RemoteApp Publishing on AWS

amazon web services | Partner Network

ADVANCED CONSULTING PARTNER
CHANNEL RESELLER PARTNER

WWW.CORPINFO.COM

Kevin Epstein & Stephen Garden
Santa Monica, California
November 2014

TABLE OF CONTENTS

ABSTRACT

Deploying Microsoft Remote Desktop Services is an advanced topic and requires knowledge and skills beyond Amazon Web Services (AWS) technologies. This whitepaper is intended to be a guide for businesses that currently deploy their applications via Remote Desktop Services and RemoteApp, and who are looking to utilize AWS as a more scalable, flexible, and cost-effective infrastructure platform to host the solution. This whitepaper also serves as a reference for businesses that are investigating deploying Remote Desktop Services. It outlines the best practices for managing large deployments on the AWS cloud platform and offers a reference architecture to guide organizations in the delivery of these complex systems.

CorpInfo is a California based Advanced AWS Consulting Partner and Microsoft Partner. We specialize in deploying Microsoft Windows solutions into the AWS cloud through a combination of these skill sets.

INTRODUCTION

Microsoft RemoteApp is part of Microsoft Remote Desktop Services. With RemoteApp, organizations can provide access to a suite of applications without having to roll those applications out to every desktop in the organization, while also being able to restrict users access to the user interface of the published RemoteApp if desired, or deliver a full Remote Desktop experience. Publishing business applications as RemoteApp programs greatly reduces the administrative overhead of managing and maintaining those applications.

WHAT WE'LL COVER

This whitepaper assumes some familiarity with Remote Desktop Services, and does not go into the technical procedures for installing Remote Desktop Services, nor publishing RemoteApp applications. Instead this whitepaper covers important topics that must be considered when deploying Remote Desktop Services into the AWS cloud.

- The trend towards remote application delivery
- Overview of Remote Desktop Services and RemoteApp
- The benefits of Remote Desktop Services
- Deploying SaaS offerings on AWS via RemoteApp
- Two different reference architectures for RemoteApp
    - Private deployment -- In this reference architecture, RemoteApp is deployed in an Amazon Virtual Private Cloud (Amazon VPC) and RemoteApp programs are not exposed to the Internet. Access to RemoteApp programs is only possible via a site-to-site VPN connection between the corporate network and the Amazon VPC.

- Public deployment -- In this reference architecture, RemoteApp is leveraged to deliver SaaS offerings to customers or business partners. Access to RemoteApp programs is handled via a gateway service. This design assumes that the Amazon VPC has no connectivity back to a corporate office.

- Additional architectural considerations

The trend towards remote application delivery

Remote application delivery is increasing within organizations of all sizes. One of the drivers of this trend is the growth in mobile device support and bring-your-own-device programs. Remote application delivery allows organizations to deliver secure applications to various user devices in a secure and compliant manner while protecting corporate data and IT assets.

Microsoft Remote Desktop Services with RemoteApp is a cost-effective approach to remote application delivery. While these technologies can be deployed on premises, there are significant benefits to deploying them in a cloud infrastructure. By deploying RemoteApp in an Infrastructure as a Service (Iaas) environment organizations can reduce upfront deployment cost and shrink the deployment window. Additionally, IaaS allows organizations to rapidly scale the infrastructure to meet fluctuating demands, thus only paying for the computing power required at any given time. Additionally, it frees the internal IT resources from some operational and support functions.

Using AWS for RemoteApp deployments adds superior security and compliance to what many organizations can internally provide. Deploying RemoteApp on AWS provides robust and secure application delivery. Applications are never sent to or stored on employee devices, but are centralized on a secure and reliable AWS instance.

Microsoft Remote Desktop Services and RemoteApp

Remote Desktop Services, formerly Terminal Services, enables users to access Windows-based applications that are installed on a Remote Desktop Session Host server. Users can access the remote server from within a corporate network or via the Internet. Applications launched within Remote Desktop Services run on the server and support multiple simultaneous user sessions.

With RemoteApp and Desktop Connection, programs accessed remotely through Remote Desktop Services appear as if they are running on the end user's local device and are integrated with the client interface. Users can install Microsoft Remote Desktop clients on their Internet-connected devices and then access applications as if they were running locally.

