AWS Federated Authentication with AD FS

**SPL-102 - Version 1.3.0**

© 2024 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. All trademarks are the property of their owners.

Note: Do not include any personal, identifying, or confidential information into the lab environment. Information entered may be visible to others.

Corrections, feedback, or other questions? Contact us at [*AWS Training and Certification*](https://support.aws.amazon.com/#/contacts/aws-training).

**Lab overview**

This lab takes you through the process of configuring Active Directory Federation Services (AD FS) with AWS Identity and Access Management (IAM), which permits Active Directory users and groups to access the AWS Management Console. You use the AWS support for Security Assertion Markup Language (SAML), an open standard used by many identity providers (IdPs). This feature activates federated single sign-on (SSO), which lets users sign in to the console or make programmatic calls to AWS application programming interfaces (APIs) by using assertions from a SAML-compliant IdP like AD FS. With identity federation, external identities or federated users are granted secure access to resources in the AWS account without requiring you to create IAM users.

**Important**

This lab uses Fleet Manager Remote Desktop, a feature of AWS Systems Manager, to connect to the Windows-based Amazon Elastic Compute Cloud (Amazon EC2) instances. As of the writing of this lab, Fleet Manager Remote Desktop supports bi-directional copy and paste to and from your local computer only in Chromium-based web browsers, such as Google Chrome.

If you use an alternate web browser, you can still complete the lab, but cannot copy text from the lab instructions to then paste into the RDP sessions.

OBJECTIVES

After completing this lab, you should be able to:

* Install and configure AD FS on a Windows server.
* Activate federated access to the AWS Management Console using an existing Active Directory server.
* Create new roles in IAM and map those to your federated users.
* Allow federated users to have access to the AWS Management Console.

TECHNICAL KNOWLEDGE PREREQUISITES

To successfully complete this lab, you should be familiar with basic Windows Server administration and also be highly fluent and conceptually solid with the techniques of federated identity and IdPs in general, SAML, Lightweight Directory Access Protocol (LDAP), Active Directory, and IAM.

DURATION

This lab takes approximately *60* minutes to complete.

**Note:** After you choose **Start Lab**, it takes approximately 10 minutes for the environment to deploy.

ICON KEY

Various icons are used throughout this lab to call attention to different types of instructions and notes. The following list explains the purpose for each icon:

* **Command:** A command that you must run.
* **Expected output:** A sample output that you can use to verify the output of a command or edited file.
* **Note:** A hint, tip, or important guidance.
* **Task complete:** A conclusion or summary point in the lab.

**Start lab**

1. To launch the lab, at the top of the page, choose **Start lab**.

 You must wait for the provisioned AWS services to be ready before you can continue.

1. To open the lab, choose **Open Console**.

You are automatically signed in to the AWS Management Console in a new web browser tab.

**Do not change the Region unless instructed.**

COMMON SIGN-IN ERRORS

**Error: You must first sign out**



If you see the message, **You must first log out before logging into a different AWS account:**

* Choose the **click here** link.
* Close your **Amazon Web Services Sign In** web browser tab and return to your initial lab page.
* Choose **Open Console** again.

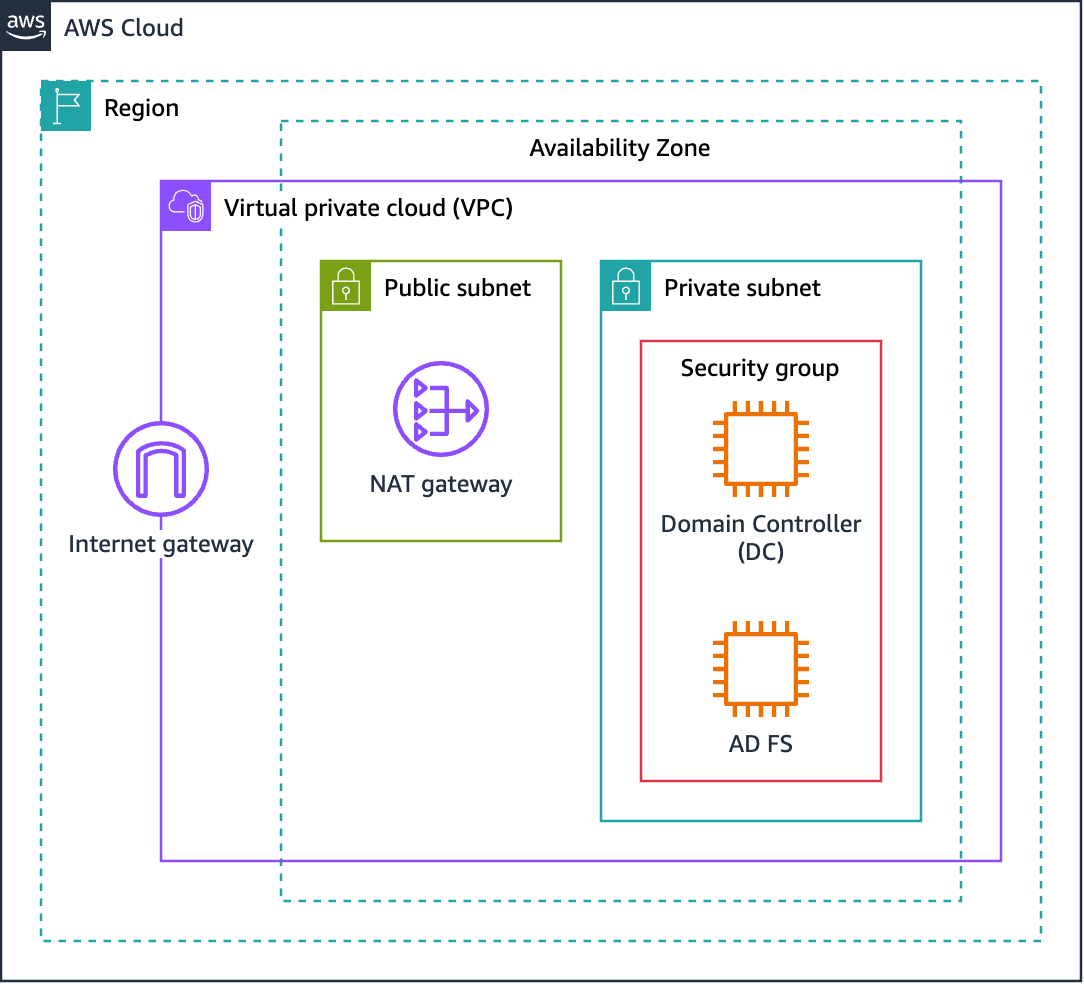
**Error: Choosing Start Lab has no effect**

