Extend Your IT Infrastructure with Amazon Virtual Private Cloud

January 2010

http://aws.amazon.com/vpc

Understanding Amazon Virtual Private Cloud

Amazon Virtual Private Cloud (Amazon VPC) is a secure and seamless bridge between your existing IT infrastructure and the Amazon Web Services cloud. Amazon VPC enables you to connect your existing infrastructure to a set of isolated AWS compute resources via a virtual private network (VPN) connection. With Amazon VPC, you can extend your existing management capabilities and security services such as DNS, LDAP, Active Directory, firewalls, and intrusion detection systems to include your AWS resources, and protect the information there the same way you do now. Amazon VPC integrates today with Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Block Store (Amazon EBS), and Amazon CloudWatch; it will integrate with other AWS services in the future. As with all Amazon Web Services, there are no long-term contracts, minimum spend, or up-front investments required. With Amazon VPC you pay only for the resources you use.

In many ways, to manage Amazon VPC resources you'll follow the same practices and use the same tools you're using now to manage your own local resources. To help you understand the similarities and differences, let's begin with an overview of the technology. Several familiar objects comprise Amazon VPC:

- A Virtual Private Cloud (VPC): an isolated portion of the AWS cloud.
- Subnet: a segment of a VPC's IP address range where you can place groups of isolated resources.
- VPN connection: the link between your Amazon VPC and your data center, corporate network, or co-location facility.
- VPN gateway: the Amazon VPC side of a VPN connection.
- Customer gateway: your side of a VPN connection.
- Router: interconnects subnets and directs traffic between the VPN gateway and subnets.

Amazon VPC provides you with one cloud and VPN connection. Within this cloud you can define up to 20 subnets, following conventional CIDR notation; subnets are connected in a star topology with a single virtual router between them and can range in size from a /18 to a /28. (For more information on CIDR notation see http://en.wikipedia.org/wiki/CIDR; on star networks see http://en.wikipedia.org/wiki/Star_network).

You define the IPv4 address range of your cloud (IPv6 isn't currently supported). It can be part of your existing internal or public range, any other public range you own, or a private range. AWS performs no address translation between your corporate network and Amazon EC2 instances in an Amazon VPC. Resources you locate inside your cloud are directly available to your internal network after you define the routing and update your security policies. None of the resources are advertised to the Internet, although you can do this if you wish using appropriate rules in the router connecting your corporate network to your Internet service provider.

The VPN connection uses industry-standard IPsec tunnel mode (with IKE-PSK, AES-128, HMAC-SHA-1, PFS) to authenticate the gateways to each other and to protect the data in transit from eavesdropping and tampering. IPsec adds minimal overhead to the traffic stream—encryption and encapsulation add about 7% additional bandwidth utilization. Most network interface cards now offload encryption functions to a specialized processor, so the performance of your customer gateway shouldn't be affected.

Resources you define in Amazon VPC belong only to you. They can't be accessed from outside your VPN connection and they have no direct connection to the Internet. If your Amazon VPC resources need to communicate externally, that traffic first passes over the VPN and through your existing infrastructure; return traffic follows the reverse route. This allows you to apply the same inspection policies and management practices that you're already using.

Just as with public Amazon EC2 instances, you can monitor the performance of the instances running inside your VPC with Amazon CloudWatch. This web service provides you with visibility into resource utilization, operational performance, and overall demand patterns—including CPU utilization, disk reads and writes, and network traffic. The information is displayed on the AWS Management Console and is also available through APIs. With some simple scripts you can integrate Amazon CloudWatch into your existing management tools. The service maintains a rolling two weeks of historical data, even after you've terminated an instance. If you want to persist more than two weeks while instances are running, or beyond two weeks after you terminate an instance, a command line tool allows you to save data in Amazon S3 or Amazon SimpleDB. In an upcoming future release, Amazon VPC will support Elastic Load Balancing and Auto Scaling for Amazon EC2 instances. (In the initial release of Amazon VPC, Elastic Load Balancing and the Auto Scaling feature of Amazon CloudWatch aren't available.)

Scenarios for Using Amazon VPC

What can you do with Amazon VPC? Imagine a data center that instantly scales according to demand, that doesn't burn money while idle, that you don't have to maintain, and that enables your organization to quickly deliver new solutions as your business needs demand. Amazon VPC can bring these qualities to the infrastructure you already have without requiring you to sacrifice security or change your management practices. To help get you started, we've described some example use cases that you can adopt today. The scenarios here are essentially variations on a theme. These deployment ideas take advantage of Amazon VPC's abilities to logically separate resources yet still permit them to communicate with each other and with resources in your corporate network. They should give you some ideas of how you can use Amazon VPC to satisfy your unique requirements.

