

Splunk Engineer Splunk Engineer Splunk Engineer - EMC Corp Charlotte, NC Overall 8+ years of IT experience and as Splunk Engineer, SQL Server Developer and System Administrator on varied projects which involves Design and Development of client/server. In platform consisting of Red Hat Linux, Windows, and Sun Solaris operating systems. Experience in installing and using Splunk apps for UNIX and Linux (Splunk. Nix). Experience in Splunk development creating Apps, Dashboards, Data Models, etc. Monitor the splunk infrastructure for capacity planning, system health, availability and optimization. Used techniques to optimize searches for better performance, Search time vs Index time field extraction and understanding of configuration files, precedence and working props.conf, transforms.conf, inputs.conf, outputs.conf setting up a forwarder Monitor stanza in inputs.conf. Prepared, arranged and tested Splunk search strings and operational strings. Expert in install, configure and administer splunk Enterprise Server and splunk Universal Forwarder, splunk Heavy Forwarder in large distributed environment comprising Windows, Red hat, Solaris, AIX with exposure various splunk Apps to monitor splunk deployments Responsible for simulating network operations with usage of monitoring tools like Netcool & Wireshark thereby resolving tickets as per the issue. Experience working with server monitoring tools like BMC Patrol, Nagios Experience with Splunk Searching and Reporting modules, Knowledge Objects, Administration, Dashboards, Clustering and Forwarder Management. Created and Managed Splunk DB connect Identities, Database Connections, Database Inputs, Outputs, lookups, access controls. Extensive experience in Installation, Configuration, and Migration, Trouble-Shooting and Maintenance of Splunk, Apache Web Server on different UNIX flavors like Linux. Normalization of fields and defining the event types used CIM (Common Information Model). Created Reports, Alerts and Dashboards by Splunk query language. Experienced in creating and running Cron Jobs for scheduled tasks. Managed Indexer Clusters including security, hot and cold bucket management and retention policies. Parsing, Indexing, Searching concepts Hot, Warm, Cold, Frozen bucketing. Knowledge about Splunk architecture and various components (Indexer, forwarder, search head, deployment server). Designed and developed intranet web applications using JavaScript and CSS. Set indexing property configurations, including time zone offset, custom source type rules.

Configure Regex transformations to perform on data inputs. Helping application teams in on-boarding Splunk and creating Dashboard, Alert, and Reports etc. Experience on use and understand of complex Reg Ex (regular expressions). Scripting and development skills using Perl and Python with strong knowledge of regular expressions. Field Extraction, Using IFX, Rex Command and RegEx in configuration files. Knowledge of Extract keyword, Sed, Knowledge objects, Knowledge of various search commands like stats, chart, time chart, transaction, strptime, strftime, eval, where,xyseries, table etc. Experience on working with CIM in which it facilitates normalization of data from different sources, and enables applications developed by Splunk to search and display Deep Discovery logs. 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. Various types of charts alert settings Knowledge of App creation, user and role access permissions. Creating and Managing Apps, Create user, role and Permissions to Knowledge objects. Troubleshooting hardware, software and configuration problems for various protocols and topologies. Strong experience in System Administration, Installation, Upgrading, Patches, Migration. More than 3 years of experience as SQL Developer in Analysis, Database Design and Presentation using SQL Server. Expertise in SQL statements to extract data from data tables and verify the output data of the reports along with creation of tables, Sub queries, Joins, Views, Indexes, SQL Functions, Set Operators and other Functionalities. Strong in Data warehousing methodologies of Star /Snow Flake schemas. Proficient in using Business Intelligence Development Studio (BIDS) Graphical User Interface (GUI) to design SQL Server Integration services (SSIS) packages for Data Management applications. Experienced in Data Extraction, Transforming and Loading (ETL) between Homogenous and Heterogeneous Systems using SQL Server tools like SSIS, DTS, Bulk Insert, BCP and XML. Proficient in creating Indexes, Views, Table Variables, Complex Stored Procedures, User and System defined functions, triggers, packages using SQL, PL/SL. Experience in creating Drill through and Drill down reports using Crystal Reports and SQL Server Reporting Services (SSRS). Configured and maintained Report Manager and Report Server for

SSRS. Experienced in Various BI Tools like TIBCO Jasper soft, Tableau for designing customized interactive and advanced rich visualization dashboards using different connectors, extensions, marks, Action, filters, parameter, calculations and Relationships. About 6 months of experience as System Administrator. Planning intra forest migration to consolidate multiple child domains. Provide procedures, documents, customize accounts migration with pre/post task to minimize user's impact after migration. Configured and maintained all primary and back-up servers to include domain controllers (DC) within an Active Directory (AD) forest. Configured and maintained Group Policy Objects (GPO) on all domains. Provided 1st level support for Active Directory end users, applications and administration teams. Built Test Forest and three Domains to implement testing plans & guidelines for applications against AD. Team player with excellent communication, presentation and interpersonal skills. Highly motivated team player with zeal to learn new technologies. Authorized to work in the US for any employer

