AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

WIN301

Security best practices for running Microsoft tech on AWS

Bill Jacobi
Principal Solutions Architect
AWS

Shawn Asfeld
Senior Solutions Architect
AWS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Security on AWS

Building and deploying security-hardened Windows

Securing AWS Directory Service for Microsoft Active Directory

Administering Amazon EC2 Windows instances securely

Deploying applications to meet FedRAMP High and other regulated industry compliance programs

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security on AWS

Building and deploying security-hardened Windows

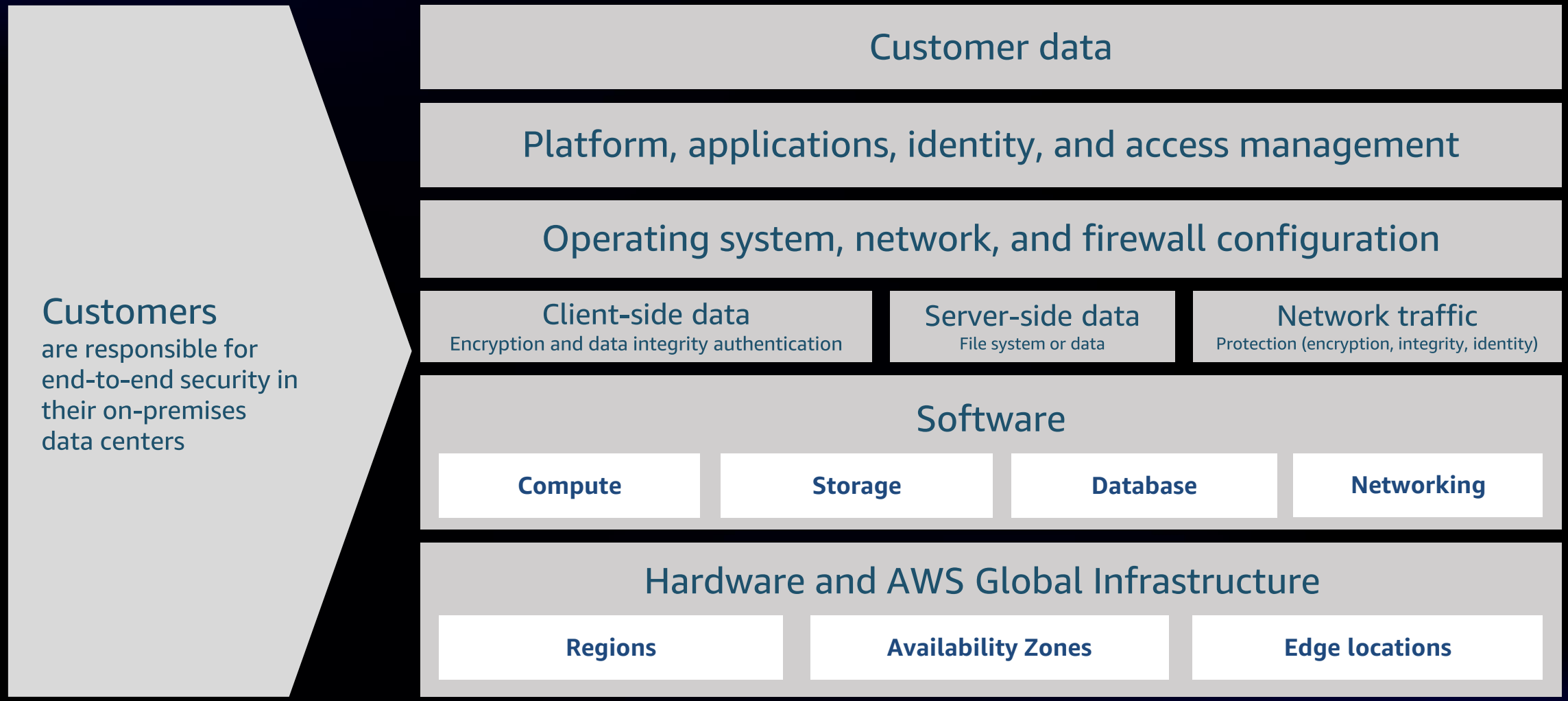
Securing AWS Directory Service for Microsoft Active Directory

Administering Amazon EC2 Windows instances securely

Deploying applications to meet FedRAMP High and other regulated industry compliance programs

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Traditional on-premises security model



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

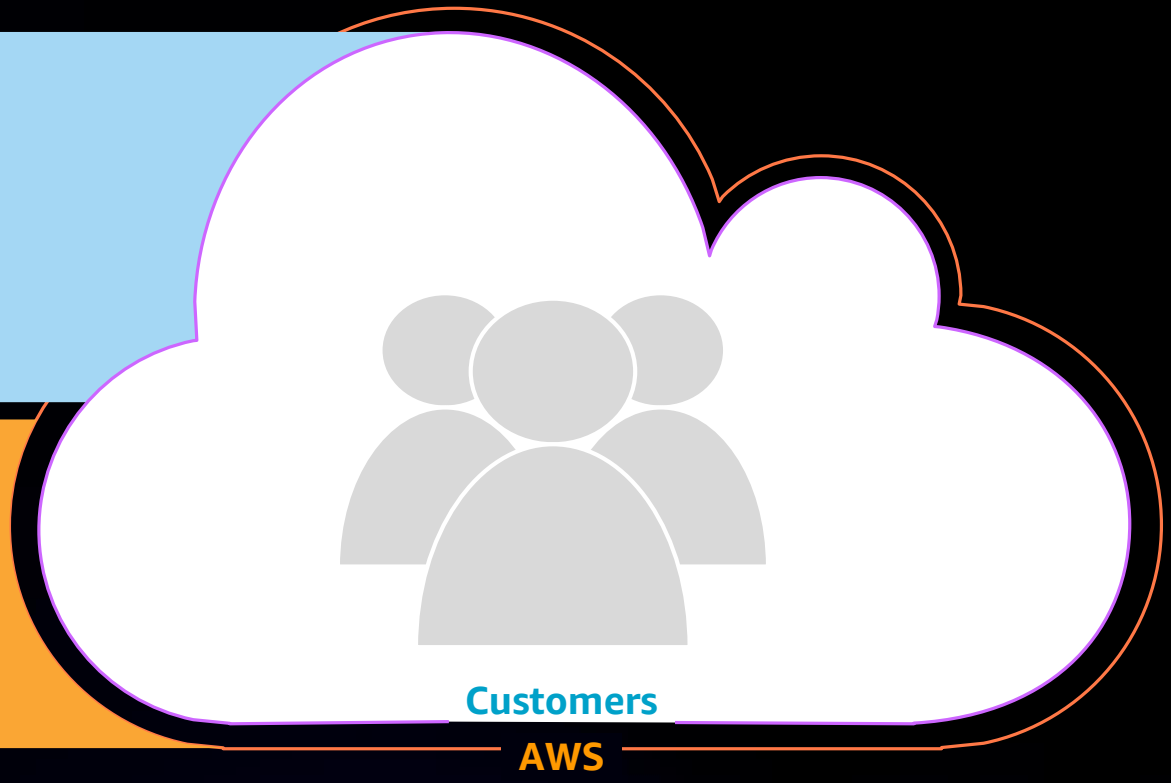
Cloud security shared responsibility model

Customer responsibility is determined by the AWS Cloud services a customer selects, e.g., enabling encryption in Amazon EBS

Security IN the Cloud

AWS is responsible for protecting the infrastructure that runs all the services offered in the AWS Cloud, e.g., offering an encryption service

Security OF the Cloud



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS security, identity, and compliance solutions



Identity and access management

AWS Identity and Access Management (IAM)

AWS Single Sign-On (AWS SSO)

AWS Organizations

AWS Directory Service

Amazon Cognito

AWS Resource Access Manager (AWS RAM)



Detective controls

AWS Security Hub

Amazon GuardDuty

Amazon Inspector

Amazon CloudWatch

AWS Config

AWS CloudTrail

VPC Flow Logs

AWS IoT Device Defender



Infrastructure protection

AWS Firewall Manager

AWS Network Firewall

AWS Shield

AWS WAF – web application firewall

Amazon Virtual Private Cloud (Amazon VPC)

AWS PrivateLink

AWS Systems Manager



Data protection

Amazon Macie

AWS Key Management Service (AWS KMS)

AWS CloudHSM

AWS Certificate Manager (ACM)

AWS Secrets Manager

AWS VPN

Server-side encryption



Incident response

Amazon Detective

Amazon EventBridge

AWS Backup

AWS Security Hub

CloudEndure Disaster Recovery



Compliance

AWS Artifact

AWS Audit Manager

Discussed in this presentation

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security on AWS

Building and deploying security-hardened Windows

Securing AWS Directory Service for Microsoft Active Directory

Administering Amazon EC2 Windows instances securely

Deploying applications to meet FedRAMP High and other regulated industry compliance programs

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

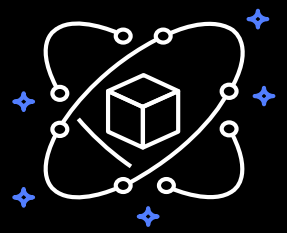
How do customers build golden images today?



