Core AWS Services

Amazon VPC

Amazon EC2

Amazon S3

Amazon Glacier

Amazon EBS

Amazon RDS

Amazon DynamoDB

Storage

AWS IAM

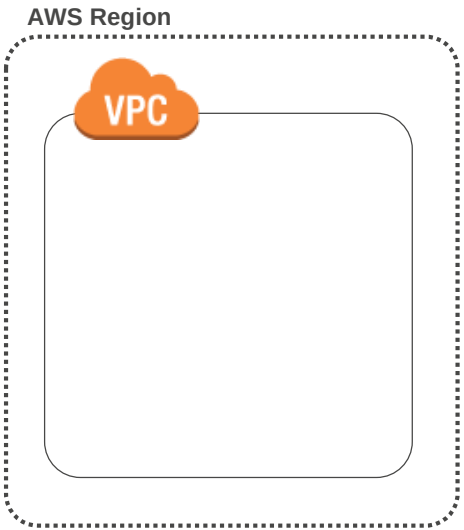
Amazon VPC Review

Amazon Virtual Private Cloud (VPC) allows you to provision virtual networks hosted on the AWS cloud and dedicated to your AWS account.

- VPCs are logically isolated from other virtual networks.
- Many AWS resources, such as Amazon EC2 instances, are launched into VPCs.
- Your VPC's key features are configurable:
  - IP ranges
  - Routing
  - Network gateways
  - Security settings

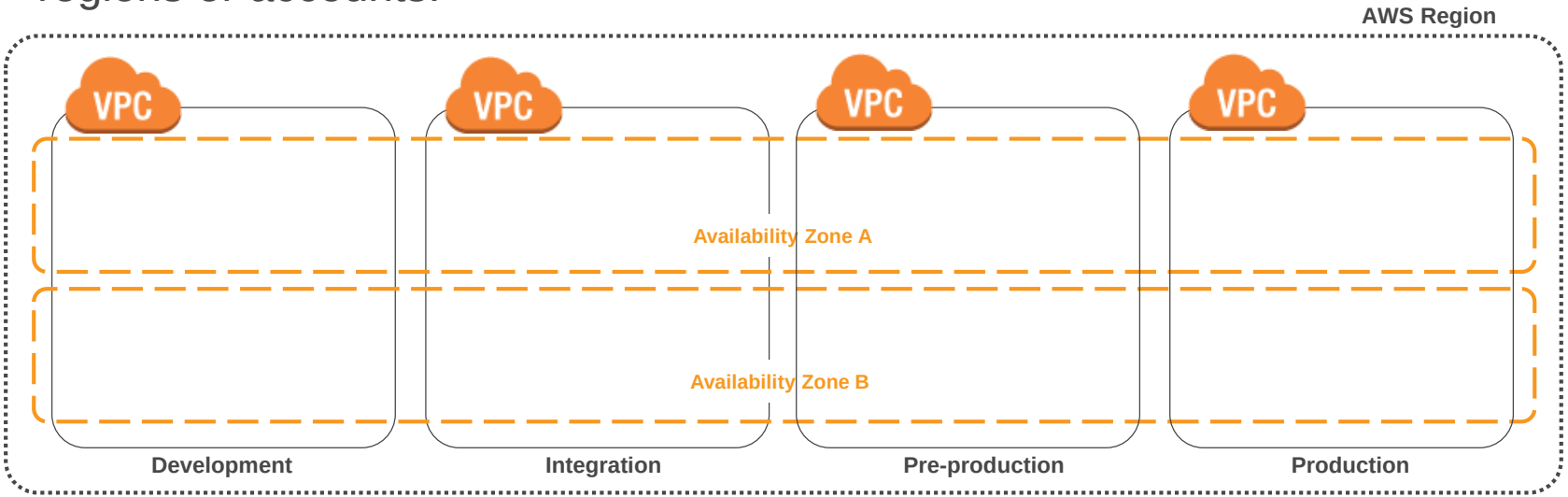
Amazon VPC Review

Each VPC lives in a region.



Amazon VPC Review

- Each VPC lives in a region.
- VPCs can include resources in more than one Availability Zone.
- You can have multiple VPCs in the same account and region and in multiple regions or accounts.



Core AWS Services

Amazon VPC

Amazon EC2

Amazon S3

Amazon Glacier

Amazon EBS

Amazon RDS

Amazon DynamoDB

Storage

AWS IAM

Amazon EC2 Review

Amazon Elastic Compute Cloud (EC2) offers virtual computing environments (instances) you can launch and manage with a few clicks of a mouse or a few lines of code.

- Most server operating systems are supported.
- Create, save, and reuse your own server images (Amazon Machine Images).
- Launch one instance at a time, or launch a whole fleet.
- Add more instances when you need them; terminate when you don't.
- CPU, memory, storage, networking, graphics, and general purpose types are available.
- Use security groups to control traffic to and from instances.

Choosing the Right Amazon EC2 Instance

AWS utilizes Intel® Xeon® processors providing customers with high performance and value

EC2 instance types are optimized for different use cases, workload requirements & come in multiple sizes.

Consider the following when choosing your instances: Core count, Memory size, Storage size & type, Network performance, & CPU technologies

Benefit from Intel® Capabilities

Intel's Haswell microarchitecture on new X1, C4, D2, & M4 instances, with custom Intel® Xeon® v3 processors, provides new features:

Haswell microarchitecture can boost existing applications performance by **30% or more**

- Better workload performance and faster response times

Newer Hardware Assisted technologies for workload acceleration

- Such as Intel® AVX2.0 instructions can double the floating-point performance for compute-intensive workloads. Provides additional instructions for compression and encryption.

X1 Instance - Tons of Memory

X1 featuring up to 2TB of memory & 100 vCPU

Using Intel E7 v3 Haswell processors

Designed for demanding enterprise workloads, including productions installations of SAP HANA, Microsoft SQL Server, Apache Spark and Presto

Available Q2 2016

Intel® Processor Technologies

Intel® AVX – Dramatically better performance for highly parallel HPC workloads such as *life science engineering, data mining, financial analysis*, or other technical computing applications. AVX also enhances *image, video, and audio* processing.

