Identity Governance Access(Saviynt)

Project report submitted in partial fulfillment of the requirement for the degree of Bachelor of Technology
in

Computer Science and Engineering/Information Technology

By

Kajal Singal (181414)

Under the supervision of

Dr. Yugal Kumar

to

Department of Computer Science & Engineering and Information Technology
Jaypee University of Information Technology Waknaghat, Solan-173234, Himachal Pradesh

Candidate’s Declaration

I hereby declare that the work presented in this report entitled **“ Identity Governance Access”** in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering/Information Technology** submitted in the department of Computer Science & Engineering and Information Technology**,** Jaypee University of Information Technology Waknaghat is an authentic record of my own work carried out over a period from February 2022 to may 2022 under the supervision of **(Dr. Yugal Kumar)** (Assistant Professor(Senior Grad) and Computer Science and Engineering & Information Technology).
The matter embodied in the report has not been submitted for the award of any other degree or diploma.

Kajal Singal
181414

This is to certify that the above statement made by the candidate is true to the best of my knowledge.

(Supervisor Signature)
Dr. Yugal Kumar
Associate Professor
Computer Science and Engineering & Information Technology
Dated:

ACKNOWLEDGEMENT

I would like to thank and express my gratitude to the project supervisor Dr. Yugal Kumar for his constant support and guidance. This project would not have been possible without his help. I would always like to give a big thanks to my mentors in Saviynt who help me in each and every step of this wonderful learning experience. This project taught me many new things and each concept was very interesting. I would also like to express my thanks to the lab assistant for contacting me and helping me in finishing the project within the stipulated time period.

Last , I would like to thank my friends and family for their support and love.

Kajal Singal(181414)

TABLE OF CONTENT

LIST OF ABBREVIATIONS

HTTP	HyperText Transfer Protocol
URL	Uniform Resource Locator
URI	Uniform Resource Identifier
SSL	Secure Sockets Layer
CA	Certificate Authority
SOAP	Simple Object Access Protocol
RESTful	Representational State Transfer
WSDL	Web Services Description Language
Hmac	Hash-based message authentication code
IKE	Internet Key Exchange

LIST OF FIGURES

CHAPTER - 1
INTRODUCTION

1.1 INTRODUCTION

With the transformation of the world in the digital world and with the companies having huge amounts of work labor, there is a need for a good and Identity governance system. It will work as a game changer for organizations as they have sensitive data and are moving towards the offsite information and using serverless over on-premise information. With the increase in the cloud services, there is a need for IAM policies for Software-as-a-Service application, on-premise and hybrid infrastructure. Each of these infrastructures have their own distinctive definitions and necessities. This also creates trouble in making a holistic IAM policy for IT enterprises. Ignoring it, there are similarities that simplify the creation of required IAM policies.

What is an Identity and Access Management Policy?

To have access control IT infrastructure, identity access management policies are required. They are different from cybersecurity policies which are present in written form. These IAM policies align with the business. Good IAM policies ensure that the specific users have access to the required and allowed resources for the required or allowed time period for the reason.

Why is it difficult to create an IAM policy?

Problematically, complex, integrated architectures typically produce poor end-user expertise. As your organization scales and incorporates new technologies you will end up troubled to make a holistic, unified identity and access program. Several organizations complain that their current IAM methods lead to:

- Lost Productivity: Users need to wait for the approval of the IT administrator for the required resources after requesting for the access.

- Poor User Experience: Individual accounts are required for each resource requested by the user and it becomes a difficult task.

- Siloed Applications: Due to the weak interconnection between applications, there is difficulty in sharing common data between the users. .

- Increased Administrative Cost: Due to multiple accounts for the resources, IT administrators take a large amount of time to respond to the problems like password management faced by the users. The problem occurs because of poor user experience.

- Increased Information Security and Compliance Risk: The risk of violating audit and compliance policies due to an increase in the number of applications and access points.

Dynamic policies are needed for the IT world. As mentioned earlier, by looking at the available online material, we can conclude that they require different definitions for users, roles and attributes. We can add another layer of definitions for them by using connecting collaboration tools like Box and O365. These roles and access change with the time period as the position of the user changes in an organization. This makes everything dynamic, Applications, users, roles, all are dynamic. So, to create good and efficient IAM policies, a flexible and dynamic approach should be followed.

1.2 Problem Statement

With the evolution of the digital era, there is an evolution of in the definitions of users for noth human and non-human. The process which used to historically contemplate user's hands members or human contractors, now embraces methods like robotic method automation(RPA), Internet of things(IoT), programmatic functions and repair accounts. Users that can be human or virtual are digital representation. These identities are the ones that interact with data systems, software and data. For authenticating its access, these identities are given credential to make it acceptable to the resources. After providing the credential these identities are given permission inside the required system or application so that they can perform the job or role for which they are granted the permission. After creating the required IAM policy, we like to create a baseline definition for it, so that all the users can use it. The trouble faced by a modern IT infrastructure is the missing unified definition across the scheme, for eg, the United Nations Agency has different infrastructure and there is a struggle for a unified definition of "users". The reason for this struggle is as follows:

- AWS: A human identity is the title.
- Azure: a human identity is defined as an individual in its Active Directory.
- Google Cloud Platform: There is no use of "users". It refers to a "Google account" as an associate degree making email of the user related to the google account.
- Alibaba: It uses a different term known as " RAM-user" for identity purposes.

The absence of an efficient approach for IAM policies makes it very difficult for the organizations to cope up with the increasing infrastructure in IT enterprise. The continuous change in the identities as they leave/join/move become a burden on the organizations. The provisioning and deprovisioning creates trouble for them. Thus, a huge number of orphan accounts remain active which increase the security risk since they are left and are unmonitored and forgotten.

1.3 OBJECTIVE

- To provide help to the organizations by customizing the product for managing the employees.
- Keeping a track of all the access provided to each employee and observing their activities.
- A very user friendly UI and easy to learn to use.

Saviynt products use artificial intelligence and usage data analytics to provide the cohesive and efficient IAM policies.These policies are comprehensive, can be used across different applications and support cloud-platforms. Saviynt product creates authoritative identities with the help of intelligent analysis done and reconciles the identity definitions.The enterprises can shape the request or verify or review methods due to our intelligent analytics. For the proper use of the resources, our product does comparison between the attributes of the user requesting the resources to the user already having the similar attributes. This helps in deciding the time period and access requirements. If the product finds dissimilarities between the information, it puts the request for the review. Further, this analysis helps the organizations to take care of the standards and other controls. If there is any SOD violation, our analysis successfully finds it and the platform alerts the administrators to take preventive actions. The cloud PAM lets the organizations monitor the accounts with privileged access on all the infrastructure i.e. on premise, cloud and hybrid. This helps in producing an efficient, identity-based information security program. This Cloud PAM discovers and corrects the risky workloads , instances , containers and alternative code-based identities by providing a time period for detection and monitoring.

1.4 Important Terminologies

1.4.1 HTTP:

It is a machine readable text which is used in transfer of files between systems. It is associated with the application layer within the internet protocols for distributed, cooperative, interactive multimedia info systems. It is a communication and transfer protocol. It is the basis of knowledge for the transfer or communication across the globe. These machine readable text holds the hyperlinks through which the users can get the required resources simply by clicking on the link etc.

Tim Berners-Lee started the development of these protocols back in 1989. This communication protocol can be summarized in a document that describes the behavior of a client and server having the primary communication. The protocol was named 0.9.

The first version evolved into the present one. Then, it became the detailed version. This detailed version has the primary draft with the information of the future version 1.0.

Requests for Comments started many years after the development of protocol. It was the result of the work done together by the Internet Engineering Task Force(IETF) and the World Wide Web Consortium(W3C). The entire work was moved to IETF later.

In 1996, HTTP/1 was finalized and was documented. This version was named 1.0. In 1997, its version 1.1 came. Further versions were the update of this, and they were released in 1999 and in 2014.

Now, over 75% of the internet sites use HTTPS which is the secure variant of HTTP.

Features of HTTP:

1. It is a plain language and human readable.
2. It is a stateless protocol which means each and every request is unique and is independent.
3. HTTP works based on request/response pairs. First, a request is made. A HTTP method is used for doing so. Then there is a response. This response has an HTTP status code.

HTTP Header:

They are used to pass information between client and server. Unlike protocol itself, they are human readable. They are present in name value pair and are separated by colon. They can transfer any standard or custom type of information.

- If the server wants to save some data for a period then it will send a cache header. These headers tell the browser what files to save, whether cached files should be updated and for how long they should be kept.

- Headers are used to provide information about server and client. This can be anything from date and time information about request response pair to a user agent header identifying the client, a server header identifying the software application, proxy information, security information, cross origin resource sharing information etc.

- With the modern technologies, HTTP2, a link can be sent as a header which pushes a file before requesting.

Anatomy of a Request Header:

It is a message that a client sends to a server while making an HTTP request to perform some action on the targeted resource.

Client starts the action by specifying the method and the targeted resources by using a regular URL. Then, It starts to list out the files types, languages types and encoding types it accepts by adding a user-agent header, using the referer header to inform the server about its location and to keep the connection alive for the future requests. In order to not save a file, cache control is set to zero for the current file.

Anatomy of Response Header:
It declares the status of the response, the server type, the date and time of the response message, the content type of the return data and other information.

HTTP Methods:

1. GET: This method requests the target resource to tell us about its state. The main purpose of this method is to get the information about the state of the resource and it does not affect resources in any way.The use of this method is considered safe compared to the use of POST method for retrieving information. It is self-addressed through the uniform resource locator. The responses we receive using this method are eligible for caching.So, we can save the information. They can be bookmarked and shared. The W3C has a principle saying, “Web application style ought to learn by the higher principles, however conjointly by the relevant limitations.”

2. POST: The Post requests that the target resource method has the illustration empowered within the request within the request consistent with the linguistic of the target resource. For instance, it is used for posting a message to an online forum, subscribing to a list, or finishing an internet looking deal.

3. PUT: The requests that the target resource produces or updates its state with the state outlined by the illustration coordinate within the request. A distinction from POST is that the shopper specifies the target location on the server.

