SASIDHAR GUNTURU

LinkedIn

sasigunturu8@gmail.com ❖ (512) 998-4568 ❖ Dallas, TX❖

TECHNICAL SKILLS

- **Languages** : Python, Bash, PowerShell
- **Databases & OS** : SQL, SPL, MySQL, RDBMS, NoSQL, Windows, MAC OS, Linux
- **Cloud & Infrastructure** : Azure, AWS, GitOps
- **Data Visualization** : Power BI, Excel
- **Tools & Softwares** : Splunk, Juniper MIST, Armis, Nagios, Zabbix, Pager Duty, Grafana, Verkada, IGEL UMS, ServiceNow, MS Admin 365, ADUC
- **Developer & AI Tools** : Cursor, Anti-Gravity, VS Code, Claude Code, GitHub Copilot

EXPERIENCE

University of Texas **Jun. 2023 - Present**

IT Specialist *(Sept. 2024 – Present)* ***Arlington, TX***

- Managed enterprise monitoring and alerting using **Splunk** and **Zabbix**, enabling proactive incident detection and improved system health visibility across distributed production environments supporting 1000+ **Azure** and **AWS** servers.
- Configured custom Zabbix triggers, alerts, and thresholds, significantly reducing **Mean Time to Resolution (MTTR)** by implementing automated PagerDuty Escalation and enhancing real-time performance monitoring.
- Administered **PagerDuty** for incident management, improving response times, escalation efficiency, and cross-team coordination during critical outages.
- Integrated **Zabbix**, **PagerDuty** and **ServiceNow** to automate incident creation and escalation for high-severity alerts, minimizing manual intervention and accelerating resolution.
- Implemented MS Teams integrations and Zabbix webhooks to deliver real-time incident notifications, detailed trigger data, and collaboration updates to operations teams.
- Utilized **Juniper Mist AI-driven analytics** to proactively identify and resolve wireless and network performance issues, improving end-user connectivity experience and reducing network-related incidents
- Developed real-time operational dashboards using **Zabbix APIs**, **Webhooks**, and **Grafana**, improving situational awareness through live system health displays and business-level visualizations.
- Leveraged **Grafana** templating and dynamic dashboards to empower technical teams with customizable monitoring views and deeper metric analysis.
- Managed endpoint infrastructure using **IGEL UMS**, ensuring secure, scalable remote device management and compliance with organizational policies.
- Configured and managed **Azure Monitor** alerts and custom alert rules using metrics and Log Analytics queries to proactively detect performance degradation and service outages across Azure VMs, applications, and cloud services.
- Integrated Azure alerts with incident management workflows and leveraged **Azure Log Analytics** for detailed log analysis and root cause investigations, reducing impact from infrastructure and application issues.
- Oversaw security monitoring systems **(Verkada)**, integrating surveillance visibility into centralized IT operations dashboards to support overall system integrity.
- Leveraged **Mist's Marvis Virtual Network Assistant** to perform root cause analysis on client connectivity failures, accelerating troubleshooting time and reducing **Mean Time to Detect (MTTD)**
- Handled **Post-Incident reviews (PIRs)** and **Root Cause Analyses (RCA)**, documenting known errors and preventive actions that reduced recurring incidents and improved long-term service stability.
- Utilized **Armis** to achieve comprehensive visibility of managed, unmanaged, and IoT devices across the network, strengthening asset inventory accuracy and reducing unknown device risk.

- Utilized **Microsoft Defender for Azure** to monitor cloud workloads, virtual machines, and services for security misconfigurations, vulnerabilities, and suspicious activity.
- Utilized **Tanium** for real-time endpoint visibility across servers and user devices, enabling rapid identification of performance issues, missing patches, and security risks.
- Applied **ITIL** best practices across **Incident, Problem, and Change Management**, including **CAB** facilitation, risk assessment, root cause analysis, and post-implementation reviews to improve service stability and reduce recurring incidents.

IT Analyst *(Jun. 2023 – Sept. 2024)*

- Managed **Microsoft 365** and identity-related user administration, supporting secure access, license management, and account lifecycle operations in enterprise environments.
- Provided **L1/L2 operational support** for infrastructure, network, and application-related incidents, ensuring minimal service disruption and adherence to **SLA targets**.
- Utilized structured troubleshooting and root cause analysis to resolve system, network, and application issues, improving service reliability and reducing repeat incidents.
- Monitored, prioritized, and escalated incidents in ServiceNow based on severity and business impact, contributing to improved **Mean Time to Resolution (MTTR)**.
- Supported remote infrastructure and endpoint environments using remote management tools to diagnose connectivity, system performance, and application access issues.
- Collaborated with network, systems, security, and application teams to support deployments, test releases, and resolve cross-domain production issues.
- Automated operational tasks and notifications using **Microsoft Power Automate**, improving workflow efficiency and reducing manual intervention in support processes.
- Analyzed incident trends and service performance metrics using **ServiceNow**, **Excel**, and **Power BI** reporting, supporting data-driven improvements to operational reliability.
- Developed and maintained technical documentation, knowledge base articles, and runbooks, while mentoring junior team members to strengthen operational readiness and incident response consistency.
- Designed and maintained ServiceNow dashboards and reports to provide real-time visibility into incident volume, severity trends, and resolution performance.

Tata Consultancy Services **Jun. 2018 – Jul. 2021**
Assistant System Engineer ***Mumbai, India***

- Managed highly available production environments across **AWS** and **Azure**, maintaining 95% uptime for mission-critical applications.
- Implemented proactive monitoring and alerting using **Nagios**, **Prometheus**, and **Grafana** improving incident detection and reducing response times.
- Centralized logging and operational analytics through **Splunk** accelerating root cause analysis and performance troubleshooting.
- Designed and managed secure cloud and data center networking using **Azure VNets** including subnets, route tables, NSGs, and security groups.
- Established hybrid connectivity via **IPSec VPNs**, **Azure VPN Gateway** ensuring secure and low-latency communication between on-prem and cloud.
- Configured and troubleshot **TCP/IP networking, BGP, OSPF, VLANs**, and **VXLAN**, resolving latency, packet loss, and routing issues across multi-site environments.

EDUCATION

The University of Texas at Arlington **May. 2023**
Masters in Computer and Information Sciences ***Arlington, TX***