SOLUTION BRIEF

TIBCO LogLogic — A Splunk Management Solution

Table of Contents

3 | State of Affairs

3 | The Challenges

5 | The Solution

6 | How it Works

7 | Solution Benefits

SOLUTION BRIEF

TIBCO LogLogic—A Splunk Management Solution

The TIBCO LogLogic solution can be inserted transparently as a physical or virtual appliance into your environment in front of the Splunk forwarders, syslog sources, and other machine data sources to immediately optimize the flow of data being sent to Splunk indexers.

State of Affairs

Every successful enterprise requires a myriad of information technologies to function in order to meet line of business challenges and address infrastructure concerns like performance and security. Whether these are applications, networks, or security devices, every technology is generating a continuous stream of log data. This log data contains vital information about your business, but most of it will go unnoticed. The sheer amount of data makes it difficult to use. This problem, Machine Big Data, can lead to unnecessary spending, complexity, and risk.

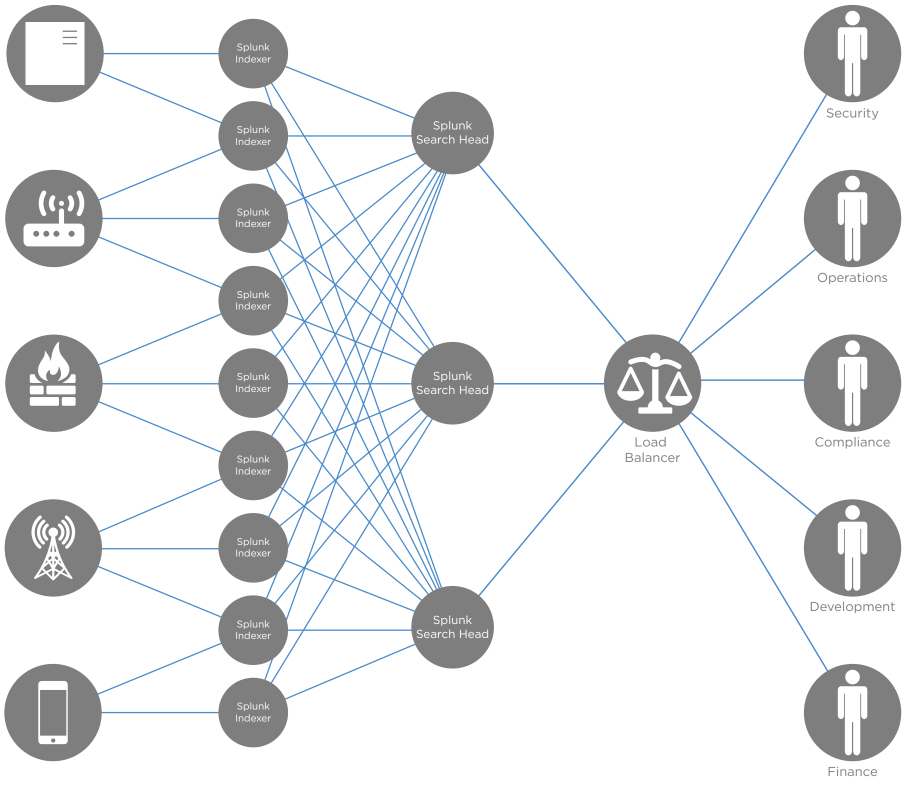
As with every form of vital information, Machine Big Data needs to be collected, stored, and distributed to the systems and people who need it. These systems or people have a variety of uses for this data such as security, operational intelligence, compliance, development, and other business needs. One such consumer is the Splunk application, a widely used tool-kit that searches, monitors, and analyzes Machine Big Data via a web-style interface. Splunk is a full text indexing application that allows users to quickly search through machine data of almost any format. Searches can then be saved and scheduled, turned into an alert or dashboard, or used for data-at-rest correlation.

The Challenges

Like SharePoint in years past, Splunk deployments often start as an easy-to-download departmental solution within the enterprise. As the deployment grows, or the enterprise starts to use Splunk as a machine data management solution, there are a variety of challenges that can occur. The first challenge has to do with the cost of licensing the application. The Splunk application is licensed based on how much machine data is ingested and indexed per day. Licensing starts at 500 MB/day and increases in price incrementally as the data rate goes up. The challenge that volume-based licensing presents is that there is rarely a fixed cost that can be established. As the Splunk deployment expands, the enterprise grows, and the Internet of Things continues to generate more machine data, Splunk licensing cost increases. Unforeseen events can cause this increase to rapidly accelerate, which can be especially problematic if the license is accidentally violated.