Manually build each golden image



Build and maintain custom automation



Build automation with open-source frameworks

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Customers asked for a one-stop shop to build golden images



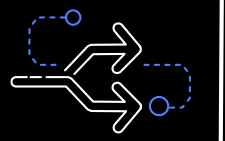
Quickly and easily build **automation** to create golden images without writing code – and a console to simplify selection of choices



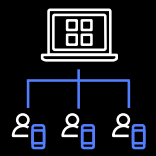
Easily **test** images with AWS-provided and custom tests before deploying to production



Secure images with AWS-provided and custom settings to meet internal and industry standards



Distribute and share images easily across accounts and AWS Regions with centralized enforcement



Build images for use on **AWS and on premises**

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Build and maintain custom automation

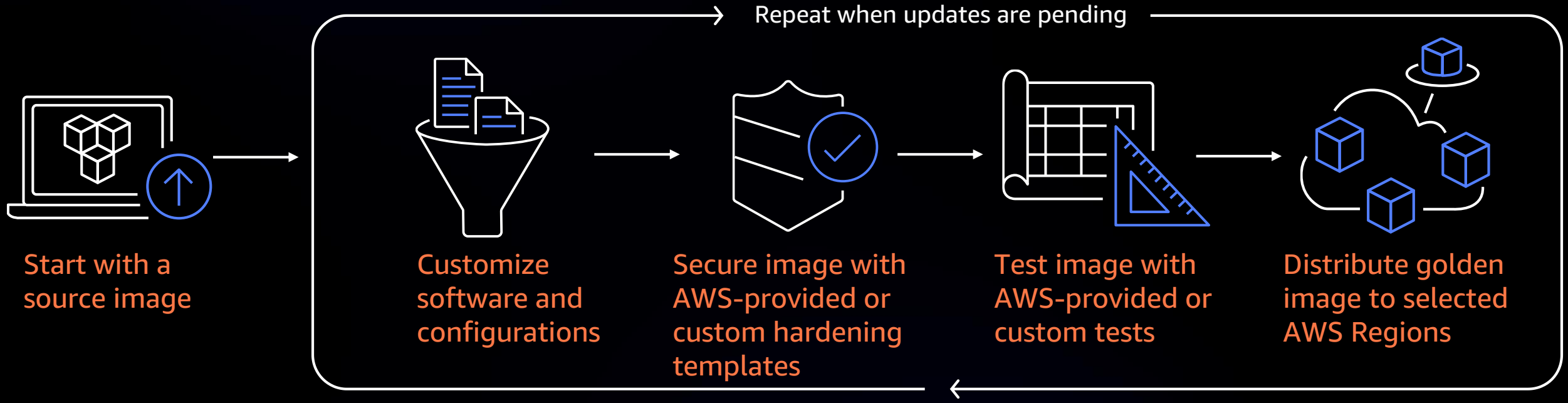


EC2 Image Builder

Build and maintain secure images

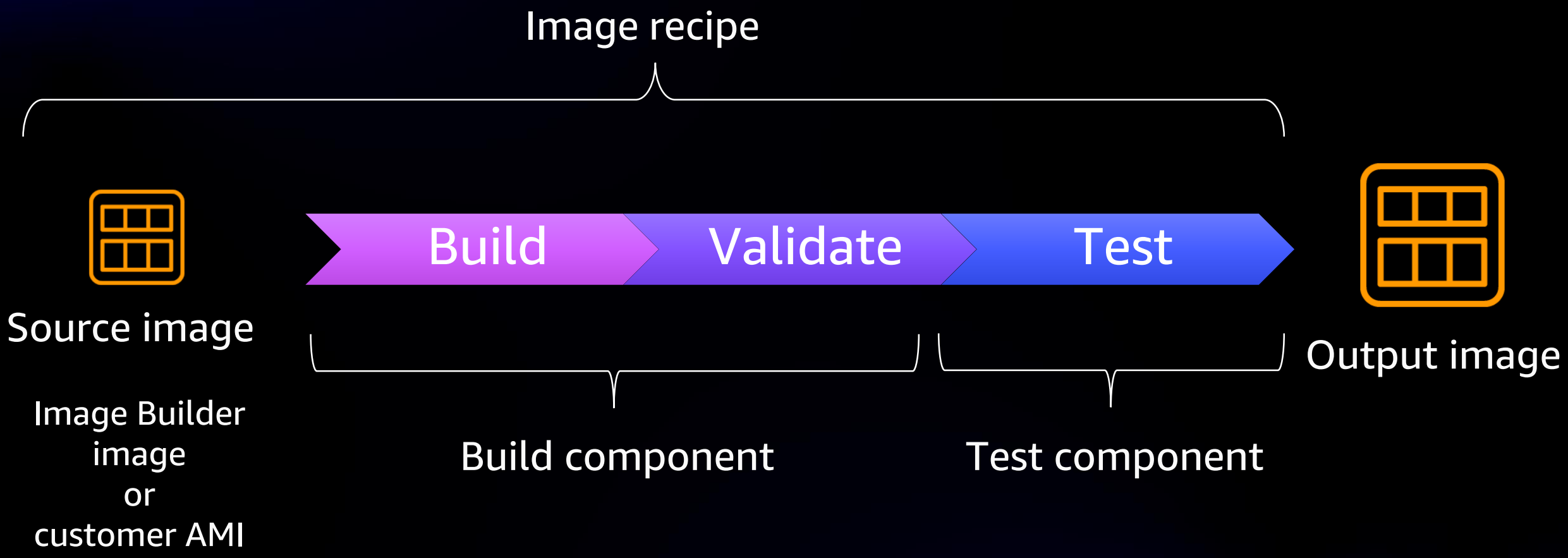
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Image Builder – How it works



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

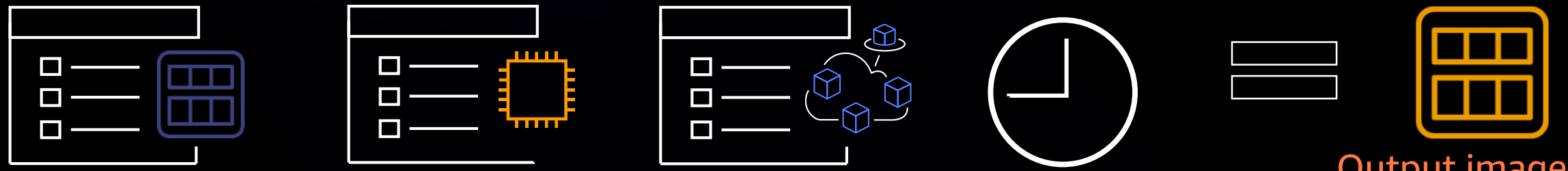
Image Builder image recipe



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Image Builder image pipeline

Pipeline



Output image

Image recipe

Source image, components

Infrastructure configuration

Instance type, subnet, SGs, SNS topic, logging, etc.

