SINGIDUNUM UNIVERSITY

- MASTER DEGREE PROGRAM -

Contemporary Information Technologies

- STUDY OPTION -

Information Systems Security and Digital Forensics

Securing the era of digital transformation

- Master's thesis -

Mentor: **Student:**

prof. dr Mladen Veinović ***Marko Tmušić***

Mandatory exams:

Scientific Research Methodology, prof. Mladen Veinović, PhD

Advanced Computer Systems, prof. Aleksandar Jevremović, PhD

Research paper, prof. Mladen Veinović, PhD

Student Internship, prof. Mladen Veinović, PhD

Master's thesis, prof. Mladen Veinović, PhD

Elective exams:

Generation and Distribution of Cryptographic Keys, prof. Mladen Veinović, PhD

Digital forensics, prof. Marko Šarac, PhD

Belgrade, 2018.

Securing the era of digital transformation

Abstract:

In this paper, the concept of identity and access management is presented. Detailed insight in the field of research shows the modern approach in respect to IT security principles and describes importance and a significant impact that identity and access management have regarding IT security and business ecosystem. IBM security solution is presented with detailed explanation of its structure, functionality and benefits.

An insight will be presented into the transformation of the digital business world, challenges that face companies, moving forward to new technologies and shifting the focus to agile and flexible environments.

Rise of the new security standards and the impact they have on the financial sector as well as the importance of digital forensics will be presented. The significance and benefits of API Economy, its future heading together with the security solution that facilitates secure APIs will be highlighted. The usefulness of the cloud-based access management solution for protecting cloud assets will be accentuated.

Keywords:

IT Security, Access management, API protection

Contents

1 Methodology

1.1 Introductory remarks

In this paper, the concept of identity and access management is presented. Security solution is presented with all functionalities and additional modules for federation and advanced access. New security standards and data protection regulations in relation to the financial sector will be described.

Digital business is a dynamic environment, technologies are changing swiftly, organizations have new ways of work, implicating the information security risk as a top concern. Robust identity and access management can protect the whole business ecosystem, implement advanced authentication and authorization techniques, provide monitored environment, assist in complying with regulatory standards, boost the business and employee productivity, integrate various applications and significantly improve user experience.

This paper will have a detailed scope of technologies, mechanisms and scenarios that IBM Security Access Manager solution can provide. The importance of having a business environment that can respond to all business needs and at the same time deal with challenges swiftly will definitely make a difference.

1.2 Subject of the research

The subject of this research is the impact that identity and access management have on information security and business productivity inside corporate system. Different scenarios, challenges and benefits of implementing IBM Security Access Manager solution will be presented. Necessary information security methodologies, standards and regulations will be accentuated along with their impact on corporate infrastructure.

1.3 Hypothesis

Holistic approach to information security is crucial in creating a multi-layer in-depth security present in every aspect of corporate infrastructure, protecting corporate resources, federating them with partner resources and making them easily accessible and available on different platforms and devices.

The cognitive era is arriving and the only business models which are agile, adaptive and secured will have the ability to successfully run a business and have a desired outcome. Rise of identity and access management will have a great impact on businesses and become essential part of IT security.

1.4 Research objectives

Research objectives include the comprehensive research on security solution, benefits from having such security solution implemented in corporate system and resulting impact on overall business ecosystem.

1.5 Scientific methods

In process of creating this paper, various science methods of description, induction, analysis, synthesis and generalization are used. Method of description was used in explanation of concepts, terms and functionalities.

Inside theoretical segments methods of induction, deduction, analysis was used and inside conclusion methods of synthesis and generalizations were used.

2 Introduction

As the global digital economy grows, the number of digital identities rises. With it, the need to protect and manage how personal information is collected, used and distributed is higher than ever. Digital identities are the key factor in online world and finding the proper way to authenticate the legitimate users is the greatest challenge. When digital identities are not secured or distributed properly the exposure of information is guaranteed. The information is then used for illicit purposes such as identity theft.

Access management solutions represent technologies that use access control engines to enable centralized access using various methods, providing the secure and productive environment. Access solutions have evolved, due to the need to enable and protect digital transformation in various scenarios. Target applications can have traditional or untraditional application architectures, running on premises, cloud, mobile or hybrid environment and in either way they must be integrated and properly secured from both inside and outside threats.

Stolen identity is a powerful tool in today's world. It can be used for a coordinated insider attack, selling digital identities on the deep web, credit card fraud, mail theft and other criminal acts. Attacks on digital identities are rapidly evolving and the highest level of attacks are on e-commerce and new accounts, where attacker uses personal information to create new financial accounts. As a result, companies endure extremely negative impact on their businesses, reputation and customer's trust.

Information security and risk management are key components that ensure continuous improving of planning, building and running security solutions adopted to business needs. As typical employee becomes more mobile and "*Bring your own identity*" trend continues to grow, accessibility and availability of enterprise services needs to be managed securely. Problem with multiple identities can be solved using distributed identities. Distributed identity implies the secure exchange of identity information across one or multiple trusted domains, providing users the ability to use one set of login credentials to access multiple applications.

3 Overview in the field of research

As digital technologies impact the business ecosystem, digital transformations have been a very interesting topic for debate between business scholars, from a critical management perspective. Today, digital transformations are being characterized as a global trend that is changing preestablished value chains across public and private sectors. [1]

As a leaders in IT Security field, with a wide range of security solutions, IBM provides security intelligence, helping companies protect their people, systems, data and improve upon their business. As crucial link in IT security, access management solutions are the first in line to protect the business ecosystem. They must detect, prevent and secure the system from both external and internal threats.

3.1 Digitally transformed business ecosystem

Digital transformation represents the integration of digital technology into all business areas, leveraging the technology to radically change and improve the business. These technologies will help businesses gather, analyze and make value from the data, guide and prepare them for new challenges and make them one step ahead from the competition. Digital transformation improves the efficiency and operational agility, customer experience, enables interconnectedness, integration of various digital technologies and empowers innovation. It is an imperative for all businesses, impacting the business and value of every organization.

It is a shift from complex and traditional methodologies to agile and flexible ones, allowing the use of open technologies and predictive analytics, user centric and iterative software delivery, intelligent systems, cognitive computing and API driven concepts. It transforms the business activities, processes, models, ecosystems, asset management, organizational culture, partnership models, approach to customers, workers and partners. And one of the most important things is that digital transformation is not only about technology, it encourages people-centric approach as well. Technology is a just part of the equation, one of the engines that pushes the company to embrace the new strategies that will make a business competitive and successful.

There are numerous causes for digital transformation, one of them is technological innovations and how are they implemented, used and embraced by the customers. Along with the rise of new technologies and services, customers' expectations are getting higher, implying the need for new technologies and approach in satisfying their requests. Economical and regulatory changes are requiring digital transformation to be implemented appropriately. Information needs to be gathered, processed and saved in a secure and predefined way. Digital transformation impacts every industry and finding the right transformational strategy to use the advantages is a key to success.

3.2 People-centric security

Confidentiality, integrity and availability are crucial parts of every security system, however in the digital business world, the CIA concept isn't enough. Digital explosion, interconnectedness of different systems, devices and the growing evolution of Internet of Things pushed the digital world into a physical world.

Protecting only information is not sufficient, providing safety for both the people and their environments must be equally important. As a result CIA concepts must be expanded with one key component – **safety**. Necessity to protect not only the digital world but physical world as well is inevitable. [2]

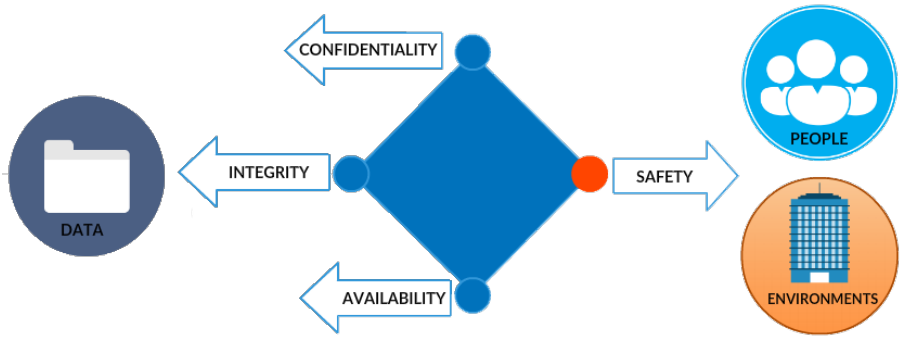

Figure 1: "CIAS" model of digital security

The concept of safety combines both people and assets. Safety of people is very important, because with proper training and rehearsals of events, employees will know how to prevent physical unauthorized access, avert danger or disaster, react quickly and respond as a team.

Safety of assets implies the physical security mechanisms such as locks, fences, surveillance, lighting etc. Both data and physical security play an important role in IT security, ensuring that with secured systems and with secured work environment high level security can be achieved. Business data is now distributed through different dynamic environments, detached from the traditional enterprise. Managing risk is a crucial part in securing business data and making sure that businesses will have a desired outcome.

Risk based approach will ensure flexible and responsive security solutions, adopted to business needs. Risk-Adjusted Value Management model can be created, integrating IT risk into corporate performance. As a result, the risk is addressed and business value is added.

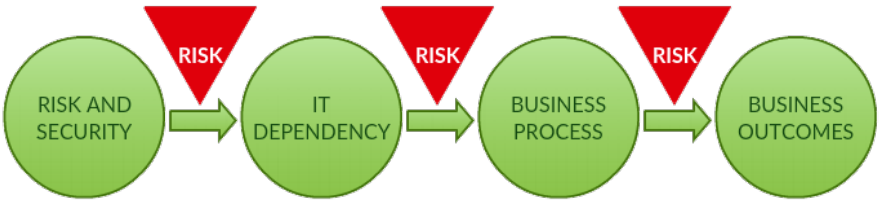

Figure 2: Risk-adjusted value management model

When designing security solutions, it is important that security products are agile, modular - adopted to business needs, ensuring smooth administration and usage. The main goal of identity and access solutions is to safely boost businesses, employee productivity and protect organization from inside and outside threats. Benefits from implementing such solutions are various:

- ✓ Secured environment, data and people
- ✓ Effectiveness and efficiency
- ✓ Productive and motivated employees
- ✓ Simplified administration and management
- ✓ Reduced integration costs and pressure on support desks

Federated identity concept is based on the creation of globally interoperable online business identity, incorporating various applications and system identities together. It is more effective and efficient to use a single sign-on type of accounts because a single user can have many accounts, passwords and usernames across dozens of systems.

