AWS Enterprise Accelerator

Microsoft Servers on the AWS Cloud

Quick Start Reference Deployment

Bill Jacobi and Santiago Cardenas
Solutions Architects, Amazon Web Services

June 2016

This guide is also available in HTML format at
http://docs.aws.amazon.com/quickstart/latest/accelerator-msservers/.

Contents

About This Guide

This Quick Start reference deployment guide discusses architectural considerations and configuration steps for deploying Microsoft business productivity servers (SharePoint Server, SQL Server, Exchange Server, and Lync Server) on the Amazon Web Services (AWS) cloud. It also provides links for viewing and launching an AWS CloudFormation template that automates the deployment.

The guide is for IT infrastructure architects, administrators, and DevOps professionals who are planning to implement or extend their Microsoft workloads on the AWS cloud.

Quick Starts are automated reference deployments for key enterprise workloads on the AWS cloud. Each Quick Start launches, configures, and runs the AWS compute, network, storage, and other services required to deploy a specific workload on AWS, using AWS best practices for security and availability.

This Quick Start is part of a set of AWS Enterprise Accelerator offerings, which help enterprise customers rapidly develop key capabilities for cloud projects.

Quick Links

The links in this section are for your convenience. Before you launch the Quick Start, please review the architecture, configuration, and other considerations discussed in this guide.

- If you have an AWS account, and you're already familiar with AWS services and Microsoft business productivity servers, you can launch the Quick Start to build the architecture shown in Figure 1 in a new Amazon Virtual Private Cloud (Amazon VPC). The deployment takes 3-4 hours. If you're new to AWS or to this Quick Start, please review the implementation details and follow the step-by-step instructions provided later in this guide.

Launch Quick Start

- If you want to take a look under the covers, you can view the AWS CloudFormation template that automates the deployment.

View template

Overview

This guide provides infrastructure and configuration information for planning and deploying Microsoft Windows workloads on the AWS cloud, with a focus on desktop as a service (DaaS) implementations. It builds the AWS infrastructure and deploys Microsoft business productivity servers such as SharePoint Server, SQL Server, Exchange Server, and Lync Server, to provide a DaaS solution for enterprise customers.

Advantages of Running Microsoft Servers on AWS

The AWS cloud provides a suite of infrastructure services that enable you to deploy Microsoft workloads in a highly available, fault-tolerant, and affordable way. By deploying Microsoft business productivity servers on the AWS cloud, you can take advantage of the email, collaboration, communications, and directory features provided by these servers along with the flexibility and security of AWS. Here are some of the advantages of running Microsoft servers on AWS:

- **Add-on compatibility**. Since AWS provides an infrastructure as a service (IaaS) platform, custom-developed and partner add-ons that run on premises are generally

compatible with the Microsoft servers deployed on AWS. This enables AWS to be a platform that replaces on-premises deployments without losing add-ons and customizations.

- **Scalability**. On AWS, it is easy to monitor a Microsoft deployment and scale horizontally or vertically as workload demands require.
- **Agility**. On AWS, vertical and horizontal scalability can take place in minutes rather than the time frame of typical corporate procurements and bare-metal deployments. AWS provides several DevOps tools and features that support rapid agility and make it easy to experiment.
- **Cost**. With AWS, you pay only for what you use, and you can turn down resources elastically according to demand or schedules to reduce costs. And you can generally bring your existing software licenses to the cloud without having to purchase new software licenses.
- **Optimization**. With AWS, you can easily increase or decrease individual resources that affect the user experience. IT can choose among several options to increase the performance of existing deployments, including choosing faster storage, more processors, faster processors, or greater network throughput, instead of purchasing new servers.
- **Reliability**. With DevOps tools on AWS, you can automate the build and deployment of Microsoft n-tier applications with version-controlled SharePoint Server farms, Exchange Server deployments, etc., and manage Microsoft server infrastructure as code.
- **High availability**. Microsoft SQL Server AlwaysOn Availability Groups enable you to distribute databases across multiple server instances and storage volumes, but it's usually complex and costly to ensure that those instances are placed in separate facilities with separate power grids, flood plains, and Internet backbones. AWS Availability Zones make it easy to achieve this.

This guide requires basic familiarity with the architecture and management of Microsoft servers. For more information about Microsoft products, including general guidance and best practices, consult the Microsoft product documentation.

DaaS Core Services and Proposed Solutions

The following table shows the alignment between DaaS core services and the Windows-based solutions that can run on AWS.

DaaS core service	Proposed solution
Email	Microsoft Exchange Server 2013
Collaboration	Microsoft SharePoint Server 2016
Unified communications	Microsoft Lync Server 2013
Office automation	Microsoft Office*
Virtual desktop	Amazon WorkSpaces*
Directory	Microsoft Active Directory
Monitoring and automation	Amazon CloudWatch Logs Amazon Virtual Private Cloud (Amazon VPC) Flow Logs AWS Config AWS CloudTrail AWS CloudFormation Microsoft Systems Center suite

* Amazon Workspaces includes both the Windows client and Microsoft Office products, but it is not included in this release of the Quick Start.

The following table shows the AWS cloud services that will be required to support DaaS workloads.

Category	AWS cloud service
Compute	Amazon Elastic Compute Cloud (Amazon EC2)
Networks, subnets, gateways, virtual private networks (VPNs)	Amazon Virtual Private Cloud (Amazon VPC)
Dedicated private network	AWS Direct Connect
Instance and subnet firewalls	Security groups and network access control lists (ACLs)
Volume storage	Amazon Elastic Block Store (Amazon EBS)
Snapshot (backup) storage	Amazon Simple Storage Service (Amazon S3)
Template-based resource creation and automation	AWS CloudFormation
Resource and custom monitoring	Amazon CloudWatch
User and access control	AWS Identity and Access Management (IAM)
Internal app store	AWS Service Catalog

For detailed information about these services, see the AWS Services section.

Templates Included with This Quick Start

AWS CloudFormation is an automated DevOps deployment service for building out *n*-tier applications and infrastructure from templates. These templates provision AWS resources such as networks, subnets, routing, firewalls, virtual machine instances, and gateways, and support the inclusion of Windows PowerShell scripting to install and configure the Microsoft servers into the AWS infrastructure.

This Quick Start consists of a main template, which integrates the deployment of five nested templates. Each nested template deploys a Microsoft server solution on AWS according to AWS best practices. The following table describes each template and its dependencies.

Template	Description	Dependencies
Main template	Primary template file that deploys the five nested templates for Microsoft server solutions.	The nested templates listed below
Active Directory Domain Services	Deploys Active Directory Domain Services (AD DS) and Domain Name Server (DNS) on AWS to provide directory services for the Microsoft server solutions automated by this Quick Start. For more information about this template and the environment it builds, see the AD DS Quick Start deployment guide.	None
SQL Server 2012 and 2014 with Windows Server Failover Clustering (WSFC)	Deploys SQL Server 2012 or 2014 instances configured in a Windows Server Failover Cluster (WSFC). For more information about this template and the environment it builds, see the SQL Server Quick Start deployment guide.	AD DS
Lync Server 2013	Implements a Lync Server environment with paired Lync Server 2013 Standard Edition pools across two Availability Zones. For more information about this template and the environment it builds, see the Lync Server Quick Start deployment guide.	AD DS
Exchange Server 2013	Deploys a small Exchange Server 2013 environment that supports 250 mailboxes. For more information about this template and the environment it builds, see the Exchange Server Quick Start deployment guide.	AD DS
SharePoint Server 2016	Deploys a SharePoint Server 2016 farm based on a traditional or streamlined topology. For more information about this template and the environment it builds, see the SharePoint Server Quick Start deployment guide.	AD DS, SQL Server

> **Note** This Quick Start does not include Windows PowerShell DSC. For more information about deploying this configuration platform on AWS, see the PowerShell DSC on AWS Quick Start.

To deploy the AWS infrastructure and the Microsoft server solutions listed in the table, use the main template when launching the stacks. You can also edit the main template to customize stacks or to omit stacks to be deployed, or deploy each stack independently.

Cost and Licenses

You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using the Quick Start itself.

The AWS CloudFormation templates provided with the Quick Start include configuration parameters that you can customize, and some settings, such as the instance types and the number of instances, can greatly affect the cost of the deployment.

The Quick Start launches the Amazon Machine Image (AMI) for Windows Server 2012 R2 and includes the license for the Windows Server 2012 R2 operating system.

By default, this Quick Start installs the free trial versions of the Microsoft business productivity servers. To use these servers beyond the trial period, you must obtain licenses from Microsoft. For production environments, you can license Microsoft server products through the Microsoft License Mobility through Software Assurance program, and provide your own product key after deployment. For development and test environments, you can leverage your existing MSDN licenses using Amazon EC2 Dedicated Hosts or Dedicated Instances. For details, see the MSDN on AWS page.

