

# GETTING STARTED WITH AWS

The proper way - No more IAM users

May 2024

#### **OKTA SAML WITH AWS**

#### Agenda

- 1. About the presenter
- 2. Introduction
- 3. Step-by-step setup
- 4. Adding other accounts and setting CLI
- 5. Summary



#### **PRESENTER**

#### **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.



2024 / brainly.com

## #1 AI EDU APP IN THE WORLD

Al Learning Companion<sup>tm</sup>
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.



2021 / brainly.com

#### 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

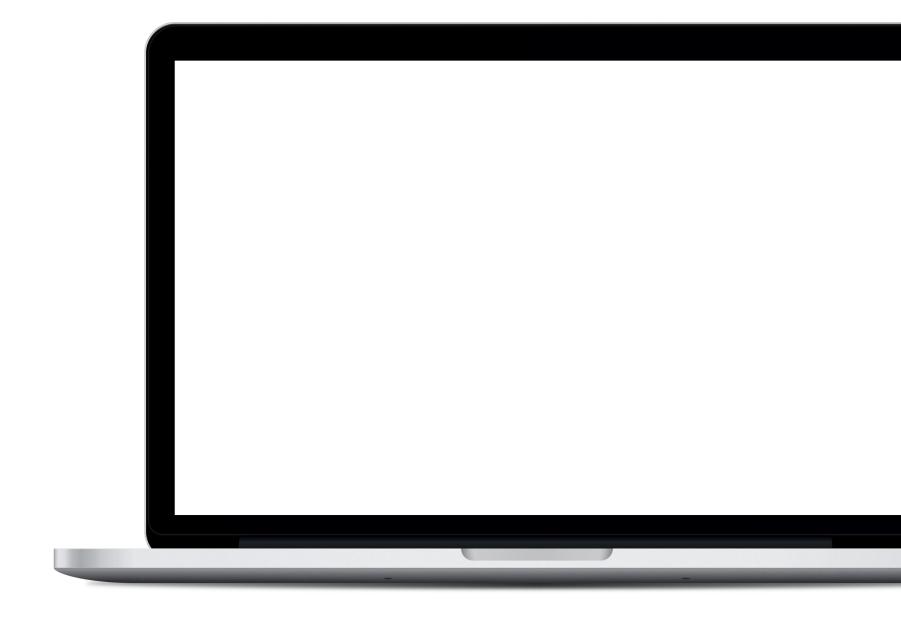
This is simplified setup to demonstrate idea and initial setup

