The Evolution of Identity and Access Management on AWS

Greg McConnel, Solutions Architect

aws

Webinar prerequisites

To get the most out of this session, you must be comfortable with several building blocks:

AWS IAM

Roles

Policies

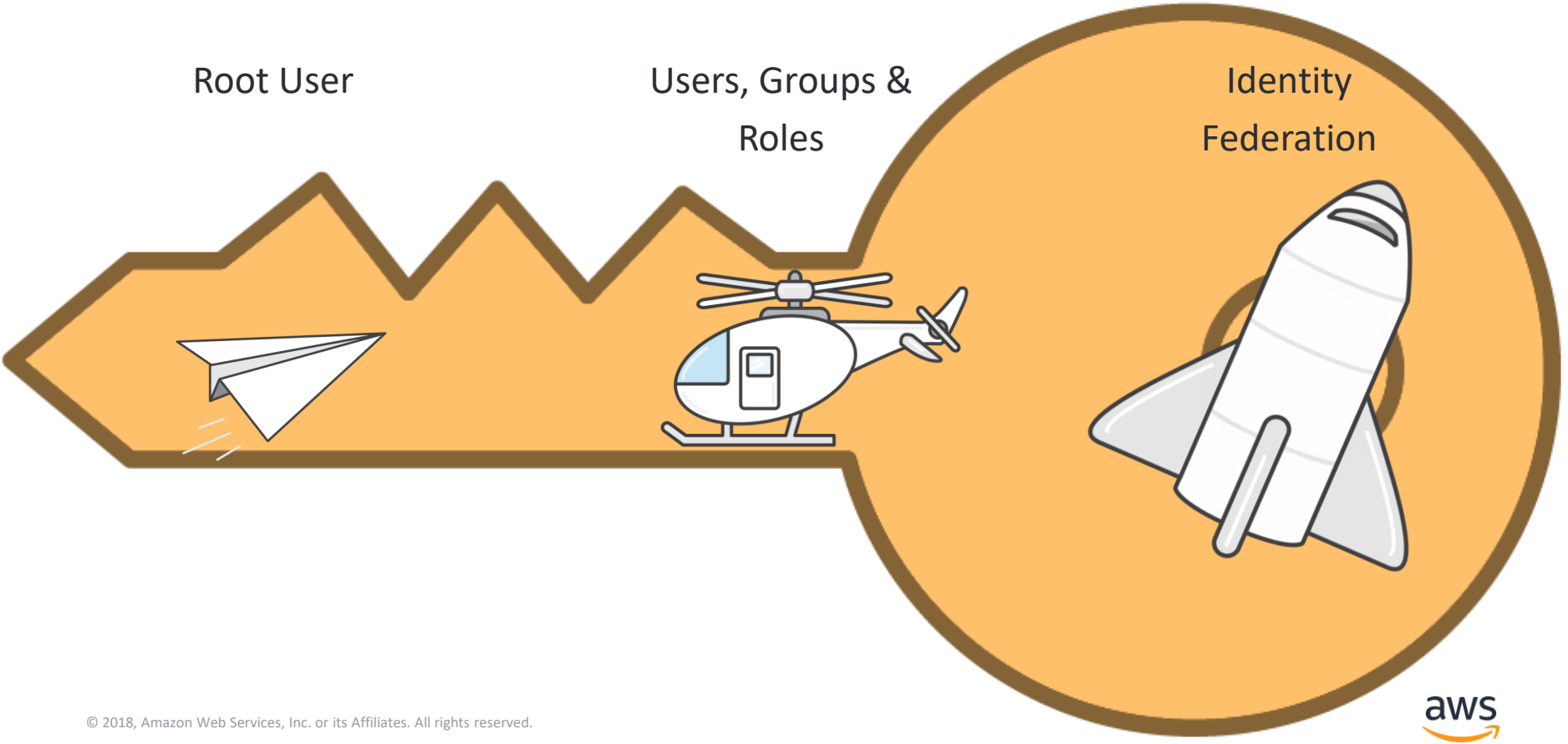
AWS STS

Long-term Access Keys

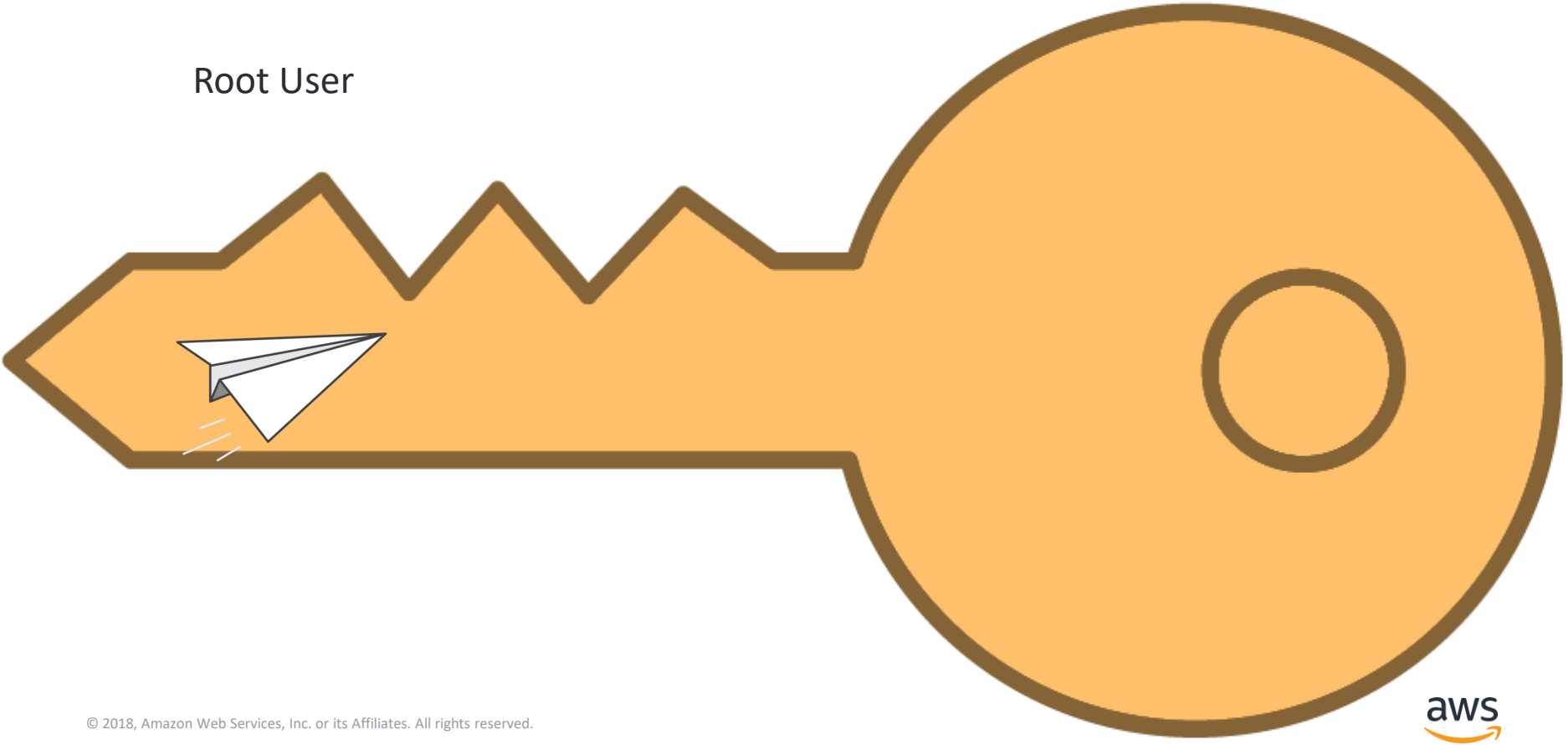
Temporary Security Credentials

aws

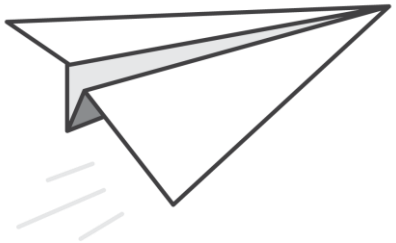
Evolution of Identity and Access Management on AWS

