Abhilash Lingala

abhilash.93821@gmail.com| 3019662718

SailPoint Identity Engineer

Professional Summary:

* IT professionals with 10 years of expertise in designing and implementing Identity and Access Management (IAM) solutions. Experienced SailPoint Engineer specializing in Identity and Access Management (IAM), with extensive expertise in designing, implementing, and enhancing SailPoint IdentityIQ (IIQ) solutions.
* Proven track record of collaborating with leading partners such as Column Technologies, Optiv Inc., and TEKsystems, delivering robust IAM solutions tailored for Fortune 500 companies and deploying 50+ applications and 100,000+ identities.
* Expertise in developing lifecycle events, such as joiner, manager, and leaver, customizing LCM workflows, Quicklink forms, and approval modifications, and optimizing workflows and applications with beanshell Rules and scripts.
* Proficient in integrating diverse applications using out-of-the-box and advanced solutions like REST Web Services connectors, ensuring seamless connectivity and governance. Experienced in IdentityIQ version upgrades (7.x, 8.x), including patch updates and continuous process improvements.
* Demonstrated expertise in OKTA and Sailpoint, directory systems (AD/LDAP), and related technologies, including SAML 2.0, Frame, Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), Single Sign-On (SSO) Hands-on experience with OKTA SSO.
* Integrated SailPoint with a variety of connectors, including Active Directory, LDAP, Delimited applications PeopleSoft, JDBC, Workday, DocuSign, Salesforce, delimited files, ServiceNow, AWS, and Okta, facilitating comprehensive identity management.
* Configured Webservice and SCIM connectors with before/after rules customizing request and response for REST API integration, Creating custom Rest API endpoints for sailpoint custom Objects.
* Implemented various access certifications, including Manager, Application Owner, Role-based, and Targeted certifications. Customized and activated certification using beanshell rules in SailPoint IdentityIQ to automate provisioning and governance processes.
* Developed workflows in SailPoint IdentityIQ to automate business processes, including dynamic role assignments and multi-level approvals. Utilized rules and integrated with Active Directory, Workday, and ServiceNow, ensuring policy compliance, audit logging, and exception handling.
* Proficient in writing complex SQL queries to analyze and troubleshoot data issues in SailPoint IdentityIQ, including identity, entitlement, and provisioning data.
* Recognized for technical problem-solving, innovative solutions, and a commitment to delivering high-quality IAM outcomes for complex environments.
* Authored comprehensive Standard Operating Procedures (SOPs) and detailed design documents in collaboration with business analysts, ensuring seamless alignment between technical deliverables and business requirements.
* Ability to support internal and external audits by providing necessary reports for regulatory affairs and documentation from SailPoint IdentityIQ
* Created Knowledge Information Documents (KIDs) specifically designed for client managers, providing step-by-step guidance to streamline the completion of access certifications and SailPoint approval workflows, improving operational clarity and efficiency.

Education: Master’s in computers and information sciences, SAU, Arkansas

Certification: [**SailPoint Identity Security Leader**](https://badgr.com/public/assertions/Tm1YajukShqoSSxaUpN7ow?identity__email=abhilashl351@gmail.com)

Industry Training: SailPoint Fundamentals of Identity IQ Implementation, SailPoint Provisioning with Identity IQ**.**

PROFESSIONAL EXPERIENCE:

SailPoint IdentityIQ Engineer June 2020 to Present

State Farm, Bloomington, IL.

Project: Implemented SailPoint IdentityIQ for State Farm, streamlining access management across systems, automating user provisioning/de-provisioning, access management, and certifications, and enhancing security through role-based access control.

Responsibilities:

