ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025
https://doi.org/10.5281/zenodo.15230804

Building A Soc Dashboard Using Splunk

K.SHWETHA[1], ARTHAM SANJANA[2], ADI NAVEEN,[3] CHITTIPOLUSAINIKHIL[4], GANDAMALA RAVITEJA[5]

[1]**(Assistant Professor)** Dept. of CS, Sri Indu College of Engineering and Technology, Hyderabad,
[2 3 4] Research Student, Dept. of CS Sri Indu College of Engineering and Technology, Hyderabad

ABSTRACT: *Log data is a definitive record of what's happening in every business, organization or agency and it's often an untapped resource when it comes to troubleshooting and supporting broader business objectives. Splunk provides the industry-leading software to consolidate and index any log and machine data, including structured, unstructured and complex multi-line application logs. You can collect, store, index, search, correlate, visualize, analyze and report on any machine-generated data to identify and resolve operational and security issues in a faster, repeatable and more affordable way. It's an enterprise ready, fully integrated solution for log management data collection, storage and visualization. Ad hoc queries and reporting across historical data can also be accomplished without third-party reporting software. Splunk software supports log data enrichment by providing flexible access to relational databases, field delimited data in comma-separated value (.CSV) files or to other enterprise data stores such as Hadoop or NoSQL. Splunk software supports a wide range of log management use cases including log consolidation and retention, security, IT operations troubleshooting, application troubleshooting and compliance reporting.*

Keywords: *LM-log management CSV-comma-separated value, HMS-hotel management system, CERT-computer emergency response team, SMS-short message service, IT-information technology, IP-internet protocol*

I. INTRODUCTION

Splunk provides the industry-leading software to consolidate and index any log and machine data, including structured, unstructured and complex multi-line application logs. It can collect, store, index, search, correlate, visualize, analyze and report on any machine-generated data to identify and resolve operational and security issues in a faster, repeatable and more affordable way. It's an enterprise ready, fully integrated solution for log management data collection, storage and visualization. Ad hoc queries and reporting across historical data can also be accomplished without third-party reporting software. Splunk software supports log data enrichment by providing flexible access to relational databases, field delimited data in comma-separated value files or to other enterprise data stores such as Hadoop. Splunk software supports a wide range of log management use cases including log consolidation and retention, security, IT operations troubleshooting, application troubleshooting and compliance reporting.

II. RELATED WORK

Telenor Case Study – A real time business insight

The Business Founded in 1855, Telenor, Norway‟s largest telecom services provider, has over 150 years of telecoms experience. The company believes “growth comes from truly understanding the needs of people to

drive relevant change." Considering that Telenor‟s mobile subscribers globally grew from 15 to 160 million in less than a decade, its belief that deeper insight leads to success is holding true. Telenor‟s service portfolio in Norway includes fixed and mobile telephony, broadband and data communication. Customers rely on Telenor to provide always-on voice, data and content services.

Challenges

With millions of customers, thousands of servers and routers, and datacenters located throughout Norway, Telenor needed to understand the essential operating details of its infrastructure. Communication between far- flung departments was challenging and there were frequent miscommunications. While some log event data was being collected, the logs were difficult to analyze. In addition, granting access to certain logs on a server often meant giving access to all the logs collected on that server, which posed definite security and privacy risks. The few people with authorized access faced the impossible task of manually browsing through hundreds of millions of log records a day. Unsurprisingly, kernel errors and other issues sporadically slipped by unnoticed.

Enter Splunk in Telenor

Splunk has provided Telenor Norway the visibility and operational insight to keep its IT systems and networks running at peak performance. Telenor is using Splunk Enterprise for troubleshooting, monitoring and security investigations. The network operations team runs dashboards visualizing network health and monitors for error events and unfamiliar patterns. The security team uses Splunk for correlation and analysis of security alarms. With Splunk they can look for, and be proactively alerted on, abnormal remote access patterns and investigate attacks on Internet-exposed services. Finally, Splunk also underpins the Telenor Computer Emergency Response Team (CERT), which is a cross-departmental incident response team. This virtual team uses Splunk for incident investigation, pinpointing the origin of large issues and performing rapid manual analysis of failing components to limit business impact. Telenor indexes 400GBs of data per day with Splunk, including data from thousands of servers, routers and data sources ranging from the datacenter, the IP infrastructure and the mobile network, to applications and services like web, email etc. This constitutes about half of Telenor‟s entire IT estate, and there is now a „Splunk first‟ policy in place, so any new data has to be put into Splunk. Telenor forwards data to a pool of Splunk indexers. Role-based access control ensures users get the access to the data they need without compromising security or violating customer privacy regulations. Industry

• Telecommunications Splunk Use Cases IT Operations Management – Server Monitoring, Network Monitoring

• Security – Incident Investigation Business Impact.

