Connecting On-Premise Systems to Cloud Infrastructure

Many organizations are moving applications and workloads to the cloud. The move enables IT to quickly scale resources based on actual need and provides consolidated management of infrastructure at a global level. Because of reliability and security issues associated with a basic internet connection, your business should be aware of alternative methods of connecting your existing network to your network in the cloud, such as Amazon’s VPC VPN and Direct Connect options. While there are many cloud providers, this article focuses on Amazon’s cloud offerings.

An effective way to utilize the cloud is to connect on-premise systems to an AWS cloud system, creating a hybrid cloud environment. There are several methods for achieving this, as well as several uses for this type of cloud environment. There are many uses for a hybrid cloud environment, including: development and test environments, building new apps (both on premise and cloud), creating apps that integrate back to on-premise systems, or migrating existing apps to the cloud. Whatever your business chooses to use the cloud for, you should be aware of the options for connecting your on-premise environment with your cloud environment.

VPC VPN

One option for connecting your on-premise environment and your AWS cloud environment is a VPN. The Amazon AWS VPC creates an encrypted private channel for transferring data between your on-premise network and your Amazon VPC network. The AWS VPC is managed through Amazon’s Virtual Private Gateway, which allows multiple VPC connections to various sites. Each VPC connection requires a ‘Customer Gateway’ which calls for a unique public IP address. Once connection is established between each site, data can be sent and received from the cloud network (VPC) as if you were using any standard VPN connection.

There are several suggested use cases for using AWS VPC to connect your on-premise system to your cloud environment. Hosting a simple public-facing web application, such as a blog or website, gives you additional security and privacy when hosting through AWS VPC. By creating security rules in the Amazon VPC console wizard you can screen incoming HTTP and SSL requests from the internet and prohibit outbound connections from your web server.

Another use for AWS VPC is to host multi-tier web applications. AWSVPC allows you to enforce access and security rules between your webservers, application servers, and databases so that the webserver is publicly accessible, but the application servers and databases are not. AWS VPC is also useful for hosting scalable web applications in the AWS cloud that are connected to your datacenter. You create a VPC where instances in one subnet, such as webservers, communicate with the Internet while instances in another subnet, such as application servers, communicate with databases on your corporate network. An IPSec VPN connection between your VPC and your corporate network secures communication between the application servers in the cloud and databases in your datacenter. This means webservers and application servers in your VPC can grow and shrink as needed.

You can also use AWS VPC to extend your corporate network by moving applications to the cloud, launching additional webservers, or adding additional computing capacity. Your VPC can be hosted behind your corporate firewall, so you can move your IT resources into the cloud without changing how users access applications.
The final use case suggested by Amazon is disaster recovery. Backing up your mission critical data from your datacenter to a small number of Amazon EC2 instances enables you to quickly launch replacement compute capacity in AWS. When the disaster is over, you send your mission critical data back to your datacenter and terminate the Amazon EC2 instances that you no longer need.

There is no additional charge for VPC aside from the normal EC2 charges. However, if you want to create a hardware VPN connection to your VPC using a Virtual Private Gateway, the current billing rate is $0.05 per hour for each VPN connection. This amounts to about $34 per month for one VPN connection. Standard AWS data transfer rates also apply.

Ease of setup, low cost for basic security, along with existing internet utilization for VPN connection round out the ongoing stream of benefits. But don’t overlook the downside of this methodology. From latency and reliability (due to complication from the number of services required to maintain the connection), to dependency on the internet, which introduces its own set of variables such as increased latency and availability issues; all issues need to be addressed. Not to mention the customer’s responsibility for implementing redundancy and failover.

**Direct Connect:**

AWS Direct Connect is, yet another, method to connect your on premise system to the cloud. It operates by linking your internal network to an AWS Direct Connect location. This allows you to bypass local internet providers and create direct virtual interfaces to AWS cloud solutions. A standard 1 or 10 gigabyte fiber optic Ethernet cable is connects to your router on one end and to an AWS Direct Connect router on the other. This connection provides access to any Amazon Web Services function in the region it is associated with, as well as to any other US region.

The dedicated connection from your datacenter, office, or collocation environment to the AWS Direct Connect location can be partitioned into multiple virtual interfaces, allowing the same connection to be used for access to public resources (such as objects stored in Amazon S3 using public IP address space) and private resources using private IP space. Network separation is maintained and the virtual interfaces can be reconfigured at any time.

There are three primary use cases for AWS Direct Connect: large data, data transfers, and real-time data feeds. The first, working with large data sets, requires enough internet bandwidth to meet web and email needs. Transferring large data sets to the cloud can cause access to be very slow when business critical network traffic competes for bandwidth with other internet usage. Increasing your bandwidth through your internet provider is one way to solve this problem. However, this typically requires expensive contract renewals and a minimum commitment.

Alternatively, AWS Direct Connect transfers business data from your local environment to and from AWS. This bypasses your Internet provider while removing network congestion, and requires payment for actual data transferred and ports used, with no minimum commitment. AWS Direct Connect is also useful for utilizing real-time data feeds, which allows you to control how your data is routed. This provides consistency over your network allowing voice and video applications, where performance is contingent on consistent network latency, to operate at full capacity. With network latency over the internet constantly changing as data is routed, AWS Direct Connect provides consistency exactly when and where it is needed.

The final use case for AWS Direct Connect is for hybrid environments. Direct Connect helps ensure that regulatory requirements regarding private connectivity use in hybrid environments is satisfied.
AWS Direct Connect has two separate charges associated with it: port-hours and data transfer. Pricing for port-hours is based on port speed, with partial hours billed as full. This charge ranges from $.03 per hour for a 50M port to $2.25 per hour for a 10G port. Data transfers are billed in the same month the usage occurs (per GB), with no charge for transfers in. Data transfers out are billed at different rates depending on the location of the Direct Connection and whether the destination is local or remote. These charges range from $.020 per GB to $.11 per GB.

Using Amazon Direct Connect to link your on-premise system to a cloud solution makes financial sense for multiple reasons. From bandwidth reduction allowing you to scale back commitment to your Internet provider to reduced data transfer rates from AWS Direct Connect. The math speaks for itself.

But the benefits don’t stop there. Direct Connect also provides consistent network performance by giving you control over which data uses the direct connection and how that data is routed. Direct Connect is compatible with all AWS services, so any AWS services accessible over the Internet are also accessible through Direct Connect. And don’t forget scalability. Being able to scale your connection to meet your needs by using any combination of 1GB and 10GB connections is a bonus. But perhaps the biggest benefit might be the elimination of VPN over internet usage. Now transferring large amounts of data is right at your fingertips.

Despite its many benefits, Direct Connect also has a couple disadvantages. The need to connect to a Direct Connect location limits you if you’re not located in the service area. AWS partners can work with you to provide access to one of these locations, but then the cost will increase. If your traffic loads are not heavy enough or you are not transferring large amounts of data to and from AWS, Direct Connect can also be an expensive option.

**Final Thoughts**

Cloud computing is an effective way to provision the right type and size of resources for your organization, while saving money and maintaining flexibility. While you can connect to the cloud via a basic internet connection, the issues with reliability and security make VPN connections and Direct Connect better options. You should review the needs of your business to decide which method of connecting your on-premise network to your cloud network is right for you.

**Resources:**


Emily Detmer, Business Intelligence Consultant
Decision First Technologies
Emily is a Business Intelligence consultant with experience in SAP Data Services, Universe Design, SAP BusinessObjects BI Suite and SAP HANA. Emily came to Decision First Technologies in 2014 after graduating from Georgia Southern University.