
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

SEC207

Simplify your existing workforce access with IAM Identity Center

Harvinder Nagpal

Sr. Identity Specialist
AWS

Jonathan VanKim

Sr. Identity Solutions Architect
AWS

Agenda

Access challenges

How AWS IAM Identity Center solves those challenges

Taking it even further with AWS Managed Microsoft AD

What’s next for IAM Identity Center and AWS Managed Microsoft AD

Learn more

Business is growing

INCREASINGLY ADOPTING A MULTI-ACCOUNT STRATEGY

Improve security

Increase agility

Accelerate innovation

Opportunities

Challenges

Striking a balance

Architect

Business processes

Security posture

Audit & compliance

Technology landscape

Striking a balance

Engineer

Business agility

Build vs. buy

API availability

Secure development

Striking a balance

Operations

Centralized access management

Locked-down access

Managing environments and services

Delegated access management

Workplace agility

FOR WORKFORCE IDENTITY – ENTERPRISE USERS

End users

Application teams
Application owners and team members

IT teams
Administrators, engineers, architects

Multi-account adoption

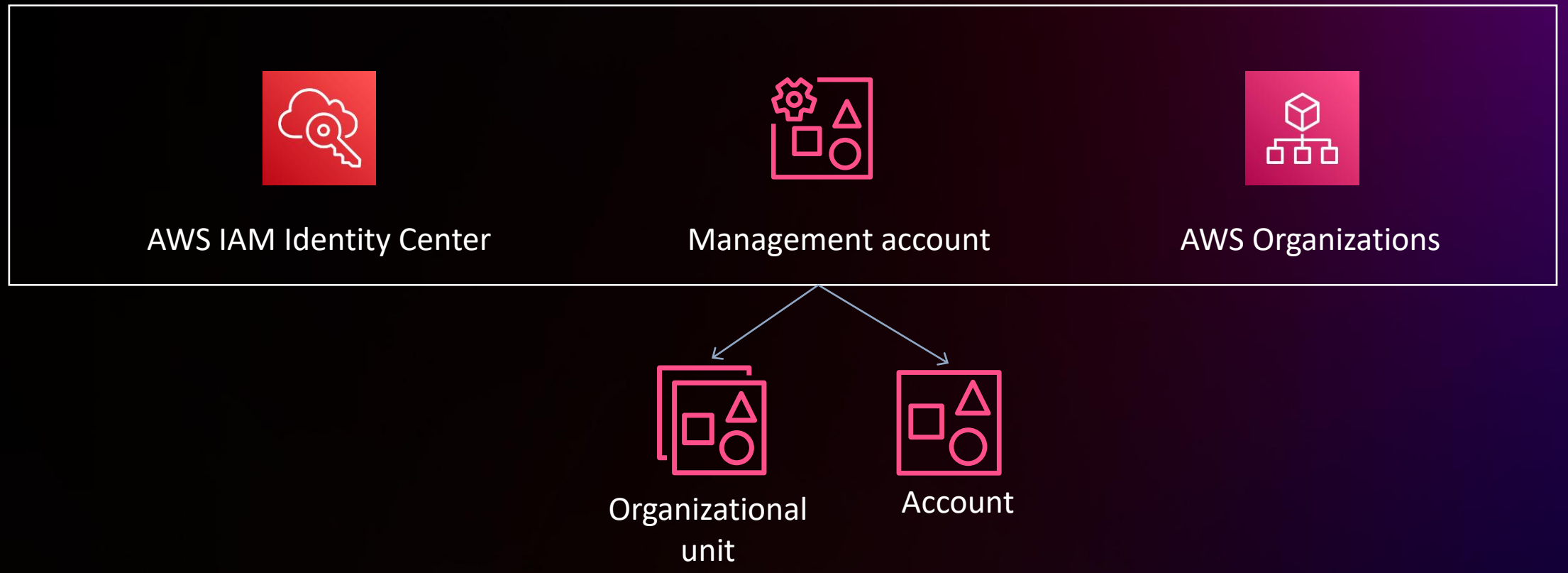
Ephemeral infrastructure

Mushrooming application portfolio

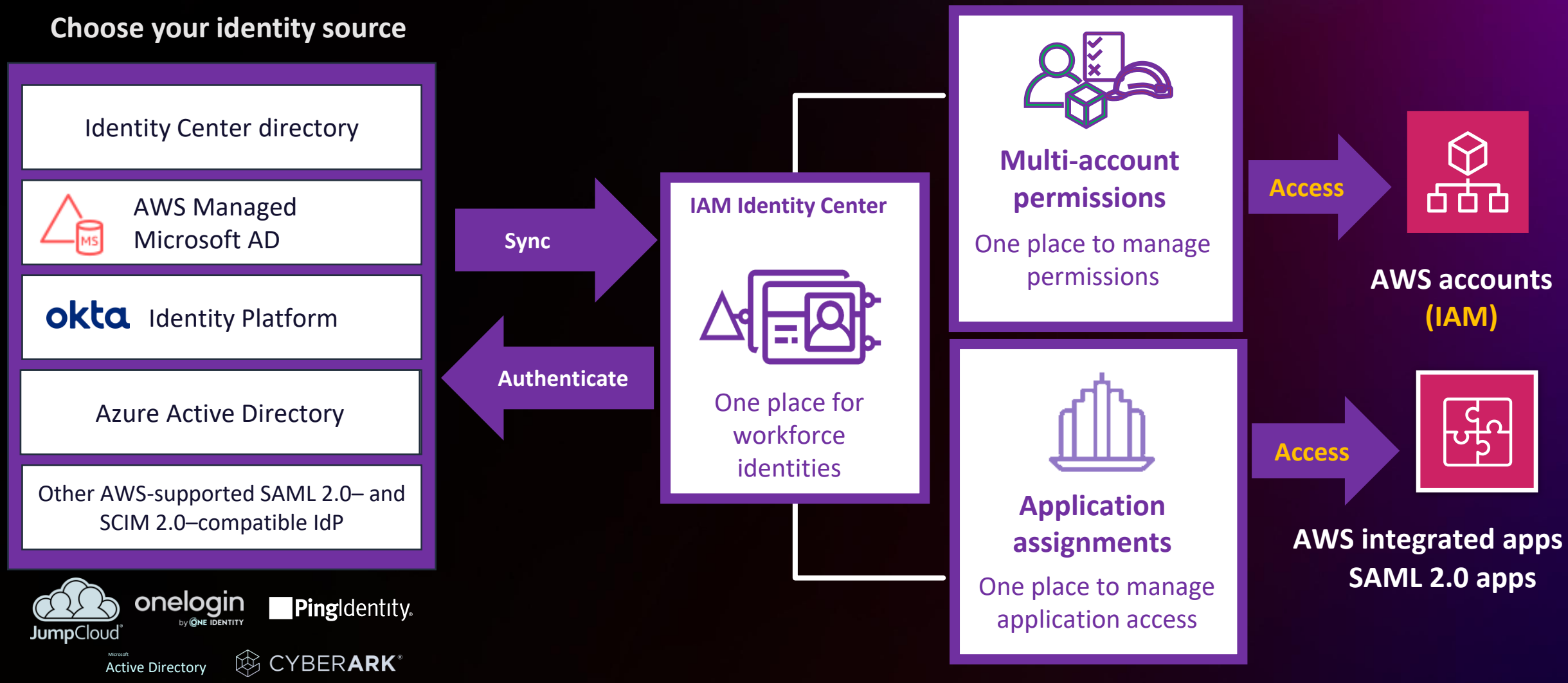
IAM Identity Center is your front door to AWS

