Okta를 이용한
AWS Multi-Account 환경 관리

Drama & Company Co,. Ltd

이정민 (Tony)

Remember

Contents

IdP
: Identity Provider

Single Source of Truth

The Central Source of Identity

IdP

Remember

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

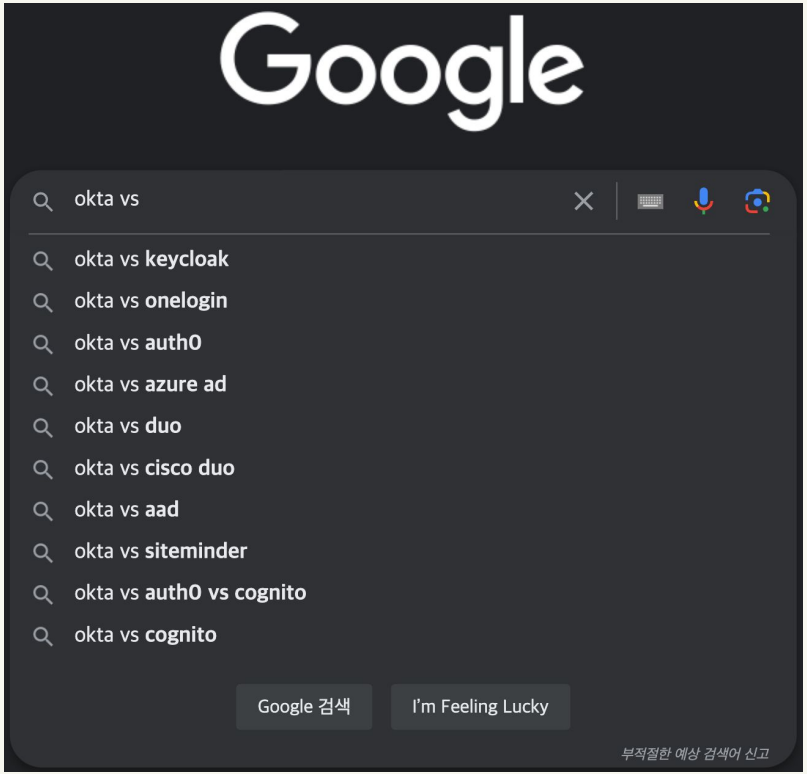
직접 운영하지 않아도 되고

여러 서비스와 연동하기 쉽고

주변 레퍼런스가 매우 많아요

Remember

Q. AWS IAM Identity Center도 IdP가 된다던데?

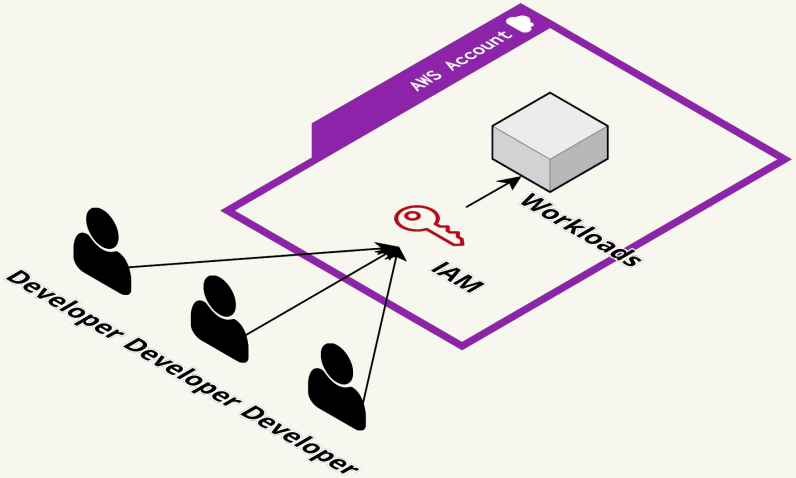


AWS Multi-Account 환경 어떻게 관리할까

Remember

IAM User로 사용자 계정을 분리할 수 있다.

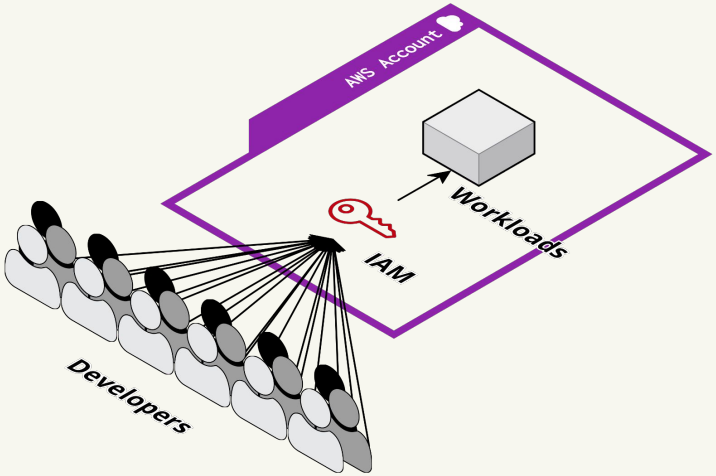
- 접근해야 하는 AWS 계정이 적거나
- 접근하는 유저가 소수일 때

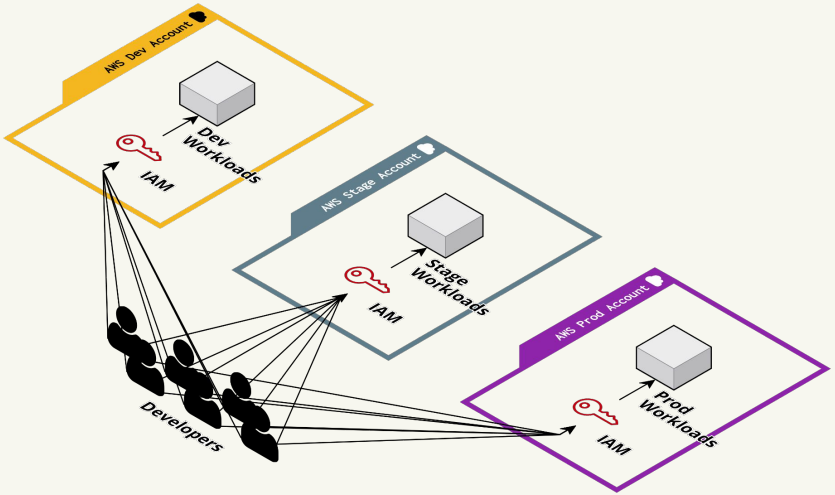


AWS IAM Identity Center

Remember

하지만..





접근해야 하는 유저가 늘어난다면?

접근해야 하는 계정이 늘어난다면?

Remember

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

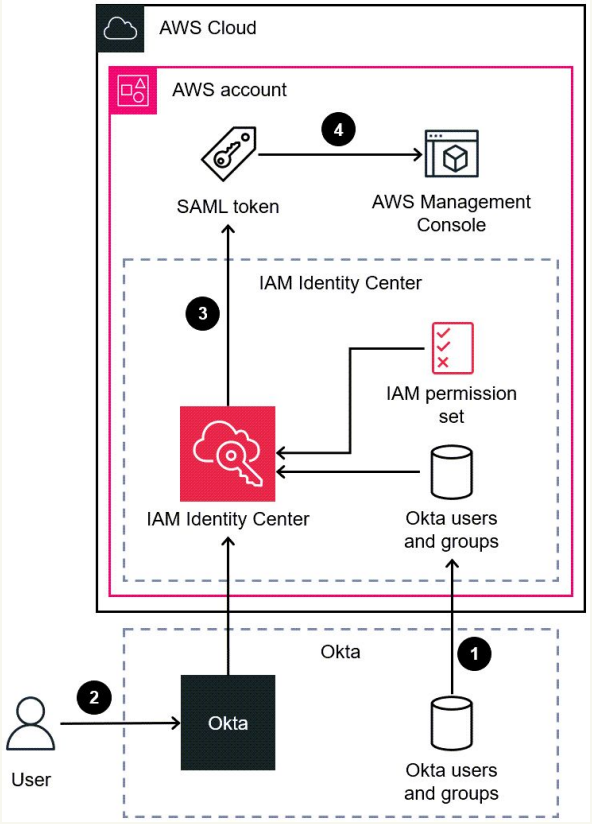
Remember

AWS IAM Identity Center*를 사용해봅시다.

