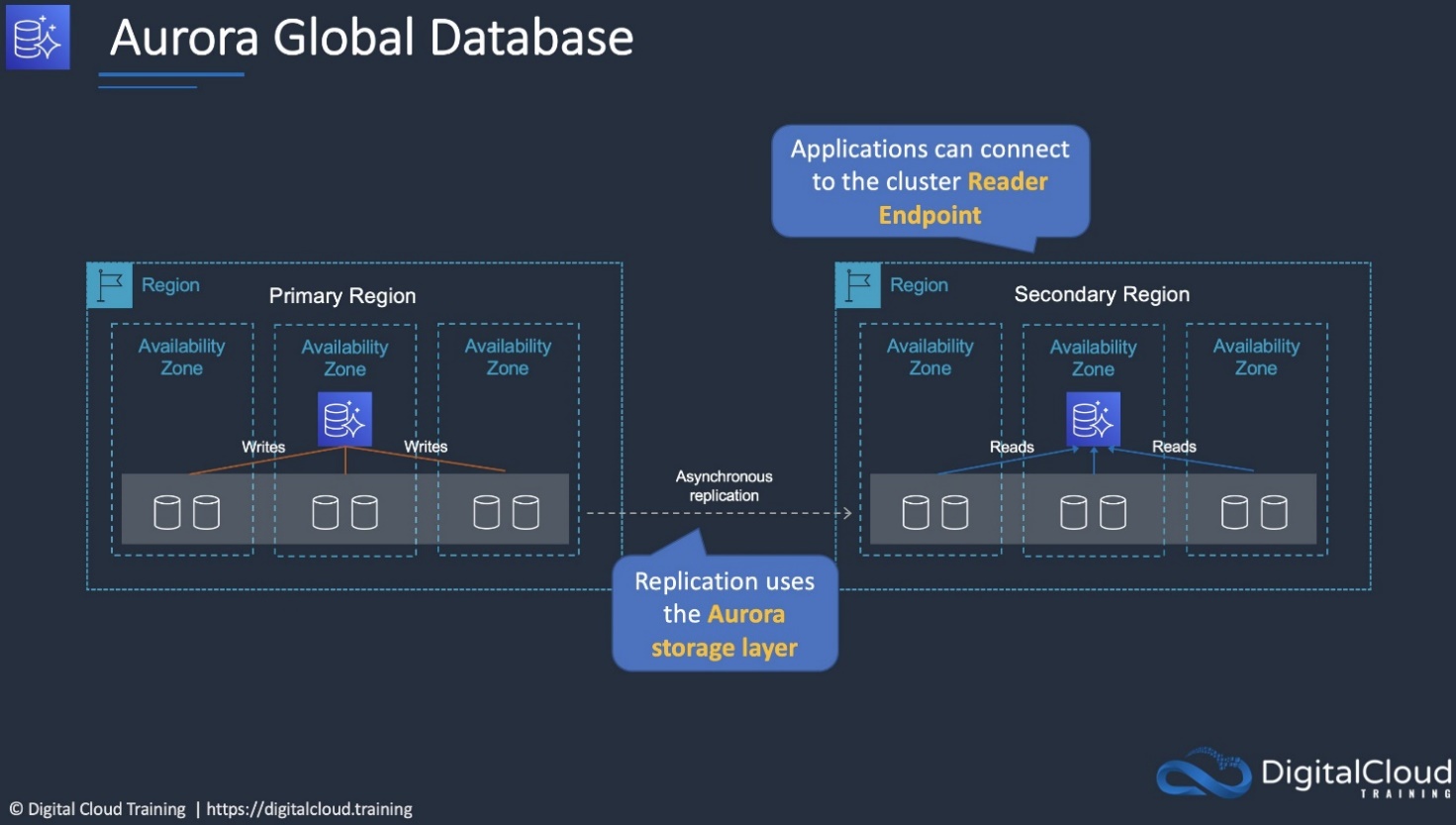
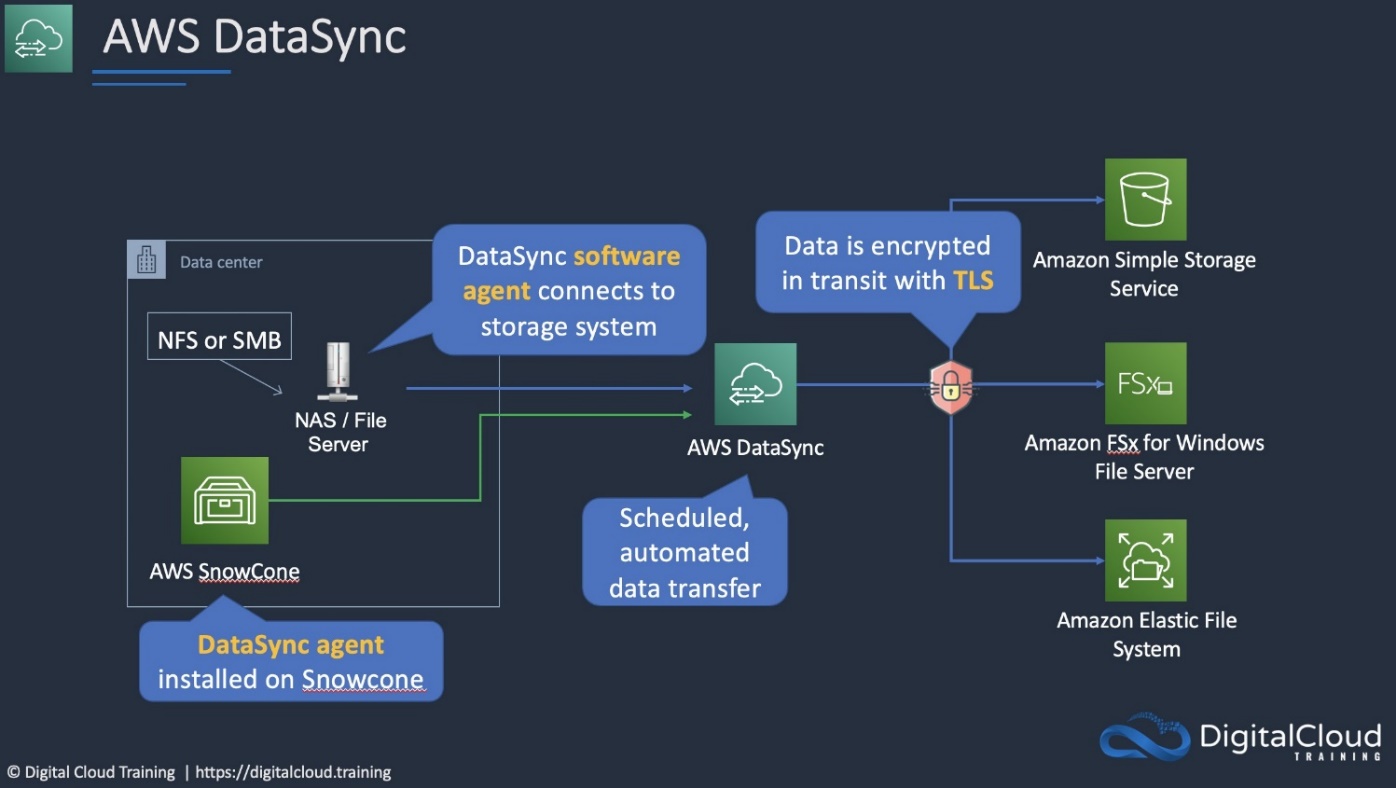
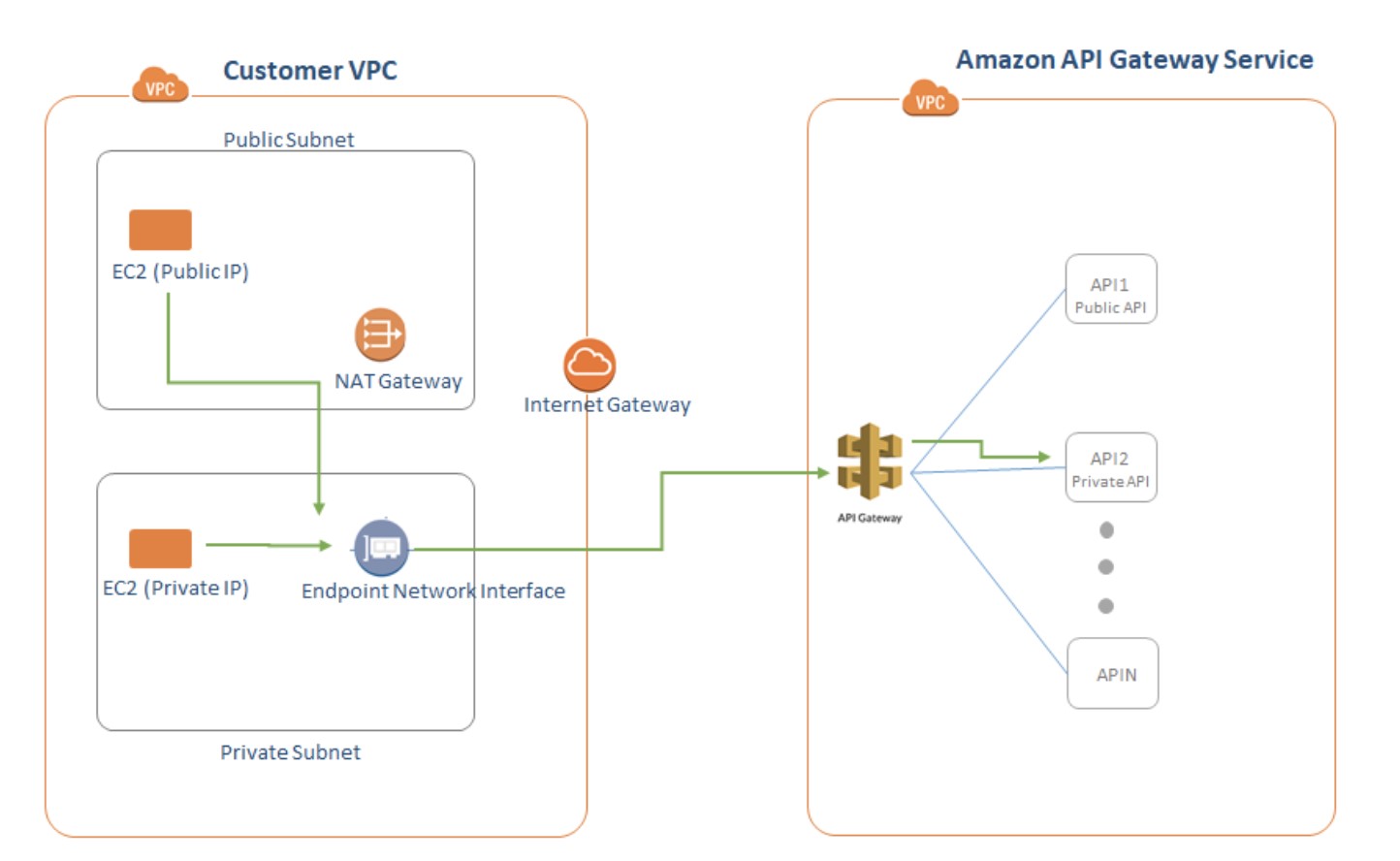
Amazon Aurora Global Database is designed for globally distributed applications, allowing a single Amazon Aurora database to span multiple AWS regions. It replicates your data with no impact on database performance, enables fast local reads with low latency in each region, and provides disaster recovery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

