RAVI
IAM DEVELOPER
Phone: +1732-783-4227
Email: ravivadla1995@gmail.com
Linkedin:www.linkedin.com/in/raviteja-v-b5587835b

PROFESSIONAL SUMMARY:

- **10+ years of experience** in design, architecture, technical development, integration, and deployment of **Identity & Access Management (IAM)** solutions and products, specializing in **SailPoint IdentityIQ (IIQ), SailPoint Identity Security Cloud (IdentityNow)**, and **Okta**, with strong expertise in **identity architecture, implementation, and production support**.
- Responsible for designing and configuring **Certification and Lifecycle Management** processes and implementing solutions using the **Provisioning Engine** in SailPoint IIQ.
- Proven experience in the **design and development of Identity and Access Management (IAM)** across **SailPoint IdentityIQ, Identity Security Cloud**, and **cloud environments including SailPoint IdentityNow**.
- Hands-on in **enterprise-level IAM setups** for **Role Mining, Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), Single Sign-On (SSO), SAML, Segregation of Duties (SoD)**, and **Identity Management (IDM)** using cybersecurity tools.
- Strong understanding of **SailPoint/IAM core concepts** — identities, account aggregation, identity refresh, correlation, multiplexing, escalation, revocation, certifications, SoD, integration configuration, and **CyberArk** integration.
- Experienced in developing **custom SailPoint IIQ and IdentityNow workflow solutions** and automation for access provisioning and governance.
- Deep integration experience connecting SailPoint with **Azure AD, Active Directory, ServiceNow, SAP, CyberArk, Ping Identity, ForgeRock**, and **cloud systems** via **OpenID Connect, OAuth, and SAML** protocols.
- Designed and implemented **Lifecycle Events (Joiner, Mover, Leaver, Rehire)** in SailPoint IIQ and Identity Security Cloud with **workflows, access reviews, cloud rules, form customizations, and bulk operations**.
- Lead the design, implementation, and enhancement of enterprise Active Directory, Azure AD, and hybrid identity solutions. And Managed enterprise PKI, certificate services, and secure LDAP.
- Develop and maintain AD Group Policies, OU structure, replication, and DNS/DHCP integration.
- **Knowledge on Group Policy Management, Kerberos, LDAP, NTLM, and authentication protocols.**
- **Familiarity with identity security frameworks (Zero Trust, PAM, MFA).**
- Experience with cloud integrations **(Microsoft 365, SaaS apps, SAML, OAuth, SCIM) and AD Group Policies, OU structure, replication, and DNS/DHCP integration.**
- Developed and customized **SailPoint IdentityIQ workflows, rules, and configurations** for provisioning, de- provisioning, and certification campaigns.
- Deployed and maintained **SailPoint IIQ and IdentityNow implementations** on **AWS and Azure**, integrating **YubiKey, PingFederate, Ping Identity**, and **Zero Trust** security models.
- Configured workflows for **automated provisioning/de-provisioning** of accounts across internal and external systems using **SailPoint IIQ, Active Directory**, and **ForgeRock**.
- Experienced in SailPoint IIQ connectors such as **Delimited File, JDBC, LDAP, AD, SAP, SCIM, REST API**, and Oracle Application Direct.
- Strong experience handling web and application servers like **Apache Tomcat, IBM WebSphere, BEA WebLogic**, and **JBoss**.
- Implemented **identity governance solutions** for **AWS Cloud Infrastructure**, ensuring compliance with **Zero Trust, SOC2, NIST, and ISO 27001** security standards using tools like **SiteMinder, CyberVault, and CyberSense**.
- Solid foundation in **Core Java and J2EE technologies** such as **Servlets, Struts, JSP, JSF, Spring Core, Spring AOP, Spring Security, Spring MVC, Hibernate, PowerApps**, and **SharePoint**.

