**Akash Dasari**

**Ph: +1 (989) 359-0786**

**Email:** **panid8111@gmail.com**

**IAM Engineer**

##### **Professional Summary**

* 8+ years of experience in the IT field and providing strong technical and security functions to companies and organizations.
* I have successfully implemented more than 250 applications for Multifactor authentication, utilizing Azure AD and creating conditional policies.
* Experience in implementation, deployment, and upgrade of various versions of CyberArk (PIM suite) including the components – Vault, PSM, CPM, PVWA and AAM
* Experience in implementation of authentication in CyberArk using LDAP, RADIUS and SAML
* Extensive experience in implementation and deployment of Privileged Account Security solution (CyberArk) for Windows, UNIX, Database servers, Security, Networks and Websites.
* Good experience in configuration of roles, policies and certifications for governance compliance.
* Hands on experience with understanding of policies in CyberArk components like CPM, PVWA, and PSM.
* Performing integration of LDAP/S, Active Directory, SSO authentication methods using CyberArk.
* I have offered expert advice on the technical development of support knowledgebase.
* I have authored technical documentation for project implementation and branch technical readiness, while also being involved in projects involving configuration, installation, and support of multiuser facilities.
* Utilized Microsoft Graph API to enhance Azure IAM capabilities, allowing for efficient querying and updating of user attributes, groups, and access policies.
* I have worked on Identity and Access Management implementations on Unix and Windows platforms, utilizing environments such as Azure, Okta and legacy CA SiteMinder
* I have carried out monitoring tasks, managed certification authority (CA), and generated reports.
* I have dealt with troubleshooting issues that arose during the implementation, upgrade, and integration of Oracle Identity Management suite components.
* I have performed integrations of LDAP, Active Directory, and SSO authentication methods.
* I have provided day-to-day operational support in Active Directory, including tasks such as creating security groups, user management, policy assignment, password complexity rules, commissioning, and decommissioning applications, as well as creating and maintaining service accounts.

##### **PROFESSIONAL EXPERIENCE**

**Client: Giant Eagle, Pittsburg, PA March 2022 to till date**

**Role: Identity & Access Management Engineer**

**Responsibilities:**

* Proficient in migrating Single Sign-on (SSO) applications from ADFS to Azure AD.
* Skilled in setting up and managing Azure Conditional Access Policies and Multi-Factor Authentication (MFA) for various client applications and systems.
* Conducted analysis and documentation of user and system requirements to establish the appropriate solution, including developing a proof of concept that showcased the solution's out-of-the-box capabilities and required customizations.
* Proficient in implementing various identity and access management features such as Entitlement Life Cycle, Self-Service Password Management, Role-Based Access Control, Strong Authentication, and Single Sign-On.
* Worked on Upgrading CyberArk V10.10 to V11.7.
* Worked on new connection components for PSM.
* Worked on CyberArk AAM (Application Access Manager).
* Experience in Microsoft Azure AD, ADFS, AD Connect.
* Successfully onboarded applications to the Azure Platform while ensuring secure identity management through access policies.
* Provided technical support and training to end-users on Single Sign-On (SSO) methods, such as SAML, OAuth, and OIDC, ensuring smooth adoption and utilization of the implemented solutions.
* Implemented SCIM provisioning for Azure AD and automating user provisioning and attribute management.
* Extensive experience in integrating access management applications and systems with Single Sign-On methods like SAML, OAuth, and OIDC.
* Provided recommendations and configured conditional access policies for enhanced security.
* Created high-level language-based patterns for conditional access policies based on different scenarios.
* Integrated with RESTful APIs and APIs to enable seamless data exchange and integration between Azure IAM and external systems.
* Utilized Microsoft Graph API to enhance Azure IAM capabilities, allowing for efficient querying and updating of user attributes, groups, and access policies.
* Configured and optimized APIs to enhance functionality and streamline processes within Azure IAM.
* Created and managed conditional access policies in Azure AD, including scenario-based policies rather than app-based policies, resulting in the consolidation of 60 policies to nearly 25.
* Designed and implemented Azure Active Directory (AAD) and Identity and Access Management (IAM) solutions for multiple clients.
* Developed and leveraged RESTful APIs to facilitate integration between Azure IAM and other systems, improving data flow and enhancing functionality.
* Implemented Password Hash Sync for seamless synchronization of passwords between on-premises Active Directory and Azure AD, simplifying user authentication processes.
* Successfully facilitated the migration of over 30 applications from ADFS to Azure AD within a period of 5 months ensuring compatibility and seamless user experience throughout the transition.
* Facilitated the automation of certificate renewal by manually uploading all SAML-based certificates to ServiceNow.