- Manage a growing number of workforce identities
- Apply fine-grained authorization at scale
- Connect to more resources and applications across your organization

IAM Identity Center architecture



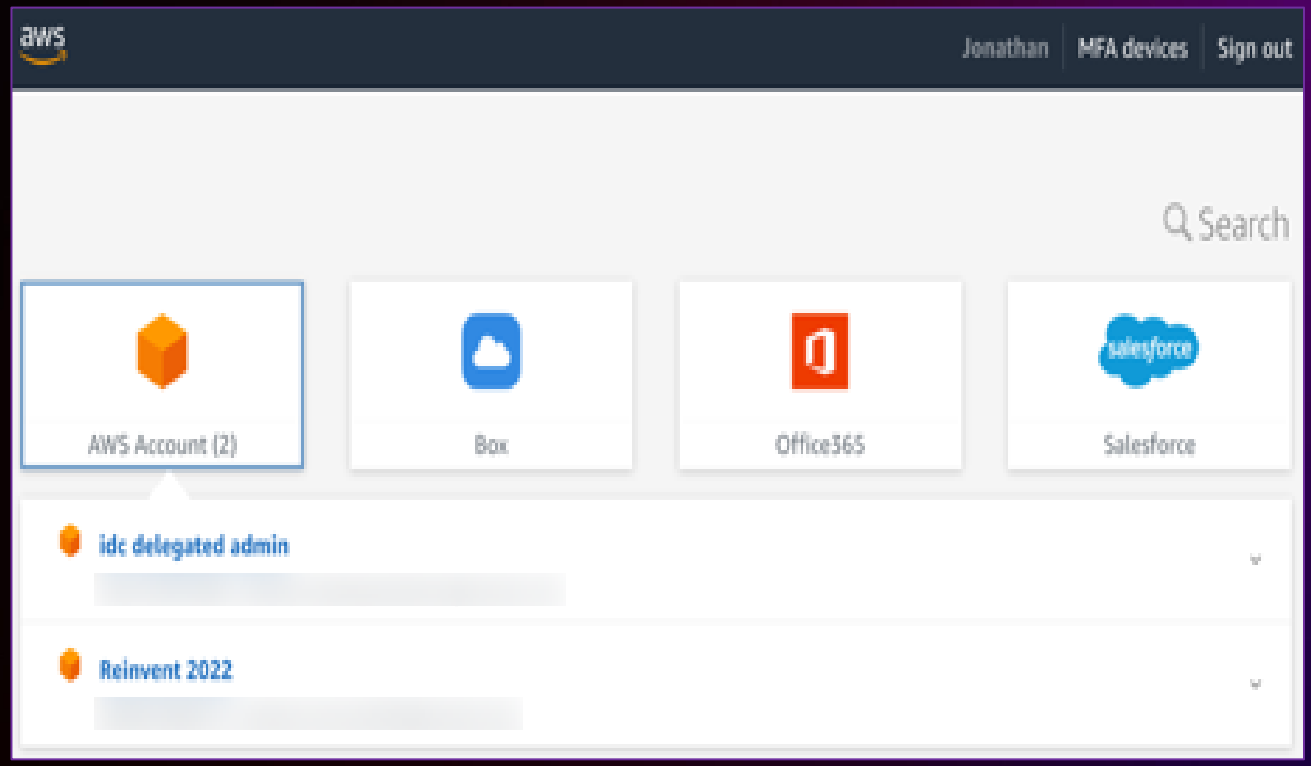
How IAM Identity Center works



Making it user-friendly

Operations

- Provide single sign-on access to AWS applications for ease of use
- Use preconfigured settings for cloud applications, including Salesforce, Box, and Office 365
- Use the application configuration wizard to add SAML-based applications



Simplifying administration

SEPARATION OF DUTIES IN ENTERPRISES WITH MULTIPLE OPERATING UNITS

Operations

Centralized administration and API access from an AWS Organizations delegated administrator account

https://go.aws/3UfmFI0

Delegated admin account can assign users and groups to applications and an organization's member accounts