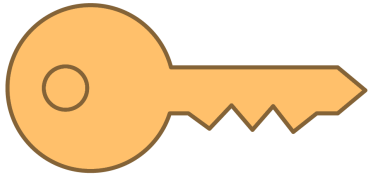


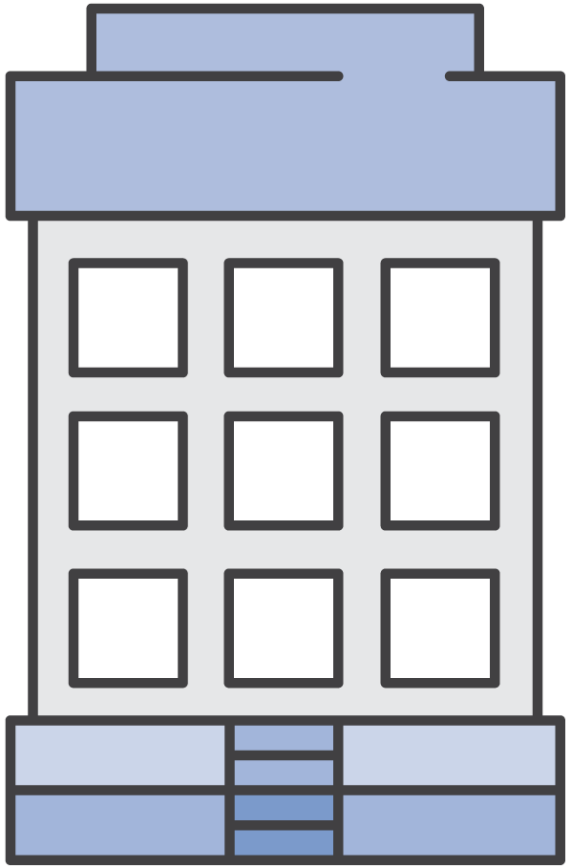
Evolution of Identity and Access Management on AWS



Root User

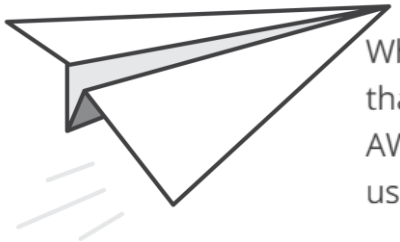






Root User

The AWS Account Root User



When you first create an Amazon Web Services (AWS) account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password that you used to create the account.

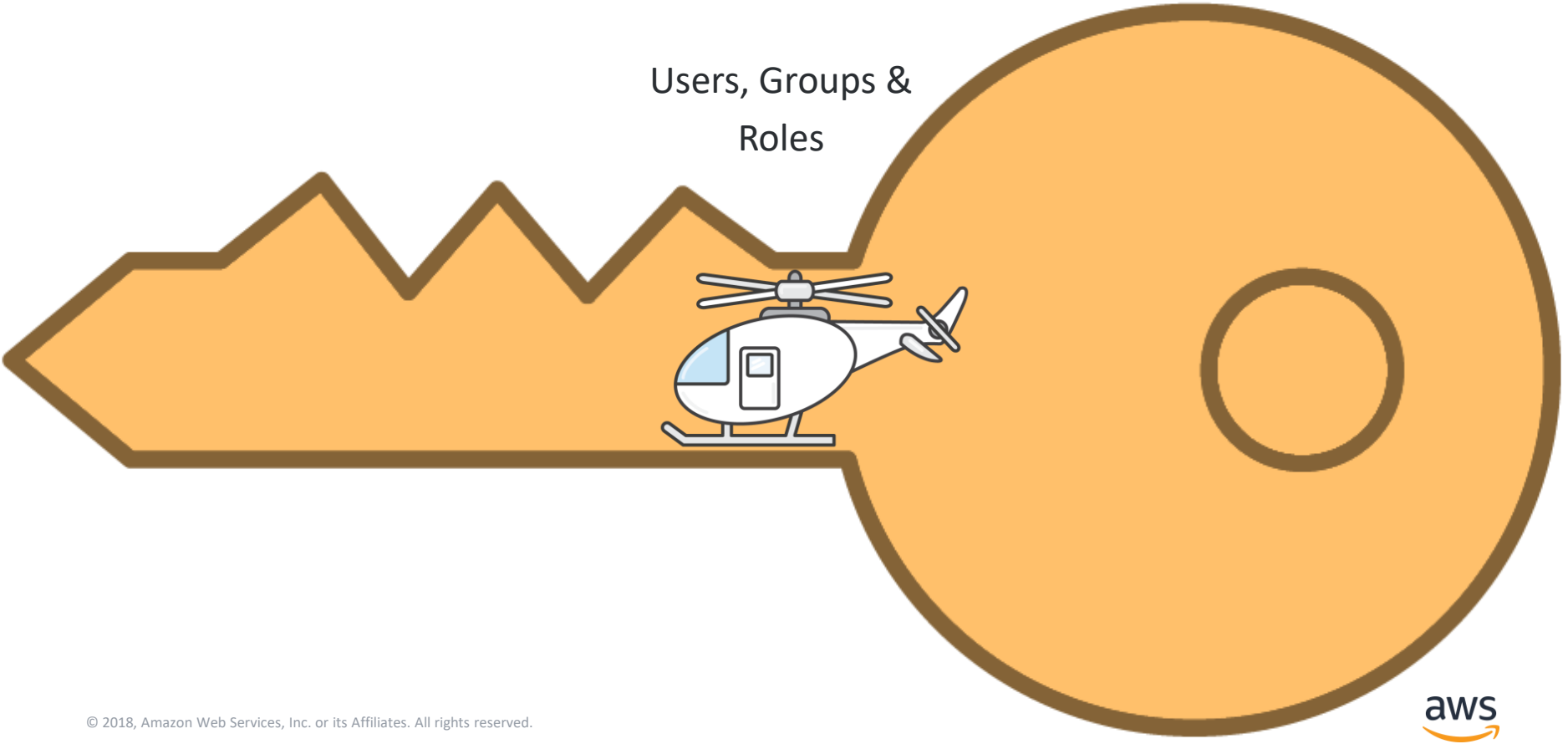
Important

We strongly recommend that you do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the best practice of using the root user only to create your first IAM user. Then securely lock away the root user credentials and use them to perform only a few account and service management tasks. To view the tasks that require you to sign in as the root user, see AWS Tasks That Require Root User. For a tutorial on how to set up an administrator for daily use, see Creating Your First IAM Admin User and Group.

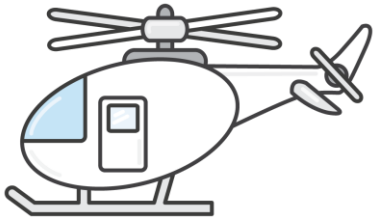
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html

