Advanced IAM Concepts: AWS IAM Identity Center, and AWS Directory Services

Andru Estes
Principal Author
andru-estes

Using AWS Directory Services

AWS Directory Services

Provides several options to set up and run Microsoft Active Directory (AD) with other AWS services

It allows you to offload the painful parts of keeping AD online over to AWS, while still giving you full control and flexibility of AD.

AWS Directory Services Options

AWS Managed Microsoft AD

This is the entire AD suite and you can easily create your own AD within AWS (*create users, manage MFA*)

Powered by a pair of highly-available Windows Server 2019 domain controllers

Less overhead and supports group policies

If a solution requires you to implement one-way or two-way trusts, it must be this service

AWS Enterprise services require two-way trusts to function properly when tying into existing AD.

Examples are Chime, AWS IAM Identity Center, and WorkSpaces

AWS Managed Microsoft AD - Trusts

One-Way Trust

Users in one domain need to access resources in the other, but not the other way around

Two-Way Trust

Trusts go in both directions. Each domain trusts the other, and users have access both ways

AD Connector

Directory gateway where you redirect requests to an on-prem Microsoft AD

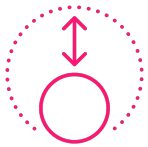
This solution does not cache any information within the cloud

Two sizes: Small, Large

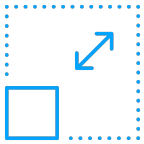
Spread loads across multiple AD Connectors to scale performance

Users are managed within your on-prem Microsoft AD only

Important AD Connector Concepts

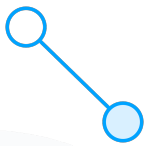


Small AD Connectors are for smaller organizations and can handle a low number of operations per second



Large AD Connectors are for larger organizations and can handle a moderate to high number of operations per second

This service does support MFA as well



Does not support Active Directory transitive trusts, and there is a strict 1-to-1 relationship between AD and your AD Connectors

Simple AD

Standalone managed directory (Samba 4 AD Compatible Server)

Two sizes: Small, Large

Offers subsets of features that are provided by AWS Managed AD

Cannot be joined with your on-prem Microsoft AD

Does not support MFA, trusts, Powershell, or certain service accounts

Simple AD Sizes

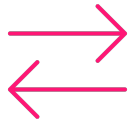
Small

Supports up to 500 users, or approximately 2,000 objects including users, groups, and computers

Large

Supports up to 5,000 users, or approximately 20,000 objects including users, groups, and computers

Exam Tips



AWS Managed Microsoft AD offers the most amount of AD features and is the best choice for more than 5,000 users, as well as the only service that supports trusts

AD Connector connects your existing on-premises Active Directory to AWS, and is the best choice when you're using existing on-premises AD and want to avoid data retention in AWS

Simple AD is the least expensive AD-compatible service offering common directory features. Perfect for simple workloads that don't need advanced capabilities.

Single-Sign On with AWS IAM Identity Center

AWS IAM Identity Center

The go-to AWS service for connecting your workforce users to your AWS accounts and AWS-managed applications

AWS IAM Identity Center Concepts

Service meant to provide you a single place to manage all logins for an org

Can connect existing identity providers (*Microsoft AD*, *Okta*, *OneLogin*)

