# MANOJ | Sr. SIEM/ Splunk Enterprise consultant

# MANOJ REDDY

# Sr. SIEM/ Splunk Developer/Admin

# Ph: +1(551)236-3989

# Email: [manojreddy.0308@gmail.com](mailto:manojreddy.0308@gmail.com)

**PROFESSIONALSUMMARY:**

* **9+ years** of extensive experience in **Splunk**, **Linux/UNIX**, **PLSQL**, **SQL DBA**. Monitoring, Data Analytics, Performance Tuning, Troubleshooting and Maintenance of Data Base.
* Experienced in creating **Reports**, **Alerts**, and **Dashboards** by Splunk **Search Processing Language (SPL),** creating and running Cron Jobs for scheduled tasks.
* Used **Splunk forwarders** to provide reliable and secure collection and delivery of data to the Splunk platform for indexing, storage, and analysis.
* Extensive experience in deploying, configuring, and administering **Splunk Clusters**.
* Created and Managed **Splunk DBConnect** Identities, Database Connections, Database Inputs, Outputs, lookups, access controls.
* Develop custom app configurations (deployment-apps) within Splunk to parse, index multiple types of log format across all application environments.
* Developed and innovated custom Splunk measurement applications, varying engineering models and proactive performance reports to assist senior management in making business critical decisions.
* Experienced in preparing, arranging, and testing Splunk search strings and operational strings.
* Supporting and monitoring Splunk cluster infra structure in **AWS cloud** environment.
* Ingesting and working with various data types like CSV, JSON, XML, Raw Logs, Syslog and parsing them with custom sourcetypes.
* Involved in writing complex **IFX**, **Rex** and **Multikv** command to extracts the fields from the log files.
* Writing PL/SQL stored procedures, functions, triggers to meet new features to be incorporated in the system to implements business rules.
* Experience in creation of **Tableau** Data Extracts with high performance.
* Experience in configuration of report server and report manager scheduling, give permissions to different level of users in **SQL Server Reporting Services (SSRS).**
* Designed, Developed and Deployed **UNIX shell scripts** and **Linux Scripts.**
* Experience in writing **UNIX Shell scripts** for various purposes like file validation, automation of **ETL** process.
* Expertise in all the phases of **SDLC** using different methodologies like **Agile, Waterfall**.
* Extensive knowledge of **BI** and **Data Warehousing concepts**, **Dimensional Models**.
* Proficient in using **SQL Server Integration Services (SSIS)** to build Data Integration and Workflow Solutions, Extract, Transform and Load (ETL) solutions for Data warehousing applications.
* Conducted database management, performance measurement and performance tuning for new databases and existing databases by using **SQL Profiler** and **SQL Analyzer**.
* Expertise with scheduling and monitoring jobs using SQL Server Agent to perform hourly/daily/monthly data loads.
* Sound knowledge of relational & dimensional modeling techniques of data warehouse concepts, the **Star** &**Snowflake** schemas, **SCD**, **OLAP, OLTP**, Normalization /Denormalization.
* Experience in creating **Unit Test cases** and development of testing methods and test logs, which are used for QA team and validate loaded data to ensure data quality.
* Self-motivated and possess ability for critical thinking, analysis, good interpersonal and communication skills. Team-oriented, technically motivated, and creative.
* Strong analytical and technical skills. Good aptitude for problem solving, troubleshooting and assimilation of new technologies.

**TECHNICALEXPERTISE:**

|  |  |
| --- | --- |
| **Monitoring Tools** | SPLUNK 6.0, SPLUNK 6.2, SPLUNK 6.3, SPLUNK 6.4, SPLUNK 6.5, **AppDynamics.** |
| **Data** **Warehousing** | SQL Server Management Studio (SSMS), Enterprise Manager, Query Analyzer, SQL Profiler, SSIS, SSAS, SSRS. |
| **Data Analysis** | Business Rules, Data modeling, Data Warehousing, system integration. |
| **Data Modeling** | Star Schema, Snow-Flake, FACT-Dimensions, Conceptual Physical and Logical Data Modeling, ER models, OLAP, OLTP concepts. |
| **Databases** | Microsoft SQL Server, Oracle Database, IBM DB2 and MySQL. |
| **Programming** | SPL, SQL, SQL Plus, Unix Shell Scripting,PowerShell, Perl, Bash,HTML, CSS,XML, C, Java, and Python. |
| **Operating systems** | Windows, Linux, Unix. |

**PROFESSIONALEXPERIENCE:**

**Progressive Corporation, Mayfield, Ohio. April 2016- Present**

# Sr. SIEM/ Splunk Developer/Administrator

Progressive is one of the largest auto insurers in the United States, with over 13 million policies in force, along with State Farm, Allstate, GEICO, Nationwide Mutual Insurance Company, Farmers Insurance Group, and USAA. The company also insures motorcycles, boats, RVs, and commercial vehicles, and provides home insurance through select companies. The data from the various branches was clustered on a Splunk platform to perform analysis and develop reports and strategies for business intelligence teams.