In some cases, certain pop-up or script blocker web browser extensions might prevent the **Start Lab** button from working as intended. If you experience an issue starting the lab:

* Add the lab domain name to your pop-up or script blocker’s allow list or turn it off.
* Refresh the page and try again.

LAB ENVIRONMENT

When you start the lab, the following resources, including some supporting resources that are not shown, are deployed to the lab environment:

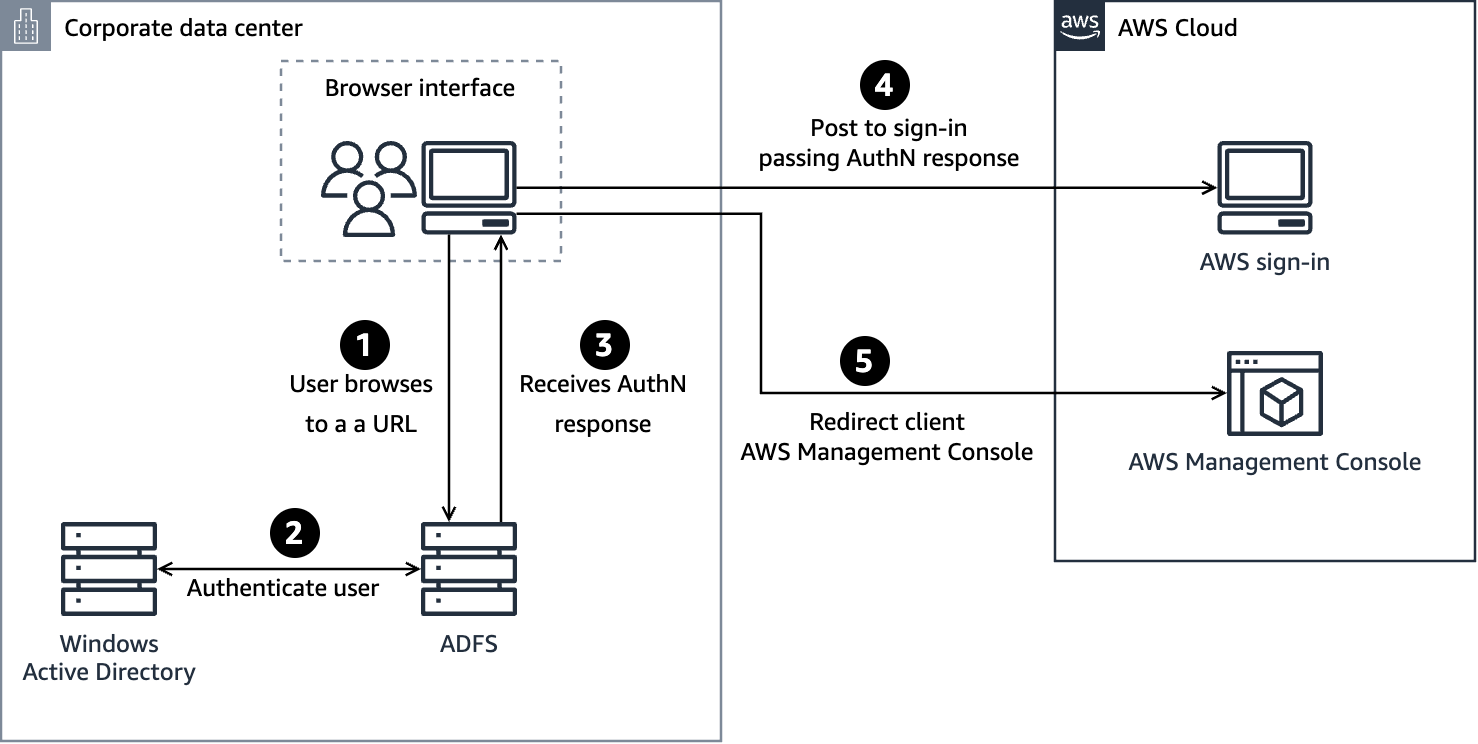


*Image description: The preceding diagram shows a virtual private cloud (VPC) with an internet gateway, one public subnet, and one private subnet. A NAT gateway is deployed to the public subnet to provide outbound internet access for the EC2 instances in the private subnet. Two EC2 instances—a Windows-based domain controller and an instance that you configure for AD FS—are deployed to the private subnet.*

In addition to deploying the domain controller instance, an Active Directory domain named *mydomain.local* is installed and configured as part of the lab environment build process.

AD FS FEDERATED AUTHENTICATION PROCESS

The following process details how a user authenticates to AWS using Active Directory and AD FS:



*Image description: The preceding diagram depicts the steps that occur when a user authenticates to the AWS Management Console. Additional details are in the following list.*

Step 1. The flow is initiated when a user browses to the AD FS sample site (*https://Fully.Qualified.Domain.Name.Here/adfs/ls/IdpInitiatedSignOn.aspx*) inside their domain. When you install AD FS, you get a new virtual directory named AD FS for your default website, which includes this page.

Step 2. The sign-on page authenticates the user against Active Directory. Depending on the user’s browser, they might be prompted for their Active Directory username and password.

Step 3. The user’s browser receives a SAML assertion in the form of an authentication response from AD FS.

Step 4. The user’s browser posts the SAML assertion to the AWS sign-in endpoint for SAML (*https://signin.aws.amazon.com/saml*). Behind the scenes, sign-in uses the AssumeRoleWithSAML API to request temporary security credentials and then constructs a sign-in URL for the AWS Management Console.

Step 5. The user’s browser receives the sign-in URL and is redirected to the console.

**Task 1: Creating Active Directory groups and users**

In this task, you use Fleet Manager Remote Desktop to connect to the domain controller (DC) instance. You then create the Active Directory groups that you eventually use to grant access to the AWS Management console for your users. Finally, you create an Active Directory user account that you use to configure AD FS.

