AWS Direct Connect

AWS Direct Connect is a network service that provides an alternative to using the Internet to connect a customer’s on premise sites to AWS.

Data is transmitted through a private network connection between AWS and a customer’s datacenter or corporate network.

Benefits:

* Reduce cost when using large volumes of traffic.
* Increase reliability (predictable performance).
* Increase bandwidth (predictable bandwidth).
* Decrease latency.

Each AWS Direct Connect connection can be configured with one or more virtual interfaces (VIFs).

Public VIFs allow access to public services such as S3, EC2, and DynamoDB.

Private VIFs allow access to your VPC.

Must use public IP addresses on public VIFs.

Must use private IP addresses on private VIFs.

Cannot do layer 2 over Direct Connect (L3 only).

From Direct Connect you can connect to all AZs **within the region.**

You can establish IPSec connections over public VIFs to remote regions.

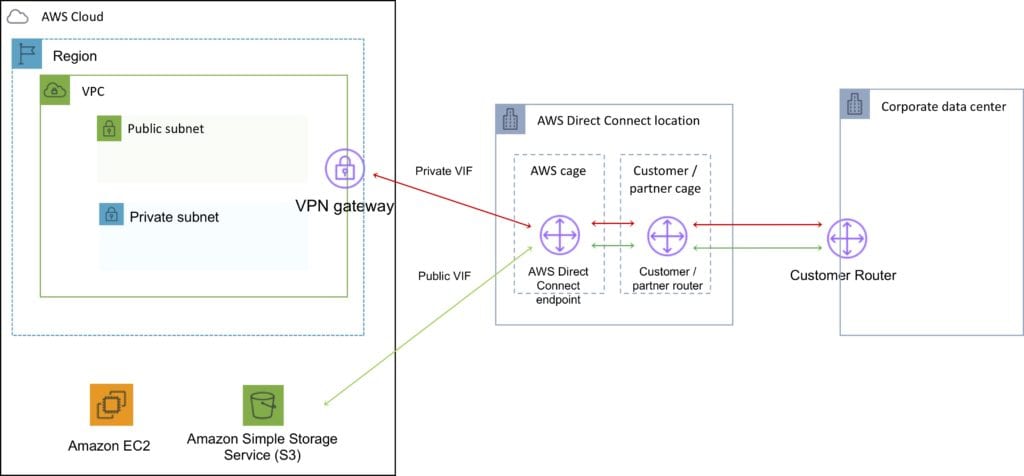
Route propagation can be used to send customer side routes to the VPC.

You can only have one 0.0.0.0/0 (all IP addresses) entry per route table.

You can bind multiple ports for higher bandwidth.

Virtual interfaces are configured to connect to either AWS public services (e.g. EC2/S3) or private services (e.g. VPC based resources).

The diagram below shoes the components of AWS Direct Connect:



Direct Connect is charged by port hours and data transfer.

Available in 1Gbps and 10Gbps.

Speeds of 50Mbps, 100Mbps, 200Mbps, 300Mbps, 400Mbps, and 500Mbps can be purchased through AWS Direct Connect Partners.

Uses Ethernet trunking (802.1q).

Each connection consists of a single dedicated connection between ports on the customer router and an Amazon router.

for HA you must have 2 DX connections – can be active/active or active/standby.

Route tables need to be updated to point to a Direct Connect connection.

VPN can be maintained as a backup with a higher BGP priority.

Recommended to enable Bidirectional Forwarding Detection (BFD) for faster detection and failover.

You cannot extend your on-premise VLANs into the AWS cloud using Direct Connect.

Can aggregate up to 4 Direct Connect ports into a single connection using Link Aggregation Groups (LAG).

AWS Direct Connect supports both single (IPv4) and dual stack (IPv4/IPv6) configurations on public and private VIFs.

Technical requirements for connecting virtual interfaces:

* A public or private ASN. If you are using a public ASN you must own it. If you are using a private ASN, it must be in the 64512 to 65535 range.
* A new unused VLAN tag that you select.
* **Private** **Connection (VPC)** – The VPC Virtual Private Gateway (VGW) ID.
* **Public Connection** – Public IPs (/30) allocated by you for the BGP session.

AWS Direct Connect Gateway

Grouping of Virtual Private Gateways (VGWs) and Private Virtual Interfaces (VIFs) that belong to the same AWS account.

Direct Connect Gateway enables you to interface with VPCs in any AWS Region (except AWS China Region).

You associate an *AWS Direct Connect gateway* with either of the following gateways:

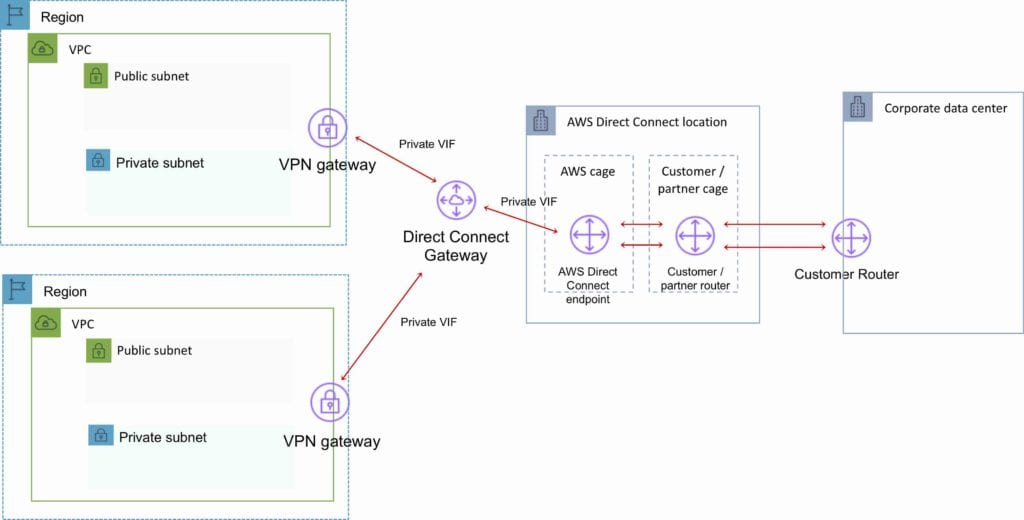
* A transit gateway when you have multiple VPCs in the same Region.
* A virtual private gateway.

Can share private virtual interface to interface with more than one Virtual Private Clouds (VPCs) reducing the number of BGP sessions.

A Direct Connect gateway is a globally available resource.

You can create the Direct Connect gateway in any public Region and access it from all other public Regions.

The diagram below depicts the components of an AWS Direct Connect Gateway configuration:



Ready to test yourself? [**Click here**](https://digitalcloud.training/certification-training/aws-solutions-architect-associate/networking-and-content-delivery/) to check out the free sample practice questions for AWS Networking and Content Delivery