



Test Lab Guide: Configure an Integrated Exchange, Lync, and SharePoint Test Lab

This document is provided “as-is”. Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2013 Microsoft Corporation. All rights reserved.

Test Lab Guide: Configure an Integrated Exchange, Lync, and SharePoint Test Lab

Joe Davies, Tony Trivison, and Mitch Duncan
Microsoft Corporation
Published: July 2013

Applies to: Exchange Server 2013, Lync Server 2013, SharePoint Server 2013

Summary: This paper contains step-by-step instructions to create a test lab containing integrated servers running Exchange Server 2013, Lync Server 2013, and SharePoint Server 2013.

Date	Description
September 30, 2013	Technical updates and links to an overview video and the Hyper-V configuration.
July 10, 2013	Initial publication

Contents

Contents	3
Introduction	3
Test Lab Guides	4
In this guide.....	4
Test lab overview.....	5
Hardware and software requirements	6
Required Test Lab Guides.....	7
Steps for Configuring the Exchange, Lync, and SharePoint Test Lab	7
Step 1: Configure the Windows Server 2012 Base Configuration Test Lab	7
Step 2: Install and configure a new server named SQL1	8
Step 3: Install SQL Server 2012 on SLQ1.....	9
Step 4: Install and configure a new client computer named CLIENT2.....	10
Step 5: Install and configure Exchange Server 2013 on EX1.....	11
Step 6: Install and configure a new server named LYNC1.....	11
Step 7: Install Lync Server 2013 Standard Edition on LYNC1	12
Step 8: Install SharePoint Server 2013 on SP1	18
Step 9: Configure integration between EX1, LYNC1, and SP1.....	21
Snapshot the Configuration	25
Additional Resources	25

Introduction

To support integrated scenarios and solutions, servers must be able to request resources from each other in a secure way. Server-to-server authentication is a new feature of Exchange Server 2013, Lync Server 2013, and SharePoint Server 2013 that allows a server to request resources of another server on behalf of a user. This feature uses the industry standard Open Authorization (OAuth) 2.0 protocol. Server-to-server authentication enables many new scenarios such as eDiscovery, high-resolution user photos, and site mailboxes.

In order for a server to service an incoming resource request, it must trust the server that is making the request. To establish this trust, you must configure a server-to-server trust relationship. To enable all possible scenarios that utilize server-to-server authentication, this document contains instructions to configure two-way server-to-server trusts among all three servers.

For more information about integration between Exchange Server 2013, Lync Server 2013, and SharePoint 2013, see [Integration with SharePoint and Lync](#) and [Cross-product solutions with Exchange, Lync, and SharePoint Server](#).

Test Lab Guides



Test Lab Guides

Wanna make something of IT?

Microsoft Test Lab Guides (TLGs) are a set of documents that step you through the configuration and demonstration of a Microsoft technology or product in a standardized test lab environment, which starts with a common base configuration that mimics a simplified intranet and the Internet. TLGs are designed to be modular, extensible, and stackable to configure complex, multi-product solutions. TLGs make learning about products, technologies, and solutions easier by providing that crucial hands-on, “I built it out myself” experience.

For more information, see [Test Lab Guides](http://microsoft.com/testlabguides) at <http://microsoft.com/testlabguides>.

A TLG stack is a set of dependent TLGs that, when configured from the bottom of the stack, create a meaningful test lab configuration. This TLG is at the top of the following TLG stack:



In this guide

The paper describes how to configure a test lab consisting of servers running Exchange Server 2013, Lync Server 2013, and SharePoint Server 2013 by using five server computers and two client computers. After verifying that all three types of servers are working, you then configure server-to-server trust relationships between them. The resulting test lab can be used as a basis for scenarios and solutions that use a combination of Exchange Server 2013, Lync Server 2013, and SharePoint Server 2013, and Microsoft Office 2013.

Important

The following instructions configure an integrated test lab by using the minimum number of computers. Individual computers are needed to separate services provided on the network and to clearly show the desired functionality. This configuration is neither designed to reflect best practices nor does it reflect a desired or recommended configuration for a production network. The configuration, including IP addresses and all other configuration parameters, is designed only to work on a separate test lab network. Attempting to adapt this test lab

configuration to a pilot or production deployment can result in configuration or functionality issues. For information about how to deploy Exchange Server 2013 in a pilot or production environment, see [Planning and Deployment: Exchange 2013 Help](#). For information about how to deploy Lync Server 2013 in a pilot or production environment, see [Deployment for Lync Server 2013](#). For information about how to deploy SharePoint Server 2013 in a pilot or production environment, see [Install and deploy SharePoint 2013](#).

For a short video that describes the configuration of this test lab, see the [Configure an Integrated Exchange, Lync, and SharePoint Test Lab overview video](#).