- Expertise in **J2EE, JSF, Spring, JSON, REST APIs, SCIM,** and **SOAP-based web service integrations** to extend IAM functionalities.
- Proficient in configuring and maintaining **SailPoint environments (DEV, QA, PROD, and DR)** for scalable identity management.
- Experienced in **managing, monitoring, and troubleshooting** IAM systems, handling **production issues, IQService configurations**, and **critical incident resolutions**.
- Hands-on experience developing **aggregation tasks, workflows, rules, roles, and Quick Links** in SailPoint IIQ for end-to-end automation.
- Designed and implemented custom **SailPoint rules** such as Build Map, Pre-Iterate, Post-Iterate, Correlation, Multiplexer, Identity Creation, Policy Violation, Escalation, and Customization Rules.
- Proficient in **connecting and deploying SailPoint IIQ connectors** for multiple authoritative and target systems.
- Experience working under **Agile methodology**, leveraging **AWS tools, Jenkins, CI/CD pipelines**, and **DevOps best practices** for continuous integration and automated deployments.
- Configured workflows integrating **SAML, OAuth, OpenID Connect**, and **Entra ID** for modern cloud identity federation and access management.
- Created and managed **multiple Identity Profiles** for onboarding authoritative sources in IdentityNow and integrating with **Excel, CMDB, IT Risk, IT Control, and IT Audit systems** using **Power Query, XLOOKUP, and VLOOKUP**.
- Built and configured **SailPoint IIQ in-built tasks** such as Account Aggregation, Account Group Aggregation, Identity Refresh, System Maintenance, Check Active Policies, and Certification Refresh for automation and governance.
- Deployed and configured **IQService servers** for provisioning and de-provisioning using **Secure LDAP (636)** and **LDAP (389)** protocols.
- Experienced in **customer interaction, leadership, stakeholder collaboration, product management**, and **mentoring** for cross-functional IAM projects.
- Skilled in **critical incident management, troubleshooting, and continuous improvement** of identity governance solutions.
- Strong knowledge of **Zero Trust architecture, CyberArk PAM, and Cloud Security integration** across AWS and Azure ecosystems.
- Proven ability to **lead IAM modernization programs**, automating lifecycle management and ensuring compliance with industry standards.
- Deep expertise in **cloud-native IAM**, integrating SailPoint with **cloud directories and SaaS applications** using SCIM and REST APIs.
- Adept at **IAM data governance, analytics, and reporting**, with experience in **Power BI, Excel dashboards, and audit support**.
- Recognized for **building scalable, secure, and compliant IAM frameworks** driving digital transformation and regulatory adherence across enterprise environments.

TECHNICAL SKILLS:

Operating Systems	**Windows, Linux (RHEL, Ubuntu), Sun Solaris, UNIX, Novell NetWare**
Languages	SQL, PL/SQL, Java, JavaScript, J2EE, HTML, XML, JSON, PowerShell, Shell Scripting, Beanshell, Eclipse IDE
Databases	Oracle 8i/9i, MySQL, MS SQL Server, MS Access
Directory Services (LDAP)	Novell eDirectory, Microsoft Active Directory
SSO and Identity	Novell Identity Manager (2.x, 3.x, 4.x), PingFederate, PingAccess, CyberArk, Novell eDirectory (8.7.x – 9.2.x), Access Manager (4.x), iManager (2.6.x – 3.2.x), Designer (2.6 – 4.7)
Cloud Platforms	**AWS, Azure**
Tools & Frameworks	Novell Identity Manager Designer, Access Manager Console, PingFederate Admin Console, CyberArk PAS, Eclipse, Visual Studio Code

PROFESSIONAL EXPERIENCE

PWC **Dec 2025- Present**

SAILPOINT DEVELOPER

Responsibilities:

- Support the implementation of access certification processes within the **IGA platform** (e.g., SailPoint, Saviynt) to ensure periodic entitlement reviews align with least-privilege principles and compliance requirements.

Contribute to the integration of applications with Single Sign-On (SSO) using identity federation protocols such as **SAML, OIDC, and OAuth2,** collaborating with application teams and security architects.

