**Identity and Access Management (IAM)**

 **(Sailpoint & Oracle) bhanuchandar0418@gmail.com**

**+1(949)5708206**

**Professional Summary:**

* I Have 11 years of professional experience in Information Technology, specializing in Identity and Access Management with a primary focus on **SailPoint IdentityIQ** and **Oracle IAM/OAM**
* Experience in designing, developing, testing, integrating, and implementing Identity and Access Management solutions using **SailPoint IIQ 7.3/8.2** and Oracle
* Proficient in **CyberArk's PAM** development, testing, and integration, ensuring robust security measures
* Installation and configuration of SailPoint application across all environments: development, staging, acceptance, and production
* Worked with **Active Directory (AD), LDAP, JDBC**, and delimited Human Resource Management Systems (HRMS) for Identity and Access Management (IAM)
* Extensive experience in customizing **PAM** solutions to align with organizational requirements
* Proficiency in installing and configuring key CyberArk components including Vault, **CPM**, **PVWA, OPM, AIM**, and PSM, ensuring a robust privileged access management **(PAM)** infrastructure.
* Implemented custom changes and extensions to SailPoint IdentityIQ Identity Manager and Access Manager, also performed integrations with multiple applications such as AD, Exchange, **RDBMS, Flat File, and LDAP** (Lightweight Directory Access Protocol)
* Integrate **OAM and Okta** with directory services such as Active Directory or LDAP for user authentication and attribute synchronization
* Manage the entire lifecycle of user identities, including provisioning, deprovisioning, and access recertification processes using OAM and Okta
* Collaborate with stakeholders, including business users, IT teams, and management, to understand business processes, identity management needs, compliance requirements, and security policies
* Configuring applications (Authoritative and Non-Authoritative) using Active Directory, Flat file, JDBC, Oracle Unified Directory, and LDAP connectors to load the Identity Cubes
* Experience working with configuration changes in **SailPoint IIQ** through connectors, Role Management, user provisioning, credential management, forms, Policies, Reports, application integration, and Life Cycle management
* Developing and designing workflows for user lifecycle processes, like **LCM** **joiner, mover, and leaver scenarios.**
* Develop test plans, **test cases**, and test scripts to validate SailPoint IIQ configurations and customizations. Conduct functional testing, integration testing.
* Customizing and configuring Sailpoint IdentityIQ according to the specific needs of the client.
* Defining and managing roles within the organization for efficient access control.
* Deploy Sailpoint Identity **IQ Console** for operations like import, checkout, connector Debug, Troubleshooting and Test Connection.
* Experienced in conducting Functional, Regression, System, and Acceptance Testing to ensure software quality and functionality.
* Proficient in configuring and troubleshooting version control systems like **GitHub, TFS, and CVS** for streamlined development workflows.
* Build and Configure Sailpoint Identity IQ in-built tasks like aggregation, Identity refresh, schedule tasks, correlation.
* Setting up and managing access certification campaigns to ensure compliance with policies and regulations.
* Participating in **SSB** architecture reviews and design discussions access data.
* Providing support and troubleshooting issues related to Sailpoint IdentityIQ.
* Training end-users on Sailpoint functionalities and creating documentation for developed solutions.

**Technical skills:**

|  |  |
| --- | --- |
| **Identity and Access Management:** | Sailpoint IdentityIQ 7.3/8.2,Oracle Identity Manager, Oracle Access Manager, Oracle Unified Directory, Oracle Internet Directory, Oracle Virtual Directory, MS Active Directory,CyberArk,,PAM,Okta |
| **Languages:** | Java, Java script, SQL, XML, SOAP, Web Services |
| **Application Servers:** | WebLogic, WebSphere, Apache Tomcat |
| **Tools/Utilities:** | Eclipse, JDeveloper, NetBeans, Apache Ant. |
| **Configuration Management:** | Git Lab,Git Hub,Git,Jenkins  |
| **Databases:** | Oracle 11g/10g/9i/8i, MS Access, MySQL, MS SQL Server |
| **Other Tools:** | MS Office Suite, MS Excel, MS Visio |