• Established distributed search, alerting, event correlation and proactive monitoring for security.

• Health monitoring using baselines to identify anomalies and issues before they become problems.

• Quick and easy troubleshooting of business-critical issues.

• Supplied role-specific, dashboard views to give appropriate data access to users across IT without compromising security.

• Delivered the IT and network teams infrastructure-wide visibility via dashboards, ad hoc searches, reporting and trend analysis Data Sources.

• Infrastructure logs: Network switch and firewall logs.

• Server logs: Linux, Windows and Unix.

• Application logs: Web, email, etc.

• IP backbone: router logs.

• Mobile network logs overview "Traditional monitoring tools just tell you when something isn‟t working. With Splunk, we can now proactively manage operations and respond before an outage occurs or service erodes."

Incident investigation and troubleshooting

When something goes wrong, it is now quick and easy for Telenor to get to the root cause of the issue and resolve it. For example, the team noticed that Telenor WebMail accounts were being abused to send hundreds of

thousands of SMS messages abroad. They used Splunk to analyze the incident and were immediately able to identify which accounts were being abused and how many SMS were being sent, as well as when and where the logins were coming from. Armed with this insight, it was a simple job to Armed with this insight, it was a simple job to abuse, preventing further revenue loss.

Stronger security

Using Splunk, the security teams can now determine the baseline for "normal" and track any shut down the offending accounts and stop the deviations from that standard. This gives Telenor the ability to quickly and efficiently detect brute force login attacks and other security issues. With this established, they can now use easy-to-compose dashboards to monitor systems and services for anomalous activity. Other examples include correlating timing and IP addresses to determine if attacks from multiple countries are coordinated, and the ability to identify vulnerable Internet exposed services.

Increased availability

Not only can the CERT, security and operations teams troubleshoot problems faster than ever, the insights gained through Splunk software lets Telenor identify a problem long before it turns into a crisis. These valuable searches are now saved and run on a schedule, providing proactive alerts in front of recurring issues. Telenor can now spot an error as soon as it occurs and start working on correcting it immediately, which can prevent or reduce downtime.

Business-critical insights

Over time, the knowledge built into Splunk has enabled Telenor to learn more about the organization‟s IT and network infrastructure and its potential for the business. Telenor is now responding to incidents more proactively and providing better service as a result. The network operations team uses baseline measurements so they can understand what constitutes normal. They have created Splunk alerts to monitor for error spikes and unfamiliar patterns. This advanced visibility lets them troubleshoot problems before users notice them or services fail. In summary, since deploying Splunk, Telenor Norway has dramatically improved visibility into its complex IT infrastructure and networks. Not only can the internal teams now investigate and resolve issues much more quickly, they are also able to use operational intelligence to create baseline views to catch errors or anomalies early on, often addressing these issues before they impact the customer experience. Telenor is now responding to incidents more proactively and providing better service as a result. Telenor can now spot an error as soon as it occurs and start working correcting it immediately, which can prevent or reduce downtime. Role- based access control ensures users get the access to the data they need without compromising security or violating customer privacy regulations.

III. PROPOSED WORK

The Scope of the project is to avoid these issues we need dedicated log review system. Organization has huge volume of staff, material, inflow and outflow of vendor materials and huge of number departments. Its very hard to a have single view of the all the above said operations, trends, upswing and downswing of cost, revenue and operations challenges. With the effectiveness of Splunk these departments can function as on their own without making much changes to their existing system. For any new Software system to be introduced the existing system needs to be changed for major part / minor part / data migration etc. Splunk avoids all such changes to be made to the existing system. With the available logs (even in any raw format) or available database (any traditional or new gen (big data)) splunk can consume the data , index and provide a user friendly dashboards.

