Microsoft Lync Server 2013 on the AWS Cloud

Quick Start Reference Deployment

Santiago Cardenas

Bill Jacobi

June 2015
Last updated: May 2016 ([*revisions*](#)*)*

This guide is also available in HTML format at
https://docs.aws.amazon.com/quickstart/latest/lync/.

amazon
web services

Contents

About This Guide

This Quick Start reference deployment guide discusses architectural considerations and configuration steps for deploying a Microsoft Lync Server 2013 environment on the Amazon Web Services (AWS) cloud. It also provides links for viewing and launching AWS CloudFormation templates that automate the deployment.

The guide is for IT infrastructure architects and administrators who are planning to implement or extend their Lync Server 2013 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.

Overview

Lync Server 2013 on AWS

Microsoft Lync Server 2013 is a communications software platform that offers instant messaging (IM), presence, conferencing, and telephony solutions for small, medium, and large businesses.

The AWS cloud provides a suite of infrastructure services that enable you to deploy Lync Server 2013 in a fault-tolerant and affordable way. By deploying Lync Server 2013 on the AWS cloud, you can take advantage of the functionality of Lync Server 2013 along with the flexibility and security of AWS.

This guide provides infrastructure and configuration information for planning and deploying a Lync Server 2013 infrastructure on the AWS cloud. It doesn't cover general installation and software configuration tasks for Lync Server 2013. For general guidance and best practices, consult the Lync Server 2013 documentation on Microsoft TechNet.

Quick Links

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

View template

The default configuration deploys two Lync Server Standard Edition pools across two Availability Zones. You can customize the template by following the instructions in this guide to optionally deploy Lync Edge Servers as well.

Launch Quick Start

Time to deploy: Approximately 2 hours

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. As of the date of publication, the cost for using the Quick Start with default settings is approximately $5 an hour. Prices are subject to change. See the pricing pages for each AWS service you will be using in this Quick Start for full details.

Lync Server 2013 can be deployed and licensed through the Microsoft License Mobility through Software Assurance program. For development and test environments, you can

leverage your existing MSDN licenses for Lync Server 2013 using Amazon Elastic Compute Cloud (Amazon EC2) Dedicated Instances. For details, see the MSDN on AWS webpage.

This deployment uses an evaluation copy of Lync Server 2013. To upgrade your version, consult Microsoft's documentation to determine any required steps based on the license type that you own.

This 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. The AMI is updated on a regular basis with the latest service pack for the operating system, so you don't have to install any updates.

Architecture Overview

Deploying this Quick Start with the **default parameters** builds the following Lync Server 2013 environment in the AWS cloud.
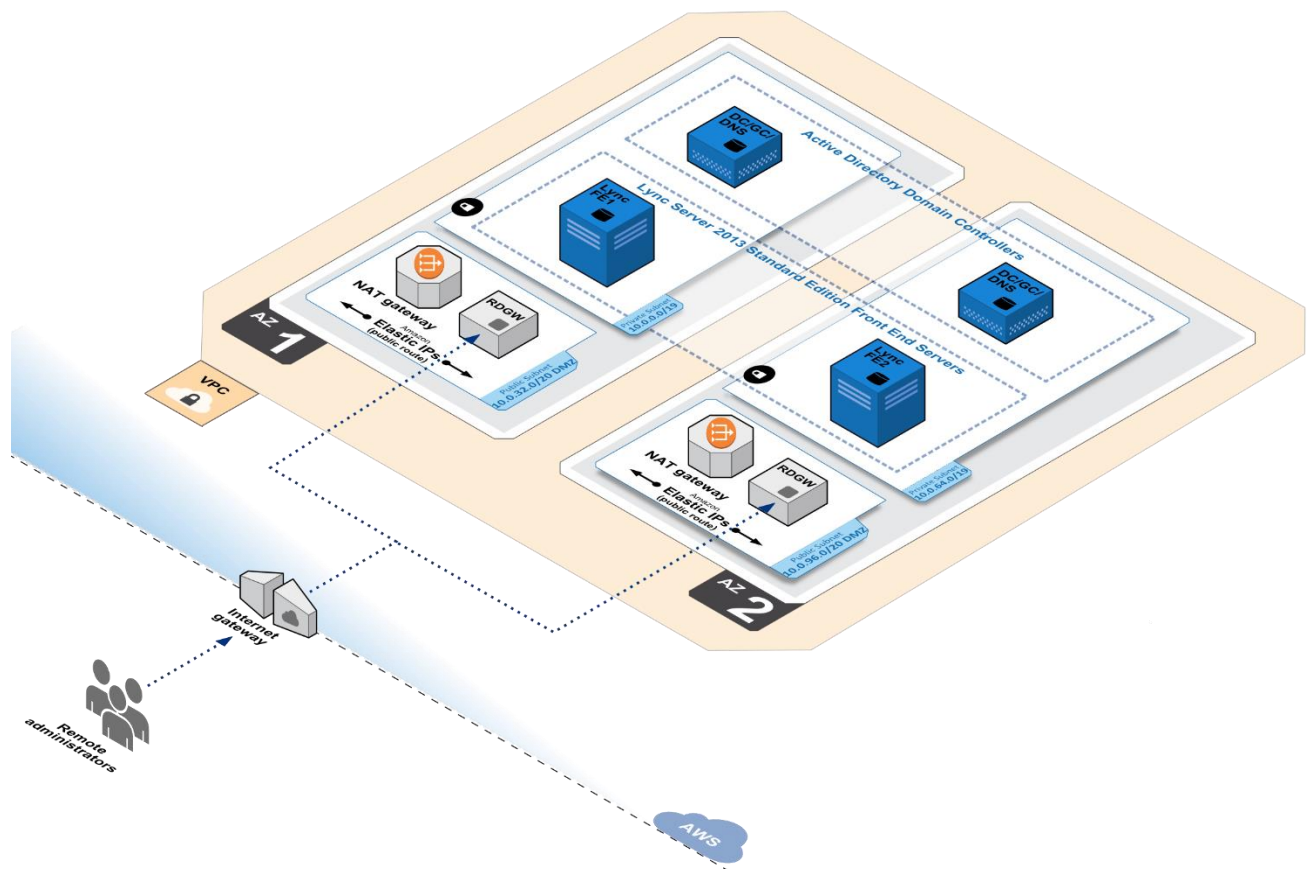

Figure 1: Quick Start Architecture for Lync Server 2013 on AWS

The AWS CloudFormation template creates a fully functional Lync Server 2013 deployment on the AWS cloud. The following components are deployed by the CloudFormation template:

- An Amazon Virtual Private Cloud (Amazon VPC) with resources distributed across two Availability Zones.

- Public subnets in each Availability Zone that provide access to and from the Internet. The public subnets include network address translation (NAT) instances for outbound Internet access, and Remote Desktop Gateway (RD Gateway) instances for inbound remote administrative access. Lync Edge Servers can optionally be deployed in these subnets for external Lync users.