**Responsibilities:**

* Installed, Configured and Administrated **Splunk Enterprise** and **Splunk Forwarders** on **Windows** Servers and **Linux** Servers.
* Involved in standardizing Splunk forwarder deployment, configuration and maintenance across UNIX and Windows platforms.
* Developed Splunk **Search Processing Language (SPL)** queries, created **Reports**, **Alerts** and **Dashboards** and customized them. Implemented Dynamic **Drilldowns** that provide greater flexibility to the end user.

**Field Extraction:** Using **IFX, RexCommand** and **REGEX** in configuration files, knowledge of **EXTRACT** keyword.

* Created various search commands like Chart, Time Chart, Strptime, Strftime, Eval, Table etc.
* Created field aliases across application events and time modifier conversion commands.
* Installed Splunk apps like Splunk on Splunk, Splunk app for WebLogic Server, Splunk app for REST API, Splunk app for Unix, Splunk app for JMX, splunk app for DB Connect, Splunk app for Microsoft cloud services, Common Information Model(CIM) etc.,
* Setup **SSL certificates** in various Splunk servers (Indexers, Search Heads and Management Servers).
* Worked on installing **Splunk UF** and **Heavy Forwarders** to bring any kind of feeds from different application servers into Splunk.
* Provide Regular support guidance to Splunk project teams on complex solution and issue resolution.
* Work closely with Application Teams to create new Splunk dashboards for Operation teams.
* Integrated the logs of Network Devices, Switches and Routers using the Network protocols like **UDP/TCP**.
* Good experience in working with SNMP traps and Syslog NG in onboarding the security devices on Splunk.
* Integrated and configured logs from different data sources like Windows, Linux/AIX, Application, Security, Network Devices, and servers.
* Worked with Splunk app for **Enterprise Security** to identify and address emerging security threats using continuous monitoring, alerting and analytics.
* Installed, configured, and manage **Splunk Enterprise Security**.
* Architecting and Deploying Splunk and coordinating Enterprise Security with Splunk
* Monitored security posture and security incidents regarding that trending outside and inside threat vectors.
* Consolidating analysis of suspicious Splunk data security event logs (Windows Defender, AppLocker, and Audit Events).
* Worked as part of Cyber Security Incident Response team to check on malware virus and threat emails.
* Assist to recommending security resolutions to management for better malware detection and endpoint security.
* Created **Shell Scripts** to install Splunk Forwarders on all servers and configure with common configuration files such as Bootstrap scripts, Outputs.conf and Inputs.conf files.
* Worked with administrators to ensure Splunk is actively and accurately running and monitoring on the current infrastructure implementation.
* Conducted and automated Splunk configuration files such as Props.conf, transforms.conf.

**Environment: Splunk Enterprise, Splunk 6.2.x, 6.3, 6.5 Universal Splunk forwarder, Splunk Db connect, Oracle, MS SQL 2008, Regular expressions, Windows, UNIX, UNIX shell scripting, XML, Microsoft Active Directory, Splunk App for Enterprise Security (SIEM).**

**ZeniMax Media,Rockville, Maryland. Oct 2014 - March 2016**

# Splunk Developer/Administrator

ZeniMax Media is a video game publisher, managed by an experienced group of executives, which has assembled a strong creative team of world-class game developers, graphic artists and designers, sound engineers, producers, and programmers to create and sell premium video game titles to a growing worldwide market. Project was to design, deploy and integrate Splunk Enterprise with the existing system infrastructure and setup configuration parameters for Logging, Monitoring and Alerting.