Users weaknesses include slow input of credentials, their forgetfulness of those credentials and weak, attack prone passwords. Federated identity also indirectly aims to improve the cost efficiency of a system, because it removes the need for many administrative roles which under a predecessor system are needed.

This approach undermines outside attackers efforts to compromise a system and also to halt a company workflow, sometimes for multiple days at a time. From this point forward there is no need for creating and managing multiple accounts, passwords and users from other systems.

Federation represents the set of business, technical and other regulations, allowing companies to share their assets and improve their business. The concept of federation includes the making of trusted infrastructure that can carry out various needs. Each solution can be deployed separately or together providing complete federation solution.

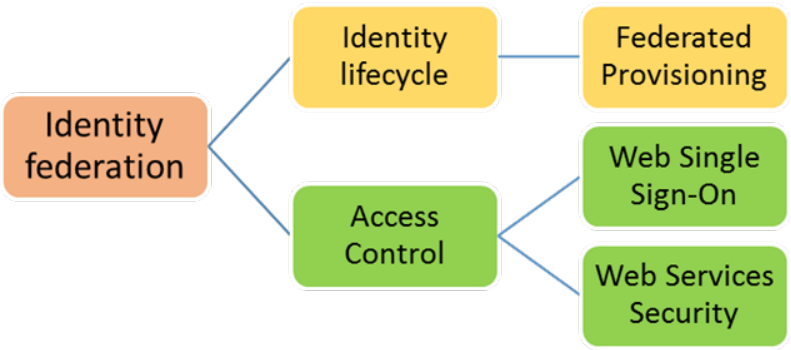

Figure 3: IBM Federated Identity Manager functionality

There are numerous benefits for implementing federated identity management in business environments. Identity management costs are reduced because companies only take care of access and don't have to deal with account administration. Using only one global identity for authentication and navigation through multiple web sites and applications improves user experience. Because of the federated identities, seamless integration between enterprise applications is ensured, enabling end to end security and trust capabilities.

3.3 Rise of new security standards in financial sector

As digital transformation effects the financial sector as well, new banking regulations have been developed. European Unions **Revised Payment Service Directive (PSD2)** and its United Kingdom implementation **- Open Banking regulation**. These regulations will radically change the banking sector. PSD2 enables clients to authorize third party providers to supervise the activities. Access to banking services is allowed using the open APIs and their protection is crucial. PSD2 is being applied as of January 2018, except some security measures that are defined in Regulatory Technical Standard (RTS).

PSD2 involves two new entities – AISPs and PISPs. The AISPs are the service providers that have access to the customer's account information and they can analyze users spending behavior and aggregate users accounts from different banks into one overview, improving the money management.

PISPs are the service providers that have the responsibility for payment initiation on behalf of the user (banks, payment institutions or new providers). They will guarantee that the money is being transferred. Competitiveness will be improved, as banks will no longer be the only main providers and non-banks will be able to enter the market and provide financial services using protected APIs.

These regulations will provide improved user experience and flexibility, customer will be able to do the payments using the third-party application. Using the multifactor authentication, biometric authentication and other advanced security measures, third-party applications will be able to access the account and make the payments. Financial institution authenticates the purchase directly without the involvement of other organizations.

Loan approval will be simplified, as customers will be able to give investors restricted access to the financial history, without giving them user credentials, making it much more secure. Transparency and control of customers information is priority, giving the customers full control about how and where the personal information will be used and processed.

Online transactions will be secured by adding the additional security measure – linking. Using the OTP mechanism transaction will be linked to its amount and to the payments' beneficiary. This security mechanism will assure that even if the breach occurs, the attackers won't be able to reuse the information from one transaction to initiate another. Open banking will significantly accelerate the use of blockchain and cryptocurrencies in mainstream financial services. [3]

Potential security threats like social engineering will still be present but if customers are aware of the regulation, they have much less probability to be realized. Phishing threats will be decreased because with this regulation there is no need to share credentials with banks or third parties. If the customer is aware he will not respond to such requests, even if it looks like the bank is sending them. Working on informing people about changes and PSD2 benefits will be crucial. Banks must be compliant with the regulation and if necessary, change the complete legacy IT infrastructure.

One of the concerns is protecting the use of personal data for advertising, as AISPs and PISPs will have significant information about transactions. By profiling the user, lenders will have advantage for placing the right advertisement and have an influence on the user.

Privacy must be equally important and the customers must completely understand every action they are taking.

3.4 GDPR regulation

General Data Protection Regulation replaces the previous directive and was created to empower and unite Europian data privacy laws and direct the apporoach to data privacy. Enforcement of the GDPR starts on **May 25th, 2018**. This regulation will be implemeted to all institutions that process personal data in the European Union, disregarding the location of the company or where the processing takes place. The regulation will apply to all participators wheather they are auditors, processors or cloud platforms. [4]

One of the biggest changes is in transparency. Clients are now in the center of the decision making and they must be notified about every activity that involves the use of their personal data. Clients are given the conscent to choose the appropriate decisions. The internal record safekeeping is mandatory for the subjects that are responsible for data proccessing. [5]

Having the appropriate security measures, being compliant with the regulation, safekeeping the data and having the right security officers is mandatory and the institutions that doesn't implement this regulation will pay high fairs.

Along with demanding requirenments GDPR brings significant benefits to the business. Information security is mandatory for all institutions, regardless of their size and the area of work. This will bring client's trust and business reputation to the next level. Knowing that the personal data is higly protected and that every decision making depends on the client will enable trusted business relationship and boost the customers loyalty. With the rise of clients loyalty, businesses will have better position on the maket and increased income.

The systems for data processing will be improved, changing the way of how, when and where the data is processed. This way processed data will be precise and it can be used for other purposes, bringing the higer data value to the client. Clients will be able to investigate and validate the gathered data, resulting the siginificant reducement of redundant and incorrect data and giving the client full control.

Organizations will have to invest in employees knowledge and give them the appropriate training for the new technologies, awareness of the cyber security threats, new methods and approach with the clients. People centric security and CIAS concept will be mandatory for all organizations.

This regulation will open the doors for the digital transformation that will completely change how companies work, their relationship with the clients, position on the market, improve competitivenes and transparancy and make the information security the top concern.

3.5 Digital forensics in cyber security era

Cyber breaches are increasing in intensity and scope. Now every organization, disregarding its size or business activity and without an appropriate security system becomes a victim of cyber-attacks. Attacks can be prevented, detected and even if a breach occurs, damage can be controlled.

The science of digital forensics involves gathering and analysis of data, identification, preservation and integration evaluation. The concepts of digital forensics are incorporated inside Security Information and Event Management (SIEM) systems. By deploying multiple collection agents to end-user devices, networks, servers SIEM systems are collecting and analyzing the data, identifying threats, potential breaches and anomalies, logging the information, alarming the administrators or other security systems to act.

As SIEM solution IBM QRadar with its capabilities can collect various information including network equipment, operating systems, vulnerabilities, user activities, behaviors and perform real-time analysis, correlate system vulnerabilities with the event and network data and prioritize incidents. It can be implemented in a cloud environment or as a modular appliance that can be extended to meet the various needs. It can be expanded with modules for risk and vulnerability management, forensics analysis and incident response.

In order to assure credibility of evidence, it is important that SIEM solutions are compliant with the regulations. QRadar is compliant with various worldwide regulations - HIPAA, PCI DSS, GLBA, NERC, SOX and others.

IBM Security Access Manager (ISAM) can be integrated with IBM QRadar solution and by combining strengths and capabilities to enable multi-layer security. Interoperability is one of the todays most challenging goals to achieve. Being able to combine different technologies so they can deliver a true value is demanding.

ISAM reverse proxy can send system and log alerts to QRadar enabling the deep inspection and analysis of the data. System alerts can be also sent to mail or to SNMP Manager. Log files of ISAM reverse proxy can also be sent to QRadar, providing detailed log information about user requests and actions.

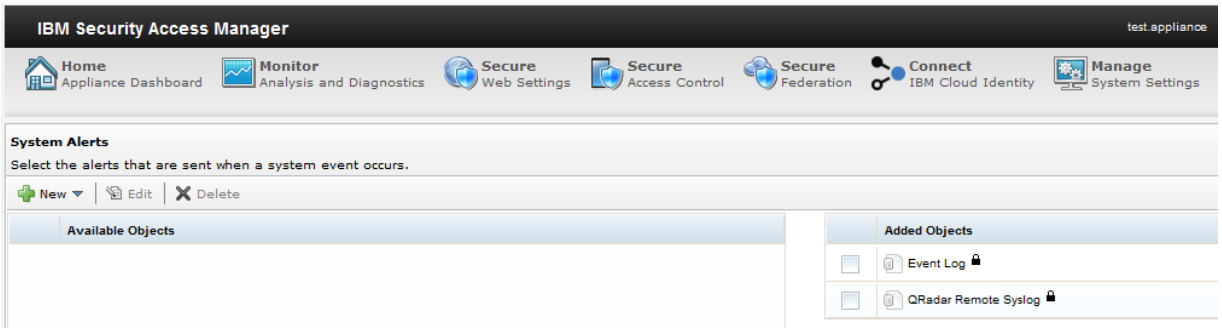

Figure 4: Adding Remote Syslog Qradar object

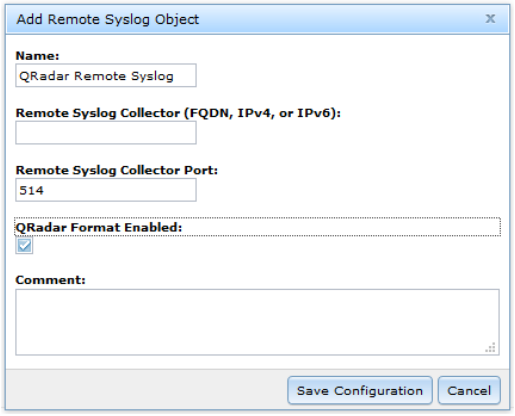

Figure 5: Remote Syslog configuration

Reverse proxy configuration should be also changed under the section ***[logging] stanza.***

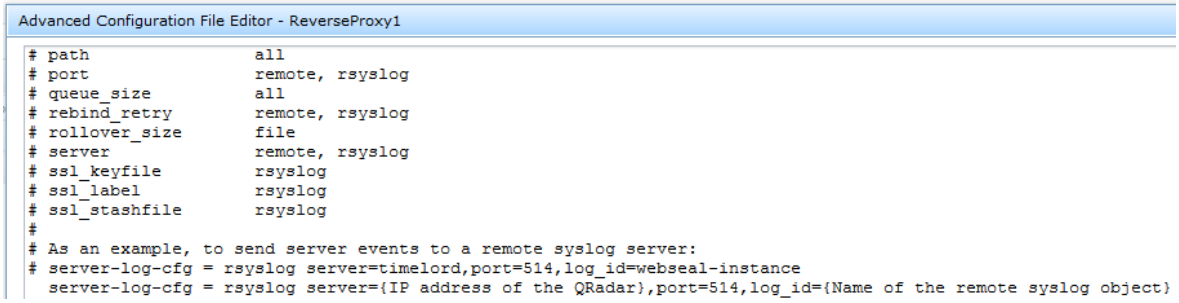

Figure 6: Reverse proxy configuration

4 Overview of the proposed solution

IBM Security Access Manager solution provides modular all-in-one security solution that helps companies protect their resources, make them easily accessible, boost business productivity and lower the integration costs. The modular nature of this solution is the core operating principle, enabling a more scalable, flexible and maintenance friendly solution.

