Identity and Access Management: IBM Stack Tools

Aayushi Dubey[1], Pronika Chawla[2], Dr. Madhumita Kathuria[3]

[1]Student, Department of Computer Science &Engineering, Manav Rachna International Institute of Research and Studies, Faridabad, Haryana, India
[2]Assistant Professor, Department of Computer Science &Engineering, Manav Rachna International Institute of Research and Studies, Faridabad, Haryana, India
[3]Assistant Professor, Department of Computer Science &Engineering, Manav Rachna International Institute of Research and Studies, Faridabad, Haryana, India

---***---

Abstract—*Securing workplace and workstation is the first and the foremost thing we do. Data which is the most valuable asset of any company or individual has to be protected at any cost from internal and external threats. Hence, there is a need for trusted, highly secure and long-lasting tools to manage who is having access to the system. Identity and access management is the section that deals in this domain. In this paper we have tried to cover how IBM security tools help in providing identity and access management.*

Keywords—Secret, Privileged Account, Role Based Access, Single Sign-On, Multi-Factor Authentication

1. INTRODUCTION

Cyber security is a highly demanded sector of IT. Every person, organization or institution whether big or small needs to secure the system(s) they're working on. Hence, they need a secure and trustable solution to apply. IBM is a leading name that offers security services to customers. It has customized tools for every section of security namely, identity management, access management, risk analysis and management, compliance and auditing, vulnerability detection and assessment, penetration testing and many more.

1.1 IDENTITY AND ACCESS MANAGEMENT

Identity [1],[2] and access management or IAM in simple terms mean managing every user who has access to the system. The access is provided only to genuine users and what the user can access in the system is also pre decided. IAM constitutes everything that helps in the management process from business processes to latest secure technologies, effective policies and capability to manage identities whether electronic or digital. When a user is entitled to perform his job, he is assigned a role. Based on this role, his identity is created, and access is granted. We also call this role based access. IAM constitutes different functions and procedures broadly classified into authorization, authentication, user management and maintaining central user repository i.e., user information.

Access means a user being able to view, create or make adjustments to a file. To provide a user, access to the system, roles are defined. The definition is based upon job position, authority, tasks that the user has to perform based on his job profile and other responsibilities.

IAM uses Single sign-on, two factor or multi factor authentication and privileged access management (PAM), it provides secure storage for identity and other related data. It ensures only genuine data is shared and provides data governance feature.

Functionalities such as single sign-on, multifactor or two-way authentication and privileged access management (managing special accounts) are present in tools and setups or systems used for IAM. It is also capable of storing identities and profiles and supervise the different methodologies by governing the different setups, tools, managements, performance and work assigned and performed. It also governs on sharing of data and ensures only necessary data is exchanged. IAM systems can be deployed on systems in offices or on cloud

1.2 IDENTITY MANAGEMENT

Identity [3] of each user is unique. Whenever a user logs into the system, the system needs to see if the login is genuine. Identity management is managing the users who have access to the system in any level. Following are the points that explain identity management in detail.

- Managing "who has access to what"
- Focused on managing **users** and their **access**
- Usually involves **reconciliation** and **provisioning**
- Users = **people** or **identities**; employees, contractors, customers. Users normally reside in a repository – HR system, directory, AD etc. Repository often hold attributes of users – job code, position code, manager, office location etc

and can be used for role based and attribute based provisioning.

- Access is the **accounts** and **access rights** on target systems
    - **Accounts** will include logon id and password, and other account attributes
    - **Access rights** may be account attributes (e.g. AUDITOR flag) or group membership (e.g. AD group) or it might be permissions and rights to access a resource (e.g. READ Sales Report)
- **Roles** are used to simplify identity management
- It includes workflow for review/approval of access requests

1.3 IDENTITY GOVERNANCE

It is focused on ensuring there are **processes** to control "who has access to what". It includes:

- Risk Policies: Separation of Duties (SoD), Sensitive Access (SA)
- Processes for managing risk, including mitigations
- Business activities defined as the auditor view of job functions, "Purchase Order Create" & "Purchase Order Approve"
- Recertification (or attestation) to periodically review access of user, how roles are defined and risks and risk mitigation.
- Reporting

Business processes impacted by the Identity Governance solution are listed as follows:

- User creation, user termination
- User assignment to organizational units
- Role lifecycle management
- Role creation, removal, and consolidation
- Role assignments
- Access lifecycle management
- Identity reconciliations such as users, attributes, application permissions, accounts
- Segregation of Duties (SoD) and Sensitive Accesses (SA) management
- Mitigations of risks
- Periodic risk analysis
- Role delegations
- Periodic recertification

1.4 ACCESS MANAGEMENT

Essentially [4] an IT and data governing process, access management is used to provide access to authentic users and bar inauthentic users.