For instance, if there is an event that causes a spike in machine data, such as a denial of service (DOS) attack, Splunk searching capabilities may be lost. According to Splunk's documentation, if you exceed your licensed daily volume of machine data on five or more days in a 30 day period, searching functionality will be disabled until a larger license is purchased, or enough time passes to allow the number of violations to be less than five days within the 30 day period. All this at a time when you need search most, in order to troubleshoot the event. These unknown costs and unforeseen events are a real challenge and pose a real risk when deploying Splunk in the enterprise.

Another challenge presents itself with regard to the scalability of the Splunk application and Total Cost of Ownership (TCO). Because Splunk is an application, the server hardware must be procured, setup, hardened, and maintained. The amount of server hardware required can grow exponentially in enterprise environments. The reason for this is the variety of Splunk components in a distributed Splunk deployment. At the collection level, there are Splunk forwarders, lite versions of the Splunk application, installed on machine data sources that collect and forward machine data to Splunk indexers. Splunk indexers receive the machine data and usually perform indexing only. To search the indexed data on the Splunk indexers, one or more Splunk search heads must be used. A typical large-scale Splunk deployment is depicted in the following graphic, with the machine data sources and Splunk forwarders on the left, and the users of the application on the right.



Clearly, the distributed Splunk deployment can be quite large and difficult to manage in an enterprise environment, and the deployment will only continue to grow. Splunk recommends adding an additional indexer for each 50-100 GB per day of additional machine data being indexed, as well as an additional search head for every additional 10 users. This can add significant overhead to the TCO.

To summarize, the challenges for an enterprise trying to deploy Splunk mainly come down to cost and risk. A volume-based license, combined with the increase of that license, hardware procurement, and the labor needed to deploy and maintain the application, can quickly make Splunk more costly than you bargained for. Add to that the possibility of being held hostage by Splunk's automatic shut-off when exceeding data quotas and the need for a Splunk management solution becomes clear.

The Solution

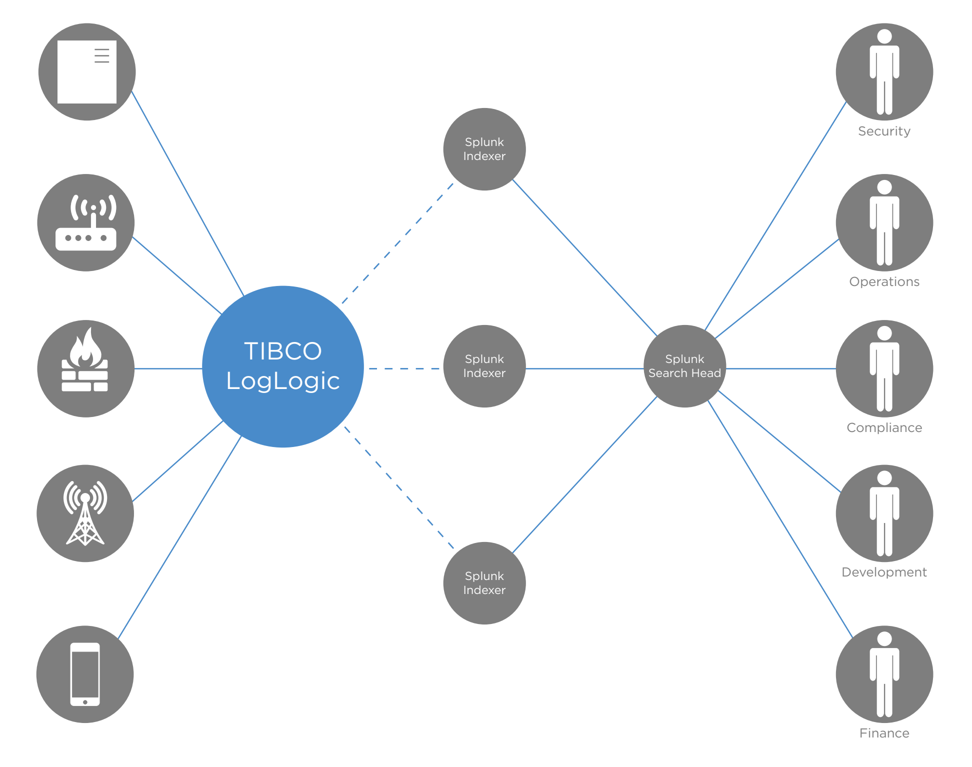
Just as normal Internet traffic needs to be routed, filtered, and secured, the same is true for Machine Big Data. Similar to a proxy server, load balancer, or any other network device that can act transparently, a true Machine Big Data solution needs the ability to not only collect this data, but filter and forward it transparently and securely to its destination, the consumer, while maintaining data integrity. The TIBCO LogLogic® solution is unique in its filtering and forwarding functionality, as well as its scalability for enterprises. This is why many companies choose the TIBCO LogLogic platform to offer Logging as a Service (LaaS) within the enterprise (see: Wikipedia —"Logging as a Serivce" http://en.wikipedia.org/wiki/Logging_as_a_Service_%28LaaS%29

