Landing Zone Immersion Day

Lab 3 – Configure AD and Deploy SSO

June 2018

Rev 2018-06-18

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:

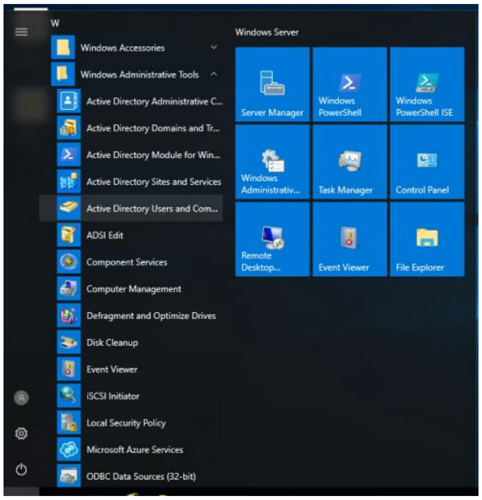
```
..................
  {
    "Sid": "Allow use of the key",
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::xxxxxxxxxxxx:role/LandingZoneCodePipelineRole",
        "arn:aws:iam::xxxxxxxxxxxx:root",
        "arn:aws:iam::xxxxxxxxxxxx:role/LandingZoneDeploymentLambdaRole",
        "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

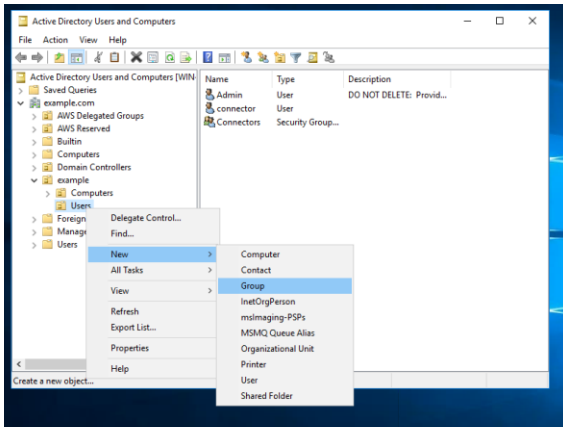
1. Navigate to the AWS Systems Manager console and click on Parameter Store.
2. Find the Elastic IP address for a Remote Desktop Gateway (RDGW) stored in the following parameter: `/org/member/sharedservices/rdgw_ip1`
3. Find the AD domain admin username stored in the following parameter: `/org/directory_service/domain_admin_user`
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.

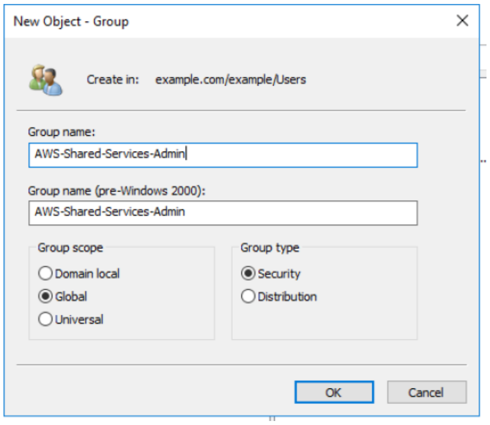


7. Create groups for access to your core accounts in the folder: example.com/example/Users:

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



Name	Type	Description
Admin	User	DO NOT DELETE: Provid...
connector	User	
Connectors	Security Group...	



Create in: example.com/example/Users

Group name:
AWS-Shared-Services-Admin

Group name (pre-Windows 2000):
AWS-Shared-Services-Admin

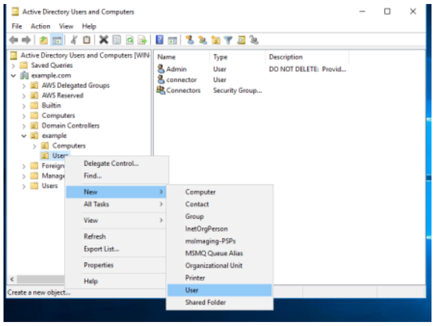
Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

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

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

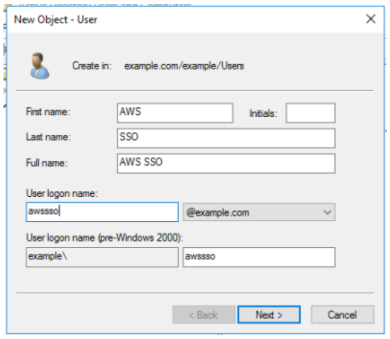
9. Add the user to ALL group(s). Note it’s unlikely you will do this in a customer deployment.



Active Directory Users and Computers

Name	Type	Description
Admin	User	DO NOT DELETE: Provid...
connector	User	
Connectors	Security Group...	