- Private subnets in each Availability Zone for running enterprise workloads such as Active Directory domain controllers and Lync Server 2013 servers, shielded from direct access over the Internet. The domain controllers act as enterprise certificate authorities (CAs) that issue the required SSL certificates to the Lync Server infrastructure.

- Security groups to tightly control the flow of traffic between your Amazon EC2 instances.

- Paired Lync Server 2013 Standard Edition pools, which are deployed in each Availability Zone to support disaster recovery and pool failover.

Keep in mind that 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 give you an active/active type of deployment, where servers in both Availability Zones are servicing users. In the event of a disaster, you can fail over to the other Availability Zone.

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.)

- 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.

- [Amazon EBS](#) – Amazon Elastic Block Store (Amazon EBS) provides persistent block-level storage volumes for use with Amazon EC2 instances in 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.

Design Considerations

Lync Server 2013 is a robust communications platform that can be architected and deployed in a number of ways, depending on your requirements. This Quick Start is designed to give you a starting point for implementing a small or medium-sized Lync Server 2013 deployment on the AWS cloud. We also cover considerations for large deployments that you can implement on your own.

Lync Server 2013 Standard and Enterprise Editions

The Standard Edition of Lync Server 2013 is intended for small organizations, and a single Standard Edition Front End Server can support approximately 5,000 users. The user and application databases are stored locally on a SQL Server Express instance. You can pair two Standard Edition pools to provide a disaster recovery failover option in the case of a lost server or Availability Zone. In this scenario, you would home 50% of your users on each pool, for an active/active deployment. If one Standard Edition server fails, you can fail the pool over to the remaining server, which can support a total of 5,000 active users.

To provide the quickest deployment option, this Quick Start deploys paired Standard Edition servers with one server in each Availability Zone.

The Enterprise Edition of Lync Server 2013 provides support for large deployments and additional high availability features. The user and application databases run on a dedicated pool of SQL servers. Larger deployments will require a number of additional servers in your topology. Additional sizing guidance and considerations for large deployments are covered later in this guide.

Selecting an Instance Type

To select the appropriate instance type for servers in your Lync deployment, you should map the recommended requirements in the following sections to compatible Amazon EC2 instance types. Additionally, we recommend that you select an instance type that supports

Amazon EBS optimization, enhanced networking, and high or 10-gigabit network performance, which results in higher performance (packets per second), lower latency, and lower jitter. The following sections provide examples of how to choose an instance type depending on the workload.

Front End Servers, Back End Servers, Standard Edition Servers, and Persistent Chat Servers

For these workloads, use the minimum requirements set by Microsoft to determine the Amazon EC2 instance type:

- CPU: 6 cores

- Memory: 32 GiB

- Disk: Solid state drives (SSDs)

- Network: 1 Gbps network adapter

When starting your design, you should choose an instance type that can provide enough vCPUs and memory to match these minimum requirements as closely as possible.

Amazon EBS General Purpose or Provisioned IOPS volumes are SSD-backed and should be used for both the root OS volume and for any database and log volumes you'll need. Amazon EBS Magnetic volumes can be used for testing, but should not be used for production workloads. Currently all M4, R3, C3, D2, and I2 instances support enhanced networking, so these instance types should be your primary candidates.

For each Lync Standard Edition Server, by default, this Quick Start uses the m4.2xlarge instance type, which provides 8 vCPUs, 32 GiB of memory, high network performance, Amazon EBS optimization, and enhanced networking. Amazon EBS General Purpose (SSD) volumes are used for storage.

Edge Servers, Standalone Mediation Servers, and Directors

For these workloads, use the minimum requirements set by Microsoft to determine the Amazon EC2 instance type:

- CPU: 4 cores

- Memory: 16 GiB

- Disk: Solid state drives (SSDs)

- Network: 1 Gbps network adapter

You should choose an instance type that can provide enough vCPUs and memory to match these minimum requirements as closely as possible.

For the Edge Server, by default, this Quick Start uses the m4.xlarge instance type, which provides 4 vCPUs, 16 GiB of memory, high network performance, and enhanced networking. Amazon EBS General Purpose (SSD) volumes are used for storage.

Additional Planning Tools

Microsoft provides the following tools to assist you in planning your deployment, sizing your servers, and testing the performance before moving into production:

- Lync Server 2013 Planning Tool – Asks you questions about your organization and the features that you are interested in. The tool then provides guidance for designing your site topology, based on your answers and on the tested Microsoft Lync Server 2013 user model.

- Lync Server 2013 Capacity Calculator – Calculates Lync Server hardware requirements based number of users, types of communication, traffic estimates, and similar information.

- Lync Server 2013 Stress and Performance Tool (LSS) – Assists in hardware and capacity planning for Lync Server. You can use LSS to configure user scenarios and measure the performance of your Lync Server 2013 deployment. LSS includes modules for simulating different types of user activity, such as IM and presence, VoIP, and conferencing, and can simulate simultaneous users on multiple Lync Servers.

We recommend using the capacity and planning tools to create more complex designs and to validate your assumptions. We also highly recommend validating the performance of those proposed designs with the LSS tool before moving into production.

Load Balancing

When designing for high availability, Front End pools, Director pools, and Edge Server pools will require load balancing. Lync Server 2013 supports two types of load balancing: Domain Name System (DNS) load balancing and hardware load balancing.

DNS load balancing can make administration and troubleshooting easier, compared with hardware load balancing, but remember that HTTP traffic will require a virtual load balancer. Many organizations often use a mix of these two load balancing options to provide load distribution and high availability for large deployments.

The AWS Marketplace includes a number of third-party load balancing solutions. Some examples of commonly used solutions are:

- [Citrix NetScaler VPX](#)

- [KEMP Virtual LoadMaster for AWS](#)

- [F5 BIG-IP Virtual Edition for AWS](#)

For details and general guidance on load balancing for Lync Server 2013, see the [Additional Resources](#) section.

Edge and Reverse Proxy Servers

Edge Servers make it possible for external users to use Lync services remotely without the use of a VPN connection. However, although the Edge Server role provides signaling and media support for external users, it does not support HTTP-based services. HTTP-based services run on the Front End Standard Edition or Enterprise Edition servers in your topology. Examples of HTTP-based services include your meeting join page and the web service used by mobile clients.

To make HTTP-based services available externally, we recommend that you use a reverse proxy server, which typically sits in a DMZ network. In the case of AWS, you can think of your public Amazon VPC subnets as your DMZ networks, and this is where your Edge Servers and reverse proxy servers should reside.

Some common reverse proxy solutions from Microsoft include [IIS Application Request Routing (ARR)](#) and the [Web Application Proxy](#) server. You can deploy either one of these as a post-configuration task after launching the Quick Start.

Certificates

Lync Server requires SSL certificates for securing both internal and external services. Although an internal enterprise certificate authority (CA) is recommended for internal servers, you can also use a public CA. External services are typically secured with commercial certificates that are purchased and issued from a public CA.

