**AWS Role Switching & Active Directory Setup**

**Table of Contents**

1. **Introduction**
   * Overview of Role Switching
   * Real-World Use Case
2. **Setting Up Cross-Account Access**
   * Creating Roles in QA & Staging Accounts
   * Creating Users & Groups in Master Account
   * Attaching Policies
3. **Role Switching Methods**
   * Manual Role Switching via AWS Console
   * Policy-Based Role Assumption
4. **Active Directory Setup (AWS + Windows Server)**
   * Launching a Windows EC2 Instance
   * Configuring DNS & Firewall
   * Installing & Promoting AD Domain Services
5. **Next Steps: AWS Managed AD & SSO**
   * AWS Directory Service
   * AD Connector for Hybrid Environments
6. **Conclusion & Best Practices**

**1. Introduction**

**What is Role Switching?**

* Role switching allows users in one AWS account to **temporarily assume roles** in another account.
* Used for:
  + **Cross-account access** (e.g., Master → Staging).
  + **Least privilege security** (grant temporary access).

**Real-World Use Case**

* **Scenario:**
  + **Master Account:** Central admin control.
  + **Staging/QA Accounts:** Isolated environments.
* **Goal:** Allow users from the **Master account** to switch roles into **Staging/QA** without permanent credentials.

**2. Setting Up Cross-Account Access**

**Step 1: Create Roles in QA & Staging Accounts**

1. **QA Account:**
   * Go to **IAM → Roles → Create Role**.
   * Select **"Another AWS account"** → Enter **Master Account ID**.
   * Attach AdministratorAccess (for testing).
   * Name: QA-Role → Create.
2. **Staging Account:**
   * Repeat the same steps → Name: Staging-Role.

**Step 2: Create Users in Master Account**

1. Go to **IAM → Users → Create User**:
   * Admin1, Admin2 (with console access).
2. **Create a User Group** (Admin-Group) and add both users.

**Step 3: Attach Inline Policy for Role Switching**

* **Policy JSON:** Allows assuming roles in QA/Staging:

json

Copy

Download

{

"Version": "2012-10-17",

"Statement": [{

"Effect": "Allow",

"Action": "sts:AssumeRole",

"Resource": [

"arn:aws:iam::QA\_ACCOUNT\_ID:role/QA-Role",

"arn:aws:iam::STAGING\_ACCOUNT\_ID:role/Staging-Role"

]

}]

}

* Attach to Admin-Group.

**3. Role Switching Methods**

**Method 1: Manual Switch via AWS Console**

1. Log in as Admin1 (Master Account).
2. Click **"Switch Role"** (top-right).
3. Enter:
   * **Account ID:** Staging/QA Account ID.
   * **Role Name:** Staging-Role or QA-Role.
4. Click **"Switch Role"** → Now operating in the target account.

**Method 2: Policy-Based Assumption**

* Attach AdministratorAccess to Admin-Group.
* Users can **directly access resources** in Master Account **or** switch roles.

**4. Active Directory Setup (AWS + Windows Server)**

**Step 1: Launch Windows EC2 Instance**

* **AMI:** Windows Server 2019.
* **Key Pair:** Save .pem for RDP access.
* **Security Group:** Allow RDP (3389).

**Step 2: Configure DNS & Firewall**

1. **Set Static DNS:**

powershell

ncpa.cpl → IPv4 → DNS: 10.0.29.112 (Instance IP), 10.0.0.2 (Instance DNS).

1. **Disable Firewall:**

powershell

firewall.cpl → Turn off Windows Firewall.

**Step 3: Install Active Directory**

1. **Server Manager → Add Roles → Active Directory Domain Services**.
2. **Select Features** 🡪 Telnet Client 🡪 Install
3. **Promote to Domain Controller**:
   * Domain: sap.com (example).
   * Set **DSRM Password** (Directory Services Restore Mode).
4. Reboot after installation.

**5. Next Steps: AWS Managed AD & SSO**

**AWS Directory Service**

* **AWS Managed Microsoft AD:** Fully managed Active Directory.
* **AD Connector:** For hybrid (on-prem + AWS) setups.

**Setting Up SSO (Tomorrow’s Session)**

* Integrate **self-hosted AD** with AWS SSO.
* Map AD users to AWS roles.

**6. Conclusion & Best Practices**

**Key Takeaways**

✔ **Role Switching:** Securely access cross-account resources.  
✔ **Active Directory:** Centralized identity management.  
✔ **Least Privilege:** Use roles instead of permanent admin access.

**Best Practices**

* **Restrict Role Permissions** (avoid AdministratorAccess in production).
* **Enable MFA** for role switching.
* **Monitor with CloudTrail**.

**Next Session:** AWS SSO with Active Directory! 🚀