Identity management in OTC Cloud

Security architecture · https://nuabee.com/documents/identity-management-otc-cloud/

Introduction

Identity and access management (IAM) is a fundamental component of cloud security systems. It enables us to control who can access which resources in the Cloud, and in what ways.

Using IAM, we have the ability to create users with finely-tuned permissions, ensuring that each individual only has access to the resources they need to perform their tasks. This approach minimizes the risks associated with unauthorized access, and strengthens the overall security of OTC's Cloud environments.

Understanding Cloud Identity and Access Management (IAM)

The Cloud IAM component is designed to offer granular control over access to Cloud resources. It allows administrators to create and manage users, groups and roles, defining specific access policies for each entity. Here are the key elements:

1. **Users and Groups**: Users are individual entities that can be assigned permissions. Groups allow users with similar access needs to be grouped together, facilitating permissions management at scale.
2. **Roles and Policies**: Roles are sets of predefined permissions that can be assigned to users or groups. Policies, on the other hand, define specific access permissions and conditions of use for resources. This enables fine-tuned control of who can do what, on which resources and under what conditions.
3. **Permissions**: IAM makes it possible to define specific permissions for precise actions, such as reading, writing, modifying and deleting particular resources. This is essential for applying the principle of least privilege, ensuring that users only have access to the resources they need to perform their tasks.

Temporary access and permissions for critical actions

At Nuabee, we have introduced a specific procedure for managing temporary access to Cloud resources, particularly for critical actions. This approach aims to reduce the risk of unauthorized access, as well as the dangers associated with performing sensitive tasks, such as deleting sensitive data or modifying security configurations.

- **Temporary Access Management**:
  - For particularly sensitive or high-risk actions, we assign temporary permissions to employees. These permissions are granted for a limited time and are designed to enable the precise execution of sensitive tasks while minimizing the associated risks. Resource usage is recorded in the cloud's log and trace management system.

- **Flexibility and security**:
  - This method enables us to maintain strict control over critical operations, while offering the flexibility needed to manage urgent interventions or planned maintenance. By limiting permissions over time, we ensure that access rights remain active only as long as necessary to complete the task, thus reducing potential risks.

- **Protecting Cloud environments**:
  - By implementing these measures, we guarantee the security and integrity of Cloud environments. This rigorous procedure ensures not only the protection of sensitive data, but also compliance with high standards of access management. In this way, we ensure that every critical operation is carried out in a secure, controlled environment.

Conclusion

Identity and Access Management (IAM) is essential for ensuring the security of Cloud environments. By using finely-tuned permissions and implementing temporary access processes for critical actions, we reinforce security while offering the flexibility needed to manage sensitive tasks efficiently.

These practices protect data and resources, while maintaining rigorous access management standards. By applying these principles, we ensure that Cloud environments remain secure and compliant with industry best practices.

To find out more: identity and access management documentation