-iso-east-1` for AWS Top Secret - East

`region = us-iso-west-1` for AWS Top Secret - West

In addition, if you have the latest version of the AWS CLI, you can omit the `endpoint-url` parameter.

Use the same region name for the Route 53 Resolver hosted zones that are served in the us-iso-west-1 Region.

Documentation for Route 53

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how Route 53 differs for AWS Top Secret Regions, as described in this topic. Also, some features and new functionality described in this documentation might not be available in the current release of AWS Top Secret Regions. There are other differences, such as links, endpoints, and screenshots.

- Amazon Route 53 Developer Guide
- Amazon Route 53 API Reference
- Route 53 section of AWS CLI Reference
- Route 53 Resolver section of AWS CLI Reference

Amazon Application Recovery Controller (ARC)

Amazon Application Recovery Controller (ARC) (ARC) provides three distinct capabilities: *readiness checks*, *routing controls*, and *zonal shifts*. With ARC, you can gain insights into whether your applications and resources are prepared for recovery, and quickly mitigate impairments for a multi-Availability Zone or multi-Region application. ARC helps you prepare for and accomplish faster recovery operations for applications running on AWS.

Zonal shift and zonal autoshift in ARC are available in the following AWS Top Secret Regions. Zonal shift helps you manage and coordinate recovery for AWS applications. You start a zonal shift to move load balancer traffic away from an Availability Zone (AZ) when you detect an issue. Temporarily moving traffic for a resource away from an impaired AZ helps your application recover quickly, minimizing impact for your customers. With zonal autoshift, you authorize AWS to shift away resource traffic for an application from a potentially impaired Availability Zone during events, on your behalf, to help reduce time to recovery.

Topics

- Region Availability
- How ARC Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for ARC

Region Availability

Amazon Application Recovery Controller (ARC) is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How ARC Differs for AWS Top Secret Regions

The implementation of ARC is different for AWS Top Secret Regions in the following ways:

- The routing control and readiness check capabilities of the ARC service are not available in the AWS Top Secret Regions.

- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

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

To connect to ARC by using the command line or APIs, use the appropriate endpoint.

Documentation for ARC

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

- Amazon Application Recovery Controller (ARC) Developer Guide
- Zonal Shift and Zonal Autoshift API Reference Guide for Amazon Application Recovery Controller (ARC)

Amazon SageMaker

SageMaker is an AWS service that enables developers to build, train, and deploy machine learning models in a managed environment.

Topics

- Region Availability
- How SageMaker Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for SageMaker

Region Availability

Amazon SageMaker is available in the following AWS Top Secret Regions:

- AWS Top Secret - East

How SageMaker Differs for AWS Top Secret Regions

The implementation of SageMaker is different for AWS Top Secret Regions in the following ways:

- Only the following features are available in the AWS Top Secret Regions.
  - Notebook instances – Only example notebooks that are confirmed to work in AWS Top Secret - East are available through the notebook instances. JupyterLab 4 is not currently supported for notebook instances in AWS Top Secret - East.
  - Training – Fast file input mode is not supported.
  - Model tuning (HPO)
  - Hosting – The following endpoint parameters for large model inference are not supported:
    - VolumeSizeInGB
    - ContainerStartupHealthCheckTimeoutInSeconds
    - ModelDataDownloadTimeoutInSeconds
    - Asynchronous Inference
    - Serverless Inference
  - Batch transform

- SageMaker Neo – PyTorch version 1.12 and TensorFlow version 2.9 are only supported for CPU instance types ml_c4, ml_c5, ml_m4, and ml_m5.
- SageMaker Ground Truth – The following features are not supported:
  - Amazon Mechanical Turk workforce.
  - The automated segmentation (auto-segmentation) tool is not included when you create an image semantic segmentation labeling job.
  - Amazon CloudWatch Logs. CloudWatch Logs logs for labeling jobs do not include worker metrics.
- SageMaker Search – Search does not return results for SageMaker features that are not available in AWS Top Secret - East.
- SageMaker Processing
- Internet Explorer is not supported on the SageMaker Console
- For the Docker registry path and other parameters for each of the SageMaker provided algorithms and Deep Learning Containers (DLC), see Docker Registry Paths and Example Code for US ISO East (us-iso-east-1).
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to SageMaker by using the command line or APIs, use the appropriate endpoint.

Documentation for SageMaker

The following documentation is based on the public AWS documentation. As you read this documentation, you should consider how SageMaker differs for AWS Top Secret Regions, as

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

- Amazon SageMaker Developer Guide
- SageMaker API Reference
- SageMaker section of AWS CLI Reference

AWS Serverless Application Model

The AWS Serverless Application Model (AWS SAM) is an open-source framework that enables you to build serverless applications on AWS. It provides you with a template specification to define your serverless application, and a command line interface (CLI) tool.

Topics

- Region Availability
- How AWS SAM Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for AWS SAM

Region Availability

AWS Serverless Application Model is available in the following AWS Top Secret Regions:

- AWS Top Secret - East

How AWS SAM Differs for AWS Top Secret Regions

The implementation of AWS SAM is different for AWS Top Secret Regions in the following ways:

- The installation links for the AWS SAM CLI are not directly available to hosts in the region. You must manually copy the AWS SAM CLI installation files to a host in the region in order to install the AWS SAM CLI.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

Documentation for AWS SAM

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

- AWS Serverless Application Model Developer Guide
- AWS SAM Specification

AWS Secrets Manager

AWS provides the service AWS Secrets Manager for easier management of secrets. *Secrets* can be database credentials, passwords, third-party API keys, and even arbitrary text. You can store and control access to these secrets centrally by using the Secrets Manager console, the Secrets Manager command line interface (CLI), or the Secrets Manager API and SDKs.

Topics

- Region Availability
- How Secrets Manager Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Secrets Manager

Region Availability

AWS Secrets Manager is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Secrets Manager Differs for AWS Top Secret Regions

The implementation of Secrets Manager is different for AWS Top Secret Regions in the following ways:

- Multi-Region secrets are not supported.
- AAAA IPv6 records for the Secrets Manager endpoint are not supported.
- The PrivateLink VPC Endpoint service name is `com.amazonaws.<region string>.secretsmanager`
- FIPS endpoints are not supported.
- Secret Rotation in the console for Amazon DocumentDB credentials is not supported.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.
- AWS Config managed rules for Secrets Manager are not supported.

- Secrets Manager API BatchGetSecretValue is not supported.
- For the AWS CloudFormation resource `AWS::SecretsManager::Secret`, the return value `GetAtt` is not supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Secrets Manager by using the command line or APIs, use the appropriate endpoint.

Documentation for Secrets Manager

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

- AWS Secrets Manager User Guide
- AWS Secrets Manager API Reference
- Secrets Manager section of AWS CLI Reference

AWS Security Hub

AWS Security Hub (Security Hub) is an AWS service that provides you with a comprehensive view of your security state in AWS and helps you assess your AWS environment against security industry standards and best practices.

Security Hub collects security data across AWS accounts, integrated AWS services, and supported third-party products and helps you analyze your security trends and identify the highest priority security issues.

To help you manage your security state, Security Hub supports multiple security standards, such as AWS Foundational Security Best Practices, Center for Internet Security (CIS) AWS Foundations Benchmark, and Payment Card Industry Data Security Standard (PCI DSS). Each standard includes several security controls, each of which represents a security best practice. Security Hub runs checks against security controls and generates control findings to help you assess your compliance against security best practices.

Security Hub also offers automation rules and an integration with Amazon EventBridge to help you triage and remediate security issues.

Topics

- How Security Hub Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Security Hub

How Security Hub Differs for AWS Top Secret Regions

The implementation of Security Hub is different for AWS Top Secret Regions in the following ways:

- The integration between Security Hub and AWS Organizations isn't available. Features that depends on this integration, including central configuration, aren't available.
- The AWS Resource Tagging Standard and the controls that apply exclusively to this standard aren't available.
- To receive Security Hub announcements through Amazon Simple Notification Service (Amazon SNS), use the following SNS topic ARNs:
  - **AWS Top Secret – East**: `arn:aws-iso:sns:us-iso-east-1:338285027051:SecurityHubAnnouncements`

- **AWS Top Secret – West**: `arn:aws-iso:sns:us-iso-west-1:309110848755:SecurityHubAnnouncements`
- Some security controls aren't available in AWS Top Secret Regions. A control is available in a specific AWS Region only if it appears on the Security Hub console when you're signed in to that Region. Programmatically, you can use the ListSecurityControlDefinitions operation of the Security Hub API, specifically the `CurrentRegionAvailability` parameter, to see if a control is available in the current Region. For a complete list of Security Hub controls across Regions, see Security Hub controls reference.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Security Hub by using the command line or APIs, use the appropriate endpoint.

Documentation for Security Hub

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

- AWS Security Hub User Guide
- AWS Security Hub API Reference
- Security Hub section of AWS CLI Reference

Amazon Simple Storage Service

Amazon Simple Storage Service (Amazon S3) is storage for the cloud. It provides a simple web service interface you can use to store and retrieve any amount of data, at any time, from anywhere on the network. It gives any developer access to the same highly scalable, reliable, secure, fast, inexpensive infrastructure solution that Amazon uses in its public cloud.

Topics

- Region Availability
- How Amazon S3 Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Amazon S3

Region Availability

Amazon Simple Storage Service is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Amazon S3 Differs for AWS Top Secret Regions

The implementation of Amazon S3 is different for AWS Top Secret Regions in the following ways:

- When you upload or copy an object to Amazon S3, your data is automatically encrypted.

> **Note**
>
> Objects created before 7/15/2014 without server-side encryption remain unencrypted. If you want to encrypt these objects, use the PUT (Copy Object) operation, set the destination object to be the same as the source object, and specify the option to preserve all metadata.
>
> If you are using versioned buckets and you want only encrypted content to be stored in Amazon S3, you must delete the unencrypted version by version ID. If you have several unencrypted old versions, you could apply a noncurrent version expiration rule. For more information, see Object Versioning and Object Expiration.

- Objects are encrypted using one of the following encryption types:
  - Server-side encryption with Amazon S3-managed encryption keys (SSE-S3)
  - Server-side encryption with AWS KMS encryption keys (SSE-KMS)
  - Server-side encryption with customer-provided encryption keys (SSE-C)
  - Dual-layer server-side encryption with AWS KMS encryption keys (DSSE-KMS)
- You can configure your Amazon S3 buckets to use SSE-S3, SSE-KMS, or DSSE-KMS for automatic encryption. Automatic encryption (also referred to as default encryption) is only used if the incoming object storage request does not specify an encryption method. If your bucket is not configured for default encryption, Amazon S3 encrypts incoming objects using SSE-S3.
- When you upload or copy an object to Amazon S3 the encryption type that is selected depends on the following factors:

Operation	Server-Side Encryption
Upload an object to Amazon S3 without specifying the SSE-S3, SSE-KMS, DSSE-KMS, or SSE-C options.	If the bucket is configured for default encryption, the object is encrypted as per the bucket configuration (SSE-S3, SSE-KMS, DSSE-KMS). Otherwise, the object is encrypted with SSE-S3.
Upload an object to Amazon S3 and specify SSE-SS3 option.	The object is encrypted with SSE-S3.
Upload an object to Amazon S3 and specify the SSE-KMS option.	The object is encrypted with SSE-KMS.
Upload an object to Amazon S3 and specify the DSSE-KMS option.	The object is encrypted with DSSE-KMS.
Upload an object to Amazon S3 and specify the SSE-C option.	The object is encrypted with SSE-C.
Copy an object within Amazon S3 and attempt to change an SSE-S3, SSE-KMS, DSSE-KMS, or SSE-C protected object to use no encryption.	The object is copied and if the bucket is configured for default encryption, the object is encrypted as per the bucket configuration

Operation	Server-Side Encryption
	(SSE-S3, SSE-KMS, or DSSE-KMS). Otherwise, the object is encrypted with SSE-S3.
Copy an object within Amazon S3 and attempt to change from SSE-S3, SSE-KMS, DSSE-KMS, or SSE-C encryption to SSE-S3, SSE-KMS, DSSE-KMS, or SSE-C encryption.	The object is copied using the requested encryption type.

- Object copy operations are permitted within AWS Top Secret Regions, and cross-region copy operations are supported between AWS Top Secret - East and AWS Top Secret - West. For more information, see Copying Objects.
- Amazon S3 objects are associated with the following storage classes:
  - DEEP_ARCHIVE
  - GLACIER
  - GLACIER_IR
  - INTELLIGENT_TIERING
  - ONEZONE_IA
  - STANDARD
  - STANDARD_IA

  For more information, see Storage Classes.
- Objects restored from the Amazon S3 GLACIER storage class are billed at the STANDARD storage rates, not RRS.
- If you are using Amazon S3 event notifications, the Reduced Redundancy Storage (RRS) object lost event is not available. For more information, see Configuring Amazon S3 Event Notifications.
- Static website hosting using Amazon S3 is available to users in AWS Top Secret Regions. The special case of apex domain website hosting is unsupported because it requires the Route 53 service, which is not available in AWS Top Secret Regions. For more information about static website hosting, see Hosting a Static Website on Amazon S3.
- The AWS Import/Export service is not available.
- Amazon S3 Transfer Acceleration is not available in AWS Top Secret Regions.
- Amazon CloudFront is not available in AWS Top Secret Regions, so content distribution techniques using CloudFront are not available in Amazon S3.

- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.
- Amazon S3 Storage Lens is not available in AWS Top Secret Regions.
- AWS PrivateLink for Amazon S3 is not available in AWS Top Secret Regions.
- Amazon S3 Object Lambda Access Points are not available in AWS Top Secret Regions.
- Amazon S3 does not support notifications for the event type of `S3 Intelligent-Tiering automatic archival events` in AWS Top Secret - West and AWS Top Secret - East.
- Sending AWS X-Ray trace headers through Amazon S3 in event notifications is not supported in AWS Top Secret - West and AWS Top Secret - East.
- Amazon S3 does not support S3 Intelligent-Tiering archive access Tiers (Archive Access tier and Deep Archive Access tier) in AWS Top Secret Regions.
- In AWS Top Secret Regions, Amazon S3 Inventory does not have the Object Access Control List and Object Owner as available object metadata fields in inventory reports.
- Amazon S3 Access Grants is not available in AWS Top Secret - West and AWS Top Secret - East.
- Amazon S3 Express One Zone is not available in AWS Top Secret Regions.
- Amazon S3 does not support Dualstack or FIPS Dualstack service endpoints in AWS Top Secret Regions.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Amazon S3 by using the command line or APIs, use the appropriate endpoint.

Documentation for Amazon S3

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

- Amazon Simple Storage Service User Guide
- Amazon S3 section of AWS CLI Reference
- Amazon Simple Storage Service API Reference

Amazon Simple Notification Service

Amazon Simple Notification Service (Amazon SNS) is a fast, flexible, fully managed push messaging service. Amazon SNS makes it simple and cost-effective to push to distributed services such as Amazon SQS queues and Lambdas, deliver notifications by email, or deliver to endpoints such as HTTP(S) in AWS Top Secret Regions.

Topics

- Region Availability
- How Amazon SNS Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Amazon SNS

Region Availability

Amazon Simple Notification Service is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Amazon SNS Differs for AWS Top Secret Regions

The implementation of Amazon SNS is different for AWS Top Secret Regions in the following ways:

- Since AWS Top Secret Regions operates as an air-gapped region, Amazon SNS cannot communicate to endpoints outside of the region.
- In AWS Top Secret Regions, Amazon SNS does not support SMS or mobile push notifications.
- Amazon SNS signs all notification deliveries using a private-public key pair based on certificates. The public key is available at https://sns.us-iso-east-1.c2s.ic.gov/SimpleNotificationService.pem.
- If you subscribe an HTTPS endpoint to a topic, that endpoint must have a server certificate signed by a trusted certificate authority (CA). Amazon SNS will deliver messages only to HTTPS endpoints that have a signed certificate from a trusted CA recognized by Amazon SNS. For a list of CAs, see Certificate Authorities (CA) Recognized by Amazon SNS for HTTPS in AWS Top Secret Regions. For more information, see Sending Messages to HTTP/HTTPS Endpoints.
- In AWS Top Secret Regions, Amazon SNS does not support Firehose delivery stream endpoints.

- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.
- Message Data Protection is not supported.
- Active tracing is not supported.
- Custom data identifiers are not supported.

Publishing a message from a VPC

To publish to an Amazon SNS topic in AWS Top Secret Regions, you need to use a different AWS CloudFormation template than described in Publishing an Amazon SNS message from Amazon VPC in the *Amazon Simple Notification Service Developer Guide*. Rather than download an AWS CloudFormation template from GitHub, copy and paste the following template into a text-only file, and then upload it to AWS CloudFormation:

```
AWSTemplateFormatVersion: 2010-09-09
 Description: CloudFormation Template for SNS VPC Endpoints Tutorial
 Parameters:
   KeyName:
     Description: Name of an existing EC2 KeyPair to enable SSH access to the instance
     Type: 'AWS::EC2::KeyPair::KeyName'
     ConstraintDescription: must be the name of an existing EC2 KeyPair.
   SSHLocation:
     Description: The IP address range that can be used to SSH to the EC2 instance
     Type: String
     MinLength: '9'
     MaxLength: '18'
     Default: 0.0.0.0/0
     AllowedPattern: '(\d{1,3})\.(\d{1,3})\.(\d{1,3})\.(\d{1,3})/(\d{1,2})'
     ConstraintDescription: must be a valid IP CIDR range of the form x.x.x.x/x.
 Mappings:
   RegionMap:
     us-east-1:
       AMI: ami-428aa838
     us-east-2:
       AMI: ami-710e2414
     us-west-1:
       AMI: ami-4a787a2a
     us-west-2:
       AMI: ami-7f43f307
     ap-northeast-1:
```

```
        AMI: ami-c2680fa4
      ap-northeast-2:
        AMI: ami-3e04a450
      ap-southeast-1:
        AMI: ami-4f89f533
      ap-southeast-2:
        AMI: ami-38708c5a
      ap-south-1:
        AMI: ami-3b2f7954
      ca-central-1:
        AMI: ami-7549cc11
      eu-central-1:
        AMI: ami-1b2bb774
      eu-west-1:
        AMI: ami-db1688a2
      eu-west-2:
        AMI: ami-6d263d09
      eu-west-3:
        AMI: ami-5ce55321
      sa-east-1:
        AMI: ami-f1337e9d
      us-isob-east-1:
        AMI: ami-02e97847c224981ce
      us-iso-east-1:
        AMI: ami-e76a5e8a
  Resources:
    VPC:
      Type: 'AWS::EC2::VPC'
      Properties:
        CidrBlock: 10.0.0.0/16
        EnableDnsSupport: 'true'
        EnableDnsHostnames: 'true'
        Tags:
          - Key: Name
            Value: VPCE-Tutorial-VPC
    Subnet:
      Type: 'AWS::EC2::Subnet'
      Properties:
        VpcId: !Ref VPC
        CidrBlock: 10.0.0.0/24
        Tags:
          - Key: Name
            Value: VPCE-Tutorial-Subnet
    InternetGateway:
```

```
      Type: 'AWS::EC2::InternetGateway'
      Properties:
        Tags:
          - Key: Name
            Value: VPCE-Tutorial-InternetGateway
    VPCGatewayAttachment:
      Type: 'AWS::EC2::VPCGatewayAttachment'
      Properties:
        VpcId: !Ref VPC
        InternetGatewayId: !Ref InternetGateway
    RouteTable:
      Type: 'AWS::EC2::RouteTable'
      Properties:
        VpcId: !Ref VPC
        Tags:
          - Key: Name
            Value: VPCE-Tutorial-RouteTable
    SubnetRouteTableAssociation:
      Type: 'AWS::EC2::SubnetRouteTableAssociation'
      Properties:
        RouteTableId: !Ref RouteTable
        SubnetId: !Ref Subnet
    InternetGatewayRoute:
      Type: 'AWS::EC2::Route'
      Properties:
        RouteTableId: !Ref RouteTable
        GatewayId: !Ref InternetGateway
        DestinationCidrBlock: 0.0.0.0/0
    SecurityGroup:
      Type: 'AWS::EC2::SecurityGroup'
      Properties:
        GroupName: Tutorial Security Group
        GroupDescription: Security group for SNS VPC endpoing tutorial
        VpcId: !Ref VPC
        SecurityGroupIngress:
          - IpProtocol: '-1'
            CidrIp: 10.0.0.0/16
          - IpProtocol: tcp
            FromPort: '22'
            ToPort: '22'
            CidrIp: !Ref SSHLocation
        SecurityGroupEgress:
          - IpProtocol: '-1'
            CidrIp: 10.0.0.0/16
```

```
      Tags:
        - Key: Name
          Value: VPCE-Tutorial-SecurityGroup
  EC2Instance:
    Type: 'AWS::EC2::Instance'
    Properties:
      KeyName: !Ref KeyName
      InstanceType: t2.micro
      ImageId: !FindInMap
        - RegionMap
        - !Ref 'AWS::Region'
        - AMI
      NetworkInterfaces:
        - AssociatePublicIpAddress: 'true'
          DeviceIndex: '0'
          GroupSet:
            - !Ref SecurityGroup
          SubnetId: !Ref Subnet
      IamInstanceProfile: !Ref EC2InstanceProfile
      Tags:
        - Key: Name
          Value: VPCE-Tutorial-EC2Instance
  EC2InstanceProfile:
    Type: 'AWS::IAM::InstanceProfile'
    Properties:
      Roles:
        - !Ref EC2InstanceRole
      InstanceProfileName: EC2InstanceProfile
  EC2InstanceRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: VPCE-Tutorial-EC2InstanceRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: ec2.amazonaws.com
            Action: 'sts:AssumeRole'
      ManagedPolicyArns:
        - 'arn:aws-iso-b:iam::aws:policy/AmazonSNSFullAccess'
  LambdaExecutionRole:
    Type: 'AWS::IAM::Role'
    Properties:
```

```
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
        - Effect: Allow
          Principal:
            Service: lambda.amazonaws.com
          Action: 'sts:AssumeRole'
      ManagedPolicyArns:
        - 'arn:aws-iso-b:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole'
  LambdaFunction1:
    Type: 'AWS::Lambda::Function'
    Properties:
      Code:
        ZipFile: |
          from __future__ import print_function
          print('Loading function')
          def lambda_handler(event, context):
            message = event['Records'][0]['Sns']['Message']
            print("From SNS: " + message)
            return message
      Description: SNS VPC endpoint tutorial lambda function 1
      FunctionName: VPCE-Tutorial-Lambda-1
      Handler: index.lambda_handler
      Role: !GetAtt
        - LambdaExecutionRole
        - Arn
      Runtime: python2.7
      Timeout: '3'
  LambdaPermission1:
    Type: 'AWS::Lambda::Permission'
    Properties:
      Action: 'lambda:InvokeFunction'
      FunctionName: !Ref LambdaFunction1
      Principal: sns.amazonaws.com
      SourceArn: !Ref SNSTopic
  LambdaLogGroup1:
    Type: 'AWS::Logs::LogGroup'
    Properties:
      LogGroupName: !Sub "/aws/lambda/${LambdaFunction1}"
      RetentionInDays: '7'
  LambdaFunction2:
    Type: 'AWS::Lambda::Function'
    Properties:
      Code:
```

```
        ZipFile: |
          from __future__ import print_function
          print('Loading function')
          def lambda_handler(event, context):
            message = event['Records'][0]['Sns']['Message']
            print("From SNS: " + message)
            return message
      Description: SNS VPC endpoint tutorial lambda function 2
      FunctionName: VPCE-Tutorial-Lambda-2
      Handler: index.lambda_handler
      Role: !GetAtt
        - LambdaExecutionRole
        - Arn
      Runtime: python2.7
      Timeout: '3'
  LambdaPermission2:
    Type: 'AWS::Lambda::Permission'
    Properties:
      Action: 'lambda:InvokeFunction'
      FunctionName: !Ref LambdaFunction2
      Principal: sns.amazonaws.com
      SourceArn: !Ref SNSTopic
  LambdaLogGroup2:
    Type: 'AWS::Logs::LogGroup'
    Properties:
      LogGroupName: !Sub "/aws/lambda/${LambdaFunction2}"
      RetentionInDays: '7'
  SNSTopic:
    Type: 'AWS::SNS::Topic'
    Properties:
      DisplayName: VPCE-Tutorial-Topic
      TopicName: VPCE-Tutorial-Topic
      Subscription:
        - Endpoint: !GetAtt
            - LambdaFunction1
            - Arn
          Protocol: lambda
        - Endpoint: !GetAtt
            - LambdaFunction2
            - Arn
          Protocol: lambda
```

To use this template, follow the Publishing an Amazon SNS message from Amazon VPC, but change the first few steps under "Step 2: Create the AWS resources" to the following:

1. Sign in to the AWS CloudFormation Console.
2. Choose **Create stack**.
3. Under **Specify template**, choose **Upload a template file** and choose the text-only file where you saved the above template.
4. Choose **Next** and then resume following the standard procedure at step 5, where you specify stack details.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Amazon SNS by using the command line or APIs, use the appropriate endpoint.