TASK 1.1: CONNECTING TO THE DOMAIN CONTROLLER INSTANCE

In this task, you use Fleet Manager, a capability of AWS Systems Manager, to open a Remote Desktop Protocol (RDP) connection to the domain controller instance within your web browser.

**Learn more**

In this lab, you use Fleet Manager Remote Desktop to connect to the Windows-based instances in the private subnet using the Remote Desktop Protocol (RDP). Fleet Manager Remote Desktop, which is powered by NICE DCV, provides you with secure connectivity to your Windows Server instances directly from the Systems Manager console.

For additional information, refer to *NICE DCV* and *Connect to a Windows Server managed instance using Remote Desktop* in the **Additional resources** section at the end of this lab.

**Important**

As of the writing of this lab, Fleet Manager Remote Desktop supports bi-directional copy and paste to and from your local computer only in Chromium-based web browsers, such as Google Chrome.

1. At the top of the AWS Management Console, in the search bar, search for and choose

Systems Manager

.

1. In the navigation pane at the left of the page, under **Node Management**, choose **Fleet Manager**.
2. On the **Fleet Manager** page, in the **Managed Nodes** section, select the **DC** node.
3. At the top-right of the **Managed nodes** section, choose **Node actions**, **Connect**, **Connect with Remote Desktop**.
4. On the **Remote Desktop** page, in the **DC** connection details section:

* For **Authentication type**, select **User credentials** if it is not selected already.
* For **Username**, enter

administrator

.

* For **Password**, copy and paste the **AdministratorPassword** value that is listed to the left of these instructions.

1. Choose **Connect**.

**Note:** The *Fleet Manager - Remote Desktop* page has various tabs, depending on the number of open connections you currently have. In this lab, there are two tabs: one for *All sessions* and one with the EC2 instance ID for each connection.

1. Choose the tab with the EC2 instance ID to activate a larger view of the Remote Desktop connection that scales with the size of your web browser window.

**Note:** If you prefer to view the connection in full screen, choose the expand icon  at the top-right of the connection window.

You are now connected to the domain controller instance in your web browser.

1. If you are prompted with a **Networks** pop-up window asking: **Do you want to allow your PC to be discoverable by other PCs and devices on this network?**, choose **Yes**.

TASK 1.2: CREATING A GROUP FOR READ ONLY ACCESS TO AMAZON EC2

1. On the **DC** instance (IP address 10.0.0.10), in the search bar at the bottom of the window, search for and choose

Active Directory Users and Computers

.