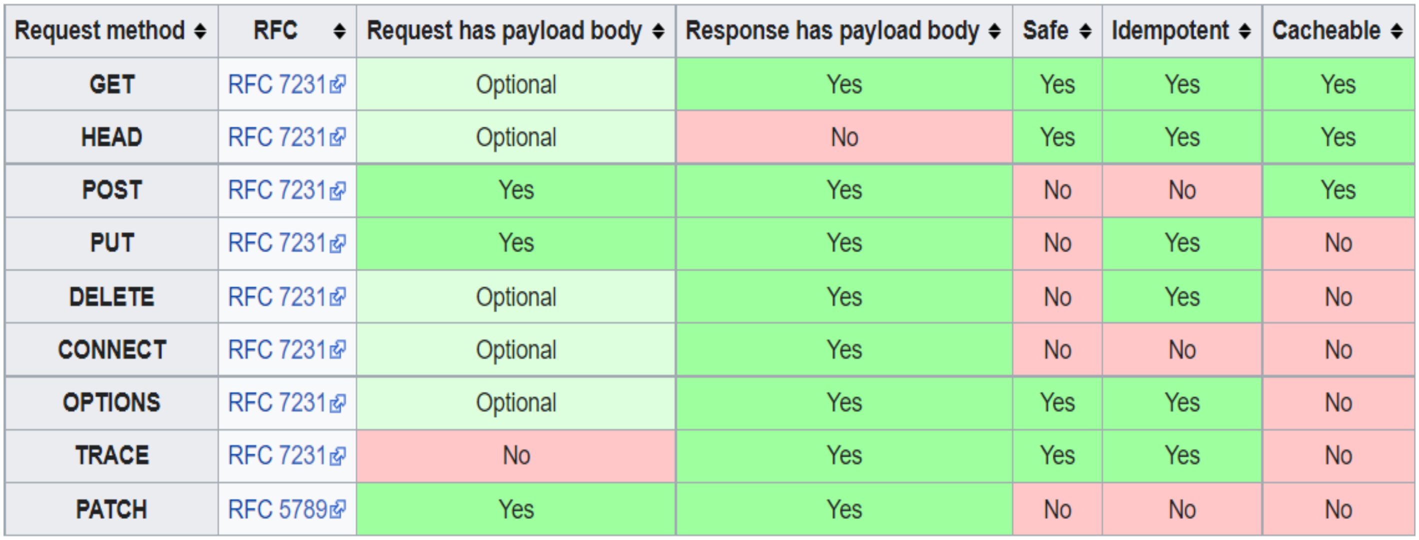
4. PATCH: The PATCH methodology requests that the target resource modify its state consistent with the partial update outlined within the illustration fencelike within the request. This may save information by changing a district of a file or document while not having to transfer it entirely.

5. DELETE: It makes the resource delete its state..

6. HEAD: The HEAD requests that the target resource transfer an illustration of its state, as for a GET request, however while not the illustration information encircled within the response body. This is often helpful for retrieving the illustration information within the response header, while not having to transfer the complete illustration. Uses embody checking whether or not a page is accessible through the standing code and quickly finding the dimensions of a file (Content-Length).

7. OPTIONS: This method is used to transfer the supported HTTP methods. We can use this method for fetching the functions of a web server by using "*" instead of the resource.

8. TRACE: This method allows us to get the received request in the response body so that we can keep a record of the changes made by the intermediaries.



Request method	RFC	Request has payload body	Response has payload body	Safe	Idempotent	Cacheable
GET	RFC 7231	Optional	Yes	Yes	Yes	Yes
HEAD	RFC 7231	Optional	No	Yes	Yes	Yes
POST	RFC 7231	Yes	Yes	No	No	Yes
PUT	RFC 7231	Yes	Yes	No	Yes	No
DELETE	RFC 7231	Optional	Yes	No	Yes	No
CONNECT	RFC 7231	Optional	Yes	No	No	No
OPTIONS	RFC 7231	Optional	Yes	Yes	Yes	No
TRACE	RFC 7231	No	Yes	Yes	Yes	No
PATCH	RFC 5789	Yes	Yes	No	No	No

Figure 1: Properties of Request Methods

HTTP Status Code:

An HTTP request always gets a response irrespective of the correctness of the response or the process was not executed successfully. Each response has a status code. This code tells about the execution of the HTTP request. Clients use this code to know whether the request is successfully handled or not.

They are:

1. 100: These codes appear rarely. They are used to inform the client about the status of the server. Examples:
   - 100 Continue -: It tells that the server has received the request header and is ready for the rest of the request body.
   - 102 Processing -: Tells the client to wait for the server to finish.

2. 200: These codes are used when a request is successfully received, understood and accepted. Examples:
   - 200 OK -: It means the request was successful.
   - 201 Created
   - 204 No Content

3. 300: They indicate redirection. The client is provided with the new URL to follow to get the requested resources. Examples:
   - 301 Moved Permanently
   - 302/303 Found at this other URI -: It means the resource is temporarily redirected to the other URI.
   - 307 Temporary redirect
   - 308 Permanent redirect

4. 400: The request contains bad syntax or cannot be fulfilled. Examples:
   - 400 Bad request
   - 401 Unauthorized
   - 403 Forbidden

- 404 Not Found
- 405 Method Not Allowed

1. 500: They are used as status code when the server is not able to fulfill a valid request. Examples:
    - 500 Internal Server Error -: IT means that something went wrong on the server.
    - 502 Bad Gateway -: Server acts as a literal gateway or proxy
    - 503 Service Unavailable

1.4.2 Browser

A web browser (also known as an Internet browser or just a browser) is an application software package for accessing the planet Wide net or a neighborhood website. Once a user requests an internet page from a specific web site, the net browser retrieves the mandatory content from an internet server so displays the page on the user's device.

1.4.3 Server

The hardware or software programs that give practicality to the functionality of the programs or devices are known as “clients”. This type of model is known as server-client model. Servers provide functionalities to the numerous programs. These functionalities are known as “services”. Some common services are sharing information or resources among multiple clients etc. One server provides functionalities to different clients and one client receives services from different servers. Different clients can connect to each other equivalently or a client can connect to a server as a distinct device over a network.

1.4.4 Proxy

Proxy acts as a middle person between the server and the client. They can be hardware or software services. Proxy is used when we need to hide the IP address of the server or the client is behind a barrier like a firewall.

1.4.5 URL

URL stands for Uniform Resource Locator. It is a link to resources present on the web. This link can also tell us about the location of the resource on the network and the method of getting it. URL is a particular type of URI. URI stands for Uniform Resource Identifier. They can also be used for file transfer, emails, databases and other applications.

1.4.6 SSL Certifies

To stop the risky steps and unwanted threats, we need to authenticate the website’s identity. For this authentication purpose, SSL certificates are used. These certificates are in digital form. SSL means Secure Sockets Layer. It is a security protocol which connects the web server and web browser in an encrypted way.

Websites should have SSL certificates in order to have online transactions securely and for keeping the information of clients private. The certificate have following content:

- Organization
- URL
- State and Country
- Valid Date Range
- Issuer

Types of SSL Certificates

1. Extended Validation certificates (EV SSL): These certies are used in those websites which include the collection of data and online payments. They are the most expensive.

2. Organization Validated certificates (OV SSL): They provide similar assurance as EV SSL. They are second most expensive. They are used for encrypting the private information of the customers..

3. Domain Validated certificates (DV SSL): They are one of the least expensive certificates and provide minimal assurance. They are used for blogs and informational websites.

4. Wildcard SSL certificates: A single certie can secure multiple sub-domain in a single base domain. The “*” is the common part of the name. Valid subdomain under the same base domain is represented by “*”.

5. Multi-Domain SSL certificates (MDC): They can be used to secure many domains and subdomains.

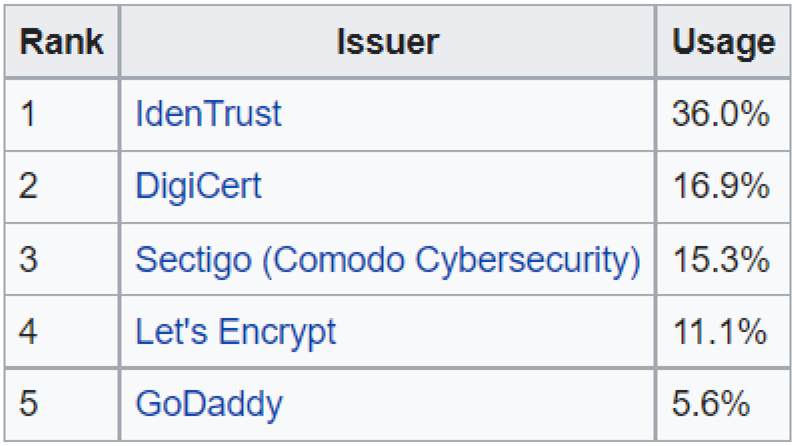
6. Unified Communications Certificates (UCC): Any website owner can use these certificates to allow multiple domain names to be secured on a single certificate.

1.4.7 Certificate Authority

The authorities that issue digital certificates to certify the owner of the public key are known as certificate authorities. Owner of the public key is certified by the name of the certificate. Therefore the relying parties i.e. the party having the private key that corresponds to the public key can rely on the signatures or on the assertion. We can say that certificate authorities are the third parties that are trusted by both, the owner of the public key and the party having the private key..

They are of different levels:

1. Root CA: They are the first level authority. Those are the ones that have the kind of ultimate authority of the internet to decide who is trustworthy and who is not. They are very few so that they cannot handle large volumes.
2. Intermediate CA: The root CAs delegate work and trust the intermediate CAs.



Rank	Issuer	Usage
1	IdenTrust	36.0%
2	DigiCert	16.9%
3	Sectigo (Comodo Cybersecurity)	15.3%
4	Let's Encrypt	11.1%
5	GoDaddy	5.6%

Figure 2 : Top CAs and their usage

1.4.8 Self- Signed Certificate

If a user requires the certificate for working internally usually only on their system, they have a self signed certificate. Users issue these certificates themselves on behalf of the CA. They are public key certificates. They do not cost money and do not have any trust value.

1.4.9 Cryptography

It is the study of techniques for secure communication within the presence of adversarial behavior. Cryptography usually stands for analyzing communication protocols that stops intermediate or extra parties from reading sensitive messages , sensitive or confidential information which include security info , protects information integrity, authentication and non-repudiation. Modern cryptography uses the disciplines of arithmetic technology, applied science and physics. Some applications of cryptography are: e-commerce, online transactions, password management, digital currencies and military communications.

Two types of Cryptography:

1. Symmetric Key Cryptography: In it, the data is encrypted and decrypted using the same key/password.

2. Asymmetric Key Cryptography: Famous with the name "public key cryptography." We have a pair of mathematically linked numbers that are derived from multiplying prime numbers. We end up with two numbers that are linked together and we refer to them as public key and private key. As the name suggests, the private key should be kept secret and secure and the public key can be shared widely.

   The advantage of having two keys is that data can be encrypted by the public using a public key and can only be decrypted by private key.

