

Okta를 이용한 AWS Multi-Account 환경 관리

Drama & Company Co.,. Ltd

이정민 (Tony)

Remember

Contents

1 IdP (Identity Provider)

2 AWS Multi-Account 환경 어떻게 관리할까

3 AWS IAM Identity Center 설정

4 Demo & Tips

5 Q&A

IdP
: Identity Provider



Single Source of Truth
The Central Source of Identity



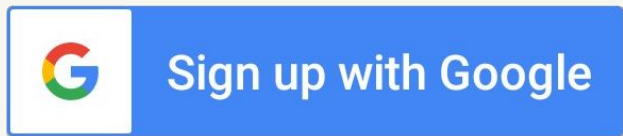
사용자 관점에서

한 개의 계정으로
모든 앱에 로그인

관리자 관점에서

사용자 계정 생성 | 삭제
RBAC
감사 로그
MFA 의무화

...



지원하지 않는 앱이 있음

계정정보 관리 이상의
기능을 제공하지 않음



전통의 LDAP

사용자 계정 관리도 가능하고
RBAC도 가능하다

그러나..

직접 운영해야 하고
네트워크의 제약도 심하며
멀티플랫폼 지원은 😞
+ 감사 로그, MFA 등등...



그래서  **okta** 를 사용하고 있습니다

직접 운영하지 않아도 되고
여러 서비스와 연동하기 쉽고
주변 레퍼런스가 매우 많아요

Q. AWS IAM Identity Center도 IdP가 된다던데?

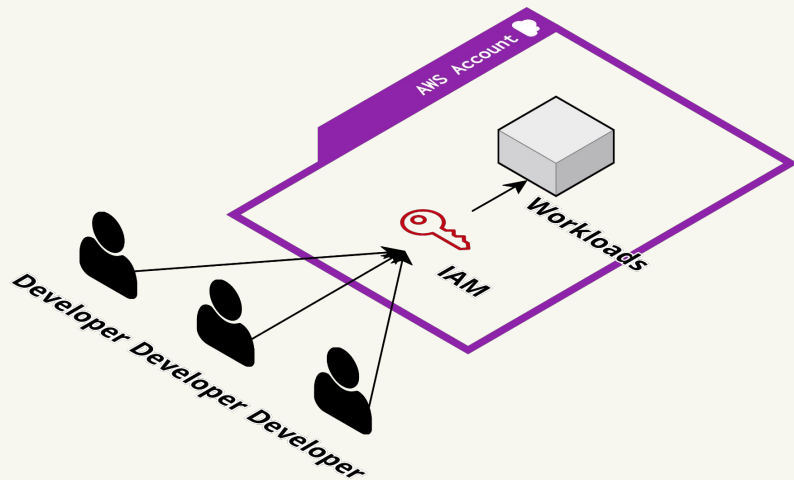


AWS Multi-Account 환경 어떻게 관리할까

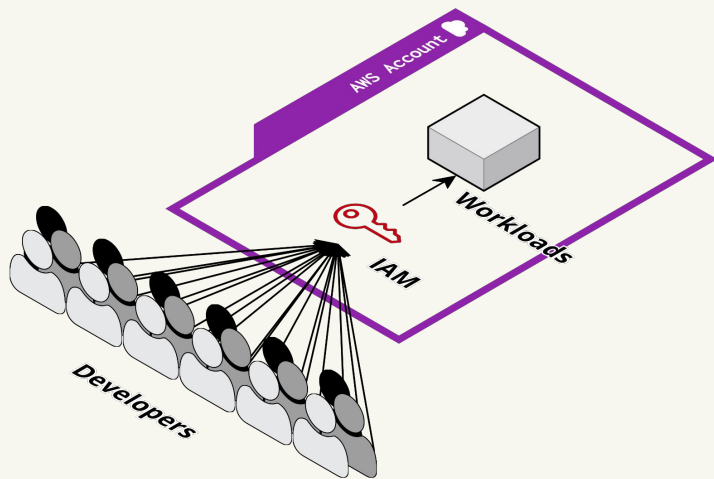


IAM User로 사용자 계정을 분리할 수 있다.

