Setting up AWS Access

Justin Menga
FULL STACK TECHNOLOGIST
@jmenga pseudo.co.de

Introduction

AWS Identity & Access Management

- Multi-Factor authentication
- Delegated access using assumed roles
- Configuring IAM policies, roles, users and groups

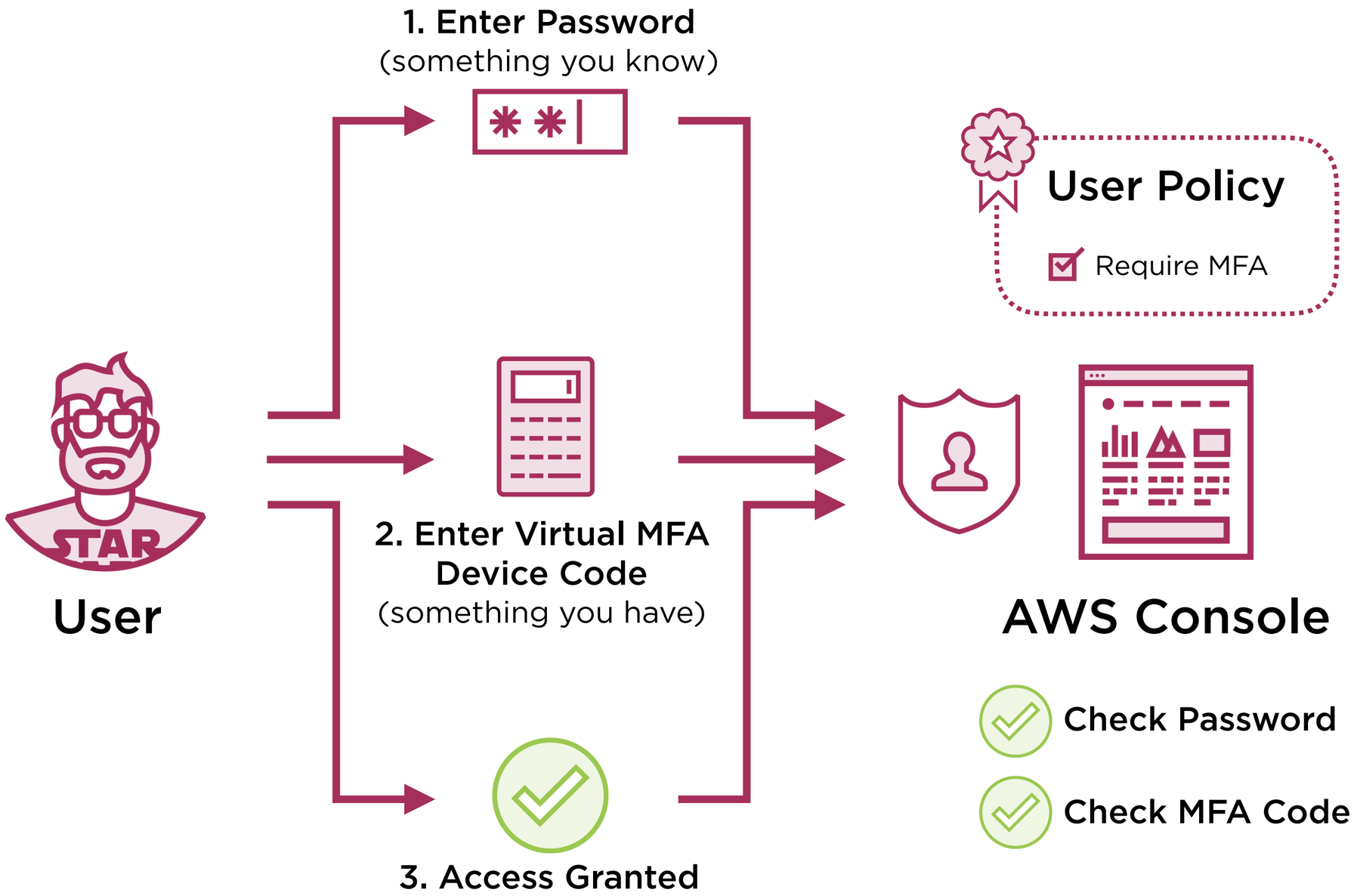
Operational Access and Tooling

- Creating an EC2 Key Pair
- Configuring the AWS CLI