Can also create and manage your users directly in IAM Identity Center

Use Case 1: Grant users access to applications hosted in AWS

Use Case 2: Grant users access to AWS accounts in multi-account orgs

Compatible Applications and Resources

Cloud apps like Salesforce, Microsoft 365, and Confluence

SAML-2.0 business applications

EC2 Windows instances

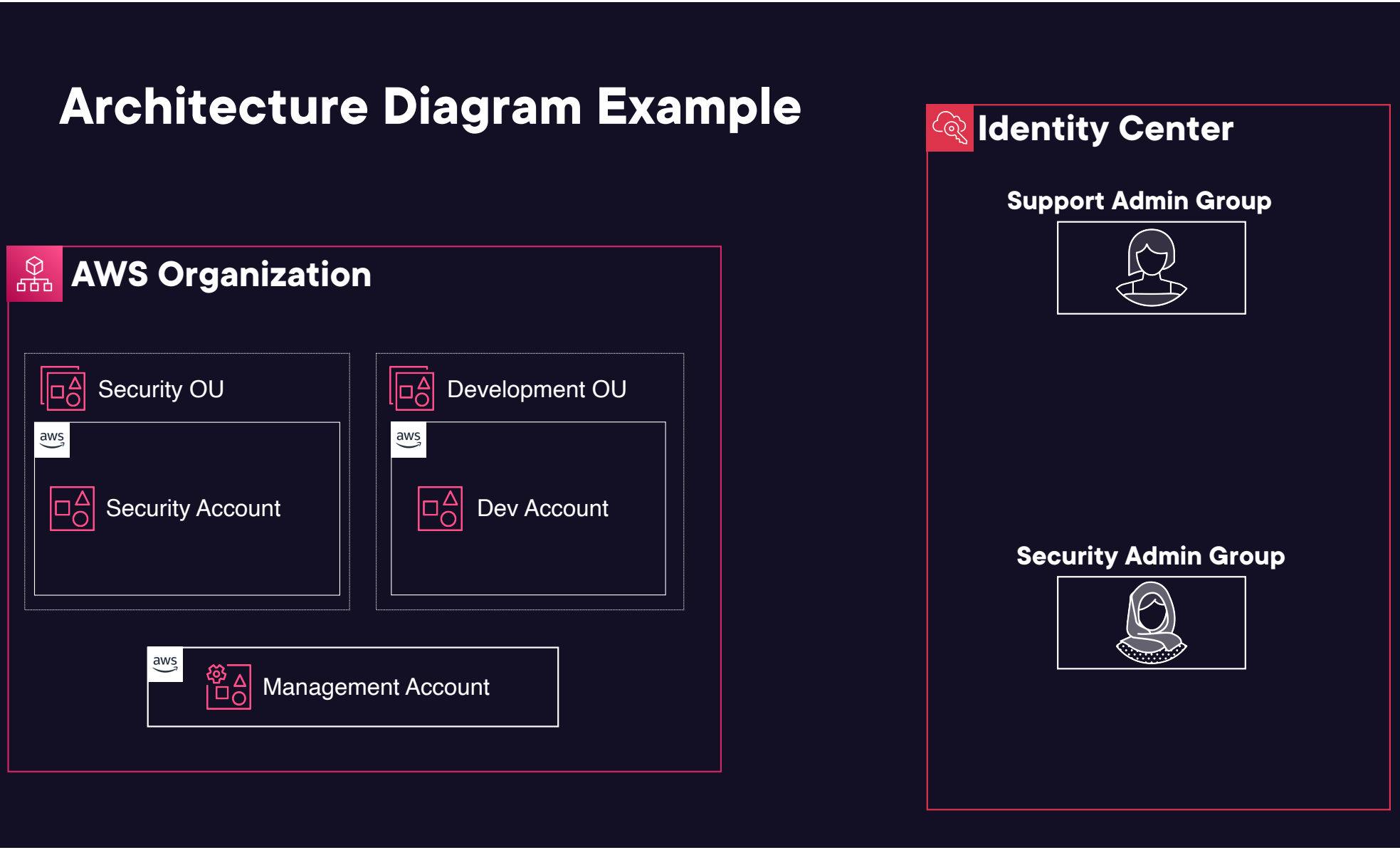
IAM Identity Center Assignments and Permissions

Assign users **Permission Sets** to specify one or more IAM policies to define the level of AWS access they have within their assigned AWS accounts that belong to an AWS Organization