**Responsibilities:**

* Created Splunk **Search Processing Language (SPL)** queries, Reports, Alerts, and Dashboards.
* Troubleshooting and resolve the Splunk - performance, search poling, log monitoring issues; role mapping, dashboard creation etc.
* Established indexes and retention policy of buckets; developed user roles to complement operational and security utilization. Set-up common source types using pre-trained datasets and constructed sourcetypes of unique data.
* Created **Regular Expressions** for Field Extractions and Field Transformations in Splunk.
* Assisted internal users of Splunk in designing & maintaining production-quality dashboard, assisted offshore team to understand the use case of business and provided technical services to projects, user requests & data queries
* Installed and configured different **Splunk apps** and **add-ons** on Splunk platform.
* Scripted SQL Queries in accordance with the Splunk.
* Splunk technical implementation, planning, customization, integration with big data.
* Knowledge about Splunk architecture and various components (indexer, forwarder, search head, deployment server), Heavy and Universal forwarder, License model.
* Splunk configuration that involves different web application and batch, create Saved search and summary search, summary indexes.
* Worked on log parsing, complex Splunk searches, including external table lookups.
* Use techniques to optimize searches for better performance, Search time vs Index time field extraction. And understanding of configuration files, precedence and working.
* Responsible for administering, maintaining, and configuring a 24 x 7 highly available, Splunk apps for production portal environment.
* Worked on configuration files inputs.conf, indexes.conf, props.conf, serverclass.conf, transforms.conf and limit.conf.
* Upgrading and Migrating the Splunk Components and setting up the Retention Policy for the indexes.
* Configuring **LDAP** and Single Sign-On for User Authentication in the organization.
* Configured Splunk for all the mission critical applications and using Splunk effectively for Application troubleshooting and monitoring post go lives.
* Worked Directly with Splunk Inc sales team in determining Log size and licensing cost for the client's Infrastructure.
* Parsed, Indexed, Searched concepts **Hot, Warm, Cold, Frozen** bucketing.
* Supported **HTTP** methods following the **REST API** subsets including the **CURD** operations like the **GET, POST,** and **DELETE** to return a HTTP status code to indicate the success of the operation or cause of a failure to fulfill the request.
* Used**c URL** and **REST** client browser plugins to exercise the API by using the curl command.

**Environment: Splunk 6.3, Splunk 6.2, Unix, Linux, SQL server, XML, Web Services, Splunk DB connect 2.2, Unix, Oracle 11g, Service Now, MS SQL Server 2012, SQL server, Python Scripting.**

**Prudential Financial, Newark, NJ. Mar 2013 - Sep 2014**

# SQL BI Developer/ Splunk Developer

Prudential Financial, Inc. has operations in the United States, Asia, Europe, and Latin America. Prudential’s diverse and talented employees are committed to helping individual and institutional customers grow and protect their wealth through a variety of products and services, including life insurance, annuities, retirement-related services, mutual funds, and investment management.

**Responsibilities:**

* Created **SSIS** packages to load robust data from heterogeneous data sources like **Oracle**, **DB2**, **Flatfiles** to SQL server.
* Used various SSIS transformations such as conditional split, data conversion task, derived column, Multicast, Merge join and look up that are used for data cleansing and validation before loading data into new tables.
* Configured and deployed SSIS packages from test to production environments.
* Scheduled jobs to run on daily and weekly basis using SQL Server Agent.
* Generated reports using **SSRS** that were used to send information to different vendors, clients, and mangers.
* Added subscription and Snapshot options to deliver the reports to end users.
* Created **ETL** packages using Heterogeneous data sources (DB2, ORACLE and Flat Files etc.) and then loaded the data into destination tables by performing different kinds of transformations using SSIS.
* Used SSIS package to load data from different platforms such as **CSV,XML,Flat file,** and **Excel.**
* Created various types of reports such as sub reports, parameterized, Tablix and Matrix using SQL server reporting Services.
* Experience in using SQL server reporting Services (SSRS) and creating various reports such as **SubReports, Parameterized, Cascading, Tabular, Matrix, Chart,** and **Drill down** reports.
* Used **For** loop, sequence container, execute SQL task, send mail task to achieve business requirements.
* Created deployment utility to deploy SSIS packages over Production, Prod support and QA environments.
* Used Event Handlers for Custom Logging using Store Procedures for various events (On Warning, On Pre-and Post-Execution, On Task Failed etc.)
* Wrote complex SQL Queries using multiple joins for creating Ad hoc reports using Report Builder based on the requirements.
* Monitored the system performance using **Splunk** and created daily and weekly dash board reports.
* **Splunk DB Connect 2.0** in search head cluster environments of Oracle.
* Scheduling regular meeting with developers and QA team for the planned releases.
* Resolving real time issues which are of critical business impact to the customer.
* Designed, implemented, and tuned jobs using PL/SQL.
* Developed **Bash Shell scripts** to automate repetitive tasks.
* Worked on bug fixes, enhancements, and data changes.
* Improved the performance of the application by rewriting the SQL queries.
* Partitioned the tables and created views to enhance the performance.
* Developing PL/SQL Packages, Procedures, functions in line with Business Requirements.
* Conducted multiple trainings in Splunk and PL/SQL at unit level.
* Coordinated with offshore team on multiple tasks to ensure on time quality deliverables.
* Performance tuning for long running queries using explain plan, hints, and indexes.

**Environment: SQL Server 2008 R2, SQL Server 2008, SQL Server Data Tools, SSIS, SSAS, SSRS, Windows7,Oracle 11g, UNIX Shell Scripting, PL\SQL, Linux, Splunk 6.0.**

**The Walt Disney Company, Burbank, CA. Jan 2012 - Feb 2013**

# SQL SERVER BI DEVELOPER

Disney is the second largest media conglomerate in terms of revenue, after Comcast and established itself as a leader in the American animation industry before diversifying into live-action film production, television, and theme parks. Than Project was to get an Acquisition of a solution and implementation of the Institutional Intranet for Disney and a module for reporting.

