Landing Zone Immersion Day

Lab 3 – Configure AD and Deploy SSO

June 2018

Table of Contents

Overview

This lab will walk you through the addition of a user to AWS AD and configuration of AWS SSO.

This Lab assumes you had followed this Step in **Lab 1 – Deploy the Landing Zone.**

Allow use of the Landing Zone KMS Key to get the AD Admin Password

1. Log into the console for the account where you deployed the **Landing Zone Implementation & Configuration Pipeline**.
2. Update the KMS key permissions to allow for the download/upload of the **Landing Zone Configuration File**
    a. Browse to the console home page - In the **AWS Services** text field type **IAM** – and click on **IAM**.
    b. Select the appropriate region for the KMS key
    c. Scroll to and click on **Encryption Keys -> Get Started**
    d. Click on **AwsLandingZoneKMSKey**
    e. Under **Key Policy** scroll to the **"Sid": "Allow use of the key"** section and under **“Principal”** add in the user account you had used to login to the console to perform these tasks as such:

    "arn:aws:iam::<masteraccountnumber>:role/<IsengardRoleName>"

At the end, the KMS key policy should look like:

```
.....
   {
      "Sid": "Allow use of the key",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::xxxxxxxxxxxx:role/LandingZoneCodePipelineRole",
          "arn:aws:iam::xxxxxxxxxxxx:root",
          "arn:aws:iam::xxxxxxxxxxxx:role/LandingZoneDeploymentLambdaRole",
          "arn:aws:iam::xxxxxxxxxxxx:role/StateMachineTriggerLambdaRole",
          "arn:aws:iam::xxxxxxxxxxxx:role/StateMachineLambdaRole",
          "arn:aws:iam::xxxxxxxxxxxx:role/LandingZoneLambdaRole",
          "arn:aws:iam::xxxxxxxxxxxx:role/<RoleName>"
        ]
```

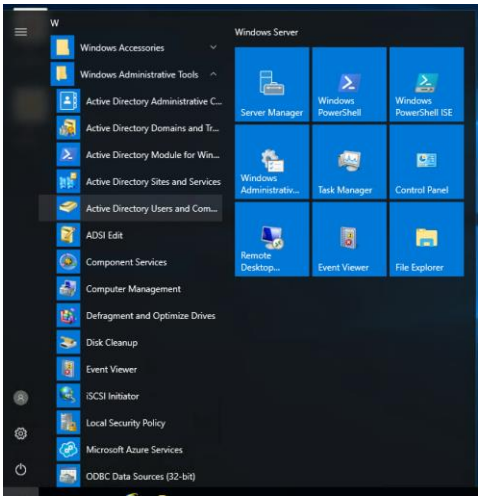
```
    },
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:ReEncrypt*",
      "kms:GenerateDataKey*",
      "kms:DescribeKey"
    ],
    "Resource": "*"
  }
```

f. Click **Save Changes**

Create Users

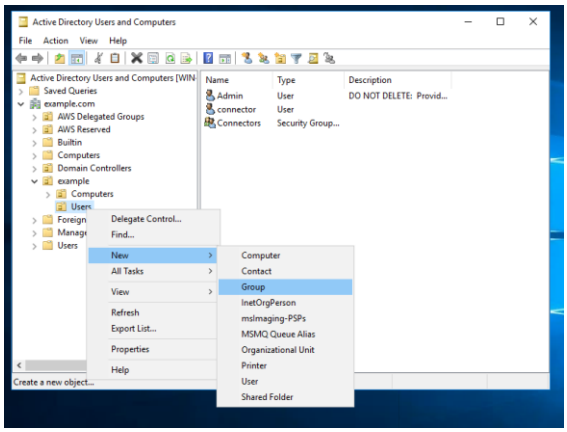
1. Navigate to the AWS Systems Manager console and click on Parameter Store.
2. Find the Elastic IP address for a Remote Desktop Gateway (RDGW) stored in the following parameter: `/org/member/sharedservices/rdgw_ip1`
3. Find the AD domain admin username stored in the following parameter: `/org/directory_service/domain_admin_user`
4. Find the AD domain admin password stored in the following parameter: `/org/ /org/directory_service/domain_admin_password`
5. Remote desktop into the RDGW using the IP, user name, and password.
6. Launch Active Directory Users and Computers (Windows Menu -> Windows Administrative Tools -> Active Directory Users and Computers)

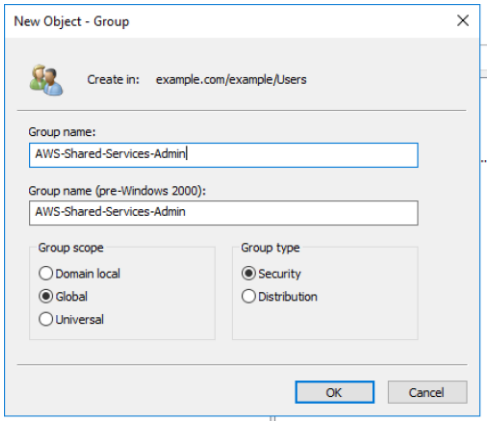
   If you have issues connecting to RDGW, please change role to the Shared Services account (via the AWSCloudFormationStackSetExecutionRole) and check the security group associated with the RDGW contains an ingress rule which allows you to access the RDGW via RDP from your IP address.