Okta도 살짝 얹어서요.

* 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)

Source:https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/integrate-okta-with-aws-iam-identity-center-to-manage-users-roles-and-multi-account-access.html

AWS
IAM Identity Center
설정

AWS IAM Identity Center

Remember

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.)

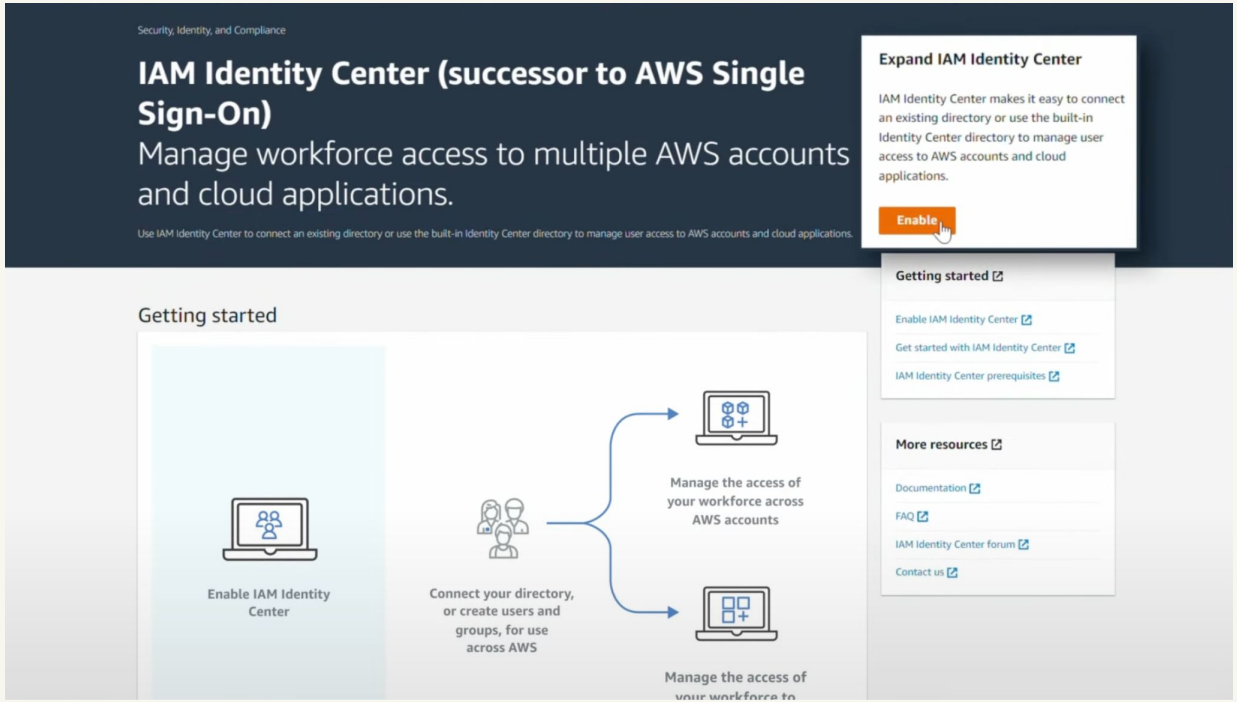
그 외에는..

IAM Identity Center는 Organization의 1개 리전에만 프로비저닝 가능해요.

