BRAINLY

GETTING STARTED WITH AWS

The proper way - No more IAM users

May 2024

Agenda

1. About the presenter

2. Introduction

3. Step-by-step setup

4. Adding other accounts and setting CLI

5. Summary

Krzysztof Szyper

Solutions Architect,

Production Infrastructure team,

Brainly

- Wrote first programs at 6yo with C-64.
- Using AWS since 2012.
- SysOps and DevOps background.
- Everything-as-Code enthusiast.
- Managing low-level cloud infrastructure.
- After work doing some portrait and aviation photography.

#1 AI EDU APP IN THE WORLD

AI Learning Companion™
15M daily active users
250M+ answers in Knowledge Base

QUICK COMPARISON

IAM USERS

- Simple solution to start with
- Complex to maintain with more than one user or AWS account
- Long-lived keys pose security risk

SAML WITH IAM ROLES

- Not straightforward, needs 3rd party service
- Scales easily with users and accounts
- RBAC out of the box
- Session token live for only few hours

IT CAN BE FAMILIAR

If you're working in a company with many AWS accounts you may already be using this approach.

IS IT WORTH THE EFFORT

Splitting your personal AWS account to many and using SAML will let you learn about workloads, cross-account access, etc.
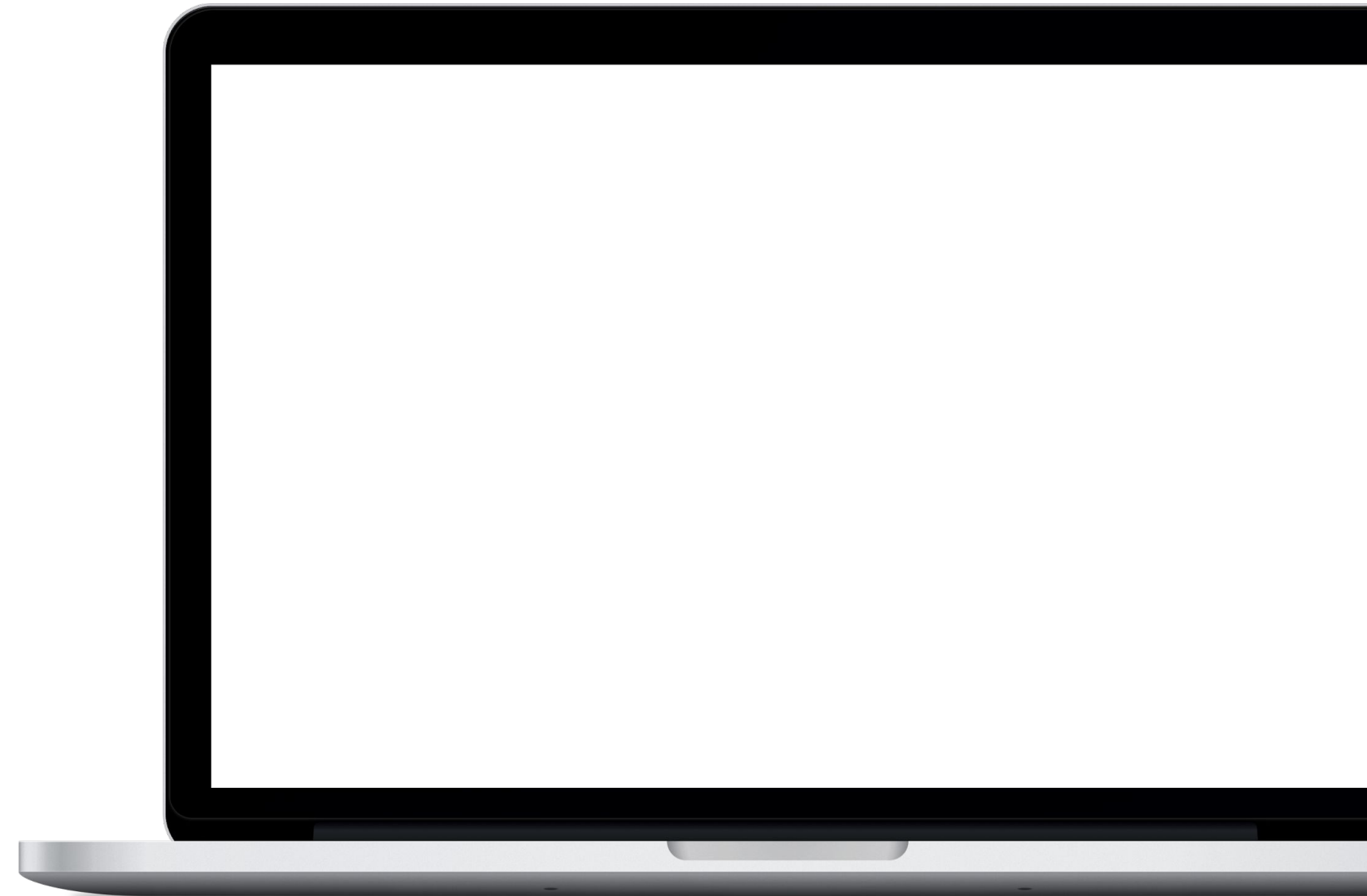
Step-by-step guide