Intel® AES-NI – Enhance your security with these encryption instructions that reduce the performance penalty associated with encrypting/decrypting data.

Intel® Turbo Boost Technology – More computing power when you need it with performance that adapts to spikes in your workload.

Intel Transactional Synchronization (TSX) Extensions – Enable execution of transactions that are independent to accelerate throughput.

P state & C state control – ability to individually tune each cores performance & sleep states to improve application performance

AWS EC2 Instances with Intel® Technologies

AWS Instance Type	High Memory X1	Compute Optimized C4	Storage Optimized D2	General Purpose M4	Memory Optimized R3	IO Optimized I2	Graphics Optimized G2	Burstable Performance T2
Intel Processor	Intel Xeon E7-8880 v3	Custom Intel Xeon E5-2666 v3	Custom Intel Xeon E5-2676 v3	Custom Intel Xeon E5-2676 v3	Intel Xeon E5-2670 v2	Intel Xeon E5-2670 v2	Intel Xeon E5-2670	Intel Xeon Family
Intel AVX	AVX 2.0	AVX 2.0	AVX 2.0	AVX 2.0	Yes	Yes	Yes	Yes
Intel AES-NI	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Intel Turbo Boost	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Intel TSX	Yes	No	No	No	No	No	No	No
Per core P- and C-state control	No	Yes (8xlarge only)	No	No	No	No	No	No
SSD Storage	EBS Optimized by default	EBS Optimized by default	No	EBS Optimized by default	Yes	Yes	Yes	EBS only

Amazon EC2 Pricing Options

	On-Demand Instances	Reserved Instances (RIs)	Spot Instances
Term	Pay as you go	One year or three years	Bid on unused capacity; instances can be lost if you are outbid
Benefit	Low cost and flexibility	Predictability ensures compute capacity is available when needed	Large scale, dynamic workload
Cost	Pay for what you use	Pay low or no upfront fee; overall cost is lower	Spot price based on supply and demand
Use case	• Short-term, spiky, or unpredictable workloads • Application development or testing	• Steady state or predictable usage workloads • Applications that require reserved capacity, including disaster recovery • Users able to make upfront payments to reduce total computing costs even further	• Applications with flexible start and end times • Applications only feasible at very low compute prices • Users with urgent computing needs for large amounts of additional capacity

Core AWS Services

Amazon VPC

Amazon EC2

Amazon S3

Amazon Glacier

Amazon EBS

Amazon RDS

Amazon DynamoDB

Storage

AWS IAM

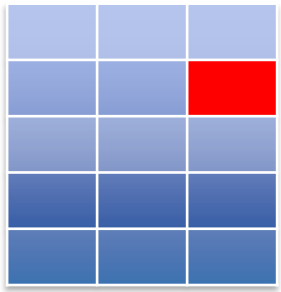
Amazon Elastic Block Store (EBS)

AWS Storage Options: Block vs. Object Storage

What if you want to change one character in a 1-GB file?

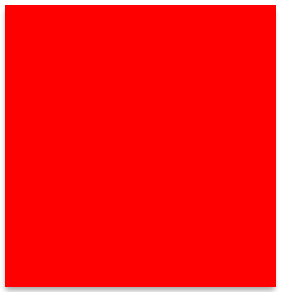
Block Storage

Change one block (piece of the file) that contains the character



Object Storage

Entire file must be updated



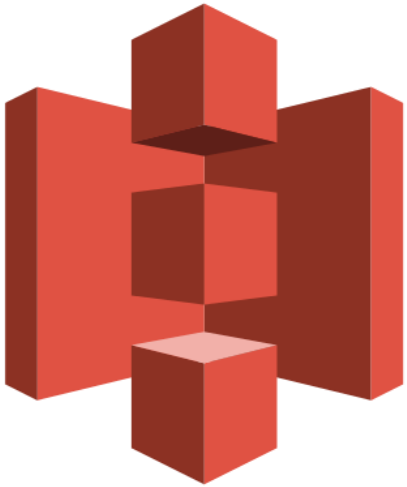
Amazon Elastic Block Store (EBS) Review

Amazon EBS allows you to create individual storage volumes and attach them to an Amazon EC2 instance.

- Amazon EBS offers Block-level storage.
- Volumes are automatically replicated within its Availability Zone.
- Can be backed up automatically to Amazon S3.
- Uses:
  - Boot volumes and storage for EC2 instances
  - Data storage with a file system
  - Database hosts
  - Enterprise applications

Amazon EBS Volume Types

	Magnetic	Cold HDD	Throughput Optimized HDD	General Purpose SSD	Provisioned IOPS SSD
Max volume size	1 TiB	16 TiB	16 TiB	16 TiB	16 TiB
Max IOPS/volume	40 to 200	250	500	10,000	20,000
Max throughput/volume	40 to 90 MiB/sec	250 MiB/s	500 MiB/s	160 MiB/sec	320 MiB/sec
Use cases	• Infrequent data access	• Workloads involving large, sequential I/O	• Workloads involving large, sequential I/O	• Boot volumes • Small to Medium DBs • Dev and Test environments	• I/O-intensive workloads • Relational DBs • NoSQL DBs



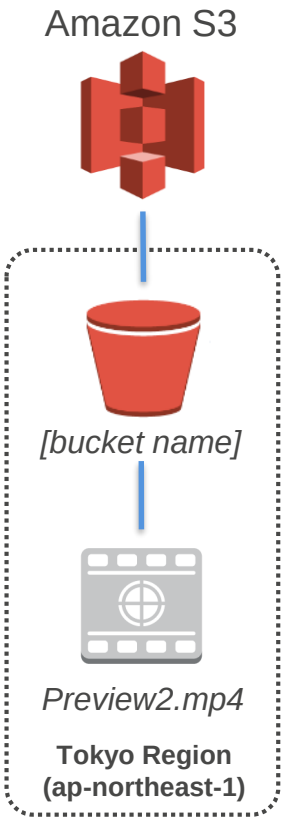
Amazon Simple Storage Service (S3)

Amazon S3 Review

Amazon S3 is a managed cloud storage solution designed to scale seamlessly and provide 99.999999999% durability.