AWS IAM Identity Center

Remember

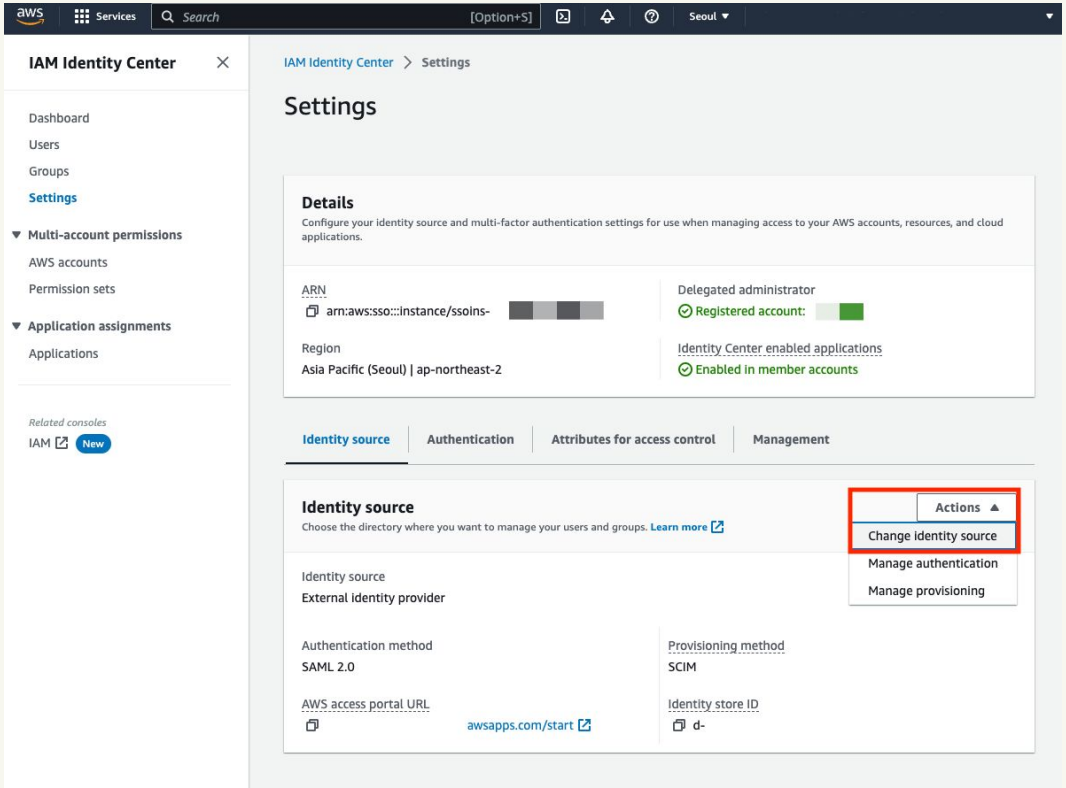
AWS: IAM Identity Center 콘솔에서 기능 활성화



AWS IAM Identity Center

Remember

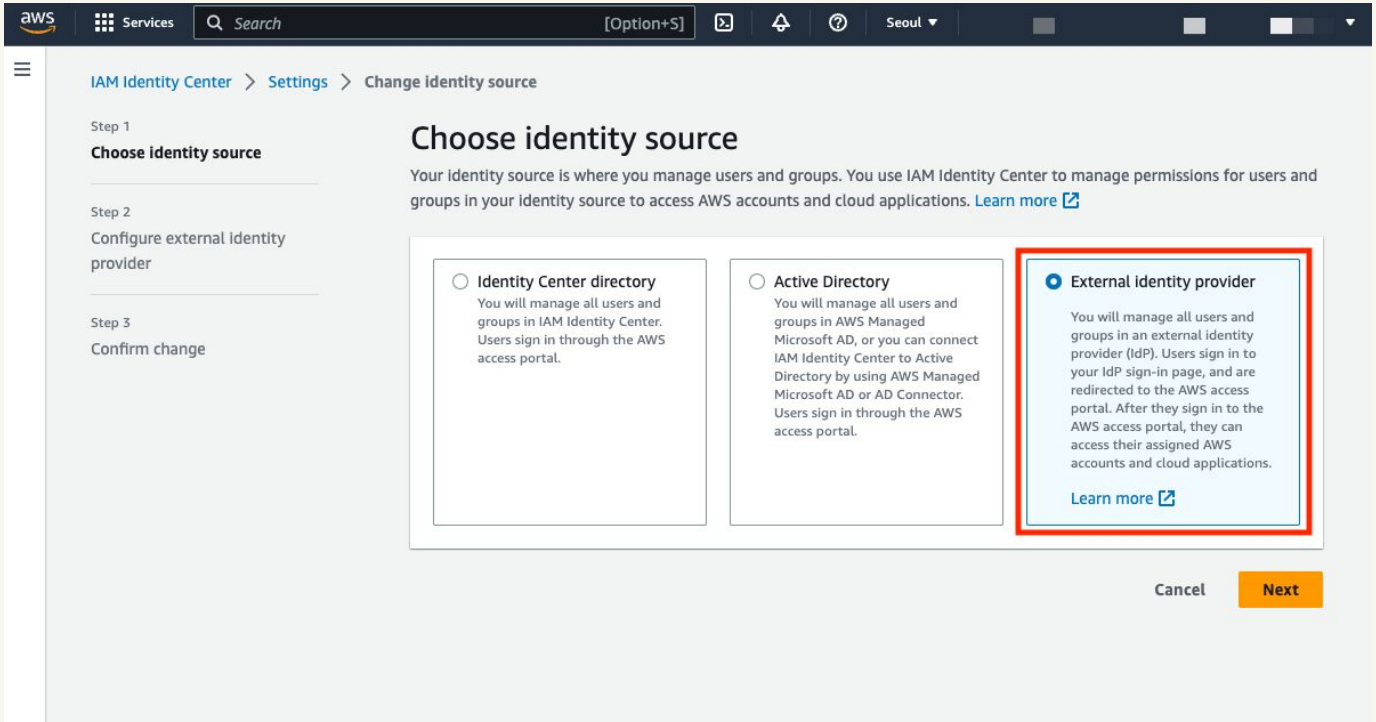
AWS: Settings -> Identity source -> Change Identity Source 선택



