**Sashank**

**IAM Engineer (ForgeRock/Okta/Ping)**

**Email:** [**gsashank.iam@gmail.com**](mailto:gsashank.iam@gmail.com)

**Mobile: +1(980) 500-9994**

**PROFESSIONAL SUMMARY:**

* Around 8+ years of experience in the IT field including Installation, Configuration, Development, Deployment, Administration, troubleshooting and network security, database systems, and Enterprise Document Management in large-scale organizations.
* Experienced in **IAM/PAM** tools with deployment, configuration, integration, and troubleshooting **CyberArk** Privileged Account Security product suite - Enterprise Password Vault, Password Vault Web Access, Central Policy Manager, Privileged Session Manager, Application Identity Manager, and Privileged Threat Analytics
* Experience in handling various modules of CyberArk, mainly Enterprise Password Vault (EPV), Application Identity Management (AIM), Central Policy Manager (CPM), Privileged Session Management (PSM), and Event Notification Engine (ENE). Upgrading CyberArk suite of products from 7.x to 9.x. (CPM, PSM, EPV and PVWA)
* Experience as a security professional in installing, managing, and monitoring CyberArk Privileged account security tool modules.
* Part of the Privileged Access Management (**PAM)** Remediation and Engineering team whose role is to secure web-based applications on user access and authorization. Performing daily operations support and maintenance of all security technologies centric to Privileged Access-related information security solutions.
* Responsible for synchronization of all Active Directory accounts and groups to utilize Okta solution.
* Worked on day-to-day activities creating and managing **OKTA** policies and creating and managing OKTA application provisioning and user provisioning.
* Installed and Configured **OKTA LDAP** Agent for delegated authentication with Okta. Migrated Users from LDAP and Active Directory to OKTA Universal Directory and provided L2 support for LDAP.
* Experience in SAML-based authentication 1.1 and 2.0 using **Ping Federation**, **Site Minder Federation**, and integration with Site Minder authentication and another adapter.
* Experience in deploying **SAML**-based highly available solutions using Ping Federate and other security products. Worked on **Ping Access** Integration with **Ping federate** to Protect the applications using Ping Access Tokens. Worked on ping federate both inbound and outbound calls using **SAML 2.0.**
* Migrated SAML and **OAuth** connections from NetIQ Access Manager to Ping Federate in the staging Environment.
* Experience with **Single Sign On** (SSO) technologies such as PingFederate, Ping Access, ADFS, and Azure AD.
* Experience with DevOps practices, CI/CD pipelines, and Git.
* Extensive experience in building CI/CD pipelines using tools such as Hudson, Bamboo, Jenkins, and TeamCity for end-to-end automation of builds and deployments.
* Proficient in designing and implementing CI/CD pipelines, optimizing application performance, and ensuring efficient and reliable software delivery.
* Strong knowledge and experience in creating CI/CD pipelines with Git/SVN, Jenkins, Maven, NEXUS, and Docker on cloud platforms like AWS.
* Hands-on experience with **IIS, IBM IHS, Apache, Sun One Web servers, and WebLogic and WebSphere Application servers** in an Identity and access management environment.
* Worked with Active Directory, LDAP/UNIX groups, Networks, and Human Resource systems for Identity and Access Management. Designed SailPoint deployment activities - connector configuration, custom rule development, workflow configuration, and development and third-party system integration.
* Experience with the Implementation and Administration of **Sail Point** for a large population of users. Experience in SailPoint tool customization, Report Generation, Integration with end/target systems, SailPoint APIs, and Application Development.
* Experience with Installation and configuration of **CyberArk Vault, CPM, CyberArk PVWA, OPM CyberArk PSM, AIM, and PSM SSH** proxy Architecture and design.
* Experience with IAM products from **ForgeRock (OpenIDM, OpenAM and OpenDJ**) and building IAM solutions implementing **OAuth2 and ODIC** specifications.
* Extensive experience onboarding Windows, UNIX, Database servers, RACF, and Network devices into CyberArk. Experience in managing applications access in Okta and Active Directory. Exposure to design and architecture of PIM using **Cyber-Ark**. Account management i.e. adding /deleting accounts /group management. Managing policies and platforms. Creating and assigning Safes, reconciling accounts, and rotating passwords.
* Generating various reports in IIQ like Identity Reports, Orphan Account reports, Account Discrepancy reports, Role composition reports and Application attribute reports, etc.
* Coordinating with the existing Provisioning Team for the application to get the existing User Access Management **(UAM)** model to make it fit into IIQ.
* Managed Terraform templates for IAM automation in Azure and AWS Cloud, optimizing infrastructure provisioning and maintenance workflows.
* Utilized NoSQL databases to store and manage IAM-related data, optimizing data retrieval and storage efficiency.
* Provisioning application requests in IdentityIQ to Create/Amend/Delete user access for the onboarded applications. Good understanding of policies in CyberArk Central Policy Manager (**CPM) and PAM.**
* Developing Application instances and entitlements and Integrating New Applications (Connected and disconnected) with OIM.
* Involvement in cross-communication across functional teams, Managing Stakeholders' expectations. Strong understanding of the full software development life cycle, including troubleshooting, debugging, and production support.
* Proven ability to tackle and succeed in all endeavors from business development to customized software development and implementation. Have repeatedly led teams in successfully deploying complex technical solutions.
* Proficient in scripting languages such as Python, Angular, React, Node.js, Spring Boot, and Java.