Distribution configuration

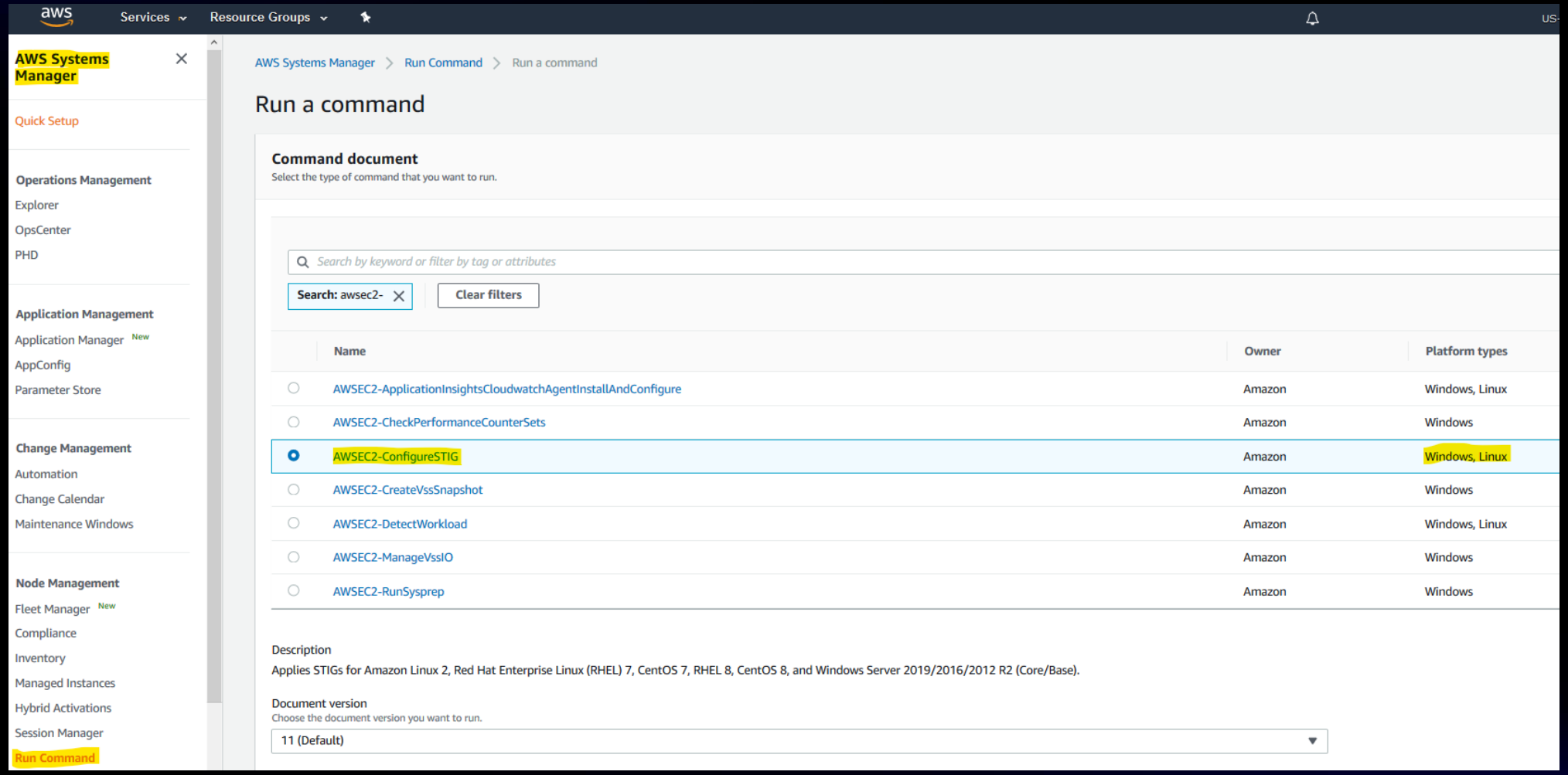
Regions, accounts

Schedule

Manual, schedule

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

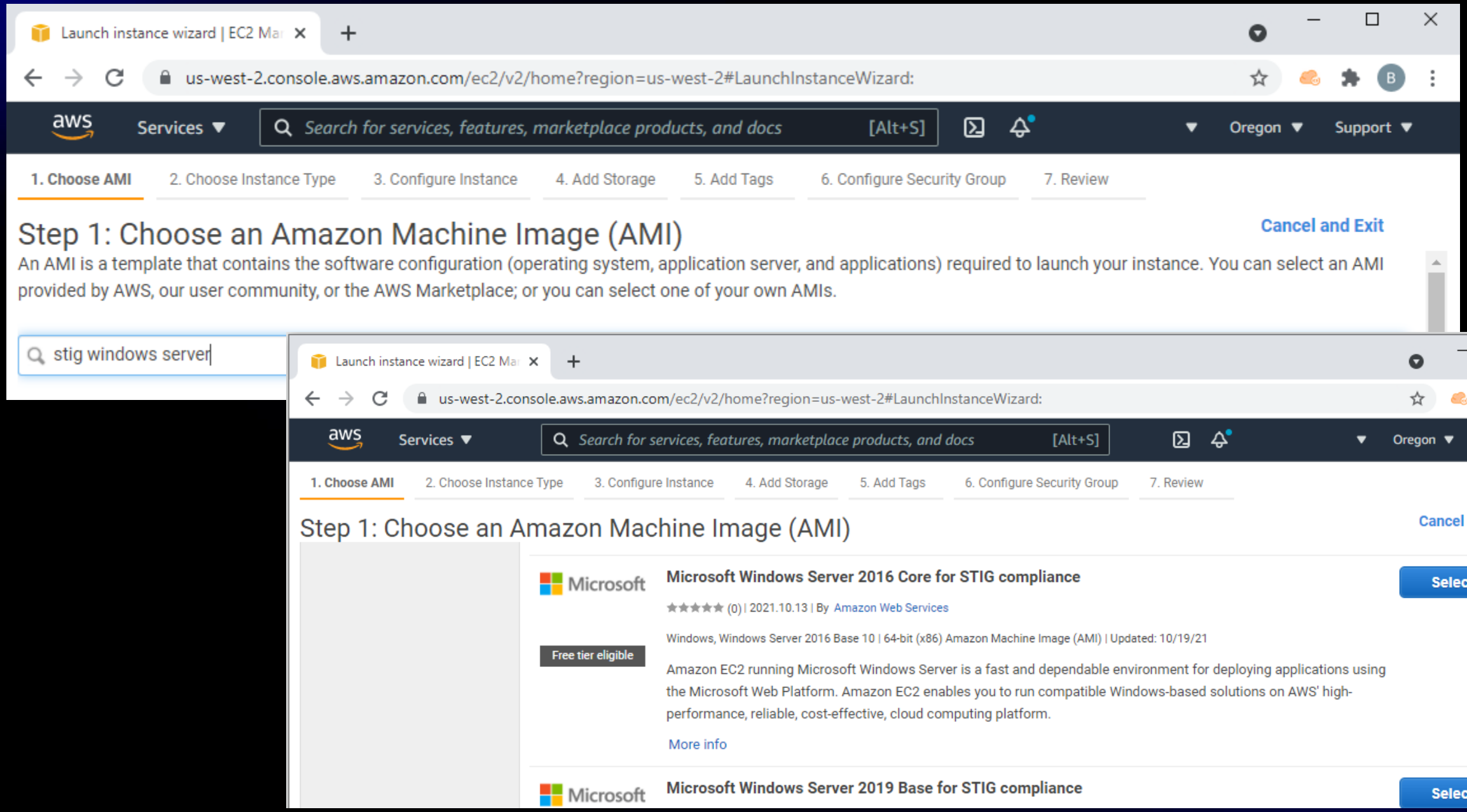
Or: AWS SSM AWSEC2-ConfigureSTIG



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Or Just pick up a hardened image from the AWS Marketplace!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security on AWS

Building and deploying security-hardened Windows

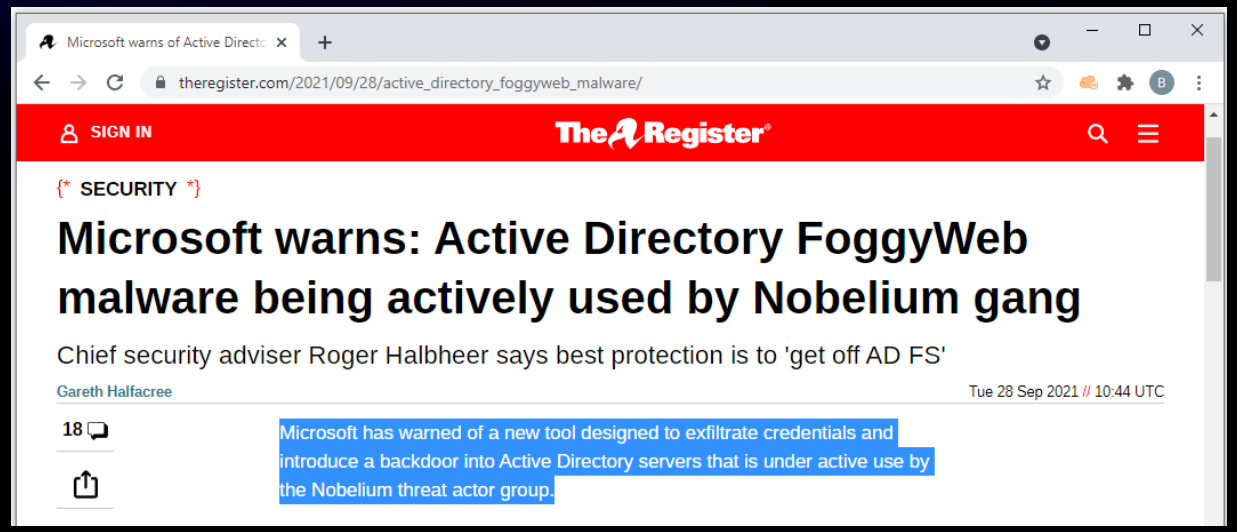
Securing AWS Directory Service for Microsoft Active Directory

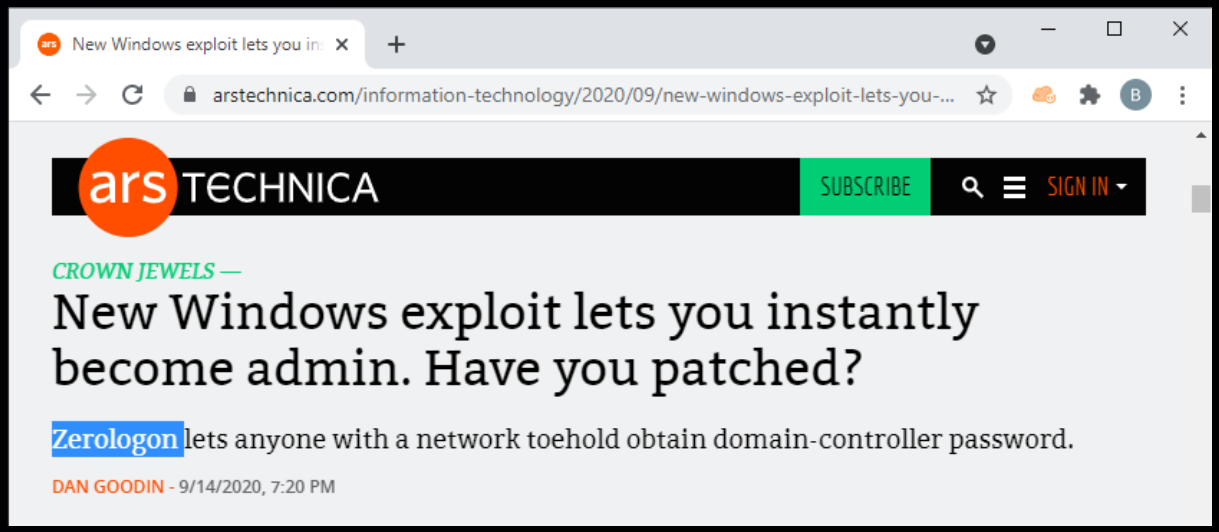
Administering Amazon EC2 Windows instances securely

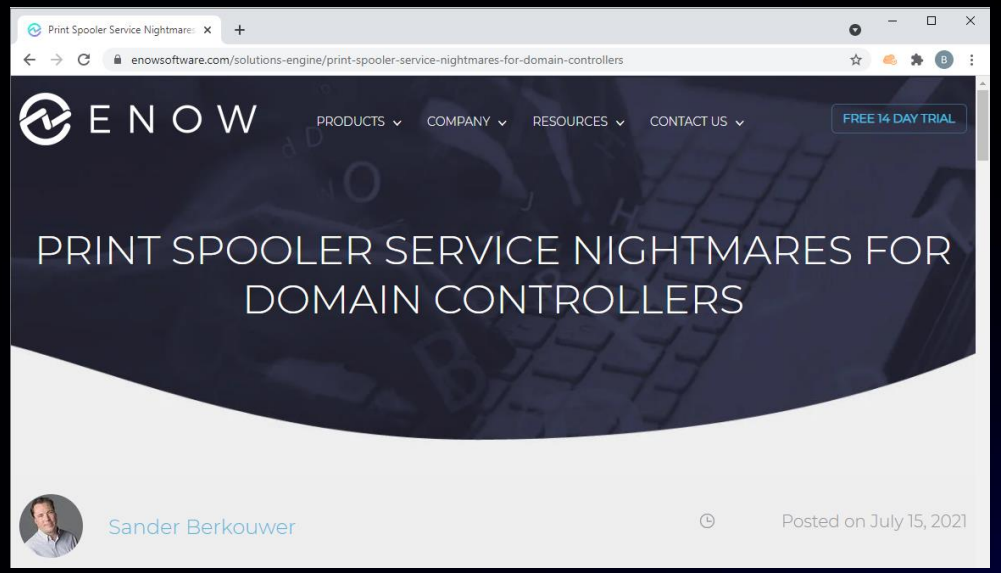
Deploying applications to meet FedRAMP High and other regulated industry compliance programs