The solution provides a procedurally simpler and reduced risk approach to securing an uninterrupted user experience. This is achieved by shielding the vital assets with the use of strong multi-factor authentication and risk engine. ISAM consists of the core module (Security Access Manager Platform), and can be extended by adding additional license-based modules. The additional modules are the advanced access control and federation.

ISAM includes various capabilities:

- ✓ Scalable reverse proxy used for access control, load balancing and web single sign-on
- ✓ Seamless federated single sign-on for external applications, business partner applications, quick connectors for cloud applications and federated user directory
- ✓ Centralized policy server for managing access to all resources
- ✓ Integrated web application firewall protection for evolving threats
- ✓ Fine-grained multi factor authentication service
- ✓ Mobile application administration and user self-service
- ✓ Compliance reporting and security intelligence integration with IBM Security QRadar SIEM
- ✓ Context-based authorization with integrated risk engine mechanism

IBM Security Access Manager (ISAM) is available as virtual or hardware appliance. Functionality can be expanded by using additional modules that can be activated by licenses. The solution secures information system by implementing access policies that enable fine-grained authentication and authorization.

With web application firewall that is created by IBM X-Force® threat research team, ISAM provides multiple layers of protection from the newest threats and vulnerabilities. Cross level protection includes application layer heuristics (algorithms that protect from malicious application use), web injection logic (protection from web attacks), shellcode heuristics (protection from vulnerability exploitation), content analysis, protocol anomaly detection (prevents the deepest network level attacks).

Access Control can be implemented on mobile, on-premises and cloud environments. Mobile enterprise is today's most commonly used way of accessing vital enterprise resources and needs to be equally protected from threats. Mobile access control policies with risk engine mechanism, mobile device identification mechanism, multi-factor authentication can be provided by ISAM to assure mobile security and prevent future incidents.

As information needs to be available and accessible almost everywhere, API calls certainly follow the trend. When using API calls on multiple platforms and for different purposes, it is crucial that there is a strong assurance for their security and resistance for malicious use. Originally APIs were designed to be used as a way for separate entities to communicate between each other in a uniformed fashion. As digital technology developed the use of APIs shifted to internal sharing of data between organizational sectors.

In recent times, public APIs were brought into the spotlight by the rapid rise of mobile technologies and the need for building strong partnerships between organizations. Company information becomes more accessible to others, which in turn means a faster exposure on the market, flexibility and reduces the costs of transactions. APIs are the core of the digital transformation, a powerful engine that facilitates an improved access to the cloud and boosts efficiency across the cloud. [6]

4.1 IBM Security Access Manager Platform

ISAM platform consists of the policy server, user registry (embedded or external), authorization server, reverse proxy, load balancer, distributed session cache. The system can be accessed using the command line or local management interface.

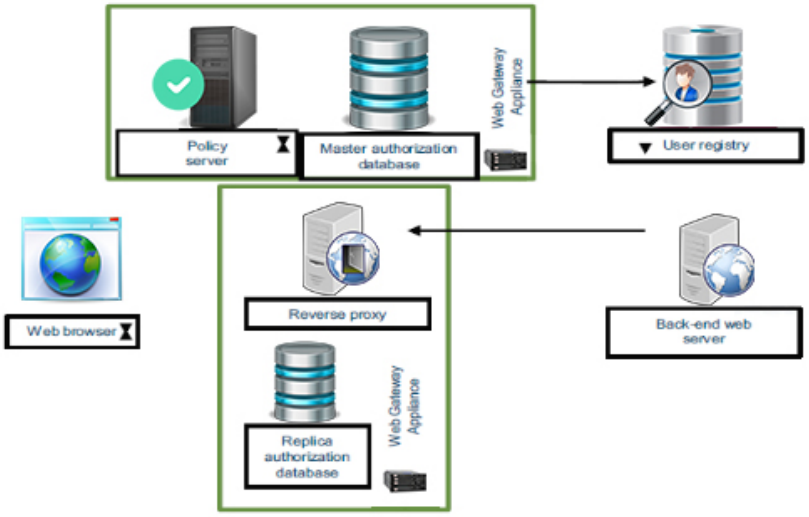

Figure 7: ISAM architecture

Policy server

Policy server have important role in this system, it processes the access control, authentication and authorization database. Security policy is distributed to the various ISAM components. Policy server also contains the copy of the authorization policy that is carried out by the reverse proxy ("WebSEAL"). High available solution can be made using clustering and enabling secondary "standby" policy server that will be promoted to primary in case of failure or maintenance.

User registry

ISAM contains multiple databases that are used for various purposes - policy, configuration, geolocation and runtime database. **Policy database** contains a master copy of the policies that are implemented by the reverse proxy and authorization server. **Configuration database** contains appliance configuration (postgreSQL). High availability can be achieved by replicating this database across a cluster. This database cannot be managed by the standard database tools. **Geolocation database** is used to link the IP address to the country and city where the device is stationed. Can be replicated across the cluster. **Runtime**

database is used to store data for device identification and other mechanisms provided by the federation and advanced access modules. It is used as embedded or as external database. Security Access Manager Platform users are usually stored on external database, embedded LDAP database is usually used for testing purposes.

Management Interface

Appliance can be managed by the Local Management Interface (LMI), Command Line Interface (CLI) and RESTful web service API. Local Management Interface represents the user-friendly graphical user interface.

Authorization server

This component enables a remote policy decision point for authentication and authorization requests using the authorization API. Authorization server isn't a mandatory component. It is often used when a remote authorization service needs the ISAM for decision making.

Reverse proxy

Reverse proxy represents the most crucial component of the system. It has a various purposes in achieving the multi-layer security approach. Reverse proxy is responsible for authentication, session management and authorization. Enforces authorization policy and stores a local copy of the authorization policy and by doing so, reduces the time for decision making.

Reverse proxy can be implemented as separate load balancer component. Using reverse proxy as load balancer component, information flow can be considerably improved by balancing load and handling fail-over. As a result, significant improvement of information flow, user experience, server response time is notable and high-availability of the system is achieved.

Reverse proxy can be used as application firewall, because it contains the IBM X-Force application firewall that can be used for threat detection, protection and prevention. He is also involved in federation process and advanced access scenarios.

Distributed session cache

Distributed session cache plays important role in clustered environment. By caching session information, user sessions are easily managed, monitored and user experience is significantly enhanced. Distributed session cache uses session cookie mechanism, session cookies are small, usually less than 100 bytes. Distributed session cache shares session and provides concurrent web sessions, centralizes management of session cookies, monitors the number of failed login attempts and provides fail-over for user sessions. Distributed session cache doesn't require encryption keys which considerably decreases the CPU usage.

DSC component resolves session inactivity and session lifetime timeout consistency issues in replicated web server environment. Improves user experience by providing the single sign-on and single sign-off capabilities between websites in the same DNS domain.

Session cache is stored inside in-memory database (SolidDB) and it can be replicated accross the appliance cluster.

Clustering

IBM Security Access Manager clustering technology enables high-available environment, resistant to failures and disruptions. By using clustering technology, environment becomes flexible and adaptable to rising challenges, while components become syncronized and more efficient.

Cluster roles:

1) Primary master
2) Replica masters (Secondary, Tertiary, Quaternary)
3) Node
4) Restricted Node
5) External reference entity

Primary master coordinates cluster operations and represents the authoritative source of data. All configuration updates and policies must be made on him, updates on replica masters are not allowed and won't be implemented. This excludes data redundancy and limits other participants in changing system configurations.

Secondary master can be promoted to primary in case of primary master failure. Components that are crucial for the system provide automatic failover.

Quaternary and Tertiary masters are used only in case of distributed session cache failover.

Nodes are the non-master appliances that join the cluster. They can access the configuration of the primary master but they cannot change it. Administrator can promote them to become the primary master.

Restricted nodes reprepresent regular nodes with significantly restriced rights in cluster. They cannot be promoted as primary masters and they are not allowed to use security policy administration capabilities or to modify any configuration. Restricted nodes should be placed in demilitarized zone, limiting any access to internal systems. They do not have any cluster data information and cannot use admin functions.

External reference entity is an external network device that helps Security Access Manager in failover detection. Main purpose of this device is to detect the failover and inform secondry master of such event. When a master loses the connection with other master, external reference entity issues a connectivity test and determines the state of the other master and checks for network issues. [7]

By using **external authentication interface (EAI)**, authentication process is extended to independent custom developed application. Identity information returned by the external authentication interface is used by the reverse proxy (WebSEAL) to build the user credentials. External authentication in returning the identity information in HTTP response headers. Application is located on a junctioned web server. Design, code and methodology used for authentication decision is the responsibility of the application developer.

Requirement of external authentication application is to return identity information in specially named HTTP response header.