**TECHNICAL SKILLS:**

|  |  |
| --- | --- |
| **RDBMS:** | Microsoft SQL Server 2008/2012, ORACLE 10g/11g |
| **Platforms and Misc.:** | Microsoft Visual Studio 2008/2010/2012 , Windows: XP /Vista / 7 / Server 2003/2008, Linux, HP Quality Centre, Active Directory, ADCS, ADFS, SCCM. |
| **Security Tools:** | IBM Identity Management and p6, CyberArk Privileged Account security 9.7.2, IBM Tivoli Access Manager 6.1.1, Tivoli Federated Identity Manager 6.2.2, Microsoft Active Directory. |
| **Operating Systems:** | SUSE Linux 9/10/11, Windows Server 2000/2003/2008/2012/2016/2019, Unix |
| **Directory Services (LDAP):** | Novel eDirectory 8.7.x/ 8.8.1/8.8.5, Sun One/iPlanet DS 5.x/6.x., eDirectory 8.X, Active directory (ADLDS), Microsoft Active Directory, ForgeRock OpenDJ 3.x/5.x/6.x, CA Directory R12.x, RedHat LDAP |
| **SSO and Identity:** | Novell/NetIQ Access Manager, ForgeRock 13.5/5.x/6.x/7.x, Ping Federate 6/7/8, SiteMinder R12 SP2, SP3 / R6 SP1, SAML 2.0. PingFederate v8.2.2, PingAccess v4 |
| **Web Servers:** | Sun One 4.1/5.1/6.1, Apache 2.0/2.2.4, IIS 5.0/6.x/7.x/8.x/10.x, Tomcat 4/5 |
| **Languages:** | SQL, J2EE, JAVA Script, Python |