Documentation for Amazon SNS

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

- Amazon Simple Notification Service Developer Guide
- Amazon SNS section of AWS CLI Reference
- Amazon Simple Notification Service API Reference

Amazon Simple Queue Service

Amazon Simple Queue Service (Amazon SQS) offers a secure, durable, and available hosted queue that lets you integrate and decouple distributed software systems and components. Amazon SQS offers common constructs such as dead-letter queues and cost allocation tags. It provides a generic web services API and it can be accessed by any programming language that the AWS SDK supports.

Topics

- Region Availability
- How Amazon SQS Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Amazon SQS

Region Availability

Amazon Simple Queue Service is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Amazon SQS Differs for AWS Top Secret Regions

The implementation of Amazon SQS is different for AWS Top Secret Regions in the following ways:

- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.
- AWS JSON protocol is not supported.
- Amazon SQS Extended Client Library for Python is not supported.

Publishing a message from a VPC

To send messages to an Amazon SQS queue in AWS Top Secret Regions, you need to use a different AWS CloudFormation template than described in Tutorial: Sending a message to an Amazon SQS queue from Amazon Virtual Private Cloud in the *Amazon Simple Queue Service Developer*

Guide. Rather than download an AWS CloudFormation template from GitHub, copy and paste the following template into a text-only file, and then upload it to AWS CloudFormation:

```
     AWSTemplateFormatVersion: 2010-09-09
     Description: CloudFormation Template for SQS VPC Endpoints Tutorial
     Parameters:
       KeyName:
         Description: Name of an existing EC2 KeyPair to enable SSH access to the
instance
         Type: "AWS::EC2::KeyPair::KeyName"
         ConstraintDescription: must be the name of an existing EC2 KeyPair.
       SSHLocation:
         Description: The IP address range that can be used to SSH to the EC2 instance
         Type: String
         MinLength: "9"
         MaxLength: "18"
         Default: 0.0.0.0/0
         AllowedPattern: '(\d{1,3})\.(\d{1,3})\.(\d{1,3})\.(\d{1,3})/(\d{1,2})'
         ConstraintDescription: must be a valid IP CIDR range of the form x.x.x.x/x.
     Mappings:
       RegionMap:
         us-iso-east-1:
           AMI: ami-0c49b61b
         us-iso-west-1:
           AMI: ami-0738591627169197f
     Resources:
       VPC:
         Type: "AWS::EC2::VPC"
         Properties:
           CidrBlock: 10.0.0.0/16
           EnableDnsSupport: "true"
           EnableDnsHostnames: "true"
           Tags:
             - Key: Name
               Value: SQS-VPCE-Tutorial-VPC
       Subnet:
         Type: "AWS::EC2::Subnet"
         Properties:
           VpcId: !Ref VPC
           CidrBlock: 10.0.0.0/24
           Tags:
             - Key: Name
```

```
            Value: SQS-VPCE-Tutorial-Subnet
    InternetGateway:
      Type: "AWS::EC2::InternetGateway"
      Properties:
        Tags:
          - Key: Name
            Value: SQS-VPCE-Tutorial-InternetGateway
    VPCGatewayAttachment:
      Type: "AWS::EC2::VPCGatewayAttachment"
      Properties:
        VpcId: !Ref VPC
        InternetGatewayId: !Ref InternetGateway
    RouteTable:
      Type: "AWS::EC2::RouteTable"
      Properties:
        VpcId: !Ref VPC
        Tags:
          - Key: Name
            Value: SQS-VPCE-Tutorial-RouteTable
    SubnetRouteTableAssociation:
      Type: "AWS::EC2::SubnetRouteTableAssociation"
      Properties:
        RouteTableId: !Ref RouteTable
        SubnetId: !Ref Subnet
    InternetGatewayRoute:
      Type: "AWS::EC2::Route"
      Properties:
        RouteTableId: !Ref RouteTable
        GatewayId: !Ref InternetGateway
        DestinationCidrBlock: 0.0.0.0/0
    SecurityGroup:
      Type: "AWS::EC2::SecurityGroup"
      Properties:
        GroupName: SQS VPCE Tutorial Security Group
        GroupDescription: Security group for SQS VPC endpoint tutorial
        VpcId: !Ref VPC
        SecurityGroupIngress:
          - IpProtocol: "-1"
            CidrIp: 10.0.0.0/16
          - IpProtocol: tcp
            FromPort: "22"
            ToPort: "22"
            CidrIp: !Ref SSHLocation
        SecurityGroupEgress:
```

```
          - IpProtocol: "-1"
            CidrIp: 10.0.0.0/16
        Tags:
          - Key: Name
            Value: SQS-VPCE-Tutorial-SecurityGroup
    EC2Instance:
      Type: "AWS::EC2::Instance"
      Properties:
        KeyName: !Ref KeyName
        InstanceType: t3.micro
        ImageId: !FindInMap
          - RegionMap
          - !Ref "AWS::Region"
          - AMI
        NetworkInterfaces:
          - AssociatePublicIpAddress: "true"
            DeviceIndex: "0"
            GroupSet:
              - !Ref SecurityGroup
            SubnetId: !Ref Subnet
        IamInstanceProfile: !Ref EC2InstanceProfile
        Tags:
          - Key: Name
            Value: SQS-VPCE-Tutorial-EC2Instance
    EC2InstanceProfile:
      Type: "AWS::IAM::InstanceProfile"
      Properties:
        Roles:
          - !Ref EC2InstanceRole
        InstanceProfileName: !Sub "EC2InstanceProfile-${AWS::Region}"
    EC2InstanceRole:
      Type: "AWS::IAM::Role"
      Properties:
        RoleName: !Sub "SQS-VPCE-Tutorial-EC2InstanceRole-${AWS::Region}"
        AssumeRolePolicyDocument:
          Version: 2012-10-17
          Statement:
            - Effect: Allow
              Principal:
                Service: ec2.c2s.ic.gov
              Action: "sts:AssumeRole"
        ManagedPolicyArns:
          - "arn:aws-iso:iam::aws:policy/AmazonSQSFullAccess"
    CFQueue:
```

```
        Type: "AWS::SQS::Queue"
        Properties:
          VisibilityTimeout: 60
```

To use this template, follow the Tutorial: Sending a message to an Amazon SQS queue from Amazon Virtual Private Cloud procedure, but change the first few steps under "Step 2: Create the AWS resources" to the following:

1. Sign in to the AWS CloudFormation Console.
2. Choose **Create stack**.
3. Under **Specify template**, choose **Upload a template file** and choose the text-only file where you saved the above template.
4. Choose **Next** and then resume following the standard procedure at step 5, where you specify stack details.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Amazon SQS by using the command line or APIs, use the appropriate endpoint.

Documentation for Amazon SQS

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

- *Amazon Simple Queue Service Developer Guide*
  - Getting Started section
- *Amazon Simple Queue Service API Reference*
- *AWS CLI Reference*
  - Amazon SQS section

Amazon Simple Workflow Service

Amazon Simple Workflow Service (Amazon SWF) is a task coordination and state management service for cloud applications. The Amazon SWF APIs, libraries, and control engine give developers the tools to coordinate, audit, and scale applications across multiple machines—in the AWS cloud and other data centers. With Amazon SWF, you can stop writing complex glue-code and state machinery and invest more in the business logic that makes your applications unique.

Topics

- Region Availability
- How Amazon SWF Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Amazon SWF

Region Availability

Amazon Simple Workflow Service is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Amazon SWF Differs for AWS Top Secret Regions

The implementation of Amazon SWF is different for AWS Top Secret Regions in the following ways:

- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Amazon SWF by using the command line or APIs, use the appropriate endpoint.

Documentation for Amazon SWF

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

- Amazon Simple Workflow Service Developer Guide
- Amazon SWF section of AWS CLI Reference
- Amazon Simple Workflow Service API Reference
- AWS Flow Framework for Java Developer Guide
- AWS Flow Framework for Java API Reference
- AWS Flow Framework for Ruby Developer Guide
- AWS Flow Framework for Ruby API Reference

AWS Snowball Edge

The AWS Snowball Edge is a type of Snowball device with on-board storage and compute power for select AWS capabilities. Snowball Edge can undertake local processing and edge-computing workloads in addition to transferring data between your local environment and the AWS Cloud.

Topics

- Region Availability
- How Snowball Edge Differs for AWS Top Secret - East
- How Command Line and API Access Differs for AWS Top Secret - East
- How Snowball Edge Differs for AWS Top Secret - West
- How Command Line and API Access Differs for AWS Top Secret - West
- Documentation for Snowball Edge

Region Availability

AWS Snowball Edge is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Snowball Edge Differs for AWS Top Secret - East

The implementation of Snowball Edge is different for AWS Top Secret - East in the following ways:

- For differences on managing Amazon EC2 instances on your device, see Amazon Elastic Compute Cloud.
- The only shipping carrier for this region is a Sponsor designated courier. The courier is approved to handle and transport AWS Top Secret - East Snowball Edge devices.
- For Compute using EC2 instances you need to have one or more supported AMIs in your AWS account before you can add any AMIs to your job creation request otherwise you will see "You have no compatible AMIs". If you believe your AMI is supported but it is not showing please open a case with AWS Top Secret Regions Support, provide your account number, your AMI IDs, and we will review why your AMIs are not appearing.

- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.
- The high performance NFS data transfer feature is not available on AWS Top Secret - East Snowball Edge Storage Optimized devices.
- The AWS Snow Family Job Management Service `CreateReturnShippingLabel` and `DescribeReturnShippingLabel` API actions are not available for AWS Top Secret - East Snow Family jobs. In the event you require a shipping label in order to return your AWS Top Secret - East Snow Family device, open a case with AWS Top Secret Regions Support, provide your AWS Snow Family Job ID, and AWS Snow Family Snowball Edge device Serial Number. AWS will then provide you with a shipping label.
- AWS Snow Family Large Data Migration Manager is not available in the AWS Top Secret - East.
- Amazon EKS Anywhere on Snow is not available in AWS Top Secret - East.
- Amazon S3 Compatible Storage is not available on Snowball Edge Compute Optimized with AMD EPYC Gen1, HDD, and optional GPU in AWS Top Secret - East.
- Snowball Edge devices in the AWS Top Secret - East do not have an embedded GPS module.

How Command Line and API Access Differs for AWS Top Secret - East

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

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

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

- https://snowball.us-iso-east-1.c2s.ic.gov

How Snowball Edge Differs for AWS Top Secret - West

The implementation of Snowball Edge is different for AWS Top Secret - West in the following ways:

- For differences on managing Amazon EC2 instances on your device, see Amazon Elastic Compute Cloud.
- The only shipping option for the AWS Top Secret - West region is individual customer provided courier. The courier must be approved to handle and transport Top Secret material and be able to pick up the device at the AWS Top Secret region data center. Once you place an order, AWS will reach out to you for next steps on picking up the device.
- For EC2 jobs, you need to have one or more supported AMIs in your AWS account before you can add any AMIs to your job creation request. If you don't have supported AMIs, open a case with AWS Top Secret Regions AWS Support, provide your account number and AMI IDs to get your AMIs added to the list of allowed AMIs. When the AMIs are allowlisted, you will be able to create your job and specify the AMIs for the job.
- The high performance NFS data transfer feature is not available on AWS Top Secret - West Snowball Edge Storage Optimized devices.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.
- The AWS Snow Family Job Management Service `CreateReturnShippingLabel` and `DescribeReturnShippingLabel` API actions are not available for AWS Top Secret - West Snow Family jobs. In the event you require a shipping label to return your AWS Top Secret - West Snow Family device, open a case with AWS Top Secret Regions Support, provide your AWS Snow Family Job ID and AWS Snow Family device Serial Number. AWS will then provide you with a shipping label.
- AWS Snow Device Management service is not available in AWS Top Secret - West because AWS IoT Greengrass is not available in AWS Top Secret - West.
- AWS Snow Family Large Data Migration Manager is not available in the AWS Top Secret - West as Amazon EventBridge is not available in AWS Top Secret - West.
- Amazon EKS Anywhere on Snow is not available in AWS Top Secret - West.
- Amazon S3 Compatible Storage is not available on Snowball Edge Compute Optimized with AMD EPYC Gen1, HDD, and optional GPU in AWS Top Secret - West.
- Snowball Edge devices in the AWS Top Secret - West do not have an embedded GPS module.
- Snowball Edge Compute Optimized with AMD EPYC Gen1, HDD, and optional GPU is not available in AWS Top Secret - West. If you have a need to order Snowball Edge Compute Optimized with AMD EPYC Gen1 52 vCPU, HDD, and optional GPU, please order from AWS Top Secret - East.

How Command Line and API Access Differs for AWS Top Secret - West

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

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

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

- https://snowball.us-iso-west-1.c2s.ic.gov

Documentation for Snowball Edge

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

- AWS Snowball Edge Developer Guide
- AWS Snowball API Reference
- AWS Snowball section of AWS CLI Reference

AWS Step Functions

AWS Step Functions is a web service that enables you to coordinate the components of distributed applications and microservices using visual workflows.

Topics

- Region Availability
- How Step Functions Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Step Functions

Region Availability

AWS Step Functions is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Step Functions Differs for AWS Top Secret Regions

The implementation of Step Functions is different for AWS Top Secret Regions in the following ways:

- Step Functions Local .jar file is not available in AWS Top Secret Regions.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.
- Synchronous Express Workflows are not available.
- Support for AWS X-Ray tracing is not available.
- Support for and from the AWS Serverless Application Model is not available.
- Support to call third-party APIs is not available.
- Support to use the TestState API is not available.
- The Step Functions Data Science SDK is not supported.
- Integration with AWS services available as of December 23, 2023 are supported in AWS Top Secret Regions if these services are available in the Region.

- Customer managed keys for AWS KMS encryption are not available in this region.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Step Functions by using the command line or APIs, use the appropriate endpoint.

Documentation for Step Functions

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

- AWS Step Functions Developer Guide
- AWS Step Functions API Reference
- AWS Step Functions section of AWS CLI Reference

AWS Storage Gateway

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

Topics

- How Storage Gateway Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Storage Gateway

How Storage Gateway Differs for AWS Top Secret Regions

The implementation of Storage Gateway is different for AWS Top Secret Regions in the following ways:

- Amazon FSx File Gateway is not supported in AWS Top Secret Regions.

> **Note**
>
> Amazon FSx File Gateway is no longer available to new customers in any AWS Region, including AWS Top Secret Regions, as of 10/28/2024.

- The AWS Storage Gateway hardware appliance is not available in AWS Top Secret Regions.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Storage Gateway by using the command line or APIs, use the appropriate endpoint.

Documentation for Storage Gateway

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

> **Important**
>
> The Amazon FSx File Gateway User Guide is no longer available in AWS Top Secret Regions. You might have been redirected to this page if you attempted to follow a link to the Amazon FSx File Gateway from within the AWS Top Secret Regions.

- AWS Storage Gateway - Amazon S3 File Gateway User Guide
- AWS Storage Gateway - Tape Gateway User Guide
- AWS Storage Gateway - Volume Gateway User Guide
- AWS Storage Gateway - API Reference

AWS Support

AWS Support for AWS Top Secret Regions offers support options ranging from online help to personal support.

Topics

- AWS Support Center
- AWS Top Secret Regions Business Support
- AWS Top Secret Regions Enterprise Support
- Service Health Dashboard
- AWS Trusted Advisor
- Region Availability
- How AWS Support Differs for AWS Top Secret Regions
- Documentation for AWS Support

AWS Support Center

AWS Support Center is your location for AWS Technical Support, which includes access to technical FAQs, service status page, and AWS Support. AWS Support Center is available in the AWS Management Console, with federated access support and enhanced case-management workflows. For more information, see AWS Support Center.

> **Note**
>
> AWS Support Center currently does not integrate with the Classification Management Tool. You must manually add classification markings when using AWS Support Center.

AWS Top Secret Regions Business Support

AWS Top Secret Regions Business Support is a one-on-one, fast-response support channel that is staffed around the clock by experienced technical support engineers. Business support is available to all customers in AWS Top Secret Regions at no additional charge. For more information, see AWS Support.

AWS Top Secret Regions Enterprise Support

The optional AWS Top Secret Regions Enterprise Support offering builds on AWS Top Secret Regions Business Support by adding features such as direct access to a Technical Account Manager (TAM). There are charges for Enterprise support. For more information, see AWS Support.

Service Health Dashboard

AWS Top Secret Regions includes a Service Health Dashboard (SHD) that provides access to current status and historical data about every AWS service in AWS Top Secret Regions. If there's a problem with a service, you'll be able to expand the appropriate line in the Details section and learn more. You can also subscribe to the RSS feed for any service. You can access the SHD from the marketing site or at http://status.c2shome.ic.gov/.

AWS Trusted Advisor

AWS Trusted Advisor is a service in the console that inspects your AWS environment and identifies ways to save money, improve system performance and reliability, or close security gaps. For more information, see Meet AWS Trusted Advisor.

Region Availability

AWS Support is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How AWS Support Differs for AWS Top Secret Regions

The implementation of AWS Support is different for AWS Top Secret Regions in the following ways:

- The **How can we help?** search bar in the AWS Support Center is not available.
- Some Trusted Advisor features are not available. See AWS Trusted Advisor.
- Only Signature Version 4 signing is supported.

Documentation for AWS Support

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

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

To connect to AWS Support by using the command line or APIs, use the appropriate endpoint.

AWS Systems Manager

AWS Systems Manager makes it easier for you to configure and manage your EC2 instances, on-premises servers, and virtual machines (VMs), including VMs in other cloud environments. Systems Manager gives you a complete view of your infrastructure performance and configuration, simplifies resource and application management, and makes it easy to operate and manage your infrastructure at scale.

Topics

- Region Availability
- How Systems Manager Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Systems Manager

Region Availability

AWS Systems Manager is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Systems Manager Differs for AWS Top Secret Regions

The implementation of Systems Manager is different for AWS Top Secret Regions in the following ways:

- The following Systems Manager capabilities are not yet available for AWS Top Secret Regions:
  - Application Manager
  - Change Manager
  - Explorer
  - Fleet Manager
  - Incident Manager
  - OpsCenter
  - Quick Setup

- The following Systems Manager features are not available for AWS Top Secret Regions:

  General

  Support for specifying a resource group as the target of an operation is not available.

  Automation

  The Document Builder feature is not available.

  Documents

  Some Automation runbooks and SSM Command documents are not available for AWS Top Secret Regions, such as the following:

  - AWS-ApplyPatchBaseline
  - AWS-ConfigureWindowsUpdate
  - AWS-FindWindowsUpdates
  - AWS-InstallMissingWindowsUpdates
  - AWS-InstallPowerShellModule
  - AWS-InstallSpecificWindowsUpdates
  - AWS-InstallWindowsUpdates
  - AWS-InstanceRebootWithHooks
  - AWS-RunPatchBaselineAssociation
  - AWS-RunPatchBaselineWithHooks

  Patch Manager

  Support for patching Window Server machines is not available in the following Regions:

  - eu-isoe-west-1
  - us-isof-south-1
  - us-isof-east-1

  The patch policies feature is not available.

  Parameter Store

  The shared parameters feature is not available.

  Session Manager

  The Block public sharing for SSM documents feature is not available.

- The URLs to download the Session Manager plugin for the AWS CLI are as follows:

Operating System	Session Manager Plugin URL
Windows Server	`https://s3.us-iso-east-1.c2s.ic.gov/session-manager-downloads/plugin/latest/windows/SessionManagerPluginSetup.exe`
macOS	`https://s3.us-iso-east-1.c2s.ic.gov/session-manager-downloads/plugin/latest/mac/sessionmanager-bundle.zip`

Linux	**x86_64:**
	`https://s3.us-iso-east-1.c2s.ic.gov/session-manager-downloads/plugin/latest/linux_64bit/session-manager-plugin.rpm`
	x86:
	`https://s3.us-iso-east-1.c2s.ic.gov/session-manager-downloads/plugin/latest/linux_32bit/session-manager-plugin.rpm`
	ARM64:
	`https://s3.us-iso-east-1.c2s.ic.gov/session-manager-downloads/plugin/latest/linux_arm64/session-manager-plugin.rpm`

Operating System	Session Manager Plugin URL

Ubuntu Server	**x86_64:**
	`https://s3.us-iso-east-1.c2s.ic.gov/session-manager-downloads/plugin/latest/ubuntu_64bit/session-manager-plugin.deb`
	x86:
	`https://s3.us-iso-east-1.c2s.ic.gov/session-manager-downloads/plugin/latest/ubuntu_32bit/session-manager-plugin.deb`
	ARM64:
	`https://s3.us-iso-east-1.c2s.ic.gov/session-manager-downloads/plugin/latest/ubuntu_arm64/session-manager-plugin.deb`

- The process for installing SSM Agent on managed instances includes the following differences for AWS Top Secret Regions:
  - The URLs to download the installers from are specific to AWS Top Secret Regions.
  - On version 2.3.714.0 and earlier versions of SSM Agent, a custom file must be created to specify the endpoint values for the agent to use.
  - SSM Agent must be restarted after creating the custom file.

  When following the instructions to install SSM Agent on Linux and Windows operating systems, see the following table for the sources of installation files to use.

Operating System	SSM Agent Installer URL

Amazon Linux and Amazon Linux 2	**Intel (x86_64) 64-bit instances:**
	`https://s3.us-iso-east-1.c2s.ic.gov/amazon-ssm-us-iso-east-1/latest/linux_amd64/amazon-ssm-agent.rpm`
	ARM (arm64) 64-bit instances:
	`https://s3.us-iso-east-1.c2s.ic.gov/amazon-ssm-us-iso-east-1/latest/linux_arm64/amazon-ssm-agent.rpm`
	Intel (x86) 32-bit instances:
	`https://s3.us-iso-east-1.c2s.ic.gov/amazon-ssm-us-iso-east-1/latest/linux_386/amazon-ssm-agent.rpm`

Ubuntu Server	`https://s3.us-iso-east-1.c2s.ic.gov/amazon-ssm-us-iso-east-1/latest/debian_amd64/amazon-ssm-agent.deb sudo dpkg -i amazon-ssm-agent.deb`

Operating System	SSM Agent Installer URL

Red Hat Enterprise Linux (RHEL)	**Intel (x86_64) 64-bit instances:**
	`https://s3.us-iso-east-1.c2s.ic.gov/amazon-ssm-us-iso-east-1/latest/linux_amd64/amazon-ssm-agent.rpm`
	ARM (arm64) 64-bit instances::
	`https://s3.us-iso-east-1.c2s.ic.gov/amazon-ssm-us-iso-east-1/latest/linux_arm64/amazon-ssm-agent.rpm`
	Intel (x86) 32-bit instances:
	`https://s3.us-iso-east-1.c2s.ic.gov/amazon-ssm-us-iso-east-1/latest/linux_386/amazon-ssm-agent.rpm`

CentOS	**64-bit instances:**
	`https://s3.us-iso-east-1.c2s.ic.gov/amazon-ssm-us-iso-east-1/latest/linux_amd64/amazon-ssm-agent.rpm`
	32-bit instances:
	`https://s3.us-iso-east-1.c2s.ic.gov/amazon-ssm-us-iso-east-1/latest/linux_386/amazon-ssm-agent.rpm`

Operating System	SSM Agent Installer URL
SUSE Linux Enterprise Server (SLES)	**64-bit instances:** `https://s3.us-iso-east-1.c2s.ic.gov/amazon-ssm-us-iso-east-1/latest/linux_amd64/amazon-ssm-agent.rpm sudo rpm --install amazon-ssm-agent.rpm`
Raspbian	`https://s3.us-iso-east-1.c2s.ic.gov/amazon-ssm-us-iso-east-1/latest/debian_arm/amazon-ssm-agent.deb`
Windows Server	`https://s3.us-iso-east-1.c2s.ic.gov/amazon-ssm-us-iso-east-1/latest/windows_amd64/AmazonSSMAgentSetup.exe`

Customize endpoints (SSM Agent versions 2.3.714.0 and earlier)

If you are running SSM Agent version 2.3.714.0 or earlier, follow these steps to specify the custom endpoints for SSM Agent. These steps are not required for versions of the agent later than 2.3.714.0.