- Work closely with IAM architects and application teams to onboard applications into the IGA platform, ensuring entitlement data, user attributes, and provisioning rules are accurately mapped and configured.
- Analyze access patterns and application entitlements to assist in role mining, entitlement rationalization, and the development of scalable, governance-aligned role models.
- Document technical specifications, data mappings, and integration workflows for **SSO and IGA** implementations, supporting both technical teams and audit requirements.
- Configure and maintain integrations between target systems and the IGA platform, ensuring proper lifecycle management of users and entitlements.
- Assist in the creation of access policies and role definitions, aligning with business and compliance requirements.
- Generate reports and provide evidence for audit activities, including **entitlement reviews, access request histories**, and policy enforcement logs.
- Identify technical gaps or inconsistencies in access controls, provisioning workflows, or entitlement structures and propose engineering solutions to address them.
- Participate in testing, validation, and deployment of IAM-related changes, ensuring proper functionality across SSO and IGA components.
- Provide technical support and knowledge sharing to application teams and business stakeholders around IAM integration processes and access governance best practices.

CHARLES SCHWAB **OCT 2024 – NOV 2025**

SAILPOINT CONSULTANT

Responsibilities:

- Worked on enhancing and optimizing **custom workflows, rules, and reports** in SailPoint to improve performance, maintainability, and compliance visibility.
- Managed, maintained, and developed the **IAM infrastructure** leveraging **SailPoint IdentityIQ, IdentityNow**, and **Okta** tools for user lifecycle and access governance.
- Designed and developed **Joiner, Mover, and Leaver workflows** and automated **onboarding processes** for critical enterprise applications.
- Led the **integration of new applications** into SailPoint, Okta, and **Identity Security Cloud (ISC)**, ensuring seamless synchronization and policy alignment.
- Strengthened **cloud platform security (AWS)** by implementing IAM governance, automation, and integrating with **CI/CD pipelines** using DevOps best practices.
- Delivered customized **Okta identity and access solutions** supporting **NCID security** and **Apple Management Console** integration.
- Developed **PowerShell scripts and rules** for **Exchange and O365 provisioning**, integrating them with Joiner workflows and **Oracle EBS**, **GCP platforms**, **PowerApps**, and **SharePoint**.
- Designed **custom rules for aggregation and provisioning** in **SuccessFactors**, ensuring accurate user data synchronization.
- Configured and developed **web service connectors** with custom rules to manage **Create, Update, and Delete operations** efficiently.
- Onboarded **Delimited File, JDBC, and Active Directory applications** in SailPoint for **Access**

Reviews and Certifications.

- Developed and implemented **provisioning policies** for multiple systems including **AD, JDBC, web service connectors, IdentityNow, and ISC**, integrating **Okta and CyberArk** for secure access management.
- Created **custom forms and workflows** to manage non-connected applications within **SailPoint IdentityIQ**, improving administrative control.
- Developed and deployed **custom connectors and rules** to extend SailPoint capabilities for enterprise integrations.
- Reviewed **test plans and QA documentation**, providing insights to enhance testing efficiency and ensure compliance with **SOC, SOX, HIPAA, and GDPR** audit requirements.
- Partnered with the **Security and Compliance teams** to execute **Identity Governance audits**, perform **role mining**, and enforce access policies.
- Guided **Application Owners and System Administrators** on **IAM best practices** for integrating and standardizing connector bundles within the identity ecosystem.
- Automated **CI/CD pipelines using DevOps** to streamline SailPoint deployments and support **IdentityNow architecture** with bulk operations, cloud rules, certification reviews, and integrations.
- Supported multiple **IAM and security projects** including **Lifecycle Management, Directory Services**, and cross- platform integrations.
- Created **Exclusion Rules and Pre-Delegation Rules** for **Certifications, SOD modules**, and **IdentityNow policies** to enforce compliance and reduce false positives.
- Customized **email templates and notifications** in SailPoint to align with client branding, ensuring consistency in communication across certification and provisioning workflows.

