

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



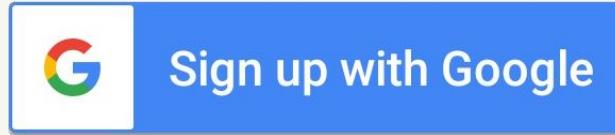
사용자 관점에서는

한 개의 계정으로
모든 앱에 로그인

관리자 관점에서는

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



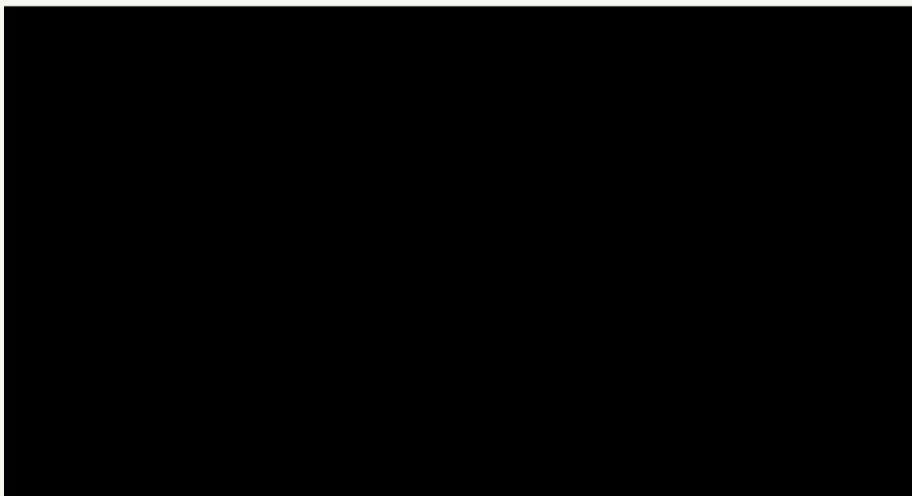
okta 를 사용하고 있습니다

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

Q. AWS IAM Identity Center도 IdP가 된다던데?

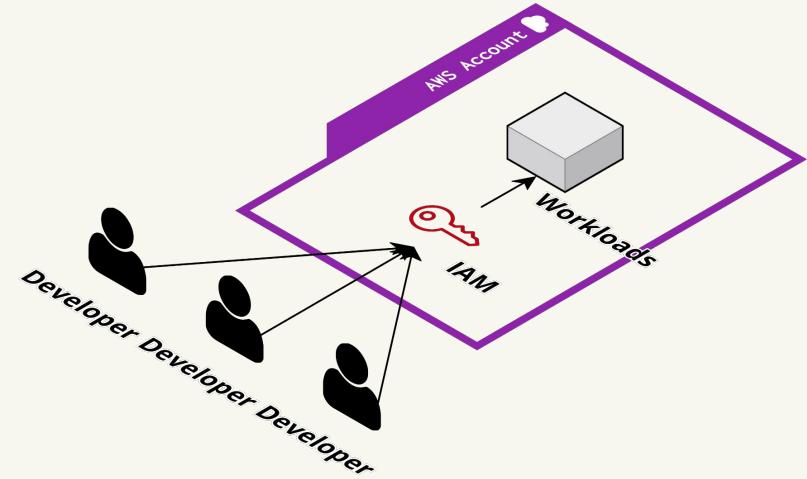


AWS Multi-Account 환경 어떻게 관리할까



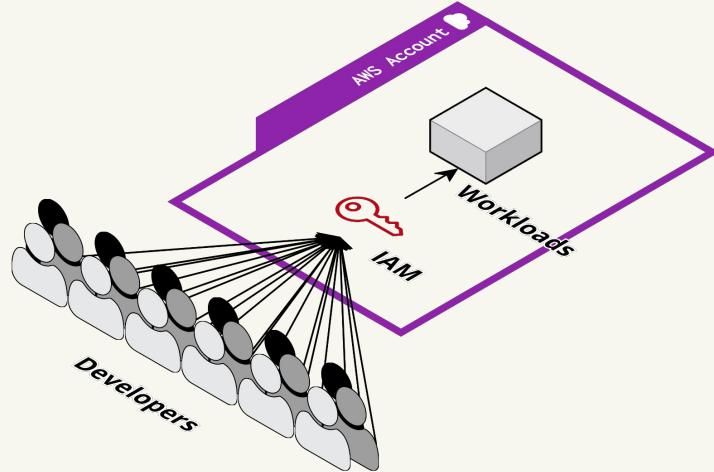
IAM User로 사용자 계정을 분리할 수 있다.