AWS Services

The core AWS components used by this Quick Start include the following AWS services. (If you are new to AWS, see the Getting Started section of the AWS documentation.)

- AWS CloudFormation – AWS CloudFormation gives you an easy way to create and manage a collection of related AWS resources, and provision and update them in an orderly and predictable way. You use a template to describe all the AWS resources (e.g., Amazon EC2 instances) that you want. You don't have to individually create and configure the resources or figure out dependencies—AWS CloudFormation handles all of that.

- Amazon VPC – The Amazon Virtual Private Cloud (Amazon VPC) service lets you provision a private, isolated section of the AWS cloud where you can launch AWS services and other resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.
- Amazon EC2 – The Amazon Elastic Compute Cloud (Amazon EC2) service enables you to launch virtual machine instances with a variety of operating systems. You can choose from existing Amazon Machine Images (AMIs) or import your own virtual machine images.
- NAT Gateway – NAT Gateway is an AWS managed service that controls NAT gateway resources. A NAT gateway is a type of network address translation (NAT) device that enables instances in a private subnet to connect to the Internet or to other AWS services, but prevents the Internet from connecting to those instances.
- IAM – AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. With IAM, you can manage users, security credentials such as access keys, and permissions that control which AWS resources users can access, from a central location.
- Amazon EBS – Amazon Elastic Block Store (Amazon EBS) provides persistent block level storage volumes for use with Amazon EC2 instances on the AWS cloud. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability. Amazon EBS volumes provide the consistent and low-latency performance needed to run your workloads.
- Amazon S3 – Amazon Simple Storage Service (Amazon S3) provides secure, durable, highly scalable cloud storage. You can use Amazon S3 to store and retrieve any amount of data at any time, from anywhere on the web.

Architecture

Figure 1 represents the Quick Start architecture of Windows servers on AWS. The most notable aspect of this architecture is that through Amazon VPC the architecture reflects the same architectural patterns and practices that Microsoft recommends for on-premises implementations. This is not surprising, because Microsoft provides the same architectural recommendations for on-premises and virtualized environments.

Note Microsoft does make allowances in its server calculators for physical vs. virtual environments, but these don't change the basic architectures as much as reflecting virtualization overhead. All the reference architectures automated by this Quick Start adhere to Microsoft TechNet guidelines and meet minimum resource requirements. The Quick Start implementations are reference implementations, and actual sizing will require performance and acceptance testing.

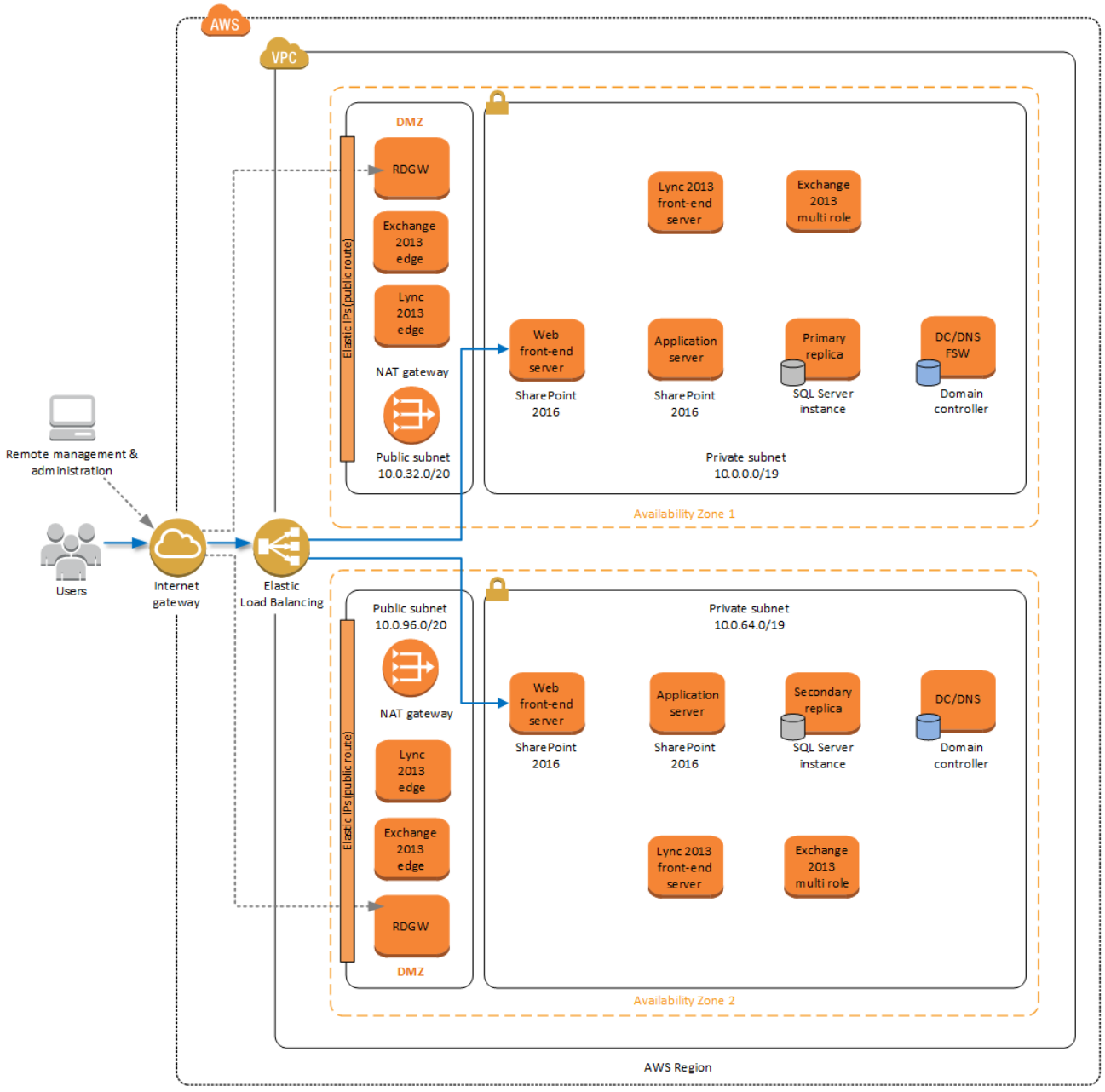

Figure 1: Quick Start architecture for Microsoft servers on AWS

The Quick Start environment combines the resources that are deployed as part of the AD DS, SQL Server, SharePoint Server, Exchange Server, and Lync Server Quick Starts. All of these Quick Starts provide a highly available Multi-AZ architecture.

- The AD DS Quick Start deploys the domain controllers and Remote Desktop Gateway bastion hosts.
- The SQL Server Quick Start deploys two SQL Server instances in a failover cluster using the file share witness.
- The SharePoint Server Quick Start deploys two web front-end servers and two application servers by selecting the traditional topology.
- The Exchange Server Quick Start deploys two multi-role servers with mailbox and client access server (CAS) roles. It can optionally also deploy two edge transport servers.
- The Lync Server Quick Start deploys two front-end servers. It can optionally also deploy two edge servers.

The following sections provide more information about these server components of the Quick Start architecture. For a detailed discussion of best practices for networking and remote administration, Windows architectural considerations on AWS, and managing and monitoring Windows instances and applications, see Appendix B.

Active Directory Domain Services

Active Directory Domain Services (AD DS) and Domain Name Server (DNS) are core Windows services that provide the foundation for many enterprise-class Microsoft-based solutions, including the Microsoft business productivity servers deployed by this Quick Start.

This Quick Start provides a new installation of AD DS in the AWS cloud, which is discussed in detail in the Quick Start deployment guide for AD DS (scenario 1).

SQL Server 2014

SQL Server hosts the SharePoint Server configuration database and the content store, and is required for SharePoint Server 2016. In an enterprise setting, SQL Server is used for high availability of the content in a SharePoint Server farm. SQL Server uses AlwaysOn Availability Groups layered over Windows Server Failover Clustering (WSFC) to provide redundant databases along with a witness server to ensure that a quorum can vote for the node to be promoted to master. In AWS, the architecture (shown in Figure 2) mirrors an

on-premises architecture of two SQL Server instances spanning two subnets placed in two different Availability Zones.

