3 step building sample AWS Management Console federation site with ADFS

November 27th, 2014
AWS Professional Services
Yuki, Chiba

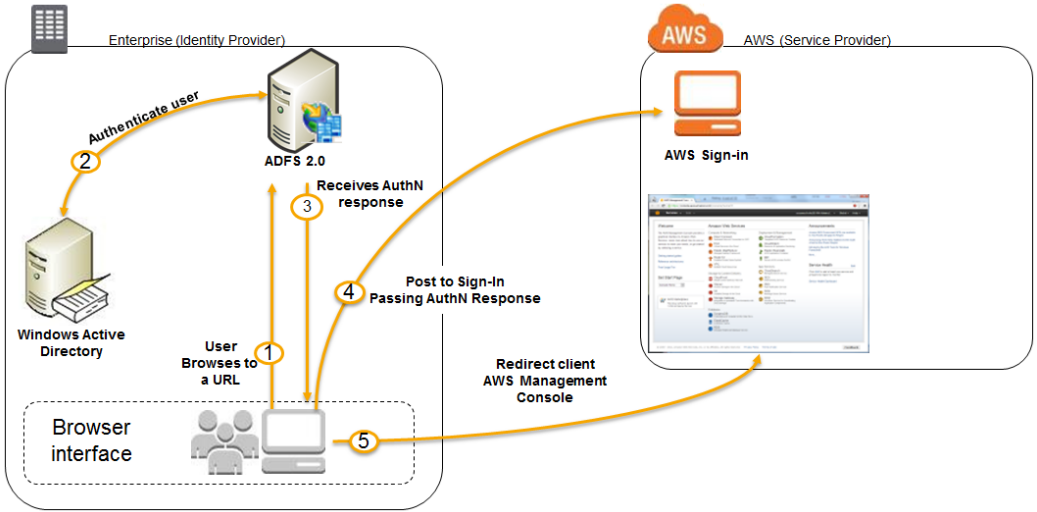
amazon web services

Introduction

- Some enterprise customers prefer leveraging their existing corporate identities to access AWS services and resources via identity federation
- This procedure enables you to build a sample federation site using Active Directory Federation Services and SAML 2.0
- Basically this procedure is along with the AWS security blog by Jeff Wierer

How Integration Between AD FS and AWS Works

1. The flow is initiated when a browses to the ADFS sample site inside his domain
2. The sign-on page authenticates the user against AD
3. The browser receives a SAML assertion in the form of an authentication response from ADFS
4. The browser posts the SAML assertion to the AWS sign-in endpoint for SAML
   - Sign-in uses the AssumeRoleWithSAML API to request temporary security credentials and then constructs a sign-in URL for the AWS Management Console
5. The browser receives the sign-in URL and is redirected to the console



amazon web services

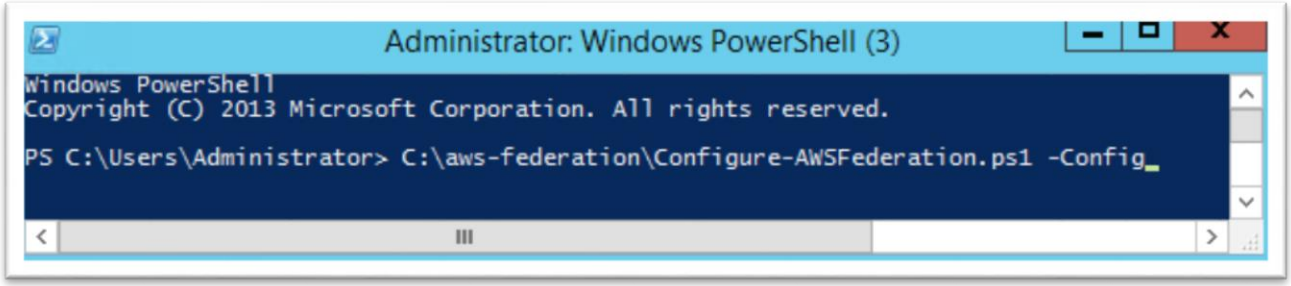
Step1 : Build Active Directory Domain

- Download the Configure-AWSFederation.ps1 script on Windows Server 2012 R2 on EC2
  - Script repository
    - https://github.com/number13/Configure-AWSFederation
  - The instance must be allowed the following access from your local computer
    - Inbound : RDP, HTTPS
- Run the script with “-Init” option
- Or, you can use the user-data when launching the instance (The instance will be rebooted automatically once after initialization)

```
<powershell>
mkdir C:\aws-federation
$ScriptFile="C:\aws-federation\Configure-AWSFederation.ps1"
Invoke-WebRequest "https://raw.githubusercontent.com/number13/Configure-AWSFederation/master/Configure-AWSFederation.ps1" -
OutFile $ScriptFile
Set-ExecutionPolicy Unrestricted
& $ScriptFile -init
</powershell>
```

