aws academy

AWS ACA Module 2
Designing Your Environment

Integrating On-Premises Components

How do you integrate on-premises components into your environment?

Amazon VPC Connections

VPN Connectivity Options	Description
AWS Hardware VPN	You can create an IPsec hardware VPN connection between your Amazon VPC and your remote network.
AWS Direct Connect	AWS Direct Connect provides a dedicated private connection from a remote network to your Amazon VPC.
AWS VPN CloudHub	You can create multiple AWS hardware VPN connections via your VPC to enable communications between various remote networks.
Software VPN	You can create a VPN connection to your remote network by using an Amazon EC2 instance in your Amazon VPC that's running a software VPN appliance.

There are several VPN connectivity options for Amazon VPC. You can connect your Amazon VPC to remote networks using an AWS Hardware VPN, AWS Direct Connect, AWS VPN CloudHub, or a Software VPN.

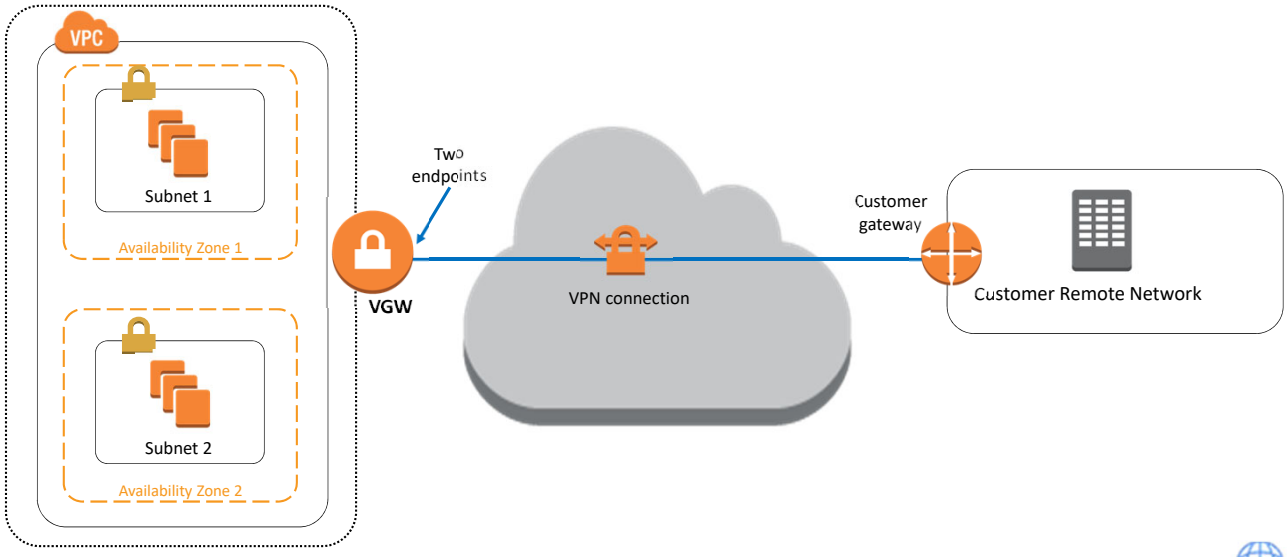
Select a link to learn more.

Amazon Virtual Private Cloud Connectivity Options whitepaper:
https://media.amazonwebservices.com/AWS_Amazon_VPC_Connectivity_Options.pdf