This is simplified setup to demonstrate idea and initial setup
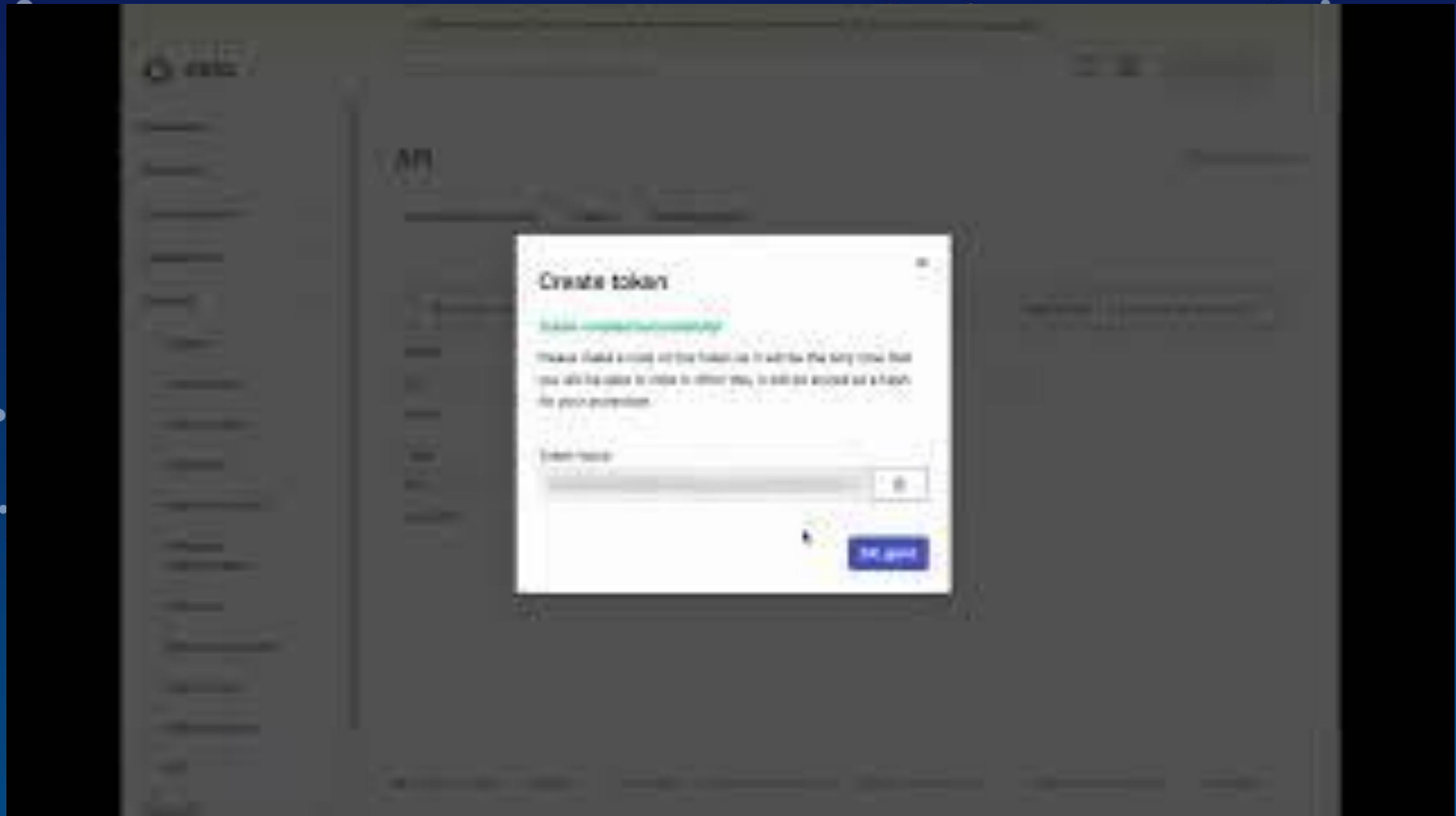
What is needed in this example?

