**ANIL**

**Ph:973-241-1675**

Summary:

* 7 plus years of hands-on experience in installation, configuration, monitoring, troubleshooting, and tuning of multiple API Gateways like Apigee Edge and Apigee X, IBM DataPower Appliances spanning multiple generations of hardware and virtual form factors, administering them and developing solutions to secure web services and RESTful API.
* Proficient in designing, developing, and managing API proxies in Apigee Edge and Apigee X.
* Extensive experience in securing APIs with Apigee X’s OAuth 2.0, JSON Web Tokens (JWT), and API Key Validation to authenticate and authorize users, ensuring secure data exchange.
* Proficient in utilizing Apigee X’s traffic management policies including Spike Arrest, Quota, and Cache to effectively manage API load and optimize performance.
* Proficient in leveraging Apigee’s mediation policies including XSLT, JSON to XML, message logging, and access control to transform and manage API data.
* Strong experience in applying threat protection policies in Apigee such as regular expression protection, JSON threat protection, and XML threat protection to prevent common API vulnerabilities and attacks.
* Expertise in leveraging Apigee X’s out-of-the-box policies such as Assign Message, Raise Fault, Service Callout, and Extract Variables to handle API requests and responses efficiently.
* In-depth experience in debugging API proxy issues in Apigee X using Trace, Debug Sessions, and API Monitoring to identify and resolve problems promptly.
* Proficient in analyzing API logs and metrics in Apigee X to troubleshoot performance issues, security breaches, and other anomalies.
* Expertise in developing custom JavaScript, or Java code to handle complex API processing logic in Apigee X.
* Strong experience in leveraging Apigee X’s features like Virtual Hosts, Environment Groups, and API Products to manage API proxies across different environments.
* Proficient in using Apigee X’s API Gateway to route, transform, and mediate API traffic, ensuring optimal API performance and reliability.
* Expertise in applying Apigee X’s security best practices like SSL/TLS, CORS, and content security policies to secure API endpoints.
* Experience in creating API definitions using OpenAPI Specification (Swagger) and YAML/JSON formats.
* Good at creating and managing SiteMinder policies to define access controls and protect web applications from unauthorized access.
* Good experience in crafting authentication schemes in SiteMinder to validate user identity using various methods such as LDAP, AD, or database authentication.
* Proficient in designing authorization policies in SiteMinder to grant or deny access to web resources based on user attributes and roles.
* Skilled in setting up and configuring SiteMinder realms to group protected resources and apply common access policies.
* Extensive experience in implementing and managing SiteMinder policy domains to organize policies, realms, and rules for efficient management.
* Proficient in using SiteMinder's policy expressions to define complex access rules based on user attributes, resource attributes, and environmental factors.
* Strong knowledge of SiteMinder's policy store and its structure, including objects like realms, rules, policies, and policy domains.
* Experience in migrating policies from one SiteMinder environment to another, ensuring consistency and continuity of access controls.
* Expert in troubleshooting and resolving policy-related issues in SiteMinder, including policy misconfigurations, rule conflicts, and access denials.
* Skilled in leveraging SiteMinder’s policy tracing and debugging tools to identify and fix policy-related problems.
* Proficient in integrating SiteMinder with external data sources such as LDAP directories and databases.
* Extensive IBM DataPower/IBM API Connect Development experience involving developing transformations using XSLT and GatewayScript.
* Hands-on experience in developing and deploying XML, REST, and SOAP-based services using IBM DataPower Gateway, enhancing security, integration, and optimization capabilities.
* Skilled in configuring security features on DataPower, such as AAA (Authentication, Authorization, and Auditing), SSL/TLS, and encryption/decryption to ensure secure data transmission.
* Implemented cryptographic features in DataPower, such as SSL/TLS, XML and JSON encryption/decryption, and digital signatures to ensure secure data transmission and processing.
* Proficient in managing cryptographic objects, including certificates, private keys, and certificate authorities, using DataPower's Crypto tools and secure key storage features.
* Skilled in writing GatewayScript code for DataPower services, enabling advanced processing, transformation, and integration capabilities.
* Proficient in using DataPower's built-in GatewayScript functions and libraries, such as the **session**, **crypto**, and **url** objects, to support diverse processing scenarios.
* Experience in handling production incidents and resolving them, troubleshooting issues in lower environments and performing regular maintenance activities as required.
* Experience with integrating IBM DataPower Gateway appliances with directory servers supporting LDAP, Active Directory (AD), and Identity and Access Management systems like Netegrity SiteMinder to control access to appliances and the services hosted on them.
* Worked on developing several AAA (Authentication, Authorization and Auditing) policies including supporting Kerberos last mile using post processing step.
* Experienced in installing and configuring IBM Cloud Pak for Integration on various platforms, including Red Hat OpenShift and Kubernetes.
* Proficient in using IBM API Connect for designing, developing, and managing APIs, with a strong understanding of RESTful API design principles.
* Familiar with AWS load balancing solutions, such as Application Load Balancer (ALB) and Network Load Balancer (NLB), to distribute traffic and enhance DataPower's availability and performance.
* Strong understanding of containerization, microservices, and cloud-native architectures.
* Expertise in implementing monitoring solutions by forwarding logs to Splunk and creating dashboards off that.
* Experience on enterprise webservice security – X.509 certs, encryption, digital signature, OAuth2.0, SAML and Kerberos.
* Excellent problem-solving skills, with the ability to troubleshoot complex API issues and provide effective solutions.
* Strong communication and interpersonal skills, effectively collaborating with both technical and non-technical stakeholders.

