Zero Trust Model

The Zero Trust model operates on the principle of
"trust no one, verify everything."

Malicious actors being able to by-pass conventional **access controls** demonstrates traditional security measures are no longer sufficient

In the Zero Trust Model **Identity** becomes the primary security perimeter.

What is the Primary Security Perimeter?
The primary or new security perimeter defines the first line of defense and its security controls that protect a company's cloud resources and assets

Network-Centric: (Old-Way)
traditional security focused on firewalls and VPNs since there were few employees or workstations outside the office or they were in specific remote offices.

Identity-Centric: (New-Way)
Bring-your-own-device, remote workstations is much more common , we can't trust if the employee is in a secure location, we have identity based security controls like MFA, or providing provisional access based on the level of risk from where, when and what a user wants to access.

Identity-Centric does not replace but ***augments*** Network-Centric Security

@Sigmund on Unsplash

Zero Trust on AWS

Identity Security Controls you can implement on AWS to meet the Zero Trust Model

AWS Identity and Access Management (IAM)

- IAM Policies
- Permission Boundaries
- Service Control Policies (Organization-wide Policies)
- IAM Policy Conditions
  - aws:SourceIp – Restrict on IP Address
  - aws:RequestedRegion – Restrict on Region
  - aws:MultiFactorAuthPresent – Restrict if MFA is turned off
  - aws:CurrentTime – Restrict access based on time of day

Your AWS Resources

AWS does not have a ready-to-use identity controls are intelligent, which is why AWS is considered to not have a true Zero Trust offering for customers, and third-party services need to be used.

A collection of AWS Services can be setup to intelligent-ish detection of identity concerns but requires expert knowledge

AWS CloudTrail
Tracks all API calls

Amazon GuardDuty
Detects suspicious or malicious activity based on CloudTrail and other logs

Amazon Detective
Used to analyze, investigate and quickly identify security issues (can ingest findings from Guard Duty)

