

IAM Best Practices

Zaher Dannawi, Senior Product Manager
AWS Identity and Access Management



Pop-up Loft



What to Expect from the Session

We will look at:

- **Best practices** – to help you get started
- **Demos** – “Show and Tell”



AWS Identity and Access Management (IAM)

- Enables you to control who can do what in your AWS account
- Users, groups, roles, and permissions
- Control
 - Centralized
 - Fine-grained - APIs, resources, and AWS Management Console
- Security
 - Secure (deny) by default
 - Multiple users, individual security credentials and permissions

IAM Best Practices

- **Identity and Credential Management**
- **Access Permission Management**
- **Delegation and Audit**

Identity & Credential Management



1. Create Individual users

Benefits

- Unique set of credentials
- Individual permissions
- Granular control
- Easy to revoke access

Do

- Create IAM user for yourself
- Create individual users for other

Don't

- Distribute your AWS root credentials
- Use your root account user

2. Configure a strong password policy

Benefits

- Ensures your users and data are protected
- Easy way to enforce passwords complexity requirements
- Increase account resilience against brute force login attempts

Do

- Require password expiration of 90 days
- Require passwords with:
 - ✓ MIN password length of 14
 - ✓ at least one uppercase letter
 - ✓ at least one lowercase letter
 - ✓ at least one symbol
 - ✓ at least one number

3. Rotate security credentials regularly

Benefits

- Reduces the window of potential unauthorized access
- Ensures that data cannot be accessed with old keys which might have been lost or stolen

Do

- Use **Access Key Last Used** to identify and deactivate credentials that have been unused in 90 or greater days
- Enable credential rotation for IAM users
- Use **Credential Report** to audit credential rotation.

Enabling credential rotation for IAM users

(Enable access key rotation sample policy)