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPN_CloudHub.htm

Extending On-Premises Network to AWS: VPN Connections

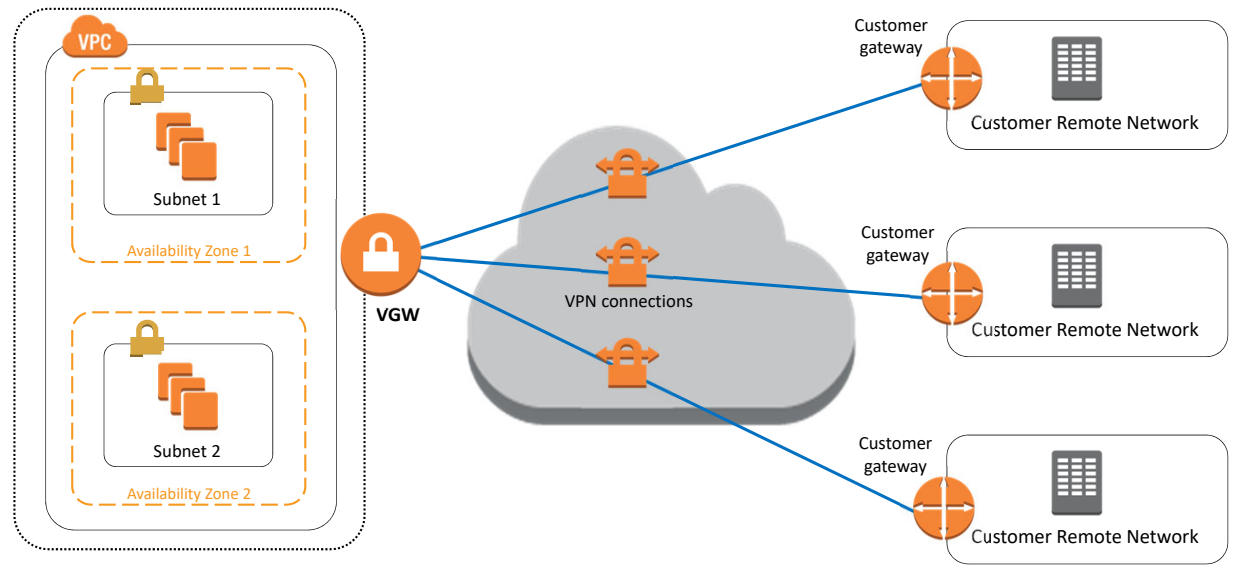


Learn more.

One solution is to use a virtual private network, or VPN, connection between your VPC's virtual private gateway, or VGW, and your data center. With an AWS hardware VPN, you are provided with two VPN endpoints to provide basic, automatic failover. To create an AWS hardware VPN, go to the AWS Managed VPN Connections documentation. http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html

You can also create a VPN connection to your remote network by using an Amazon EC2 instance in your VPC that's running a software VPN appliance. AWS does not provide or maintain software VPN appliances. However, you can choose one from a range of products that partners and open source communities provide through the AWS Marketplace.

Extending On-Premises Network to AWS: Multiple VPN



Amazon Virtual Gateway also supports and encourages multiple customer gateway connections so that customers can implement redundancy and failover on their side of the VPN connection, as shown on this slide. Both dynamic and static routing options are provided to give customers flexibility in their routing configuration. Dynamic routing uses Border Gateway Protocol, or BGP, peering to exchange routing information between AWS and these remote endpoints. Dynamic routing also allows customers to specify routing priorities, policies, and weights or metrics in their BGP advertisements, and to influence the network path between their networks and AWS.

It is important to note that when BGP is used, both the IPSec and the BGP connections must be terminated on the same customer gateway device, so it must be capable of terminating both IPSec and BGP connections.

AWS Direct Connect

AWS Direct Connect provides you with a private network connection between AWS and your data center.

It is a network service alternative to using the internet to access AWS Cloud services.