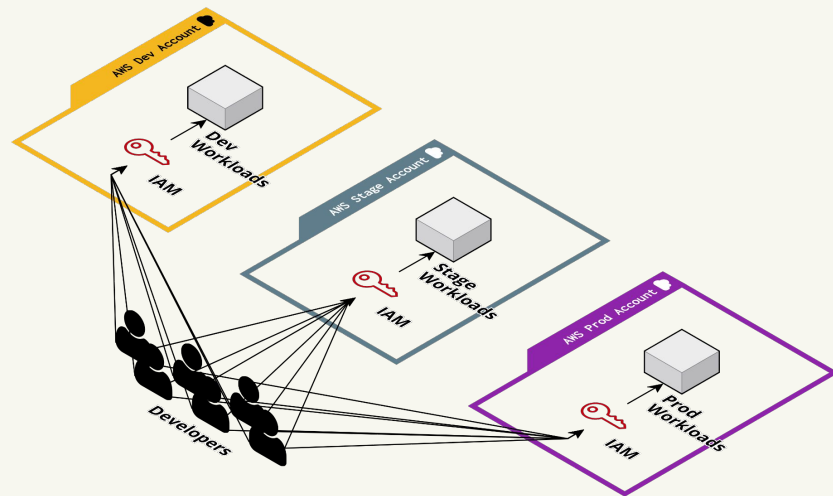
- 접근해야 하는 **AWS 계정**이 적거나
- 접근하는 **유저**가 **소수**일 때



하지만..



접근해야 하는 **유저가** 늘어난다면?



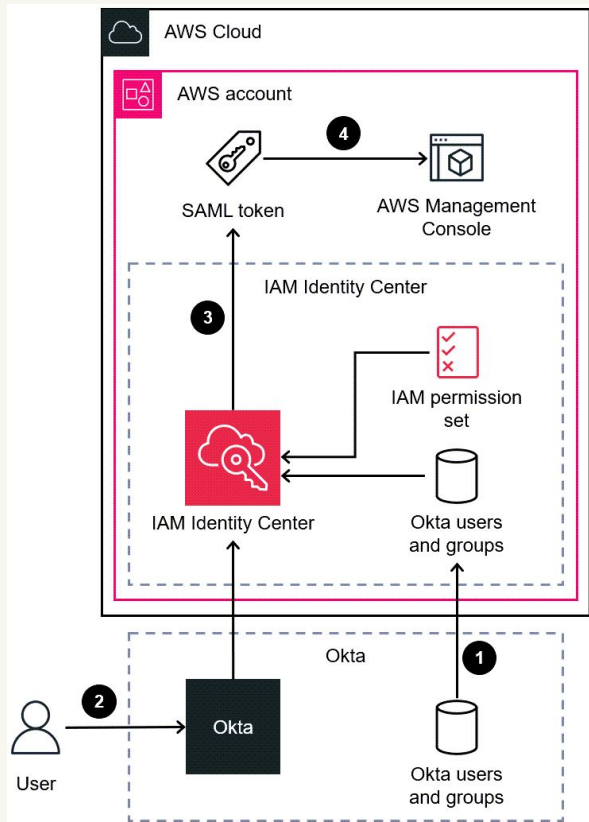
접근해야 하는 **계정이** 늘어난다면?

혹은 유저와 계정이 모두 늘어난다면?

유저 수 * AWS 계정 수 만큼 IAM User를 관리해야 하는데..

- 패스워드 변경 정책
- MFA Device 관리
- IAM Access Key Rotate

AWS IAM Identity Center*를 사용해봅시다.
Okta도 살짝 없어요.



IAM Identity Center를 사용한 로그인

1. Okta의 유저와 그룹 정보를 IAM Identity Center와 동기화(SCIM)
2. 사용자는 Okta를 통해 IAM Identity Center에 로그인
3. IAM Identity Center에서 해당 사용자 / 그룹에 정의된 IAM Permission Set에 따라 SAML token 발행
4. SAML token을 통해 접속하려는 AWS Account의 IAM Role을 Assume(STS:AssumeRoleWithSAML)

AWS IAM Identity Center 설정



Prerequisites

AWS Organization의 root 계정에서 생성해야 해요.