Access keys

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "iam:CreateAccessKey",
      "iam:DeleteAccessKey",
      "iam:ListAccessKeys",
      "iam:UpdateAccessKey"],
    "Resource":
      "arn:aws:iam::123456789012:
      user/${aws:username}"
  ]}]}
```

Steps to rotate access keys

1. While the first set of credentials is still active, create a second set of credentials, which will also be active by default.
2. Update all applications to use the new credentials.
3. Change the state of the first set of credentials to Inactive.
4. Using only the new credentials, confirm that your applications are working well.
5. Delete the first set of credentials.

4. Enable MFA for Privileged users

Benefits

- Provides an extra layer of protection
- Increase security for console and programmatic access

Do

- Enable **MFA** for your root account
- Protect sensitive actions with **MFA**


1. Create a new user called Rob
2. Enable **MFA** for Rob
3. Set a new **password policy**

Demo
Time



Amazon Web Services (AW... x


https://aws.amazon.com

Menu  AWS re:Invent Products Solutions Pricing More English My Account Sign In to the Console

ElastiCache announces Redis Cluster support

Access up to 3.5TB of data with sub-millisecond latency

Get Started with your in-memory datastore >




Manage Your Resources

Sign In to the Console


AWS Console Mobile App
View your resources on iOS and Android devices

Download the Mobile App >




AWS re:Invent
NOVEMBER 28 - DEC. 2, 2016


AWS RE:INVENT 2016 IN LAS VEGAS
The largest global cloud computing conference. Register today



MAKE THE BEST OUT OF RE:INVENT
Sign up for the informational webinar series to get the tips and tricks!




AWS CUSTOMER STORIES
Learn how AWS is powering a revolutionary big-data solution to Major League Baseball.



AWS FEATURED PARTNER: DATADOG
See real-time granular metrics from all your AWS services. Try free

Explore Our Products



EC2 Reserved Instance Update
Two new RI capabilities make reducing EC2 costs even easier

[Learn more](#)



Manage Your Resources

[Sign In to the Console](#)

AWS Console Mobile App

View your resources on iOS and Android devices

[Download the Mobile App](#)



AWS RE:INVENT 2016 IN LAS VEGAS
The largest global cloud computing conference. Register today



MAKE THE BEST OUT OF RE:INVENT
Sign up for the informational webinar series to get the tips and tricks!




AWS CUSTOMER STORIES
Learn how AWS is powering a revolutionary big-data solution to Major League Baseball.



AWS FEATURED PARTNER: DATADOG
See real-time granular metrics from all your AWS services. Try free

Explore Our Products

Menu

amazon
web services

AWS re:Invent

Products ▾

Solutions

Pricing

More ▾

English ▾

My Account ▾

Sign In to the Console

PRODUCTS & SERVICES

AWS Console >

AWS Console Mobile App >

FAQs >

RELATED LINKS

Documentation

Articles & Tutorials

Developer Tools

Public Data Sets

Amazon Machine Images (AMIs)

Videos & Webinars

What's New

Manage Your Resources

Sign In to the Console

AWS Management Console


Access and manage Amazon Web Services through a simple and intuitive web-based user interface. You can also use the [AWS Console mobile app](#) to quickly view resources on the go.

Manage Your AWS Resources

Sign in to the Console


Features

Administer your AWS account




The Console facilitates cloud management for all aspects of your AWS account, including monitoring your monthly spending by service, managing security credentials, or even setting up new IAM Users.

Manage AWS resources from your mobile device



With the [AWS Console mobile app](#), you can quickly and easily view your existing resources, including CloudWatch alarms, and perform operational tasks from your mobile device. Download our mobile app from [Amazon Appstore](#), [Google Play](#), or [iTunes](#).

<https://console.aws.amazon.com/console/home>

amazon
web services

Access Permission Management



5. Manage permissions with groups

Benefits

- Reduces the complexity of access management as number of users grow
- Reduces the opportunity for a user to accidentally get excessive access
- Easy way to reassign permissions based on change in responsibility
- Easy way to update permissions for multiple users

Do

- Create groups that relate to job functions
- Attach policies to groups