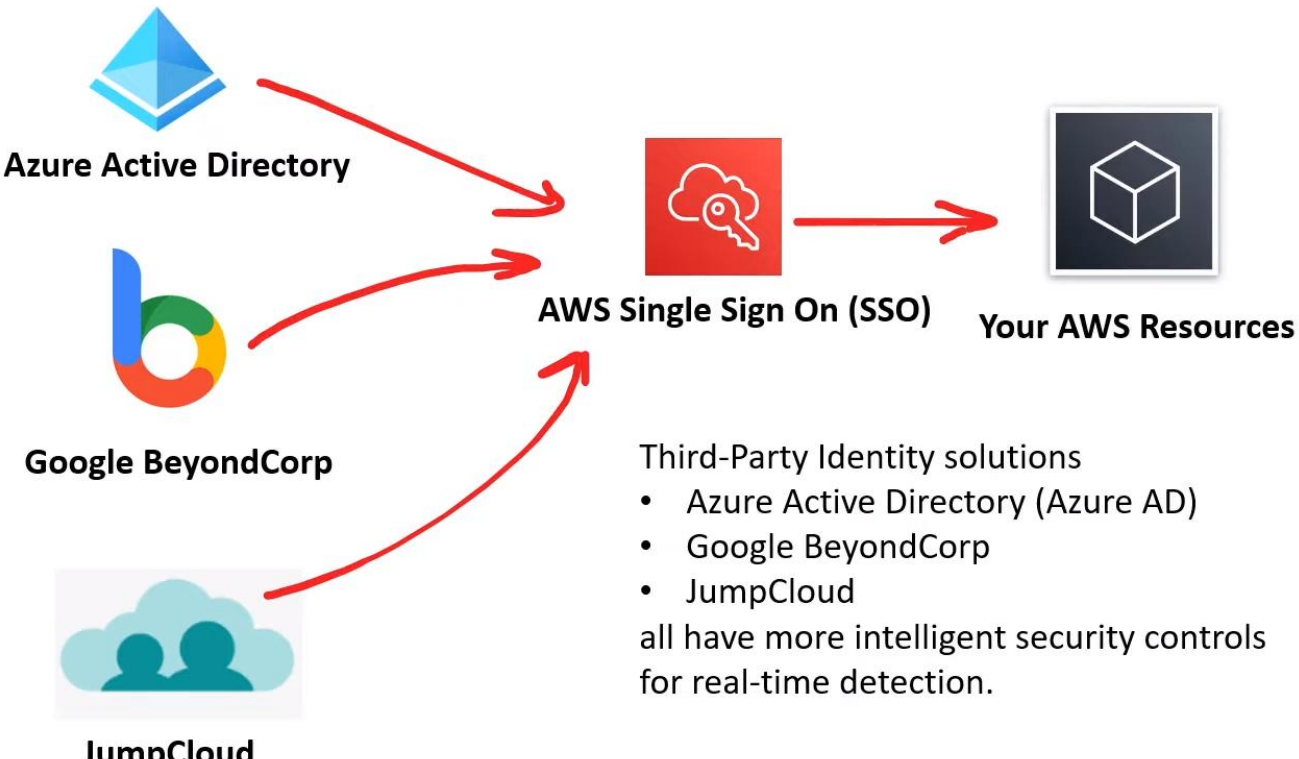
Zero Trust on AWS with Third Parties

AWS does technically implement a Zero Trust Model but does not allow for intelligent identity security controls.

For example:
Azure Active Directory has Real-time and calculated risk detection based more data points than AWS eg:

- Device and Application
- Time of Day
- Location
- MFA turned on
- What is being accessed

And the security controls, verifications or logic restriction is much more robust.



Third-Party Identity solutions

- Azure Active Directory (Azure AD)
- Google BeyondCorp
- JumpCloud

all have more intelligent security controls for real-time detection.

Directory Service

What is a directory service?

A directory service maps the **names of network resources to their network addresses.**

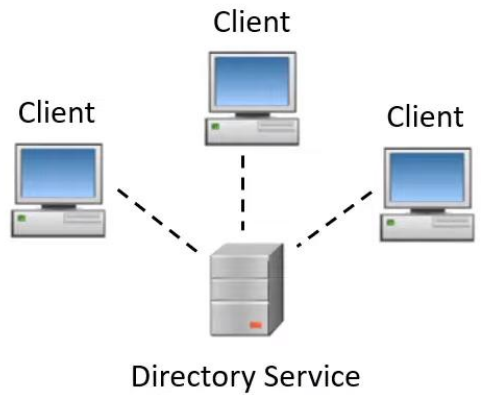
A directory service is shared information infrastructure for **locating, managing, administering and organizing** resources:

- Volumes
- Folders
- Files
- Printers
- Users
- Groups
- Devices
- Telephone numbers
- other objects

A directory service is a critical component of a network operating system

A directory server (name server) is a server which provides a directory service

Each resource on the network is considered an object by the directory server. Information about a particular resource is stored as a collection of attributes associated with that resource or object