AWS IAM Identity Center

Remember

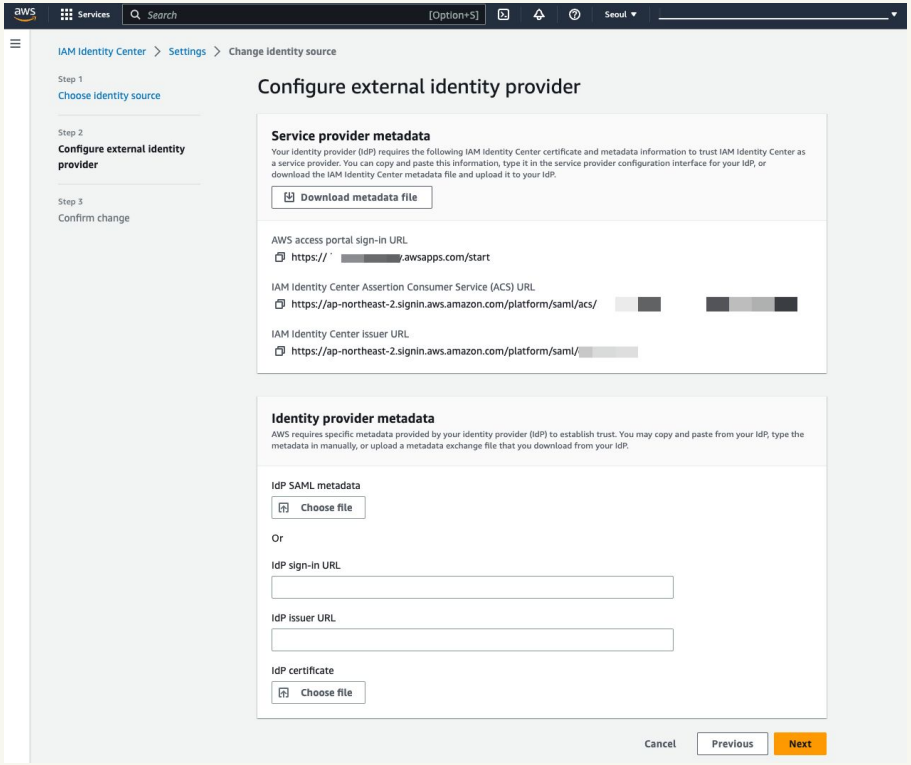
AWS: External Identity Provider 선택



AWS IAM Identity Center

Remember

AWS: External Identity Provider 설정



Service Provider metadata

- AWS의 metadata
- Okta에서 Integration 생성 시 정보 입력

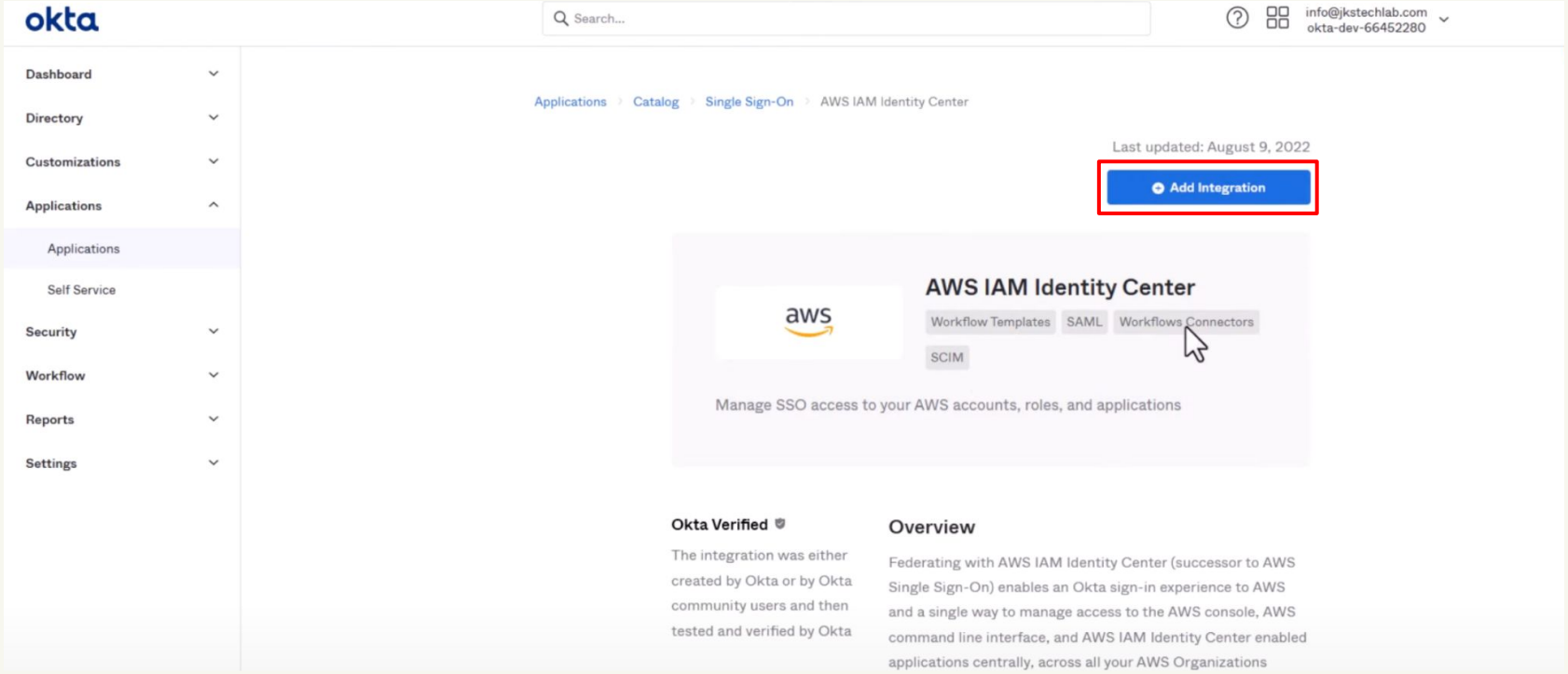
Identity Provider metadata

- Okta의 metadata
- Okta Integration 완료 후 제공되는 정보 입력

AWS IAM Identity Center

Remember