- Use **managed policies** to logically manage permissions
- Manage group membership to assign permissions

6. Grant least privilege.

Benefits

- Minimize chances of accidentally performing privileged actions
- Easier to relax than tighten up
- More granular control

Do

- Start with a minimum set of permissions and grant additional permissions as necessary
- Restrict privileged access further with **conditions**
- Regularly check **Access Advisor** to restrict access
- Control access to specific resources using **resource-based** policy

1. Create a group and attach a managed policy
2. Manage user's permission using group membership
3. Use **Access Advisor** to identify overly permissive policies.

Demo
Time



AWS Management Console

https://us-west-2.console.aws.amazon.com/console/home?region=us-west-2

Search

AWS

Services

Edit

zackAWS

vcs21

Oregon

Support

Amazon Web Services

Compute

EC2

Virtual Servers in the Cloud

EC2 Container Service

Run and Manage Docker Containers

Elastic Beanstalk

Run and Manage Web Apps

Lambda

Run Code without Thinking about Servers

Server Migration

Migrate on-premises servers to AWS

Storage & Content Delivery

S3

Scalable Storage in the Cloud

CloudFront

Global Content Delivery Network

Elastic File System

Fully Managed File System for EC2

Glacier

Archive Storage in the Cloud

Snowball

Large Scale Data Transport

Storage Gateway

Hybrid Storage Integration

Database

RDS

Managed Relational Database Service

DynamoDB

Managed NoSQL Database

ElastiCache

In-Memory Cache

Redshift

Fast, Simple, Cost-Effective Data Warehousing

DMS

Managed Database Migration Service

Developer Tools

CodeCommit

Store Code in Private Git Repositories

CodeDeploy

Automate Code Deployments

CodePipeline

Release Software using Continuous Delivery

Management Tools

CloudWatch

Monitor Resources and Applications

CloudFormation

Create and Manage Resources with Templates

CloudTrail

Track User Activity and API Usage

Config

Track Resource Inventory and Changes

OpsWorks

Automate Operations with Chef

Service Catalog

Create and Use Standardized Products

Trusted Advisor

Optimize Performance and Security

Security & Identity

Identity & Access Management

Manage User Access and Encryption Keys

Directory Service

Host and Manage Active Directory

Inspector

Analyze Application Security

WAF

Filter Malicious Web Traffic

Certificate Manager

Provision, Manage, and Deploy SSL/TLS Certificates

Analytics

Internet of Things

AWS IoT

Connect Devices to the Cloud

Game Development

GameLift

Deploy and Scale Session-based Multiplayer Games

Mobile Services

Mobile Hub

Build, Test, and Monitor Mobile Apps

Cognito

User Identity and App Data Synchronization

Device Farm

Test Android, iOS, and Web Apps on Real Devices in the Cloud

Mobile Analytics

Collect, View and Export App Analytics

SNS

Push Notification Service

Application Services

API Gateway

Build, Deploy and Manage APIs

AppStream

Low Latency Application Streaming

CloudSearch

Managed Search Service

Elastic Transcoder

Easy-to-Use Scalable Media Transcoding

SES

Email Sending and Receiving Service

SQS

Message Queue Service

SWF

Workflow Service for Coordinating Application Components

Resource Groups

Learn more

A resource group is a collection of resources that share one or more tags. Create a group for each project, application, or environment in your account.

Create a Group

Tag Editor

Additional Resources

Getting Started

Read our documentation or view our training to learn more about AWS.

AWS Console Mobile App

View your resources on the go with our AWS Console mobile app, available from Amazon Appstore, Google Play, or iTunes.

AWS Marketplace

Find and buy software, launch with 1-Click and pay by the hour.

AWS re:Invent Announcements


Explore the next generation of AWS cloud capabilities. See what's new

Service Health

All services operating normally.

Updated: Oct 31 2016 10:27:00 GMT-0700

Service Health Dashboard



amazon
web services

[Learn more](#)

tion of

A resource group is a collection of resources that share one or more tags. Create a group for each project, application, or environment in your account.

Tag Editor

Create a Group

Additional Resources

[Getting Started](#)

Getting Started 

Read our documentation or view our training to learn more about AWS.