**Note:** In some situations, the clipboard in the RDP session might not refresh with the contents that you copy from your local computer, such as text from the lab guide. In these instances, copy text inside of the RDP session, and then re-copy the text from your local computer.

1. Open the context (right-click) menu for **mydomain.local**, and then choose **New**, **Group**.
2. In the **New Object - Group** window, for **Group name**, enter

AWS-View-EC2

.

**Important**

When working with AD FS and SAML, group names and user names in Active Directory and IAM are case-sensitive.

1. Choose **OK**.
2. At the right side of the window, open (double-click) **mydomain.local**.
3. Open the context (right-click) menu for **AWS-View-EC2**, and then choose **Properties**.
4. Choose the **Members** tab.
5. Choose **Add**.
6. For **Enter the object names to select**, enter

Administrator

.

1. Choose **Check Names**.
2. Choose **OK**, and then choose **OK** again to close the windows.

TASK 1.3: CREATING A GROUP FOR READ ONLY ACCESS TO AMAZON S3

Next, create a second group to see how you can restrict user AWS Management Console access using Active Directory. In a production environment, you would assign users to groups as appropriate; however, for this lab you will use a single user and put them in multiple groups so you can see the functionality.

1. At the upper-right of the **Active Directory Users and Computers** window, choose the left arrow icon to return to the **mydomain.local** level.
2. Open the context (right-click) menu for **mydomain.local**, and then choose **New**, **Group**.
3. In the **Create Group** window, for **Group name**, enter

AWS-View-S3

.

1. Choose **OK**.
2. At the right side of the window, open (double-click) **mydomain.local**.
3. Open the context (right-click) menu for **AWS-View-S3**, and then choose **Properties**.
4. Choose the **Members** tab.
5. Choose **Add**.
6. For **Enter the object names to select**, enter

Administrator

.

1. Choose **Check Names**.
2. Choose **OK**, and then choose **OK** again to close the windows.

TASK 1.4: CREATING AN AD FS SERVICE ACCOUNT USER

Next, you create a user that you use later to configure AD FS.

1. At the upper-right of the **Active Directory Users and Computers** window, choose the left arrow icon to return to the **mydomain.local** level.
2. Open the context (right-click) menu for **mydomain.local**, and choose **New**, **User**.
3. In the **New Object - User** window, configure the following:

* For **First name**, enter

ADFSSVC

.

* For **User logon name**, enter

ADFSSVC

.

**Important**

When working with AD FS and SAML, group names and user names in Active Directory and IAM are case-sensitive.

1. Choose **Next**.
2. Clear **User must change password at next logon**.
3. For **Password** and **Confirm password**, enter

Mypa$$word123

.

1. Choose **Next**.
2. Choose **Finish**.
3. To close the remote session to the domain controller instance, choose **Actions**, **End session**.
4. In the **End session** pop-up window, choose **End session**.

**Task complete:** You have successfully created Active Directory user and groups that you use in upcoming tasks to configure AD FS.

**Task 2: Joining the AD FS instance to the domain**

In this task, you connect to the AD FS instance and join it to the *mydomain.local* domain.

TASK 2.1: CONNECTING TO THE AD FS INSTANCE

1. On the **Fleet Manager - Remote Desktop** page, choose **Add connection**.
2. In the **Add new session** pop-up window, for **Nodes**, select **ADFS**.
3. Choose **Add**.
4. On the **Remote Desktop** page, in the **ADFS** connection details section:

* For **Authentication type**, select **User credentials** if it is not selected already.
* For **Username**, enter

administrator

.

* For **Password**, copy and paste the **AdministratorPassword** value that is listed to the left of these instructions.

1. Choose **Connect**.
2. Choose the tab with the EC2 instance ID to activate a larger view of the Remote Desktop connection that scales with the size of your web browser window.

**Note:** If you prefer to view the connection in full screen, choose the expand icon  at the top-right of the connection window.

You are now connected to the AD FS instance in your web browser.

1. If you are prompted with a **Networks** pop-up window asking: **Do you want to allow your PC to be discoverable by other PCs and devices on this network?** Choose **yes**.

TASK 2.1: SETTING THE PREFERRED DNS SERVER

Next, configure the server’s preferred DNS server to use the lab domain controller.

1. On the **ADFS** instance (IP address 10.0.0.15), in the search bar at the bottom of the window, search for and choose

Windows PowerShell

.

1. To open the **Network Connections** window, run the following command:

C:\Windows\System32\control.exe ncpa.cpl

**Note:** You can press CTRL+V or open the context (right-click) menu to paste into Windows PowerShell.

1. In the **Network Connections** window, open the context (right-click) menu for the **Ethernet** icon, and then choose **Properties**.
2. In the **Ethernet Properties** window, open (double-click) **Internet Protocol Version 4 (TCP/IPv4)**.
3. Choose **Use the following DNS server addresses**.
4. For **Preferred DNS server**, enter

10.0.0.10

.