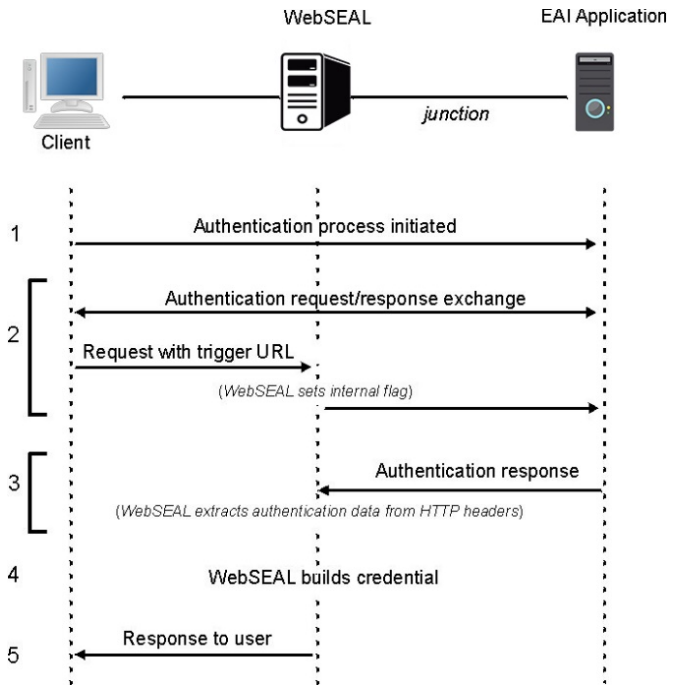

Figure 8: External authentication interface process flow

IBM Security Access Manager Key Capabilities

Security Access Manager key capabilities include:

- ✓ Improved user producitivity while protecting access to applications on web and mobile platforms and providing SSO, multi-factor authentication, session control and specialized access policies
- ✓ Enables multi-layer security, covering OWASP top 10 most critical security risks
- ✓ Integrates with various platforms and products with ability to externalize authentication and authorization
- ✓ Scales to support millions of users
- ✓ Provides federated single sign-on, resources are protected, easily accessible - including easily configurable connections to popular SaaS applications, system integration cost is reduced

4.2 Federation Module

ISAM is also a federated single sign-on solution, implemented as the additional federation module, whose infrastructure enables identity propagation through SSO capabilities, eliminating the need for multiple user identities and passwords. Identities can be federated through multiple security infrastructures. Multiple deployment scenarious are supported, and each scenario can be deployed separately.

Federated single-sign on scenario facilitates creation and management of federated SSO environments. Web service security scenario represents an authorization solution, ensuring that only properly evaluated user requests can access resources through different domains.

Provisioning scenario enhance current provisioning solutions across the internet using web services standards. Identity token exchange deployment scenario provides the transmission of user credential information between different identity tokens.

During federation, business entities can have the following rolles: identity provider or service provider. The main resposibility of identity provider is providing authentication and identity assertion for the particular user to trusted business partner – service provider. The assertion consists of authentication statements, assuring that user is successfully authenticated. Identity provider controls the account management and provisioning.

Trust relationship is formed between the identity and service provider, information about user is trusted and service provider delivers the required service or information to the user. Trust relationship is ensured by cryptographic keys used to encrypt and sign messages. By doing identity tasks, identity provider relieves business partners (service providers) from redundant identity management. Identity and service provider reduces the identity and access management cost and improves user experience.

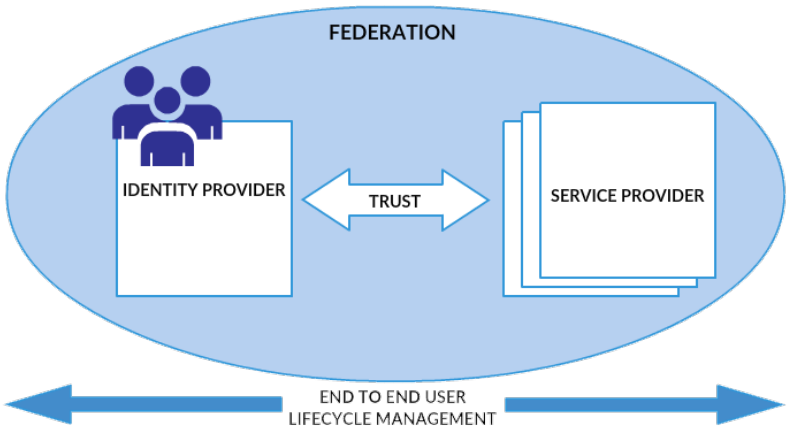

Figure 9: End-to-end user life cycle management

If the user is successfully authenticated, the identity provider affirms user's identity to the service providers, granting him federated access to applications and services. In order to accomplish interoperability both sides must agree upon technical terms.[8]

Firstly, the security token information needs to be managed. The security token made by one partner needs to be acceptable to the other partner. The terms about which information is exchanged inside the token and how it's used must be agreed on.

Generation and consumption of security tokens in federation module are managed by the trust service and enforced by the SSO protocol service.

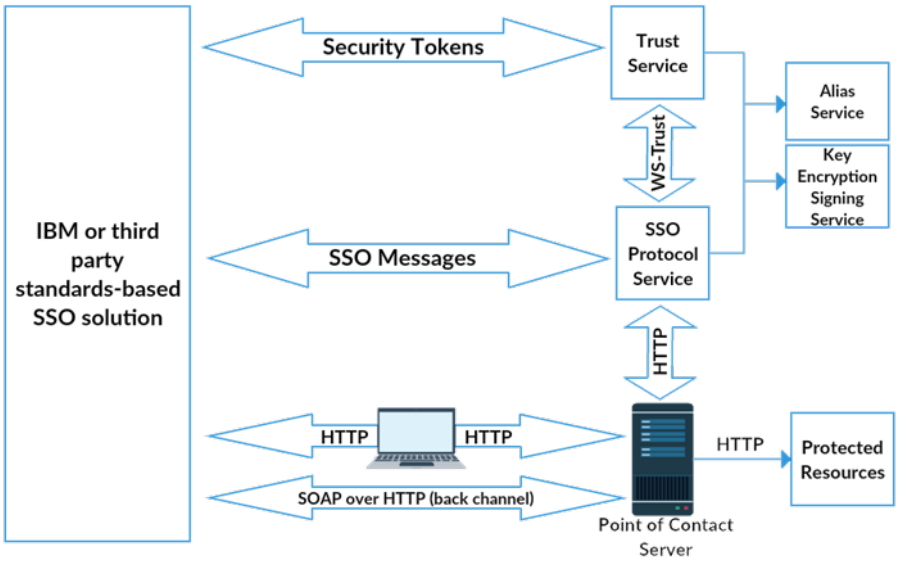

Figure 10: Single sign-on components and communication between layers

Secondly, the SSO protocol needs to be managed. SSO protocol specifies the communication between the parties. It describes how the security token will be requested and presented. SSO protocol messages are managed by the SSO protocol service.

All communication and HTTP messages are managed by the reverse proxy. At the protocol layer, SSO messages are exchanged with the third-party through the point of contact server. Security tokens are transferred between the federation module and the third party through the SSO Protocol Service.

Presently, companies are striving to embrace business on demand solutions. The business model needs to be responsive, adaptive, focused and resilient. In order to do so, deconstruction of the enterprise is inevitable. Deconstruction of infrastructure to partners, customers, suppliers can be accelerated by implementing open standards and service oriented architecture. Open standards are the key components that enables interoperability between different systems, services and applications.

With a wide range of supported open standards and cryptographic protocols, federaion module provides security customization and web service protection. Authentication information is managed through security open standards based identity and security tokens. Security token service is embedded inside federation module. It enables the identity mediation services, allowing the managing, mapping and propagating identities. The module expands on the capabilities of the core federation solution for SSO and identity mediation for enterprise applications as well as SaaS. [9]

IBM Federated Identity Manager provides support for SAML 2.0, OpenID connect, OAuth, WS-Federation, WS-Security, WS-Trust, Information Card Profile, IBM Resource Access Control Facility, SHA-2, X509, Kerberos tokens.

Advanced Access Control Module has risk-based access capabilities, calculating the risk and protecting the information flow. Risk-based access enhance security of authentication and authorization mechanisms, estimate the risk and calculate the risk score. The module is activated by explicitly using an IBM license.

Integrated audit data collection and reporting generate the audit logs, tracking and incident reports to aid compliance activities. Federated Identity Manager enables two-factor authentication with One-time password (OTP) capability. OTP improves authentication mechanism and can be implemented through configuration. The functionalities of the utmost importance for this module are OAuth support, context-based access, fingerprinting, multifactor authentication and device registration.

The business ecosystem needs to be carefully designed and connected. Federated SSO extends the availability and accessibility of applications to business partners, customers and consumers. As a result, resources are protected, easily accessible and the system integration cost is reduced.

In this day and age customers and companies are more and more reliant on well-structured interoperable systems in which the aspect of security solutions is significant. This ensures the greater and safer flow of information, especially considering the immense presence of large multinational corporations on the internet.

4.3 Advanced Access Control Module

With the evolution of digital business, mobile devices have become imminent part in every corporate architecture. Business transactions, remote access to corporate network and constant use and change of corporate data needs to be monitored and managed appropriately.

IBM Advanced Access Control module protects the business ecosystem and extends it's assets by implementing advanced risk engine mechanism, fine-grained access policies, multi-factor protection and user self-care mechanism. Advanced Access Control supports the requirements that are defined by the NIST standards.

Context-based access enhances security during authentication and authorization decisions. Access is enabled by estimating the dynamic risk assessment or confidence level of a transaction. Context-based access uses static, behavioral and contextual data analysis to calculate risk. Risk score is configured to comply with business environment and secure all of it's resources. Risk is calculated on multiple weighted attributes, resulting a decision that can be permitted, denied or challenged for further authentication.

These attributes are part of a risk profile that is used for determining the risk score. Multiple risk profiles can be created but only one risk profile can be active. On each attribute administrator can set desired weight and form risk score limit. After every transaction risk report is created. Access policy is a combination of attributes, obligations or authentications and a risk profile.

Risk report provides the outcome of the risk score calculation, matcher that the risk score engine used for the comparison, attributes that were compared, other calculations that were made. Risk reports are essential part for complying activities, monitoring and reports

that are required for GDPR. These reports are also useful for creating a more effective risk policies and monitoring of the system activity.

User can register devices that they commonly use and associate the registered devices with the user credentials. Challenge can be requested if the user tries to authenticate with the same credentials from another unregistered device. When a user accesses a resource from a device that he previously used and maintains typical usage paterns. Context-based access improves the user experience by limiting secondary authentication challenges.

Special multifactor authentication mechanism can be used to access a protected resource. The following authentication mechanisms are supported - Consent to device registration, Email message, Email OTP, End-User License Agreement, Fingerprint approval, HOTP, HTTP Redirect, Info Map Authentication, Knowledge questions, MAC OTP, MMFA Authenticator, OTP, RSA OTP, SCIM Endpoint Configuration, SMS OTP, TOTP, USC Account Create, USC Lost ID, USC Password Reset, User Presence Approval, Username Password, reCAPTCHA verification.