[AWS Console Mobile App](#)

AWS Console Mobile App 

View your resources on the go with our AWS Console mobile app, available from Amazon Appstore, Google Play, or iTunes.

[AWS Marketplace](#)

AWS Marketplace 

Find and buy software, launch with 1-Click and pay by the hour.

AlWS re invent Announcements [↗](#)

AWS re:Invent Announcements
Explore the next generation of AWS cloud capabilities. See what's new

Service Health

Service Health

 All services operating normally

✔ All services operating normally

Updated: Oct 31 2016 10:30:09 GMT-0750

Service Health Dashboard

Service Health Dashboard

AWS Management Console

https://us-west-2.console.aws.amazon.com/console/home?region=us-west-2#

Search

zackAWS @ vcs21 Oregon Support

Amazon Web Services

Compute

EC2

Virtual Servers in the Cloud

EC2 Container Service

Run and Manage Docker Containers

Elastic Beanstalk

Run and Manage Web Apps

Lambda

Run Code without Thinking about Servers

Server Migration

Migrate on-premises servers to AWS

Storage & Content Delivery

S3

Scalable Storage in the Cloud

CloudFront

Global Content Delivery Network

Elastic File System

Fully Managed File System for EC2

Glacier

Archive Storage in the Cloud

Snowball

Large Scale Data Transport

Storage Gateway

Hybrid Storage Integration

Database

RDS

Managed Relational Database Service

DynamoDB

Managed NoSQL Database

ElastiCache

In-Memory Cache

Redshift

Fast, Simple, Cost-Effective Data Warehousing

DMS

Managed Database Migration Service

Developer Tools

CodeCommit

Store Code in Private Git Repositories

CodeDeploy

Automate Code Deployments

CodePipeline

Release Software using Continuous Delivery

Management Tools

CloudWatch

Monitor Resources and Applications

CloudFormation

Create and Manage Resources with Templates

CloudTrail

Track User Activity and API Usage

Config

Track Resource Inventory and Changes

OpsWorks

Automate Operations with Chef

Service Catalog

Create and Use Standardized Products

Trusted Advisor

Optimize Performance and Security

Security & Identity

Identity & Access Management

Manage User Access and Encryption Keys

Directory Service

Host and Manage Active Directory

Inspector

Analyze Application Security

WAF

Filter Malicious Web Traffic

Certificate Manager

Provision, Manage, and Deploy SSL/TLS Certificates

Analytics

Internet of Things

AWS IoT

Connect Devices to the Cloud

Game Development

GameLift

Deploy and Scale Session-based Multiplayer Games

Mobile Services

Mobile Hub

Build, Test, and Monitor Mobile Apps

Cognito

User Identity and App Data Synchronization

Device Farm

Test Android, iOS, and Web Apps on Real Devices in the Cloud

Mobile Analytics

Collect, View and Export App Analytics

SNS

Push Notification Service

Application Services

API Gateway

Build, Deploy and Manage APIs

AppStream

Low Latency Application Streaming

CloudSearch

Managed Search Service

Elastic Transcoder

Easy-to-Use Scalable Media Transcoding

SES

Email Sending and Receiving Service

SQS

Message Queue Service

SWF

Workflow Service for Coordinating Application Components

Resource Groups

Learn more

A resource group is a collection of resources that share one or more tags. Create a group for each project, application, or environment in your account.

Create a Group Tag Editor

Additional Resources

Getting Started

Read our documentation or view our training to learn more about AWS.

AWS Console Mobile App

View your resources on the go with our AWS Console mobile app, available from Amazon Appstore, Google Play, or iTunes.

AWS Marketplace

Find and buy software, launch with 1-Click and pay by the hour.

AWS re:Invent Announcements

Explore the next generation of AWS cloud capabilities. See what's new

Service Health

All services operating normally.

Updated: Oct 31 2016 11:21:08 GMT-0700

Service Health Dashboard



Delegation & Audit

7. Use IAM roles to share access

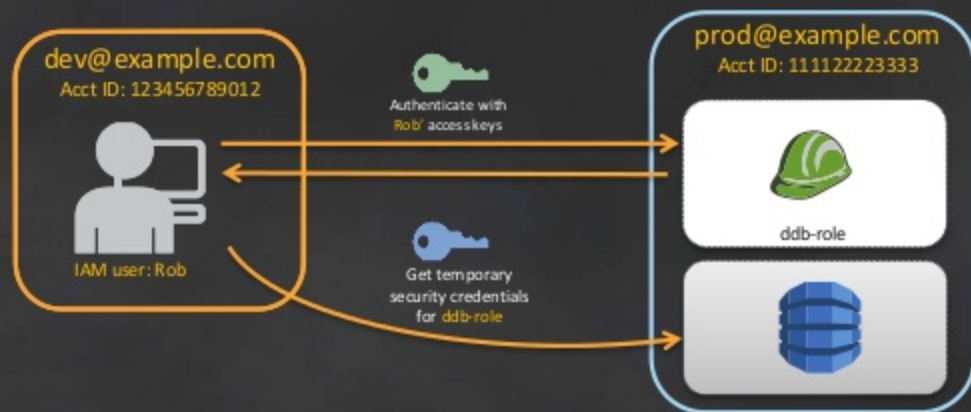
Benefits

- No need to share security credentials
- No need to store long-term credentials
- Control who has access

Do

- Use **roles** to delegate cross-account access
- Use **roles** to delegate access within an account
- Use **roles** to provide access for federated users

How does federated access work?



ddb-role trusts IAM users from the AWS account
dev@example.com (123456789012)