This Quick Start leverages an internal enterprise CA running on the Active Directory domain controllers. Both the internal and external services are secured using certificates issued for the internal enterprise CA. If you choose to deploy Edge and reverse proxy servers, keep in mind that you'll likely want to purchase certificates from a public CA to secure those external services. This will allow external devices that are not part of your

organization to trust the issuing CA and therefore make use of your external Edge and reverse proxy infrastructure.

For details, see the [Certificate infrastructure requirements for Lync Server 2013](#) on Microsoft TechNet.

Enterprise Voice

Enterprise Voice is a set of features that provides a complete telephony solution with connectivity to the Public Switched Telephone Network (PSTN). For a cloud-based deployment of Lync Server on AWS, you can utilize Session Initiation Protocol (SIP) trunks from an IP telephony provider to deliver PSTN calling capabilities to your Lync users.

To connect a SIP trunk to your Lync environment, you can deploy a Session Border Controller (SBC) appliance into the public DMZ subnets in your Amazon VPC. This will keep your Lync servers in the private subnets shielded from the Internet, and you can benefit from the additional security features offered by most SBC appliances.

There are a number of SIP trunking and SBC providers that you can use to enable Lync Enterprise Voice with your deployment on AWS. IntelePeer ([intelepeer.com](#)) is a well-known provider of SIP trunking services, and Sansay ([sansay.com](#)) offers their VSXi SBC appliance as an Amazon Machine Image (AMI). Your AWS Direct Connect partner may be able to connect you to other Microsoft-certified SIP trunk providers.

Office Web Apps Server

Lync Server 2013 uses [Office Web Apps Server](#) to deliver Microsoft PowerPoint presentations. You may need to deploy at least one additional server if you intend to use this functionality in your deployment. You can make this role highly available by deploying at least two servers and load balancing them with a virtual load balancer.

Considerations for Large Deployments

To design large deployments for the best performance and high availability, you'll need the Enterprise Edition of Lync Server, and a topology with more than one server per Availability Zone. Here are some considerations for the various server roles in a large deployment.

- **Front End Servers** – Microsoft states that you should have one Front End Server for every 6,600 users homed in the pool. The maximum number of users in a Front End pool is 80,000, which means that a Front End pool can have a maximum of 12 servers. This Quick Start deploys Standard Edition servers (one Front End per pool). For larger

deployments you'll want to use Enterprise Edition and scale out accordingly; see the [Sample Enterprise Deployment](#) section for details.

- **Mediation Servers** – For smaller deployments, you can collocate the Mediation Server role on your Front End Servers. You may benefit from deploying a dedicated Mediation Server pool if you need to support a large number of users. This depends on several factors, such as the number of Enterprise Voice users and concurrent calls.

- **Back End Servers** – The Enterprise Edition of Lync Server moves some of the Lync databases to dedicated Back End Servers (which are SQL servers). You should use SQL servers that run on Amazon EC2 instances, as opposed to Amazon Relational Database Service (RDS) DB instances. You can easily deploy these Back End Servers using a SQL Server Standard AMI, or you can manually build your own SQL servers on Amazon EC2 instances. The Back End Servers can be made highly available through SQL mirroring. Note that Microsoft has announced the deprecation of SQL mirroring, but will support SQL AlwaysOn Availability Groups in future versions of the Lync/Skype server platform.

- **Monitoring and Archiving Servers** – If installed, the Monitoring and Archiving services run on your Front End Servers. However, these services use a SQL store that is separate from the Back End Servers. You should use SQL servers that run on Amazon EC2 instances, as opposed to Amazon RDS DB instances. You can easily deploy these servers using a SQL Server Standard AMI, or you can manually build your own SQL servers on Amazon EC2 instances.

- **Persistent Chat Server** – The Persistent Chat Server is available with Enterprise Edition as a dedicated pool, separate from your Front End Servers. Persistent Chat Server requires a Back End Server to store chat room content and metadata. Microsoft recommends that you install Persistent Chat content on a dedicated Back End Server, but also states that you can choose to install it on an existing Back End Server if needed.

- **Stress testing** – Use the [Lync Server 2013 Stress Testing Guide](#) to validate capacity planning assumptions through a stress testing exercise.

- **Operations management** – Systems Center Operations Manager 2007 R2 and 2012 support a Lync Server 2013 management pack that will monitor the operational metrics of your Lync environment. This will require installing an additional instance of SQL Server. For more information, see [Configuring Lync Server 2013 to work with System Center Operations Manager](#) on Microsoft TechNet.

For additional details on planning a Lync Server 2013 deployment, see [Capacity planning for Lync Server 2013](#) on Microsoft TechNet.

Sample Enterprise Deployment

The following diagram shows an enterprise deployment of Lync Server 2013 on AWS in a single Availability Zone. This will provide high availability for Lync within the Availability Zone in the event of a server failure. To design a solution that spans an entire AWS region, you can deploy an identical pool in a second Availability Zone, and then pair those pools for disaster recovery purposes.
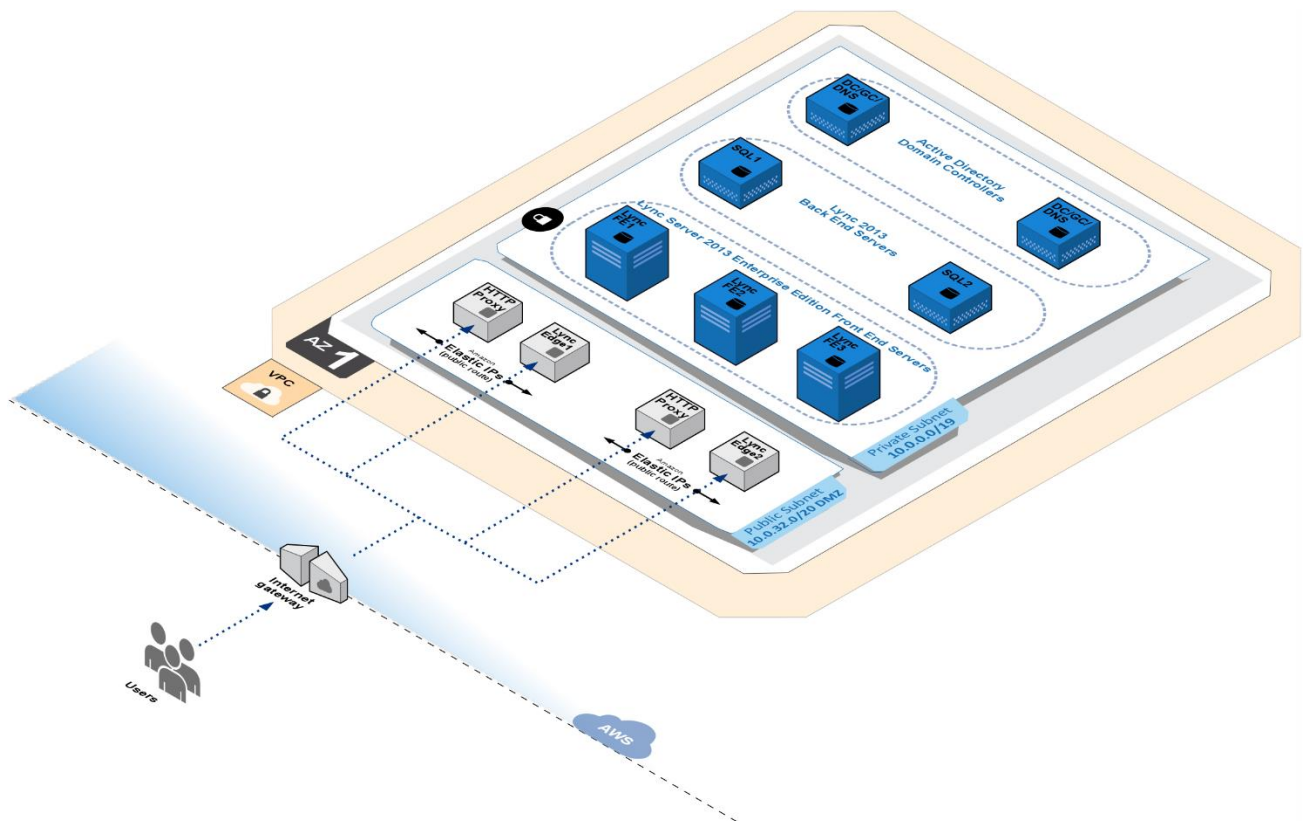