* Implemented SailPoint IdentityIQ (IIQ) for state farm, including comprehensive configuration and customization. Deployed and configured SailPoint IdentityIQ across multiple environments (Dev, Test, Staging, prod), overseeing JBoss and Java installations, server setup, SSL certificate management for secure communication, and establishing IdentityNow across multiple tenants.
* Integrated OKTA with SailPoint IdentityIQ, enhancing secure access management for over 900,000 identities and ensuring compliance with enterprise security policies.
* Integrated SailPoint IIQ with a variety of connectors such as Active Directory, M365, PeopleSoft, JDBC, Workday, DocuSign, Salesforce, delimited files, ServiceNow, SAP S/4HANA, GRC, AWS, Webservice, SCIM etc.. facilitating comprehensive identity management.
* Implemented advanced LCM workflow enhancements, including handling scenarios like confidential hires and examiner hires, by designing and deploying custom joiner, mover, and leaver BeanShell scripts. Developed robust provisioning logic and integrated with ServiceNow APIs to automate email notifications and streamline business processes.
* Implemented various SailPoint IdentityIQ rules, including Aggregation, Correlation, Manager Correlation, Creation, and Customization Rules. Proficient in customizing Managed Entitlement, Provisioning (Before and After), and Schema (account/group) Rules to optimize identity lifecycle management, account provisioning, and entitlement processes.
* Experience configuring JDBC connectors and customizing SQL statements for account aggregation and provisioning.
* Developed and optimized PowerShell scripts to automate and streamline AD processes, including workflow management, enhancing overall system efficiency and accuracy in identity governance.
* Customized SailPoint IdentityIQ QuickLinks, forms, and workflows; implemented dynamic multi-level approval processes using advanced workflow attributes (postBack, dynamic, validation Scripts); integrated business logic and policy enforcement to ensure SOD compliance with internal controls and industry regulations.
* Implemented SailPoint IAM Access Certifications, managing the configuration and customization of certification campaigns. Executed multiple certifications, including Manager Certification, Application and Entitlement Owner Certification, Advanced Certification, and Targeted Certification.
* Developed and managed Certification Rules in SailPoint IdentityIQ, including End Period Enter Rules, Exclusion Rules, Pre-delegation Rules, and Sign Off Approver Rules to enhance access review processes, ensure accurate entitlement management, and streamline certification workflows.
* Customized email templates in IdentityIQ using velocity script, XML, and dynamic variables, improving communication for access certifications and reducing manual notification efforts
* Developed and enforced IAM Segregation of Duties (SOD) policies, reducing policy violations and creating customized quick links and workflows tailored to client requirements.
* Developed and customized reports in SailPoint IdentityIQ using XML specifications, Form customizations, and core Java, SQL, spring, J2EE, Apache Tomcat, HTTP, AJAX, REST, SOAP, and Beanshell. Experience in UI test automation using frameworks like Selenium and Mocha.
* Created standard and complex custom reports to meet specific business needs for compliance monitoring, using Splunk and managing CI/CD pipelines using Jenkins and GitLab, with strong proficiency in Git for version control, cloud deployments on AWS, Azure, and GCP, and incident management using Jira and ServiceNow.
* Demonstrated a strong commitment to enhancing organizational security and operational efficiency through the strategic implementation of identity and access management solutions, resulting in improved compliance, reduced risk, and streamlined processes across the enterprise.

SailPoint Engineer AUG 2019 to May 2020  
Caterpillar, Peoria, IL

Project: Implemented SailPoint to manage access requests and certify employees regularly, focusing on rapidly onboarding 4,000 applications and developing various certification processes.

Responsibilities:

* Onboarded 4,000 applications, developing and modifying IAM SailPoint certifications to meet client-specific requirements.
* Configured and implemented SailPoint IdentityIQ (IIQ), including coordination with vendor leadership, technical services teams, and end-user customers to ensure smooth integration.
* Developed IAM Lifecycle Manager workflows and lifecycle events, including work on Joiner, Mover, and Leaver processes, SailPoint certifications, custom email templates, and task definitions.
* Maintained databases with a strong understanding of the IdentityIQ database structure and design for optimal performance.
* Designed and managed quick links and custom reports, troubleshooting web services by analyzing logs and resolving identified issues effectively.
* Implemented Beanshell-based rules for Manager Correlation, Build-map, pre-iteration, customization, provisioning, and connector rules, ensuring precise control over IAM processes.
* Executed various certifications, including Entitlement Owner, Manager, and Application Owner Certifications, for all identified applications and roles.
* Familiarity with configuring and troubleshooting database connections for IdentityIQ, including Microsoft SQL Server and MySQL
* Configured certifications based on client requirements, developed Beanshell exclusion rules, and created advanced certification processes to meet complex needs.

IAM Engineer. Nov 2017 to Aug 2019

Optiv Security Inc. Client: Department of Labor, DC

Project: CDM Homeland Security Presidential Directive (HSPD – 12) – “Policy for a Common Identification Standard for Federal Employees and Contractors” was issued to create a standard for secure and reliable forms of identification. Department of Labor (“DOL”) engaged Optiv Security, Inc. (“Optiv”) to configure SailPoint IdentityIQ in support of its Identity and Access Management (IAM) program.

