# Lab Answer Key: Module 13: Planning and configuring identify federation

# Lab: Planning and configuring identity federation

## Exercise 1: Deploying Active Directory Federation Services (AD FS) and Web Application Proxy

#### Task 1: Add DNS records required for AD FS

1. On LON-DC1, click **Start** and then click **Windows PowerShell**.
2. At the Windows PowerShell prompt, type the following command, and then press Enter:

Get-ADForest

1. Verify that the domain gsp.Adatumvsxxxx.virsoftlabs.com is listed as one of the UPN Suffixes for the local Active Directory Forest. That is the domain that will be federated with Office 365.
2. At the Windows PowerShell prompt, type the following command, and then press Enter:

certlm.msc

1. In the Certificates console for the local computer, in the left pane, expand Personal, and then select Certificates.

*Notice that in the lab environment, a publicly issued wildcard certificate (\*.virsoftlabs.com) for the virsoftlabs.com domain is already loaded on LON-DC1. Office 365 trusts this certificate when connecting to the AD FS public endpoint in the lab environment.*

1. Close the Certificates console.
2. At the Windows PowerShell prompt, type the following command, and then press Enter:

ping publicip.virsoftlabs.com

*The command returns the public IP address provided by the lab hosting platform, which you should use for this lab. External clients connect to this IP address to access the AD FS server through the AD FS Proxy. Note that the DNS name publicip.virsoftlabs.com is only used in this lab exercise, the DNS name is not used by the AD FS software.*

**Public IP Address : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. Type **IPConfig** and press Enter.

*The command returns the private IP address (172.16.0.10) of LON-DC1 where AD FS will be installed. Later in this exercise, you will configure the AD FS Proxy (on LON-WAP1) to forward AD FS network traffic to this IP address.*

1. Record the IPv4 address assigned to the server.

**Private IP Address : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. On LON-DC1, open Server Manager, click **Tools**, and then click **DNS**.
2. Expand **LON-DC1**, expand **Forward Lookup Zones**, and then click **Adatumvsxxxx.virsoftlabs.com**. You need to create a record in **Adatumvsxxxx.virsoftlabs.com,** not **gsp.Adatumvsxxxx.virsoftlabs.com.**
3. Right-click **Adatumvsxxxx.virsoftlabs.com** , and then click **New Host (A or AAAA)**.
4. In the New Host dialog box, leave the Name box empty, in the **IP address** box, type the External IP address provided by the hosting partner.
5. Click **Add Host**, and then click **OK**, and then click **Done**.

*Note: To configure AD FS, you would normally not leave the host name blank, but instead use fs.gsp.Adatumvsxxxx.virsoftlabs.com or adfs.gsp.Adatumvsxxxx.virsoftlabs.com. However, in the lab environment a single wildcard certificate \*.virsoftlabs.com is used, which only matches one subname level in front of virsoftlabs.com, not two subname levels.*

#### Task 2: Install and configure the AD FS server role

1. Sign in to the **LON-DC1** virtual machine as **ADATUM\Administrator** with a password of **Pa55w.rd**.
2. Click Start, right click **Windows PowerShell**, and then click **Run as Administrator**.
3. At the command prompt, type the following command and press Enter. This command creates the Key Distribution Services root key to generate group Managed Service Account passwords for the account that will be used later in this lab. You should receive a Guid value as a response to this command.

Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))

1. At the Windows PowerShell prompt, type the following command, and then press Enter:

Get-KdsRootKey

*The Add-KdsRootKey command creates a root key that is needed by the Key Distribution Service (KDS) to generate and maintain the password for a Group Managed Service Account (gMSA), instead of manually creating and maintaining a new service account to run the AD FS service. To allow for replication between multiple domain controllers, a new KDS root key is not available until 10 hours after creation. In a single DC environment, you can safely set the "effective time" 10 hours in the past, so that the root key is available immediately.*