IV. SPLUNK

Splunk reads data from a source, such as file or port, or on a host. It classifies source into source type and extracts timestamps .It breaks up the source into individual events. Splunk writes each event into an index on disk. It performs searching of events which are retrieved from disk. Events returned from a search can then be powerfully transformed using splunk‟s search language to generate reports.

ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

V. MYSQL

MySQL is the world's second most widely used open-source relational database management system (RDBMS). It is named after co-founder Michael Widenius's daughter, My. The SQL phrase stands for Structured Query Language. The MySQL development project have made its source code available under the terms of the GNU General Public License, as well as under a variety of proprietary agreements. MySQL was owned and sponsored by a single for-profit firm, the Swedish company MySQL AB, now owned by Oracle Corporation. MySQL is a popular choice of database for use in web applications, and is a central component of the widely used LAMP open source web application software stack (and other 'AMP' stacks). LAMP is an acronym for "Linux, Apache, MySQL, and Perl/PHP/Python." Free-software-open source projects that require a full-featured database management system often use MySQL.

VI. DEVELOPMENT TOOL

NetbeansIDE are integrated development environment (IDE) for designing and developing the Java based applications.

VII. NETBEANS

Net Beans IDE is the official IDE for Java 8. With its editors, code analyzers, and converters, you can quickly and smoothly upgrade your applications to use new Java 8 language constructs, such as lambdas, functional operations, and method references. Batch analyzers and converters are provided to search through multiple applications at the same time, matching patterns for conversion to new Java 8 language constructs. With its constantly improving Java Editor, many rich features and an extensive range of tools, templates and samples, Net Beans IDE sets the standard for developing with cutting edge technologies out of the box.

VIII. JSP

The most significant of the many good reasons for this is that it is amazingly easy to develop sophisticated Web sites with JSPs. Anyone who can write HTML can quickly create rich, dynamic, and responsive Web sites that enable users to get the most out of their online time. Through a mechanism called JavaBeans, JSPs have made it possible for large teams or individuals working on complex projects to divide the work in such a way as to make each piece simple and manageable, without sacrificing any power. JSPs also provide a great deal of flexibility when generating HTML, through the ability to create HTML-like custom tags.

In addition to this fundamental ease of development, high-quality JSP tools are readily available and easy to use. Developers do not need to buy expensive software or commit to a particular operating system in order to use JSPs. The CD-ROM accompanying this book contains everything a JSP author needs to get started, and the tools are powerful enough to serve even a midsized Web site without problems. These free, open-source tools are stable and secure and run on nearly every platform. Of course, high-quality commercial JSP tools are available as well, suitable for serving even the most complex and high-traffic Web sites. Although JSPs have been useful and powerful since the beginning, this is an especially exciting time to be a JSP developer. The recently released version 2.0 of the JSP Specification provides even more features that simplify the process of creating Web sites. In addition, a standard tag library that provides many JSP tags that solve a wide range of common problems has been released. Finally, in the time since they were released, a number of best practices for using JSPs have emerged. This book covers all the topics: the basic powerful features of the JSP specification, the improvements introduced with version 2.0, as well as the new standard tag library and all the things it does. In addition, this book discusses how best to use these tools, based on real-world experiences. However, before we get into all the fun, let's take a look back at how the Web has evolved. This will highlight the kinds of problems that Web authors have faced since the 12 beginning. Once this is understood, it will be clear how JSPs solve these problems and make page creation so easy.

ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

IX. IMPLEMENTATION

The traditional Hotel Management system is used to demonstrate the new generation smart log management system the SPLUNK.

Log files are generated with every transaction done at the Hotel Management.

Customer doing the hotel booking from his place through online – This provides the facility to check the availability of the rooms, flexibility to check the type of rooms and addition detail.

HMS system user

doing the Checkin,

Check out, food rooms

services and billing.

Admin user – adding

required new details of

room, food etc.

HMS Splunk user – Senior management from HMS, survey staff, marketing staff, external agencies, insourcing and outsourcing companies, vendors etc. – They require this data to make business decisions, changes to the existing system, changes to existing business based on the trends of HMS system. This is the key in leveraging the usage of splunk.

