AppStream2.0 with ADFS Integration Automation Guide

**Author’s Name** Vickie Hsu

**Issue Date** 10th April 2018

**Document Version** 0.1

Table of Contents

[Introduction 4](#_Toc511138921)

[Solution Overview 5](#_Toc511138922)

[Deployment 7](#_Toc511138923)

[Preparation 7](#_Toc511138924)

[Infrastructure Deployment 7](#_Toc511138925)

[AppStream2.0 Deployment 8](#_Toc511138926)

[Testing/Verification 9](#_Toc511138927)

[Appendix A 11](#_Toc511138928)

# Introduction

The solution described in this document is an automated deployment solution for AppStream 2.0 with Active Directory identity federation to provide users with single sign-on access to AppStream 2.0.

# Solution Overview

After setting up SAML 2.0 federation for AppStream 2.0, users can browse to a specially crafted (AD FS RelayState) URL and be taken directly to their AppStream 2.0 applications.

When users sign in with this URL, they are authenticated against Active Directory. After they are authenticated, the browser receives a SAML assertion as an authentication response from AD FS, which is then posted by the browser to the AWS sign-in SAML endpoint. Temporary security credentials are issued after the assertion and the embedded attributes are validated. The temporary credentials are then used to create the sign-in URL. The user is redirected to the AppStream 2.0 streaming session. The following diagram shows the process:

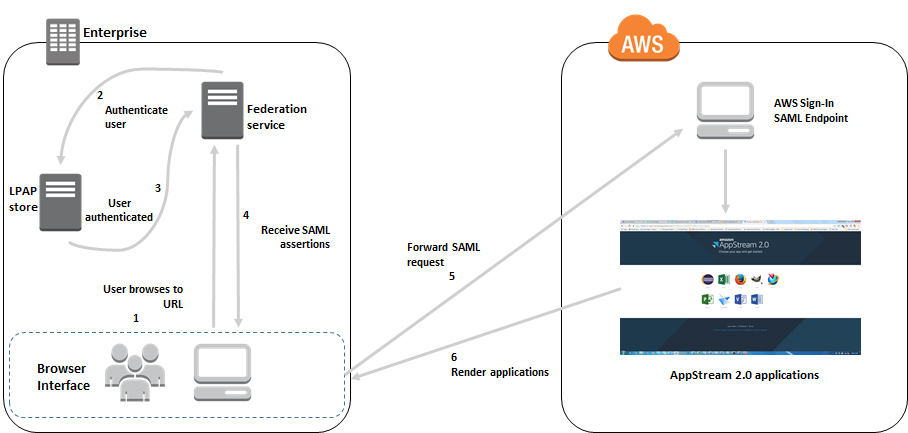


Figure 1. AppStream2.0 Single Sign-On

1. The user browses to https://applications.exampleco.com. The sign-on page requests authentication for the user.
2. The federation service requests authentication from the organization’s identity store.
3. The identity store authenticates the user and returns the authentication response to the federation service.
4. On successful authentication, the federation service posts the SAML assertion to the user’s browser.
5. The user’s browser posts the SAML assertion to the AWS Sign-In SAML endpoint (https://signin.aws.amazon.com/saml). AWS Sign-In receives the SAML request, processes the request, authenticates the user, and forwards the authentication token to the AppStream 2.0 service.
6. Using the authentication token from AWS, AppStream 2.0 authorizes the user and presents applications to the browser.