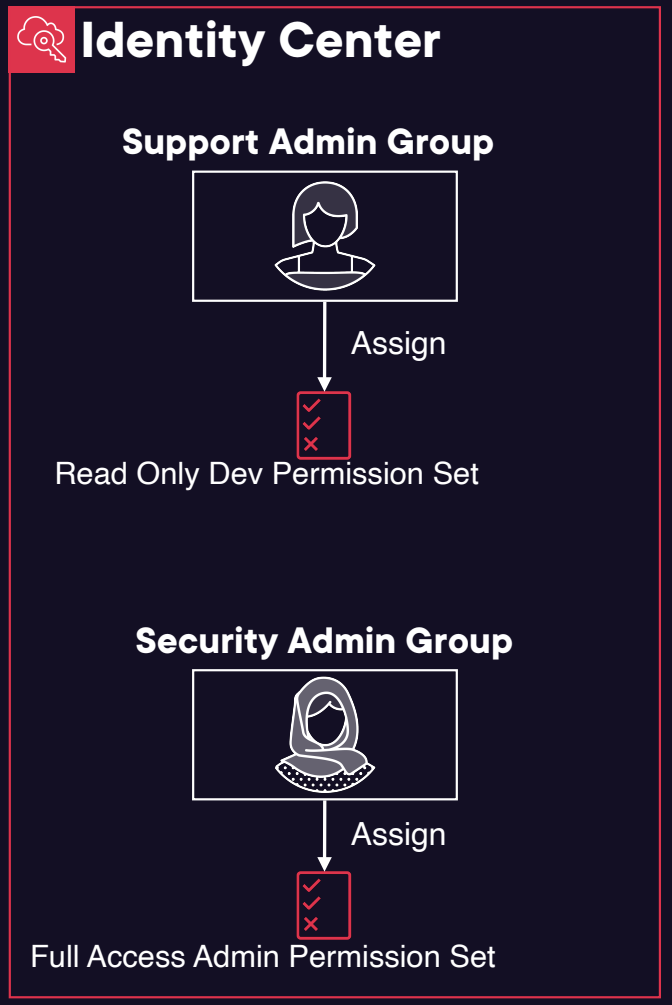
Application Assignments allow you to assign users within the service to actually login to an application within the cloud (*Salesforce*, *Jira*)

Attribute-based Access Control (ABAC) allows you to implement fine-grained access controls for levels of access based on a user's attributes (*department*, *location*, *title*)