AM is used in combination with IAM. While identity management creates and manages users, roles and policies, AM makes certain that these are followed. So, an AM based system is responsible for storing user roles and profiles that are created in IM. When a user makes request that is valid, it is checked that the request is coming from an authorized user, its authenticity is checked, and access is granted or denied based on the profiles, roles and policies stored in AM systems.

1.5 PRIVILEGE ACCOUNT AND ACCESS MANAGEMENT

PAM is required specially for the purpose of managing special, privileged accounts. These accounts are powerful and meant to perform important jobs. PAM also needs identity and access management to authorize and authenticate its users and can be considered as a domain of IAM.

It manages accounts and passwords, through features like credential managements and account governance. Fig. 1 shows the privileged users:

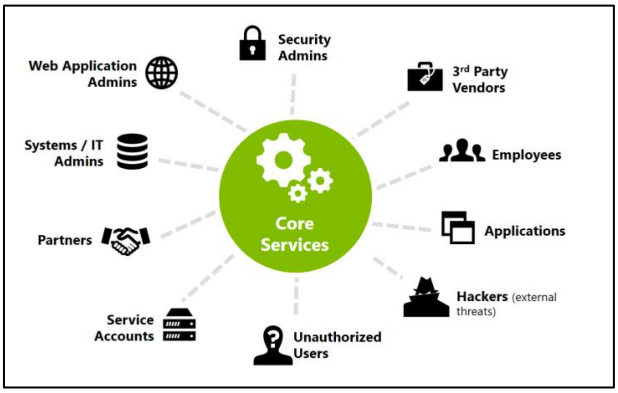

Fig.1: Privileged Users

2. IBM STACK TOOLS

IAM being an important part of security has various requirements based on the description. IBM is one of the leading service providers in the field of security and provides a set of full-fledged tools that fulfil the requirement. Fig. 2 shows the market share of IBM. This section contains description of three main tools that are designed specifically to tackle identity and access management. IGI for identity governance and management, ISAM for access management and ISSS for managing special and privileged accounts.

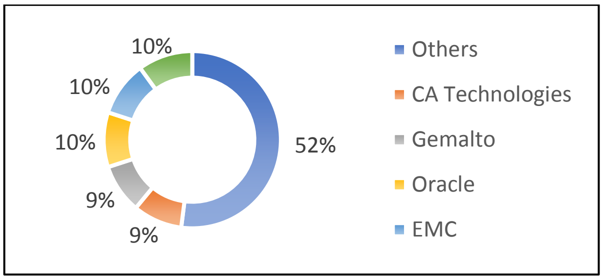

Fig.2: IBM Market Share

2.1 IBM IDENTITY GOVERNANCE AND INTELLIGENCE (IGI)

IGI [5],[6]enables corporations to set rules that manage user access and perform risks management. This is done by describing rules and policies suitable to business, on how governance shall take place. It also decides who is authorised to perform these duties (project leads, managers, risk managers, admins, auditors, etc.) across different business areas in applications and services.
Features [7] of IGI:

- Powerful identity analytics:

  Follows the path of very strong identity analytics to determine risks related to unauthorized users. It helps in access optimization giving crucial visual perception on unsafe users and behaviour and allowing better user control for role mining and modelling.

- End to end user lifecycle management:

  Reducing the need for manual labour by streamlining access management and automating lifecycle process. It helps to manage roles, multiple workflows and passwords, and offers application adapters for the cloud and on-prem.

- Integration with privileged account management products:

  Manage and control all identities, including privileged identities and entitlements, certification, delegation and separation of duties.

- Helps in auditing and compliance

- Reduce business risk (separation of duties control) and operational costs

- Enhanced password synchronization:

  Complete analysis of password management secures the end user experience, using password synchronisation, reverse password synchronisation and desktop password reset assistant (DPRA).

The IGI architecture (Fig. 3) has three basic components- IGI server, adapters and connectors and data store. The main server provides interfaces namely, admin console (for admins) and service centre for user interaction. Adapters and connectors are used to load user identities and other user information from external sources. Adapters can be agent less or agent based and they provide provisioning and reconciliation. Data stores divided into database and directory store data, roles and policies.