Remote Desktop Services allows non-mobile Windows programs to run on mobile devices. By deploying a Windows application in the cloud, users can access the application from their mobile device even if the application does not have a mobile version. The program can be run easily as when the processing takes place on the Remote Desktop Session Host server.

Benefits of Remote Desktop Services

Remote Desktop Services has several benefits that empower users, streamline IT operations, increase business agility, improve cash flow, and create greater overall efficiencies. Microsoft outlines the benefits of Remote Desktop Services as follows:

- **Application deployment:** You can quickly deploy Windows-based programs to computing devices across an enterprise. Remote Desktop Services is especially

useful when you have programs that are frequently updated, infrequently used, or difficult to manage.

- **Application consolidation:** Programs are installed and run from a Remote Desktop Session Host server which eliminates the need for updating programs on client computers. This also reduces the amount of network bandwidth that is required to access programs.
- **Remote access:** Users can access programs that are running on a Remote Desktop Session Host server from devices such as home computers, kiosks, low-powered hardware, and operating systems other than Windows.
- **Branch office access:** Remote Desktop Services provides better program performance for branch office workers who need access to centralized data stores. Data-intensive programs sometimes do not have client/server protocols that are optimized for low-speed connections. Programs of this kind frequently perform better over a Remote Desktop Services connection than over a typical wide area network.
- **Secure remote access to sensitive data**: Organization may need to provide access to sensitive data that should not be stored and handled on client machines. With RemoteApp users are empowered to perform their job functions without risking data leaking outside of the organization.
- **Support for diverse devices:** Remote Desktop Services supports various operating systems, tablets, and phones including iOS, Mac OS X, and Android.

Deploying SaaS Offerings on Amazon Web Services

In addition to the increased adoption of remote application delivery, organizations are rapidly moving towards greater usage of Software as a Service (SaaS) offerings. SaaS not only helps to support mobility and bring-your-own-device programs, but it can also reduce IT complexity, provide rapid application deployment, and reduce capital expenditures.

With the increasing adoption of cloud services, software vendors that fail to provide cloud-based applications risk losing market share, or even eroding their current install base. However, it is cost prohibitive to build a data center capable of hosting reliable, secure, and compliant SaaS offerings. This barrier can be overcome by leveraging existing IaaS environments.

Innovative developers have been turning to Amazon Web Services for a robust, world-class infrastructure on which to host SaaS offerings. Microsoft Remote Desktop Services with RemoteApp can be deployed on AWS to provide a cost-effective solution for delivering SaaS offerings for Windows applications.

Solution Components

The Remote Desktop Services solution on AWS consists of the following solution components:

MICROSOFT ACTIVE DIRECTORY

Active Directory is the fabric of any Windows deployment. It is a database that manages user accounts, user groups, service accounts, security groups, DNS, and machine accounts, and many other aspects of the Windows network. Active Directory is managed by one or more Domain Controllers, and in some cases Read-Only Domain Controllers.

MICROSOFT DESKTOP CONNECTION BROKER

Remote Desktop Connection Broker (RD Connection Broker), formerly Terminal Services Session Broker (TS Session Broker), is a role service that provides the following functionality:

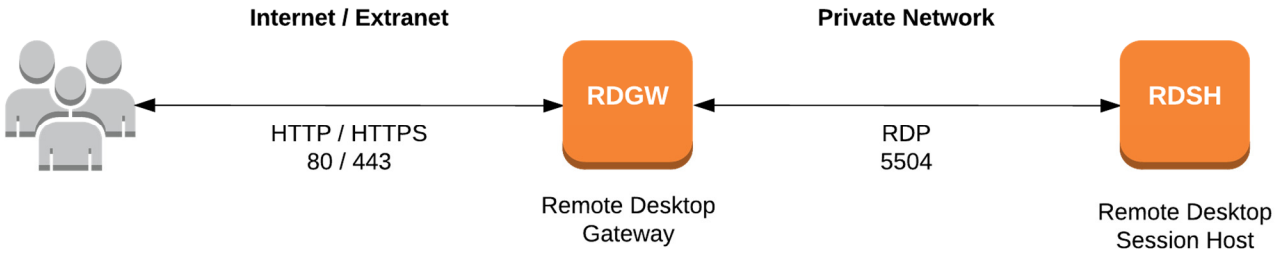
- Allows users to reconnect to their existing sessions in a load-balanced RD Session Host server farm. This prevents a user with a disconnected session from being connected to a different RD Session Host server in the farm and starting a new session.