https://go.aws/3DWZe19

Ensuring service availability

APPLICATIONS NEED TO BE ACCESSIBLE

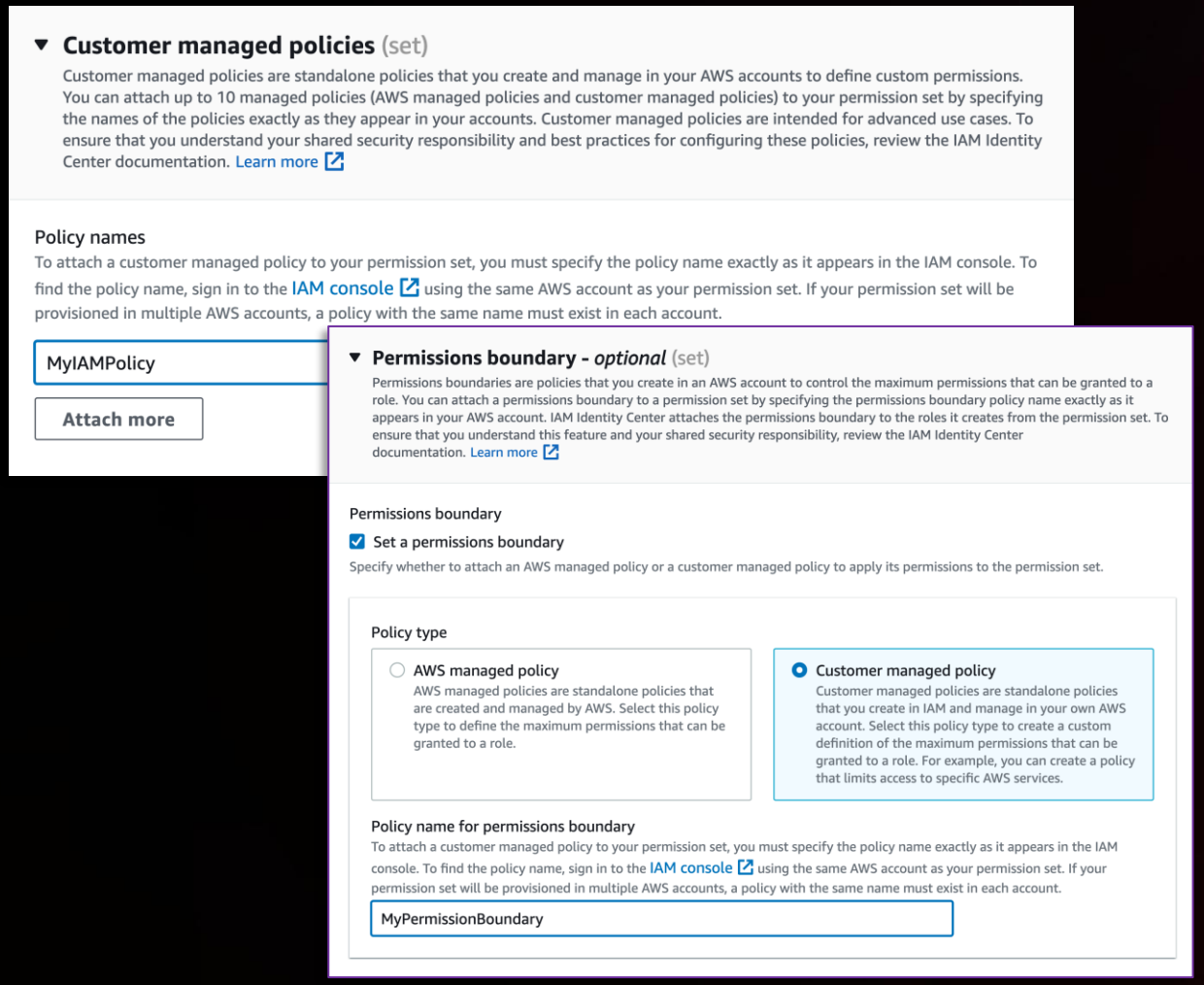
Operations

Deployed in multiple Availability Zones within a Region

Providing secured access

RIGHTLY SCOPED PRIVILEGES WITH ON-DEMAND ACCESS

Operations



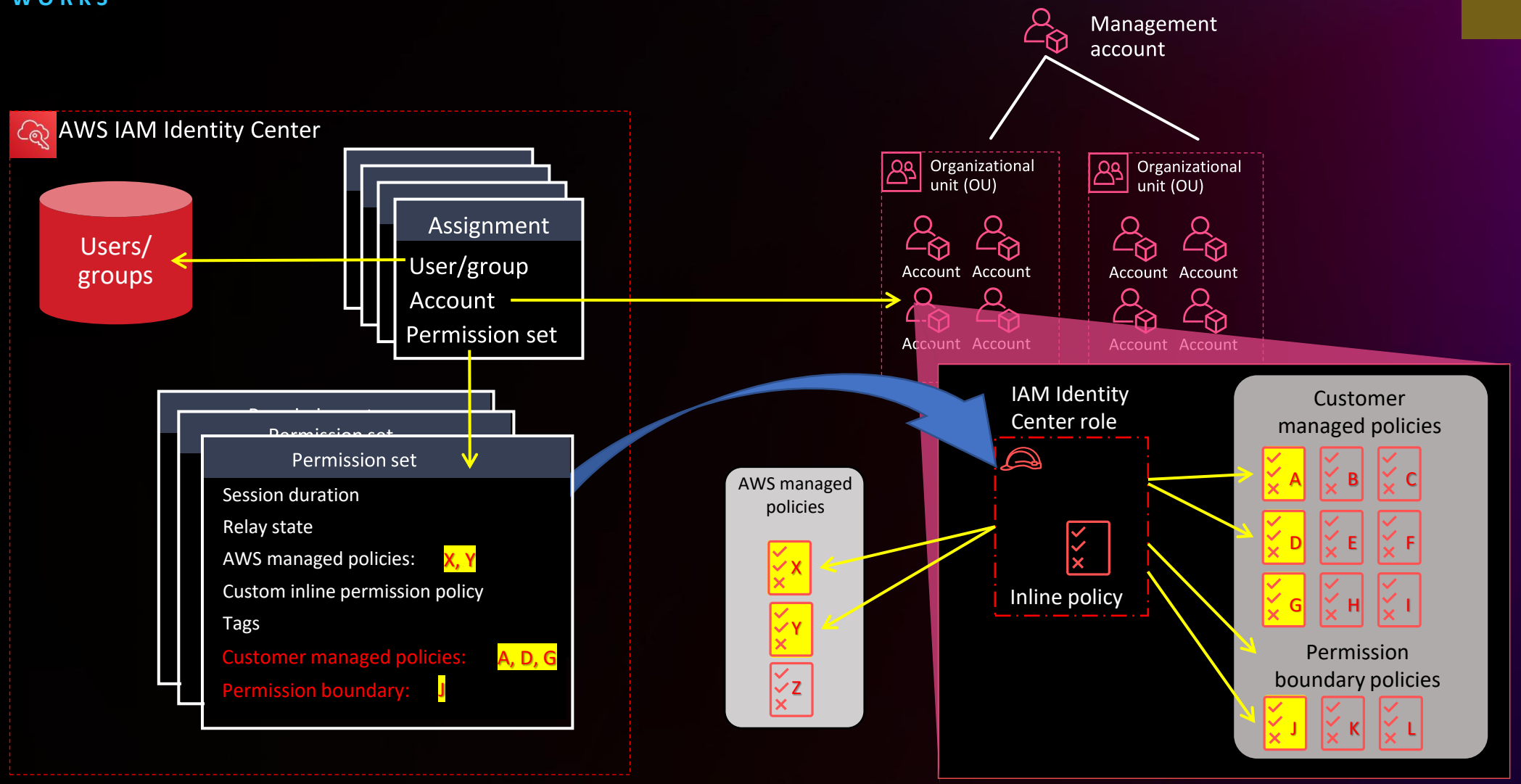
What is supported

- Predefined permission set
- Custom permission set
  - AWS managed policies
  - Customer managed policies (new this year!)
  - Inline policies
  - Permissions boundaries (new this year!)