1.4.10 Web Services

Web services can be known as for eg:

- services offered for the communication between the electronic devices using the World Wide Web, or
- a server. It can request for the resources , documents and lists the requests a single port is handling in the network.

We can transfer machine readable files such as XML and JSON using the web technology present in the web services.

"A web service commonly provides an object oriented Web-based interface to a database server, utilized for example by another Web server, or by a mobile app, that provides a user interface to the end-user. Many organizations that provide data in formatted HTML pages will also provide that data on their server as XML or JSON, often through a Web service to allow syndication, for example, Wikipedia's Export. Another application offered to the end-user may be a mashup, where a Web server consumes several Web services at different machines and compiles the content into one user interface."

Advantages of Web Services:

1. Reusability: Web services are reusable and can be used by multiple systems. Therefore, third parties can develop the services for the organizations. It helps in reducing the development time and produces efficient applications.

2. Language Transparency: A service is initially developed in one language by the service provider. Communication between the service and the client is not affected irrespective of the language of the client.

3. Usability: Easy way to make the data available to other systems in a secure way. The data can be used by a wide range of audiences and platforms.

4. Deployability: They are deployed over standard internet technologies making them easily available on a global level.

Considerations of Web Services:

1. Latency: It is the amount of time taken by a request to return a response. It increases when client and server are running on different machines and can slow some systems down.

2. Partial Failure: It is the name given process when a server fails to respond back to the calling client. It usually happens when the network is down or the server is overloaded with requests. The more the number of web services used in an application, the bigger is the risk.

Common principles for web services are:

1. Authentication: Validating the identity of a client that is attempting to call a web service that accesses secure data. Identity is validated with user credentials such as a username and password.

2. Authorization: It determines the level of client's access. Basic authentication also refers to as basic auth is the simplest protocol available for performing web services authentication over HTTP protocol.

Two main types of web services are:

1. SOAP Web Service: It falls under the messaging protocol. Since this protocol uses XML as language, applications present on different systems and platforms can communicate with others. It also adds an overhead and therefore many other operations like security, transactions and ACID compliance. ACID stands for atomicity, consistency, isolation and durability. To structure the messages and security, rules are also defined by it. There is a file known as WSDL. This file contains information about the service offered by the web service. These documents have all the information including the operations that a web service can perform.

Four Parts of SOAL messages:

- Envelope: A message is transferred inside the envelope. They are starting and ending tags of the messages..
- Header: This part is optional. We can send additional information using the header.
- Body: This part has actual data that the server wants to transmit in XML language.
- Fault: This part is also optional. This part has information regarding the errors faced while the message was processed.

“SOAP issues for enterprise- level web services that require high security and are complex transactions. Examples: APIs for financial services, payment gateways, CRM software, Identity management etc.”

2. RESTful APIs: They are a set of guidelines used by an application developer to design APIs.

   Four principles that APIs follows:

   - URI identifies the data and functionalities of the API. These data and functionalities are known as resources.
   - Certain operations are used to manipulate the resources..
   - There are many formats available for representing resources present on the web like HTML, XML etc.
   - Server never remembers anything about the state of client since the communication between them is stateless.

Benefits of REST:

- Payload: It promotes loose coupling. This means that the system should be designed so that changes and enhancements to web services do not break clients that are already using them.
- Systems that use RESTful API can start small and evolve over time.
- It allows a greater variety of data formats. You can use XML or JSON or something else.
- It adds a lot of flexibility for application developers.
- Lightweight

CHAPTER 2
LITERATURE SURVEY

2.1 Java

Java could be a high-level, class-based, object-oriented programming language that's designed to own as few implementation dependencies as potential. it's a all-purpose programing language meant to let programmers write once, run anyplace (WORA),which means that compiled Java code will run on all platforms that support Java while not the necessity to recompile.[18] Java applications area unit generally compiled to bytecode that may run on any Java virtual machine (JVM) despite the underlying pc design. The syntax of Java is comparable to C and C++, however it has fewer low-level facilities than either of them. The Java runtime provides dynamic capabilities (such as reflection and runtime code modification) that are generally not out there in ancient compiled languages. As of 2019, Java was one among the foremost common programming languages in use in step with GitHub,significantly for client–server internet applications, with nine million developers.

2.1.1 History

James Gosling, Mike Sheridan, and Patrick Naughton initiated the Java language project in June 1991, Java was originally designed for interactive television, but it was too advanced for the digital cable television industry at the time. The language was initially called Oak after an oak tree that stood outside Gosling's office. Later the project went by the name Green and was finally renamed Java, from Java coffee, a type of coffee from Indonesia. Gosling designed Java with a C/C++ style syntax that system and application programmers would find familiar.

Sun Microsystem released the first public implementation as Java 1.0 in 1996. It promised write once, run anywhere (WORA) functionality, providing no-cost run-times in popular platforms. Fairly secure and featuring configurable security, it allowed network and file access restrictions. Major web browsers soon incorporated the ability to run Java applets within web pages, and Java quickly became popular. The Java

1.0 compiler was re-written in Java by Arthur van Hoff to comply strictly with the Java 1.0 language specification. With the advent of Java 2 (released initially as J2SE 1.2 in December 1998 – 1999), new versions had multiple configurations built for different types of platforms. J2EE included technologies and APIs for enterprise applications typically run in server environments, while J2ME featured APIs optimized for mobile applications. The desktop version was renamed J2SE. In 2006, for marketing purposes, Sun renamed new J2 versions as Java EE, Java ME, and Java SE, respectively.

In 1997, Sun Microsystems approached the ISO/IEC JTC 1 standards body and later the Ecma International to formalize Java, but it soon withdrew from the process. Java remains a de facto standard, controlled through the Java Community Process. At one time, Sun made most of its Java implementations available without charge, despite their proprietary software status. Sun generated revenue from Java through the selling of licenses for specialized products such as the Java Enterprise System.

On April 2, 2010, James Gosling resigned from Oracle.

In January 2016, Oracle announced that Java run-time environments based on JDK 9 will discontinue the browser plugin.

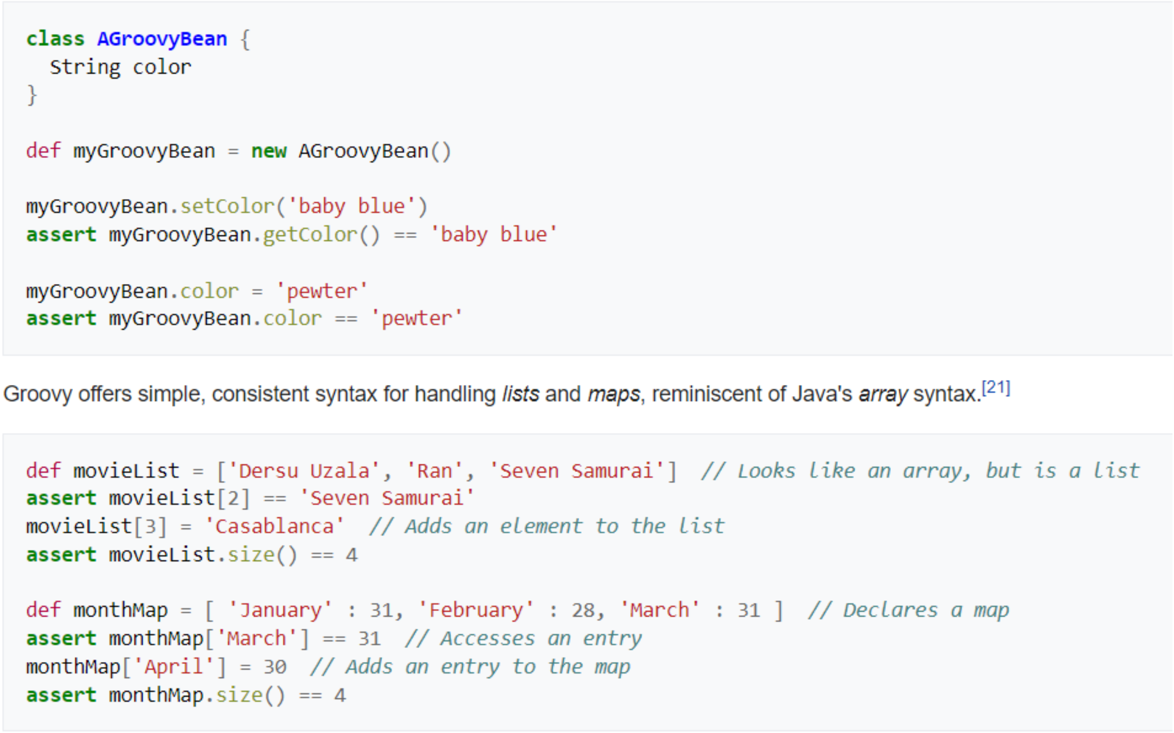
Java software runs on everything from laptops to data centers, game consoles to scientific supercomputers.

2.2 Groovy

Apache Groovy is a Java-syntax-compatible object-oriented programming language for the Java platform. It is both a static and dynamic language with features similar to those of Python, Ruby, and Smalltalk. It can be used as both a programming language and a scripting language for the Java Platform, is compiled to Java virtual machine (JVM) bytecode, and interoperates seamlessly with other Java code and libraries. Groovy uses a curly-bracket syntax similar to Java's. Groovy supports closures, multiline strings, and expressions embedded in strings. Much of Groovy's power lies in its AST transformations, triggered through annotations.

2.2.1 Properties

Groovy implicitly generates getters and setters. In the following code, setColor(String color) and getColor() are implicitly generated. The last two lines, which appear to access color directly, are actually calling the implicitly generated methods.



```
class AGroovyBean {
  String color
}

def myGroovyBean = new AGroovyBean()

myGroovyBean.setColor('baby blue')
assert myGroovyBean.getColor() == 'baby blue'

myGroovyBean.color = 'pewter'
assert myGroovyBean.color == 'pewter'
```

Groovy offers simple, consistent syntax for handling *lists* and *maps*, reminiscent of Java's *array* syntax.[21]

```
def movieList = ['Dersu Uzala', 'Ran', 'Seven Samurai']  // Looks like an array, but is a list
assert movieList[2] == 'Seven Samurai'
movieList[3] = 'Casablanca'  // Adds an element to the list
assert movieList.size() == 4

def monthMap = [ 'January' : 31, 'February' : 28, 'March' : 31 ]  // Declares a map
assert monthMap['March'] == 31  // Accesses an entry
monthMap['April'] = 30  // Adds an entry to the map
assert monthMap.size() == 4
```

Figure 3: Groovy Property

Furthermore, Groovy automatically imports the common libraries. We need not to put the semicolon at the end of statements. It also offers functional Programming.

