Khóa học luyện thi chứng chỉ AWS

Dành cho Kiến trúc sư giải pháp và nhà phát triển trong 3 tuần

Đà Nẵng, năm COVID thứ 2

IAM 1

AWS Identity and Access Management (IAM)

- **IAM Resources** - user, group, role, policy, identity provider
- **Root User** - When you first create an AWS account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account.
- **IAM Users** - A user that represents an application is called a Service Account.
- **IAM Credentials** - Can be used in API calls, CLI and PowerShell.
- **IAM Groups**
  - You can add a user to a maximum of 10 groups.
  - Groups cannot be nested.
  - A group cannot be identified as a Principal in a resource-based policy.
- **IAM Permissions** - Permissions decision tree:
  - Firstly looks for explicit denies,
  - Secondly looks for explicit allows,
  - Lastly denies any action that is not explicitly allowed.

IAM 2

- **IAM Roles**
  - An IAM identity that you can create in your account that has specific permissions.
  - Has some similarities to an IAM user. Roles and users are both AWS identities with permissions policies that determine what the identity can and cannot do in AWS.
  - However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it.
  - When you assume a role, the AWS Security Token Service (STS) provides you with temporary security credentials for your role session.
  - Assuming a role = getting temporary keys to perform the actions allowed for that role.
  - While a user is assuming a role, he looses access to his original user permissions.
- **AWS Service Roles** - A service role: A role that a service assumes to perform actions in your account on your behalf.
- **AWS Service-Linked Role** - Service-linked roles are predefined by the linked service and include all the permissions that the linked service requires to call other AWS services on your behalf.

IAM 3

- **IAM Policies** - AWS supports six types of policies: identity-based policies, resource-based policies, permissions boundaries, Organizations SCPs, ACLs, and session policies.
- **Inline Policies** - Main use case for inline polices: you want to be sure that the permissions in a policy are not inadvertently assigned to an identity other than the one they're intended for.
- **Managed Policies**
  - Customer-Managed Policies
  - AWS-Managed Policies
  - Job Functions
- **Permission Boundaries** - A permissions boundary is an advanced feature used to set the maximum permissions that an identity-based policy can grant to an IAM entity.
- **Cross-Account Access**
  - Using roles for Cross-account access
  - Using Resource-based policies for Cross-account access

IAM 4

- **IAM Identity Federation** - Federated users are users (or applications) who do not have AWS accounts.
    - IAM supports IdPs that are compatible with OpenID Connect (OIDC) or SAML 2.0.
- **AWS Single Sign-On (AWS SSO)** - A cloud-based single sign-on (SSO) service focused on SSO for employees when accessing AWS services or cloud apps.
- **AWS Directory Service**
    - **AWS Directory Service for Microsoft Active Directory** - Also known as AWS Managed Microsoft AD.
    - **AD Connector** - A proxy service to establish a trusted relationship between your Active Directory and AWS.
    - **Simple AD** - Supports basic Active Directory features such as user accounts, group memberships, joining a Linux domain or Windows based EC2 instances, Kerberos-based SSO, and group policies.
    - **Amazon Cognito** - This fully managed service scales to support hundreds of millions of users.
- **EC2 Instance Profile** - An IAM role that you can attach to an EC2 instance.

IAM 5

- **Cognito User Pools** - With Cognito user pool, your users can sign up and sign in to your web or mobile app.
- **Amazon Cognito identity pools (federated identities)** - Enables identity federation to allow access to AWS services (authorization) for federated users.
  - Supported IdPs:
    - Public providers: Amazon, Facebook, Google, Apple.
    - Amazon Cognito User Pools.
    - OIDC IdPs
    - SAML IdPs
  - Auth Flow:
    - Your app authenticates to the IdP and gets a token from this IdP.
    - Your app calls GetId to Cognito Identity Pools which returns an identity.
    - Your app calls GetCredentialsForIdentity to Cognito Identity Pools which calls AWS STS on behalf of the user and returns the STS token to your app.

IAM 6

- **Amazon Cloud Directory**
  - A highly available multi-tenant directory-based store in AWS.
  - Can scale automatically to hundreds of millions of objects as needed for applications.
  - You can organize directory objects into multiple hierarchies to support many organizational pivots and relationships across directory information.
  - Examples:
    - A directory of users may provide a hierarchical view based on reporting structure, location, and project affiliation.
    - A directory of devices may have multiple hierarchical views based on its manufacturer, current owner, and physical location.