- Amazon S3 provides object-level storage.
- Store as many objects as you want.
- Data is stored redundantly.
- Access Amazon S3 with the AWS Management Console, one of the AWS SDKs, or a third-party solution.
- Object uploads or deletes can trigger notifications, workflows, or even scripts.
- Data in transit and at rest can be encrypted automatically.

Amazon S3 Review



To upload your data (photos, videos, documents, etc.):

1. Create a bucket in one of the AWS Regions.
2. Upload any number of objects to the bucket.

Bucket

https://s3-ap-northeast-1.amazonaws.com/[bucket name]/

Region code

Bucket name

Object

https://s3-ap-northeast-1.amazonaws.com/[bucket name]/Preview2.mp4

Key

Amazon S3 Review

Pay only for what you use, including:

- GBs per month
- Transfer OUT to other regions
- PUT, COPY, POST, LIST, and GET requests

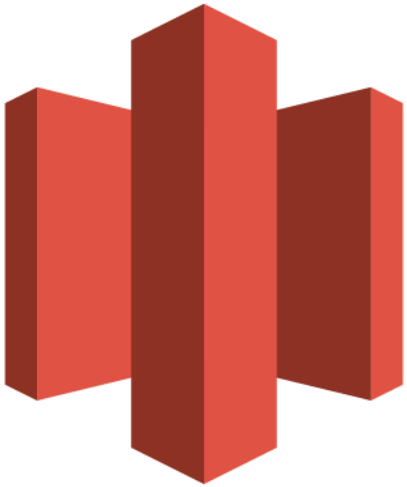
You do NOT have to pay for:

- Transfer IN to Amazon S3
- Transfer OUT from Amazon S3 to Amazon CloudFront or Amazon EC2 in the same region

Amazon S3 Review

Options:

- General purpose: Amazon S3 Standard
  - Higher availability requirements: Use cross-region replication
- Infrequently accessed data: Amazon S3 Standard - Infrequent Access
  - Lower cost per GB stored
  - Higher cost per PUT, COPY, POST, or GET request
  - 30-day storage minimum



Amazon Glacier

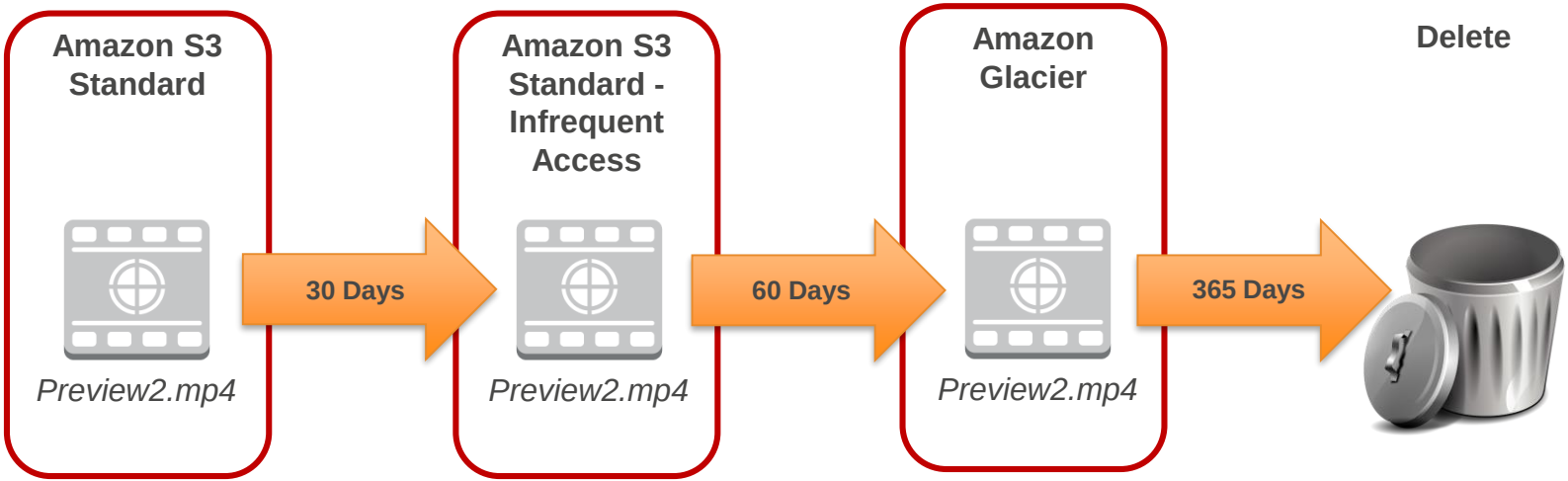
Amazon Glacier Review

Amazon Glacier is a data archiving service designed for security, durability, and an extremely low cost.

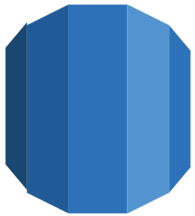
- Amazon Glacier is designed for durability of 99.999999999% of objects.
- Amazon Glacier supports SSL/TLS encryption of data in transit and at rest.
- The Vault Lock feature enforces compliance via a lockable policy.
- Extremely low-cost design is ideal for long-term archiving;
  - Data retrieval will take 3-5 hours to begin.

Lifecycle Policies

Amazon S3 lifecycle policies allow you to delete or move objects based on age.



Amazon Database Review



Amazon Relational Database Service (RDS)

Amazon DynamoDB

Amazon Relational Database Service (RDS)

Amazon Relational Database Service (RDS) Review

Amazon RDS lets you set up, operate, and scale relational databases in the cloud. Features:

- Managed service
- Accessible via the AWS Management Console, AWS RDS Command-Line Interface, or simple API calls
- Scalable (compute and storage)
- Automated redundancy and backup available
- Supported database engines:
  - Amazon Aurora
  - MySQL
  - ORACLE
  - PostgreSQL
  - MariaDB
  - Microsoft SQL Server

When To Use Amazon RDS

Use Amazon RDS when your app requires:

- Complex transactions or complex queries
- A medium-to-high query/write rate – up to 30K IOPS (15K reads + 15K writes)
- No more than a single worker node/shard
- High durability

Do **not** use Amazon RDS when your app requires:

- Massive read/write rates (e.g., 150K write/second)
- Sharding due to high data size or throughput demands
- Simple GET/PUT requests and queries that a NoSQL database can handle
- RDBMS customization

Amazon DynamoDB

Amazon DynamoDB Review

Amazon DynamoDB is a fully managed NoSQL database service.