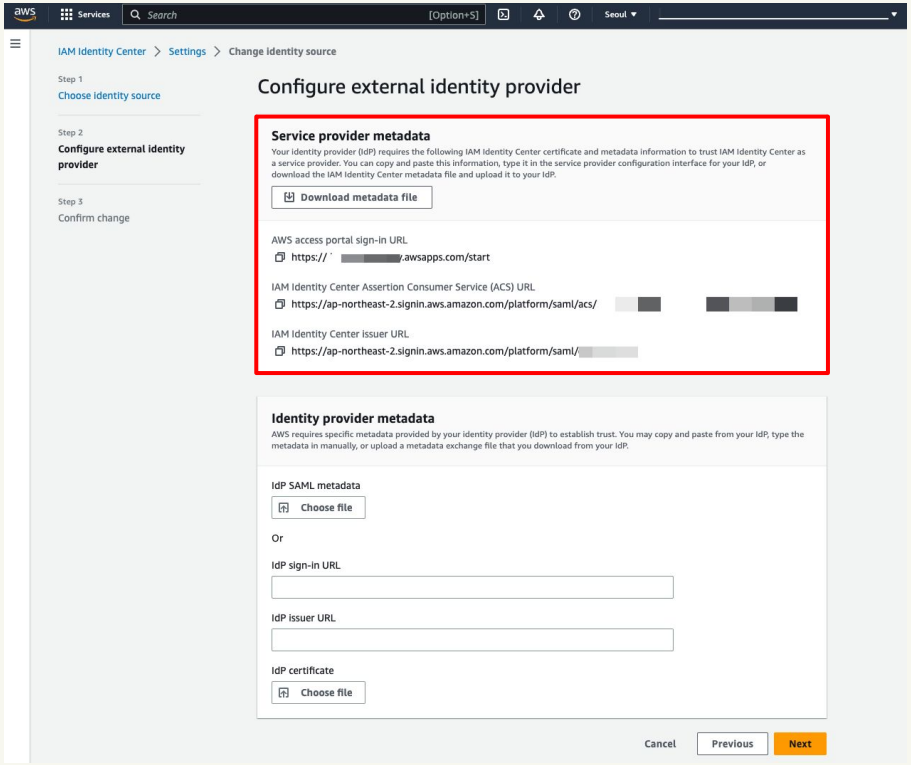
Okta: App Catalog에서 Integration 추가

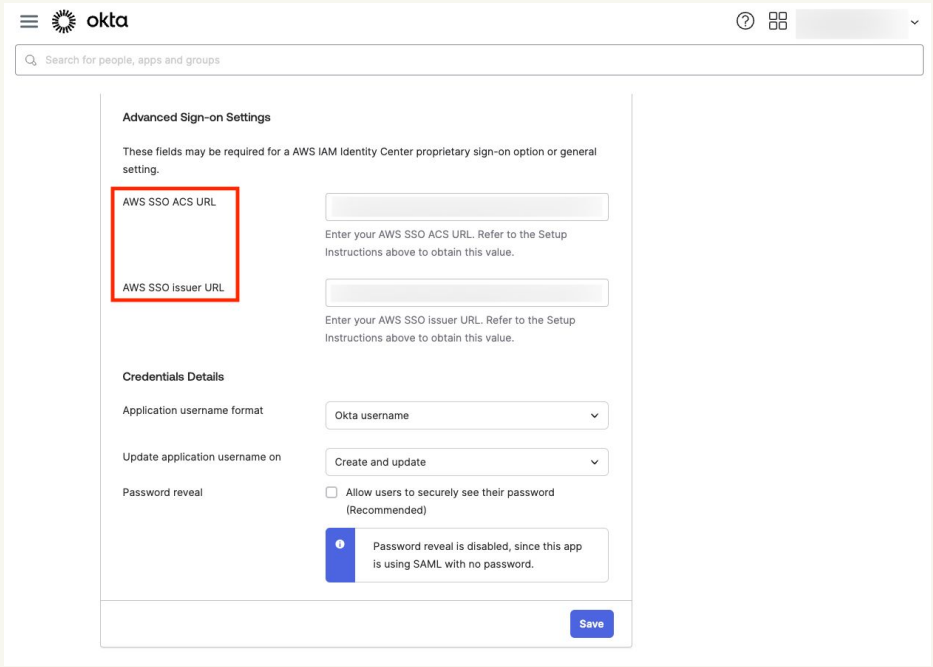


AWS IAM Identity Center

Remember

AWS: External Identity Provider 설정

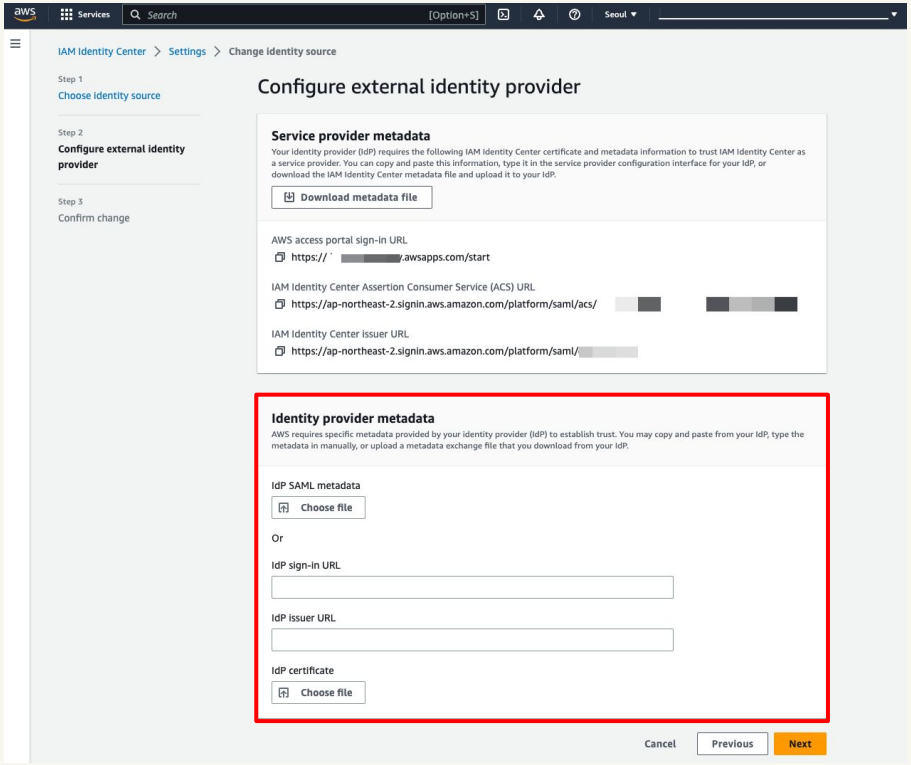


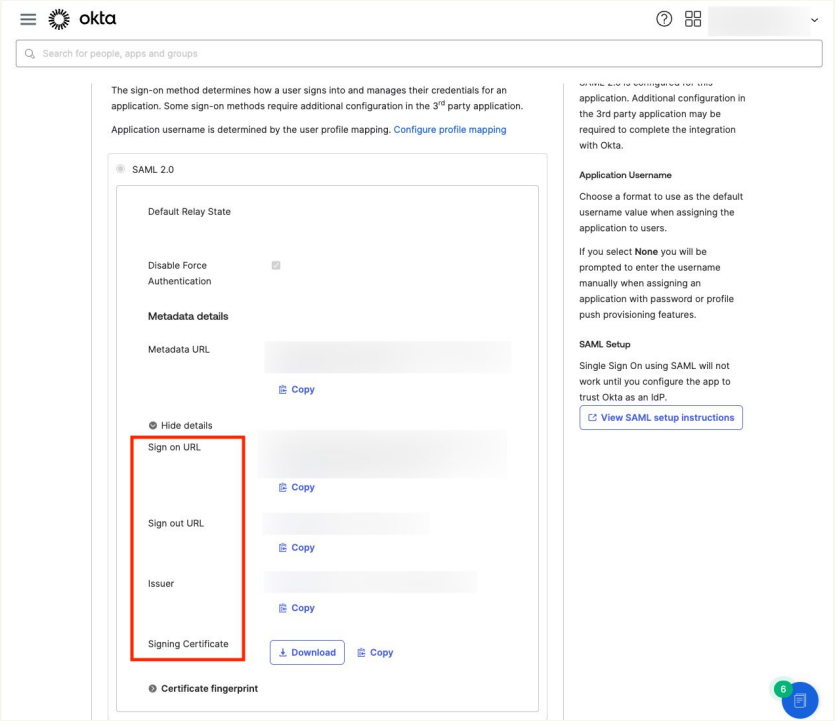


AWS IAM Identity Center

Remember

AWS: External Identity Provider 설정



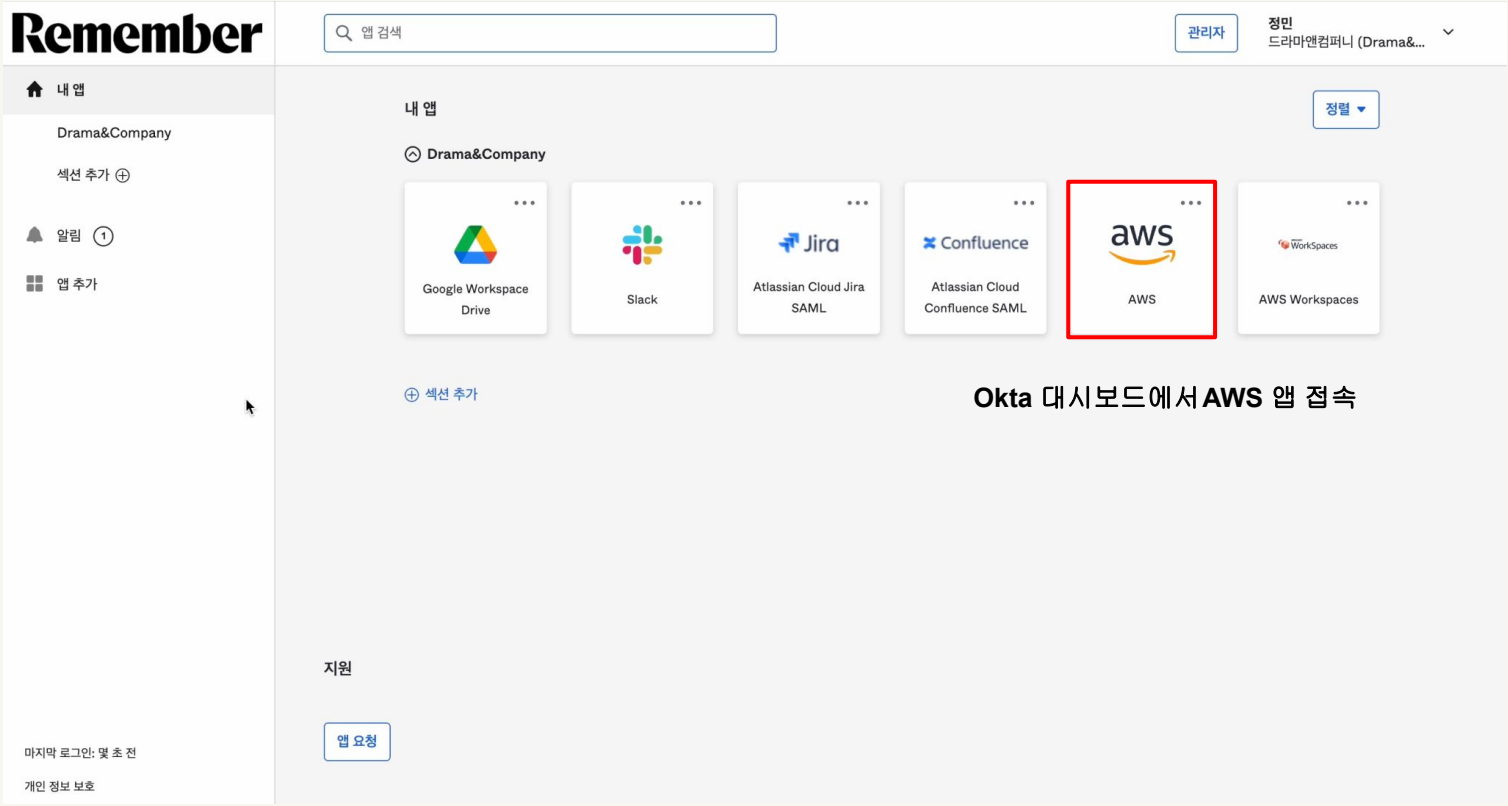


Demo & Tips

