IAM

AUTOMATION IN IDENTITY & ACCESS MANAGEMENT

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Identity and access management (IAM) is a critical aspect of information security that involves managing and controlling access to resources within an organization. Automation has become an increasingly important aspect of IAM as organizations look to improve efficiency, reduce costs, and increase security. This paper will discuss the importance of automation in IAM and how it can be used to improve various aspects of the process.

INTRODUCTION

Identity and access management (IAM) is a process that ensures that only authorized individuals have access to sensitive resources. In today's fast-paced business environment, organizations need to be able to manage and control access to resources quickly and efficiently. Automation has become an increasingly important aspect of IAM as organizations look to improve efficiency, reduce costs, and increase security.

PROBLEM STATEMENT

Manual processes in IAM can be time-consuming and prone to errors. This can result in decreased efficiency and increased costs for the organization. In addition, manual processes can also increase the risk of security breaches, which can be costly in terms of both financial and reputational damage.

SOLUTION

Automation in IAM can help organizations to improve efficiency, reduce costs, and increase security. Automating repetitive tasks, such as provisioning and de-provisioning user accounts and accesses, can save significant time and resources, especially in large organizations with a high volume of users. Automating these tasks also ensures consistency and accuracy, reducing the risk of human error. For example, implementing Role Based Access Controls ensures that employees within the organization has the right access during onboarding and can effectively remove access when employees leave the organization thus reducing security risk of ungoverned accesses.

IAM/IGA tools also have the capability to monitor what access each user within the organization has provide alerts and send violations to respective personnels. Using compliance management and governance supervisors can effectively control whether subordinates reporting to them have the right access. For example, these tools provide automation to launch access review campaigns and detect separation of duties (SOD) violations where supervisors can take actions on each of their subordinates' access.

IAM/IGA tools also include the ability to monitor and detect potential security threats by implementing different governance policies and zero trust policies. These systems can be configured to automatically detect and respond to potential security threats, such as unauthorized access attempts. This can help organizations to detect and respond to potential security breaches more quickly, reducing the risk of damage to the organization. For example, using IAM tools organizations can implement single sign on and detect any abnormal behavior patterns prompting additional authentication factors.

USE CASES:

Implementing Zero Trust with IAM

- **Identity Verification:** Users in an organization must be verified before they are granted access to the network and its resources. Verification processes like Multi–factor Authentication (MFA) such as password, biometrics or a one-time code sent to mobile devices.

- **Limiting Privileged Access:** Accesses that can modify a system or that gives access to sensitive data within an organization can be categorized as Privileged access. Implementing strict SOD policies, leveraging PAM (Privileged Access Management) tools to continuously govern privileged access will help organizations limit the level of access an employee needs to perform their job functions.

- **Continuous Monitoring** – Implementing functionalities that govern user access and activities that will allow an organization to pro-actively detect and respond to suspicious activity and anomalies.

- **Access Controls** – Automating access controls through the principles of Role-based access control (RBAC) or attribute-based access control (ABAC) will allow an organization to define fine grained access policies based on the user's identity which allows the organization to ensure only the right necessary access are being granted to the user.

Implementing Compliance and Governance

Implementing compliance and governance in Identity and Access Management in an organization involves creating processes and procedures to ensure that the organization's IAM system adheres to relevant laws, regulations, and industry standards. Identification of laws and regulations is a prerequisite to developing a solid IAM Governance structure that will ensure the organization is always ahead of compliance requirements.

With a complete understanding of the compliance an organization needs to comply to, a solid access governance structure can be built which will allow the organization to continuously monitor access, periodically run Access Reviews which will help the organization to remain compliant with the industry standards.

Automating Life Cycle Management of Employee

Automating the lifecycle management of employees in an organization requires automating an entire lifecycle of an employee starting from their initial onboarding, transfer within the organization, rehires to the termination of an employee. IAM tools allow organizations to automate these lifecycles by implementing the functionalities below.

Employee Onboarding (Joiners): When a new employee joins the company, a process can be put in place to automatically provision their email, network, and other IT accounts, as well as assign them the appropriate roles and permissions in various systems. This can be done using an identity and access management (IAM) system that integrates with other IT systems and applications, such as HR and payroll software.

Transfer within an organization (Movers) : When an employee changes roles or departments within the company, their access to various systems and applications should be updated accordingly. This can be automated using an IAM system that integrates with other IT systems and applications and allows for the automatic assignment and removal of roles and permissions.

Termination (Leavers): When an employee leaves the company, their access to various systems and applications should be revoked to ensure the security of the company's data. This can be automated using an IAM system that integrates with other IT systems and applications and allows for the automatic removal of roles and permissions.

Rehires: When an employee returns to the company after leaving, their access to various systems and applications should be re-provisioned. This can be automated using an IAM system that integrates with other IT systems and applications and allows for the automatic assignment of roles and permissions.

Implementing Role Based Access Control

Organizations today have access to many different applications and systems that are necessary for providing better customer satisfaction. However, managing access without implementing compliance and governance policies can pose security risks and threaten data privacy. Automation is becoming increasingly important in data and access management because it is less prone to error than manual management. Many organizations are also moving towards using cloud-based platforms, which means they don't have direct control over their data. Implementing a centralized IAM (Identity and Access Management) and IGA (Identity Governance and Administration) platform allows organizations to effectively manage their data and the access associated with users.

One of the main challenges organizations faces is controlling access, which is where Role Based Access Control (RBAC) comes in. RBAC is a method of regulating access based on the roles of individual users within an organization. In this model, roles are created for various job functions and a set of permissions is associated with each role. Users are assigned to one or more roles, and through those roles, they are granted access to the resources they need to perform their job functions.

Within RBAC, Role Engineering is the process of implementing and maintaining access control associated with roles. There are three main approaches to role engineering: Top-down, Bottom-up, and Hybrid.

In the Top-Down approach, roles and access controls are designed at the highest level of an organization and then implemented in a hierarchical manner, which is best for organizations with a clear chain of command and well-defined roles and responsibilities.

In the Bottom-up approach, roles and access controls are designed at the lowest level of an organization and then implemented in a hierarchical manner, which is best for organizations with a more decentralized structure or where roles and responsibilities are less well defined.

The Hybrid approach combines elements of both the top-down and bottom-up approaches. It starts with a top-down approach to identify high-level roles and responsibilities, and then allows for more granular roles and access controls to be defined at lower levels of the organization. This approach is commonly used as it provides a balance of centralized and decentralized controls and allows for more flexibility in implementing roles and access controls.

CONCLUSION

Automation in IAM can provide significant benefits to organizations in terms of efficiency, cost savings, and security. Automating repetitive tasks, such as provisioning and de-provisioning user accounts, can save organizations time and resources, while also ensuring consistency and accuracy. Automating access management can help organizations to manage access to resources more effectively, while also reducing the risk of unauthorized access. In addition, automating the detection and response to potential security threats can help organizations to detect and respond to potential security breaches more quickly, reducing the risk of damage to the organization. Real-world examples show that companies that have implemented automation in their IAM process have seen significant improvements in their processes. Automation should be considered as a key aspect of any organization's IAM strategy to achieve optimal results.