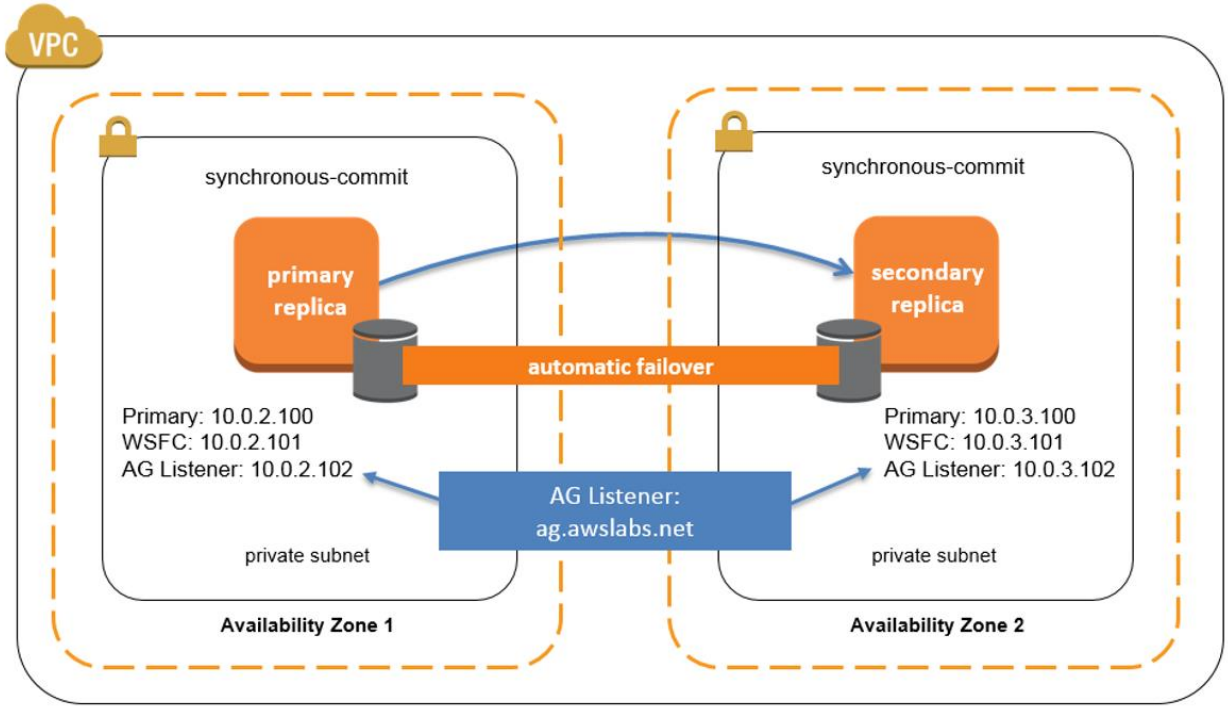

Figure 2: SQL Server AlwaysOn Availability Group supports automatic failover

For detailed information about the SQL Server and WSFC components of this Quick Start deployment, see the Quick Start deployment guide for SQL Server with WSFC.

SharePoint Server 2016

There are a number of ways to design the topology of a SharePoint Server farm depending on your requirements. Microsoft provides guidance for two separate architectural approaches for SharePoint Server 2016: traditional topology and streamlined topology. The AWS CloudFormation template provided by this guide is built with flexibility in mind, and lets you choose either topology for your SharePoint Server farm.

By default, the template builds the highly available SharePoint Server farm illustrated in Figure 3. This is based on the traditional topology, which includes web servers, application servers, and database servers.

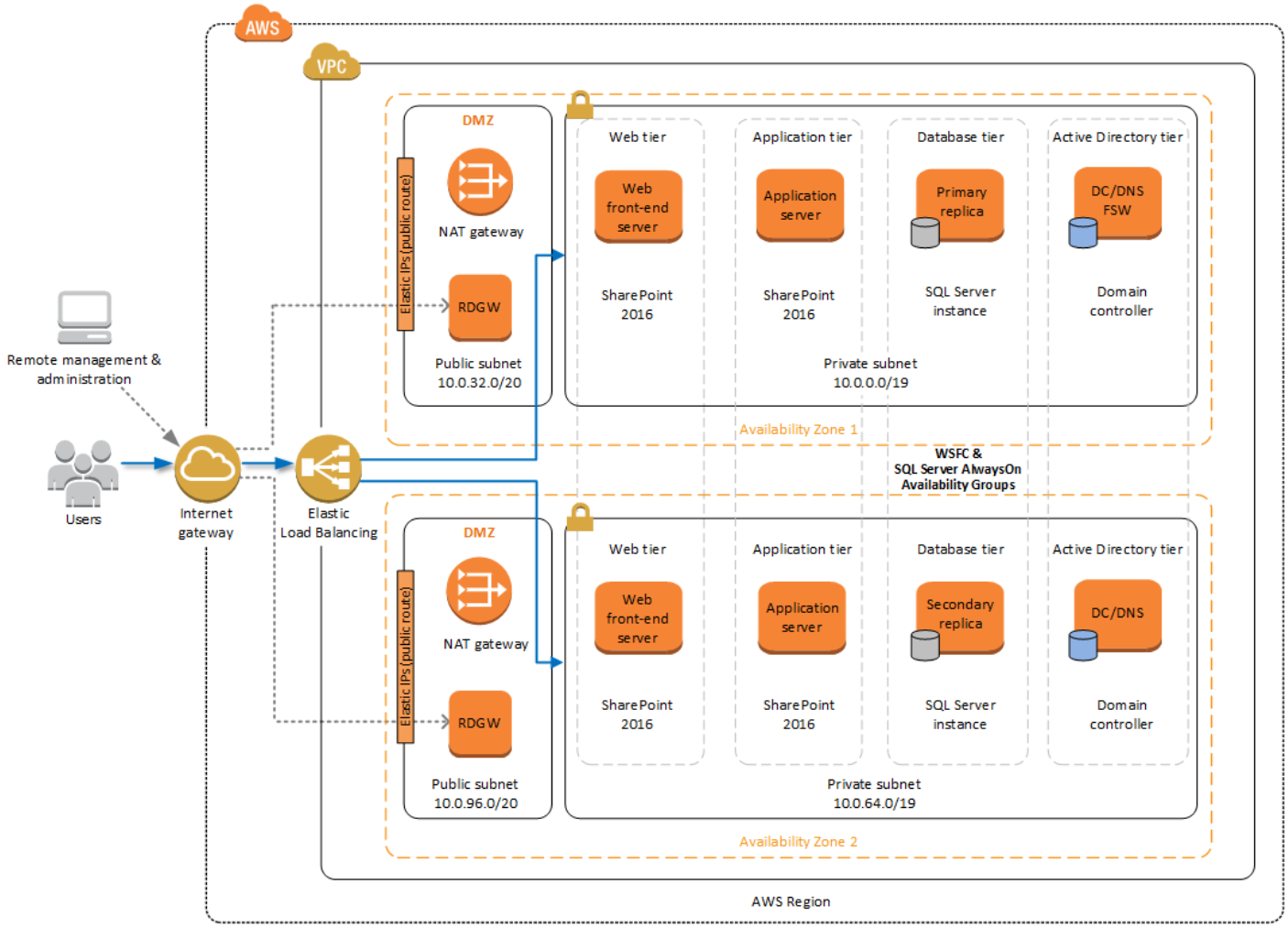

Figure 3: Default Quick Start architecture for SharePoint farm (traditional topology)

For more information about traditional and streamlined topologies and other details for the SharePoint Server part of this Quick Start deployment, see the Quick Start for SharePoint Server 2016.

Exchange Server 2013

In the Quick Start architecture for Exchange Server 2013, critical workloads such as Exchange Server instances and Exchange edge transport servers are placed in two or more Availability Zones. The Remote Desktop Gateway instances remain in the management subnet. Similar to the SQL Server AlwaysOn architecture, Exchange Server employs a Database Availability Group (DAG) architecture that is built into the mailbox role. These roles are deployed across two Availability Zones to increase availability.

This Quick Start builds the minimal amount of infrastructure to provide Exchange Server high availability for 250 mailboxes. In addition to providing the minimal amount of infrastructure for high availability, you might want to consider the Microsoft Preferred Architecture for Exchange Server 2013 (Exchange PA). Although the Exchange PA calls for running Exchange on dedicated physical servers, it also includes many design aspects that can be beneficial in any environment. For details on Exchange PA and guidelines for designing for performance and high availability, see the Quick Start deployment guide for Exchange Server.

Lync Server 2013

Lync Server employs a highly available architecture for the Lync front-end role. These roles are deployed across two Availability Zones to increase availability.

The default configuration deploys two Lync Server Standard Edition pools across two Availability Zones to support disaster recovery and pool failover. You can home 50% of the users on the first pool and home the remaining 50% of the users on the second pool. This will provide an active-active type of deployment, where servers in both Availability Zones are servicing users. In the event of a disaster, the pool can fail over to the other Availability Zone.

You can also customize the template to optionally deploy Lync edge servers. For additional information about the Lync Server deployment and customization instructions, see the Quick Start deployment guide for Lync Server.

Deployment Steps

The AWS CloudFormation template provided with this Quick Start bootstraps the AWS infrastructure and automates the deployment of Microsoft servers on the AWS cloud. Follow the step-by-step instructions in this section to set up your AWS account, customize the template, and deploy the software into your account.