2024 / brainly.com

#### **PREREQUISITES**

## What is needed in this example?

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





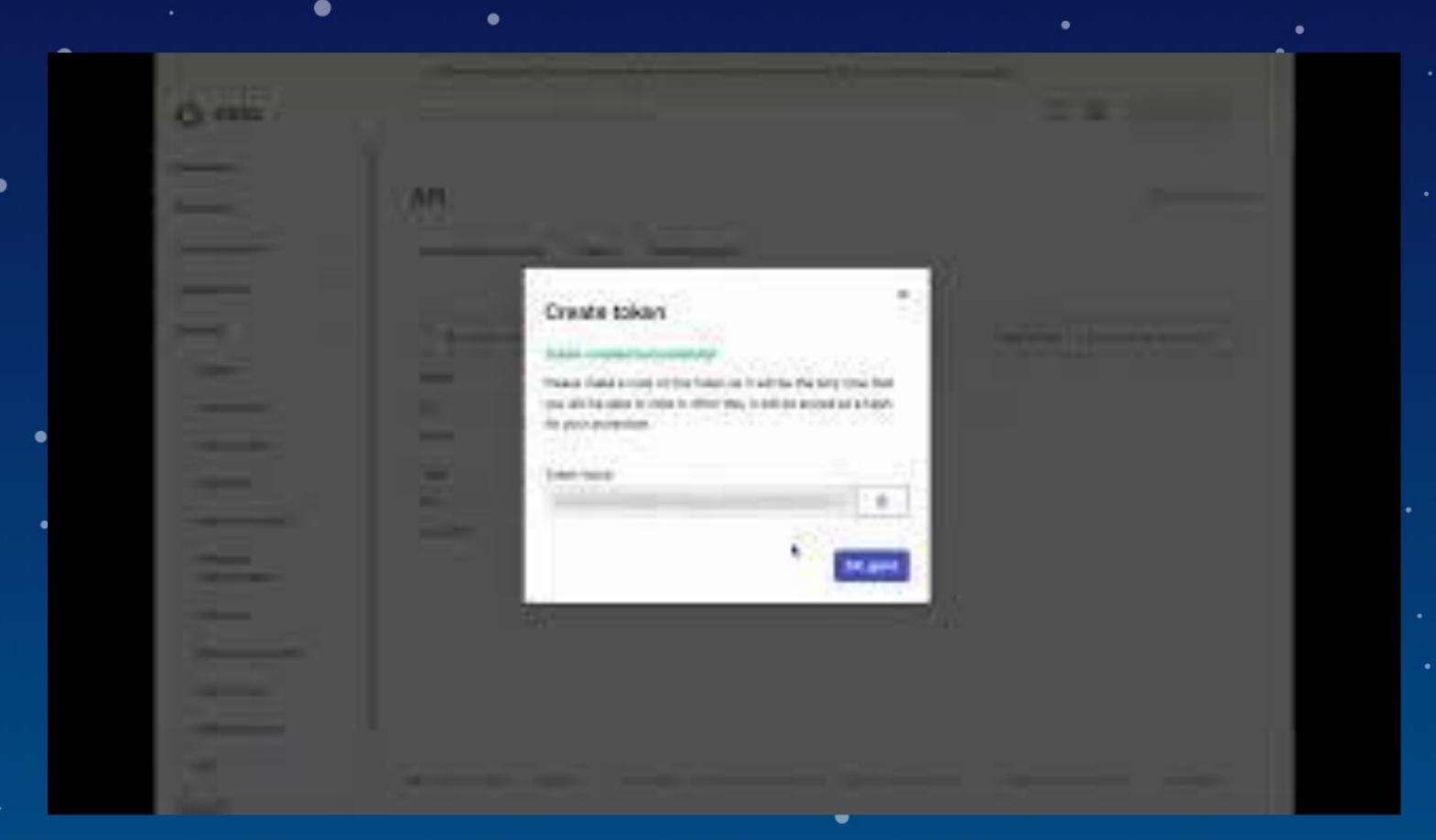
2024 / brainly.com

#### **OKTA API TOKEN**

# Token will be used by Terraform to provision Okta resources.



### CREATE OKTA API TOKEN FOR TERRAFORM

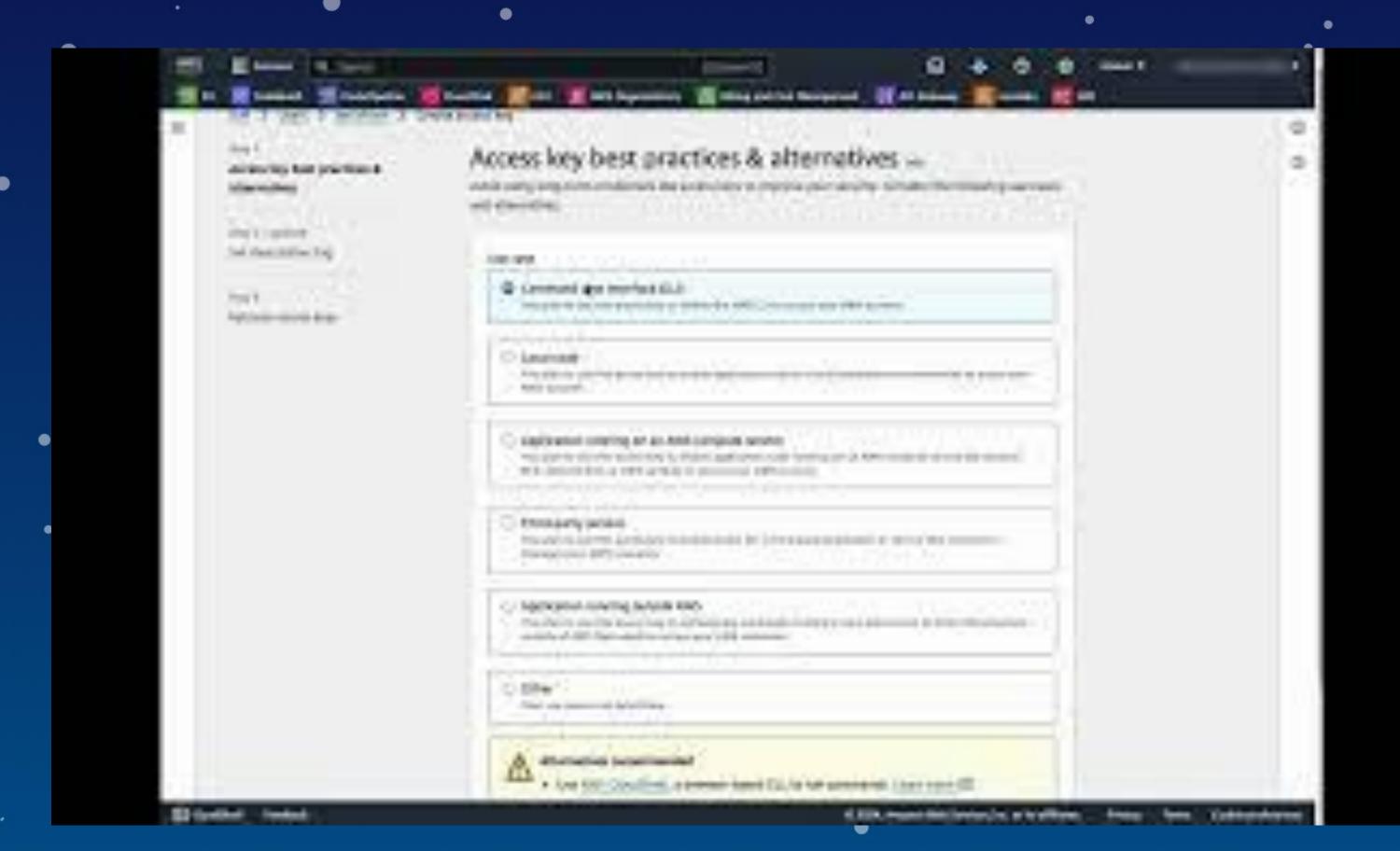


#### IAM USER FOR TERRAFORM

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

**OKTA SAML WITH AWS** 

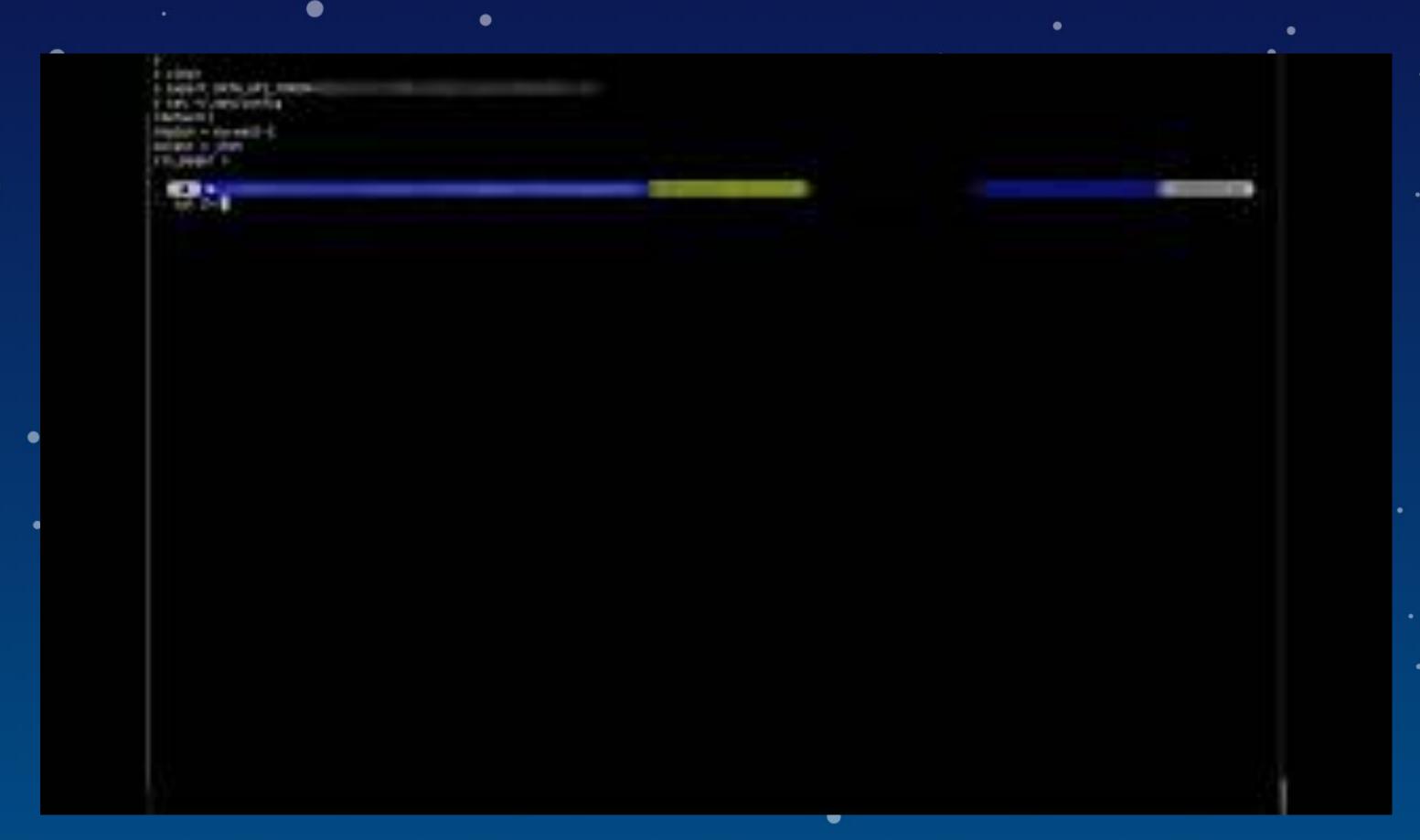
#### CREATE AWS IAM USER FOR TERRAFORM



#### **SET LOCAL ENVIRONMENT**

# Okta token and AWS credentials for Terraform providers.

### SET CREDENTIALS IN TERMINAL



#### PREPARE TERRAFORM CODE

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



**OKTA SAML WITH AWS** 

#### PREPARE TERRAFORM CODE

```
I Secretaria de Arbeiro de contra
 of the service of the
1 10 104
                                                                                                                                                                                                         10/10/91
1 The Secretary Laboratory
                                                                                                                                                                                                                     PRODUCTION AND A THE LABOR.
- British de maris
TO SHOW AND ADDRESS.
                                                                                                                                                                                                                     Destroy Company 1
- British warrings
                                                                                                                                                                                                                         time a feet.

    Winners could be a proper

                                                                                                                                                                                                                                            Auto 1 hard organic
- British Confession
                                                                                                                                                                                                                                              mendate of Table 2 (27)
* Birelandining
 The Control of the Asset Asset
                          Their.
                             Windshield.
                                                                                                                                                                                                                                 Miles - 4
                           AL THURSDAY OF
                                                                                                                                                                                                                                            party of Tonas contract
                             T. Charles St.
                            To provide the
  * Scientification
              1. SE LONGO D.
              1 THE PARTY.
                             A DOMESTIC OF
                             4 Artistanti - 1
                            T DOM:
                             Table 1
       Str. of Str.
                N. STORY
                al Jacons
               T. P. STANSON, N.
                                                                                                                                                                                                                  STATE OF THE PARTY.
               PARAMIE
               4-re-time-colo
   th Executive Absolute
   "s trephological barriers."
                                                                                                                                                                                                                     FIRST ARREST TO THE PARTY OF TH
                                                                                                                                                                                        a construction to be a series of the contract of the Contract
```