- Enables the session load to be evenly distributed among RD Session Host servers in a load-balanced RD Session Host server farm.

- Provides users access to virtual desktops hosted on RD Virtualization Host servers and to RemoteApp programs hosted on RD Session Host servers through RemoteApp and Desktop Connection.

MICROSOFT REMOTE DESKTOP GATEWAY

A Remote Desktop Gateway (RDGW) is typically used to bridge two disparate networks, usually the Internet or an extranet, and the company's private network. Communications between users in the Internet or extranet and the gateway are usually done over HTTP or HTTPS, while communications between the gateway, and the Remote Desktop Session Host is done on TCP port 5504. In larger deployments where load-balancing between Session Hosts is required, the RDGW may communicate with a Remote Desktop Connection Broker instead of directly with the Session Host.

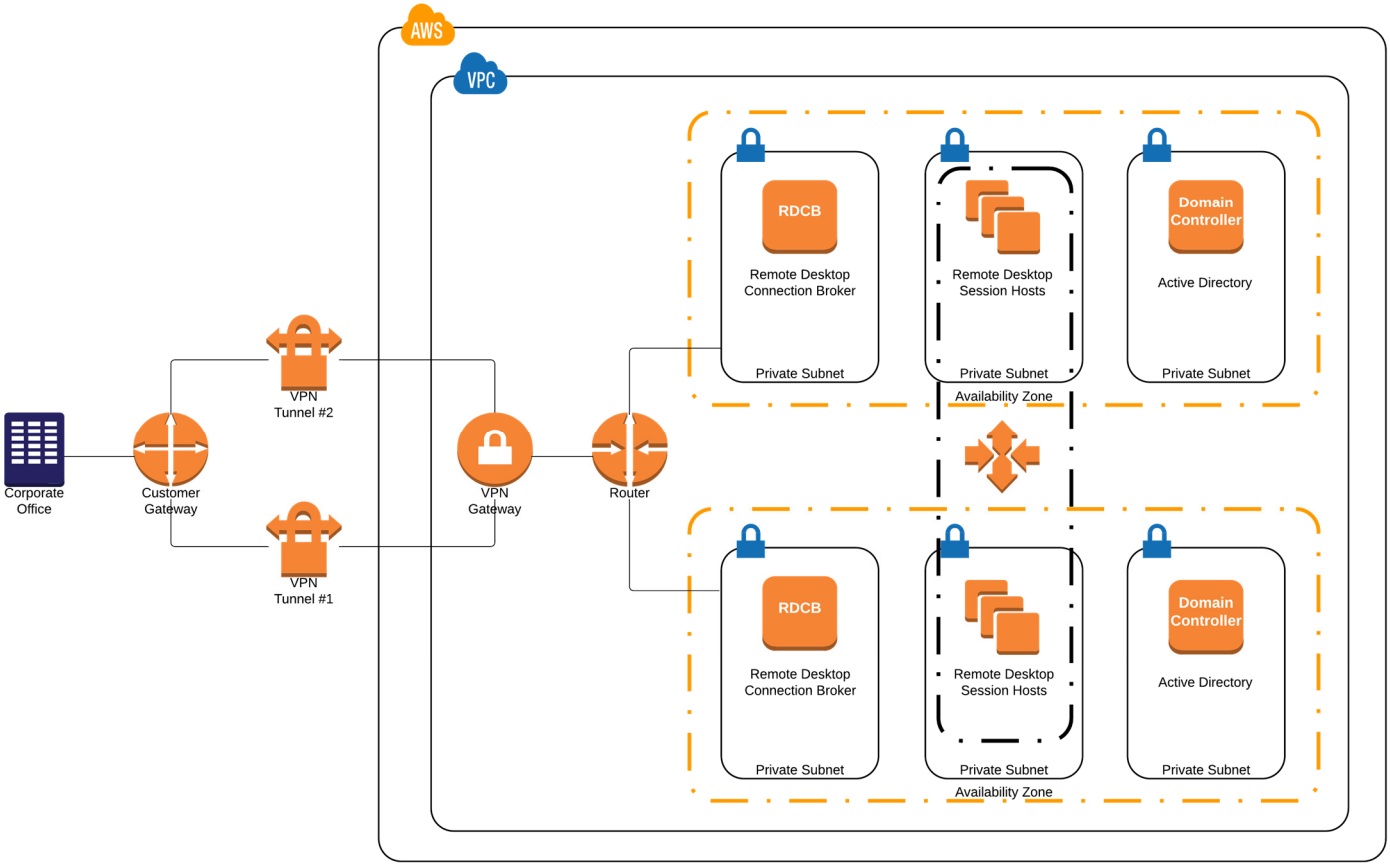


A Remote Desktop Gateway (RD Gateway) server is a type of gateway that enables authorized users to connect to remote computers on a corporate network from any computer that has an Internet connection. RD Gateway uses the Remote Desktop Protocol (RDP) along with the HTTPS protocol to help create a more secure, encrypted connection.

REMOTE DESKTOP SESSION HOST

The Remote Desktop Session Host (RDSH) is the machine onto which user applications are installed and published as RemoteApp programs, or on which full Remote Desktops are published. It is common to deploy multiple RDSH machines in groups called "farms". Users are load-balanced across Session Hosts in the farm by the Connection Broker.

Solution Description



In this scenario the RemoteApp infrastructure is being hosted in the AWS cloud, but all connectivity to and from the AWS cloud is routed over a site-to-site VPN connection.