- Unix-like OS
- Terraform
- Okta account
- At least one AWS account

OKTA API TOKEN

Token will be used by Terraform to provision Okta resources.
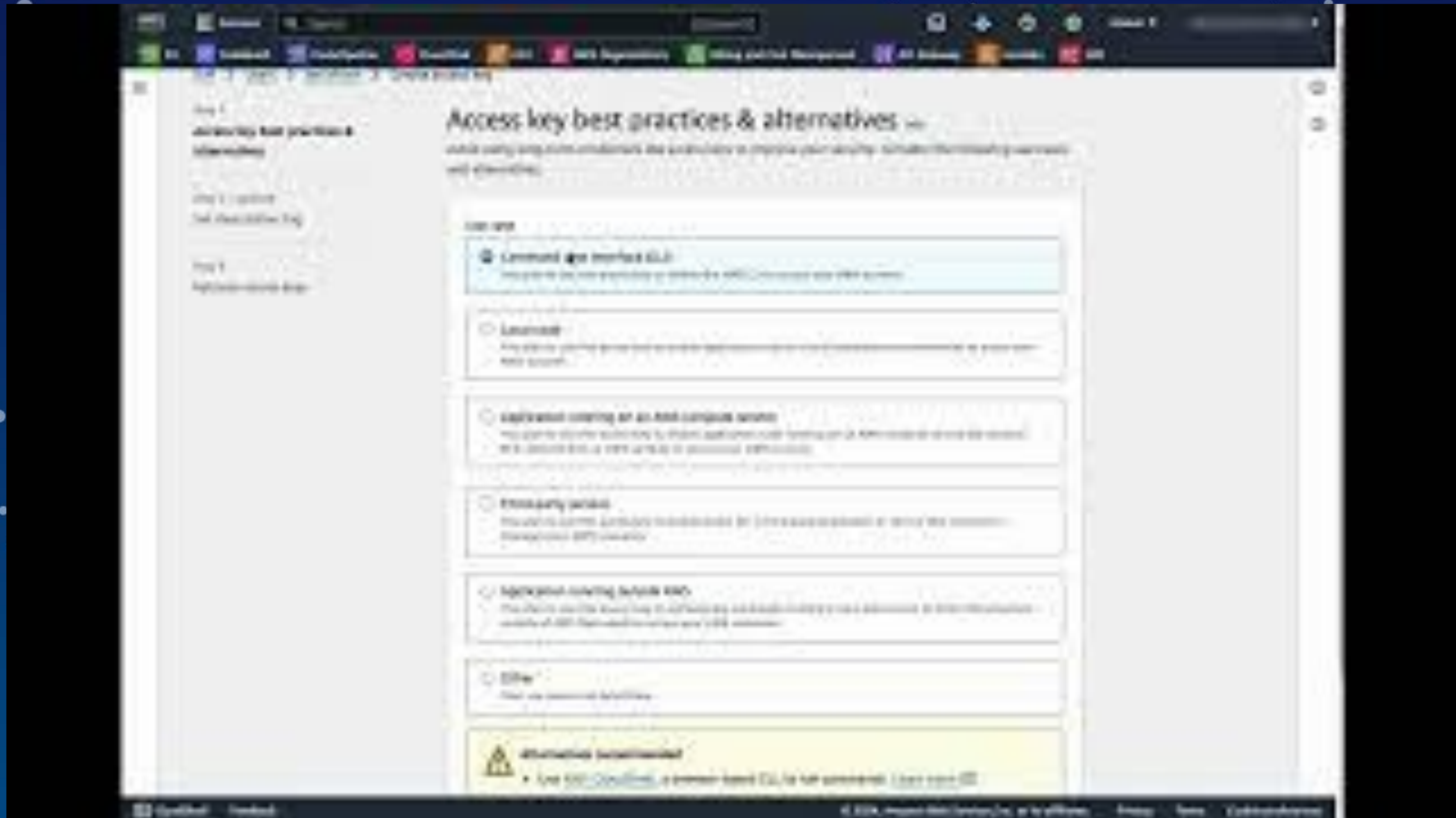
CREATE OKTA API TOKEN FOR TERRAFORM

IAM user for initial provisioning of AWS resources.
Can be deleted afterwards.