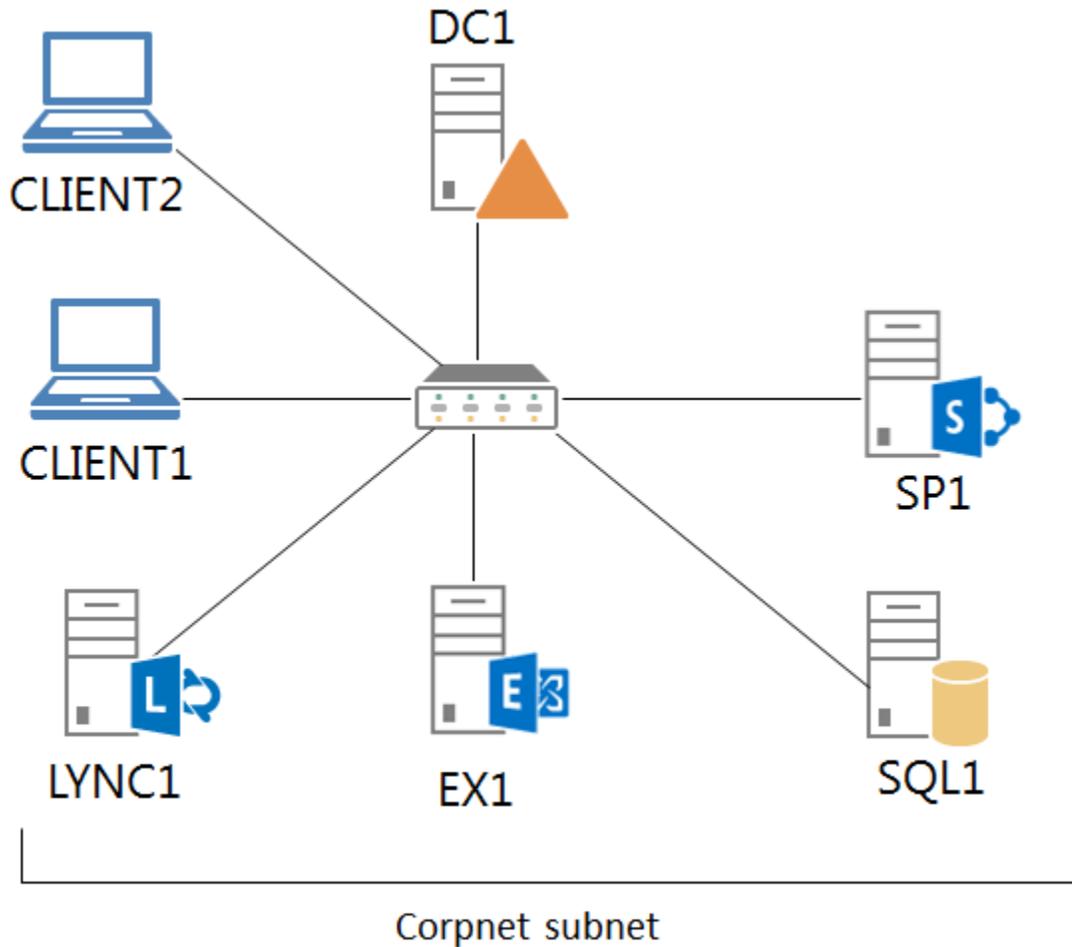
For information about how to configure this test lab in Hyper-V, see [Hosting the integrated Exchange, Lync, and SharePoint test lab with Windows Server 2012 Hyper-V](#).

Test lab overview

In this test lab, integrated functionality is deployed by using the following:

- One computer running Windows® Server® 2012 named DC1 that is configured as an intranet domain controller, Domain Name System (DNS) server, and DHCP server.
- One intranet member server running Windows Server 2012 named SQL1 that is configured as a SQL database server and enterprise root certification server.
- One intranet member server running Windows Server 2012 named SP1 that is configured as an enterprise root certification authority and a SharePoint Server 2013 web server.
- One intranet member server running Windows Server 2012 named EX1 that is configured as the Exchange Server 2013 email server.
- One intranet member server running Windows Server 2012 named LYNC1 that is configured as the Lync Server 2013 Standard Edition server.
- One member client computer running Windows 8 named CLIENT1.
- One member client computer running Windows 8 named CLIENT2.

The integrated test lab consists of a single subnet named Corpnet (10.0.0.0/24) that simulates a private intranet. Computers on the Corpnet subnet connect by using a hub or switch. See the following figure.



Hardware and software requirements

The following are required components of the test lab:

- The product disc or files for Windows Server 2012. For an evaluation copy, see [Download Windows Server 2012](#) in the TechNet Evaluation Center.
- The product disc or files for Windows 8. For an evaluation copy, see [Download Windows 8 Enterprise Evaluation](#).
- The product disc or files for Microsoft SQL Server 2012. For an evaluation copy, see [SQL Server 2012 Evaluation](#).
- The product disc or files for Exchange Server 2013. For an evaluation copy, see [Download Microsoft Exchange Server 2013](#).
- The product disc or files for Lync Server 2013. For an evaluation copy, see [Download Microsoft Lync Server 2013 Evaluation](#).
- The product disc or files for SharePoint Server 2013. For an evaluation copy, see [Download Microsoft SharePoint Server 2013](#).

- Five computers that meet the minimum hardware requirements for Windows Server 2012.
- Two computers that meet the minimum hardware requirements for Windows 8.

Required Test Lab Guides

Download or print these guides before you start.

- [Test Lab Guide: Windows Server 2012 Base Configuration](#)
- [Test Lab Guide Mini-Module: Basic PKI for Windows Server 2012](#)
- [SQL Server 2012 Test Lab Guide](#)
- [Test Lab Guide: Install Exchange Server 2013](#)
- [Test Lab Guide Mini-Module: Installing Microsoft Office Professional Plus 2013 on CLIENT1](#)

Steps for Configuring the Exchange, Lync, and SharePoint Test Lab

There are nine steps to follow when setting up the integrated test lab.

1. Set up the Windows Server 2012 Base Configuration test lab.
2. Install and configure a new server named SQL1.
3. Install SQL Server 2012 on SQL1.
4. Install and configure a new client computer named CLIENT2.
5. Install and configure Exchange Server 2013 on EX1.
6. Install and configure a new server named LYNC1.
7. Install Lync Server 2013 Standard Edition on LYNC1.
8. Install SharePoint Server 2013 on SP1.
9. Configure integration between EX1, LYNC1, and SP1.

Note

You must be logged on as a member of the Domain Admins group or a member of the Administrators group on each computer to complete the tasks described in this guide. If you cannot complete a task while you are logged on with an account that is a member of the Administrators group, try performing the task while you are logged on with an account that is a member of the Domain Admins group.

The following sections provide details about how to perform these steps.

Step 1: Configure the Windows Server 2012 Base Configuration Test Lab

Set up the Base Configuration test lab for the Corpnet subnet using the procedures in the “Steps for Configuring the Corpnet Subnet” section of the [Test Lab Guide: Windows Server 2012 Base Configuration](#).

In this procedure, you rename the server APP1 to SP1.

► **To rename the server APP1 to SP1**

1. On APP1, from the **Start** screen, click **Control Panel**.
2. In Control Panel, click **System and Security**. In the **System** group, click **See the name of this computer**.
3. Click **Change settings**, click **Change**, type **SP1** in **Computer name**, and then click **OK**.
4. Click **OK** and then restart the computer when prompted.

Add a public key infrastructure to the test lab using the procedures in the [Test Lab Guide Mini-Module: Basic PKI for Windows Server 2012](#), substituting SP1 for APP1 in the instructions. This makes SP1 a root certification authority for the contoso.com domain and configures autoenrollment of certificates.

Step 2: Install and configure a new server named SQL1

In this procedure, you install the Windows Server 2012 operating system and the latest updates on a new server named SQL1.

► **To install Windows Server 2012 on SQL1**

1. Start the installation of Windows Server 2012.
2. Follow the instructions to complete the installation, specifying Windows Server 2012 (full installation), the computer name SQL1, and a strong password for the local Administrator account.
3. Once the installation completes, log on using the local Administrator account.
4. Connect SQL1 to a network that has Internet access and run Windows Update to install the latest updates for Windows Server 2012.
5. Once the updates are complete, restart SQL1 and log on as the local Administrator.
6. Connect SQL1 to the Corpnet subnet.

