IAM: Identity Federation & SSO

How would you implement federation with corporate identity providers?

✅ What is Federation?

- Federation allows users to **log in to AWS using corporate credentials** (SSO).
- No need to create IAM users for each employee.
- Uses **SAML 2.0**, **OIDC**, or **Web Identity Federation**.

OpenID Connect (OIDC) is . It's an authentication protocol that verifies user identity and provides basic profile information. Essentially, it allows clients to verify the identity of a user based on authentication performed by an identity provider (IdP)

How to Implement Federation :

1. **Choose your Identity Provider (IdP)**
    - E.g., Azure AD, Okta, Google Workspace.
2. **Create a SAML Identity Provider in AWS IAM**
    - Go to IAM → Identity Providers → Add provider → Choose SAML.
    - Upload the IdP's metadata XML.
3. **Define IAM Role(s) for Federation**
    - Create a role with trust policy for the IdP.
    - Add permissions (e.g., EC2ReadOnly, S3FullAccess).
4. **Set Up Trust Relationship**

- The role's trust policy should allow the IdP to `sts:AssumeRole`.

5. **Configure the IdP**
    - Add AWS as a "SAML application" in IdP (like Azure AD).
    - Set role mapping and pass SAML assertions.
6. **Test Login via SSO**
    - Users log in to corporate portal → click AWS app → get temporary access.

Note:

- You can use **AWS CLI with SAML** using tools like `aws-iam-authenticator` or scripts to fetch credentials.
- Use in **DevOps pipelines** without hardcoding IAM users.

What is SAML 2.0, OIDC, and Web Identity Federation?

These are **identity federation protocols** — they allow users to **sign in to one system (like Google or Facebook)** and then access another system (like your company's internal tool) **without needing a new username and password**.

---

1. SAML 2.0 (Security Assertion Markup Language)

- **Used mostly in enterprise (corporate)** setups.
- Based on **XML**.
- Common with tools like **Salesforce, Office 365, SAP**, etc.
- Enables **Single Sign-On (SSO)**.

How it works:

- You try to access a service (e.g., Salesforce).
- You're redirected to your **Identity Provider (IdP)** (e.g., Okta, ADFS).
- IdP authenticates you and sends a **SAML assertion** (an XML file) back to Salesforce.
- You're logged in.

---

2. OIDC (OpenID Connect)

- Built on top of **OAuth 2.0**.

- Used for **modern web/mobile apps**.
- Based on **JSON** and REST APIs.
- Supported by **Google, Microsoft, AWS Cognito**, etc.

How it works:

- User logs in through an Identity Provider (e.g., Google).
- They are issued an **ID token** (JWT) + **Access token**.
- The app uses these tokens to log you in and access resources.

---

3. Web Identity Federation

- Lets users **sign in using third-party identity providers** (like Google, Facebook, Amazon) to access **cloud resources**, especially **AWS**.

Common with:

- AWS **Cognito + IAM roles**.
- Mobile/web apps that don't have their own authentication system.

How it works (AWS example):

- User signs in with Google.
- Google returns a token.
- That token is exchanged for **temporary AWS credentials**.
- The user accesses AWS services **securely without hardcoding keys**.

Why These Are Required:

Problem	Why Identity Federation Helps
🔐 Multiple logins	Users can use one identity across apps (SSO)
🛡️ Security risks	Reduces password reuse and phishing risk
👨‍💼 Centralized control	Companies can manage access policies from one place
📱 Mobile/web apps	Supports third-party login without storing passwords
☁️ Cloud resource access	Enables temporary, secure access (no need for long-term keys)

Quick Summary:

Protocol	Best For	Format	Common Use
SAML 2.0	Enterprises	XML	SSO in corporate apps
OIDC	Web/Mobile apps	JSON (JWT)	Login via Google, Apple, etc.
Web Identity Federation	Cloud apps (AWS)	Token exchange	Secure AWS access with third-party login

---

1. Which of the following protocols is most commonly used for enterprise Single Sign-On (SSO)?

A. OAuth 2.0
B. OpenID Connect
C. SAML 2.0
D. LDAP

✅ **Answer:** C. SAML 2.0

---

2. Which protocol uses JSON Web Tokens (JWTs) and is built on top of OAuth 2.0?

A. Kerberos
B. OpenID Connect
C. SAML 2.0
D. Basic Auth

✅ **Answer:** B. OpenID Connect

---

3. In AWS, Web Identity Federation allows users to sign in using:

A. IAM usernames and passwords
B. MFA codes only
C. Social identity providers like Google, Facebook
D. Static access keys only

✅ **Answer:** C. Social identity providers like Google, Facebook