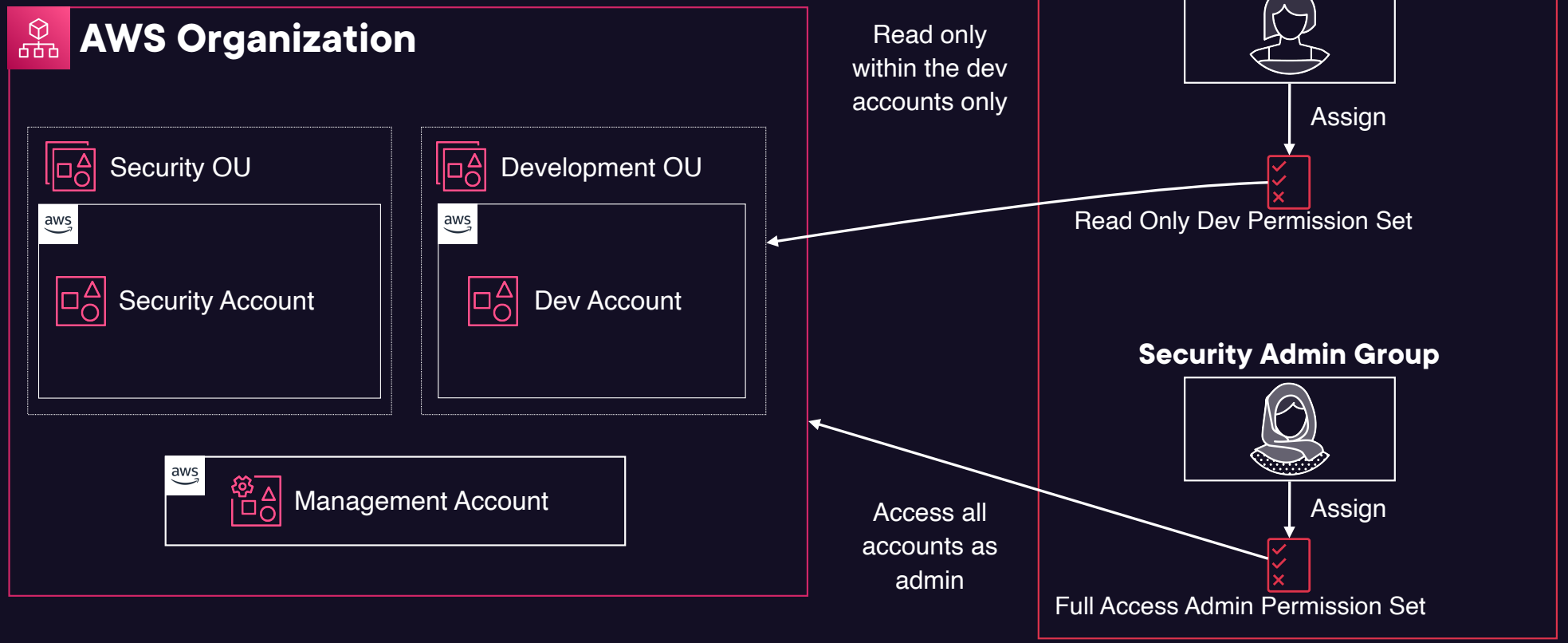
Architecture Diagram Example



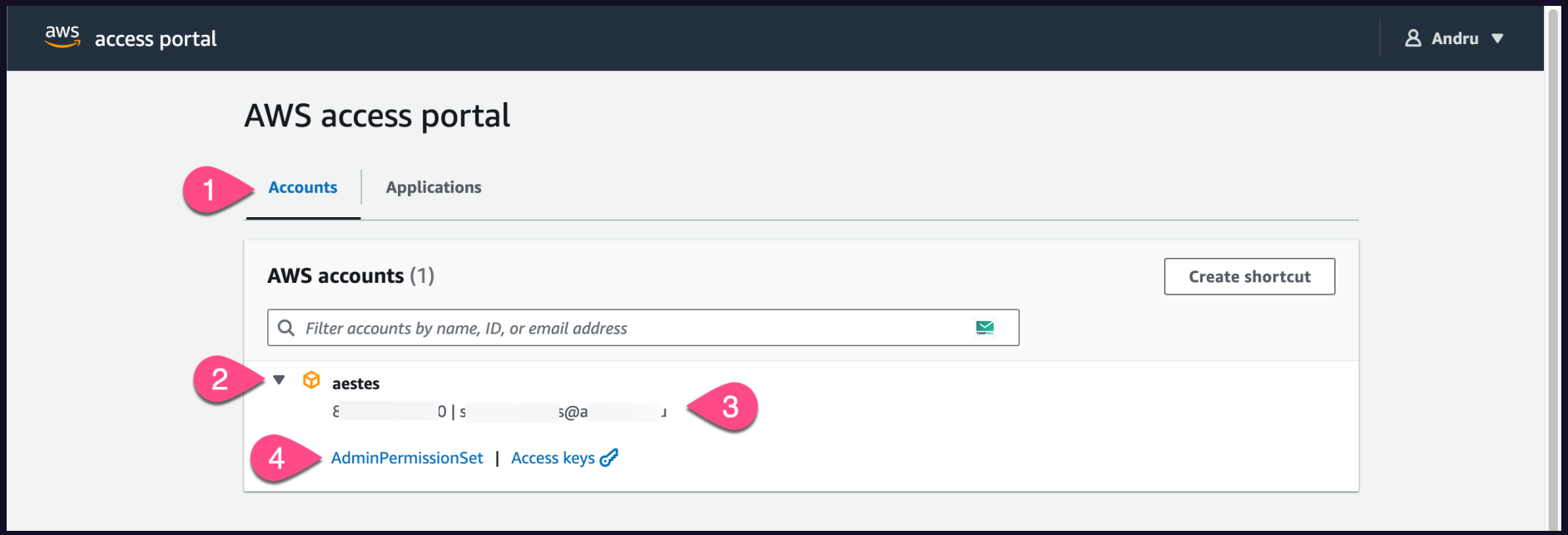
Architecture Diagram Example



Architecture Diagram Example



AWS IAM Identity Center Console View



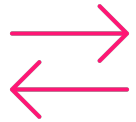
1. View the assigned AWS accounts or cloud application assignments
2. The name of the AWS accounts that have been assigned to you
3. The AWS account ID and account root email address
4. The assigned Permission Set (*IAM permissions*)

Exam Pro Tip #1: You must have AWS Organizations set up to use AWS IAM Identity Center.

Exam Pro Tip #2: If you need single-sign on and have multiple AWS accounts, think AWS IAM Identity Center.

Module Summary and Exam Tips

AWS Directory Services Exam Tips



AWS Managed Microsoft AD offers the most amount of AD features and is the only service that supports trusts

AD Connector is the best choice when you're using existing on-premises AD and want to avoid data retention in AWS

Simple AD is the least expensive AD-compatible service and is perfect for simple workloads that don't need advanced capabilities

AWS IAM Identity Center Exam Tips

You must have AWS Organizations set up to use AWS IAM Identity Center

Grant access to AWS accounts via Permission Sets

Grant access to cloud applications via Application Assignments

You can use ABAC to set up fine-grained access controls into accounts

Leverage existing Identity Providers (*Okta*, *AD*) with IAM Identity Center

Question about single-sign on or managing access to multiple AWS accounts? AWS IAM Identity Center!