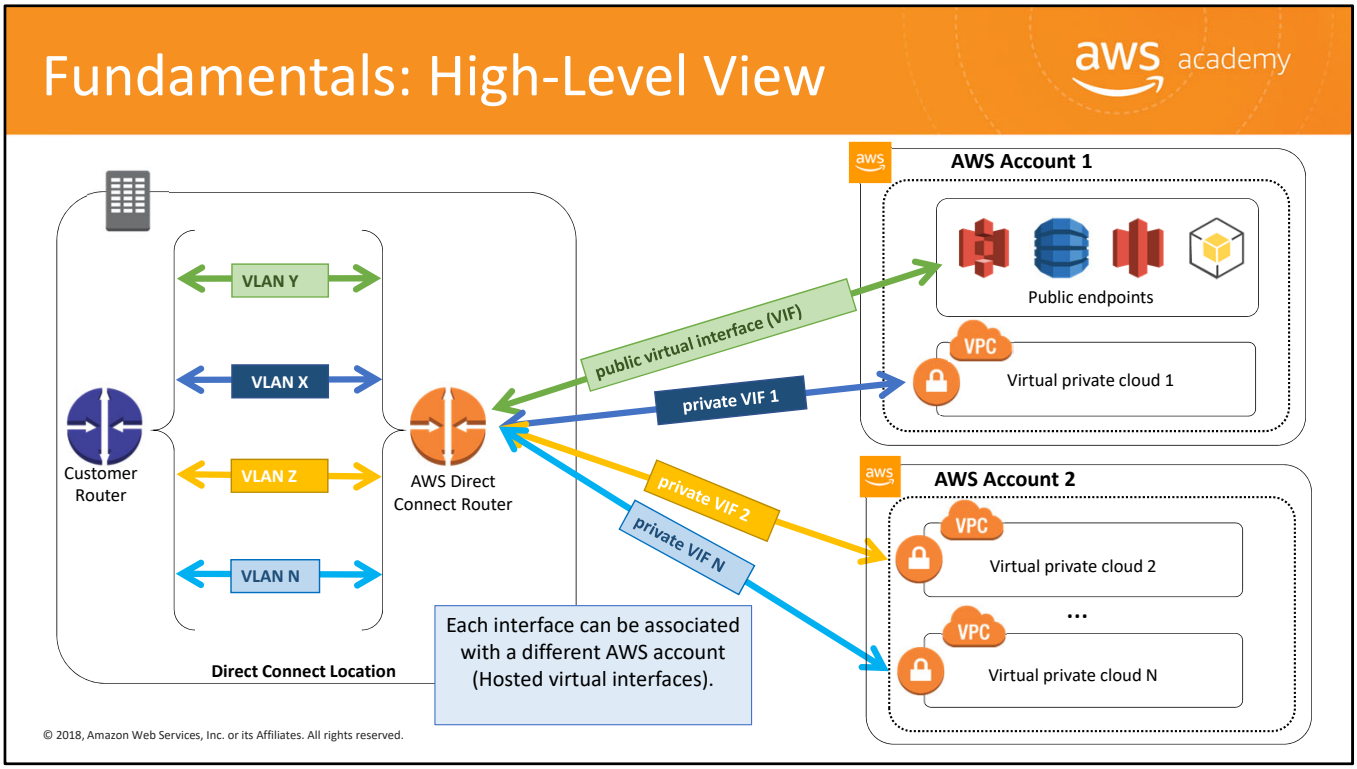
Benefits:

- Dedicated, private fiber to AWS.
- Create virtual interfaces directly to AWS cloud.
- Provides access to AWS in the region it is associated with.
- Provision a single connection and use it to access public AWS services in all regions in the U.S.A. and AWS GovCloud (more locations being added).

AWS Direct Connect provides you with a private network connection between AWS and your data center.

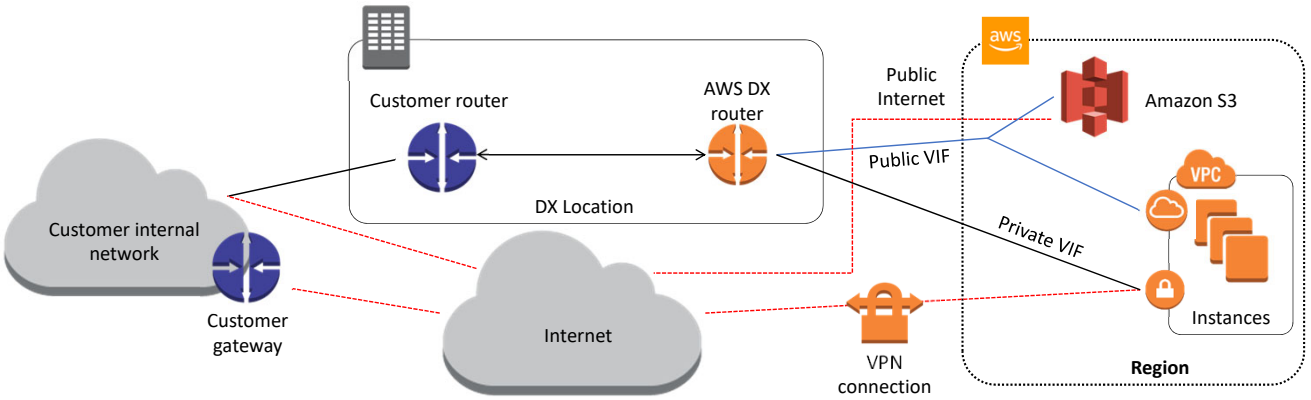
It is a network service alternative to using the internet to access AWS Cloud services.

AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 1-gigabit or 10-gigabit Ethernet fiber-optic cable. One end of the cable is connected to your router, and the other is connected to an AWS Direct Connect router. With this connection in place, you can create virtual interfaces directly to AWS cloud (for example, to Amazon Elastic Compute Cloud, or Amazon EC2, Amazon Simple Storage Service, or Amazon S3, and to Amazon Virtual Private Cloud, or Amazon VPC, bypassing Internet service providers in your network path). An AWS Direct Connect location provides access to Amazon Web Services in the region it is associated with, and to other regions in the United States of America. For example, you can provision a single connection to any AWS Direct Connect location in the U.S.A. and use it to access public AWS services in all regions in the U.S.A. and AWS GovCloud.



At a high-level, here are the various ways in which you can connect your on-prem data center to AWS resources via Direct Connect. In this diagram, you can see the connection between connecting public virtual interfaces, or VIFs, to public endpoints and private virtual interfaces to private endpoints.

Single Router, Single Port lus VPN Backup



- AWS Managed VPN supports up to 1.25 Gbps throughput per VPN tunnel.
- Overlapping routes only via propagated routes.
- If AWS Direct Connect fails, internet backup for public VIF connections, VPN backup for private VIF connections.
- BGP with VPN configuration for faster failover.

Let’s look at this in more detail.

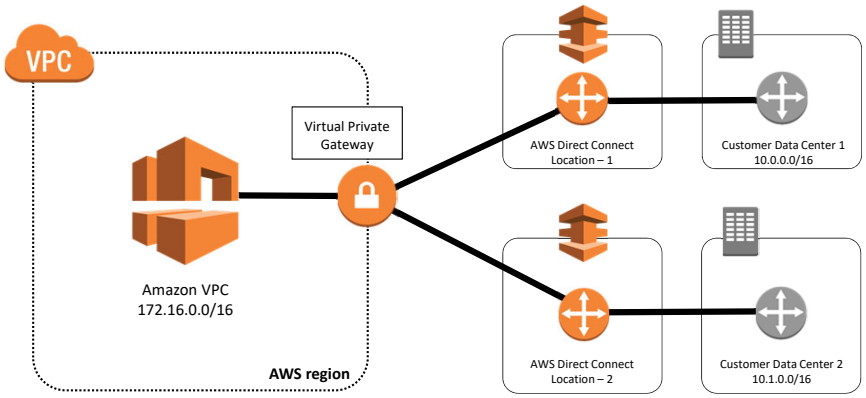
Here is a basic diagram of how a single router, and a single port connection to AWS over Direct Connect would route traffic, along with how traffic would flow, in case there's an issue with the Direct Connect connection and a VPN connection is used as a backup.

It is important to understand that AWS Managed VPN supports up to 1.25 Gbps throughput per VPN tunnel and does not support Equal Cost Multi Path (or ECMP) for egress data path in the case of multiple AWS Managed VPN tunnels terminating on the same VGW. Thus, we do not recommend architectures using AWS Managed VPN as a backup for AWS Direct Connect connections with speeds greater than 1 Gbps.

High Resiliency For Critical Workloads

aws academy

Single Connection Multiple Locations



Learn more.

This configuration consists of AWS Direct Connect connections to separate AWS Direct Connect routers in two locations from two independently configured customer devices. This might be used for critical production workloads that require high resiliency. This would ensure resilience to connectivity failure due to fiber or a device failure as well as a complete location failure.

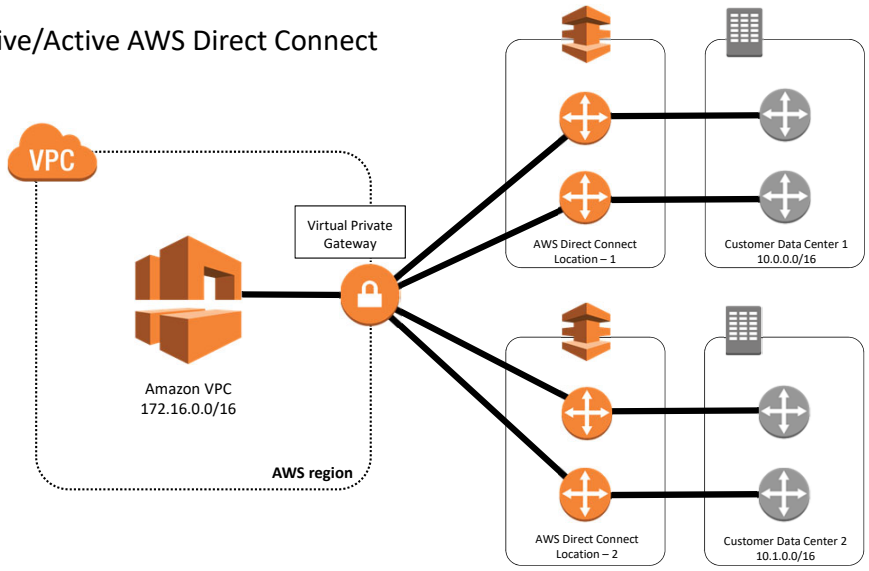
AWS provides example router configurations to assist in establishing AWS Direct Connect connections and configuring BGP for dynamic routing. In addition to the AWS-provided configuration details, customers must configure VPCs to efficiently route traffic to their data center networks.