User self-care capability enables the end user capability to do self-management tasks, such as password reset, manage registered devices and configure knowledge questions. User self-care capabilities enabled by avanced access module, significantly impact the user experience and reduce pressure on support desks. Behavioral patterns of the user can be used as a factor in risk score calculation. Access time outside of normal business hours can be denied or forced to authenticate with secondary challenge.

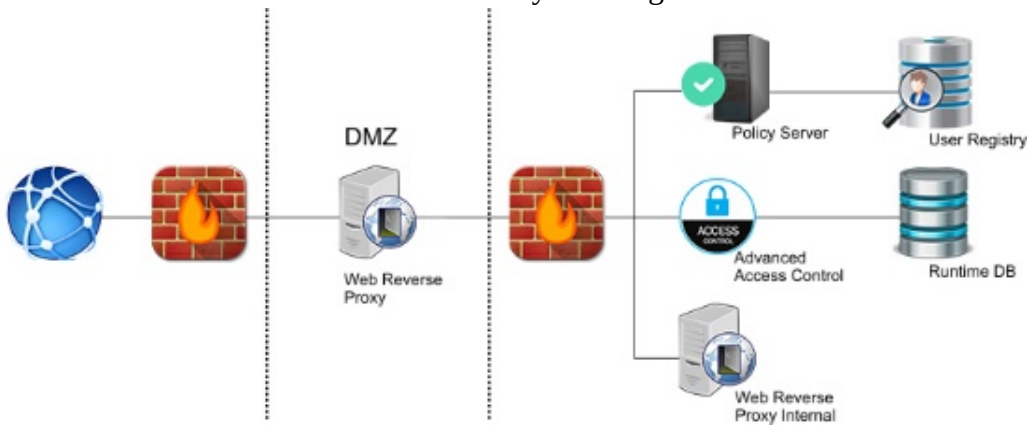

Figure 11: ISAM Advanced Access Control typical deployment pattern

Illustrated deployment pattern, shows typical deployment pattern of Advanced Access Control. Web Reverse proxy is located in demilitarized zone and presents first point of contact between client request and internal servers.

All appliances are clustered and policy server is working on the primary master. Other appliances are dedicated as secondary masters. Appliances inside DMZ zone are defined as restricted nodes. Restricted node provides additional security measure by denying access to policy administration and change of any configuration. Restriction also includes inability of the restricted node to be promoted as secondary or master node. Advanced Access Control policy is enforced by the point of contact server - reverse proxy.

Advanced Access Control can use embedded high volume database for testing purposes or external database IBM DB2, Oracle DB and Solid DB. [10]

4.4 The power of API management

API calls can be protected by using Security Access Manager API Protection feature, using OAuth 2.0 protocol. ISAM Restful API calls can be also used to control and automatize ISAM tasks and improve efficiency and reduce time needed for manual configuration. The following OAuth 2.0 flows can be implemented.

4.4.1 Implicit grant flow

Implicit grant flow is one way of implementing OAuth protocol, recommended for OAuth clients that are not able to keep the authentication information confidential, used in communication with the authorization server. Commonly used in scenarios where the client is JavaScript running in users' browser or client is interacting using APIs which are not authenticated by the current session or cookie domain. This flow is also used when the environment has certain restrictions, for example when the client needs access a token but is not allowed to communicate with the token endpoint. That is possible due to the ability of the user agent to run the granted script locally, extracting the access token and passing it to the client.

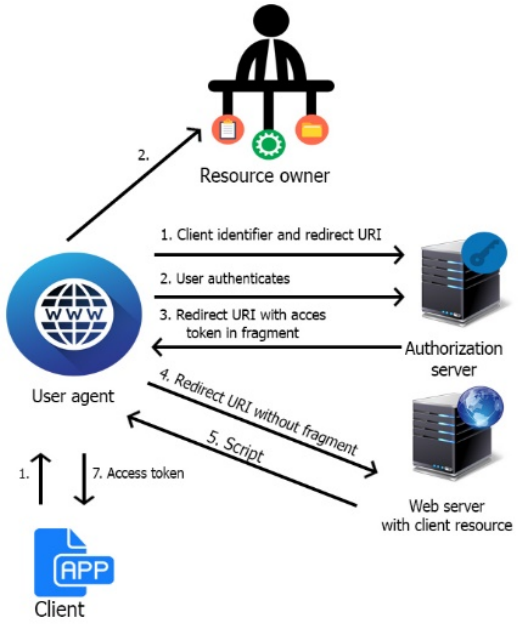

Figure 12: Implicit grant flow

4.4.2 Authorization code flow

This flow is recommended for OAuth clients that are able to keep the authentication information confidential, used in communication with the authorization server. Commonly used in scenarios when the user is accessing servers using the web browser, where the OAuth Client is a third-party server. Authorization code flow is especially suitable for the financial sector, where users can have access to a particular service without the need to share their credentials with third party server.

During such scenario, users only need to enter their ISAM credentials into the ISAM protected domain. Refresh token is used as a mechanism for the expired access token, along with client credentials.

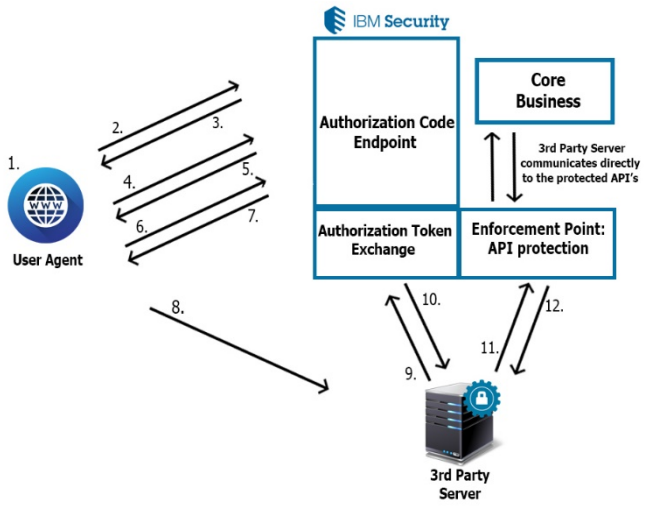

Figure 13: Authorization code flow

1) Customer initiates flow via the user agent (browser)
2) Customer passes Client ID and Redirect URI to the authorization server
3) ISAM sends request for authentication if user is not authenticated
4) User authenticates to the server
5) ISAM prompts user to consent to code exchange with Client (optional)
6) User approves the request
7) ISAM returns an authorization code to the user agent along with a redirect to the Client Server Redirect URI
8) Redirect to the third-party server with authorization code
9) Authorization code is exchanged for access token and refresh token
10) Return authorization code
11) API request
12) Response with access token

4.4.3 Client credentials flow

Client credentials flow is implemented when OAuth clients request an access token by using their credentials, similar to a basic authentication flow. Commonly used in scenarios where the third-party server needs to update some metadata or share the information which is not associated with the user.

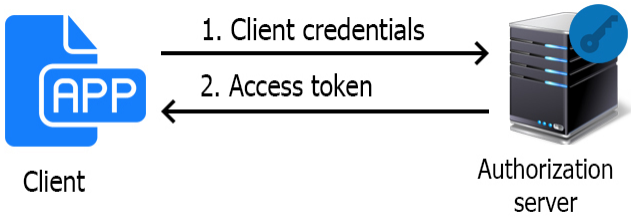

Figure 14: Client credentials flow

4.4.4 Resource Owner Password Credential flow

Resource Owner Password Credential flow is recommended for communication with trusted clients (trusted application, OS, etc.). User credentials are provided inside application before the authentication flow and the application is responsible for confidentiality and dispose of used credentials after the authentication flow. Commonly used in scenarios when the OAuth client has already obtained the credentials of the resource owner. [11]

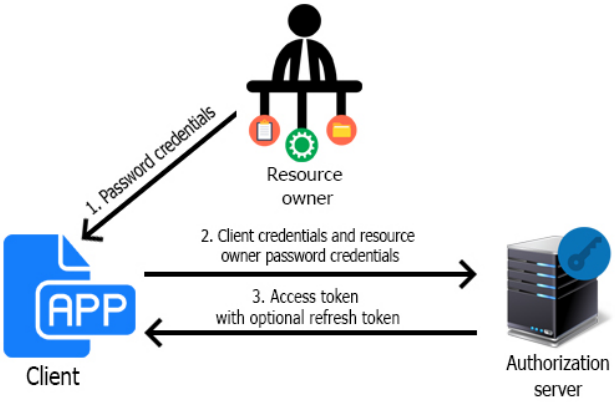

Figure 15: Resource Owner Password Credential flow

API Protection feature inside IBM Security Access Manager solution contains the following components:

1) API Protection Definitions

API protection definition is a list of configurations that define how resources are accessed and protect resources from unauthorized access. Using fine grained configurations, resources can be protected appropriately.

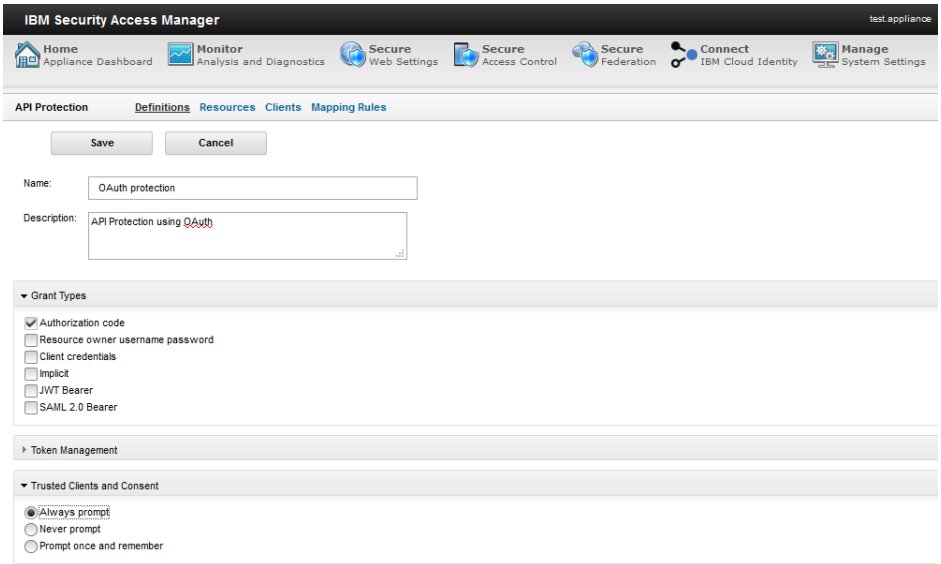

Figure 16: API Protection definition

Token Management option contains detailed configurations about the access token. Refresh token PIN policy provides additional level of protection, when issuing the refresh token. It requires the knowledge of PIN code in order to ISAM grant a user new access token.