Setting up AWS Identity & Access Management

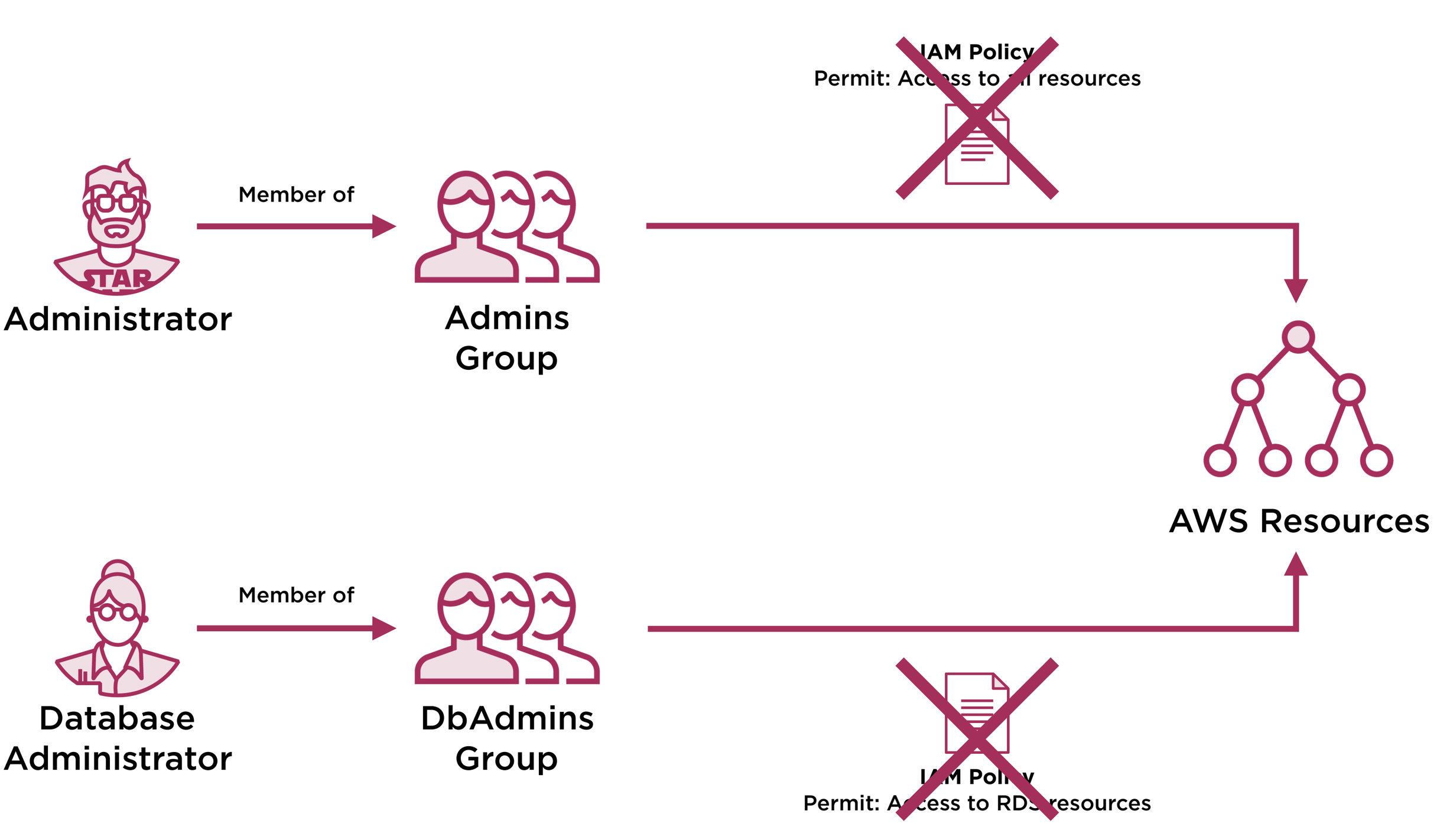
IAM Best Practice

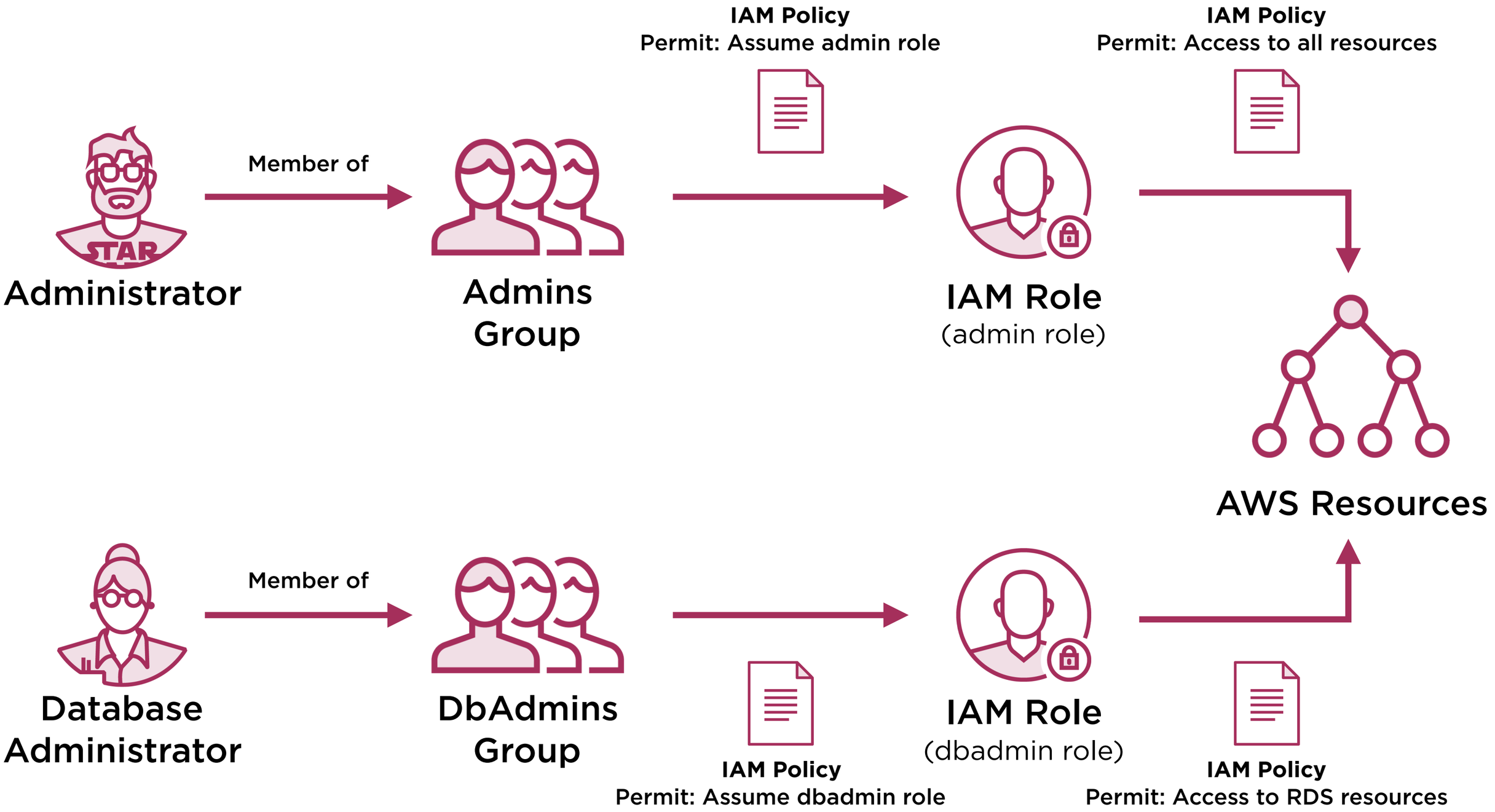
Use Multi-factor Authentication

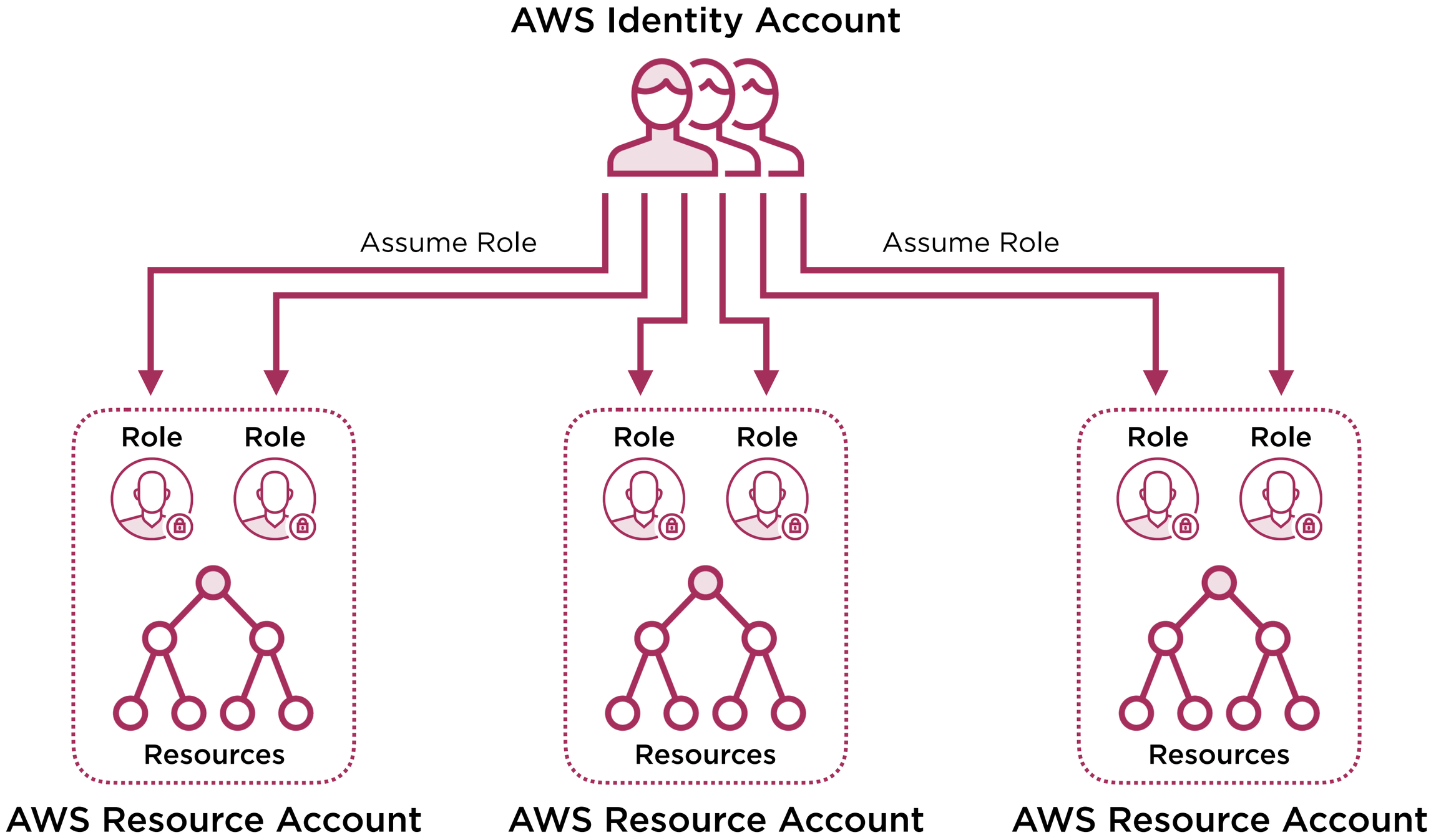

1. Enter Password
(something you know)
User Policy
Require MFA
User
2. Enter Virtual MFA
Device Code
(something you have)
AWS Console
Check Password
Check MFA Code
3. Access Granted