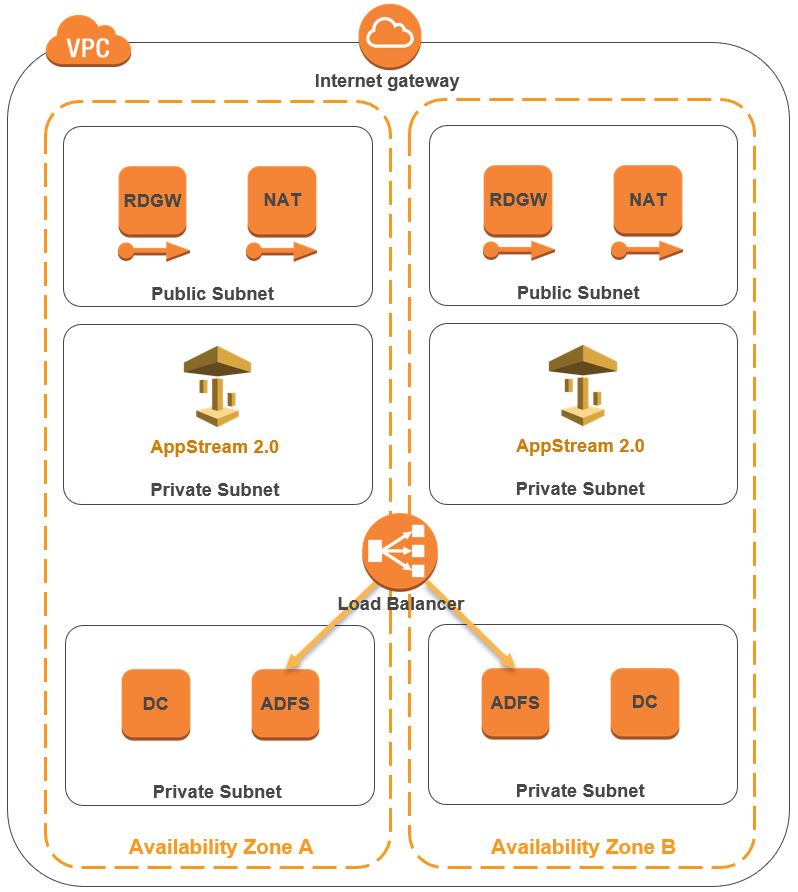


Figure 2. Highly available AppStream 2.0, AD and ADFS architecture.

# Deployment

The deployment is separated into two parts, Infrastructure and AppStream2.0 deployments.

Infrastructure Deployment - The Cloudformation templates perform the following tasks:

* Deploy VPC, subnets, Internet Gateway, DHCP options, NACLs, Security Groups, route tables,
* Deploy and configure NAT service.
* Create IAM instance profile, IAM policies, federated role and identify provider.
* Create self-signed SSL certificates for remote desktop connection.
* Deploy and configure AD, ADFS and Remote Desktop Gateway.
* Launch and configure load balancer and register ADFS instances with the load balancer.
* Create AD users and AD security groups.
* Configure SAML identity federation for single sign-on to the AppStream2.0 console.

AppStream2.0 Deployment - Powershell script performs the following tasks:

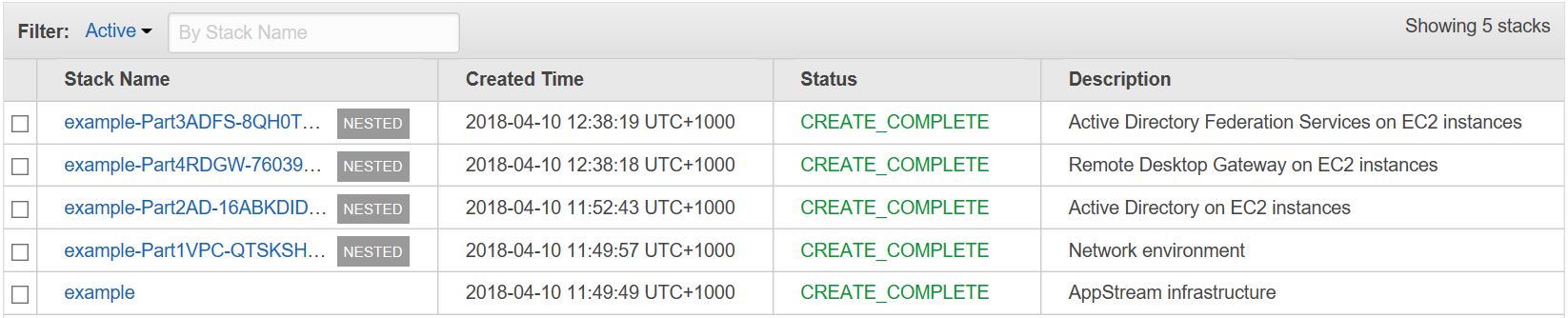
* Create a directory config in AppStream2.0.
* Deploy an Image Builder.
* Launch pre-signed Image Builder URL from the Internet Explore browser.
* Create a custom image from the Image Builder.
* Launch fleet and stack.
* Associate the stack with the fleet.

## Preparation

* Choose a region for the deployment, esnure the region supports AWS AppStream2.0 service.
* Create an EC2 key pair by following the instruction: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html#having-ec2-create-your-key-pair>