1. Choose **OK**.
2. Choose **OK**.
3. Close the **Network Connections** window.
4. To verify that you can now resolve the **mydomain.local** DNS name, return to the Windows PowerShell window and run the following command:

ping mydomain.local

**Expected output:** *mydomain.local* should resolve to *10.0.0.10*, which is the IP address of the domain controller.

TASK 2.3: CHANGING THE SERVER’S COMPUTER NAME AND JOINING IT TO THE DOMAIN

Next, change the computer name of the AD FS server to more easily identify it.

1. To open the **System Properties** window, run the following command:

systempropertiescomputername

1. In the **System Properties** window, choose **Change**.
2. In the **Computer Name/Domain Changes** window, configure the following:

* For **Computer name**, enter

adfsserver

.

* For **Member of**, choose **Domain**.
* For **Domain**, enter

mydomain.local

.

1. Choose **OK**.
2. In the **Windows Security** pop-up window configure the following:

* For **User name**, enter

administrator

.

* For **Password**, paste the **AdministratorPassword** value that is listed to the left of these instructions.

1. Choose **OK**.
2. In the welcome pop-up box, window **OK**.
3. In the restart notification pop-up window, choose **OK**.
4. Close any open windows.

The system prompts you to reboot the instance.

1. Choose **Restart Now**.

**Task complete:** You have successfully changed the computer name and joined it to the *mydomain.local* domain.

**Task 3: Adding the web server role and creating a self-signed certificate on AD FS**

In this task, you connect to the AD FS instance as the domain administrator, add the web server (IIS) role, and create a self-signed certificate.

TASK 3.1: CONNECTING TO THE AD FS INSTANCE

1. Wait 2 minutes for the AD FS instance to restart.
2. Reconnect to the AD FS instance with the following credentials:

* For **Username**, enter

mydomain\administrator

.

* For **Password**, enter the **AdministratorPassword** value that is listed to the left of these instructions.

If you prefer detailed steps to connect to the instance, expand the following **Detailed connection steps** section:

**Detailed connection steps**

TASK 3.2: ADDING THE WEB SERVER ROLE

1. On the **ADFS** instance (IP address 10.0.0.15), in the search bar at the bottom of the page, search for and choose

Server Manager

.

**Note:** It might take a 10–15 seconds for Server Manager to load completely.

1. If you see a window that says, **Try Windows Admin Center and Azure Arc today**, choose the **X** at the upper-right corner of the window to close it.
2. Choose **Add roles and features**.
3. On the **Before you begin** page, choose **Next**.
4. On the **Select installation type** page, choose **Next**.
5. On the **Select destination server** page, choose **Next**.
6. On the **Select server roles** page, select **Web Server (IIS)**.
7. In the **Add features that are required for Web Server (IIS)?** pop-up window, choose **Add Features**.
8. Choose **Next**.
9. On the **Select features** page, choose **Next**.
10. On the **Web Server Role (IIS)** page, choose **Next**.
11. On the **Select role services** page, choose **Next**.
12. On the **Confirm installation selections** page, choose **Install**.
13. Wait for the installation to finish, and then choose **Close**.

TASK 3.3: CREATING A SELF-SIGNED CERTIFICATE

1. At the upper-right of the window, on the **Tools** menu, choose **Internet Information Services (IIS) Manager**.
2. In the navigation pane at the left of the window, choose **ADFSSERVER**.
3. Open (double-click) **Server Certificates**.

**Note:** You may need to scroll down to see the Server Certificates icon.

1. In the **Actions** pane at the right of the window, choose **Create Self-Signed Certificate**.
2. In the **Create Self-Signed Certificate** window, configure the following:

* For **Specify a friendly name for the certificate**, enter

adfs

.

* For **Select a certificate store for the new certificate**, select **Web Hosting**.

1. Choose **OK**.
2. In the server certificates list, open the context (right-click) menu for the **adfs** certificate, and then choose **Export**.
3. In the **Export Certificate** window, configure the following:

* For **Export to**, enter

C:\Users\administrator.mydomain\Desktop\adfs.pfx

.

* For **Password**, enter

Mypa$$word123

.

* For **Confirm password**, enter

Mypa$$word123

.

1. Choose **OK**.
2. Close the **Internet Information Services (IIS) Manager** window.

**Task complete:** You have successfully added the web server role to the AD FS server and created a self-signed certificate.

**Task 5: Installing AD FS**

In this task, you add the Active Directory Federation Services role to the *ADFS* instance.

1. In the **Server Manager** window, choose **Add roles and features**.
2. On the **Before you begin** page, choose **Next**.
3. On the **Select installation type** page, choose **Next**.
4. On the **Select destination server** page, choose **Next**.
5. On the **Select server roles** page, select **Active Directory Federation Services**.
6. Choose **Next**.
7. On the **Select features** page, choose **Next**.
8. On the **Active Directory Federation Services (AD FS)** page, choose **Next**.
9. On the **Confirm installation selections** page, select **Restart the destination server automatically if required**.
10. When prompted to allow automatic restarts, choose **Yes**.
11. Choose **Install**.
12. Wait for the installation to complete, and then choose the **Configure the federation service on this server** link.