The deployment procedure consists of the following steps. For detailed instructions, follow the links for each step.

Step 1. Prepare an AWS account

- Sign up for an AWS account, if you don't already have one.
- Choose the region where you want to deploy the stack on AWS.
- Create a key pair in the region.

- Review account limits for Amazon EC2 instances, and request a limit increase, if needed.

[Step 2. Launch the Quick Start]

- Launch the AWS CloudFormation template into your AWS account.
- Enter values for required parameters.
- Review the other template parameters, and customize their values if necessary.

[Step 3. Post-deployment tasks]

- Add users to Active Directory.
- Enable those users for Exchange in Exchange Administration Center.
- Enable those users for Lync in Lync Server Control Panel.
- Test for high availability and automatic failover, and set up one or two enterprise templates in SharePoint.

Step 1. Prepare an AWS Account

1. If you don't already have an AWS account, create one at http://aws.amazon.com by following the on-screen instructions. Part of the sign-up process involves receiving a phone call and entering a PIN using the phone keypad.
2. Use the region selector in the navigation bar to choose the AWS Region where you want to deploy Microsoft servers on AWS.

Figure 4: Choosing an AWS Region

Consider choosing a region closest to your data center or corporate network to reduce network latency between systems running on AWS and the systems and users on your corporate network.

> **Important** This Quick Start uses M4, R3, and C3 instances for server deployments, and NAT gateways for outbound Internet access. At the time of this writing, some of these features aren't available in the China (Beijing), South America (São Paulo), or Asia Pacific (Seoul) regions.

3. Create a key pair in your preferred region. To do this, in the navigation pane of the Amazon EC2 console, choose **Key Pairs**, **Create Key Pair**, type a name, and then choose **Create**.

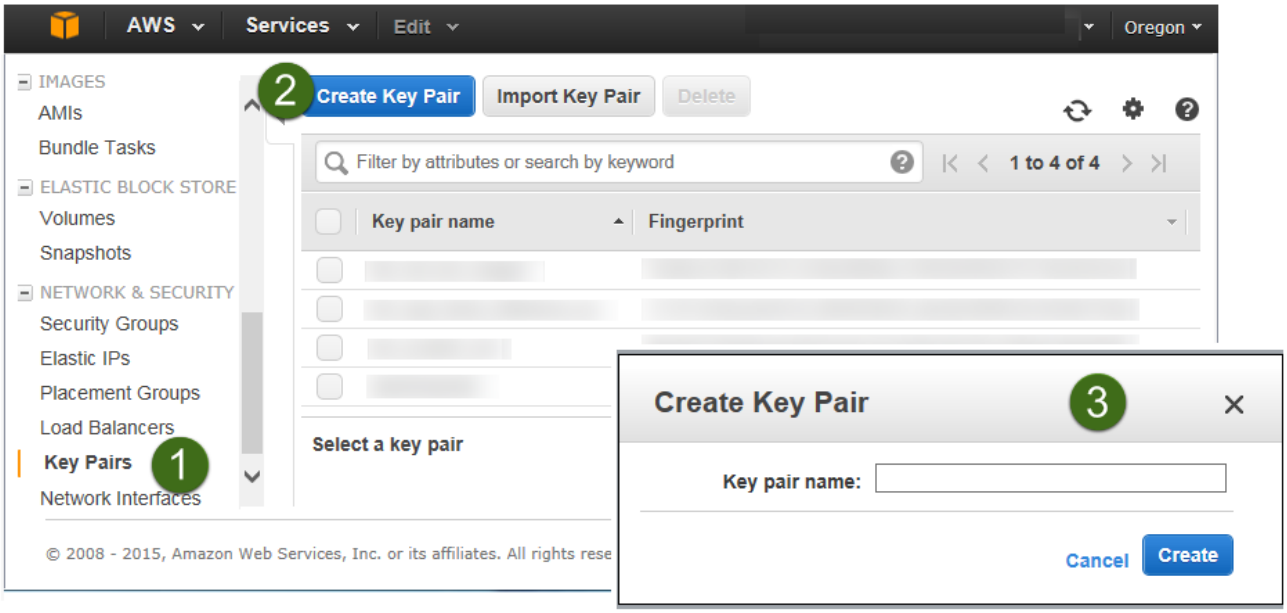

Figure 5: Creating a key pair

Amazon EC2 uses public-key cryptography to encrypt and decrypt login information. To be able to log in to your instances, you must create a key pair. With Windows instances, we use the key pair to obtain the administrator password via the Amazon EC2 console and then log in using Remote Desktop Protocol (RDP), as explained in the step-by-step instructions in the *Amazon Elastic Compute Cloud User Guide*.

4. If necessary, request a service limit increase for the instance types used in the Quick Start. To do this, in the AWS Support Center, choose **Create Case**, **Service Limit Increase**, **EC2 instances**, and then complete the fields in the limit increase form.

You might need to request an increase if you already have an existing deployment that uses these instance types, and you think you might exceed the default limit with this reference deployment. It might take a few days for the new service limit to become effective. For more information, see Amazon EC2 Service Limits in the AWS documentation.

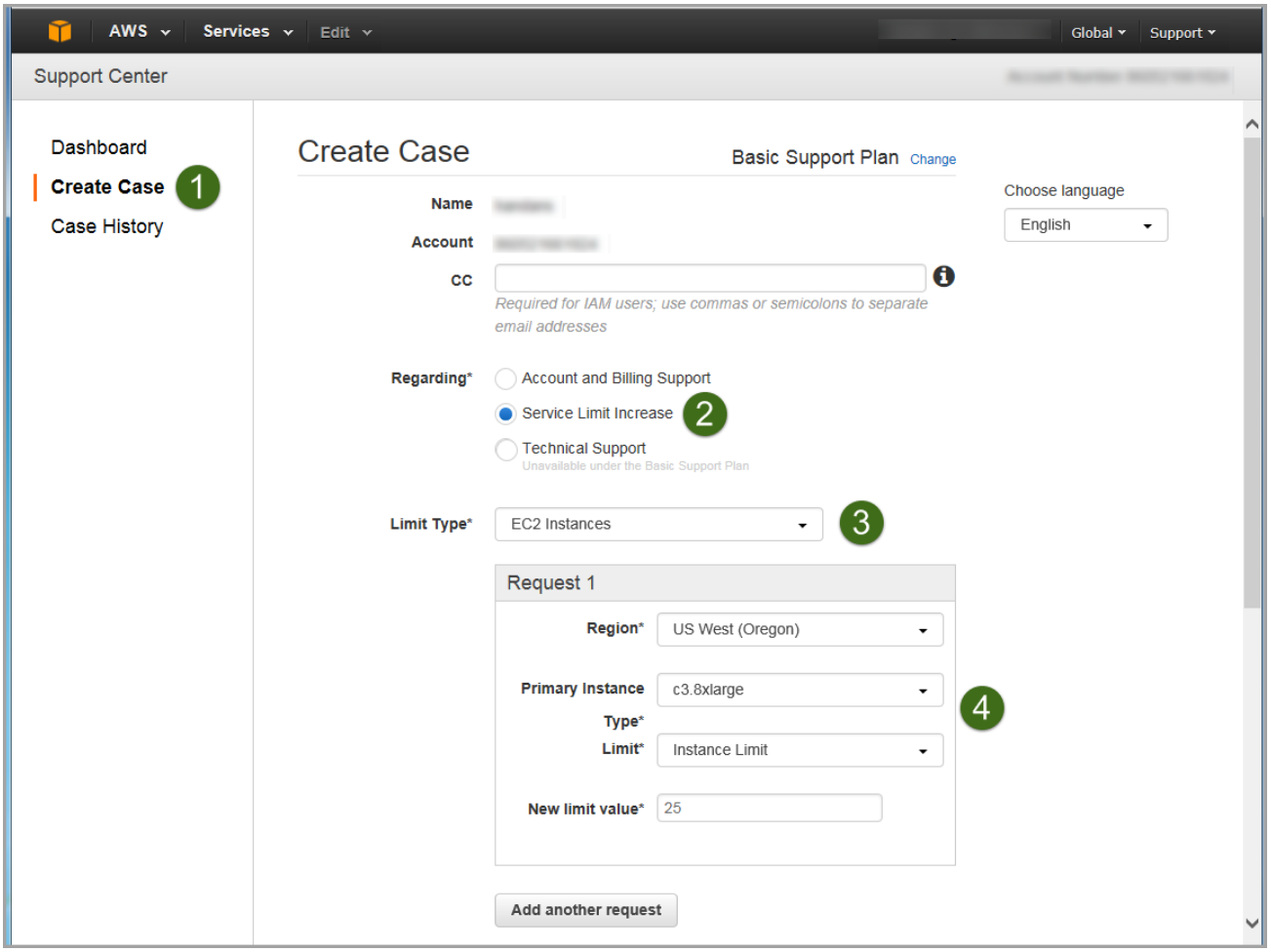

Figure 6: Requesting a service limit increase

Step 2. Launch the Quick Start

1. Launch the AWS CloudFormation template into your AWS account.

   Launch Quick Start

   The template is launched in the US West (Oregon) Region by default. You can change the region by using the region selector in the navigation bar.