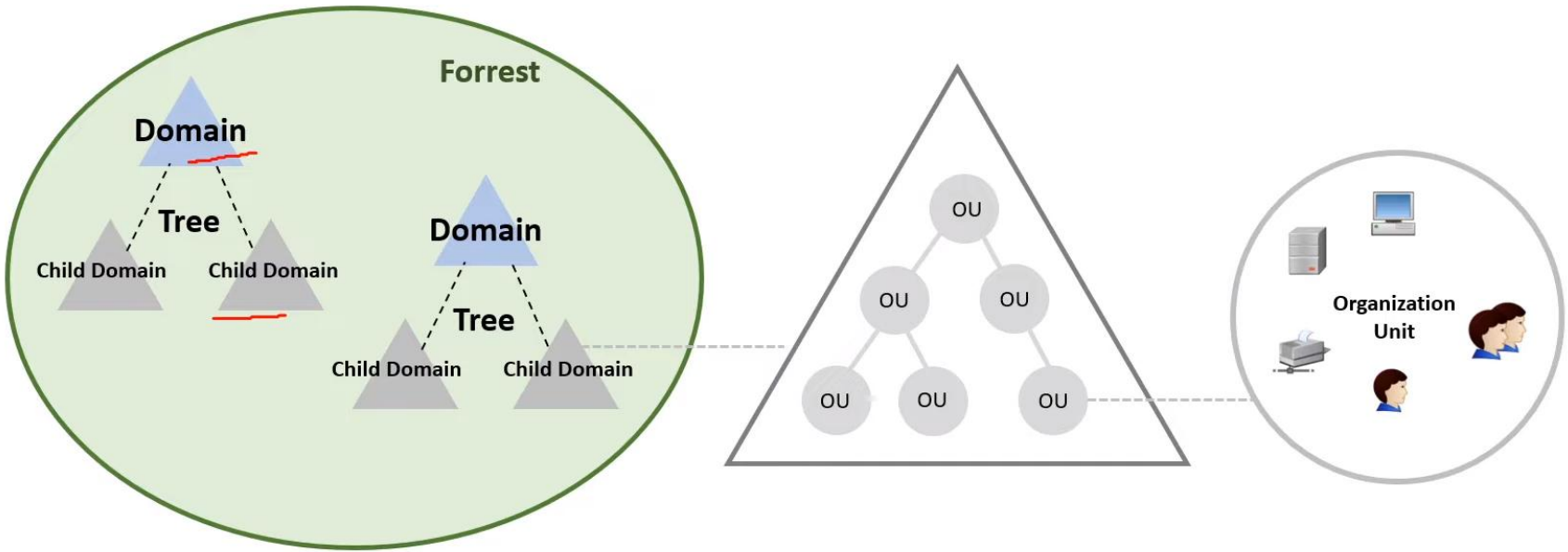


Well known directory services:

- Domain Name Service (DNS)
  - the directory service for **the internet**
- **Microsoft Active Directory**
  - Azure Active Directory
- Apache Directory Server
- Oracle Internet Directory (OID)
- OpenLDAP
- Cloud Identity
- JumpCloud

Active Directory

Microsoft introduced **Active Directory** Domain Services in **Windows 2000** to give organizations the ability to manage multiple on-premises infrastructure components and systems using a single identity per user.



Identity Providers (IdPs)

Identity Provider (IdP) a system entity that creates, maintains, and manages identity information for principals and also provides authentication services to applications within a **federation** or distributed network.
A trusted provider of your user identity that lets you use authenticate to access other services.
Identity Providers could be: **Facebook, Amazon, Google, Twitter, Github, LinkedIn**

Federated identity is a method of linking a user's identity across multiple separate identity management systems

OpenID
open standard and decentralized authentication protocol. Eg be able to login into a different social media platform using a Google or Facebook account
OpenID is about providing who are you

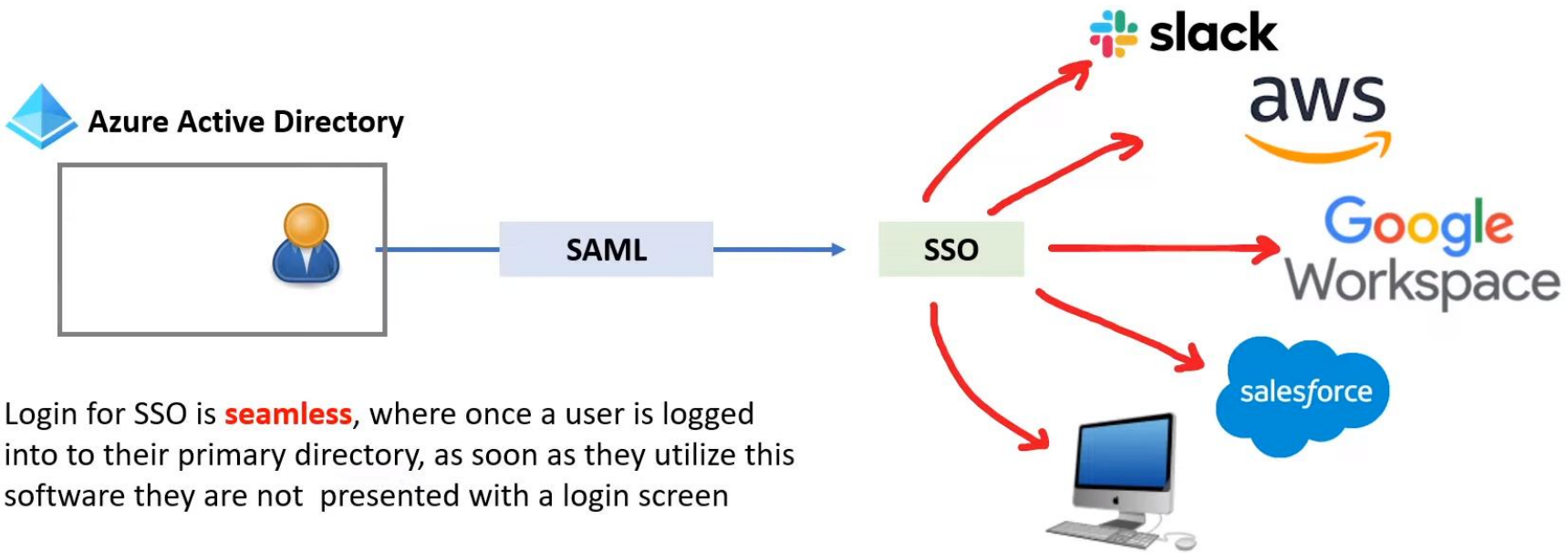
OAuth2.0
industry-standard protocol for authorization OAuth doesn't share password data but instead uses authorization tokens to prove an identity between consumers and service providers.
Oauth is about granting access to functionality

