**ALI Husnain   
Sr. IAM Engineer**

Email: [husanaina16@gmail.com](mailto:husanaina16@gmail.com) |

LinkedIn: <https://www.linkedin.com/in/ali-husnain-730030235/>

Location: Massachusetts | **Open to Relocate anywhere in USA.**

**PROFESSIONAL SUMMARY:**

As an experienced IAM professional with over 10 years of expertise, I have a comprehensive background in Identity and Access Management (IAM) and Privileged Access Management (PAM), working with technologies such as SailPoint, CyberArk, Okta, ForgeRock, LDAP, Active Directory, SAML, OpenID, and SSO. I have successfully implemented CyberArk Enterprise Password Vault solutions, managed Okta Universal Directory and Org2Org integrations, and worked on cloud environments like AWS and Azure, integrating applications with Radiant Logic. My expertise extends to SCIM 2.0 for identity provisioning, SailPoint IdentityIQ for on-premises identity management, and developing automation tools using Python and Shell scripting. I am highly skilled in ITSM, PAM operational tasks, risk-based access using Zero Trust, and have configured and implemented various IAM solutions such as Okta, SailPoint, Saviynt, and ForgeRock. Additionally, I have extensive experience in SSO, federated SSO using SAML, OAuth 2.0, and OpenID Connect, as well as configuring secure authentication processes across multiple platforms.

**TECHNICAL SKILL:**

**Identity Application**: IAM, CyberArk, Identity Now etc.

**Access Management Platforms:**IAM, CA Single Sign On (Site Minder), CA AUTH minder, CA Risk minder, Ping Identity Ping Federate, CA API Gateway, CA Secure Proxy Server, CyberArk.

**Open Standards:** OAuth2.0, OpenID, Fast Identity Online (FIDO), SAML

**LDAP directories:** Microsoft Active Directory, CA directory, Oracle RDBMS, MySQL, IBM DB2, Sun Java Enterprise System (JES) Directory Server, Oracle Virtual Directory. BOSS 4.1, I Planet, Sun One, Tomcat 6.

**Programming and Markup Languages:** Java, Bean shell, PHP, Perl, Unix Shell (Bourne, Bash, Korn/ksh), HTML/XHTML, XML/XSL, JavaScript, C/C++, SQL, Oracle PL/SQL, Python, Visual Basic.

**Web Technologies:** Apache web server, IBM HIS, ASP.NET, C#, VB.NET, Web Services, JSP, JAVA, HTML / DHTML, XML, SAML, OAUTH WebLogic and WebSphere.

