aws cloudshell - Alternative to AWS CLI

Universal
Date 8 Apr
Page No.

IAM (Global)
(Identity and access Management)

IAM is a web service that helps you securely control access to AWS resources. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.

(1.) There is an Indentity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user.

IAM Features

(1) Shared access to your AWS account -

You can grant other people permission to admin adminster and use resources in your AWS account without having to share your password or access key.

(2) Granular permissions -

You can grant different permissions to different people for different resources.

(3) Secure access to AWS resources for applications that run on Amazon EC2 -

You can

use IAM features to securely provide credentials for applications that runs on EC2 instances. These credentials provide permissions for your application to access other AWS resources.

(4) Multi-factor authentication (MFA) -

You can add two factor authentication to your account and to individual users for extra security.

(5) Identity Federation -

You can allow users who already have passwords elsewhere to get temporary access to your AWS account.

(6) Identity Information for assurance -

If you use AWS CloudTrail, you receive log records that include information about those who made requests for resources in your account.

(7) PCI DSS Compliance -

IAM supports the processing, storage and transmission of credit card data by a merchant or service provider and has been validated as being compliant with Payment Card Industry (PCI) Data security standard (DSS).

(8) Integrated with many AWS services -

(9) Eventually Consistent -

IAM, like many other AWS services, is eventually consistent.

(10) Free to use -

IAM & STS (security Token service) are features of your AWS account offered at no additional charge.

Terms

(i) Resources -

The user, group, role, policy and identity provider objects that are stored in IAM.

(ii) Identities -

The IAM resource objects that are used to identify and group. These include users, groups and roles.

(iii) Entities -

The IAM resource objects that AWS uses for authentication. These include IAM users, federated users and assumed IAM roles.

(iv) Principals -

A person or application that uses the AWS account root user,

on IAM user or on IAM role to sign in and make requests to AWS.

Entities represent the actors on the system, and they may each have multiple Identities.

Principal

A principal is a person or application that can make a request for an action or operation on an AWS Resource. The principal is authenticated as the AWS account root user or an IAM entity to make requests to AWS.

Request

The request includes the following information

(i) Action or operations -

The actions or operations that the principal wants to perform.

(ii) Resource - The AWS Resource object upon which the actions or operations are performed.

(iii) Principal -

The person or application that used an entity (user or role) to send the request.

(iv) Environment data -

Information about the IP addresses

Access key ID ~= UserName
Secret Access key ~= Password

Universal
Mon Tue Wed Thu Fri Sat
Date / /
Page No.

user agent, SSL enabled status or the time of day.

(v) Resource data -

Data related to the resource that is being requested.

Users

(1) Root User
(2) IAM Users
(3) Federating existing Users

IAM Roles

Some AWS Service will need to perform actions on your behalf. To do so we will assign permissions to AWS services with IAM Roles.

Policies

→ JSON document that outlines permissions for users or groups.

(1) Identity based policies -

Identity based policies are permissions policies that you attach to an IAM identity, such as an IAM user, group or role. Identity based policies control what actions the identity can perform, on which resources and under what conditions. Identity-based policy can be further categorized -

(i) Managed policies -

Standalone identity-based policy that you can attach to multiple users, groups and roles in your AWS account.

(a) AWS Managed policies -

Managed policies that are created and managed by AWS.

(b) Customer Managed policies-

Managed policies that you create and manage in your AWS account.

(ii) Inline policies-

Policies that you create and manage and that are embedded directly into a single user, group or role.

(2) Resource - based policies-

Resource - based policies control what actions a specified principal can perform on that resource and under what conditions. Resource - based policies are inline policies and there are no managed resource - based policies.

The IAM service supports only one type of resource - based policy called a role-trust policy, which is attached to an IAM role.

ABAC

(Attribute - based access Control)

ABAC is an authorization strategy that defines permissions based on attributes. In AWS, these attributes are called tags. You can create a single ABAC policy or small set of policies for your IAM principals. These ABAC policies can be designed to allow operations

$ aws <command> <subcommand> [options and parameters]

when the principal's tag matches the resources tag.

Amazon EC2 (Elastic Compute Cloud)

Amazon EC2 provides scalable computing capacity in the Amazon Web services cloud. Amazon EC2 is hosted in multiple locations world-wide. These locations are composed of Regions, Availability zones, Local zones, AWS outposts and wavelength zones.