   The stack takes 3-4 hours to create.

   > **Note** You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using this Quick Start. See the pricing pages for each AWS service you will be using in this Quick Start and the AWS Simple Monthly Calculator for details.

2. On the **Select Template** page, keep the default setting for the template URL, and then choose **Next**.
3. On the **Specify Details** page, review the parameters for the template. Provide values for the following required parameters.

Parameter	Default	Description
Amazon EC2 Configuration		
Key Pair Name	*Requires input*	Public/private key pair, which allows you to connect securely to your instance after it launches. When you created an AWS account, this is the key pair you created in your preferred region.
Microsoft Active Directory Configuration		
Restore Mode Password	*Requires input*	Password for a separate administrator account when the domain controller is in Restore Mode. This password must meet Microsoft's default password complexity requirements.
Domain Admin Password	*Requires input*	Password for the domain administrator user. This password must meet Microsoft's default password complexity requirements.
Microsoft SQL Server Configuration		
Service Account Password	*Requires input*	Password for the SQL Server service account. This password must meet Microsoft's default password complexity requirements.
Microsoft SharePoint Configuration		
Installation Media ISO Image File URI	*Requires input*	Amazon S3 URI to the S3 bucket that contains the ISO image file for the SharePoint Server 2016 installation media (e.g., s3://sample-bucket/microsoft/sharepoint/installation-

Parameter	Default	Description
		media.img). You can also specify an HTTP/HTTPS URI (e.g., https://example.com/microsoft/sharepoint/installation-media.img), but we recommend using an S3 bucket for optimal performance.
Farm Account Password	*Requires input*	Password for the SharePoint farm account. This password must meet Microsoft's default password complexity requirements.
Microsoft Lync Configuration		
Installation Media ISO Image File URI	*Requires input*	Amazon S3 URI to the S3 bucket that contains the ISO image file for the Lync Server 2013 Standard Edition installation media (e.g., s3://sample-bucket/microsoft/lync/installation-media.iso). You can also specify an HTTP/HTTPS URI (e.g., https://example.com/microsoft/lync/installation-media.iso), but we recommend using an S3 bucket for optimal performance.

For all other parameters, review the default settings and customize them as necessary. (See Appendix A for a complete parameter list.)

When you finish reviewing and customizing the parameters, choose **Next**.

> **Note** You can also download the template and edit it to create your own parameters based on your specific deployment scenario.

4. On the **Options** page, you can specify tags (key-value pairs) for resources in your stack and set advanced options. When you're done, choose **Next**.
5. On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the check box to acknowledge that the template will create IAM resources.
6. Choose **Create** to deploy the stack.
7. Monitor the status of the stack. When the status is **CREATE_COMPLETE**, the Microsoft server cluster is ready.

Step 3. Post-Deployment Tasks

After the Quick Start deployment is complete, you can test the Microsoft productivity servers on AWS and create users and content:

1. Add users to Active Directory. Use **Active Directory Users and Computers** or PowerShell to create users with domain user permissions in Active Directory. We recommend that you include most of the standard fields, such as first name, last name, user principal name, and email.

2. Enable those users for Exchange in **Exchange Administration Center**, by following the instructions in the Microsoft documentation for Exchange Server. See the Quick Start deployment guide for Exchange Server for some useful post-configuration links.
3. Enable those users for Lync in **Lync Server Control Panel** or PowerShell. For instructions, see step 3 in the Quick Start deployment guide for Lync Server.
4. Test for high availability and automatic failover of your SharePoint servers by following the steps in the Quick Start deployment guide for SharePoint, and then set up one or two enterprise templates in SharePoint. For instructions, see the Microsoft documentation for SharePoint Server.

Troubleshooting

When you deploy the Quick Start, if you encounter a CREATE_FAILED error instead of the CREATE_COMPLETE status code, we recommend that you re-launch the template with **Rollback on failure** set to **No**. (This setting is under **Advanced** in the AWS CloudFormation console, **Options** page.) With this setting, the stack's state will be retained and the instance will be left running, so you can troubleshoot the issue.

> **Important** When you set **Rollback on failure** to **No**, you'll continue to incur AWS charges for this stack. Please make sure to delete the stack when you've finished troubleshooting.

The following table lists specific CREATE_FAILED error messages you might encounter.

Error message	Possible cause	What to do
API: ec2: RunInstances Not authorized for images: *ami-ID*	The template is referencing an AMI that has expired.	We refresh AMIs on a regular basis, but our updates sometimes lag behind AWS AMI changes. If you get this error message, notify us, and we'll update the template with the new AMI ID. If you'd like to fix the template yourself, you can download it and update the `Mappings` section with the latest AMI ID for your region.
We currently do not have sufficient *instance-type* capacity in the AZ you requested	One of the instance types is currently not available.	Switch to an instance type that supports higher capacity, or complete the request form in the AWS Support Center to increase the Amazon EC2 limit for the instance type or region. Limit increases are tied to the region they were requested for.
Instance *ID* did not stabilize	You have exceeded your IOPS for the region.	Request a limit increase by completing the request form in the AWS Support Center.

Error message	Possible cause	What to do
System Administrator password must contain at least 8 characters	The master password contains $ or other special characters.	Check the password parameters before you re-launch the Quick Start. The passwords must be at least 8 characters, consisting of uppercase and lowercase letters and numbers. Follow the guidelines for complex passwords, and avoid using special characters such as @ or $.

If failure is signaled or a wait condition or resource signal times out, remote into the affected machine and launch Event Viewer. Under **Custom Views**, **Administrative Events** or under **Windows Logs**, **Application**, look for errors of source **AWSQuickStart**. These will indicate the failing script, line number, and exception that was reported.

For more information, see Troubleshooting AWS CloudFormation on the AWS website.

Additional Resources

AWS services

- AWS CloudFormation
  http://aws.amazon.com/documentation/cloudformation/
- Amazon EBS
  http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html
  - Volume types:
    http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html
  - Optimized instances:
    http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSOptimized.html
- Amazon EC2
  http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/
- Amazon VPC
  http://aws.amazon.com/documentation/vpc/

Deploying Microsoft software on AWS

- Microsoft on AWS
  http://aws.amazon.com/microsoft/
- Secure Microsoft applications on AWS
  http://media.amazonwebservices.com/AWS_Microsoft_Platform_Security.pdf

- Microsoft Licensing Mobility
  http://aws.amazon.com/windows/mslicensemobility/
- MSDN on AWS
  http://aws.amazon.com/windows/msdn/
- AWS Windows and .NET Developer Center
  http://aws.amazon.com/net/

Active Directory Domain Services

- Active Directory Domain Services documentation
  https://technet.microsoft.com/en-us/library/dd448614.aspx
- Active Directory Sites and Services
  https://technet.microsoft.com/en-us/library/cc730868.aspx

Microsoft SQL Server and SharePoint Server

- Configure SQL Server 2012 AlwaysOn Availability Groups for SharePoint 2013
  https://technet.microsoft.com/en-us/library/jj715261.aspx
- Availability Group Listeners, Client Connectivity, and Application Failover (SQL Server)
  https://msdn.microsoft.com/en-us/library/hh213417(v=sql.120).aspx

Microsoft Exchange Server 2013

- Microsoft preferred architecture
  http://blogs.technet.com/b/exchange/archive/2014/04/21/the-preferred-architecture.aspx
- Storage configuration options
  http://technet.microsoft.com/en-us/library/ee832792(v=exchg.150).aspx
- Namespace planning
  http://blogs.technet.com/b/exchange/archive/2014/02/28/namespace-planning-in-exchange-2013.aspx
- Database availability groups
  http://technet.microsoft.com/en-us/library/dd979799(v=exchg.150).aspx
- Load balancing
  http://blogs.technet.com/b/exchange/archive/2014/03/05/load-balancing-in-exchange-2013.aspx
- Edge subscriptions
  http://technet.microsoft.com/en-us/library/aa997438(v=exchg.150).aspx

- Backup, restore, and disaster recovery
  http://technet.microsoft.com/en-us/library/dd876874(v=exchg.150).aspx