2.3 Apache Tomcat

Apache Tomcat (called "Tomcat" for short) is a free and open source implementation of the Jakarta Servlet, Jakarta Expression Language and WebSocket technologies. Tomcat provides a "pure Java" HTTP Web Server environment in which Java code can run.

Tomcat is developed and maintained by an open community of developers under the auspices of Apache Software Foundation, released under the Apache License 2.0 license.

2.3.1 Components:

Catalina

Catalina in Tomcat's servlet container. Catalina implements Sun Microsystem' specifications for servlet and JavaServer Pages (JSP). In Tomcat, a Realm element represents a "database" of usernames, passwords, and roles (similar to Unix groups) assigned to those users. Different implementations of Realm allow Catalina to be integrated into environments where such authentication information is already being created and maintained, and then use that information to implement Container Managed Security as described in the Servlet Specification.

Coyote

Coyote is a Connector component for Tomcat that supports the HTTP 1.1 and 2 protocol as a web server. This allows Catalina, nominally a Java Servlet or JSP container, to also act as a plain web server that serves local files as HTTP documents. Coyote listens for incoming connections to the server on a specific TCP port and forwards the request to the Tomcat Engine to process the request and send back a response to the requesting client. Another Coyote Connector, Coyote JK, listens similarly but instead forwards its requests to another web server, such as Apache, using the JK Protocol. This usually offers better performance.

Jasper

Jasper is Tomcat's JSP Engine. Jasper parses JSP files to compile them into Java code as servlets (that can be handled by Catalina). At runtime, Jasper detects changes to JSP files and recompiles them.

As of version 5, Tomcat uses Jasper 2, which is an implementation of the Sun Microsystems' JSP 2.0 specification. From Jasper to Jasper 2, important features were added:

- JSP Tag library pooling – Each tag markup in a JSP file is handled by a tag handler class. Tag handler class objects can be pooled and reused in the whole JSP servlet.
- Background JSP compilation – While recompiling modified JSP Java code, the older version is still available for server requests. The older JSP servlet is deleted once the new JSP servlet has finished being recompiled.

Recompile JSP when included page changes – pages can be inserted and included into a JSP at runtime. The JSP will not only be recompiled with JSP file changes but also with included page changes.

- JDT Java compiler – Jasper 2 can use the Eclipse JDT (Java Development Tools) Java compiler instead of Ant and javac.

Three new components were added with the release of Tomcat 7:

Cluster

This component has been added to manage large applications. It is used for load balancing that can be achieved through many techniques. Clustering support currently requires the JDK version 1.5 or higher.

High availability

A high-availability feature has been added to facilitate the scheduling of system upgrades (e.g. new releases, change requests) without affecting the live environment. This is done by dispatching live traffic requests to a temporary server on a different port while the main server is upgraded on the main port. It is very useful in handling user requests on high-traffic web application.

Web application

It has also added user- as well as system-based web applications enhancement to add support for deployment across the variety of environments. It also tries to manage sessions as well as applications across the network.

Tomcat is building additional components. A number of additional components may be used with Apache Tomcat. These components may be built by users should they need them or they can be downloaded from one of the mirrors.

2.4 Postman

Postman is an API platform for building and using APIs. Postman simplifies each step of the API lifecycle and streamlines collaboration so you can create better APIs—faster.

Postman began out as a venture of software program engineer Abhinav Asthana, who desired to simplify API testing. He released Postman as a loose app withinside the Chrome Web Store. As the app’s utilization grew, Abhinav recruited former colleagues Ankit Sobti and Abhijit Kane to assist create Postman Inc. The 3 co-founders lead the business enterprise today, with Abhinav serving as CEO and Sobti as CTO.

In 2021, Postman turned into ranked #fifty four at the Forbes Cloud a hundred list, up from #fifty nine the preceding year.

CHAPTER 3

SYSTEM DEVELOPMENT

3.1 Different Process

3.1.1 How to obtain an SSL Certificate?

CA issues the SSL certificate according to the requirement of the user. Users can obtain it for from zero to a few dollars. The price of such certificates depends on the level of security. Different CA offers different packages. After deciding the type, one can search for a suitable CA to get the certificate.

- Firstly, we need to prepare the server. Make sure that the "WHOIS" record is correct. This record is matched by the CA before providing the certificate. It should show the correct information abou the company like the company name etc.
- Your company can provide help in this step. We need to generate a CSR.
- Now, this CSR is submitted to the company for validating the domain and details of company.
- After this process, they provide the certificate which needed to be installed.

3.1.2 Handshaking

1. A browser sends a request to a secure server.
2. After receiving the request, the server sends its SSL certificate back to the browser. This certificate helps browsers to trust the server as it contains the public key of the server and the details about it.
3. After receiving the SSL certificate from the server, the browser validates it, usually looking at the expiration date.
4. If the browser finds the server trustable, it encrypts the password with the help of a public key sent by the server. Then, the browser sends the password back to the server..
5. Server uses the private key corresponding to the public key to decrypt the password.

After the above process, a communication link is set up between the browser and the server as they have the same shared password. Now, these two use this secret shared password for all the future communications. They encrypt the data using symmetric key cryptography. Like this , we start the process with asymmetric and moves to symmetric to take the advantages of both the algorithms.

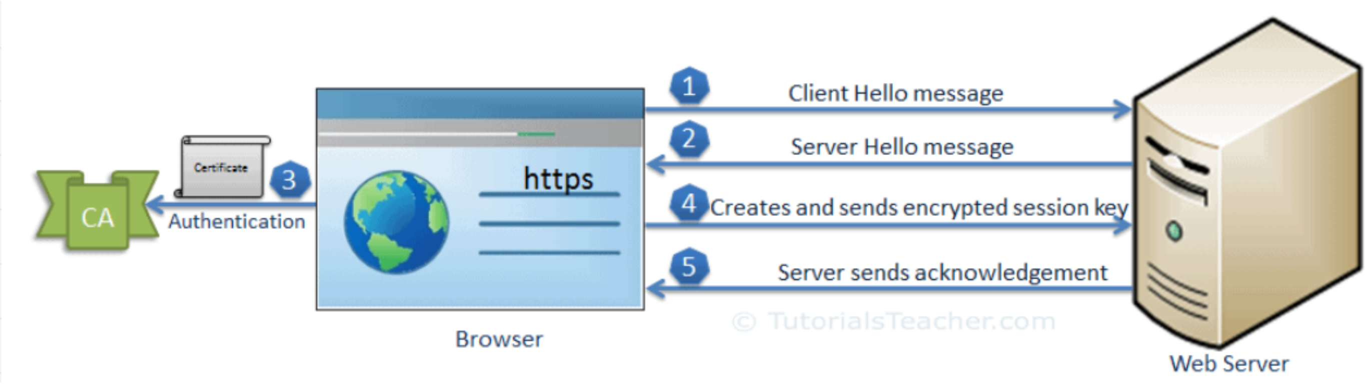


Figure 4: SSL Handshake

3.1.3 HTTP Flow

1. The communication starts when a TCP connection is opened by the browser to the server. This connection ensures the transferring of data from one point to another endpoint. It also assures that the data will not change during transmission. If the HTTPS is used for connection, then the entire process of handshaking occurs and the communication also occurs accordingly..
2. The browser sends HTTP messages. It contains a method and an address pointing to the resource. IT can also contain header like cookie etc.
3. Server performs the requested action and sends back the response. This response has an HTTP status message, header about the response and other information. This data can be HTML documents, CSS etc.
4. TCP connection is closed.

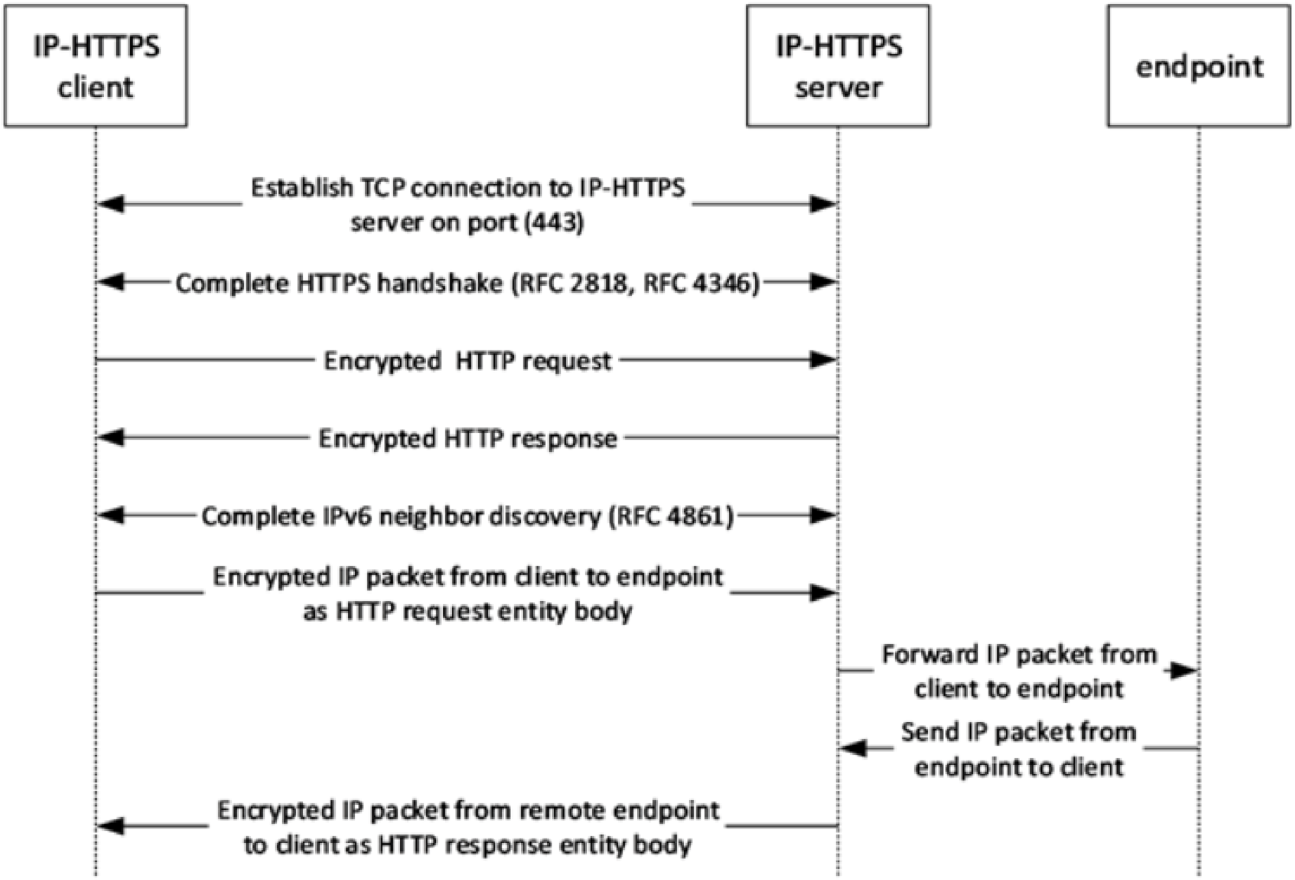

IP-HTTPS client
IP-HTTPS server
endpoint
Establish TCP connection to IP-HTTPS server on port (443)
Complete HTTPS handshake (RFC 2818, RFC 4346)
Encrypted HTTP request
Encrypted HTTP response
Complete IPv6 neighbor discovery (RFC 4861)
Encrypted IP packet from client to endpoint as HTTP request entity body
Forward IP packet from client to endpoint
Send IP packet from endpoint to client
Encrypted IP packet from remote endpoint to client as HTTP response entity body