**Note:** If you closed the window before choosing the link, choose the notification icon in the Server Manager menu bar to open the next wizard.

1. On the **Welcome** page, choose **Create the first federation server in a federation server farm** if it is not already selected, and then choose **Next**.
2. On the **Connect to Active Directory Domain Services** page, verify that **mydomain\administrator** is listed.

**Note:** If \_mydomain\administrator is not listed, do the following:

* Choose **Change**.
* For **User name**, enter

mydomain\administrator

.

* For **Password**, enter the **WindowsPassword** value that is listed to the left of these instructions.
* Choose **OK**.

1. Choose **Next**.
2. On the **Specify Service Properties** page, choose **Import**.
3. Select the **adfs.pfx** certificate file that you created earlier, and then choose **Open**.
4. When prompted for the certificate password, enter

Mypa$$word123

 and then choose **OK**.

The **SSL Certificate** and **Federation Service Name** fields are updated.

1. For **Federation Service Display Name**, enter

AWSADFS

.

1. Choose **Next**.
2. On the **Specify Service Account** page, choose **Select**.
3. For **Enter the object name to select**, enter

ADFSSVC

.

1. Choose **Check Names**, and then choose **OK**.
2. For **Account Password**, enter

Mypa$$word123

.

1. Choose **Next**.
2. On the **Specify Configuration Database** page, choose **Next**.
3. On the **Review Options** page, review your options, and then choose **Next**.
4. On the **Pre-requisite Checks** page, choose **Configure**.

**Note:** When the installation is finished, you might see an error message related to SPN configuration. This is a known issue that sometimes occurs with AD FS setup. If you receive the error, open Windows PowerShell and run the following command:

setspn -a host/localhost adfssvc

This command registers the Service Principal Names. The success message should look like the following:

Checking domain DC=mydomain,DC=local

Registering ServicePrincipalNames for CN=ADFSSVC,DC=mydomain,DC=local

host/localhost

Updated object

1. In the AD FS Configuration Wizard, choose **Close**.
2. Close the **Server Manager** window.
3. Open **Windows PowerShell**.
4. To download the SAML metadata document for the AD FS instanceO, run the following commands separately :

cd ~\Desktop

wget https://adfsserver.mydomain.local/FederationMetadata/2007-06/FederationMetadata.xml -OutFile FederationMetadata.xml

1. From the desktop, open the **FederationMetadata.xml** file with a text editor, such as Notepad.
2. Copy the contents of the file to a text file on your personal desktop.
3. Save the text file as

FederationMetadata.xml

.

Next, you upload the *FederationMetadata.xml* file to the AWS Management Console.

**Task complete:** You have successfully installed AD FS on the ADFS instance.

**Task 6: Configuring AWS IAM to work with AD FS**

In this task, you create an identity provider in IAM.

1. At the top of the AWS Management Console, in the search bar, search for

IAM

 and open the link in a new web browser tab.

1. In the navigation pane, under **Access management**, choose **Identity providers**.
2. At the upper-right of the **Identity providers** page, choose **Add provider**.
3. On the **Add an Identity provider** page, in the **Configure provider** section, configure the following:

* For **Provider Type**, choose **SAML**.
* For **Provider Name**, enter

ADFS

.

1. Choose **Choose file**.
2. Browse to and select the **FederationMetadata.xml** file that you saved earlier.
3. Choose **Add provider**.

**Note:** If you receive an error when saving your changes, verify that there isn’t a hidden or null character at the end of the *FederationMetadata.xml* file you created.

**Task complete:** You have successfully configured IAM to work with AD FS.

**Task 7: Setting up AWS as a trusted relying party**

For this lab, two IAM roles have been created for you to use for logging into the AWS Management Console. The *AWS-View-EC2* role allows you to view all EC2 information, while the *AWS-View-S3* role allows you to view all S3 resources.

In this task, you configure the ADFS server to allow these roles to be assumed by domain users that are in the groups that you created previously. You then examine the AWS Management Console to see how access is restricted.

TASK 7.1: ADDING A RELYING PARTY TRUST

1. Return to your web browser tab with the RDP session to the AD FS instance (10.0.0.15).
2. To download the AWS relying party XLM file, run the following commands:

cd ~\Desktop

wget https://signin.aws.amazon.com/static/saml-metadata.xml -Outfile saml-metadata.xml

1. Open **Server Manager**.
2. In the left navigation pane, choose **Local Server**.
3. In the **PROPERTIES** section, for **IE Enhanced Security Configuration**, choose the **On** link.
4. For both **Administrators** and **Users**, choose **Off**.
5. Choose **OK**.
6. On the **Tools** menu at the upper-right of the window, choose **AD FS Management**.
7. In the **Actions** pane at the right, choose **Add Relying Party Trust**.