- Consistent, single-digit millisecond latency at any scale
- No table size or throughput limits
- Runs exclusively on SSDs
- Document and key-value store models supported
- Ideal for mobile, web, gaming, ad tech, and IoT applications
- Accessible via the AWS Management Console, the AWS Command-Line Interface, or simple API calls

Provisioned Throughput

You specify your throughput capacity requirements (read/write), and DynamoDB allocates the resources you need.

Read capacity unit:

- One ***strongly*** consistent read per second for items as large as 4 KB.
- Two ***eventually*** consistent reads per second for items as large as 4 KB.

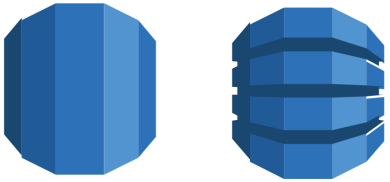
Write capacity unit:

- One write per second for items as large as 1 KB.

Core AWS Services

Amazon VPC

Amazon EC2



Storage

AWS IAM

AWS Identity And Access Management (IAM)

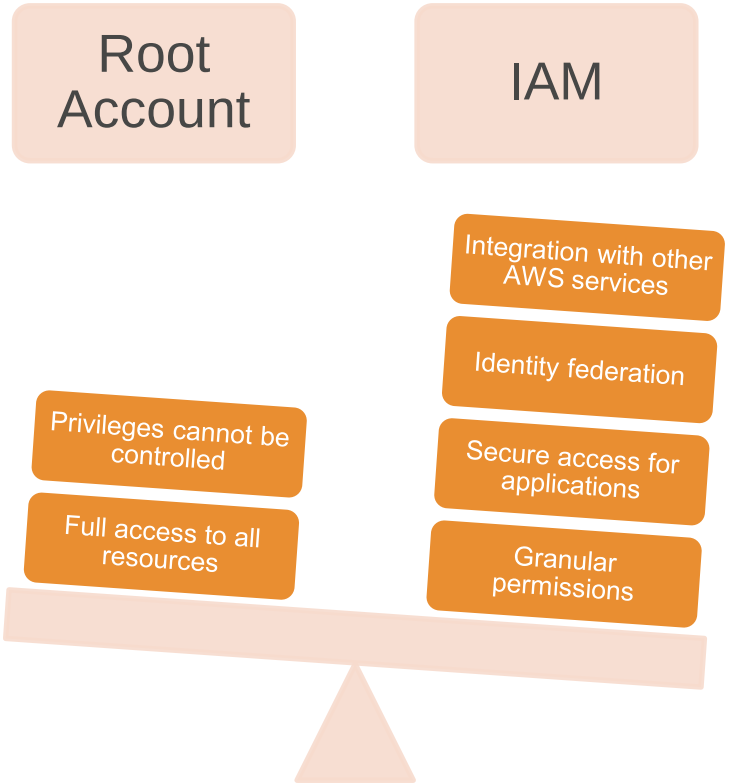
Centrally manage access and authentication of your users to your AWS resources.

- Offered as a feature of your AWS account for no charge.
- Create users, groups, and roles, and apply policies to them to control their access to AWS resources.
- Manage what resources can be accessed and how they can be accessed (e.g., terminating EC2 instances).
- Define required credentials based on context (e.g., who is accessing which service and what are they trying to do?).

Types Of Security Credentials

Email address and password	Associated with your AWS account (root)
IAM user name and password	Used for accessing the AWS Management Console
Access keys	Typically used with CLI and programmatic requests like APIs and SDKs
Multi-Factor Authentication	Extra layer of security Can be enabled for root account and IAM users
Key pairs	Used only for specific AWS services like Amazon EC2

Root Account Access vs. IAM Access



IAM allows you to follow the **least privilege** principle.

IAM Permissions

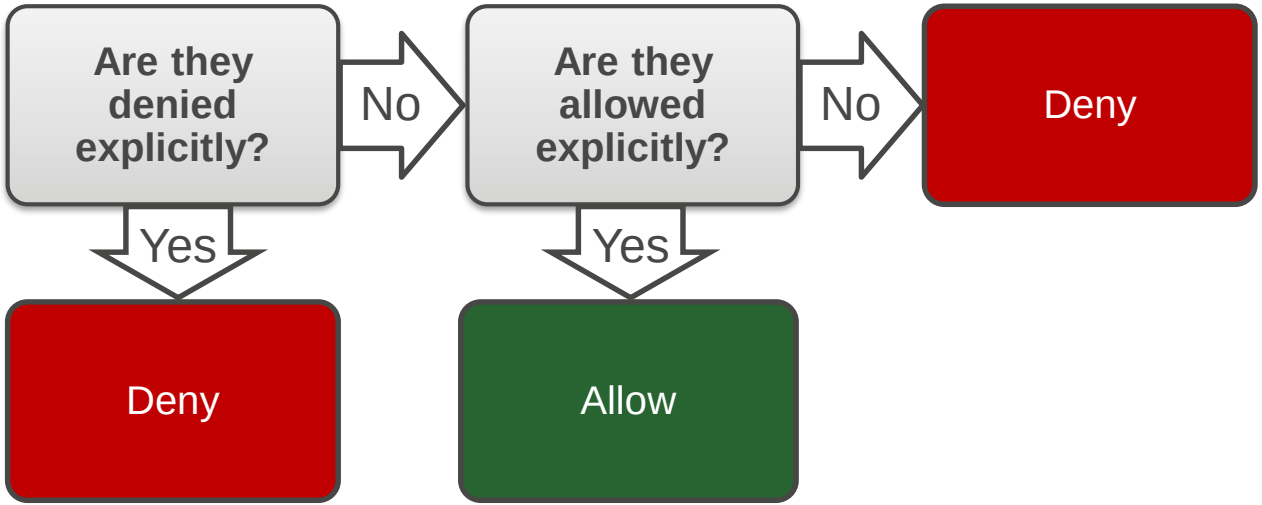
Permissions determine which resources and which operations are allowed to be used.

