**Srikanth Konari**

**+1734-469-7802**

**Email ID: sriam998599@gmail.com**

Professional Summary:

 Around 8+ years of IT experience in IAM Engineering, Cloud engineering with Excellent knowledge in IAM Administration Cloud Operations Engineering in AWS/Azure/Google cloud platform, Implementation of Scripting languages such as Bash, Python, and PowerShell to consolidate the workflow within the organization with Agile best practices.

Overall Summary:

* Experienced IAM Engineer specializing in multi-cloud environments, including Google Cloud, Azure AD, Okta, and Ping Identity.
* Expertise in implementing Conditional Access Policies and role-based access control (RBAC) to enforce secure, compliant access across cloud platforms.
* Proficient in SAML 2.0 SSO integration for centralized authentication and seamless user experience across cloud applications.
* Skilled in Okta Adaptive Authentication, Azure AD Conditional Access, and Ping Identity to enforce dynamic, risk-based access controls (e.g., MFA) based on user context and activity.
* Led the automation of identity lifecycle management (provisioning, de-provisioning, and role assignments) to ensure efficient, compliant, and secure user access.
* Designed and deployed Zero Trust Architecture with MFA, adaptive authentication, and least-privilege policies across both cloud and on-prem environments.
* Extensive experience in identity federation and SSO integration using Okta, Azure AD, and PingFederate for seamless access management across hybrid cloud ecosystems.
* Conducted IAM audits, and access reviews, and implemented identity governance models to ensure adherence to compliance standards (SOC 2, PCI-DSS, GDPR).
* Implemented and optimized IAM policies for secure, auditable access, reducing the risk of unauthorized access and ensuring a robust security posture.
* Collaborated with Risk Management and Security teams to deploy proactive security controls and monitor for potential identity-based threats in cloud environments.
* Worked with Muli-cloud environments and assisted in the setup and maintenance of Active Directory Federation Services (ADFS) to enable secure and seamless single sign-on (SSO) for enterprise applications.

Merck Jan 2024 – Dec 2024

New Jersey, USA

Role: Senior Cloud Engineer

Responsibilities:

* Designed and implemented Azure AD Conditional Access Policies to enforce adaptive security controls based on user location, device compliance, and sign-in risk, ensuring secure access across cloud and on-prem environments.
* Integrated Okta SSO and Ping Identity with SAML 2.0 for centralized authentication, enabling seamless Single Sign-On (SSO) across enterprise applications like Salesforce, Workday, and custom web apps.
* Configured Azure AD and Okta as SAML Service Providers (SP), providing secure federated authentication and role-based access across cloud platforms, including Google Cloud and Azure.
* Leveraged Okta Adaptive Authentication and Ping Identity to apply dynamic access controls based on user risk factors, enforcing multi-factor authentication (MFA) in high-risk situations.
* Automated identity lifecycle management in Okta and Azure AD, including user provisioning, de-provisioning, and role assignments to ensure compliance with governance standards and reduce manual errors.
* Enforced least privilege access using Azure RBAC, Google Cloud IAM, and Okta’s Identity Governance to protect sensitive resources and consistently review user access.
* Implemented role-based governance models and access reviews in Okta and Azure AD to maintain regulatory compliance (SOC 2, PCI-DSS, GDPR) through automated audit processes and periodic access reviews.
* Integrated PingFederate with Azure AD to enable federated SSO and secure access to applications across a hybrid cloud environment, improving user experience while maintaining strong access control.
* Conducted regular IAM audits and access logging using Okta System Logs, Azure AD Audit Logs, and Cloud Logging to identify and remediate unauthorized access or policy violations.
* Collaborated with Risk Management and Security teams to implement Zero Trust Architecture using MFA, conditional access, and adaptive authentication policies across all cloud and on-prem applications to enhance security posture.
* Integrated Azure IAM with CI/CD pipelines to automate the provisioning and de-provisioning of users and access permissions based on DevOps processes.
* Implemented by granting users temporary, time-limited access to resources based on predefined policies, ensuring access is only provided when needed and automatically revoked after the task is completed.