- 접근해야 하는 AWS 계정이 적거나
- 접근하는 유저가 소수일 때

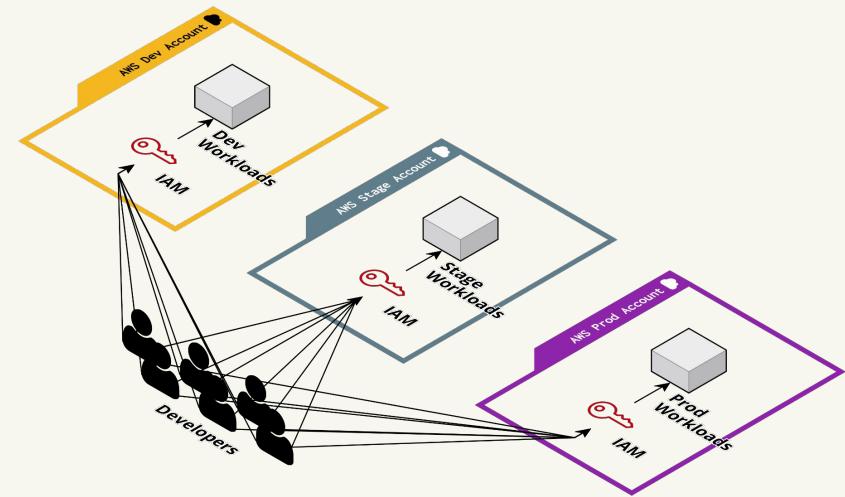


AWS IAM Identity Center

하지만..



접근해야 하는 **유저가 늘어난다면?**



접근해야 하는 **계정이 늘어난다면?**

혹은 유저와 계정이 모두 늘어난다면?

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

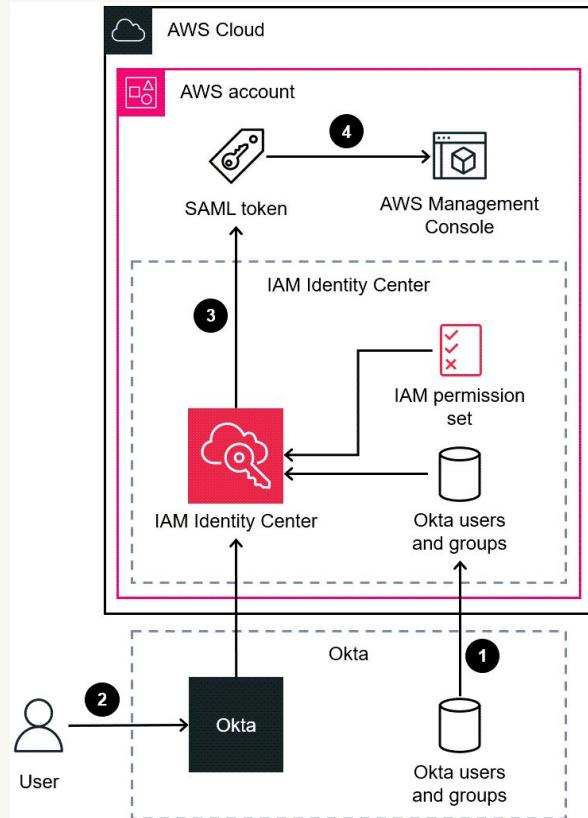
- 패스워드 변경 정책
- MFA Device 관리
- IAM Access Key Rotate

AWS IAM Identity Center*를 사용해봅시다.

