**NARESH**

**Summary:**

* Proficient Software Engineer 7+ years of Total IT experience out of which 3-4 years in configuring, implementing and supporting Splunk Server Infrastructure across Windows, UNIX and Linux. Experience with a variety of operating systems protocols and tools.
* **Certified splunk administrator V-6**
* **Certified Power User in Splunk Enterprise V-6**
* Expertise in Installation, Configuration, and Migration, Trouble-Shooting and Maintenance of Splunk, Apache Web Server on different UNIX flavors like Linux and Solaris.
* Experience with Splunk Searching and Reporting modules, Knowledge Objects, Administration, Add-On's, Dashboards, Clustering and Forwarder Management, Visualizations, alerts, reports.
* Strong knowledge of security risk, common attack vectors and indicator of compromise.
* Understanding of networking and application protocols.
* Knowledge of security threats and vulnerabilities and how to detect and mitigate them.
* Experience building security monitoring and incident management solutions using Splunk.
* Provide regular support guidance to Splunk project teams on complex solution and issue resolution.
* Good Understanding of configuration files, precedence and daily work exposure to Props.conf, transforms.conf, inputs.conf, outputs.conf and Setting up a forwarder information based on the requirement.
* Created and Managed Splunk DB connect Identities, Database Connections, Database Inputs, Outputs, lookups, access controls.
* Working knowledge with scripting languages, application development, databases, and analytical tools.
* Analyzing security logs to identify security events to implement alerts to monitor & respond by the 24x7 Security Operations Center (SOC).
* Production error monitoring and root cause analysis using Splunk.
* Expertise in using Splunk with shell script in creating scripts for various activities like Generating Server Status and Healthy reports, Deployment on large scale configuration of servers.
* Expertise in Splunk UI experience, able to write searches, debug search queries and have experience in scripting languages like java script.
* Excellent understanding of project issues, tracking of issues, solving issues and closing issues.
* Expertise in using rex, erex, sed and IFX to extract the fields from log files.
* Experience with SIEM (Security Information and Event Management) systems, security breaches and security event correlation.
* Good knowledge on various Splunk security technologies like firewall, proxy, Time attendance.
* Write Bash / Perl scripts to simplify server tasks and functionality.­­­­­­
* Experienced in Installation and Maintenance of Splunk Universal Forwarders, Solving Forwarder Issues, Deployment Server Classes and Apps through Deployment Server.
* Implemented Forwarders (Universal and Heavy) with Load Balancing, Splunk Forwarder Management.
* Self-motivated and self-educating, yet willing and able to work collaboratively with both customers and fellow Splunkers.
* Team player with excellent communication, presentation and interpersonal skills.
* Excellent written and oral communication skills, including conducting presentations to teams and to customers.

**TECHNICAL SKILLS:**

|  |  |
| --- | --- |
| Relational Databases | SQL Server/2008R2/2008/2005., Oracle9i/10g. |
| Tools and Packages | Splunk 6.2.2,Linux,JBOSS 5x & 6x,Apache2.0,Solaris,SQL Server Management studio, SSIS, SSRS, Microsoft Visual Source Safe, SQL Query Editor, Performance Point Server 2007 |
| Languages | T-SQL ,SPL,SQL, C, python,unix shell scripting,DNS,DHCP |
| Operating Systems | Windows 2010/2008/2007/2003/Windows Vista, Windows XP |
| Web Technologies | HTML, CSS |
| Application Packages | MS Office, MS Outlook (Microsoft Office Suite) |

**Client: TIAA, NC Aug2015- Present**

**Role: Splunk (Admin)**

**Description**: TIAA-CREF is an organization which manages the teacher's insurance for the major educational institutes in the USA. File Life Cider Logger Project is basically a custom EFL framework initiative based on data analytics taken by the organization in order to identify various data points and mitigate the number of failures during the customer file processing and also to provide a holistic reporting mechanism to understand the trend of the file processing status in various internal subsystems.

