AWS cloud sandbox

Tags: ACG

The AWS Cloud Sandbox is designed to provide a real, no-risk AWS environment for you to learn by doing on cloud along with ACG courses. We are compatible with a wide variety of tools and services, so you have as many choices as possible when working through your training. Follow along with labs, brush up on skills, or just explore.

Available services

- Amazon Certificate Manager (ACM)
- Analytics: CloudSearch
- API Gateway v1
- API Gateway V2
- Application Autoscaling
- Application Discovery Service
- AppSync
- Athena
- Auto Scaling
- AWS Fault Injection Simulator
- AWS Network Firewall Service
- Batch
- Cloud Directory
- Cloud9
- CloudFormation
- CloudFront
- CloudTrail
- CloudWatch
- CodeArtifact
- Codebuild
- CodeCommit
- CodeDeploy

- Codeguru
- CodePipeline
- Codestar
- Comprehend
- Config
- Cognito-identity
- cognito-idp
- cognito-sync
- DataPipeline
- Database Migration Service
- DocumentDB
- ds
- DynamoDB
- DynamoDB Accelerator (DAX)
- EC2 Container Registry (ECR)
- EC2 Container Service (ECS)
- Elastic Beanstalk
- Elastic Compute Cloud (EC2)
- Elastic Container Service for Kubernetes (EKS)
- Elastic File System (EFS)
- Elastic Load Balancing (ELB)
- Elastic MapReduce (EMR)
- Elastic Transcoder
- ElastiCache
- Events
- Firehose
- Glue
- Greengrass
- GuardDuty
- Health APIs and Notifications
- Identity and Access Management (IAM)
- Inspector Classic

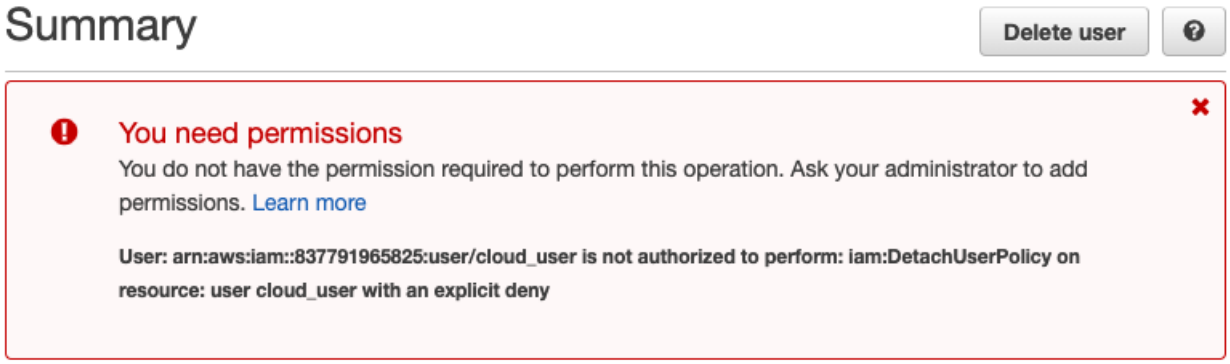
- Inspector2
- IoT
- IoT Analytics
- IoT OneClick (Projects only)
- Kafka
- Key Management Service (KMS)
- Keyspaces
- Kinesis
- Kinesis Video Streams
- Lambda
- Lex
- Machine Learning
- MachineLearning: Comprehend
- MachineLearning: Kafka
- MachineLearning: Polly
- MachineLearning: TranscribeService
- MachineLearning: Translate
- Migration Hub
- OpenSearch Service
- OpsWorks
- OpsWorksCM
- Performance Insights
- Polly
- QLDB
- Redshift
- Relational Database Service (RDS)
- Resource Groups
- Resource Groups Tagging API
- Route 53
- Route 53 Resolver
- Secrets Manager
- Security Hub

- Security Token Service (STS)
- Server Migration Service
- Simple Email Service (SES)
- Simple Notification Service (SNS)
- Simple Queue Service (SQS)
- Simple Storage Service (S3)
- Simple Systems Manager (SSM)
- States (Step Functions)
- Timestream
- Transcribe
- Translate
- Web Application Firewall (WAF) v1 ONLY
- Web Application Firewall (WAF) Regional v1 ONLY
- xray

> **Important:** This list is limited to US-EAST-1 (N. Virginia) or US-WEST-2 (Oregon). If the feature is not in this list, it is not currently offered on the AWS Cloud Sandbox.

Offered services limitations

We try to minimize the limitations of our Sandboxes to provide the most comprehensive training opportunity possible. Unfortunately, there are some limits to what we can provide. Refer to the list below for specific limits we enforce on our AWS Sandbox. You'll receive an alert if you do not have access.



All services

- No Purchasing or Billing Permissions
- Cannot modify Account settings

- Organizations
- Lightsail

S3 bucket limits

- Can only be launched in US-EAST-1 and US-WEST-2. This is to maximize the number of services available to students.

EC2 limits

- ONLY these Instance Types are allowed:
    - t2.micro to t2.medium
    - t3.micro to t3.medium
- Max Volume Size of 50GB
- Max Volume IOPS of 150
- No Elastic GPU

EMR limits

- ONLY m4.large instance type

IAM limits

- Cannot modify cloud_user or admin role
- Cannot use or set up SSO
- Additional checks enforced via Abuse Checks (bottom of page)

RDS limits

- ONLY these Instance types are allowed:
    - db.t2.micro to db.t2.medium
    - db.t3.micro to db.t3.medium
- Cannot use Provisioned IOPS
- Max Storage size of 50GB

Redshift

- ONLY dc1.large or dc2.large Instance types
- Max Cluster Node count of 3

Comprehend

- No Custom Classifiers

- No Custom Entity Recognizers
- No Custom Endpoints

Cloud Playground abuse

Cloud Playground is for educational purposes. We actively monitor Cloud Playground for abusive, prohibited, or otherwise un-awesome behavior. To avoid workarounds, we do not provide the specifics of how or what we look for. The purpose of this abuse detection is to ensure compliance with the Terms of Use (opens in new tab) agreed upon at sign-up.

A few general examples of abuse are listed below. This list is not comprehensive, so if you have any questions on your activity, please contact Support (opens email form) prior to starting the activity.

- Incorrect instance type
- Ten or more instances created at a time
- Ten or more vCPU across all instances
- Attempting to use resources for Bitcoin mining
- Excessive network traffic
- DDoS or port scanning external hosts
- Keep ECS tasks to a minimum (4 max)

Learn, have fun, and please respect the playground.

If you need help, please email Pluralsight Support (opens email form) for 24/7 assistance.