- 파트너사를 통해 AWS를 사용중인 경우, Organization root 계정에 접근이 불가할 확률이 높습니다. root 계정 접근 권한을 요청하신 후 작업을 진행해야 합니다. (작업 계획도 여유있게 잡으시고요.)

그 외에는..

IAM Identity Center는 Organization의 1개 리전에만 프로비저닝 가능해요.

AWS: IAM Identity Center 콘솔에서 기능 활성화

Security, Identity, and Compliance

IAM Identity Center (successor to AWS Single Sign-On)

Manage workforce access to multiple AWS accounts and cloud applications.

Use IAM Identity Center to connect an existing directory or use the built-in Identity Center directory to manage user access to AWS accounts and cloud applications.

Expand IAM Identity Center

IAM Identity Center makes it easy to connect an existing directory or use the built-in Identity Center directory to manage user access to AWS accounts and cloud applications.

Enable

Getting started

```
graph LR; A[Enable IAM Identity Center] --> B[Connect your directory, or create users and groups, for use across AWS]; B --> C[Manage the access of your workforce across AWS accounts]; B --> D[Manage the access of your workforce to cloud applications];
```

Enable IAM Identity Center

Connect your directory, or create users and groups, for use across AWS

Manage the access of your workforce across AWS accounts

Manage the access of your workforce to cloud applications

Getting started

- [Enable IAM Identity Center](#)
- [Get started with IAM Identity Center](#)
- [IAM Identity Center prerequisites](#)

More resources

- [Documentation](#)
- [FAQ](#)
- [IAM Identity Center forum](#)
- [Contact us](#)

AWS: Settings -> Identity source -> Change Identity Source 선택

The screenshot displays the AWS IAM Identity Center console. The left sidebar shows the navigation menu with 'Settings' selected. The main content area is titled 'Settings' and contains a 'Details' section with information about the identity source and multi-factor authentication settings. Below this, there are tabs for 'Identity source', 'Authentication', 'Attributes for access control', and 'Management'. The 'Identity source' tab is active, showing details about the external identity provider, including the authentication method (SAML 2.0) and the provisioning method (SCIM). A red box highlights the 'Actions' dropdown menu, which is open, showing the 'Change identity source' option.

Identity source

Choose the directory where you want to manage your users and groups. [Learn more](#)

Identity source	Provisioning method
External identity provider	SCIM
Authentication method	Identity store ID
SAML 2.0	d-
AWS access portal URL	
awsapps.com/start	

AWS: External Identity Provider 선택

The screenshot shows the AWS IAM Identity Center console. The top navigation bar includes the AWS logo, a 'Services' menu, a search bar, and a location dropdown set to 'Seoul'. The breadcrumb trail is 'IAM Identity Center > Settings > Change identity source'. On the left, a sidebar shows the progress: 'Step 1: Choose identity source' (active), 'Step 2: Configure external identity provider', and 'Step 3: Confirm change'. The main content area is titled 'Choose identity source' with a description: 'Your identity source is where you manage users and groups. You use IAM Identity Center to manage permissions for users and groups in your identity source to access AWS accounts and cloud applications. [Learn more](#)'. Below this, three options are presented in boxes: 'Identity Center directory', 'Active Directory', and 'External identity provider'. The 'External identity provider' option is selected with a radio button and is highlighted by a red rectangular box. It includes a description: 'You will manage all users and groups in an external identity provider (IdP). Users sign in to your IdP sign-in page, and are redirected to the AWS access portal. After they sign in to the AWS access portal, they can access their assigned AWS accounts and cloud applications.' and a 'Learn more' link. At the bottom right, there are 'Cancel' and 'Next' buttons.

aws Services Search [Option+S] Seoul

IAM Identity Center > Settings > Change identity source

Step 1
Choose identity source

Step 2
Configure external identity provider

Step 3
Confirm change

Choose identity source

Your identity source is where you manage users and groups. You use IAM Identity Center to manage permissions for users and groups in your identity source to access AWS accounts and cloud applications. [Learn more](#)

☐ **Identity Center directory**
You will manage all users and groups in IAM Identity Center. Users sign in through the AWS access portal.