SAML
Security Assertion Markup Language is an open standard for exchanging authentication and authorization between an identity provider and a service provider.
An important use case for SAML is **Single-Sign-On via web browser**.

Single-Sign-On

Single sign-on (**SSO**) is an authentication scheme that **allows a user to log in with a single ID and password to different systems and software**.

SSO allows IT departments to administrator a single identity that can access many machines and cloud services.



Login for SSO is **seamless**, where once a user is logged into to their primary directory, as soon as they utilize this software they are not presented with a login screen

LDAP

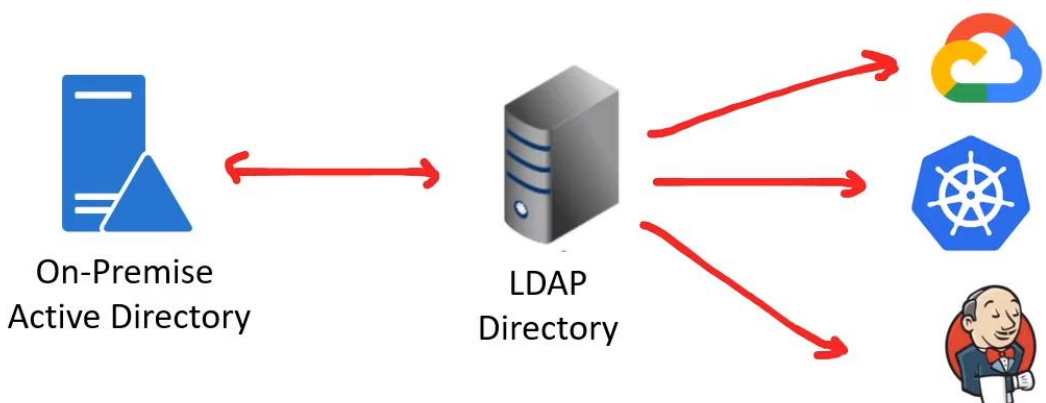
Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard **application protocol for accessing and maintaining distributed directory information services** over an Internet Protocol (IP) network.

A common use of LDAP is to provide a central place to store usernames and passwords

LDAP enables for **same-sign on.** Same sign-on allows users to single ID and password, but they have to enter it in every time they want to login.

Why use LDAP when SSO is more convenient?

Most SSO systems are using LDAP.
LDAP was not designed natively to work with web-applications.
Some systems only support integration with LDAP and not SSO