**PROFESSIONAL EXPERIENCE**

**Foundation Healthcare Services, CA                                                        Nov 2021 to Present**

**Sr. IAM Engineer**

**Responsibilities:**

* Involved in the design, migration, and implementation of multiple enterprise-level Identity & Access Management (IAM) solutions.
* Collaborated with Microsoft support teams to resolve escalated issues and provide feedback on API functionality and performance.
* Administration experience of CyberArk vault with Safe creation, integration with LDAP and other authentication methods.
* Implement responsive and intuitive user interfaces for identity and access management applications using React.
* Implemented and configured Oracle Identity Manager (OIM) to streamline user provisioning, reconciliation, and attestation processes.
* Developed and implemented identity and access management solutions tailored to meet the specific needs of B2B clients.
* Hands-on experience in integrating SiteMinder with WebSphere Portal Application Server.
* Develop, configure, and deploy SailPoint IdentityIQ solutions using JSON for data integration and transformation.
* Designed and configured technical access control solutions using Saviynt for managing RBAC and ABAC, ensuring the access policies align with business requirements.
* Responsible to onboard/Integrate new applications to Azure AD and Ping Identity with SAML, OAuth and OpenID Connect standards.
* Deployed and configured BeyondTrust Privileged Remote Access (PRA) and Privileged Password Management (PPM) to secure and manage privileged access across the organization.
* Designed, implemented, and managed the integration of CIEM tools with public cloud environments (e.g., AWS, Azure, Google Cloud) to enhance cloud security and manage entitlements.
* Design, implement, and manage identity and access management solutions using Entra ID.
* Utilized Microsoft Graph API for interactions with Microsoft services such as Office 365 and Azure AD.
* Optimize identity-related data flow and automation using JSON scripts, ensuring accuracy and efficiency in user provisioning and access certification.
* Configured and maintained SSO and federation services to provide a unified login experience across multiple B2C applications.
* Assisted in the design and implementation of Thycotic Secret Server PAM products.
* Implement identity and access management systems to comply with industry standards (SOC 2, SOX, PCI-DSS, HIPAA).
* Deployed SaaS applications using cloud technologies (AWS, Azure, Google Cloud) and managed authentication and authorization of privileged user.
* Experienced in setting up Active Directory, LDAP, Oracle, and Flat Files for application access.
* Designed, implemented, and managed identity and access management solutions within the ServiceNow platform.
* Developed custom integrations and automation scripts using APIs and scripting languages (PowerShell, Python).
* Installed and configured CA SiteMinder, Sun One LDAP Directory, and Sun Identity Manager for multiple projects.
* Identified, analyzed, and resolved system design weaknesses, troubleshooting complex issues related to identities, accounts, authentication, authorization, and entitlements. Prioritized and recommended appropriate resolutions to system defects and access control issues.
* Designed and implemented Identity and Access Management (IAM) solutions using Proofpoint's security technologies.
* Implemented OAuth2.0 and OpenID for mobile and web-based authentication using PingFederate.
* Seamlessly integrated IAM solutions with various B2B applications and services.
* Monitor and respond to identity and access management incidents, ensuring secure authentication flows between Okta and CyberArk.
* Customized OIM workflows and policies to meet organizational security requirements and business needs.
* Worked with audit teams to generate access review reports and automated audit trail capture for compliance frameworks like SOC 2, SOX, and PCI-DSS. Developed and maintained integrations using Microsoft Graph API for custom application development.
* Adept at modern authentication protocols (OIDC, OAuth 2.0) and transitioned organizations to modern authentication.
* Automated compliance control audits, generating evidence for SOC 2, SOX, PCI-DSS, HIPAA, and FedRAMP, improving audit readiness and reducing audit timelines.
* Troubleshot and resolved issues related to SailPoint Identity Now, including connector failures and provisioning errors.
* Developed PowerShell scripts for automating tasks and troubleshooting configuration issues in Office 365.
* Created and managed AMIs using HashiCorp Packer.
* Utilize JSON for creating and managing application integrations, connectors, and APIs.
* Improved IAM tool performance through system tuning and resolved issues related to SCIM 2.0 integration.
* Implemented and managed Radiant Logic's Radiant One Federated Identity and Directory Service.
* Ensured compliance with security standards in SCIM implementation and protected APIs using OAuth2.0 in PingFederate.
* Worked extensively with web servers (IIS, IBM IHS, Apache) and application servers (WebLogic, WebSphere) in IAM environments. Integrated more than 25+ applications with Okta for SSO and MFA, enhancing security and user experience.
* Configured and maintained SCIM 2.0 endpoints for seamless user provisioning and de-provisioning.
* Expert-level skills in Java Multithreading, JSP, PHP, JavaScript, Enterprise JavaBeans, and XML-related technologies.
* Strong involvement in Service Oriented Architecture (SOA) and distributing AMI.
* Hands-on experience in IAM requirement analysis, implementation of Access Gateways, and SAML, OAuth2.0, WSFed, and OpenID-based integrations using PingFederate.
* Enhanced security measures, visibility, and reporting capabilities through automation using CI/CD pipelines, PowerShell scripting, and terraform for infrastructure as code (IaC) deployments.
* Developed and enforced role-based access control (RBAC) models within OIM, defining roles, permissions, and access levels.
* Ensured compliance with security standards and best practices in SCIM implementation to safeguard sensitive identity information.
* Migrated all SSO apps configured in CA SiteMinder to the Okta platform to leverage the combination of SSO and contextual MFA.
* Developed and enforced access control policies using BeyondTrust to ensure secure access to critical systems and data.
* Created AWS AMIs using HashiCorp Packer. Added direct connectors for Active Directory, LDAP, Exchange Online, Box, and UNIX.
* Responsible for improving the overall performance of IAM tools through system tuning.
* Configured and supported SSO (Single Sign-On) solutions leveraging Radiant Logic.
* Troubleshot and resolved issues related to SCIM 2.0 integration, data synchronization, and schema compatibility.
* Developed PowerShell scripts for automating tasks and troubleshooting configuration issues.
* Expert in installing Okta from scratch with directory integration, MFA, and SAML integration.