Figure 2: Lync 2013 Enterprise Deployment in a Single Availability Zone

There are several key points to take into consideration based on the architecture shown in Figure 2:

- The public subnet contains a pool of two Lync 2013 Edge Servers. These servers make it possible for external users to use Lync without a VPN connection. These Edge Servers can be load balanced with DNS load balancing or by using a virtual load balancer appliance.

- The public subnet contains a pair of HTTP proxy servers. These provide external access to various Lync components that operate over HTTP. These servers can be running the reverse proxy solutions mentioned earlier in this guide, or many others. These reverse

proxy servers can be load balanced using a virtual load balancer appliance, or with Amazon Route 53 failover record sets.

- The private subnet contains a pool of three Lync Server 2013 Enterprise Edition Front End Servers. Front End pools use a distributed model where user data is kept on three Front End Servers in the pool. Microsoft recommends that all your Enterprise Edition Front End pools include at least three Front End Servers.

- The private subnet contains two SQL Server 2014 servers to act as the database back end. These servers use SQL mirroring for failover.

- The private subnet contains two Active Directory domain controllers. Although it is possible to use one server for this role, a second domain controller is included in this architecture to make every service redundant and highly available within the Availability Zone.

For further details on highly available Lync Server 2013 architectures, see Topologies and components for Front End Servers, instant messaging, and presence in Lync Server 2013 on Microsoft TechNet.

Automated Deployment

The AWS CloudFormation template provided with this Quick Start bootstraps the AWS infrastructure and automates the deployment of Lync Server 2013 on the AWS cloud from scratch. 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.

What We'll Cover

The procedure for deploying the Lync Server 2013 architecture on AWS 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 stack

- Launch the AWS CloudFormation template into your AWS account.
- Enter a value for the required *KeyPairName* parameter.

- Review the other template parameters, and adjust if necessary.

Step 3. Test your Lync Server 2013 deployment

- Connect to the Lync servers.

- Enable one or more users for Lync.

- Install the Lync client and validate sign-in.

- Test pool failover for disaster recovery.

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 Amazon EC2 region where you want to deploy Lync Server 2013 on AWS.
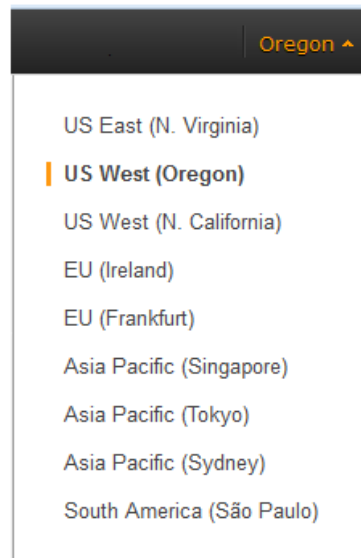
Figure 3: Choosing an Amazon EC2 Region

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 the **m4.2xlarge** instance type for the Lync Server 2013 portion of the deployment. M4 instance types are currently available in all AWS Regions except GovCloud (US), China (Beijing), and South America (São Paulo).

> The Quick Start also uses NAT gateways, which are not available in all regions. See the Amazon VPC Pricing page for details.
>
> It is important to be aware of which services are available in the region you choose to deploy. To see the latest list of supported services per region, see AWS Regions and Endpoints in the AWS documentation. We recommend that you check service availability before you choose a region. Otherwise, deployment will fail.

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**.
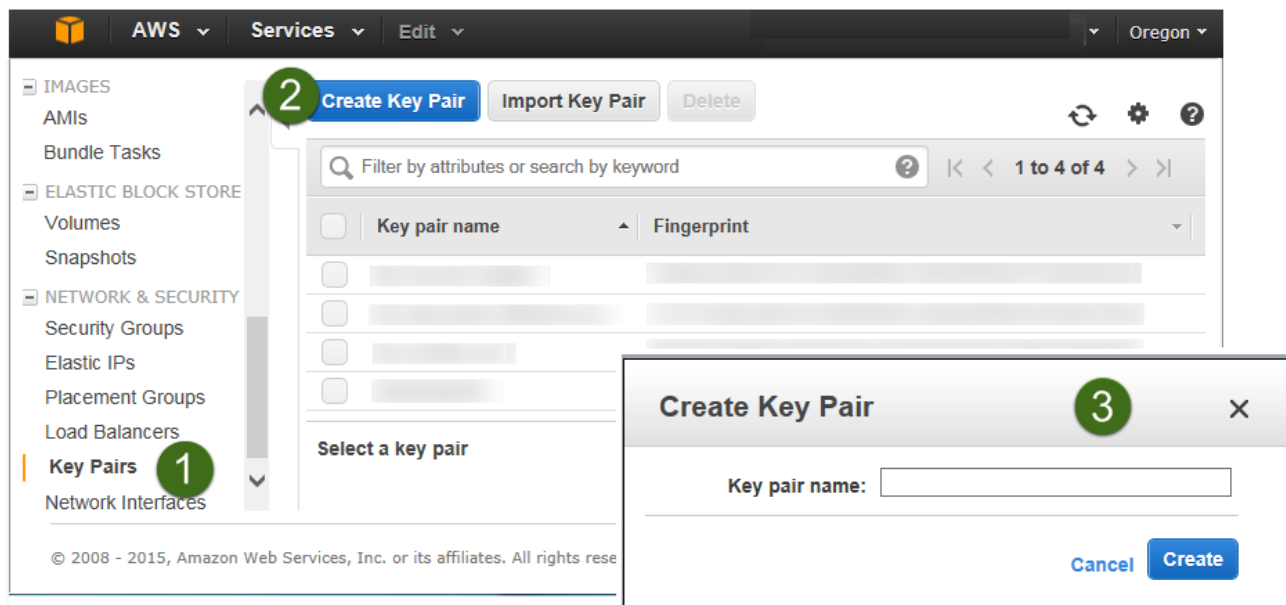
Figure 4: Creating a Key Pair

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 Amazon EC2 m4.2xlarge instance type. 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. The current default limit is 20. 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 5: Requesting a Service Limit Increase

Step 2. Launch the Lync Server 2013 Stack

This automated AWS CloudFormation template deploys Lync Server 2013 in multiple Availability Zones into an Amazon VPC. Please make sure that you've created a key pair in your chosen region before launching the stack.