**PROFESSIONAL EXPERIENCE:**

**Client: DXC Technologies, New Orleans, Louisiana (Mar 2021 to Present)**

**Role: Sr. IAM Consultant (ForgeRock/Ping Federate/ Okta/LDAP)**

**Responsibilities:**

* Working as an IAM Engineer as part of the Cybersecurity engineering team to support and administer ForgeRock OpenAM/OpenDJ or Oracle LDAP/SiteMinder infrastructure of various applications.
* Involved in implementing the B2B portal, which includes building the SiteMinder/ ForgeRock or Oracle LDAP/ForgeRock OpenAM servers and Reverse proxy servers for SiteMinder or ForgeRock web agents.
* Involved in implementing various SAML SSO setups where SiteMinder acts as a Service Provider or Identity Provider and external vendors act as Identity Providers or service providers using SAML 2.0 in IDP/SP initiated method.
* Involved in Designing and building ForgeRock OpenAM & OpenDJ environments from scratch as part of the migration from SiteMinder infrastructure for B2B & B2E portals.
* Involved in planning and implementing migration from SiteMinder to ForgeRock OpenAM environment for various portals.
* Worked with various application teams to migrate from SiteMinder Web Agent to ForgeRock Web Agent for various portals successfully.
* Worked on setting up ForgeRock J2EE Agents on various application servers like Tomcat/IIS.
* Worked on various ForgeRock Web agent upgrades from 4.x to 4.2 & 5.x as well and resolved any issues.
* Worked with various vendors or banks or application teams to implement SSO using SAML or OIDC where ForgeRock can act as IDP or SP & authorization servers.
* Worked on designing, building, and migrating environment from Oracle ODSEE LDAP to ForgeRock OpenDJ where OpenDJ will act as an authentication provider for almost 60k+ Linux clients.
* Involved in upgrading and building a new environment globally across 4 data centers with ForgeRock OpenAM 6.x along with deploying authentication modules & and trees and migrated almost 300+ applications to the new platform without any issues.
* Worked on upgrading ForgeRock OpenAM versions from AM 13.5 to 6.x and agents from 4.x to 5.x.
* Integrated efforts for SSO protocols including SAML 2.0, WS-Federation, OAuth 2.0, and OpenID Connect, ensuring seamless authentication across systems.
* Utilized Node.js, Spring Boot, and AWS Lambda to build robust backend services that supported IAM workflows.
* Collaborated with cross-functional teams to ensure seamless integration of CI/CD pipelines into the development and deployment workflows.
* Worked on optimizing CI/CD pipelines for performance, scalability, and cost efficiency.
* Strong troubleshooting and problem-solving skills to identify and resolve issues in CI/CD pipeline.
* Strong IT Experience with the major portion of IAM specializing in Okta.
* Managed access to applications access in Okta and the active directory.
* Created custom rules to prompt users for multifactor authentication after logging to the OKTA portal.
* Customized end-user login page using the OKTA admin portal.
* Performed attribute mapping on Okta and provided support for OKTA service/help desk queue - Identified and troubleshooted issues.
* Implemented SSO by Integrating on-prem applications with Okta Infrastructure using SAML, Open ID Connect (OIDC), and OAuth 2.0 service.
* Created different Okta Sign On policies and Okta MFA enrollment policies based on requirements for application IDs and different user types.
* Involved in various project meetings to analyze the requirements and implement them accordingly to integrate with B2B Portal.
* Worked with CA/Oracle/ForgeRock/Broadcom vendors to troubleshoot the various issues as part of integrating applications with B2B Portal.
* Worked in documenting the various applications for integrating with B2B Portal and handed them over to the operations team for implementation in higher environments.

**Environment:**Red Hat Linux 5.x/6.x/7.x/8.x, Solaris 8/9/10, IIS 6.x/7.x/8.x/10.x, AIX 5.x/6.x, SiteMinder 6.x/R12, SiteMinder Web agent 6.x/R12.x,, Web Sphere Application Server, Oracle Directory Server 5.x/6.x/11g,ForgeRock OpenAM 13.5/5.x/6.x, ForgeRock OpenDJ 3.x/5.x/6.x/7.x, CA Directory R12.x, Red Hat LDAP.