Microsoft Lync Server 2013

- Getting started with Lync Server 2013
  https://technet.microsoft.com/en-us/library/gg398676(v=ocs.15).aspx
- Planning for Lync Server 2013
  https://technet.microsoft.com/en-us/library/gg398447(v=ocs.15).aspx
- Deployment of Lync Server 2013
  https://technet.microsoft.com/en-us/library/gg398664(v=ocs.15).aspx
- Load balancing requirements for Lync Server 2013
  https://technet.microsoft.com/en-us/library/gg615011(v=ocs.15).aspx
- DNS requirements for Lync Server 2013
  https://technet.microsoft.com/en-us/library/gg398758(v=ocs.15).aspx
- Deploying external user access in Lync Server 2013
  https://technet.microsoft.com/en-us/library/gg398918(v=ocs.15).aspx
- Capacity planning for Lync Server 2013
  https://technet.microsoft.com/en-us/library/gg399017(v=ocs.15).aspx

Quick Start reference deployments

- AWS Quick Start home page
  https://aws.amazon.com/quickstart/
- Microsoft Active Directory on AWS
  http://docs.aws.amazon.com/quickstart/latest/active-directory-ds/
- Microsoft Remote Desktop Gateway on AWS
  http://docs.aws.amazon.com/quickstart/latest/rd-gateway/
- Microsoft SQL Server with WSFC on AWS
  http://docs.aws.amazon.com/quickstart/latest/sql/
- Microsoft Exchange Server on AWS
  http://docs.aws.amazon.com/quickstart/latest/exchange/
- Microsoft SharePoint Server on AWS
  http://docs.aws.amazon.com/quickstart/latest/sharepoint/
- Microsoft Lync Server on AWS
  http://docs.aws.amazon.com/quickstart/latest/lync/

Appendix A: AWS CloudFormation Parameters

The following tables provide a complete list of parameters provided in the AWS CloudFormation template for this Quick Start, listed by category.

Network Configuration parameters:

Parameter	Default	Description
VPC CIDR	10.0.0.0/16	CIDR block for the Amazon VPC.
Private Subnet 1 CIDR	10.0.0.0/19	CIDR block for the Active Directory server tier located in Availability Zone 1.
Private Subnet 2 CIDR	10.0.64.0/19	CIDR block for the Active Directory server tier located in Availability Zone 2.
Public Subnet 1 CIDR	10.0.32.0/20	CIDR block for the public (DMZ) subnet located in Availability Zone 1.
Public Subnet 2 CIDR	10.0.96.0/20	CIDR block for the public (DMZ) subnet located in Availability Zone 2.

Amazon EC2 Configuration parameters:

Parameter	Default	Description
Key Pair Name	*Requires input*	Public/private key pair, which allows you to connect securely to your instance after it launches. When you created an AWS account, this is the key pair you created in your region.
Remote Desktop Gateway Server Instance Type	m4.xlarge	Amazon EC2 instance type for the Remote Desktop Gateway instance.
Domain Controller 1 Instance Type	m4.xlarge	Amazon EC2 instance type for the first Active Directory instance.
Domain Controller 1 NetBIOS Name	DC1	NetBIOS name of the first Active Directory server (up to 15 characters).
Domain Controller 1 Private IP Address	10.0.0.10	Fixed private IP for the first Active Directory server located in Availability Zone 1.
Domain Controller 2 Instance Type	m4.xlarge	Amazon EC2 instance type for the second Active Directory instance.
Domain Controller 2 NetBIOS Name	DC2	NetBIOS name of the second Active Directory server (up to 15 characters).
Domain Controller 2 Private IP Address	10.0.64.10	Fixed private IP for the second Active Directory server located in Availability Zone 2.
Exchange Edge Transport Server Instance Type	m3.large	Amazon EC2 instance type for the Exchange 2013 Edge Transport servers.

Parameter	Default	Description
Exchange Multi Role Server Instance Type	r3.xlarge	Amazon EC2 instance type for the Exchange 2013 multi-role servers.
Exchange Server 1 Private IP Address 1	10.0.0.150	Primary private IP for the first Exchange server located in Availability Zone 1.
Exchange Server 1 Private IP Address 2	10.0.0.151	Secondary private IP for the first Exchange server in Availability Zone 1.
Exchange Server 2 Private IP Address 1	10.0.64.150	Primary private IP for the second Exchange server located in Availability Zone 2.
Exchange Server 2 Private IP Address 2	10.0.64.151	Secondary private IP for the second Exchange server located in Availability Zone 2.
Lync Front End Server Instance Type	m4.2xlarge	Amazon EC2 instance type for the Lync Standard Edition Front End Servers.
Lync Front End Server 1 Private IP Address	10.0.0.160	Primary private IP for the first Lync Front End Server.
Lync Front End Server 2 Private IP Address	10.0.64.160	Primary private IP for the second Lync Front End Server.
Lync Edge Server Instance Type	m4.xlarge	Amazon EC2 instance type for the Lync Edge Servers.
Lync Edge Server 1 Private IP Address	10.0.0.161	Primary private IP for the first Lync Edge Server.
Lync Edge Server 1 Public IP Address	10.0.32.161	Public subnet IP for the first Lync Edge Server.
Lync Edge Server 2 Private IP Address	10.0.64.161	Primary private IP for the second Lync Edge Server.
Lync Edge Server 2 Public IP Address	10.0.96.161	Public subnet IP for the second Lync Edge Server.
WSFC Node 1 Instance Type	r3.2xlarge	Amazon EC2 instance type for the first WSFC node.
WSFC Node 1 NetBIOS Name	WSFCNode1	NetBIOS name of the first WSFC node (up to 15 characters).
WSFC Node 1 Private IP Address 1	10.0.0.100	Primary private IP for the first WSFC node located in Availability Zone 1.
WSFC Node 1 Private IP Address 2	10.0.0.101	Secondary private IP for the WSFC cluster on the first WSFC node.
WSFC Node 1 Private IP Address 3	10.0.0.102	Third private IP for the Availability Group Listener on the first WSFC node.
WSFC Node 2 Instance Type	r3.2xlarge	Amazon EC2 instance type for the second WSFC node.
WSFC Node 2 NetBIOS Name	WSFCNode2	NetBIOS name of the second WSFC node (up to 15 characters).

Parameter	Default	Description
WSFC Node 2 Private IP Address 1	10.0.64.100	Primary private IP for the second WSFC node located in Availability Zone 1.
WSFC Node 2 Private IP Address 2	10.0.64.101	Secondary private IP for the WSFC cluster on the second WSFC node.
WSFC Node 2 Private IP Address 3	10.0.64.102	Third private IP for the Availability Group Listener on the second WSFC node.
SharePoint Server Instance Type	c3.2xlarge	Amazon EC2 instance type for the SharePoint web front-end servers.
Office Online Server Instance Type	m3.xlarge	Amazon EC2 instance type for the Office Online Server instances.
ELB Configuration	external	How to configure the ELB load balancer. Options are external or internal. For more information, see the section on Intranet SharePoint Server farms in the Quick Start deployment guide for SharePoint Server.

Microsoft Active Directory Configuration parameters:

Parameter	Default	Description
Domain DNS Name	example.com	Fully qualified domain name (FQDN) of the forest root domain.
Domain NetBIOS Name	example	The NetBIOS name (up to 15 characters) of the domain, for users of earlier versions of Windows.
Restore Mode Password	*Requires input*	Password for a separate administrator account when the domain controller is in Restore Mode. This password must meet Microsoft's default password complexity requirements.
Domain Admin User Name	StackAdmin	User name for the account that will be added as the domain administrator. This is separate from the default "Administrator" account.
Domain Admin Password	*Requires input*	Password for the domain administrator user. This password must meet Microsoft's default password complexity requirements.

Microsoft SQL Server Configuration parameters:

Parameter	Default	Description
Version	2014	The version of SQL Server to install on WSFC nodes. Supported versions are 2012 and 2014.
Service Account Name	sqlsa	User name for the SQL Server service account. This account is a domain user.
Service Account Password	*Requires input*	Password for the SQL Server service account, which must meet Microsoft's default password complexity requirements.

Microsoft SharePoint Configuration parameters:

Parameter	Default	Description
Installation Media ISO Image File URI	*Requires input*	Amazon S3 URI to bucket that contains the ISO image file for the SharePoint Server 2016 installation media (e.g., s3://sample-bucket/microsoft/sharepoint/installation-media.img). You can also specify an HTTP/HTTPS URI (e.g., https://example.com/microsoft/sharepoint/installation-media.img), but we recommend using an S3 bucket for optimal performance.
Product Key	*trial key*	The trial key for SharePoint Server 2016 is provided by default, but you can replace it with your own product key.
Farm Topology	traditional	The topology for the SharePoint Server farm to be deployed. The two options are traditional and streamlined. For more information, see the section on customizing your topology in the Quick Start deployment guide for SharePoint Server.
Farm Account Name	spfarm	User name for the SharePoint Server farm account.
Farm Account Password	*Requires input*	Password for the SharePoint farm account, which must meet Microsoft's default password complexity requirements.
Include Office Online Servers	false	Set to **true** to include an Office Online Server in each Availability Zone. For more information, see the section on Office Online Servers in the Quick Start deployment guide for SharePoint Server.