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

   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.

   Launch Quick Start

This stack takes approximately 2 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. As of the date of publication, the cost for using the Quick Start with default settings is approximately $5 an hour, and you can complete the initial deployment for about $10. Prices are subject to change. See the pricing pages for each AWS service you will be using in this Quick Start for full details.

You can also download the template to use as a starting point for your own implementation.

2. On the **Select Template** page, keep the default settings for **Stack** and **Template Source**.

3. On the **Specify Parameters** page, review the parameters for the template. Provide a value for the parameters that require your input.

Parameter	Default	Description
AD1PrivateIp	10.0.0.10	Primary private IP for the first domain controller in Availability Zone 1
AD2InstanceType	m4.xlarge	Amazon EC2 instance type for the second Active Directory instance
AD2PrivateIp	10.0.64.10	Primary private IP for the domain controller in Availability Zone 2
ADInstanceType	m4.xlarge	Amazon EC2 instance type for the first Active Directory instance
ADServerNetBIOSName1	DC1	NetBIOS name of the first Active Directory server (up to 15 characters)
ADServerNetBIOSName2	DC2	NetBIOS name of the second Active Directory server (up to 15 characters)
DMZ1CIDR	10.0.32.0/20	CIDR block for the public DMZ subnet located in Availability Zone 1
DMZ2CIDR	10.0.69.0/20	CIDR block for the public DMZ subnet located in Availability Zone 2
DomainAdminPassword	*Requires input*	Password for the domain administrator user (StackAdmin). This must be a complex password that's at least 8 characters long. This password will also be set for the local administrator account on each Lync Edge Server, if you've set the **IncludeEdge** parameter to **true**.
DomainAdminUser	StackAdmin	User name for the account that will be added as domain administrator
DomainDNSName	Example.com	Fully qualified domain name (FQDN) of the forest root domain

Parameter	Default	Description
DomainNetBIOSName	EXAMPLE	NetBIOS name of the domain (up to 15 characters) for users of earlier versions of Windows
FE1PrivateIP	10.0.0.160	Primary private IP for the first Lync Front End Server
FE2PrivateIP	10.0.64.160	Primary private IP for the second Lync Front End Server
IncludeEdge	false	Set this parameter to **true** to include Lync Edge Servers in the public subnets
KeyPairName	*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.
LE1PrivateIp	10.0.0.161	Primary private IP for the first Lync Edge Server
LE1PublicIp	10.0.32.161	Public subnet IP for the first Lync Edge Server
LE2PrivateIp	10.0.64.161	Primary private IP for the second Lync Edge Server
LE2PublicIp	10.0.96.161	Public subnet IP for the second Lync Edge Server
LyncEdgeInstanceType	m4.xlarge	Amazon EC2 instance type for the Lync Edge Servers
LyncFEInstanceType	m4.2xlarge	Amazon EC2 instance type for the Lync Standard Edition Front End Servers
LyncISOImageURI	*Requires input*	Amazon S3 URI to the S3 bucket that contains the ISO image file for the Lync Server 2016 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.
PrivSub1CIDR	10.0.0.0/19	CIDR block for the private subnet located in Availability Zone 1
PrivSub2CIDR	10.0.64.0/19	CIDR block for the private subnet located in Availability Zone 2
RDGWInstanceType	m4.xlarge	Amazon EC2 instance type for the Remote Desktop Gateway instances
RestoreModePassword	*Requires input*	Password for a separate administrator account when the domain controller is in Restore Mode. This must be a [complex password](#) that's at least 8 characters long.
VPCCIDR	10.0.0.0/16	CIDR block for the Amazon VPC

> **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, keep the default settings.

5. On the **Review** page, review and confirm the settings.

6. Choose **Create** to deploy the stack.

7. Monitor the status of the stack. When the status is **CREATE_COMPLETE**, the Lync Server cluster is ready.

Step 3. Test Your Lync Server 2013 Deployment

Once your Lync stack is up and running, you can connect to your servers and test your deployment. In this section, we'll explain how to create and enable users for Lync, and test sign-in from the Lync client. Then we'll take a look at how to fail over from one Availability Zone to the other.

Connecting to Lync Servers

1. Remote into the environment through one of the Remote Desktop Gateway (RD Gateway) instances. Use the **StackAdmin@example.com** user name and the password you set when you launched the stack.

   You can retrieve the Elastic IP address (EIP) for each RD Gateway instance from the Amazon EC2 console. You can use the Remote Desktop Gateway Quick Start to fully configure your RD Gateway instances, or you can simply connect to the desktop of your RD Gateway instances, and then start a new RDP client to connect internally to your remaining servers.

2. RDP to the FE1 server, which is the Lync Front End Server in the first Availability Zone. From the **Start** menu, launch the Lync Control Panel. The Lync Control Panel is a Microsoft Silverlight-based web application, and the Silverlight client is already installed on the Lync servers.
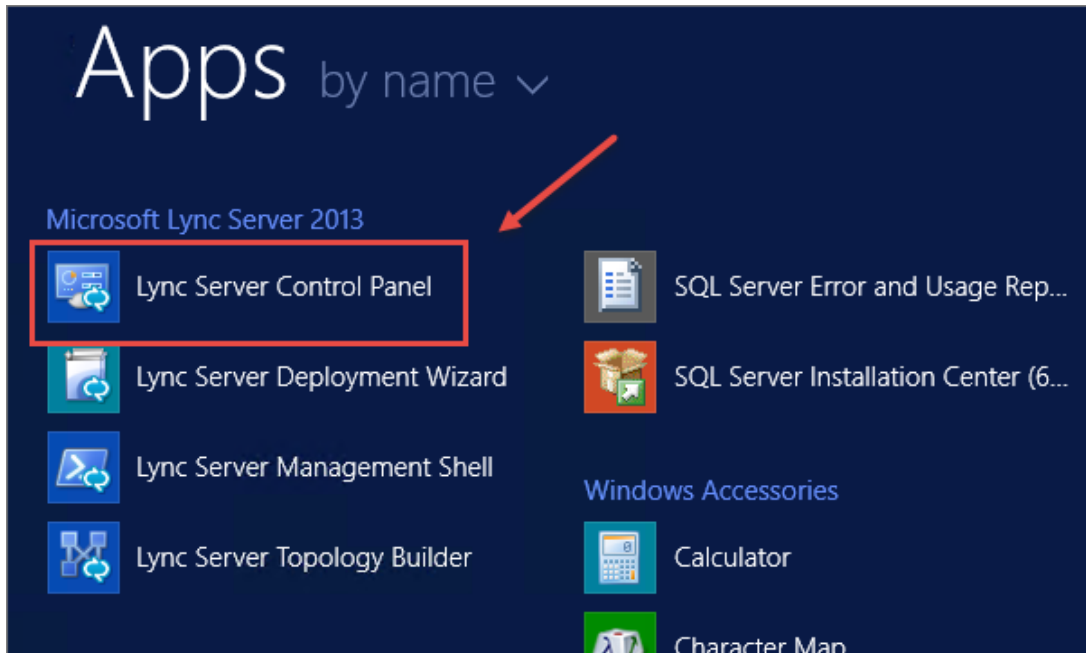
Figure 6: Launching the Lync Control Panel