CREATE AWS IAM USER FOR TERRAFORM

Okta token and AWS credentials for Terraform providers.

SET CREDENTIALS IN TERMINAL

User access assignment and initial configuration,
e.g. Okta organization.

PREPARE TERRAFORM CODE

PROVISION RESOURCES

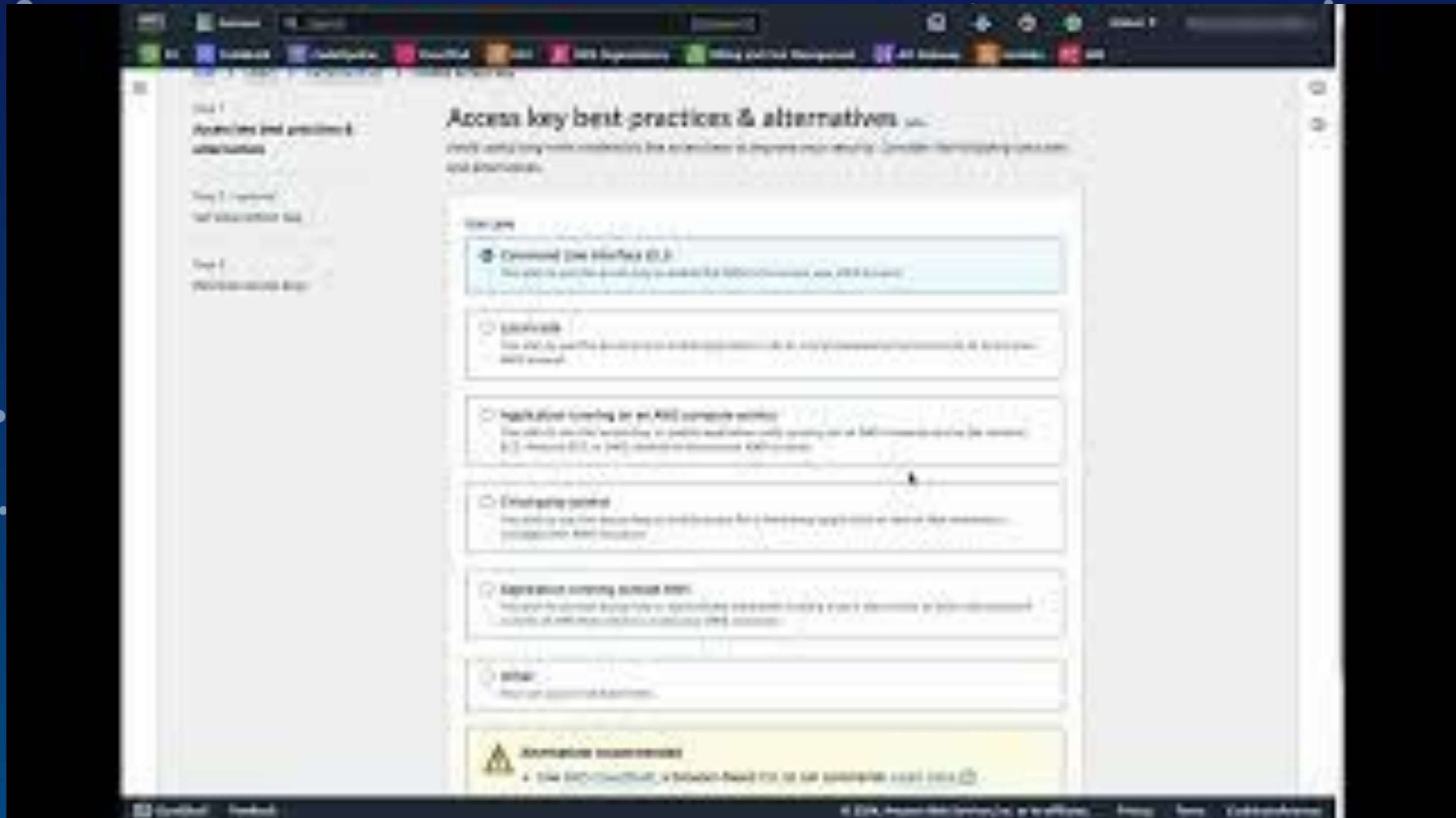# SAML app and access groups in Okta, IAM user and roles for Okta in AWS.