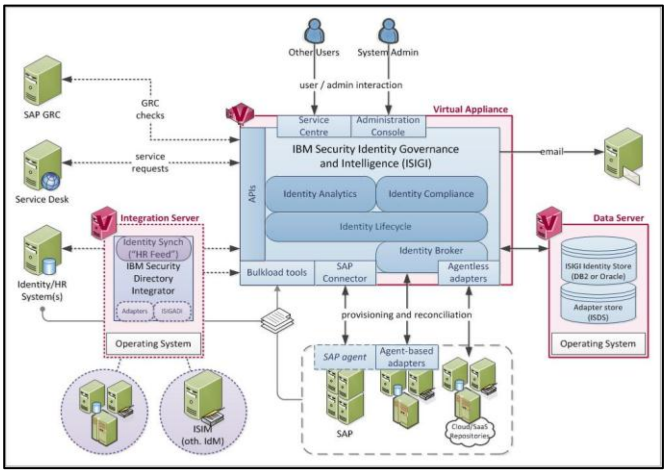

Fig.3: Identity Governance and Intelligence Architecture

2.2 IBM SECURITY SECRET SERVER (ISSS)

ISSS [8] works particularly for privileged and special or undetected accounts. It shields those accounts from unauthorized access by hackers and other form of internal and external threats, follows developing regulations and allows authorised access to users. Access can be to the system, accounts, networks, servers, database, etc. based on the job profile of the user (user profile), rules, regulations and policies. It prevents malicious applications from invading the environment by detecting, managing and auditing privileged accounts and controlling the accounts run on endpoints and servers.

Secret: it can be considered as the smallest unit of secret server and is defined as the information stored and managed within secret server. It consists of privileged passwords on routers, servers, applications and devices. Storage of key files, SSL certificates, license keys, network documentation, MS word or excel is also possible. Features [9] of IBM Secret Server:

- Discover, monitor and manage privileged, shared and service accounts

- Protect and manage passwords:

  Provides an option to set a time period to change passwords automatically. Provides encryption to assist secure management.

- Session management/ monitoring feature:

  Every activity performed by the user can be recorded and viewed as per routine. Session recording records a video of ongoing session accessed by the users and keeps a track of every operation performed by them. Remote sessions can also be recorded. It also offers the service of keystroke logging where everything entered by the user is saved in logs for future reference or in support of security.

- Role based access control is where domain admins can manage what users can and cannot do by assigning them different roles

- Used distributed engines(large in number):

  Helps to locate and control unlimited networks and special (privileged/ non privileged) accounts present on end points.

- Integrates with many IBM Security solutions like IGI and cloud to provide authentication features (SSO, MFA).

- Automation, Discovery, Auditing and Reporting, Compliance, Approval Workflow, Disaster Recovery.

- ISSS provides the strongest encryption available for password management software which is AES 256-bit encryption. It can be used with other features provided by IBM, HSM or DoubleLock to keep passwords more secure.

The secret server platform (Fig. 4) is mainly designed in such a way that it discovers privileged accounts successfully. Secrets are created for different tasks that are performed by admins. Users in discovered accounts can also access the sessions. The platform has launchers (remote desktop, web and custom launcher) to manage sessions other than the current one on the platform.

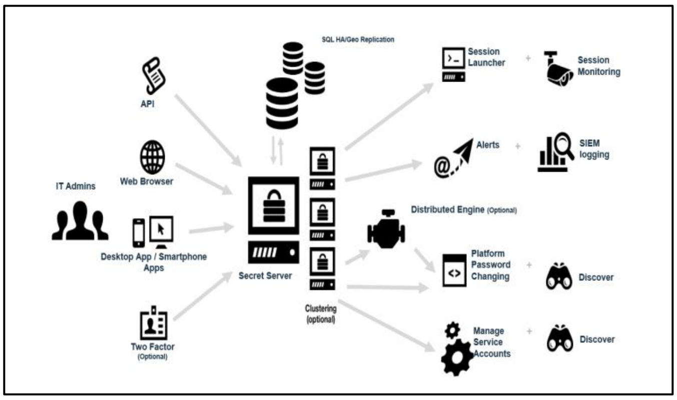

Fig.4: ISS Architecture

2.3 IBM SECURITY ACCESS MANAGER (ISAM)

ISAM [10] ensures delivery of access management to organisations for digital transformation without risking security. It administers risk based policies to give minimum friction while authentication to a known user, and multi-factor authentication if there is a risk. Its purpose is to provide secure communication between clients and servers on the web.