```
{ "Statement": [
  {
    "Effect": "Allow",
    "Principal": {"AWS": "123456789012"},
    "Action": "sts:AssumeRole"
  }
]}
```

Permissions assigned to **ddb-role**

```
{ "Statement": [
  {
    "Action": [
      "dynamodb:GetItem",
      "dynamodb:BatchGetItem",
      "dynamodb:DescribeTable",
      "dynamodb:ListTables"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }
]}
```

Permissions assigned to
Rob granting him
permission to assume **ddb-
role** in account B

Call AWS APIs using
temporary security
credentials
of **ddb-role**

```
{ "Statement": [
  {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource":
      "arn:aws:iam::111122223333:role/ddb-role"
  }
]}
```

8. Use IAM roles for Amazon EC2 instances.

Benefits

- Easy to manage access keys on EC2 instances
- Automatic key rotation
- AWS SDKs fully integrated
- AWS CLI fully integrated

Do

- Use **roles** instead of long term credentials
- Assign least privilege to the application

9. Enable AWS CloudTrail to get logs of API calls

Benefits

- Enables API activity monitoring in your account
- Enables security analysis, resource tracking and compliance auditing

Do

- Ensure **AWS CloudTrail** is enabled in all regions
- Ensure **AWS CloudTrail** log file validation is enabled
- Ensure the **Amazon S3** bucket of **CloudTrail** logs is not publicly accessible

1. Use **Switch Role** between two accounts
2. Attach a role to a running EC2 instance
3. Enable **AWS CloudTrail** for the account

Demo
Time



Amazon Web Services

Compute

- EC2**
Virtual Servers in the Cloud
- EC2 Container Service**
Run and Manage Docker Containers
- Elastic Beanstalk**
Run and Manage Web Apps
- Lambda**
Run Code without Thinking about Servers
- Server Migration**
Migrate on-premises servers to AWS

Storage & Content Delivery

- S3**
Scalable Storage in the Cloud
- CloudFront**
Global Content Delivery Network
- Elastic File System**
Fully Managed File System for EC2
- Glacier**
Archive Storage in the Cloud
- Snowball**
Large Scale Data Transport
- Storage Gateway**
Hybrid Storage Integration

Database

- RDS**
Managed Relational Database Service
- DynamoDB**
Managed NoSQL Database
- ElastiCache**
In-Memory Cache
- Redshift**
Fast, Simple, Cost-Effective Data Warehousing
- DMS**
Managed Database Migration Service

Developer Tools

- CodeCommit**
Store Code in Private Git Repositories
- CodeDeploy**
Automate Code Deployments
- CodePipeline**
Release Software using Continuous Delivery

Management Tools

- CloudWatch**
Monitor Resources and Applications
- CloudFormation**
Create and Manage Resources with Templates
- CloudTrail**
Track User Activity and API Usage
- Config**
Track Resource Inventory and Changes
- OpsWorks**
Automate Operations with Chef
- Service Catalog**
Create and Use Standardized Products
- Trusted Advisor**
Optimize Performance and Security

Security & Identity

- Identity & Access Management**
Manage User Access and Encryption Keys
- Directory Service**
Host and Manage Active Directory
- Inspector**
Analyze Application Security
- WAF**
Filter Malicious Web Traffic
- Certificate Manager**
Provision, Manage, and Deploy SSL/TLS Certificates

Analytics

Internet of Things

- AWS IoT**
Connect Devices to the Cloud

Game Development

- GameLift**
Deploy and Scale Session-based Multiplayer Games

Mobile Services

- Mobile Hub**
Build, Test, and Monitor Mobile Apps
- Cognito**
User Identity and App Data Synchronization
- Device Farm**
Test Android, iOS, and Web Apps on Real Devices in the Cloud
- Mobile Analytics**
Collect, View and Export App Analytics
- SNS**
Push Notification Service

Application Services

- API Gateway**
Build, Deploy and Manage APIs
- AppStream**
Low Latency Application Streaming
- CloudSearch**
Managed Search Service
- Elastic Transcoder**
Easy-to-Use Scalable Media Transcoding
- SES**
Email Sending and Receiving Service
- SQS**
Message Queue Service
- SWF**
Workflow Service for Coordinating Application Components

Resource Groups [Learn more](#)

A resource group is a collection of resources that share one or more tags. Create a group for each project, application, or environment in your account.

