An IAM role is similar to a user; it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it.

An IAM role does not have standard long-term credentials (password or access keys) associated with it. Instead, if a user assumes a role, temporary security credentials are created dynamically and provided to the user. You can use roles to delegate access to users, applications, or services that normally don't have access to your AWS resources.

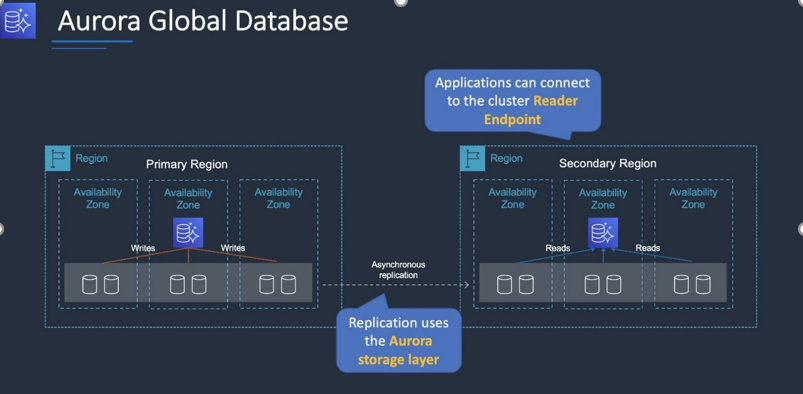
Always assign a role to the EC2 Instance to ensure secure access to AWS resources from EC2 Instances

Elastic Load Balancing **automatically distributes your incoming traffic across multiple targets, such as EC2 instances, containers, and IP addresses, in one or more Availability Zones**. It monitors the health of its registered targets, and routes traffic only to the healthy targets.

AWS Auto Scaling **monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost**. Using AWS Auto Scaling, it's easy to setup application scaling for multiple resources across multiple services in minutes.

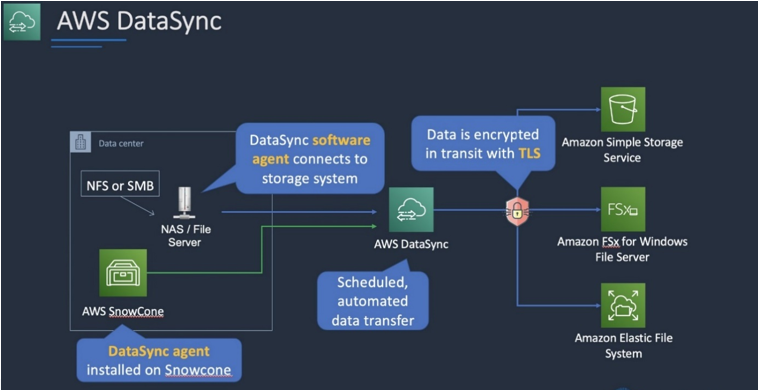
Adding Lifecycle Hooks to Auto Scaling group puts the instance into wait state before termination. During this wait state, you can perform custom activities to retrieve critical operational data from a stateful instance. Default Wait period is 1 hour.

Amazon Aurora Global Database is designed for globally distributed applications, allowing a single Amazon Aurora database to span multiple AWS regions. It replicates your data with no impact on database performance, enables fast local reads with low latency in each region, and provides disaster recovery from region-wide outages.



AWS DataSync can be used to automate and accelerate the replication of data to AWS storage services. Note that Storage Gateway is used for hybrid scenarios where servers need local access to data with various options for storing and synchronizing the data to AWS storage services. Storage Gateway does not accelerate replication of data.