**Fleet Pride, GA                                                                                                           Sep 2018 – Oct 2021**

**Sr. IAM Engineer**

**Responsibilities:**

* Worked on Provisioning use case development, building to meet compliance and IAM governance.
* Implement and maintain JSON-based configurations for identity data mappings, attribute transformations, and connector settings.
* Implemented RBAC and ABAC for better access control across applications.
* Designed, developed, tested, and implemented enterprise-level IAM systems and solutions for Azure environments, ensuring that all information resources were adequately protected against unauthorized access and security threats.
* Worked closely with cross-functional teams to integrate ForgeRock solutions with existing systems and applications. Experience with supporting IAM (SAILPOINT/ SAVIYNT).
* Hands on experience with IAM products (Oracle IDM, IBM identity manager, ForgeRock and Ping identity.
* Implement and manage CyberArk vault policies, account onboarding, and session management.
* Automated user account provisioning and de-provisioning processes using OIM, ensuring timely and accurate access management.
* Seamlessly integrate BeyondTrust solutions with existing Identity and Access Management (IAM) systems to streamline access management processes.
* Developed provisioning use cases to meet compliance and IAM governance requirements.
* Implemented OAuth 2.0 authorization framework using Okta API to secure APIs and enable secure access to protected resources.
* Develop and enforce IAM policies and standards tailored to B2B interactions.
* Review code contributions from team members to ensure adherence to best practices and security standards in both IAM and React development.
* Automate user provisioning and deprovisioning processes leveraging Entra ID APIs and integration.
* Responsible for mapping requirements to IAM capabilities, SOX controls, and PCI controls.
* Ensure proper identity provisioning and de-provisioning workflows are established and maintained in ServiceNow.
* Automated IAM processes using Microsoft PowerShell scripts and terraform, improving efficiency and reducing manual interventions in user provisioning and access reviews.
* Created Joint Condition from AD and Sun One directory server defined in VDS Radiant Logic for user Search from SiteMinder Policy Server.
* Experience working with Multiple IDP’s available in market and SSO configuration to application.
* Deploy CIEM tools to manage and monitor cloud infrastructure entitlements, ensuring least privilege access across public cloud environments (e.g., AWS, Azure, GCP).
* Built data feeds from various infrastructure applications to ensure seamless identity data integration with Saviynt.
* Designed and developed custom connectors for integrating new applications into the IAM landscape, utilizing REST APIs, SCIM, and JSON to enable data synchronization between systems.
* Integrate infrastructure and application identity data into the organization’s IAM tools using REST APIs and SCIM.
* Gained experience with Oracle Fusion Middleware products (WebLogic Server, SOA Suite, WebCenter Content).
* Designed and implemented OAuth 2.0 authentication and authorization for Graph API resources using Okta API, including Org2Org implementation and management.
* Experience working with Multiple IDP’s available in market and SSO configuration to application.
* Develop and implement scalable IAM solutions tailored for B2C environments, ensuring secure and seamless user experiences.
* Worked on Provisioning/Deprovisioning of SaaS-based applications and ensured the security of identity data via SCIM 2.0.
* Conducted research on emerging technologies, troubleshooting ForgeRock implementations, and collaborated on Okta configurations and policies. Installed and configured CA SiteMinder Web Agent on various web servers and developed custom PowerShell scripts.
* Managed cloud-based services access with Identity.
* Developed and integrated IAM solutions within Azure, focusing on federated identity management using SAML, OAuth, and OpenID Connect to support single sign-on (SSO) and multi-factor authentication (MFA) initiatives.
* Implement and manage role-based access control (RBAC) within Entra ID.
* Collaborated with internal audit teams to ensure continuous compliance with federal and corporate security standards.
* Customized ISIM based IAM solutions, updated on IAM standards (SAML, SOAP, LDAP, OAuth2.0).
* Experienced in SOA, AWS Console and API Integration, and implemented HashiCorp tools (Vagrant, Terraform, Consul, Vault) with Docker container management.
* Managed identity lifecycle processes, including onboarding, role changes, and offboarding, through OIM.
* Implemented ForgeRock Open DJ for LDAP data store and ensured data sync between Active Directory and LDAP.
* Maintained systems built using Java Technologies, experienced in token generation/validation, SAML encryption/decryption.
* Managed RBAC Resource Groups in Active Directory and CyberArk Safe, created PowerShell scripts for identity lifecycle management, and handled identity and access management operations.
* Develop and maintain identity governance and compliance strategies, including role-based access control (RBAC) and privileged identity management (PIM) in Azure.
* Documented SCIM configurations and workflows, worked on various connectors (LDAP, AD, JDBC), and designed and implemented Okta SSO and MDM solutions.
* Worked on SailPoint IIQ IAM solution components, troubleshooting SSO and LDAP issues, and ensured compliance with Microsoft Graph API usage policies.
* Integrate BeyondTrust with various IT systems, including Active Directory, SIEM, and ITSM solutions, to streamline access management and enhance security. Integrate Radiant Logic with enterprise authentication systems including SAML, OAuth, and OpenID Connect.
* Secure APIs used for B2B interactions, ensuring robust authentication and authorization mechanisms are in place.
* Showcased excellent programming skills in Scala, Java, and Python.
* Integrate ServiceNow with various identity stores such as Active Directory, LDAP, and cloud-based directories.
* Optimize IAM systems for performance and scalability to handle large volumes of B2C transactions and user activities.
* Regularly installed and upgraded Okta Agents (Active Directory, Radius, LDAP) to maintain system integrity and security.
* Integrated new applications with SiteMinder and configured them to work under SSO.