Environment: SailPoint IdentityIQ, SailPoint IdentityNow, Identity Security Cloud (ISC), Okta, CyberArk, AWS, Azure AD, PowerShell, Exchange, O365, Oracle EBS, SuccessFactors, GCP, PowerApps, SharePoint, JDBC, Active Directory, REST API, DevOps (Jenkins, Git), CI/CD Pipelines, SOC/SOX/HIPAA/GDPR Compliance, Role Mining, SOD, Certification Campaigns, Workflow Automation.

PRINCIPAL GROUP SERVICES **AUG 2021 TO JULY 2024**
SAILPOINT CONSULTANT
Responsibilities:

- Configured **Organizational, Business, and IT roles** for various application entitlements to establish structured role-based access governance across enterprise systems.
- Enforced **least privilege principles** within the **RBAC model**, designing and developing the **Role-Based Access Control framework from scratch**, with hands-on experience in **CyberArk** for privileged account governance.
- Integrated **SailPoint IdentityIQ** technologies with **in-house and third-party applications** to enable **birthright provisioning, access request fulfillment**, and **custom workflows**, using **DevOps tools** such as GitHub and Jenkins.
- Ensured compliance with **SOX, SOD, and InfoSec controls**, collaborating with internal audit and risk teams to maintain strong governance alignment.
- Designed and implemented **Active Directory connectivity** for automated user data aggregation, reconciliation, and access provisioning.
- Created **Business and IT roles** aligned with **InfoSec, HR, and compliance requirements**, ensuring accurate role hierarchy and data ownership.
- Provisioned and managed user access using **Lifecycle Manager (LCM)** and **Identity Security Cloud**, streamlining access onboarding and termination workflows.
- Acted as **Subject Matter Expert (SME)** for **business-critical tasks**, including data migration, testing, and post- implementation validation during IAM transformation programs.
- Participated in the **Service Standard Build (SSB)** process for custom SailPoint enhancements during the implementation phase, leveraging **IdentityNow architecture** and **Identity Security Cloud (ISC)** components.

- Developed **Lifecycle Manager workflows, lifecycle events, certification events**, and **custom email templates**, along with **task definitions, certification management**, **log analysis**, and **custom web agents**.
- Gained hands-on experience in **CyberArk integrations** and **product management**, contributing to secure privileged access and credential vaulting strategies.
- Built frameworks for **Role Mining, Role-Based Access Control (RBAC), Entitlement Management**, and **Identity UI Customization**, leveraging **AWS tools like Bitbucket** for version control and automation.
- Designed and deployed **custom forms** in the **SailPoint UI**, enabling administrators to manually provision users and manage **L3 support tickets** efficiently.
- Defined and documented **use cases and business processes** for support groups on **role, entitlement, provisioning, and de-provisioning**, across **IdentityNow** and **Identity Security Cloud environments**.
- Managed **administrative functions** within SailPoint, including **data loading, role creation, policy management, task scheduling, certification campaigns**, and **report generation**.
- Worked with various **connectors** such as **Active Directory, PeopleSoft, JDBC, Mainframe ACF2, Workday, Salesforce, MySQL, Delimited File, RSA**, and web/app servers like **Tomcat and WebLogic**.
- Served as a **SailPoint Consultant**, providing **best practice recommendations**, conducting **health checks**, and contributing to **design documents** for improved SailPoint performance and stability.
- Performed **data analytics and validation** to ensure data accuracy prior to staging and activating **certifications and role campaigns**.
- Configured and customized **SOD policies** and **policy violation workflows** to align with business and audit requirements.
- Worked extensively with **Power Query, CMDB, IT Risk, IT Control, and Audit modules**, ensuring audit readiness and process transparency.
- Demonstrated strong **communication, leadership, and mentoring skills**, collaborating with stakeholders, customers, and technical teams to troubleshoot production issues and resolve critical incidents.
- Provided **on-call support** for high-priority IAM incidents, ensuring minimal business disruption and maintaining compliance with security SLAs.

Environment: SailPoint IdentityIQ, IdentityNow, Identity Security Cloud (ISC), CyberArk, Active Directory, PeopleSoft, Workday, Salesforce, JDBC, MySQL, Mainframe ACF2, RSA, Tomcat, WebLogic, AWS, Bitbucket, GitHub, Jenkins, Power Query, CMDB, IT Risk/Control/Audit, SOX, SOD, InfoSec Controls, LCM, Certification Campaigns, Role Mining, Policy Violation Workflows, Lifecycle Events, DevOps, Data Analytics, Log Analysis.

