AWS Single Sign-On (SSO)

business

Anand Murugesan, Sr. Product Manager

2/1/2017

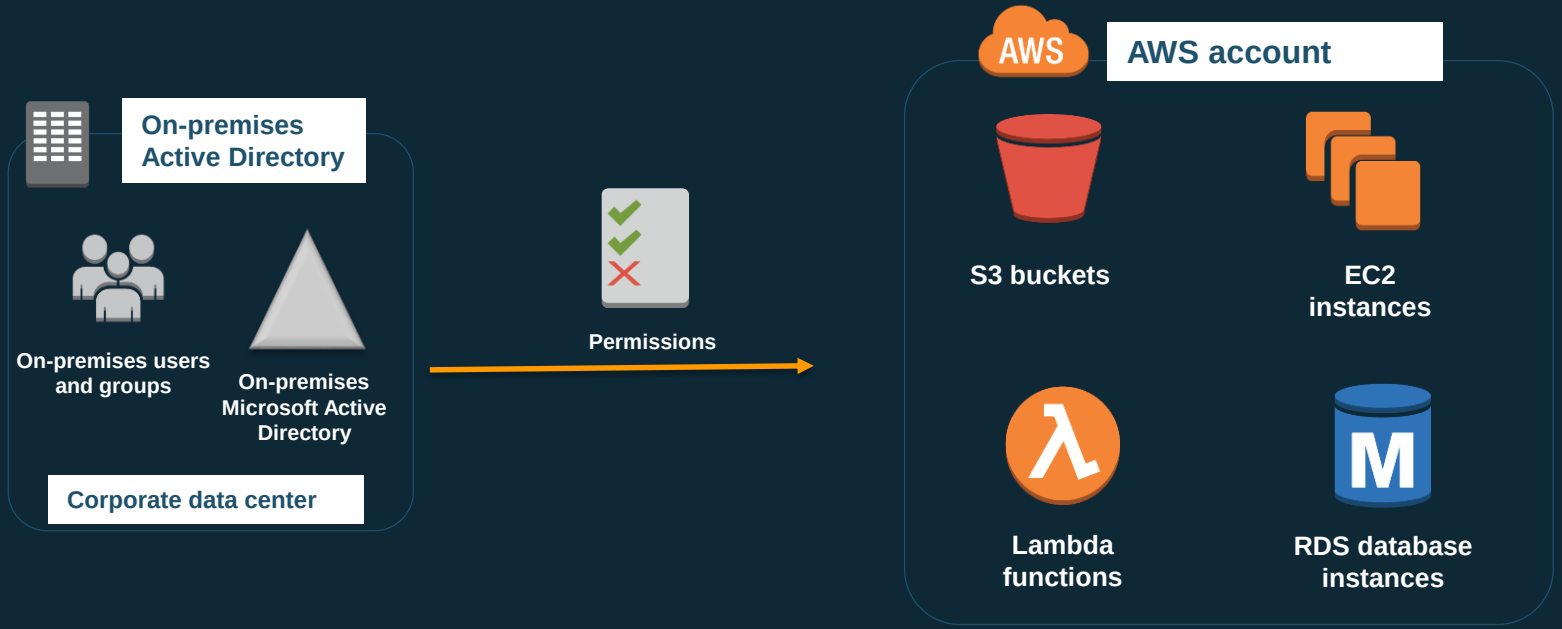
Agenda

- Challenges in managing cloud services access
- Introducing AWS SSO
- Pricing and availability
- Demonstration
- Q &A

How customers manage access to AWS accounts

- Permissions defined as policies
- Attached to roles, users, and groups
- Create AWS IAM users and assign permissions