7. Create groups for access to your core accounts:

   AWS-Shared-Services-Admin
   AWS-Shared-Services-Read-Only
   AWS-Security-Admin
   AWS-Security-Read-Only
   AWS-Logging-Admin
   AWS-Logging-Read-Only

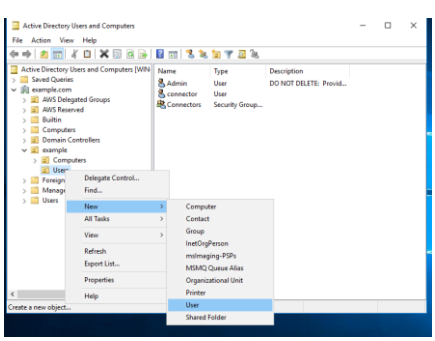


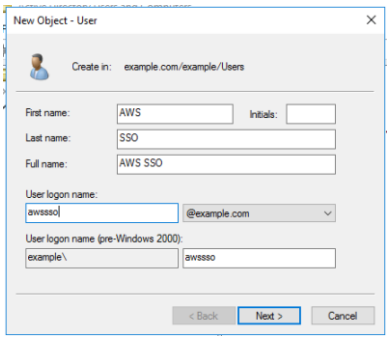


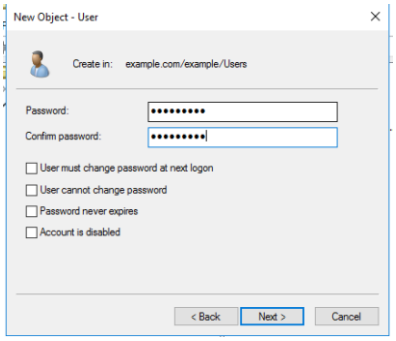
8. Create an **AWS SSO** user.

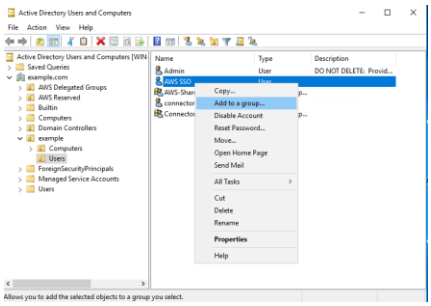
   Note: When creating the user check off the box for “User must change the password at next logon”