In this procedure, you configure the TCP/IP properties on SQL1 so that it can join the corp.contoso.com domain.

► **To configure the TCP/IP properties on SQL1**

1. In Server Manager, click **Local Server** in the console tree. Click the link next to **Ethernet** in the Properties tile.
2. In the **Network Connections** window, right-click **Ethernet**, and then click **Properties**.
3. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
4. Select **Use the following IP address**. In **IP address**, type **10.0.0.4**. In **Subnet mask**, type **255.255.255.0**. In **Default Gateway**, type **10.0.0.1**. In **Preferred DNS server**, type **10.0.0.1**.
5. Click **Advanced**, and then click the **DNS** tab. In **DNS suffix for this connection**, type **corp.contoso.com**, click **OK** twice, and then click **Close**.
6. Close the **Network Connections** window and leave **Server Manager** open.

7. To check name resolution and network communication between SQL1 and DC1, open the **Command Prompt**. To do this, pressing the Windows button, type **cmd** or **command**, and choose when it appears in the search results.
8. In the Command Prompt window, type **ping dc1.corp.contoso.com**.
9. Verify that there are four replies from 10.0.0.1.
10. Close the Command Prompt window.

In this procedure, you join SQL1 to the corp.contoso.com domain.

▶ **To join SQL1 to the corp.contoso.com domain**

1. In **Server Manager**, click **Local Server** in the console tree. Click the link next to **Computer name** in the Properties tile.
2. In the **System Properties** dialog box, on the **Computer Name** tab, click **Change**.
3. In **Member of**, click **Domain**, type **corp.contoso.com**, and then click **OK**.
4. When you are prompted for a user name and password, type **User1** and its password, and then click **OK**.
5. When you see a dialog box welcoming you to the corp.contoso.com domain, click **OK**.
6. When you are prompted that you must restart the computer, click **OK**.
7. On the **System Properties** dialog box, click **Close**.
8. When you are prompted to restart the computer, click **Restart Now**.
9. After the computer restarts, click the **Switch User arrow icon**, and then click **Other User** and log on to the CORP domain with the User1 account.

Step 3: Install SQL Server 2012 on SQL1

Install and configure SQL Server 2012 on SQL1 as described in Steps 2, 3, and 4 of the [SQL Server 2012 Test Lab Guide](#), substituting SQL1 for APP1 in the instructions.

In this procedure, you configure an inbound rule in Windows Firewall with Advanced Security to allow incoming traffic to the SQL Server service.

▶ **To configure the Windows Firewall for an inbound rule**

1. On SQL1, log on using the CORP\User1 user account.
2. From the **Start** screen, click **Administrative Tools**, and then double-click **Windows Firewall with Advanced Security**.
3. In the tree pane, click **Inbound Rules**, right-click **Inbound Rules**, and then click **New Rule**.
4. On the Rule Type page, click **Port**, and then click **Next**.
5. On the Protocols and Ports page, type **1433-1434** in **Specific local ports**, and then click **Next**.
6. On the **Action** page, click **Next**.
7. On the **Profile** page, click **Next**.
8. On the **Name** page, type **SQL Server TCP ports** in **Name**, and then click **Finish**.

Step 4: Install and configure a new client computer named CLIENT2

First, install Windows 8 on CLIENT2.

▶ To install the operating system on CLIENT2

1. Start the installation of Windows 8 Enterprise.
2. When you are prompted for a PC name, type **CLIENT2**.
3. When you are prompted by the Settings dialog, click **Use express settings**.
4. At the Log on prompt, click **Don't want to sign in with a Microsoft account?** Click **Local account**.
5. When you are prompted for a user name, type **User2**. Type a strong password twice, type a password hint, and then click **Finish**.
6. Connect CLIENT2 to a network that has Internet access and run Windows Update to install the latest updates for Windows 8.
7. Connect CLIENT2 to the Corpnet subnet. Click **Yes, turn on sharing and connect to devices** when prompted.

Next, join CLIENT2 to the corp.contoso.com domain.

▶ To join CLIENT2 to the CORP domain

1. From the Start screen, right-click **Computer**, and then click **Properties**.
2. On the **System** page, click **Advanced system settings**.
3. In the **System Properties** dialog box, on the **Computer Name** tab, click **Change**.
4. In the **Computer Name/Domain Changes** dialog box, click **Domain**, type **corp.contoso.com**, and then click **OK**.
5. When you are prompted for a user name and password, type the user name and password for the CORP\User1 domain account, and then click **OK**.
6. When you see a dialog box that welcomes you to the corp.contoso.com domain, click **OK**.
7. When you see a dialog box that prompts you to restart the computer, click **OK**.
8. In the **System Properties** dialog box, click **Close**. Click **Restart Now** when prompted.
9. After the computer restarts, click the **Switch User** arrow icon, and then click **Other User**. Log on to the CORP domain with the User1 account.

Next, verify that intranet web and file share resources on SP1 can be accessed by CLIENT2.

▶ To test access to intranet resources

1. From the **Start** screen, click the **Internet Explorer** icon.
2. In the **Address** bar, type **http://sp1.corp.contoso.com/**, and then press ENTER. You should see the default IIS 8 web page for SP1.
3. From the **Start** screen or the desktop taskbar, click the **File Explorer** icon.
4. In the address bar, type **\\sp1\Files**, and then press ENTER.
5. You should see a folder window with the contents of the Files shared folder.
6. In the Files shared folder window, double-click the **Example.txt** file. You should see the contents of the Example.txt file.
7. Close the **example.txt - Notepad** and the **Files** shared folder windows.

Step 5: Install and configure Exchange Server 2013 on EX1

Follow the instructions in Steps 2-5 of [Test Lab Guide: Install Exchange Server 2013](#).

Install Microsoft Office Professional Plus 2013 on CLIENT2 as described in [Test Lab Guide Mini-Module: Installing Microsoft Office Professional Plus 2013 on CLIENT1](#), substituting CLIENT2 for CLIENT1 in the instructions.

Step 6: Install and configure a new server named LYNC1

In this procedure, you install the Windows Server 2012 operating system and the latest updates on a new server named LYNC1.

