International Journal of Management, IT & Engineering
Vol. 13 Issue 02, February 2023,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Identity and Access Management System

Prasantha Kumar Kondakagari
Sr. IAM Consultant & Department of Computer Science

Abstract **-**The importance of this article is to examine what is key role is playing Identity and access management in organizations/enterprises. IAM is a set of tools and technologies to change a user's access during the user on boarded and off boarded and monitor user activities and privileges to a variety of cloud and on-premises applications. In the organization, all the users, including employees and non-employees, suppliers, and partners, should follow the core IAM systems policies and processes once identity and access management are established. The importance of the IAM in today's global workforce is complex. The different access requirements and the interconnected needs to keep the workforce effective. After increasing internet usage, all the user information is exhibited to the internet, and there are high chances of attacking secure information like usernames and passwords. To protect the organizations/enterprise, the IAM one identity should be in place.
Keywords – Identity and Access Management System, IAM Tools, Top IAM Tools, Cyber Security.

1. Introduction

In the current world, data is being accessed and shared outside of the companies to protect their information outside the company's walls; the old-fashioned way of securing credentials and sensitive information is impossible.Many IAM tools are in cloud and on-premises applications that will onboard and offboard users and system access to the organization fully automated without human involvement.The traditional way identity is maintained by the companies trusted to secure their information in their data stores. Organizations have many applications that users need to access dailyfor their duties.So grating the access to the induvial application, it's very pain full job and lot of human work.

2. List of IAM Tools in the Market.

- SailPoint
- Ping Identity Intelligent Identity Platform
- Okta
- Azure Active Directory
- ForgeRock
- CyberArk
- One Login

All the above IAM tools are essential in the market at present, and below are activities that will do the above IAM tools.

Provisioning

When the user is in the organization, create the identity, and define their access privileges automatically based on their job code, department, or cost center.

De-provisioning

Once the user is terminated from the organization, it removes the entire identity cube of the terminated user**.**

Lifecycle State of Identity

Based on the LCS, the identity is set provision, de-provision identity access, and syncs the attribute's value. The LCS status is prehire,active, onleave, suspended or terminated. The LCS changes based on the organization.

Password

Passwords are a time-honored cornerstone of computing security. Good password policies, education, and enforcement can help make passwords themselves more effective; the tools used to facilitate password management may introduce additional attack surfaces. All the above IAM tools' password management services have a security infrastructure strong enough to ensure that credentials are never exposed to attackers. It will have additional checks using Multi-Factor Authentication (MFA)when we log in using the username and password. The

MFAdoes the extra step of sending the code viaSMS tothe phone or entering the code from authentication apps face deduction or biometrics.

Roles-Based Access Control (RBAC)

In IAM,RBAC'sidea of assigning permissions to users based on their role with an organization. For example,the user works in the Finance department based on his cost center, or the department grants access to the user. Suppose the user transfers from one department to another department. In that case,the access automaticallyrevokes the existing access and assigns new department access based on the RBAC setup in the IAM tool.

The benefits of RBAC are that the access becomes systematic and repeatable, and it is easier to audit user access and remove unwanted access.

Single sign-on

User access to the application is controlled through an authentication process in which the user's sign-on credentials are validated against an authentication source. One set of login credentials can be used to access multiple applications. Theprimarytools for Single Sign-on DUO, OKTA, Ping, OneLogin SSO,etc.. using these tools IT Administrationand security team benefits,and SSO reduces the risk of lost or weak passwords as well as evaluates associated with managing account access.

Context-Aware Security

Restrict the sign-in permitted for users based on the below-configured restrictions.

- IP address blocks that define your network to prevent access from off-network IP addresses.
- A Block List to prevent user access from specified countries.
- Detects any requests for access that occur outside of customary times and days for the user
- An Allow/Whitelist List to permit user access only from specified countries.

Access Management

In the organization, people control user validation and resource access based on their job roles, identity, and access management. The right digital resources at the right time and for the right reasons**.**

Entitlement/Groups

Based on the target IAM connected, we call different names like entitlement,privilegesgroups, or memberOf in Active Directory, but all these entitlements, privileges groups, or memberOf the specific or grant the access connected target system.

Email Notifications

When the user is onboarded, offboarded, password reset, or forgets password inthe organization IAM system triggers the email notification ina timely manner.