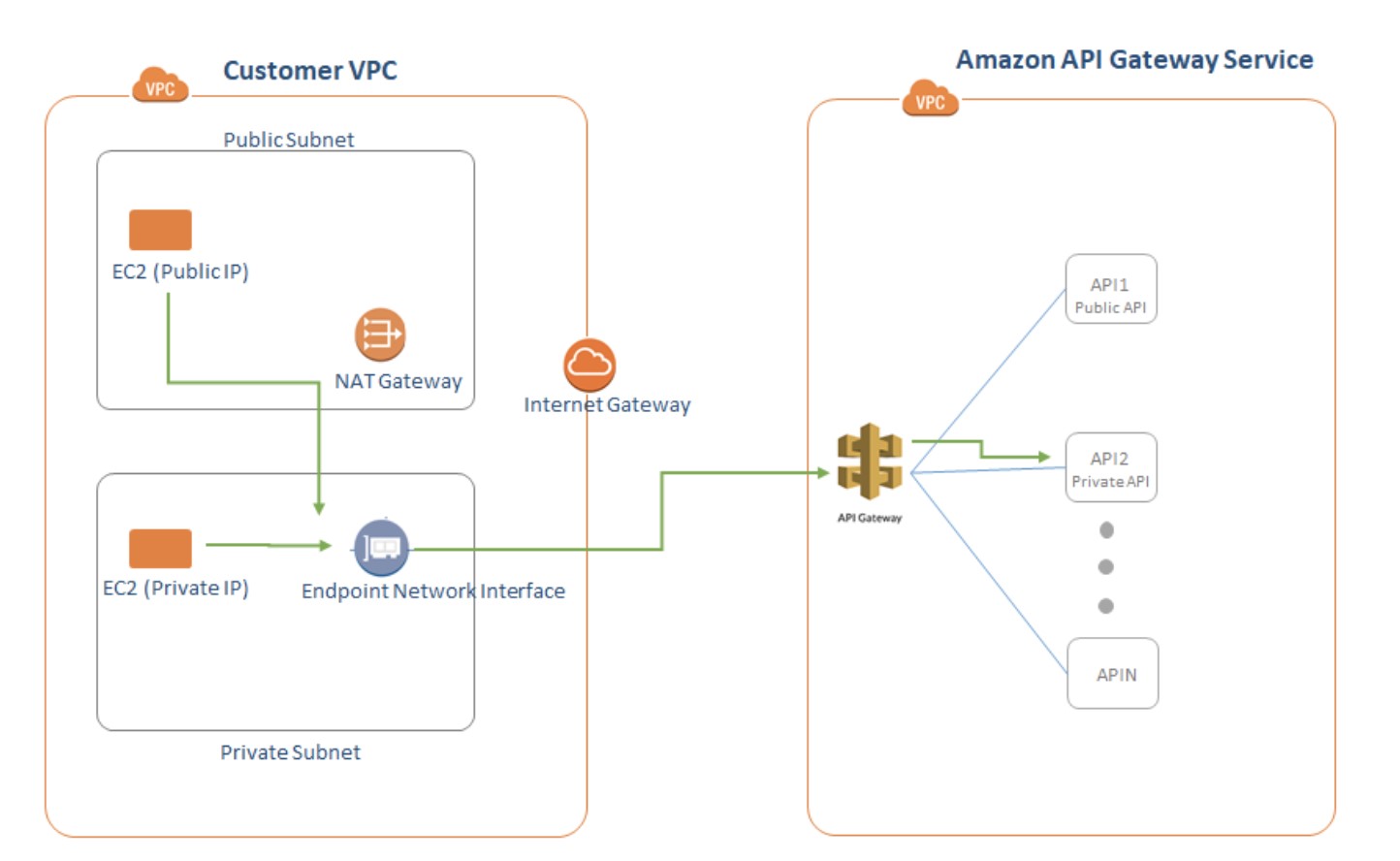
To deploy DataSync an agent must be installed. Then a task must be configured to replicated data to AWS. The task requires a connection to a service endpoint. To keep the data private and send it across the DX connection, a VPC endpoint should be used.



You can create your own application in your VPC and configure it as an AWS PrivateLink-powered service (referred to as an *endpoint service*). Other AWS principals can create a connection from their VPC to your endpoint service using an [interface VPC endpoint](https://docs.aws.amazon.com/vpc/latest/userguide/vpce-interface.html). You are the *service provider*, and the AWS principals that create connections to your service are *service consumers*.