**Client:** **Global Atlantic Financial Group, Indianapolis, IN Jun 2020 - Feb 2022**

**Role: Identity & Access Management Engineer**

**Responsibilities:**

* Worked on various IAM Identity provider systems like Okta, Azure.
* Experienced in vaulting and troubleshooting of Managed Accounts in CyberArk Password Vault
* Experience in implementation, deployment, and upgrade of various versions of CyberArk (PAM suite) including the components – Vault, PSM, CPM, PVWA and AAM
* Experience in implementation of authentication in CyberArk using LDAP, RADIUS and SAML
* Extensive experience in implementation and deployment of Privileged Account Security solution (CyberArk) for Windows, UNIX, Database servers, Security, Networks and Websites.
* Experience in LDAP technologies, provisioning using workflows and policies.
* Experience in Single Sign-On (SSO) Application migrations from ADFS to Azure AD.
* Analyzed and documented user and system requirements to define the solution and developed a proof of concept to showcase the out of the box capabilities and customization needed for implementing the solution.
* Entitlement Life Cycle, Self Service Password Management, Role-Based access control, Strong Authentication and Single Sign On.
* Strong understanding of authentication protocols and standards, including SAML, OAuth, OpenID Connect, and LDAP.
* Integrated with RESTful APIs and to enable seamless data exchange and integration between Azure IAM and external systems.
* Utilized Microsoft Graph API to enhance Azure IAM capabilities, allowing for efficient querying and updating of user attributes, groups, and access policies.
* Configured and optimized APIs to enhance functionality and streamline processes within Azure IAM.
* On-board applications to maintain the okta Platform, securing the identities with access policies.
* Experience in access management app & application integrations with SAML, OAuth, OIDC.
* Designed and implemented Azure Active Directory (AAD) and Identity and Access Management (IAM) solutions for multiple clients.
* Configured and managed Azure Conditional Access Policies and Multi-Factor Authentication (MFA) for client applications and systems.
* Implemented Azure Identity Protection to detect and respond to identity-based threats.
* Developed PowerShell scripts to automate user provisioning, deprovisioning, and other administrative tasks.
* Configured Azure Information Protection for data classification and protection.
* Implemented Identity for identity governance and access management, ensuring compliance and enforcing access controls.
* Worked closely with the security team to ensure compliance with security and regulatory requirements.
* Leveraged Okta API Access Management for securing application APIs and defining custom access policies for managing tokens lifetime.
* Setup MFA for all applications for Okta such as Okta push, Okta verify, SMS authentication, security questions.
* Integrated sustainable number of Okta provisioning via APIs.
* Day to day operational support in adding and deleting accounts, applying policies, assigning safes, synchronizing failed accounts, password rotations.
* Handling issues and providing 24/7 support during after-hours.
* I have experience with Python, PowerShell, Java Script, JSON, REST.
* Optimized Directory Mapping for user and group authentication.
* Experience with LDAP, SAML, SSO