▶ To install Windows Server 2012 on LYNC1

1. Start the installation of Windows Server 2012.
2. Follow the instructions to complete the installation, specifying Windows Server 2012 (full installation), the computer name LYNC1, and a strong password for the local Administrator account.
3. Once the installation completes, log on using the local Administrator account.
4. Connect LYNC1 to a network that has Internet access and run Windows Update to install the latest updates for Windows Server 2012.
5. Once the updates are complete, restart LYNC1 and log on as the local Administrator.
6. Connect LYNC1 to the Corpnet subnet.

In this procedure, you configure the TCP/IP properties on LYNC1 so that it can join the corp.contoso.com domain.

▶ To configure the TCP/IP properties on LYNC1

1. In Server Manager, click **Local Server** in the console tree. Click the link next to **Ethernet** in the Properties tile.
2. In the **Network Connections** window, right-click **Local Area Connection**, and then click **Properties**.
3. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
4. Select **Use the following IP address**. In **IP address**, type **10.0.0.5**. In **Subnet mask**, type **255.255.255.0**. In **Default Gateway**, type **10.0.0.1**. In **Preferred DNS server**, type **10.0.0.1**.
5. Click **Advanced**, and then click the **DNS** tab. In **DNS suffix for this connection**, type **corp.contoso.com**, click **OK** twice, and then click **Close**.
6. Close the **Network Connections** window.
7. To check name resolution and network communication between LYNC1 and DC1, from the **Start** screen, type **cmd**, and then press **ENTER**.
8. In the Command Prompt window, type **ping dc1.corp.contoso.com**.
9. Verify that there are four replies from 10.0.0.1.

10. Close the Command Prompt window.

In this procedure, you join LYNC1 to the corp.contoso.com domain.

► To join LYNC1 to the corp.contoso.com domain

1. In Server Manager, click **Local Server** in the console tree. Click the link next to **Computer name** in the Properties tile.
2. In the **System Properties** dialog box, on the **Computer Name** tab, click **Change**.
3. In **Member of**, click **Domain**, type **corp.contoso.com**, and then click **OK**.
4. When you are prompted for a user name and password, type **User1** and its password, and then click **OK**.
5. When you see a dialog box welcoming you to the corp.contoso.com domain, click **OK**.
6. When you are prompted that you must restart the computer, click **OK**.
7. On the **System Properties** dialog box, click **Close**.
8. When you are prompted to restart the computer, click **Restart Now**.
9. After the computer restarts, click the **Switch User arrow icon**, and then click **Other User** and log on to the CORP domain with the User1 account.

Step 7: Install Lync Server 2013 Standard Edition on LYNC1

In this procedure, you install Lync Server 2013 on LYNC1, enable users in the Lync Server Control Panel, and verify the installation by sending instant messages between users.

► To install Lync Server 2013 prerequisites on LYNC1

1. Log on to LYNC1 as **CORP\User1**.
2. On the **Dashboard** screen of Server Manager, under **Configure this local server**, click **Add roles and features**.
3. Click **Next** three times to get to the server role selection screen.
4. In **Select server roles**, click **Web Server (IIS)**, and then click **Add Features**.
5. Click **Next**.
6. In the **Features** list, expand **.NET Framework 4.5 Features (Installed) > WCF Services (Installed)**.
7. Click **HTTP Activation**, and then click **Add Features** when prompted.
8. In the **Features** list, click **Media Foundation**.
9. Expand **Remote Server Administration Tools (Installed) > Role Administration Tools (Installed)**.
10. Select **AD DS and AD LDS Tools**.
11. In the **Features** list, select **Windows Identity Foundation 3.5**.
12. Click **Next** twice.
13. In **Role services**, under **Health and Diagnostics**, click **Logging Tools** and **Tracing**.
14. Under **Performance**, click **Dynamic Content Compression**.
15. Under **Security**, click **Client Certificate Mapping Authentication** and **Windows Authentication**.
16. Expand **Application Development** and click **ASP.NET 3.5**. Click **Add Features** when prompted.

17. Select **ASP.NET 4.5**. Click **Add Features** when prompted.
18. Under **Management Tools**, click **IIS Management Scripts and Tools**.
19. Click **Next**.
20. On the **Confirm installation selections page**, click **Specify an alternate source path**.
21. In the Path box, type **d:\sources\sxs**, or an equivalent drive where the Windows Server 2012 media is located. Click **OK**.
22. Click **Install**.
23. Click **Close** and restart the LYNC1 server.
24. Log on to LYNC1 as **CORP\User1**.

▶ **To prepare Active Directory**

1. On LYNC1, start the installation of Lync Server 2013 Standard Server.
2. Connect LYNC1 to a network that has Internet access and configure the TCP/IP protocol on the Ethernet network connection as needed. The Lync Server 2013 installer must download and install components from the Microsoft Download Center. For example, if the network that has access to the Internet uses DHCP, configure the Internet Protocol version 4 (TCP/IPv4) component from the properties of the Local Area Connection in the Network Connections folder to use automatic addressing and to automatically configure a DNS server.
3. From the desktop, click **Server Manager**.
4. In the console tree of **Server Manager**, click **Local Server**.
5. In the **Properties for DC1** pane, click **On** next to **IE Enhanced Security Configuration**.
6. In **Internet Explorer Enhanced Security Configuration**, click **Off** twice, and then click **OK**.
7. From the Start screen, click **Internet Explorer**.
8. In the address bar, type **http://www.microsoft.com/silverlight**, and then press ENTER.
9. On the **Microsoft Silverlight** web page, click **Download Now**.
10. When prompted, click **Run**.
11. In the **Install Silverlight** window, click **Install now**.
12. In the **Enable Microsoft Update** window, click **Next**.
13. In the **Installation successful** window, click **Close**.
14. Start the installation of Lync Server 2013 Standard Server by clicking **Setup.exe** in the Setup\AMD64 folder containing the Lync installation files.
15. Click **Yes** to install the Visual C++ x64 Runtime.
16. Connect LYNC1 to the Corpnet subnet and configure the TCP/IP protocol on the Ethernet as needed. For example, configure the Internet Protocol version 4 (TCP/IPv4) component from the properties of the Local Area Connection in the Network Connections folder to use the address 10.0.0.5 with a subnet mask of 255.255.255.0 and the preferred DNS server of 10.0.0.1.
17. On the Lync Server 2013 Installation Location page, click **Install**.
18. Accept the terms in the license agreement and click **OK**.