Create a new object...



New Object - User

Create in: example.com/example/Users

First name: AWS

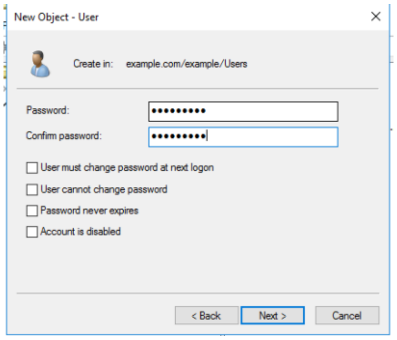
Initials:

Last name: SSO

Full name: AWS SSO

User logon name: awssso @example.com

User logon name (pre-Windows 2000): example\ awssso



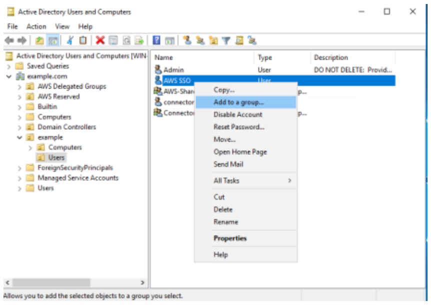
New Object - User

Create in: example.com/example/Users

Password: •••••••••

Confirm password: •••••••••

□ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Account is disabled



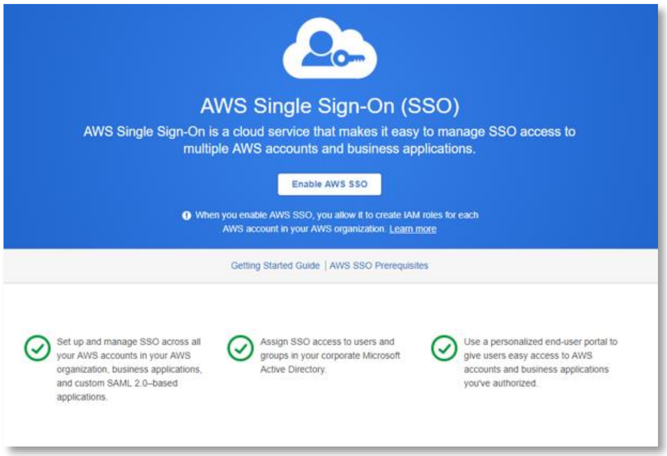
Active Directory Users and Computers

Name	Type	Description
Admin	User	DO NOT DELETE: Provid...
AWS SSO	User	
AWS-Shar	...p...	
connector		
Connector	...p...	

Allows you to add the selected objects to a group you select.

Configure AWS SSO

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



AWS Single Sign-On (SSO)

AWS Single Sign-On is a cloud service that makes it easy to manage SSO access to multiple AWS accounts and business applications.

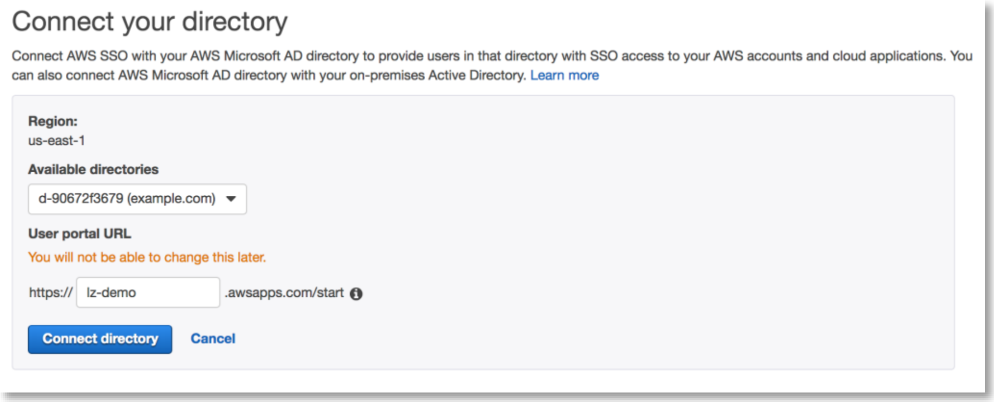
When you enable AWS SSO, you allow it to create IAM roles for each AWS account in your AWS organization. Learn more

Set up and manage SSO across all your AWS accounts in your AWS organization, business applications, and custom SAML 2.0–based applications.

Assign SSO access to users and groups in your corporate Microsoft Active Directory.