> **Tip**
>
> For all operating system types, you can locate the SSM Agent version number on the **Managed Instances** page in the Systems Manager console.

1. Open the file `amazon-ssm-agent.json.template` from the appropriate location.

   All Unix-based operating systems and Raspbian:

   `/etc/amazon/ssm/amazon-ssm-agent.json.template`

Windows Server:

```
C:\Program Files\Amazon\SSM\amazon-ssm-agent.json.template
```

2. For the following elements in the file, enter the endpoints as specified in the **Endpoint** column.

Element	Endpoint
Mds	`ec2messages.us-iso-east-1.c2s.ic.gov`
Ssm	`ssm.us-iso-east-1.c2s.ic.gov`
Mgs	`ssmmessages.us-iso-east-1.c2s.ic.gov`
S3	`s3.us-iso-east-1.c2s.ic.gov`
Kms	`kms.us-iso-east-1.c2s.ic.gov`

3. Save the file as `amazon-ssm-agent.json`.
4. Restart SSM Agent.

- A table in the topic About minimum S3 Bucket permissions for SSM Agent lists two Amazon Simple Storage Service (S3) buckets that can provide access to the distribution service used by version 2.2.45.0 and later of SSM Agent. (This service is used to run the document `AWS-ConfigureAWSPackage`).

  In AWS Top Secret Regions, the bucket that SSM Agent requires access to is the one in the format `arn:aws:s3:::aws-ssm-distributor-file-`*`region`*`/*` .
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Systems Manager by using the command line or APIs, use the appropriate endpoint.

Documentation for Systems Manager

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

- AWS Systems Manager User Guide
- AWS Systems Manager API Reference
- Systems Manager section of AWS CLI Reference

Amazon Textract

Amazon Textract enables you to add document text detection and analysis to your applications. You provide a document image to the Amazon Textract API, and the service detects the document text. Amazon Textract works with formatted text and can detect words and lines of words that are located close to each other. It can also analyze a document for items such as related text, tables, key-value pairs, and selection elements.

Topics

- Region Availability
- How Amazon Textract Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Amazon Textract

Region Availability

Amazon Textract is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Amazon Textract Differs for AWS Top Secret Regions

The implementation of Amazon Textract is different for AWS Top Secret Regions in the following ways:

- The following Amazon Textract features are not available in AWS Top Secret Regions:
  - AnalyzeExpense
  - AnalyzeID
  - AnalyzeLending
  - Custom Queries
  - Table Model Update - Includes merged cell support
  - Clickables Model Update - Includes support for implied clickables
  - Self Service Limits

- Amazon Textract does not use or store customer data to improve its models.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

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

To connect to Amazon Textract by using the command line or APIs, use the appropriate endpoint.

Documentation for Amazon Textract

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

- Amazon Textract Developer Guide

Amazon Transcribe

Amazon Transcribe uses advanced machine learning technologies to recognize speech in audio files and transcribe them into text. You can 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.

Topics

- Region Availability
- How Amazon Transcribe Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Amazon Transcribe

Region Availability

Amazon Transcribe is available in the following AWS Top Secret Regions:

- AWS Top Secret - East

How Amazon Transcribe Differs for AWS Top Secret Regions

The implementation of Amazon Transcribe is different for AWS Top Secret Regions in the following ways:

- Amazon Transcribe Medical is not supported in AWS Top Secret Regions.
- The following Amazon Transcribe features are not available in AWS Top Secret Regions:
  - Automatic content redaction
  - Custom language models
  - Job queuing
  - Automatic language identification
  - Call Analytics
- The following languages are not available in AWS Top Secret Regions:
  - Afrikaans
  - Mandarin Chinese (Traditional)

- Danish
- New Zealand English
- South African English
- Thai
- Amazon Transcribe does not use or store customer data to improve its transcription models.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Amazon Transcribe by using the command line or APIs, use the appropriate endpoint.

Documentation for Amazon Transcribe

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

- Amazon Transcribe Developer Guide

AWS Transit Gateway

A *transit gateway* is a network transit hub that you can use to interconnect your virtual private clouds (VPCs) and on-premises networks.

Topics

- Region Availability
- How AWS Transit Gateway Differs for AWS Top Secret Regions
- Documentation for AWS Transit Gateway

Region Availability

AWS Transit Gateway is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How AWS Transit Gateway Differs for AWS Top Secret Regions

The implementation of AWS Transit Gateway is different for AWS Top Secret Regions in the following ways:

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

- Transit Gateway Connect is not supported.
- IGMP multicast is not supported.

- Connect peers are not supported.
- AWS Network Manager is not supported.
- Inter-Region peering is only supported between AWS Top Secret - East and AWS Top Secret - West. You can't create an Inter-Region peering with any other AWS Special Region or commercial Region.
- Transit gateway peering attachments for these AWS Top Secret Regions must be initiated from either the AWS CLI or from the AWS Top Secret - West console. Transit gateway peering attachments can't be initiated from the AWS Top Secret - East console.

Documentation for AWS Transit Gateway

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

- Amazon VPC Transit Gateways
- Amazon EC2 section of AWS CLI Reference
- Amazon EC2 API Reference

Amazon Translate

Amazon Translate is a text translation service that uses advanced machine learning technologies to provide high-quality translation on demand. You can use Amazon Translate to translate multiple types of documents or to build applications that work in multiple languages.

Topics

- Region Availability
- How Amazon Translate Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Amazon Translate

Region Availability

Amazon Translate is available in the following AWS Top Secret Regions:

- AWS Top Secret - East

How Amazon Translate Differs for AWS Top Secret Regions

The implementation of Amazon Translate is different for AWS Top Secret Regions in the following ways:

- Asynchronous batch translation does not support these features at this time:
  - Resource level permissions
  - Tagging support
  - Masking Profanity
  - Setting formality
  - Active Custom Translation (Customizing with parallel data)
  - Automatic language detection
- Real-Time Document Translation is not available at this time.
- Amazon Translate does not use or store customer data to improve its translation model.

- The supported browsers for the Amazon Translate console are Firefox and Microsoft Edge. In the AWS Top Secret Regions region, the Amazon Translate console does not support Internet Explorer, Safari, Chrome, or Opera.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Amazon Translate by using the command line or APIs, use the appropriate endpoint.

Documentation for Amazon Translate

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

- Amazon Translate Developer Guide
- Amazon Translate API Reference
- Amazon Translate section of AWS CLI Reference

AWS Trusted Advisor

AWS Trusted Advisor helps you provision your resources by following best practices. Trusted Advisor inspects your AWS environment and finds opportunities to save money, improve system performance and reliability, or help close security gaps.

Topics

- Region Availability
- How AWS Trusted Advisor Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for AWS Trusted Advisor

Region Availability

AWS Trusted Advisor is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How AWS Trusted Advisor Differs for AWS Top Secret Regions

The implementation of AWS Trusted Advisor is different for AWS Top Secret Regions in the following ways:

- The organizational view feature is not supported.
- Not all checks are supported in this AWS Region. For a list of available checks, see the Trusted Advisor check reference.
- Trusted Advisor does not support sending weekly notification emails for checks at this time.
- Monitoring Trusted Advisor checks with Amazon CloudWatch Events is not supported.
- The AWS Security Hub integration feature is not supported.
- The Trusted Advisor APIs are not supported.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

> **Note**
>
> To call the Trusted Advisor API, use the same endpoint as AWS Support.

To connect to AWS Trusted Advisor by using the command line or APIs, use the appropriate endpoint.

Documentation for AWS Trusted Advisor

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

- AWS Support User Guide
- AWS Support API Reference
- Trusted Advisor section of AWS CLI Reference

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the AWS Top Secret Regions cloud where you can launch resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

Topics

- Region Availability
- How Amazon VPC Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for Amazon VPC

Region Availability

Amazon Virtual Private Cloud is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How Amazon VPC Differs for AWS Top Secret Regions

The implementation of Amazon VPC is different for AWS Top Secret Regions in the following ways:

- Tag on create and vanity DNS are not supported on AWS PrivateLink.
- You can't configure IGMP multicast on transit gateways.
- AWS Network Manager is not supported.
- Traffic Mirroring is not supported.
- Reachability Analyzer is not supported.
- Network Access Analyzer is not supported.
- Amazon VPC IP Address Manager (IPAM) is not supported.
- Internet gateways do not connect to the public Internet.

- You can't assign a private DNS name to a VPC endpoint service.
- You can enable IPv6 to support traffic flow within a single VPC and between multiple VPCs. AWS Site-to-Site VPN, transit gateways, and AWS Direct Connect do not support IPv6.
- IPv6 only subnets are not supported.
- The following IPv6 ranges are supported:
  - us-iso-east-1 – 2600:1f1a::/36
  - us-iso-west-1 – 2600:1f1d::/36
- The following APIs do not support resource-level permissions: CreateVpnConnection, DeleteVpnConnection, CreateVpnGateway, DeleteVpnGateway, CreateCustomerGateway, DeleteCustomerGateway, AttachVpnGateway, DetachVpnGateway, CreateVpnConnectionRoute, DeleteVpnConnectionRoute, and ModifyVpnTunnelCertificate.
- You can't add a tag when you create a VPC, network interface, or Elastic IP address using the Amazon VPC console.
- You can view and use AWS-managed prefix lists with security groups only.
- The following algorithms are not supported:
  - Encryption: AES128-GCM-16, AES256-GCM-16
  - Integrity: SHA2-384, SHA2-512
  - Diffie-Hellman groups: 19, 20, 21
- The transfer Elastic IP address feature is not available.
- DNS64 and NAT64 are not available.
- Security group referencing support for transit gateways and transit gateway attachments is not available.
- When creating a DHCP option set, the IPv6 Preferred Lease Time option is not available.
- If you send VPC flow logs to Amazon S3, the `Parquet`, `Hive-compatible S3 prefixes` and `Hourly partitions` log file options are not available.
- Fields related to Amazon ECS that were released in VPC Flow Logs version 7 are not available.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.
- The Security Group VPC associations feature and the Shared Security Group feature are not available.
- The VPC Block Public Access (BPA) feature is not available.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to Amazon VPC by using the command line or APIs, use the appropriate endpoint.

Documentation for Amazon VPC

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

- Amazon VPC Getting Started Guide
- Amazon VPC User Guide
- AWS Site-to-Site VPN Network Administrator Guide
- Amazon EC2 section of AWS CLI Reference
- Amazon EC2 API Reference
- Amazon VPC Transit Gateways

AWS Virtual Private Network

AWS Virtual Private Network lets you establish a secure and private tunnel from your network or device to the AWS Cloud. You can extend your existing on-premises network into a VPC, or connect to other AWS resources from a client. AWS VPN offers two types of private connectivity that feature the high availability and robust security necessary for your data.

Topics

- Region Availability
- How AWS VPN Differs for AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for AWS VPN

Region Availability

AWS Virtual Private Network is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How AWS VPN Differs for AWS Top Secret Regions

The implementation of AWS VPN is different for AWS Top Secret Regions in the following ways:

- AWS Site-to-Site VPN integration with Global Accelerator is not available.
- Configurable Security Algorithms and Timer Settings is not supported.
- Certificate authentication and customer gateway modification are not supported.
- The following APIs do not support resource-level permissions: CreateVpnConnection, DeleteVpnConnection, CreateVpnGateway, DeleteVpnGateway, CreateCustomerGateway, DeleteCustomerGateway, AttachVpnGateway, DetachVpnGateway, CreateVpnConnectionRoute, DeleteVpnConnectionRoute, and ModifyVpnTunnelCertificate.
- VPN single tunnel and VPN tunnel endpoint replacement notifications are not available.
- IPv6 is not supported.
- You cannot initiate Internet Key Exchange (IKE) negotiations for your VPN connections from AWS.

- The following algorithms are not supported:
  - Encryption: AES128-GCM-16, AES256-GCM-16
  - Integrity: SHA2-384, SHA2-512
  - Diffie-Hellman groups: 19, 20, 21
- AWS Site-to-Site VPN private IP VPN with AWS Direct Connect is not available.
- Integration with Direct Connect gateways is not supported in us-iso-west-1.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.
- AWS Site-to-Site VPN logging feature is not available.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to AWS VPN by using the command line or APIs, use the appropriate endpoint.

Documentation for AWS VPN

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

- Amazon VPC User Guide
- AWS Site-to-Site VPN Network Administrator Guide
- Amazon EC2 section of AWS CLI Reference

- Amazon EC2 API Reference
- Amazon VPC Transit Gateways

Amazon WorkSpaces

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

Topics

- Region Availability
- How WorkSpaces Differs for AWS Top Secret Regions
- How to Add the Required IAM Role Needed to Register a Directory for WorkSpaces in AWS Top Secret Regions
- Downloading WorkSpaces Clients in AWS Top Secret Regions
- How Command Line and API Access Differs for AWS Top Secret Regions
- Documentation for WorkSpaces

Region Availability

Amazon WorkSpaces is available in the following AWS Top Secret Regions:

- AWS Top Secret - East
- AWS Top Secret - West

How WorkSpaces Differs for AWS Top Secret Regions

The implementation of WorkSpaces is different for AWS Top Secret Regions in the following ways:

- The AWS service principal for Amazon WorkSpaces in AWS Top Secret - East is `workspaces.c2s.ic.gov`. The AWS service principal for Amazon WorkSpaces in AWS Top Secret - West is `workspaces.amazonaws.com`. For access to Amazon WorkSpaces in both AWS Top Secret - East and AWS Top Secret - West you are required to have

`workspaces.c2s.ic.gov` and `workspaces.amazonaws.com` attached to the workspaces_DefaultRole.

- Amazon WorkSpaces Application Manager is not available in AWS Top Secret Regions.
- Graphics based WorkSpaces are not available in AWS Top Secret - West.
- BYOL WorkSpaces are not available in AWS Top Secret - West.
- the Always_On running mode is not available for Graphics type workspace bundles.
- Simple AD is not available in AWS Top Secret Regions.
- Amazon WorkDocs is not available in AWS Top Secret Regions.
- In order to register an WorkSpaces Directory, the IAM Role `workspaces_DefaultRole` needs to be created and added for your account. See How to Add the Required IAM Role Needed to Register a Directory for WorkSpaces in AWS Top Secret Regions for details on how to do this.
- To register a directory for use with AWS Top Secret - East WorkSpaces, the directory must be located in the `us-iso-1a` or the `us-iso-1b` Availability Zone. WorkSpaces AWS Top Secret - East is not available in the `us-iso-1c` Availability Zone.
- To register a directory for use with AWS Top Secret - West WorkSpaces, the directory must be located in the `us-iso-1b` or the `us-iso-1c` Availability Zone.
- The WorkSpaces client `.msi` file is downloaded from Amazon S3 in AWS Top Secret Regions. See Downloading WorkSpaces Clients in AWS Top Secret Regions for details.
- The following features are not yet available in AWS Top Secret Regions:
  - CloudWatch Logging of Successful Login Events
  - WorkSpaces Streaming Protocol and underlying features. (Smart Cards, Ubuntu, 2-Way Audio/Video, Protocol Migration, Maxibon, etc.)
  - Cross Region Redirection
  - WorkSpaces Secure Browser
  - WorkSpaces Pools
  - WorkSpaces Multi-Region Resilience
  - The "Remember me" feature for self-service permissions.
- Because public internet access to public update servers (including the Microsoft Update Server) is unavailable in AWS Top Secret Regions, customers need to distribute software updates (not changes to the configuration) to update the Windows OS (using SCCM or a WSUS server), Linux OS, and individual applications running on Amazon WorkSpaces.
- WorkSpace Client Diagnostic Log Uploads are not available in AWS Top Secret Regions.

- The Web Access client is not available in AWS Top Secret Regions.
- Amazon Resource Names (ARNs) and endpoints have different values.
- Only Signature Version 4 signing is supported.

How to Add the Required IAM Role Needed to Register a Directory for WorkSpaces in AWS Top Secret Regions

1. From the AWS Console, go to IAM.
2. Under **Roles**, click **Create role**.
3. Under **Choose the service that will use this role**, select **EC2**.
4. Click **Next: Tags**.
5. Click **Next: Review**.
6. In the **Role Name** field, enter `workspaces_DefaultRole` and enter a Role Description of your choice.
7. Click **Create role**.
8. In **Roles**, click the role you created: `workspaces_DefaultRole`.
9. Under the **Permissions** tab, click **Add inline policy**.
10. Under the **JSON** tab, paste this permission:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Action": [
"ec2:CreateNetworkInterface",
"ec2:DeleteNetworkInterface",
"ec2:DescribeNetworkInterfaces",
"ds:DescribeDomains"
],
"Effect": "Allow",
"Resource": "*"
}
]
}
```

11. Click **Review policy**.

12. In the **Name** field, enter `WorkSpacesServiceAccess`.
13. Click **Create policy**.
14. In **Roles**, click the role you created: `workspaces_DefaultRole`.
15. Under the **Trust relationships** tab, click **Edit trust relationship**.
16. In the **Policy Document field**, remove the existing text, and paste this trust policy:

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Principal": {
"Service": [
"workspaces.c2s.ic.gov",
"workspaces.amazonaws.com"
]
},
"Action": "sts:AssumeRole"
}
]
}
```

17. Click **Update Trust Policy**.

Downloading WorkSpaces Clients in AWS Top Secret Regions

- The Linux Client for AWS Top Secret Regions (.deb) can be downloaded by end users here.
- The Windows Desktop Client for AWS Top Secret Regions (.msi) can be downloaded by end users here.

> **Note**
>
> Windows Client 5.3.x or newer are required to utilize AWS Top Secret - West WorkSpaces.

How Command Line and API Access Differs for AWS Top Secret Regions

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

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

To connect to WorkSpaces by using the command line or APIs, use the appropriate endpoint.

Documentation for WorkSpaces

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

- Amazon WorkSpaces Admin Guide
- Amazon WorkSpaces User Guide
- Amazon WorkSpaces API Reference
- Amazon WorkSpaces section of AWS CLI Reference

Document History

The following table describes the document history for the *AWS Top Secret Regions User Guide*.

> **Note**
>
> For new features and feature updates of AWS Services in AWS Top Secret Regions, please refer to the AWS Top Secret Regions Marketing page.

Latest significant documentation updates can be referenced in below table:

Change	Description	Date
ElastiCache	The Valkey 8 engine is not available for ADC.	November 21, 2024
Amazon EKS	The observability dashboard isn't available.	November 20, 2024
Amazon RDS	Amazon RDS gp3 storage is now supported.	November 19, 2024
Amazon DynamoDB	Import from Amazon S3 is now available in AWS Top Secret - West.	November 12, 2024
Amazon EC2	You can't modify, reset, or view the address attributes of an Elastic IP address.	November 8, 2024
Amazon DCV	New service launch.	November 8, 2024
Amazon SageMaker	JupyterLab 4 is not supported for notebook instances.	November 6, 2024
Amazon Athena	JDBC 3.3.0 driver release.	November 6, 2024

AWS Modular Data Center Rack	New service launch.	November 6, 2024
Aurora	Features that involve using multiple AWS Regions, including cross-Region snapshot copying, cross-Reg ion replication, and Aurora Global Database, are now supported.	October 31, 2024
Amazon FSx	Added FSx for ONTAP.	October 30, 2024
AWS Storage Gateway	The Amazon FSx File Gateway User Guide is no longer available in AWS Top Secret Regions.	October 30, 2024
Amazon EKS	Dual-stack endpoints for EKS clusters aren't available.	October 23, 2024
Amazon CloudWatch	Metrics Insights is now available.	October 23, 2024
Amazon EC2 Image Builder	Image Builder now supports image workflows in AWS Top Secret Regions.	October 16, 2024
Amazon SNS	Amazon SNS now supports FIFO topics, payload-based filtering, and archive and replay.	October 10, 2024
AWS Systems Manager	A list has been added of Automation runbooks and SSM Command documents that are not supported for AWS Top Secret Regions.	October 9, 2024

AWS Systems Manager	The Distributor capability is now available.	October 2, 2024
AWS Systems Manager	Automation support for adding attachments to the `aws:executeScript` action now available.	October 2, 2024
Amazon ECS	Amazon ECS Application Autoscaling is now supported.	September 25, 2024
Amazon EKS	Mountpoint for Amazon S3 CSI Driver is now available as a managed add-on.	September 6, 2024
Amazon RDS	Storage autoscaling is now supported.	September 5, 2024
Amazon ECS	You can tag Amazon ECS resources in the AWS Top Secret Regions.	September 4, 2024
Amazon EKS	AWS PrivateLink is available to create a private connectio n between your VPC and Amazon EKS.	August 30, 2024
Amazon Application Recovery Controller (ARC)	Zonal autoshift for Amazon Application Recovery Controller (ARC) is now available in the following AWS Top Secret Regions: AWS Top Secret - East and AWS Top Secret - West.	August 28, 2024

AWS Identity and Access Management	AWS PrivateLink interface VPC endpoints for IAM are not available in AWS Top Secret Regions.	August 23, 2024
Lambda	Lambda recursive loop detection is not available in AWS Top Secret Regions.	August 21, 2024
AWS ParallelCluster	EC2 Image Builder and Amazon FSx for Lustre is supported by AWS ParallelC luster 3.10.1 and newer.	August 21, 2024
Amazon EventBridge	Dead-letter queues (DLQs) are now supported.	August 14, 2024
AWS Trusted Advisor	The Trusted Advisor APIs are not supported.	August 14, 2024
Lambda	The FilterCriteria parameter is now available in AWS Top Secret Regions.	August 7, 2024
Amazon SageMaker	SageMaker Processing is now available.	August 7, 2024
Amazon EKS	Dual-stack API endpoint for the Amazon EKS OIDC Issuer URL isn't available.	August 7, 2024
Amazon EKS	Dual-stack API endpoint for the Amazon EKS API isn't available.	August 7, 2024
Amazon ECR	Improved basic scanning isn't available in AWS Top Secret Regions.	August 7, 2024

Amazon OpenSearch Service	OpenSearch version 2.13 is now supported.	July 31, 2024
Amazon Linux 2023	Addition of guide.	July 31, 2024
AWS Step Functions	Customer managed keys for AWS KMS encryption are not available in this region.	July 31, 2024
Elastic Load Balancing	Network Load Balancers in AWS Top Secret Regions do not support attaching security groups.	July 24, 2024
Amazon EKS	Amazon EKS access entries is now available in AWS Top Secret Regions.	July 24, 2024
Amazon EKS	IP prefix assignment can now be used with the Amazon VPC CNI plugin.	July 24, 2024
Amazon Data Firehose	Apache Iceberg Tables isn't available as a destination.	July 24, 2024
Amazon WorkSpaces	WorkSpaces Pools are not available in AWS Top Secret Regions.	July 10, 2024
Amazon Route 53	Updated details of Route 53 alias records support.	July 10, 2024
Amazon DynamoDB	VPC Endpoints are now available in AWS Top Secret - West.	July 9, 2024