Okta도 살짝 없어서요.

* 이전 서비스 이름은 AWS SSO였는데 IAM Identity Center로 통합되었어요.

AWS IAM Identity Center



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

AWS: IAM Identity Center 콘솔에서 기능 활성화

The screenshot shows the 'Getting started' section of the IAM Identity Center console. It features three main steps:

- Enable IAM Identity Center**: A light blue box containing a laptop icon with two people on it.
- Connect your directory, or create users and groups, for use across AWS**: A light gray box containing a user icon.
- Manage the access of your workforce across AWS accounts**: A light gray box containing a laptop icon with a gear and plus sign.

On the right side, there are three panels:

- Expand IAM Identity Center**: Describes connecting to an existing directory or using the built-in Identity Center directory. An **Enable** button is highlighted with a mouse cursor.
- Getting started**: Links to 'Enable IAM Identity Center', 'Get started with IAM Identity Center', and 'IAM Identity Center prerequisites'.
- More resources**: Links to 'Documentation', 'FAQ', 'IAM Identity Center forum', and 'Contact us'.

AWS IAM Identity Center

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

The screenshot shows the AWS IAM Identity Center Settings page. On the left, a sidebar lists 'Dashboard', 'Users', 'Groups', and 'Settings' (which is selected). Under 'Multi-account permissions', there are 'AWS accounts' and 'Permission sets'. Under 'Application assignments', there is an 'Applications' link. At the bottom of the sidebar are 'Related consoles' links for IAM and a 'New' button.

The main content area is titled 'Settings'. It contains a 'Details' section with configuration for managing access to AWS accounts, resources, and cloud applications. It shows an ARN (arn:aws:sso:::instance/ssoinst-), a 'Delegated administrator' status (Registered account), a Region (Asia Pacific (Seoul) | ap-northeast-2), and 'Identity Center enabled applications' (Enabled in member accounts).

Below this is a navigation bar with tabs: 'Identity source' (which is selected and highlighted in blue), 'Authentication', 'Attributes for access control', and 'Management'.

The 'Identity source' tab displays settings for managing users and groups. It includes fields for 'Identity source' (set to 'External identity provider'), 'Authentication method' (SAML 2.0), 'AWS access portal URL' (awsapps.com/start), 'Provisioning method' (SCIM), and 'Identity store ID' (d-). To the right of these fields is a 'Actions' dropdown menu, which is highlighted with a red box. The menu contains three options: 'Change identity source', 'Manage authentication', and 'Manage provisioning'.

AWS IAM Identity Center

AWS: External Identity Provider 선택

The screenshot shows the AWS IAM Identity Center interface. At the top, there's a navigation bar with the AWS logo, 'Services' button, search bar, and other account settings. Below the navigation, the path 'IAM Identity Center > Settings > Change identity source' is visible. On the left, a sidebar lists three steps: 'Step 1 Choose identity source' (selected), 'Step 2 Configure external identity provider', and 'Step 3 Confirm change'. The main content area is titled 'Choose identity source' and contains a descriptive paragraph about managing users and groups. It offers three options:

- 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.

A red box highlights the 'External identity provider' option. Below the options is a 'Learn more' link. At the bottom right, there are 'Cancel' and 'Next' buttons.

AWS IAM Identity Center

AWS: External Identity Provider 설정

The screenshot shows the AWS IAM Identity Center interface. In the top navigation bar, 'Services' is selected. The main title is 'Configure external identity provider'. On the left, a sidebar shows 'Step 1 Choose identity source' and 'Step 2 Configure external identity provider' (which is currently active). Below the sidebar, there are three tabs: 'AWS access portal sign-in URL' (selected), 'IAM Identity Center Assertion Consumer Service (ACS) URL', and 'IAM Identity Center issuer URL'. Each tab has a copy icon and a URL field. Under 'AWS access portal sign-in URL', the URL is 'https://[REDACTED].awsapps.com/start'. Under 'IAM Identity Center Assertion Consumer Service (ACS) URL', the URL is 'https://ap-northeast-2.sigin.aws.amazon.com/platform/saml/acs/[REDACTED]'. Under 'IAM Identity Center issuer URL', the URL is 'https://ap-northeast-2.sigin.aws.amazon.com/platform/saml/[REDACTED]'. At the bottom of the page, there are 'Cancel', 'Previous', and 'Next' buttons.