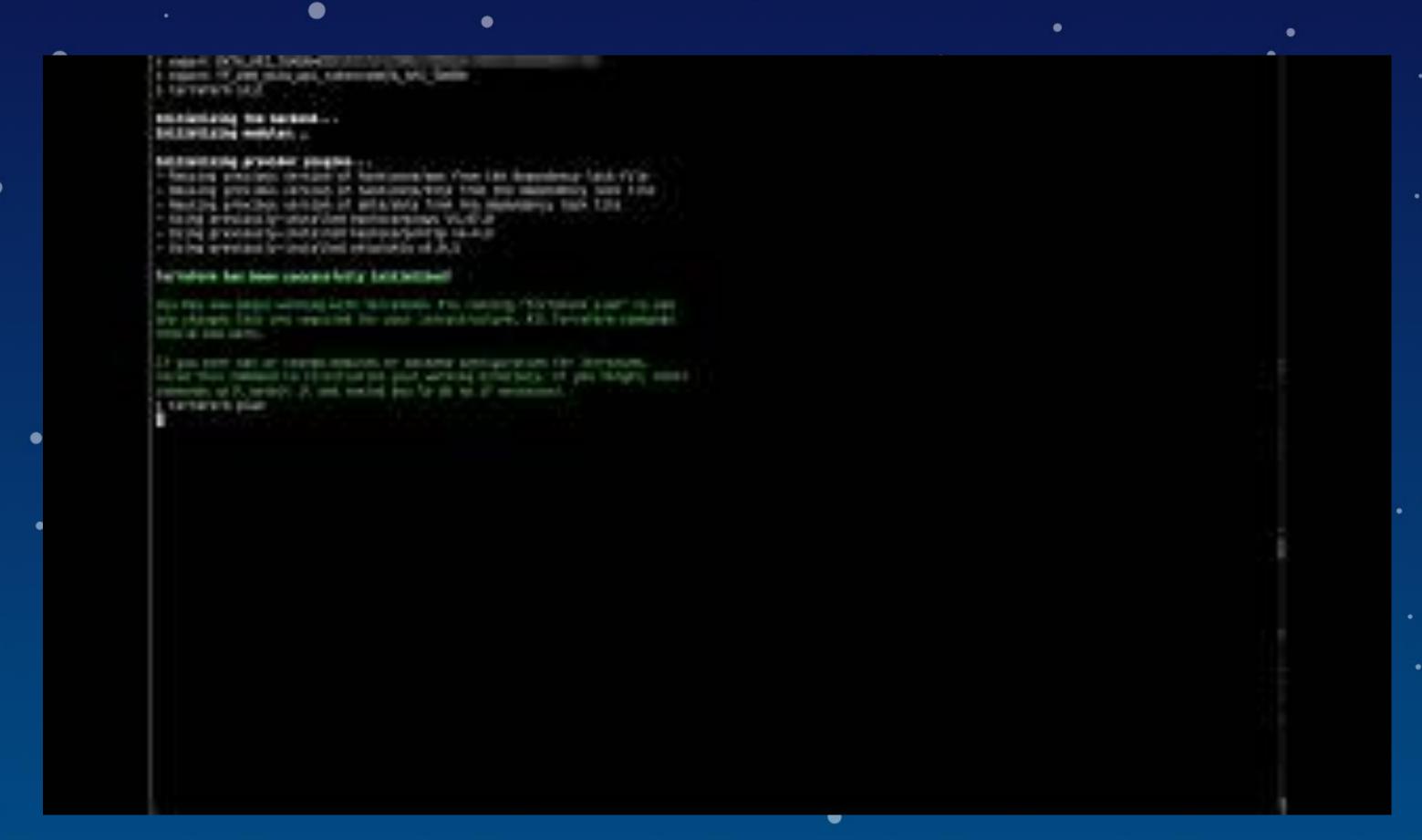
#### **PROVISION RESOURCES**

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



**OKTA SAML WITH AWS** 

#### **RUN TERRAFORM APPLY**

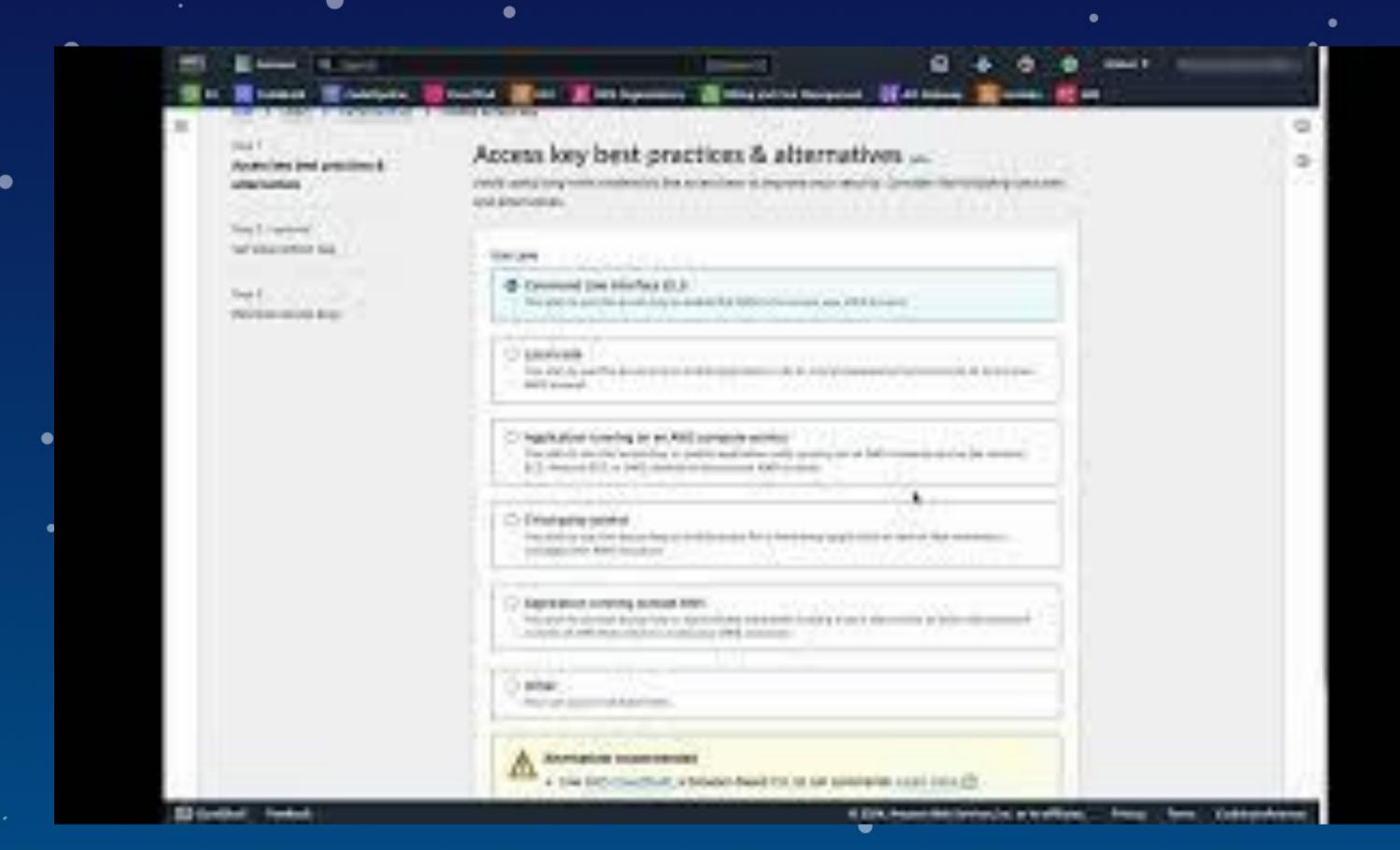


#### IAM ACCESS KEYS FOR OKTA

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

