AWS Cloud Management

AWS Organizations

AWS organizations allows you to consolidate multiple AWS accounts into an organization that you create and centrally manage.

Available in two feature sets:

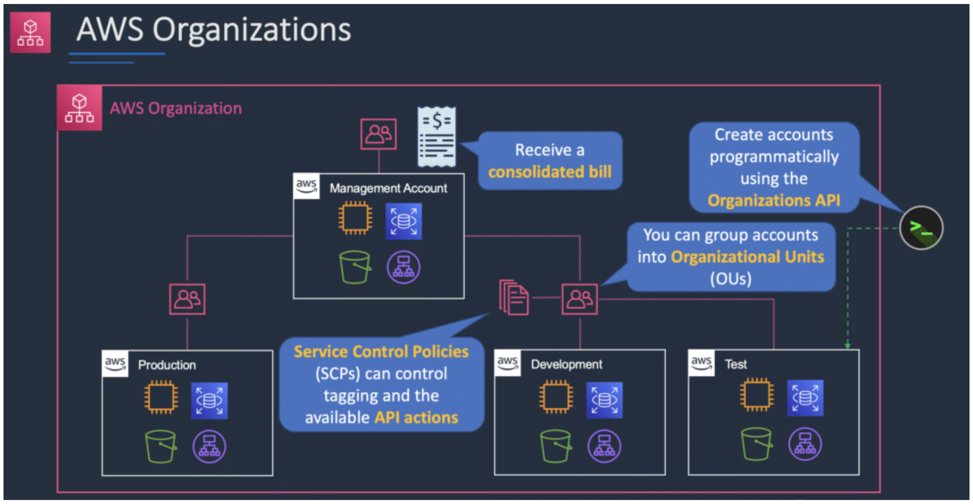
- Consolidated Billing.
- All features.

Includes root accounts and organizational units.

Policies are applied to root accounts or OUs.

Consolidated billing includes:

- Paying Account – independent and cannot access resources of other accounts.
- Linked Accounts – all linked accounts are independent.



AWS Organizations

Receive a consolidated bill

Create accounts programmatically using the Organizations API

You can group accounts into Organizational Units (OUs)

Service Control Policies (SCPs) can control tagging and the available API actions

AWS Control Tower

Simplifies the process of creating multi-account environments.

Sets up governance, compliance, and security guardrails for you.

Integrates with other services and features to setup the environment for you including:

- AWS Organizations, SCPs, OUs, AWS Config, AWS CloudTrail, Amazon S3, Amazon SNS, AWS CloudFormation, AWS Service Catalog, AWS Single Sign-On (SSO).

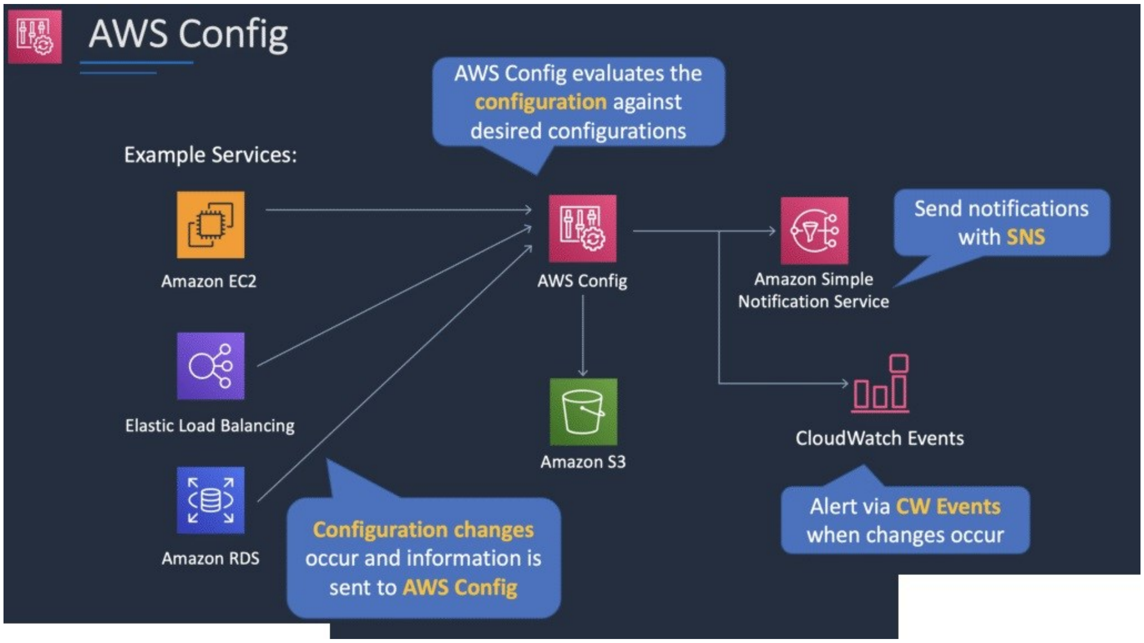
Examples of guardrails AWS Control Tower can configure for you include:

- Disallowing public write access to Amazon Simple Storage Service (Amazon S3) buckets.
- Disallowing access as a root user without multi-factor authentication.
- Enabling encryption for Amazon EBS volumes attached to Amazon EC2 instances.

AWS Config

AWS Config is a fully-managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and regulatory compliance.

With AWS Config, you can discover existing and deleted AWS resources, determine your overall compliance against rules, and dive into configuration details of a resource at any point in time. AWS Config enables compliance auditing, security analysis, resource change tracking, and troubleshooting.



AWS Config

AWS Config evaluates the configuration against desired configurations

Send notifications with SNS

Alert via CW Events when changes occur

Configuration changes occur and information is sent to AWS Config

AWS Service Catalog

AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS.

AWS Service Catalog allows you to centrally manage commonly deployed IT services.

IT services can include virtual machine images, servers, software, and databases and multi-tier application architectures.

Enables users to quickly deploy only the approved IT services they need.

AWS Systems Manager

Manages many AWS resources including Amazon EC2, Amazon S3, Amazon RDS etc.

Systems Manager Components:

- Automation.
- Run Command.
- Inventory.
- Patch Manager.
- Session Manager.
- Parameter Store.

AWS Personal Health Dashboard

AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact you.

Personal Health Dashboard gives you a personalized view into the performance and availability of the AWS services underlying your AWS resources.

The dashboard displays relevant and timely information to help you manage events in progress.

Also provides proactive notification to help you plan for scheduled activities.

Alerts are triggered by changes in the health of AWS resources, giving you event visibility, and guidance to help quickly diagnose and resolve issues.

You get a personalized view of the status of the AWS services that power your applications, enabling you to quickly see when AWS is experiencing issues that may impact you.

Also provides forward looking notifications, and you can set up alerts across multiple channels, including email and mobile notifications, so you receive timely and relevant information to help plan for scheduled changes that may affect you.

Alerts include remediation details and specific guidance to enable you to take immediate action to address AWS events impacting your resources.

Can integrate with Amazon CloudWatch Events, enabling you to build custom rules and select targets such as AWS Lambda functions to define automated remediation actions.

The AWS Health API allows you to integrate health data and notifications with your existing in-house or third-party IT Management tools.

Service Health Dashboard

AWS publishes up-to-the-minute information on service availability.

This information is not personalized to you (unlike Personal Health Dashboard).

AWS OpsWorks

AWS OpsWorks is a configuration management service that provides managed instances of Chef and Puppet.

Updates include patching, updating, backup, configuration and compliance management.

AWS Trusted Advisor

AWS Trusted Advisor is an online tool that provides you real time guidance to help you provision your resources following AWS best practices.

Trusted Advisor checks help optimize your AWS infrastructure, improve security and performance, reduce your overall costs, and monitor service limits.

AWS Basic Support and AWS Developer Support customers get access to 6 security checks (S3 Bucket Permissions, Security Groups – Specific Ports Unrestricted, IAM Use, MFA on Root Account, EBS Public Snapshots, RDS Public Snapshots) and 50 service limit checks.

AWS Business Support and AWS Enterprise Support customers get access to all 115 Trusted Advisor checks (14 cost optimization, 17 security, 24 fault tolerance, 10 performance, and 50 service limits) and recommendations.