9. Add the user to ALL group(s). Note it’s unlikely you will do this in a customer deployment.



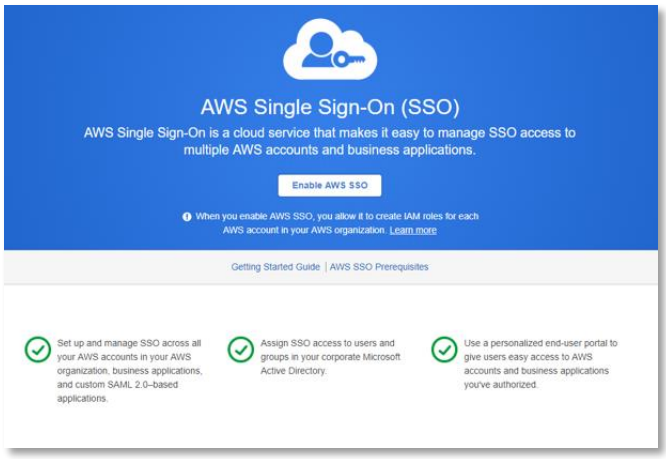




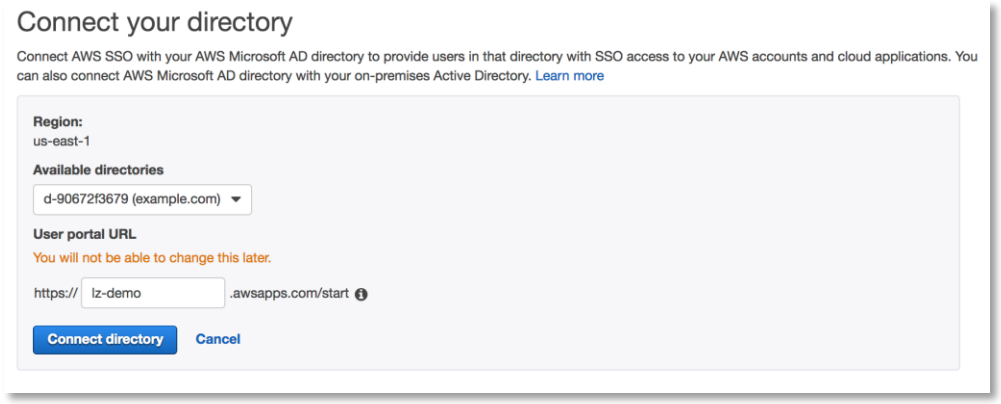


Configure AWS SSO

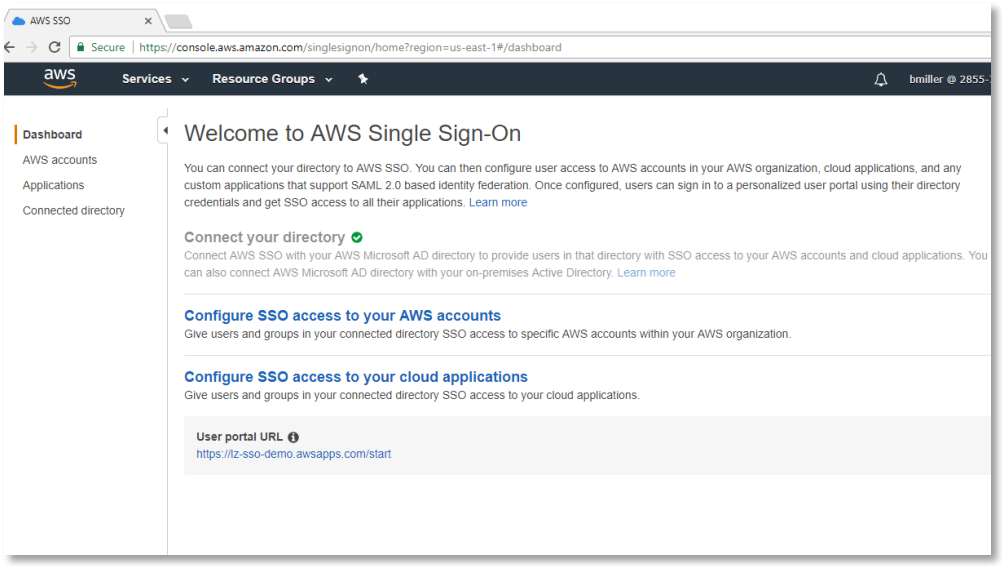
1. Navigate to the AWS SSO console and select **Enable SSO**.



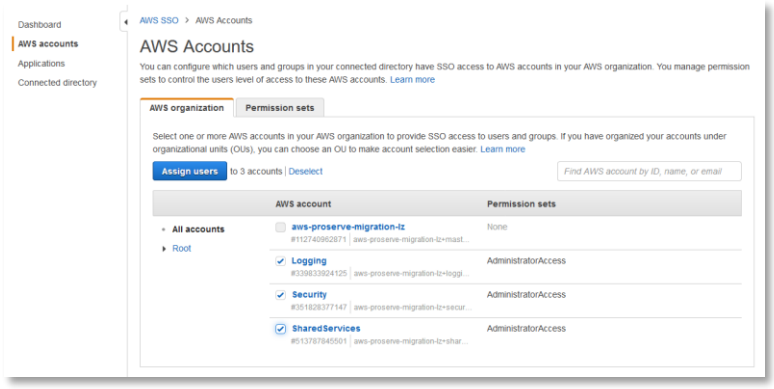
2. Select **Connect your directory**.
3. Select the AWS Landing Zone created directory from **Available directories**.
4. Choose a name for the URL you would like to access SSO e.g. lz-demo.



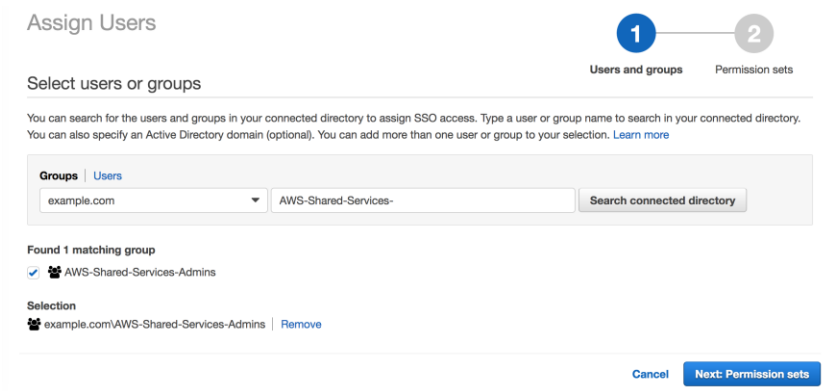
5. Navigate to the Dashboard and select Configure SSO access to your AWS accounts.