ISAM comprises of web, mobile, and cloud access management, multi-factor and risk-based authentication, web application protection and identity federation. It can be deployed on work location (premises) or on cloud. Features [11] of IBM Security Access Manager (ISAM):

- Provides identity federation that helps to reduce password memorization, forgetting password and other relates issues by offering single sign-on facility. It therefore builds a bridge to integrate the infrastructure to other outside or third-party applications. Single sign-on can be achieved without any mess through your laptops and phones.

- Multifactor Authentication:

  To increase security of your working devices and to protect it from unauthorized access, multi-factor authentication is provided that allows or denies user requests. The criteria may vary depending on geographical locations, IP address restrictions, data requested, etc.

- Establishing risk-based access:

  Risk based access can be achieved through regular auditing, compliance and logging of user entries, threat discoveries, monitoring unauthorized and unauthentic access. ISAM's risk-scoring engine helps in achieving this feature. Since logs are maintained and checked and user access and working information is also maintained, providing risk base access becomes easier.

- user-friendly authentication (password free authentication) like multi or two factor authentication, OTP system, email verification secret questions.
- Web seal acts as a reverse proxy between client and server
- All requests are passed through web seal
- Provides extra layer of security
- Load balancing between multiple instances

ISAM architecture has three basic components: Advanced Access Control, Federation and IBM Access Manager. The access manager is the main platform where we manage user access. It has provisions to create reverse proxies, federation and manage mobile applications from a single platform. Authentication is done by referring to the database that stores user credentials. ACL, POP and other policies can be generated that are used in order to provide authorization to the users when they want to access resources on server. It can provide both authorized and unauthorized access as maintained in the settings. Both processes take place at WebSEAL.

WebSEAL acts as a reverse proxy and provides a security layer between the client or user on internet wanting to access servers on web. The identity of servers and client is hidden by the reverse proxy to provide security. Apart from this is acts as a center for authentication, authorization, federation, etc. When user wants to send a request, WebSEAL first authenticates the user and check what authorization or rights the user holds. These are stored in databases and directories. If the user is genuine, the request is sent to the demanded server by hiding the actual information about the client, server processes the request and responds which is again handled by the WebSEAL to hide the server information before providing it to client otherwise it shows an error page. Fig. 5,6 describe the architecture of ISAM and web proxy.

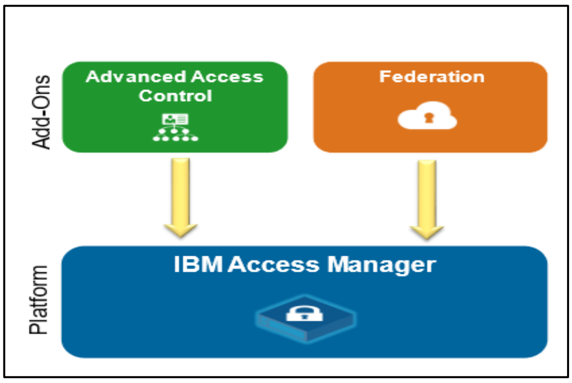

Fig. 5: ISAM Architecture

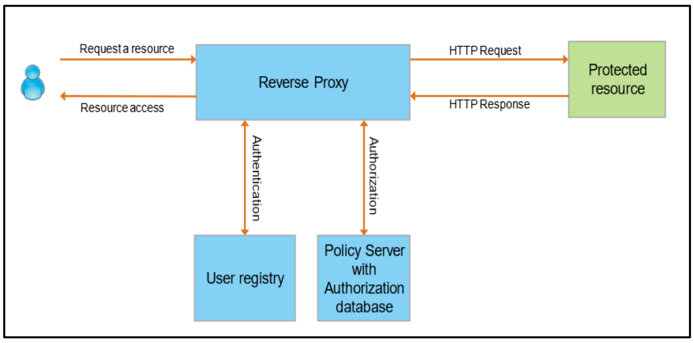

Fig. 6: Web Proxy

2.4 SOFTWARE SPECIFICATIONS

1) IGI

- **Virtual machine monitor-** VMWare, Red Hat KVM
- **DB2 Enterprise** Server Edition- version 10.5
- **Oracle Database** 12c Release 1- version (12.1.0.0.0) Standard Edition, (12.1.0.0.0) Enterprise Edition

2) ISSS

- **Operating system**: Windows (32 or 64 gb), Mac
- **Microsoft SQL Server Enterprise Edition-** version up to 2017 and future fix packs
- **Microsoft SQL Server Standard Edition-** version up to 2017 and future fix packs
- **Microsoft .NET Framework-** version up to 4.7 and future fix packs
- **Microsoft Internet Information Services (IIS)-** version up to 10.0 and future fix packs

3) ISAM

VIRTUAL APPLIANCE:

- Supported hypervisors, databases, user registries, and browsers. The general minimum requirements for the virtual appliance are:
- **Disk space requirement:** 100 GB
- **Memory requirement:** 4 GB
- **Virtual network devices:** 1 (Maximum 8)

WebSEAL

- Relies on a number of client characteristics that are either not defined or are loosely defined by RFC 2616 and RFC 7540.
- Examples of such characteristics include Cookie management, SSL support, Concurrency of multiple connections, widely used browsers such as Firefox, Chrome, Safari, and Internet Explorer support such characteristics during typical use.