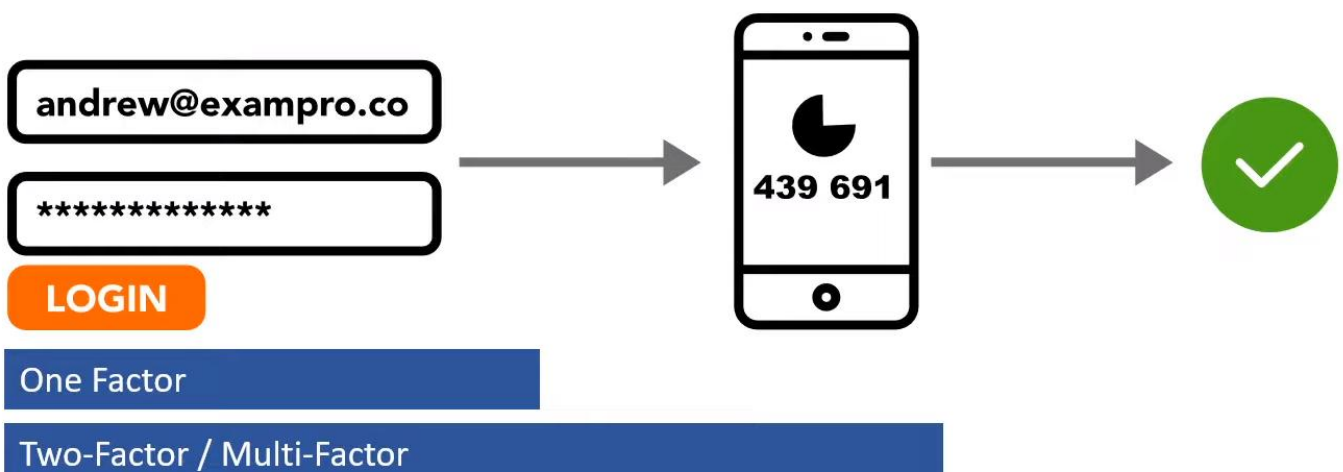
Multi-Factor Authentication

What is Multi-Factor Authentication (MFA)?

A security control where after you fill in your username/email and password **you have to use a second device** such as a phone to confirm that its you logging in.

MFA **protects** against people who have stolen your password.

MFA is an option in most cloud providers and even social media websites such as Facebook.



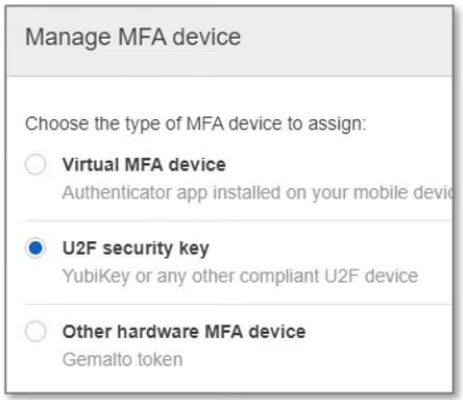
Security Keys

What is a Security Key?

A secondary device used as second step in authentication process to gain access to a device, workstation or application.

A popular brand of security key is an Yubikey

A security key can resemble a memory stick. When your finger makes contact with a button of exposed metal on the device it will generate And autofill a security token.



- Works out of the box with Gmail, Facebook, and hundreds more
- Supports **FIDO2**/WebAuthn, U2F
- Waterproof and crush resistant
- USB-A and NFC dual connectors on a single key

AWS Identity and Access Management (IAM)

AWS Identity and Access Management (IAM) you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

IAM **Policies**

JSON documents which grant permissions for a specific user, group, or role to access services. Policies are attached to **IAM Identities**

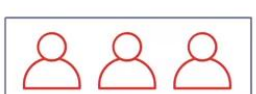
IAM **Permission**

The API actions that can or cannot be performed.
They are represented in the IAM Policy document

IAM Identities

IAM **Users**

End users who log into the console or interact with AWS resources programmatically or via clicking UI interfaces



IAM **Groups**

Group up your Users so they all share permission levels of the group
eg. Administrators, Developers, Auditors

IAM **Roles**

Roles grant AWS resources permissions to specific AWS API actions
Associate policies to a Role and then assign it to an AWS resource

Anatomy of an IAM Policy

IAM Policies are written in JSON, and contain the permissions which determine what API actions are allowed or denied.

Version policy language version. 2012-10-17 is the latest version.

Statement container for the policy element you are allowed to have multiples

Sid (optional) a way of labeling your statements.

Effect Set whether the policy will Allow or Deny

Action list of actions that the policy allows or denies

Principal account, user, role, or federated user to which you would like to allow or deny access