Microsoft Lync Configuration parameters:

Parameter	Default	Description
Installation Media ISO Image File URI	*Requires input*	Amazon S3 URI to the S3 bucket that contains the ISO image file for the Lync Server 2013 Standard Edition installation media (e.g., s3://sample-bucket/microsoft/lync/installation-media.iso). You can also specify an HTTP/HTTPS URI (e.g., https://example.com/microsoft/lync/installation-media.iso), but we recommend using an S3 bucket for optimal performance.
Include Lync Edge Servers	false	Set this parameter to **true** to include Lync Edge Servers in the public subnets.

Microsoft Exchange Configuration parameters:

Parameter	Default	Description
Include Exchange Edge Transport Servers	false	Set this parameter to **true** to include Exchange Edge Transport servers in the public subnets.

Appendix B: Best Practices

Networking and Security

The networking and security components of the Quick Start architecture and key considerations include:

- Amazon VPC
- Security groups and network access control lists (ACLs)
- VPC Flow Logs
- Remote administration
- Principle of least privilege

These are discussed in the following sections.

Amazon VPC

Amazon VPC allows IT to configure Internet Protocol (IP) ranges, public/private subnets, routing tables, and Internet gateways or virtual private gateways. The customer has complete control over their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways.

Customers can easily customize the network configuration for their Amazon VPC. For example, they can create a public-facing subnet for their web servers that has access to the Internet and place their backend systems such as databases or application servers in a private-facing subnet with no Internet access. They can leverage multiple layers of security, including security groups and network access control lists (ACLs), to help control access to Amazon EC2 instances in each subnet.

Additionally, customers can create a hardware VPN connection between their corporate data center and their Amazon VPC, and leverage the AWS cloud as an extension of their corporate data center.

Security Groups and Network ACLs

There are two features that you can use to increase security for your Amazon VPC:

- Security groups, which act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level.

- Network ACLs, which act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level.

When you launch an instance in a VPC, you can associate one or more security groups that you've created. Each instance in your VPC could belong to a different set of security groups. If you don't specify a security group when you launch an instance, the instance automatically belongs to the default security group for the VPC. For more information about security groups, see the Security Groups for Your VPC section of the *Amazon VPC User Guide*.

You can secure your VPC instances using only security groups, or you can add network ACLs as a second layer of defense. For more information about network ACLs, see the Network ACLs section of the *Amazon VPC User Guide*.

You can use AWS Identity and Access Management (IAM) to control who in your organization has permission to create and manage security groups and network ACLs. For example, you can give that permission to your network administrators, but not to personnel who only need to launch instances. For more information, see the Controlling Access to Amazon VPC Resources section of the *Amazon VPC User Guide*. Amazon security groups and network ACLs don't filter traffic to or from link-local addresses (for example, `169.254.0.0/16`) or AWS reserved addresses (the first four IP addresses and the last one in each subnet). These addresses support the following services: Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Amazon EC2 instance metadata, AWS Key Management Service (AWS KMS) for license management of Windows instances, and routing in the subnet. You can implement additional firewall solutions in the instances to block network communication with link-local addresses.

The following table summarizes the differences between security groups and network ACLs.

Security group	Network ACL
Operates at the instance level (first layer of defense)	Operates at the subnet level (second layer of defense)
Supports allow rules only	Supports allow rules and deny rules
Is stateful: Return traffic is automatically allowed, regardless of any rules	Is stateless: Return traffic must be explicitly allowed by rules
Evaluates all rules before deciding whether to allow traffic	Processes rules in numerical order when deciding whether to allow traffic
Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on	Automatically applies to all instances in the subnets it's associated with (backup layer of defense, so customers don't have to rely on someone specifying the security group)

VPC Flow Logs

VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data is stored using Amazon CloudWatch Logs. After you create a flow log, you can view and retrieve its data in CloudWatch Logs.

Flow logs can help you with a number of tasks; for example, to troubleshoot why specific traffic is not reaching an instance, which, in turn, can help you diagnose overly restrictive security group rules. You can also use flow logs as a security tool to monitor the traffic that is reaching your instance.

Remote Administration

Components for remote administration include:

- **Amazon VPC** with network ACLs for provisioning a private, isolated section of the AWS cloud for launching services.
- **Amazon EC2** for launching virtual machine instances. This deployment uses the m4.xlarge instance type for RD Gateway instances and the t2.small instance type for Network Address Translation (NAT) instances.
- **Microsoft Windows Server 2012 R2**.
- **Remote Desktop Gateway (RD Gateway)**, which uses RDP for remote Windows administration.

This Quick Start uses an Amazon Machine Image (AMI) with preconfigured settings to set up remote Windows administration using the Remote Desktop Protocol (RDP) in your AWS account in minutes. You can use the trial deployment for up to 60 days. When you are ready for production or if you want to customize your deployment, follow the instructions in the Quick Start deployment guide for Remote Desktop Gateway.

Architecture components

The architecture is deployed into the US West (Oregon) region by default, but you can change the region of a Quick Start during launch. To customize the configuration or to deploy RD Gateway into an existing Amazon VPC, see the Quick Start deployment guide for Remote Desktop Gateway.

Features

- **High availability** – Critical workloads are deployed into two private Amazon VPC subnets in separate Availability Zones to ensure high availability.

- **Security** – Components such as web servers, application servers, database servers, and domain controllers are placed in separate tiers for effective traffic management. Internal and other non-Internet facing servers are placed in private subnets to prevent direct access from the Internet.
- **Remote administration** – The RD Gateway uses RDP over HTTPS to establish a secure, encrypted connection between remote users and Windows-based Amazon EC2 instances without needing to configure a VPN connection. This architecture helps reduce the attack surface on your Windows-based instances while providing a remote administration solution. For information about configuring RDP over HTTPS, see the Quick Start deployment guide for Remote Desktop Gateway.

Users and administrators can connect from an on-premises facility over a VPN and/or dedicated private network using the architecture shown in Figure 7.

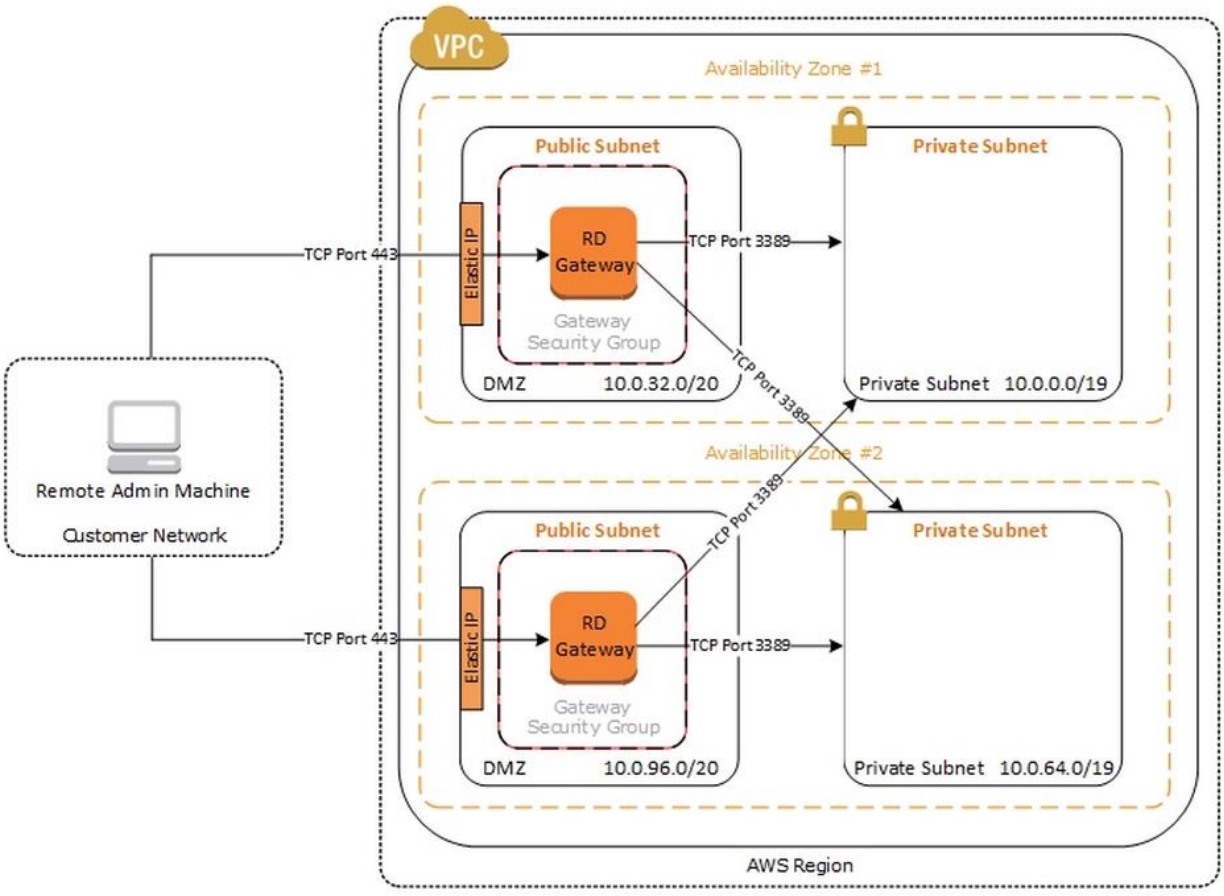

Figure 7: Remote administration architecture on AWS

Principle of Least Privilege

When you create AWS IAM policies, you should follow the standard security advice of granting least privilege—that is, granting only the permissions required to perform a task. Essentially, determine what your users need to do, and then craft policies for them that let the users perform only those tasks. It's more secure to start with a minimum set of permissions and grant additional permissions as necessary, rather than starting with permissions that are too lenient and then trying to tighten them later. Defining the right set of permissions requires some research to determine what is required for the specific task, what actions a particular service supports, and what permissions are required in order to perform those actions.