This configuration is powered by AWS PrivateLink and clients do not need to use an internet gateway, NAT device, VPN connection or AWS Direct Connect connection, nor do they require public IP addresses.

Another option is to use a VPC Peering connection. A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account.

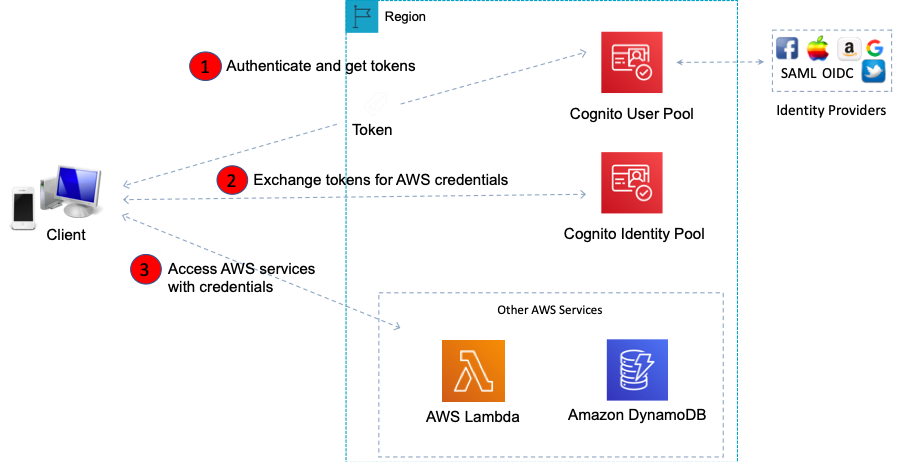


What is Amazon Cognito?

Amazon Cognito is **a simple user identity and data synchronization service that helps you securely manage and synchronize app data for your users across their mobile devices**.

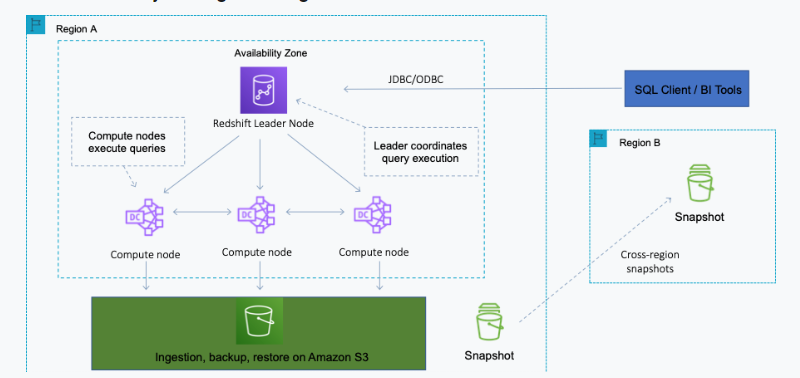
Amazon Cognito identity pools provide temporary AWS credentials for users who are guests (unauthenticated) and for users who have been authenticated and received a token. An identity pool is a store of user identity data specific to your account.

With an identity pool, users can obtain temporary AWS credentials to access AWS services, such as Amazon S3 and DynamoDB.



Amazon Redshift is an enterprise-level, petabyte scale, fully managed data warehousing service. An Amazon Redshift data warehouse is an enterprise-class relational database query and management system. Redshift supports client connections with many types of applications, including business intelligence (BI), reporting, data, and analytics tools.

Using Amazon Redshift Spectrum, you can efficiently query and retrieve structured and semistructured data from files in Amazon S3 without having to load the data into Amazon Redshift tables. Redshift Spectrum queries employ massive parallelism to execute very fast against large datasets.



Used together, RedShift and RedShift spectrum are suitable for running massive analytics jobs on both the structured (RedShift data warehouse) and unstructured (Amazon S3) data.

Some facts about Amazon EBS encrypted volumes and snapshots:

- All **EBS** types support encryption and all instance **families** now support encryption.

- Not all **instance** types support encryption.

- Data in transit between an instance and an encrypted volume is also encrypted (data is encrypted in trans.

- You can have encrypted an unencrypted EBS volumes attached to an instance at the same time.