Work Experience

Splunk Engineer
EMC Corp - Charlotte, NC January 2017 to Present

Responsibilities:

- Design, support and maintain large Splunk environment in a highly available, redundant, dispersed environment
- Requirement gathering and analysis. Interacted with team members and users during the design and development of the applications and Splunk Objects.
- Installed Splunk on nix & Splunk SOS and maintained Splunk instance for monitoring the health of the clusters
- Created user roles in LDAP and integrated Splunk with active directory, LDAP authentication and also set up of certificate authentication (SSL).
- Optimized Splunk for peak performance by splitting Splunk indexing and search activities across different machines.
- By using AWS collect detailed billing data and in depth analysis of Amazon Web server.
- Worked on Amazon AWS, configuring, launching Linux and windows server instances for splunk deployment.
- Supporting and monitoring splunk cluster infrastructure in AWS cloud environment.
- Created a test environment of splunk clustered environment in AWS EC2 instances and S3 storage.
- Monitored and tracked Splunk performance problems, administrations and open tickets with Splunk.
- Developed customized Shell scripts in order to install, manage, configure multiple instances of splunk forwarders, indexers, search heads, deployment servers.
- Monitor the splunk Infrastructure (Identify bad searches, dashboards and

overall health of splunk) and collaborate with respective teams to improve performance. Created and customized Splunk applications, searches and dashboards as desired by IT teams and business. Monitored Database Connection Health by using Splunk DB Connect v 2.0, health dashboards, JBoss, Apache Tomcat. Developed Application Health Monitoring scripts using Shell and Perl for Tomcat Clustered & Non-Clustered environments. Experience with customizing the dashboards such as CSS stylesheets and Java script files by using simple XML extensions. Expert in Splunk processing language (SPL) to design/develop and visualize log data. Configured and maintained hot, warm, and cold buckets depending upon the data retention requirements. Hands on development experience in customizing Splunk dashboards, visualizations, configurations, reports and search capabilities using customized Splunk queries. Configured Clusters, Server groups and Cloning for improved availability and failover capacity. Excellent skills on troubleshooting and problem determination of HTTP/System/ Network related problems including monitoring, capacity planning and maintenance by providing 24X7 support on call for all mission critical applications. Responsible for documenting the current architectural configurations and detailed data flow and troubleshooting guides for application support. Knowledge about Splunk architecture and various components (indexer, forwarder, search head, deployment server), Heavy and Universal forwarder, License model. Provide regular support guidance to Splunk project teams on complex solution and issue resolution. Splunk administering in environments like UNIX, Window Servers and Red Hat Linux Enterprise Servers. Strong experience in System Administration, Installation, Upgrading, Patches, Migration. Environment: SPLUNK 6.5,6.3,DB connect, Hunk, Apache 2.x, PERL ,Tomcat 6.0/5.x , Oracle 9i/10g,Linux, Windows, Python, Bash, UNIX,HDFS. Splunk Admin Kaiser Permanente - Silver Spring, MD September 2016 to January 2017 Responsibilities: Expertise with Splunk UI/GUI development and operations roles. Installation of Splunk Enterprise, Splunk forwarders, Splunk Indexer, Apps in multiple servers (Windows, Linux & Unix) with automation. Experience with deployment server to manage forwarder deployment Administrated to ensure the active and accurate running of splunk and monitoring on the current infrastructure implementation. Install and maintain the Splunk add-on

including the DB Connect, Active Directory LDAP for work with directory and SQL database. Played a major role in understanding the logs, server data and brought insight of the data for the users. Provided architecture validation testing, troubleshooting on issues such as Out of Memory, 100% CPU Usage hung Thread sessions, session replication, JVM Crashes. Created Dashboards to web application to show user flow for End to End Architecture and also to detect the Workflow for particular user session. Established indexes and retention policy of buckets; developed user roles to complement operational and Security utilization. Implemented Google map identifiers in Splunk dashboards using geo lookup commands. Implemented prediction in application events using Splunk Algorithms. Good knowledge in building Splunk Apps for custom application requirement. Installed and configured Splunk Hadoop Connect and Data Base connect Application.. Used Datameer to analyze the transaction data for the client. Installed, configured and managed Datameer users on the Hadoop cluster. Created Splunk Dashboards to capture the Authentication breaches across application and to track the Application usage in peak times. Created HTML dashboards with java scripts and CSS to create customized visualizations. Installed and configured DB Connect plug in to get the data from Oracle, MySQL and MSSQL. Worked on repository to create and manage user profiles. Created EVAL Functions where necessary to create new field during search run time. Configured Splunk Searching and Reporting modules, Knowledge Objects, Administration, Regex, Dashboards, Clustering and Forwarder Management. Provided technical services to projects, user requests and data queries. Responsible for Scheduling and Automating Database tasks - Jobs, Alerts, Emails, Notification. Involved in writing complex IFX, rex and Multikv commands to extract the fields from the log files. Worked on the Windows Servers and RHEL Linux OS deployments. Worked on VM creation, templates, clones and snapshots. Monitor and track Splunk performance problems and open tickets (Used Jira) with Splunk if there is need. Involved in installing and using Splunk app for windows. Environment: Splunk 6.1, 5.0, Windows, Bash. Hadoop, Datameer, power shell, DB connect, Linux, UNIX. SQL server Developer Target - Minneapolis, MN June 2015 to September 2016 Responsibilities: Gathered business requirements, definition and design of the data sourcing and data flows, data