ADNIC **JAN 2017 – JULY 2021**

IAM DEVELOPER

Responsibilities:

- Demonstrated **expertise in the design and development of multi-tiered web-based enterprise applications** using **J2EE technologies** such as JSP, Servlets, JDBC, and Web Services.
- Utilized **PowerShell scripting, Shell scripting, VS Code, Bitbucket, and Jira (SSD)** to automate tasks, enhance integration, and maintain code repositories for IAM and related backend services.
- Gained strong experience in **Swing, Struts, Spring (Core, MVC, JDBC), and Hibernate Frameworks** for building scalable and secure enterprise-grade applications integrated with IAM systems.
- Proficient in **Eclipse** and **Rational Application Developer (RAD)** IDE tools for code development, debugging, and deployment processes.
- Deployed existing code, configuration files, and connectors on **Apache Tomcat servers** across **Dev, Test, and Production** environments, ensuring smooth build migrations and version control.
- Ensured seamless **communication between endpoint systems and SailPoint IIQ** by configuring connectors, performing attribute mappings, and testing provisioning flows.
- Resolved issues and bugs arising during **SailPoint upgrade testing** and post-implementation analysis, improving system stability and reducing identity provisioning delays.
- Scheduled and implemented various **User Entitlement Reviews** for applications, databases, and

directory services to meet compliance with **SOX, HIPAA, and GDPR**, with integration to **CyberArk** for privileged access management.

- Performed **attribute mapping and troubleshooting in Okta**, supporting Okta service/help desk queues, identifying root causes for provisioning failures, and validating integration with **CyberVault, Cyber Sense**, and other cybersecurity tools.
- Gained experience in **CyberArk, SCIM, OAuth, REST API, and SAML** protocols for secure application onboarding, identity federation, and single sign-on (SSO) implementation.
- Installed and configured **Okta Lightweight Agents** for directory synchronization and integrated with **Active Directory and Entra ID (Azure AD)** for automated identity lifecycle management ,Access Request Tool Suite (ARTS) and Automated Security Access Removal (ASAR).
- Designed and implemented **IAM build processes, code migration pipelines, and source control strategies**, ensuring alignment with CI/CD practices.
- Extensively utilized **SailPoint IIQ APIs** to develop **custom functionalities**, supporting advanced identity correlation, account aggregation, and provisioning workflows integrated with **Azure, AWS, Ping Identity, Ping Federation, and YubiKey**.
- Worked on **out-of-the-box connectors and web service integrations** provided by **SailPoint IIQ** and configured integrations with **IdentityNow, Identity Security Cloud (ISC)**, and **IDM** systems for unified identity management.
- Collaborated with business stakeholders to **gather requirements, define roles, and implement access control models** within SailPoint, ensuring compliance with InfoSec standards.
- Supported clients in **post-implementation testing, user acceptance (UAT), debugging, and production maintenance**, improving operational efficiency and minimizing onboarding delays.
- Provided **knowledge transfer (KT) and post-production support**, focusing on SSO, federation (SAML), and integration with **ForgeRock**, maintaining IAM platform reliability.
- Developed **custom rules for Lifecycle Events**, and configured **Lifecycle Manager, Compliance Manager, and Password Manager Services** for automated provisioning, de-provisioning, and compliance certifications.
- Automated CI/CD pipelines for identity management components using **DevOps tools**,JavaScript, Scala, **Terraform, Git, CI/CD pipelines, AWS OpenSearch, Lambdas,**

  integrating with **AWS, OpenID Connect, OAuth, Kerberos, and IDAM** protocols.
- Customized and enhanced **desktop password reset functionalities** within complex **Active Directory environments**, ensuring secure authentication across distributed enterprise systems.
- Contributed to **cybersecurity awareness and incident response initiatives**, performing testing on **cyber resilience, data restore, and identity backup** to mitigate risks from potential cyberattacks.