Service Provider metadata

- AWS의 metadata
- Okta에서 Integration 생성 시 정보 입력

Identity Provider metadata

- Okta의 metadata
- Okta Integration 완료 후 제공되는 정보 입력

AWS IAM Identity Center

Okta: App Catalog에서 Integration 추가

The screenshot shows the Okta application catalog interface. On the left, there is a sidebar with navigation links: Dashboard, Directory, Customizations, Applications (selected), Applications, Self Service, Security, Workflow, Reports, and Settings. The main content area shows the path: Applications > Catalog > Single Sign-On > AWS IAM Identity Center. At the top right, there is a search bar, a help icon, a user dropdown with email info@jkstechlab.com and user ID okta-dev-66452280, and a dropdown menu. Below the path, it says "Last updated: August 9, 2022". A prominent blue button labeled "Add Integration" is highlighted with a red box. To its right, there is a preview card for the "AWS IAM Identity Center" integration. The card features the AWS logo, tabs for "Workflow Templates", "SAML", "Workflows Connectors" (which has a cursor pointing at it), and "SCIM". Below the tabs, it says "Manage SSO access to your AWS accounts, roles, and applications". At the bottom of the card, there is a "Okta Verified" badge with a shield icon and some descriptive text about the integration's verification status.

okta

Search...

Dashboard

Directory

Customizations

Applications

Applications

Self Service

Security

Workflow

Reports

Settings

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

Last updated: August 9, 2022

Add Integration

AWS IAM Identity Center

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 IAM Identity Center

AWS: External Identity Provider 설정

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](https://[REDACTED].awsapps.com/start)

IAM Identity Center Assertion Consumer Service (ACS) URL.
<https://ap-northeast-2.sigin.aws.amazon.com/platform/saml/acs/>

IAM Identity Center issuer URL.
<https://ap-northeast-2.sigin.aws.amazon.com/platform/saml/>

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](#)

Advanced Sign-on Settings

These fields may be required for a AWS IAM Identity Center proprietary sign-on option or general setting.

AWS SSO ACS URL

Enter your AWS SSO ACS URL. Refer to the Setup Instructions above to obtain this value.

AWS SSO issuer URL

Enter your AWS SSO issuer URL. Refer to the Setup Instructions above to obtain this value.

Credentials Details

Application username format
 Okta username

Update application username on
 Create and update

Password reveal
 Allow users to securely see their password (Recommended)

Note: Password reveal is disabled, since this app is using SAML with no password.

[Save](#)

AWS IAM Identity Center

AWS: External Identity Provider 설정

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](https://[REDACTED].awsapps.com/start)

IAM Identity Center Assertion Consumer Service (ACS) URL
<https://ap-northeast-2.sigin.aws.amazon.com/platform/saml/acs/>

IAM Identity Center issuer URL
<https://ap-northeast-2.sigin.aws.amazon.com/platform/saml/>

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](#)

okta

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](#)