**Open Door, TX                                                                                                               Jan 2017 – August 2018**

**Sr. IAM Engineer**

**Responsibilities:**

* Improved Identity and Access Management (IAM) capabilities by controlling access to applications and systems that contain critical and sensitive information.
* Developed custom rules and workflows using Bean Shell and Java.
* Configure and manage Single Sign-On (SSO) solutions for various applications integrated with Azure AD, enhancing user experience and security.
* I am skilled in developing custom rules and workflows utilizing Bean Shell and Java.
* Conducted regular system audits to identify and remediate security vulnerabilities, keeping privileged access environments secure and compliant.
* I specialized in CyberArk for the deployment and engineering of PAM and IAM solutions.
* Integrated OIM with various enterprise applications and systems, such as Active Directory, databases, and cloud services, for seamless identity management.
* Develop and configure ServiceNow modules related to IAM, including user administration, role management, and access control.
* Support and training to end-users and administrators to ensure effective use of BeyondTrust solutions.
* Monitored and maintained IAM systems, resolving incidents, problems, and system changes to ensure continuous availability and reliability.
* Develop custom workflows, rules, and policies using JSON, Java, and XML for provisioning, de-provisioning, and access management processes.
* Implement SSO capabilities for cloud applications using Entra ID, enabling seamless user experiences while maintaining security.
* Developed automated processes to generate compliance audit reports using Saviynt for SOC 2, SOX, PCI-DSS, and HIPAA compliance.
* Developed IdentityIQ Quick links, Forms, Rules, and Custom Objects for workflow design.
* Worked with APIs and SCIM to develop connectors for syncing identity data between applications and IAM tools.
* Automated user provisioning and de-provisioning workflows using SCIM APIs and scripts.
* Resolved Azure AD issues related to Office 365 and Active Directory integrations.
* Implemented and supported SaaS solutions, customizing them for customer requirements.
* Troubleshoot and resolve issues related to identity integrations and data synchronization, leveraging JSON for debugging and analysis.
* Created developer and stakeholder documentation on utilizing Graph API effectively.
* Configured various sources in the Identity Now platform including AD, LDAP, and JDBC.
* Utilized HashiCorp Packer for AMI management and automated AMI creation with Jenkins.
* Integrated PAM MFA and SSO solutions, including configuring MFA policies.
* Configure and manage Azure AD authentication protocols such as SAML, OAuth, and OpenID Connect for secure application integration.
* Worked on the Installation and fine tuning of the SiteMinder web agents for the accomplishment of the business and user requirements. Secured Restful APIs with OAuth2.0 in PingFederate, ensuring access only through Access Tokens.
* Implemented OAuth2.0 for protected API access using various grant types.
* Worked on Automating day-to-day activities using the Rest APIs provided by CA for Federated based SSO Integrations.
* Developed dynamic emails and web pages using JavaScript, HTML/HTML5, and CSS.
* Created RBAC templates for various platforms and assisted with CyberArk integrations.
* Synchronized data between Active Directory and LDAP using ForgeRock OpenIDM.
* Develop and manage identity governance policies, including access reviews, entitlement management.
* Developed Java classes adhering to J2EE design patterns and specifications.
* Conducted POCs to evaluate CA PAM and CA Identity Manager products.
* Audited and assessed SCIM configurations for vulnerabilities and optimization opportunities.
* Demonstrated an excellent understanding of IAM principles.
* Configuring new SAML Federations for external clients, interacting with client to test and support SAML SSO.
* Developed enterprise-level web applications integrated with LDAP and Active Directory.
* Responsible for improving overall performance of IAM tools through system tuning.

