Sign in to the AWS Console with UW NetID

Purpose

This page describes how an AWS (Amazon Web Services) account owner can configure single sign-on (SSO) to AWS Management Console, including SAML configuration for signing in with UW NetID and management of UW groups to map group memberships to AWS roles in your AWS account.

Instructions

An AWS account owner can configure federated sign-in using these steps:

1. Send UW-IT your Amazon Account ID
    a. Account ID is on the "My Account" AWS Console page
    b. Email iam-support@uw.edu your Account ID
    c. UW-IT will create a UW group stem for you to manage your AWS roles
        i. u_weblogin_aws_*(accountid)*
2. Add the UW IdP as an Identity Provider
    a. "AWS Console" "IAM" "Identity Providers" "Create Provider"
        i. Provider Type: "SAML"
        ii. Provider Name: "UW"
        iii. Metadata Document:
            1. Attach the IdP's metadata as a file
        iv. Next Step
            1. "Create"
3. Create an AWS role for SAML login
    a. "IAM" Service -> "Roles" -> "Create New Role"
    b. Select "SAML 2.0 federation"
        i. SAML provider: *select what you created from step #2*
        ii. Attribute: "SAML:aud"
        iii. Value: "https://signin.aws.amazon.com/saml"
    c. Click "Next Permissions"
        i. Choose the AWS Policies that you want to grant to this role
    d. Click "Next Review"
        i. Role Name
            1. Must consists of: lowercase letters, digits, dashes, dots only!
            2. The role name will/must match the corresponding UW group ID (see step 4c below)
        ii. Click "Create Role"
4. Create a UW group that will be granted your AWS role
    a. Sign in to the UW groups service (https://groups.uw.edu)
    b. Create a new group under the group stem created for you (in step 1c)
    c. The last part of the Group ID (after the final "_") must match your AWS Role Name (*rolename*):
        i. u_weblogin_aws_*(accountid)*_(*rolename*)
    d. Add the UW NetIDs of people who can sign in and assume the role as members of this new group
        i. Users must be added as members of the group (direct or effective). Adding a user as an admin (or another non-member role) will not permit SSO.
5. Sign in to the AWS Console
    a. Amazon uses IdP-initiated SSO. This is also known as "unsolicited" SSO since the it isn't initiated by the service provider.
    b. A static link is used to initiate sign-in from the UW IdP.
        i. Either click this link: Sign in to the AWS Console with UW NetID
        ii. Or copy and use this location: https://idp.u.washington.edu/idp/profile/SAML2/Unsolicited/SSO?providerId=urn:amazon:webservices
    c. Clicking the link above initiates sign-in from the UW IdP to Amazon.
    d. The maximum session duration defaults to one hour. You can edit the AWS role itself to have a longer session duration.
    e. After the AWS session duration ends, the session with the AWS Console will expire.
    f. Use the IdP-initiated SSO link again to establish a new session.
6. Note: 2FA is enabled for all users by default.
    a. To learn more about 2FA options and eligibility, refer to two-factor authentication in IT Connect.

Notes

If you use AWS CloudTrail, refer to this blog on "How to Easily Identify Your Federated Users by Using AWS CloudTrail".
https://aws.amazon.com/blogs/security/how-to-easily-identify-your-federated-users-by-using-aws-cloudtrail/