Technical Skills:

|  |  |
| --- | --- |
| Programming Languages: | GatewayScript/JavaScript. |
|  |  |
|  |  |
| Databases: | Oracle Directory Server Enterprise Edition, Oracle Unified Directory, Active Directory, IBM DB2, LDAP. |
|  |  |
| Middleware/Application Servers: | IBM WebSphere, Apigee Edge, Apigee X, IBM DataPower, IBM API Connect. |
|  |  |
| Web Technologies: | XML, XML Schema Language, XSLT, XPath, XQuery, JSON, YAML, JSONiq, SOAP, WSDL, RESTful. |
|  |  |
| Load Balancers: | Citrix NetScaler, F5, AWS ELB, AWS NLB |
| Protocols & Cryptography | SSL(Deprecated), TLS 1.1(Deprecated), TLS 1.2, RSA, ECDHA, AES, DES, Diffie–Hellman, TCP/IP |
|  |  |
| Tools: | Splunk, Elastic Search, Altova XMLSpy, XMLSpy, SoapUI, IBM DataPower Operations Dashboard, Putty, WinSCP. |
|  |  |
| Operating Systems/Cloud: | OpenShift, Linux, and Windows. |
|  |  |

Professional Experience:

**Client: Blue Cross and Blue Shield of Florida (Florida Blue).**

**Role:** Sr IT Systems Engineer

**Duration**: January 2022 to Current

**Project**

**Title:** IBM DataPower /IBM API Connect Administration & Development

**Location:** Jacksonville, FL

**Role:** Sr IT Systems Engineer

**Technologies:** Apigee Edge, Apigee X, GCP, Azure, AWS, IBM DataPower Gateways, XI52, XB62, IDG, IBM API Connect, CA Single Sign-On, LDAP, AD, OpenShift, Docker, Kubernetes, IIS, IBM WebSphere, Apache Tomcat, MQ, DataPower Gateway Script, XSL, XQuery, Java, JavaScript, and JSON, Node.js, JSONiq.

**Responsibilities:**

* Developed API proxies on Apigee Edge and Apigee X, specifically focusing on customizing request and response flows for improved API performance and user experience.
* Implemented API security policies in Apigee including OAuth 2.0, SAML, API Key Validation, and JSON Web Tokens (JWT) to authenticate and authorize users.
* Leveraged Apigee's spike arrest and quota policies to protect APIs from traffic spikes and ensure fair usage among consumers.
* Applied Apigee's cache policy to improve API response times, thereby enhancing the overall performance of the API ecosystem.
* Utilized Apigee's mediation policies, such as XSLT and JSON to XML, to efficiently handle data transformations and facilitate seamless communication between diverse systems.
* Integrated third-party services and backend systems with Apigee proxies using service callout policies and custom code, ensuring data consistency and availability
* Developed comprehensive API documentation using OpenAPI specifications to standardize API communication and improve developer experience.
* Configured SiteMinder to secure web applications, creating and managing web access control policies that defined access rules for protected resources.
* Implemented SiteMinder single sign-on (SSO) to enable users to access multiple applications with a single set of credentials, improving user convenience.
* Customized SiteMinder login pages and error messages to provide a branded and user-friendly authentication experience.
* Managed SiteMinder Policy Store, ensuring that all policies, realms, rules, and policy domains were accurately defined and consistently applied.
* Integrated SiteMinder with LDAP directories and other identity stores, utilizing these sources for user authentication and authorization.
* Configured session management in SiteMinder, defining session timeout values and other related settings to maintain the security of user sessions.
* Monitored and reported on user access and policy enforcement using SiteMinder’s auditing and reporting features.
* Troubleshot and resolved issues related to API proxy behavior, security policy enforcement, and third-party integrations in both Apigee and SiteMinder environments.
* Worked collaboratively with cross-functional teams, including developers, QA engineers, and product managers, to ensure the successful delivery of API solutions and web application security measures.
* Installation and configuration of new DataPower Appliances
* Performed Secure Backup, Secure Restore, System Backup, Import and Export of Configurations, Firmware Upgrade.
* Configuring WSPs, MPGWs and its policy, MQ Queue Managers, XML Managers, FSHs, etc. in Data power
* Implementing access controls to DataPower appliances by integrating with LDAP based directory servers and setting up RBM (role-based management)
* Implemented Multi-Protocol Gateways to support secure RESTful API proxying
* Participated in multiple Disaster Recovery exercises and recovered the DataPower appliances and their configuration to production state
* Executed regular firmware upgrades and rotation of secrets like passwords, keys and certificates
* Configuring DataPower local load balancers to distribute the load to target systems and optimizing connection management using persistence settings and using LDAP connection pools.
* Building DataPower policies using Authentication, Authorization and Auditing (AAA) actions, multiple security protocols
* Hands on coding with DataPower Gateway Script, XSL, XQuery, building DataPower deployment policies and other related objects
* Building the multi-protocol gateway to support message types with different protocols and integrations with MQ
* Integrating with WebSphere MQ
* Trouble-shooting DataPower domain application issues and certificate crypto object issues
* Tuning DataPower objects for any performance issues
* Data power device health check configuration, monitoring and reports generation through monitoring tool
* Creating DataPower objects and provided high level transport level, message level security using AAA, OAuth, JWE, JOSE, Encryption, Decryption, Sign and verify functionalities.
* Troubleshooting connectivity, monitoring the transactions and implemented the log mechanism to push the system logs and API analytic logs to Splunk
* DataPower services transaction monitoring through monitoring tools like Operations Dashboard and Splunk
* Working on middleware architecture and various middleware application servers’ integration.
* Configuring Tomcat or WebSphere application servers
* Solid understanding of data security and network security with a focus on OSI reference model Layer 2- Layer 7.
* Expertise in networking and transport protocols, routing solutions, proxy and reverse proxy servers, NetScaler load balancers
* Building defensive security constructs, including digital signatures, PKI, firewalls
* Solid understanding of current web and web application servers
* An ability to provide solutions to common web application vulnerabilities i.e. SQL injection, cross site scripting, web cookie security, session management, etc.
* Building Authentication and Authorization protocols/frameworks. Specifically, OpenID Connect, OAuth, SAML
* IBM API Connect V10 administration.
* Handling platform related activities like APIM, CMC upgrades and its portal patches.
* Supported production deployments and issues during prod deployments.
* Defining/Build the standalone API’s or defining the API definitions using YAML files.
* Worked on platform and development activities in CITI on APIC V5 upgrades and patches.
* Configuring advance developer portals, Organizations, catalogs, adding the runtime servers in CMC and defining the clusters in API Connect.
* Defining the properties, Configuring security definitions like user registries, TLS profiles.
* Defining the Products, API, content-based routing and implemented the business logic in assembly.
* Validating the API’s, Staging and publishing to custom developer portals.
* Creating and configuring the API’s and defining the parameters, rate limits and the security definitions of an API in APIM.
* Working on Identity and Access Management and/or Role Based Access Control projects