1. In **Server Manager**, on the **Tools** menu, click **Services**.
2. In the **Services** console, ensure that **Microsoft Key Distribution Service (kdssvc)** is running. Start the service is not running
3. Close the **Services** console.
4. In Server Manager, click **Manage**, and then click **Add Roles and Features**. If you get a Server Manger message about collecting inventory data, click **OK**. Wait a minute and then try this step again.
5. In the Add Roles and Features Wizard, on the **Before you begin page**, click **Next**.
6. On the **Select installation type** page, click **Role-based or Feature-based installation**, and then click **Next**.
7. On the **Select destination server** page, click **Select a server from the server pool**, verify that the target computer is highlighted, and then click **Next**.
8. On the **Select server roles** page, click **Active Directory Federation Services**, and then click **Next**.
9. On the **Select features** page, click **Next**.
10. On the **Active Directory Federation Service (AD FS)** page, click **Next**.
11. On the **Confirm installation selections** page, click **Install**.
12. When installation completes, on the **Installation progress** page, click **Close**.
13. Click the exclamation mark icon on the toolbar, and then click **Configure the federation service on this server**.
14. In the **Active Directory Federation Services Configuration Wizard**, on the **Welcome** page, click **Create the first federation server in a federation server farm**, and then click **Next**.
15. On the **Connect to AD DS** page, click **Next**.
16. On the **Specify Service Properties** page, use the following settings, and then click **Next**:

* For **SSL Certificate**, click the wild card certificate provided by the hosting partner.
* For **Federation Service Name**, type **Adatumvsxxxx.virsoftlabs.com** , replacing xxxx with your unique Adatum number. Make sure to type **Adatumvsxxxx.virsoftlabs.com,** not **gsp.Adatumvsxxxx.virsoftlabs.com.**
* For **Federation Service Display Name**, type **Adatum Corporation**.

1. On the **Specify Service Account** page, select the option **Create a Group Managed Service Account**, for **Account Name** type **svc-ADFS**, and then click **Next**.
2. On the **Specify Configuration Database**, click **Create a database on this server using Windows Internal Database**, and then click **Next**.
3. On the **Review Options** page, click **Next**.

Note: You can ignore the warning about the root key replication.

1. Once the prerequisites check is complete, on the **Pre-requisite Checks** page, click **Configure**.

Note : Some warnings are expected to be shown.

1. When the configuration completes, on the **Results** page, click **Close**.
2. Restart the computer.

#### Task 3: Install the Web Application Proxy server role service

1. Sign in to the **LON-WAP1** virtual machine as **LON-WAP1\Administrator** with a password of **Pa55w.rd**.
2. On LON-WAP1, open **Windows PowerShell**.
3. At the **Windows PowerShell** prompt, type the following command, and then press Enter:

certlm.msc

1. In the **Certificates** console for the local computer, in the left pane, expand **Personal**, and then select **Certificates**.

*In the lab environment, the publicly issues wildcard certificate \*.virsoftlabs.com is already loaded on LON-WAP1.*

1. Close the **Certificates** console.
2. At the **Windows PowerShell** prompt, type the following command, and then press Enter:

ipconfig /all

*Notice that the LON-WAP1 server represents a Web Application Proxy (WAP) server in a corporate DMZ area. It is not configured with the DNS address of the internal domain. You must edit the local hosts file, so that the AD FS service name (Adatumvsxxxx.virsoftlabs.com, or fs.gsp.Adatumvsxxxx.virsoftlabs.com, etc.) can resolve to the AD FS server on the internal network.*

1. At the Windows PowerShell prompt, type the following command, and then press Enter:

notepad.exe C:\Windows\System32\drivers\etc\hosts

1. At the end of the hosts file, on a separate line, add the following text:

172.16.0.10 Adatumvsxxxx.virsoftlabs.com

1. Close **Notepad**, and click **Save** to save the changes to the hosts file.
2. Open **Internet Explorer** and browse to

https://Adatumvsxxxx.virsoftlabs.com/adfs/services/trust/mex.

1. Verify that Internet Explorer displays federation meta data in xml-format, and that Internet Explorer does not give a warning message about the security certificate.