19. Click **Prepare Active Directory**.
20. Click **Yes** to install the Visual C++ Runtime.
21. On **Step 1: Prepare Schema**, click **Run**, and then click **Next**.
22. Click **Finish** to close the Prepare Schema page.
23. On **Step 3: Prepare Current Forest**, click **Run**, and then click **Next** twice.
24. Click **Finish** to close the Prepare Forest page.
25. On **Step 5: Prepare Current Domain**, click **Run**, and then click **Next**.
26. Click **Finish** to close the **Prepare Domain** page.
27. Click **Back** to return to the Lync Server 2013 Deployment Wizard.
28. On DC1, from the **Start** screen, click **Active Directory Administrative Center**.
29. In the console tree, click the arrow to expand **corp (local)**, and then click **Users**. This adds Users as a recent navigation link in the console tree.
30. Select user **User1**, right-click the user and choose **Properties** from the context menu.
31. Under the **Member Of** section, click **Add**.
32. In the **Select Groups** window, type **CSAdministrator** and then click **Check Names**.
33. Click **OK** twice.
34. Exit the Active Directory Administrative Center.

► **To add A and DNS SRV records**

1. From the DC1 **Start** screen, click **DNS**.
2. In console tree of DNS Manager, open DC1 > Forward Lookup Zones > corp.contoso.com > _tcp.
3. Right-click **_tcp**, and then click **Other new records**.
4. In **Resource Record Type**, click **Service Location (SRV)** in the resource record type list, and then click **Create Record**.
5. In **New Resource Record**, type the following:
 - a. **_sipinternal** in **Service**
 - b. **_tcp** in **Protocol**
 - c. **5061** in **Port number**
 - d. **lync1.corp.contoso.com.** in **Host offering this service**
6. Click **OK** to add the new record.
7. In **Resource Record Type**, click **Service Location (SRV)** in the resource record type list, and then click **Create Record**.
8. In **New Resource Record**, type the following:
 - a. **_sipinternalTLS** in **Service**
 - b. **_tcp** in **Protocol**
 - c. **5061** in **Port number**
 - d. **lync1.corp.contoso.com.** in **Host offering this service**
9. Click **OK** to add the new record.

10. In **Resource Record Type**, click **Done**.
11. In the console tree, right-click **corp.contoso.com**, and then click **New Host (A or AAAA)**.
12. In **New Host**, type the following:
 - a. **admin** in **Name**
 - b. **10.0.0.5** in **IP address**
13. Click **Add Host**, click **OK**, and then click **Done**.

► **To verify the A and DNS SRV records from CLIENT1**

1. Log on to **CLIENT1** with the CORP\User1 account.
2. From the Start screen, type **cmd**, and then press Enter.
3. At the command prompt, type **nslookup**, and then press ENTER.
4. Type **set type=srv**, and then press ENTER.
5. Type **_sipinternal._tcp.corp.contoso.com**, and then press ENTER. The output displayed for the record should be the following:
 - a. Server: dc1.corp.contoso.com
 - b. Address: 10.0.0.1
 - c. Non-authoritative answer: _sipinternal._tcp.corp.contoso.com SRV service location:
 - i. priority = 0
 - ii. weight = 0
 - iii. port = 5061
 - d. srv hostname = LYNC1.corp.contoso.com
 - e. LYNC1.corp.contoso.com = 10.0.0.5
6. Type **_sipinternaltls._tcp.corp.contoso.com**, and then press ENTER. The output displayed for the Transport Layer Security (TLS) record should be the following:
 - a. Server: dc1.corp.contoso.com
 - b. Address: 10.0.0.1
 - c. Non-authoritative answer: _sipinternaltls._tcp.corp.contoso.com SRV service location:
 - i. priority = 0
 - ii. weight = 0
 - iii. port = 5061
 - d. srv hostname = LYNC1.corp.contoso.com
 - e. LYNC1.corp.contoso.com = 10.0.0.5
7. Type **exit** and then press ENTER.
8. At the command prompt, type **ping lync1.corp.contoso.com** and then press ENTER. You should see the name resolved to 10.0.0.5.
9. At the command prompt, type **ping admin.corp.contoso.com** and then press ENTER. You should see the name resolved to 10.0.0.5.
10. Close the command prompt window.

▶ **To prepare the first Standard Edition server**

1. On server LYNC1, from the Lync Server 2013 Deployment Wizard, click **Prepare first Standard Edition server**, and then click **Next**.
2. Click **Finish** to close the Prepare single Standard Edition Server wizard.
3. From the Lync Server 2013 Deployment Wizard, click **Install Administrative Tools**.

▶ **To define and configure the topology**

1. On LYNC1, from the Start screen, click **Computer**, and then double-click the **C:** drive.
2. Right-click an empty area, point to **New**, and then click **Folder**.
3. Type **Files**, and then press ENTER.
4. Right-click the **Files** folder, point to **Share with**, and then click **Specific people**.
5. In the drop-down box, click **Everyone**, click **Add**, click the down arrow for the **Everyone** group in the **Permission Level** column, click **Read/Write**, click **Share**, and then click **Done**.
6. From the **Start** screen, click **Lync Server Topology Builder**.
7. Select **New Topology** and then click **OK**.
8. For **File name:** type **Contoso** and then click **Save**.
9. For **Primary SIP domain:** type **corp.contoso.com**.
10. Click **Next** twice.
11. For **Name**, type **Contoso**.
12. Click **Next** twice, click **Finish** and then click **Next**.
13. On the **Define the Front End pool FQDN** page:
 - a. For **Pool FQDN**, type **lync1.corp.contoso.com**
 - b. Select **Standard Edition Server**
14. Click **Next**.
15. On the **Select features** page, leave all features cleared and then click **Next** four times.
16. On the **Define the file store** page, under **File share** replace the word **share** with the word **Files**, and then click **Next**. Click **Finish**.
17. In Topology Builder, right-click **Lync Server** and click **Edit Properties**.
18. Click **Simple URLs**.
19. Under **Administrative access URL**, type **https://admin.corp.contoso.com**.
20. Under **Central Management Server**, select **lync1.corp.contoso.com Contoso**, and then click **OK**.
21. From the Topology Builder **Action** menu, select **Publish Topology**.
22. Click **Next** twice.
23. Click **Finish** to close the publishing wizard.