quality analysis, working in conjunction with the data warehouse architect on the development of logical data models. Develop reporting standards and protocols within the Claim payment department. Involved in complete life cycle of SSRS (Authoring, Managing and Delivery reports) SQL, PL/SQL and T-SQL to create stored procedures create and alter tables and databases. Worked as a developer in creating complex T-SQL, Stored Procedures, triggers, cursors, tables, and views and other SQL joins and statements for applications. Created Cross-Tab, Drill-down, Drill-through and Sub-Report using RDL. Promoted RDLs to Reporting Service Server. Wrote the queries for the drill down reports. Complex SSIS package for data transfer from three different sources to a single destination like SQL Server 2008 was designed. Extensively used the advanced features of PL/SQL like Records, Tables, Dynamic and SQL Objects types. Designed and implemented complex SSIS package to migrate data from multiple data sources for data analyzing, deploying and dynamic configuring of SSIS packages. Designed ETL architecture for overall data transfer from the OLTP to OLAP with the help of SSIS. Developed complex data Mappings to extract Provider data from XML Files and SQL Server and load to SQL server target data warehouse. Run hourly and daily queue reports to ensure claims do not exceed turnaround times. Create VB based form ETL interface as a tool for date range input and filter data extraction from Oracle data warehouse into data mart. Defined parameters for parameterized Reports using SSRS. Designed, Developed and Deployed reports in MS SQL environment using SSRS 2008. Consult with cross-departmental staff in defining claim payment reporting need. Expertise in developing T-SQL (DDL, DML) statements, Data Integrity (constraints), Performance Tuning, and Query Optimization. Environment: Microsoft SQL Server 2012, MSSQL Server Reporting Services 2012, MSSQL Server Integration Services 2012, Bash, DTS, SQL Profiler, MS Office. SQL Database Administrator Globalsign.in - Hyderabad, Telangana June 2013 to June 2015 Responsibilities: Creating and managing of databases, Performance monitoring, troubleshooting, enhancing high availability and disaster recovery solutions. Tested and configured automated routine maintenance tasks like performance tuning, indexes and stores procedures, checked deadlocks and created scheduled jobs. Created and managed schema objects such as tables, views, stored procedures,

and triggers and maintained Referential Integrity. Created new database objects like Procedures, Functions, Packages, Triggers, Indexes and Views using T-SQL in Development and Production environment for SQL Server. Developed Database Triggers to enforce Data integrity and additional Referential Integrity. Developed SQL Queries to fetch complex data from different tables in remote databases using joins, database links and formatted the results into reports and kept logs.

Used SQL Profiler and Query Analyzer to optimize DTS package queries and stored procedures. Involved in performance tuning and monitoring of T-SQL. Involved in data migration and data integration. Prepared test reports and bug logs for the testing done and reporting the status to Sr. Management. Served as developer for the solutions designed by other team members.

Environment: SQL server 2005, Oracle 9i Server, SQL Plus, PL/SQL, Query Analyzer, SQL Profiler, DTS, Import/Export tools, SQL Server Agent, SQL Server Enterprise Manager, SQL Jobs, VB Script, ODBC, Database Engine Tuning Advisor, Windows 2005 Server. System Administrator Bengaluru, Karnataka August 2011 to February 2013 Responsibilities: System Administrator in Windows with experience in managing information technology specializing in systems Administration including Windows Active Directory, End-user Services, and Server Operations. AD Team Change Coordinator - create, review and plan changes affecting AD Externally and internally using ITSM Service Now. Review technical aspects of changes ensuring they meet Policy requirements and avoid scheduling, Conflicts. Provide 1st level support for Active Directory end users, applications and administration. Built Test Forest and three Domains to implement testing plans and guidelines for applications to test against AD. Verified daily back-ups of servers. Help Desk-assisted clients with computer problems (hardware and software issues), installation of hardware and software, updates, etc. Setup of new clients in network and management of client accounts using Active Directory. Installation of new computers and building of computer for machines. Microsoft Windows XP and 7 installations and troubleshooting. Environment: Active Directory, Domain Controller, DNS, TCP, DHCP, Windows 2008/2008R2. Education Jawaharlal Nehru Technological University May 2009 Skills DB2, MS ACCESS, SQL SERVER, SQL SERVER 2000, MYSQL, OLTP, ORACLE, ORACLE FORMS, PL/SQL, SQL, SYBASE, JMS, NOSQL, OLAP, SPLUNK, STAR

SCHEMA, ACTIVE DIRECTORY, C++, HTML, PERL

Name: Benjamin Moore

Email: qwillis@example.net

Phone: 487.586.3258x5365