**Responsibilities:**

* Worked on gathering business requirements and translating them in to Technical Design
* Worked on creating tables for Logical model and then refactored them to physical names using **SSDT (SQL Server Data Tools)**.

Extensively used **T-SQL** in constructing user defined functions, views, indexes, constraints, and relational database models and data integrity.

* Worked as a developer in creating stored procedures, tables, views, Data migration scripts and other SQL joins and statements for other applications
* Develop reports in **SQL Server Reporting Services (SSRS)**.
* Created various **Tabular** and **Matrix** Reports using SSRS.
* Created various **Drills down** reports using SSRS.
* Experience in deploying reports to System Test and Product test environments.
* Involved in the post deployment maintenance of reports.
* Experience in integrating SharePoint Server with SSRS and deploying SSRS reports on to **SharePoint Server**.
* Proficient in SQL and at least one **ETL** development tool such as **SSIS, Informatica**, etc.
* Created packages in SSIS with error handling.
* Used SSIS to create ETL Packages to perform extract, transform and load data from different source to destination tables.
* Implemented Data Cleansing, Incremental Data Loading, Event Handling, and Error Handling.
* Used different types of transformations such as data conversion, conditional split, look up, derived column, aggregate, Multicast etc.,
* Proficient in using SQL Server Integration Services (SSIS) to build Data Integration and Workflow Solutions, Extract, Transform and Load (ETL) solutions for Data warehousing applications.
* Experience in design of ETL packages for integrating data from heterogeneous sources like (Excel, Oracle, Flat file, CSV) by using multiple transformations provided by SSIS.
* Created SSIS packages to perform filtering options and to import the data on daily basis from file server into database tables.

**Environment: SQL Server 2008R2/2008, Server Integration Services 2008/2005, SQL server**

**Reporting Service 2008, windows 7.**

**Cerner, North Kansas City, MI Oct 2010 - Dec 2011**

**BI/SSRS Developer**

Cerner Corporation is an American supplier of health information technology (HIT) solutions, services, devices, and hardware. The project supported an existing OLTP database system to speed up data processing for storing new fixed income product sales data, portfolio details, and daily financial transaction data.

**Responsibilities:**

* Gathered user requirements and system specifications for the modeling of an **OLAP** database.
* Designed a conceptual, logical, and physical model of the databases **(OLTP and OLAP).**
* Created various database objects such as tables, views, indexes, stored procedures, functions, and cursors as per the business need.
* Developed new procedures and modified existing code, tables, views, and scripts to meet changed system requirements.
* Responsible for developing, supporting, and maintenance of **ETL** (extract, transform, and load) packages using **SSIS.**
* Designed and developed SSIS packages for ETL operations such as data profiling, data cleansing, and data transformation.
* Incorporated error redirection during ETL load in SSIS packages.
* Involved in the troubleshooting of several package and solved several issues related to execution and performance.
* Utilized XML, parent package variable, and SQL table package configurations to provide an easy solution for migrating packages to different environments.
* Wrote test scripts in T-SQL to validate data on staging tables and data mart tables to validate the data results.
* Built a SSRS project to generate reports with desired formats to present business information to management.
* Generated RDLs using reporting services for account aggregation reports.
* Created report models for end-users to create ad-hoc reports utilizing report builder.
* Generated reports to identify bug trends and implemented code changes using team foundation server.

**Environment: MS SQL Server 2008R2/08, BIDS, SSIS, SSAS, SSRS, Access, Excel, SQL Agent,**

**Profiler, TFS, Power Pivot.**

**Andhra Bank, Hyderabad, India August 2008 - Sep 2010**

# SQL Server Developer/SSRS

Andhra Bank has ranked No.1 in terms of number of Life Insurance Policies mobilised amongst all the agency banks dealing with the Life Insurance Corporation of India. The bank also has tie-up with United India Insurance Company Limited under Bancassurance (Non-Life).

**Responsibilities:**

* Managed database objects like stored procedures, views, tables etc.
* Optimized queries that were taking long time to display desired result set.
* Created groups, roles, users and assigning access privileges to users.
* Created new stored procedures and modifying existing ones as per business requirements.
* Created various types of reports such as sub reports, parameterized, Tablix and Matrix using **SQL Server Reporting Services.**
* Performed data analysis to generate various trend reports.
* Performed identification, analysis and resolved report defects within time scope and established development guidelines.

**Environment: SQL Server 2005, SQL Server Management Studio, SQL Server Reporting Services (SSRS).**

**EDUCATIONAL DETAILS:**

* **Bachelors**

**Electronics and Communication Engineering**

**Jawaharlal Nehru University**