▶ **To install Lync Server 2013 core components**

1. From the Lync Server 2013 Deployment Wizard, click **Install or Update Lync Server System**.
2. For step 1, click **Run** and then click **Next**. Once completed, click **Finish**.
3. For step 2, click **Run** and then click **Next**. Once completed, click **Finish**.
4. For step 3, click **Run**.
5. Select **Default certificate** and then click **Request**.
6. Click **Next** five times until you reach the **Name and Security Settings** page.
7. For **Friendly name**, type **default** and click **Next** seven times.
8. On the **Executing Commands** page, click **Next**, then click **Finish**.
9. From the **Certificate Assignment** page, click **Next** twice.
10. Click **Finish**.
11. From the **Certificate Wizard** page, select the **OAuthTokenIssuer** certificate and then click **Request**.
12. Click **Next** five times until you reach the **Name and Security Settings** page.
13. For **friendly name**, type **OAuth** and click **Next** six times.
14. When **Task status** shows completed, click **Next** and then click **Finish**.
15. From the **Certificate Assignment** page, click **Next** twice.
16. Click **Finish** and then **Close** to close the Certificate Wizard.
17. From **step 4: Start Services**, click **Run** and then click **Next**.
18. When **Task status** shows completed, click **Finish**.

In this procedure, you enable users in the Lync Server Control Panel. You'll use these users to verify your Lync Server installation.

▶ **To enable users in the Lync Server Control Panel**

1. From the LYNC1 **Start** screen, choose **Lync Server Control Panel**. (If a security error appears, you may need to add https://localhost/Cscsp to the list of trusted sites in Internet Explorer by selecting **Tools > Internet options** and choosing the **Security** tab.)
2. Install Silverlight. (Like in the previous step, you may need to add the URL for the Silverlight download to your trusted sites in Internet Explorer.) Close and re-open the Lync Server control panel
3. Under **Top Actions**, click **Enable users for Lync Server**.
4. Click the **Enable Users** button.
5. Under **New Lync Server User**, click the **Add** button.
6. In **Select from Active Directory**, in the **Search** box, type **Janet Schorr**. When the name appears in the results, click **Ok**.
7. Repeat step 6 for **Chris Ashton**. Ensure that both users appear in the **Users** list.
8. For **Assign users to a pool**, choose **lync1.corp.contoso.com**.
9. For **Generate user's SIP URI**, keep the selection **Use user's email address**.

10. Click the **Enable** button to enable the users.

In this procedure, you have an instant-message conversation between the two users you enabled in the previous procedure.

▶ **To communicate between enabled Lync Server users**

1. Log on to CLIENT1 with the Janet Schorr account (CORP\janet).
2. Open the Lync client by choosing **Lync 2013** from the **Start** screen.
3. Type **janet@corp.contoso.com** as the **Sign-in address** on CLIENT1. Click **Sign In**. (Initial sign in can take some time.) When sign in completes, you'll see Janet's name in the Lync client and her availability.
4. Log on to CLIENT2 with the Chris Ashton account (CORP\chris). Upon completion, both users are signed in on separate client computers. (Ideally, you can view the client computers simultaneously.)
5. On CLIENT1, in the **Find someone** box of the Lync client, type **chris@corp.contoso.com**. When he appears in the list, double-click his contact. An instant-messaging window appears.
6. Type a message and send it. An IM window appears in CLIENT2 with the message sent from CLIENT1.
7. Type a reply on CLIENT2. You should be able to send messages back and forth between the two users.

Step 8: Install SharePoint Server 2013 on SP1

In this procedure, you install the prerequisite software components for SharePoint Server 2013 on SP1.

▶ **To install the SharePoint Server 2013 prerequisite software**

1. On SP1, log on using the CORP\User1 user account.
2. Connect SP1 to a network that has Internet access and configure the TCP/IP protocol on the Local Area Connection as needed. The SharePoint Server 2013 prerequisite installer must download and install components from the Microsoft Download Center. For example, if the network that has access to the Internet uses DHCP, configure the Internet Protocol version 4 (TCP/IPv4) component from the properties of the Local Area Connection in the Network Connections folder to use automatic addressing and to automatically configure a DNS server.
3. On SP1, navigate to the location that contains the SharePoint Server 2013 installation files and double-click **default.hta**.
4. On the **SharePoint 2013** page, click **Install software prerequisites**.
5. On the **Welcome to the Microsoft SharePoint Products Preparation Tool** page, click **Next**.
6. On the **License Terms for software product** page, review the terms, select the **I accept the terms of the License Agreement(s)** check box, and then click **Next**.
7. On the **Installation Complete** page, click **Finish**.

The computer might restart to install some of the prerequisites. After it does the Products Preparation Tool will run again and install the remaining prerequisites. The computer must be restarted again to install these prerequisites.

8. On the **Installation Complete** page, click **Finish**.

In this procedure, you prepare DC1 and SQL1 for the installation of SharePoint Server 2013 on SP1.

▶ To prepare DC1 and SQL1

1. On DC1, from the **Start** screen, click **Administrative Tools**, and then double-click **Active Directory Users and Computers**.
2. In the console tree, open **corp.contoso.com**, right-click **Users**, point to **New**, and then click **User**.
3. In the **New Object - User** dialog box, in **Full name**, type **SPFarmAdmin**, and in **User logon name**, type **SPFarmAdmin**.
4. Click **Next**.
5. In **Password** and in **Confirm password**, type **P@ssword1**.
6. Clear **User must change password at next logon**.
7. Select **Password Never Expires**.
8. Click **Next**, and then click **Finish**.
9. On SQL1, log on with the User1 account.
10. From the **Start** screen, click **SQL Server Management Studio**.
11. In **Connect to Server**, click **Connect**.
12. In **SQL Server Management Studio**, in the tree pane, open **Security**.
13. Right-click **Logins**, and click **New Login**.
14. In **Login - New**, type **CORP\SPFarmAdmin** in **Login name**.
15. In the **Select a page** pane, click **Server Roles**.
16. In the **Server Roles** pane, select **dbcreator** and **SecurityAdmin**, and then click **OK**.
17. Close **SQL Server Management Studio**.

In this procedure, you install SharePoint Server 2013 on SP1.

▶ To install SharePoint Server 2013

1. Connect SP1 to the Corpnet subnet and configure the TCP/IP protocol on the Local Area Connection as needed. For example, configure the Internet Protocol version 4 (TCP/IPv4) component from the properties of the Local Area Connection in the Network Connections folder to use the address 10.0.0.3 with a subnet mask of 255.255.255.0 and the preferred DNS server of 10.0.0.1.
2. Click the **Server Manager** icon. In **Security Information**, click **Configure IE ESC**.
3. In the **Internet Explorer Enhanced Security Configuration** dialog box, click **Off** in **Administrators**, click **Off** in **Users**, and then click **OK**.
4. Close **Server Manager**.