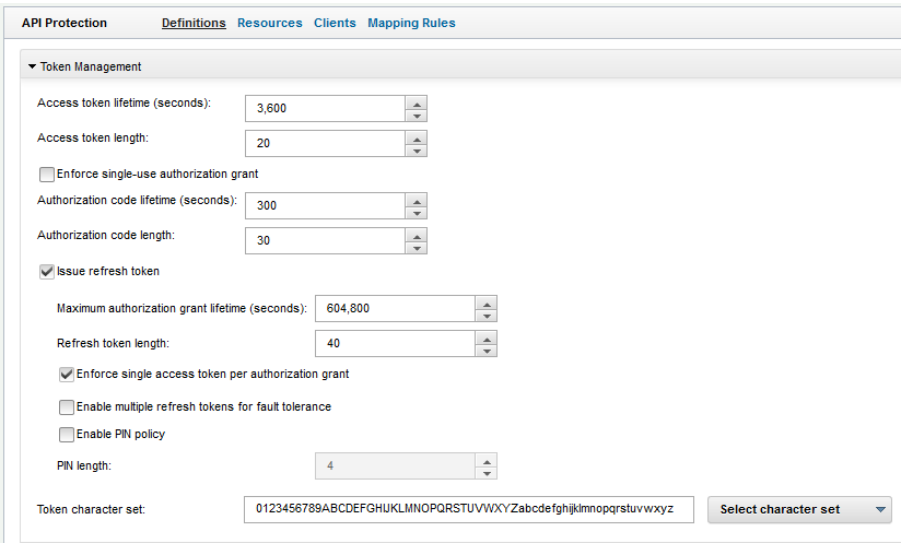

Figure 17: API Protection – Token Management

2) API Protection Resources

Using API protection Resources feature, resources that needs to be protected can be selected and previously created API definition can be applied on them. In order to be activated, attached API definitions must be published.

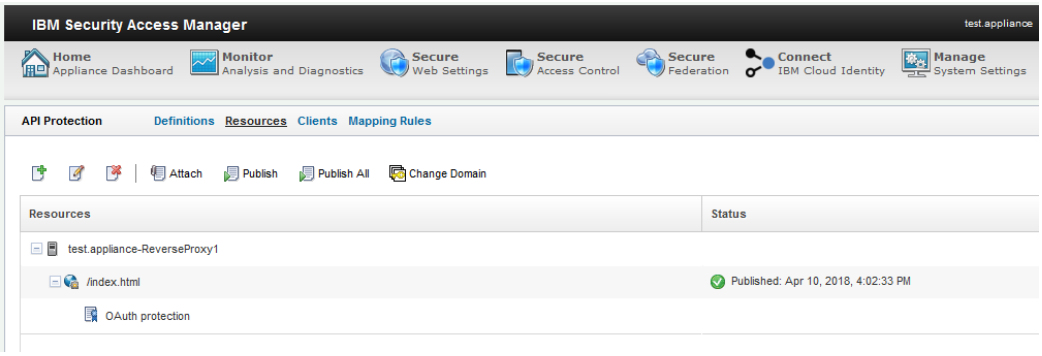

Figure 18: API Protection – Resources

3) API Protection Clients

Clients represent the entities against which OAuth tokens are granted.

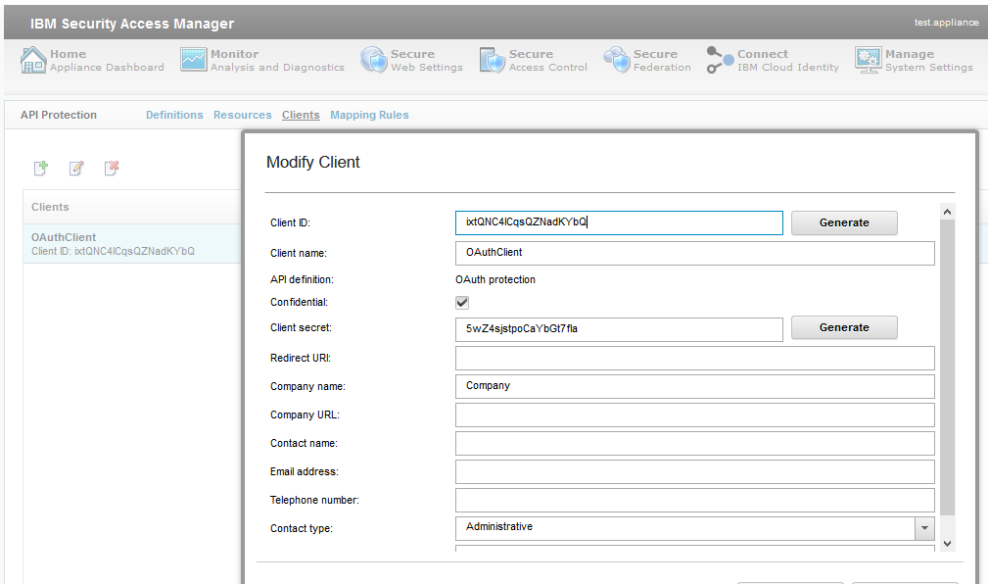

Figure 19: API Protection – Clients

4) API Protection Mapping rules

Mapping rules are JavaScript code that runs during the authentication or in this case before and after token generation. Mapping rules can be customized and they can define the mechanism for expired token detection and deletion, number of issued tokens etc. By doing so they reduce the space for potential malicious use of issued access tokens.

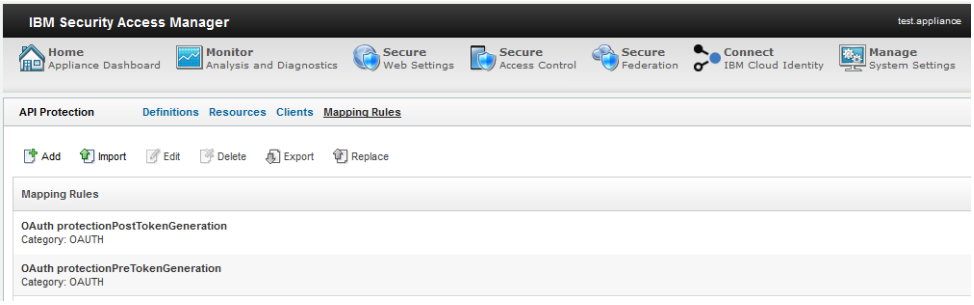

Figure 20: API Protection - Mapping rules

4.5 Centralized control using restful APIs

One of the many API advantages is using restful API calls to administer the ISAM tasks, enable automatization, boost performance and efficiency, deploy configurations, gather data such as logs, traces and statistics. Using tools such as Postman or Curl, clients can send a request containing method, URL, headers, parameters (optional), body (optional). Server replies with the information consisting of content, status and headers. Appliance contains a list of predefined commands that should be used for the direct command path API call, under the section Manage System Settings – File downloads.

Pdadmin command-line is a preinstalled utility, part of the Security Access Manager. Using this command line interface, various administrative tasks can be achieved: management of access control lists, users, groups, objects and other resources. Pdadmin commands are also used inside API calls. API calls can be used with pdadmin utility or with the direct command path to component that contains the desired service that will be executed.

1) Request method format

Depending on the command, HTTP request method can be GET, POST, PUT, DELETE for the direct command to the component or just POST for pdadmin utility. Format of the request for pdadmin utility should be: https://{appliance_hostname}/pdadmin

2) Authorization section

Authorization section is by default set to basic authentication, but it can be modified for using OAuth protocol as an authentication mechanism.

3) Header section

Json headers are used when communicating with ISAM. Headers should accept application/json and content type should be application/json.

4) Body section (optional)

Body section is used depending on the request, for example if the request method is PUT or POST, the body should be filled with the appropriate parameters. Body format should be raw – json (application/json).

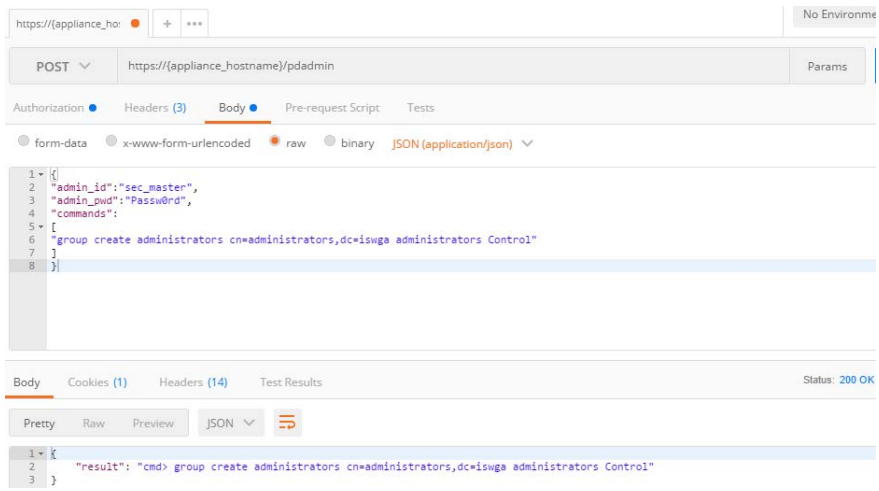

Figure 21: Postman tool - API Call using pdadmin utility

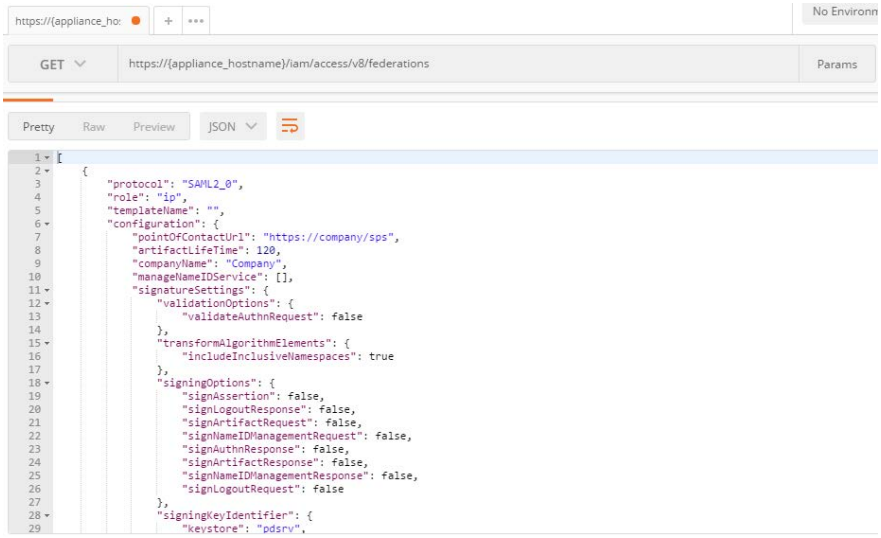

Figure 22: Postman tool - API Call using direct command path

4.6 Security on cloud – IBM Security Access Manager on Docker

Docker provides an environment, which consists of containers, enabling the digital transformation even in the complex infrastructure by making the component independent environment. The result is agile and flexible environment which is empowered by innovation.