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Attacks on Active Directory



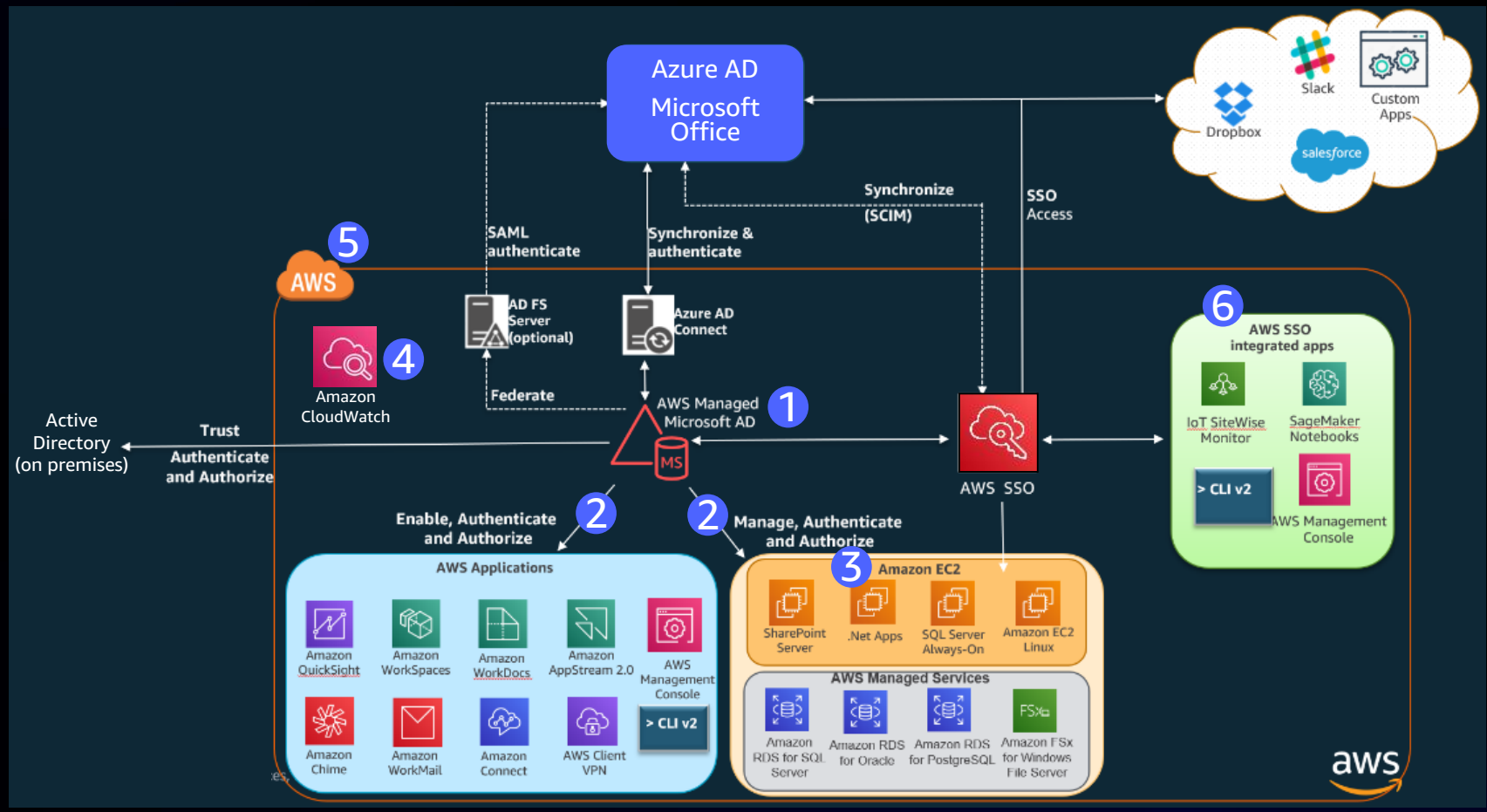




© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is AWS Managed Microsoft AD?

1. Managed directory service based on Active Directory on Microsoft Windows Server
2. Multi-AZ, multi-Region
3. Automated patching
4. Automated logging and monitoring
5. Compliance: FedRAMP, PCI, HIPAA, SOC
6. Integrates with AWS SSO, AWS applications, and AWS Managed Services

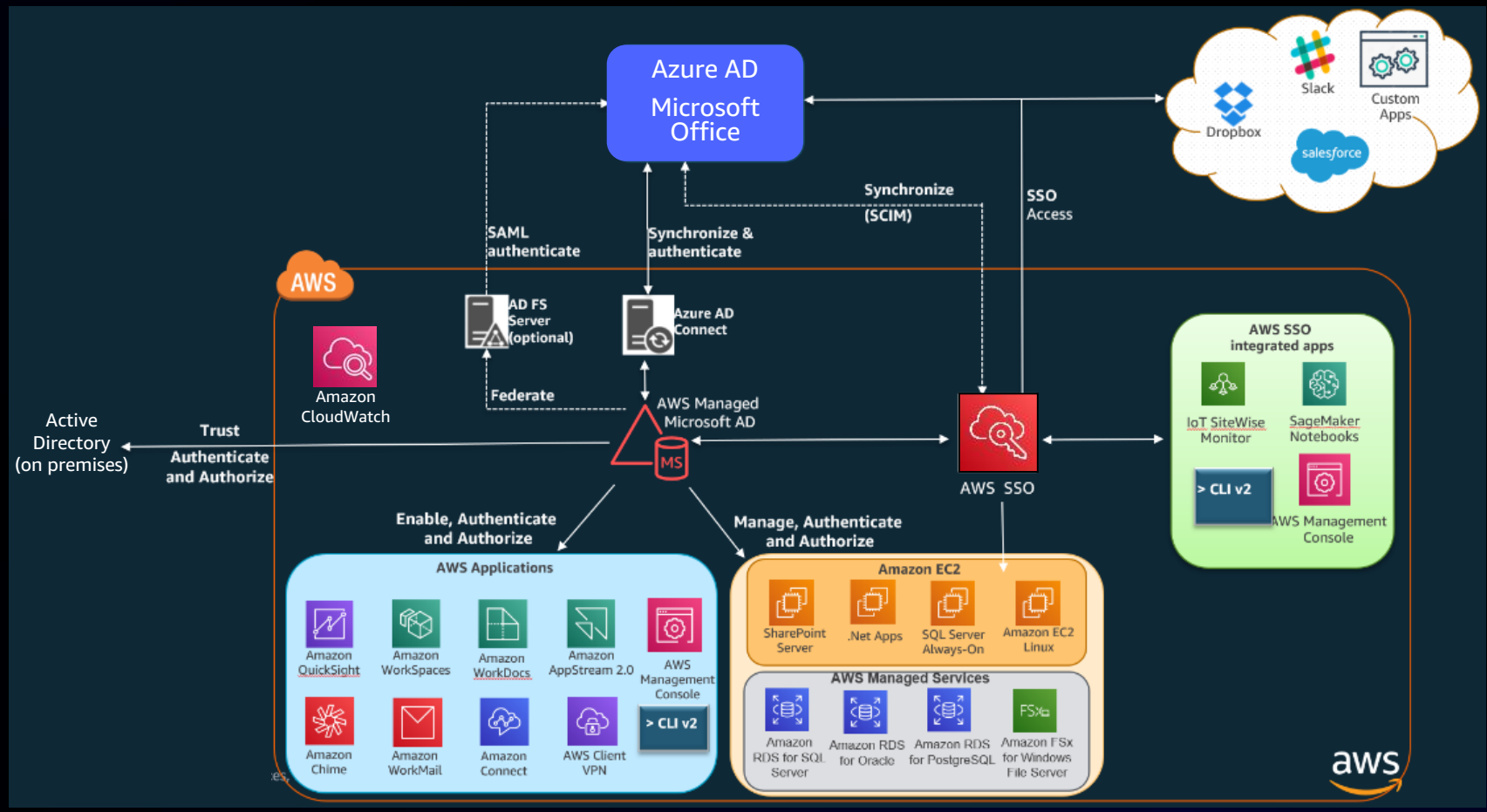


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Managed Microsoft AD

CUSTOMER RESPONSIBILITY

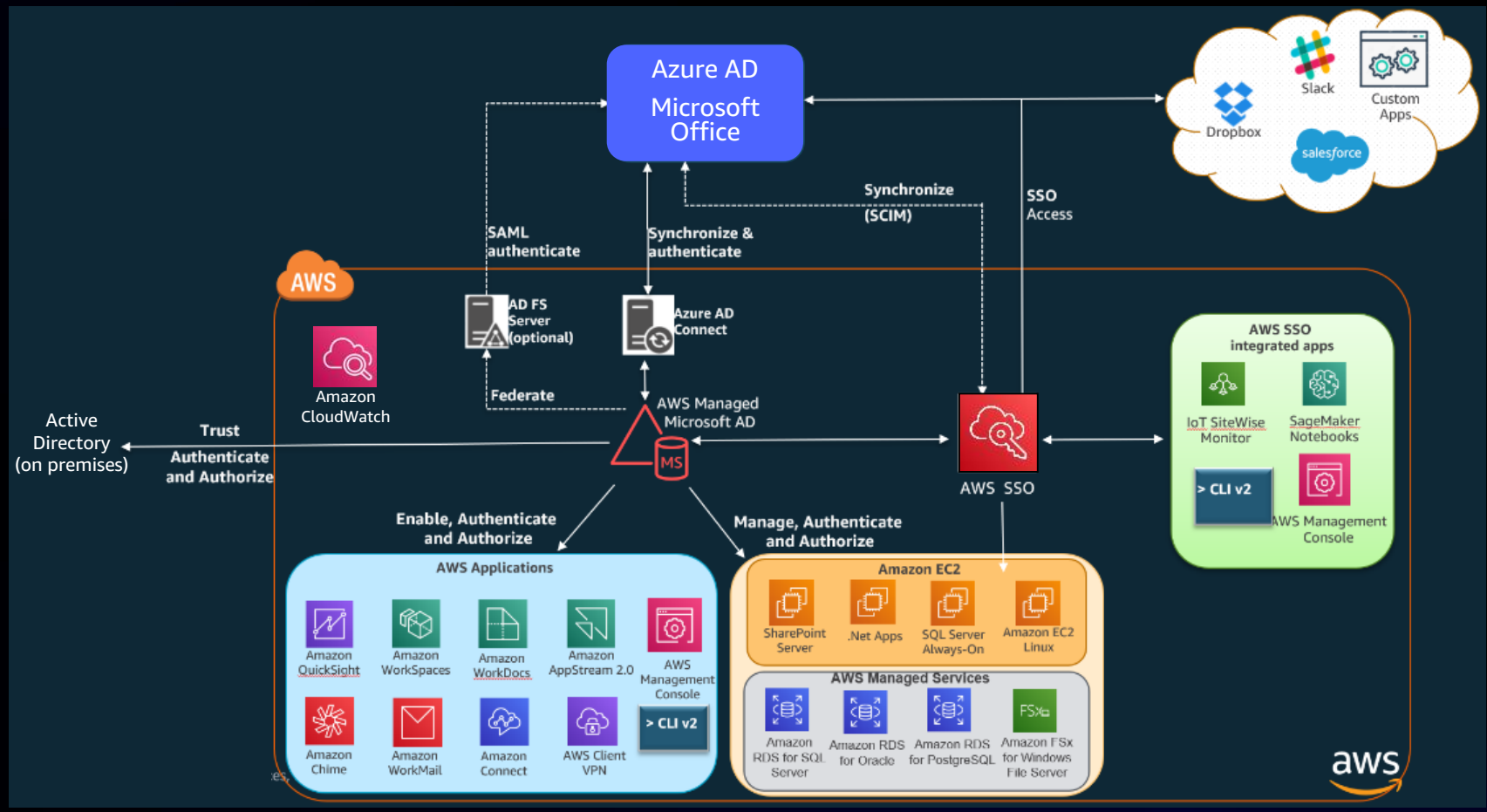
- Administer users, groups, GPO password policies
- Configure trust relationships
- Configure CA
- Configure Managed AD with AWS Managed Services, AWS applications, AWS SSO
- Enable LDAPS, MFA, PrivateLink, log forwarding



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Enable LDAPS support on server and client

- By default, communications over LDAP are not encrypted
- With LDAPS, you can encrypt LDAP calls
- Enable LDAPS on the server
- Enable LDAPS on the client