- Snapshots of encrypted volumes are encrypted automatically.

- EBS volumes restored from encrypted snapshots are encrypted automatically.

- EBS volumes created from encrypted snapshots are also encrypted.

An IAM group is a collection of IAM users. Groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users.

The following facts apply to IAM Groups:

- Groups are collections of users and have policies attached to them.

- A group is not an identity and cannot be identified as a principal in an IAM policy.

- Use groups to assign permissions to users.

- IAM groups cannot be used to group EC2 instances.

- Only users and services can assume a role to take on permissions (not groups).

DynamoDB best practices include:

- Keep item sizes small.

- If you are storing serial data in DynamoDB that will require actions based on data/time use separate tables for days, weeks, months.

- Store more frequently and less frequently accessed data in separate tables.

- If possible compress larger attribute values.

- Store objects larger than 400KB in S3 and use pointers (S3 Object ID) in DynamoDB.

Security groups are stateful, we do not have to configure outbound traffic. What enters the inbound traffic is allowed in the outbound traffic too.

Note: The default network ACL is configured to allow all traffic to flow in and out of the subnets to which it is associated.

Amazon Glacier

Vault Lock - This feature of allows you to lock your vault with a variety of compliance controls that are designed to support such long-term records retention.

Expedited retrieval - It allows you to quickly access your data when occasional urgent requests are required for a subset of archives. The data is available within 1 - 5 minutes.

Bulk retrieval - They are the lowest-cost retrieval option, enabling you to retrieve large amounts of data within 5 - 12 hours.

Standard Retrieval-

Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. APIs act as the "front door" for applications to access data, business logic, or functionality from your backend services. Using API Gateway, you can create RESTful APIs and WebSocket APIs that enable real-time two-way communication applications. API Gateway supports containerized and serverless workloads, as well as web applications.

API Types:

RESTful APIs

Build RESTful APIs optimized for serverless workloads and HTTP backends using HTTP APIs. [HTTP APIs](https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api.html) are the best choice for building APIs that only require API proxy functionality. If your APIs require API proxy functionality and API management features in a single solution, API Gateway also offers [REST APIs](https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-vs-rest.html).

WEBSOCKET APIs

Build real-time two-way communication applications, such as chat apps and streaming dashboards, with [WebSocket APIs](https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-websocket-api-overview.html). API Gateway maintains a persistent connection to handle message transfer between your backend service and your clients.

Amazon Athena is a suitable tool for querying Network Load Balancers logs. A large amount of logs are saved in S3 buckets from Network load balancer, Amazon Athena can be used to query logs and generate required details of client IP address and TLS handshake time.

-AWS Athena pricing is based upon per query and the amount of data scanned in each query.

-Uploading a large amount of data simultaneously, this data needs to be partitioned based upon location & date.

-A separate Workgroup can be created based upon users, teams, application or workloads. This will lead to minimizing the amount of data scanned for each query, improving performance & reducing cost.

-As processing a large number of logs directly from the S3 console will be a time-consuming process.

-Amazon QuickSight will be useful in case you need data visualization.

AWS Elastic Beanstalk makes it even easier for developers to quickly deploy and manage applications in the AWS Cloud. Developers simply upload their application, and Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring.

Note: Beanstalk is not serverless

A Lightsail instance is a virtual private server (VPS) that lives in the AWS Cloud. Use your Lightsail instances to store your data, run your code, and build web-based applications or websites.

What is the difference between Lightsail and Beanstalk?

Lightsail - is similar but more user friendly management option and good for small applications. Beanstalk - an orchestration tool, which does all the work to create an EC2, install application, software and give you freedom from manual tasks in creating an environment.

What is Apache Cassandra?

Apache Cassandra is an open source NoSQL distributed database trusted by thousands of companies for scalability and high availability without compromising performance. Linear scalability and proven fault-tolerance on commodity hardware or cloud infrastructure make it the perfect platform for mission-critical data.