**OKTA SAML WITH AWS** 

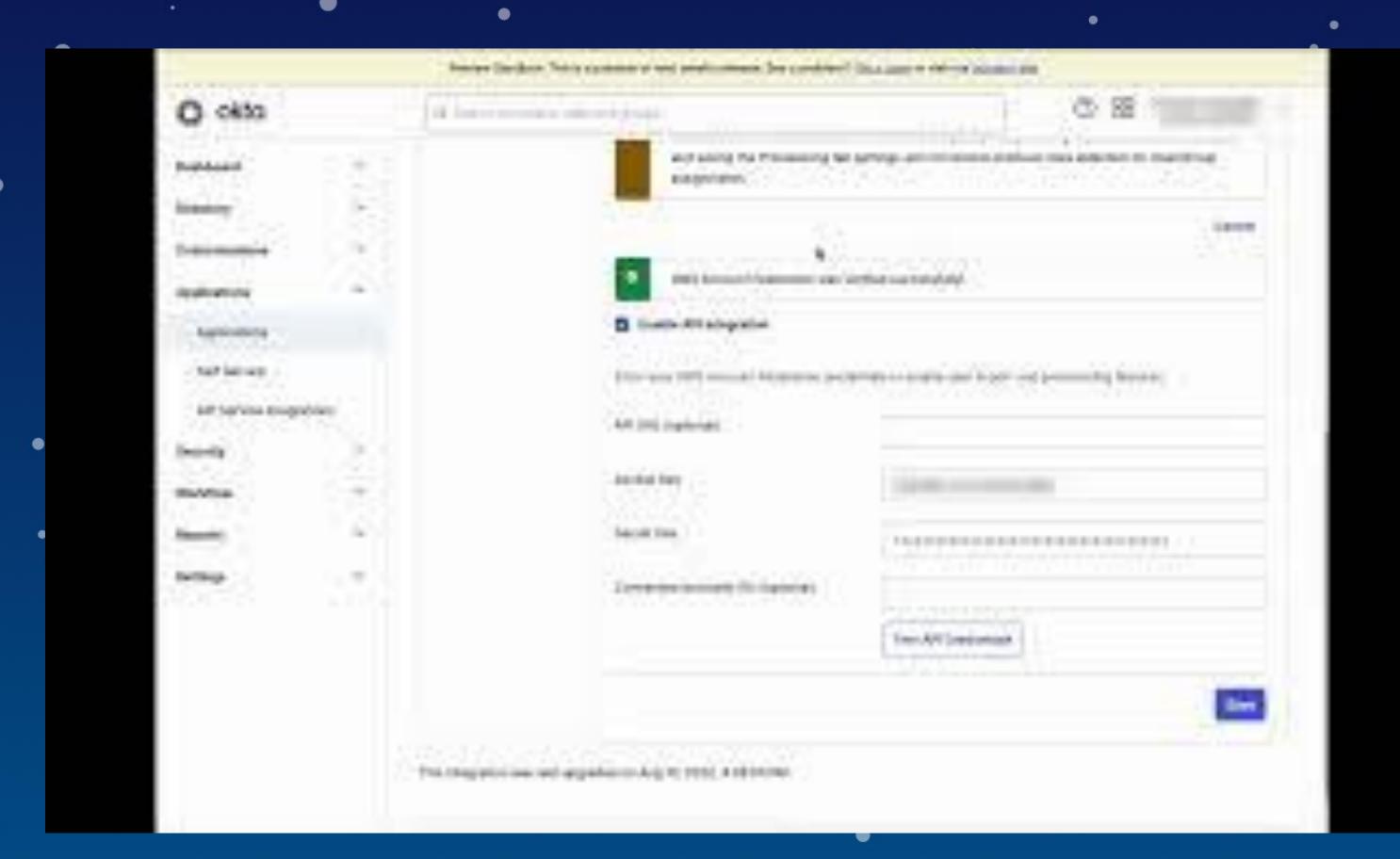
#### GET KEYS FOR OKTA IAM USER



#### **CONFIGURE OKTA AND TEST LOGIN**

# Enter those IAM access keys in Okta provisioning configuration.

### UPDATE OKTA PROVISIONING



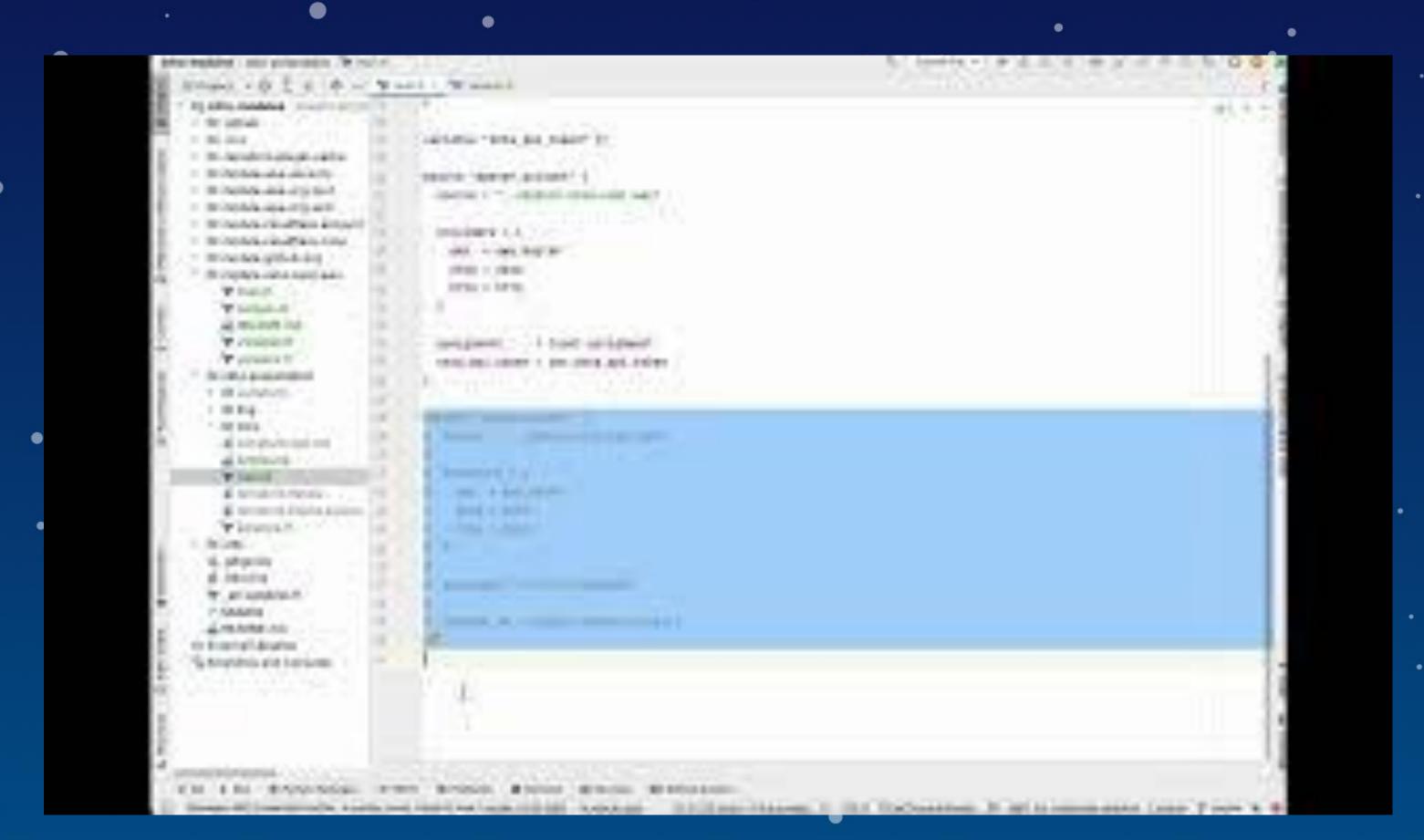