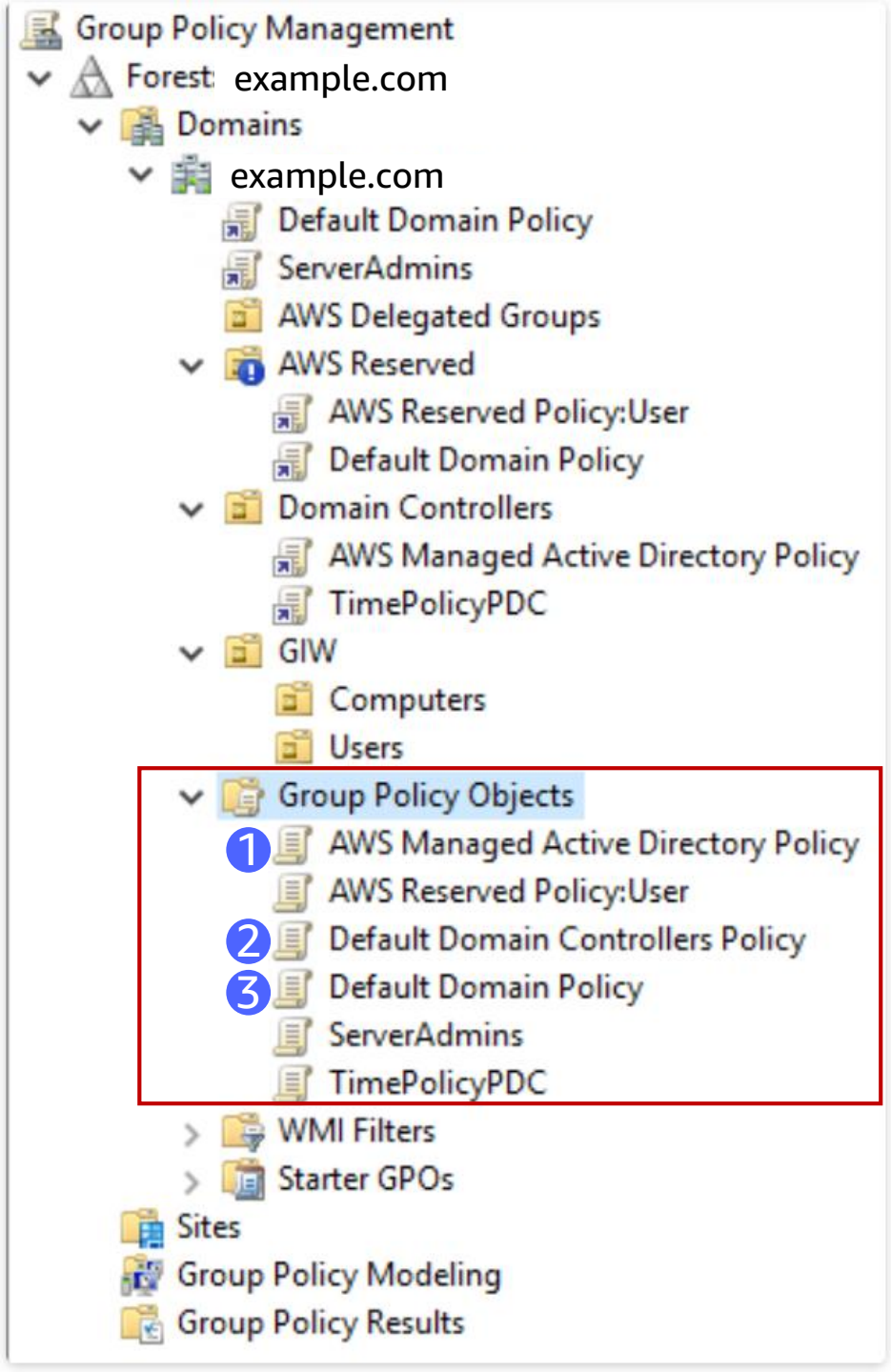
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Built-in GPOs

THERE ARE 1,238 GPO CONFIGURABLE SETTINGS

- AWS and default GPOs are provided with Managed AD

1. AWS Managed Active Directory Policy
   - Settings to enable FedRAMP, HIPAA, and PCI compliance
   - Fine-grained password policies such as minimum history reuse, minimum length, minimum age, maximum age, complexity, etc.
   - Enable lockout policies, such as maximum # failed logon attempts, lockout duration, etc.
   - AWS-delegated server administrators are added to BUILTIN\Administrators
2. Default Domain Controllers Policy (DDCP) GPO
   - Built-in defaults
3. Default Domain Policy (DDP) GPO
   - Force logoff when logon hours expire

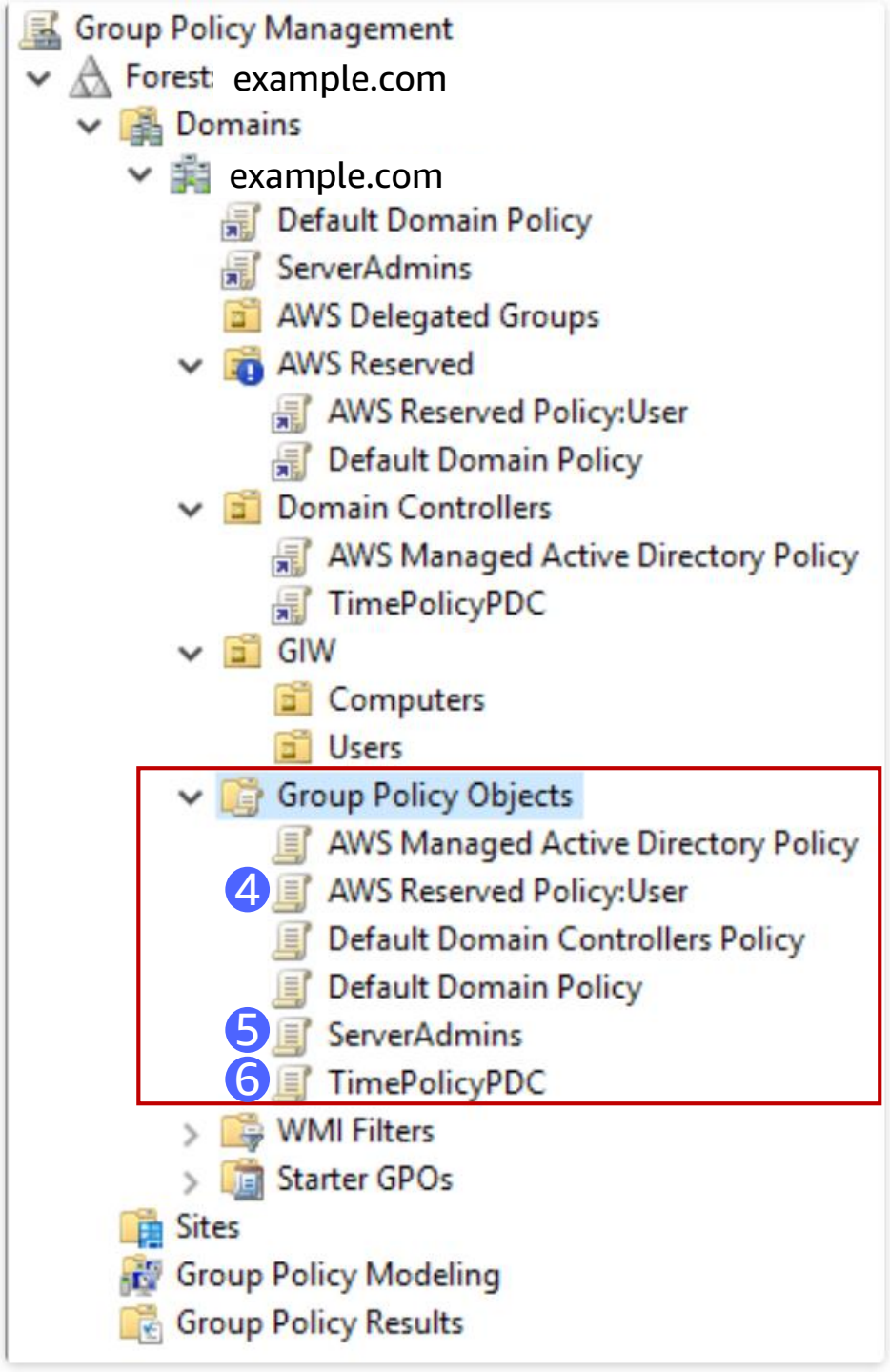


Built-in GPOs

THERE ARE 1,238 GPO CONFIGURABLE SETTINGS

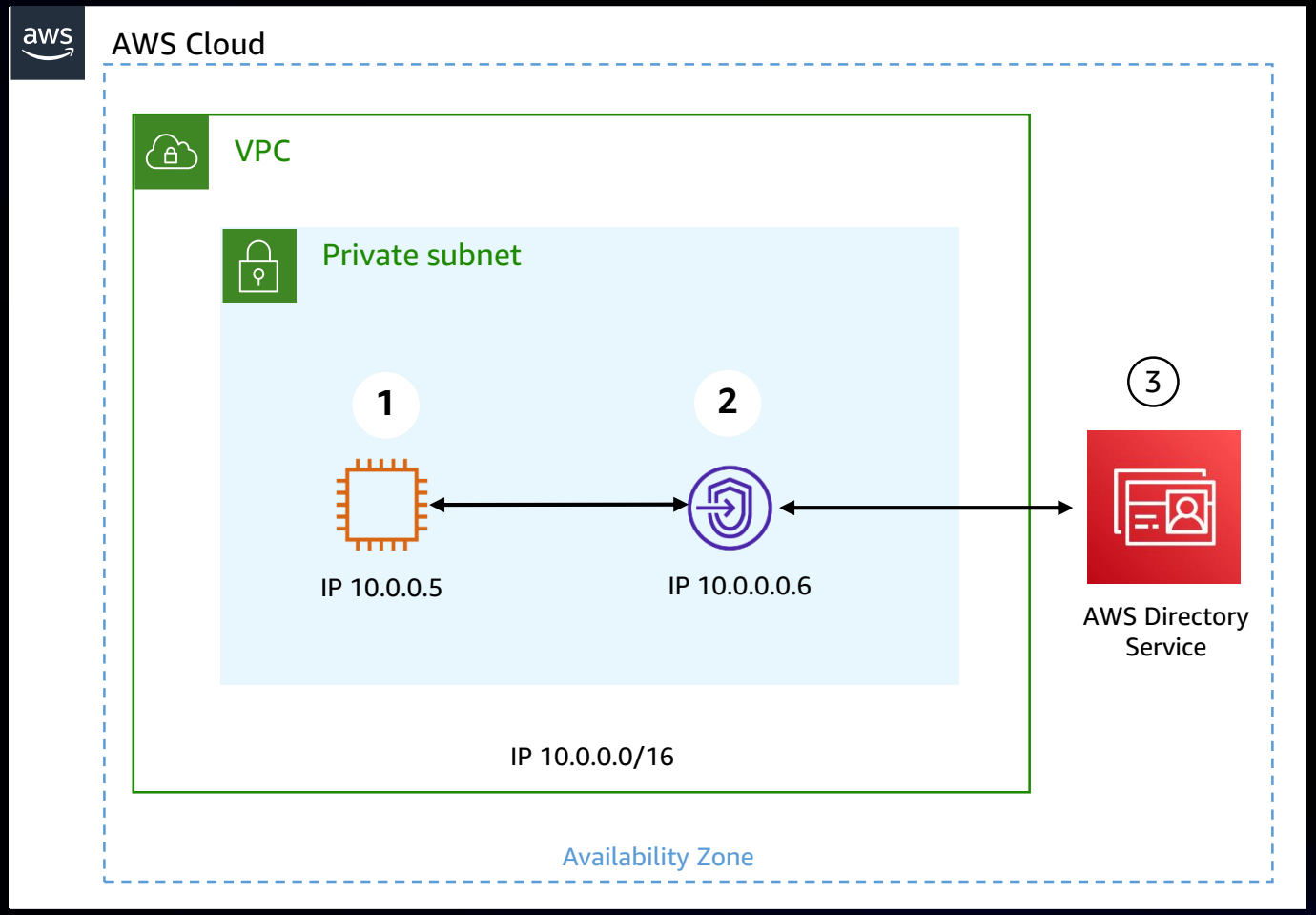
- AWS and default GPOs are provided with Managed AD