- All permissions are *implicitly* denied by default.
- If something is *explicitly* denied, it can never be allowed.

Best Practice: Follow the **least privilege** principle.

IAM Permissions

How IAM determines permissions:



IAM Policies

An IAM policy is a formal statement of one or more permissions.

- You attach a policy to any IAM entity: user, group, or role.
- Policies authorize the actions that may, or may not, be performed by the entity.
  - Enables fine-grained access control.
- A single policy can be attached to multiple entities.
- A single entity can have multiple policies attached to it.

Best practice: When attaching the same policy to multiple IAM users, put the users in a group and attach the policy to the group instead.

IAM Policy Example

```
{
  "Version": "2012-10-17",
  "Statement":[{
    "Effect":"Allow",
    "Action":["dynamodb:*","s3:*"],
    "Resource":["arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",
      "arn:aws:s3:::bucket-name",
      "arn:aws:s3:::bucket-name/*"]
    },
    {
    "Effect":"Deny",
    "Action":["dynamodb:*","s3:*"],
    "NotResource":["arn:aws:dynamodb:region:account-number-without-hyphens:table/table-name",
      "arn:aws:s3:::bucket-name",
      "arn:aws:s3:::bucket-name/*"]
    }
  ]
}
```

Gives users access to a specific DynamoDB table and…

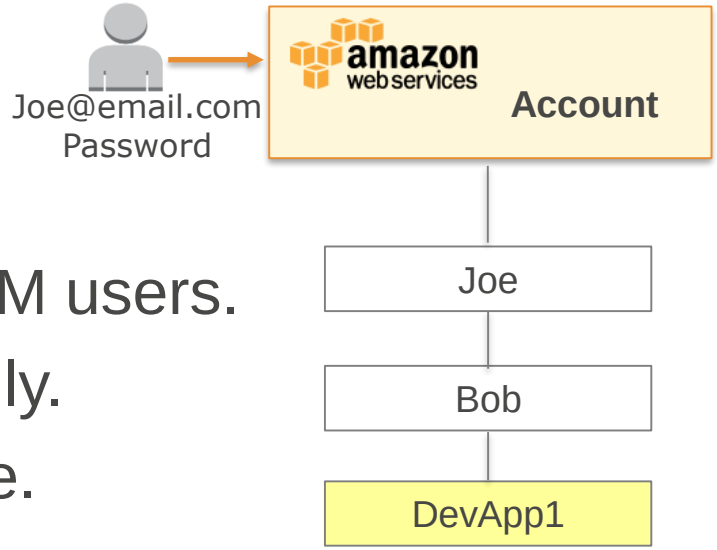
…Amazon S3 buckets

Explicit deny ensures that the users cannot use any other AWS actions or resources other than that table and those buckets

An explicit deny statement **takes precedence** over an allow statement

IAM Users

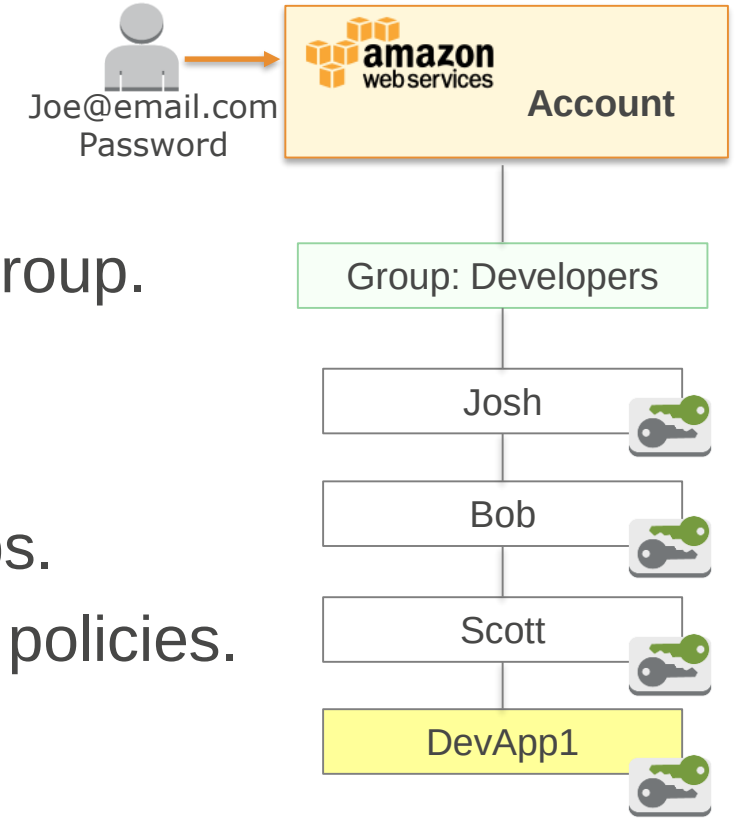
- An entity you create in AWS.
- Provides a way to interact with AWS.
- No default security credentials for IAM users.
  - You have to assign them specifically.
- IAM users are not necessarily people.



Best practice: Create a separate IAM user account with administrative privileges for the root account user.

IAM Groups

- Collection of IAM users.
- Specify permissions for the entire group.
- No default groups.
- Groups cannot be nested.
- A user can belong to multiple groups.
- Permissions are defined using IAM policies.