https://go.aws/3zDfx0p

Customer managed policy support

HOW IT WORKS

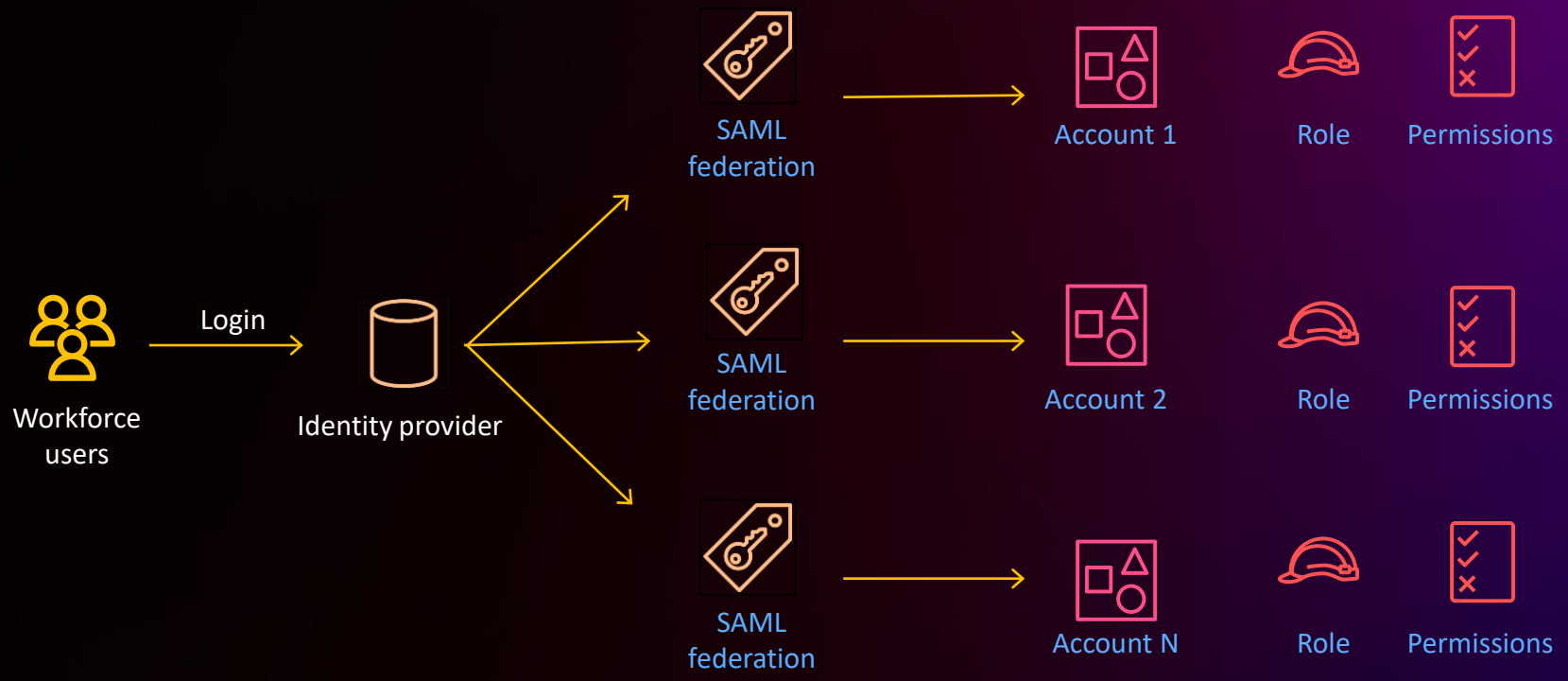


IAM-based federation

SO WHAT'S THE CHALLENGE

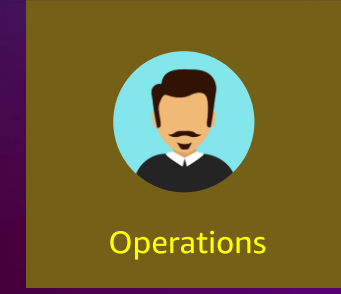
Operations

- Federation per AWS account
- Authorization stored in each account
- Can be automated with AWS CloudFormation StackSets