*The result confirms that the LON-WAP1 server can now correctly resolve the Adatumvsxxxx.virsoftlabs.com name, and connect to the AD FS server on the internal network.*

1. Close **Internet Explorer**.
2. Click Start and then click **Server Manager**.
3. In Server Manager, click **Manage**, and then click **Add Roles and Features**.
4. In the Add Roles and Features Wizard, on the **Before you begin** page, click **Next**.
5. On the **Select installation type** page, click **Role-based or Feature-based installation**, and then click **Next**.
6. On the **Select destination server** page, click **Select a server from the server pool**, verify that the target computer is highlighted, and then click **Next**.
7. On the **Select server roles** page, click **Remote Access**, and then click **Next**.
8. On the Select features page, click **Next**.
9. On the Remote Access page, click **Next**.
10. On the **Select role services** page, click **Web Application Proxy**, in the popup window, click **Add Features**, and then click **Next**.
11. On the **Confirm installation selections** page, click **Install**.
12. When the installation is complete, on the **Installation progress** page, click **Close**.

#### Task 4: Configure the Web Application Proxy server

1. On LON-WAP1, in Server Manager, click **Tools**, and then click **Remote Access Management**.
2. In the Remote Access Management Console, in the left navigation pane, click **Web Application Proxy**. In the middle navigation pane, click **Run the Web Application Proxy Configuration Wizard**.
3. In the Web Application Proxy Configuration Wizard, on the **Welcome** page, click **Next**.
4. On the **Federation Server** page, use the following settings, and then click **Next**:

* Federation service name: **Adatumvsxxxx.virsoftlabs.com** , replacing xxxxx with your unique Adatum number. Make sure to type **Adatumvsxxxx.virsoftlabs.com,** not **gsp.Adatumvsxxxx.virsoftlabs.com.**
* User name: **Adatum\Administrator**
* Password: **Pa55w.rd**

1. On the **AD FS Proxy Certificate** page, select the **\*.virsoftlabs.com**  certificate, and then click **Next**.
2. On the **Confirmation** page, click **Configure**.
3. When the configuration is complete, on the **Results** page, click **Close**.

#### Task 5: Verify that the AD FS server is working

1. Switch to the LON-DC1 virtual machine.
2. In Server Manager, click **Tools**, and then click **Event Viewer**.
3. In Event Viewer, in the details pane, expand **Applications and Services Logs**, expand **AD FS**, and then click **Admin**.
4. In the **Event ID** column, verify that event ID **100** displays.

**Note:** If the federation server is configured properly, you should see a new event with event ID 100 in the Event Viewer Application log. This event verifies that the federation server was able to communicate successfully with the Federation Service.

1. On LON-DC1, open Internet Explorer and connect to **https://Adatumvsxxxx.virsoftlabs.com /adfs/fs/federationserverservice.asmx**, replacing *xxxx* with your unique Adatum number, and then press Enter.
2. If you get a message stating **There is a problem with this website's security certificate**, click **Continue to this website**.

**Note:** The expected output is a display of XML with the service description document. If this page displays, then Microsoft Internet Information Services (IIS) on the federation server is operational and serving pages successfully.

**Result**: After completing this exercise, you should have deployed the AD FS server in a federation server farm, and deployed the Web Application Proxy server to support AD FS.

## Exercise 2: Configuring federation with Microsoft Office 365

#### Task 1: Switch the Office 365 tenant to federated mode

1. Switch to the LON-DC1 virtual machine.
2. Open Internet Explorer, and then connect to **https://portal.office.com**.
3. Sign in as **holly@gsp.Adatumvsxxxx.virsoftlabs.com**  with the password ‘Pa55w.rd’.
4. Click **Admin**.
5. If you are connected to the previous Office 365 admin center, click the banner at the top of the page to access the new Office 365 admin center
6. Click **Users** and then click **Active Users**.
7. Click **Holly Spencer**, and then, in the **User name/Email Aliases** section, click **Edit**.
8. Change the primary email alias to **gspAdatumvsxxxx.onmicrosoft.com**. In the Warning window, click **Save**, and then click **Sign Out**.
9. Close Internet Explorer.