VIRTUAL PRIVATE CLOUD

The foundation of any AWS deployment should always be Amazon Virtual Private Cloud (Amazon VPC), and this is, in fact, the default when new AWS accounts are created. Within the Amazon VPC, six private subnets are deployed. Different parts of the deployment will reside across those six subnets. Deploying the application's logical components across multiple subnets increases flexibility and provides a number of options from a security point of view.

Access to the subnets is controlled with Network Access Control lists (NACLs). Within the subnets, access to individual servers is controlled with security groups. Within the Amazon VPC, subnets are considered either public or private. The differentiator between the two is whether or not the routing table the subnet is associated with has an Internet Gateway as the default route. Private subnets only have access to the Internet via a Network Address Translation (NAT) instance. In this scenario, all the subnets are private.

CONNECTIVITY VIA VPN GATEWAY

Connectivity from the corporate office and the Amazon VPC is established via a VPN gateway. The VPN gateway is a highly available (HA) service offered by AWS. To take advantage of the HA nature of the VPN gateway, two tunnels are established on the corporate office side even if there is only a single VPN device. If a failure occurs on the AWS side, traffic can route over the second tunnel.

HIGH AVAILABILITY

To achieve high-availability for a RemoteApp deployment two Availability Zones (AZs) are leveraged. The AZs are physically separate data centers within a region, located on different flood plains and power grids. In the event of a partial or full AZ failure, the application will continue to run in the remaining AZ.