AWS Security

As an AWS customer you inherit all the best practices of AWS policies, architecture, and operational processes.

The AWS Cloud enables a shared responsibility model.

AWS manages security OF the cloud, you are responsible for security IN the cloud.

You retain control of the security you choose to implement to protect your own content, platform, applications, systems, and networks no differently than you would in an on-site data center.

Benefits of AWS Security

- **Keep Your Data Safe** – the AWS infrastructure puts strong safeguards in place to help.
- **Protect your privacy** – All data is stored in highly secure AWS data centers.
- **Meet Compliance Requirements** – AWS manages dozens of compliance programs in its infrastructure. This means that segments of your compliance have already been completed.
- **Save Money** – cut costs by using AWS data centers. Maintain the highest standard of s security without having to manage your own facility.
- **Scale Quickly** – security scales with your AWS Cloud usage. No matter the size of your business, the AWS infrastructure is designed to keep your data safe.

Compliance

AWS Cloud Compliance enables you to understand the robust controls in place at AWS to maintain security and data protection in the cloud.

As systems are built on top of AWS Cloud infrastructure, compliance responsibilities will be shared.

Compliance programs include:

-
  -
  - Certifications / attestations.
  - Laws, regulations, and privacy.
  - Alignments / frameworks.

AWS Artifact

AWS Artifact is your go-to, central resource for compliance-related information that matters to you.

It provides on-demand access to AWS' security and compliance reports and select online agreements.

Reports available in AWS Artifact include our Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls.

Agreements available in AWS Artifact include the Business Associate Addendum (BAA) and the Nondisclosure Agreement (NDA).

Amazon GuardDuty

Amazon GuardDuty offers threat detection and continuous security monitoring for malicious or unauthorized behavior to help you protect your AWS accounts and workloads.

Intelligent threat detection service.

Detects account compromise, instance compromise, malicious reconnaissance, and bucket compromise.

Continuous monitoring for events across:

- AWS CloudTrail Management Events.
- AWS CloudTrail S3 Data Events.
- Amazon VPC Flow Logs.
- DNS Logs.

AWS WAF & AWS Shield

WAF:

-
  -
  - AWS WAF is a web application firewall.
  - Protects against common exploits that could compromise application availability, compromise security or consume excessive resources.
  - WAF lets you create rules to filter web traffic based on conditions that include IP addresses, HTTP headers and body, or custom URIs.
  - WAF makes it easy to create rules that block common web exploits like SQL injection and cross site scripting.
  - The rules are known as Web ACLs.

Shield:

-
  -
  - AWS Shield is a managed Distributed Denial of Service (DDoS) protection service.
  - Safeguards web application running on AWS with always-on detection and automatic inline mitigations.
  - Helps to minimize application downtime and latency.
  - Two tiers – Standard and Advanced.

AWS Key Management Service

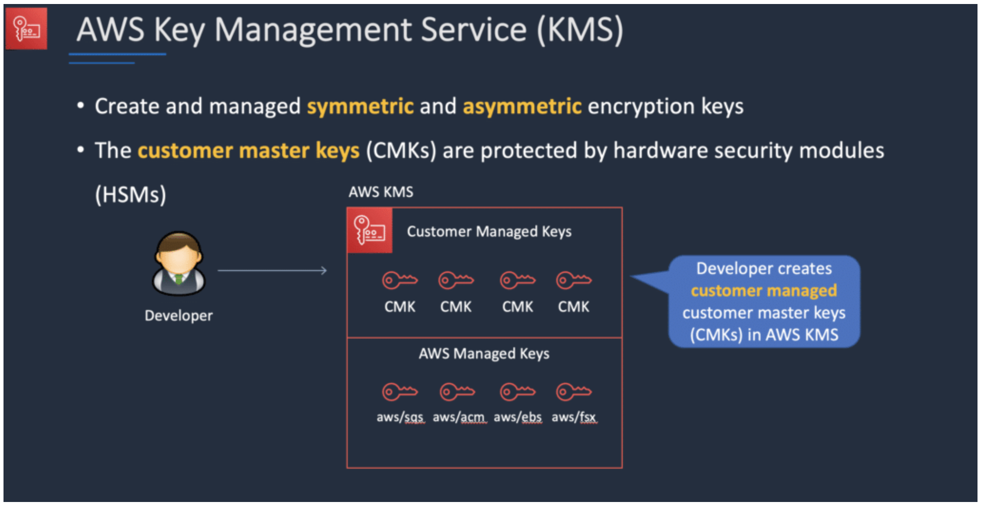
AWS Key Management Service gives you centralized control over the encryption keys used to protect your data.