Thyrocare June 2020 – March 2023

Bangalore, India

Role: Senior IAM Engineer

Responsibilities:

* Configured and managed Azure RBAC and GCP IAM roles for fine-grained access control at resource, project, and subscription levels.
* Integrated Azure AD and Google Identity with third-party IdPs (Okta, Ping) for SSO and centralized identity management.
* Defined Azure AD Conditional Access policies for adaptive security based on user context and risk levels.
* Implemented Azure Activity Logs and GCP Cloud Audit Logs to monitor and review IAM activities for security and compliance.
* Managed Azure Managed Identities and GCP Service Accounts for secure, credential-free resource access.
* Applied least privilege access controls using Azure AD PIM and GCP IAM roles to minimize exposure of sensitive resources.
* Enforced resource governance with Azure Policy and GCP Organization Policies to ensure compliance with standards.
* Configured identity federation between Azure AD and GCP for seamless multi-cloud access management.
* Enabled MFA in Azure AD and GCP to enhance security for user and admin access.
* Automated user and service account lifecycle management (provisioning, de-provisioning) in both Azure and GCP environments.

QueLabs Technologies Pvt Ltd May 2018 – April 2020

Hyderabad, India

Role: Cloud IAM Engineer

Responsibilities:

* Managed user accounts and permissions for a simple application using Active Directory (AD) or a cloud-based IAM solution like Azure AD or Okta.
* Implemented role-based access control (RBAC) to ensure appropriate user permissions based on roles and responsibilities.
* Performed user provisioning and de-provisioning, ensuring new hires have timely access and offboarded users are promptly removed from the system.
* Configured Single Sign-On (SSO) for seamless user authentication across the application, improving user convenience and reducing login issues.
* Integrated multi-factor authentication (MFA) to enhance security for critical application access.
* Ensured compliance with basic security standards and assisted in user authentication setup for application-specific security requirements.
* Architected and deployed RBAC and IAM policies for multi-tier applications migrating to Google Cloud, utilizing Okta, Azure AD, and Ping Identity.
* Integrated Okta SSO with Google Cloud to enable identity federation and centralized access management across cloud services.
* Implemented Azure AD B2B and B2C for secure cross-organization collaboration and external access management.
* Configured Ping Identity for SSO and MFA, ensuring secure application access across multi-cloud environments.
* Led identity federation efforts using OAuth 2.0, OpenID Connect, and SAML 2.0 for secure identity management between cloud platforms.
* Defined and managed granular Google Cloud IAM roles and Azure RBAC policies based on least privilege access principles.
* Automated IAM policy enforcement and compliance checks using Terraform and Azure ARM Templates.
* Conducted IAM audits to ensure compliance with regulatory standards.
* Partnered with Risk Management teams to implement conditional access policies and monitor identity threats using Azure AD Identity Protection.
* Troubleshoot IAM-related issues across multi-cloud environments using Audit Logs, Okta System Logs, and Cloud Logging.
* Worked with third-party vendors to integrate external identity providers into cloud environments using Okta Identity Cloud and PingFederate.
* Developed and deployed Zero Trust access policies, leveraging MFA and adaptive authentication in Okta and Ping Identity.

 Confluxsys

 May 2016 – April 2018

 Pune, India

 Role: IAM admin

 Responsibilities:

* Supported the setup and configuration of user self-service portals, enabling users to reset passwords, update profiles, and manage their access permissions.
* Troubleshoot issues with self-service tools, ensuring users could manage their account settings with minimal support independently.
* Identified areas for process improvement in IAM workflows and suggested automation solutions to streamline user provisioning and access management.
* Assisted in automating user access requests and approvals to improve efficiency and reduce the risk of manual errors.
* Helped implement and maintain scripts or tools for bulk user updates, provisioning, and de-provisioning tasks.
* Performed routine IAM tasks, such as adding/removing users, resetting passwords, and updating roles and permissions.
* Setting up MFA using emails and MFA using Phone.
* Documented user access procedures, access levels, and any custom workflows for internal use and training.
* Investigate the root cause of IAM incidents, such as authentication failures or unauthorized privilege escalations, to prevent recurrence.
* Detect and respond to **IAM security incidents**, such as unauthorized access attempts, account compromises, and policy violations.
* Implement incident containment measures, such as disabling compromised accounts, resetting credentials, or applying additional security controls (e.g., MFA).
* Conduct post-incident reviews to analyze incident handling effectiveness, document findings, and update IAM policies or procedures to prevent future incidents.