Multi-User Environments in AWS

Q. Examples:

Scenario 1: Individual Server Environments for Trainees

TechFusion Inc. could launch 30 Amazon EC2 instances using Amazon Machine Images (AMIs) that have the required software and tools pre-installed for each trainee's needs. Security Groups and Key Pairs could be used to provide secure access.

Scenario 2: Limited User Access to AWS Management Console for Sales Team

TechFusion Inc. could create IAM users for each Cloud Advisor and assign them to an IAM group with a policy that only allows access to specific services like Amazon S3 and Amazon Quicksight for report storage and visualization. This ensures that each team member can only access what's relevant to their role.

Scenario 3: Separate AWS Accounts for Each User in the R&D Team

TechFusion Inc. could use AWS Organizations to create a master account and then provision separate member accounts for each Cloud Engineer. This allows for complete isolation of resources, and with Service Control Policies (SCPs), they can enforce specific permissions.

Q: Use case:

Scenario 1: Individual Server Environments for Trainees

A coding bootcamp may use a similar approach to provide students with access to consistent and isolated development environments. Each student receives their own EC2 instance, which ensures they have the necessary software without needing to worry about conflicting versions or other students' actions affecting their work.

Scenario 2: Limited User Access to AWS Management Console for Sales Team

A real estate agency with agents across different regions might use a similar approach. Agents are given access to the AWS Management Console to manage listings and client data, but they're restricted to specific services and regions. This way, they can handle their workload without the risk of accidentally accessing or modifying other parts of the system.

Scenario 3: Separate AWS Accounts for Each User in the R&D Team

A pharmaceutical company's R&D department might employ a similar strategy. Researchers working on different drug development projects can have isolated AWS accounts, ensuring that there's no interference or accidental sharing of sensitive information between projects. Each researcher can continue working on their project without impacting others and may retain the account for future innovations and developments.

Q. Separate AWS accounts required for each user:

Scenario 1: Individual Server Environments for Trainees

No, separate AWS accounts are not required; individual EC2 instances within a single account are sufficient for the trainees

Scenario 2: Limited User Access to AWS Management Console for Sales Team

No, IAM users are created within the existing AWS account, and access is controlled through permissions policies.

Scenario 3: Separate AWS Accounts for Each User in the R&D Team

Yes, separate AWS accounts are created for each Cloud Engineer within the AWS Organization.

Q. Major steps for setup:

Scenario 1: Individual Server Environments for Trainees

- Create an Amazon Machine Image (AMI) with the required software.
- Launch 30 EC2 instances using the AMI.
- Set up Security Groups and Key Pairs for secure access.
- Provide private keys and connection instructions to the trainees.

Scenario 2: Limited User Access to AWS Management Console for Sales Team

- Create 65 IAM users for the Cloud Advisors.
- Create an IAM group and assign users to it.
- Attach a permissions policy to the group to define allowed/denied access.
- Provide IAM credentials and login URLs to the Cloud Advisors.

Scenario 3: Separate AWS Accounts for Each User in the R&D Team

- Create an AWS Organization with a master account.
- Provision separate AWS accounts for each Cloud Engineer.
- Apply Service Control Policies (SCPs) for access control.
- Share account credentials with each Cloud Engineer.

Q. Users can provision additional AWS resources, resulting in additional charges:

Scenario 1: Individual Server Environments for Trainees

No, trainees only have access to their EC2 instances and cannot provision additional AWS resources.

Scenario 2: Limited User Access to AWS Management Console for Sales Team

Depends on the permissions policy; if they are given rights to provision resources, they could incur additional charges.

Scenario 3: Separate AWS Accounts for Each User in the R&D Team

Yes, Cloud Engineers with separate accounts can provision additional resources, potentially leading to additional charges.

Q. Users have access to AWS Management Console or APIs:

Scenario 1: Individual Server Environments for Trainees

No, trainees only have access to their EC2 instances and not the AWS Management Console or APIs.

Scenario 2: Limited User Access to AWS Management Console for Sales Team

Yes, Cloud Advisors have limited access to the AWS Management Console as defined by their permissions policy, and this access could extend to APIs if allowed.

Scenario 3: Separate AWS Accounts for Each User in the R&D Team

Yes, Cloud Engineers have full access to the AWS Management Console and APIs in their separate accounts.

Q. User charges paid by the management AWS account:

Scenario 1: Individual Server Environments for Trainees

Yes, all charges for the individual EC2 instances for trainees are billed to the management AWS account.

Scenario 2: Limited User Access to AWS Management Console for Sales Team

Yes, all charges related to the IAM users and services they access are billed to the management AWS account.

Scenario 3: Separate AWS Accounts for Each User in the R&D Team

If the accounts are created within an AWS Organization, billing can be consolidated to the master (management) AWS account, so yes, it can pay the charges.

Q. Separation between user environments:

Scenario 1: Individual Server Environments for Trainees

Separation is achieved through individual EC2 instances, with each trainee having a dedicated instance.

Scenario 2: Limited User Access to AWS Management Console for Sales Team

Separation is controlled by IAM permissions, limiting users to specific services and resources.

Scenario 3: Separate AWS Accounts for Each User in the R&D Team

Full separation is achieved by creating separate AWS accounts for each Cloud Engineer within the AWS Organization.

Q. Individual user credit cards or invoicing required

Scenario 1: Individual Server Environments for Trainees

No, all charges are consolidated to the management AWS account.

Scenario 2: Limited User Access to AWS Management Console for Sales Team

No, all charges are consolidated to the management AWS account.

Scenario 3: Separate AWS Accounts for Each User in the R&D Team

Depends on the setup; if billing is consolidated at the AWS Organization level, individual credit cards or invoicing would not be required.

Q. Billing alerts can be used to monitor charges

Scenario 1: Individual Server Environments for Trainees

Yes, billing alerts can be set up to monitor charges for individual EC2 instances.

Scenario 2: Limited User Access to AWS Management Console for Sales Team

Yes, billing alerts can be configured to monitor the usage and charges for the services accessed by the Cloud Advisors.

Scenario 3: Separate AWS Accounts for Each User in the R&D Team

Yes, billing alerts can be set up for each separate AWS account or at the master account level to monitor overall charges.