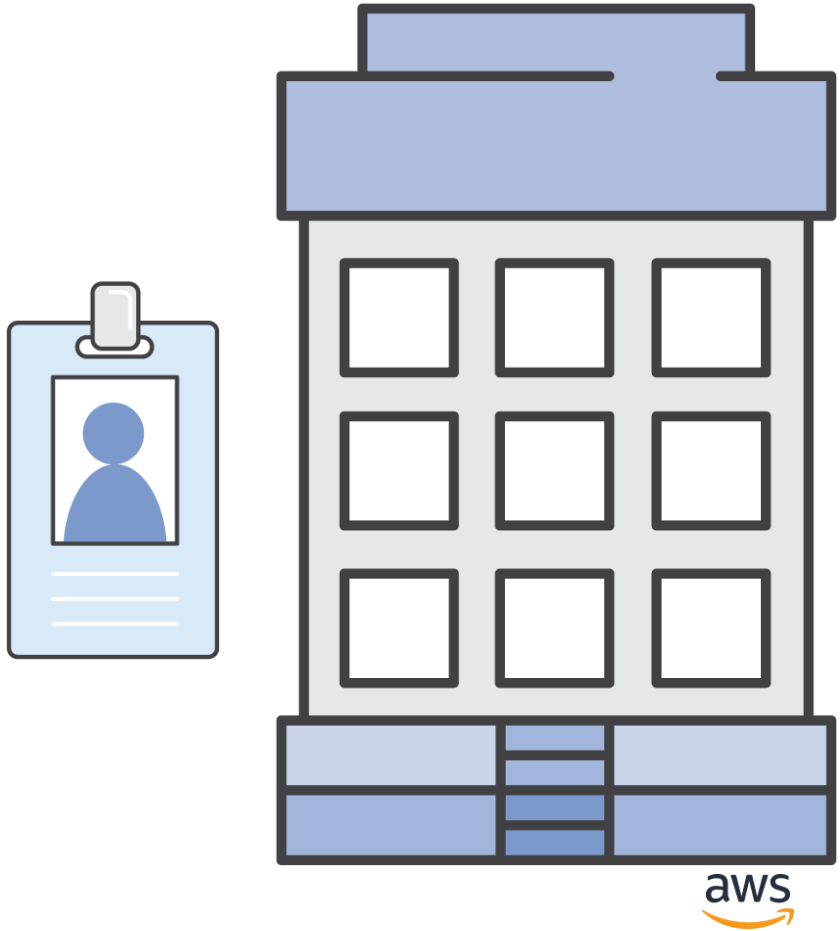
aws

Evolution of Identity and Access Management on AWS

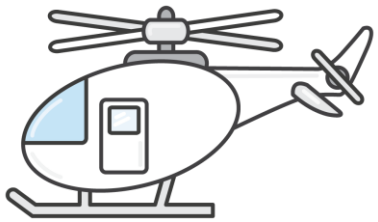


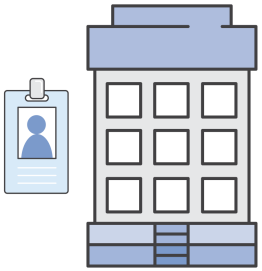
IAM Users/Groups/Roles

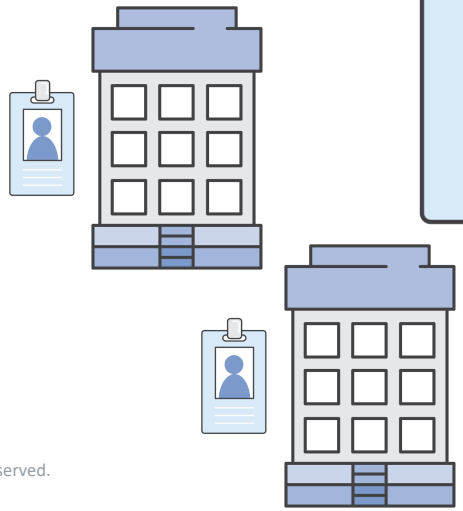


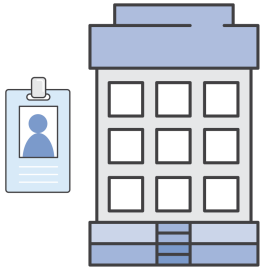


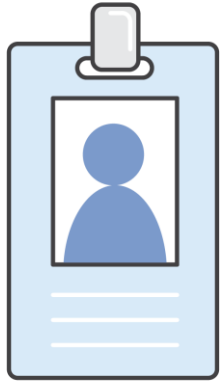
IAM Users/Groups/Roles

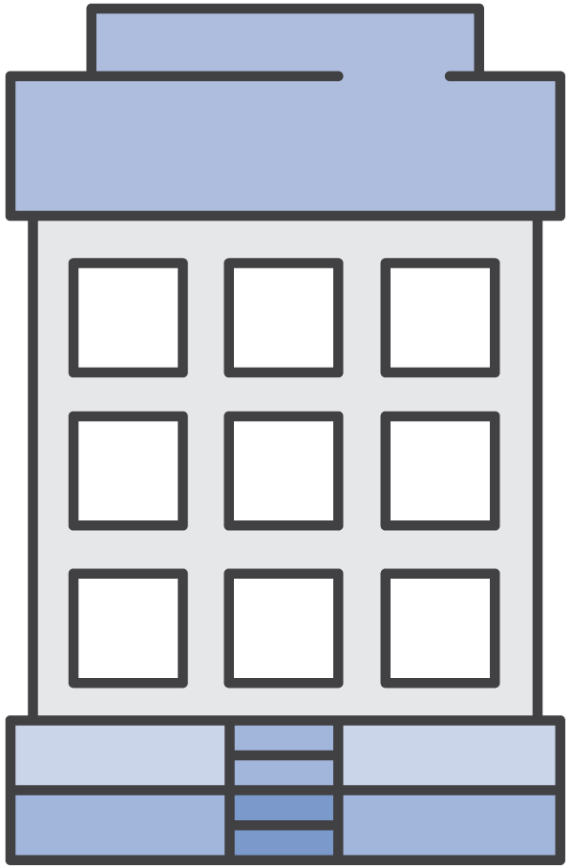




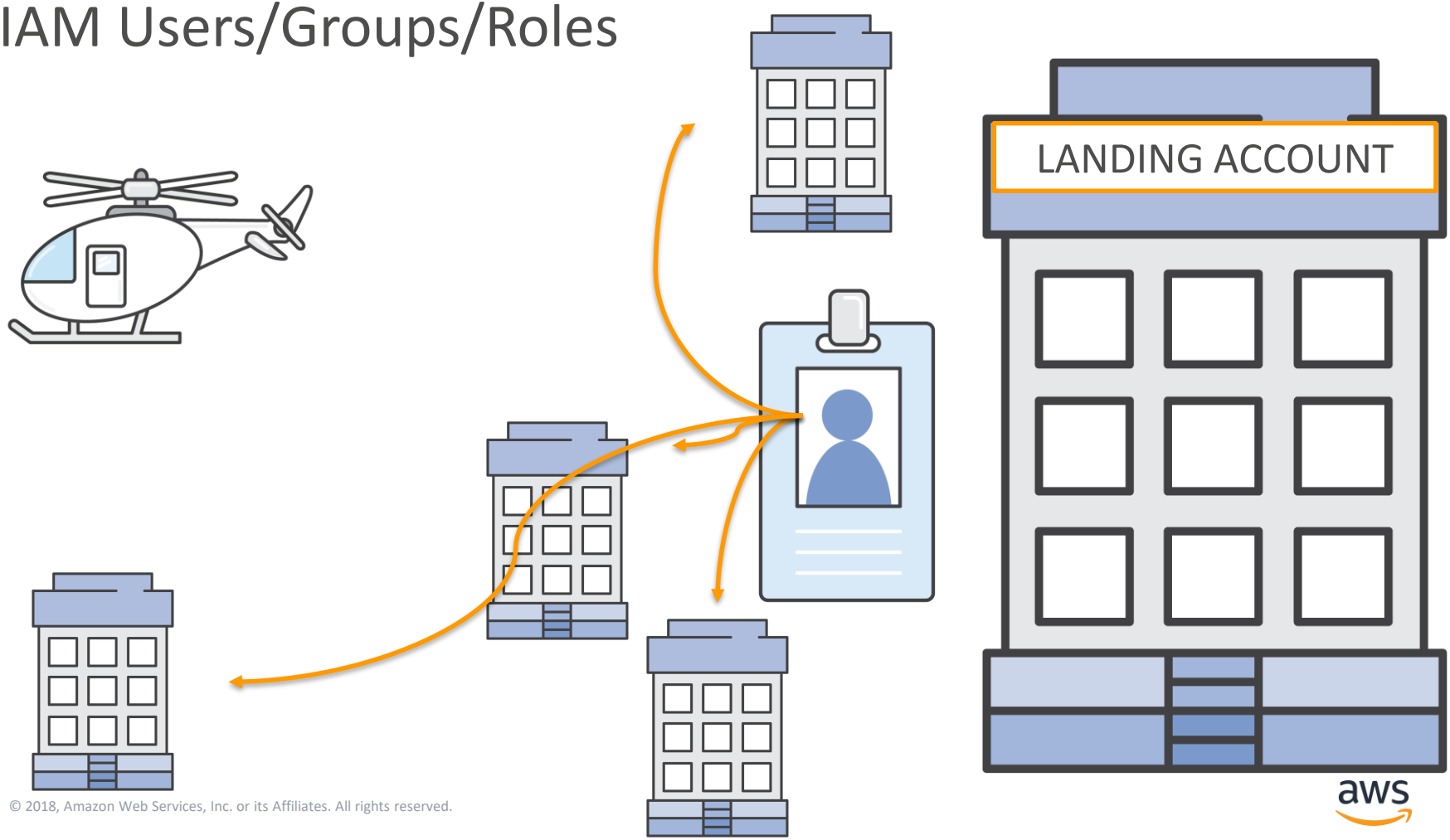