5. Navigate to the location that contains the SharePoint Server 2013 installation files and double-click **default.hta**.
6. On the **SharePoint 2013** page, click **Install SharePoint Server**.
7. On the **Enter Your Product Key** page, type your product key as needed, and then click **Continue**. For the 180-day trial version of SharePoint Server 2013, use the product key NQTMW-K63MQ-39G6H-B2CH9-FRDWJ.
8. On the **Read the Microsoft Software License Terms** page, review the terms, select the **I accept the terms of this agreement** check box, and then click **Continue**.
9. On the **Server Type** tab, click **Complete**, and then click **Install Now**.
10. When Setup finishes, a dialog box prompts you to complete the configuration of your server. Ensure that the **Run the SharePoint Products and Technologies Configuration Wizard now** check box is selected, and then click **Close** to start the configuration wizard.
11. On the **Welcome to SharePoint Products** page, click **Next**.
12. In the dialog box that notifies you that some services might need to be restarted during configuration, click **Yes**.
13. On the **Connect to a server farm** page, click **Create a new server farm**, and then click **Next**.
14. On the **Specify Configuration Database Settings** page, type **SQL1** in **Database server**, type **CORP\SPFarmAdmin** in **User name**, type **P@ssword1** in **Password**, and then click **Next**.
15. On the **Specify Farm Security Settings** page, type **P@ssphrase** in both **Passphrase** and **Confirm passphrase**, and then click **Next**.
16. On the **Configure SharePoint Central Administration Web Application** page, click **Next**.
17. On the **Completing the SharePoint Products Configuration Wizard** page, click **Next**.
18. On the **Configuration Successful** page, click **Finish**. Internet Explorer launches with a tab named Initial Farm Configuration Wizard.
19. In the **Help Make SharePoint Better** dialog box, click **No, I don't wish to participate**, and then click **OK**.
20. For **How do you want to configure your SharePoint farm?**, click **Start the Wizard**.
21. On the **Configure your SharePoint farm** page, in **Service account**, click **Use existing managed account**.
22. In **Services**, clear all the check boxes except the box next to **State Service**, and then click **Next**. The **Working on it** page might display for a while before it completes.
23. On the **Create Site Collection** page, in **Title and description**, type **Contoso Corporation** in **Title**, from the URL list select **"/**", and then click **OK**.
This step creates a team site at the URL <http://sp1>.
24. On the **This completes the Farm Configuration Wizard** page, click **Finish**. The Internet Explorer tab shows the SharePoint 2013 Central Administration site.

In this procedure, you click through the default SharePoint facilities and resources for the Contoso Corporation team site at <http://sp1/>.

► **To see the facilities of the default Contoso Corporation team site**

1. Log on to CLIENT1 with the CORP\User1 account.
2. Start Internet Explorer.
3. In the Address bar, type **http://sp1/** and then press ENTER.
You should see a SharePoint team site for the Contoso Corporation. The site might take a while to render.

Step 9: Configure integration between EX1, LYNC1, and SP1

In order for the EX1, LYNC1, and SP1 servers to participate in cross-product scenarios and solutions, they must be configured to trust each other through server-to-server authentication trusts.

First, to support secured connections, SP1 must be configured to use Secure Sockets Layer (SSL).

► **To configure SSL on SP1**

1. On SP1, from the **Start** screen, click **Administrative Tools**, and then double-click **IIS Manager**.
2. In the console tree, expand **SP1** and **Sites**, and then click the **SharePoint – 80** site.
3. In the **Actions** pane, under **Edit Site**, click **Bindings**.
4. In **Site Bindings**, click **Add**.
5. In **Add Site Binding**, under **Type**, select **https**.
6. In SSL certificate, select the certificate with the name sp1.corp.contoso.com, click **OK**, and then click **Close**.
7. Close the **IIS Manager**.

Next, you create the server-to-server trusts from SP1 and EX1 to LYNC1, so that LYNC1 trusts requests from both EX1 and SP1.

► **To create the server-to-server trusts from SP1 and EX1 to LYNC1**

1. On LYNC1, from the **Start** screen, click **Lync Server Management Shell**.
2. At the prompt, type the following commands and run them:

```
$x = (Get-CsCertificate -Type Default).Thumbprint
Set-CsCertificate -Identity global -Type OAuthTokenIssuer -Thumbprint $x
```

3. Create a C:\Scripts folder.
4. Copy the following into Notepad and save it as c:\scripts\s2sauth.ps1:

```
if ((Get-CsPartnerApplication -ErrorAction SilentlyContinue) -ne $Null)
{
    Remove-CsPartnerApplication app
}
```

```
$exch = Get-CsPartnerApplication microsoft.exchange -ErrorAction
SilentlyContinue

if ($exch -eq $null)
{
    New-CsPartnerApplication -Identity microsoft.exchange -MetadataUrl
    https://ex1.corp.constoso.com/autodiscover/metadata/json/1 -
    ApplicationTrustLevel Full
}
else
{
    if ($exch.ApplicationIdentifier -ne "00000002-0000-0ff1-ce00-
    000000000000")
    {
        Remove-CsPartnerApplication microsoft.exchange
New-CsPartnerApplication -Identity microsoft.exchange -MetadataUrl
    https://ex1.corp.contoso.com/autodiscover/metadata/json/1 -
    ApplicationTrustLevel Full
    }
    else
    {
        Set-CsPartnerApplication -Identity microsoft.exchange -
    ApplicationTrustLevel Full
    }
}

$shp = Get-CsPartnerApplication microsoft.sharepoint -ErrorAction
SilentlyContinue

if ($shp -eq $null)
{
    New-CsPartnerApplication -Identity microsoft.sharepoint -
    MetadataUrl https://sp1.corp.contoso.com/_layouts/15/metadata/json/ -
    ApplicationTrustLevel Full
}
```

```

else
{
    if ($shp.ApplicationIdentifier -ne "00000003-0000-0ff1-ce00-
000000000000")
    {
        Remove-CsPartnerApplication microsoft.sharepoint

        New-CsPartnerApplication -Identity microsoft.sharepoint -
MetadataUrl https://sp1.corp.contoso.com/_layouts/15/metadata/json/ -
ApplicationTrustLevel Full
    }
    else
    {
        Set-CsPartnerApplication -Identity microsoft.sharepoint -
ApplicationTrustLevel Full
    }
}

Set-CsOAuthConfiguration -ServiceName 00000004-0000-0ff1-ce00-
000000000000

```

5. In the Lync Server Management Shell, type the following commands:

```

cd c:\Scripts
.\s2sauth.ps1

```

Tip: If an error occurs when you run the PowerShell commands, it could be because of security settings in Internet Explorer that restrict browsing from server to server. You may need to add ex1.corp.contoso.com and sp1.corp.contoso.com to the list of **Trusted sites** in Internet Explorer. You can find these in **Tools > Internet options**, under the **Security** tab. Additionally, if you use self-signed certificates, you may have to import the certificates from EX1 and SP1 into the **Trusted Root Certification Authority\Certificate** folder of LYNC1's **Local Computer** certificate store.