Connect corporate directory



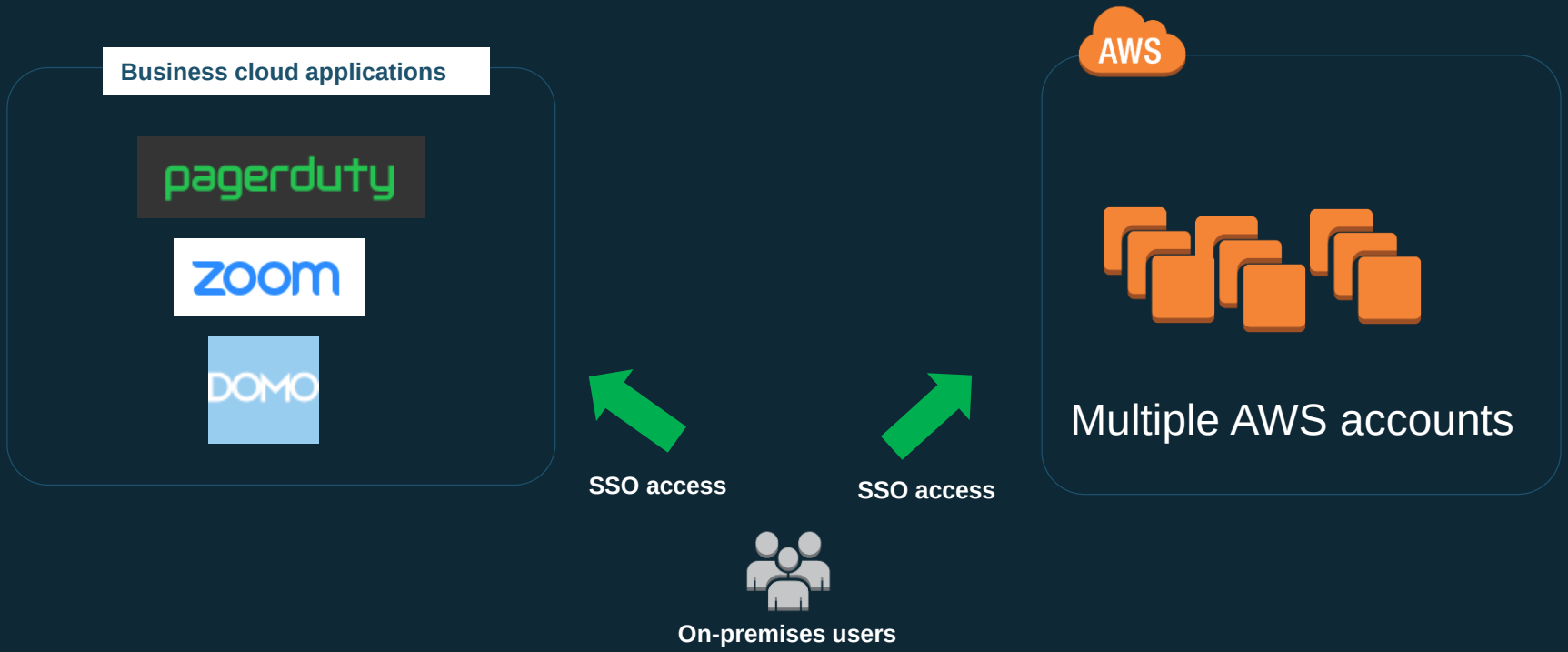
Use it to control access to
AWS resources through existing corporate Active Directory

Business scaling up

Growing business

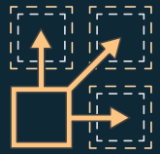
- Demand for AWS resources
  - Different departments
  - Different purposes for same teams
- Multiple AWS accounts provide security isolation

Cloud applications for business agility



Challenges

Managing access to multiple AWS accounts and business applications is expensive, hard, and time-consuming.



Managing multiple AWS accounts requires effort

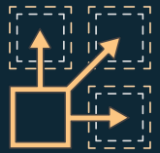
Numerous credentials

No centralized security controls

Access to business applications takes time and effort, and is expensive

Hard to set up, operate, and use

Challenges – Managing multiple AWS accounts



Managing multiple AWS accounts requires effort

- Maintain a list of AWS accounts
- General-purpose SSO solutions treat AWS accounts as separate applications and don't integrate deeply
- SSO Setup – Cut-and-paste configuration across consoles
- New account? Repeat the setup process. Can't scale business quickly
- Set up roles in each account. Keep the roles updated
- Managing user access to accounts

aws

Challenges – Credentials and security control

Numerous credentials

No centralized security controls

- Different password policies for different accounts and cloud applications
- Numerous passwords–Password fatigue leads to weak passwords, writing down in cleartext
- Access changes needs to be performed in cloud services manually
- Removing access to cloud services is a manual process
- Exposes critical business data to unauthorized access

aws

Challenges – Access to business applications

Access to business applications takes time and effort, and is expensive

- Setting up SSO and troubleshooting each application typically took days
- In some cases, this setup could take weeks because it required you to communicate back and forth with application vendors
- Vendor changes to the application configuration results in unexpected loss of access and requires changes to configuration and troubleshooting again
- Requires you to understand the nuances of SAML integration