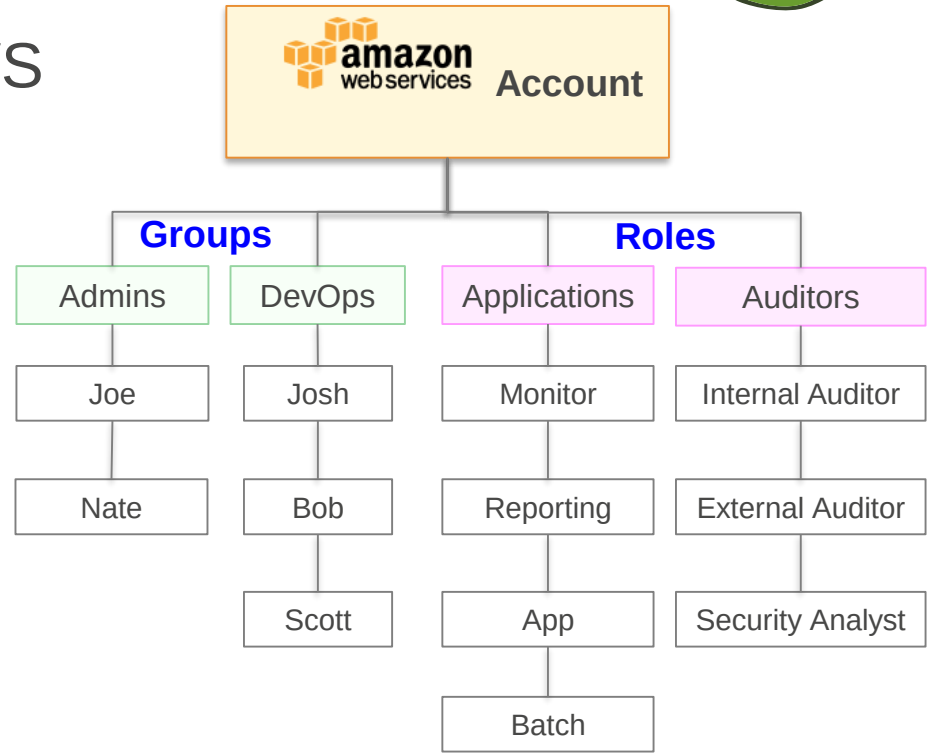
IAM Roles

Used to **delegate** access to AWS resources.

- Provides temporary access
- Eliminates the need for static AWS credentials

Permissions are:

- Defined using IAM policies
- Attached to the role, not to an IAM user or group



IAM Roles

Use cases:

- Provide AWS resources with access to AWS services.
- Provide access to externally authenticated users.
- Provide access to third parties.
- Switch roles to access resources in:
  - Your AWS account.
  - Any other AWS account (cross-account access).

What are the first things to do with a new AWS account?

Day One With AWS

1. Stop using the root account as soon as possible.

   The root account has completely unrestricted access to your resources.

   To stop using the root account, take the following steps:

   1) With the root account, create an IAM user for yourself.
   2) Create an IAM group and give it full administrator permissions.
   3) Sign in with your IAM user credentials.
   4) Store your root account credentials in a very secure place. Disable and remove your root account access keys, if you have them.

Day One With AWS

2. Require multi-factor authentication for access.
    a. Require MFA for your root account and all IAM users.
    b. You can also use MFA to control access to AWS service APIs.

Software MFA options: AWS Virtual MFA, Google Authenticator, Authenticator (Windows phone app), or SMS notification

Hardware MFA options: Key fob or display card offered by Gemalto: onlineoram.gemalto.com

3. Enable AWS CloudTrail.

   AWS CloudTrail logs all API requests to resources in your account.

   1) Via the CloudTrail console: create a trail, give it a name, apply it to all regions, and enter a name for the new Amazon S3 bucket that the logs will be stored in.
   2) Ensure that the Amazon S3 bucket you use for CloudTrail has its access restricted to only those who should have access, such as admins.

Log API Calls With AWS CloudTrail

Do you need to track the API calls for one or more AWS accounts?

Use cases enabled by CloudTrail:

- Security analysis
- Track changes to AWS resources
- Troubleshoot operational issues
- Compliance aid
- Use with AWS Config to identify responsibility for a change

Track Changes To Resources With AWS Config

- Provides AWS resource inventory, configuration history, and configuration change notifications.
- Provides continuous details on all configuration changes associated with AWS resources.
- Combines with CloudTrail for full visibility into what contributed to a change.
- Enables compliance auditing, security analysis, resource change tracking, and troubleshooting.

Day One With AWS

4. Enable a billing report, such as the AWS Cost and Usage Report.
    a) Billing reports provide information about your usage of AWS resources and estimated costs for that usage.
    b) AWS delivers the reports to an Amazon S3 bucket that you specify and updates the reports at least once a day.
    c) The AWS Cost and Usage Report tracks your AWS usage and provides estimated charges associated with your AWS account, either by the hour or by the day.

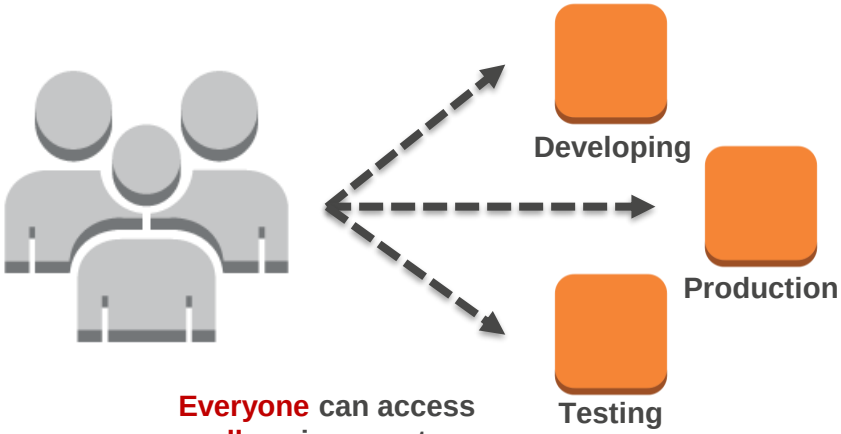
Appendix A: Amazon EC2 Best Practices

Amazon EC2: Security (1 of 3)

Manage access to AWS resources and APIs using identify federation, IAM users, and IAM roles.