How can TIBCO LogLogic's LaaS solution manage a Splunk deployment? By using TIBCO LogLogic as the collection and storage layer for Machine Big Data, you can securely and transparently filter and forward the machine data that consumers such as Splunk receive. Splunk's documentation shows that this is a best practice for a Splunk deployment:

"You'll invariably need to restart Splunk for various config changes you make"

"If you plan to receive syslog messages via tcp or udp, resist the urge to have Splunk listen for it. You'll invariably need to restart Splunk for various config changes you make, while a separate rsyslog or syslog-ng daemon will simply hum along continuing to receive data while you're applying Splunk changes." — http://wiki.splunk.com/Things_I_wish_I_knew_then

Leaving aside the limitations of low-end logging solutions, the TIBCO LogLogic solution is a proven enterprise class Machine Big Data, LaaS solution. Much more than just a change management solution for Splunk, the TIBCO LogLogic solution will also help you reduce the costs involved with a Splunk deployment as discussed in the previous section. It can do this by filtering or limiting the data that is sent to Splunk so that the Splunk application receives only the data that it needs to meet your company's needs. This frees up your Splunk deployment from having to act as a machine data management solution and allows you to create a fixed cost for your Splunk license and your TCO. As depicted in the following graphic, this solution often results in a much smaller, lower maintenance Splunk footprint within the enterprise.