**Responsibilities:**

* Implementation of the Splunk solution as per the design agreed.
* Ability to work analytically to solve both tactical and strategic problems.
* Strong experience implementing and supporting Splunk technologies
* Experience on splunk monitoring tools with ability to create dashboards and configure alerting.
* Experience with administration of Splunk Search Heads, Indexers, and Forwarders
* Experience with Splunk ES: Enterprise Security.
* All security devices to be integrated with ES app.
* Splunk Enterprise security event monitoring, log index and correlation planning.
* Splunk Universal Forwarder configuration and Splunk dashboard management.
* Ability to mentor and train users on utilizing Splunk get requested reporting.
* Strong experience with Splunk apps such as: Splunk App for Security and Compliance, PCI
* Strong experience with logging tools such as syslog-ng, Rsyslog, LogLogic.
* Knowledge on architecting/operating solutions built on AWS.
* Experience providing security operations support by troubleshooting incident tickets related to security.
* Provide peer code reviews, perform Git merges and repository maintenance.
* Basic knowledge of Active Directory structure.
* Work with Compliance, Internal Audit, and Business teams to identify and analyze risks
* Work with stakeholders to provide security solutions that support their business requirements.
* Identify, develop, and implement mechanisms to detect security incidents in order to enhance compliance with and support of security standards and procedures in place.
* Work with Incident Response team to discovered security incidents by informing appropriate custodians, determining root cause, and actions (if necessary) required to re-establish respective information system security.
* Understand compliance requirements that may impact security and work with business areas and project teams to develop security solutions that address these requirements.
* Maintain current knowledge of industry trends and standards.

**Environment: Environment:** Splunk Enterprise 6.x , Splunk DB Connect, Splunk app for windows, Splunk app for Linux/Unix, Splunk web analytics, SOS and other modules, Git, Solaris 10, LINUX, IIS, AD,LDAP, Apache 2.x, python, centos.

**Client: TD BANK, NJ May2014- Jul 2015**

**Role: Splunk Admin**

**Description:** TD Bank is one of the 10 largest banks in the U.S.TD Bank focuses on the financial needs of growing companies and their executives, consumers and commercial and middle-market. The bank offers a broad range of online services, treasury management tools for businesses and traditional depository and lending products

**Responsibilities:**

* Experience building security monitoring and incident management solutions using Splunk.
* Expertise in creating and customizing Splunk applications, searches and dashboards as desired by IT teams and business.
* Provide Regular support guidance to Splunk project teams on complex solution and issue resolution.
* Involved in standardizing Splunk forwarder deployment, configuration and maintenance across UNIX and Windows platforms.
* Created many of the proof-of-concept dashboards for IT operations, and service owners which are used to monitor application and server health.
* Experience with data analytics, logging solutions and system/network monitoring.
* Managing indexes and cluster indexes, Splunk web framework, data model and pivot tables.
* Performed troubleshooting and/or configuration changes to resolve Splunk integration issues.
* Hands on experience in development experience in customizing Splunk dashboards, visualizations, configurations, reports and search capabilities using customized Splunk queries.
* Knowledge about Splunk architecture and various components (indexer, forwarder, search head, deployment server), Heavy and Universal forwarder, License model.
* Expertise in Actuate Reporting, development, deployment, management and performance tuning of Actuate reports.
* Good understanding of software development life-cycle (SDLC) process , Followed Agile scrum and story maps for dev tracking.
* Strong understanding of security principles in order to provide solutions for sensitive data in a shared environment.
* Onboard new log sources with log analysis and parsing to enable SIEM correlation.
* Parsing, Indexing, Searching concepts Hot, Warm, Cold, Frozen bucketing.
* Field Extraction, Using Ifx, Rex Command and Regex in configuration files, Various types of charts Alert settings Knowledge of app creation, user and role access permissions.
* Ability to review network diagrams and device configurations to ensure security standards are in place.
* Creating and managing app, Create user, role, Permissions to knowledge objects.
* Use techniques to optimize searches for better performance, Search time vs Index time field extraction and understanding of configuration files, precedence and working.

**Environment:** Splunk Enterprise 6.x , Splunk DB Connect, Splunk app for windows, Splunk app for Linux/Unix, and other modules, Oracle 9i/10g, Solaris 10, LINUX, IIS, AD,LDAP, Apache 2.x, python and SVN.

**Client: VCE Company, TX May 2013-Apr 2014**

**Role: Splunk Developer**

**Description:** VCE (Virtual Computing Environment) is a subsidiary of EMC Corporation that manufactures converged infrastructure appliances for enterprise environments. The company manufactures converged datacenter units known as Vblock, which incorporate Cisco servers and networking hardware, EMC storage systems, and VMware for virtualization. Founded in 2009 under the name Acadia, it was originally a joint venture between EMC and Cisco Systems, with additional investments by Intel and EMC subsidiary VMware. EMC acquired a 90% controlling stake in VCE from Cisco in October 2014, giving it majority ownership.

**Responsibilities:**

* Expertise with Splunk UI/GUI development and operations roles.
* Prepared, arranged and tested Splunk search strings and operational strings.
* Helped the client to setup alerts for different type of errors.
* Played a major role in understanding the logs, server data and brought a insight of the data for the users.
* Involved in setting up alerts for different type of errors.
* Analyzed security based events, risks and reporting instances.
* Developed, evaluated and documented specific metrics for management purpose.
* Using SPL created Visualizations to get the value out of data.
* Created Dashboards for various types of business users in organization.
* Provided technical services to projects, user requests and data queries.
* Involved in assisting offshore members to understand the use case of business.
* Assisted internal users of Splunk in designing and maintaining production-quality dashboard.
* Involved in helping the Unix and Splunk administrators to deploy Splunk across the UNIX and windows environment.
* Worked with administrators to ensure Splunk is actively and accurately running and monitoring on the current infrastructure implementation.