You can create, import, rotate, disable, delete, define usage policies for, and audit the use of encryption keys used to encrypt your data.

AWS Key Management Service is integrated with most other AWS services making it easy to encrypt the data you store in these services with encryption keys you control.

AWS KMS is integrated with AWS CloudTrail which provides you the ability to audit who used which keys, on which resources, and when.

AWS KMS enables developers to easily encrypt data, whether through 1-click encryption in the AWS Management Console, or using the AWS SDK to easily add encryption in their application code.



AWS Key Management Service (KMS)

- Create and managed **symmetric** and **asymmetric** encryption keys
- The **customer master keys** (CMKs) are protected by hardware security modules (HSMs)

Developer creates **customer managed** customer master keys (CMKs) in AWS KMS

AWS CloudHSM

AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud.

With CloudHSM, you can manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs.

CloudHSM offers you the flexibility to integrate with your applications using industry-standard APIs, such as PKCS#11, Java Cryptography Extensions (JCE), and Microsoft CryptoNG (CNG) libraries.

AWS Inspector and AWS Trusted Advisor

AWS Inspector:

-
    -
        - Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS.
        - Inspector automatically assesses applications for vulnerabilities or deviations from best practices.
        - Uses an agent installed on EC2 instances.
        - Instances must be tagged.

AWS Trusted Advisor:

-
    -
        - Trusted Advisor is an online resource that helps to reduce cost, increase performance and improve security by optimizing your AWS environment.
        - Trusted Advisor provides real time guidance to help you provision your resources following best practices.
        - Advisor will advise you on Cost Optimization, Performance, Security, and Fault Tolerance.

Trusted Advisor scans your AWS infrastructure and compares is to AWS best practices in five categories:

-
    -
        - Cost Optimization.
        - Performance.
        - Security.
        - Fault Tolerance.
        - Service Limits.

Trusted Advisor comes in two versions.

Core Checks and Recommendations (free):

-
    -
        - Access to the 7 core checks to help increase security and performance.
        - Checks include S3 bucket permissions, Security Groups, IAM use, MFA on root account, EBS public snapshots, RDS public snapshots.

Full Trusted Advisor Benefits (business and enterprise support plans):

-
    - ○
    - Full set of checks to help optimize your entire AWS infrastructure.
    - Advises on security, performance, cost, fault tolerance and service limits.
    - Additional benefits include weekly update notifications, alerts, automated actions with CloudWatch and programmatic access using the AWS Support API.

Penetration Testing

Penetration testing is the practice of testing one's own application's security for vulnerabilities by simulating an attack.

AWS allows penetration testing. There is a limited set of resources on which penetration testing can be performed.

You do not need permission to perform penetration testing against the following services:

- Amazon EC2 instances, NAT Gateways, and Elastic Load Balancers.
- Amazon RDS.
- Amazon CloudFront.
- Amazon Aurora.
- Amazon API Gateways.
- AWS Lambda and Lambda Edge functions.
- Amazon Lightsail resources.
- Amazon Elastic Beanstalk environments.

You can read the full vulnerability and penetration testing support policy here.

In case an account is or may be compromised, AWS recommend that the following steps are taken:

-
  -
    1. Change your AWS root account password.
    2. Change all IAM user's passwords.
    3. Delete or rotate all programmatic (API) access keys.
    4. Delete any resources in your account that you did not create.
    5. Respond to any notifications you received from AWS through the AWS Support Center and/or contact AWS Support to open a support case.