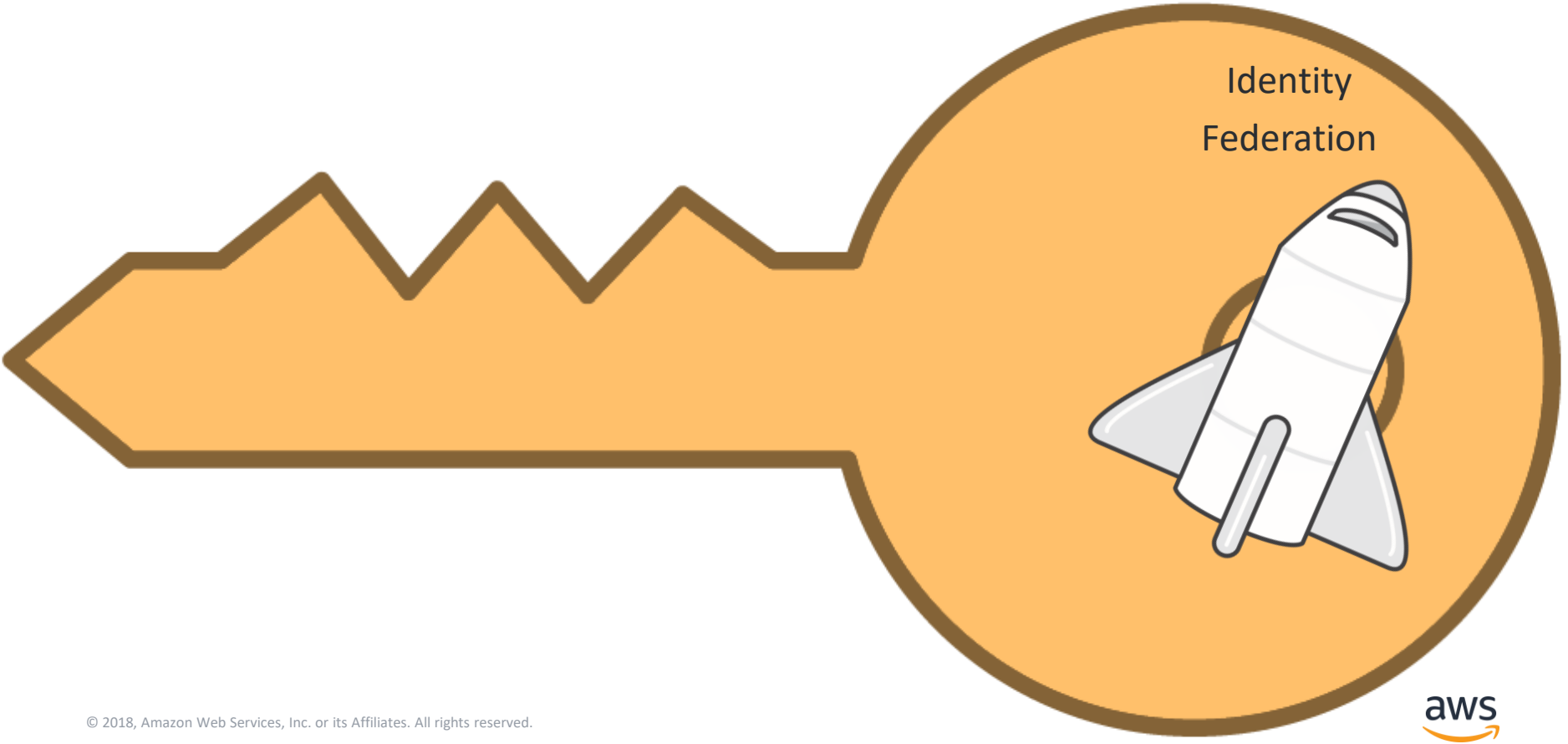




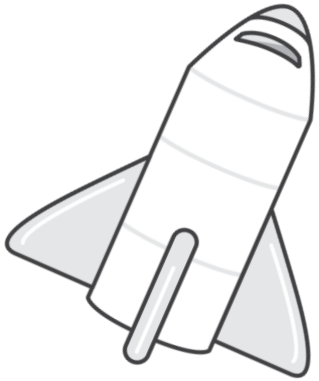
IAM Users/Groups/Roles

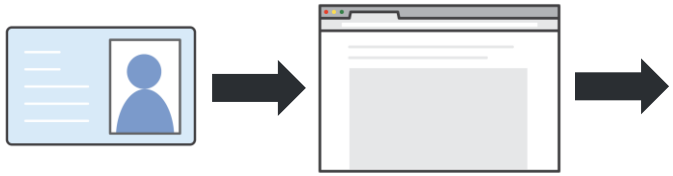


Evolution of Identity and Access Management on AWS



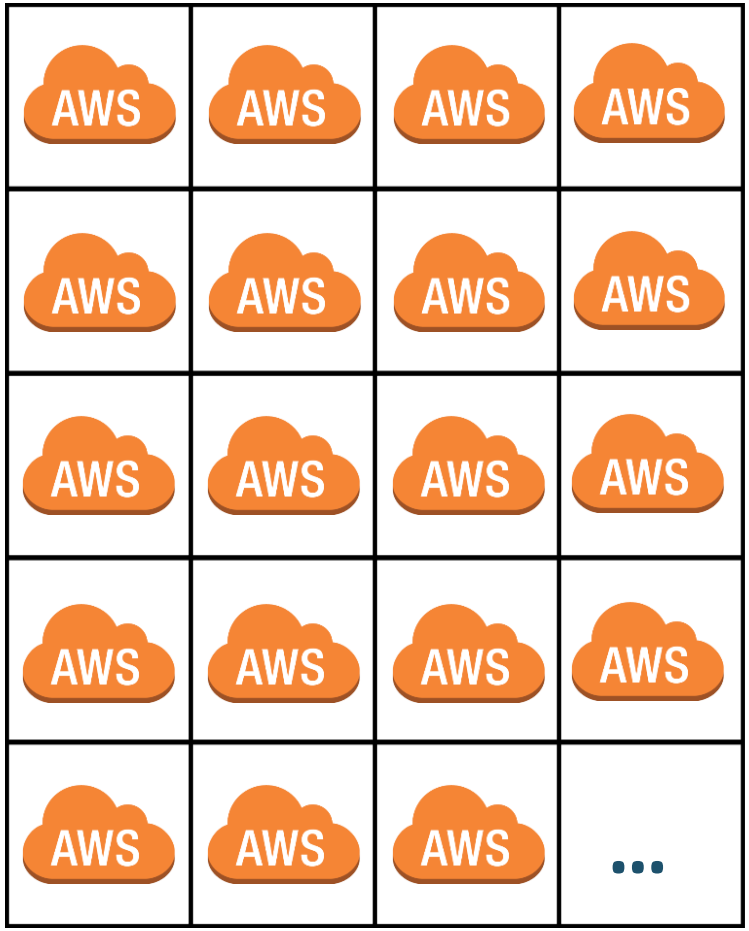
Identity Federation



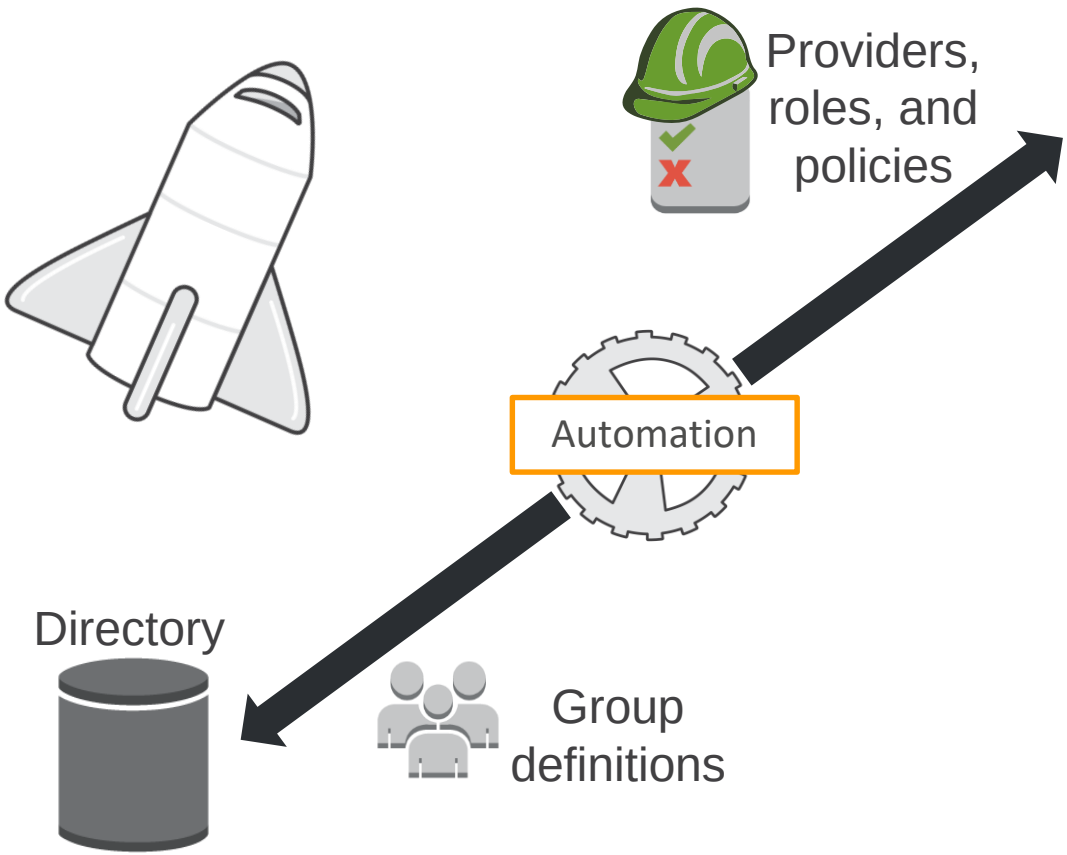


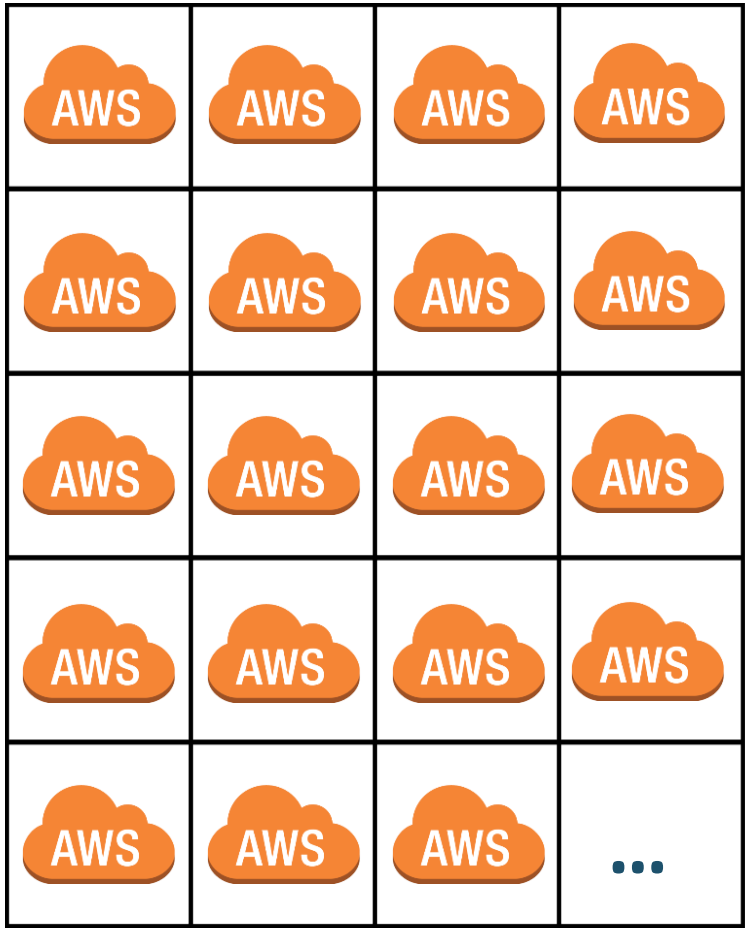
Corporate Identity

Identity Provider



Identity Federation





aws

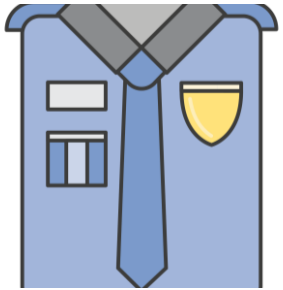
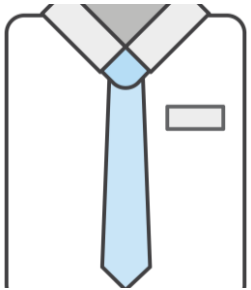
Agenda:

* Evolution of Identity Management
* Identity Federation Primer
* Two Demos

Identity Federation Benefits

- Help manage AWS at scale (but you will need automation)
- Align corporate user provisioning and de-provisioning with AWS identity and access management
- Centralize entitlement management
- Ease of access for users