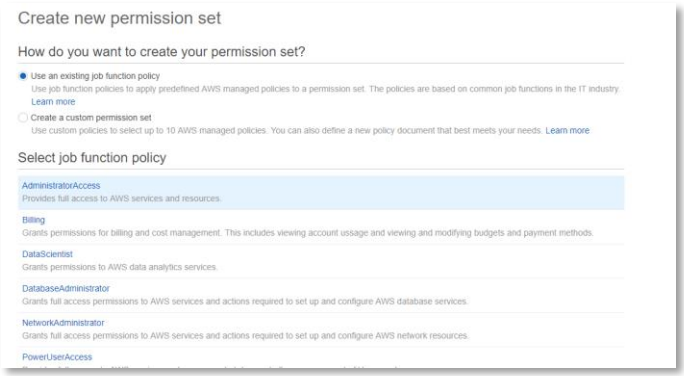
6. Select the **AWS accounts** to map Groups/Users to.



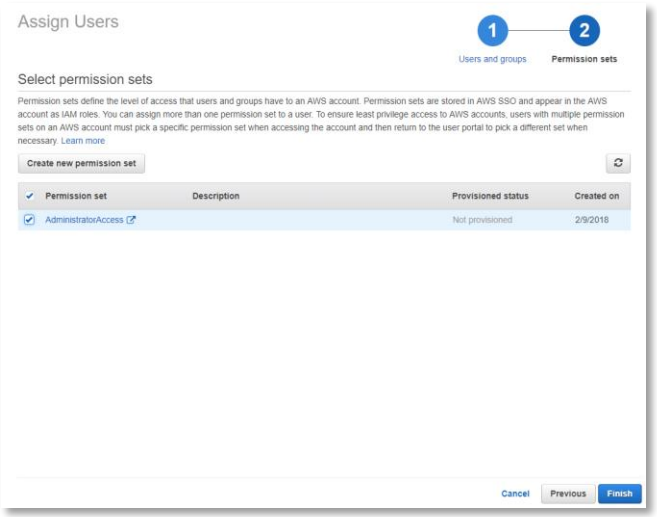
7. Select **Assign Users** and search or enter the Group/User Name.

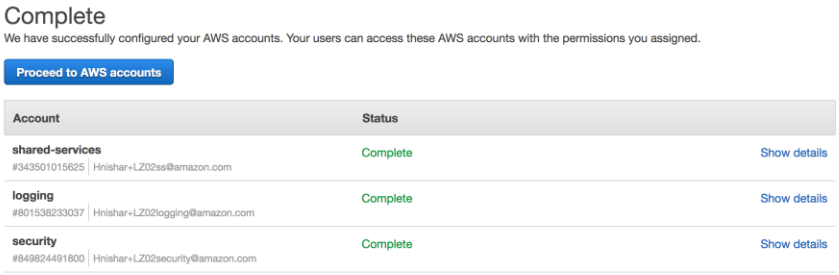


8. Select Next: Permission sets.
9. Select Create New Permission Set.
10. Select **Use and existing job function policy** and select the appropriate policy.

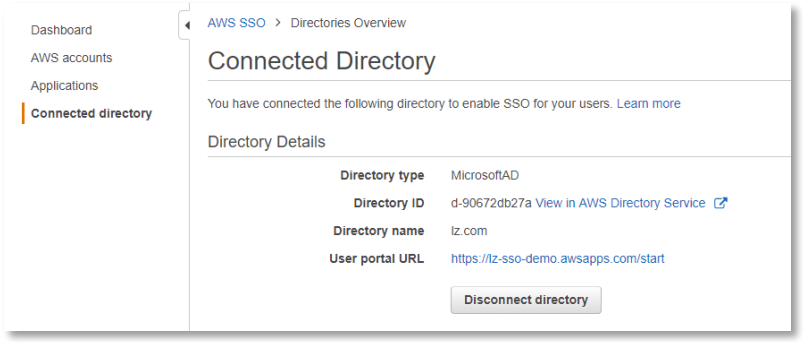


11. Select the **permission set** and select **Finish**.





Once the process is finished, you can look at the Connected Directory to find the **AWS SSO URL**.



12. Login to one of the account you've created by selecting the link and 'Open in new tab'.