AWS IAM Identity Center

Remember

웹 콘솔에 로그인해봅시다

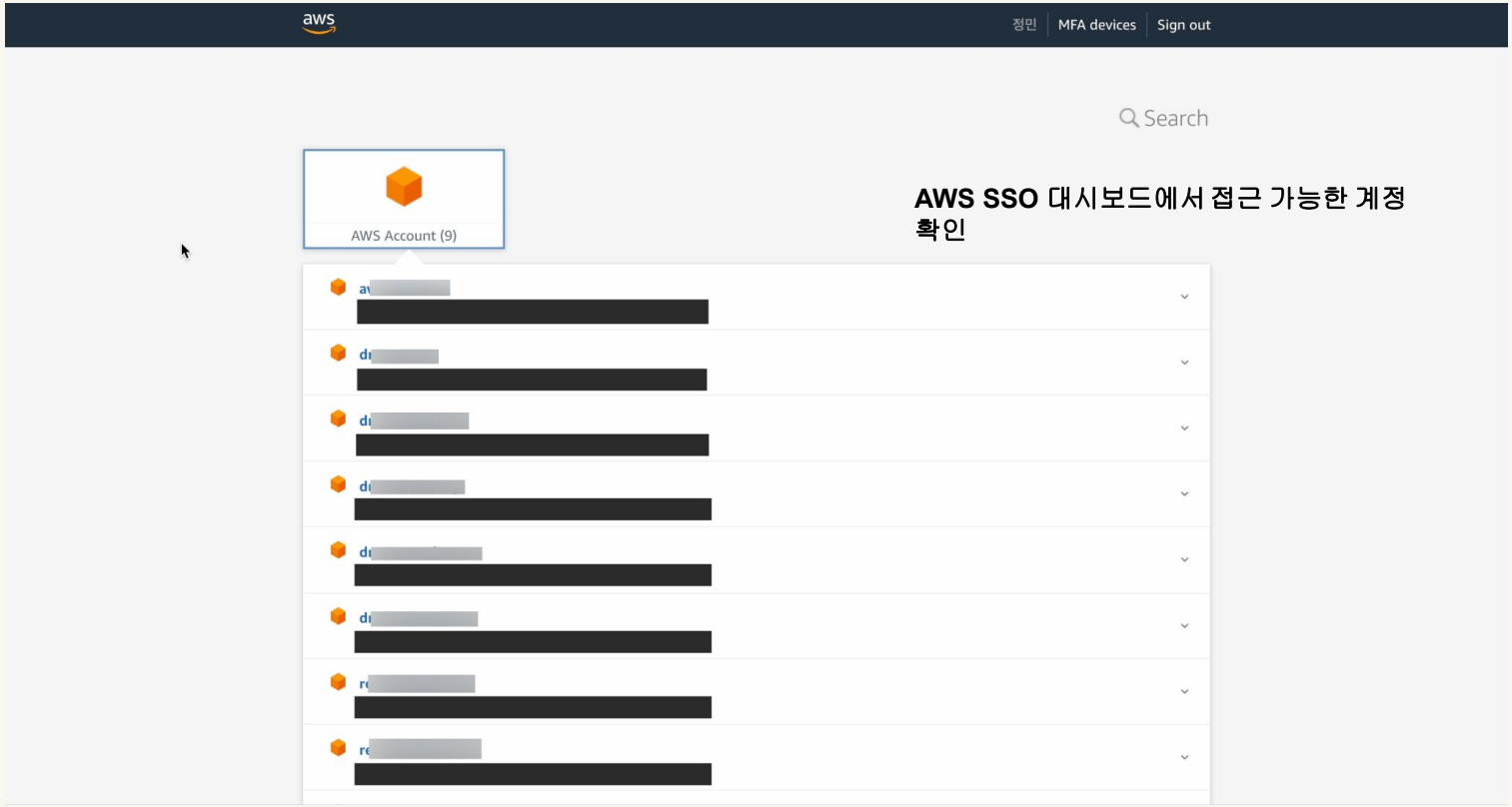


Okta 대시보드에서 AWS 앱 접속

AWS IAM Identity Center

Remember

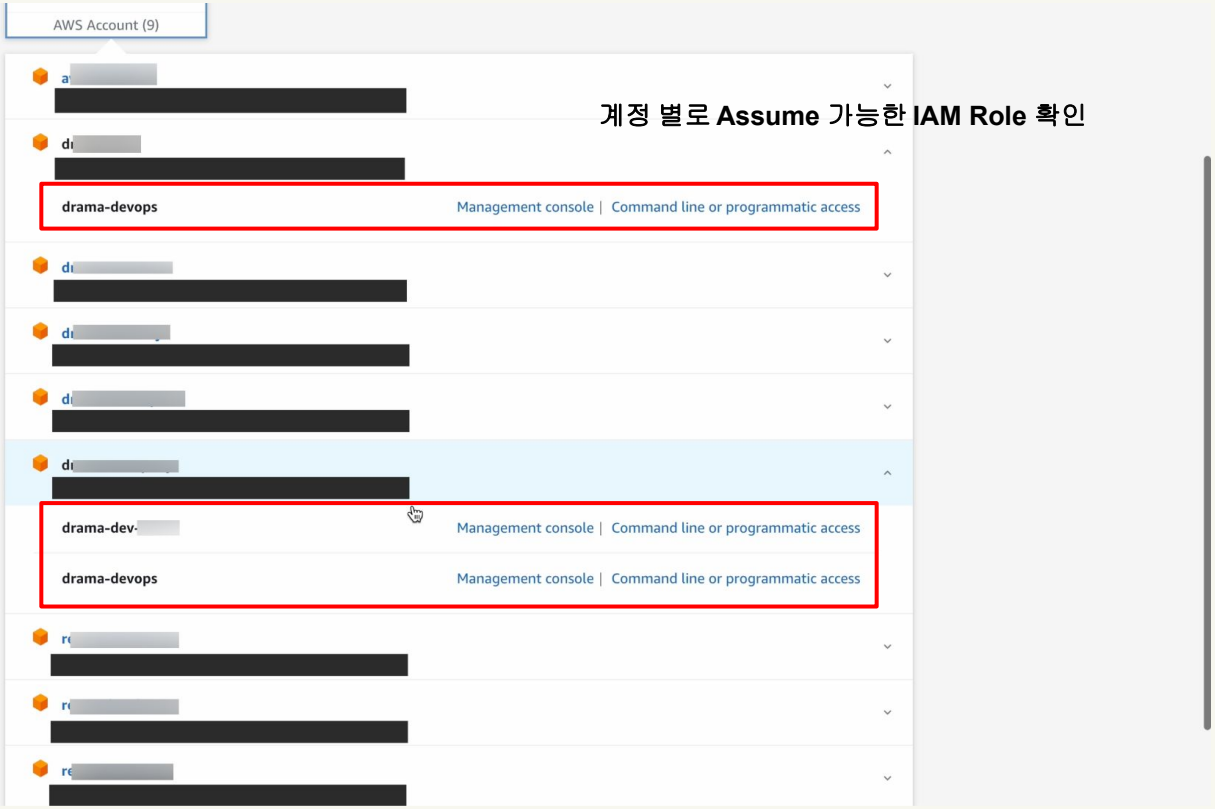
웹 콘솔에 로그인해봅시다



AWS IAM Identity Center

Remember

웹 콘솔에 로그인해봅시다

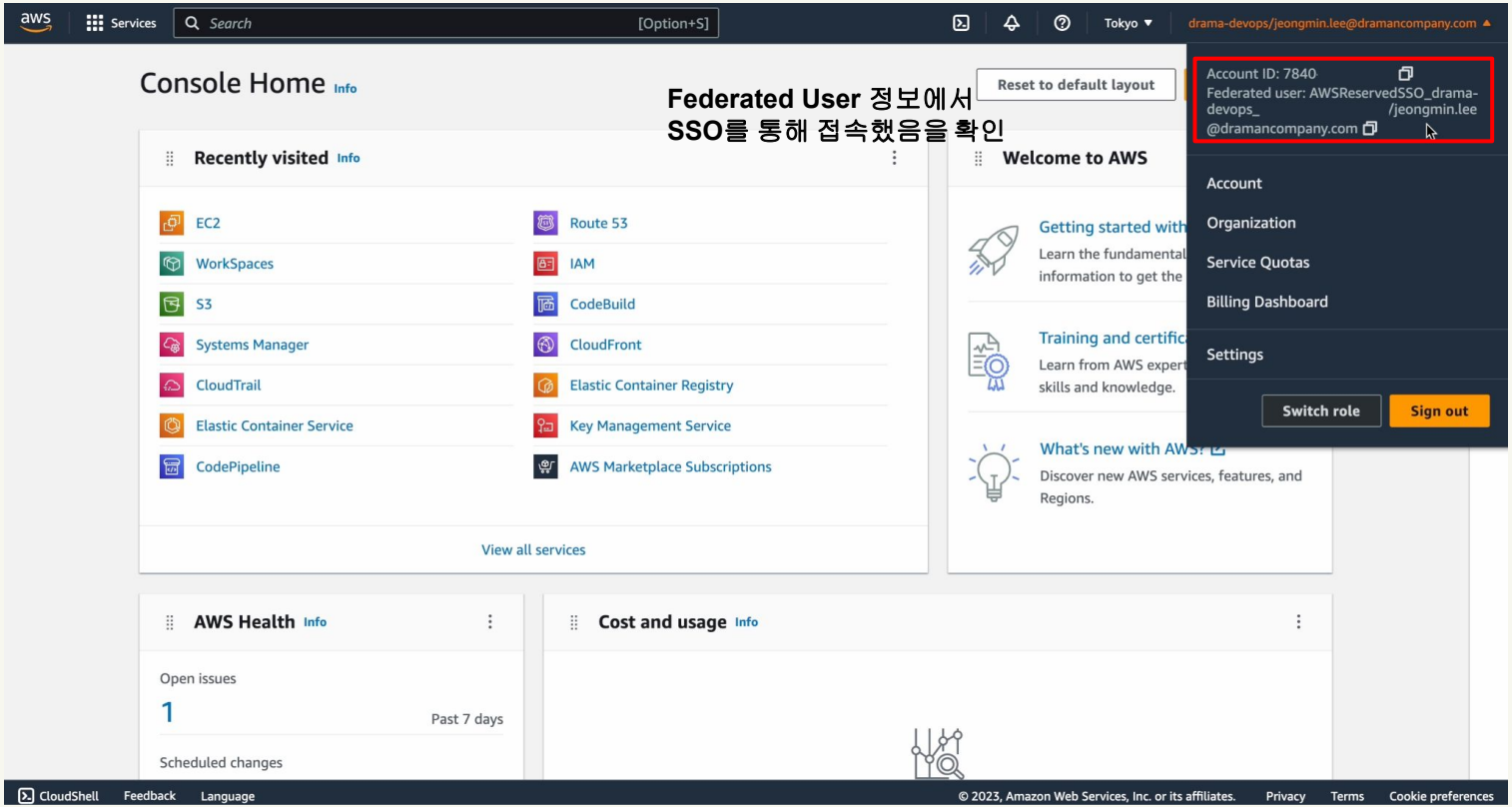


계정 별로 Assume 가능한 IAM Role 확인

AWS IAM Identity Center

Remember

웹 콘솔에 로그인해봅시다



AWS IAM Identity Center