$ aws ec2 describe-key-pairs --key-name ec22
↓ keyname

$ aws ec2 delete-key-pair --key-name ec22

$ aws ec2 create-security-group --group-name "my-sg" --description "my command line sg" --vpc-id vpc-f8c53693

$ aws ec2 describe-security-groups --group-ids sg-903004f8

$ aws ec2 authorize-security-group-ingress --group-id ___
--protocol tcp --port ___ --cidr ___

→ EC2 User Data Scripts runs with the root user

Contd... (after 2 pages)

AWS Global Infrastructure

AWS Regions

→ A cluster of data centers

How to choose a region?

(i) Compliance
(ii) Proximity (reduced latency)
(iii) Available services within a region
(iv) Pricing (varies Region to Region)

Availability Zones

→ Each region has many availability zones.
(usually - 3, min-2, max-6)

→ Each AZ has one or more discrete data centers with redundant power, networking & connectivity.

Point of presence (Edge locations)

→ Amazon has 216 points of presence.

Universal

Mon
Tue
Wed

Date 1 1

Page No.

AWS Services scope

Global	Regional
→ IAM	→ Amazon EC2 (IaaS)
→ Route 53	→ Elastic Beanstalk (PaaS)
→ CloudFront	→ Lambda (FaaS)
→ Web Application Firewall (WAF)	→ Rekognition (SaaS)

... Contd.

EC2 Instance Types

AWS has following naming convention

m5.2xlarge

m - instance class
5 - generation (AWS improves them over time)
2xlarge - size within the instance class

General Purpose (t2.micro, T2g, T3, M6g, M5)

→ Great for a diversity of workloads such as web servers or code repositories
→ Balance between -
- Compute
- Memory
- Networking

Compute Optimized (c6g, c6gn, C5, C5a, C5n, C4)

→ For Compute Intensive tasks that require high performance processor.
→ For -
- Batch processing workloads
- Media Transcoding
- High performance web servers
- " " Computing
- Scientific Modeling & Machine learning
- Dedicated gaming servers

Memory Optimized (R4g, R5, R5a, R5b, X1e, X1)

→ For workloads that process large data sets in memory.

→ For -

- → High performance relational/non-relational databases
- → Distributed web scale cache stores
- → In memory databases optimized for BI
- → Applications performing real-time processing for big unstructured data

Storage optimized (I3, I3en, D2, D3, D3en, H1)

→ Great for storage-intensive tasks that require high, sequential read and write access to large data sets on local storage.

→ For

- High frequency online Transaction processing (OLTP) systems
- Relational & NoSQL databases
- Cache for in memory databases
- Data warehousing application
- Distributed file systems

Security Groups

→ They control how traffic is allowed into or out of our EC2 Instances.

→ only contains Allow rules.

→ Security groups are acting as "firewall" on EC2 instances

→ If we change Region or VPC we will have to create a new security group.

EC2 Instances Purchasing Options

On Demand Instances

→ Pay for what you use.
→ Has the highest cost but no upfront payment
→ No long term commitment
→ Recommanded for short-term and un-interrupted workloads, where you can't predict how the application will behave

Reserved Instances

→ Upto 72% discount Compared to On-demand
→ Reservation period:
  1 year = + discount
  3 years = +++ discount
→ Reserve a specific instance type
→ Recommanded for steady-state usage applications

- Convertible Reserved Instance -
  ⇒ can change the EC2 instance type
  ⇒ Up to 45% discount
- Scheduled Reserved Instance -
  ⇒ launch within time window you reserve
  ⇒ when you require a fraction of day / week / month
  ⇒ Commitment for 1 year only.

Spot Instances

→ Can get a discount upto 90% Compared to On-demand.

→ Instances that you can "lose" at any point of time if your max price is less than the current spot price.

→ The most cost efficient instances in AWS.

→ Useful for workloads that are resilient to failure -
  → Batch jobs
  → Data analysis
  → Image Processing
  → Any distributed workloads
  → Workloads with a flexible start and end time.

→ Not suitable for critical jobs or databases.

Dedicated Hosts

→ It is a physical server with EC2 instance capacity fully dedicated to your use. Dedicated hosts can help you address compliance requirements and reduce costs by allowing you to use your existing server-bound software licenses.

→ Allocated to your account for 3-year period reservation.

→ More expensive

→ Useful for Companies that have strong regulatory or compliance needs.

Which purchasing option is right for me?

On demand -

Coming and staying in resort whenever we like, we pay the full price.

Reserved -

Like planning ahead and if we plan to stay for a long time, we may get a good discount.

Spot Instances -

The hotel allows people to bid for the empty rooms and the highest bidder keeps the rooms. You can get kicked out at any time.

Dedicated Hosts -

We book an entire building of the resort.