aws

Challenges – Hard to set up and manage

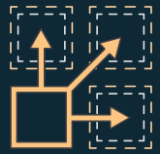
Hard to set up, operate, and use

- Prepackaged SSO software requires you to procure hardware and install OS and patches
- Involves SSO software installation and ongoing patching and upgrade
- High availability and security require expertise and time
- Upfront investment and ongoing maintenance costs
- Visibility into access requires manual reconciliation of data across multiple accounts, applications, and corporate directory
- Hard for administrators and users to keep track of application access details

aws

Challenges - Summary

Managing access to multiple AWS accounts and business applications is expensive, hard, and time-consuming.



Managing multiple AWS accounts requires effort

Numerous credentials

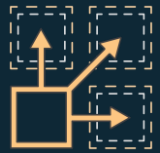
No centralized security controls

Access to business applications takes time and effort and is expensive

Hard to set up, operate, and use

Introducing AWS SSO

Centrally manage single sign-on (SSO) access to multiple AWS accounts and business applications.



Centrally manage access to multiple AWS accounts

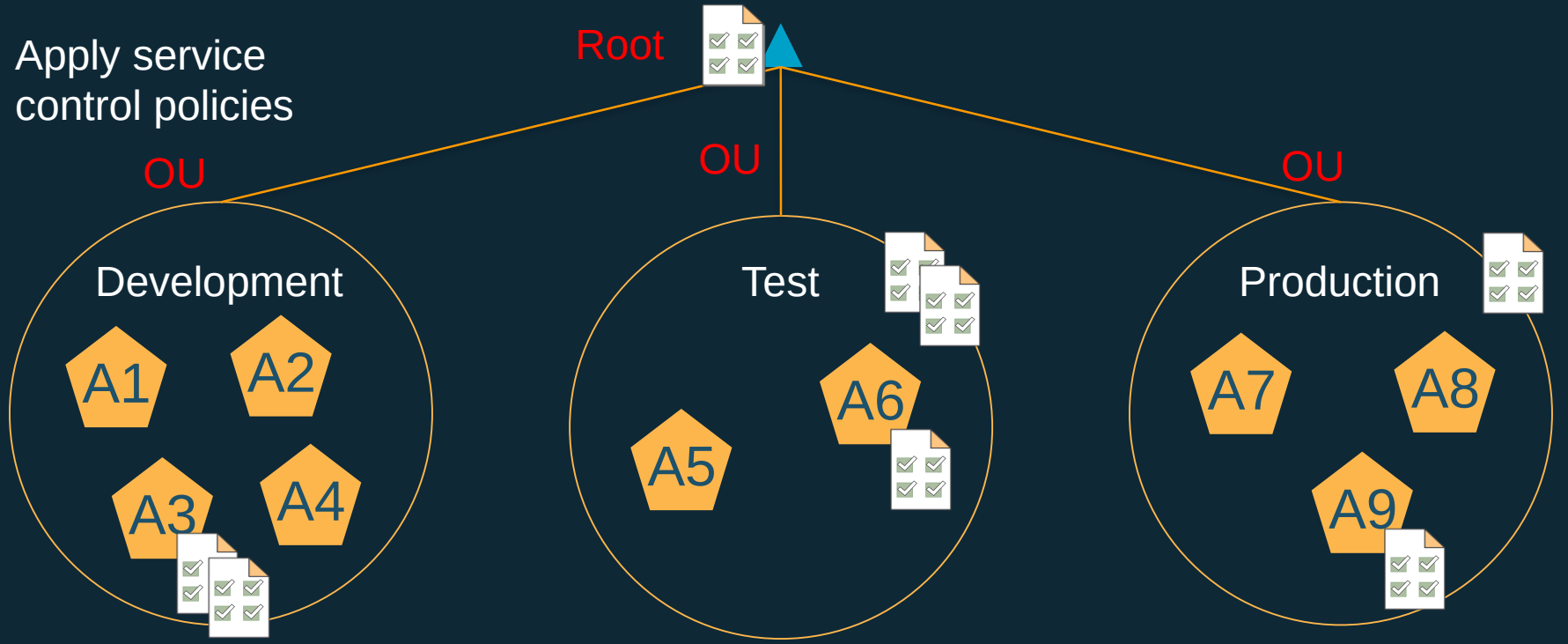
Use your existing corporate identities

SSO access to business applications

Easy to enable and use

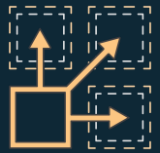
AWS Organizations – Account management

Apply service control policies



Allows you to organize AWS accounts
Controls access to AWS services

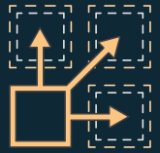
Central access to AWS accounts



Centrally manage access to multiple AWS accounts

- Lists AWS accounts managed in AWS Organizations
- Works with all AWS accounts and integrates deeply
- SSO setup to AWS accounts is automatic.
- New accounts are set up automatically
- Provisions permissions into all AWS accounts
- Manage access to all accounts from a central place

AWS SSO - Central access to AWS accounts



Centrally manage access to multiple AWS accounts

AWS SSO - Central access to AWS accounts

- Connects to AWS Organizations and lists your AWS accounts
- Allows filtering accounts by OU
- Automatic SSO setup to AWS accounts
- Centralized management of account permission sets
- Define, apply, and reapply permission sets to all AWS accounts

Single password to access cloud services

Use your existing corporate identities

- Single corporate password works for cloud services
- Stronger passwords improve security of cloud services
- Access changes to cloud services as group membership changes in on-premises Active Directory
- Immediate revocation of access to leaving employees.
- Protects critical business data from unauthorized access

aws

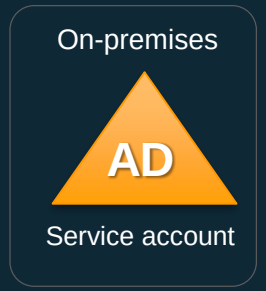
AWS SSO – Connect your existing Active Directory