**Client: Comcast, Philadelphia, PA (Feb 2019 to Mar 2021)**

**Role: IAM Engineer**

**Responsibilities:**

* Manage client requirements and configure Sail Point connectors for various applications. Develop Rules like Build Map, Correlation, Exclusion, Policy Violation, Policy Formatting etc., as part of connector development.
* Design & Implementation of SailPoint IIQ. SailPoint IIQ Installation and Configuration as required by the design solution. Implementation of Self-Service feature, Password features (PTA, forgot password, Change Password provisioning feature, configuring various roles and policies in SailPoint Set up SailPoint IIQ policy server on 4 environments (Dev., QA, UAT, and Production).
* Designed and deployed Identity & Access Management solutions to improve user experience, meet compliance, and reduce costs. Involved in Designing & and Implementing SailPoint IdentityIQ. Implementation of Self-Service feature, Password features (PTA, forgot password, Change Password), provisioning feature, configuring various roles and policies in SailPoint.
* Worked on resolving tickets using ServiceNow implementation. Involved in Application development by using connector configurations like Oracle unified directory, delimited, DB, SAP Active Directory etc. Supported operations & and maintenance of SailPoint and LDAP connectivity. Triggering custom mail notifications to the manager when the company or department or manager of an Identity is updated in IdentityIQ.
* Developed a new environment and deployed Novell Access Manager 4.2 for implementing OAuth 2.0. Configured OAuth 2.0 to test different grant types. Used OAuth playground to retrieve access token and refresh token.
* Experience securing Single Page Applications (SPAs) and working with various IAM technologies like SSO Identity Provider, Cognito, Azure AD, AWS IAM.
* Strong experience with SSO Identity Providers such as Cognito, Azure AD, and Active Directory.
* Documented and presented different OAuth flows to different teams. Upgraded Novell Access Manager from 4.2 to 4.3 to fix issues faced in OAuth 2.0. Worked with different teams to implement single sign on using SAML 2.0.
* Frame set up for Role mining, Role Based Access Control (RBAC), Entitlement Management and Identity Management. Successfully organized, tested, and upgraded SailPoint IdentityIQ version 6.3 to version 7.1p1.
* Provisioning application's requests in IIQ to Create/Amend/Delete user access for the on boarded applications. Configuration of Roles, Policies and Certifications for governance compliance and configure business processes to manage ongoing changes.
* Working experience in the development of WebSphere Portals, Portlets, CA-SiteMinder Single sign-on Services with SiteMinder configurations (setting up policies, realms, rules, and responses), Google Federation along with posting credentials to FCC from a custom Application Login JSP/HTML page.
* Involved in creating custom reports, and certifications to cater to various data feeds knowledge in bean shell scripting and workflow rules.

**Environment:** Sail Point IIQ, Active Directory, LDAP, C, JAVA, J2EE, JDBC, JavaScript, CSS, HTML, XML, AJAX, Oracle database, SAML 2.0, OAuth2.0, E-directory, SunOne Directory Server, CyberArk, Ping federate 7, Ping Access, Apache 2.x, Webserver 6.1, Tomcat 4/5.SQL Developer, SQL, PL/SQL, NetIQ Access Manager 3.2/4.2/4.3, Ping Federate 7/8, CyberArk Privileged Account security 9.7.2