4. AWS Reserved Policy: user
   - Turn on screensavers, require screensaver passwords, prevent sharing files in profiles
5. ServerAdmins GPO
   - Add the AWS-delegated server administrators to BUILTIN\Administrators
6. TimePolicyPDC
   - Use NTP servers or DCs for system time



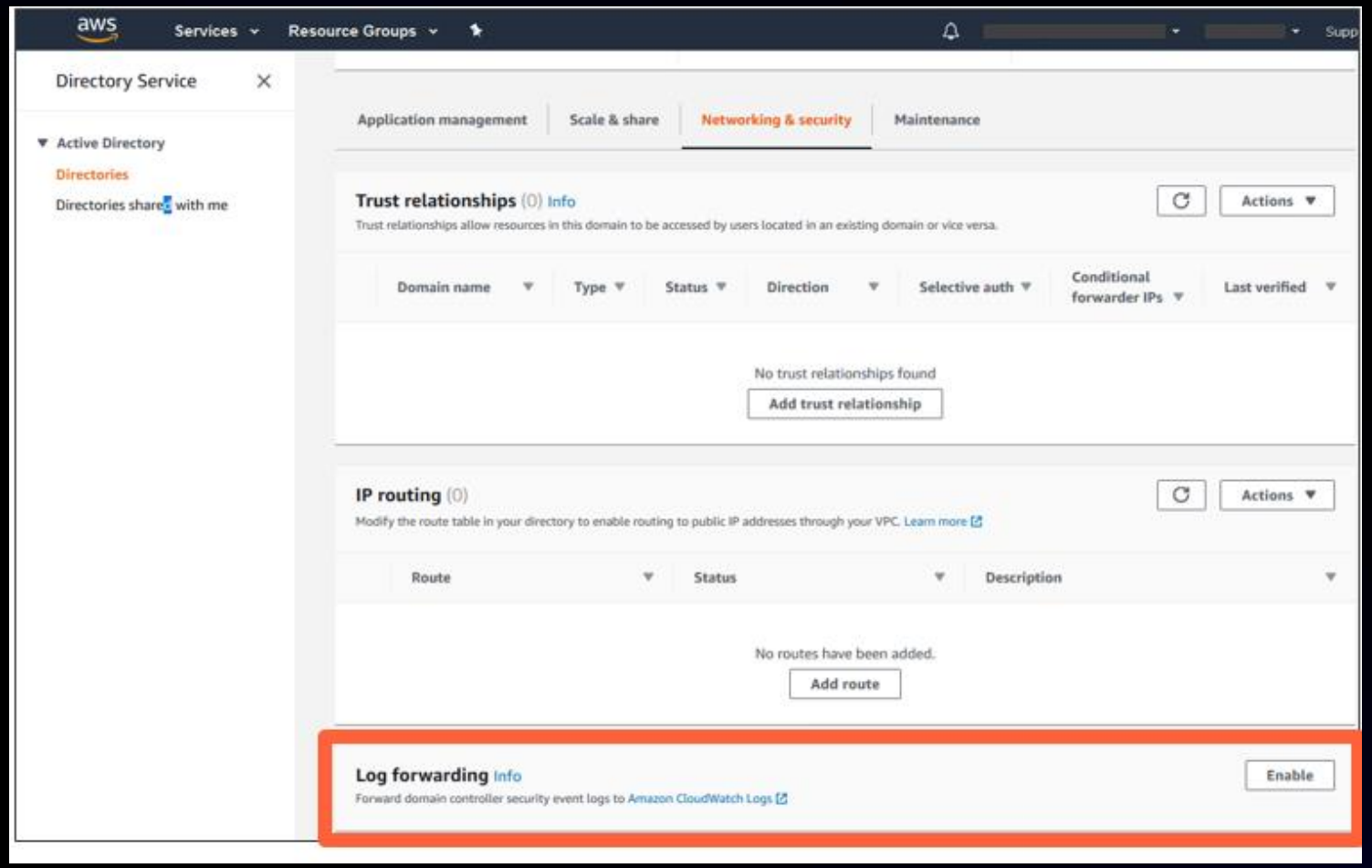
AWS PrivateLink for AWS Managed Microsoft AD

- PrivateLink establishes private connectivity between your VPC and AWS Managed Microsoft AD
- Access AWS Managed Microsoft AD over PrivateLink
- Share AWS Managed Microsoft AD over PrivateLink



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security event logging to Amazon CloudWatch and third-party SIEM systems



Security events

- CloudWatch logs
- Splunk
- Sumo Logic
- Others

Anomaly detection, pattern recognition, identify security correlations

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security on AWS

Building and deploying security-hardened Windows

Securing AWS Directory Service for Microsoft Active Directory

Administering Amazon EC2 Windows instances securely

Deploying applications to meet FedRAMP High and other regulated industry compliance programs

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Attacks on Remote Desktop Protocol

SIGN IN

The Register

{* SECURITY *}

Attacks against Remote Desktop Protocol endpoints have exploded this year, warns ESET's latest Threat Report

Security firm points to a 'stalkerware' epidemic, new Nobelium group activity

Gareth Halfacree

8

Security specialist ESET's latest Threat Report warns of a massive increase in attacks on Remote Desktop Protocol (RDP) endpoints – and new activity from the Nobelium gang against European government organisations.

ESET's figures show attacks on RDP servers having gone up 103.9 per cent since its T1 report in June - it publishes three a year - representing a total of 55 billion detected brute-force attacks, thanks in no small part to a campaign focused on Spanish targets.

DARKTRACE

Technology Products Blog Resources Company

Darktrace Blog

Botnet malware: Remote Desktop Protocol (RDP) attack

Max Heinemeyer, Director of Threat Hunting | Monday March 15, 2021



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Systems Manager

SECURE END-TO-END MANAGEMENT SOLUTION FOR HYBRID CLOUD ENVIRONMENTS

Operations management

- Explorer
- OpsCenter
- Incident Manager

Application management

- Application Manager
- AppConfig
- Parameter Store

Change management

- Change Manager
- Automation
- Maintenance Window
- Change Calendar

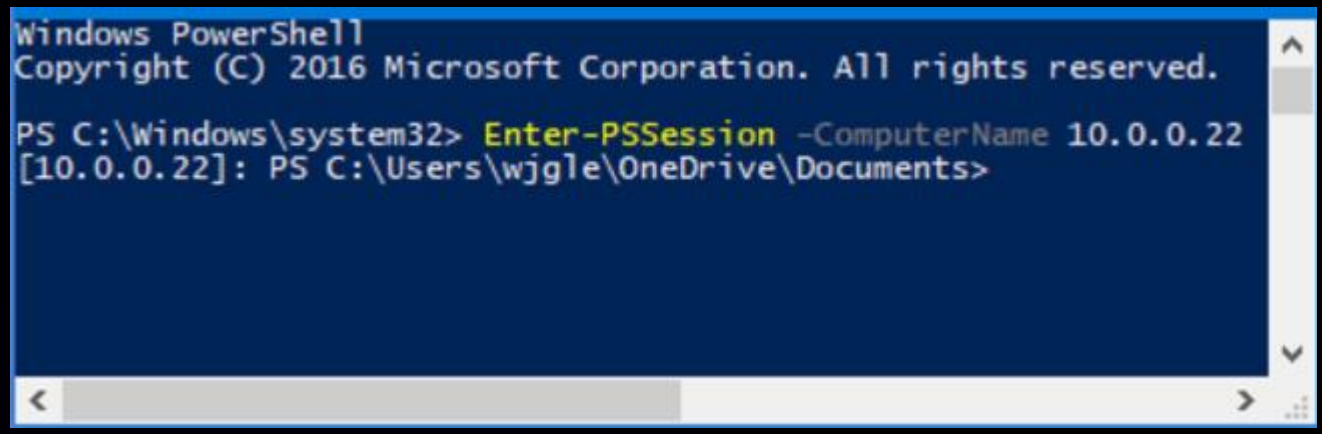
Node management

- Fleet Manager
- Inventory
- Run Command
- Patch Manager
- Distributor
- State Manager
- Session Manager

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Session Manager: Provides secure and auditable privileged access to your compute nodes

- Instance remoting solution using VPC endpoints and private IPs
- Eliminates the need for bastion hosts and inbound firewall exceptions
- Central access controls via IAM
- Enables detailed activity and session logging to CloudWatch, Amazon S3, and CloudTrail



aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security on AWS

Building and deploying security-hardened Windows

Securing AWS Directory Service for Microsoft Active Directory

Administering Amazon EC2 Windows instances securely

Deploying applications to meet FedRAMP High and other regulated industry compliance programs

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS GovCloud (US) Regions

AWS GovCloud (US) is isolated AWS infrastructure and services for customers with strict regulatory and compliance requirements and sensitive data



AWS GovCloud (US)

2 Regions

Aug 2011 – AWS GovCloud (US-West)
Nov 2018 – AWS GovCloud (US-East)

Isolated, secure, and compliant services

Built for **sensitive and regulated data** including Controlled Unclassified Information (CUI)

Mission- and business-critical workload delivery

Tools and resources to **accelerate time to compliance**

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS GovCloud (US) customer requirements