Corporate Active Directory

Corporate Active Directory connection options

Managed AD

1



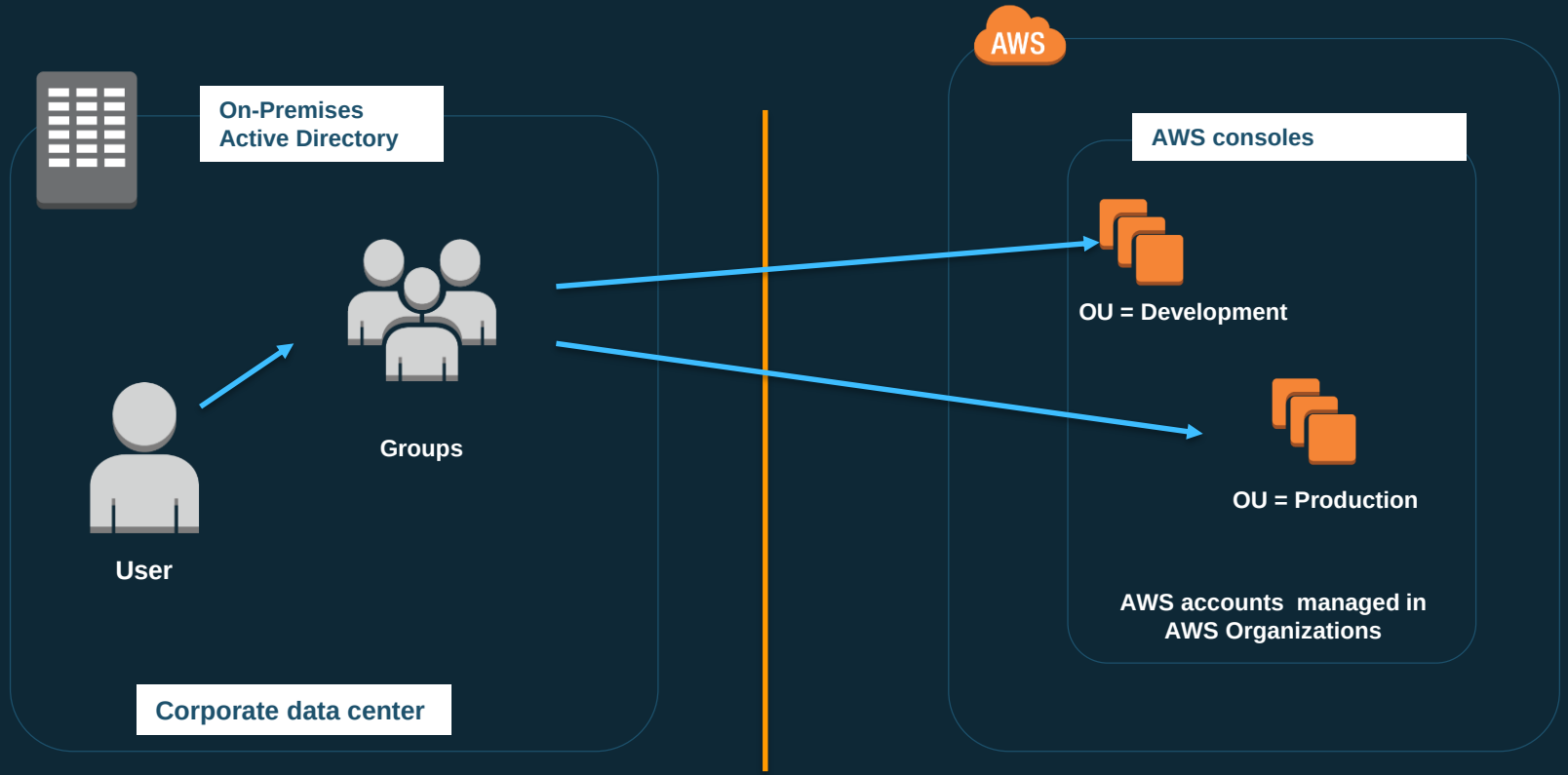
AD Connector

2

AD Trust

3

AWS SSO – Extends your existing business processes



Map on-premises AD groups to accounts and applications

Access to business applications

SSO access to business applications

- Preintegrated with commonly used cloud applications
- Set up using simple step-by-step instructions
- Vendor changes to the application configuration are taken care by AWS
- Nuances of SAML integration simplified
- Configure any SAML 2.0 application using application configuration wizard

aws

AWS SSO – Application configuration wizard

CHOOSE

1 + 1 = 2

Pick a preintegrated application

Follow step-by-step customized instructions for each application

Configure SSO

Assign access

aws

Supports SAML 2.0 for custom applications

Supports Security Assertion Markup Language 2.0

- Configure applications not in the preintegrated list
- Internal applications built by you
- Internal applications supplied by partners
