

### Cloud Computing Models (SI)

|            |  |
|------------|--|
| On-Premise | You are the owner of the infrastructure  |
| Cloud      | Someone owns the servers, you are responsible for setting up the cloud services and the code |
| Hybrid     | Mix of the previous approaches   |

### Amazon Simple Storage Service (S3) SI

Object Storage Service. It will allow us to store objects in buckets, and each object can have a maximum of 5TB. Each object has a key, value, metadata, access control information and version ID.

### Amazon S3 - Security & Policies (SI)

|           |  |
|-----------|--|
| Effect    | Allow/Deny                                       |
| Principal | Who can perform an action over the bucket/object |
| Action    | What the user can do over the bucket/object      |
| Resource  | Object/bucket affected                           |

### Amazon S3 - Encryption (SI)

|  |  |
|--|--|
| Server Side Encryption - S3                  | Amazon S3 manages the encryption key   |
| Server Side Encryption - KMS                 | AWS KMS manages the encryption key   |
| Server Side Encryption - C                   | The customer provides the encryption keys  |
| Client Side Encryption                       | Encrypting data before sending it to Amazon S3                                     |
| Dual-layer Server Side Encryption - DSSE-KMS | It applies two layers of encryption to objects when they are uploaded to Amazon S3 |

### AWS CloudTrail (SI)

Monitor and record account activity across your AWS infrastructure. For example, you can check the account that deleted an EC2 instance. There are two types of events:

- **Data events:** Visibility into the resource operations performed on or within a resource.
- **Management events:** Visibility into management operations performed in our AWS accounts.

### A PARTIR DE AQUI TODO ES NEW

### Amazon CloudFront - Cache

|                    |   |
|--------------------|---|
| Edge Location      | Each Edge Location has its own cache  |
| Cache Key          | Unique identifier for an object in the cache  |
| Cache Policies     | Based on HTTP headers, Cookies, or Query Strings. Automatically included in the origin request. You can use TTL |
| Cache Invalidation | Entire Refresh (invalidating all files) or Partial Refresh (invalidating a set of files) of the cache           |
| Cache Behaviors    | Settings that describes how CloudFront processes requests   |

### AWS CodeCommit - Authentication

|       |                                    |
|-------|------------------------------------|
| HTTPS | AWS Access Key                     |
| HTTPS | GIT credentials generated with IAM |
| SSH   | SSH keys associated with IAM user  |

### Files/Folders Summary

|                             |                    |
|-----------------------------|--------------------|
| CodeBuild                   | buildspec.yml      |
| CodeDeploy (Lambda/ECS)     | appspec.yml        |
| CodeDeploy (EC2/On-premise) | appspec.yml        |
| Elastic Beanstalk           | ebextensions       |
| Elastic Beanstalk (Docker)  | dockerrun.aws.json |



By cabanasj486

Not published yet.  
Last updated 10th April, 2024.  
Page 1 of 5.

Sponsored by [CrosswordCheats.com](https://crosswordcheats.com)  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### AWS STS - Main API Functions

|                           |  |
|---------------------------|--|
| AssumeRole                | Returns a set of temporary security credentials that you can use to access AWS resources   |
| AssumeRoleWithSAML        | Request temporary security credentials for an IAM role for users authenticated via SAML. The user authenticates against an external SAML-based identity provider |
| AssumeRoleWithWebIdentity | Returns a set of temporary security credentials for users who have been authenticated in a mobile or web application with a web identity provider                |
| GetSessionToken           | Used when using MFA to protect programmatic calls  |
| AWSRevokeOlderSession     | Revoke all active sessions.  |

Service to request temporary, limited-privilege credentials for users. The AssumeRole functions have a duration of 15min - 12h. When assuming a role, you give up your original permissions.

You can pass session tags and use the `aws:PrincipalTag` condition in your policies to allow/deny access based on these tags.