Responsibilities:

* Led Installation and configuration of IAM SailPoint IIQ, Radiant Logic, and PingFederate on Dev, Test, Stage, and Production in Linux Environments.
* CDM Dashboard: Worked on the CDM Initiative with CGI to develop a consolidated DHS dashboard.
* Knowledge of monitoring and managing security tools like Sailpoint Identity IQ, Cyber-Ark PAM modules, Radiant Logic, and Ping federate solutions.
* Experience in Identity Access Management IAM modules and Implemented Lifecycle and certifications for the Department of Labor.
* Managed the administration functionality of SailPoint IAM, such as loading data, creating roles, creating policies, scheduling tasks and certifications, and reports.
* Configuration and development of SailPoint IAM Life Cycle Events (LCM)such as Joiner mover and Leaver. Developed custom rules and workflows using Bean Shell
* Developed IAM modules such as Joner, Mover, and Leaver workflows to Create, Update, and Delete user accounts on the target application.
* Implemented Beanshell-based Manager Correlation, Build-map, pre-iterate, Customization before provisioning and after provisioning, and Escalation rules.
* Generated & released access certification reports to managers or entitlement owners.
* Build and Configure SailPoint in-built tasks like aggregation, ID refresh, schedule tasks, correlation, etc.
* Involved in gathering the stakeholders' requirements and translating business processes into functional specifications such as Connectors type, Schema, Entitlements, Roles, and Policies of the applications.
* Implementation of self-service features, password features (PTA, Forgot Password, Change Password), provisioning features, and configuration of various roles and policies in SailPoint.
* Implementation and testing for enterprise request-approval process, set up Sandbox, development environment, implemented global user provisioning, service account provisioning, and re-certification workflows, including Active Directory with Muti-Forest Environment, SQL JDBC, etc.
* Experience with database maintenance and performance tuning for IdentityIQ implementations, including index optimization
* Provided knowledge transfer and post-production support activities, as necessary.

IAM Analyst June 2017 to Oct 2017

First Republic Bank, SFO CA

Project: Implementation of enterprise-wide Identity and Access Management (IAM) platform to streamline secure access management processes and meet compliance requirements at First Republic Bank

Responsibilities:

* Responsible for design implementation and Testing of IAM designs and Involved in all phases of the project, from the analysis and requirement phase to delivering the project. Worked in Agile/Scrum Methodology.
* Designed, implemented, and tested IAM solutions across all project phases, following Agile/Scrum methodologies.
* Configured and deployed out-of-the-box (OOTB) connectors to integrate IAM platforms with in-scope applications, ensuring seamless access management.
* Defined and implemented certification workflows to enhance access reviews, achieving compliance with Regulatory Affairs SOX, PCI-DSS, and internal governance standards.
* Developed secure access management solutions incorporating RBAC and ABAC models, enabling scalable and policy-driven authorization mechanisms.
* Conducted gap analyses to identify deficiencies in existing IAM tools and processes, proposing improvements to enhance identity lifecycle management and governance.
* Collaborated with SMEs and stakeholders to map business requirements to IAM capabilities, compliance controls, and governance frameworks.
* Established an IAM Maturity Model, enabling the organization to assess and advance IAM capabilities incrementally, focusing on certifications and secure access mechanisms.
* Provided end-user training and walkthroughs to business stakeholders, ensuring smooth adoption of IAM functionalities and defining UAT test cases.
* Conducted thorough testing and validation of IAM configurations, ensuring fixes and enhancements were aligned with production requirements.

**Crown Technologies April 2015 to May 2017**

**IAM Administrator, Dayton, OH**

**Responsibilities:**

* Implemented and maintained IAM platforms, enabling seamless integration with applications and directories, ensuring system security and compliance.
* Managed user lifecycle processes by integrating IAM systems with HR databases, automating provisioning, and de-provisioning of accounts across applications using custom scripts.
* Designed and enforced role-based access control (RBAC) models by analyzing business requirements and mapping roles to appropriate entitlements within enterprise systems.
* Conducted access reviews by generating reports from directory services and applications, ensuring adherence to compliance frameworks like SOX and GDPR.
* Configured directory services such as Active Directory and LDAP, implementing organizational units (OUs) and group policies for efficient access control management.
* Reviewed and updated IAM policies, procedures, and documentation to align with evolving organizational requirements and industry best practices.
* Ensured compliance with password policies, account expiration settings, and lockout thresholds to maintain a secure access environment.
* Facilitated identity access reviews by generating and analyzing reports to support audits and ensure minimal access risks.
* Provided training and support to end-users and teams on access management policies and tools, promoting security awareness across the organization.