☐ **Active Directory**
You will manage all users and groups in AWS Managed Microsoft AD, or you can connect IAM Identity Center to Active Directory by using AWS Managed Microsoft AD or AD Connector. Users sign in through the AWS access portal.

☒ **External identity provider**
You will manage all users and groups in an external identity provider (IdP). Users sign in to your IdP sign-in page, and are redirected to the AWS access portal. After they sign in to the AWS access portal, they can access their assigned AWS accounts and cloud applications.
[Learn more](#)

Cancel Next

AWS: External Identity Provider 설정

aws Services Search [Option+S] Seoul

IAM Identity Center > Settings > Change identity source

Step 1
Choose identity source

Step 2
Configure external identity provider

Step 3
Confirm change

Configure external identity provider

Service provider metadata

Your identity provider (IdP) requires the following IAM Identity Center certificate and metadata information to trust IAM Identity Center as a service provider. You can copy and paste this information, type it in the service provider configuration interface for your IdP, or download the IAM Identity Center metadata file and upload it to your IdP.

AWS access portal sign-in URL

IAM Identity Center Assertion Consumer Service (ACS) URL

IAM Identity Center issuer URL

Identity provider metadata

AWS requires specific metadata provided by your identity provider (IdP) to establish trust. You may copy and paste from your IdP, type the metadata in manually, or upload a metadata exchange file that you download from your IdP.

IdP SAML metadata

Or

IdP sign-in URL

IdP issuer URL

IdP certificate

Service Provider metadata

- AWS의 metadata
- Okta에서 Integration 생성 시 정보 입력

Identity Provider metadata

- Okta의 metadata
- Okta Integration 완료 후 제공되는 정보 입력

Okta: App Catalog에서 Integration 추가

The screenshot shows the Okta Admin Console interface. On the left is a navigation sidebar with options like Dashboard, Directory, Customizations, Applications, Self Service, Security, Workflow, Reports, and Settings. The main content area displays the 'AWS IAM Identity Center' integration page. At the top right of this page, there is a blue button labeled 'Add Integration' which is highlighted with a red rectangular box. Below this button, the AWS logo is shown next to the title 'AWS IAM Identity Center'. Under the title are four tabs: 'Workflow Templates', 'SAML', 'Workflows', and 'Connectors'. A mouse cursor is pointing at the 'Connectors' tab. Below the tabs, the text 'Manage SSO access to your AWS accounts, roles, and applications' is visible. At the bottom of the page, there are two sections: 'Okta Verified' and 'Overview'.

Okta

Search...

info@jksstechlab.com
okta-dev-66452280

Applications > Catalog > Single Sign-On > AWS IAM Identity Center

Last updated: August 9, 2022

[Add Integration](#)

aws

Workflow Templates SAML Workflows Connectors

SCIM

Manage SSO access to your AWS accounts, roles, and applications

Okta Verified

The integration was either created by Okta or by Okta community users and then tested and verified by Okta

Overview

Federating with AWS IAM Identity Center (successor to AWS Single Sign-On) enables an Okta sign-in experience to AWS and a single way to manage access to the AWS console, AWS command line interface, and AWS IAM Identity Center enabled applications centrally, across all your AWS Organizations

AWS: External Identity Provider 설정

The screenshot shows the AWS IAM Identity Center console. The breadcrumb navigation is "IAM Identity Center > Settings > Change identity source". The left sidebar shows the steps: "Step 1: Choose identity source", "Step 2: Configure external identity provider" (which is the current step), and "Step 3: Confirm change". The main content area is titled "Configure external identity provider". It contains two main sections: "Service provider metadata" and "Identity provider metadata". The "Service provider metadata" section is highlighted with a red box. It includes a "Download metadata file" button, a text area for "AWS access portal sign-in URL" with the value "https://[redacted].awsapps.com/start", and two text areas for "IAM Identity Center Assertion Consumer Service (ACS) URL" and "IAM Identity Center issuer URL", both with values starting with "https://ap-northeast-2.signin.aws.amazon.com/platform/saml/". The "Identity provider metadata" section includes a "Choose file" button for "IdP SAML metadata", a text area for "IdP sign-in URL", a text area for "IdP issuer URL", and a "Choose file" button for "IdP certificate". At the bottom, there are "Cancel", "Previous", and "Next" buttons.