RUN TERRAFORM APPLY

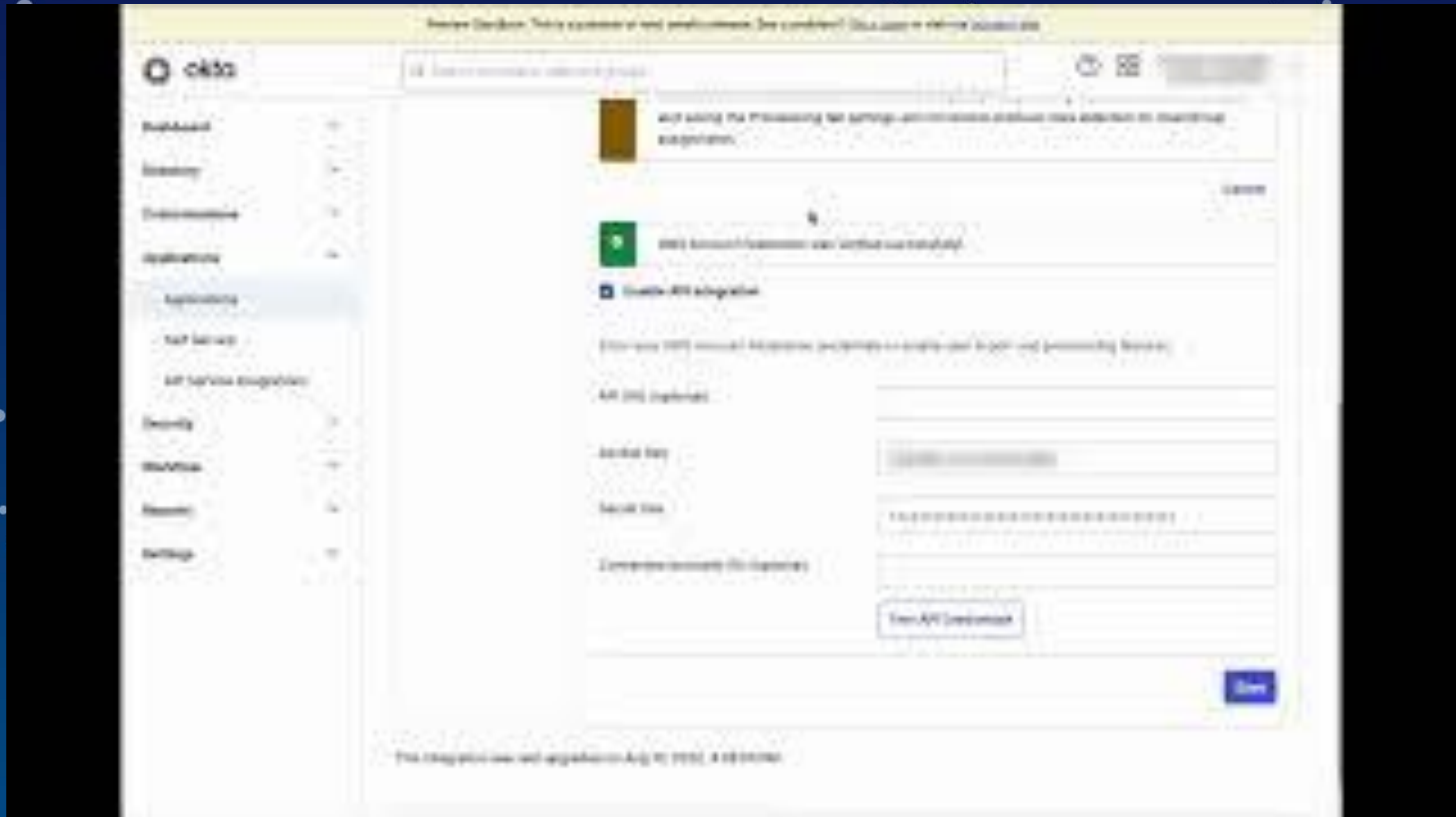## IAM ACCESS KEYS FOR OKTA

Keys will be used to read IAM roles and assume them in all AWS accounts.

GET KEYS FOR OKTA IAM USER

Enter those IAM access keys in Okta provisioning configuration.