Next, you create the server-to-server trusts from SP1 and LYNC1 to EX1, so that EX1 trusts requests from SP1 and LYNC1.

► **To create the server-to-server trusts from SP1 and LYNC1 to EX1**

1. On EX1, from the **Start** screen, click **Exchange Management Shell**.
2. At the Windows PowerShell prompt, type the following commands:

```

cd c:\'Program Files'\Microsoft\'Exchange Server'\V15\Scripts

```

```
.\Configure-EnterprisePartnerApplication.ps1 -AuthMetadataUrl  
https://lync1.corp.contoso.com/metadata/json/1 -ApplicationType Lync  
  
.\Configure-EnterprisePartnerApplication.ps1 -AuthMetadataUrl  
https://sp1.corp.contoso.com/_layouts/15/metadata/json/1 -  
ApplicationType SharePoint
```

By default, EX1 uses a self-signed certificate for its HTTPS connections, which is not trusted by SP1. In this procedure, you export the EX1 self-signed certificate and import it into the Trusted Root Certification Authorities\Certificates folder of the Local Computer certificates store on SP1.

► To install EX1's self-signed certificate on SP1

1. On EX1, from the **Start** screen, type **mmc**, and then click the **mmc** app.
2. Choose **Add/Remove Snap-in** from the **File** menu.
3. From **Add or Remove Snap-ins**, choose **Certificates**, and then click the **Add** button. A dialog appears. Choose **Computer account**. Click **Next** and then **Finish**.
4. Click **OK** to return to the console.
5. Expand **Certificates (Local Computer)**. Expand **Personal**. Select **Certificates**.
6. Right-click the certificate with the friendly name "Microsoft Exchange" (you may need to expand the snap in to see the friendly names), point to **All Tasks**, and then click **Export**.
7. In the Certificate Export Wizard, click **Next** twice. (Don't choose to export the private key or change the file format.)
8. Name the exported certificate file EX1.CER. Click **Next**.
9. Take note of where the file is saved and click **Finish** to complete the wizard.
10. Copy the EX1.CER file to a location on SP1.
11. On SP1, create a Certificates snap-in using steps 1 through 4 in this procedure.
12. In the console tree, expand **Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates**
13. Right-click **Certificates**, point to **All Tasks**, and then click **Import**.
14. In the Certificate Import Wizard, click **Next**.
15. On the File to Import page, click **Browse**, select the EX1.CER file stored on SP1, and then click **Next**.
16. Click **Finish**.

By default, SP1 does not run the Application Management service application, which is needed to configure application permissions for EX1. In this procedure, you add the Application Management service application to the farm running on SP1.

► To Create the Application Management service application

1. On SP1, from the **Start** screen, click **SharePoint 2013 Central Administration**.
2. Click **Application Management** in the Quick List, and then click **Manage service applications**.
3. Click **New**, and then click **App Management**.
4. For **Service Application Name**, type **AppMgmt**. For **Application Pool**, click **Use existing application pool**, select **SharePoint Web Services Default**, and then click **OK**.

Next, create the server-to-server trusts from EX1 and LYNC1 to SP1, so that SP1 trusts requests from EX1 and LYNC1.

► **To create the server-to-server trusts from EX1 and LYNC1 to SP1**

1. On SP1, from the **Start** Screen, click **SharePoint 2013 Management Shell**.
2. At the Windows PowerShell prompt, type the following commands:

```
New-SPTrustedSecurityTokenIssuer -MetadataEndpoint
    "https://ex1/autodiscover/metadata/json/1" -Name "Exchange Server"

$exchange=Get-SPTrustedSecurityTokenIssuer

$app=Get-SPAppPrincipal -Site http://sp1 -NameIdentifier
    $exchange.NameId

$site=Get-SPSite http://sp1

Set-SPAppPrincipalPermission -AppPrincipal $app -Site $site.RootWeb -
    Scope sitesubscription -Right fullcontrol -EnableAppOnlyPolicy

New-SPTrustedSecurityTokenIssuer -MetadataEndpoint
    "https://lync1.corp.contoso.com/metadata/json/1" -IsTrustBroker -Name
    "Lync Server"
```

Snapshot the Configuration

This completes the integrated test lab. To save this configuration so that you can quickly return to a working configuration from which you can test solutions or for your own experimentation and learning, do the following:

1. On all physical computers or virtual machines in the test lab, close all windows and then perform a graceful shutdown.
2. If your lab is based on virtual machines, save a snapshot of each virtual machine and name the snapshots **OfficeServer2013Integrated**. If your lab uses physical computers, create disk images to save the integrated test lab configuration.

Additional Resources

To provide the authors of this guide with feedback or suggestions for improvement, send an email message to modacontent@microsoft.com.

For more information about Exchange Server 2013, see the [Microsoft Exchange product information web page](#) and [Exchange Server for IT pros](#).

For more information about Lync Server 2013, see the [Lync product information web page](#) and [Lync Server for IT pros](#).

For more information about SharePoint Server 2013, see the [SharePoint 2013 product information web page](#) and [SharePoint for IT pros](#).

Microsoft strongly encourages you to develop and publish your own TLG content for SharePoint Server 2013, either in the TechNet Wiki (example: [Test Lab Guide: Demonstrate Remote Access VPNs](#)) or in your own publishing forum (example: [Test Lab Guide \(Part 1\) - Demonstrate TMG](#))

[PPTP, L2TP/IPsec and SSTP Remote Access VPN Server](#)). If you want to publish your own TLG content, see [Wiki: Creating and Publishing Test Lab Guide Content](#) for information about the types of content you can create and for links to guidance and templates.

For a list of additional Microsoft TLGs, see [Test Lab Guides](#) in the TechNet Wiki.