Account holder must be a **US person: a US citizen or Green Card holder**



US entity incorporated to do business in the United States and **based on US soil**



The customer **can handle export controlled data**

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Inherit security and compliance controls



International Traffic in Arms Regulation (ITAR)



FedRAMP Moderate and High



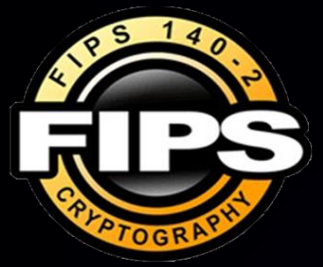
DOD Cloud Security Req's Guide (SRG) IL 4 and 5



Criminal Justice Information Service Security Policy (CJIS)



IRS – 1075 (Section 6103 (p))



Federal Information Processing Standard Pub (FIPS) 140-2



SP 800-53 (rev 4) SP 800-171

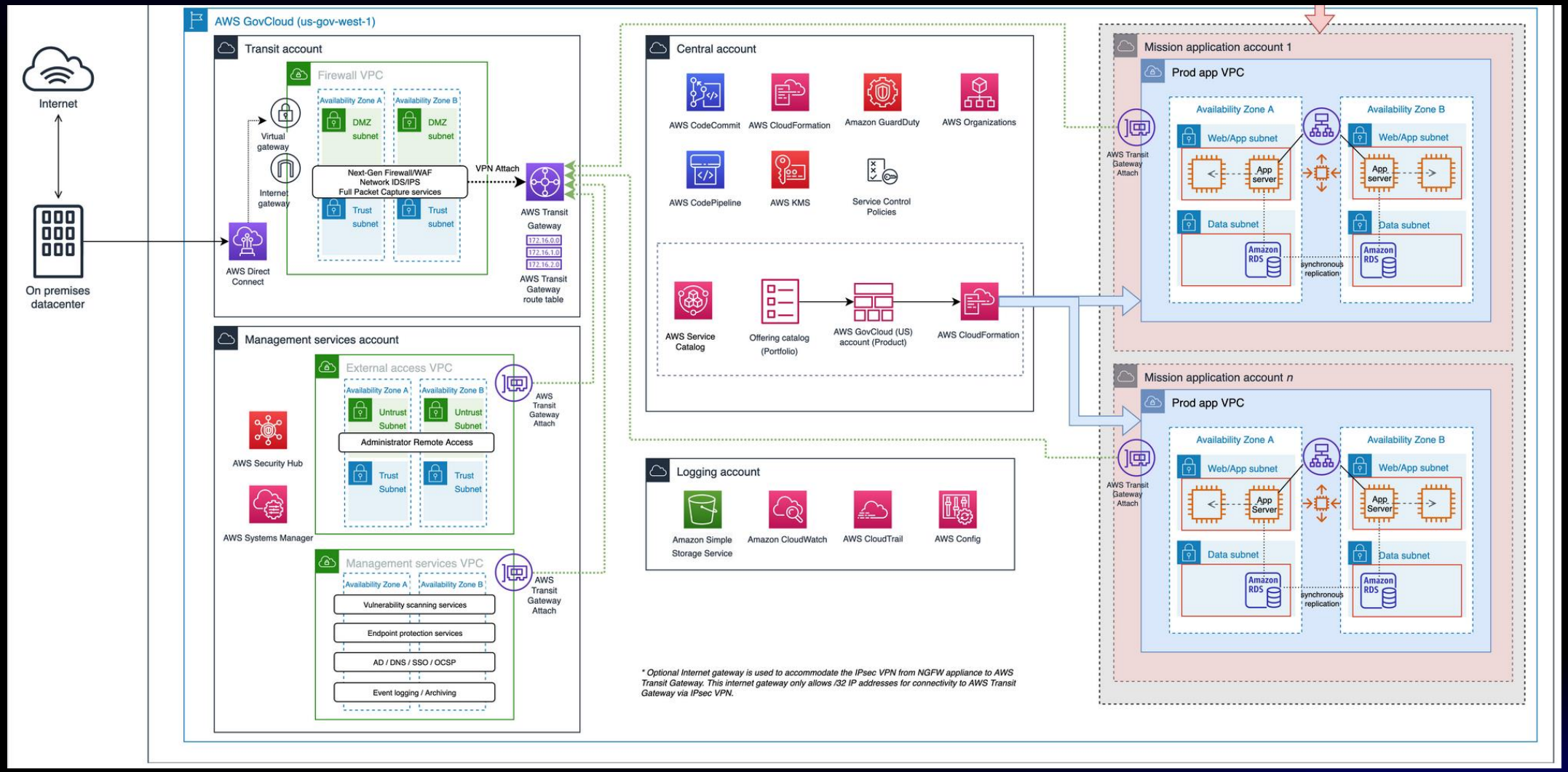


Defense Federal Acquisition Regulation Supplement (DFARS)

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

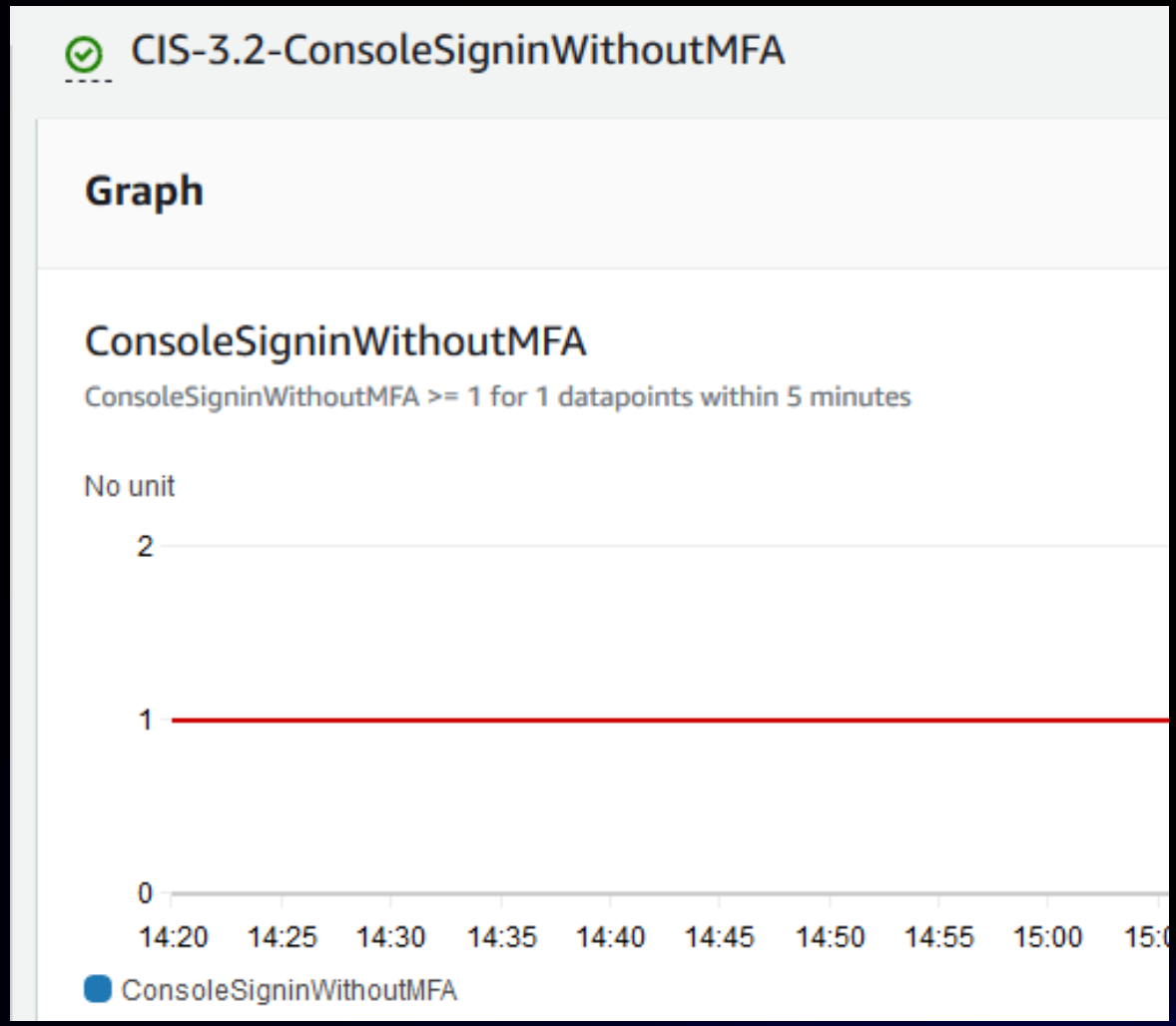
Compliant framework for federal and DoD workloads in AWS GovCloud (US)



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

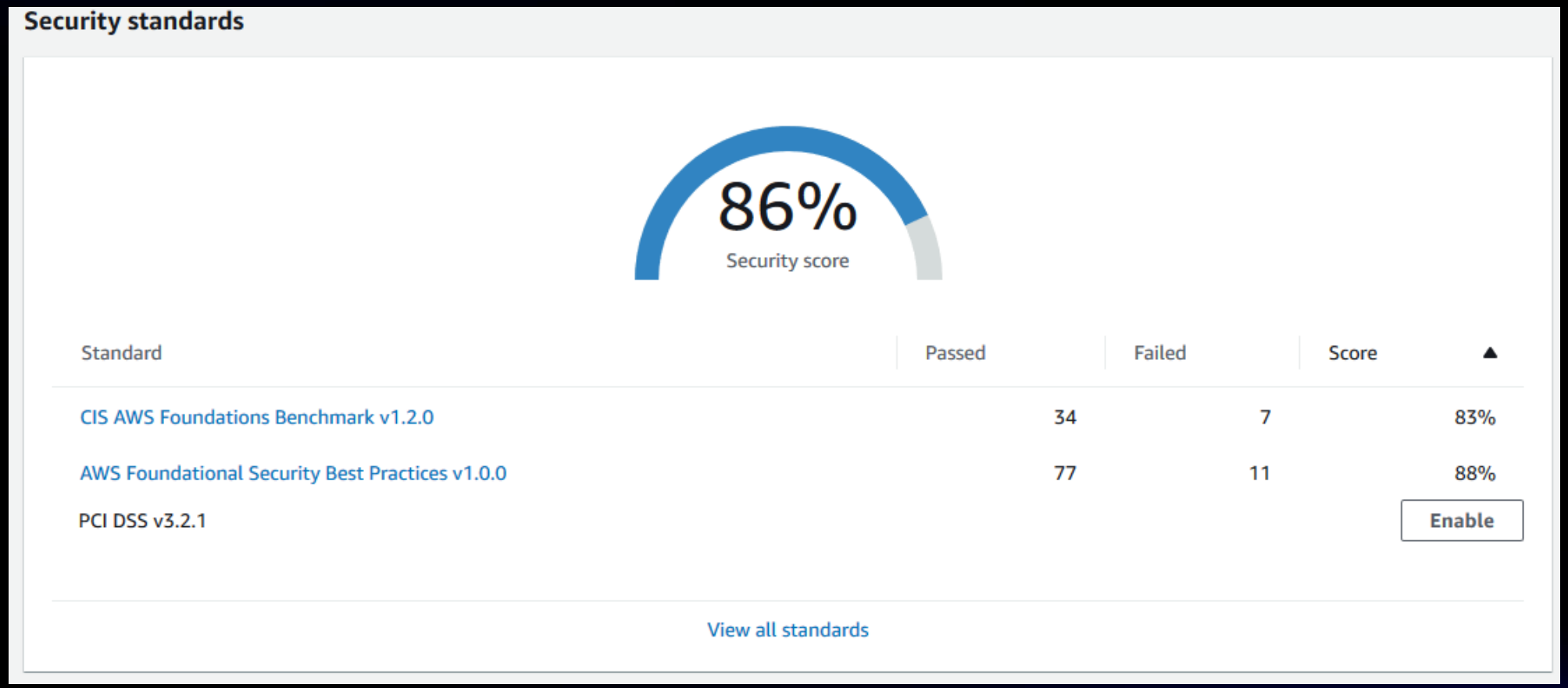
An event has occurred!