[Create a Group](#)[Tag Editor](#)

Additional Resources

Getting Started [↗](#)

Read our [documentation](#) or view our [training](#) to learn more about AWS.

AWS Console Mobile App [↗](#)

View your resources on the go with our AWS Console mobile app, available from [Amazon Appstore](#), [Google Play](#), or [iTunes](#).

AWS Marketplace [↗](#)

Find and buy software, launch with 1-Click and pay by the hour.

AWS re:Invent Announcements [↗](#)

Explore the next generation of AWS cloud capabilities. [See what's new](#)

Service Health

✓ All services operating normally.

Updated: Oct 31 2016 12:47:00 GMT-0700

[Service Health Dashboard](#)

Amazon Web Services

Compute

- EC2**
Virtual Servers in the Cloud
- EC2 Container Service**
Run and Manage Docker Containers
- Elastic Beanstalk**
Run and Manage Web Apps
- Lambda**
Run Code without Thinking about Servers
- Server Migration**
Migrate on-premises servers to AWS

Storage & Content Delivery

- S3**
Scalable Storage in the Cloud
- CloudFront**
Global Content Delivery Network
- Elastic File System**
Fully Managed File System for EC2
- Glacier**
Archive Storage in the Cloud
- Snowball**
Large Scale Data Transport
- Storage Gateway**
Hybrid Storage Integration

Database

- RDS**
Managed Relational Database Service
- DynamoDB**
Managed NoSQL Database
- ElastiCache**
In-Memory Cache
- Redshift**
Fast, Simple, Cost-Effective Data Warehousing
- DMS**
Managed Database Migration Service

Developer Tools

- CodeCommit**
Store Code in Private Git Repositories
- CodeDeploy**
Automate Code Deployments
- CodePipeline**
Release Software using Continuous Delivery

Management Tools

- CloudWatch**
Monitor Resources and Applications
- CloudFormation**
Create and Manage Resources with Templates
- CloudTrail**
Track User Activity and API Usage
- Config**
Track Resource Inventory and Changes
- OpsWorks**
Automate Operations with Chef
- Service Catalog**
Create and Use Standardized Products
- Trusted Advisor**
Optimize Performance and Security

Security & Identity

- Identity & Access Management**
Manage User Access and Encryption Keys
- Directory Service**
Host and Manage Active Directory
- Inspector**
Analyze Application Security
- WAF**
Filter Malicious Web Traffic
- Certificate Manager**
Provision, Manage, and Deploy SSL/TLS Certificates

Analytics

Internet of Things

- AWS IoT**
Connect Devices to the Cloud

Game Development

- GameLift**
Deploy and Scale Session-based Multiplayer Games

Mobile Services

- Mobile Hub**
Build, Test, and Monitor Mobile Apps
- Cognito**
User Identity and App Data Synchronization
- Device Farm**
Test Android, iOS, and Web Apps on Real Devices in the Cloud
- Mobile Analytics**
Collect, View and Export App Analytics
- SNS**
Push Notification Service

Application Services

- API Gateway**
Build, Deploy and Manage APIs
- AppStream**
Low Latency Application Streaming
- CloudSearch**
Managed Search Service
- Elastic Transcoder**
Easy-to-Use Scalable Media Transcoding
- SES**
Email Sending and Receiving Service
- SQS**
Message Queue Service
- SWF**
Workflow Service for Coordinating Application Components

Resource Groups [Learn more](#)

A resource group is a collection of resources that share one or more tags. Create a group for each project, application, or environment in your account.

Create a Group

Tag Editor

Additional Resources

Getting Started

Read our [documentation](#) or view our [training](#) to learn more about AWS.

AWS Console Mobile App

View your resources on the go with our AWS Console mobile app, available from [Amazon Appstore](#), [Google Play](#), or [iTunes](#).

AWS Marketplace

Find and buy software, launch with 1-Click and pay by the hour.

AWS re:Invent Announcements

Explore the next generation of AWS cloud capabilities. [See what's new](#)

Service Health

All services operating normally.

Updated: Oct 31 2016 12:41:00 GMT-0700

[Service Health Dashboard](#)

AWS Management Console

Deleting a Trail - AWS Cloud...

+

https://us-west-2.console.aws.amazon.com/console/home?region=us-west-2

cloudtrail disable

AWS

Services

Edit