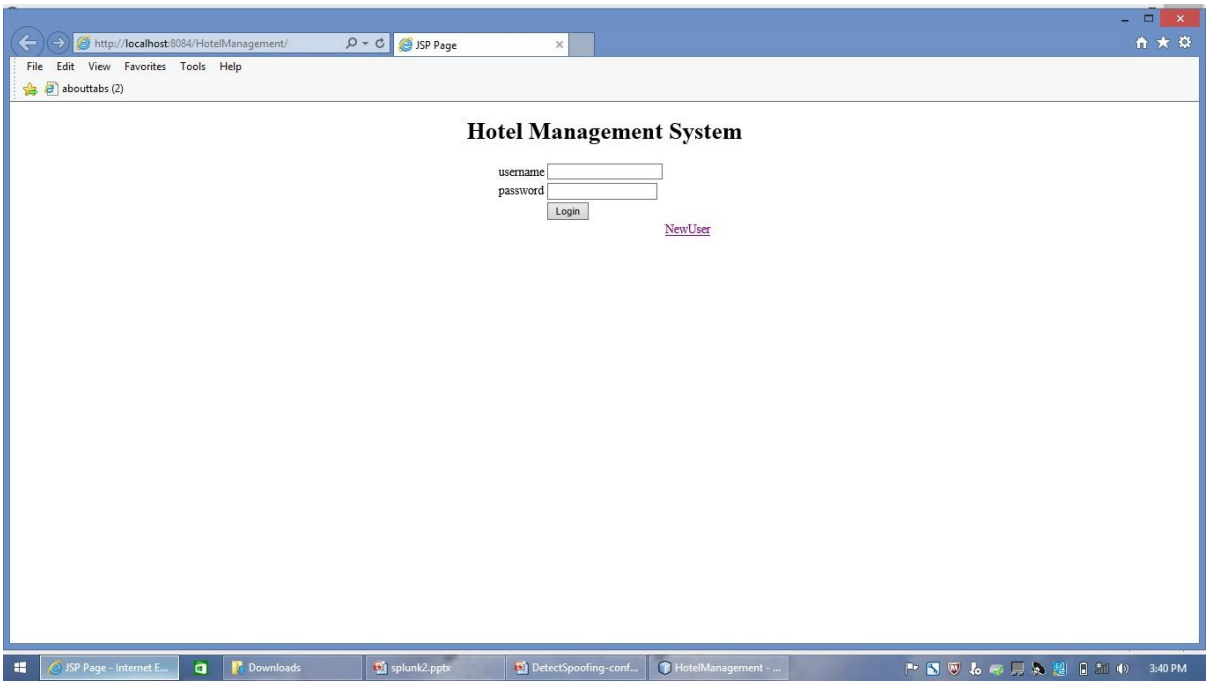
All the investment made of deploying, developing, implementing and usage of splunk is to provide the business users valuable information from the various department of the Hotel.

Large Hotel has huge volume of staff, material, inflow and outflow of vendor materials and huge of number departments.

Its very hard to a have single view of the all the above said operations, trends, upswing and downswing of cost, revenue and operations challenges.