#### **ADDING OTHER ACCOUNTS**

# For each AWS account IAM user is needed to provision initial AWS resources. User can be deleted later.



**OKTA SAML WITH AWS** 

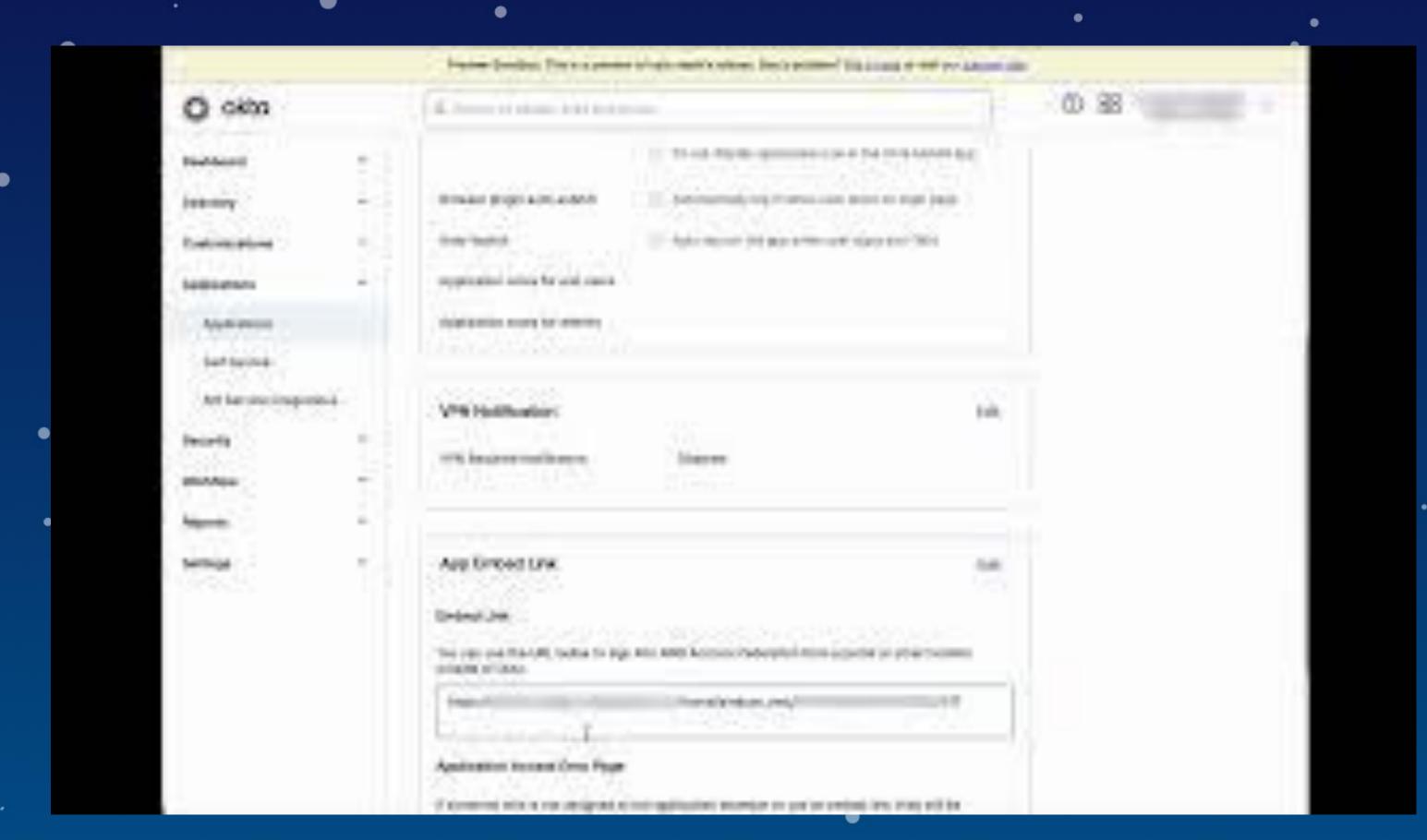
#### ADD ANOTHER ACCOUNT



#### **SETUP CLI FOR AWS**

Setup gimme-aws-creds (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

2024 / brainly.com 28

#### **BONUS TIPS**

#### 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.





## THANK YOU

Krzysztof Szyper

#### **MORE INFORMATION**

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



2024 / brainly.com

User Groups

KRAKÓW - POLAND



### Quiz time







https://bit.ly/AWSxGP