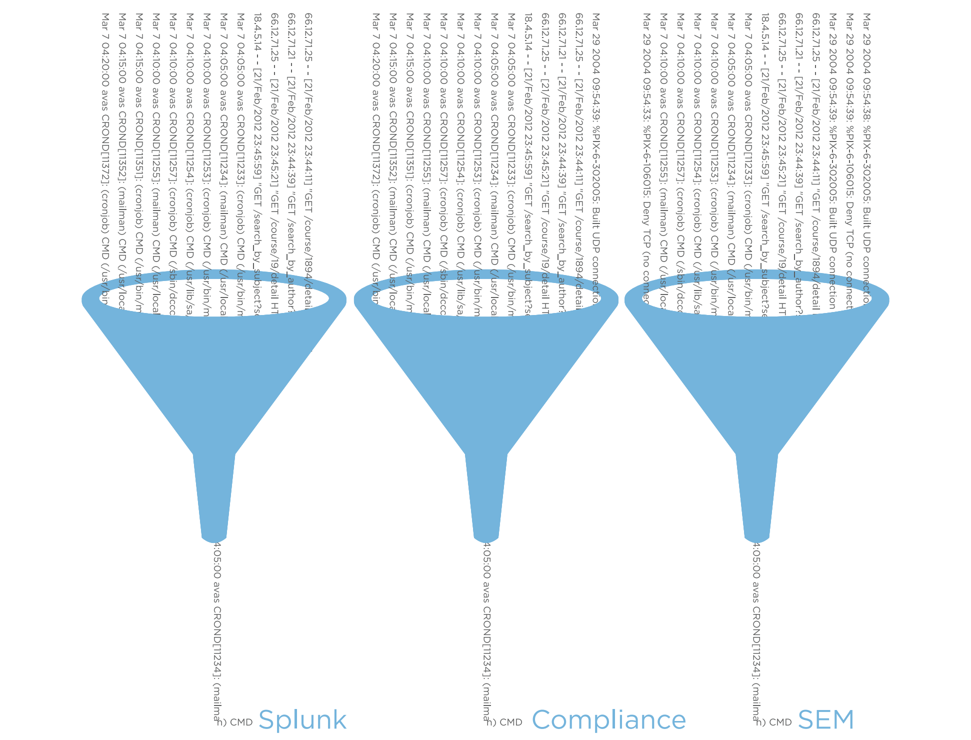
How it Works

The TIBCO LogLogic platform can securely collect Machine Big Data via a variety of methods as required by the log source. For example, this data may be transmitted through a Secure Shell (SSH) connection or retrieved via a Secure Copy (SCP) file transfer. Once the Machine Big Data is collected, TIBCO LogLogic software performs a Secure Hash Algorithm (SHA-256) of the data to prove integrity. Additionally, granular data retention policies allow for custom retention periods for each set of log data so that only the data your enterprise needs is retained. This data can be retained on the TIBCO LogLogic software for up to 10 years, as well as searched, reported, and alerted on.

Most enterprises will also need this data to be transparently filtered and forwarded in real time to a variety of destinations or consumers, including Splunk. Some other examples of machine data consumers include:

- Security event management (SEM) systems
- Security operations centers (SOC)
- Managed security service providers (MSSPs)
- Governance, risk, and compliance (GRC) applications
- Data analytics software
- Network monitoring solutions
- Software development tools

The TIBCO LogLogic filtering and forwarding functionality allows for the creation of rules to securely and transparently route Machine Big Data to any destination in real time.



```
66.12.71.25 - - [21/Feb/2012 23:44:11] "GET /course/1894/detai
66.12.71.21 - - [21/Feb/2012 23:44:39] "GET /search_by_author?
66.12.71.25 - - [21/Feb/2012 23:45:21] "GET /course/19/detail HT
18.4.5.14 - - [21/Feb/2012 23:45:59] "GET /search_by_subject?se
Mar 7 04:05:00 avas CROND[11233]: (cronjob) CMD (/usr/bin/m
Mar 7 04:05:00 avas CROND[11234]: (mailman) CMD (/usr/local
Mar 7 04:10:00 avas CROND[11253]: (cronjob) CMD (/usr/bin/m
Mar 7 04:10:00 avas CROND[11254]: (cronjob) CMD (/usr/lib/sa/
Mar 7 04:10:00 avas CROND[11257]: (cronjob) CMD (/sbin/dccc
Mar 7 04:10:00 avas CROND[11255]: (mailman) CMD (/usr/local
Mar 7 04:15:00 avas CROND[11351]: (cronjob) CMD (/usr/bin/m
Mar 7 04:15:00 avas CROND[11352]: (mailman) CMD (/usr/loca
Mar 7 04:20:00 avas CROND[11372]: (cronjob) CMD (/usr/bin
```

```
4:05:00 avas CROND[11234]: (mailman) CMD
```

```
Mar 29 2004 09:54:39: %PIX-6-302005: Built UDP connectio
66.12.71.25 - - [21/Feb/2012 23:44:11] "GET /course/1894/detai
66.12.71.21 - - [21/Feb/2012 23:44:39] "GET /search_by_author?
66.12.71.25 - - [21/Feb/2012 23:45:21] "GET /course/19/detail HT
18.4.5.14 - - [21/Feb/2012 23:45:59] "GET /search_by_subject?se
Mar 7 04:05:00 avas CROND[11233]: (cronjob) CMD (/usr/bin/m
Mar 7 04:05:00 avas CROND[11234]: (mailman) CMD (/usr/local
Mar 7 04:10:00 avas CROND[11253]: (cronjob) CMD (/usr/bin/m
Mar 7 04:10:00 avas CROND[11254]: (cronjob) CMD (/usr/lib/sa/
Mar 7 04:10:00 avas CROND[11257]: (cronjob) CMD (/sbin/dccc
Mar 7 04:10:00 avas CROND[11255]: (mailman) CMD (/usr/local
Mar 7 04:15:00 avas CROND[11351]: (cronjob) CMD (/usr/bin/m
Mar 7 04:15:00 avas CROND[11352]: (mailman) CMD (/usr/loca
Mar 7 04:20:00 avas CROND[11372]: (cronjob) CMD (/usr/bin
```

```
4:05:00 avas CROND[11234]: (mailman) CMD
```