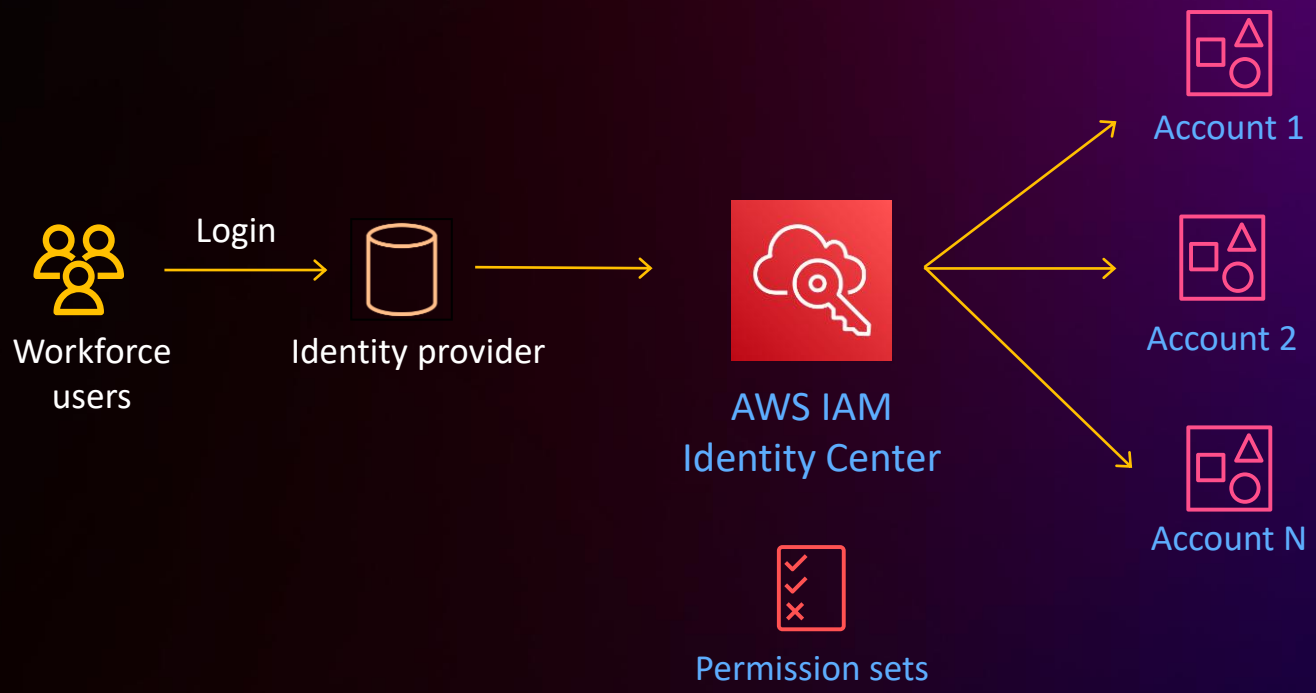


IAM Identity Center–based federation

SIMPLIFIED AND SCALABLE

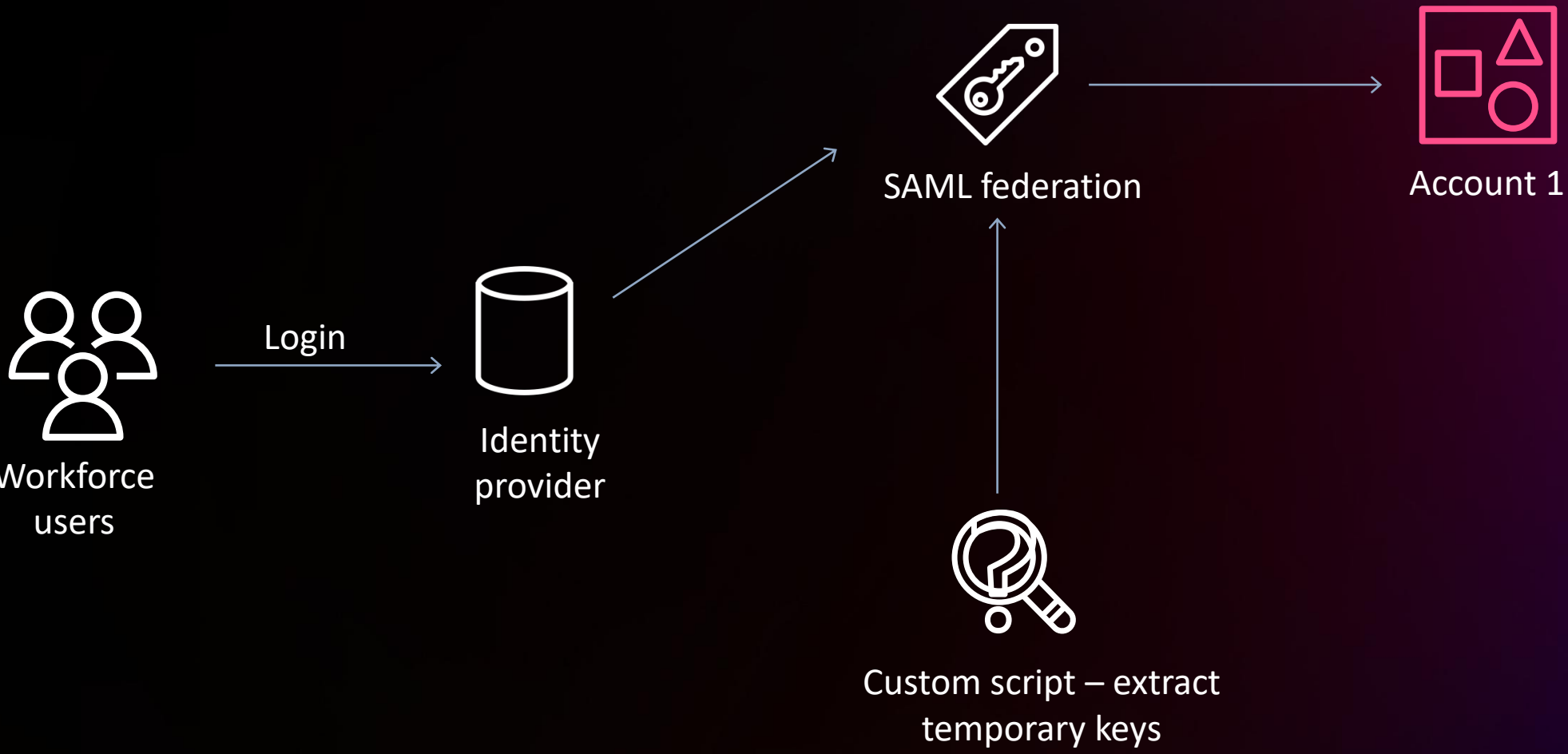


- Centralized management of roles and policies
- Scales permission management with growing number of accounts
- Integrates with AWS CLI version 2
  - Exclusive to IAM Identity Center
  - Human access to temporary credentials – access key and secret key
- Now published as part of updated IAM best practices