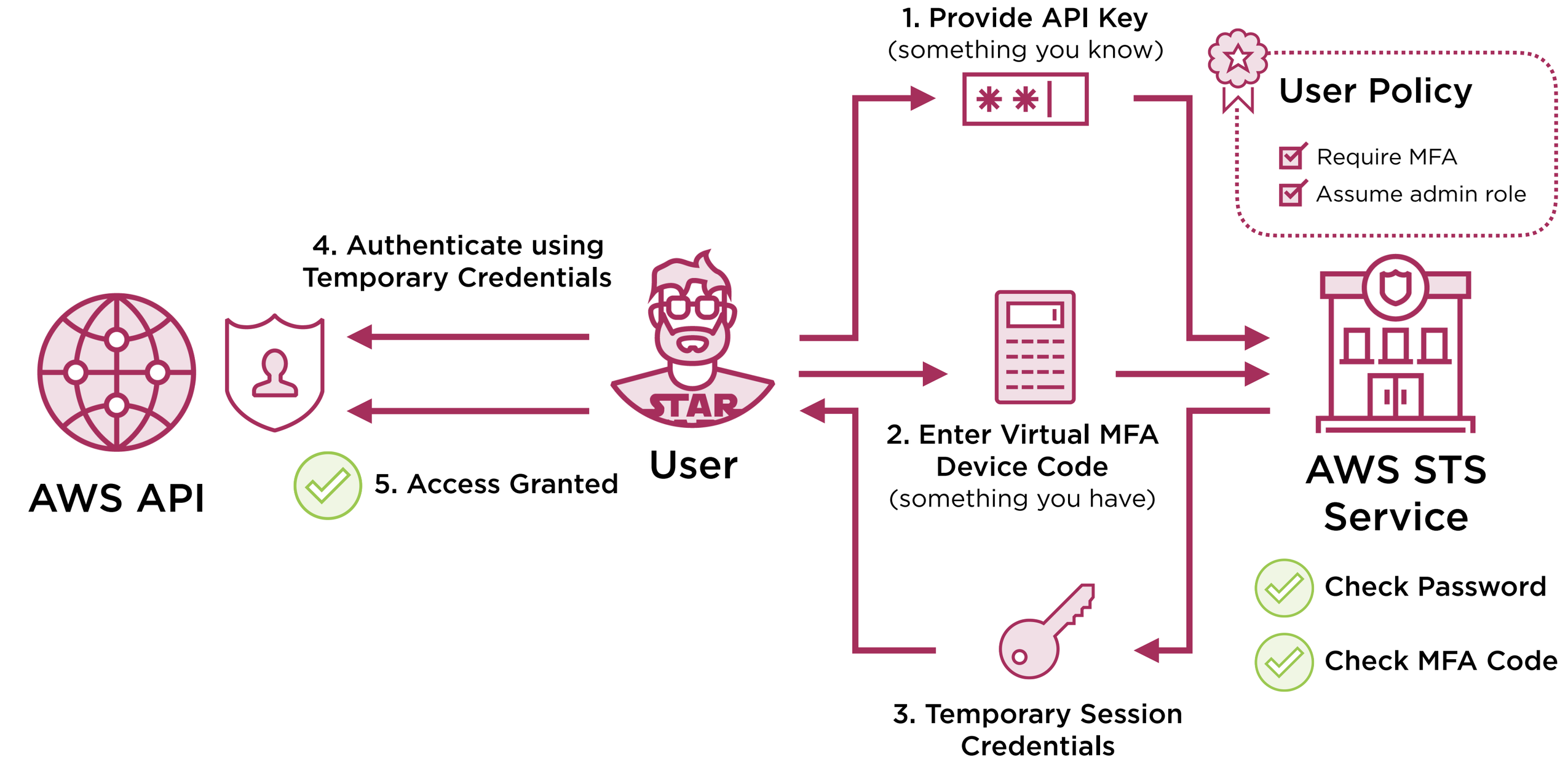
IAM Best Practice

Use IAM Roles to grant access to resources


IAM Policy
Permit: Access to all resources
Member of
Administrator
Admins Group
AWS Resources
Member of
Database Administrator
DbAdmins Group
IAM Policy
Permit: Access to RDS resources


IAM Policy
Permit: Assume admin role
IAM Policy
Permit: Access to all resources
Member of
Administrator
Admins
Group
IAM Role
(admin role)
AWS Resources
Member of
Database
Administrator
DbAdmins
Group
IAM Role
(dbadmin role)
IAM Policy
Permit: Assume dbadmin role
IAM Policy
Permit: Access to RDS resources


AWS Identity Account
Assume Role
Assume Role
Role
Role
Resources
AWS Resource Account
Role
Role
Resources
AWS Resource Account
Role
Role
Resources
AWS Resource Account


1. Provide API Key
(something you know)
User Policy
Require MFA
Assume admin role
4. Authenticate using
Temporary Credentials
AWS API
5. Access Granted
User
2. Enter Virtual MFA
Device Code
(something you have)
AWS STS
Service
Check Password
Check MFA Code
3. Temporary Session
Credentials

Demo

Setting up AWS IAM

- Creating an Account Alias
- Creating IAM Roles
- Creating Groups
- Creating IAM Policies that enforce MFA
- Creating Users
- Enrolling Users for MFA