Amazon EC2	The DescribeInstanceEventNotificationAttributes, RegisterInstanceEventNotificationAttributes, and DeregisterInstanceEventNotificationAttributes APIs are now available in AWS Top Secret Regions.	July 3, 2024
Amazon Data Firehose	Snowflake isn't available as a destination.	July 3, 2024
AWS CloudFormation	AWS CloudFormation Hooks are available in AWS Top Secret Regions.	July 3, 2024
AWS Lambda	Lambda Advanced Logging Controls are now available in AWS Top Secret Regions.	July 3, 2024
Amazon S3	Amazon S3 Replication Time Control (S3 RTC) is now available in AWS Top Secret Regions.	June 26, 2024
AWS Lambda	Event destinations are now available in AWS Top Secret Regions.	June 26, 2024
Amazon EventBridge	EventBridge Pipes is not supported. The EventBridge Scheduler service is not supported.	June 19, 2024
AWS CloudFormation	The AWS CloudFormation AWS::LanguageExtensions transform is available in AWS Top Secret Regions.	June 19, 2024

AWS Config	Added a link to a list of supported AWS Config managed rules by Region availability.	June 19, 2024
AWS KMS	AWS KMS does not support the `KeyUsage` value of `KEY_AGREEMENT` for asymmetric keys in AWS Top Secret Regions.	June 19, 2024
AWS KMS	AWS KMS does not support the DeriveSharedSecret operation in AWS Top Secret Regions.	June 19, 2024
ElastiCache (Memcached)	Memcached serverless is not available for ADC.	June 12, 2024
Amazon EMR	Version 5.36.2 is now available in AWS Top Secret Regions.	June 12, 2024
Amazon EC2	Amazon Linux 2023 is now available.	June 12, 2024
AWS Lambda	`ReportBatchItemFailures` and `ParallelizationFactor` event source mapping parameters are now available.	June 12, 2024
Amazon S3	Date-based partitioning of Amazon S3 Server Access Logs is now supported in AWS Top Secret Regions.	June 5, 2024

Amazon Route 53	Dual-stack endpoint types are now supported.	June 5, 2024
Amazon Route 53	DNS over HTTPS is now supported.	June 5, 2024
AWS Config	AWS Config custom rules created with Guard are now supported.	June 5, 2024
AWS Lambda	Lambda now supports increased ephemeral storage in AWS Top Secret Regions.	June 5, 2024
Elastic Load Balancing	Network Load Balancers in AWS Top Secret Regions now support: unhealthy draining interval, deregistr ation delay, SetSubnets API, source IP preservation, TLS SNI, MinimumHealthyTarg ets, target group cross-zone, downstate flush, DNS zonal affinity, and Application Load Balancers as targets.	May 31, 2024
Amazon S3	Amazon S3 now supports the `GetObjectAttributes` API operation in AWS Top Secret Regions.	May 29, 2024
AWS KMS	Importing asymmetric and HMAC keys is now supported in AWS Top Secret Regions.	May 29, 2024
Security Hub	Security Hub is now available in AWS Top Secret Regions.	May 22, 2024

GuardDuty	GuardDuty Lambda Protection is now available in AWS Top Secret Regions.	May 22, 2024
Amazon WorkSpaces	The "Remember me" feature for self-service permissions is not available.	May 22, 2024
Amazon RDS	Amazon RDS Extended Support isn't available.	May 22, 2024
Amazon RDS	Events in the security patching event category aren't available.	May 22, 2024
AWS CloudFormation	The force delete stack option is not available in AWS Top Secret Regions.	May 22, 2024
Amazon ElastiCache	You can test automatic failover on up to 5 shards (called node groups in the ElastiCache API and AWS CLI) in any rolling 24-hour period.	May 15, 2024
Amazon EFS	Amazon EFS can only support 500 MiB/s throughput per client in AWS Top Secret - West.	May 15, 2024
Lambda	Lambda Kinesis trigger cross-account access is not available in AWS Top Secret Regions.	May 8, 2024
Amazon S3	Generating a manifest is only supported for Amazon S3 Batch Replication jobs in AWS Top Secret Regions.	May 8, 2024

Amazon S3	Amazon S3 Batch Operations and Amazon S3 Batch Replication are now available in AWS Top Secret Regions.	May 8, 2024
Amazon RDS	Copying an option group isn't available.	May 8, 2024
AWS Management Console	Unified Search only supports service and feature searches. Console Home widgets are unavailable. myApplications is unavailable.	May 8, 2024
GuardDuty	GuardDuty S3 Protection is now available in AWS Top Secret Regions.	May 1, 2024
Amazon OpenSearch Service	Custom dictionaries are now supported.	May 1, 2024
Amazon Route 53	Route 53 Profiles are not available.	April 24, 2024
License Manager	Added differences for AWS Top Secret Regions.	April 17, 2024
Lambda	The Ruby 3.3 (`ruby3.3`) runtime is not available in AWS Top Secret Regions.	April 17, 2024
Aurora	Publishing database logs to Amazon CloudWatch Logs now supported for Aurora MySQL and Aurora PostgreSQL.	April 17, 2024
Amazon RDS	All SQL Server options are now supported.	April 17, 2024

DataSync	Manifests are now available in AWS Top Secret Regions.	April 10, 2024
Amazon Redshift	Amazon Redshift Spectrum is available in AWS Top Secret - East but not in AWS Top Secret - West.	April 10, 2024
Amazon FSx	New service launch.	April 10, 2024
AWS SDK for Rust	Added section for using SDK for Rust in AWS Top Secret Regions	April 10, 2024
Amazon S3	Amazon S3 now supports notifications for the event types of `S3 Lifecycle expiration events` , `S3 Lifecycle transition events`, `Object ACL PUT events`, `Object tagging events`, and the `s3:ObjectRestore:Delete` event in AWS Top Secret - West and AWS Top Secret - East.	April 3, 2024
Amazon EMR	Version 6.15.0 is now available in AWS Top Secret Regions.	April 3, 2024
AWS Snowball Edge	Amazon S3 Compatible Storage is not available on Snowball Edge Compute Optimized with AMD EPYC Gen1, HDD, and optional GPU in AWS Top Secret - East and AWS Top Secret - West.	April 3, 2024

AWS Snowball Edge	Snowball Edge Storage Optimized 210TB is now available in AWS Top Secret - East and AWS Top Secret - West.	April 3, 2024
DataSync	Task reports are now available in AWS Top Secret Regions.	March 27, 2024
Amazon EKS	Corrected the list of features of the AWS Load Balancer Controller that aren't available.	March 27, 2024
AWS Elemental MediaPackage	MediaPackage V2 features aren't available in AWS Top Secret Regions.	March 27, 2024
AWS Elemental MediaLive	Resource group tagging is not supported.	March 27, 2024
AWS Transit Gateway	Appliance mode is now supported.	March 27, 2024
Amazon VPC	You can view and use AWS-managed prefix lists with security groups only.	March 20, 2024
Amazon RDS	There's no longer a maximum number of databases supported on a Microsoft SQL Server DB instance.	March 20, 2024
Amazon OpenSearch Service	OpenSearch version 2.11 is now supported.	March 20, 2024
Amazon EKS	Amazon GuardDuty is now available in AWS Top Secret - East.	March 20, 2024

Amazon DynamoDB	Resource-based policies are not available.	March 20, 2024
Amazon DynamoDB	Global Tables are now available in AWS Top Secret Regions.	March 20, 2024
Amazon DynamoDB	AWS PrivateLink is not supported for DynamoDB.	March 20, 2024
API Gateway	Custom domain name for WebSocket API is not yet available in AWS Top Secret - East.	March 20, 2024
AWS SDK for Kotlin	Added section for using SDK for Kotlin in AWS Top Secret Regions	March 20, 2024
AWS CloudFormation	Stack drift detection is available in AWS Top Secret Regions.	March 20, 2024
Amazon VPC	When creating a DHCP option set, the IPv6 Preferred Lease Time option is not available.	March 13, 2024
Amazon EKS	Amazon Linux 2023 isn't available.	March 13, 2024
API Gateway	Clarified wording about communicating with endpoints outside of AWS Top Secret Regions.	March 13, 2024
Amazon Textract	New service launch.	March 6, 2024

Amazon EKS	The Amazon EFS Cloud Storage Interface (CSI) driver is now available.	March 6, 2024
AWS Step Functions	Integration with AWS services available as of December 23, 2023 are supported in AWS Top Secret Regions if these services are available in the Region.	March 6, 2024
Lambda	The .NET 8 (`dotnet8`) runtime is not available in AWS Top Secret Regions.	February 28, 2024
DataSync	You can't use task reports for monitoring your DataSync transfers, and you can't use manifests for specifying the exact files or objects that you want DataSync to transfer.	February 28, 2024
Amazon ECS	Extensible Ephemeral Storage on AWS Fargate is supported , EphemeralStorageReservation and Ephemeral StorageUtilization metrics are available in CloudWatch Container Insights in AWS Top Secret Regions.	February 28, 2024
AWS Glue	AWS Glue 3.0 is now available for AWS Glue and AWS Glue Studio.	February 27, 2024

Amazon CloudWatch	Using AWS CloudFormation to add or remove tags on CloudWatch alarms is not supported.	February 21, 2024
Amazon Application Recovery Controller (ARC)	Amazon Application Recovery Controller (ARC) is now available in the following AWS Top Secret Regions: AWS Top Secret - East and AWS Top Secret - West.	February 21, 2024
API Gateway	The VPC endpoints `execute-api.us-iso-east-1.c2s.ic.gov` and `apigateway.us-iso-east-1.c2s.ic.gov` are not available in the AWS Top Secret - East Region.	February 21, 2024
AWS Step Functions	Added support for AWS PrivateLink, so you can start a workflow from your Amazon Virtual Private Cloud without traversing the public internet.	February 21, 2024
AWS Systems Manager	Patch Manager now supports Windows Server and Mac operating systems.	February 21, 2024
AWS Systems Manager	In the Parameter Store capability, the shared parameters feature is not available.	February 21, 2024
Amazon VPC	Amazon CloudWatch metrics per attachment are now supported.	February 14, 2024

Amazon Simple Queue Service	Amazon SQS Extended Client Library for Python is not supported.	February 14, 2024
AWS CloudTrail	Downloading events from the **Insights** page on the AWS Management Console is not supported.	February 14, 2024
AWS Transit Gateway	VPC attachments and VPN attachments can now be created.	February 14, 2024
Lambda	The Python 3.11 (`python3.11`) runtime is now available in AWS Top Secret Regions.	February 7, 2024
Amazon EFS	Using AWS DataSync to transfer data into or out of Amazon EFS file systems is now available.	February 7, 2024
AWS CloudFormation	AWS CloudFormation in AWS Top Secret Regions does not support AWS CloudFormation IaC generator (infrastructure as code generator).	February 7, 2024
AWS Config	AWS Config service-linked roles (such as `AWSServiceRoleForConfig`) are now supported.	February 7, 2024
Neptune	Neptune inaugural launch into AWS Top Secret Regions.	January 31, 2024

Amazon EFS	File systems using Elastic throughput can drive a maximum of 90,000 read IOPS for infrequently accessed data.	January 31, 2024
AWS CloudTrail	You can now configure advanced event selectors for trails by using the AWS Management Console.	January 31, 2024
AWS Directory Service	Log Forwarding to CloudWatch Logs is now supported.	January 31, 2024
AWS Identity and Access Management	The aws:RequestedRegion global condition key is now supported.	January 31, 2024
AWS Step Functions	Support for using the `Map` state in Distributed mode and setting up large-scale parallel workloads are now available.	January 31, 2024
DataSync	DataSync inaugural launch into AWS Top Secret Regions.	January 24, 2024
Amazon WorkSpaces	Self-Service WorkSpaces Client and Self-Service Client Customization are now available in AWS Top Secret Regions.	January 24, 2024

Amazon EC2 Auto Scaling	Amazon EC2 Auto Scaling now supports configuring an instance refresh to set its status to failed and roll back when it detects that a specified CloudWatch alarm has gone into the `ALARM` state.	January 24, 2024
Amazon Simple Queue Service	Attribute-based access control (ABAC) is now supported.	January 17, 2024
Amazon Data Firehose	Data delivery to Amazon OpenSearch Service domains located in a VPC is now available.	January 17, 2024
AWS Billing and Cost Management	When opting in to Cost Explorer, only the current month's data is available. Access to AWS Cost Explorer in the console is provided by the `aws-portal:ViewBilling` permission. Granular permissions provided by `ce:*` actions are not supported in AWS Top Secret Regions.	January 17, 2024
AWS Lambda	The Future runtime launch dates are not applicable in AWS Top Secret Regions.	January 17, 2024
AWS ParallelCluster	Amazon EC2 Capacity Blocks for ML is not supported	January 17, 2024
GuardDuty	New service launch.	January 10, 2024

Amazon WorkSpaces	The Web Access client is not available in AWS Top Secret Regions.	January 10, 2024
Amazon Redshift	Amazon Redshift query editor is not available in AWS Top Secret Regions.	January 10, 2024
Amazon EKS	Amazon EKS Upgrade insights aren't available.	January 10, 2024
Amazon EC2 Auto Scaling	Amazon EC2 Auto Scaling supports instance maintenance policies in AWS Top Secret Regions.	January 10, 2024
Amazon EC2	UEFI boot mode is not supported.	January 10, 2024
AWS Config	AWS Config recording of third-party resources is now supported.	January 10, 2024
Amazon SageMaker	Asynchronous Inference and Serverless Inference are not supported.	December 27, 2023
Amazon Route 53	DNS over HTTPS is not supported.	December 27, 2023
Amazon Kinesis Data Streams	Only **Extended data retention** (retention of up to seven days) is supported . **Long-term data retention** (retention of more than seven days and up to 365 days) is not supported.	December 27, 2023

Amazon S3	Amazon S3 Express One Zone is not available in AWS Top Secret Regions.	December 20, 2023
Amazon OpenSearch Service	OpenSearch version 2.9 is now supported.	December 20, 2023
Amazon OpenSearch Service	Cross-cluster search, cross-cluster replication, and remote reindex are now supported.	December 20, 2023
Amazon EKS	Amazon EKS Pod Identities aren't available.	December 20, 2023
Amazon EC2 Image Builder	Image Builder doesn't support image lifecycle policies and image workflows in AWS Top Secret Regions.	December 20, 2023
Amazon EC2	Launching an instance with an AWS Marketplace AMI is not supported in AWS Top Secret - West.	December 20, 2023
Amazon CloudWatch	Contributor Insights with CloudWatch is now supported .	December 20, 2023
AWS Directory Service	Mapping users to IAM roles for access to the AWS Management Console is now supported.	December 20, 2023
AWS Directory Service	Directory sharing with other AWS accounts and directory security settings are not supported.	December 20, 2023

AWS Lambda	The Python 3.12 (`python3.12`) runtime is not available in AWS Top Secret Regions.	December 20, 2023
Amazon EFS	Replicating to an existing file system is not supported.	December 13, 2023
AWS CloudFormation	AWS CloudFormation registry now available.	December 13, 2023
AWS Lambda	The asynchronous invocation metrics, `AsyncEventsReceived`, `AsyncEventAge`, and `AsyncEventsDropped` are now available in AWS Top Secret Regions.	December 13, 2023
AWS Step Functions	Remove a bullet about Support for accessing cross-account resources is not available.	December 13, 2023
AWS Step Functions	Support to call third-party APIs is not available.	December 13, 2023
Amazon S3	Amazon S3 Access Grants is not available in AWS Top Secret - West and AWS Top Secret - East.	December 6, 2023
Amazon S3	Amazon S3 Object Lock is now available in AWS Top Secret Regions.	December 6, 2023
Amazon EKS	Mountpoint for Amazon S3 CSI Driver is only available as a self-managed installation.	December 6, 2023

Amazon DynamoDB	DynamoDB operation logging to CloudTrail now includes more than just control plane activities.	December 6, 2023
AWS CloudTrail	When logging CloudTrail data events, Amazon DynamoDB API activity on streams is now available.	December 6, 2023
AWS Lambda	Lambda Advanced Logging Controls are not available in AWS Top Secret Regions.	December 6, 2023
AWS Secrets Manager	Secrets Manager API BatchGetSecretValue is not supported.	December 6, 2023
Amazon VPC	Security group referenci ng support for transit gateways and transit gateway attachments is not available.	November 22, 2023
Amazon VPC	You can now assign a primary private IPv4 address to the NAT gateway. You can also associate secondary private IPv4 addresses and secondary Elastic IP addresses to a NAT gateway.	November 22, 2023
Amazon S3	Amazon S3 does not support date-based partitioning in S3 Server Access Logs in AWS Top Secret Regions.	November 22, 2023
Amazon Route 53	Updated details of Route 53 alias records support.	November 22, 2023

Amazon EKS	Added that the CSI snapshot controller is only available as a self-managed installation. Added missing statement that Amazon Managed Service for Prometheus isn't available . Added additional links, reorganized the order to match the user guide better, and other cleanup.	November 22, 2023
Amazon EFS	The Elastic Throughput mode is now available.	November 22, 2023
Amazon EC2 Auto Scaling	Amazon EC2 Auto Scaling does not currently support instance maintenance policies in AWS Top Secret Regions.	November 22, 2023
Amazon EC2	Amazon EC2 instance topology is not available in AWS Top Secret Regions.	November 22, 2023
AWS CloudFormation	Interface VPC endpoints (AWS PrivateLink) for AWS CloudFormation are now available in the AWS Top Secret - West.	November 22, 2023
AWS Lambda	Multi-VPC connectivity for Amazon Managed Streaming for Apache Kafka event source mappings is not available in AWS Top Secret Regions.	November 22, 2023
AWS Lambda	The Java 21 (`java21`) runtime is not available in AWS Top Secret Regions.	November 22, 2023

Amazon S3	Amazon S3 Lifecycle rules based on object size is now available in AWS Top Secret Regions.	November 15, 2023
Amazon OpenSearch Service	OpenSearch version 2.7 is now supported.	November 15, 2023
Amazon EKS	Added missing statements that Amazon EKS Anywhere, Amazon CloudWatch Observability Operator, and AWS Distro for OpenTelem etry (ADOT) Operator aren't available.	November 15, 2023
Amazon EBS	Amazon EBS Direct APIs are now available in AWS Top Secret - West.	November 15, 2023
AWS Health	Added support for AWS Health Dashboard - Service health	November 15, 2023
AWS Lambda	The Amazon Linux 2023 (`provided.al2023`) runtime is not available in AWS Top Secret Regions.	November 15, 2023
AWS Lambda	The Node.js 20 (`nodejs20.x`) runtime is not available in AWS Top Secret Regions.	November 15, 2023
Amazon EMR	Updated and reformatted list of supported instance types.	November 8, 2023

AWS CloudTrail	You can only configure advanced event selectors for trails by using the AWS CLI. Configuration using the AWS Management Console is not supported.	November 8, 2023
Amazon SNS	Custom data identifiers are not supported.	November 1, 2023
Amazon EKS	Amazon EKS Extended Support for Kubernetes Versions isn't available.	November 1, 2023
Amazon EKS	Private clusters are now supported in AWS Top Secret - West.	November 1, 2023
Amazon SNS	Amazon SNS message archiving and replay is not supported.	October 25, 2023
Amazon EC2 Auto Scaling	You can now use an instance reuse policy to return instances to a warm pool when your Auto Scaling group scales in (terminates instances).	October 25, 2023
Amazon DynamoDB	`ReturnValuesOnConditionCheckFailure` is now available.	October 25, 2023
AWS Glue	AWS Glue Studio is now available.	October 25, 2023

AWS Glue	The Apache Hudi, Apache Iceberg, and Linux Foundation Delta Lake data lake formats are not supported in AWS Top Secret Regions.	October 25, 2023
AWS Lambda	Lambda doesn't support Lambda@Edge in AWS Top Secret Regions.	October 25, 2023
AWS Step Functions	Support for creating state machine versions and aliases is now available.	October 25, 2023
Amazon EMR	Version 5.36.1 now available in AWS Top Secret Regions.	October 18, 2023
Amazon ECS	Extensible Ephemeral Storage on AWS Fargate is not supported, Ephemeral StorageReservation and EphemeralStorageUtilization metrics are unavailable in CloudWatch Container Insights in AWS Top Secret Regions.	October 18, 2023
AWS Lambda	Outbound IPv6 traffic is not supported in AWS Top Secret Regions.	October 18, 2023

Amazon VPC	You cannot assign a primary private IPv4 address to the NAT gateway; one is chosen for you at random from the CIDR in the subnet. You cannot associate secondary private IPv4 addresses or secondary Elastic IP addresses to a NAT gateway.	October 11, 2023
Amazon ECS	CloudWatch Container Insights is now supported.	October 11, 2023
Amazon EC2	Amazon Linux 2023 is not available.	October 11, 2023
Amazon EC2	Attached EBS status checks are not available in AWS Top Secret Regions.	October 11, 2023
Amazon EC2	The Simplified automatic recovery feature is now available in AWS Top Secret Regions.	October 11, 2023
Amazon SNS	Payload-based message filtering is not supported.	October 4, 2023
Amazon S3	Amazon S3 now sends Event Notifications to Amazon EventBridge in AWS Top Secret Regions	October 4, 2023
Amazon ElastiCache	Increase Replica Count feature is not supported in AWS Top Secret Regions for AWS Management Console, AWS CLI, or ElastiCache API.	October 4, 2023

Amazon EKS	The Amazon EBS CSI driver is now also available as an Amazon EKS managed add-on.	October 4, 2023
Amazon EC2	The DescribeInstanceEventNotificationAttributes, RegisterInstanceEventNotificationAttributes, and DeregisterInstanceEventNotificationAttributes APIs are not available in AWS Top Secret Regions.	October 4, 2023
AWS Identity and Access Management	Updated feature differences. Removed bullet “You cannot pass session tags when you assume a role or federate a user.” Added information about the IAM control plane.	October 4, 2023
AWS KMS	The Hybrid Post-Quantum TLS feature is now available in AWS Top Secret Regions. TLS 1.3 is now available in AWS Top Secret Regions.	October 4, 2023
Amazon RDS	The maximum number of databases supported on a Microsoft SQL Server DB instance is 30 for all instance classes.	September 27, 2023
Amazon OpenSearch Service	Audit Logs are now available.	September 27, 2023
Amazon OpenSearch Service	OpenSearch version 2.5 is now supported.	September 27, 2023

AWS KMS	The `kms:ScheduleKeyDeletionPendingWindowInDays` condition key, which enables you to further constrain the values that principals can specify in the PendingWindowInDays parameter of a ScheduleKeyDeletion request, is now supported.	September 27, 2023
AWS Step Functions	The Step Functions Workflow Studio is now available.	September 27, 2023
Amazon OpenSearch Service	Amazon Cognito for OpenSearch Dashboards (previously Kibana) is not supported.	September 20, 2023
Amazon EC2 Auto Scaling	The gp3 EBS volume type can now be specified in the block device mappings for launch configurations.	September 20, 2023
Amazon Translate	Asynchronous batch translation does not support automatic language detection.	September 13, 2023
AWS Identity and Access Management	Web identity federation (authenticating using well-known web-based identity providers) is now available in AWS Top Secret Regions.	September 13, 2023

Amazon SNS	Attribute-based access controls (ABAC) for Amazon SNS resources is now supported.	September 6, 2023
AWS Lambda	Lambda now supports the ability to integrate with Amazon Elastic File System (EFS) natively.	September 6, 2023
AWS Step Functions	Integration with AWS services available as of June 16, 2023 are supported in AWS Top Secret Regions if these services are available in the Region.	September 6, 2023
Aurora	Updated Amazon S3 integrati on features.	August 30, 2023
Amazon EKS	Amazon EKS is now available in AWS Top Secret - West. Clusters running Kubernete s v1.27 or higher can use Kubernetes Secrets Store CSI driver with AWS Secrets Manager.	August 30, 2023
Amazon ECR	Encryption with customer master keys (CMKs) is now supported.	August 30, 2023
Amazon EC2 Image Builder	Image Builder is now available in AWS Top Secret Regions.	August 30, 2023
Amazon EC2	`ExportImage` and the Replace Root Volume feature is now supported.	August 30, 2023