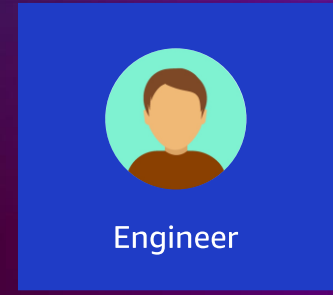


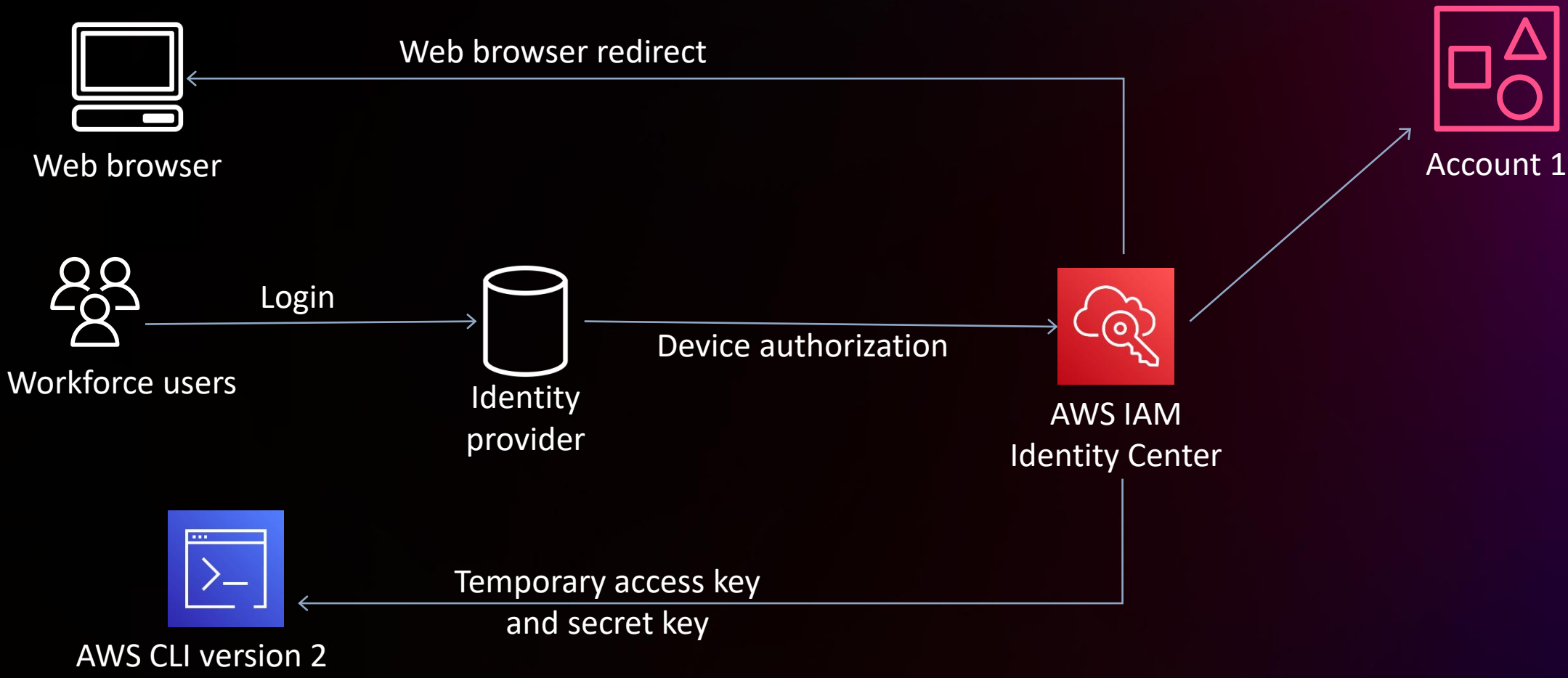
IAM federation – Temporary credentials

Engineer



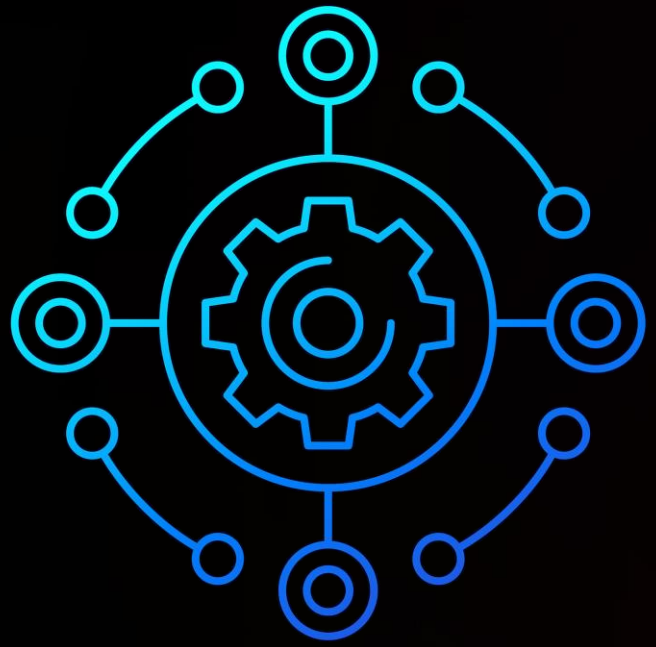
IAM Identity Center – Temporary credentials





Automate

SECURE AND SCALE

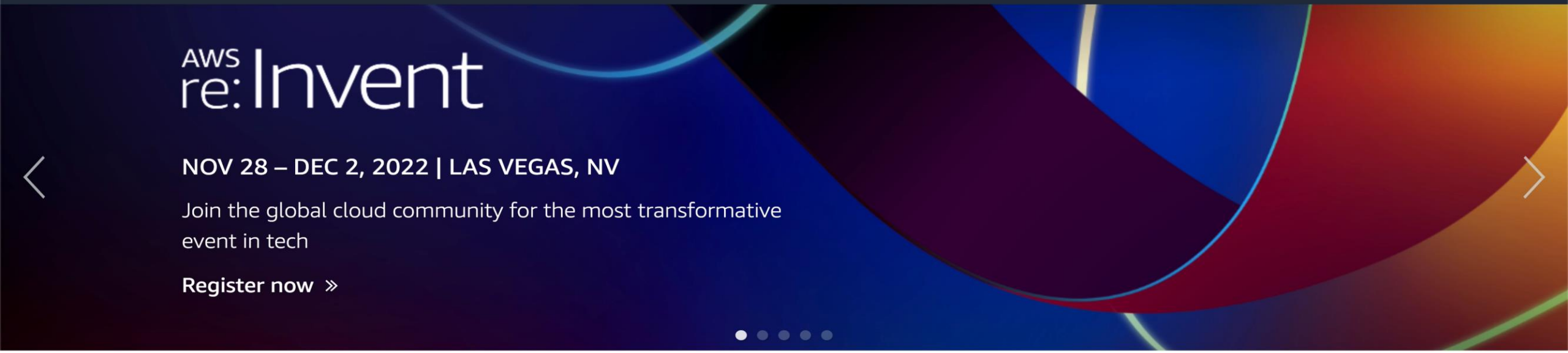


Engineer

Automate administrative tasks to reduce manual effort, save time, and scale efficiently

AssumeRole to gain short-lived access on-demand

```
jonathanvankim@JONATHANs-MacBook-Pro ~ % aws configure sso
SSO start URL [None]:
```



Amazon Lightsail Extended Free Tier
New customers get up to three months free on select virtual private servers

Supplemental Storage for VMware Workloads
Explore the jointly-engineered datastore using Amazon FSx for NetApp ONTAP

Security redefined With Amazon Neptune
Start today with 1 month free trial

Enhance Cloud Security
Learn how to elevate your security in the cloud

Solutions
View our AWS Solutions library

Explore Our Products
Explore our cloud-based products

Training & Certification
Learn how to build on AWS

Powering Customer Innovation
Read our customer successes

Security & Compliance
Scale cloud security with AWS

Accelerating the cloud journey

WITH LEAST TECHNOLOGY DISRUPTION

Architect

Connect your existing identity provider to manage access across multiple AWS accounts

IAM Identity Center coexistence with IAM for a phased transition

Shared security model with industry standard compliance certifications

Accelerating adoption of IAM Identity Center

- Low risk with two-way door
- Co-exists with existing authentication setup
- Minimal financial impact