The screenshot shows the Okta console. The breadcrumb navigation is "Search for people, apps and groups". The main content area is titled "Advanced Sign-on Settings". It includes a section for "AWS SSO ACS URL" and "AWS SSO issuer URL", both of which are highlighted with a red box. Below these are sections for "Credentials Details" and "Password reveal". The "Credentials Details" section includes a dropdown for "Application username format" (set to "Okta username") and a dropdown for "Update application username on" (set to "Create and update"). The "Password reveal" section includes a checkbox for "Allow users to securely see their password (Recommended)" which is unchecked, and a blue button with a white exclamation mark icon and the text "Password reveal is disabled, since this app is using SAML with no password." At the bottom right, there is a "Save" button.

AWS: External Identity Provider 설정

Services

Search

[Option+5]

Seoul

IAM Identity Center > Settings > Change identity source

Step 1

Choose identity source

Step 2

Configure external identity provider

Step 3

Confirm change

Configure external identity provider

Service provider metadata

Your identity provider (IdP) requires the following IAM Identity Center certificate and metadata information to trust IAM Identity Center as a service provider. You can copy and paste this information, type it in the service provider configuration interface for your IdP, or download the IAM Identity Center metadata file and upload it to your IdP.

Download metadata file

AWS access portal sign-in URL

https://[redacted].awsapps.com/start

IAM Identity Center Assertion Consumer Service (ACS) URL

https://ap-northeast-2.signin.aws.amazon.com/platform/saml/acs/[redacted]

IAM Identity Center issuer URL

https://ap-northeast-2.signin.aws.amazon.com/platform/saml/[redacted]

Identity provider metadata

AWS requires specific metadata provided by your identity provider (IdP) to establish trust. You may copy and paste from your IdP, type the metadata in manually, or upload a metadata exchange file that you download from your IdP.

IdP SAML metadata

Choose file

Or

IdP sign-in URL

IdP issuer URL

IdP certificate

Choose file

Cancel

Previous

Next

Search for people, apps and groups

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application. Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0

Default Relay State

Disable Force Authentication

☐

Metadata details

Metadata URL

Copy

Hide details

Sign on URL

Copy

Sign out URL

Copy

Issuer

Copy

Signing Certificate

Download

Copy

Certificate fingerprint

Application Username

Choose a format to use as the default username value when assigning the application to users.

If you select **None** you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

SAML Setup

Single Sign On using SAML will not work until you configure the app to trust Okta as an IdP.

View SAML setup instructions

25

Demo & Tips



웹 콘솔에 로그인해봅시다

Remember

🏠 내 앱

Drama&Company

섹션 추가 ⊕

🔔 알림 ①

🧩 앱 추가

🔍 앱 검색

관리자 정민 드라마엔컴퍼니 (Drama&... ▼)

내 앱

정렬 ▾

🔍 Drama&Company

Google Workspace Drive

Slack

Atlassian Cloud Jira SAML

aws

AWS

AWS Workspaces

⊕ 섹션 추가

지원

앱 요청

마지막 로그인: 몇 초 전

개인 정보 보호

Okta 대시보드에서 AWS 앱 접속

웹 콘솔에 로그인해봅시다

정민 | MFA devices | Sign out

Search


AWS Account (9)

av[redacted]

[redacted]

▼

dt[redacted]

[redacted]

▼

dt[redacted]

[redacted]

▼

dt[redacted]

[redacted]

▼

dt[redacted]

[redacted]

▼

dt[redacted]

[redacted]

▼

re[redacted]

[redacted]

▼

re[redacted]

[redacted]

▼

AWS SSO 대시보드에서 접근 가능한 계정
확인

웹 콘솔에 로그인해봅시다

AWS Account (9)