3. You'll be prompted to select the server to connect to. Choose **fe1.example.com**.
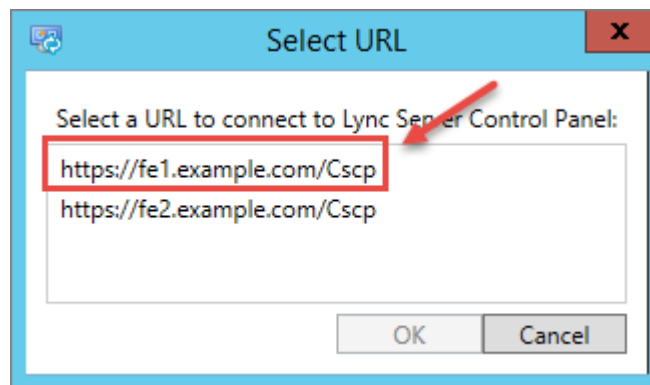
Figure 7: Selecting the Server URL

Creating Test Users

Follow the instructions in the Microsoft documentation to create test 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.

Enabling Users

1. In the Lync Control Panel, choose **Users** from the left navigation bar, and then choose **Enable users**.
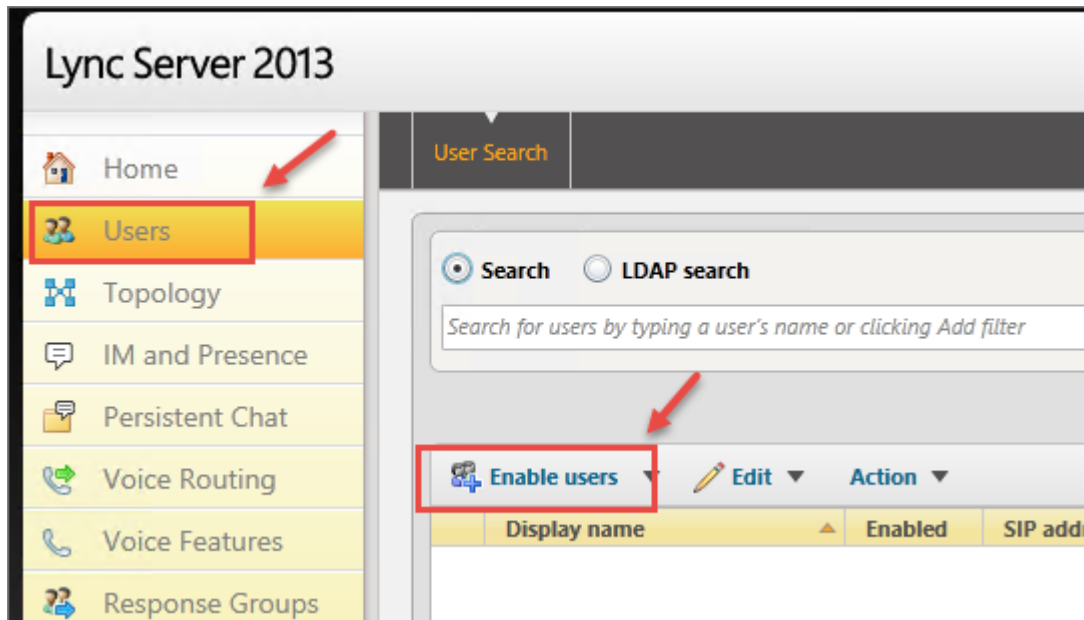
Figure 8: Navigating to User Administration in the Lync Control Panel

2. In the **New Lync Server User** dialog box, choose **Add**.

3. In the **Select from Active Directory** dialog box, choose **Find**. This will allow you to select a user to enable for Lync. You can use the accounts you created in Active Directory. Make sure that you use a non-administrative account.

   Make a note of the user principal name (UPN), as this will serve as the sign-in name for the user. Choose **OK** when you're done.
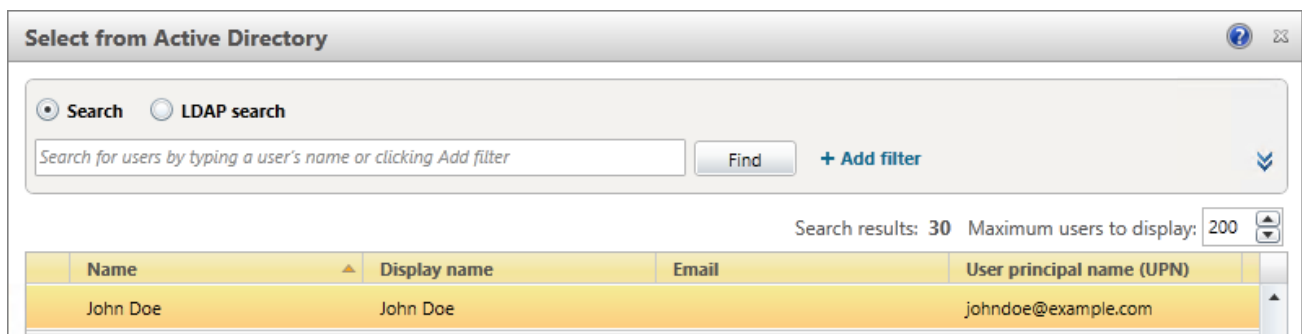
Figure 9: Finding a User to Lync-Enable