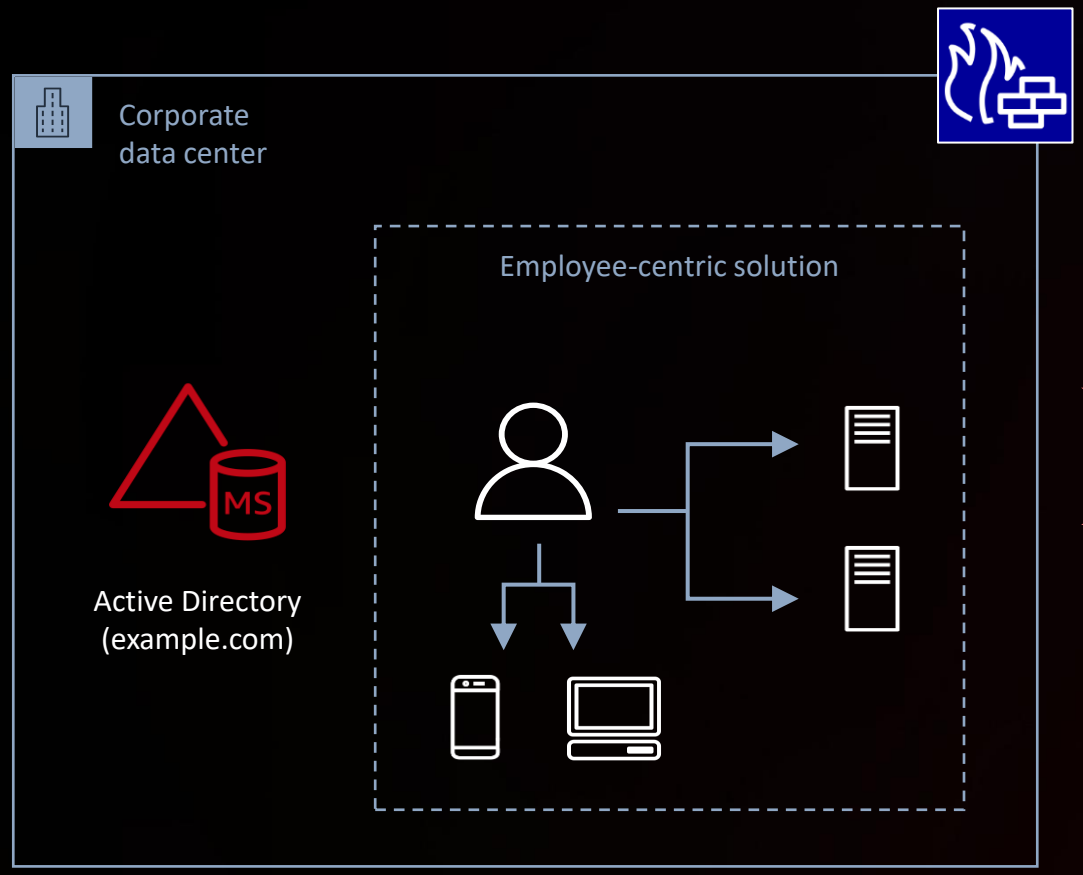
Pick your option prudently

CONSIDER - BUSINESS IMPACT, SECURITY AND COMPLIANCE, ENTERPRISE ARCHITECTURE

Phased (Crawl-Walk-Run)	HYBRID	Turbocharged (Lift-n-Shift)
Pilot with noncritical user access		Automate policy migration or used customer-managed policies
Verify appropriate access without disruption		Automate user and access assignment
Disable previous access		Validate migrated access or revert back if needed
Iterate with additional users		Remove (old) IAM based access
		Implement for every AWS account

Modernizing identity store

GAIN OPERATIONAL EFFICIENCY WITH A FRICTIONLESS EXPERIENCE



Architect

aws **Lift-and-shift** migrations

T3 P4d R6g HMI

aws **Modernize** directly into the cloud

Amazon Aurora Amazon RDS

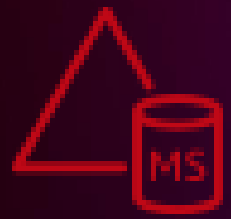
Cloud migration journey with AWS Directory Service

Architect

FOCUSING ON BUSINESS INNOVATION INSTEAD OF MAINTAINING TECHNOLOGY

AD Connector

- Redirect authentication requests from AWS to on-premises Active Directory (AD)
- Highly available across 2 Availability Zones by default



AWS Managed AD

- Host AD users and groups or connect to on-premises AD
- Highly available with multi-region replication capabilities

AWS Managed Microsoft AD

IMPROVING OPERATIONAL EFFICIENCIES

Operations

Fully managed service for Windows Active Directory

- Single-tenant domain (single forest, single domain)
- Highly available across multi-AZ, multi-Region
- Default 2x domain controllers, can scale out per Region

AWS responsibility

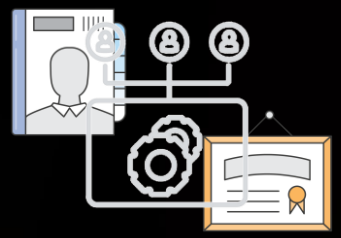
- Deployment
- Patch
- Monitor
- Snapshot/Restore

Customer responsibility

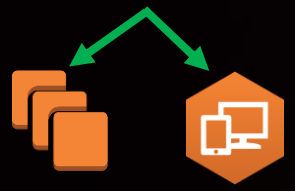
- Administering users, groups, GPOs, etc.
- Configuring password policies
- Managing trust relationships

Key Features of AWS Managed Microsoft AD

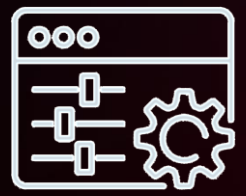
SECURE, FLEXIBLE, CONFIGURABLE AND SCALABLE