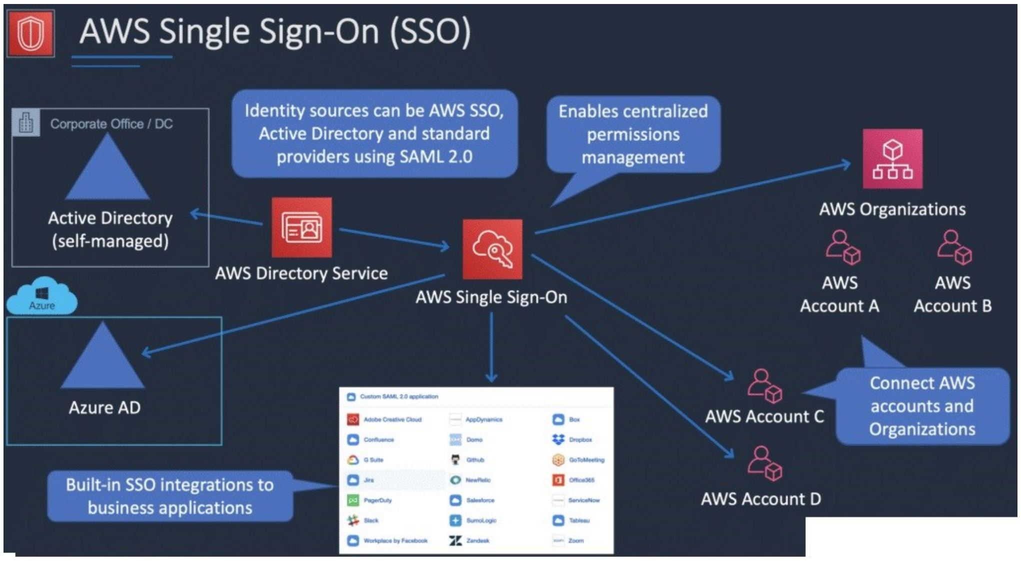
AWS Single Sign-On (AWS SSO)

AWS Single Sign-On is a cloud-based single sign-on (SSO) service that makes it easy to centrally manage SSO access to all of your AWS accounts and cloud applications.

It helps you manage SSO access and user permissions across all your AWS accounts in AWS Organizations.

AWS SSO also helps you manage access and permissions to commonly used third-party software as a service (SaaS) applications, AWS SSO-integrated applications as well as custom applications that support Security Assertion Markup Language (SAML) 2.0.

AWS SSO includes a user portal where your end-users can find and access all their assigned AWS accounts, cloud applications, and custom applications in one place.



AWS Single Sign-On (SSO)

Identity sources can be AWS SSO, Active Directory and standard providers using SAML 2.0

Enables centralized permissions management

Connect AWS accounts and Organizations

Built-in SSO integrations to business applications

Amazon Cognito

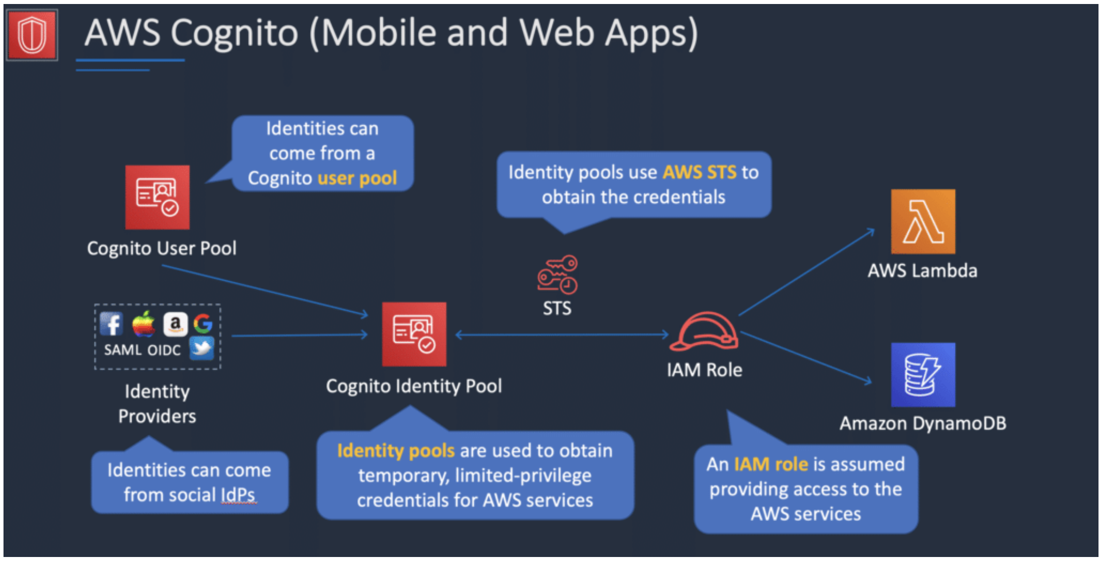
Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily.