**Client: T-Mobile, Atlanta, GA (May 2017 to Jan 2019)**

**Role: SSO/IAM Engineer**

**Responsibilities:**

* Configured SiteMinder for SAML Federated Authentications by configuring ID Provider/Consumer using SAML 2.0 POST binding, Installed Web agent Option Pack and created Partnerships, Documented Visio for SAML, Auth Schema and Day-to-day maintenance of SiteMinder policy servers and troubleshooting production issues.
* Coordinated with the Service providers and identity providers during the SAML Certificate upgrade and architectural changes, Upgraded CA SiteMinder to R12 from 6 installed the Admin UI, and configured the FSS Admin GUI.
* Engaged to help clients design and implement a Single Sign-on Solution using the ForgeRock stack using Open AM and OpenDJ for a billion users, with a rapidly changing software base using an Agile model and continual build/test process.
* Installed and Configured Ping Federate. Integrated internationalization for Ping One web applications. Hands-on experience on Ping Federate, CA Single Sign-ON, CA Advance Authentication, CA Secure Proxy Server, Ping Access, and Ping Cloud. Have good knowledge of Ping Access. Worked on version 4.0.
* Experience in SAML-based authentication 1.1 and 2.0 using Ping Federation, SiteMinder Federation, and integration with SiteMinder authentication and adapter. Experienced in migrating NetIQ Access Manager to Ping Federate. Deployed Ping One in the Cloud and integrated with Ping federate on-premises Created ACO, HCO, and User Directory for LDAP and AD.
* Implemented SiteMinder monitoring using SiteMinder SNMP client, SiteScope, and Zabbix monitoring system. Implemented SiteMinder password policies for external SunOne LDAP user repositories. Installed and configured BOXI Report Server for SiteMinder audit logs registered with JBOSS. Installed, configured, and administered Sun One LDAP Directory and Site-Minder Policy Servers. Optimized volumes, and AWS EC2 instances by creating multiple VPC's and balanced load effectively.
* Extensive hands-on experience on SailPoint IdentityIQ, ForgeRock OpenAM & OpenDJ, IBM Security Identity Manager, IBM Security Access Manager and IBM Security Access Manager for Enterprise Single Sign On, IBM Security Directory server, IBM Security Directory Integrator, Session Management Server, WebSphere Application Server, and SUN Identity Manager implementations.
* Configured and deployed Scheduled Tasks, developing process forms and child forms and doing customizations in connector configurations using the design console. Implemented AWS solutions using EC2, S3, RDS, EBS, Elastic Load Balancer, and Auto scaling groups.
* Designed and deployed Forge Rock Open AM and Open IDM to migrate from the CA Cloud minder. Multi-Factor Authentication (RSA, DUO, SecureAuth, ForgeRock, SailPoint, CA Arcot, Okta). Configured Process Tasks, Adapters, and Event Handlers for provisioning and de-provisioning of users.

**Environment:** CA SiteMinder 12.52/12.6, CA SPS, F5 APM module CA API Gateway and Mobile API Gateway, CA IDM, CA Advanced Authentication (CA Strong Auth and CA Risk Auth), Apache, Linux, IBM Lotus Notes, LDAP, Oracle Identity Manager 11g R2, Microsoft Active Directory, OIG, OID 11.1.1.6, Web logic 10.3.6

**Client: United Airlines, Chicago, IL (Oct 2015 to Apr 2017)**

**Role: Jr. IAM Engineer**

**Responsibilities:**

* Integrate applications from development to production and assist development teams in identifying and resolving various issues related to SiteMinder. Created **Rules, Rule groups, Response, Response groups, Realms, and Policies** for Directory Server users, implemented SiteMinder policy-based security.
* **Coordinated** with the Service providers and identity providers during the **SAML Certificate upgrade** and architectural changes. Worked with the SiteMinder engineering team to document technical specifications and procedures for SiteMinder best practices.
* **Implementation of SSO** and authentication services using CA Netegrity SiteMinder. Responsible for Performance Tuning for SiteMinder to provide better response time, low latency, high availability, and maximum throughput.
* Created policies, realms, rules, and responses in the SiteMinder Policy Server to protect the applications and validate the users to work under the SSO environment. Understand business processes and challenges to supply recommended Identity Management Solutions and educate application teams on how to integrate with Identity and access Management solutions.
* Communication of project status to project managers and management. Identify issues within a solution and supply leadership with technical answers and options, provide support and documentation to assist in sustaining the project during the transition to production.
* Experienced in overall administration and technical support of CA SSO and CA Access Gateway ensuring acceptable and consistent levels of performance through optimization. Installed and Configured CA SiteMinder Policy Server 12.7, CA Access Gateway 12.7 and CA Web Agent 12.52 on Microsoft Windows, CentOS, Red Hat Enterprise Linux, and Solaris environments.
* Configured Policy Stores, Key Stores on CA Directory, User Store on Active Directory and Session Store on SQL Servers, Configured and defined the Policy Domains, User directories, Rules, Realms, Policies, Password Policies, and Responses in SiteMinder to protect and manage access to enterprise resources.

**Environment:** CA SiteMinder R12 SP3, Sun Solaris 9/10, Windows Server 2003, SunOne Directory Server, IIS 6.0, Apache 2.x, Webserver 6.1, Tomcat 4/5. SiteMinder policy server R12 to latest, CA Directory, Secure Proxy Server, JBoss, Tomcat 6x, Red Hat 5/6.