Identity Management at AWS

Analyst Webinar, August 31, 2015
#AWS-IAM

What are the goals

- Better understanding of the scope of our identity services
- Walkthrough of our most common use cases
- Understanding our pricing
- Address open questions

Overview

- Broad selection of identities
  - AWS, corporate or social
  - AWS-managed, self-managed or bring your own identity
  - Standards-compliant – SAML, OIDC, Active Directory
- AWS Identity-related services
  - AWS Identity and Access Management (IAM)
  - AWS Security Token Service (STS)
  - AWS Directory Service
  - Amazon Cognito

AWS-Managed Identities (AWS IAM)

- Centralized authentication & authorization for AWS services
- Full lifecycle management of identities and credentials
  - Create IAM users, groups, policies in an AWS account
  - Grant permissions (entitlements) using IAM policy language
  - Delegate access within your AWS account
  - Manage credentials (e.g., passwords and access keys)
- Multi-factor authentication (MFA)
  - TOTP-based
  - Gemalto
  - App-based (e.g., Google Authenticator)
- AWS CloudTrail provides audit

IAM Console Overview

DEMO

Enterprise Federation

- Standards-based (SAML 2.0) or custom federation
- Enable existing users with SSO access to the console
  - Generate a claim/token from a trusted identity provider (IdP)
  - Use STS to exchange token for temporary AWS credentials
  - Seamless login to the AWS Management Console
- Requirements
  - A trusted *entity* (e.g., AD FS, Ping, Okta, OneLogin, other)
  - IAM roles to define the permissions to be granted to the entity

SAML-enabled SSO to the AWS Management Console

DEMO

Partners and Open Source

amazon web services

AWS Directory Services

- AWS-managed, highly available, and ready in minutes
  - AD Connector – integrates with an on-premises AD / RADIUS MFA
  - Simple AD – cloud-based, Active Directory compatible directory
- Use cases
  - Easily launch Windows instances as part of an AD domain
  - Enable existing on-premises AD users SSO access to:
    - AWS Management Console
    - WorkSpaces, WorkDocs and WorkMail

Setting up Simple AD and single sign-on (SSO)
to the AWS Management Console

DEMO

Social Identities

- AWS-backed apps that support sign in from social identity providers
- Enable apps to access your AWS account resources
- Amazon Cognito
  - Mobile identity management & data sync service
  - Unified identity across devices
  - Sync app data across devices
- Supported Identity providers
  - Login with Amazon, Facebook, Google+, Twitter, Digits
  - Any OpenID Connect (OIDC) provider
  - Unauthenticated guest users
  - Custom application-specific identity pools

Web app with OIDC-based sign in for Salesforce users

DEMO

Pricing

- IAM is provided at no additional cost
- AWS Directory Services
  - Free trial
  - $0.05 per hour per directory for small (~500 users) Simple AD and $0.15 for large (~5,000 users)
  - http://aws.amazon.com/directoryservice/pricing/
- Amazon Cognito
  - Free Tier
  - Identity federation provided at no additional cost
  - $0.15 for each 10,000 sync operations and $0.15 per GB of sync store per month
  - http://aws.amazon.com/cognito/pricing/

QUESTIONS