Amazon EBS	Recycle Bin is now available in AWS Top Secret - West.	August 30, 2023
AWS Billing and Cost Management	RI discounts sharing is enabled for all accounts in AWS Top Secret Regions and cannot be disabled.	August 30, 2023
Aurora	Export to Amazon S3 is supported only for DB snapshots.	August 23, 2023
Amazon SNS	Amazon SNS now supports message batching.	August 23, 2023
Amazon RDS	Amazon RDS Custom is not available in AWS Top Secret Regions.	August 23, 2023
Amazon OpenSearch Service	OpenSearch version 2.3 is now supported.	August 23, 2023
AWS VPN	AWS Site-to-Site VPN logging feature is not available.	August 23, 2023
Resource Groups	New service launch.	August 16, 2023
Lambda	TumblingWindowInSeconds and ParallelizationFactor are not available in AWS Top Secret Regions.	August 16, 2023
Cloud Control API	Cloud Control API supports any AWS resources published on the CloudFormation registry that are either fully mutable or immutable.	August 16, 2023

Amazon EMR	Version 6.12.0 now available in AWS Top Secret Regions.	August 16, 2023
Amazon DynamoDB	Export to Amazon S3 is now available.	August 16, 2023
Amazon VPC	You can view and use AWS-managed prefix lists with security groups only except for the prefix list for Amazon DynamoDB. You cannot create, manage, or use customer-managed prefix lists.	August 9, 2023
Amazon S3	Standard retrievals for restore requests that are made through S3 Batch Operation s have the same restore times as other Standard retrieval requests for AWS Top Secret Regions.	August 9, 2023
Amazon S3	Server-side encryption with AWS KMS encryption keys (SSE-KMS)	August 9, 2023
Amazon EKS	The Amazon EFS CSI driver is only available as a self-mana ged installation. Corrected some links throughout this document.	August 9, 2023

Amazon EC2 Auto Scaling	Amazon EC2 Auto Scaling does not currently support configuring an instance refresh to set its status to failed and roll back when it detects that a specified CloudWatch alarm has gone into the `ALARM` state.	August 9, 2023
AWS Snowball Edge	Snowball Edge devices are available in the AWS Top Secret - West region.	August 9, 2023
AWS Secrets Manager	AWS Config managed rules for Secrets Manager are not supported.	August 9, 2023
AWS Data Pipeline	AWS Data Pipeline was retired from AWS Top Secret Regions.	August 9, 2023
Lambda	Provisioned concurrency is available in AWS Top Secret Regions, but Application Auto Scaling for provisioned concurrency is not available in AWS Top Secret Regions.	August 2, 2023
Amazon Route 53	AWS-managed prefix lists are not available.	August 2, 2023
Amazon RDS	Oracle on Amazon RDS doesn't support cross-Region features, except for cross-Region read replicas.	August 2, 2023
Lambda	The Python 3.11 (`python3.11`) runtime is not available in AWS Top Secret Regions.	July 26, 2023

Amazon RDS	SQL Server Web and Express editions aren't available.	July 26, 2023
Amazon EBS	The General Purpose SSD (gp3) volume type is available .	July 26, 2023
Amazon Simple Queue Service	AWS JSON protocol is not supported.	July 19, 2023
Amazon S3	In AWS Top Secret Regions, Amazon S3 Inventory does not have the Object Access Control List and Object Owner as available object metadata fields in inventory reports.	July 19, 2023
Amazon EKS	Fully private cluster functionality isn't available.	July 19, 2023
Amazon RDS	Read replicas for Amazon RDS for Oracle aren't supported.	July 12, 2023
Amazon Linux 2	Updated links.	July 12, 2023
Amazon EMR	Version 6.11.0 now available in AWS Top Secret Regions.	July 12, 2023
Amazon EC2 Auto Scaling	Instance refresh rollback features are now available in AWS Top Secret Regions.	July 12, 2023
AWS Step Functions	Support for creating state machine versions and aliases is not available.	July 12, 2023

Lambda	The Java 17 (`java17`), Ruby 3.2 (`ruby3.2`), and Python 3.10 runtimes are now available in AWS Top Secret Regions.	July 5, 2023
Amazon Simple Queue Service	Dead-letter queue (DLQ) redrive APIs are currently not supported.	July 5, 2023
Amazon EKS	Amazon EKS AWS CloudFormation resources and `Eksctl` are now available.	July 5, 2023
Amazon DynamoDB	`ReturnValuesOnConditionCheckFailure`, an optional parameter that returns the item attributes for an operation that fails a condition check, is not available.	July 5, 2023
Amazon Data Firehose	Enabling server-side encryption (SSE) with the use of Customer_MANAGED_CMKs is now supported.	July 5, 2023
AWS ParallelCluster	AWS ParallelCluster is now available in AWS Top Secret - East.	July 5, 2023
Amazon S3	Amazon S3 Bucket Keys for SSE-KMS are now available in AWS Top Secret Regions.	June 28, 2023

Amazon EC2	Capacity Reservation sharing is not supported with the Amazon EC2 console in the AWS Top Secret - West Region. It is supported only with the AWS CLI and SDKs in this Region. Capacity Reservation Fleet is not supported with the Amazon EC2 console. It is supported with the AWS CLI and SDKs only.	June 28, 2023
AWS Config	Moved the list of supported resource types to Resource Coverage by Region Availability.	June 28, 2023
AWS Systems Manager	Patch Manager is now available.	June 28, 2023
Amazon Translate	Updated content on asynchronous batch translate.	June 23, 2023
Elastic Load Balancing	Added a link to the Gateway Load Balancers User Guide.	June 21, 2023
Amazon S3	Amazon S3 Inventory reports are now available in Apache optimized row columnar (ORC) or Apache Parquet (Parquet) formats in AWS Top Secret Regions.	June 21, 2023
Amazon ECS	The `splunk` log driver is not supported.	June 21, 2023

AWS Billing and Cost Management	The AWS Cost Explorer API is not available in AWS Top Secret Regions.	June 21, 2023
AWS Step Functions	The Amazon SageMaker service integration is now available.	June 21, 2023
Amazon EC2	Amazon EC2 Instance Connect Endpoint is not available in AWS Top Secret Regions.	June 14, 2023
AWS Account Management	Account Management page added to this guide.	June 14, 2023
AWS Config	AWS Config Updates to supported resource types.	June 14, 2023
AWS Step Functions	Express Workflows are now available.	June 14, 2023
Lambda	The Ruby 3.2 (`ruby3.2`) runtime is not available.	June 7, 2023
Amazon ECS	Extensible Ephemeral Storage on AWS Fargate is not supported.	June 7, 2023

AWS KMS	The `kms:ScheduleKeyDeletionPendingWindowInDays` condition key, which enables you to further constrain the values that principals can specify in the PendingWindowInDays parameter of a ScheduleKeyDeletion request, is not supported in AWS Top Secret Regions. The feature that allows you to import key material into an AWS KMS key only supports importing symmetric key material in AWS Top Secret Regions.	June 7, 2023
AWS Resource Access Manager	AWS RAM supports resource sharing for more resource types.	June 7, 2023
Application Auto Scaling	Reworked the differences section.	May 31, 2023
Amazon VPC	DNS64 and NAT64 are not available	May 31, 2023
Amazon Route 53	Updated information: In AWS Top Secret - East and AWS Top Secret - West, you can alias to an Elastic Load Balancing (Application Load Balancer and Network Load Balancer) or VPC endpoint, but only using the AWS CLI.	May 31, 2023

AWS KMS	The key material must be a 256-bit symmetric encryption key. Importing asymmetric and HMAC keys is not supported in AWS Top Secret Regions.	May 31, 2023
AWS Step Functions	The Amazon EMR service integration is now available.	May 31, 2023
Amazon SageMaker	Add Neo and unsupported fast-file-mode and inference parameters.	May 24, 2023
Amazon EC2 Auto Scaling	Amazon EC2 Auto Scaling does not currently support the AttachTrafficSources, DetachTrafficSources, and DescribeTrafficSources API operations.	May 24, 2023
Amazon EBS	The Data Lifecycle Manager (DLM) feature is now available. Recycle Bin is now available in AWS Top Secret - East.	May 24, 2023
Cloud Control API	New service launch.	May 17, 2023
Amazon RDS	Updated the availability of SQL Server editions and DB engine versions.	May 17, 2023
AWS Snowball Edge	Snowball Edge devices in the AWS Top Secret Regions do not have an embedded GPS module.	May 17, 2023

AWS Billing and Cost Management	Savings Plans are not supported in AWS Top Secret Regions.	May 17, 2023
AWS Directory Service	AWS PrivateLink is not currently supported by AWS Directory Service.	May 17, 2023
Lambda	The `dotnet6` runtime is now available.	May 10, 2023
Amazon S3	Amazon S3 Bucket Access Points, Amazon S3 Access Points aliases, and Amazon S3 Block Public Access are now available.	May 10, 2023
Amazon EMR	Version 6.10.0 now available in AWS Top Secret Regions.	May 10, 2023
Amazon EC2	ED25519 keys are now supported when using the Amazon EC2 console.	May 10, 2023
Amazon CloudWatch Logs	Creating a subscription to stream logs data to Amazon OpenSearch Service is not supported.	May 10, 2023
AWS Snowball Edge	Snowball Edge Compute Optimized with 104 vCPUs, 416GB RAM, and 28TB SSD NVMe Storage is now available.	May 10, 2023
AWS Step Functions	Removed a note about Lambda availability in the differences list.	May 10, 2023

AWS Systems Manager	AWS AppConfig is now available in AWS Top Secret - West.	May 10, 2023
AWS Transit Gateway	Multicast is now supported.	May 10, 2023
Lambda	The Java 17 (`java17`) runtime is not available.	May 3, 2023
Amazon OpenSearch Service	Amazon OpenSearch Ingestion is not supported.	May 3, 2023
Amazon Kinesis Data Streams	Kinesis Data Streams On Demand does not support 1 GB/s increase in write capacity and 2GB/s read capacity.	May 3, 2023
Amazon EC2	AMD Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP) is not available.	May 3, 2023
AWS CloudTrail	CloudTrail Lake is not available.	May 3, 2023
AWS Transit Gateway	Transit Gateway Flow Logs is now supported.	May 3, 2023
Amazon DynamoDB	Restores are limited to 4 concurrent operations.	April 26, 2023
AWS Snowball Edge	Amazon S3 Compatible Storage on AWS Snowball Edge Compute Optimized devices is not available in AWS Top Secret Regions.	April 26, 2023

AWS CodeDeploy	AWS Lambda deployments are now supported in AWS Top Secret - West	April 26, 2023
AWS KMS	Multi-Region keys are now available in AWS Top Secret Regions.	April 26, 2023
License Manager	License Manager is now available in the AWS Top Secret Regions AWS Top Secret - West.	April 19, 2023
Lambda	The Python 3.10 runtime is not available in AWS Top Secret Regions.	April 19, 2023
Amazon Redshift	Updated links for redshift drivers.	April 19, 2023
Amazon RDS	Kerberos authentication isn't supported in the RDS console.	April 19, 2023
Amazon EFS	The Elastic Throughput mode is not available.	April 19, 2023
Amazon CloudWatch	Composite alarm action suppression with AWS CloudFormation is now supported.	April 12, 2023

AWS Snowball Edge	For Compute using EC2 instances you need to have one or more supported AMIs in your AWS account before you can add any AMIs to your job creation request otherwise you will see "You have no compatible AMIs".	April 12, 2023
Amazon RDS	Kerberos authentication is only supported for RDS for MySQL DB instances.	April 5, 2023
Amazon EKS	Amazon GuardDuty isn't available.	April 5, 2023
Amazon EC2	UEFI boot mode on Intel- and AMD-based instances is available in AWS Top Secret Regions.	April 5, 2023
Elastic Load Balancing	Elastic Load Balancing does not support standalone creation of target groups with protocol version HTTP/2 or gRPC in AWS Top Secret Regions.	March 29, 2023
Elastic Load Balancing	Network Load Balancers now support TLS in AWS Top Secret Regions.	March 29, 2023
Amazon RDS	Updated MS SQL Server features in AWS Top Secret Regions.	March 29, 2023
Amazon Linux 2	Updated links.	March 29, 2023

Amazon ElastiCache	Reader endpoints are not available in AWS Top Secret Regions.	March 29, 2023
Amazon EMR	The old Amazon EMR management console is the default console for AWS Top Secret Regions.	March 29, 2023
Amazon EMR	Version 6.9.0 now available in AWS Top Secret Regions.	March 29, 2023
AWS Snowball Edge	Snowball Edge cluster feature is now available in AWS Top Secret Regions.	March 29, 2023
Amazon EKS	Added link to Kubernetes versions in documentation.	March 22, 2023
Amazon EC2 Auto Scaling	The metric math feature for target tracking scaling policies is not available.	March 22, 2023
AWS KMS	List of HMAC keys types that cannot be created/managed with a CFN template in AWS Top Secret Regions.	March 22, 2023
Amazon OpenSearch Service	AWS::OpenSearchSer vice::Domain CloudFormation is now supported.	March 15, 2023
Amazon EKS	Amazon EKS Advanced Configuration is now available .	March 15, 2023
Amazon EC2	Stop Protection feature is now available in AWS Top Secret Regions.	March 15, 2023

Amazon CloudWatch	In the AWS Top Secret - West Region, the CloudWatch agent is not available. In AWS Top Secret - East Region, the CloudWatch agent is available .	March 15, 2023
AWS KMS	HMAC KMS keys are now available in AWS Top Secret Regions.	March 15, 2023
Lambda	Added DocumentDB as an event source (link).	March 8, 2023
Amazon Route 53	IPv6 and dual-stack Route 53 endpoint types are not supported.	March 8, 2023
AWS Serverless Application Model	Updated multi-destination connectors region availability.	March 8, 2023
Customer Compliance Guide	Customer Compliance Guide is now available.	March 1, 2023
Amazon ECS	Task definition deletion is not supported.	March 1, 2023
AWS Snowball Edge	AWS Lambda compute functionality is now available in AWS Top Secret Regions.	March 1, 2023
AWS CloudFormation	AWS Secrets Manager features are now available : RotationSchedule, Secret, SecretTargetAttachment.	March 1, 2023
AWS Config	AWS Config Updates to supported resource types.	March 1, 2023

AWS Serverless Application Model	Multi-destination connectors for AWS SAM is not available.	March 1, 2023
AWS Secrets Manager	AWS Top Secret - West is now supported.	March 1, 2023
Lambda	ReportBatchItemFailures is not available in AWS Top Secret Regions.	February 22, 2023
Amazon ECR	Amazon ECR multi-arc hitecture images are supported.	February 22, 2023
AWS Snowball Edge	Amazon EKS Anywhere on Snow is not available in AWS Top Secret Regions.	February 22, 2023
AWS DMS	Added AWS DMS 3.4.7 list of changes.	February 22, 2023
Amazon Route 53	IPv6 and dual-stack Route 53 endpoint types are now supported.	February 15, 2023
Amazon EC2 Auto Scaling	The instance refresh rollback features are not available AWS Top Secret Regions; Setting up an instance refresh to ignore or terminate instances that are in `Standby` state or protected from scale in is not supported in AWS Top Secret Regions.	February 15, 2023
AWS Direct Connect	VPC associations are available in the Top Secret Regions.	February 15, 2023

Lambda	The asynchronous invocation metrics, `AsyncEventsReceived`, `AsyncEventAge`, and `AsyncEventsDropped` are not available in AWS Top Secret Regions.	February 8, 2023
Amazon Route 53	IPv6 and dual-stack Route 53 endpoint types are not supported and IPv6 is not supported as a Route 53 rule target.	February 8, 2023
Lambda	Some EventInvokeConfig functions and parameters are not available in AWS Top Secret Regions; Maximum concurrency for Amazon SQS event sources (ScalingConfig) is not available in AWS Top Secret Regions;Lambda SnapStart is not available in AWS Top Secret Regions.	February 1, 2023
Aurora	Blue/Green Deployments and Secret Manager integration are not available for Aurora MySQL and Aurora PostgreSQL.	February 1, 2023

Amazon S3	Restore requests, at a rate of up to 1,000 transactions per second, is now supported in AWS Top Secret Regions; Amazon S3 does not support S3 Intelligent-Tiering archive access Tiers (Archive Access tier and Deep Archive Access tier) in AWS Top Secret Regions.	February 1, 2023
Amazon RDS	Blue/Green deployments and Secrets Manager integration are not supported.	February 1, 2023
AWS Elemental MediaPackage	Services listed as not available : Access logging, CloudFront distribution, CDN.	February 1, 2023
Lambda	Runtime management configuration is not available in AWS Top Secret - East or AWS Top Secret - West.	January 25, 2023
Amazon EFS	One day lifecycle policies are now supported.	January 25, 2023
Amazon EC2	Using AWS Systems Manager parameters instead of AMI IDs in launch templates is not available in AWS Top Secret Regions.	January 25, 2023

AWS CloudTrail	The IAM condition keys aws:SourceArn and aws:SourceAccount are now supported in resource policies for resources that you associate with a trail.	January 25, 2023
Amazon EC2	Simplified Auto Recovery is not available in AWS Top Secret Regions at this moment.	January 18, 2023
Amazon EKS	You can't use AWS PrivateLink to create a private connection between your VPC and Amazon EKS.	January 4, 2023
Amazon EFS	One day lifecycle policies are not supported.	January 4, 2023
Amazon EC2	`ExportImage` is not supported in AWS Top Secret Regions.	January 4, 2023
Amazon DynamoDB	The following features are not available: DynamoDB Accelerator (DAX), Import from Amazon S3, Export to Amazon S3, CloudWatch Contributor Insights for DynamoDB, NoSQL Workbench, Kinesis Data Streams integration for change capture, and PartiQL API actions.	January 4, 2023

Amazon CloudWatch Logs	AWS PrivateLink support for CloudWatch Logs is now available.	January 4, 2023
AWS Config	AWS Config Updates to supported resource types.	December 28, 2022
Amazon EFS	The updated Amazon EFS console that simplifies file system creation and management is available in AWS Top Secret - East; Creating an Amazon EFS file system automatically using the service preferred settings is available in AWS Top Secret - East.	December 21, 2022
Amazon WorkSpaces	Amazon WorkSpaces is now available in AWS Top Secret - West.	December 14, 2022
Amazon OpenSearch Service	OpenSearch version 1.3 is now supported.	December 14, 2022
Amazon EKS	Amazon EKS add-ons - Advanced Configuration isn't available.	December 14, 2022
Amazon ECR	Interface VPC endpoints(AWS PrivateLink) for Amazon ECR are supported.	December 14, 2022
AWS Directory Service	AWS CloudFormation is now supported by AWS Directory Service.	December 14, 2022

AWS Glue	AWS Glue is now available in the AWS Top Secret - East region.	December 14, 2022
AWS Step Functions	Support for using the `Map` state in Distributed mode, set up large-scale parallel workloads, and accessing cross-account resources is not available.	December 14, 2022
Amazon EFS	Elastic Throughput mode is not available.	December 7, 2022
Amazon ECS	Amazon ECS Service Connect is not supported in the us-iso-west-1 Region.	December 7, 2022
AWS KMS	External key stores, a new type of custom key store, are not supported in AWS Top Secret Regions.	November 29, 2022
Amazon Simple Queue Service	Attribute-based access control (ABAC) is not supported.	November 23, 2022
Amazon S3	Restore requests, at a rate of up to 1,000 transactions per second, is not supported in AWS Top Secret Regions.	November 23, 2022
Amazon Data Firehose	Amazon Kinesis Data Firehose is available in AWS Top Secret - West.	November 23, 2022
AWS Transit Gateway	Transit Gateway Flow Logs is not supported.	November 23, 2022

Amazon SNS	Active tracing is not supported.	November 16, 2022
Amazon ElastiCache	Redis OSS engine version 7.0 and IAM Authentication are not supported in AWS Top Secret Regions.	November 16, 2022
Amazon ECS	Service Discovery is not available in AWS Top Secret Regions.	November 16, 2022
Amazon ECS	Fargate Ephemeral Storage feature is not available in AWS Top Secret Regions.	November 16, 2022
Amazon ECS	Container Insights aren't supported for Amazon ECS Fargate.	November 16, 2022
Amazon WorkSpaces	Bring Your Own License (BYOL) is available.	November 9, 2022
Amazon EFS	Amazon EFS is available in AWS Top Secret - West.	November 9, 2022
Amazon VPC	The transfer Elastic IP address feature is not available.	November 2, 2022
Amazon OpenSearch Service	The UltraWarm feature is now available.	November 2, 2022
Amazon EventBridge	Amazon EventBridge is now availabl in AWS Top Secret Regions	November 2, 2022

Amazon EC2 Auto Scaling	Specifying a default instance warmup for an Auto Scaling group is now available in AWS Top Secret Regions.	November 2, 2022
Amazon EC2	Tags in instance metadata are now available in AWS Top Secret Regions, but are not available in the Amazon EC2 console in the AWS Top Secret - East Region. The transfer Elastic IP address feature is not available.	November 2, 2022
AWS Config	AWS Config Custom Policy rules with Guard, organizat ional deployment, remediati on actions and monitorin g config with EventBrid ge or CloudWatch are not supported in AWS Top Secret Regions.	November 2, 2022
Lambda	The FilterCriteria parameter is not available in AWS Top Secret Regions.	October 26, 2022
Amazon WorkSpaces	WorkSpace Client Diagnostic Log Uploads are not available and CreateWorkspaceImage API is now available in the AWS Top Secret Regions.	October 26, 2022
Amazon Linux 2	Removed the more informati on section.	October 26, 2022

AWS Systems Manager	A list of Systems Manager plugin download links was added.	October 26, 2022
AWS Snowball Edge	The enhanced Snowball Edge Compute Optimized with 104 vCPUs, 416GB RAM, and 28TB SSD NVMe Storage is not available in AWS Top Secret Regions.	October 25, 2022
Amazon RDS	Read replicas for SQL Server are not supported.	October 19, 2022
AWS Systems Manager	Systems Manager is now available in AWS Top Secret - West.	October 19, 2022
Elastic Load Balancing	Elastic Load Balancers in AWS Top Secret Regions now support an endpoint for PrivateLink.	October 12, 2022
AWS Transit Gateway	Transit gateway peering attachments for these AWS Top Secret Regions must be initiated from either the AWS CLI or from the AWS Top Secret - West console. Transit gateway peering attachmen ts can't be initiated from the AWS Top Secret - East console.	October 12, 2022
Amazon SWF	Support for AWS PrivateLink is only available in the AWS Top Secret - West Region.	October 5, 2022

Amazon ECR	The following task definitio n sizes are not supported: 8 vCPU, 16 vCPU.	October 5, 2022
AWS VPN	Integration with Direct Connect gateways is not supported in us-iso-west-1.	October 5, 2022
Amazon OpenSearch Service	Custom endpoints are not supported.	September 28, 2022
Amazon EC2	The Simplified automatic recovery feature is now available in AWS Top Secret Regions.	September 28, 2022
AWS KMS	Attribute-based access control (ABAC) is now fully supported in AWS Top Secret Regions.	September 28, 2022
AWS Resource Access Manager	AWS RAM is now available in AWS Top Secret - West.	September 28, 2022
AWS Transit Gateway	Transit Gateway is now available in AWS Top Secret - West.	September 28, 2022
Amazon OpenSearch Service	OpenSearch version 1.2 is now supported.	September 21, 2022
Amazon ECR	The following task definitio n sizes are not supported: 8 vCPU, 16 vCPU.	September 21, 2022
Windows AMIs	Changes to Windows AMI implementation section.	September 14, 2022
AWS CDK	Updates to installation and configuration sections.	September 14, 2022