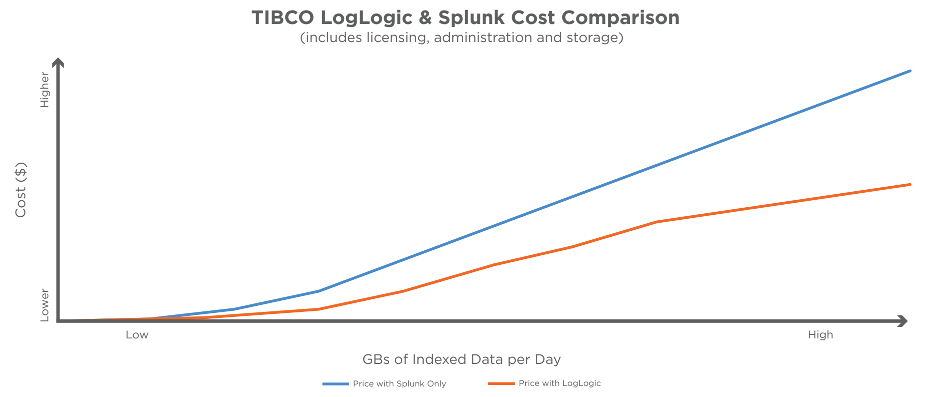
```
Mar 29 2004 09:54:38: %PIX-6-302005: Built UDP connectio
Mar 29 2004 09:54:39: %PIX-6-106015: Deny TCP (no connect
Mar 29 2004 09:54:39: %PIX-6-302005: Built UDP connection
66.12.71.25 - - [21/Feb/2012 23:44:11] "GET /course/1894/detail
66.12.71.21 - - [21/Feb/2012 23:44:39] "GET /search_by_author?
66.12.71.25 - - [21/Feb/2012 23:45:21] "GET /course/19/detail HT
18.4.5.14 - - [21/Feb/2012 23:45:59] "GET /search_by_subject?se
Mar 7 04:05:00 avas CROND[11233]: (cronjob) CMD (/usr/bin/m
Mar 7 04:05:00 avas CROND[11234]: (mailman) CMD (/usr/loca
Mar 7 04:10:00 avas CROND[11253]: (cronjob) CMD (/usr/bin/m
Mar 7 04:10:00 avas CROND[11254]: (cronjob) CMD (/usr/lib/sa
Mar 7 04:10:00 avas CROND[11257]: (cronjob) CMD (/sbin/dccc
Mar 7 04:10:00 avas CROND[11255]: (mailman) CMD (/usr/loca
Mar 29 2004 09:54:33: %PIX-6-106015: Deny TCP (no connec
```

```
4:05:00 avas CROND[11234]: (mailman) CMD
```

Additionally, each destination will only receive the data it needs to meet your company's needs, helping to avoid overloading the consumer or over-extending its licensing. The end result is a streamlined LaaS architecture that reduces enterprise costs in a variety of ways including for management overhead, network congestion, storage requirements, data security, and licensing.

Solution Benefits

TIBCO LogLogic's LaaS platform does not have any volume-based licensing, so you never have to worry about unpredictable costs. LogLogic has a fixed cost that in most cases provides proven savings and ROI in under two years, especially when used to manage your Splunk deployment. In many scenarios, a single TIBCO LogLogic appliance can ingest machine data at a rate that requires five to ten Splunk servers. The following value model shows this scenario.



For more information, head to www.tibco.com/loglogic

With TIBCO LogLogic managing your Machine Big Data, you no longer have to worry about setting varying retention periods for Splunk indexers because your retention policies are now quickly and easily managed. Additionally, indexed machine data retention policies can be separated from raw machine data retention policies. This means that storage resources are used more effectively, and compressed raw machine data can be searched outside of your index retention period.

The TIBCO LogLogic LaaS platform is a plug and play solution that offers an effortless lifecycle. Setup is quick and easy and can be completed without a full time employee. This means it is never too late to put the brakes on a Splunk deployment that is growing too rapidly.

The TIBCO LogLogic appliance can be inserted transparently into your environment in front of the Splunk forwarders, syslog sources, and other machine data sources to immediately curb the flow of data being sent to Splunk indexers. Additionally, while the TIBCO LogLogic solution can parse or normalize machine data, it always stores 100 percent of the raw machine data. This complete storage allows the solution to act as the system of record for your Machine Big Data and any modification of data by the machine data consumer can proceed as needed. TIBCO LogLogic also contains many enterprise features such as high availability (HA) so you never have to worry about losing machine data during a Splunk configuration change. TIBCO LogLogic is a true LaaS platform that helps you manage Splunk and all of your Machine Big Data.

Global Headquarters
3307 Hillview Avenue
Palo Alto, CA 94304

Tel: +1 650-846-1000
+1 800-420-8450
Fax: +1 650-846-1005

www.tibco.com