Using AWS Direct Connect for High Resiliency

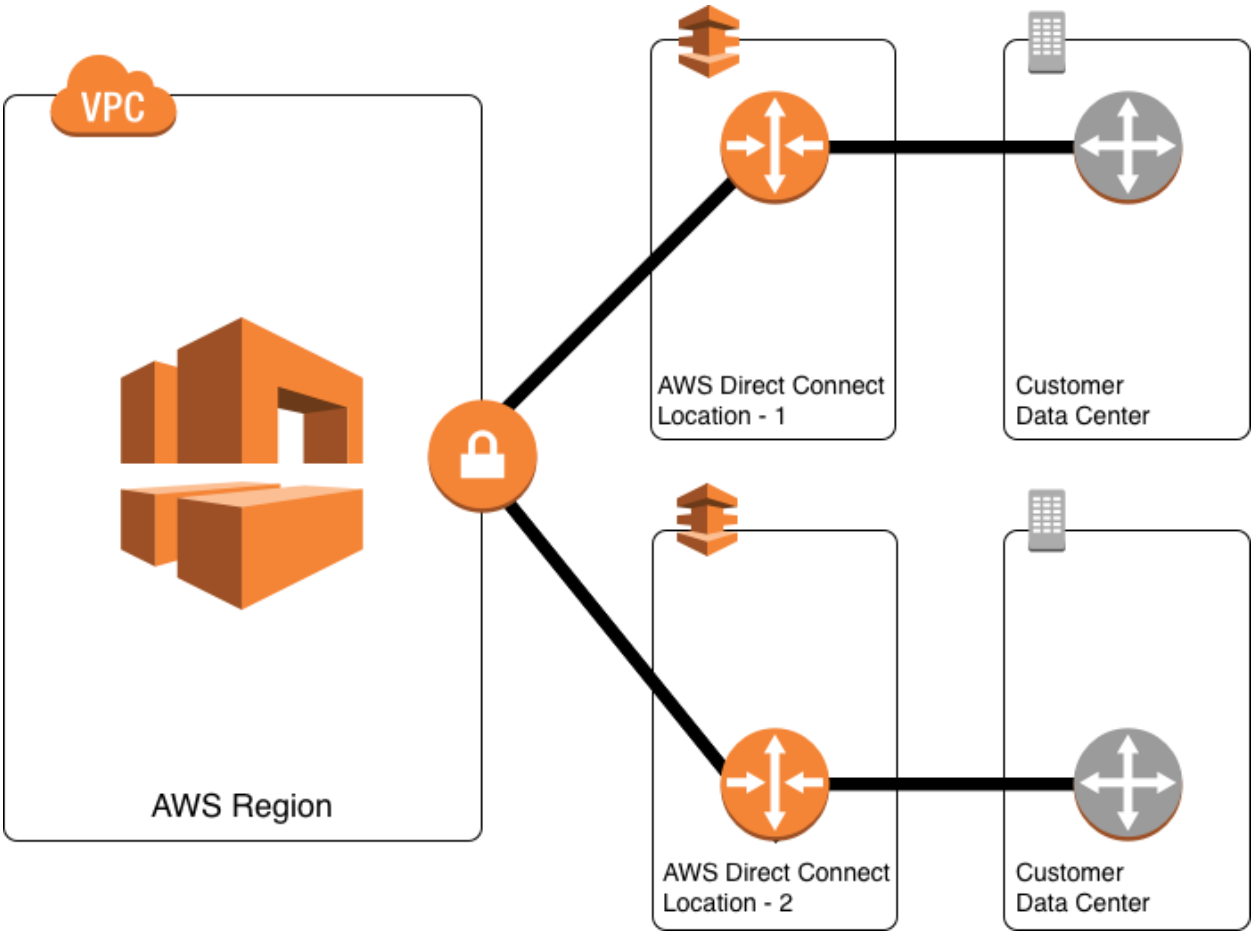
Amazon Web Services (AWS) offers customers the ability to achieve highly resilient network connections between Amazon Virtual Private Cloud (Amazon VPC) and their on-premises infrastructure. This capability extends customer access to AWS resources in a reliable, scalable, and cost-effective way. This page documents our best practices for ensuring high resiliency with AWS Direct Connect.

Recommended Best Practices

Highly resilient, fault-tolerant network connections are key to a well-architected system. AWS recommends connecting from multiple data centers for physical location redundancy. When designing remote connections, consider using redundant hardware and telecommunications providers. Additionally, it is a best practice to use dynamically routed, active/active connections for automatic load balancing and failover across redundant network connections. Provision sufficient network capacity to ensure that the failure of one network connection does not overwhelm and degrade redundant connections.