Windows Architectural Considerations on AWS

Key architectural considerations include the following:

- Regions and Availability Zones
- Installing critical workloads in at least two Availability Zones
- Placing application servers in private subnets

Regions and Availability Zones

AWS data centers are built in clusters in various global AWS Regions. You can decide which AWS Region(s) house your data, and how long the data remains there. AWS provides you with the flexibility to place instances and store data within multiple geographic Regions, as well as across multiple Availability Zones within each Region.

The AWS products and services that are available in each region are listed at the Region Table on the AWS website.

Each AWS region contains multiple distinct locations called Availability Zones. Each Availability Zone is engineered to be isolated from failures in other Availability Zones and to provide inexpensive, low-latency network connectivity to other zones in the same region. By launching instances in separate Availability Zones, you can protect applications from the failure of a single location.

For a list of AWS Regions and Availability Zones, see AWS Global Infrastructure on the AWS website.

Install Critical Workloads in at Least Two Availability Zones

This Quick Start deploys critical workloads into two or more private Amazon VPC subnets in separate Availability Zones to ensure high availability. Although Availability Zones

provide service-level agreements (SLAs) for Amazon EC2, Amazon S3, Amazon CloudFront, Amazon Route 53, and Amazon Relational Database Service (Amazon RDS), and support a redundant architecture for core services per Availability Zone, designing for multiple Availability Zones ensures that a single Availability Zone outage will not affect production workloads. Because Availability Zones support single-millisecond latency between each other, they enable application architectures that assume a single physical location.

AWS currently provides SLAs for several products. Due to the rapidly evolving nature of AWS's product offerings, we recommend that you review the SLAs on the AWS website; for example, at http://aws.amazon.com/ec2-sla/ for Amazon EC2.

Place Application Servers in Private Subnets

From an application perspective, Availability Zones are transparent. The application will need to know only about subnets. In Amazon VPC, subnets can span multiple Availability Zones. Placing application servers in private subnets provides two benefits:

- Tying subnet definitions to different Availability Zones increases availability.
- Using private subnets ensures that application servers and their data are accessible only through security group firewall rules and network ACLs that manage ingress/egress at a subnet level.

Active Directory Hybrid Deployments

Figure 8 provides an example of using an Amazon VPC and a virtual private gateway to enable communication with your own network over an IPsec VPN tunnel. Active Directory is deployed in the customer data center, and Windows Server instances are deployed into two Amazon VPC subnets. After deploying the VPN connection, you can promote the Windows instances to domain controllers in the on-premises Active Directory forest, making Active Directory Domain Services highly available in the AWS cloud.

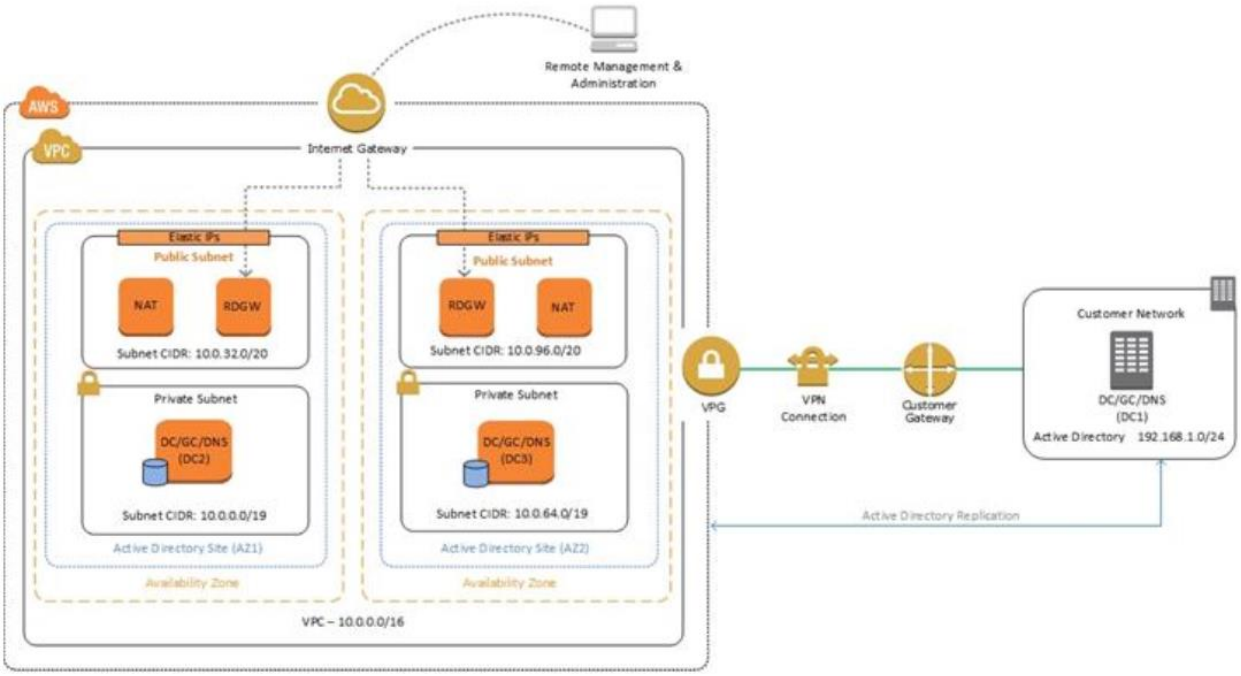

Figure 8: Reference architecture for an Amazon VPC extended to an on-premises network

After deploying the VPN connection and promoting servers to domain controllers, you can launch additional instances into the empty Amazon VPC subnets in the web, application, or database tiers. These instances will have access to cloud-based domain controllers for secure, low-latency directory services and DNS. All network traffic, including Active Directory Domain Services communication, authentication requests, and Active Directory replication, is secured either within the private subnets or across the VPN tunnel.

For detailed information about extending your on-premises AD DS to the AWS cloud, see the Quick Start deployment guide for AD DS.

Managing and Monitoring Windows Instances and Applications

Amazon CloudWatch will monitor instances in real time with standard and custom alarms on events. Standard monitoring includes capturing and setting rules around metrics and performance counters such as CPU utilization, disk read/write operations, bytes read/written, status checks, network-in/out, etc. In addition, you can export all Windows Server messages in the system, security, application, and Internet Information Services (IIS) logs to CloudWatch Logs and monitor them using Amazon CloudWatch metrics. EC2Config adds the ability to export any event log data, Event Tracing (Windows), or text-based log files to CloudWatch Logs. In addition, you can export performance counter data

to Amazon CloudWatch. To manage the performance counters and logs for multiple instances, you can use Amazon EC2 Simple Systems Manager (SSM).

Managing Applications in Systems Center Operations Manager

In addition to managing AWS and operating system metrics, it is a best practice to run Systems Center Operations Manager (SCOM) with the Management Packs that Microsoft has released. SCOM provides a management platform for monitoring and taking action on server events. Microsoft has released SCOM Management Packs for the servers and technologies deployed by this Quick Start. These Management Packs are useful in a physical or virtual environment and are designed to provide application-level guidance above and beyond the infrastructure layer.

Send Us Feedback

We welcome your questions and comments. Please post your feedback on the AWS Quick Start Discussion Forum.

You can visit our GitHub repository to download the templates and scripts for this Quick Start, and to share your customizations with others.

Document Revisions

Date	Change	In sections
June 2016	Initial publication	—

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

The software included with this guide is licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at http://aws.amazon.com/apache2.0/ or in the "license" file accompanying this file. This code is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.