계정 별로 Assume 가능한 IAM Role 확인

a		
di		
drama-devops	Management console	Command line or programmatic access
di		
di		
di		
di		
drama-dev-	Management console	Command line or programmatic access
drama-devops	Management console	Command line or programmatic access
ri		
ri		
ri		

웹 콘솔에 로그인해봅시다

The screenshot shows the AWS IAM Identity Center console interface. At the top, there's a navigation bar with the AWS logo, 'Services', a search bar, and a user profile dropdown. The main content area is titled 'Console Home' and features a 'Recently visited' section with links to various AWS services like EC2, WorkSpaces, S3, Systems Manager, CloudTrail, Elastic Container Service, CodePipeline, Route 53, IAM, CodeBuild, CloudFront, Elastic Container Registry, Key Management Service, and AWS Marketplace Subscriptions. On the right, there's a 'Welcome to AWS' section with links to 'Getting started with...', 'Training and certification', and 'What's new with AWS...'. A red box highlights the 'Account ID: 7840' field in the user profile dropdown, which also shows the federated user information: 'Federated user: AWSReservedSSO_drama-devops_jeongmin.lee@dramancompany.com'. Below the main content, there are sections for 'AWS Health' (showing 1 open issue) and 'Cost and usage'. The footer contains links to CloudShell, Feedback, Language, and copyright information.

Federated User 정보에서 SSO를 통해 접속했음을 확인

Account ID: 7840
Federated user: AWSReservedSSO_drama-devops_jeongmin.lee@dramancompany.com

Switch role Sign out

CLI도 로그인해봅니다

```
leejeongmin@ip-192-168-250-80:~  
27% 20 GB 14 kB↓ 10 kB↑  
sso_start_url = https://          .awsapps.com/start#/  
sso_region = ap-northeast-2  
sso_role_name = drama-devops  
sso_account_id =  
region = ap-northeast-2  
  
[profile      ]  
sso_start_url = https://          .awsapps.com/start#/  
sso_region = ap-northeast-2  
sso_role_name = drama-devops  
sso_account_id =  
region = ap-northeast-2  
  
[profile      ]  
sso_start_url = https://          .awsapps.com/start#/  
sso_region = ap-northeast-2  
sso_role_name = drama-devops  
sso_account_id =  
region = ap-northeast-2  
  
[profile      ]  
sso_start_url = https://          .awsapps.com/start#/  
sso_region = ap-northeast-2  
sso_role_name = drama-devops  
sso_account_id =  
region = ap-northeast-2  
leejeongmin ~
```

~/aws/config 에 저장된 설정 정보

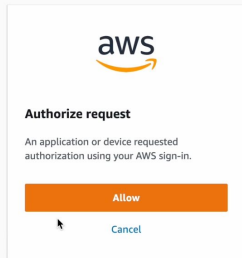
CLI도 로그인해봅니다

특정 계정에 접근 시도 시,
브라우저를 통해 IdP(Okta) 로그인 페이지로
리디렉션



Identity provider(으)로 리디렉션 중

CLI도 로그인해봅시다



```
leejeongmin@ip-192-168-250-80:~$ aws-vault exec ops
Opening the SSO authorization page in your default browser (use Ctrl-C to abort)
https://device.sso.ap-northeast-2.amazonaws.com/?user_code=BKCQ-XBSX
Starting subshell /bin/zsh, use `exit` to exit the subshell
leejeongmin@ip-192-168-250-80:~$
```

Authorize Request Allow 시
CLI 접속 환경에 Temporary Credential 발행

CLI도 로그인해봅니다

```
aws sts get-caller-identity
{
  "UserId": "jeongmin.lee@dramancompany.com",
  "Account": "72",
  "Arn": "arn:aws:sts::72:assumed-role/AWSReservedSSO_drama-devops_jeongmin.lee@dramancompany.com"
}
(END)
```

aws sts get-caller-identity로
SSO를 통해 접속한 유저임을 확인할 수 있음

Tip: **aws-vault***를 사용하면 CLI 사용이 조금 더 쉬워져요

- Temporary Credential을 로컬 keystore에 저장
- 특정 프로필 로그인 시 Subshell로 실행

* <https://github.com/99designs/aws-vault>

Tip: IAM Identity Center는 Delegated Administrator*를 설정합니다

- AWS 계정이 추가될 때마다 설정을 변경해주어야 해서, 생각보다 자주 건드리게 됨
- 매번 root 계정으로 계속 작업을 수행하는 것이 부담스러움
- Management 계정을 Delegated Administrator로 설정하면 관리자의 접근성이 좋아짐