4. The **New Lync Server User** dialog box will be redisplayed. Assign the user to the
    fe1.example.com pool. Make sure that you choose **Use the user principal name
    (UPN)** for the SIP URI. Then choose **Enable**.
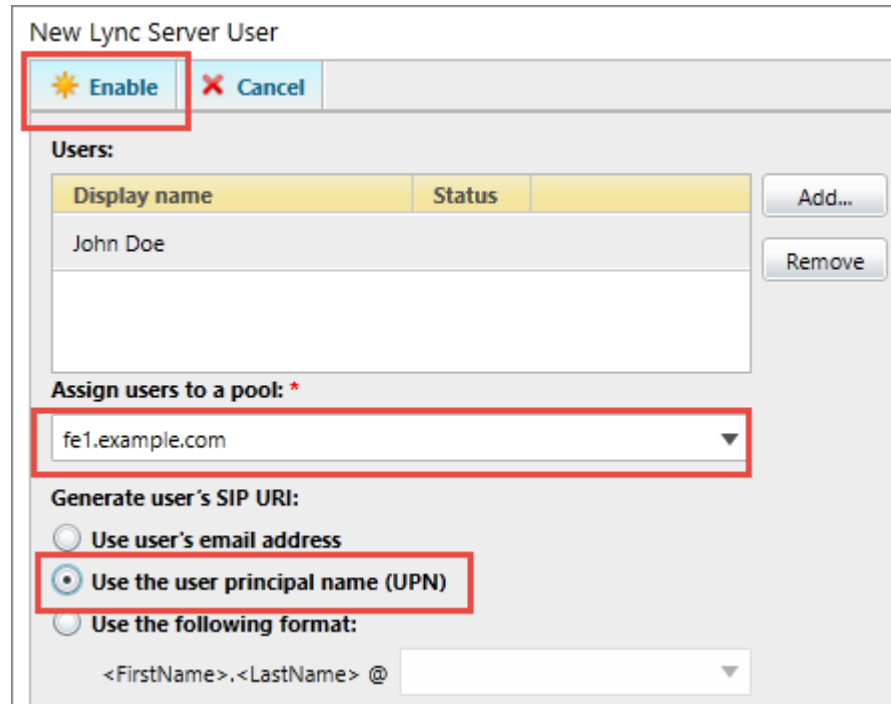
<div align="center">**Figure 10: Enabling a User for Lync**</div>

Validating the Lync Sign-in

Now that you have a Lync-enabled user, you can install the Lync client and test the sign-in
to the Lync Server.

1. Install a Lync client. For this task, you can use one of the Remote Desktop Gateway
    instances as a client machine. For example, from the RDGW1 server, you can install
    Office Professional Plus 2013, which includes the Lync client, or you can install the free
    Lync Basic 2013 client. You can download the Lync Basic client from the Microsoft
    Download Center. There are no special instructions for installing the Lync Basic client;
    follow the instructions on the setup screen and accept all the default settings.

2. Launch the Lync client you installed in the previous step. Use the UPN for the user as
    the sign-in name. If you used one of the pre-created test accounts, use **p@ssword123**
    for the password. Once you've successfully signed in, you'll see a green presence
    indicator next to your name.
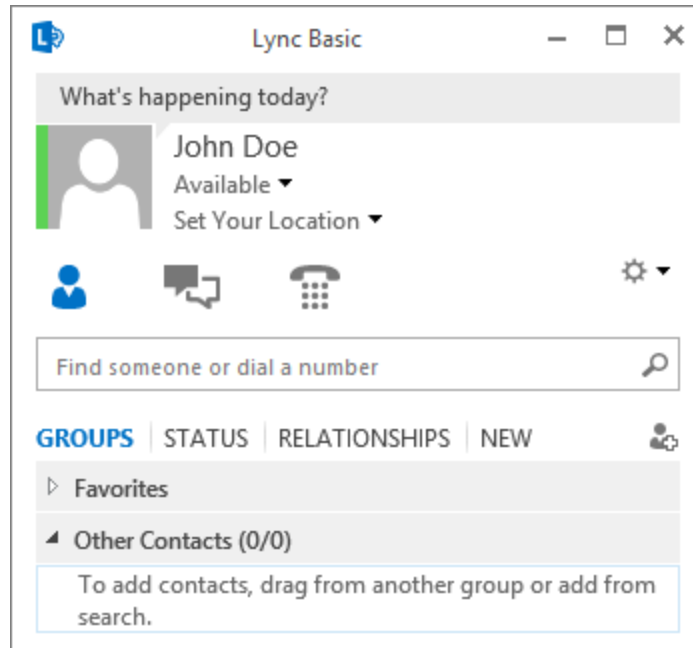
Figure 11: Signing into Lync with a Test Account

Testing Pool Failover for Disaster Recovery

Since you are now signed in with an account homed on the fe1.example.com pool, you can simulate a failure of that pool and invoke a pool failover for disaster recovery.

1. On the **FE1** server, stop the **Lync Server Front-End** service. You can do this in the GUI, or by using Windows PowerShell with the following command:
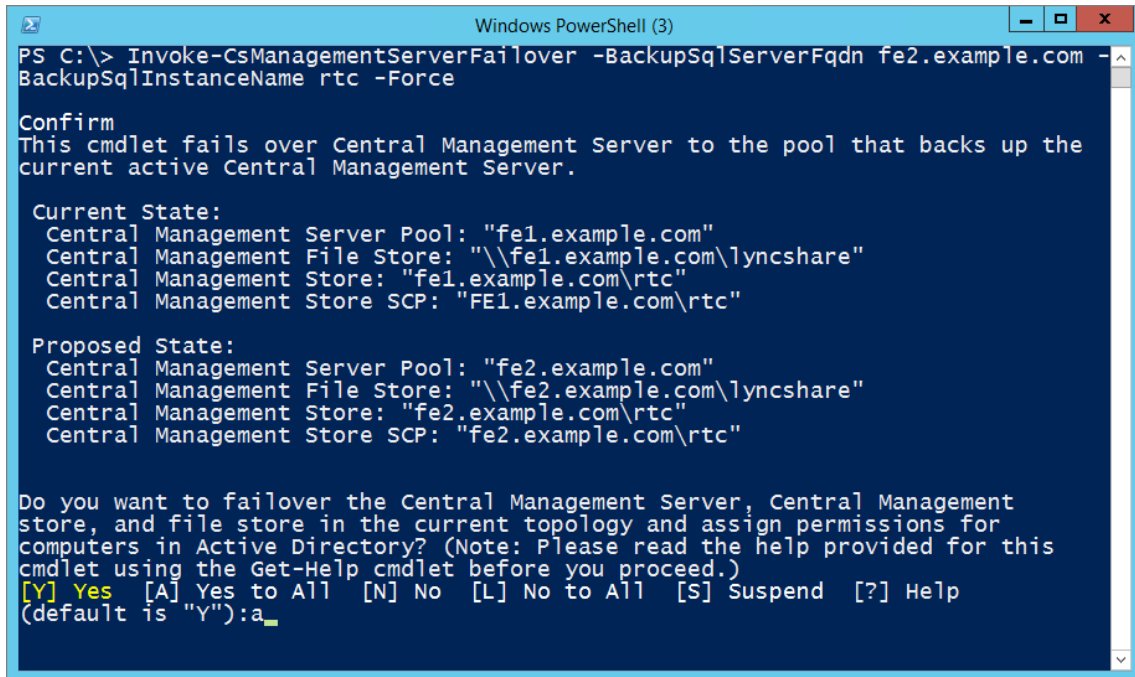
   ```
   Stop-Service RtcSrv -Force
   ```

   This will simulate a server outage, and you should notice your Lync client getting disconnected.