## Infrastructure Deployment

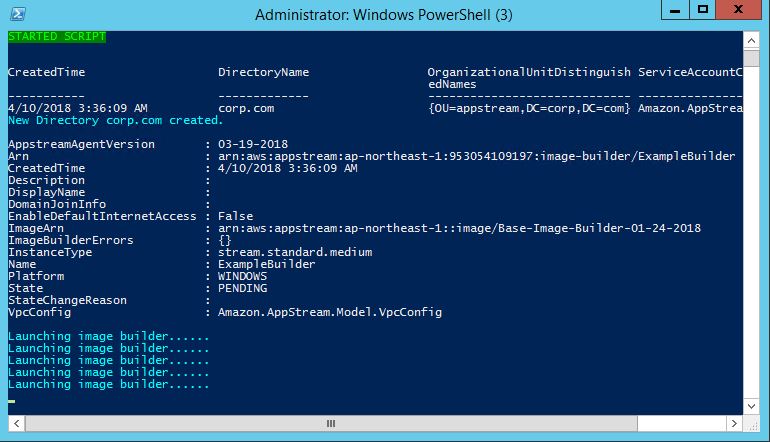
1. Log into AWS console. Select CloudFormation service.
2. In CloudFormation console, select **Create Stack**.
3. Choose **Upload a template to Amazon S3**. Choose **Browse**. Select the file .\AppStreamADFS\AppStreamInfra\AppStreamInfra.yml
4. Click on **Next** to provide a Stack name and the name of the Key Pair you created during the preparation. Click on **Next**.
5. Click on **Next** and **Create**. The deployment will take 1.5 hour to complete.



## AppStream2.0 Deployment

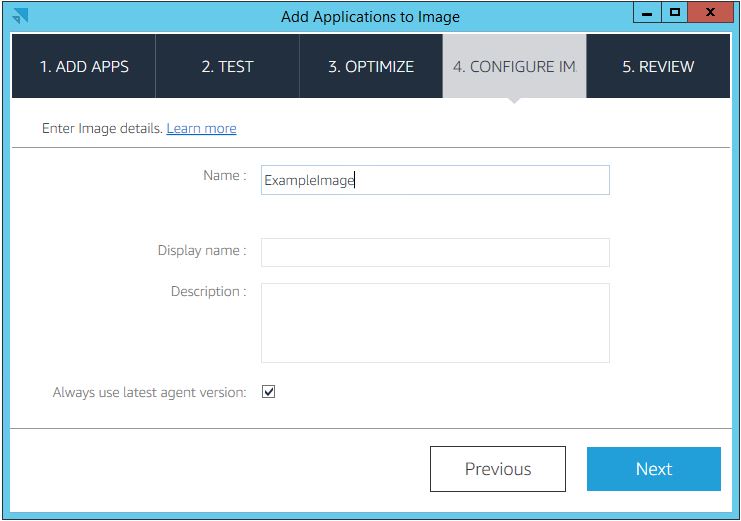
1. RDP into the RDGW01 using public IP address. The public IP address can be found in EC2 console. Log in with domain admin credential that you provided in CloudFormation template.
2. Upload the file .\AppStreamADFS\AppStreamBuild\AppStreamDeployment.ps1 to RDGW01. Open the file with PowerShell ISE. Modify the highlighted parameters.



1. Save the PowerShell file and open up Powershell command prompt (Run as administrator) and execute the script .\AppStreamDeployment.ps1
2. In about 8 minutes, a new AppStream 2.0 image builder is launched. (Do not close the Powershell command prompt.)
3. A new browser launched, connects to the AppStream 2.0 Image Builder. You can upload and install new applications. In this exercise, we will use notepad.
4. Click on **Image Assistant** icon on the desktop. Under Image Assistant, add the application notepad C:\Windows\System32\notepad.exe. Click on **Next.**
5. Click **Next**.
6. Click on **Launch** and **Continue**. Close browser.
7. Enter the name of the image. The name of the image must match with $GoldImageName parameter in the Powershell script. The display message in PowerShell command prompt also tells the name of the image should be. Remember it is case sensitive.