External ID for additional security control

### AWS CONTROL TOWER

|                 |  |
|-----------------|--|
| Account Factory | Automate the provisioning and management of accounts   |
| Guardrail       | Framework to help you prepare for audits by detecting and remediating policy violations. Types: preventive and detective |

TODO: ADD DESCRIPTION QUE YA ESTÁ EN EL OTRO LADO

### AWS Directory Services

|                          |  |
|--------------------------|--|
| AWS Managed Microsoft AD | It's a Microsoft Active Directory (AD) as an AWS managed service. You can also configure a trust relationship (not replication) between AWS Managed Microsoft AD in the AWS Cloud and your existing on-premises Microsoft Active Directory.  |
| AD Connector             | Gateway with which you can redirect directory requests to your on-premises Microsoft Active Directory. It does not support Active Directory transitive trusts, it works as a 1-to-1 relationship with your on-premise AD domain. The on-premise network must be connected to your VPC through a VPN connection or AWS Direct Connect |
| Simple AD                | Standalone managed directory. It does NOT support some features like MFA, trust relationships, and more.   |

### Migration Strategies - The 6 R's

|                            |   |
|----------------------------|---|
| Rehosting (lift-and-shift) | Moving to the cloud without making significant changes to the architecture:                     |
| Replatforming              | Moving to the cloud making minor architecture adjustments. For example, an on-premise DB to RDS |
| Repurchasing               | Moving to a different product   |
| Refactoring                | Re-architecting your application, typically using cloud native features                         |
| Retire                     | Get rid of the application  |



By **cabanasj486**

Not published yet.  
Last updated 10th April, 2024.  
Page 2 of 5.

Sponsored by **CrosswordCheats.com**  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### Migration Strategies - The 6 R's (cont)

Retain Do nothing (for now)

### AWS Organizations

Main Components Organizational Units (OUs), and Service Control Policies (SCPs)

Type of Accounts Main Account, and Member Account

Tag Policies Standardize tags across resources in your organization's accounts

Feature Sets All features and Consolidated Billing features

Move Accounts between Organizations Remove Account from Org1, invite the account from Org2, and accept invite

You can programmatically create new AWS accounts and allocate resources, group them, apply policies, and simplify billing by using a single payment method for all your accounts

### Spot Fleet - Allocation Strategies

priceCapacityOptimized (best choice) Provide a balance between capacity availability and cost optimization

capacityOptimized Analyzes the available Spot Instance pools across all selected instance types in an AWS Region and launches instances from the most available pools

diversified Distribute Spot Instances across all pools

### Spot Fleet - Allocation Strategies (cont)

lowest-Price Launches instances from the Spot Instance pool with the lowest price

A Spot Fleet is a set of Spot Instances and optionally On-Demand Instances that is launched based on criteria that you specify.

### AWS IAM Policy Types

Identity-based policies Grant permissions to an identity (users, groups, or roles)

Resource-based policies Attach inline policies to resources. Amazon S3 bucket policies is an example

Permissions boundaries Maximum permissions that the identity-based policies can grant to an entity (only users or roles). It doesn't grant permissions by itself

Organizations SCPs Maximum permissions for account members of an organization or organizational unit (OU)

Access control lists (ACLs) Cross-account permissions policies that grant permissions to the specified principal. They are not in JSON format

Session policies Permissions that the role or user's identity-based policies grant to the session created assuming a role or federated user

### Elastic Compute Cloud (EC2) (SI)

EC2 is a web service to provide compute capacity in the cloud. It's one of the core services of AWS, including processor, storage, networking, operating system, and purchase model. It's composed of Virtual machines (EC2), Block-storage service (EBS), Load Balancer (ELB) and Elasticity of the resources (Auto Scaling Group)



By cabanasj486

Not published yet.  
Last updated 10th April, 2024.  
Page 3 of 5.