Certify the Access

Certification is the process that allowsreview of the access that has users in the organization. These certification reviewers are source owners, Managers, or entitlement owners. The certifiers determine whether the access is appropriate for those users or should be revoked.

Challenges in identification access management implementation

Integration - Integrate across all the organization applications into the central system and,from there,automatethe Onboarding and offboarding of users and users'self-service. In the organization, multiple application, and each application have a different way of grating accesslike Excel spreadsheets (manual activity), JDBC, SAP, Salesforce, and workday, etc..,application. When we want to integrate all these different kinds of database applications and integrate it into one identity, the correlation part is the most difficult the reason; eachapplication Correlation refers to the process of correlating, or combining, all of the information discovered by the IAM tool to create and maintain the single identity Cubes.

Birthright access

Birthright access plays a significant role in automating access when users are onboarding and offboarding. To define in such a way,RBAC requires a variety of principles and tools to analyze, design, and create for different job functions across the

organization and distribute to each user based on his/her responsibilities and qualificationsis a very difficult job for adminsat the initial design stage and it is much time taken.

Key benefits of IAM for Business/Organization.

Reduce the admin time

After implementing the IAM, the administration cost and time willbe reduced to 90%; the reasons areon and offboarding, password expiration update and reset, and access and approval processare automated, and one IAM system will handle all the identity process if anything goes wrong it is easy to trace. Before the IAM solution, all these activitiesare donemanually by the admin team or by the script for induvial applications.

Reporting for Audit/Management

With IAM,it is possible to get the in-build report, or a little customization report can be built and sharedwith the organization's colleagues or customers safely and securely. Foraudit purposes,it is a convenient review.

Saves the service cost

Mainly, there are two ways to reduce the cost of the service; to provide access to each application in the organization,the cost of the induvial infrastructuregetsreduced with one IAM system, and it reduces helpdesk/servicedesk costonce it isautomated all the on and offboarding process.

Full security for companies

The IAM tools simplify authentication and authorization, particularlyregarding identities that access internal or external networks. The companies can set up SSO,whichallows for multi-factor authenticationand restricts the sign-in permitted for users-based network IP addresses and Whitelist lists to permit user access.

Improve Compliance

Every organizationrequires strict access controls. TheIAM central system helps you to keep all identity credentials and log-in details in one place to streamline.

Centralize Log

All the IAM tools automatically generate logs, and these logs will useby companies for their compliance requirements and audit usage, and these logs can store in the cloud as well so that often a more convenient and affordable way to access in online anywhere the market there are many online logs storage software like Splunk, Datadog, BusinessLog, etc.,

Conclusion

Modern enterprise requires an in-depthapproach to organization security, visibility, and control over users, applications, and data, along with their relationships,to make identity. Access managementcan significantly improve how its business is operated, managed, and implemented.Users and customers will work comfortably for their workwithout any multiple tasks.
(like SSO, Password). We connect different kinds of applications daily with the organization; for that reason, security and safety must be there with IAM tools.

References

[1] J. Balmer and S. Greyser, "Managing the Multiple Identities of the Corporation", California Management Review, vol. 44, no. 3, pp. 72-86, 2002.

[2] R. Scherer and G. Cheney, "Rhetoric in an Organizational Society: Managing Multiple Identities", Sociological Analysis, vol. 53, no. 1, p. 111, 1992.

[3] J. González, M. Rodríguez, M. Nistal and L. Rifón, "Reverse OAuth: A solution to achieve delegated authorizations in single sign-on e-learning systems", Computers & Security, vol. 28, no. 8, pp. 843-856, 2009.

[4] G. Larson and G. Pepper, "Strategies For Managing Multiple Organizational Identifications", Management Communication Quarterly, vol. 16, no. 4, pp. 528-557, 2003.

[5] C. Zang, Y. Fan and R. Liu, "Architecture, mplementation and application of complex event processing in enterprise information systems based on RFID", Information Systems Frontiers, vol. 10, no. 5, pp. 543-553, 2008.

[6] D. Bates, "The Athens Access Management System", SSRN Electronic Journal, 2001.

[7] Yang Yan, Chen Xingyuan, Wang Guangxia, Ca o Lifeng "An Identity and Access Management Architecture in Cloud " in Computational Intelligence and Design (ISCID), 2014 Seventh International Symposium on, 2 (13-14) (Dec 2014), pp. 200-203