2. Now you're ready to fail over to the second Availability Zone. Remote into the **FE2** server, and fire up PowerShell. To fail over the Central Management Server, run:

   ```
   Invoke-CsManagementServerFailover -BackupSqlServerFqdn
   fe2.example.com -BackupSqlInstanceName rtc -Force
   ```

   When you're prompted for confirmation, type **A**, and then press **Enter** to continue.

Figure 12: Invoking Management Server Failover

3. Next, run the following PowerShell command to fail the **FE1** pool over to **FE2**:

```
Invoke-CsPoolFailOver -PoolFqdn fe1.example.com –DisasterMode -Force
```

When prompted for confirmation, type **A**, and then press **Enter** to continue.

Figure 13: Invoking Pool Failover

4. After a few moments, the Lync client should reconnect to the pool in the second Availability Zone. If nothing happens, close the client (make sure the lync.exe process is closed) and try signing back in.

5. You can view the client configuration by pressing the Ctrl key, right-clicking the Lync icon in the notification area, and choosing **Configuration Information**. You should see that the connected Lync server is now **fe2.example.com**.
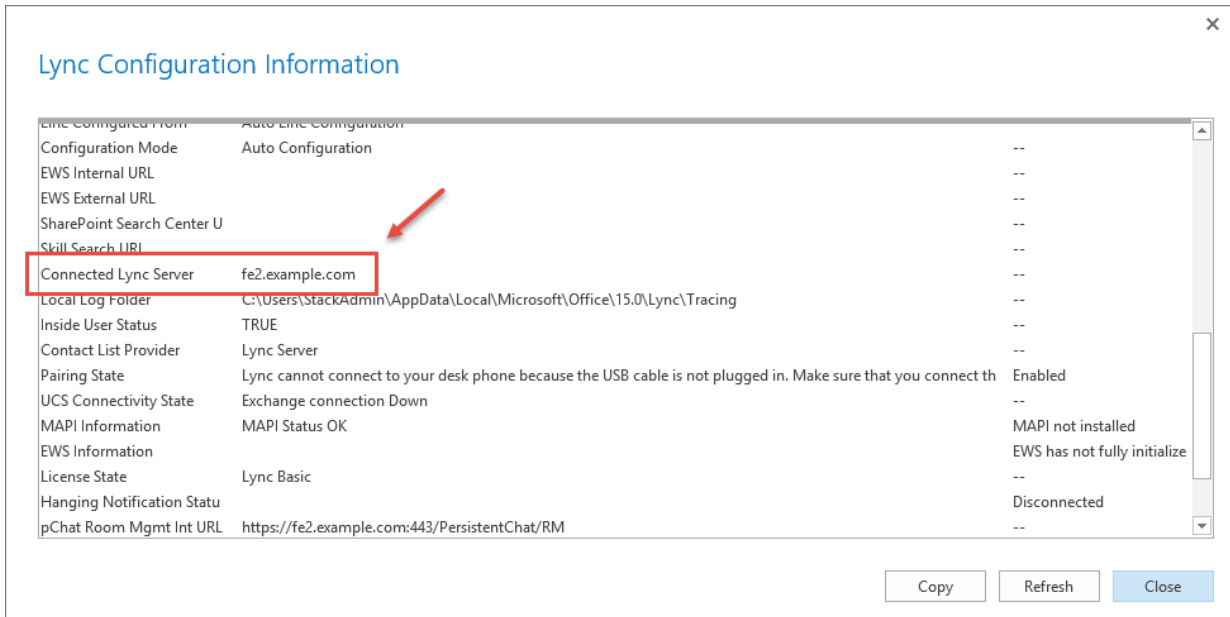
Figure 14: Viewing Lync Client Configuration Information

6. At this point, you can fail the pool back to **FE1**. To do so, start the **RtcSrv** service on **FE1**, and run the following command on the **FE2** server:

```
Invoke-CsPoolFailBack -PoolFqdn fe1.example.com -Force
```

For more information, see Managing Lync Server 2013 disaster recovery, high availability, and Backup Service on Microsoft TechNet.

Security

When you build systems on the AWS infrastructure, security responsibilities are shared between you and AWS. This shared model can reduce your operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. In turn, you assume responsibility and management of the guest operating system (including updates and security patches), other associated applications, as well as the configuration of the AWS-provided security group firewall. For more information about security on AWS, visit the AWS Security Center.

Operating System Security

All the Windows Servers deployed by this Quick Start (with the exception of optional Lync Edge Servers) are domain-joined. You can authenticate to these instances by using the

stackadmin@example.com domain administrator account. You can specify the password for this account as you launch the stack. The local administrator password for domain-joined instances can be retrieved by using the *KeyPairName* parameter specified during the launch.

The optional Lync Edge Servers will be deployed in Workgroup mode. The local administrator password will be reset to the value specified for the *DomainAdminPassword* parameter when launching the stack. To connect and authenticate to these servers, use `administrator` for the user name.

Operating system patches are your responsibility and should be performed on a periodic basis.

Security Groups

A *security group* acts as a firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. You can modify the rules for a security group at any time. The new rules are automatically applied to all instances that are associated with the security group.

The security groups created and assigned to the individual instances as part of this solution are restricted as much as possible while allowing access to the various functions needed by Lync Server 2013. We recommend reviewing security groups to further restrict access as needed once the deployment is up and running.

Additional Resources

AWS services

- AWS CloudFormation
  http://aws.amazon.com/documentation/cloudformation/

- Amazon EBS
  - User guide:
    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 Route 53
  http://aws.amazon.com/documentation/route53/

- Amazon VPC
  http://aws.amazon.com/documentation/vpc/

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

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/

Tools

- Lync Server 2013 Planning Tool
  https://www.microsoft.com/en-us/download/details.aspx?id=36823

- Lync Server 2013 Capacity Calculator
  https://www.microsoft.com/en-us/download/details.aspx?id=36828

- Lync Server 2013 Stress and Performance Tool
  https://www.microsoft.com/en-us/download/details.aspx?id=36819

- Lync Server 2013 Stress Testing Guide
  https://www.microsoft.com/en-us/download/details.aspx?id=41935

- Load-balancing solutions in the AWS Marketplace
  https://aws.amazon.com/marketplace/

Associated Quick Start reference deployments

- Microsoft Active Directory on AWS
  https://docs.aws.amazon.com/quickstart/latest/active-directory-ds/

- Microsoft Remote Desktop Gateway on AWS
  https://docs.aws.amazon.com/quickstart/latest/rd-gateway/

- Additional reference deployments
  https://aws.amazon.com/quickstart/

Send Us Feedback

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

Document Revisions

Date	Change	In sections
May 2016	Added information about creating test users	Step 3
September 2015	In the sample templates, changed the default type for Active Directory and RD Gateway instances from **m3.xlarge** to **m4.xlarge** for better performance and price.	Step 2 (template customization table)
June 2015	Initial publication	—