

Splunk Engineer Splunk Engineer Splunk Engineer - State Farm Insurance Co Phoenix, AZ

Around 5+ years of experience in the IT industry with years of expertise in Splunk, Linux/UNIX, PLSQL, SQL DBA. Monitoring, Data Analytics performance tuning Troubleshooting and Maintenance of Data Base. Around 4 years of experience as Splunk Developer performed activities including requirement analysis, design, and implementations of various client server based applications using Splunk Experience on Splunk Enterprise Deployments and enabled continuous integration on as part of configuration (props.conf, Transform.conf, Output.conf) management. Experience with Splunk Searching and Reporting modules, Knowledge Objects, Administration, Add-On's, Dashboards, Clustering and Forwarder Management. Created and Managed Splunk DB connect Identities, Database Connections, Database Inputs, Outputs, lookups, access controls. Expertise Splunk query language and Monitored Database Connection Health by using Splunk DB connect health dashboards. Hands on experience in understanding of splunk, its various components and integrations with other systems like Service Now, rsyslog server etc. Experience with Splunk technical implementation, planning, customization, integration with big data and statistical and analytical modeling. Monitored Database Connection Health by using Splunk DB connects health dashboards. Helping application teams in Log on-boarding Splunk and creating Dashboard, Alert, and Reports etc. Worked on log parsing, complex Splunk searches, including external table lookups. Time chart attributes such as Span, Bins, Tag, Event types, Creating Dashboards, Reports using XML. Create Dashboard from search, Scheduled searches of Inline search vs. scheduled search in a Dashboard. Scripting and development skills (Perl, Python,) with strong knowledge of regular expressions Experience in using Rsyslog (v.7) in UNIX computer systems for forwarding log messages in an ipnetwork, write it to a file or database or forward it to a remote host. Having hands-on experience in managing the rsyslog server by creating configuration files to define the filters, destinations to ingest data / logs from the various networking and infrastructure devices. Extensive experience in integrating rsyslog server with splunk to consume and parse the data and then used splunk to search the logs Experience in writing Evidentio signatures JSon and Ruby, building a security dashboards. Extensive experience in Log

monitoring and log on boarding process during data indexing and Splunk data flow, components, features and product capability. Experience on Splunk search construction with ability to create well-structured search queries that minimize performance impact. Installed Splunk DB Connect 2.0 in Single and distributed server environments and Parsing, Indexing, Searching concepts Hot, Warm, Cold, Frozen bucketing. Expertise in using Splunk with shell script in creating scripts for various activities like Generating Server Status and Health reports, Deployments on large scale configuration of servers. Designed and implemented the application based load balancing, clustering and mirroring. Experienced in Performance Monitoring, Security, Troubleshooting, and Backup, Disaster recovery, Maintenance and Support in accordance with established policies, procedures and service level agreements. Exposure to couple of ticketing systems like Remedy, Clarify. Experience in Performance monitoring, usage and load of the system, changing kernel parameters for better performance, creating new Slices with format and creating huge Slices with Daisy Chains. Proficient in System Backup and Recovery from tapes using ufsdump, ufsrestore, tar and cpio. Performance Monitoring & Tuning - iostat , vmstat & netstat, nfsstat. Experienced in remote network installations like KickStart & Jumpstart. Hands on experience on Version one and JIRA. Excellent client relation skills and the ability to communicate effectively with all levels of management and the client community. Great communication skills, wonderful team leader and awesome team player. Sponsorship required to work in the US Work Experience Splunk Engineer State Farm Insurance Co - Tempe, AZ January 2016 to Present Responsibilities Expertise in Installation, Configuration, Migration, Trouble-Shooting and Maintaining Splunk. Configured Splunk Searching and Reporting modules, Knowledge Objects, Administration, Add-On's, Dashboards, Clustering and Forwarder Management. Installation and configuration of Splunk product at different environments. Installation of SplunkEnterprise, Splunk forwarded, Splunk Indexer, Apps in multiple servers (Windows and Linux) with automation. Splunk technical implementation, planning, customization, integration with big data and statistical and analytical modeling. Performed Splunk administration tasks such as, Installing, configuring, monitoring and tuning. Installed and configured WebLogic 10 and integrated with Splunk for both development

and production environments. Deployed various WAR, JAR, EAR applications in clustered environment. Worked on log parsing, complex Splunk searches, including external table lookups. Experience in using rsyslog (v.7) in UNIX computer systems for forwarding log messages in an ipnetwork, write it to a file or database or forward it to a remote host. Having hands-on experience in managing the rsyslog server by creating configuration files to define the filters, destinations to ingest data / logs from the various networking and infrastructure devices. Extensive experience in integrating rsyslog server with splunk to consume and parse the data and then used splunk to search the logs. Experience in using monitor text files and convert their contents into syslog messages. Most of the time worked to install Universal Forwarders and but we have Heavy Forwarders set up to see data from syslog server side. Configured and administered JDBC, JMS, JNDI, and SNMP on Web Logic Server 10mp1. Designing and maintaining production-quality Splunk dashboards. Splunk configuration that involves different web application and batch, create Saved search and summary search, summary indexes. Experience in writing Evidentio signatures JSon and Ruby, building a security dashboards. Experience in Log monitoring and log on-boarding process during data indexing. By using Splunk Mobile app view and analyze dash boards on Android and iOS Devices. Splunk DB Connect 2.0 in search head cluster environments of Oracle, MySql. Experience with Splunk UI/GUI development and operations roles. Deployed applications on multiple WebLogic Servers and maintained Load balancing, high availability and Fail over functionality. Install and maintain the Splunk add-on including the DB Connect 1, Active Directory LDAP for work with directory and SQL database. By using Data on boarding put assist in boarding new data. Installed and configured Splunk DB Connect in Single and distributed server environments. Worked on the Deployment Server for Deploying the basic configurations on to servers and deploying License. Monitored the database (data tables and error tables), WebLogic error log files and application error log files to track and fix bugs. Parsing, Indexing, Searching concepts Hot, Warm, Cold, Frozen bucketing. Configured WebLogic JMS Servers, JMS Modules, JDBC Data Sources, JDBC Connection Pools. Environment: Splunk 6.x, Splunk DB Connect and other modules, Oracle WebLogic 9.x/10.x, JBoss 5.x/6.x, Tomcat 5.x/6.x, Oracle 9i/10g, Solaris 10,