AWS CloudFormation Drift Detection can be used to detect changes made to AWS resources outside the CloudFormation Templates. It only checks property values that are explicitly set by stack templates or by specifying template parameters. It does not determine drift for property values that are set by default. To determine drift for these resources, you can explicitly set property values which can be the same as that of the default value.

What does Amazon detective do?

Amazon Detective automatically collects log data from your AWS resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data that enables you to easily conduct faster and more efficient security investigations.

AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail.

AWS CloudTrail monitors and records account activity across your AWS infrastructure, giving you control over storage, analysis, and remediation actions.

 By default, CloudTrail event log files are encrypted using Amazon S3 server-side encryption (SSE). You can also choose to encrypt your log files with an AWS Key Management Service (AWS KMS) key. You can store your log files in your bucket for as long as you want. You can also define Amazon S3 lifecycle rules to archive or delete log files automatically. If you want notifications about log file delivery and validation, you can set up Amazon SNS notifications.

AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud.

\*\*\* AWS Hesabinda Kim ne yapmış cloud trail, Neler yapilmış aws config

**EMR** is mainly used for Hadoop ecosystem-based data used for Big data analysis. Amazon Kinesis streams are used to read the data from thousands of sources like social media, survey-based data, etc. The Kinesis streams can be used to analyze the data and can feed it using AWS EMR to the analytics-based database like RedShift which works on OLAP.

**Amazon Kinesis** makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information. Amazon Kinesis offers key capabilities to process streaming data cost-effectively at any scale, along with the flexibility to choose the tools that best suit the requirements of your application.

With Amazon Kinesis, you can ingest real-time data such as video, audio, application logs, website clickstreams, and IoT telemetry data for machine learning, analytics, and other applications.



**Lambda:**

* Lambda is a serverless function. You upload your code and it runs without you managing or provisioning any servers
* Officially supported by Lambda: Ruby, Python, Java, NodeJs, C#, Powershell, and Go
* AWS API Gateway and AWS Step Functions  invoke synchronously and asynchronously the AWS Lambda function.
* You can use Lambda as scheduled event and read log files from AWS CloudWatch or CloudTrail and report any errors through SNS notifications.
* The maximum batch size supported by AWS SQS for ReceiveMessage call is 10.
* **Amazon Simple Notification Service (SNS)**

Encrypt topics via KMS

AWS Lambda automatically monitors Lambda functions on your behalf, reporting metrics through Amazon CloudWatch. To help you troubleshoot failures in a function, Lambda logs all the requests handled by your function and also automatically stores logs generated by your code through Amazon CloudWatch Logs.

With AWS SAM, the application can be tested locally by invoking Lambda function & event sources locally. Using these SAM templates, the application can be tested thoroughly before deploying in the AWS cloud. Also, CodeDeploy is built with AWS SAM which can help to deploy gradually within Cloud along with the existing applications which can minimize risks

**Cloud9:**  A cloud-based integrated development environment (IDE) that lets you write, run, and debug your code with just a browser. It includes a code editor, debugger, and terminal. Cloud9 comes prepackaged with essential tools for popular programming languages, including JavaScript, Python, PHP, and more, so you don’t need to install files or configure your development machine to start new project

**Simple Queue Service (SQS)** is a queuing service using messages with a queue.

* To read SQS use need to pull the queue using the AWS SDK and uses pull-based (polling) not push-based.
* Messages can be kept in the queue from 1 minute to 14 days Messages will be deleted from the queue after a job has processed
* The default visibility time-out is 30 seconds. The timeout can be 0 seconds to a maximum of 12 hours.
* Message size between 1 byte to 256 kb,

With a VPC endpoint, you can privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for IAM users or for users that you authenticate (federated users). The steps performed by the custom identity broker to sign users into the AWS management console are:

- Verify that the user is authenticated by your local identity system

- Call the AWS Security Token Service (AWS STS) AssumeRole or GetFederationToken API operations to obtain temporary security credentials for the user

- Call the AWS federation endpoint and supply the temporary security credentials to request a sign-in token

- Construct a URL for the console that includes the token

- Give the URL to the user or invoke the URL on the user’s behalf