Microsoft AD 2019

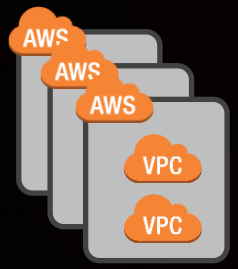


Manage users, groups, group policies

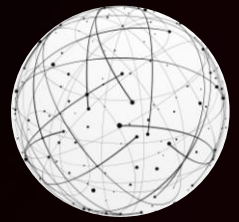


Configurable directory settings

Trust support



Support multiple accounts and VPCs

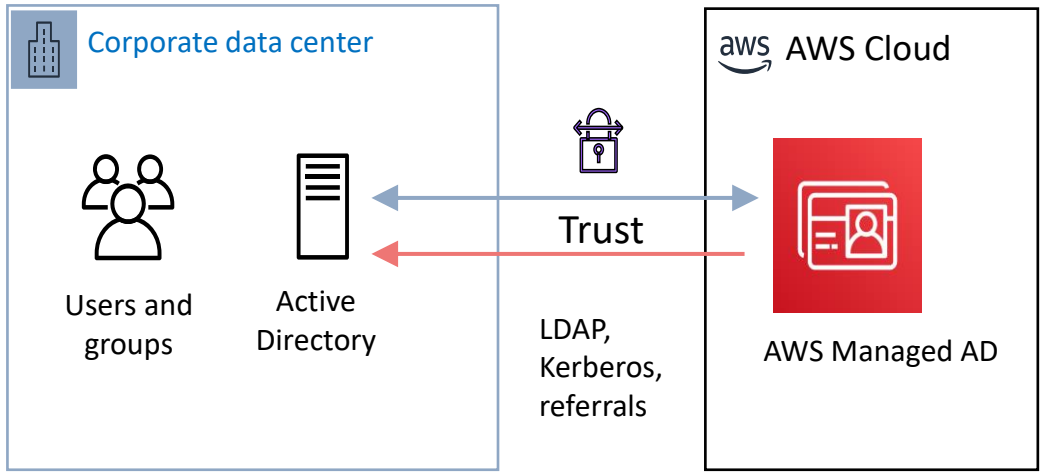


Multi-region replication

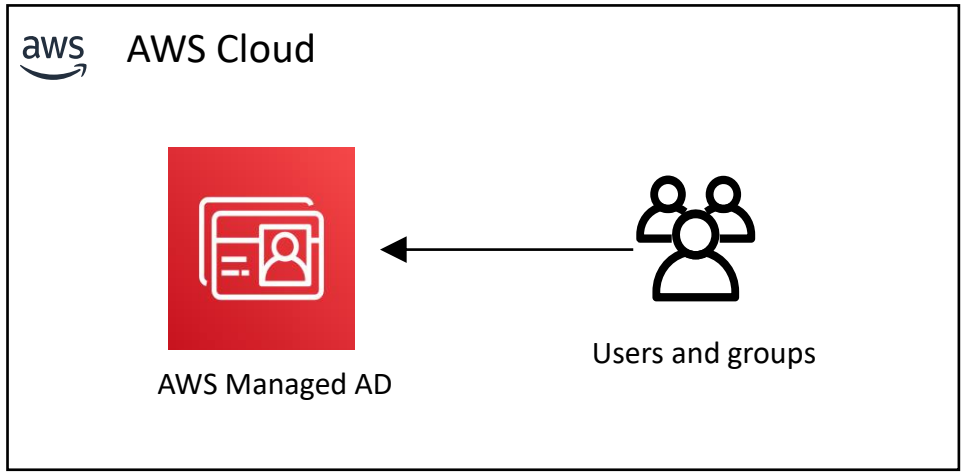
AWS-managed infrastructure

AWS Managed AD: Migrate and Modernize

Architect



AWS Managed AD with on-premise AD trust



Standalone AWS Managed AD

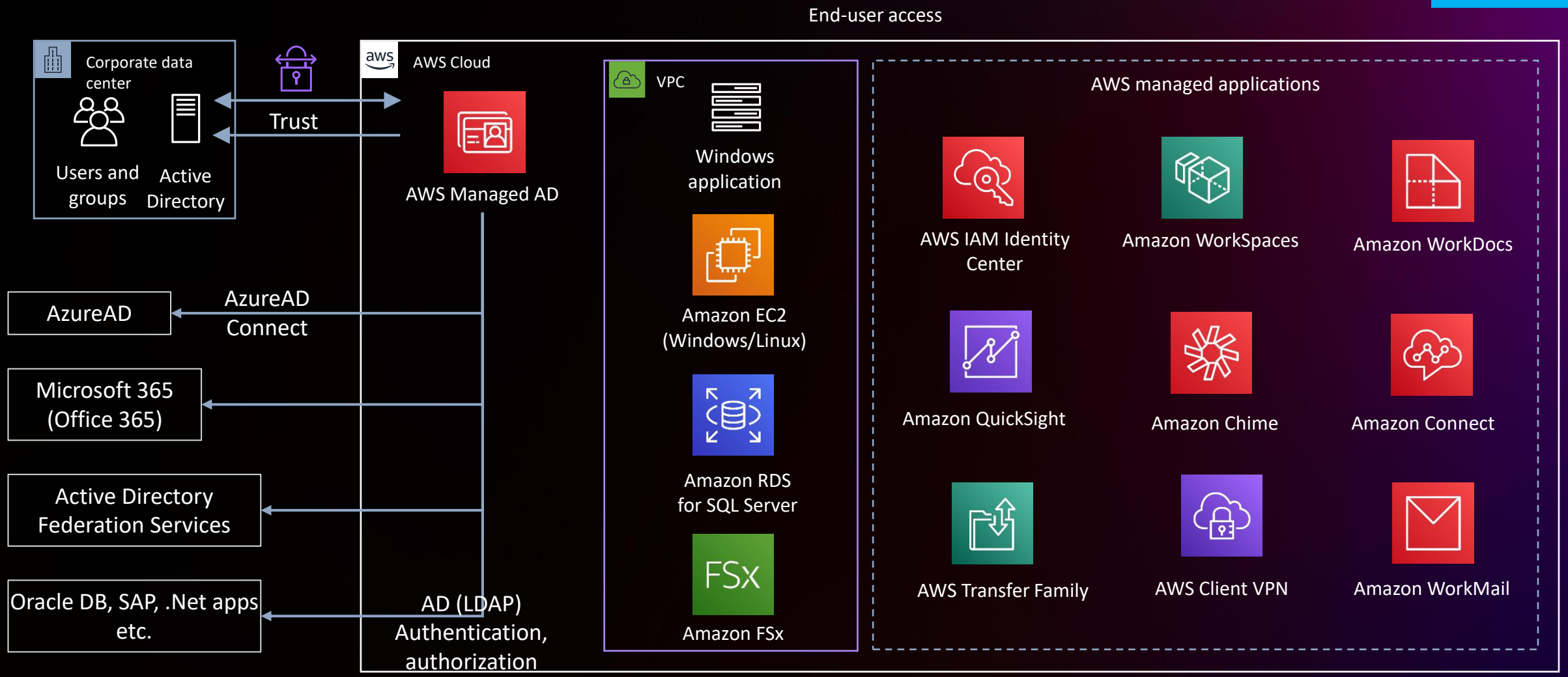
- Integrate with your existing enterprise AD with one-way or two trust relationships
- Migrate AD users and groups in a phased approach

- Migrate identities to/from divestiture/acquisitions to AWS Managed AD
- Empower dev teams to innovate and build quickly by setting up ephemeral non-production environments

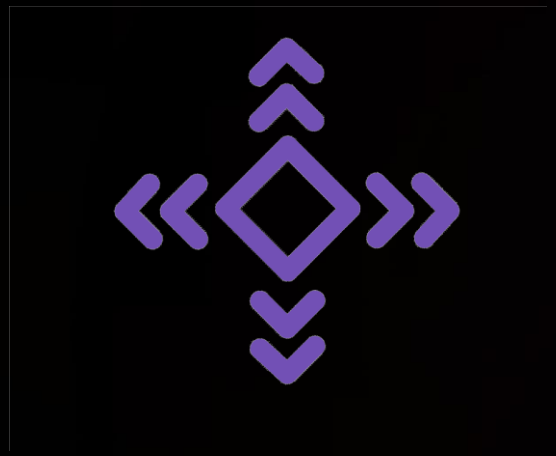
Application integration

INTEGRATE 10+ AWS SERVICES AND MANY MORE DIRECTORY AWARE WORKLOADS IN A SNAP

Architect



We continue to invest in these pillars



Flexible

Scalable

Adoptable

Resources

IAM Identity Center overview
https://go.aws/3U2L7N8

IAM best practices
https://go.aws/3FELskM

IAM workshops
https://workshops.aws/categories/Identity

AWS Managed Microsoft AD
https://go.aws/3UmdA06

Quick Start for AD
https://go.aws/3sZIobj

AWS workshop for AD
https://workshops.aws/categories/Active Directory

Free MFA security keys in the Village

We’re offering free MFA security keys at re:Invent as a thank you to attendees

Pick up your key at:

1. The Security, Identity and Compliance kiosk at the Village, Booth 1335 (in the Venetian)
2. Cloud Operations Governance, Financial Management, and Observability kiosks at The Village, Booth 1335 (in the Venetian)

Thank you!

Harvinder Nagpal

https://www.linkedin.com/in/harvindernagpal/

Jonathan VanKim

https://www.linkedin.com/in/jonathanvankim/

Please complete the session survey in the **mobile app**