**Environment:** Apache Web server. Jboss App server, Oracle database, Splunk 6.1, Splunk 5.2, Splunk 5.1, Agile, Actuate Reports, SDLC, POCs

**Client: Religare Technova Global Solutions Ltd, Bangalore, India Aug 2011-Apr 2013**

**Role: MS SQL Server BI/SSRS/SSIS Developer**

**Description:** **Religare Technova Global Solutions Limited (RTGSL),** formerly Asian CERC Information Technology Limited, provides software solutions to the financial services industry. The Company’s primary business segments include Trading Solutions (including customization, installation and support services) and Information Services Division (subscription/data content feed).

**Responsibilities:**

* Create rules, defaults, tables, views, clustered & non-clustered index, user defined data types, and user defined functions.
* Actively designed the database to fasten certain daily jobs, stored procedures.
* Optimize query performance by creating indexes.
* Write T-SQL statements for retrieval of data and Involved in performance tuning of T-SQL
* Involved in merging existing databases and designed new data models to meet the requirements.
* Create joins and sub-queries for complex queries involving multiple tables.
* Use DDL and DML for writing triggers, stored procedures, and data manipulation.
* Created Stored Procedures to transform the Data and worked extensively in T-SQL for various needs of the transformations while loading the data
* Created and developed data dictionary, tables, views, indexes, functions and advanced queries for databases by using Query Analyzer and SQL Server Enterprise Manager
* Interacted with Business Users and Analyzed user requirements and built reporting solutions such as relational database reports OLAP reporting, dashboards, and scorecards.
* Created SSIS packages to pull data from SQL Server and exported to Excel Spreadsheets and designed SSIS Packages to extract, transfer, load (ETL) existing data into SQL Server 2008 from different environments for the SSAS cubes.
* Created the SSIS /DTS packages and scheduled them using Sql Server agent
* Developed ETL packages with different data sources (SQL Server, Flat Files, Excel source files, XML files etc.) and loaded the data into target tables by performing different kinds of transformations using SQL Server Integration Services (SSIS).
* Designed and developed efficient SSIS packages for processing fact and dimension tables using transformations like Fuzzy lookup, lookup, merge, merge join, script component and Slowly changing dimension .
* Utilized event handling effectively to generate audits and logs for the generated SSIS packages.
* Performed archiving and achieved automated processing of the raw data through the ETL process in SSIS.
* Used Vb.net and C# in Script task of SSIS 2008 Packages
* Performing data transfer/migration using Export/Import and Data Transformation Services.
* Pulled data from various tables and databases to generate reports using different types of joins

**Environment:** Erwin, SQL Server 2008R(2), MS Server Integration services, SSRS (MS server Reporting Services), MS SSAS, Window 2007 Server, Oracle 9i,Db2

**Client: Aircel, Hyderabad, India. Jun 2009- Jul 2011**

**Role: SQL Server / SSIS / SSRS / Developer**

**Description:** Telecommunication Company that provides communications services from dial tone to sophisticated cloud-based technology at low cost. Also provides VoIP, Mobile-Internet-Access, web hosting, voice and cloud-based technology to school and business.

**Responsibilities:**

* Developing T-SQL queries, triggers, functions, cursors and stored procedures.
* Responsible for logical and physical design of SQL Server databases.
* Designed and created SQL Databases, tables, indexes, and views based on user requirements.
* Worked with the application developers and provide necessary SQL Scripts using T-SQL.
* Monitored and modified Performance using execution plans and Index tuning.
* Created User Defined Functions, Stored Procedures, and Triggers.
* Involved in Scheduling jobs using MS SQL server Agent.
* Created and managed users, login IDs, security, and add groups to Windows and SQL Server.
* Involved in Performance tuning of existing database objects such as stored procedures and complex stored procedures.
* Prepared documentation related to database design, objects security and rules.
* Created DTS Packages for migration of data between SQL Server and other databases like MS Access, MS Excel and Flat Files.
* Performed daily database backup & restoration and monitor the performance of Database Servers.
* Generate various ad hoc reports using MS Reporting services

**Environment:** SQL Server 2000/2005, Query Analyzer, Enterprise Manager, DTS, SSIS, SSRS, T-SQL,

Windows XP.

**EDUCATION:**

* Bachelor's degree from Acharya Nagarjuna University, India.