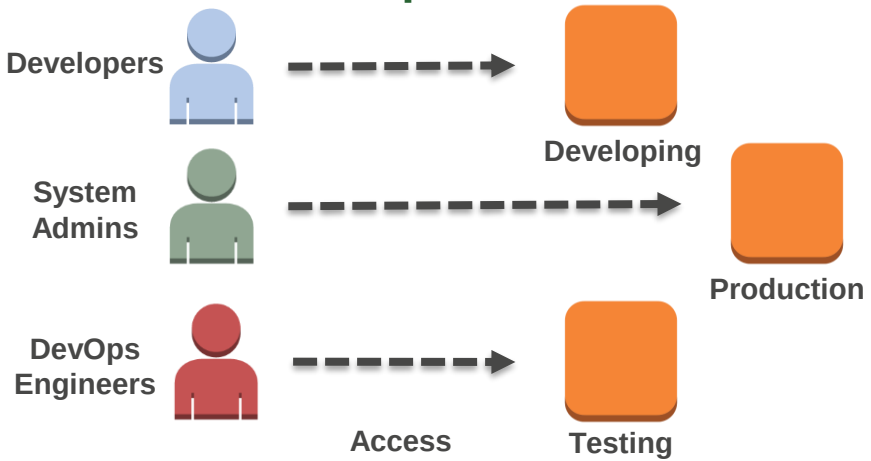
Establish credential management policies and procedures for creating, distributing, rotating, and revoking AWS access credentials.

Anti-pattern



Everyone can access **all** environments

Best practice



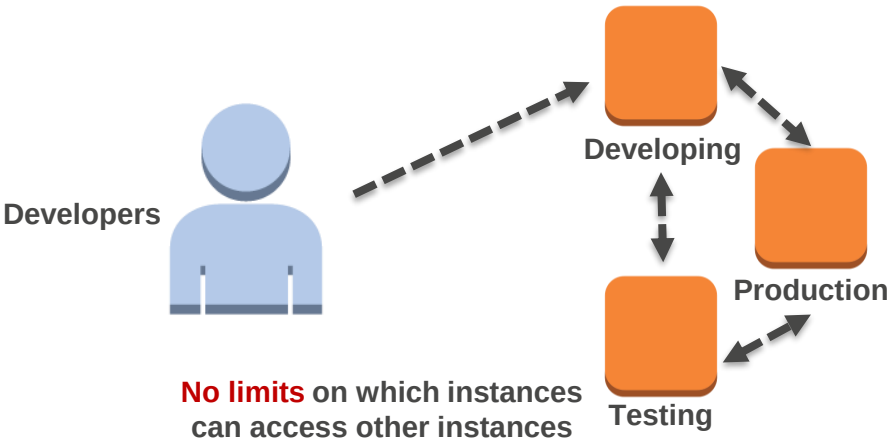
Access **separated** by role

Amazon EC2: Security (2 of 3)

Implement least permissive rules for your security group.

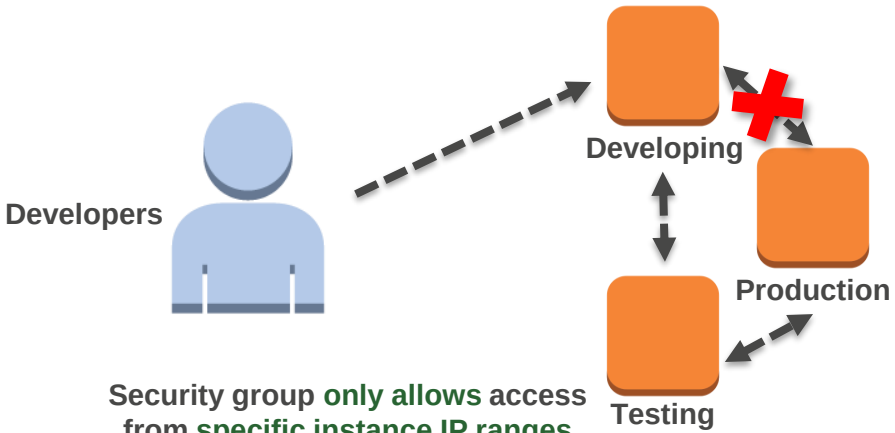
Ensure that instances are only accessible from specified IPs, IP ranges, and other resources.

Anti-pattern



No limits on which instances can access other instances

Best practice



Security group **only allows** access from **specific instance IP ranges**

Amazon EC2: Security (3 of 3)

Regularly patch, update, and secure your OS and applications.

Under the Shared Responsibility Model, you are responsible for securing your instance's OS and applications.

Updating instances:

- SSH into Linux instances, RDP into Windows instances
- Install all updates or just specific ones
- Reboot once updates are complete
- Save an image of your updated, secured instance for re-use when launching new instances

Amazon EC2: Storage

Only use instance store-backed storage with your instance when appropriate.

Backing your instance with an instance store volume has critical implications for data persistence, backup, recovery, and total size.

	Instance store-backed	Amazon EBS-backed
Default data persistence	Deleted when instance terminates	Persists after instance termination
Backup	Requires additional tools	Use a single command or a few mouse clicks
Recovery if instance stops/reboots	Data lost	Data persisted
Maximum storage	10 GiB	16 TiB

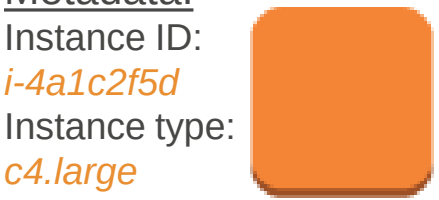
Amazon EC2: Resource management (1 of 2)

Ensure that all instances that are launched into your environment are tracked appropriately.

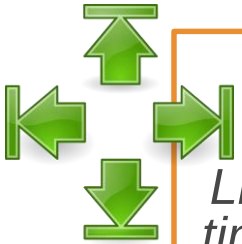
Track and identify your instances more easily using instance metadata and custom tags.

Important concepts:

- Instance metadata:
  - What is it?
  - What kinds of data categories does it include?
- Tags:
  - What are they?
  - What are the best ways to tag instances and other AWS resources?