Environment:SailPoint IdentityIQ, Okta, CyberArk, ForgeRock, AWS, Azure, Ping Identity, Ping Federation, YubiKey, Entra ID (Azure AD), Active Directory, PowerShell, Shell Scripting, Java/J2EE, Spring, Hibernate, Eclipse, RAD, Tomcat, Bitbucket, Jira, DevOps, Jenkins, REST API, OAuth, SCIM, SAML, Kerberos, OpenID Connect, IdentityNow, ISC, IDM

SINGAPORE BANK, OFFSHORE INDIA **JAN 2015 TO DEC 2016**

IAM JAVA ENGINEER

Responsibilities:

- Installation, configuration, and administration of **eDirectory/IDM** on **RHEL (Red Hat Enterprise Linux)** environments.
- Responsible for administering one of the **largest Novell/NetIQ Identity Manager environments** with **62,000+ users**, **30 drivers**, **4 Identity Vaults**, and **180 servers**, ensuring high availability and scalability.
- Performed **eDirectory/IDM administrative tasks** including schema extensions, partition and replica management, driver configuration, backups, health checks, and system patching.
- Upgraded **eDirectory/IDM** to the latest **service packs and patches** to maintain stability, compliance, and performance.
- Designed and enhanced existing **IDM drivers** and developed new ones based on evolving business requirements.
- Worked extensively with **edir-edir, Cayosoft, Active Directory, and BeyondTrust PAM drivers**

for secure integration and identity synchronization.

- Performed **fine-tuning and performance optimization** of IDM drivers by optimizing rule placement, indexing, and trace file management.
- Actively contributed to multiple **IDM driver enhancement projects**, supporting continuous improvement and automation initiatives.
- Troubleshot and resolved user, password synchronization, and authentication issues across distributed IDM environments.
- Utilized tools like **iManager, ConsoleOne, Designer, and LDAP Browser** for IDM administration, driver configuration, and identity synchronization tasks.
- Collaborated closely with **help desk teams and end-users** to resolve daily operational and access management issues.
- Led **enterprise-wide user migration** from short names to unique IDs to standardize identity formats.
- Coordinated with **application owners** to integrate business systems with IDM for **Single Sign-On (SSO)** and federated authentication, leveraging technologies such as **Java, .NET, Angular, UNIX, SQL, Windows, Active Directory, and XML**.
- Generated scheduled **daily and weekly reports** based on business and compliance requirements.
- Configured and maintained **Self-Service Password Reset (SSPR)** for password management within the IDM environment.
- Created and managed **user groups in IDM**, assigning roles and entitlements as per business requirements.
- Processed **onboarding requests** for new hires, ensuring timely provisioning of access and accounts.
- Monitored **user profile attribute changes**, performed **database cleanup**, patching, and system performance tuning on a daily basis.
- Managed and administered the **RSA environment for multi-factor authentication (MFA)**, improving login security posture.
- Created and managed **Active Directory users, groups, and service accounts** to support both internal and external applications.
- Administered and supported **25,000+ external vendor portal users**, ensuring controlled access and handling L1 engineering support tickets.
- Managed **email accounts, distribution lists, and shared mailboxes** on **Office 365**, leveraging **Power Automate** for workflows and **Power BI** for reporting insights.

- Performed periodic **user cleanup operations** in IDM as per compliance and governance requirements.
- Familiar with **Identity Governance and Administration (IGA)** tools and frameworks for identity lifecycle and compliance management.
- Generated **weekly operational reports** for active users, service accounts, and vendor access audits.

Environment: Novell/NetIQ eDirectory, IDM, RHEL, Active Directory, BeyondTrust PAM, RSA MFA, Cayosoft, Office 365, Power Automate, Power BI, Java, .NET, Angular, UNIX, SQL, XML, iManager, ConsoleOne, Designer, LDAP Browser, Jenkins, Git/Bitbucket, SSPR, AWS, Azure, CyberArk, IGA tools (SailPoint, Okta).