UPDATE OKTA PROVISIONING
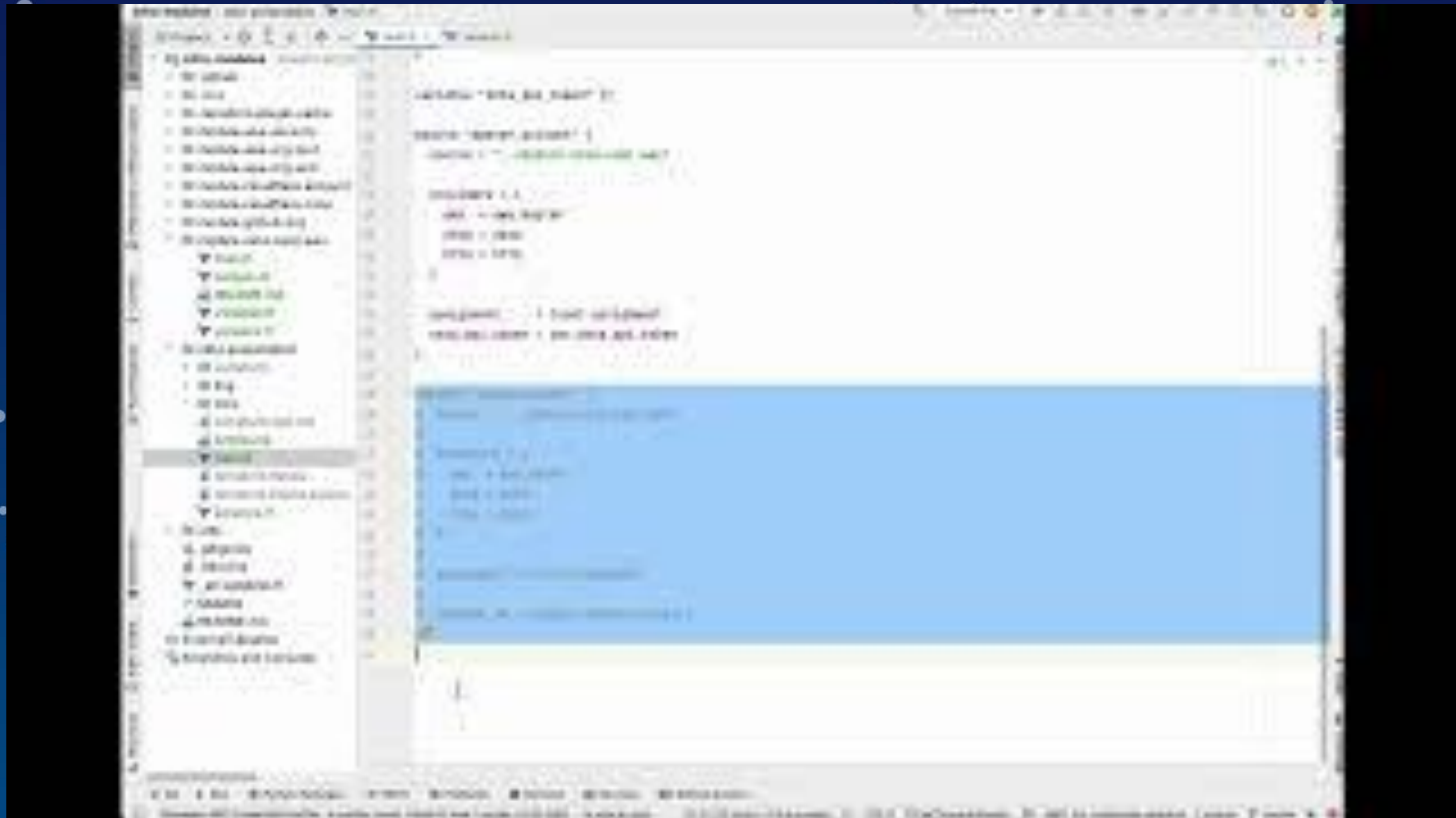
For each AWS account IAM user is needed to provision initial AWS resources.

User can be deleted later.

ADD ANOTHER ACCOUNT

Setup <u>gimme-aws-creds</u> (presenters's favorite) to assume IAM roles in terminal.
Will require updating profiles for AWS providers in Terraform, but IAM users can be deleted.

CLI FOR TERRAFORM AND TERMINAL

Summary

Some bonus tips to grow faster

That's only a beginning, now...

Scale with Terragrunt

With it you don't need to create IAM users in AWS sub-accounts. It will create IAM role for each one under the hood and use it.

Use auto-provisioning

Assigning to Okta groups can be easily automated, so every new user having specified attribute can gain access to roles and accounts on creation.

Use CI/CD tools

Automating low-level infrastructure and configuration can make any change easier. For example native AWS CodeBuild and CodePipeline.

BRAINLY

THANK YOU

Krzysztof Szyper

MORE INFORMATION

github.com/ChristophShyper/presentation-okta-saml-aws

https://bit.ly/AWSxGP