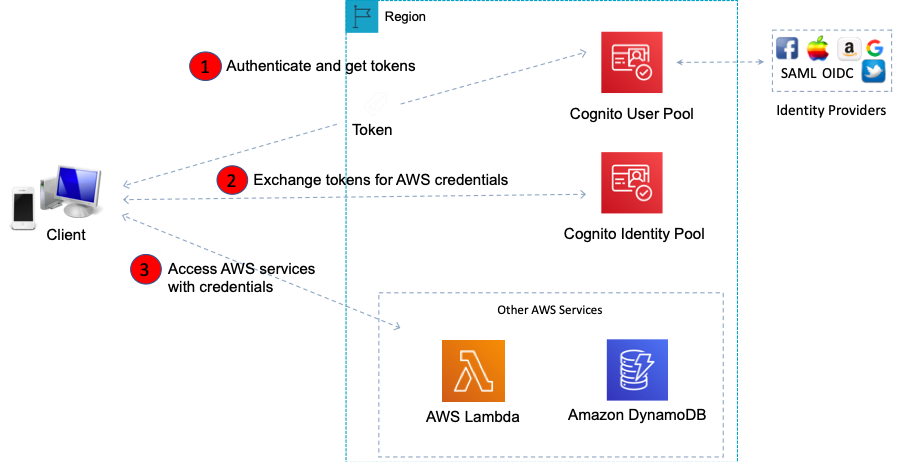


This configuration is powered by AWS PrivateLink and clients do not need to use an internet gateway, NAT device, VPN connection or AWS Direct Connect connection, nor do they require public IP addresses.

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.

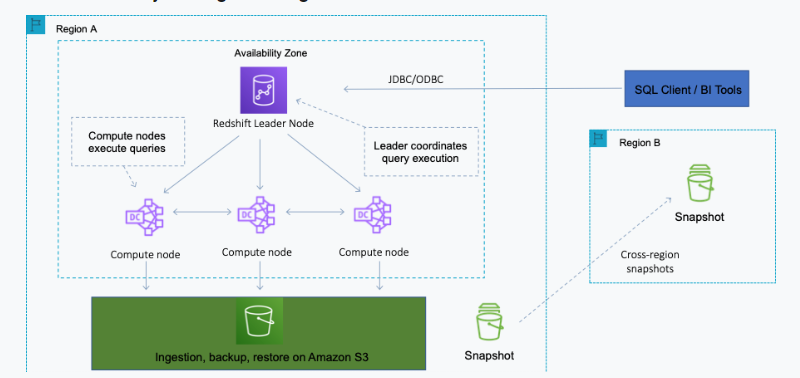
Amazon Cognito identity pools provide temporary AWS credentials for users who are guests (unauthenticated) and for users who have been authenticated and received a token. An identity pool is a store of user identity data specific to your account.

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.