**Client:** **BONYM, New York Sep’2018 – May 2020**

**Role: Identity & Access Management Analyst**

**Responsibilities:**

* Led and managed multiple IAM projects from initiation to successful completion, ensuring alignment with business objectives and delivering high-value product visions.
* Collaborated with cross-functional teams, including technical teams, to gather requirements and translate them into detailed user stories, refining them with subject matter experts.
* Facilitated Agile ceremonies, including sprint.
* I have experience with Python, PowerShell, Java Script, JSON, REST.
* Experience with LDAP, SAML, OAuth, SSO
* Optimized Directory Mapping for user and group authentication.
* Experience in Microsoft Azure AD, ADFS, AD Connect
* Migrating Single Sign-on (SSO) applications from ADFS to Azure AD.
* Skilled in setting up and managing Azure Conditional Access Policies and Multi-Factor Authentication (MFA) for various client applications and systems.
* Conducted analysis and documentation of user and system requirements to establish the appropriate solution, including developing a proof of concept that showcased the solution's out-of-the-box capabilities and required customizations.
* Proficient in implementing various identity and access management features such as Entitlement Life Cycle, Self-Service Password Management, Role-Based Access Control, Strong Authentication, and Single Sign-On.
* Integrated with RESTful APIs and to enable seamless data exchange and integration between Azure IAM and external systems.
* Successfully onboarded applications to the Azure Platform while ensuring secure identity management through access policies.
* Led successful on-premises to cloud migration projects, leveraging Okta's integration capabilities and best practices.
* Collaborated with stakeholders to assess current IAM infrastructure and designed migration strategies to transition from on-premises systems to cloud-based solutions, such as Okta.
* Implemented Okta Life Cycle Management workflows for the migrated cloud environment, automating user provisioning, deprovisioning, and user lifecycle management processes.
* Configured and optimized Okta Identity Governance and Administration features in the cloud environment, enforcing RBAC models, access policies, and access certifications to maintain compliance and enhance security.
* Designed and deployed Okta SSO solutions (SAML, OIDC, OAuth), integrating cloud-based applications and on-premises legacy systems, ensuring a seamless user experience across hybrid environments.
* Integrated on-premises directories, such as Active Directory, with Okta's cloud-based identity platform, enabling efficient user synchronization and centralized management.
* Developed custom solutions using Okta APIs and SDKs to address migration-specific requirements, automating user migrations, and data synchronization processes.
* Provided troubleshooting and support for Okta-related issues during the migration process, collaborating with cross-functional teams and Okta support to ensure successful migration outcomes.
* Implemented security best practices within the cloud-based Okta configurations, ensuring compliance with industry standards and regulations during and after the migration.

**Client:** **iBing Software Solutions Private Limited, India March’2015 – June’2018**

**Role: Identity & Access Management Analyst**

**Responsibilities**:

* Led and managed multiple IAM projects from initiation to successful completion, ensuring alignment with business objectives and delivering high-value product visions.
* Collaborated with cross-functional teams, including technical teams, to gather requirements and translate them into detailed user stories, refining them with subject matter experts.
* Facilitated Agile ceremonies, including sprint.
* I have experience with Python, PowerShell, Java Script, JSON, REST.
* Experience with LDAP, SAML, OAuth, SSO
* Optimized Directory Mapping for user and group authentication.
* Experience in Microsoft Azure AD, ADFS, AD Connect
* Experience in designing, implementing, and supporting CA SiteMinder identity and access management solutions.
* Strong understanding of authentication protocols and standards, including SAML, OAuth, OpenID Connect, and LDAP.
* Resolved complex SiteMinder-related issues by conducting root cause analysis, troubleshooting system configurations and collaborating with vendors for technical support.
* Automated vault activity reports and audit reports via scheduled tasks.
* Integrated Password Vault log reporting to the SIEM solution (Splunk).
* Setup LDAP integration, email alert notifications (Exchange Integration).

**Programming languages:** Python, Java script, C#, PowerShell

**Education**:

Bachelor of Technology in Information Technology from Velagapudi Ramakrishna Siddhartha Engineering College - 2015

**Certification:** Certified Okta Professional