Resource the resource to which the action(s) applies

Condition (optional) circumstances under which the policy grants permission

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "Deny-Barclay-S3-Access",
        "Effect": "Deny",
        "Action": "s3:*",
        "Principal": {"AWS": ["arn:aws:iam:123456789012:barclay"]},
        "Resource": "arn:aws:s3:::my-bucket"
    },{
        "Effect": "Allow",
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "*",
        "Condition": {
            "StringLike": {
                "iam:AWSServiceName": [
                    "rds.amazonaws.com",
                    "rds.application-autoscaling.amazonaws.com"
                ]
            }
        }
    }]
}
```

Principle of Least Privilege (PoLP)

Principle of Least Privilege (PoLP) is the computer security concept of providing a user, role, or application the least amount of permissions to perform a operation or action.

Just-Enough-Access (JEA)
Permitting only the exact actions for the identity to perform a task

Just-In-Time (JIT)
Permitting the smallest length of duration an identity can use permissions

ConsoleMe is an open-source Netflix project to self-serve short-lived IAM policies so an end user can access AWS resources while enforcing JEA and JIT

https://github.com/Netflix/consoleme

Risk-based adaptive policies
Each attempt to access a resource generates a risk score of how likely the request is to be from a compromised source.
The risk score could be based on many factors e.g. device, user location, IP address what service is being accessed and when.

AWS at the time of this recording does not have Risk-based adaptative policies built into IAM

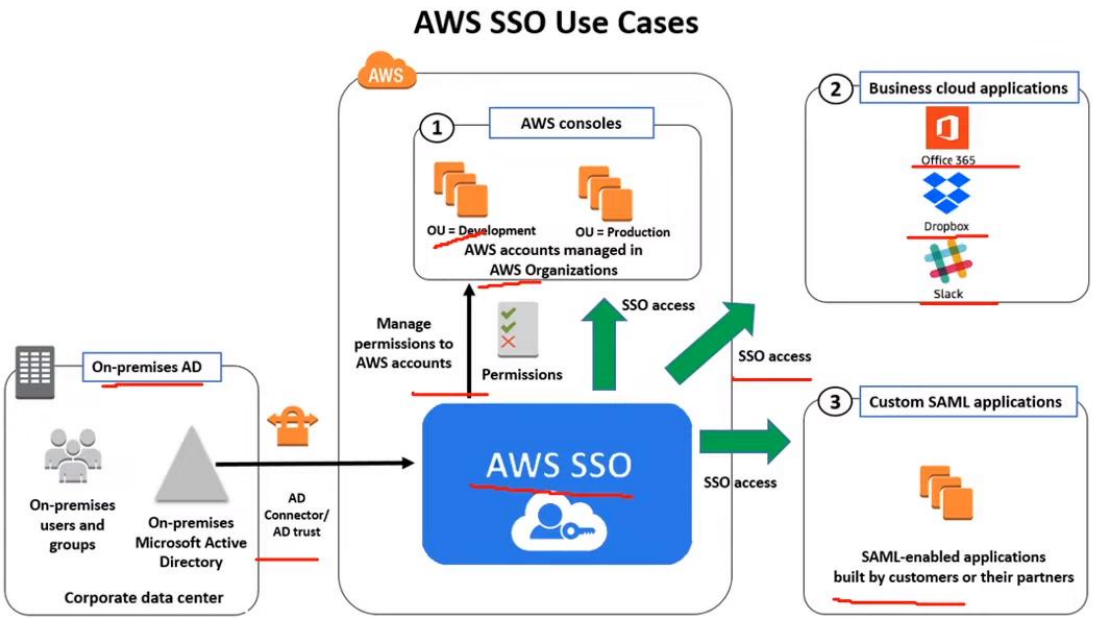
AWS Account Root User

Administrative Tasks **that only the Root User can perform**:

- **Change your account settings**.
  - includes the account name, email address, root user password, and root user access keys.
  - Other account settings, such as contact information, payment currency preference, and Regions, do not require root user credentials.
- Restore IAM user permissions.
  - If the only IAM administrator accidentally revokes their own permissions, you can sign in as the root user to edit policies and restore those permissions.
- Activate IAM access to the Billing and Cost Management console.
- View certain tax invoices
- **Close your AWS account**.
- **Change or Cancel AWS Support plan**
- Register as a seller in the Reserved Instance Marketplace.
- Enable MFA Delete on an S3 Bucket.
- Edit or delete an Amazon S3 bucket policy that includes an invalid VPC ID or VPC endpoint ID.
- Sign up for GovCloud.

AWS Single-Sign On

AWS Single Sign-On (AWS SSO) is where you create, or connect, your workforce identities in AWS **once** and manage access centrally across your AWS organization.



Choose your Identity Source

- AWS SSO
- Active Directory
- SAML 2.0 IdP

Managed User Permissions Centrally

- AWS Account
- AWS Applications
- SAML Applications

Uses get Single Click Access