Creating an Account Alias

Creating IAM Roles

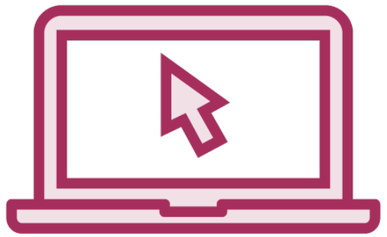
Creating Groups

Creating and Enrolling Users for MFA

Setting up an EC2 Key Pair

EC2 Key Pair

Management Host

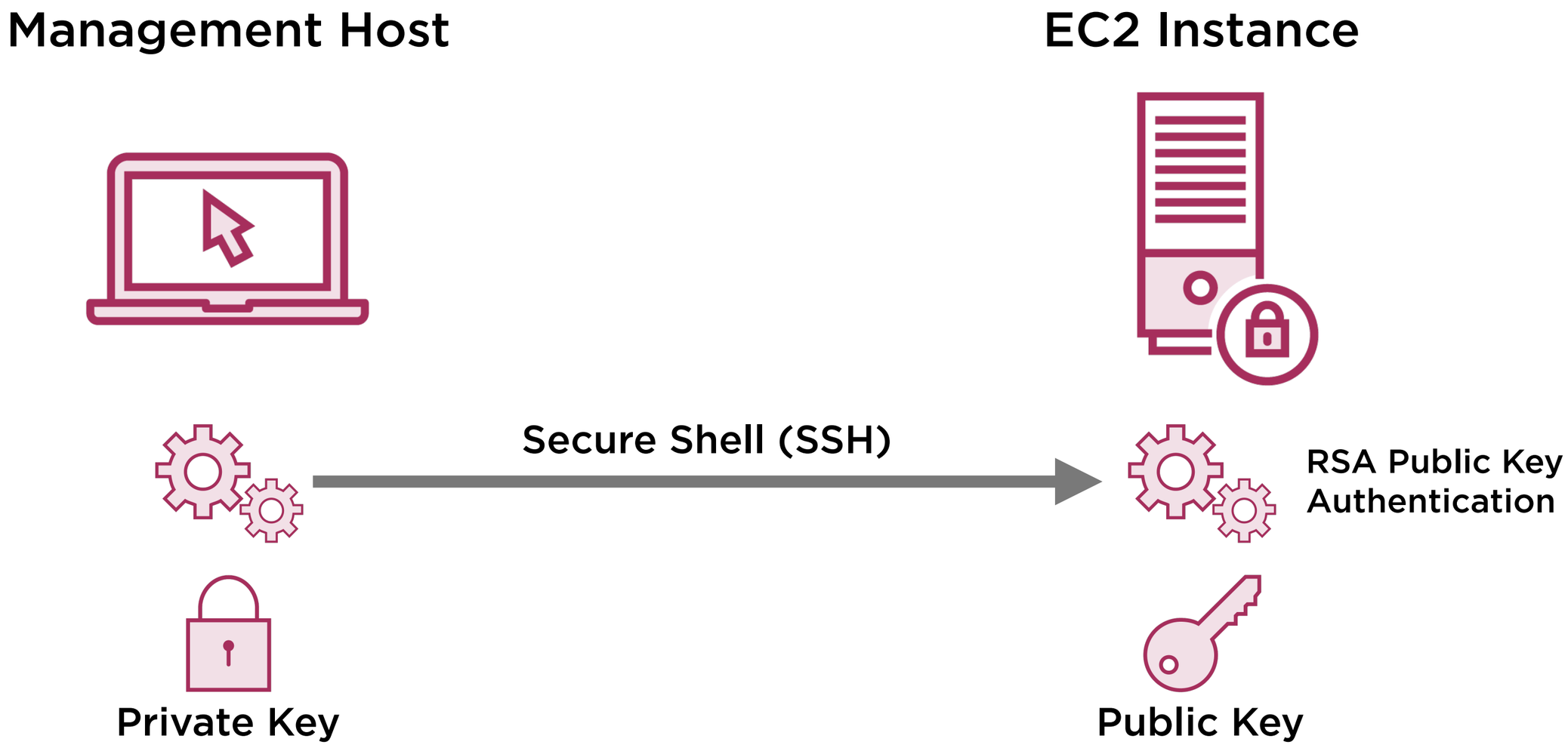


EC2 Instance

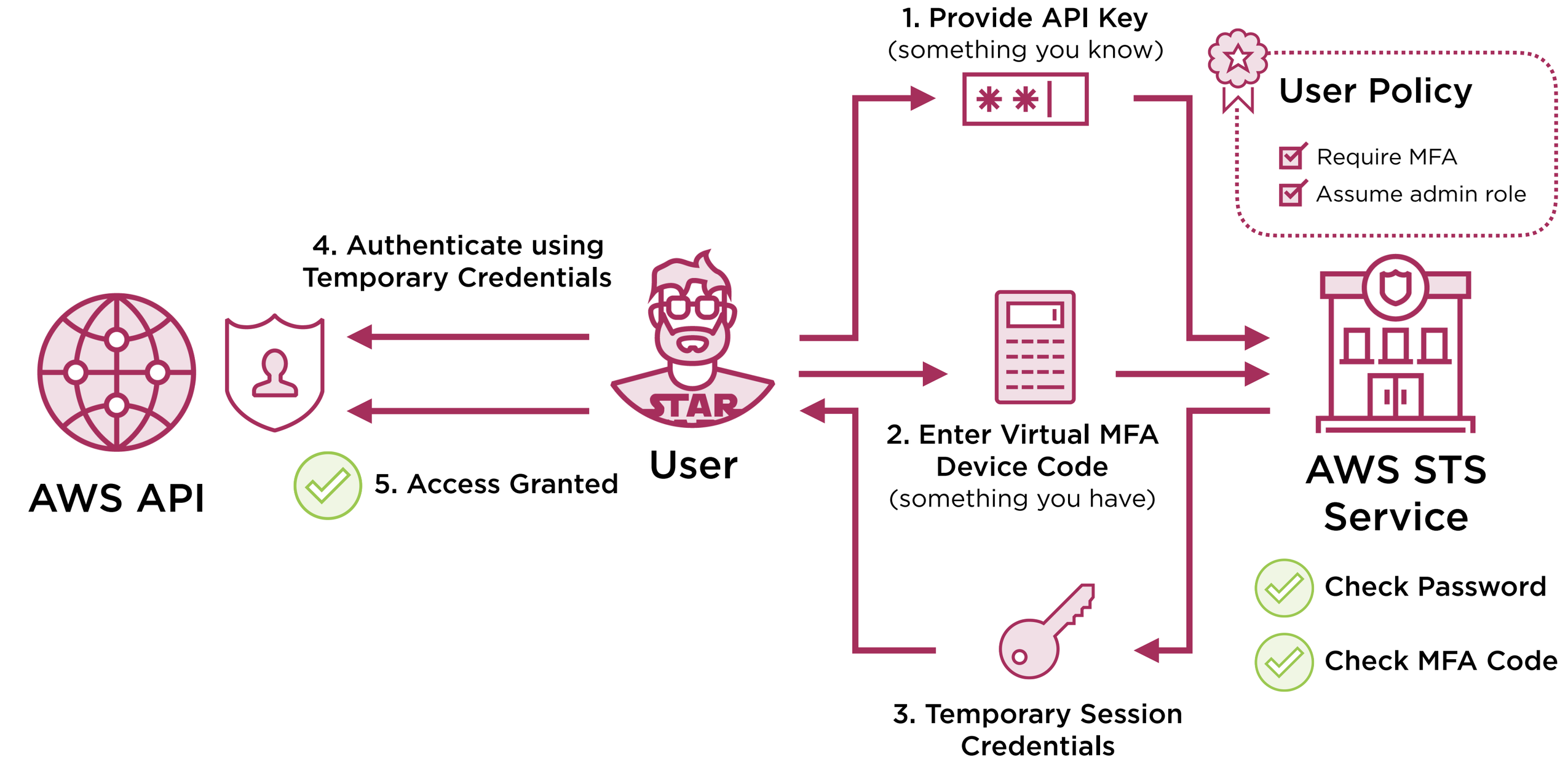
EC2 Key Pair

Private Key **Public Key**

EC2 Key Pair


Management Host
EC2 Instance
Secure Shell (SSH)
RSA Public Key Authentication
Private Key
Public Key

Setting up AWS CLI Access


1. Provide API Key
(something you know)
User Policy
Require MFA
Assume admin role
4. Authenticate using
Temporary Credentials
AWS API
5. Access Granted
User
2. Enter Virtual MFA
Device Code
(something you have)
AWS STS
Service
Check Password
Check MFA Code
3. Temporary Session
Credentials

Summary

AWS IAM Setup

- Multi-factor Authentication
- Assuming IAM Roles
- Roles, Policies, Users and Groups

AWS Tools Setup

- EC2 Key Pair
- AWS CLI role assumption
- AWS CLI MFA support