eg,

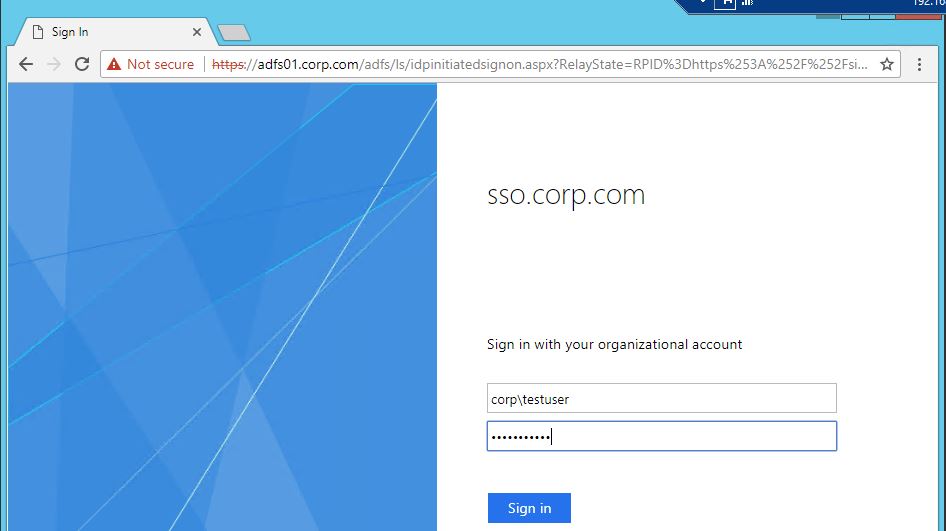
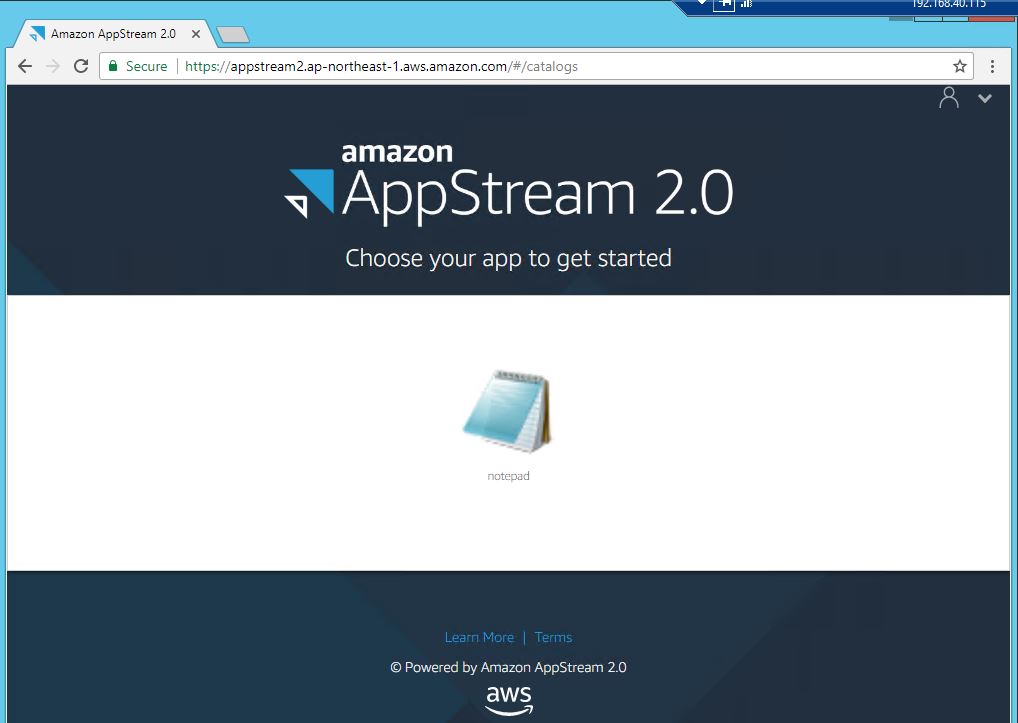




Click on **Next**.

1. Click on **Disconnect and Create Image**.
2. The snapshot process will take 10-15 minutes to complete. Wait for PowerShell command prompt to complete the rest of the build.

## Testing/Verification

1. From RDGW01 RDP into ADFS01. The IP address of ADFS01 can be found in EC2 console.
2. Follow Appendix A on how to generate the AppStream 2.0 RelayState URL.
3. Open up RelayState URL.
4. Log into AppStream2.0 with an AD account. By default, a test account is already created. User name: **corp\testuser** Password: **Password123**
5. After successful log in, click on Notepad icon. 
6. Log in with testuser account.



# Appendix A

**Create the AppStream 2.0 RelayState URL**

Use this tool to generate the URL: http://jackstromberg.com/adfs-relay-state-generator/

To generate the values, you need three pieces of information:

* IDP URL String
* Relying Party Identifier
* Relay State / Target App

IDP URL String

The IDP URL string is the URL you use to hit your AD FS sign-on page. For example:

https://<ADFSInstance>/adfs/ls/idpinitiatedsignon.aspx

In this configuration, use the following:

https://adfs01.example.com/adfs/ls/idpinitiatedsignon.aspx

Relying Party Identifier

This value is always the following:

https://signin.aws.amazon.com/saml

Relay State / Target App

This is the RelayState link to your AppStream 2.0 stack. The format for this URL is as follows:

https://appstream2.<region>.aws.amazon.com/saml?stack=Case\_Sensitive\_Stack\_Name&accountId=account\_id\_without\_hyphens

Ultimately, the URL looks like the following example, which is for us-east-1, with a stack name of ExampleStack, and an account ID of 012345678910. The stack name is case-sensitive.

https://appstream2.ap-northeast-1.aws.amazon.com/saml?stack=ExampleStack&accountId=012345678910