zackAWS vcs21 Oregon Support

Amazon Web Services

Compute

EC2

Virtual Servers in the Cloud

EC2 Container Service

Run and Manage Docker Containers

Elastic Beanstalk

Run and Manage Web Apps

Lambda

Run Code without Thinking about Servers

Server Migration

Migrate on-premises servers to AWS

Storage & Content Delivery

S3

Scalable Storage in the Cloud

CloudFront

Global Content Delivery Network

Elastic File System

Fully Managed File System for EC2

Glacier

Archive Storage in the Cloud

Snowball

Large Scale Data Transport

Storage Gateway

Hybrid Storage Integration

Database

RDS

Managed Relational Database Service

DynamoDB

Managed NoSQL Database

ElastiCache

In-Memory Cache

Redshift

Fast, Simple, Cost-Effective Data Warehousing

DMS

Managed Database Migration Service

Developer Tools

CodeCommit

Store Code in Private Git Repositories

CodeDeploy

Automate Code Deployments

CodePipeline

Release Software using Continuous Delivery

Management Tools

CloudWatch

Monitor Resources and Applications

CloudFormation

Create and Manage Resources with Templates

CloudTrail

Track User Activity and API Usage

Config

Track Resource Inventory and Changes

OpsWorks

Automate Operations with Chef

Service Catalog

Create and Use Standardized Products

Trusted Advisor

Optimize Performance and Security

Security & Identity

Identity & Access Management

Manage User Access and Encryption Keys

Directory Service

Host and Manage Active Directory

Inspector

Analyze Application Security

WAF

Filter Malicious Web Traffic

Certificate Manager

Provision, Manage, and Deploy SSL/TLS Certificates

Analytics

Internet of Things

AWS IoT

Connect Devices to the Cloud

Game Development

GameLift

Deploy and Scale Session-based Multiplayer Games

Mobile Services

Mobile Hub

Build, Test, and Monitor Mobile Apps

Cognito

User Identity and App Data Synchronization

Device Farm

Test Android, iOS, and Web Apps on Real Devices in the Cloud

Mobile Analytics

Collect, View and Export App Analytics

SNS

Push Notification Service

Application Services

API Gateway

Build, Deploy and Manage APIs

AppStream

Low Latency Application Streaming

CloudSearch

Managed Search Service

Elastic Transcoder

Easy-to-Use Scalable Media Transcoding

SES

Email Sending and Receiving Service

SQS

Message Queue Service

SWF

Workflow Service for Coordinating Application Components

Resource Groups

Learn more

A resource group is a collection of resources that share one or more tags. Create a group for each project, application, or environment in your account.

Create a Group

Tag Editor

Additional Resources

Getting Started

Read our documentation or view our training to learn more about AWS.

AWS Console Mobile App

View your resources on the go with our AWS Console mobile app, available from Amazon Appstore, Google Play, or iTunes.

AWS Marketplace

Find and buy software, launch with 1-Click and pay by the hour.

AWS re:Invent Announcements

Explore the next generation of AWS cloud capabilities. See what's new

Service Health

All services operating normally.

Updated: Nov 07 2016 17:32:06 GMT-0800

Service Health Dashboard

amazon

web services

10. Reduce or remove use of root.

Benefits

- Reduces the risk of accidental changes and unintended disclosure of highly privileged credentials

Do

- Enable **MFA** for root account user
- If possible, remove root access keys
- Use a strong password for your account
- Use individual users

Top 10 IAM best practices

1. **Users** – Create individual users.
2. **Password** – Configure a strong password policy.
3. **Rotate** – Rotate security credentials regularly.
4. **MFA** – Enable MFA for privileged users.
5. **Groups** – Manage permissions with groups.
6. **Permissions** – Grant least privilege.
7. **Sharing** – Use IAM roles to share access.
8. **Roles** – Use IAM roles for Amazon EC2 instances.
9. **Auditing** – Enable AWS CloudTrail to get logs of API calls.
10. **Root** – Reduce or remove use of root.



Pop-up Loft

Questions?





Pop-up Loft

Everything and Anything Startups Need to Get Started on AWS

aws.amazon.com/activate