* <https://docs.aws.amazon.com/singlesignon/latest/userguide/delegated-admin.html>

Q&A

**Q. 개인별로 부여받은 IAM 권한이 다른 경우가 있을텐데,
IAM Permission Set을 사용할 때 이를 어떻게 해결하였는지**

A. 정책적으로 해결할 수 밖에 없는 문제라고 생각합니다.

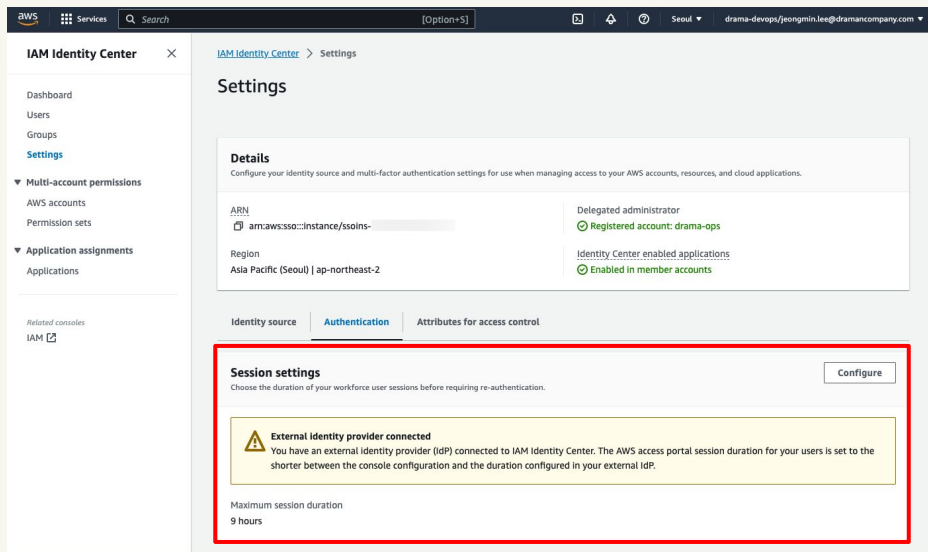
작업을 진행하며 팀 혹은 직무 단위로 IAM Permission Set을 정의하였고,
추가적인 Action은 Terraform 코드를 작성하여 Atlantis를 통해 배포하는 방법으로 가이드를 진행하였습니다.

그럼에도 부득이한 경우에는 Individual한 IAM Permission Set을 만들어 사용자에게 부여할 수 있습니다.

Q. CLI 사용 시 발급되는 Temporary Credential의 Session Duration 관리

A. 세션의 유효기간은 External IdP(Okta)와 AWS IAM Identity Center에서 각각 정의할 수 있습니다.

AWS의 Session Duration은 15분 ~ 10800분(7일) 사이로 설정할 수 있어요.



Q. 신규 입/퇴사자 관리는 어떻게 이루어지는지

A. 신규 입사자의 Okta 계정을 생성하고, Okta에서 AWS 사용 권한을 부여하면 계정 정보가 SCIM을 통해 AWS IAM Identity Center에 동기화됩니다.

퇴사자의 경우 Okta 계정을 삭제 혹은 비활성화하여 권한 회수가 완료됩니다.

Q. 외부 사용자(외주, 아르바이트 등)에게 권한을 부여하는 방법

**A. Okta에 외부 사용자의 계정을 만들고 AWS 사용 권한을 부여할 수 있습니다.
외부 사용자의 이메일 주소로 Okta 계정을 생성할 수 있어요. (Okta 유저 라이선스 비용은 과금됨)**

Remember

Thank You