Remember, too, that your Amazon VPC resources behave like Amazon EC2 instances. Physical servers of your own can be powered off, then powered back on and will resume from their prior state. Amazon EC2 server instances, once terminated, can't be resumed (although you can reboot them if necessary). You can use Reserved Instances with Amazon VPC and you will receive the standard discounted effective hourly rate, although during the beta we can't guarantee instance availability. In some of the scenarios below we describe how you can save snapshots of running server instances and restart from these as necessary.

Build a test environment

Software environments are in constant flux, with new versions, added features, patches, and updates. Software changes must often be deployed rapidly, with little time to test how they might affect what's already in production. In an ideal world you'd have a test lab that mirrors your production environment, and here you'd install and exercise software updates against a typical workload. Once the update or new version passes, then you can roll it into production with greater confidence.

Amazon VPC can help you build an economical and functional test lab. In-house test labs require hardware, which most of the time goes unused. Often, dedicated test hardware that sits idle gets repurposed into production hardware, and your lab ends up disappearing despite the best of intentions. By building your lab in Amazon VPC, you don't need to budget for extra hardware and you can easily modify your lab to remain current with your production environment.

Amazon EC2 provides you with pre-configured Amazon Machine Images (AMIs) that you can customize to approximate your environment. Once you complete the initial image creation, you bundle your customized images and save them in

Amazon Simple Storage Service (Amazon S3). When it's time to conduct a test, you start new instances from your custom AMIs. You now have a test lab that looks like your production environment, but is isolated from it. You install the software on these instances and perform your tests. After you're satisfied with the behavior, and have ensured that any other modifications to existing software don't affect performance or exhibit unexpected behavior, you install the updates into your production environment and repeat any modifications made to the test environment. Finally, you bundle the updated instances into new custom AMIs and terminate the instances. When the next test cycle comes, you simply repeat this procedure.

Model and establish a greenfield production environment

The day will come when some or all of your business requires a fundamental shift in the technology it uses and the ways in which it is used. While the urge to "throw it all away and start over" can be very strong, actual opportunities are rare. Building a greenfield environment next to a legacy environment is risky. Unknown dependencies might creep in and new services might be discovered and used before they're ready. A better alternative would be to build your greenfield environment separately from the current environment, incorporate only the expected applications and behaviors, and cleanly shift users over after the greenfield environment is thoroughly tested.

Amazon VPC can simplify this transition. Start with Amazon's standard machine images and construct your new environment. Through the VPN connection, you can control how "local" the VPC resources appear to your legacy environment. You can expose them to internal users, authenticate to your existing enterprise directory, and manage them with the tools and practices you already have. You should publish a timeline that lets users know when data will be migrated and create guidance that instructs users how to switch to the new environment. Because your existing infrastructure remains in place, you can easily roll back from Amazon VPC should this become necessary.

Create branch office and business unit networks

If you have branch offices that require separate but interconnected local networks, consider deploying resources inside Amazon VPC and assign each office its own subnet. Applications within a subnet can freely communicate with each other. Applications can also communicate across subnets through the virtual router. Because instances inside Amazon VPC are already protected by the VPN, there's no need for the security group virtual firewall required for standard Amazon EC2 instances exposed to the Internet. If you need to limit flows within or across subnets, you can configure software firewalls or create IPsec transport-mode security associations on the instances to define which servers are permitted to communicate with each other. (Note: this is separate from the IPsec tunnel-mode security association that you create between your customer gateway and the Amazon VPC VPN gateway.)

You could use this same idea to group applications according to business unit functions, too. Applications specific to particular business units can be installed into separate subnets, one for each unit. Similar to the branch office scenario, you can add software firewalls or IPsec security associations if you need to control inter- and intra-subnet communications.

In the future, Amazon VPC will allow you to define multiple private clouds, configure more than one VPN connection and customer gateway, and provide a mechanism to define security groups on the virtual router. This will give you even more flexibility for controlling traffic between your network and your clouds, as well as traffic among your clouds.

Admittedly, the distinction between using Amazon VPC for branch office and business unit resources might seem slight when compared to installing dedicated resources in each office. In both cases, IT operations will need to utilize remote management tools to configure and maintain the resources. The principal advantages of Amazon VPC over dedicated hardware derive from the same advantages Amazon EC2 offers elsewhere: you can elastically scale the resources to meet the demand required, ensuring that you don't under- or over-provision. Adding capacity is easy: turn on additional instances using your custom images. When the time comes to decrease capacity, simply terminate the unneeded instances. While the operational tasks may be the same to keep assets running properly within a VPC branch office as compared to a hardware-oriented branch office, you won't need dedicated remote staff. You'll enjoy the cost savings that comes from AWS's pay-as-you-go pricing and not have to explain why you've invested in resources that largely don't perform to full capacity.