**Barclays, AL July 2015 to Dec 2016**

**IAM Engineer**

**Responsibilities: -**

* Ensured that documentation was clear, concise, and easily understandable for both technical and non-technical stakeholders.
* Worked on onboarding connectors like Active Directory, LDAP and other Out of the Box connectors, UNIX and Outlook Office 365.
* Consult and configure access management policies for customer applications using enterprise level identity management tools.
* Troubleshoot and tune Splunk deployment for servers, applications and network devices.
* Developed API-based solutions and integrated applications with RESTful services, allowing seamless interaction between IAM systems and third-party applications.
* Involved in design and implementation of Identity IQ solution, configuring Active Directory, and Shared Folders. Wrote and tested JAVA code for plugins, schedule, transformation, and tasks.
* Design and implement RBAC strategies to enforce the least privilege access principles and manage user roles effectively within Azure AD.
* Managing identity data, leveraging HTML5, JavaScript, React.js, and Node.js to create intuitive and efficient management portals.
* Actively engaged in the development of Identity Management (IDM) applications using SailPoint and Java, including participation in requirement analysis, design, unit testing, and providing 3rd Level Support.
* Installing and configuring SiteMinder Policy Servers to authenticate and authorize access to Enterprise resources.
* Extensively worked on Identity Governance including User Provisioning, Access Certifications, Access request, Workflow, Delegated Administration and Password Self-Service.
* Integrate multi-factor authentication (MFA) and data encryption to enhance security controls as required by standards like PCI-DSS and HIPAA.
* Worked on developing user provisioning and deprovisioning workflows, aggregation, tasks, rules.
* Actively involved in the development of Identity and Access Management (IAM) applications using SailPoint and Java technologies. Managed sessions in Privileged session management (PSM).
* Participated in the enhancement and customization of SailPoint applications to meet evolving security and compliance requirements.
* Implemented solutions to automate routine audit tasks, allowing for more focused attention on critical compliance activities.
* I specialize in designing and implementing audit reports to ensure adherence to regulatory frameworks such as SOX, PCI, and CPNI.

**VP Mart, Pakistan Jun 2014 to April 2015**

**IAM Engineer**

**Responsibilities: -**

* Configured Affiliate agents, RADIUS agents to provide federation of web services in the SSO environment providing authentication & authorization to IDM. Microsoft FIM, SailPoint IIQ, Oracle IM, SAP IDM, NetIQ IDM ForgeRock OpenIDM and CA Identity Manager.
* Provide SailPoint application consulting and development support to consumer applications as required.
* Implemented SailPoint PAM module to connect CyberArk.
* Integrated applications to enable Single Sign-On (SSO) by coordinating with application development and business team.
* Providing support to networks containing more than 2000 Cisco devices.
* Carrying out documentation for tracking network issue symptoms and large-scale technical escalations ProxySG
* Integrated web service-based applications to authenticate and authorize users based on their access and data in SailPoint IIQ.
* Implemented and Customized Manage Access and Manage Identity modules as per customer requirements in SailPoint IIQ.

**Education:** Bachelor’s From Punjab University in 2014