AWS KMS	Attribute-based access control (ABAC), the ability to control access to an AWS KMS key based on its aliases and tags, is supported in the AWS Top Secret - East Region, but is not supported in the AWS Top Secret - West Region. AWS KMS does not support the kms:RequestAlias, kms:ResourceAliases, or aws:ResourceTag condition keys in key policies in the AWS Top Secret - West Region.	September 14, 2022
Aurora	Removed list of unsupported engine versions and added CLI command available.	September 7, 2022
Amazon WorkSpaces	Plus applications bundle for Windows Server 2019 Powered WorkSpaces is not available in AWS Top Secret Regions.	September 7, 2022
Amazon S3	Glacier Instant Retrieval now available in AWS Top Secret Regions	September 7, 2022
Amazon RDS	Added a CLI command to identify supported engine versions.	September 7, 2022
Amazon EKS	AWS for Fluent Bit is now available.	September 7, 2022

Amazon EC2	The Optimize CPU Options feature is now available in AWS Top Secret Regions	September 7, 2022
AWS Systems Manager	Not all Automation runbooks and SSM Command documents are available for AWS Top Secret Regions.	September 7, 2022
Amazon WorkSpaces	Graphics WorkSpaces and Bring Your Own License are not available in the AWS Top Secret Regions.	August 31, 2022
Amazon S3	Amazon S3 does not support the `GetObjectAttributes` API operation in AWS Top Secret - West and AWS Top Secret - East.	August 31, 2022
Amazon ECR	Amazon ECS Fargate is not available in the AWS Top Secret - West Region and Amazon ECS Fargate Ephemeral Storage feature is not available in AWS Top Secret Regions.	August 31, 2022
Amazon EC2	Amazon EC2 Images now supports create-restore-image-task, create-store-image-task or describe-store-image-task in the AWS Top Secret - East Region.	August 31, 2022
Amazon CloudWatch	Updated the CloudWatch Synthetics availability information.	August 31, 2022

Amazon WorkSpaces	Graphics, GraphicsPro, Graphics.g4dn, and GraphicsPro.g4dn WorkSpaces are not available in the AWS Top Secret Regions.	August 24, 2022
Amazon OpenSearch Service	The following OpenSearch versions are supported: 1.0, 1.1	August 24, 2022
Amazon EMR	The document was reworked to improve the customer experience.	August 24, 2022
Amazon S3	Amazon S3 Object Ownership now available in AWS Top Secret - West.	August 17, 2022
Amazon EBS	You can't exclude data (non-root) volumes from multi-volume snapshot sets in AWS Top Secret Regions.	August 17, 2022
AWS VPN	AWS Site-to-Site VPN integration with Transit Gateway (TGW) is available.	August 17, 2022
Amazon WorkSpaces	Added the Linux client download link and CreateWorkspaceImage API is not available in AWS Top Secret Regions.	August 3, 2022
Amazon EMR	Automatic Amazon Linux updates, as discussed in the Amazon EMR Management Guide, are not enabled in AWS Top Secret Regions.	August 3, 2022

Amazon SWF	Support for AWS PrivateLink is only available in the AWS Top Secret - East Region.	July 27, 2022
Amazon EC2	On-demand instance quotas are based on number of vCPUs in AWS Top Secret Regions.	July 27, 2022
Amazon S3	Amazon S3 Object Ownership is available using the S3 Console in AWS Top Secret - East.	July 20, 2022
Amazon EMR	Amazon EMR version 6.6.0 is now supported and instance types were updated.	July 20, 2022
Amazon ECR	Amazon ECS limit increases aren't available through AWS Service Quotas.	July 20, 2022
Amazon CloudWatch	Composite alarm action suppression with AWS CloudFormation is not supported.	July 20, 2022
Lambda	Lambda doesn't support increased ephemeral storage in AWS Top Secret Regions. Functions still have 512 MB of ephemeral storage available at /tmp in the file system.	July 13, 2022

Lambda	Lambda doesn't support the ability to integrate with Amazon Elastic File System (EFS) natively in AWS Top Secret Regions.	July 13, 2022
Lambda	Lambda doesn't support base images that conform to the Open Container Initiative (OCI) Specification formats in AWS Top Secret Regions.	July 13, 2022
Aurora	The underlying storage for Aurora grows automatically as needed, up to 128 tebibytes (TiB) instead of 64 tebibytes.	July 13, 2022
Amazon ElastiCache	Redis OSS engine version 6.0 is not available, but supported Redis OSS engine 6.2 includes all cumulative updates.	July 6, 2022
Amazon ElastiCache	Role-Based Access Control (RBAC) is not supported in AWS Top Secret Regions.	July 6, 2022
Amazon EKS	ARM, Bottlerocket, and Windows AMIs aren't available in AWS Top Secret Regions.	July 6, 2022
AWS CloudFormation	SageMaker endpoints now available.	July 6, 2022
AWS Identity and Access Management	IAM Roles Anywhere is not supported in the AWS Top Secret Regions.	July 6, 2022

Lambda	For EventSourceMapping Configuration, the MaximumBatchingWindowInSeconds parameter is not available in AWS Top Secret Regions.	June 29, 2022
Amazon EKS	Amazon EKS 1.22 now available in AWS Top Secret Regions.	June 29, 2022
Amazon CloudWatch	Choosing custom colors for metrics in the console is now available.	June 29, 2022
AWS Systems Manager	In the Session Manager capability, the Block public sharing for SSM documents feature is not available.	June 29, 2022
Amazon EC2	The Optimize CPU Options feature is not available in AWS Top Secret Regions.	June 22, 2022
Amazon DynamoDB	Global Tables no available in AWS Top Secret Regions.	June 22, 2022
Amazon CloudWatch	Anomaly detection now available.	June 22, 2022
AWS Snowball Edge	T100 Storage Device has been deprecated in the AWS Top Secret Regions.	June 22, 2022
AWS VPN	AWS Site-to-Site VPN private IP VPN with AWS Direct Connect is not available.	June 22, 2022

Amazon S3	Amazon S3 event notifications for the event type of `s3:ObjectRestore:Completed` no longer emitted on a best-effort basis only in AWS Top Secret - East.	June 15, 2022
Amazon ECR	You must explicitly specify the AWS service endpoint in the Fluent Bit output definition using the endpoint option supported by all AWS plugins.	June 15, 2022
Amazon EC2	The Stop Protection feature is not available in AWS Top Secret Regions.	June 15, 2022
Amazon EC2	The Replace Root Volume feature is not available in AWS Top Secret Regions.	June 15, 2022
Amazon EC2	The Simplified automatic recovery feature is not available in AWS Top Secret Regions.	June 15, 2022
Aurora	Logical replication now available.	June 8, 2022
Amazon CloudWatch	CloudWatch Synthetics does not support the `Names` filter parameter for the `DescribeCanaries` or `DescribeCanariesLastRun` operations.	June 8, 2022

AWS CloudFormation	Interface VPC endpoints (AWS PrivateLink) for AWS CloudFormation are not available in the AWS Top Secret - West.	June 8, 2022
Elastic Load Balancing	More than one SSL certificate per Listener is not supported in AWS Top Secret Regions.	June 1, 2022
Amazon OpenSearch Service	Fine-grained access control is supported.	June 1, 2022
Amazon RDS	SQL Server Audit option now available.	May 25, 2022
Amazon EC2	AMI deprecation is now available in AWS Top Secret Regions.	May 25, 2022
Amazon CloudWatch	CloudWatch Metrics Insights is not available.	May 25, 2022
AWS Snowball Edge	AWS Snow Family Large Data Migration Manager is not available in the AWS Top Secret Regions.	May 25, 2022
Amazon EBS	CreateSnapshots is available in AWS Top Secret Regions.	May 11, 2022
AWS CloudTrail	CloudTrail can now send events to Amazon CloudWatch Events.	May 11, 2022

AWS Health	You can navigate to the Service Health Dashboard page to view the health of all AWS services without signing in to your AWS account.	May 4, 2022
AWS Health	If you sign in to your AWS account, you can find events specific to your account and services in the Personal Health Dashboard.	May 4, 2022
AWS Health	AWS Health does not support tagging resources.	May 4, 2022
Amazon SNS	Message Data Protection is not supported.	April 27, 2022
Amazon EC2 Auto Scaling	Specifying a default instance warmup for an Auto Scaling group is not available in AWS Top Secret Regions.	April 27, 2022
Amazon Simple Queue Service	Update CloudFormation template for "Publishing a message from a VPC" section.	April 20, 2022
Amazon S3	Amazon S3 Object Ownership is not available in AWS Top Secret - West.	April 20, 2022
Amazon S3	Amazon S3 Object Ownership is not available using the S3 Console in AWS Top Secret - East.	April 20, 2022

Amazon S3	Amazon S3 strong read-after-write consistency now available in AWS Top Secret Regions.	April 20, 2022
Amazon EKS	The Amazon EBS CSI driver is only available as a self-mana ged installation.	April 20, 2022
AWS KMS	HMAC KMS keys, which generate and verify hash-based message authentic ation codes, are not available in AWS Top Secret Regions Regions. AWS KMS does not support the `GenerateMac` and `VerifyMac` APIs in AWS Top Secret Regions Regions.	April 20, 2022
Lambda	AWS Lambda Function URLs is not available in AWS Top Secret - East or AWS Top Secret - West.	April 13, 2022
Lambda	The `dotnet6` runtime is not available in AWS Top Secret Regions.	April 13, 2022
Elastic Load Balancing	Network Load Balancers in AWS Top Secret Regions do not support TLS. You can use TCP or UDP listeners. However, TLS is now available in the AWS Top Secret - West Region.	April 13, 2022

Amazon Simple Queue Service	Amazon SQS VPC Endpoints are now supported in AWS Top Secret - West.	April 13, 2022
Amazon Elastic Container Service	Amazon ECS Exec Suite not supported against Fargate Containers	April 13, 2022
Amazon ECR	Interface VPC endpoints(AWS PrivateLink) for Amazon ECR are not supported.	April 13, 2022
Amazon ECR	Interface VPC endpoints(AWS PrivateLink) for Amazon ECS are not supported.	April 13, 2022
AWS Snowball Edge	AWS Snow Device Management service is not available in AWS Top Secret Regions because AWS IoT Greengrass is not available in AWS Top Secret Regions	April 13, 2022
AWS KMS	Updated AWS KMS Transport Layer Security (TLS) endpoint details for AWS Top Secret Regions.	April 13, 2022
Amazon S3	Amazon S3 Replication Time Control (S3 RTC) is not available in AWS for AWS Top Secret Regions.	April 6, 2022
Amazon S3	Amazon S3 Object Ownership is available in AWS Top Secret Regions.	April 6, 2022

Amazon S3	Amazon S3 Replication is now available in AWS Top Secret Regions. .	April 6, 2022
Amazon EKS	Inaugural launch into AWS Top Secret Regions.	April 6, 2022
Amazon OpenSearch Service	The new `AWS::OpenSearchService::Domain` CloudFormation resource is not supported.	March 23, 2022
Amazon DynamoDB	Export to S3 is a feature not currently available in the AWS Top Secret - West.	March 23, 2022
Amazon CloudWatch Logs	CloudWatch Logs Insights is is now supported.	March 23, 2022
AWS Resource Groups Tagging API	Resource Groups Tagging API is now available in AWS Top Secret Regions.	March 23, 2022
Aurora	Update database engine information re: RDS Aurora launch.	March 16, 2022
Amazon OpenSearch Service	OpenSearch Service rebrand.	March 16, 2022
Amazon EC2 Auto Scaling	Retrieving the target lifecycle state through instance metadata is not available in AWS Top Secret Regions.	March 16, 2022

Amazon EC2 Auto Scaling	Remove: Currently, specifyin g a Lambda function as a custom termination policy for an Auto Scaling group is available only if you use the AWS CLI or an SDK.	March 16, 2022
Changing Your Account Email	Added section on changing IAM role email account.	March 9, 2022
Amazon EC2	The `lastLaunchedTime` AMI attribute is not available in AWS Top Secret Regions.	March 9, 2022
Elastic Load Balancing	Application Load Balancers and Classic Load Balancers in AWS Top Secret Regions do not support desync mitigation mode.	March 2, 2022
Amazon EC2	On-Demand Instance hibernation is not available in AWS Top Secret Regions.	March 2, 2022
Amazon EBS	Recycle Bin is not available in AWS Top Secret Regions.	March 2, 2022
Amazon EBS	Amazon EBS Snapshots Archive is not available in AWS Top Secret Regions.	March 2, 2022
Amazon EBS	You can create multi-volume snapshots of instances using the Amazon EC2 API, AWS CLI, or AWS SDKs only.	March 2, 2022

Amazon EBS	You can copy snapshots between the AWS Top Secret Regions only. You can't copy snapshots from the AWS Top Secret Regions to any other AWS Region.	March 2, 2022
Amazon EBS	Recycle Bin is not available in AWS Top Secret Regions.	March 2, 2022
AWS Snowball Edge	Snowcone is not available in AWS Top Secret Regions because AWS DataSync is not available in AWS Top Secret Regions.	March 2, 2022
AWS Snowball Edge	Snow Family Job Management Service CreateReturnShippingLabel and DescribeReturnShippingLabel API	March 2, 2022
AWS CloudFormation	The AWS CloudFormation service principal in AWS Top Secret Regions is `cloudformation.amazonaws.com` .	March 2, 2022
AWS Step Functions	Step functions update	March 2, 2022
Amazon EC2	The EC2 Reserved Instance Marketplace is not available in AWS Top Secret Regions.	February 23, 2022
Amazon EC2	Seamless domain join is not enabled in AWS Top Secret Regions.	February 23, 2022

AWS KMS	AWS KMS supports version 1.2 of Transport Layer Security (TLS) for FIPS endpoints in AWS Top Secret Regions.	February 23, 2022
AWS KMS	AWS KMS supports versions 1.0—1.2 of Transport Layer Security (TLS) for endpoints in AWS Top Secret Regions.	February 23, 2022
AWS Trusted Advisor	The AWS Security Hub integration feature is not supported.	February 23, 2022
Amazon S3	Amazon S3 Batch Replicati on is not available in AWS for AWS Top Secret Regions.	February 16, 2022
Amazon EC2 Auto Scaling	You currently cannot use an instance reuse policy to return instances to a warm pool when your Auto Scaling group scales in (terminates instances).	February 16, 2022
Amazon EC2 Auto Scaling	The warm pools feature is now available in AWS Top Secret Regions.	February 16, 2022
Amazon EC2 Auto Scaling	Amazon EC2 Auto Scaling is now supported for AWS PrivateLink in AWS Top Secret - West.	February 16, 2022

Amazon EC2 Auto Scaling	Currently, specifying a Lambda function as a custom termination policy for an Auto Scaling group is available only if you use the AWS CLI or an SDK. This option is not available from the console.	February 16, 2022
Amazon CloudWatch	The AWS PrivateLink endpoint for CloudWatch in the AWS Top Secret - East updated.	February 16, 2022
Amazon SNS	In AWS Top Secret Regions, Attribute-based access controls (ABAC) for Amazon SNS resources is not supported.	February 9, 2022
Amazon ECR	Amazon ECR doesn't emit any events to Amazon EventBrid ge in AWS Top Secret Regions.	February 9, 2022
Amazon EFS	EFS Replication is not available.	February 2, 2022
Amazon CloudWatch	AWS PrivateLink support for CloudWatch is available in the AWS Top Secret - East Region but is not available in the AWS Top Secret - West Region.	February 2, 2022

AWS KMS	AWS KMS CloudFormation resources are limited in this Region. You cannot use an AWS CloudFormation template to create or manage asymmetric KMS keys or multi-Region KMS keys (primary or replica).	February 2, 2022
Amazon EBS	Recycle Bin for EBS snapshots is not available.	January 26, 2022
Amazon DynamoDB	Updated unavailable features.	January 26, 2022
AWS Snowball Edge	The high performance NFS data transfer feature is not available on AWS Top Secret Regions Snowball Edge Storage Optimized devices because AWS DataSync is not available in the AWS Top Secret Regionss.	January 26, 2022
AWS Snowball Edge	Snowball Edge cluster feature is not available in AWS Top Secret Regions.	January 26, 2022
AWS Snowball Edge	Removed bullet "AWS Systems Manager AMIs are currently not available in AWS Top Secret Regions"	January 26, 2022
AWS CodeDeploy	AWS Lambda deployments are not supported in AWS Top Secret - West	January 26, 2022

Amazon EC2	Tags in instance metadata are currently not available in AWS Top Secret Regions.	January 19, 2022
AWS Snowball Edge	AWS Snowball with Tape Gateway is not available in AWS Top Secret Regions as AWS Storage Gateway is not available in AWS Top Secret Regions.	January 19, 2022
Amazon Simple Queue Service	The SQS dead-letter queue redrive feature is not supported.	January 5, 2022
Amazon EMR	Added content related to Log4j vulnerabilities.	January 5, 2022
AWS Resource Access Manager	Added details on how the AWS RAM implementation in AWS Top Secret Regions does not support resource sharing for all services and resource types.	January 5, 2022
Amazon S3	Amazon S3 Object Ownership is not available in AWS Top Secret Regions.	December 20, 2021
Amazon ElastiCache	PrivateLink feature is not available in AWS Top Secret Regions.	December 20, 2021

Amazon EC2	Amazon EC2 Images does not currently support `create-restore-image-task`, `create-store-image-task` or `describe-store-image-task` in AWS Top Secret Regions.	December 20, 2021
Amazon DynamoDB	Updated local versions of Amazon DynamoDB link location.	December 20, 2021
AWS DMS	Update snowball edge differences. Apple Mac no longer supported.	December 20, 2021
Lambda	Lambda does not support batch sizes greater than 10 for Lambda SQS triggers.	December 15, 2021
Aurora	Updated the list of available DB instance classes which is at Database Instance Classes.	December 15, 2021
Amazon SageMaker	Changes to intro section; new services supported	December 15, 2021
Amazon S3	Amazon S3 Lifecycle rules based on object size is not available in AWS for AWS Top Secret Regions.	December 15, 2021
Amazon Elastic Container Service	Private Registry Authentication is not supported.	December 15, 2021
Aurora	Encryption at rest now supported for the db.t2.medium DB instance.	December 8, 2021

Amazon VPC	Amazon VPC IPv6 now supported in AWS Top Secret Regions.	December 8, 2021
Amazon VPC	Amazon VPC IP Address Manager (IPAM) is not available.	December 8, 2021
Amazon Redshift	Removed multiple bullets, and update node types.	December 8, 2021
Amazon RDS	AWS Top Secret - East Encryption at rest isn't supported for the db.m2 instance class.	December 8, 2021
AWS Identity and Access Management	Removed bullet: "You cannot simulate permissio ns boundaries on IAM entities using the IAM Policy Simulator..."	December 8, 2021
Amazon VPC	Removed bullet: Inter-region VPC peering connections are not supported.	November 22, 2021
Amazon SNS	In AWS Top Secret Regions, Amazon SNS does not support message batching.	November 22, 2021
Amazon ElastiCache	Redis OSS engine 6.2 data-tiering, at-rest encryption and in-transit encryption are not available in AWS Top Secret Regions.	November 22, 2021

AWS CloudTrail	The IAM condition keys `aws:SourceArn` and `aws:SourceAccount` are not supported in resource policies for resources that you associate with a trail, such as those for Amazon S3 buckets, AWS KMS keys, or Amazon SNS topics.	November 22, 2021
AWS DMS	Removed multiple bullets in 'How AWS DMS differs section'.	November 22, 2021
AWS Config	AWS Config Rule feature launch in AWS Top Secret Regions.	November 17, 2021
AWS Config	AWS Config does not support monitoring AWS Config rules with Amazon CloudWatch Events in AWS Top Secret Regions.	November 17, 2021
Amazon RDS	Some older minor DB engine versions don't support the latest generation DB instance classes.	November 10, 2021
Amazon Linux 2	Added section on updating AMIs to work in the Region.	November 10, 2021
Amazon CloudWatch Logs	Tagging CloudWatch Logs Groups is unsupported.	November 10, 2021
API Gateway	Multi-level base path mapping is not yet available in AWS Top Secret Regions.	November 10, 2021

Amazon SQS	The Amazon SQS dead-letter queue `RedriveAllowPolicy` feature is not available.	November 7, 2021
Amazon EBS	AWS CloudTrail data events are not supported in AWS Top Secret Regions.	November 3, 2021
Amazon RDS	Performance Insights for Amazon RDS isn't supported.	October 27, 2021
Amazon EC2 Auto Scaling	The attribute-based instance type selection feature is not available.	October 27, 2021
Amazon EC2 Auto Scaling	Specifying `lowest-price` for the `OnDemandAllocationStrategy` property of a mixed instances group is currently not supported.	October 27, 2021
Amazon EC2	The attribute-based instance type selection feature for EC2 Fleet and Spot Fleet is not available.	October 27, 2021
Amazon Elastic Container Service	Amazon ECS resources are not supported CloudWatch targets	October 20, 2021
Amazon EBS	Amazon EBS Direct APIs are now available in AWS Top Secret Regions.	October 20, 2021

Amazon EBS	Amazon EBS Direct APIs are now available in AWS Top Secret Regions.	October 20, 2021
AWS CloudTrail	When logging CloudTrail data events, Amazon DynamoDB API activity on streams is currently not available.	October 20, 2021
AWS DMS	Added the endpoint informati on to the AWS CLI section of the page.	October 20, 2021
Lambda	Lambda is now available in the AWS Top Secret - West Region.	October 11, 2021
Elastic Load Balancing	Elastic Load Balancing and Network Load Balancer are now available in the AWS Top Secret - West Region.	October 11, 2021
Elastic Load Balancing	Network Load Balancers in AWS Top Secret Regions do not support configuring Application Load Balancers as targets.	October 11, 2021
Application Auto Scaling	Application Auto Scaling is now available in the AWS Top Secret - West Region.	October 11, 2021
Amazon VPC	Tag on create and vanity DNS are not supported on AWS PrivateLink.	October 11, 2021

Amazon SWF	Amazon SWF is now available in the AWS Top Secret - West Region.	October 11, 2021
Amazon SQS	Amazon SQS is now available in the AWS Top Secret - West Region.	October 11, 2021
Amazon SNS	Amazon SNS is now available in the AWS Top Secret - West Region.	October 11, 2021
Amazon S3 Glacier	Amazon S3 Glacier is now available in the AWS Top Secret - West Region.	October 11, 2021
Amazon S3	Amazon S3 is now available in the AWS Top Secret - West Region.	October 11, 2021
Amazon Route 53	Amazon Route 53 is now available in the AWS Top Secret - West Region.	October 11, 2021
Amazon Redshift	Amazon Redshift is now available in the AWS Top Secret - West Region.	October 11, 2021
Amazon RDS	Amazon RDS is now available in the AWS Top Secret - West Region.	October 11, 2021
Amazon Kinesis Data Streams	Amazon Kinesis Data Streams is now available in the AWS Top Secret - West Region.	October 11, 2021
Amazon ElastiCache	Amazon ElastiCache is now available in the AWS Top Secret - West Region.	October 11, 2021

Amazon EMR	Amazon EMR is now available in the AWS Top Secret - West Region.	October 11, 2021
Amazon ECS	Amazon ECS is now available in the AWS Top Secret - West Region.	October 11, 2021
Amazon ECR	Amazon ECR is now available in the AWS Top Secret - West Region.	October 11, 2021
Amazon EC2 Auto Scaling	Amazon EC2 Auto Scaling is now available in the AWS Top Secret - West Region.	October 11, 2021
Amazon EC2	Amazon EC2 and VM Import/Export are now available in the AWS Top Secret - West Region.	October 11, 2021
Amazon EBS	Amazon EBS is now available in the AWS Top Secret - West Region.	October 11, 2021
Amazon DynamoDB	Amazon DynamoDB is now available in the AWS Top Secret - West Region.	October 11, 2021
Amazon CloudWatch Logs	Amazon CloudWatch Logs is now available in the AWS Top Secret - West Region.	October 11, 2021
Amazon CloudWatch	Amazon CloudWatch is now available in the AWS Top Secret - West Region.	October 11, 2021