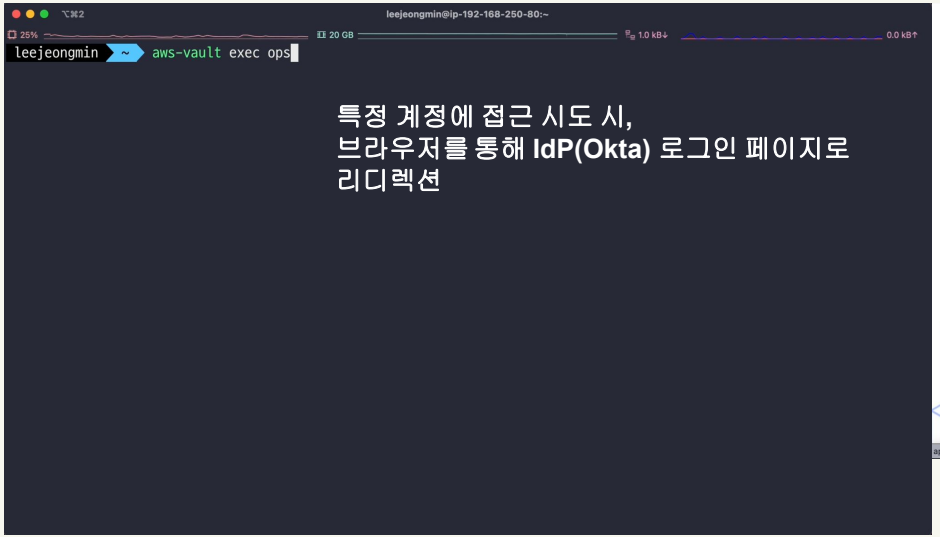
Remember

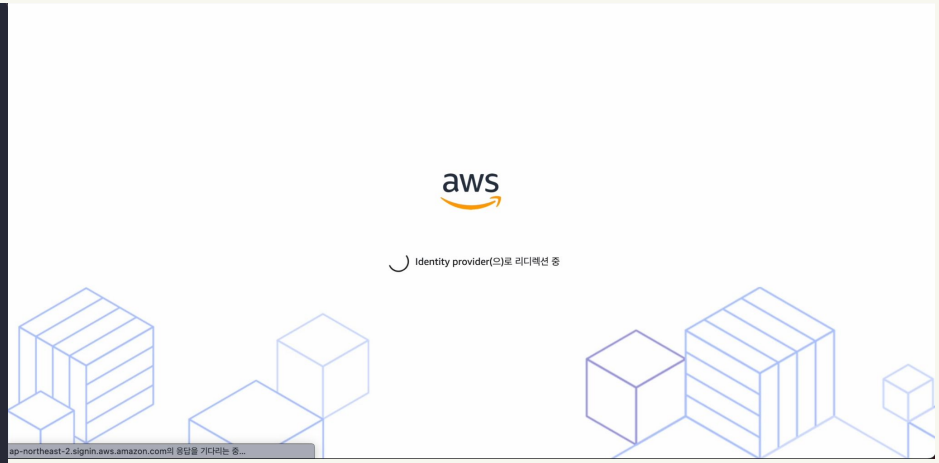
CLI도 로그인해봅니다

AWS IAM Identity Center

Remember

CLI도 로그인해봅니다

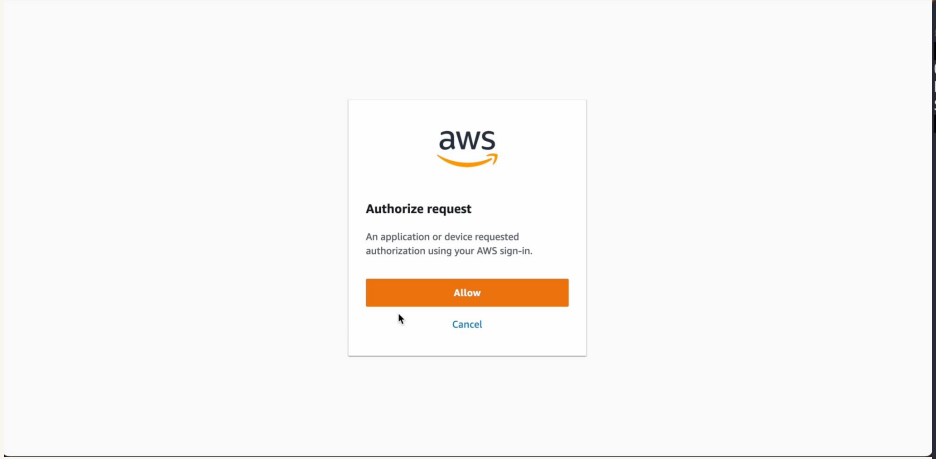


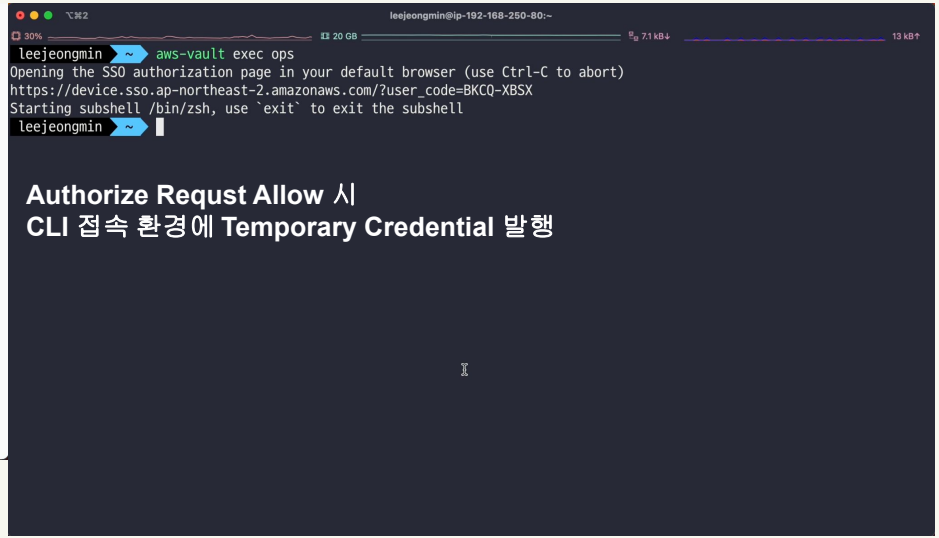


AWS IAM Identity Center

Remember

CLI도 로그인해봅니다

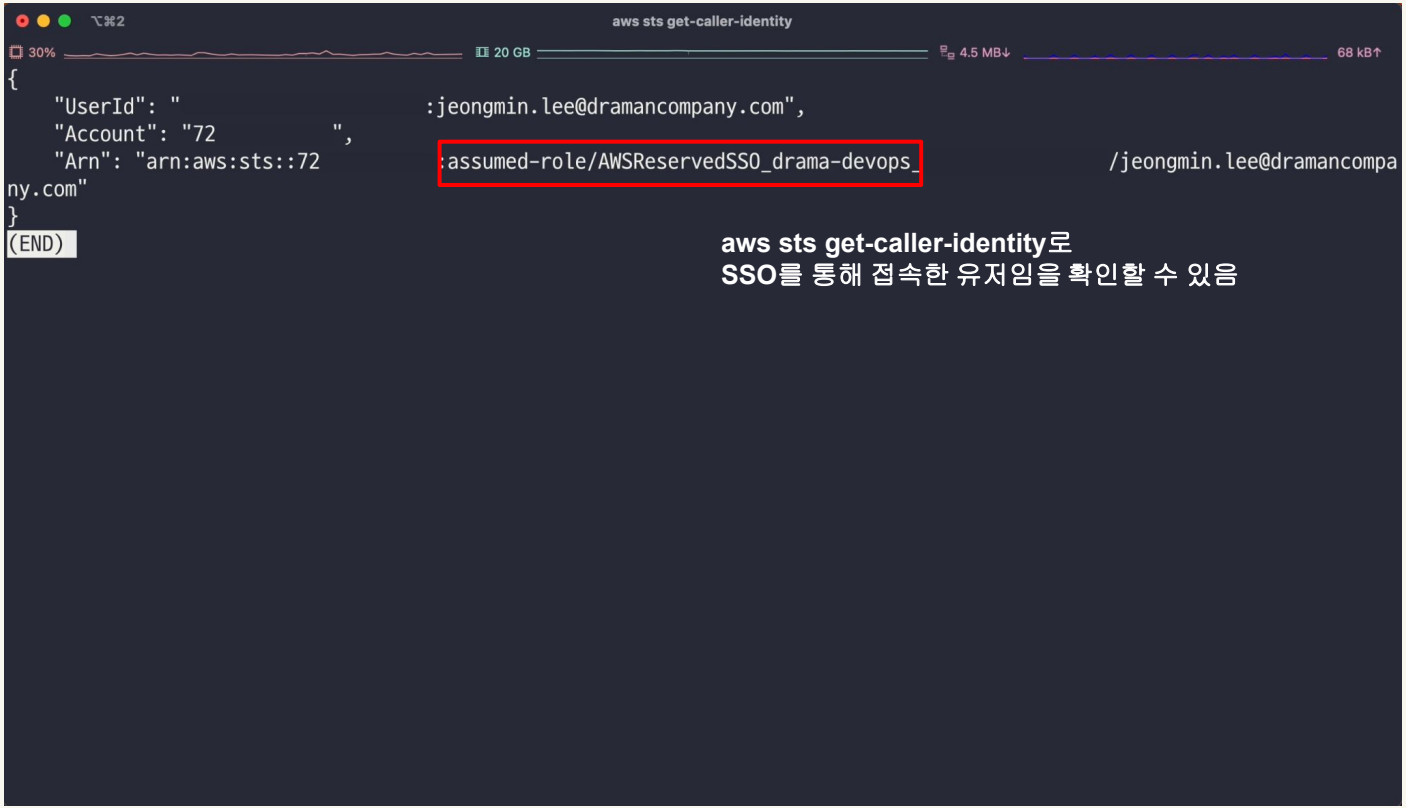




AWS IAM Identity Center

Remember

CLI도 로그인해봅니다



AWS IAM Identity Center

Remember