Identity Federation Benefits

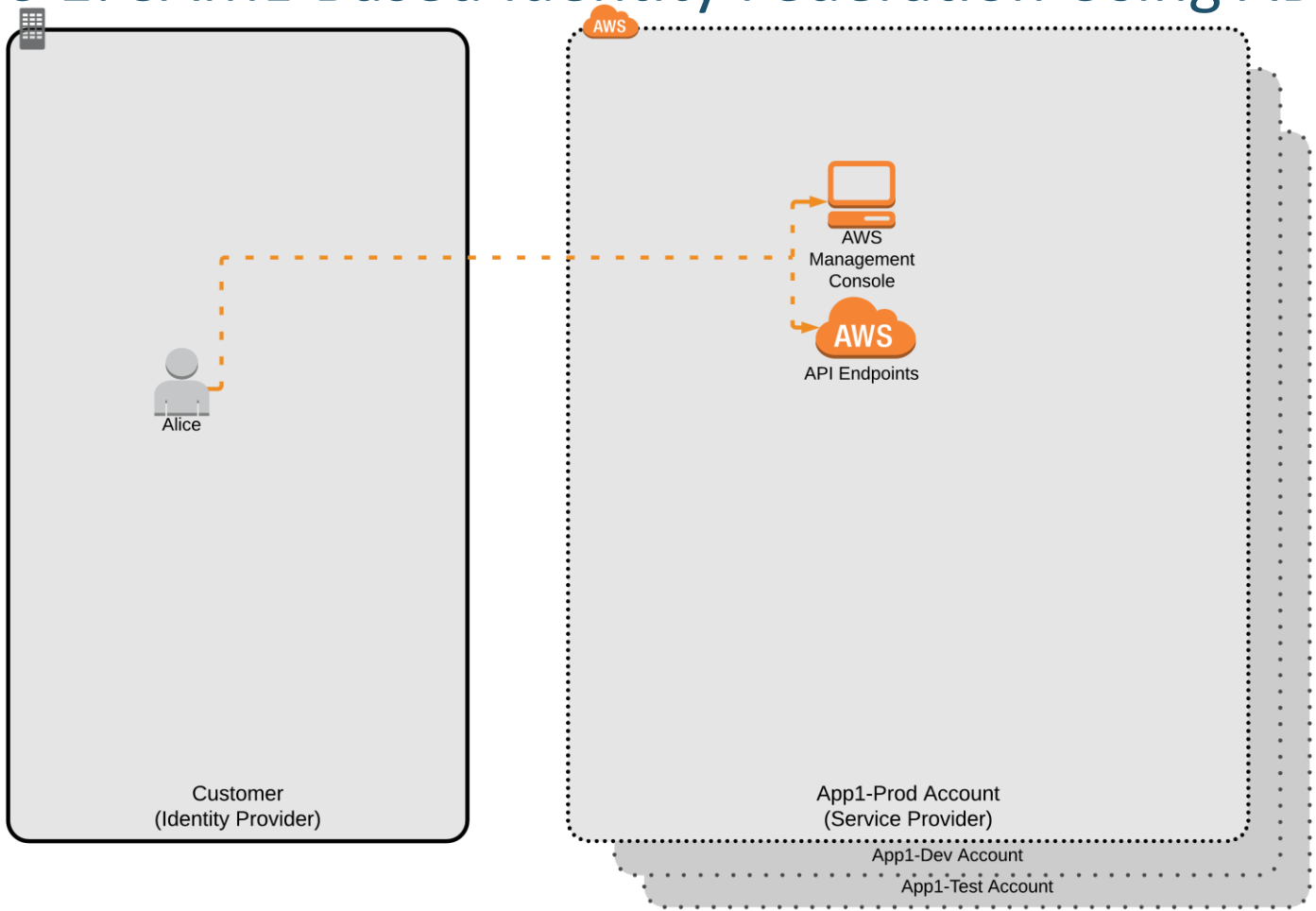
	Users	Security	Compliance
			
Before:	Unique credentials	Long-term Access Keys	One-off
After:	**Single Sign-on**	**Temporary Security Credentials**	**Aligned with Internal Controls**

Agenda:

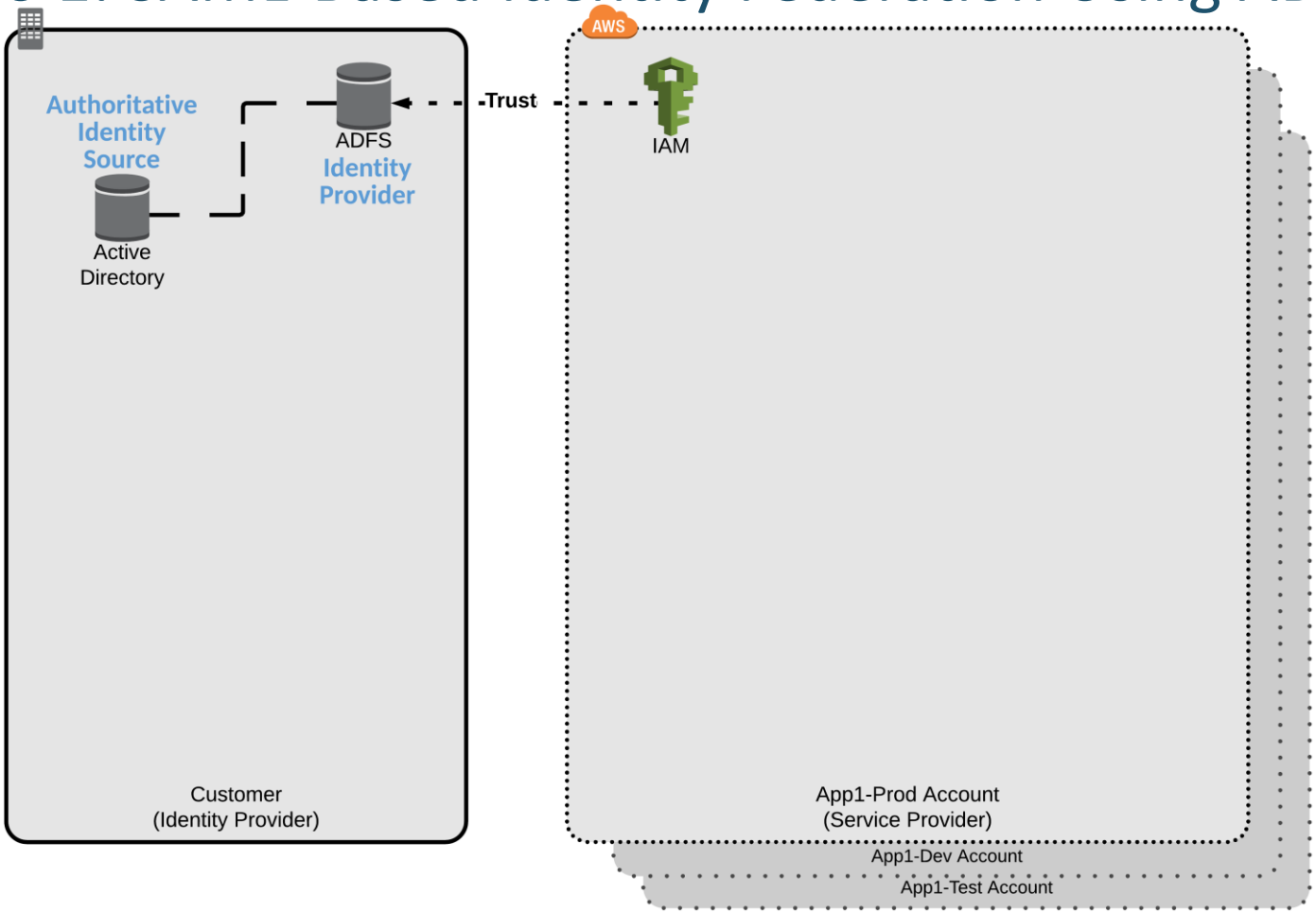
* Evolution of Identity Management
* Identity Federation Primer
* Two Demos

Demo 1 – SAML Federation with ADFS

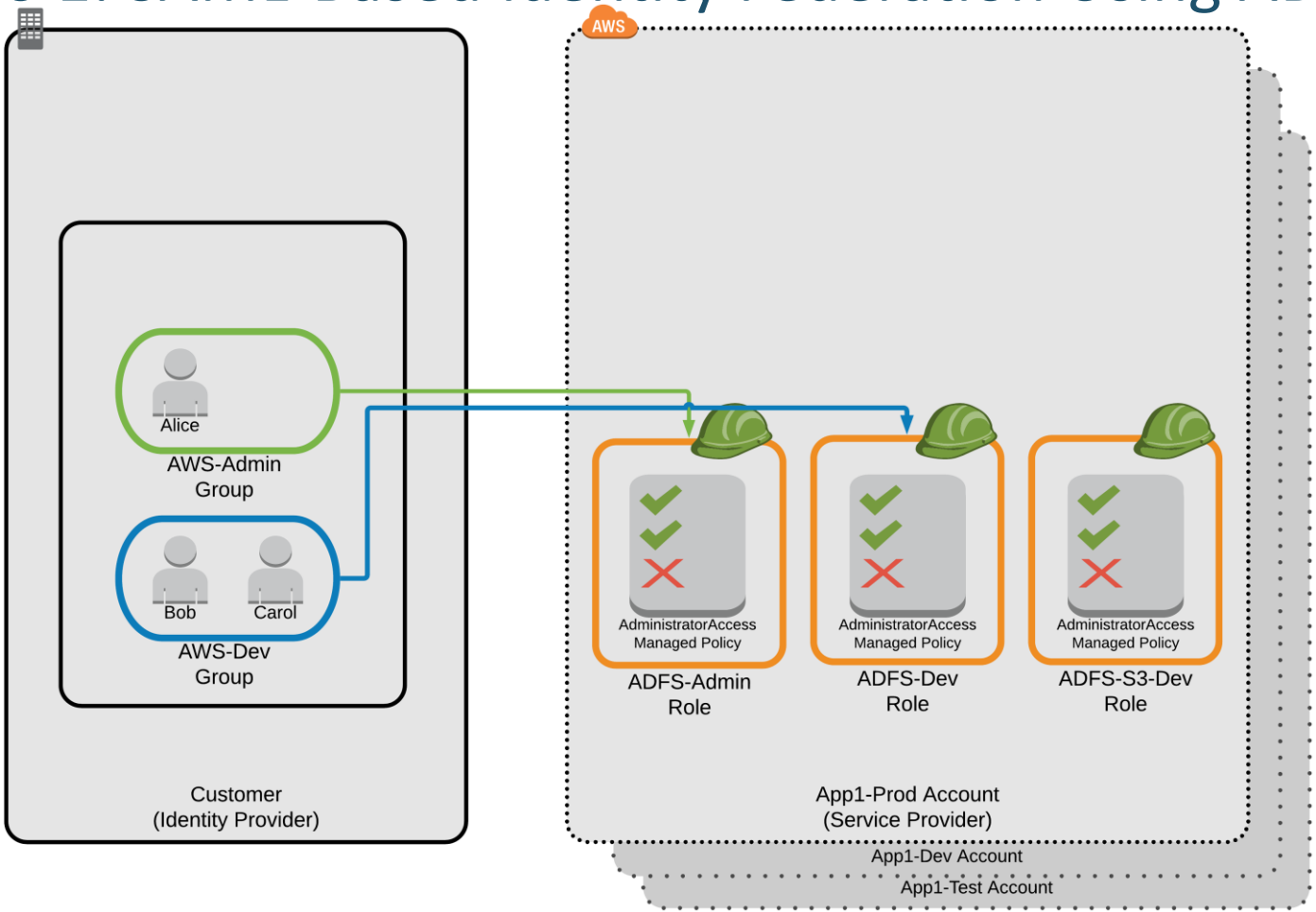
Demo 1: SAML-Based Identity Federation Using ADFS