**Note:** You can also choose *Required: Add a trusted relying party* in the *Overview* section.

1. On the **Welcome** page, choose **Start**.
2. On the **Select Data Source** page, choose **Import data about the relying party from a file**.
3. Choose **Browse**.
4. Browse to and select the

C:\Users\administrator.MYDOMAIN\Desktop\saml-metadata.xml

 file you created previously.

1. Choose **Open**.
2. Choose **Next**.
3. On the **Specify Display Name** page, for **Display name**, enter

AWS Management Console Single Sign-On

.

1. Choose **Next**.
2. On the **Choose Access Control Policy** page, choose **Next**.
3. On the **Ready to Add Trust** page, choose **Next**.
4. On the **Finish** page, select **Configure claims issuance policy for the application**.
5. Choose **Close**.

TASK 7.2: CONFIGURING CLAIM RULES FOR THE AWS RELYING PARTY

In this section, you add and configure claim rules, which ensure that elements such as NameId, RoleSessionName, and Roles are added to the SAML authentication response. AWS requires these elements; AD FS does not provide them by default.

1. In the **AD FS Management** area of Server Manager, in the left navigation pane, choose the **Relying Party Trusts** folder.

**Note:** To access the AD FS Management area of Server Manager, on the **Tools** menu, choose **AD FS Management**. The **Tools** menu is at the upper-right corner of the Server Manager dashboard.

1. In the **Actions** pane at the right, choose **Edit Claim Issuance Policy**.
2. Choose **Add Rule**.

**Adding a new claim rule: *Transform an Incoming Claim***

1. For **Claim rule template**, choose **Transform an Incoming Claim**.
2. Choose **Next**.
3. On the **Configure Claim Rule** page, configure the following:

* For **Claim rule name**, enter

Name ID

.

* For **Incoming claim type**, choose **Windows account name**.
* For **Outgoing claim type**, choose **Name ID**.
* For **Outgoing name ID format**, choose **Persistent Identifier**.

1. Choose **Finish**.

**Adding a new claim rule: *Send LDAP Attributes as Claims***

1. Choose **Add Rule** again.
2. For **Claim rule template**, choose **Send LDAP Attributes as Claims**.
3. Choose **Next**.
4. On the **Configure Claim Rule** page, configure the following:

* For **Claim rule name**, enter

RoleSessionName

.

* For **Attribute store**, choose **Active Directory**.
* For **LDAP Attribute**, choose **SAM-Account-Name**.
* For **Outgoing Claim Type**, enter

https://aws.amazon.com/SAML/Attributes/RoleSessionName

.

1. Choose **Finish**.

**Adding a new claim rule: *Send Claims Using a Custom Rule* to get AD groups**

1. Choose **Add Rule** for the third time.
2. For **Claim rule template**, choose **Send Claims Using a Custom Rule**.
3. Choose **Next**.
4. On the **Configure Claim Rule** page, configure the following:

* For **Claim rule name**, enter

Get AD Groups

.

* For **Custom rule**, copy and paste the following:

c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"] => add(store = "Active Directory", types = ("http://temp/variable"), query = ";tokenGroups;{0}", param = c.Value);

**Note:** This rule uses the standard Active Directory schema to identify user groups from Active Directory and pass them to IAM.

1. Choose **Finish**.
2. Leave the **Edit Claim Issuance Policy** window open.

**Adding a new claim rule: *Send Claims Using a Custom Rule* to get IAM roles**

1. Return to your web browser tab with the AWS Management Console.
2. At the top of the AWS Management Console, in the search bar, search for and choose

IAM

.

1. In the navigation pane, choose **Identity providers**.
2. On the **Identity providers** page, choose the **ADFS** link to view its details.
3. On the **ADFS** page, in the **Summary** section, copy the **ARN** value and save it to your favorite text editor.

 The value should look similar to the following: *arn:aws:iam::111122223333:saml-provider/ADFS*

1. In the navigation pane, choose **Roles**.
2. Choose the link for the **AWS-View-EC2** role to view its details.
3. On the **AWS-View-EC2** page, in the **Summary** section, copy the **ARN** value and save it to your favorite text editor.

 The value should look similar to the following: *arn:aws:iam::111122223333:role/AWS-View-EC2*

1. In your text editor, delete **View-EC2** from the end of the role ARN.

**Expected result:** The value should now look similar to the following: *arn:aws:iam::111122223333:role/AWS-*

1. Return to your web browser tab with the RDP session to your AD FS instance.
2. In the **Edit Claim Issuance Policy** window, choose **Add Rule**.

**Note:** If you closed the Edit Claim Issuance Policy window, follow these steps to open it:

* Within Server Manager, on the **Tools** menu, choose **AD FS Management**.
* In the left navigation pane, select the **Relying Party Trusts** folder.
* In the **Actions** pane at the right, select **Edit Claim Issuance Policy**.

1. For **Claim rule template**, choose **Send Claims Using a Custom Rule**.
2. Choose **Next**.
3. On the **Configure Claim Rule** page, configure the following:

* For **Claim rule name**, enter

Roles

.