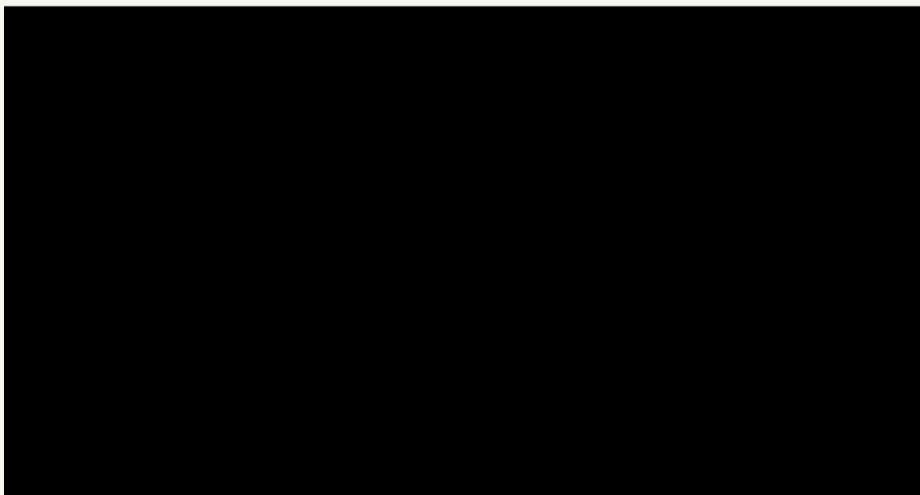
Signing Certificate

[Download](#) [Copy](#)

Certificate fingerprint

[View SAML setup instructions](#)

Demo & Tips



AWS IAM Identity Center

웹 콘솔에 로그인해봅시다

The screenshot shows the Remember web console interface. On the left, there's a sidebar with navigation links: '내 앱' (My Apps), 'Drama&Company', '섹션 추가 +', '알림 1', and '앱 추가'. The main area is titled '내 앱' (My Apps) and shows a section for 'Drama&Company' with various app icons: Google Workspace Drive, Slack, Atlassian Cloud Jira SAML, Confluence, AWS, and AWS Workspaces. The 'AWS' icon is highlighted with a red box. Below this, there's a link '+ 섹션 추가' (Add section). On the right side of the main area, there's a search bar with '앱 검색' (Search app), a '관리자' (Administrator) button, and a dropdown menu showing '정민 드라마엔컴퍼니 (Drama&...)' and a '정렬' (Sort) button. At the bottom, there's a '지원' (Support) link and a blue '앱 요청' (App Request) button. A note at the bottom left says '마지막 로그인: 몇 초 전' (Last login: a few seconds ago) and '개인 정보 보호' (Data protection).

정렬

Okta 대시보드에서 AWS 앱 접속

지원

마지막 로그인: 몇 초 전

개인 정보 보호

앱 요청

AWS IAM Identity Center

웹 콘솔에 로그인해봅시다

The screenshot shows the AWS SSO Dashboard. At the top, there's a navigation bar with the AWS logo, a search bar labeled "Search", and links for "정민", "MFA devices", and "Sign out". Below the navigation bar is a section titled "AWS SSO 대시보드에서 접근 가능한 계정 확인". This section contains a list of accounts, each represented by a small orange hexagon icon and a truncated email address. The list includes "a", "dr", "di", "dr", "dr", "dr", "re", and "re". Each account entry has a dropdown arrow icon on the right. To the left of this list is a box containing an orange cube icon and the text "AWS Account (9)". A cursor arrow is visible on the far left.

Account
a
dr
di
dr
dr
dr
re
re

AWS IAM Identity Center

웹 콘솔에 로그인해봅시다

AWS Account (9)

계정 별로 Assume 가능한 IAM Role 확인

Role Name	Assume Options
drama-devops	Management console Command line or programmatic access
drama-dev-	Management console Command line or programmatic access
drama-devops	Management console Command line or programmatic access

AWS IAM Identity Center

웹 콘솔에 로그인해봅시다

Federated User 정보에서
SSO를 통해 접속했음을 확인

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

Recently visited

- EC2
- WorkSpaces
- S3
- Systems Manager
- CloudTrail
- Elastic Container Service
- CodePipeline
- Route 53
- IAM
- CodeBuild
- CloudFront
- Elastic Container Registry
- Key Management Service
- AWS Marketplace Subscriptions