Isolate legacy and experimental applications from the corporate network

Most of the scenarios described here mention using Amazon VPC for new applications and for adding capacity to your IT environment. Every organization also has older applications that were designed for an earlier era. These might require using an operating system you're migrating away from or a server configuration that isn't compatible with your standard builds. Rather than maintaining the equipment yourself and managing corresponding policy exceptions, consider creating a legacy subnet inside a VPC and housing your legacy applications there.

You can isolate this subnet from the rest of your corporate network with rules you create either on the customer gateway on your side of the VPN connection or elsewhere in your own security infrastructure (perhaps the firewall behind your gateway). Although the individual server images running in this subnet will have automatically-assigned addresses, remember that you define the address range. With rules configured in your gateway and infrastructure, you can limit what traffic is allowed to pass between the legacy subnet's CIDR block and your corporate network.

The same logic applies to experimental applications. Perhaps you're evaluating a software package that you'd like to keep isolated from your production environment while you examine its functions and behavior. You can conduct your evaluations on a few Amazon EC2 instances inside your VPC. If all goes well, then consider transitioning these images into production and granting access to authorized users through your customer gateway. This will save you the cost of purchasing, installing, and maintaining additional hardware in your own data center.

Establish a disaster recovery and business continuity plan

No one likes to spend time planning for unpleasant events. Alas, they do happen, and without prior planning the consequences can be devastating. Traditional approaches to disaster recovery usually require labor-intensive backups and expensive standby equipment whose capacity is wasted. Instead, consider including Amazon VPC in your disaster recovery plan. The elastic, dynamic nature of AWS is ideal for disaster scenarios where there are sudden spikes in resource requirements.

Start by identifying those IT assets that are most critical to your business. Similar to the test lab scenario, you can build specialized Amazon EC2 AMIs inside your VPC that are customized to duplicate the functionality of your critical assets. Using automated processes, you can back up your production data into additional Amazon EBS volumes. In the unfortunate event of a disaster, you can quickly transition your business to your VPC by starting new instances from your custom AMIs, attaching your data volumes, and directing access to these servers. If your disaster involved only the loss of data from your existing in-house servers, you can recover it easily from the Amazon EBS data volumes you've been using as backup storage (although EBS volumes shouldn't be your only mechanism for backing up your data).

If your loss includes your physical location, then access to your Amazon VPC resources isn't possible because your customer gateway is unavailable. In such a scenario you have a couple options. If you have more than one site, we can work with you to quickly re-establish connectivity to your VPC from another location. As soon as routing information re-plumbs through your network, users in unaffected sites will regain access to your VPC. If you have only a single site, then all isn't lost—you'd instead work with the public side of AWS, using Internet-accessible Amazon EC2 instances. From anywhere on the Internet you can log into your AWS account and create a temporary data center completely in the cloud, using your custom AMIs and existing EBS data volumes. Simply starting new instances from your AMIs and attaching your data volumes is all you need to do. Remember in this case that you also need to define security groups to protect your running instances, because these aren't protected by the security policies normally defined in your corpnet.

Stream applications and create virtual desktops

Several of Amazon's partners, including Citrix, AppZero, InstallFree, and Nasstar have built client virtualization and application streaming solutions that can be hosted inside Amazon EC2 machine images. You can do many things when you host virtual desktops or stream client applications from your VPC. For example, you can deliver training courses that require specific images, allow onsite contractors to run virtualized desktops that follow your corporate standards, and provide remote employees and home users connected to your corporate VPN with the same environment they have at the office.

If you're hosting an internal seminar and you need to deploy a number of client PCs for attendees to use, you can minimize your costs by leasing thin-client computers and configure them to run a customized virtual desktop that's loaded from your VPC. Any project or program that requires desktop PCs for a short period of time is a good candidate for virtual desktops or application streaming. For example, you can use a virtual desktop infrastructure (VDI) to test new or updated client applications before deployment. If you have a business requirement to run a specific application that you want to keep isolated from the rest of your environment, a VDI can provide an effective sandbox.

Consider also the advantages you can gain from deploying a virtual desktop infrastructure for persistent uses, too. By moving the compute workload into Amazon VPC, you can delay the purchase of new desktop PCs and extend the life of existing client hardware. A centrally managed VDI allows you to more easily keep operating systems patched and updated and provides a simple way to deploy new client applications. Plus, in highly-regulated industries with non-mobile employees, a VDI can significantly reduce the risks of data loss and malware infection.

A VDI can help you reduce your organization's energy consumption by allowing you to cut power to offices at night and during weekends; when users return each morning, their computers will be powered up and their sessions resumed from Amazon VPC.

<Insert your idea here>

We hope this short paper has triggered some ideas of your own. We believe these scenarios are great ways to begin exploring the opportunities Amazon VPC enables. We look forward to learning from you how Amazon VPC has improved your organization's ability to better integrate IT with the business.