

Features of Ironstream for Splunk

Darshan Harish

Contents

Introduction	4
Splunk.....	4
Challenges getting Mainframe data into Splunk.....	5
Ironstream for Splunk	6
Ironstream Architecture Features	7
Benefits	9
Other Key Features	10

Table of Figures

Figure 1: Why Splunk your Mainframe?	4
Figure 2: IBM Mainframe	5
Figure 3: Mainframe data into Splunk	6
Figure 4: Ironstream Architecture	7
Figure 5: Sample Mainframe Log Data that can be Splunked.....	8

Introduction

Splunk

Splunk is a log management product aimed at large enterprises and is typically deployed on premises. It is a powerful platform for analyzing machine data (that machines emit in great volumes) but which is not used effectively.

Splunk produces software for searching, monitoring, and analyzing machine-generated big data, via a web-style interface.

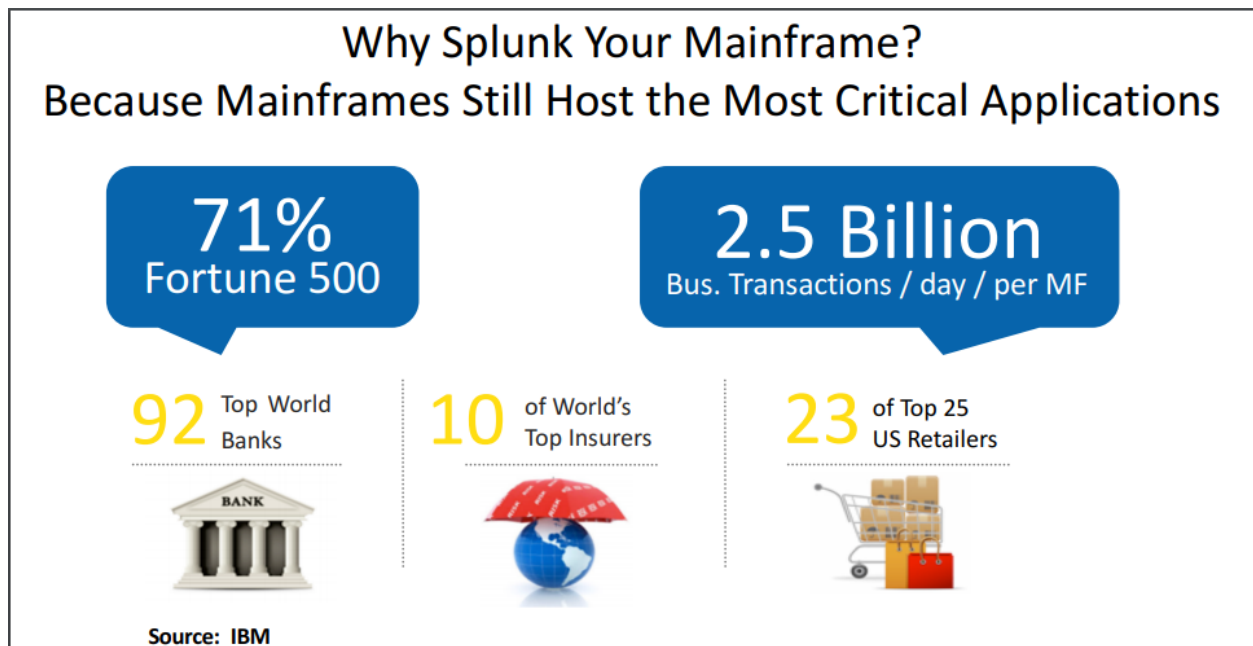


Figure 1: Why Splunk your Mainframe?

Challenges getting Mainframe data into Splunk

Splunk does not support collection of machine data from traditional IBM mainframe and IBM i systems.



Figure 2: IBM Mainframe

The following factors are responsible for the challenge:

- Integration
 - Data conversion: EBCDIC to ASCII; Binary to readable
 - Complex Mainframe data structures: System Management Facilities (SMF) Data
- Security
 - Hosts mission critical sensitive data, which makes it difficult to access.
- Cost
 - Processing on the mainframe costs CPU cycles (MIPS) – including data transmission (TCP, FTP, etc.)
 - Cannot interfere in system throughput.
- Operational
 - Log file migration is complex.
 - Tracking delta from log files is difficult.
 - Getting Real time data is complex.

Ironstream for Splunk

Precisely Ironstream makes it simple to collect, transform and securely stream data from these traditional IBM platforms into Splunk with no need for mainframe or IBM i expertise.

Ironstream is the industry's leading automatic forwarder of z/OS mainframe log data and IBM i machine data to Splunk Enterprise. Mainframe and IBM i data forwarded by Ironstream can be merged with other machine data from across an organization's IT infrastructure to support enterprise-wide IT Operations Analytics (ITOA), Security Information and Event Management (SIEM) and IT Service Intelligence (ITSI).