Figure 5: HTTP Flow

3.2 Softwares Used:

3.2.1 Openvpn

VPN stands for virtual private network. Openvpn is a software which executes some techniques in the backend to create secure point to point connection in routed or bridged configurations and remote access facilities. This software provides the standard norm of authentication like pre-shared secret keys, username/password and certificates. When there are multiple clients for a single server, it provides certificates to each client for authentication by having a certificate authority and signatures. It has many security as well as control features. It uses OpenSSL library and TLS protocol.

3.2.1.1 Architecture

1. Encryption

OpenSSL is used for providing encryption to both the data and the control channels. For adding an additional layer of security to the connection, it uses the HMAC packet authentication.

2. Authentication

As stated earlier, this software uses the standards measures used by several other servers and browsers for providing authentication. Pre-shared keys are one of the easiest methods and certificates are robust and feature-rich. In the new versions, we can also use the username/password method for authentication with or without certificates.

3. Networking

It uses both UDP and TCP for the successful creation of SSL tunnels on a single TCP/UDP port.

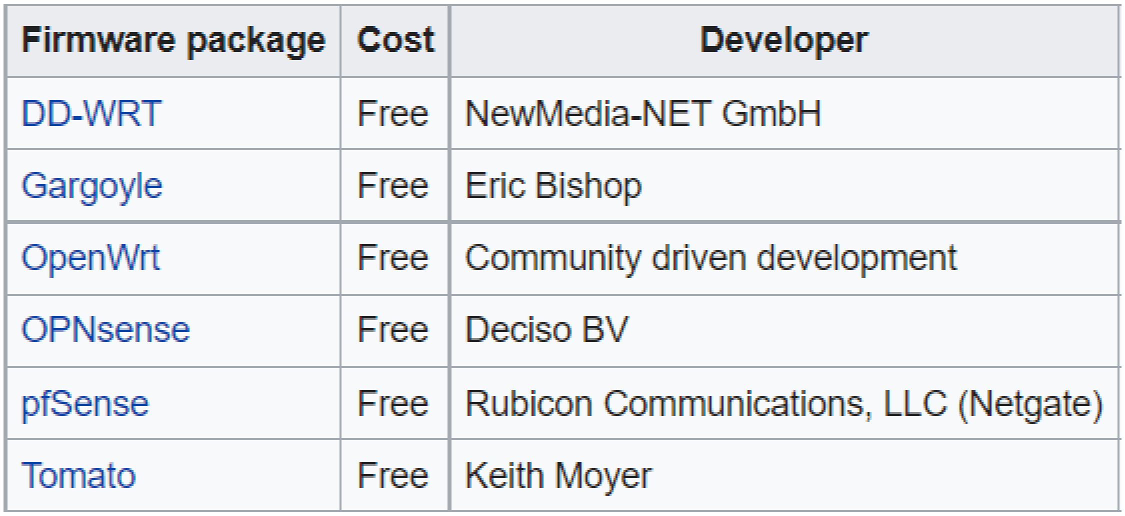
Now, openvpn supports the complete package of IPv6 as protocols. It can even use it for establishing connections. These new protocols help in getting through the proxy servers and getting out of firewalls. In the openvpn server configuration, we can even push certain network configuration options to the clients. It offers two types of interfaces. They are: layer-3 based IP tunnel and layer-2 based Ethernet TAP.

4. Security

With the help of openSSL, it achieves upto 256-bit encryption. Furthermore, instead of using an IP stack for running , it uses userspace. It does not provide support for IKE, IPsec, or PPTP but use SSL and TLS based custom security protocols.

5. Extensibility

Third-party plugins or scripts can be used for the extension of openvpn so that the software can be used with more advanced logging, enhanced authentication ,dynamic firewall updates and RADIUS integration and so on.

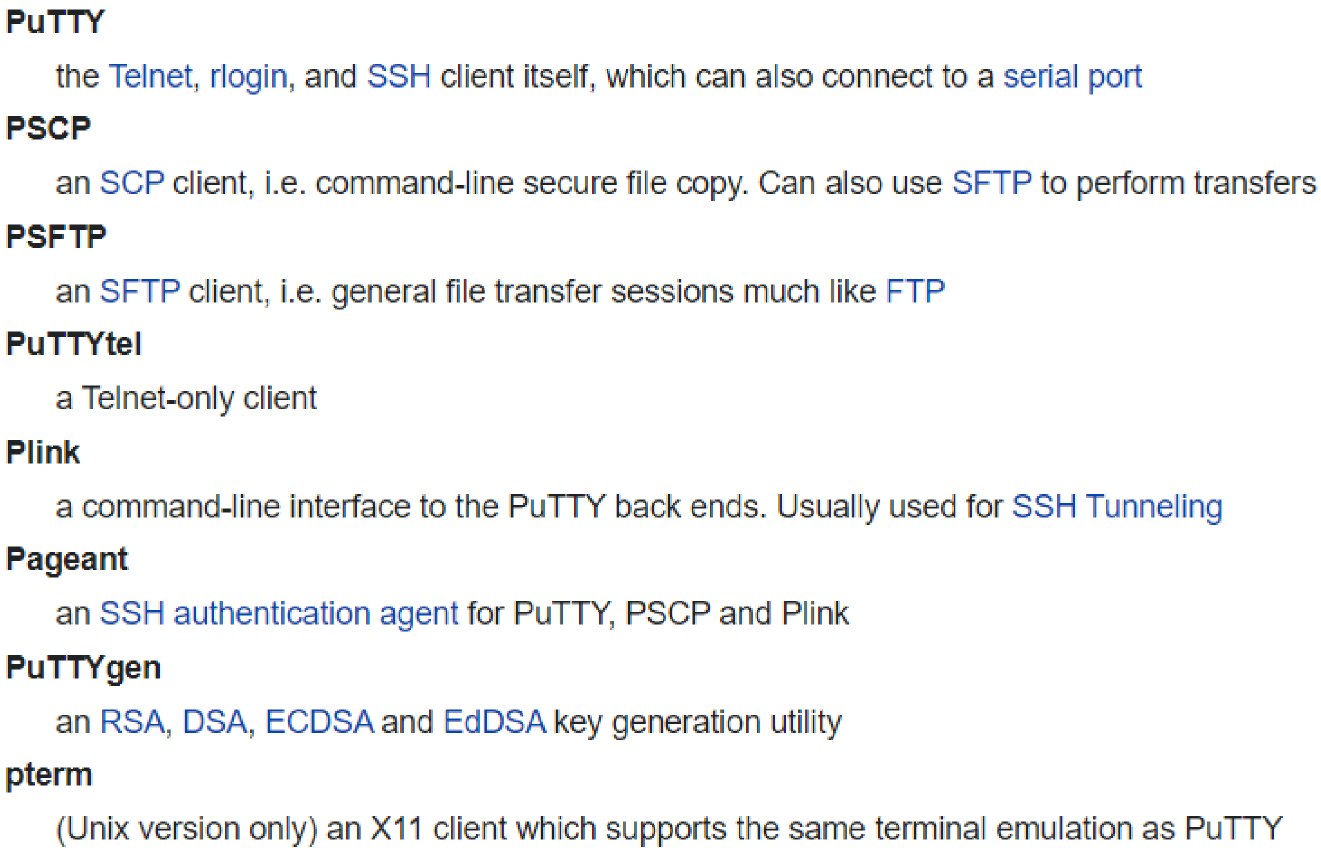


Firmware package	Cost	Developer
DD-WRT	Free	NewMedia-NET GmbH
Gargoyle	Free	Eric Bishop
OpenWrt	Free	Community driven development
OPNsense	Free	Deciso BV
pfSense	Free	Rubicon Communications, LLC (Netgate)
Tomato	Free	Keith Moyer

Figure 6: Notable firmware packages with openvpn integrations

3.2.2 PuTTY

It may sound like the word PuTTY has a full form or any official meaning but in reality, none are present. It is an free and open source terminal emulator which helps in file transmission over a network. It supports various protocols. It was originally written for Microsoft Windows. Now, it can be used for different operating systems. This software was developed by Simon Tatham who is a british programmer and is looking after it.