Container image represents a lightweight, independent package of a piece of software, containing the code, system tools, settings, runtime and system libraries. Container represents runtime instance of a Docker image and it is built of a docker image, execution environment and a standard set of instructions. Docker image is the base of a container. Docker images for Security Access Manager are provided by IBM on Docker Hub.

Containers are feasible for both Windows and Linux applications, based on open standards and the software functionality will not be changed, disregarding the environment. By segregating the environment, containers provide a more secure environment. Applications are isolated from one another and from the underlying environment. This makes problem solving much easier as the issue is assigned to a single container instead to all components.

Simplified network - networking is now on the docker platform, which makes it much easier to configure, administer and control. The Docker host is responsible for the networking of the Docker containers. Containers can communicate internally or externally by utilizing the Docker host port mapping capabilities.

IBM Security Access Manager architecture now consists of containers and every container provides a single service – Configuration, User registry, Runtime database for advanced access and federation, Distributed Session Cache, WebSEAL Reverse Proxy instance etc.

Configuration container is responsible for generation of configuration data shared with other containers. All configuration must be done using the configuration container. Docker orchestration tools can be used to simplify the process of deploying the Security Access Manager to a Docker environment. Various orchestration and clustering tools are available: Docker Compose, Docker Swarm and Kubernetes. [12]

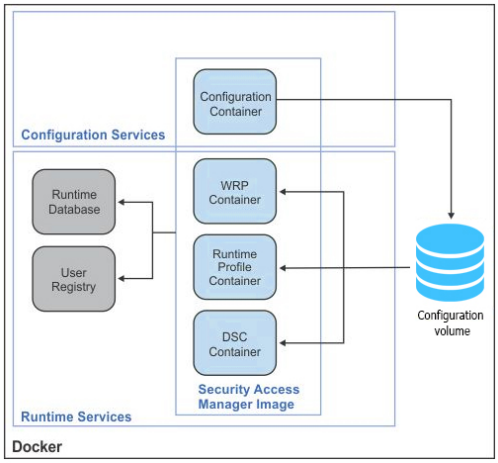

Figure 23: IBM Security Access Manager on Docker

Virtual machines represent the abstraction of physical hardware and contain full copy of the operating system, applications, binaries, libraries and consume much memory, docker images are quite opposite. Docker images represent the abstraction at the application layer that is responsible for code and dependencies. Numerous containers can be on the same machine, consuming much less space than the virtual machines, share OS kernel, run independently and even faster than virtual machines.

Appliance can be easily migrated to the Docker by importing the appliance snapshot into a running Security Access Manager configuration container. Certain conditions must be met in order to migrate appliance on Docker:

- For a SAM Base module activation, a snapshot must be taken on version 9.0.0 or later. For an Advanced Access Control or Federation module activation, a snapshot must be taken on version 9.0.2.0 or later.
- Appliance was configured to use embedded configuration database and an external runtime database.
- Appliance runtime environment was using an external LDAP server.

New features for Security Access Manager are now available and some features are extended. New features are listed by the corresponding module [13]:

1) **SAM Platform** (Paravirtualization on hardware assisted virtualization (PVHVM) mode for XenServer, Security protocol specification for the LMI, Management of static routes using the CLI, Snapshot migration, EAI log out functionality, LDAP client debug, HTTP/2 support, Customization of cluster identifier, Data from the embedded user registry can be imported in snapshot files, External PostgreSQL database support, Forwardment of log entries to a remote syslog server, Trial license request).

2) **Federation Module** (Support for importing a mapping rule into another mapping rule, New scripting support for template pages, Template page scripting limitations removed, SAML token one-time use, OAuth revocation endpoint, Customization of NameID attribute in Transient NameID format (SAML), API protection support for OpenID Connect Providers, Exclusion of session index in SAML 2.0 logout requests, New Security Token Service (STS) module for SAML 1.1, Module redirect URIs for an API Protection client, Proof Key for Code Exchange (PKCE) support, OIDC Claims Customization, Automated reverse proxy configuration for OAuth and OIDC provider, WS-Federation federations, Access Policies for use with SAML, OAuth and OpenID Connect protocols, Enhanced support for OpenID Connect (OIDC) Relying Party, Multiple assertion consumer service URLs support for service provider partners, RACF PassTicket Token, Dynamic application names in RACF PassTicket token modules, Support for OAuth and OIDC client assertion authentication, Configuration for outbound HTTP Proxy)

3) **Advanced Access Module** (One button functionality for enabling or disabling all authentication policies, SigningHelper class, Achievement of completed Mobile Multi-Factor Authentication (MMFA) transactions, External DSC server support, MMFA configuration for a specific Reverse Proxy instance, Cross-domain Identity Management (SCIM) group support, SCIM updates)

When running IBM Security Access Manager on Docker due to architecture and technology change, some functionalities are restricted: [14]

- Authorization server is not supported
- Front-end load balancer is not supported
- IP reputation policy information point capability (PIP) of Advanced Access Control is not supported
- Every configuration change requires reload of service containers
- Network HSM devices are not supported, all keys are stored locally
- Sample geo-location database is not provided
- Pre-installed federation partner templates are not provided
- WebSEAL Reverse proxy flow data or Protocol Analysis Module (PAM) statistics are not supported

4.7 Analysis and Monitoring

ISAM appliance provides a wide range of dashboard monitoring widgets inside Local Management Interface. These widgets are used to monitor the crucial components of the system including Network Traffic, Interfaces, Disk Usage, Reverse Proxy Health, Partition Information, Load Balancer Health, Reverse Proxy Throughput, Average Response Time, Security Actions, Certificate Expiry. They enable accurate, fast and concise monitoring, displayed on the home page of the ISAM.

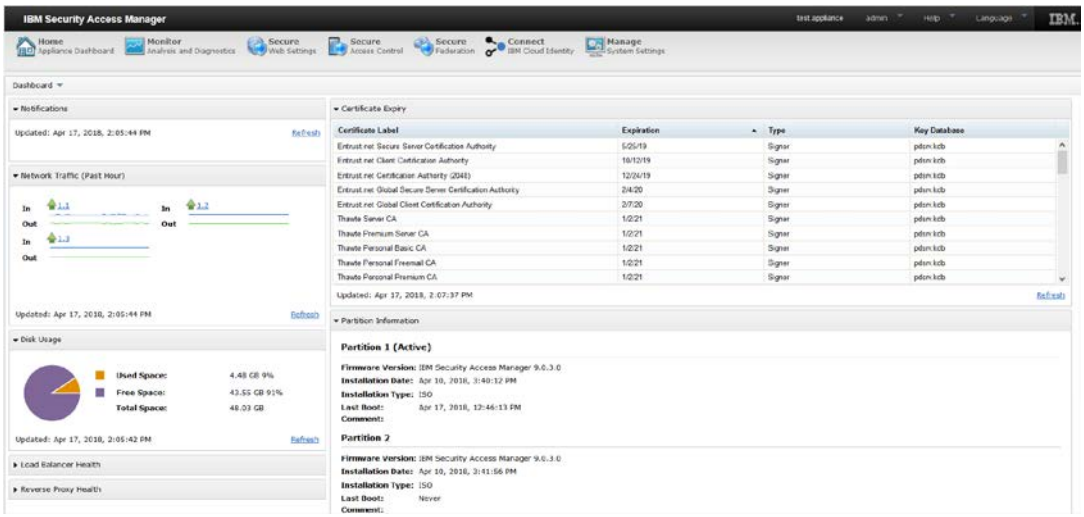

Figure 24: ISAM monitoring widgets

Additional monitoring tools and reports can be found under the section Monitor-Analysis and Diagnostics. Monitoring widgets can be repositioned and each component included or excluded.

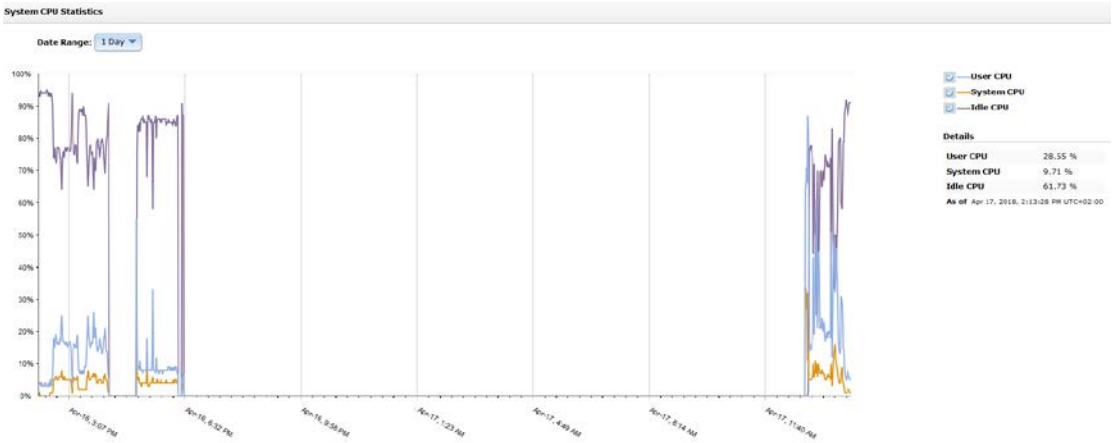

Figure 25: System CPU Statistics

Systems graphs can be represented depending on the conditions and parameters. Data range can be 1/3/7 or 30 days. Additional parameters can be enabled or disabled on the right side of the graph.