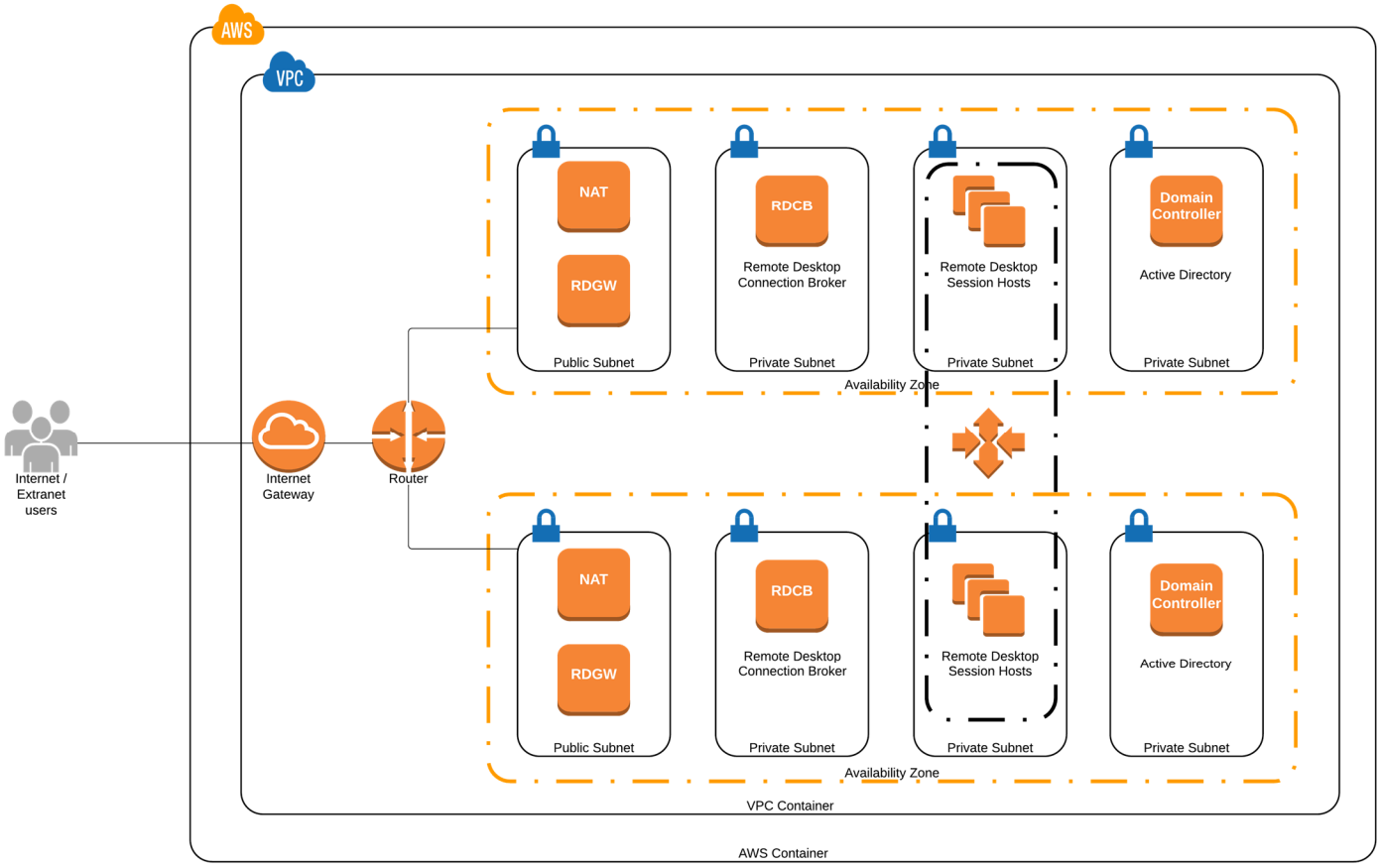
The Windows network is governed by Active Directory. In this deployment, we have a Domain Controller in each AZ to cover both high availability of AD services and application performance.

AUTO-SCALING BASED ON LOAD

The Remote Desktop Session hosts are machines that run the applications that have been published as RemoteApp programs. This tier of the application can be configured to auto-scale based on load. For Active Directory to be aware of new instances as the auto scaling group scales out, Amazon Elastic Compute Cloud (Amazon EC2) “user-data” is used to run Microsoft Windows PowerShell scripts to automatically join the new machines to the domain, and to place them in the correct groups in Active Directory. When an auto-scaled instance is no longer needed and the auto-scaling group scales back, the instance can be configured to remove itself from Active Directory as part of the shutdown sequence. This is an important step; otherwise, Active Directory will be populated with out-of-date information about machines that no longer exist.

USER SESSION MANAGEMENT

The Remote Desktop Connection Broker will manage user sessions. When a user starts a new session, the Connection Broker will direct traffic to the least busy Session Host. Once that user session has been created, the user is associated with that Session host for the duration of the session, even if the user disconnects, and then reconnects at a later time. The Connection Broker will maintain an inventory of sessions, and reconnect the user to their existing session.



This second deployment pattern is similar in many respects to the previous example. The significant difference is that now the RemoteApp deployment is exposed to public networks.

ACTIVE DIRECTORY DOMAIN CONTROLLERS

In this scenario there are two approaches to deploying Active Directory Domain Controllers.

- Deploy a new Active Directory Domain that is completely isolated from the rest of the corporate network (as depicted in the previous diagram).
- Deploy Domain Controllers as Read-Only Domain Controllers that replicate from Domain Controllers in another isolated Amazon VPC or on-premises data center.