LINUX, Sun ONE Directory Server 6, SunOne Web Server 6.0, Apache 2.x, Jython, ANT, AWK, IIS, Netegrity SiteMinder Policy Server 5.5/6.0, LDAP, Windows 2003/XP, Oracle 9i Systems Administrator TEKbiz Soft Solutions - IN January 2012 to June 2014 Roles and Responsibilities:

Experience in installation, Configuration and Administration of Linux (RHEL 4/5, SLES 10) Solaris 8/9/10. Expertise in installing, configuring and maintaining Debian/RedHat Servers at multiple Data Centers. Configuration and administration of DNS, LDAP, NFS, NIS, NIS+ and Send mail on RedHat Linux and Debian Servers. Configured RedHat Kickstart server for installing multiple production servers. Hands on experience working with production servers at multiple data centers.

Automated server building using Kickstart and Jumpstart. Planning, documenting and supporting high availability, data replication, business persistence, and fail-over, fail-back using Veritas Cluster Server in Solaris, Redhat Cluster Server in Linux. Configured Global File System (GFS) and Zetta byte File System (ZFS). Configured yum repository server for installing packages from a centralized server. Installed and configured DHCP server to give IP leases to production servers.

Management of RedHat Linux user accounts, groups, directories and file permissions. Configured, managed ESX VM's with virtual center and VI client. Performance monitoring using Sar, iostat, VMstat and MPstat on servers. Performed Kernel tuning with the sysctl and installed packages with yum and rpm. Configuration and Administration of Apache Web Server and SSL. Backup management Recovery through Veritas Net Backup (VNB). Performed Disk management with the help of LVM (Logical Volume Manager). Established and maintained network users, user environment, directories, and security.

Monitoring the Web Sphere / Web Servers Logs file System. Installed SSL certificates for Web Server & Application Servers Troubleshooting Web Sphere issues. Configuring Web Sphere configuration details. Performance Tuning of Web Sphere application servers. Password-less setup and agent-forwarding done for SSH login using ssh-keygen tool. Documented strongly the steps involved for data migration on production servers and also testing procedures before the migration. Provided 24/7 on call support on Linux Production Servers. Responsible for maintaining security on RedHat Linux. Environment: RHEL 5.x/4.x , Solaris 8/9/10, Sun Fire, Websphere 5.x/6.x, Apache 1.2/1.3/2.x, iPlanet, Oracle 11g/10g/9i,

Logical Volume Manager, Veritas netbackup 5.x/6.0, SAN Multipathing (MPIO, HDLM, Powerpath), VM ESX 3.x/2.x. Education Master of Computer Science in Computer Science University of Central Missouri Bachelors of Computer Science in Computer Science JNT University Skills Linux (5 years), SNMP (2 years), Solaris (5 years), Splunk (4 years), Sun (5 years), Project Management, Customer Service, Java Additional Information TECHNICAL SKILLS      Operating Systems: Red Hat Linux 5.x, 6.x, IBM AIX 7.x, 6.x, 5.x, Fedora, SUSE, Debian, Ubuntu, CentOS, Sun Solaris 8/9/10, vSphere 4.0,5.0 Windows - NT/2000/2003/2007 Server/XP Pro/Vista/7/8      Volume Management Tools: Solaris Volume Manager, Veritas Volume Manager 4.0, 5.0, Logical Volume Manager, RAID, Veritas Cluster.      Splunk Modules: Splunk 5.x/6.x, Splunk Cloud, Splunk DB Connect, Splunk Enterprise, Splunk on Splunk, Splunk IT Service Intelligence, Splunk Web Framework.      Network Services: SMTP, SNMP, DHCP, POP, NIS, NIS+, NFS, DNS, FTP/TFTP, ARP/RARP, SSH, TCP/IP, NTP, TELNET      Virtual Server: VMware ESX 3.5.0 Server, VMware Infrastructure Client 2.5 & Xen 3.2      Monitoring Tools: Splunk, Hyperic, HPDiagnostics, Perceiver,Best1,Mulesoft Qlikview, Prometheus, and Grafana and OPNET.      Other tools: DNS(BIND), DHCP, Samba, FTP, NFS, NIS, KickStart, rsync, SAS ODBC, VERITAS Netbackup 5.1/6.5.3, RAID, SVN, CVS, TCP/IP, Webmin, Puppet, netstat, sar, ps, dig, strace, tcpdump, lsof, yum, rpm, ping, lookup, trace, tar and parted.

Name: Joseph Navarro

Email: ereid@example.org

Phone: 675-407-0358