**Education: Master of Computer Application, JNTU -2012**

**Client Kemper (Chicago) Oct 2023- Till date**

**Role: IAM Technical Lead**

**Responsibilities:**

* Collaborated with stakeholders to define requirements and configured the platform accordingly.
* Customized Sailpoint forms, **workflows**, and user interfaces to satisfy client requirements
* Coordinated the user onboarding, transfers, and offboarding phases of the identity lifecycle management process.
* Process simplification to increase effectiveness and decrease manual intervention
* Configuration of Roles, Policies and Certifications for governance compliance
* Centralizing identity management required integrating SailPoint with a variety of HRMS and directory servers
* Analyze existing systems, processes, and data flows to identify gaps, inefficiencies, and areas for improvement. Document business requirements, functional specifications, use cases, and user stories for SailPoint IIQ implementations.
* Participate in project planning, resource allocation, timeline management, and status reporting for SailPoint IIQ implementation projects.
* Collaborate with stakeholders to gather and analyze requirements for IAM systems, translating business needs into technical specifications.
* Conduct risk assessments and security audits to identify vulnerabilities in IAM systems and recommend mitigation strategies.
* Created and improved identity management process automation workflows and Reduced manual intervention
* Build and Configure SailPoint Identity IQ in-built tasks like aggregation, Identity refresh, schedule tasks, correlation.
* Design and develop new audit report templates according to the specifications of SOX (Sarbanes-Oxley Act), PCI (Payment Card Industry), and CPNI (Customer Proprietary Network Information) regulations.
* Upgraded SailPoint Identity IQ 7.3 to 8.2 in both Prod and Non-Prod.
* Integrated web service-based applications to authenticate and authorize users based on their access and data in SailPoint Identity IQ.
* Collaborate with stakeholders to understand requirements for integrating Microsoft Azure AD, Windows AD, and LDAP with Identity and Access Management (IAM) systems.
* Involved in Configuration and development of SailPoint Life Cycle Events (LCM).
* Designe SailPoint IIQ deployment activities - connector configuration, custom rule development, workflow configuration and development, third party system integration in both Production and Non-Production Environments.
* Conduct thorough root cause analysis (RCA) investigations for critical incidents to identify underlying issues and contributing factors.
* Participate in the production support on-call rotation scheduled to provide timely assistance and resolution for system issues outside of regular business hours.
* Used SSB for build, configuration management and solution deployment of custom components.
* Deploy SailPoint Identity IQ Console for operations like import, checkout, connector Debug, Troubleshooting and Test Connection.
* Development of identity federation connectors from SailPoint Identity IQ to target systems, along with subsequent access control by Secure AUTH
* Integrate web service-based applications to authenticate and authorize users based on their access and data in SailPoint IIQ
* Evaluate IAM vendors and technologies, assessing their suitability for meeting organizational requirements and objectives.
* Stay updated on emerging IAM trends, technologies, and threats, and recommend enhancements to existing systems to improve security posture and efficiency.
* Configure various certifications in Sail point like Manager, Advanced and Account Group Permissions with Delegation s Rules
* Provide support during User Acceptance Testing (UAT), addressing any issues and ensuring successful deployment.
* Ensure documentation is comprehensive and accessible for reference by team members and stakeholders.
* Execute smoke and System Integration testing to validate the functionality and integrity of developed so
* Maintenance of Sail point and LDAP connectivity.
* Implement user provisioning from Sail point and aggregate users into Sail point from connectors like Active Directory

**Environment**: SailPoint IIQ 7.3/8.2 IAM, CA SiteMinder, Windows Server 2012, OracleDSEE 6.2, IIS 6.0, Apache 9.2, Sun One Web Server 6.2, LDAP, Apache..