Sponsored by [CrosswordCheats.com](https://crosswordcheats.com)  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### EC2 Instances Types (SI)

|                 |   |
|-----------------|---|
| R               | Application requires <b>RAM</b>                                   |
| C               | Application requires <b>CPU</b>                                   |
| M               | Balanced Applications <b>Medium</b>                               |
| I               | Application requires <b>I/O</b>                                   |
| G               | Application requires <b>GPU</b>                                   |
| T2/T3           | Burstable instances   |
| T2/T3 Unlimited | Burstable instances that you can pay more to not lose performance |

You can find a lot of different instance types at the following link.  
<https://instances.vantage.sh/>

### EC2 Security Groups (SI)

|                  |  |
|------------------|--|
| Inbound Traffic  | Traffic that tries to access the instance. |
| Outbound Traffic | Traffic that leaves the instance           |

Security Groups act as a virtual firewall to control inbound and outbound traffic for your instance. You can specify **allow rules**, but **not deny rules**. They live outside of EC2, so you can attach them to multiple instances.

### EBS (SI - edit)

Block-storage service for EC2. It's a network storage drive, and you pay for the capacity you provision. You can back up the data on your Amazon EBS volumes to Amazon S3 by taking point-in-time incremental snapshots.

You will also need to create snapshots to migrate an EBS between AWS Regions. You'll have to restore the snapshot in the Region where you want to copy it.

### EBS Types (SI)

|             |   |
|-------------|---|
| GP2/GP3 SSD | General Purpose SSD volumes   |
| IO1/IO2 SSD | Highest performance. They support <b>EBS Multi-Attach</b> (attach IO1 or IO2 volume to multiple EC2 instances in the same AZ) |
| ST1 HDD     | Frequently accessed, throughput-intensive workloads   |
| SC1 HDD     | Lowest cost per GB  |

### Instance Store (SI)

Temporary physically attached storage for your instance. It provides high performance / IOPS.

### Elastic File System (EFS) (SI)

|                   |                           |
|-------------------|---------------------------|
| Performance Modes | General Purpose & Max I/O |
| Storage Classes   | Standard & Standard-IA    |

EFS allows you to mount a file storage system across multiple AZs and instances. It provides massively parallel shared access to thousands of instances.

### Main Serverless Services (SI)

- AWS Lambda
- Lambda@Edge
- DynamoDB
- API Gateway
- Amazon Cognito
- AWS Serverless Application Model

### A PARTIR DE AQUI TODO ES NEW (copy)

### AWS Resources Access Manager (RAM)

Share your AWS resources across AWS accounts, within your organization, or organizational units (OUs). VPC Subnets, Prefix List, etc.

### Identity Federation

|   |   |
|---|---|
| Federation with IAM                       | Centralized access management. You can manage access using permission sets to different AWS accounts and external services (Slack, Salesforce, custom apps) from the same place. Build-in and 3rd party IdPs. |
| Identity Center (Successor to AWS SSO)adf |   |



By [cabanasj486](#)

Not published yet.  
 Last updated 10th April, 2024.  
 Page 4 of 5.

Sponsored by [CrosswordCheats.com](https://crosswordcheats.com)  
 Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

### Identity Federation (cont)

**Federation with SAML 2.0** Integrating AWS with an external identity provider (IdP) that supports the SAML 2.0 standard. You can use the AssumeRoleWithSAML API call or Active Directory Federation Services (AD FS)

**Web Identity Federation** Allowing users to authenticate using identity providers like Amazon Cognito (recommended), Google, Facebook, or other OpenID Connect (OIDC) providers. AssumeRoleWithWebIdentity API

**Federation with Custom Identity Broker** A custom identity broker acts as an intermediary between AWS and your organization's authentication system

Process of linking an organization's existing identity management system (for example, Active Directory) with AWS services to enable secure and seamless access to AWS resources. Users can log into the AWS Management Console or call the AWS API operations without you having to create an IAM user.

TODO: AGREGAR FOTO DEL PROCESO.



By **cabanasj486**

Not published yet.

Last updated 10th April, 2024.

Page 5 of 5.

Sponsored by **CrosswordCheats.com**

Learn to solve cryptic crosswords!

<http://crosswordcheats.com>