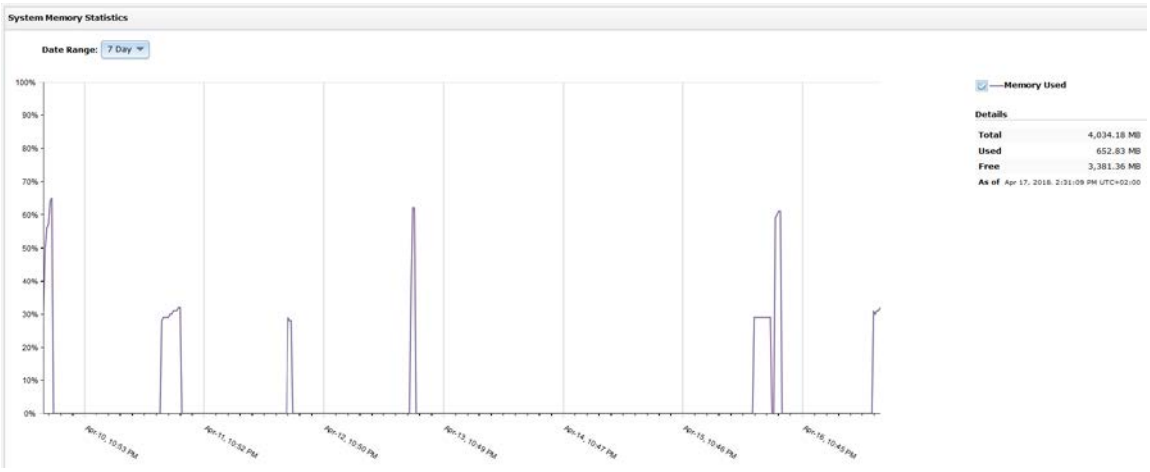

Figure 27: System Memory Statistics

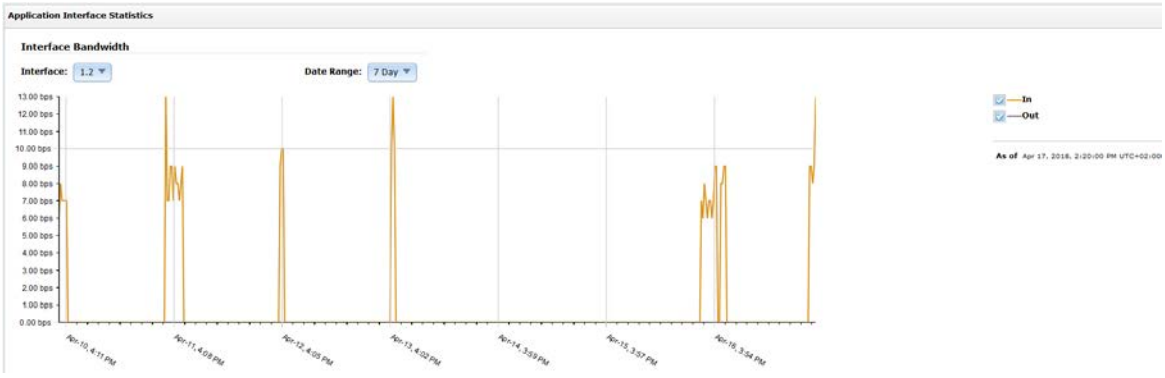

Figure 26: Application Interface Statistics

Monitoring on ISAM appliance can be externalized by using Simple Network Management Protocol (SNMP). Appliance supports both SNMP Agentless Monitoring and SNMP System Alerts. Main components of SNMP are SNMP Managers, SNMP agents and MIB's.

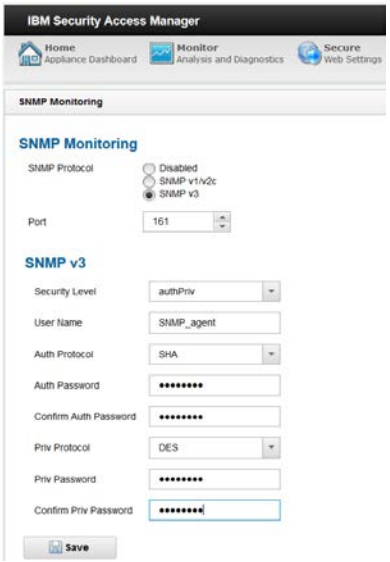

Figure 28: SNMP Monitoring configuration

SNMP agent is a program that is responsible for information gathering, organization of that data and sending the required information to SNMP Manager using SNMP protocol.

SNMP Manager is a computer that queries SNMP agents for information. Management Information Database (MIB) is hierarchical, pre-defined structure that stores information from SNMP agents.

Due to lack of password encryption and implementation difficulties in previous versions, recommended SNMP protocol version is 3. Authentication password is protected using SHA protocol and password for privacy passphrase is protected using DES or DES CBC mode. Using the SNMP Walk tool on SNMP manager, results can be queried.

4.8 Access Management Solution Leaders

IBM was named for the leader in the access management worldwide, according to Gartners' research in June 2017. ISAM and cloud identity were tested, along with solutions from 14 other vendors.

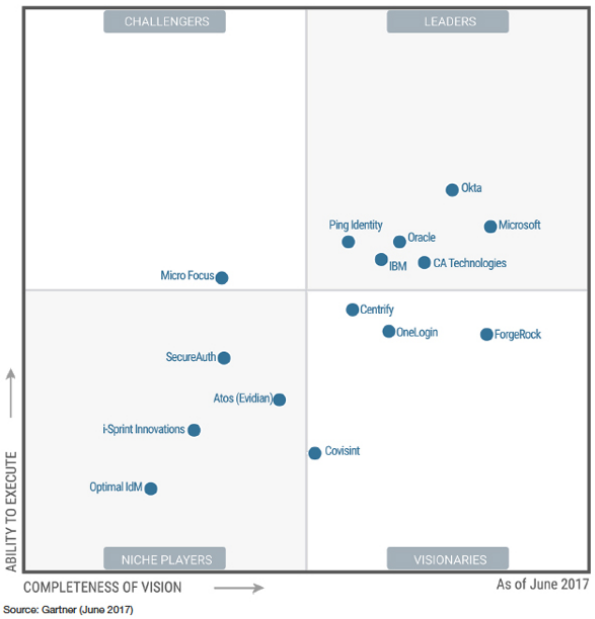

Figure 29: Gartners' Magic Quadrant for Access Management, Worldwide

Access management vendors used in this research: Atos (Evidian), CA Technologies, Centrify, Covisint, ForgeRock, IBM, i-Sprint Innovations, Micro Focus, Microsoft, Okta, OneLogin, Optimal IdM, Oracle, Ping Identity, SecureAuth. [15]

As a **criteria for access management vendors ability to execute** gartner analyzed multiple parameters including product and service, sales activities, market analysis, customer response and others.

As a **criteria for access management vendors completeness of vision**, gartner analyzed market, sales and product strategy, innovation, industrial and geographical strategy.

Conclusion

As the digital era grows and expands, along with it the cyber security threats continue to evolve and adapt, creating a massive damage in digital economy. The uncontrolled and unsecured growth of Internet of Things will continue to threaten cyber security. If not secured, the increased growth of botnet networks made up of hacked IoT devices will produce massive DDOS attacks.

Identity and Access Management solutions will be crucial for protecting the business ecosystems. IAM solutions will also have to protect the IoT systems and provide Identity of Things (IDoT). The concept of identity management will broaden to include what users own, use and share. [16]

The cloud will provide businesses with the ability to quickly and efficiently transform their processes, embrace the digital transformation and use its benefits. Digital security is a vital part of the transition to the cloud. It should and must be the foundation of cloud-based business mindset of companies. According to Oracles research by 2020 it is predicted that 87% of businesses will deliver a multi-channel experience and 67% will interact with customers via mobile apps supported by cloud services. [17]

API Economy will be the crucial part of the chain for organizations and their development. According to Gartner's predictions ¾ of all leading businesses in the world will open up to public APIs. Along with APIs, the biggest shifts in the market will be the increased use of Internet of Things, cognitive, AI and hybrid technologies, Big Data and intelligent cyber security solutions.

Predictive analytics, machine learning and artificial intelligence will be an essential part of every security solution. These concepts will produce security solutions that are more intelligent and give them the ability to learn from previous actions so they can predict and prevent attacks on time. Adaptive and behavior-based authentication will be commonly used, providing more effective and efficient authentication mechanisms.

However, having technology is not enough, people are the most important link of the chain. Digital transformation in not only about changing the technologies, it is also about changing the approach to people, appreciating their work, investing in their knowledge and making them the main engine for the digital revolution.

5 References

[1] Shahyan Khan, “Leadership in the digital age – A study on the effects of digitalization on top management leadership”, Stockholm University, June 2017

[2] Managing Risk and Security at the Speed of Digital Business, February 2016, from https://www.gartner.com

[3] Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payments, from https://ec.europa.eu/commission

[4] European Union General Data Protection Regulation (GDPR), from http://www.eugdpr.org/

[5] European Union General Data Protection Regulation Key Changes, from http://www.eugdpr.org/key-changes.html

[6] Jean Diederich, “API Economy, Why Public API’s are so important”, October 2017

[7] Shahnawaz Backer, James Darwin, Vasfi Gucer, Chris Hockings, Trevor Norvill, Nilesh Patel, Martin Schmidt, Asha Shivalingaiah, Serge Vereecke, “IBM Security Access Manager Appliance Deployment Patterns”, October 2015

[8] IBM Security - Federated Identity Management and Web Services Security with IBM Tivoli Security Solutions, October 2005

[9] IBM Software - IBM Tivoli Federated Identity Manager, February 2013

[10] Advanced Access Control administration, from https://www.ibm.com/

[11] Oauth2 support, from https://www.ibm.com/

[12] Docker support, from https://www.ibm.com/

[13] IBM Security Access Manager 9.0.4, from https://www.ibm.com/

[14] Docker image for Security Access Manager, from https://www.ibm.com/

[15] Magic Quadrant for Access Management Worldwide, https://www.gartner.com

[16] Ray Wagner, “Identity and Access Management 2020”, ISSA Journal, June 2014

[17] Oracle - How digital security can enable the journey to the cloud, 2016