Step2 : Configure ADFS farm and craims

- Log on to the instance as “example\Administrator” through remote desktop
- Run the Configure-AWSFederation.ps1 script with “-Config” option



- Download the federation meta-data xml file
  - Download URL
    - https://<your_instance_public_dns>/FederationMetadata/2007-06/FederationMetadata.xml

amazon web services

Step3 : Configuring AWS

- Log in to the IAM Management console
- Create SAML Provider in IAM
  - Provider Type : SAML
  - Provider Name : ADFS (must be this name)
  - Metadata Document : Specify the xml file downloaded in setp2
- Create two IAM Roles for SAML-Based Federation
  1. Admin Role
     - Role Name : ADFS-Admin (must be this name)
     - Role Type : Grant Web Single Sign-On (WebSSO) access to SAML providers
     - SAML Provider : ADFS
     - Permission : Administrator Access
  2. Read only Role
     - Role Name : ADFS-RO (must be this name)
     - Role Type : Grant Web Single Sign-On (WebSSO) access to SAML providers
     - SAML Provider : ADFS
     - Permission : Read Only Access

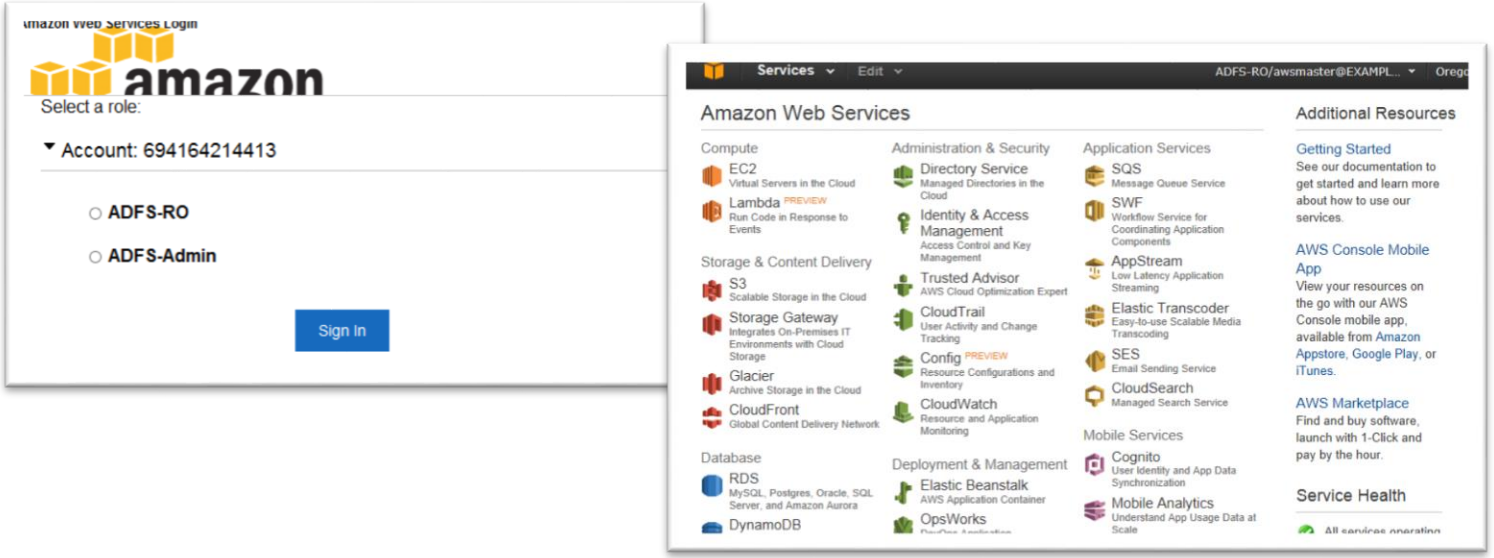
Now you can try SSO!

- Access to the ADFS federation site
  - https://<your_instance_public_dns>/adfs/ls/IdpInitiatedSignOn.aspx
  - You can sign in the site as following users (Password : P@ssW0rd)
    - awsmaster@example.com
    - awsadmin@example.com
    - awsreadonly@example.com

amazon web services

Now you can try SSO!

- If you log on as awsmaster, you can see the role selection view
- Select a role and then click **Sign In**. Then you can sign into the Management Console



- If you log on as awsadmin or awsreadonly, you skip the role selection step and automatically sign into the AWS Management Console

amazon web services