- Seamless access to applications during migration to the AWS Cloud

SAML 2.0

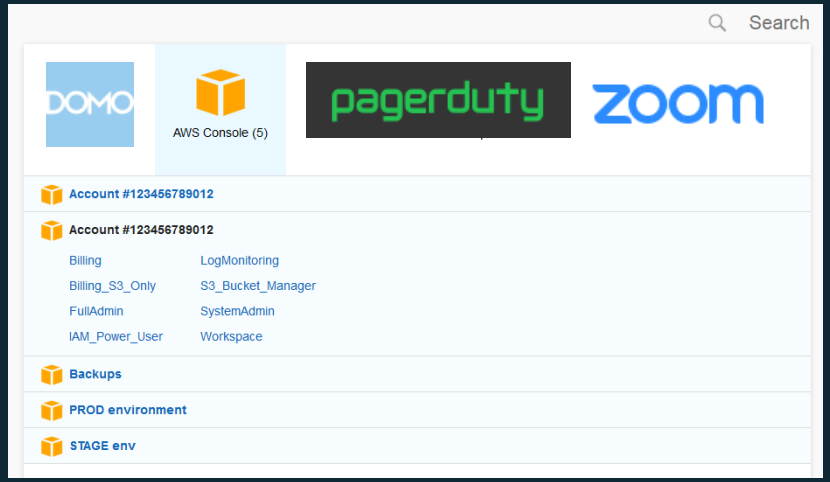
Easy to enable and use

Easy to enable and use

- No software or hardware needed
- AWS managed service
- No upfront investment or ongoing maintenance costs
- Highly available service
- Better visibility into access of cloud services using centralized auditing
- Application access is instantaneous
- Users can access cloud services from a central user portal

aws

Central place to access



- One place to find all:
  - AWS consoles
  - Business applications
  - Custom internal applications
- Easily search and find applications
- No need to distribute or remember URLs or roles
- Single corporate credentials give access to cloud services

Centralized auditing

- Audit all SSO access in AWS CloudTrail
- Increased visibility into users' SSO access to AWS accounts and cloud applications

Pricing and availability

- Included with your AWS accounts at no additional charge
- Public Preview in the US East (N. Virginia) Region

Demonstration

Questions?