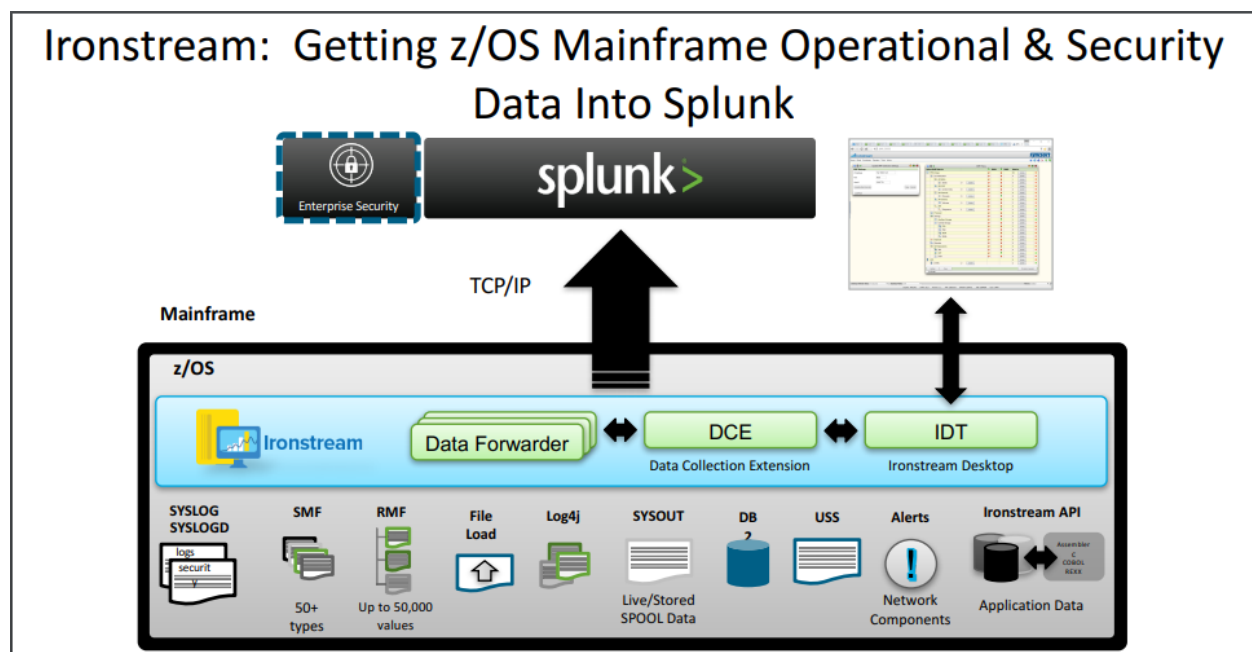


Figure 3: Mainframe data into Splunk

Ironstream Architecture Features



Figure 4: Ironstream Architecture

Ironstream has the following considerations regarding its architecture:

- Ultra Light Weight
 - Minimal MIPS impact even for billions of SMF records.
- Non-intrusive
 - Collect data from critical system
 - Zero impact to throughput
- Fast
 - Collect data in real time
- Secure and Reliable
 - Error recovery
 - Security
 - Load balancing

Sample Mainframe Log Data That Can Be “Splunked”




	Operational Analytics	Mainframe Application Operator logs for DB2, CICS, IMS, etc	Related Mainframe Logs Syslog
	Application Monitoring	DB2 Accounting Records CICS Accounting Records WebSphere Job / Step Accounting Records	SMF Type 101 SMF Type 110 Log4j SMF Type 30
	Security & Compliance	RACF Intrusion Detection	SMF Type 80 SyslogD

Figure 5: Sample Mainframe Log Data that can be Splunked

Benefits

There are a lot of benefits of using Ironstream for Splunk. They are listed as follows:

- **Less Complexity:** It breaks down silos and seamlessly integrates with Splunk for a single view of all your systems, with no mainframe expertise required.
- **Precise security information:** Complete visibility into enterprise wide security alerts and risks for all systems.
- **Healthier IT operations:** Anomalies in the IT environment are accessible for analytics and diagnosis along with the information coming from other platforms.
- **Better problem-resolution management:** Acting fast with real-time access to data.
- **Higher operational efficiency:** Enabled by advanced filtering of records, utilization of zIIP processors, and data loss protection.
- **Visibility into cross-platform transactions:** To monitor and improve IT service delivery and application performance.
- **Integrates with Splunk Enterprise Security*:** Ensuring that mainframe security information is correlated and displayed alongside security data from distributed platforms in all Enterprise Security dashboards.
- **Integrates with Splunk IT Service Intelligence*:** Ensuring that the KPIs for mainframe components including CICS and DB2 are mapped to critical business services for total visibility into IT service delivery.
- **Ironstream Mainframe Data Model*:** Assists Splunk users typically not mainframe experts , to understand the mainframe logs better and integrating them with other data for a more complete view of their IT Operations.
- **Ironstream API*:** Enables COBOL, REXX, and Assembler applications to directly forward application data to an analytics platform for enhanced visualization of application information.
- **zIIP Processors utilized*:** To reduce CPU consumption and minimize overhead associated with capturing and forwarding data to analytics platforms.
- **Logstream SMF collection*:** Enables asynchronous collection of SMF data in high transaction rate systems to ensure application performance and low latency.

Other Key Features

Apart from the aforementioned features and benefits, the other Key Features of Ironstream for Splunk is to support all critical IBM mainframe z/OS data sources and IBM i Data sources.

The list of support features for IBM mainframe z/OS data sources are as follows:

- **IMS log data:** The Information Management System (IMS) is a database and transaction management system. A log file is a file that usually records the user's activity log in the Operating System or any other Software's running on the respective Devices.
- **SMF and Syslog records:** System Management Facilities (SMF) Data and the Syslog files are System log files. It is used when we must determine a particular action that has happen in the system like error, exception and other things occurring in the system.
- Security information from RACF, ACF2, and Top Secret
- Resource Measurement Facility III data
- UNIX Systems Services (USS) and Log4J files
- Network-performance data

Advanced Filtering of captured data uses low overhead exits with no log stream dependencies. Filtering reduces data volume and network traffic ensuring that only critical records and fields required for desired analytics and visualization are forwarded.

The list of support features for IBM i Data sources are as follows:

- Operating System
- Message Queue Data
- System Audit Journal
- Custom Data
- History Log (QHST)
- System Performance Data
- Custom Data