AWS Direct Connect supports these port speeds over single-mode fiber: 1 Gbps: 1000BASE-LX (1310nm) and 10 Gbps: 10GBASE-LR (1310nm).
It is important to understand that AWS Managed VPN supports up to 1.25 Gbps throughput per VPN tunnel and does not support Equal Cost Multi Path for egress data path in the case of multiple AWS Managed VPN tunnels terminating on the same VGW.

To learn more about AWS Direct Connect for high resiliency, select the link.
https://aws.amazon.com/directconnect/resiliency-recommendation/

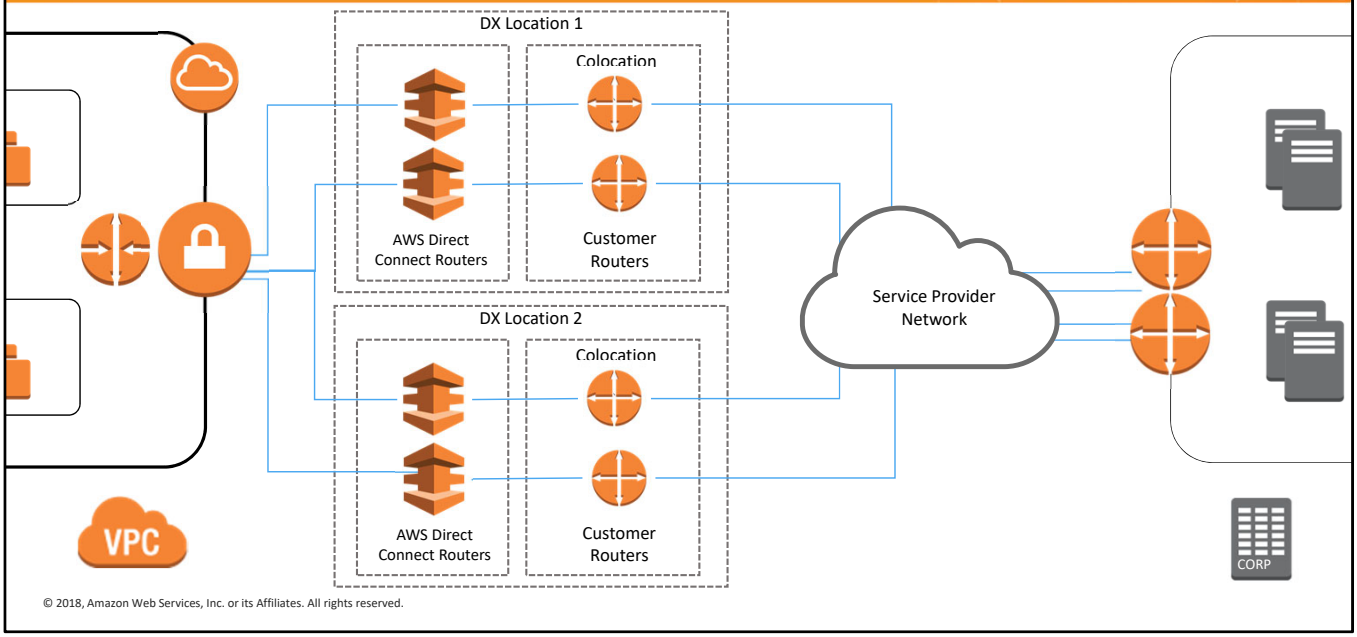
Maximum Resiliency for Critical Workloads

Redundant Active/Active AWS Direct Connect Connections



For maximum resiliency, separate connections terminating on separate devices in more than one location is the recommended architecture. This topology provides resilience to device failure, connectivity failure, and complete location failure.

Dual DX – Dual Location



One further variation in this deployment is dual connections at dual locations with virtual interfaces on each connection. The choice of how much diversity and resilience you choose to deploy depends on your specific resiliency needs.