* For **Custom rule**, copy and paste the following:
  + Replace the **SAMLARN** placeholder value with the **provider ARN** value you saved earlier.
  + Replace the **ROLEARN** placeholder value with the **role ARN** value that you saved earlier.

c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-"] => issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value = RegExReplace(c.Value, "AWS-", "SAMLARN,ROLEARN"));

**Expected result:** The custom rule text should now look similar to the following:

c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-"] => issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value = RegExReplace(c.Value, "AWS-", "arn:aws:iam::111122223333:saml-provider/ADFS,arn:aws:iam::111122223333:role/AWS-"));

1. Choose **Finish**.
2. Choose **OK**.
3. Close the **AD FS Management** window.
4. Close **Server Manager**.

**Activating the AD FS sign-on page**

1. Open **Windows PowerShell**.
2. To activate the AD FS sign-on page, run the following command:

Set-AdfsProperties -EnableIdpInitiatedSignonPage $true

**Task complete:** You have successfully configured AD FS and IAM to allow Active Directory users to sign-in to the AWS Management Console with designated permissions.

**Task 8: Testing the configuration by signing in to the AWS Management Console**

Now that you have configured the connection between AD FS and IAM, verify that you can sign in to the AWS Management console with an Active Directory user account. After you sign in, validate that the permissions you expect to have as that user.

1. On the **ADFS** instance, open **Google Chrome**.
2. If you are prompted to sign in to Chrome, choose **Don’t sign in**.
3. If you are prompted to set Chrome as the default web browser, choose **Skip**.

**Note:** You may use any browser; however, you may need to change security configuration settings based on the browser type.

1. Copy and paste the following URL in the address bar:

https://localhost/adfs/ls/IdpInitiatedSignOn.aspx

**Note:** If prompted that the connection is not private, choose **Advanced**, and then choose the **Proceed to localhost (unsafe)** link.

1. Select **Sign in to one of the following sites**, and then choose **Sign in**.
2. On the **AWSADFS** sign in page, enter the following values:

* For **User name**, enter

mydomain\Administrator

.

* For **Password**, enter the **AdministratorPassword** value that is listed to the left of these instructions.

1. Choose **AWS-View-EC2**.
2. Choose **Sign in**.

You are now signed in to the AWS Management Console as **AWS-View-EC2/Administrator**.

1. At the top of the AWS Management Console, in the search bar, search for and choose

EC2

.

1. In the navigation pane, under **Instances**, choose **Instances**.

**Expected result:** You should see two instances listed. This is because the role you assumed has read access to EC2.

**Note:** If you do not see any resource information on the EC2 dashboard, verify that the Region you are using on the console within the RDP session matches the **AwsRegionName** value that is listed to the left of these instructions.

1. At the top of the AWS Management Console, in the search bar, search for and choose

S3

.

1. In the navigation pane at the left of the page, choose **Buckets**.

**Expected result:** Since you logged in with a role that only allows you to view EC2 information, you are denied access to view any information about Amazon S3.

1. Copy and paste the following URL in the address bar to return to the localhost AD FS login page:

https://localhost/adfs/ls/IdpInitiatedSignOn.aspx

1. Choose **Sign in**.
2. Choose **AWS-View-S3**.
3. Choose **Sign In**.
4. At the top of the AWS Management Console, in the search bar, search for and choose

EC2

.

1. In the navigation pane, under **Instances**, choose **Instances**.

**Expected result:** You should see a warning indicating *You are not authorized to perform this operation.* This is because the role you signed in with does not have permission to use EC2.

1. At the top of the AWS Management Console, in the search bar, search for and choose

S3

.

**Expected result:** You should see several buckets listed.

By creating IAM roles and AD FS groups, you can assign specific permissions to users to limit their access to appropriate parts of the AWS Management Console.

For reference, see the following detailed blog article on this topic (with Windows Server 2008 R2): <https://blogs.aws.amazon.com/security/post/Tx71TWXXJ3UI14/Enabling-Federation-to-AWS-using-Windows-Active-Directory-ADFS-and-SAML-2-0>

**Task complete:** You have successfully validated that you can sign in to the AWS Management Console as an Active Directory user and assume an IAM role that grants specific permissions to AWS services.

**Conclusion**

You have successfully done the following:

* Installed and configured AD FS.
* Added an AD FS server to a Windows domain.
* Configured AWS as a trusted relying party.
* Added sample rules.
* Tested the configuration.

**End lab**

Follow these steps to close the console and end your lab.

1. Return to the **AWS Management Console**.
2. At the upper-right corner of the page, choose **AWSLabsUser**, and then choose **Sign out**.
3. Choose **End lab** and then confirm that you want to end your lab.

**Additional resources**

* [NICE DCV](https://docs.aws.amazon.com/dcv/latest/adminguide/what-is-dcv.html)
* [Connect to a Windows Server managed instance using Remote Desktop](https://docs.aws.amazon.com/systems-manager/latest/userguide/fleet-rdp.html)