PuTTY

the Telnet, rlogin, and SSH client itself, which can also connect to a serial port

PSCP

an SCP client, i.e. command-line secure file copy. Can also use SFTP to perform transfers

PSFTP

an SFTP client, i.e. general file transfer sessions much like FTP

PuTTYtel

a Telnet-only client

Plink

a command-line interface to the PuTTY back ends. Usually used for SSH Tunneling

Pageant

an SSH authentication agent for PuTTY, PSCP and Plink

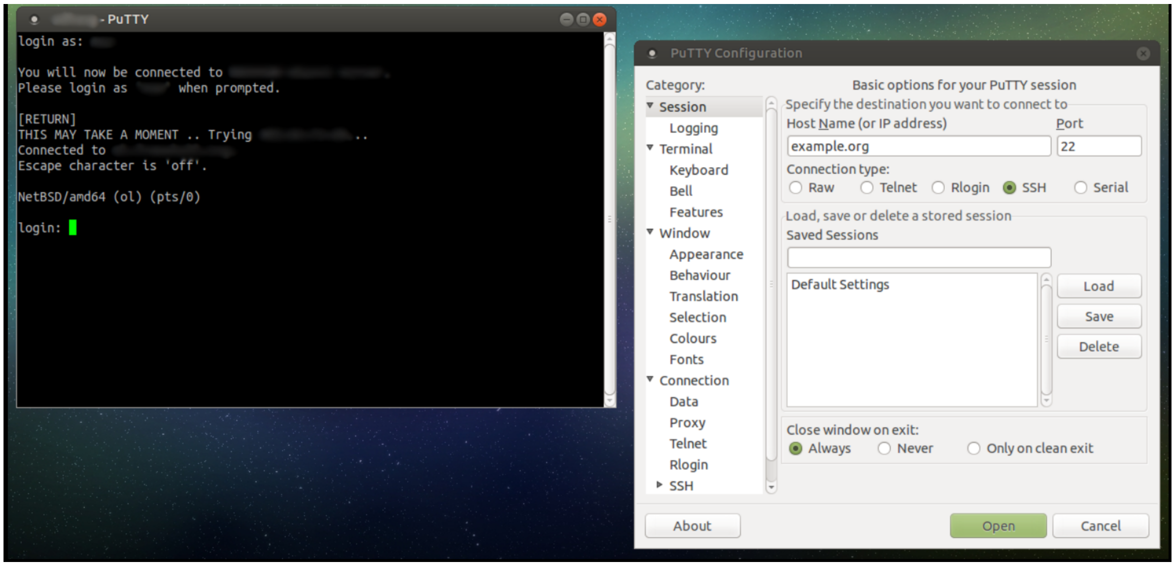
PuTTYgen

an RSA, DSA, ECDSA and EdDSA key generation utility

pterm

(Unix version only) an X11 client which supports the same terminal emulation as PuTTY

Figure 7: Components of PuTTY



```
login as: [redacted]

You will now be connected to [redacted].
Please login as '[redacted]' when prompted.

[RETURN]
THIS MAY TAKE A MOMENT .. Trying [redacted]...
Connected to [redacted].
Escape character is 'off'.

NetBSD/amd64 (ol) (pts/0)

login: 
```

Host Name (or IP address): example.org
Port: 22

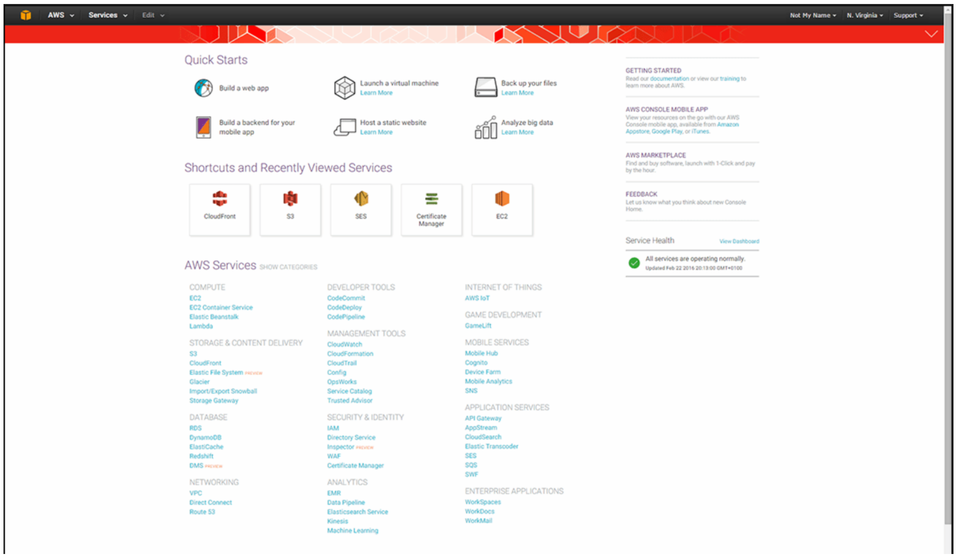
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Close window on exit: ● Always ○ Never ○ Only on clean exit

Figure 8: PuTTY running in Ubuntu

3.2.3 AWS Console

It is a browser based GUI which can be used for controlling features provided by amazon web services. The users can use the drag/ drop for the service links required. Users can also view resources and applications that are sharing common tags. They can use tag editors to view and make quick changes to all the resources and applications sharing common tags. It supports almost all the operating systems.



GETTING STARTED
Read our documentation or view our training to learn more about AWS.

AWS CONSOLE MOBILE APP
View your resources on the go with our AWS Console mobile app, available from Amazon Appstore, Google Play, or iTunes.

AWS MARKETPLACE
Find and buy software, launch with 1-Click and pay by the hour.

FEEDBACK
Let us know what you think about new Console Home.

All services are operating normally.
Updated Feb 22 2016 20:13:00 GMT+0100

Figure 9: AWS console interface

3.2.4 Jumpbox

Jumpbox can be considered as a system that keeps a check of the two dissimilar security zones. It helps in controlling and accessing the devices and information between different security zones present in the same network.

3.2.5 Azure

It is also known as Microsoft azure. It provides cloud computing services which are managed by microsoft data centers. It supports almost all the types of services like software as a service and platform as a service etc and we can use different tools frameworks with azure etc. Azure is extensible.

3.2.6 Amazon Web Services

They provide different cloud computing services and it is a subsidiary of amazon. These cloud computing internet offerings offer dispensed computing processing ability and software program equipment thru AWS server farms. AWS users can work according to their will and whenever they want without any trouble because they are given EC2 service through which a cluster of computer systems is present with the users. These digital systems are almost the exact copy of original systems with almost all the attributes , hardwares and other units.

AWS servers are present in the entire world and the services are offered worldwise with there help. They have different plans for different kinds of customers. They follow a “Pay-as-you-go model”. They charge according to the utilization of the resources like the hardware, number of running systems, softwares used etc. Amazon also ensures the safety of the subscribers and as mentioned operates worldwide with 6 places in North America.

Amazon markets AWS to subscribers as a manner of acquiring large-scale computing ability extra speedy and cost effectively than constructing a real bodily server farm. All offerings are billed primarily based totally on utilization, however every provider measures utilization in various ways. As of 2021 Q4, AWS has 33% marketplace proportion for cloud infrastructure even as the following competition Microsoft Azure and Google Cloud have 21%, and 10% respectively, in step with Synergy Group.

3.2.7 Freshdesk

It is an American cloud based customer engagement company.

Features:

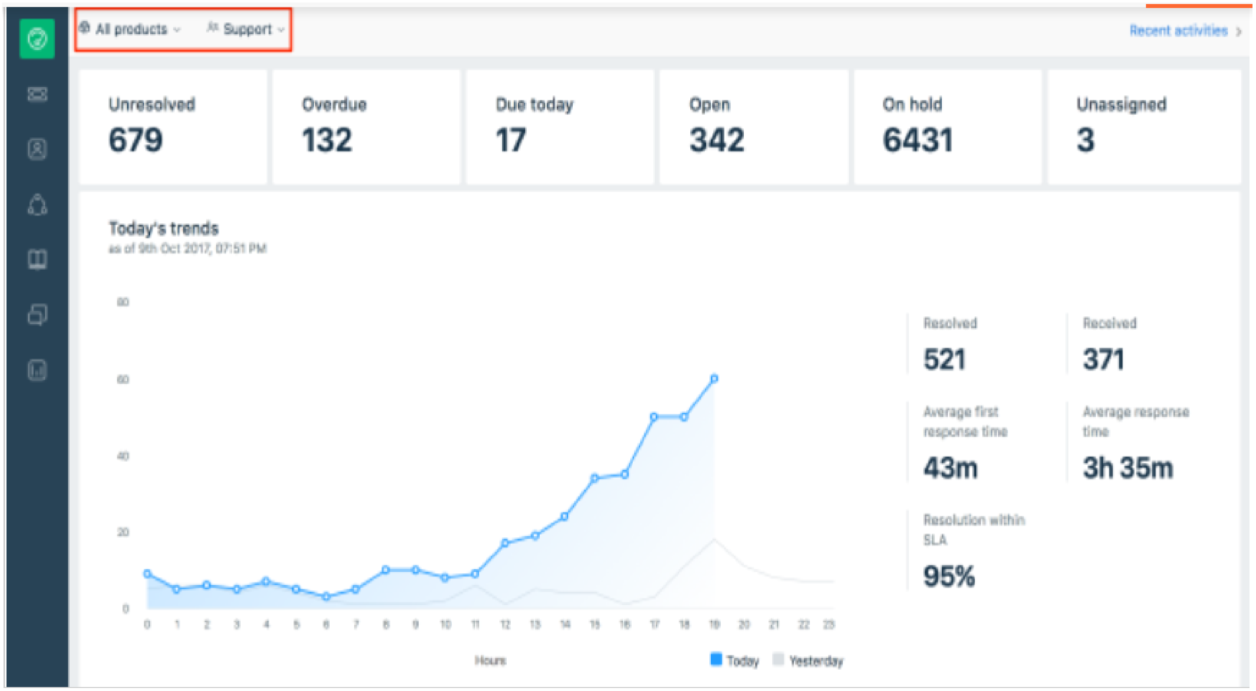
1. Support channels: It has different channels like chat,email, phone, twitter and facebook etc.

2. Productivity hacks:
    - Tags: It helps in categorizing the tickets.
    - Dispatch: Rules can be created for tickets and workflows automation can be done for support.
    - Automatic email notification: Agents and customers are sent an email when changes are made.
    - Canned responses: Templates can be created and saved for reusing while replying to a customer.
    - Customizable help desk:

3. Helpdesk management:
    - Notes: Public notes can be added for informing customers and private notes can be added to inform fellow team members.
    - Ticket Activities: Changes made in the ticket can be viewed in the history for that day.
    - Team Inbox: Shared inbox is present for the team members.
    - Merge Tickets: Tickets from different channels can be merged in chronological order.
    - To-dos: Add a task in the ticket or in the dashboard. Prioritize your work.
    - Freshconnect collaboration: Connect with other team members within the freshdesk.

4. Self- Service:
    - Knowledge Base: Knowledge pages can be created to share important information with customers.
    - Email to knowledge base:

5. Reporting:
    - Default Dashboard: We can view trends in the tickets, recent activities, forums etc.
    - Freshdesk analytics(beta): View performances of agents ,ticket lifecycle, group performance etc.