**Client: AT &T (Charlotte NC) Oct2022- Oct 2023**

**Role: Implementation- Principal Consultant**

**Responsibilities:**

* Perform installation and configuration of Sailpoint IdentityIQ
* Involve in designing and implementing SailPoint Implementation
* Design Custom Tasks, Custom Reports to cater client needs in IIQ (Sailpoint)
* Develop custom connectors within SailPoint IdentityIQ to facilitate smooth integration with PAM applications
* Implement automated workflows in SailPoint IdentityIQ for efficient governance of privileged access to PAM applications
* Develop various reports like Uncorrelated Accounts Report, New Accounts Reports.
* Implement password reset management for the client
* Implement End user Access Request
* Use IIQ Console for operations such as checkout, import, connector Debug.
* Develop Correlation Rule as part of one of the client requirements
* Develop Custom java classes to fetch Custom Tasks in IIQ
* Adhere to established SDLC processes and best practices to ensure the quality and reliability of deliverables.
* Develop custom reports with client specific requirements to attain their Revocation and Audit Reports
* Design and developed the application using Java Server Faces (JSF) framework and Struts framework
* On-board Delimited file applications, LDAP, UNIX and ESS applications
* Coordinating with the Team for fixing the issues and reassigning the issues back to QA team for verification and closure
* Configure connectors, adapters, or agents to establish connectivity between Azure AD, Windows AD, and LDAP directories and the IAM solution.
* Collaborate with customers to understand their specific use cases and configurations.
* Lead the development of IAM solutions, including designing and implementing identity provisioning, authentication, authorization, and access control mechanisms.
* Provide technical leadership in IAM projects, guiding the development team in implementing robust and scalable solutions.
* Respond to customer inquiries and issues related to SailPoint'.
* Use incident management systems to track and document customer-reported issues.
* Validate and troubleshoot data integrity issues during migration.
* Plan and roll out of phase wise implementation of recertification applications globally.
* Manage both low and high-severity incidents across the entire incident life-cycle in accordance with availability, resolution and restoration
* Perform routine system administration tasks, such as user provisioning, workflow configuration, and policy management.
* Improve Identity and Access Management (IAM) capabilities by controlling access to applications and systems that contain critical and sensitive information
* Administered and enhanced the ITIL best practices in Problem Management process and other ITIL Processes, such as Change Management and Incident Management
* Integrated application utilizing SailPoint IIQ Out of the Box connectors and custom connectors
* Documented and maintained the audit communications, metrics and recertification artifacts
* Environment: Sailpoint IIQ 7.0, 6.4, XML, HTML, CSS, Java Script, BeanShell Scripting, Apache, Tomcat 7.0, Oracle SQL 11g.