2.5 HARDWARE SPECIFICATIONS

Table-1: Hardware Specifications

	IGI	ISSS		ISAM
		WEB SERVER	DATABASE SERVER	
DISK SPACE	At least 100 GB free hard disk space	25 GB	100+ GB	960GB solid-state drive
PROCESSOR	CPU: Minimum 2.2 GHz, four cores (64-bit)	4CPU Cores	8 CPU Cores	IntelXeon Processor E3-1275 v5, 8M Cache, 3.60 GHz
MEMORY	Minimum 16 GB system (DB2 and Oracle); minimum 24 GB system (internal database).	16 GB RAM	16 GB RAM	64GB
NETWORK	-	adapters, drivers, protocols		6 * network ports

3. SCOPE OF FUTURE ENHANCEMENTS

IBM acts as a service provider where it offers interested clients the desired products that suit their requirements. IBM specific tools are exclusive and not available in the market as open source products that could be downloaded easily by anyone. It must be requested and purchased.

IBM tools are expensive and thus it is preferable to provides service to a large-scale company. A normal user will not generally prefer to purchase a tool when he has options available on the internet by other companies to fulfil the exact requirements.

Since, IBM is a trusted company and provides best security solutions, people want to use its products. Hence, in future, IBM should let out products that are more suited for small scale firms and people who can’t spend enough money. If it is possible, products could be made open source.

4. CONCLUSION

The paper is about implementation of training I went under in the internship at IBM. Being a security analyst intern, I was trained on the Identity and Access Management domain of security. It describes three basic tools that are implemented for identity management and governance and access management namely, IGI, ISSS and ISAM.

ACKNOWLEDGEMENT

The successful realization of the paper is an outgrowth of a consolidated effort of people from desperate fronts. I am thankful to **Mrs. Pronika Chawla** (Assistant Professor) and **Dr. Madhumita Kathuria** for her variable advice and support extended to me without which I could not be able to complete my paper for a success. I am also thankful to our manager **Mr. Vishal Mittal** and all other **technical and project mentors** at **IBM** for training me on the tools without which I could

not have started this paper.

REFERENCES

[1] Mayuri Dhamdhere, Sridevi Karande, "Identity and Access Management: Concept, Challenges, Solutions", *International Journal of Latest Trends in Engineering and Technology*,vol.8, issue1, pp.300-308

[2] SharilTumin, Sylvia Encheva, " A Closer Look at Authentication and Authorization Mechanisms for Web Based Applications" presented at the conf of Recent Researches in Applied Information Science, January 2012

[3] Mumina Uddin, David Preston, "Systematic Review of Identity Access Management in Information Security", *Journal of Advances in Computer Networks*, vol. 3, No. 2, June 2015, pp.150-156

[4] Manav A. Thakur, Rahul Gaikwad, "User identity and Access Management trends in IT infrastructure- an overview", presented in 2015 International Conference on Pervasive Computing (ICPC)

[5] IBM Security Identity Governance and Intelligence. [Online]. Availabe- https://www.ibm.com/products/identity-governance-and-intelligence

[6] LindembergNaffah Ferreira, Ariadne de Fátima Soares Raimundo, KêniaTatiane Vieira do Amaral, "Identity management: A comparative approach", presented in 2013 47th International Carnahan Conference on Security Technology (ICCST)

[7] IBM Security Identity Governance and Intelligence. [Online]. Availabe- https://www.ibm.com/products/identity-governance-and-intelligence/details

[8] IBM Security Secret Server. [Online]. Available- https://www.ibm.com/products/secret-server

[9] IBM Security Secret Server. [Online]. Available- https://www.ibm.com/products/secret-server/details

[10] IBM Security Access Manager. [Online]. Available- https://www.ibm.com/in-en/marketplace/access-management/details

[11] IBM Security Access Manager. [Online]. Available- https://www.ibm.com/in-en/marketplace/access-management