Amazon Cognito scales to millions of users and supports sign-in with social identity providers, such as Apple, Facebook, Google, and Amazon, and enterprise identity providers via SAML 2.0 and OpenID Connect.

The two main components of AWS Cognito are user pools and identity pools:

- User pools are user directories that provide sign-up and sign-in options for your app users.
- Identity pools enable you to grant your users access to other AWS services.

You can use identity pools and user pools separately or together.



AWS Cognito (Mobile and Web Apps)

Identities can come from a Cognito user pool

Identity pools use AWS STS to obtain the credentials

Identities can come from social IdPs

Identity pools are used to obtain temporary, limited-privilege credentials for AWS services

An IAM role is assumed providing access to the AWS services

AWS Directory Services

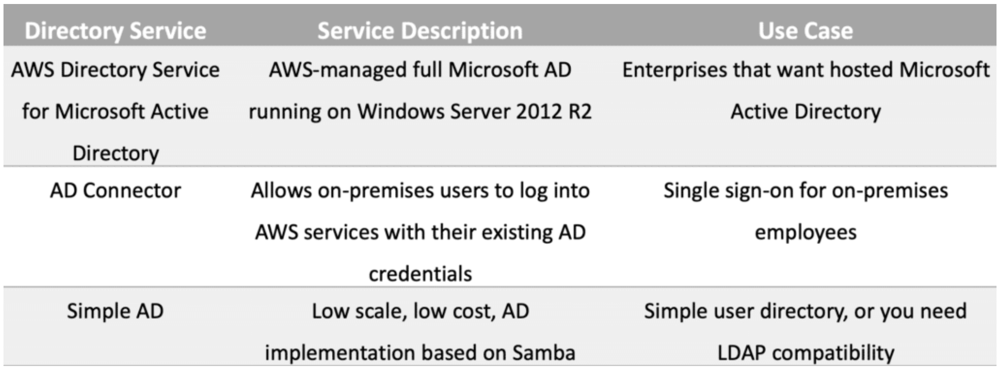
AWS provide a number of directory types.

The following three types currently feature on the exam and will be covered on this page:

- Active Directory Service for Microsoft Active Directory.
- Simple AD.
- AD Connector.

As an alternative to the AWS Directory service you can build your own Microsoft AD DCs in the AWS cloud (on EC2).

The table below summarises the directory services covered on this page as well as a couple of others, and provides some typical use cases:



Directory Service	Service Description	Use Case
AWS Directory Service for Microsoft Active Directory	AWS-managed full Microsoft AD running on Windows Server 2012 R2	Enterprises that want hosted Microsoft Active Directory
AD Connector	Allows on-premises users to log into AWS services with their existing AD credentials	Single sign-on for on-premises employees
Simple AD	Low scale, low cost, AD implementation based on Samba	Simple user directory, or you need LDAP compatibility

AWS Systems Manager Parameter Store

Provides secure, hierarchical storage for configuration data management and secrets management.

It is highly scalable, available, and durable.

You can store data such as passwords, database strings, and license codes as parameter values.

You can store values as plaintext (unencrypted data) or ciphertext (encrypted data).

You can then reference values by using the unique name that you specified when you created the parameter.

AWS Secrets Manager

Similar to Parameter Store.

Allows native and automatic rotation of keys.

Fine-grained permissions.

Central auditing for secret rotation.