View all services

AWS Health

Open issues 1 Past 7 days

Scheduled changes

Cost and usage

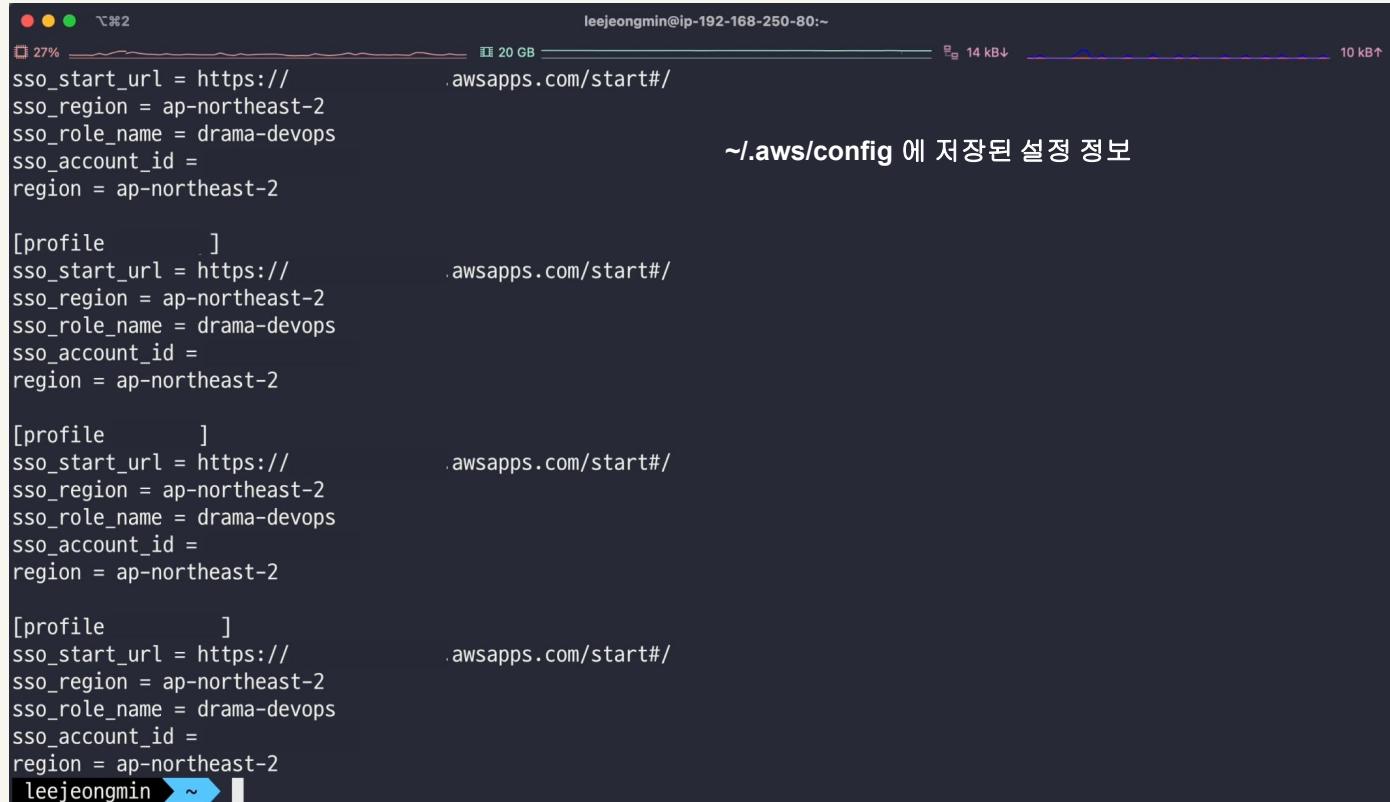
Switch role Sign out

CloudShell Feedback Language

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS IAM Identity Center

CLI도 로그인해봅니다



The screenshot shows a macOS terminal window with the following details:

- Terminal title: leejeongmin@ip-192-168-250-80:~
- Background: A dark-themed desktop background.
- Terminal content:

```
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

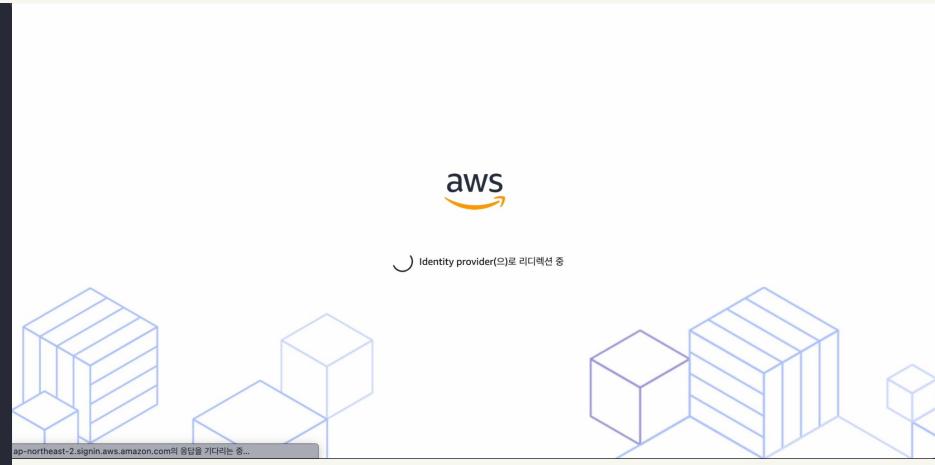
[profile      ]
sso_start_url = https://awsapps.com/start#
sso_region = ap-northeast-2
sso_role_name = drama-devops
sso_account_id =
region = ap-northeast-2
leejeongmin ➤ ~ ]
```
- Status bar: Shows battery level (27%), disk usage (20 GB), network speed (14 kB↓), and upload speed (10 kB↑).

AWS IAM Identity Center

CLI도 로그인해봅니다

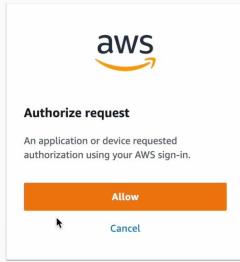
```
25% ~ 20 GB 1.0 kB+ 0.0 kB↑
leejeongmin ~ aws-vault exec ops

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



AWS IAM Identity Center

CLI도 로그인해봅니다

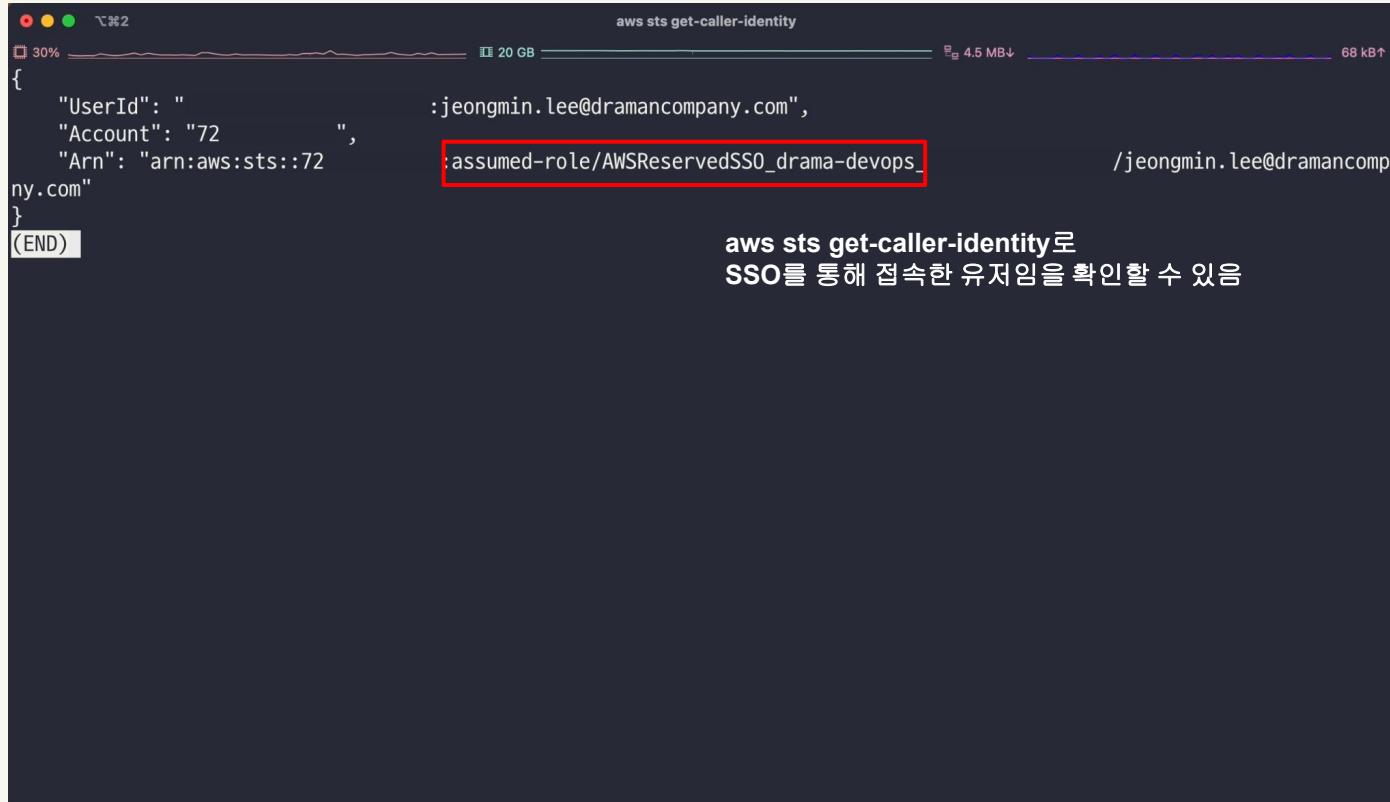