Amazon CloudWatch



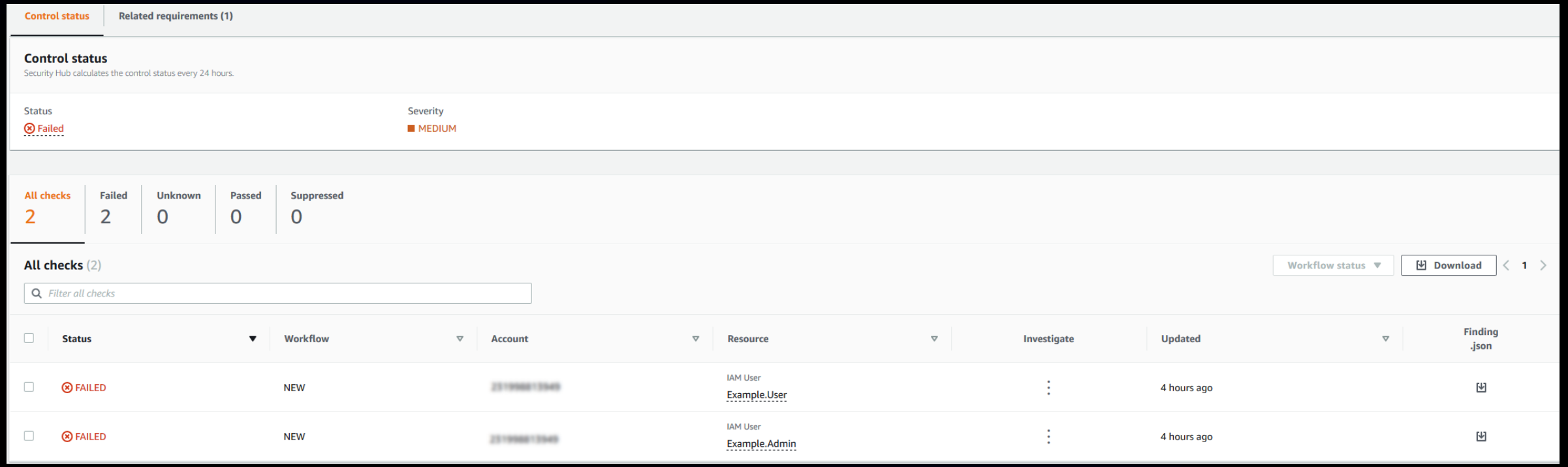
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Security Hub



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Investigate



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.



AWS Config

Rules applied

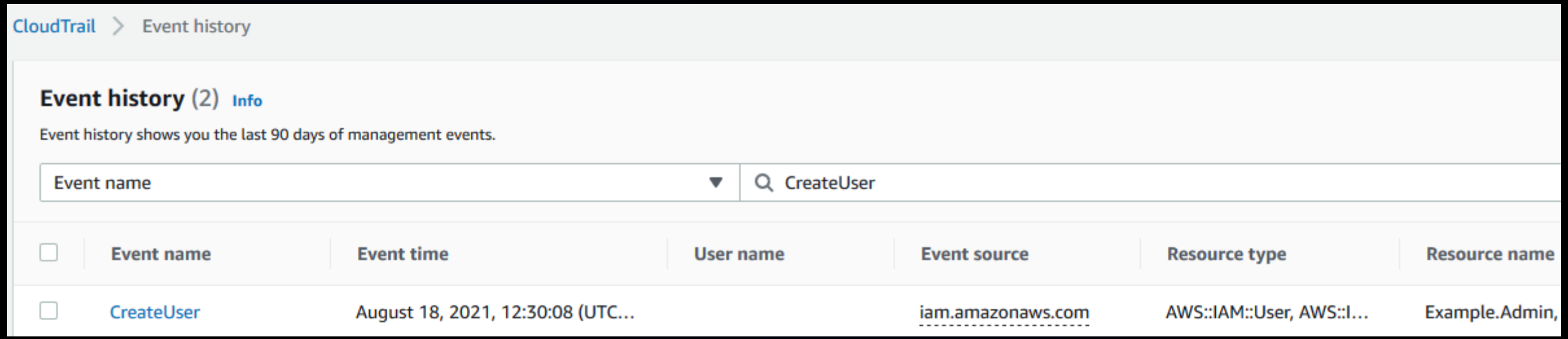
Resource compliance status Noncompliant with 2 rules

Add rule | Rule actions

Name	Compliance	Remediation action	Last remediation
securityhub-mfa-enabled-for-iam-console-access-2f570530	Noncompliant	Not set	n/a
compliant-framework-iam-user-mfa-enabled	Noncompliant	Not set	n/a

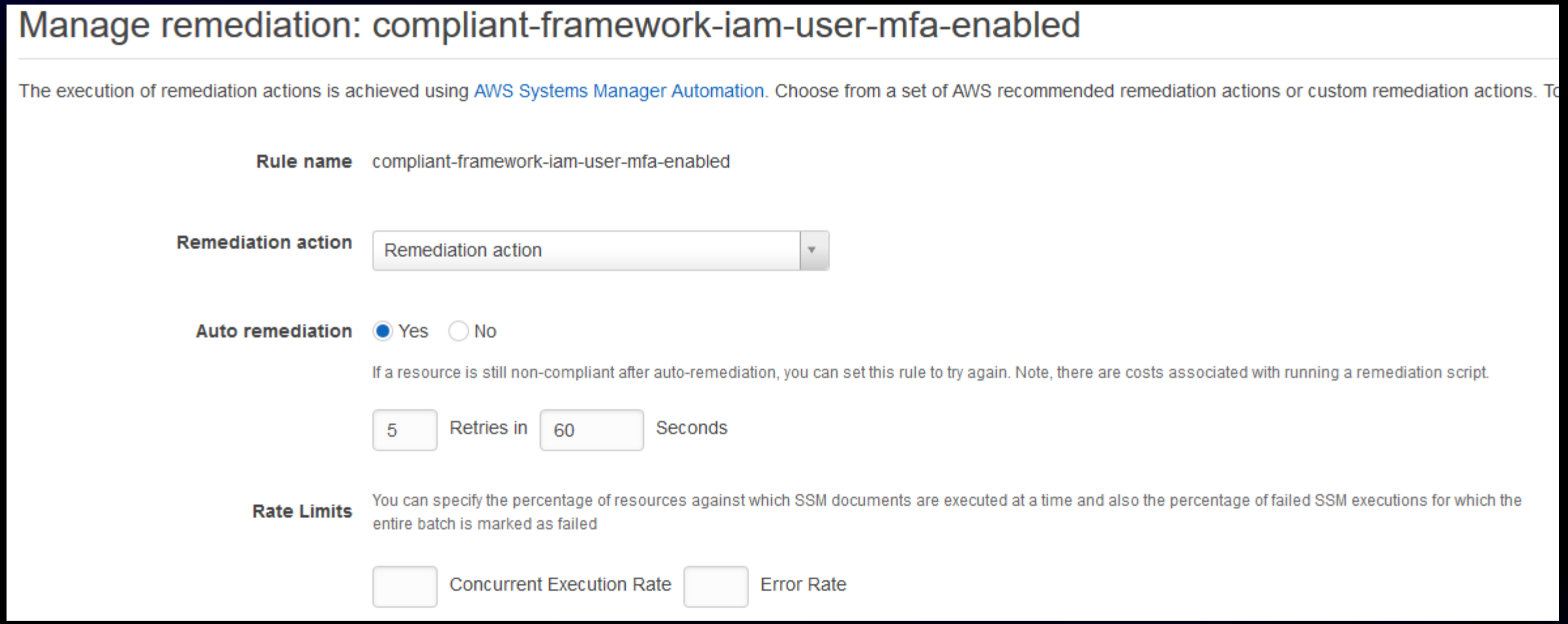
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS CloudTrail



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Remediate



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Summary

Security on AWS

Building and deploying security-hardened Windows

Securing AWS Directory Service for Microsoft Active Directory

Administering Amazon EC2 Windows instances securely

Deploying applications to meet FedRAMP High and other regulated industry compliance programs

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resources

- AWS Security Blog
  aws.amazon.com/blogs/security
- Automate OS Image Build Pipelines with EC2 Image Builder
  aws.amazon.com/blogs/aws/automate-os-image-build-pipelines-with-ec2-image-builder
- Secure your AWS Managed Microsoft AD directory
  docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_security.html
- Manage AWS resources with Session Manager port forwarding
  aws.amazon.com/blogs/mt/manage-aws-managed-microsoft-ad-resources-with-session-manager-port-forwarding

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resources

- Microsoft FIPS140-2 validation
  docs.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation
- Restricting encryption algorithms on Windows
  docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings
  https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-security/restrict-cryptographic-algorithms-protocols-schannel
- DISA STIG page
  public.cyber.mil/stigs/

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resources

- AWS GovCloud (US) user guide
  docs.aws.amazon.com/govcloud-us/latest/UserGuide/welcome.html
- ATO on AWS
  aws.amazon.com/partners/programs/ato
- FedRamp compliance on AWS
  aws.amazon.com/compliance/fedramp

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Bill Jacobi
bjacobi@amazon.com

Shawn Asfeld
sasfeld@amazon.com

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.