**Environment:** Sailpoint 7.0, Java, Tomcat 5.6/8.0.x, WebLogic 10.3.6, WebSphere 8.5.0, GitHub.

**Client: Rio Tinto (Denver) May 2017- Sep2022**

**Role: Identity Management -Sr.Consultant**

**Responsibilities:**

* Installed and configured of OIM, OAM, SOA, OID and OHS servers.
* Installed and Integrated OIM 11gand Connectors and provisioned users to target applications.
* Created Adapter tasks for User and Connector specific process definition form like Entity adapter task, Rule generator adapter task, Pre-populate adapter tasks
* Configure and administer single sign-on (SSO) solutions across various applications and services using OAM and Okta capabilities.
* Define and enforce access control policies based on user roles, groups, and attributes to ensure secure and compliant access to resources.
* Integrate diverse applications and services with OAM and Okta for centralized authentication, access management, and user provisioning.
* Ensure adherence to security standards and regulatory requirements (e.g., GDPR, HIPAA) by implementing appropriate controls and audit mechanisms in OAM and Okta environments.
* Monitor and respond to security incidents and access-related issues, conducting root cause analysis and implementing corrective actions as necessary.
* Establish federated identity relationships with trusted partners and external identity providers (IdPs) to enable seamless access to shared resources.
* Assess security risks related to identity and access management, and implement risk mitigation strategies and controls in OAM and Okta environments.
* Automate user provisioning and de-provisioning processes across applications and systems, ensuring timely and accurate access management.
* Implement self-service capabilities for users, such as password reset and profile management, using OAM and Okta self-service tools.
* Configure Trusted and Target Application resources with OIMLDAPCoding Adapters, Schedulers, Event Handlers and Custom Connectors
* Approval based Provisioning of Resources
* Design and Develop Adapters, Schedule Tasks for Application Resources
* Developed and arranged the Roles with Access policies to procurement of clients in to the LDAP Groups.
* Configured and Implemented Role and Attribute Based Access Control Policies using Oracle Access Manager.
* Troubleshooting WEBGATE which is unable to connect to its associated access server
* Setup Reconciliation of users with HRMS systems, which was used as source of truth for IAM solutions.
* Implemented SSO using OAM 11g R2 and configured multiple authentication schemes and authorization plug-in based on the requirement
* Having knowledge on Configuring Identity Store, Application Domains.
* Created Identity Assertor and Identity Authentication Provider in WebLogic Console Security Realms for SSO.
* Designed OIM system integration with all target systems based on client IAM and integration requirements and configured access policies through role to provision users automatically into OID Target System
* Worked on Oracle Identity Manager 11g provisioning and request approval workflows for adapters, process tasks, process definitions,
* rule designer, schedule tasks, form designer
* Developed and arranged the Roles with access policies to procurement of clients in to the LDAP Groups
* Developed Pre-populate, Process task Adapter
* Consult and configure access management policies for customer applications using enterprise level identity management tools
* Provide support to security and develop appropriate audit controls and procedures to ensure the integrity of applications.
* Provide the capability of categorizing user access by job description for ease of user access provisioning
* Configuration the integration of the Process Form and Process Definition, involved in development of Pre-Populate Adapters
* configuring Periodic reconciliation with HRMS, AD,OID and Third Party Custom applications
* Auto provisioning of users to Application resources

**Environment**: Oracle IDM/IAM Suite 11.1.1.6, Oracle SOA Suite 11.1.1.6, OSB11.1.1.6, Web logic 10.3.6, AIA FP 11.1.1.6, Oracle Database 11g, Oracle Web center Portal, Web Center Content, ODI 11.1.1.6, Jdeveloper 11.1.1.6

**Client: New Co (Vodafone ) -UK Feb2013-April 2017**

**Role: Identity Management Consultant**

**Responsibilities:**

* Responsible for planning, designing, developing, testing, and implementing Oracle identity and access management (IAM) systems.
* Implemented and configured Oracle OIM, OAM and OIDcluster for high availability.
* Applied every quarterly patches(PSU’s) to all dev, test, and prod environments.
* Strong knowledge ofLDAP and Access management.
* Experience working with WebLogic 12c, web services, endpoint security, OWSM, etc.
* Work on resolving service requests by customers on various cloud operational requirements.
* Re-factored schedule tasks and event handlers to enhance and improve existing solution.
* Performed impact analysis on the existing customizations of connectors, workflows and OIM components.
* Preformed Pre upgrade steps and generated reports to identity and resolve the incompatible steps.
* Debugged and fixed the issues.
* Performed smoke test successfully in DEV/QA and PROD environments. Preparation of deployment guide with detailed instructions.
* Design Role management process and customize approval workflows.
* Documented the approach and test evidence for the issues and enhancement.
* Managed user provisioning to Active Directory, LDAP**.**
* Designed scheduled tasks for user reconciliation and clean-up processes.
* Implemented password synchronization between OIM and AD.
* Setup direct connectors for AD, LDAP.
* Configuration of Roles, Policies and Certifications for governance compliance.

**Environment:** OIM 11gR1, OAM 11gR1, WebLogic, SOA, JDeveloper, Explorer, Putty, Linux, XML, Oracle Internet Directory (OID) 11g,Oracle Virtual Directory (OVD) 11g, Windows 7, Red Hat Enterprise Linux 5, Oracle 11g