Use a personalized end-user portal to give users easy access to AWS accounts and business applications you've authorized.

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.



Connect your directory

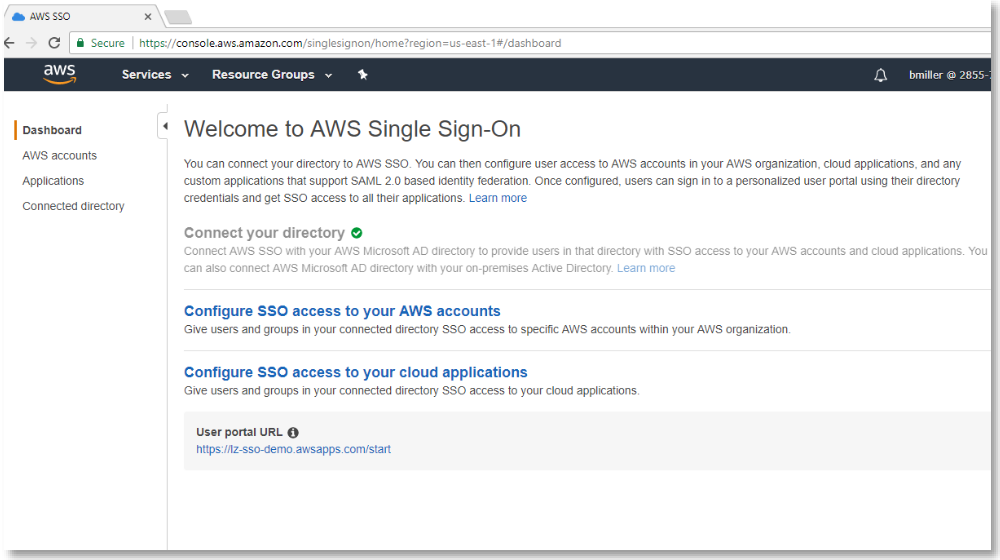
Connect AWS SSO with your AWS Microsoft AD directory to provide users in that directory with SSO access to your AWS accounts and cloud applications. You can also connect AWS Microsoft AD directory with your on-premises Active Directory. Learn more

Region:
us-east-1

Available directories
d-90672f3679 (example.com)

User portal URL
You will not be able to change this later.
https:// lz-demo .awsapps.com/start

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



Welcome to AWS Single Sign-On

You can connect your directory to AWS SSO. You can then configure user access to AWS accounts in your AWS organization, cloud applications, and any custom applications that support SAML 2.0 based identity federation. Once configured, users can sign in to a personalized user portal using their directory credentials and get SSO access to all their applications. Learn more

Connect your directory ✓

Connect AWS SSO with your AWS Microsoft AD directory to provide users in that directory with SSO access to your AWS accounts and cloud applications. You can also connect AWS Microsoft AD directory with your on-premises Active Directory. Learn more

Configure SSO access to your AWS accounts

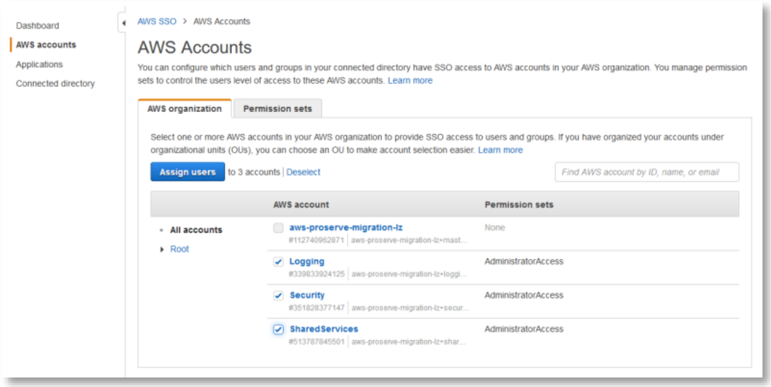
Give users and groups in your connected directory SSO access to specific AWS accounts within your AWS organization.

Configure SSO access to your cloud applications

Give users and groups in your connected directory SSO access to your cloud applications.