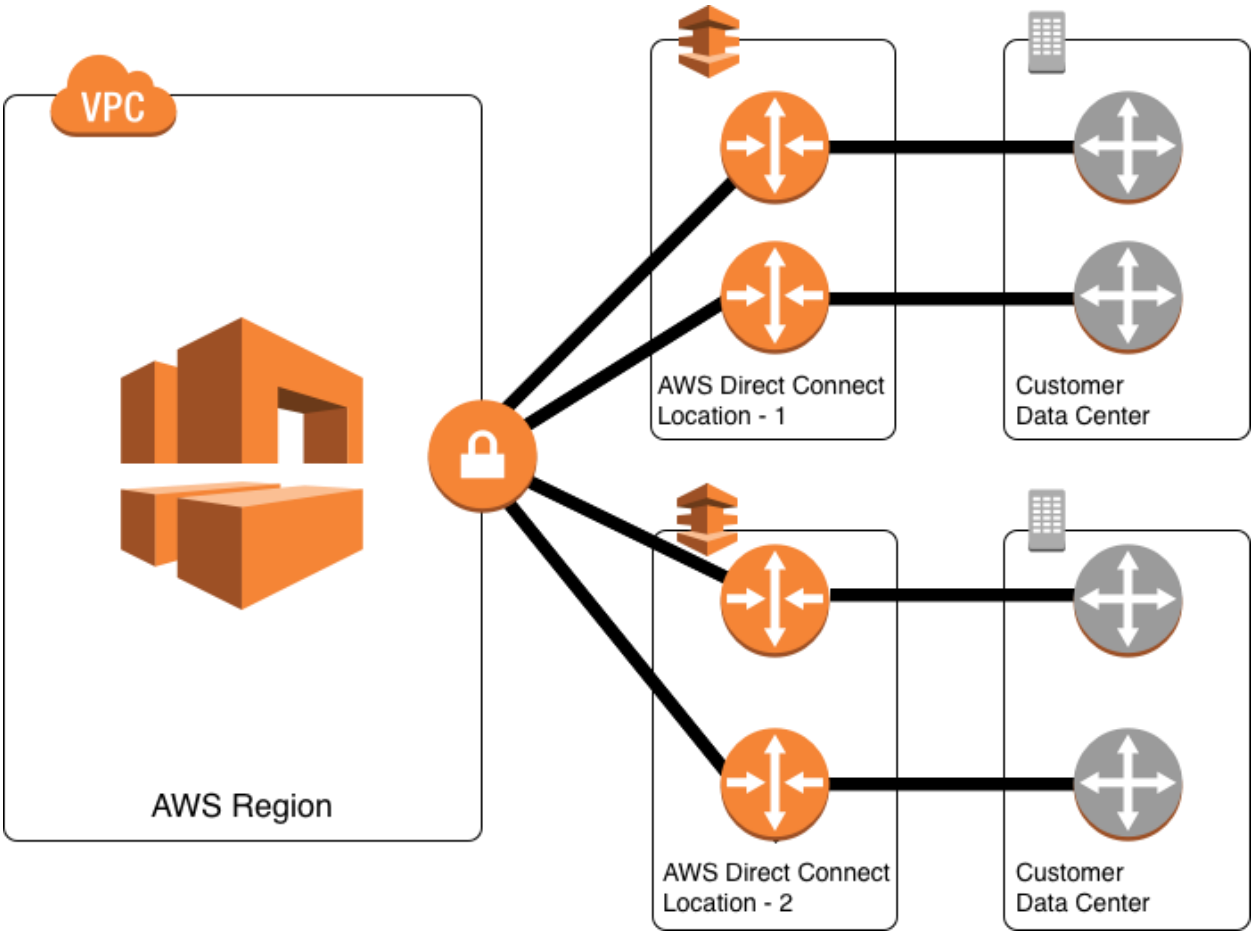
Keep the following topology guidelines in mind when connecting to AWS:

High Resiliency for Critical Workloads



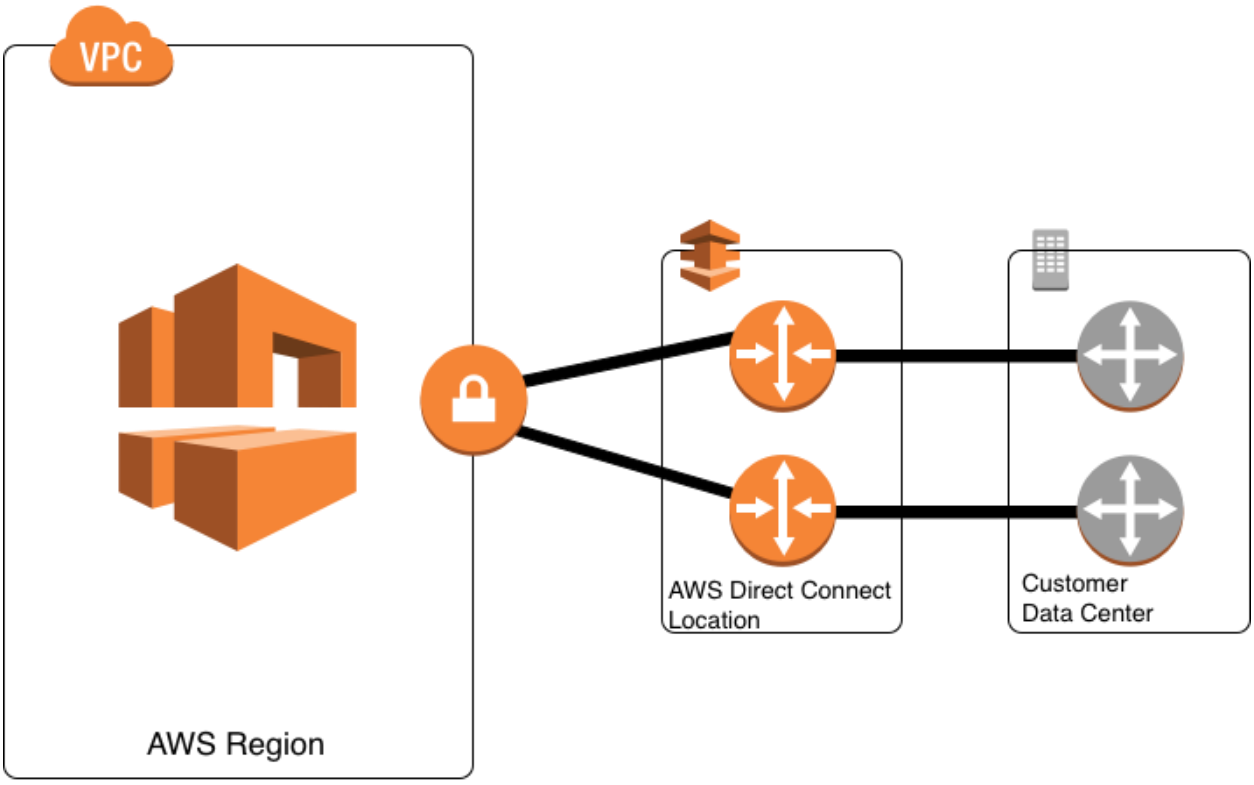
For critical production workloads that require high resiliency, it is recommended to have one connection at multiple locations. As shown in the figure above, such a topology ensures resilience to connectivity failure due to a fiber cut or a device failure as well as a complete location failure. You can use Direct Connect Gateway to access any AWS Region (except AWS Regions in China) from any AWS Direct Connect location.

Maximum Resiliency for Critical Workloads



Maximum resilience is achieved by separate connections terminating on separate devices in more than one location. This configuration offers customers maximum resilience to failure. As shown in the figure above, such a topology provides resilience to device failure, connectivity failure, and complete location failure. You can use Direct Connect Gateway to access any AWS Region (except AWS Regions in China) from any AWS Direct Connect locations.

Non Critical Production Workloads or Development Workloads



For non critical production workloads and development workloads that do not require high resiliency, it is recommended to have at least two connections terminating on different devices at a single location. As shown in the figure above, such a topology helps in the case of the device failure at a location but does not help in the event of a total location failure.

AWS Managed VPN connections as a backup for the Direct Connect

Some AWS customers would like the benefits of one or more AWS Direct Connect connections for their primary connectivity to AWS, coupled with a lower-cost backup connection. To achieve this objective, they can establish AWS Direct Connect connections with a VPN 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 (ECMP) for egress data path in the case of multiple AWS Managed VPN tunnels terminating on the same VGW. Thus, we do not recommend customers use AWS Managed VPN as a backup for AWS Direct Connect connections with speeds greater than 1 Gbps.

Recommendation for AWS Direct Connect Partner selection

AWS Direct Connect Partners help customers establish network connectivity between AWS Direct Connect locations and their data centers, offices or colocation environments. When selecting AWS Direct Connect Partners, consider a dual-vendor approach, if financially feasible, to ensure private-network diversity. When planning your connectivity, work with your selected Partner(s) to determine which of the above best practices are right for your needs, and learn how your selected Partner(s) can enable you to achieve them.

Summary

AWS recommends customers use multiple dynamically routed, rather than statically routed, connections to AWS at multiple AWS Direct Connect locations. This will allow remote connections to fail over automatically. Dynamic routing also enables remote connections to automatically leverage available preferred routes, if applicable, to the on-premises network. Highly resilient connections require redundant hardware, even when connecting from the same physical location. Avoid relying on a single on-premises device connecting to a single AWS Direct Connect device. Avoid relying on AWS Managed VPN as backup for connections that are greater than 1Gbps.