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

Remember

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

Remember

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.

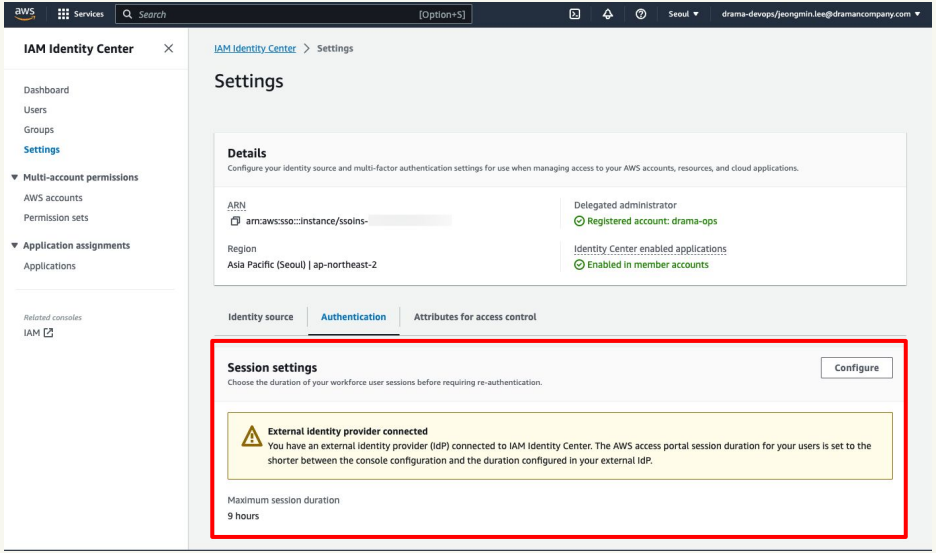
Q&A

Remember

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

Remember

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

Remember

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