**Identity Services in Azure**

**Azure Active Directory (Azure AD / Microsoft Entra ID)**

Azure AD (Entra ID) is Microsoft’s cloud-based identity service used for authentication and authorization.

* Supports **SSO (Single Sign-On)** and integrates with on-premises Active Directory (AD) using **AD Connect**.
* Provides **RBAC (Role-Based Access Control)** for managing permissions at different levels:
  + **Owner** – Full control including permission assignments.
  + **Contributor** – All actions except assigning roles.
  + **Reader** – View-only access.

**Azure AD Plans**

Azure AD offers different plans with varying levels of features. *(Refer to Microsoft Entra Pricing)*

**Azure AD B2B & B2C**

* **B2B (Business-to-Business):** Allows guest user access (similar to IAM users in AWS).
* **B2C (Business-to-Customer):** Enables customer authentication through Azure AD apps (similar to AWS Cognito user pools).

**Service Principal in Azure**

A service principal is used to provide credentials for automation and programmatic access.

**Creating a Service Principal:**

az ad sp create-for-rbac --name "forubuntuvm" --role reader --scope "/subscriptions/<subscription-id>"

**Logging in with Service Principal:**

az login --service-principal -u "<app-id>" -p "<password>" --tenant "<tenant-id>"

Used in **CI/CD pipelines and automation**.

**Azure RBAC (Role-Based Access Control)**

Permissions in Azure are assigned using **IAM (Identity and Access Management)** at various levels:

* **Subscription Level**
* **Resource Group Level**
* **Resource Level** (inheritance applies from parent levels)

**Creating Custom Roles**

**Basic role structure:**

{

"properties": {

"roleName": "customRole",

"description": "Custom role for storage and read permissions",

"assignableScopes": ["/subscriptions/xxxxxx"],

"permissions": [

{

"actions": ["Microsoft.Storage/\*", "\*/read"],

"notActions": [],

"dataActions": [],

"notDataActions": []

}

]

}

}

**Connecting On-Premises AD to Azure**

* **Azure AD Connect** is used to sync on-prem AD with Azure AD.
* **Hybrid Identity** allows seamless integration between on-prem AD and cloud services.

**Audit & Logging in Azure**

* **Activity Log:** Tracks changes in Azure resources.
* **Azure Monitor:** Monitors logs, metrics, and security alerts.
* **Azure Security Center:** Helps with compliance and security monitoring.

**Azure CLI for Automation**

**Login to Azure CLI:**

az login

**Execute Azure CLI commands:**

az vm list

Azure CLI enables scripting for automating infrastructure provisioning.