Unresolved 679

Overdue 132

Due today 17

Open 342

On hold 6431

Unassigned 3

Today's trends
as of 9th Oct 2017, 07:51 PM

Resolved 521

Received 371

Average first response time 43m

Average response time 3h 35m

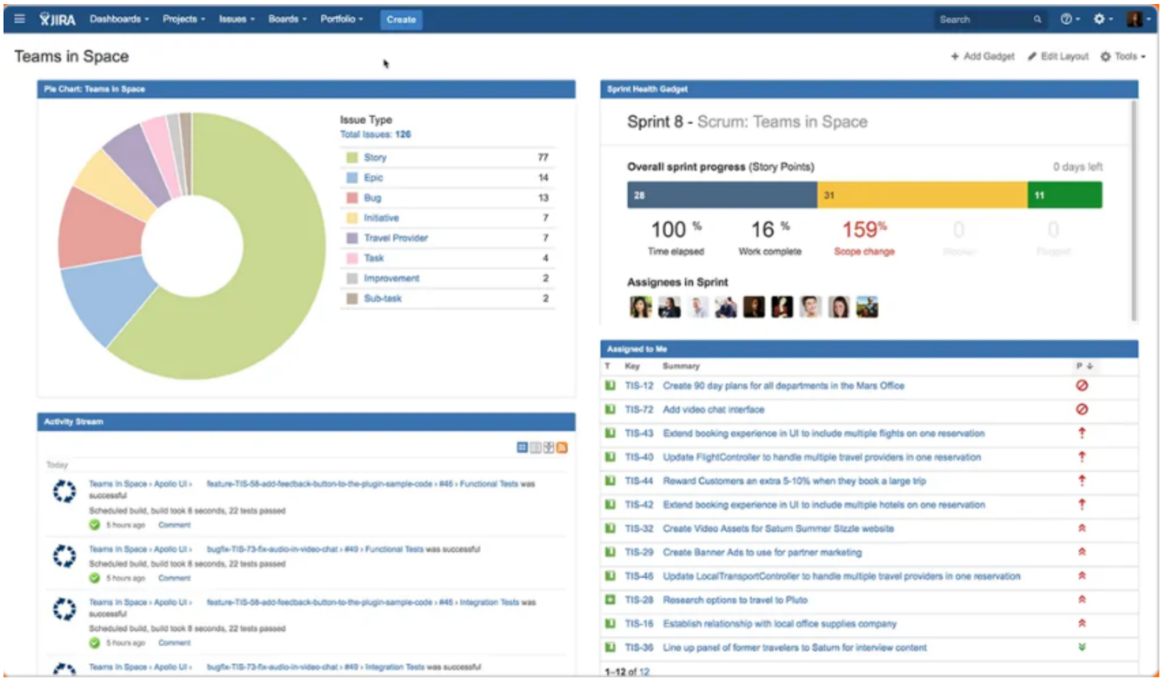
Resolution within SLA 95%

Figure 10: Freshdesk Dashboard

3.2.8 Jira

This software was developed by Atlassian which tracks issues and allows agile project management. Jira is offered in four packages:

1. Jira Work Management: A generic project management.
2. Jira software: It is the base software which includes agile project management.
3. Jira Service Management: It is used for IT operations and business service desks.
4. Jira Align: It is strategic product and portfolio management.



Teams in Space

Issue Type
Total Issues: 126

🟩	Story	77
🟦	Epic	14
🟥	Bug	13
🟨	Initiative	7
🟪	Travel Provider	7
▨	Task	4
▨	Improvement	2
🟫	Sub-task	2

Sprint 8 - Scrum: Teams in Space

Overall sprint progress (Story Points) 0 days left

100 % Time elapsed
16 % Work complete
159% Scope change
0 Blocker
0 Flagged

Teams in Space › Apollo UI › feature-TIS-58-add-feedback-button-to-the-plugin-sample-code › #46 › Functional Tests was successful
Scheduled build, build took 8 seconds, 22 tests passed
✓ 5 hours ago Comment

Teams in Space › Apollo UI › bugfix-TIS-73-fix-audio-in-video-chat › #49 › Functional Tests was successful
Scheduled build, build took 8 seconds, 22 tests passed
✓ 5 hours ago Comment

Teams in Space › Apollo UI › feature-TIS-58-add-feedback-button-to-the-plugin-sample-code › #46 › Integration Tests was successful
Scheduled build, build took 8 seconds, 22 tests passed
✓ 5 hours ago Comment

Teams in Space › Apollo UI › bugfix-TIS-73-fix-audio-in-video-chat › #49 › Integration Tests was successful

Assigned to Me

T	Key	Summary	P ↓
🟩	TIS-12	Create 90 day plans for all departments in the Mars Office	⊘
🟩	TIS-72	Add video chat interface	⊘
🟩	TIS-43	Extend booking experience in UI to include multiple flights on one reservation	↑
🟩	TIS-40	Update FlightController to handle multiple travel providers in one reservation	↑
🟩	TIS-44	Reward Customers an extra 5-10% when they book a large trip	↑
🟩	TIS-42	Extend booking experience in UI to include multiple hotels on one reservation	↑
🟩	TIS-32	Create Video Assets for Saturn Summer Sizzle website	⇈
🟩	TIS-29	Create Banner Ads to use for partner marketing	⇈
🟩	TIS-46	Update LocalTransportController to handle multiple travel providers in one reservation	⇈
🟩	TIS-28	Research options to travel to Pluto	⇈
🟩	TIS-16	Establish relationship with local office supplies company	⇈
🟩	TIS-36	Line up panel of former travelers to Saturn for interview content	⇊

1–12 of 12

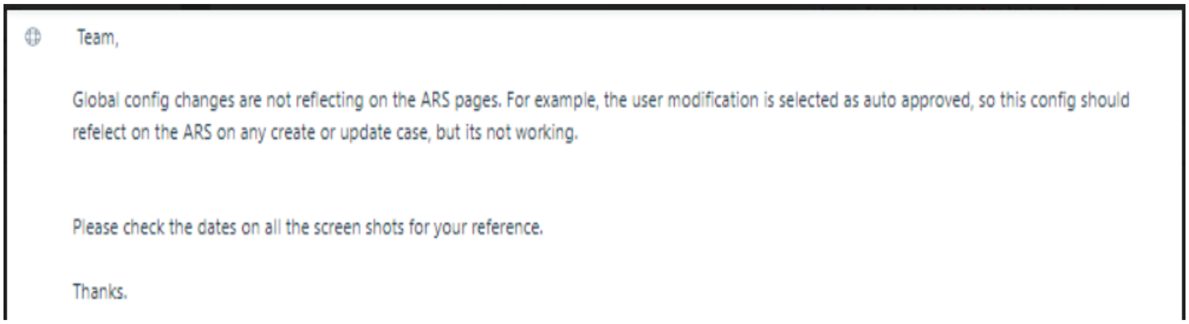
Figure 11: Jira Dashboard

CHAPTER 4

PERFORMANCE ANALYSIS

4.1 Ticket Resolved

One of our customer raised the following ticket:



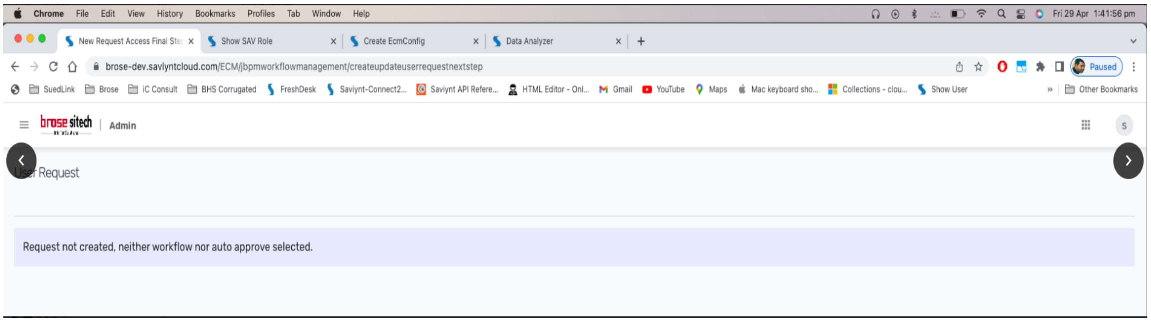
Team,

Global config changes are not reflecting on the ARS pages. For example, the user modification is selected as auto approved, so this config should refelect on the ARS on any create or update case, but its not working.

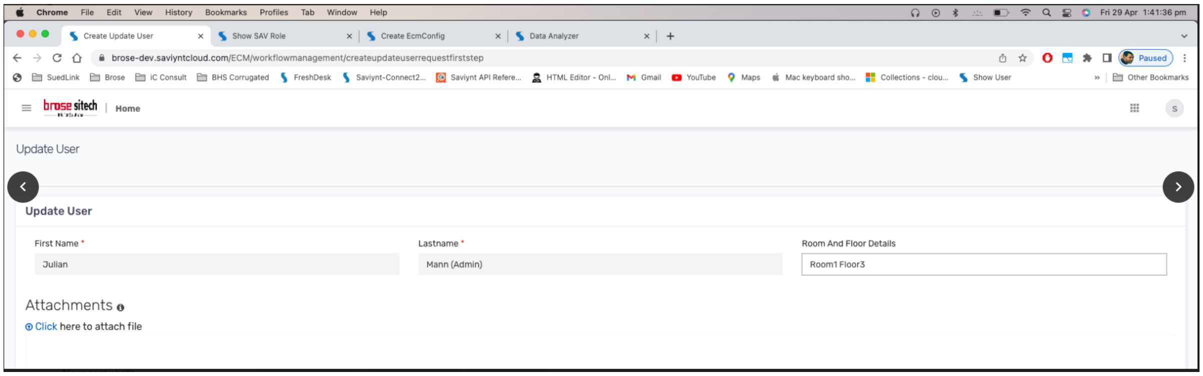
Please check the dates on all the screen shots for your reference.

Thanks.

So, the issue faced by them while using the Saviynt product was that they were trying to update the user that uses the dynamic attribute. But they were unable to change and save the attribute value.So they error they were receiving was as follows:



Request not created, neither workflow nor auto approve selected.