User portal URL
https://lz-sso-demo.awsapps.com/start

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



AWS Accounts

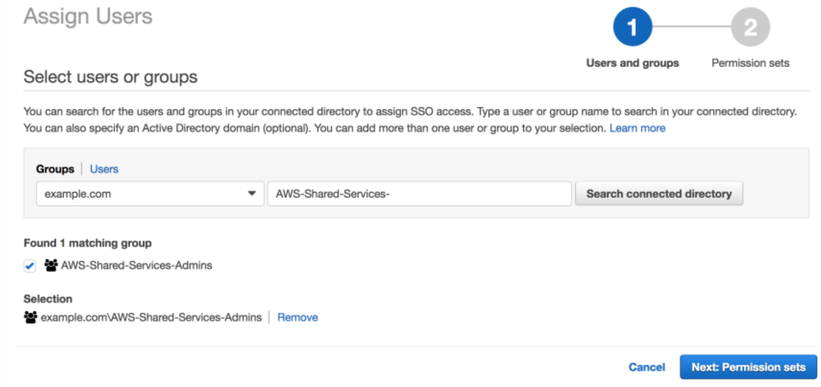
You can configure which users and groups in your connected directory have SSO access to AWS accounts in your AWS organization. You manage permission sets to control the users level of access to these AWS accounts. Learn more

Select one or more AWS accounts in your AWS organization to provide SSO access to users and groups. If you have organized your accounts under organizational units (OUs), you can choose an OU to make account selection easier. Learn more

Assign users to 3 accounts | Deselect

AWS account	Permission sets
□ aws-proserve-migration-lz #112740962871 | aws-proserve-migration-lz+mast...	None
☑ Logging #339833924125 | aws-proserve-migration-lz+loggi...	AdministratorAccess
☑ Security #351828377147 | aws-proserve-migration-lz+secur...	AdministratorAccess
☑ SharedServices #513787845501 | aws-proserve-migration-lz+shar...	AdministratorAccess

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



Assign Users

Select users or groups

You can search for the users and groups in your connected directory to assign SSO access. Type a user or group name to search in your connected directory. You can also specify an Active Directory domain (optional). You can add more than one user or group to your selection. Learn more

example.com
AWS-Shared-Services-

Found 1 matching group

☑ AWS-Shared-Services-Admins

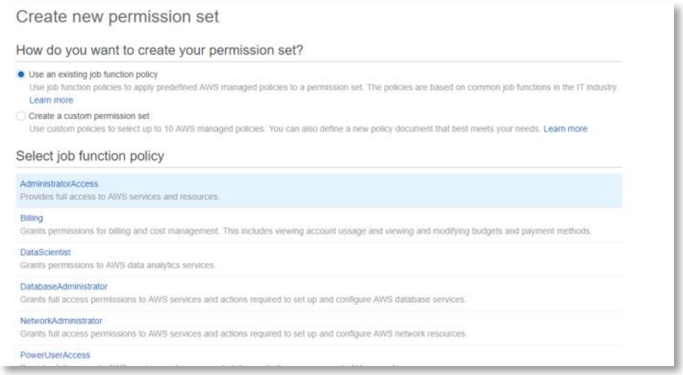
Selection

example.com\AWS-Shared-Services-Admins | Remove

8. Select Next: Permission sets.

9. Select Create New Permission Set.

10. Select **Use and existing job function policy** and select the appropriate policy.



Create new permission set

How do you want to create your permission set?

● Use an existing job function policy
Use job function policies to apply predefined AWS managed policies to a permission set. The policies are based on common job functions in the IT industry. Learn more

○ Create a custom permission set
Use custom policies to select up to 10 AWS managed policies. You can also define a new policy document that best meets your needs. Learn more

Select job function policy

AdministratorAccess
Provides full access to AWS services and resources.

Billing
Grants permissions for billing and cost management. This includes viewing account ussage and viewing and modifying budgets and payment methods.

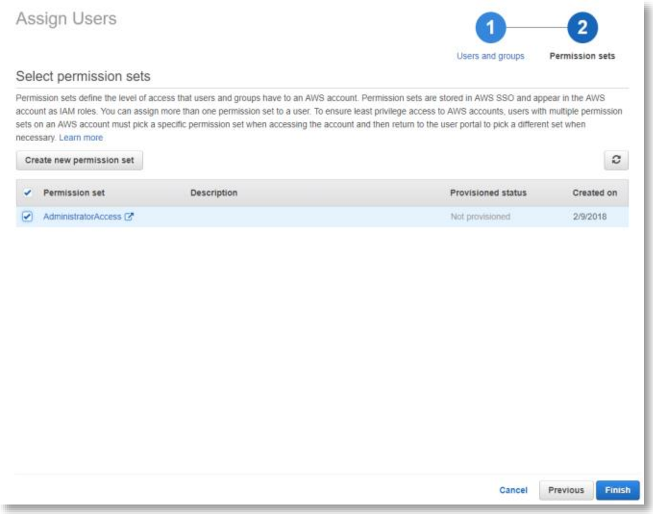
DataScientist
Grants permissions to AWS data analytics services.