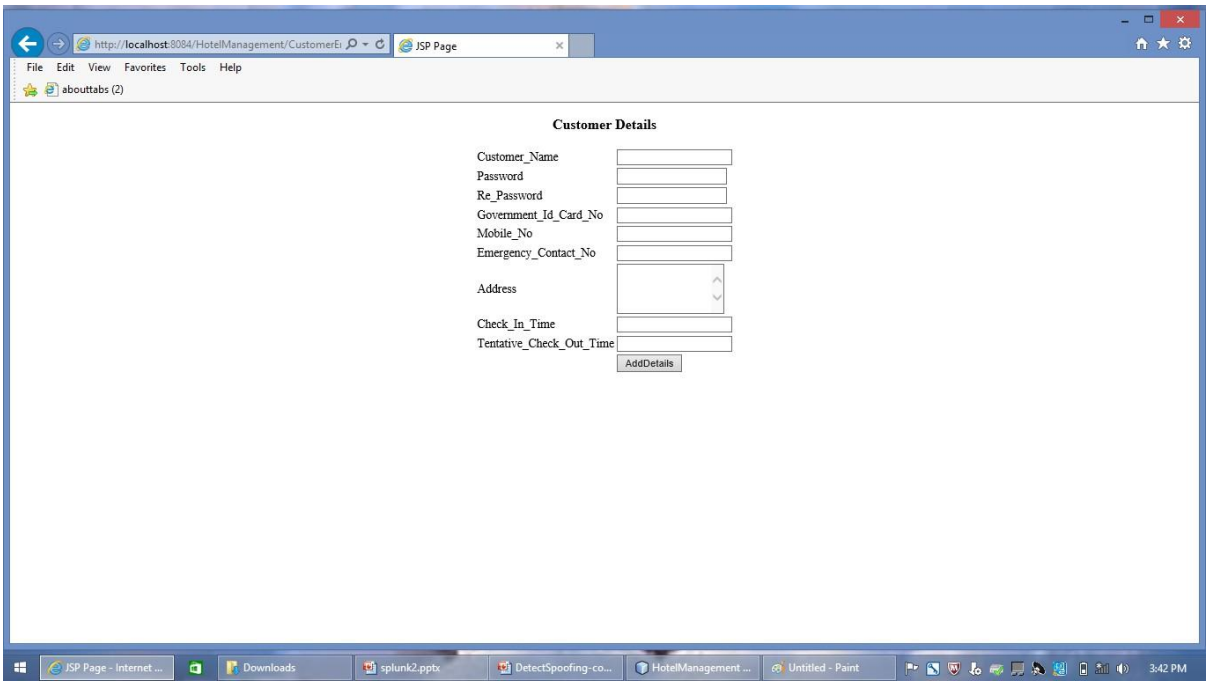
With the effectiveness of Splunk these departments can function as on their own without making much changes to their existing system.

Log In Activity:

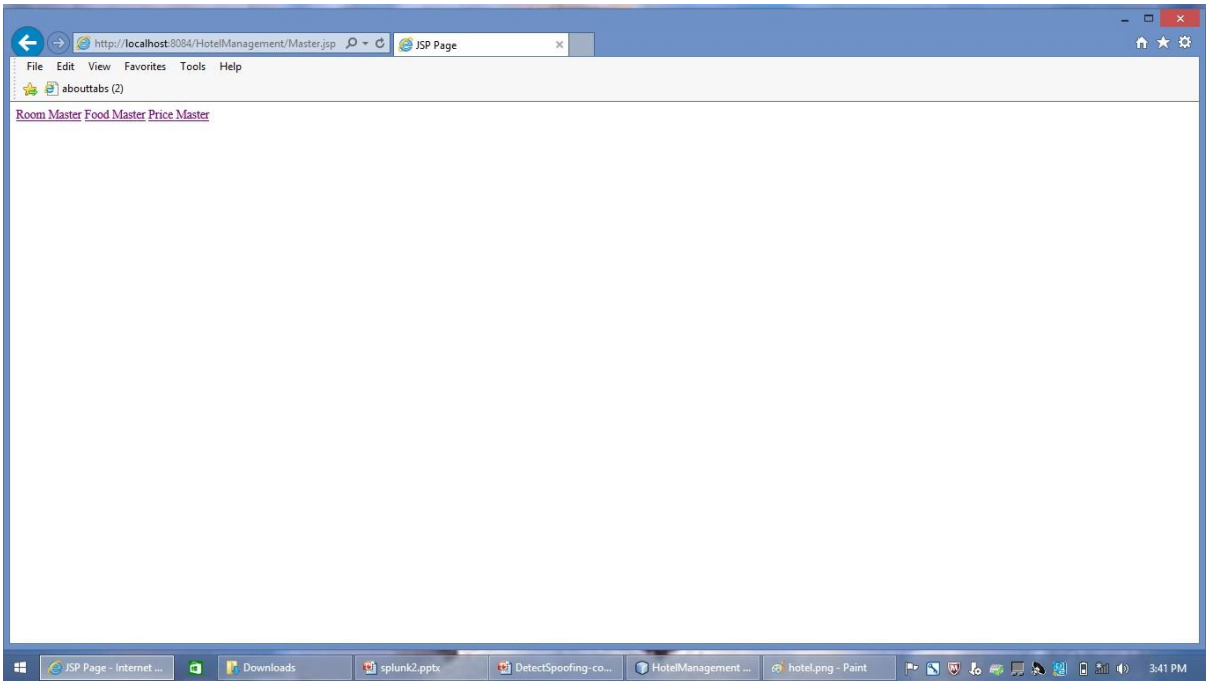


ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

User Module:

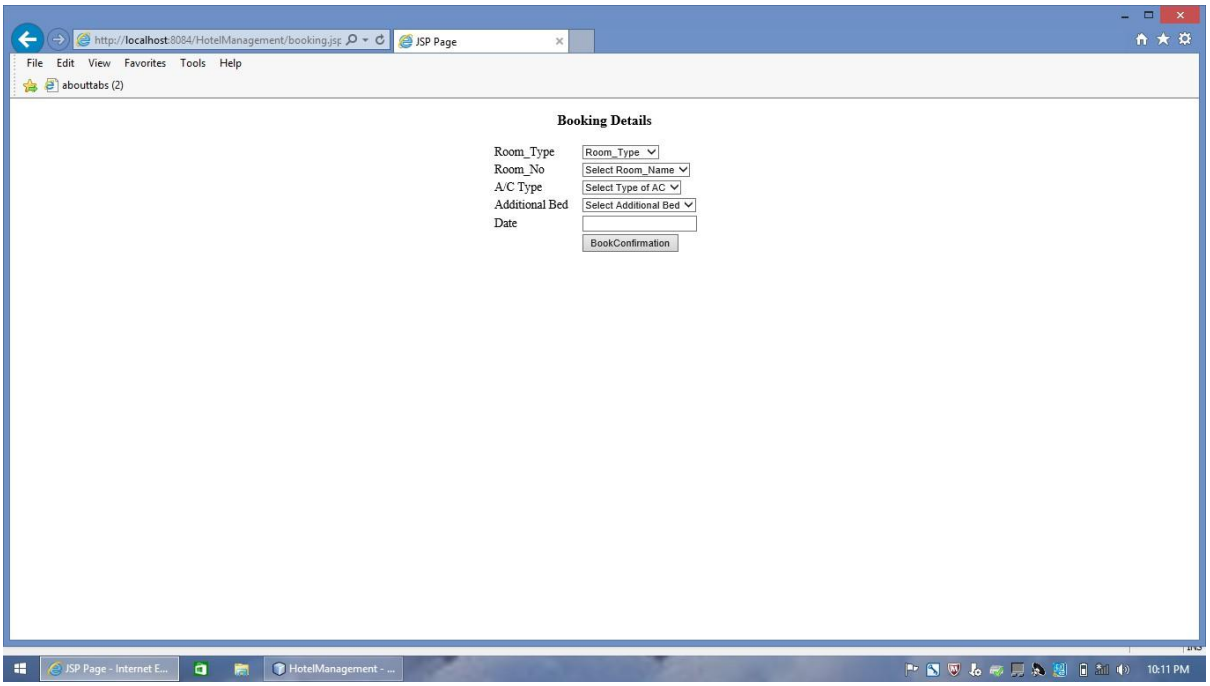


Admin Module:



ISSN: 2456-1134 www.isjcresm.com
Vol-10 Issue-01 Mar 2025

Booking Activity:



ADVANTAGES:

I. To help analyze, reproduce and solve bugs

II. To help test new features in a development stage

III. Deploy and search across on-premise, hybrid-cloud and private/public-cloud based installations

CONCLUSION:

In this project we have generated log files successfully. Each and every transaction in that log file has been tracked. splunk project has been developed to break down huge and complex log files. Then the user friendly dashboard, form, report has been created to improve operational excellence. In summary, since deploying Splunk, this has dramatically improved visibility into its complex IT infrastructure and networks. Not only can the internal teams now investigate and resolve issues much more quickly, they are also able to use operational intelligence to create baseline views to catch errors or anomalies early on, often addressing these issues before they impact the customer experience.

FUTURE WORK:

Splunk project has been developed to break down huge and complex log files. Then the user friendly dashboard, form, report has been created to improve operational excellence.

REFERENCES:

www.splunk.com/base/images/tutorial/sampledata.zip.

docs.splunk.com/documentation/splunk/4.2/user/interactivefield

docs.splunk.com/documentation/splunk/4.2/user/welcometosplunktutorial.

docs.splunk.com/documentation/splunk/4.2/user/adddatatutorial

www.splunkbase.com

www.lkhill.com/splunk-overview