Create Update User
Show SAV Role
Create EcmConfig
Data Analyzer
brose-dev.saviyntcloud.com/ECM/workflowmanagement/createupdateuserrequestfirststep
brose sitech
Home

Update User

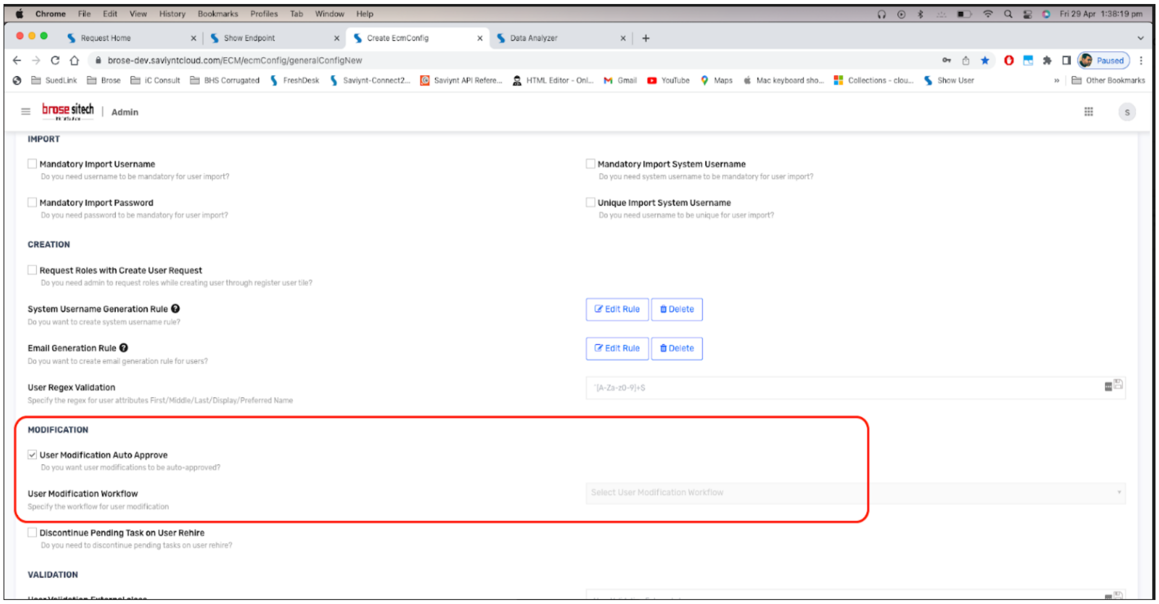
Update User

First Name *	Lastname *	Room And Floor Details
Julian	Mann (Admin)	Room1 Floor3

Attachments

Click here to attach file

In order to understand the error and to check whether the same error occurs when we try to do it, we replicate it in our system. First of all, we check the settings. The most important setting that needed to be checked is marked in the red box below.



IMPORT

□ Mandatory Import Username
Do you need username to be mandatory for user import?

□ Mandatory Import System Username
Do you need system username to be mandatory for user import?

□ Mandatory Import Password
Do you need password to be mandatory for user import?

□ Unique Import System Username
Do you need username to be unique for user import?

CREATION

□ Request Roles with Create User Request
Do you need admin to request roles while creating user through register user tile?

System Username Generation Rule
Do you want to create system username rule?

Email Generation Rule
Do you want to create email generation rule for users?

User Regex Validation
Specify the regex for user attributes First/Middle/Last/Display/Preferred Name
^[A-Za-z0-9]+$

MODIFICATION

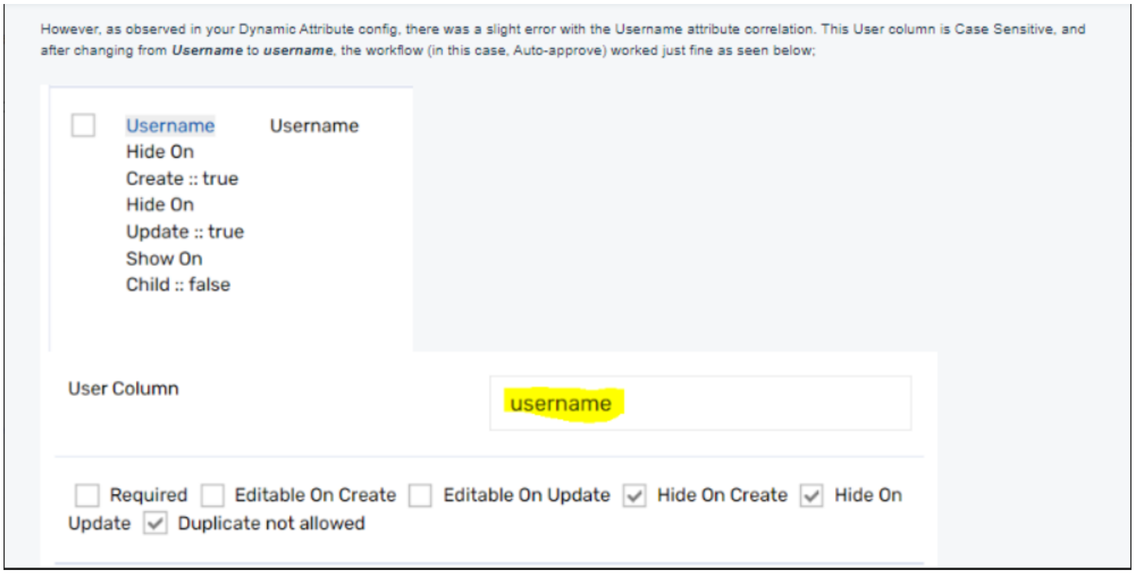
☑ User Modification Auto Approve
Do you want user modifications to be auto-approved?

User Modification Workflow
Specify the workflow for user modification
Select User Modification Workflow

□ Discontinue Pending Task on User Rehire
Do you need to discontinue pending tasks on user rehire?

VALIDATION

Next, we created the same dynamic attributes used by the customer. We found out that while creating the dynamic attribute "username", they were using wrong spelling and the word was not matching with the word used in the database. They were using "Username" instead of "username". The database was :



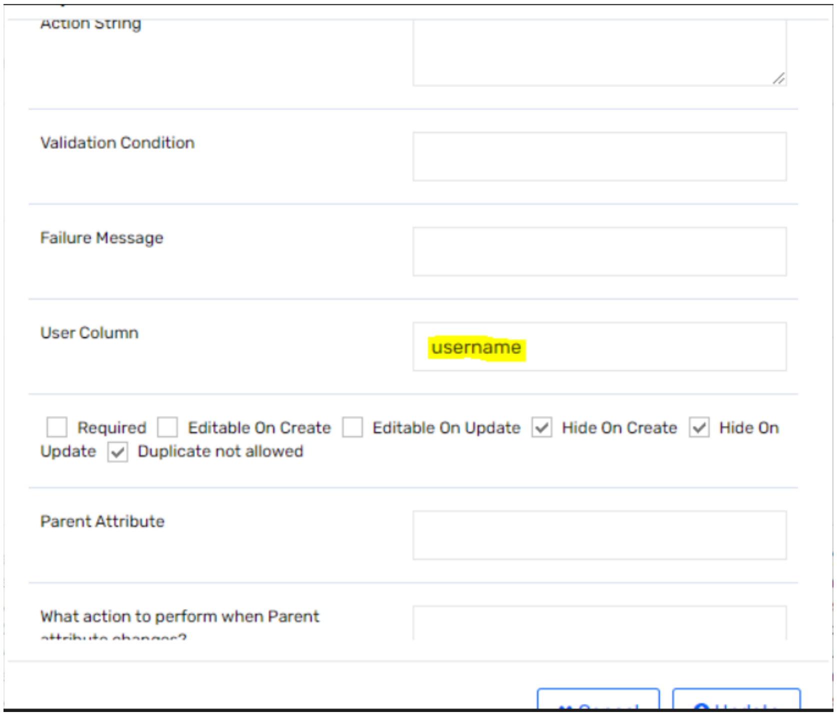
However, as observed in your Dynamic Attribute config, there was a slight error with the Username attribute correlation. This User column is Case Sensitive, and after changing from ***Username*** to ***username***, the workflow (in this case, Auto-approve) worked just fine as seen below;

□ Username Hide On Create :: true Hide On Update :: true Show On Child :: false Username

User Column username

□ Required □ Editable On Create □ Editable On Update ☑ Hide On Create ☑ Hide On Update ☑ Duplicate not allowed

We changed the name of the column/attribute in the form as follows:



Action String

Validation Condition

Failure Message

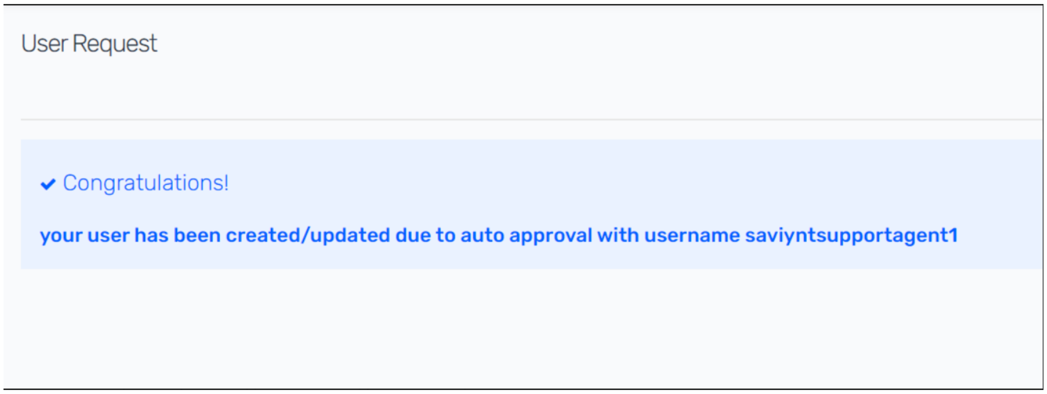
User Column: username

□ Required □ Editable On Create □ Editable On Update ☑ Hide On Create ☑ Hide On Update ☑ Duplicate not allowed

Parent Attribute

What action to perform when Parent attribute changes?

After making the following changes, the issue was resolved.



User Request

✓ Congratulations!

your user has been created/updated due to auto approval with username saviyntsupportagent1

CHAPTER 5
CONCLUSION

5.1 Conclusion

The past one month has been great for learning. The concepts I learnt have cleared my basics. These topics were ones I have not explored before. They raise my curiosity and I wish to learn more. Cyber security is one of the main concerns. Saviynt is on a mission to safeguard enterprises through intelligent, cloud-first identity governance & access management solutions.” Saviynt was created to challenge the status quo. We always realized that identity could be so much more – and the leading solutions weren’t up to the task. So we set out to build the most innovative cloud identity & access governance platform on the market.”

“It hasn’t always been easy, but we’re here to solve challenges, not hide from them. Today we’ve grown into a global organization scaling at breakneck speed to help the largest enterprises in the world transform their identity programs and protect their people, assets, and infrastructure.”

REFERENCES

1.https://www.linkedin.com/learning/introducing-postman
2.https://www.linkedin.com/learning/programming-foundations-apis-and-web-services
3.https://www.linkedin.com/learning/http-essential-training
4.https://www.linkedin.com/learning/ssl-certificates-for-web-developers
5.https://www.linkedin.com/learning/learning-groovy
6.https://www.linkedin.com/learning/learning-apache-tomcat