CONNECTION VIA REMOTE DESKTOP GATEWAY

In addition to the Active Directory Domain Controller considerations, this is also now a new tier in the deployment. All connections to the environment are made through the Remote Desktop Gateway (RDGW) server located in the public subnets. The RDGW forwards traffic to the Session Broker(s) which in turn forward traffic to the Session Hosts. The RDGW communicates with external clients over SSL encrypted connections. Internally communications are done over TCP port 5504.

Network Address Translation

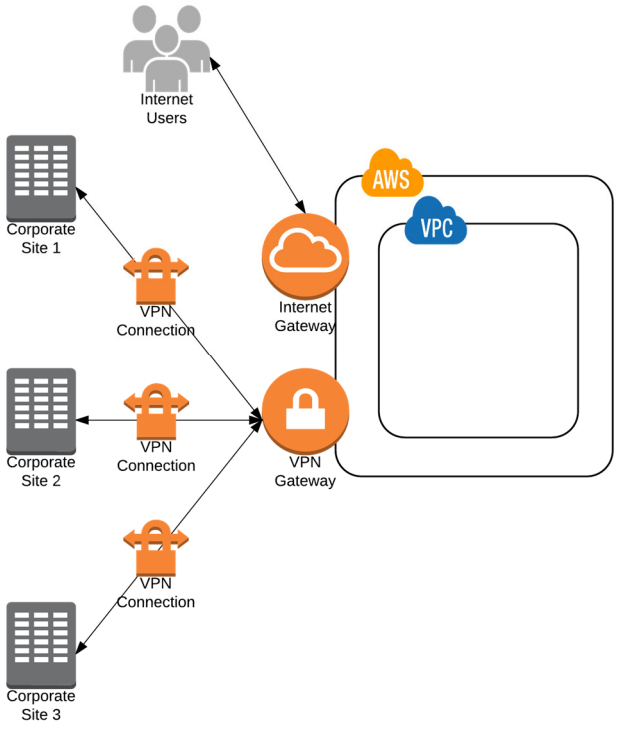
In this public facing scenario Network Address Translation (NAT) instances are introduced into the public subnets. The NAT instance is usually a single-purpose machine tasked with masquerading outbound IP traffic from the private subnets to the Internet. AWS make Amazon Machine Images (AMIs) available for the NAT instance, thus simplifying the task of deploying the NAT instance. Since the only task the NAT instance has is to forward IP traffic, the instance size is usually dictated by the anticipated network throughput rather than by CPU or memory requirements. In many cases, this means that relatively small and inexpensive machines can be deployed. In this deployment, the RemoteApp traffic does not traverse the NAT instance.

Additional Architectural Considerations

More complex network environments

The two reference architectures described in this paper are relatively simple, single-purpose network designs, and do not reflect the usual complexities that are associated with production network infrastructures. There may be more than a single corporate site to be connected to the Amazon VPC. Alternatively, there may be a hybrid of corporate sites and public sites where both corporate users and external clients or business partners access the RemoteApp infrastructure. The following illustration shows the potential complexities that could be encountered.

In the event that clients are spread across the globe, Amazon Route 53 can be leveraged to improve application responsiveness by routing clients to the nearest region in which the application has been deployed.



High Availability and Disaster Recovery

Two important issues that have not been addressed in the reference architectures is high availability and disaster recovery. The AWS infrastructure offers the tools to build highly available applications and services. It is critical that applications are spread across at least two Availability Zones. High availability can be further solidified by deploying the infrastructure and applications across disparate AWS regions. Amazon Route 53, the AWS DNS service, can be leveraged to facilitate this. As part of a more comprehensive disaster recovery plan, data and machine images can be copied across multiple regions.

CONCLUSION

Businesses are increasingly realizing the value of deploying and managing RemoteApp programs and Remote Desktops. As user and customer bases grow, and applications become more complex to maintain and deploy, Microsoft Remote Desktop Services offers a solid solution to the challenges. To be able to have a successful deployment, business need a highly available infrastructure that can dynamically expand and contract in response to user load. AWS provides a secure, robust, and scalable platform on which to build Remote Desktop Services.

Further Reading

Overview of CorpInfo
http://corpinfo.com

Overview of RemoteApp
http://technet.microsoft.com/en-us/library/cc755055.aspx

Active Directory Domain Services
http://technet.microsoft.com/en-us/library/dd448614.aspx

AWS VPC
http://aws.amazon.com/vpc/

AWS EC2
http://aws.amazon.com/ec2/