Demo 1: SAML-Based Identity Federation Using ADFS

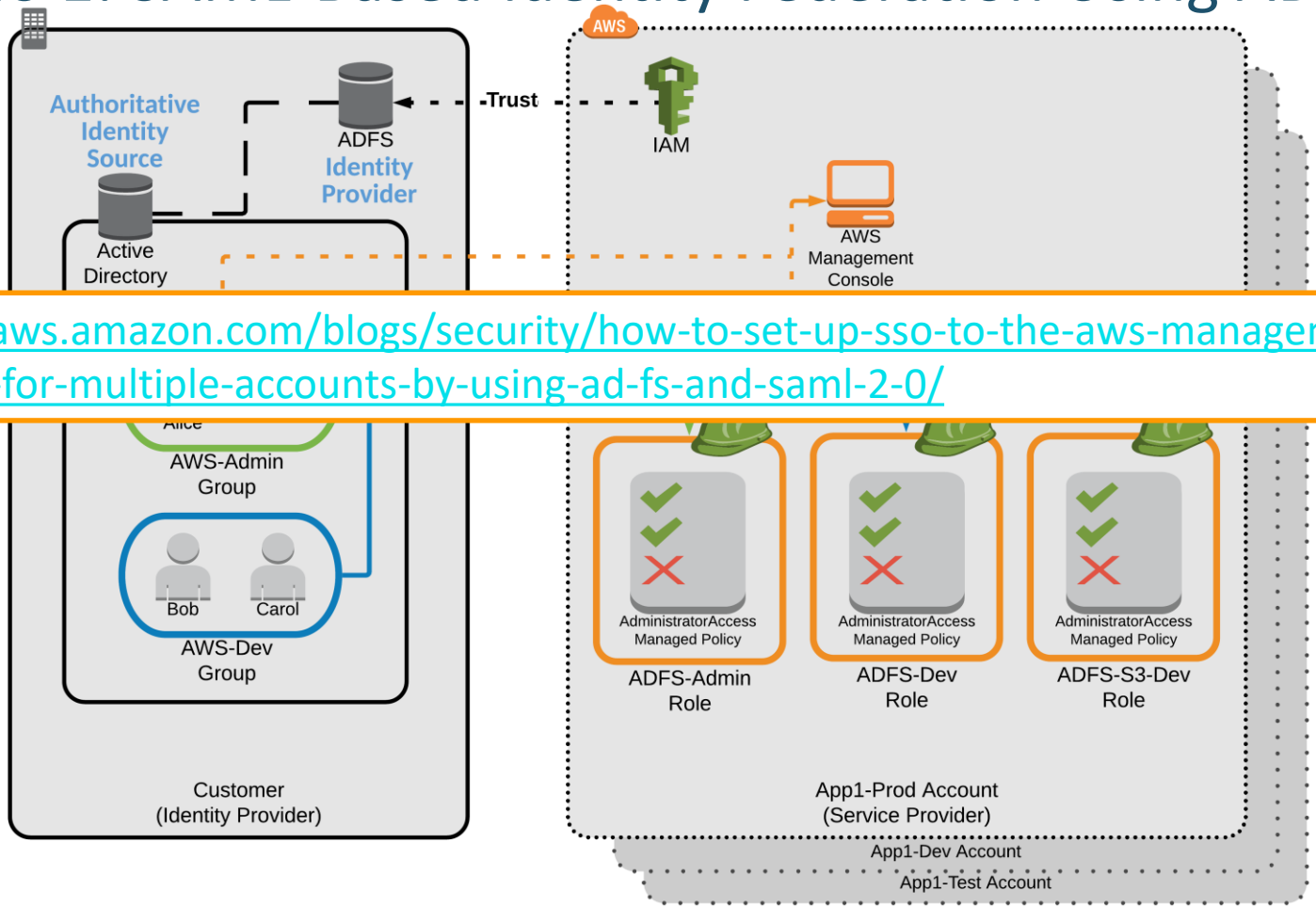


Demo 1: SAML-Based Identity Federation Using ADFS



aws

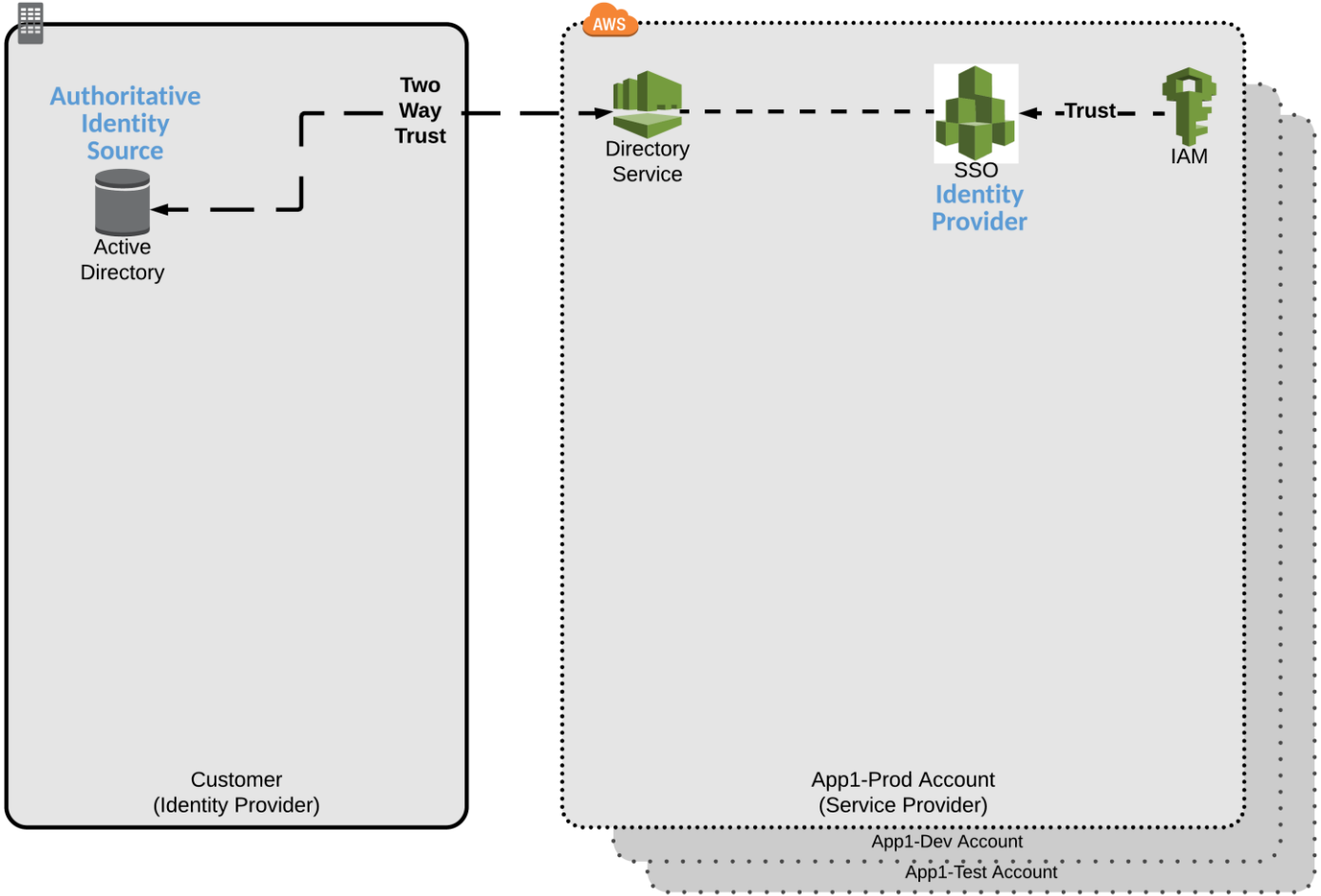
Demo 1: SAML-Based Identity Federation Using ADFS