DatabaseAdministrator
Grants full access permissions to AWS services and actions required to set up and configure AWS database services.

NetworkAdministrator
Grants full access permissions to AWS services and actions required to set up and configure AWS network resources.

PowerUserAccess

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

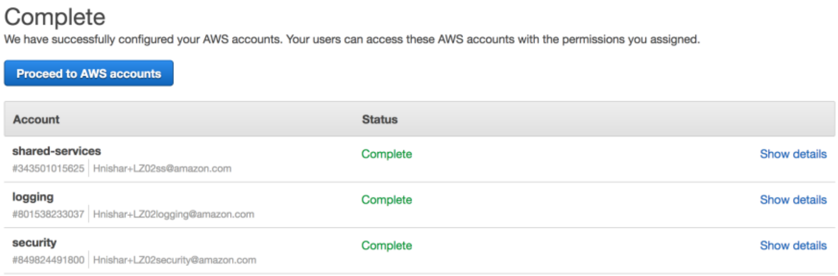


Assign Users

Select permission sets

Permission sets define the level of access that users and groups have to an AWS account. Permission sets are stored in AWS SSO and appear in the AWS account as IAM roles. You can assign more than one permission set to a user. To ensure least privilege access to AWS accounts, users with multiple permission sets on an AWS account must pick a specific permission set when accessing the account and then return to the user portal to pick a different set when necessary. Learn more

✓	Permission set	Description	Provisioned status	Created on
☑	AdministratorAccess		Not provisioned	2/9/2018

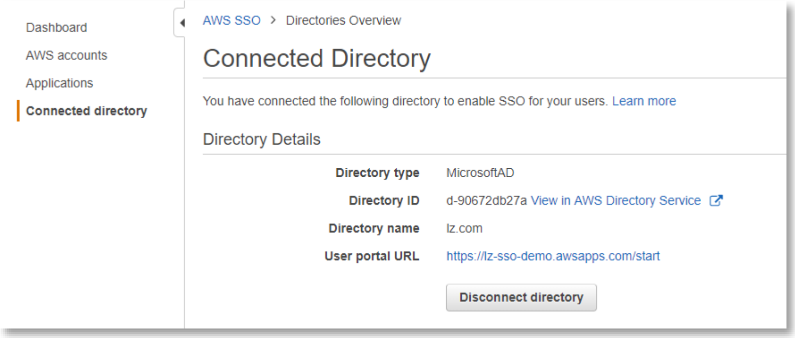


Complete

We have successfully configured your AWS accounts. Your users can access these AWS accounts with the permissions you assigned.

Account	Status	
shared-services #343501015625 | Hnishar+LZ02ss@amazon.com	Complete	Show details
logging #801538233037 | Hnishar+LZ02logging@amazon.com	Complete	Show details
security #849824491800 | Hnishar+LZ02security@amazon.com	Complete	Show details

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



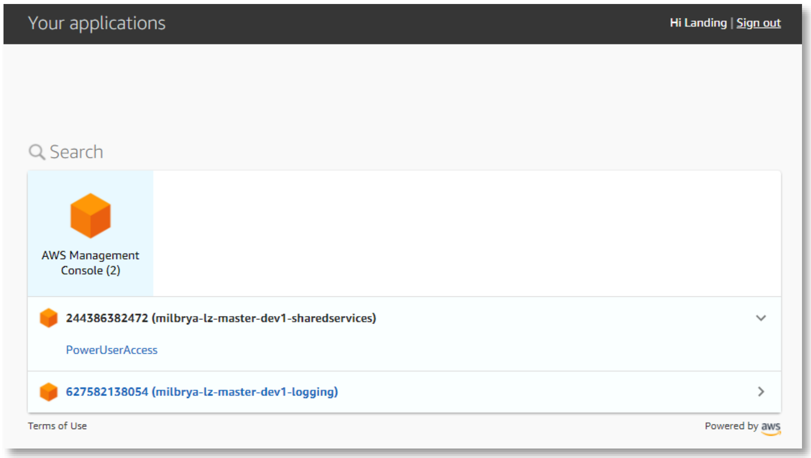
Connected Directory

You have connected the following directory to enable SSO for your users. Learn more

Directory Details

Directory type	MicrosoftAD
Directory ID	d-90672db27a View in AWS Directory Service
Directory name	lz.com
User portal URL	https://lz-sso-demo.awsapps.com/start

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



244386382472 (milbrya-lz-master-dev1-sharedservices)

PowerUserAccess

627582138054 (milbrya-lz-master-dev1-logging)