Amazon EC2: Resource management (2 of 2)



Plan to request any limit increases in advance. Limit increase requests take time to be reviewed by AWS.

All accounts are initially limited in how many key pairs, instances, and AMI copies they can have.

Amazon EC2-VPC limits:

- Key pairs: 5,000 maximum
- On-demand and Spot instances: Limits vary depending on instance type, region, and account.
- Reserved instances: 20 instance reservations per AZ, per month
- AMI copies: Destination regions limited to 50 at a time, with no more than 25 coming from a single source region.

Amazon EC2: Backup and Recovery

Best practices:

- Regularly back up your instances.
- Deploy critical components of your app across multiple AZs.
- Design your apps to handle dynamic IP addressing for when your instance restarts.
- Monitor and respond to events.
- Ensure that you are prepared to handle failover.
- Regularly test your instance and EBS volume recovery processes.

Appendix B: Core Services Additional Info

Get Consistent Visibility of Logs Using CloudTrail

CloudTrail provides:

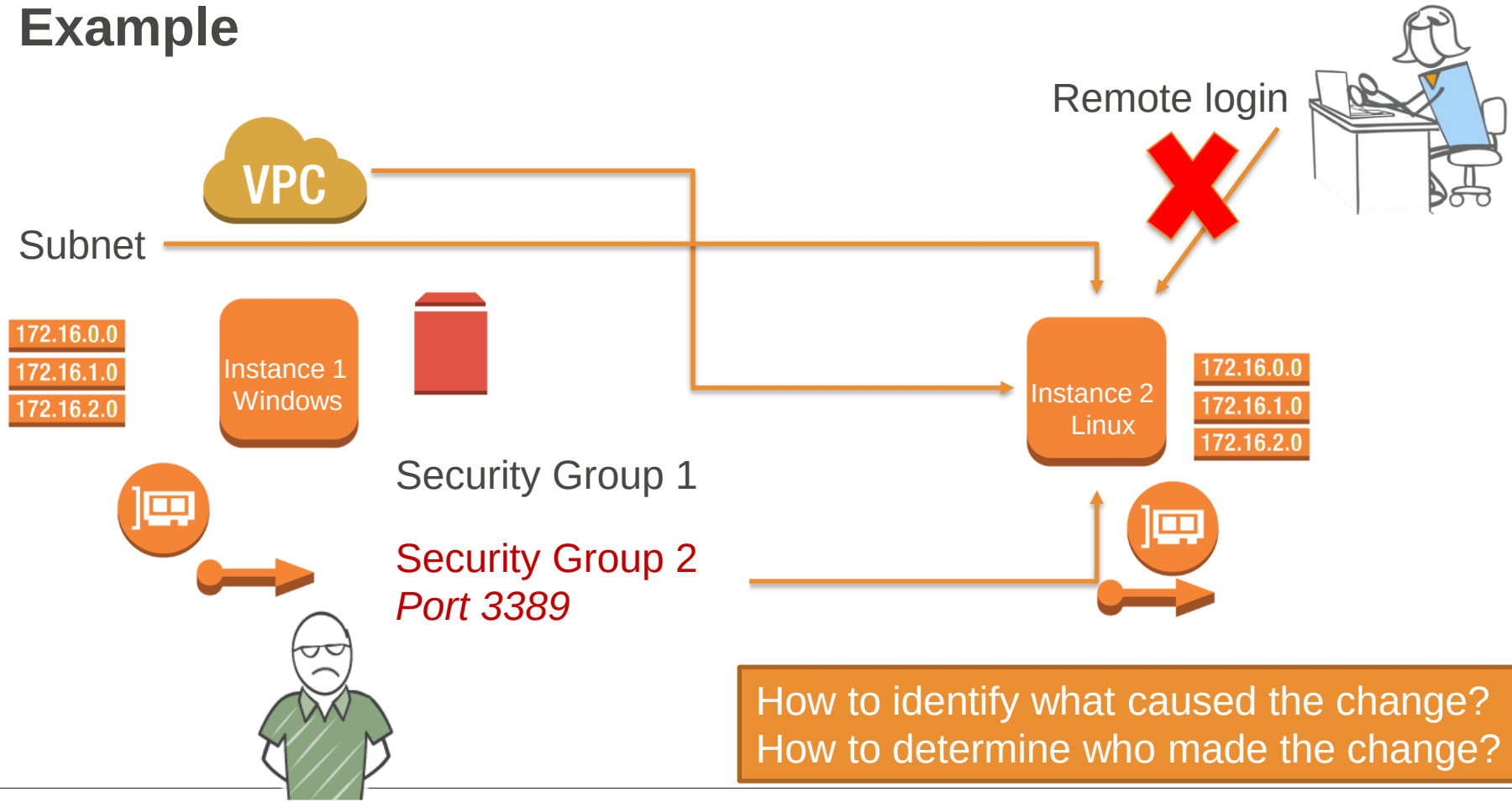
- Full visibility of your AWS environment.
  - CloudTrail records all API calls to your resources and saves logs in your designated Amazon S3 buckets.
  - The vast majority of AWS services are supported by CloudTrail.
- Out-of-box integration with log analysis tools from APN partners including Splunk, AlertLogic, and SumoLogic.
- Support for many AWS services to track who did what and when.
  - Easily aggregate all API logs in one place.
  - Use AWS Config to track changes to resource inventory and configurations.

Using AWS Config

- Get a snapshot of your current AWS configuration.
- Retrieve configuration of your AWS resources.
- Retrieve historical configuration of your AWS resources.
- Receive a notification when a resource is changed.
- View relationships between resources.

Is everything safe?
Where is the evidence?
What will this change affect?
What resources exist?
What has changed?

Example


Remote login
VPC
Subnet
172.16.0.0
172.16.1.0
172.16.2.0
Instance 1
Windows
Security Group 1
Security Group 2
Port 3389
Instance 2
Linux
172.16.0.0
172.16.1.0
172.16.2.0
How to identify what caused the change?
How to determine who made the change?