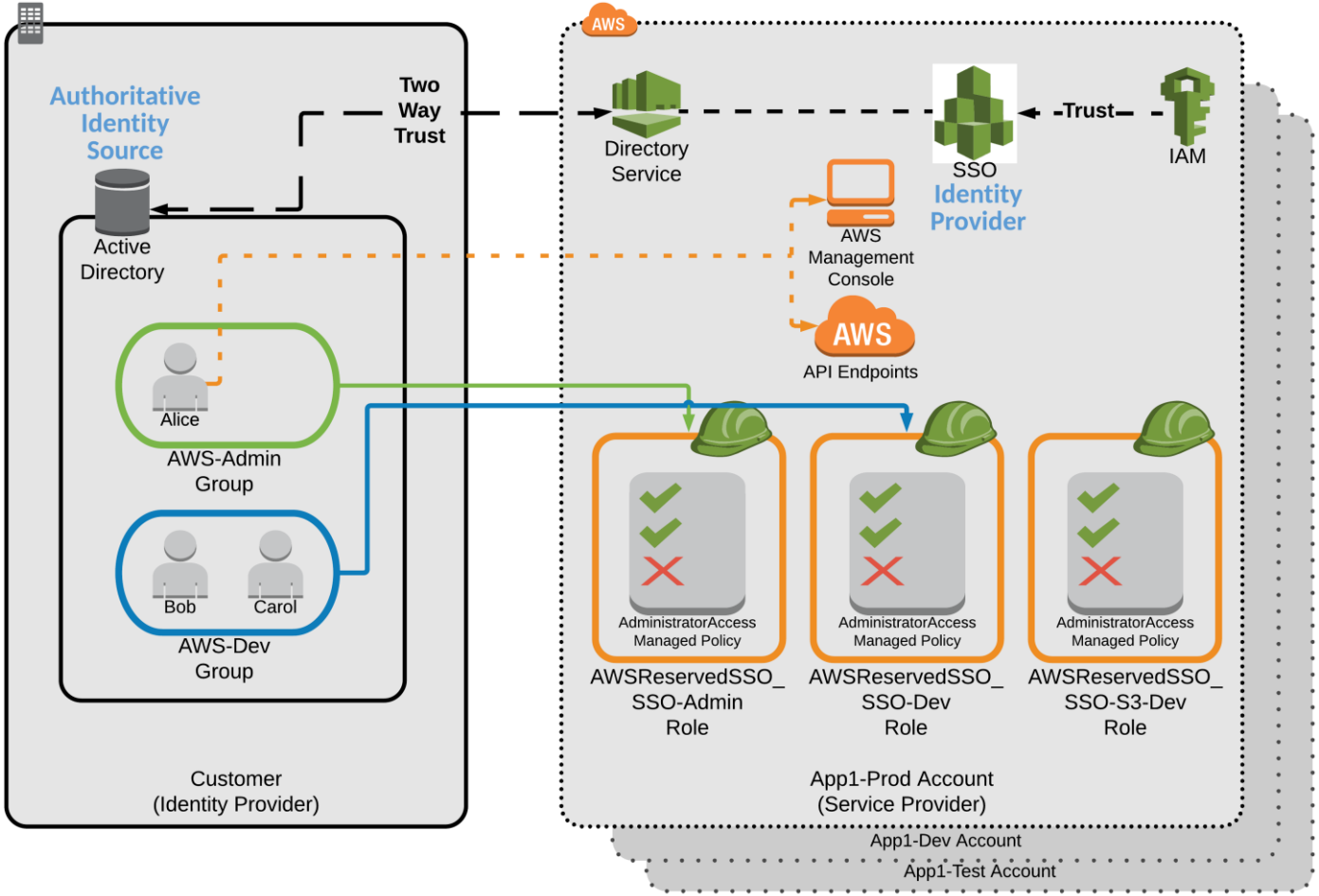
https://aws.amazon.com/blogs/security/how-to-set-up-sso-to-the-aws-management-console-for-multiple-accounts-by-using-ad-fs-and-saml-2-0/

Demo 2 – AWS SSO

Demo 2: Identity Federation Using SSO



Demo 2: Identity Federation Using SSO



Next Steps

- Lock down the Root user
- Investigate identity federation using your current identity provider, a 3rd party provider or consider AWS SSO
    - https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_saml_3rd-party.html
    - https://aws.amazon.com/single-sign-on/

aws

Resources

PowerShell scripts to automate SAML Federation Setup (AD FS 3.0 on Windows Server 2012 R2)	https://aws.amazon.com/blogs/security/how-to-set-up-sso-to-the-aws-management-console-for-multiple-accounts-by-using-ad-fs-and-saml-2-0/
Solution to resolve issues with ADFS certificate expiration	https://aws.amazon.com/blogs/security/how-to-set-up-uninterrupted-federated-user-access-to-aws-using-ad-fs/
How to install new certificates into ADFS	https://blogs.technet.microsoft.com/rmilne/2016/03/21/updating-windows-server-2012-r2-adfs-ssl-and-service-certificates/
PowerShell and SAML	https://aws.amazon.com/blogs/security/how-to-set-up-federated-api-access-to-aws-by-using-windows-powershell/
Troubleshooting SAML	http://docs.aws.amazon.com/IAM/latest/UserGuide/troubleshoot_saml.html http://docs.aws.amazon.com/IAM/latest/UserGuide/troubleshoot_saml_view-saml-response.html
SAML Information	http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_create_saml_assertions.html
SAML with Shibboleth	https://d0.awsstatic.com/whitepapers/aws-whitepaper-single-sign-on-integrating-aws-open-ldap-and-shibboleth.pdf
API/CLI Access via SAML (ADFS 2)	https://aws.amazon.com/blogs/security/how-to-implement-federated-api-and-cli-access-using-saml-2-0-and-ad-fs/
API/CLI Access via SAML (ADFS 3)	https://aws.amazon.com/blogs/security/how-to-implement-a-general-solution-for-federated-apicli-access-using-saml-2-0/
AWS CLI tool for getting temp creds via Identity Federation	https://github.com/awslabs/awsprocesscreds
Okta SAML Federation for CLI/API with MFA	https://github.com/oktadeveloper/okta-aws-cli-assume-role
Identity federation and AppStream 2.0	https://aws.amazon.com/blogs/compute/enabling-identity-federation-with-ad-fs-3-0-and-amazon-appstream-2-0/
3rd Party Identity Provider Information	http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_saml_3rd-party.html

aws

Thank you!