**Client: Blue Cross and Blue Shield of Florida (Florida Blue).**

**Role:** IT Systems Engineer

**Duration**: August 2017 to Dec2021

**Project**

**Title:** IBM DataPower Administration & Development

**Location:** Jacksonville, FL

**Role:** Sr IT Systems Engineer

**Technologies:** IBM DataPower Gateways, XI52, XB62, IDG, IBM API Connect, CA Single Sign-On, LDAP, AD, OpenShift, Docker, Kubernetes, IIS, IBM WebSphere, Apache Tomcat, MQ, DataPower Gateway Script, XSL, XQuery, Java, JavaScript, and JSON, Node.js, JSONiq.

**Responsibilities:**

* Installation and configuration of new DataPower Appliances
* Regular interactions with Functional Team and Business Analysts to discuss design requirements.
* Gathered requirements from product owners and BA and prepared specifications for Multiple Clients and successfully managed to finish the tasks on time for the releases.
* Created API documentations along with working on API Connect upgrades, customize advanced developer portal.
* Participated in design sessions and prepared design documents.
* Performed Secure Backup, Secure Restore, System Backup, Import and Export of Configurations, Firmware Upgrade.
* Worked extensively on API management console, creating REST APIs.
* Configuring WSPs, MPGWs and its policy, MQ Queue Managers, XML Managers, FSHs, etc. in Data power
* Building DataPower policies using Authentication, Authorization and Auditing (AAA) actions, multiple security protocols
* Hands on coding with DataPower Gateway Script, XSL, XQuery, building DataPower deployment policies and other related objects
* Building the multi-protocol gateway to support message types with different protocols and integrations with MQ
* Integrating with WebSphere MQ
* Trouble-shooting DataPower domain application issues and certificate crypto object issues
* Tuning DataPower objects for any performance issues
* Data power device health check configuration, monitoring and reports generation through monitoring tool
* DataPower services transaction monitoring through monitoring tools like Operations Dashboard and Splunk
* Working on middleware architecture and various middleware application servers’ integration.
* Configuring Tomcat or WebSphere application servers
* Solid understanding of data security and network security with a focus on OSI reference model Layer 2- Layer 7.
* Expertise in networking and transport protocols, routing solutions, proxy and reverse proxy servers, NetScaler load balancers
* Building defensive security constructs, including digital signatures, PKI, firewalls
* Solid understanding of current web and web application servers
* An ability to provide solutions to common web application vulnerabilities i.e., SQL injection, cross site scripting, web cookie security, session management, etc.

Education:

Master’s in computer science –Troy University, AL - **2017**

Bachelors in Electronics and Communication Engineering – KLU (Koneru Lakshmaiah University), India**-2015**