**Note:** Holly cannot change the gsp.Adatumvsxxxx.virsoftlabs.com to a federated domain if she is logged in using an account from this domain.

1. Click Start, and then click the **Windows PowerShell** icon.
2. At the Windows PowerShell prompt, type the following commands, pressing Enter at the end of each line:

Set-ExecutionPolicy Unrestricted -force Import-Module MSOnline

1. At the Windows PowerShell prompt, type the following command, and then press Enter:

$msolcred = Get-Credential

1. In the **Windows PowerShell Credential** dialog box, enter the following credentials, and then click **OK**:

* User name: **holly@gspAdatumvsxxxx.onmicrosoft.com**
* Password: the password ‘Pa55w.rd’

1. At the Windows PowerShell prompt, type the following command, and then press Enter:

Connect-MsolService -Credential $msolcred

1. At the Windows PowerShell prompt, type the following command, and then press Enter:

Get-MsolDomain

1. Verify that your lab domain, gsp.Adatumvsxxxx.virsoftlabs.com , is listed as **Verified and Managed**.

**Note:** If you were running this from a computer other than the AD FS federation server, you would need to use the **Set-MsolAdfsContext** to reference the AD FS server.

1. At the Windows PowerShell prompt, type the following command, and then press Enter:

Set-MsolAdfsContext -Computer LON-DC1.Adatum.com

*Note: The Set-MsolAdfsContext command sets up a remote connection to the AD FS server. The command is not really needed when the AD FS server is the local computer.*

1. At the Windows PowerShell prompt, type the following command, and then press Enter:

Convert-MsolDomainToFederated -DomainName gsp.Adatumvsxxxx.virsoftlabs.com

1. Verify that you get a **Successfully updated gsp.Adatumvsxxxx.virsoftlabs.com domain** message.
2. At the Windows PowerShell prompt, type the following command, and then press Enter:

Get-MsolFederationProperty -DomainName gsp.Adatumvsxxxx.virsoftlabs.com

**Note:** This command reports the status of the domain federation, and provides details of URLs and certificates.

**Result**: After completing this exercise, you should have enabled a federation trust between your on-premises Active Directory domain and Office 365 through your AD FS federation server, and you should have converted your domain for federated authentication in Office 365.

## Exercise 3: Verifying single sign-on (SSO)

#### Task 1: Verify SSO for internal users

1. Switch to **LON-CL1**.
2. On LON-CL1, open Microsoft Edge, and then connect to **https://portal.office.com**.
3. Type **beth@gsp.Adatumvsxxxx.virsoftlabs.com** as the user name, and then press Tab.
4. Verify that you are redirected to the Adatum sign in page.
5. Type **Pa55w.rd** as the password, and then press Enter.
6. Verify that you are connected to Office 365.
7. Close Microsoft Edge.

#### Task 2: Verify SSO for external users

1. On your local computer, open a Web browser (use an **InPrivate browsing** window, if possible).
2. In the Address bar, type **https://portal.office.com**, and then press Enter.
3. Type **grover@gsp.Adatumvsxxxx.virsoftlabs.com**  as the user name, and then press Tab.
4. Verify that you are redirected to the Adatum sign in page.
5. Type **Pa55w.rd** as the password, and then press Enter.
6. Review the Office 365 page for Grover Chambliss, and then close the Web browser window.

**Result**: After completing this exercise, you should have verified SSO authentication to Office 365 for a user on your corporate network and for a user on your host computer that is connected to the Internet.

©2016 Microsoft Corporation. All rights reserved.

The text in this document is available under the [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/legalcode), additional terms may apply. All other content contained in this document (including, without limitation, trademarks, logos, images, etc.) are **not** included within the Creative Commons license grant. 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.

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 are for illustration only and are fictitious. No real association is intended or inferred. Microsoft makes no warranties, express or implied, with respect to the information provided here.