API Gateway	API Gateway is now available in the AWS Top Secret - West Region.	October 11, 2021
AWS Billing and Cost Management	AWS Billing and Cost Managements is now available in the AWS Top Secret - West Region.	October 11, 2021
AWS CloudFormation	AWS CloudFormation is now available in the AWS Top Secret - West Region.	October 11, 2021
AWS CloudTrail	AWS CloudTrail is now available in the AWS Top Secret - West Region.	October 11, 2021
AWS CodeDeploy	AWS CodeDeploy is now available in the AWS Top Secret - West Region.	October 11, 2021
AWS Config	AWS Config is now available in the AWS Top Secret - West Region.	October 11, 2021
AWS Direct Connect	AWS Direct Connect is now available in the AWS Top Secret - West Region.	October 11, 2021
AWS Identity and Access Management	AWS Identity and Access Management and AWS Security Token Service are now available in the AWS Top Secret - West Region.	October 11, 2021
AWS KMS	AWS KMS is now available in the AWS Top Secret - West Region.	October 11, 2021

AWS Step Functions	AWS Step Functions is now available in the AWS Top Secret - West Region.	October 11, 2021
AWS Trusted Advisor	AWS Trusted Advisor is now available in the AWS Top Secret - West Region.	October 11, 2021
AWS VPN	AWS VPN is now available in the AWS Top Secret - West Region.	October 11, 2021
Amazon EFS	17-character format resource IDs for EFS file system and mount target resource types are not available.	October 6, 2021
AWS Serverless Application Model	New page for AWS SAM.	October 6, 2021
AWS Secrets Manager	Multi-Region secrets are not supported.	October 6, 2021
AWS Step Functions	The Step Functions Workflow Studio and all AWS SDK service integrations are not available.	October 6, 2021
AWS Support	The AWS Support section of this guide was moved under the Services heading.	October 6, 2021

AWS Trusted Advisor	Monitoring Trusted Advisor checks with Amazon CloudWatch Events is not supported and Trusted Advisor does not support sending weekly notification emails for checks at this time.	October 6, 2021
Aurora	Enhanced monitoring is now supported.	September 29, 2021
Aurora	Enhanced monitoring and Performance Insights are now supported.	September 29, 2021
Amazon Redshift	Amazon Redshift console query editor is now available.	September 29, 2021
AWS Config	Updated the service principal information.	September 22, 2021
AWS Resource Access Manager	AWS RAM now supports resource sharing with Amazon Route 53.	September 22, 2021
AWS Trusted Advisor	Added a new page to this guide.	September 22, 2021
AWS VPN	The following APIs are not supported: GetVpnConnectionDeviceTypes and GetVpnConnectionDeviceSampleConfiguration and Sample configuration files using IKEv2 are not available.	September 22, 2021
Aurora	Updated the certificate authority information.	September 15, 2021

Amazon Elastic Container Service	Updated the RDS Certificate Authority information.	September 15, 2021
Amazon Elastic Compute Cloud	ED25519 keys are supported in the AWS CLI, but are not supported when using the Amazon EC2 console.	September 8, 2021
Amazon CloudWatch Logs	AWS PrivateLink support for CloudWatch Logs is not available	September 8, 2021
Amazon OpenSearch Service	Updated terminology for OpenSearch Service rebrand.	September 7, 2021
Application Auto Scaling	ElastiCache (Redis OSS) clusters (replication groups) are not supported.	September 1, 2021
Amazon Transcribe	Added a list of languages which are not available.	September 1, 2021
Amazon ElastiCache	Added Elasticache's S3 Bucket canonical ID.	September 1, 2021
Amazon Data Firehose	Dynamic partitioning is NOT supported.	September 1, 2021
Amazon CloudWatch	AWS PrivateLink support for CloudWatch is not available.	September 1, 2021
Elastic Load Balancing	Application Load Balancers in AWS Top Secret Regions now support Lambda functions as a target.	August 25, 2021
Amazon Elastic Compute Cloud	ED25519 keys are currently not supported .	August 25, 2021

AWS AppConfig	AWS AppConfig is now available in AWS Top Secret Regions	August 25, 2021
Amazon VPC	Traffic Mirroring and VPC Reachability Analyzer are not supported.	August 18, 2021
Amazon EFS	EC2 Launch Instance Wizard is now available.	August 18, 2021
AWS Billing and Cost Management	Reviewed and updated the entire differences section.	August 18, 2021
Amazon Route 53	Resolver Endpoints Added to Route 53 in AWS Top Secret Regions.	August 11, 2021
Amazon S3	Amazon S3 Access Points aliases are not available in AWS Top Secret Regions.	August 4, 2021
Amazon OpenSearch Service	Updated multiple items in the differences section.	August 4, 2021
License Manager	License Manager is now available in AWS Top Secret Regions.	July 28, 2021
Amazon Simple Notification Service	Tagging Amazon SNS resources is not supported.	July 28, 2021
AWS Lambda	Event destinations are not available in AWS Top Secret Regions	July 28, 2021
Amazon Elastic Compute Cloud	Custom time windows for scheduled events are currently not available.	July 21, 2021

Amazon EC2 Auto Scaling	Added service principal for Amazon EC2 Auto Scaling information.	July 21, 2021
AWS Marketplace	The AWS Marketplace section of AWS is available in AWS Top Secret Regions.	July 21, 2021
AWS Pricing Calculator	AWS Pricing Calculator now available.	July 21, 2021
Amazon Redshift	Added a list of features that are not available.	July 7, 2021
Amazon CloudWatch	Added three bullets related to CloudWatch Synthetics.	July 7, 2021
Amazon WorkSpaces	Updated the service principal information.	June 30, 2021
Amazon Elastic Container Service	Updated the service principal information.	June 30, 2021
Amazon Elastic Compute Cloud	Updated the service principal information.	June 30, 2021
Amazon EMR	Updated the service principal information.	June 30, 2021
Amazon CloudWatch	Composite alarms are now available.	June 30, 2021
API Gateway	TLS authentication is not available.	June 30, 2021
AWS CloudFormation	Updated the service principal information.	June 30, 2021
AWS CodeDeploy	Updated the service principal information.	June 30, 2021

AWS Config	Updated the service principal information.	June 30, 2021
AWS KMS	Removed a bullet "AWS KMS supports VPC endpoints in AWS Top Secret Regions. This feature lets you connect directly to AWS KMS through a private endpoint in your VPC. However, AWS KMS does not yet support VPC endpoint policies in AWS Top Secret Regions."	June 30, 2021
Aurora	Parallel query clusters are now supported in Aurora MySQL.	June 23, 2021
Amazon Simple Queue Service	Added the section titled "Publishing a message from a VPC".	June 23, 2021
Amazon Simple Notification Service	Removed three bullets and added a new section titled "Publishing a message from a VPC".	June 23, 2021
Amazon Elastic Compute Cloud	AMI deprecation is currently not available.	June 23, 2021
Amazon EFS	Amazon Elastic Container Service with Amazon EFS is now available.	June 23, 2021
AWS DMS	Added a bullet noting a discrepancy in the user guide download steps.	June 23, 2021

AWS KMS	Multi-Region keys are not available in AWS Top Secret Regions. You cannot create multi-Region primary keys or multi-Region replica keys in any AWS Top Secret Regions Region.	June 16, 2021
Aurora	Updating the certificate date from `rds-ca-2015` to `rds-ca-2019` .	June 9, 2021
Amazon S3	Support for BitTorrent is now available.	June 9, 2021
Amazon Redshift	Amazon Redshift Spectrum is not available.	June 9, 2021
Amazon Elastic Container Service	The ECS Anywhere is not supported and added note about Docker in region.	June 9, 2021
Amazon Elastic Container Service	Updated the RDS ca from `rds-ca-2015` to `rds-ca-2019` .	June 9, 2021
Amazon EC2 Auto Scaling	The gp3 EBS volume type cannot be specified in the block device mappings for launch configurations.	June 9, 2021
Amazon EC2 Auto Scaling	Removed bullet "You can create scheduled actions in UTC only. Specifying your time zone is currently not supported."	June 2, 2021

Aurora	Several unsupported features: Adding bullets for limitations in the region.	May 26, 2021
Amazon RDS	Several unsupported features: Adding bullets for limitations in the region	May 26, 2021
Amazon EMR	Amazon EMR release versions 6.3.0 is supported in AWS Top Secret Regions.	May 26, 2021
AWS Identity and Access Management	Added bullet for the identifier for a service principal.	May 26, 2021
AWS Step Functions	The Amazon EventBridge service integration is not available.	May 26, 2021
Amazon EMR	Amazon EMR release versions 5.27.1 is supported in AWS Top Secret Regions.	May 19, 2021
Amazon EC2 Auto Scaling	Describing scaling activitie s for deleted Auto Scaling groups using version 2 of the AWS CLI is currently not supported.	May 19, 2021
AWS Snowball Edge	Removed bullet "In AWS Top Secret Regions, the 1 year or 3 year commitment upfront charge model is not supported. If this is required, work with your AWS account team." in the How Snowball Edge Differs' section.	May 19, 2021

Amazon RDS	RDS Proxy is not available for Aurora MySQL and Aurora PostgreSQL.	May 12, 2021
Amazon RDS	RDS Proxy is not available for MariaDB, MySQL, and PostgreSQL.	May 12, 2021
Aurora	Size-flexible reserved DB instances aren't supported .clarified support for a couple of items.An Aurora cluster that is a read replica can't be promoted to read-writ e capability using the RDS console. To promote such a cluster, use the AWS CLI or RDS API.	May 5, 2021
Amazon SageMaker	Remove supported Tensorflo w versions bullets.And Small update for Ground Truth.	May 5, 2021
Amazon RDS	Size-flexible reserved DB instances aren't supported.	May 5, 2021
Amazon Elastic Compute Cloud	Root volume replacement for running instances is not available.	May 5, 2021
Amazon EMR	The release versions 5.33.0 is available in AWS Top Secret Regions.	May 5, 2021
Amazon EFS	Added three bullets to the section defining differences.	May 5, 2021

Amazon EC2 Auto Scaling	You cannot create a predictiv e scaling policy in AWS Top Secret Regions.	May 5, 2021
Amazon EFS	Amazon EFS is available in AWS Top Secret Regions.	May 3, 2021
Elastic Load Balancing	Network Load Balancers in AWS Top Secret Regions do not support custom private IPv4 addresses.	April 28, 2021
Amazon EC2 Auto Scaling	Removed bullet "Instance refresh checkpoints are currently not available in AWS Top Secret Regions."	April 28, 2021
AWS Config	Reworked the differences section.	April 28, 2021
Amazon EC2 Auto Scaling	The warm pools feature is currently not available in AWS Top Secret Regions.	April 21, 2021
AWS Identity and Access Management	IAM Access Analyzer policy generation is not available in AWS Top Secret Regions.	April 21, 2021
AWS Systems Manager	Adding supported predefined Systems Manager documents.	April 21, 2021
Amazon VPC	Moved VPN content to a separate page and removed bullet AWS Site-to-Site VPN integration with Global Accelerator is not available.	April 14, 2021
Amazon Elastic Container Service	The ECS CLI is not supported.	April 14, 2021

Amazon EC2 Auto Scaling	Removed multiple bullets and added Instance refresh checkpoints are currently not available.	April 14, 2021
AWS SDK for Python (Boto)	Removed note: If you're using Amazon Linux 2 AMI, the AWS SDK for Python (Boto3) is already installed and configured. (The Boto version isn't included.)	April 14, 2021
AWS CodeDeploy	To use CodeDeploy with Amazon Virtual Private Cloud, you must use CodeDeploy agent 1.3.1 or later.	April 14, 2021
AWS VPN	Created AWS Virtual Private Network section.	April 14, 2021
Amazon Elastic Compute Cloud	EC2 Serial Console is currently not available.	April 7, 2021
Amazon ElastiCache	Engine version Redis6.x is not available in AWS Top Secret Regions. Global Datastores are not available in AWS Top Secret Regions.	April 7, 2021
Amazon EMR	IMDSv2 (instance metadata service) is supported in EMR versions 5.32.0 and later, and 6.2.0 and later. There is no support for IMDSv2 in EMR versions 5.27.1 and 5.23.1	April 7, 2021
Amazon Data Firehose	Inaugural launch into AWS Top Secret Regions.	April 7, 2021

AWS Direct Connect	MAC Security (MACsec) is not supported.	April 7, 2021
Amazon Simple Queue Service	Tagging SQS resources is not supported.	March 31, 2021
Amazon Simple Notification Service	Adding multiple bullets to the document.	March 31, 2021
Amazon Route 53	Reviewed and improved the document.	March 31, 2021
Amazon Kinesis Data Streams	Reviewed and improved the document.	March 31, 2021
Amazon EMR	Reviewed and updated the document.	March 31, 2021
Amazon DynamoDB	Added 2 bullets to "How DynamoDB Differs for AWS Top Secret Regions".	March 31, 2021
Amazon CloudWatch	Removed the download link and updated Contributor Insights to not available.	March 31, 2021
AWS CloudTrail	Added bullets to "How CloudTrail Differs for AWS Top Secret Regions" and "Services Supported within CloudTrail" sections.	March 31, 2021
AWS Config	Updates to resource types and supported features.	March 31, 2021

AWS KMS	The AWS KMS console feature that lets you filter KMS keys based on their tags is not supported in AWS Top Secret Regions.	March 31, 2021
AWS Systems Manager	General document updates and removed bullet that stated support for virtual private cloud endpoints is not available.	March 31, 2021
AWS Transit Gateway	Initial Release	March 31, 2021
Amazon Athena	Initial document creation.	March 30, 2021
Amazon S3	Amazon S3 Object Lambda Access Points are not available in AWS Top Secret Regions.	March 24, 2021
Amazon Elastic Compute Cloud	UEFI boot mode on Intel- and AMD-based instances is not available.	March 24, 2021
Amazon EBS	Added multiple items in the differences section.	March 24, 2021
Amazon CloudWatch	Dashboard sharing is not available.	March 24, 2021
AWS Snowball Edge	Removed bullet AWS OpsHub for Snow Family is not available in AWS Top Secret Regions.	March 24, 2021
AWS CodeDeploy	ECS capacity providers are not supported.	March 24, 2021

AWS Directory Service	Added multiple bullets defining differences in the region.	March 24, 2021
AWS Identity and Access Management	IAM Access Analyzer policy validation checks are not available in AWS Top Secret Regions.	March 24, 2021
AWS Lambda	Updated multiple items in the differences section.	March 24, 2021
AWS Step Functions	Added multiple bullets defining differences in the region.	March 24, 2021
Amazon S3	Added five bullets to the bottom of the list of differenc es.	March 17, 2021
Amazon OpenSearch Service	Reworded and updated multiple items in the differenc es section.	March 17, 2021
Amazon EC2 Auto Scaling	You can create scheduled actions in UTC only. Specifyin g your time zone is currently not supported.	March 17, 2021
Amazon Comprehend	Amazon Comprehend Medical APIs are not supported.	March 17, 2021
Amazon CloudWatch Logs	CloudWatch Logs Insights is not available.	March 17, 2021
AWS CodeDeploy	Automatically updating outdated instances is not supported.	March 17, 2021

AWS DMS	Added five bullets to the bottom of the section on how DMS Differs for AWS Top Secret Regions.	March 17, 2021
Amazon WorkSpaces	IP-Based Access Control Groups available.	March 10, 2021
Amazon S3	S3 Replication, including Cross-Region & Same-Region replication, not available.	March 10, 2021
Amazon RDS	Deleted stray TDE bullet.	March 10, 2021
Amazon RDS	S3 export not supported.	March 10, 2021
Amazon Elastic Container Service	Numerous updates by ECS tech writer - please re-read chpater.	March 10, 2021
Amazon CloudWatch	Composite alarms not available.	March 10, 2021
AWS Health	Organizational view feature not supported.	March 10, 2021
AWS Systems Manager	Automation capability for adding attachments to the `aws:executeScript` action not available.	March 10, 2021
Amazon WorkSpaces	Added a bullet noting that WorkSpaces directories must be located in the `us-iso-1a` or the `us-iso-1b` Availability Zone.	March 3, 2021

Amazon ECR	Cross-region and cross-account replication is not supported.	March 3, 2021
API Gateway	HTTP APIs are not available.	March 3, 2021
AWS Identity and Access Management	Added a list of IAM resources that cannot use IAM tags.	March 3, 2021
Amazon Elastic Container Registry	OCI artifacts not supported.	February 24, 2021
Elastic Load Balancing	Updated Route 53 Hosted Zone ID table.	February 17, 2021
Amazon Transcribe	Custom language models not available.	February 17, 2021
Amazon Elastic Container Service	AWS Fargate Spot not available.	February 17, 2021
Amazon EMR	Release versions 5.30.0 and 6.1.0 not available.	February 17, 2021
Amazon EC2 Auto Scaling	Launch template can't be specified from the console if it has multiple network interfaces.	February 17, 2021
Elastic Load Balancing	ALB's don't support: Cognito user authentication in listener rules, Lambda functions as a target, the least outstandi ng requests algorithm, Application cookie stickines s, AWS WAF (Web Application Firewall).	February 10, 2021

Elastic Load Balancing	ELB's don't support an endpoint for PrivateLink.	February 10, 2021
Amazon VPC	Elastic IP address tagging only by using the allocate-address AWS CLI command.	February 10, 2021
Amazon SageMaker	SageMaker Search now available.	February 10, 2021
Amazon RDS	Transparent Data Encryption (TDE) now supported; but no other SQL Server options are supported.	February 10, 2021
Amazon Kinesis Data Streams	Long term retention for data streams not supported.	February 10, 2021
Elastic Load Balancing	NLBs in AWS Top Secret Regions don't support changing source IP preservat ion defaults.	February 3, 2021
Amazon RDS	Performance Insights not supported. Oracle TDE not supported.	February 3, 2021
Amazon Linux 2	Removed bullet: AWS SDK for Python (Boto3) as already being installed & configured.	February 3, 2021
Amazon Elastic Container Service	AWS Fargate now available.	February 3, 2021
Amazon Elastic Compute Cloud	Tagging AMIs and their snapshots on AMI creation now supported.	February 3, 2021

Amazon CloudWatch	Percentile statistics & High-definition metrics now available via console.	February 3, 2021
AWS KMS	Added link to Services section of AWS Top Secret Regions for AWS KMS integration.	February 3, 2021
AWS Outposts	Inaugural launch into AWS Top Secret Regions.	February 3, 2021
AWS VPN	Internet Key Exchange negotiations can't be initiated for VPN connections. Noted algorithms not supported.	February 3, 2021
Amazon RDS	Noted which versions of PostgreSQL S3 import feature are supported.	January 27, 2021
Amazon EC2 Auto Scaling	Auto Scaling group max instance types is 20.	January 27, 2021
Amazon Comprehend	Removed many restrictions previously notated as more features are now available in AWS Top Secret Regions.	January 27, 2021
AWS Elemental MediaLive	Inaugural launch into AWS Top Secret Regions.	January 27, 2021
AWS Systems Manager	Inaugural launch into AWS Top Secret Regions.	January 27, 2021
Amazon SageMaker	Noted that SageMaker Studio is not available.	January 13, 2021
Amazon Elastic Container Service	Tagging Amazon ECS resources not available.	January 13, 2021

Aurora	IAM database authentication available via the RDS console.	December 16, 2020
Aurora	Aurora PostgreSQL patch versions aren't supported: 1.7.6, 2.5.6, and 3.2.6.	December 16, 2020
Amazon SageMaker	Updated & alphabetized the features not available list.	December 16, 2020
Amazon RDS	IAM database authentic ation for RDS DB engines is supported.	December 16, 2020
Amazon Elastic Compute Cloud	AMIs and their snapshots on AMI creation cannot be tagged.	December 16, 2020
Amazon Comprehend	Custom Entity Recognition no longer restricted to just English.	December 16, 2020
AWS Direct Connect	Link Aggregation Groups (LAGs) now available.	December 16, 2020
AWS Elemental MediaPackage	Inaugural launch into AWS Top Secret Regions.	December 16, 2020
AWS KMS	The ability to control access to an AWS KMS key based on its aliases and tags is not supported.	December 16, 2020
AWS Secrets Manager	Inaugural launch into AWS Top Secret Regions.	December 16, 2020

Aurora	IAM database authentication can't be enabled in the RDS console, but only via the AWS CLI or RDS API.	November 24, 2020
Aurora	Encryption at rest not supported for db.t2.medium DB instance class.	November 24, 2020
Amazon RDS	SQL Server builds no longer restricted to the R4 instance type.	November 24, 2020
Amazon RDS	Storage autoscaling not supported.	November 24, 2020
Amazon RDS	IAM database authentic ation for RDS DB engines not supported.	November 24, 2020
Amazon RDS	PostgreSQL S3 import feature not supported.	November 24, 2020
Amazon RDS	Encryption at rest not supported for db.t2.medium DB instance class.	November 24, 2020
Amazon ElastiCache	At-rest encryption & in-transit encryption not supported.	November 24, 2020
Amazon SageMaker	SageMaker Ground Truth service now available, but its Amazon Mechanical Turk Workforce feature, auto-segm entation tool, and CloudWatc h worker metrics are not supported.	November 18, 2020

Amazon Elastic Compute Cloud	Noted that instant fleet types cannot be deleted.	November 18, 2020
Amazon Comprehend	PiiEntities APIs now available in AWS Top Secret Regions.	November 18, 2020
Amazon Translate	Inaugural launch into AWS Top Secret Regions.	November 11, 2020
Amazon RDS	Release 11.2.0.4 of Oracle Database now available.	November 11, 2020
Amazon Comprehend	Amazon Comprehend Events now available in AWS Top Secret Regions.	November 11, 2020
AWS DMS	AWS Health Dashboard (PHD) notifications are now available.	November 11, 2020
Elastic Load Balancing	Application LBs do not support registering IP addresses as targets, Network LBs do not support TLS.	November 4, 2020
Amazon SageMaker	SageMaker built-in algorithm s no longer have different ECR image paths.	November 4, 2020
Amazon RDS	Oracle Gen5 instances are available.	November 4, 2020
Amazon Elastic Compute Cloud	AWS Nitro Enclaves not available.	November 4, 2020
Amazon CloudWatch	Percentile statistics only available through CloudWatch API calls.	November 4, 2020

AWS CodeDeploy	Service principal corrected, "Getting Started Wizard" not supported, notification rules not supported.	November 4, 2020
AWS VPN	For either default VPC or EC2-Classic, the RevokeSecurityGroupEgress command now includes the security group rules that were not revoked in the output.	November 4, 2020
AWS VPN	Single Tunnel & Tunnel Replacement notifications not available.	November 4, 2020
Amazon RDS	Oracle Gen5 instances and release 11.2.0.4 not available.	October 28, 2020
Amazon Elastic Container Service	Noted special instructions for Clusters section of the console.	October 28, 2020
Amazon Elastic Container Service	CloudWatch Container Insights, Attaching Elastic Inference accelerators, ECS cluster auto scaling, & AWS Copilot not supported.	October 28, 2020
Amazon Elastic Container Registry	Image scanning, Multi-architecture images, & Encryption with customer master keys not available.	October 28, 2020

Amazon VPC	For either default VPC or EC2-Classic, the RevokeSecurityGroupEgress command does not include the security group rules that were not revoked in the output.	October 21, 2020
Amazon CloudWatch	Percentile statistics now available.	October 21, 2020
Application Auto Scaling	Noted Amazon Comprehend document classification and entity recognizer endpoints resources not supported.	October 7, 2020
Application Auto Scaling	Managed Streaming for Apache Kafka (MSK) cluster storage not supported.	September 30, 2020
Amazon RDS	S3 export is only supported for MySQL.	September 30, 2020
AWS DMS	AWS Health Dashboard (PHD) notifications are not available.	September 30, 2020
Aurora	Inaugural launch into AWS Top Secret Regions.	September 28, 2020
Application Auto Scaling	Aurora replicas are now scalable.	September 28, 2020
Amazon VPC	Customer gateway, virtual private gateway, & VPN connection now support tagging on creation.	September 16, 2020