```
leejongmin ~ aws-vault exec ops
Opening the SSO authorization page in your default browser (use Ctrl-C to abort)
https://device.sso.ap-northeast-2.amazonaws.com/?user_code=BKQ-XBSX
Starting subshell /bin/zsh, use `exit` to exit the subshell
leejongmin ~
```

**Authorize Request Allow 시
CLI 접속 환경에 Temporary Credential 발행**

AWS IAM Identity Center

CLI도 로그인해봅니다



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

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

AWS IAM Identity Center

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>

AWS IAM Identity Center

Tip: IAM Identity Center는 Delegated Administrator*를 설정합시다

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

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

Q&A



Q&A

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

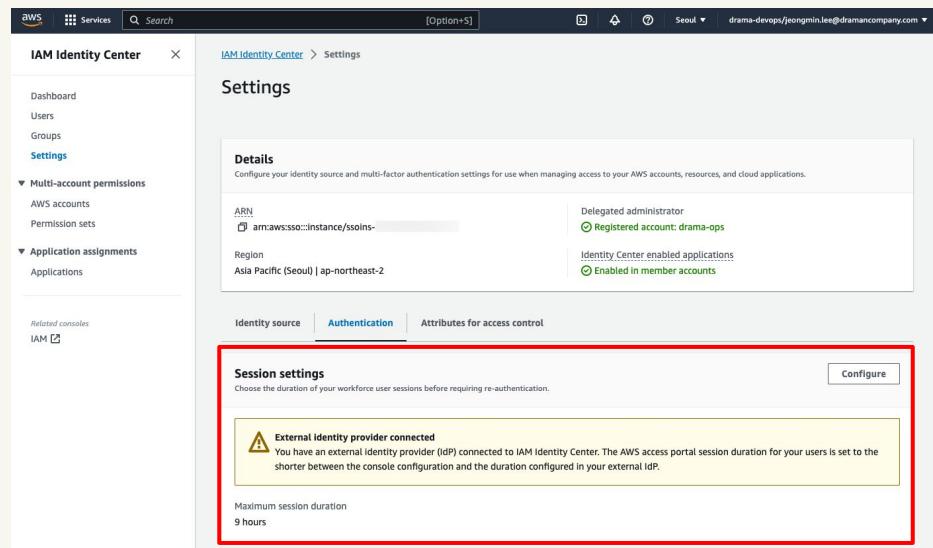
A. 정책적으로 해결할 수 밖에 없는 문제라고 생각합니다.

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&A

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&A

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