AWS Direct Connect	AWS Direct Connect gateway no longer restricted to just virtual private gateway association.	September 16, 2020
Elastic Load Balancing	IDP endpoints need to be within the AWS Top Secret Regions WAN and not open internet.	September 2, 2020
Application Auto Scaling	SageMaker endpoint variants are now scalable.	September 2, 2020
Amazon VPC	Noted less limitations for creating transit gateway attachments.	September 2, 2020
Amazon S3	Noted bucket owner condition s & restrictions regarding account IDs.	September 2, 2020
Amazon RDS	Database activity streams aren't supported.	September 2, 2020
Amazon Elastic Compute Cloud	Provisioned IOPS SSD (io2) EBS volume type not available.	September 2, 2020
Amazon EBS	Provisioned IOPS SSD (io2) EBS volume type not available.	September 2, 2020
AWS Direct Connect	AWS Direct Connect console v2 now available in AWS Top Secret Regions. For TGW, IPv6 will not be supported . Removed virtual interface limitations.	September 2, 2020

Amazon VPC	Noted managed prefix lists can't be created, but can be viewed.	August 26, 2020
Amazon SageMaker	Search will not return results for features not available in your region.	August 26, 2020
Amazon EC2 Auto Scaling	Disable scaling policies not available from the console.	August 26, 2020
Amazon VPC	Noted tag can't be added when creating a VPC or network interface using the VPC Console.	August 19, 2020
Amazon VPC	Application & EC2 Auto Scaling endpoints now supported for AWS PrivateLink.	August 12, 2020
Amazon EC2 Auto Scaling	Instance refreshes not available from the console.	August 12, 2020
Amazon Elastic Compute Cloud	Notated EC2Launch v2 from SSM Distributor restrictions with a SSM RunCommand document not supported.	August 5, 2020
AWS VPN	Noted resource types that do not support tagging on creation.	August 5, 2020
AWS VPN	Noted APIs that do not support resource-level permissions.	August 5, 2020

Amazon RDS	Publishing database logs to Amazon CloudWatch Logs now supported for MariaDB and MySQL.	July 29, 2020
Amazon ElastiCache	Exporting ElastiCache snapshots to S3 buckets now supported.	July 29, 2020
Amazon EMR	Notated features that are not available in EMR version 5.30.1.	July 29, 2020
Amazon EMR	All Hadoop versions supported. Tez UI and YARN timeline history not available . Docker containers not available.	July 22, 2020
Amazon Redshift	New download links for new versions of drivers.	July 15, 2020
Amazon Transcribe	Amazon Transcribe inaugural launch into AWS Top Secret Regions.	July 8, 2020
Amazon SageMaker	C5 and M5 all instance types fully supported via console.	July 8, 2020
Amazon EMR	Clusters with multi-master nodes now supported via console.	July 8, 2020
AWS KMS	VPC endpoint policies not supported in AWS Top Secret Regions.	July 8, 2020

Amazon VPC	Sagemaker, Sagemaker Notebooks, Kinesis-firehose, Kinesis-sagemaker.api endpoints now supported.	July 1, 2020
Amazon EMR	Release version 5.30.0 not available in AWS Top Secret Regions.	July 1, 2020
Amazon WorkSpaces	GraphicsPro WorkSpaces & PowerPro WorkSpaces now supported.	June 24, 2020
Amazon EC2 Auto Scaling	Instance refreshes are not available.	June 24, 2020
Application Auto Scaling	Amazon EMR clusters now supported.	June 17, 2020
Amazon EMR	Automatic Scaling in Amazon EMR now supported via console.	June 17, 2020
Amazon Elastic Compute Cloud	On-Demand Capacity Reservations now available.	June 3, 2020
Amazon ElastiCache	R5, M5, & T3 Amazon EC2 instance famlies now supported.	June 3, 2020
Amazon CloudWatch	Automatic dashboards now available.	June 3, 2020
Amazon EC2	Elastic Fabric Adapter (EFA) now fully supported.	May 27, 2020
AWS Identity and Access Management	IAM tags can be used to add metadata and control permissions.	May 27, 2020

Amazon SageMaker	AWS PrivateLink for SageMaker Runtime now available.	May 6, 2020
Amazon RDS	Oracle S3 integration now supported via console.	May 6, 2020
Amazon OpenSearch Service	Amazon OpenSearch Service now available in AWS Top Secret Regions.	May 6, 2020
Amazon VPC	Support for transit gateways added.	April 29, 2020
AWS Snowball Edge	Hardware updates.	April 29, 2020
Windows AMIs	Changes to EC2Launch and EC2Config.	April 22, 2020
Amazon RDS	Publishing database logs to Amazon CloudWatch Logs is not supported for MariaDB and MySQL.	April 22, 2020
Amazon DynamoDB	BackupRestore and PointInTimeRecovery now available.	April 22, 2020
Amazon CloudWatch Logs	Encryption context with the ARN of log groups is not available.	April 22, 2020
AWS Identity and Access Management	Restrictions on simulating permissions boundaries.	April 22, 2020
Amazon EC2 Auto Scaling	Reserved instances are supported.	April 15, 2020

Amazon RDS	Amazon S3 integration is supported with Oracle using the AWS CLI only.	April 8, 2020
AWS CloudFormation	Launch templates supported.	April 8, 2020
AWS Marketplace	Initial launch of AWS Marketplace in AWS Top Secret Regions.	June 1, 2016
AWS Systems Manager	A list has been added of Regions in AWS Top Secret Regions where support is not available for patching Window Server machines with Patch Manager.	

Change	Description	Date Changed
Amazon Comprehend	NEW OR COMING SOON Amazon Comprehend is now available in AWS Top Secret Regions. See Amazon Comprehend .	March 2020
AWS Snowball Edge	NEW OR COMING SOON AWS Snowball Edge is now available in AWS Top Secret Regions. See AWS Snowball Edge .	March 2020
Amazon S3	NEW OR COMING SOON Enabled DEEP_ARCHIVE as an available storage class. See Storage Classes for Archiving Objects.	October 2019

Change	Description	Date Changed
Amazon Route 53	NEW OR COMING SOON Amazon Route 53 is now available in AWS Top Secret Regions. See Amazon Route 53 .	September 2019
Amazon SageMaker	NEW OR COMING SOON Amazon SageMaker is now available in AWS Top Secret Regions. See Amazon SageMaker .	August 2019
Amazon Elastic Container Registry and Amazon Elastic Container Service	NEW OR COMING SOON Amazon ECR and Amazon ECS are now available in AWS Top Secret Regions. See Amazon Elastic Container Registry and Amazon Elastic Container Service .	July 2019
Application Auto Scaling	NEW OR COMING SOON Application Auto Scaling is now available in AWS Top Secret Regions. See Application Auto Scaling .	June 2019
AWS Key Management Service	NEW OR COMING SOON New AWS KMS management console is now available in AWS Top Secret Regions. See Getting Started.	June 2019
Amazon EMR	NEW OR COMING SOON M5 and C5 instance types now available for Amazon EMR. See Amazon EMR .	June 2019

Change	Description	Date Changed
AWS Lambda	NEW OR COMING SOON AWS Lambda Layers, Custom AWS Lambda Runtimes, and Ruby 2.5 Runtime are now available.	June 2019
Amazon Virtual Private Cloud	NEW OR COMING SOON AWS PrivateLink in Amazon VPC is now supported.	May 2019
AWS Site-to-Site VPN	NEW OR COMING SOON Site-to-Site VPN is now supported. See AWS Site-to-Site VPN User Guide.	May 2019
Amazon DynamoDB	NEW OR COMING SOON DynamoDB Encryption at Rest is now supported. See DynamoDB Encryption at Rest.	April 2019
Amazon Elastic Compute Cloud	NEW OR COMING SOON • Enabled support for C5, C5d, M5, M5d, R5, R5d instance types. For more information, see Amazon EC2 Instance Types. • Enabled support for T2 Unlimited and T3 instance types. For more information, see Amazon EC2 Instance Types. • Enabled support for Service-Linked Roles for EC2 Auto Scaling. For more information, see Service-Linked Roles for Amazon EC2 Auto Scaling.	April 2019

Change	Description	Date Changed
Amazon API Gateway	NEW OR COMING SOON Initial release for API Gateway. See Amazon API Gateway .	February 2019
AWS Lambda	NEW OR COMING SOON Initial release for AWS Lambda. See AWS Lambda .	February 2019
Amazon RDS	NEW OR COMING SOON Amazon RDS Enables Stopping and Starting of Multi-AZ Database Instances via AWS CLI. See Amazon Relational Database Service .	January 2019
Amazon Elastic Compute Cloud	NEW OR COMING SOON Enabled support for Attaching, Detaching, and Replacing an IAM role to an instance. For more information, see Amazon EC2 IAM Roles.	January 2019
Amazon Linux 2	NEW OR COMING SOON Added information about how Amazon Linux 2 differs. See Amazon Linux 2 AMI for AWS Top Secret Regions .	December 2018
Amazon WorkSpaces	NEW OR COMING SOON Initial release for AWS Top Secret Regions. See Amazon WorkSpaces .	November 2018
AWS Step Functions	Initial release for AWS Top Secret Regions. See AWS Step Functions.	September 2018

Change	Description	Date Changed
Amazon Virtual Private Cloud	Creating a Default Subnet is now supported.	September 2018
Amazon ElastiCache	ElastiCache is launching in DCA54 with new instance families - M4s & R4s. See Amazon ElastiCache .	September 2018
Amazon Virtual Private Cloud	Enabled support for Amazon VPC NAT Gateway.	August 2018
Kinesis Data Streams	Enhanced Fan-out and HTTP/2 reads for Kinesis Data Streams. See Reading Data from Amazon Kinesis Data Streams.	August 2018
Amazon Virtual Private Cloud	Enabled support for Amazon VPC Adding IPv4 CIDR Blocks to a VPC.	August 2018
Amazon S3	Enabled ONEZONE_IA as an available storage class. See Storage Classes.	August 2018
Amazon RDS	Enabled Microsoft SQL Server as a supported database engine on Amazon RDS. See Microsoft SQL Server on Amazon RDS.	August 2018
Amazon Elastic Compute Cloud	Added support for Auto Recovery for Dedicated Instances.	August 2018
Amazon DynamoDB	Enabled support for DynamoDB Streams.	July 2018
Amazon Elastic Compute Cloud	Added support for automatic instance recovery for shared instances.	June 2018
Amazon Elastic Compute Cloud	Enabled support for dedicated hosts.	June 2018

Change	Description	Date Changed
AWS Identity and Access Managemen t	You cannot use the maximum session duration setting for a role to allow users assuming the role to request a longer 12-hour role session. API and CLI users are limited to a 1-hour maximum role session duration.	May 2018
AWS Health	Initial release for AWS Top Secret Regions. Added topic describing differences. See the section called "AWS Health" .	May 2018
Amazon Simple Storage Service	Enabled support for SSE-KMS as default encryption for Amazon S3. See Amazon Simple Storage Service .	April 2018
AWS Config	Enabled support for Elastic Load Balancing Classic Load Balancers and Amazon EC2 Auto Scaling groups. See AWS Config .	April 2018
AWS Key Management Service	Enabled support for FIPS 140-2 validated hardware security modules (HSM) and supports FIPS 140-2 validated endpoints. See the section called "AWS Key Management Service" .	April 2018
Amazon DynamoDB	Added support for Tagging for DynamoDB and Time To Live (TTL).	April 2018
AWS Deep Learning AMIs	Initial release for AWS Top Secret Regions. Added topic describing differences. See *AWS Deep Learning AMIs* .	April 2018
Elastic Load Balancing	Added support for Application Load Balancers. See the section called "Elastic Load Balancing" .	April 2018
Amazon Virtual Private Cloud	Enabled support for creating a default VPC using the CLI or API and adding security group rule descriptions using only the CLI. For more information, see Creating a default VPC and Security Groups for your VPC.	March 2018

Change	Description	Date Changed
Amazon Elastic Compute Cloud	Enabled support for `m4.16xlarge` instance types. For more information, see the section called "How Amazon EC2 Differs for AWS Top Secret Regions" .	March 2018
AWS Database Migration Service	Initial release for AWS Top Secret Regions. Added topic describing differences. See AWS Database Migration Service .	November 2017
AWS CloudFormation	Updated features for AWS CloudFormation from April 28, 2017 to June 7, 2017. See AWS CloudFormation and AWS CloudFormation Release History.	November 2017
Amazon Elastic Block Store	Enabled support for encrypted Amazon EBS boot volumes. For more information, see Amazon EBS Encryption.	October 2017
AWS Config	Enabled support for Amazon S3 buckets and Amazon CloudWatch Alarms resource types.	August 2017
Amazon Relational Database Service	Enabled MariaDB on Amazon Relational Database Service. For more information, see MariaDB on Amazon RDS.	July 2017
Amazon Virtual Private Cloud	Enabled VPC Flow Logs. For more information, see VPC Flow Logs.	July 2017
Amazon Virtual Private Cloud	Enabled the ability to reference security groups over a VPC peering connection. For more information, see Security Group Rules.	July 2017
Amazon Elastic Compute Cloud	Added support for copying AMIs. For more information, see Copying an AMI.	July 2017
AWS Snowball	Initial release for AWS Top Secret Regions. Added topic describing differences.	June 2017

Change	Description	Date Changed
AWS CloudTrail	Enabled the ability to encrypt log files and validate the integrity of log files. See AWS CloudTrail .	June 2017
Amazon Elastic Block Store	Added information about the new cost allocation support for EBS snapshots. For more information, see Amazon Elastic Block Store Volumes and Snapshots	May 2017
AWS Config	Initial release for AWS Top Secret Regions. Added topic describing differences. See AWS Config .	May 2017
Amazon CloudWatch Logs	Initial release for AWS Top Secret Regions. See Added information about standalone installation of the CloudWatch Logs agent.	May 2017
Enhanced uploader	Removed obsolete information about the enhanced uploader for Amazon S3.	May 2017
AWS CloudFormation and AWS CloudTrail	Updated differences for AWS CloudFormation and CloudTrail. See AWS CloudFormation and AWS CloudTrail .	December 2016
Amazon S3	Updated information about AWS KMS–managed keys (SSE-KMS). See Amazon Simple Storage Service .	November 2016
Amazon RDS	Added version upgrade information for the Amazon RDS service. See Amazon Relational Database Service .	November 2016
Amazon ElastiCache	Added information about the ElastiCache service. See Amazon ElastiCache .	August 22, 2016
AWS CloudFormation	Added additional information about `aws-cfn-bootstrap` and `aws-cfn-bootstrap-config-us-iso-east-1` . See AWS CloudFormation .	August 4, 2016
Amazon RDS	Updated SSL connection information about the Amazon RDS service. See Amazon Relational Database Service .	August 4, 2016

Change	Description	Date Changed
Amazon EC2	Added download links for `ixgbevf` modules to enable enhanced networking. See Amazon Elastic Compute Cloud .	July 19, 2016
Amazon EC2	Updated instance type information for Amazon EC2. See Amazon Elastic Compute Cloud .	June 23, 2016
IAM	Added information about the `iam:GetAccountEmailAddress` and `iam:UpdateAccountEmailAddress` permissions. See AWS Identity and Access Management .	June 23, 2016
Amazon DynamoDB	Added information about tools available for DynamoDB. See Amazon DynamoDB .	May 27, 2016
Amazon Simple Notification Service	Added information about signing notification deliveries and certificate authorities that Amazon SNS recognizes. See Amazon Simple Notification Service .	May 24, 2016
Amazon EC2	Added certificate information for instance identity documents. See Amazon Elastic Compute Cloud .	May 24, 2016
Amazon EMR	Added information about EMRFS encryption. See Amazon EMR .	April 14, 2016
AWS Key Management Service	Added information about AWS KMS service. See AWS Key Management Service .	April 4, 2016
Amazon EMR	Updated info about Amazon EBS volumes and D2 instances types for Amazon EMR. See Amazon EMR .	March 23, 2016
Certificates	Added a new topic about certificates and certificate authority rotation. See Digital Certificates for AWS Top Secret Regions .	January 26, 2016

Change	Description	Date Changed
Instances types	Updated list of instance types for D2 instances. See Amazon Elastic Compute Cloud .	December 16, 2015
AWS CloudFormation	Added additional information about the `cfn-hup` and `cfn-auto-loader` helper scripts. See AWS CloudFormation .	December 15, 2015
Windows AMIs	Updated information about Windows AMIs. See AWS Windows AMIs for AWS Top Secret Regions .	December 7, 2015
AWS CLI	Updated information about creating a certificate bundle for AWS CLI. See AWS CLI .	December 7, 2015
Amazon S3	Update information about supported storage classes and bucket limit increases. See Amazon Simple Storage Service .	November 11, 2015
Amazon S3 Glacier	Added information about S3 Glacier service. See Amazon S3 Glacier .	November 5, 2015
Amazon RDS	Added information about support for Oracle. See Amazon Relational Database Service .	October 28, 2015
Amazon RDS	Added information about security groups. See Amazon Relational Database Service .	October 21, 2015
Amazon Linux AMI	Added information about how the Amazon Linux AMI differs. See Amazon Linux for AWS Top Secret Regions .	October 21, 2015
Amazon DynamoDB	Updated information about the DynamoDB service. See Amazon DynamoDB .	October 19, 2015
VM Import and Windows BYOL	Added additional information about VM Import and Windows BYOL. See Amazon Elastic Compute Cloud .	October 15, 2015

Change	Description	Date Changed
Amazon Kinesis	Added information about Kinesis service. See Amazon Kinesis Data Streams .	October 14, 2015
Amazon S3	Added a difference about bucket limit increases. See Amazon Simple Storage Service .	October 14, 2015
Amazon CloudWatch	Added a difference about CloudWatch alarm actions when using the temporary security credentials. See Amazon CloudWatch .	September 21, 2015
AWS Direct Connect	Added example AWS CLI commands to configure AWS Direct Connect. See AWS Direct Connect .	July 13, 2015
Amazon Redshift	Added information about Amazon Redshift service. See Amazon Redshift .	July 13, 2015
Amazon DynamoDB	Added information about the DynamoDB service. See Amazon DynamoDB .	July 13, 2015
Amazon EMR	Updated instances types for Amazon EMR. See Amazon EMR .	June 29, 2015
AWS Direct Connect	Added information about AWS Direct Connect service. See AWS Direct Connect .	June 15, 2015
Amazon CloudWatch	Added a link to the Amazon CloudWatch Monitoring Scripts for Linux. See Amazon CloudWatch .	June 15, 2015
Windows components	Updated snapshot ID for the Windows 2012 R2 installation media. See Amazon Elastic Compute Cloud .	June 15, 2015
AWS CloudTrail	Added information about the account ID and Amazon S3 bucket policy to use with CloudTrail. See AWS CloudTrail .	June 15, 2015
AWS CloudFormation	Added a link to example AWS CloudFormation templates. See AWS CloudFormation .	May 11, 2015

Change	Description	Date Changed
Instances types	Updated list of instance types for GPU instances. See Amazon Elastic Compute Cloud .	May 5, 2015
AWS CloudFormation	Added additional information about the `cfn-init` and `cfn-signal` helper scripts. See AWS CloudFormation .	May 5, 2015
VM Import	Added information about supported instance types when importing instances. See Amazon Elastic Compute Cloud .	April 30, 2015
AWS Trusted Advisor	Added information about Trusted Advisor. See AWS Support .	April 23, 2015
Amazon S3	Added information about cross-region replication. See Amazon Simple Storage Service .	April 13, 2015
Amazon RDS	Added information about certificate rotation guidance for Amazon RDS DB instances. See Amazon Relational Database Service .	April 9, 2015
Amazon EC2	Added information about installing the latest version of the EC2Config service and upgrading Citrix drivers. See Amazon Elastic Compute Cloud .	April 6, 2015
Amazon S3	Added information about Amazon S3 event notifications. See Amazon Simple Storage Service .	March 26, 2015
IAM	Added information about policies. See AWS Identity and Access Management .	March 19, 2015
Amazon Linux AMI	Added information about setting up the Amazon EC2 CLI tools to use a proxy server.	February 25, 2015
Amazon EC2	Added information about limits for Reserved Instances. See Amazon Elastic Compute Cloud .	February 25, 2015

Change	Description	Date Changed
Amazon RDS	Updated information about Amazon RDS differences. See Amazon Relational Database Service .	February 16, 2015
Windows components	Added information about how to install Windows components. See Amazon Elastic Compute Cloud .	January 28, 2015
Amazon RDS	Updated list of Amazon RDS DB instance classes. See Amazon Relational Database Service .	January 28, 2015
Amazon EMR	Updated list of Amazon EC2 instance types for Amazon EMR. See Amazon EMR .	January 28, 2015
Amazon EC2	Updated information about instance types and Red Hat Enterprise Linux (RHEL). See Amazon Elastic Compute Cloud .	January 28, 2015
Amazon Linux AMI	Added information about the Amazon Linux AMI. See Amazon Linux for AWS Top Secret Regions .	January 21, 2015
AWS SDKs and tools	Updated information about AWS SDKs. See AWS CLI and Tools for AWS Top Secret Regions .	January 21, 2015
Amazon EMR	Updated information about Amazon EMR. See Amazon EMR .	January 21, 2015
AWS CloudFormation	Updated information about AWS CloudFormation. See AWS CloudFormation .	January 21, 2015
Instances types	Updated list of instance types with R3 and I2. See Amazon Elastic Compute Cloud .	January 6, 2015
AWS Support Center	Updated information about AWS Support Center and classification management. See AWS Support .	November 26, 2014
Enhanced uploader	Added information about how to set up the enhanced uploader for Amazon S3.	November 20, 2014

Change	Description	Date Changed
AWS CloudFormation	Updated information about how AWS CloudFormation is different. See AWS CloudFormation .	November 20, 2014
SDK for Ruby	Updated instructions for installing the SDK for Ruby. See AWS CLI and Tools for AWS Top Secret Regions .	November 20, 2014
Console	Auto Scaling console is available. See Amazon EC2 Auto Scaling .	October 27, 2014
Console	Updated instructions for opening the console. See Using the AWS Management Console .	October 27, 2014
Amazon RDS	Added a download link for a public key to use when connecting to a DB instance with SSL using the MySQL utility. See Amazon Relational Database Service .	October 27, 2014
Amazon S3	Added a note about objects and server-side encryption in Amazon S3. See Amazon Simple Storage Service .	October 27, 2014
Billing and Cost Management	Documented the account ID to use if depositing reports into an Amazon S3 bucket. See AWS Billing and Cost Management .	September 16, 2014
Amazon EC2	Added a link to the Amazon EC2 CLI Tools. See Amazon Elastic Compute Cloud .	September 16, 2014
Account email address	Added a topic that describes how to change your account email address. See Changing Your Account Email Address .	August 27, 2014
Accounts	Added information about accounts and signing up. See Getting Started with AWS Top Secret Regions , Signing Up , and Using the AWS Management Console .	August 27, 2014
Network time	Added a topic about Network Time Protocol (NTP). .	August 27, 2014

Change	Description	Date Changed
Added links	Added a topic for redirected documentation links. See Documentation Notice . Added a link to the AWS glossary.	August 9, 2014
CloudWatch	Updated list about how CloudWatch is different. See Amazon CloudWatch .	July 24, 2014
Amazon S3 and CloudWatch	Added information about server side encryption for Amazon S3 and CloudWatch Logs. See Amazon Simple Storage Service and Amazon CloudWatch .	July 17, 2014
AWS SDKs and tools	Added information about how AWS SDKs and command line tools differ for AWS Top Secret Regions. See AWS CLI and Tools for AWS Top Secret Regions .	July 2, 2014
Initial publication	This is the first publication of *AWS Top Secret Regions User Guide*. This guide provides instructions for setting up your account and identifies differences between the public AWS cloud offerings and the private AWS Top Secret Regions operational environment.	May 16, 2014

Not Applicable to AWS Top Secret Regions

It appears that you clicked an AWS Documentation link that does not apply to AWS Top Secret Regions.

We are continuously updating AWS Top Secret Regions with additional services and documentation. For a list of services and documentation you can use today, see the following page:

- Services in AWS Top Secret Regions

AWS Glossary

For the latest AWS terminology, see the AWS glossary in the *AWS Glossary Reference*.