Ironstream for Splunk®

1. Objective

The objective of this product specification document is to explain Ironstream for Splunk®, its features and benefits.

2. Scope

Precisely' s Ironstream® is available for the platforms that follow:

1. Splunk®
2. ServiceNow®
3. Micro Focus®
4. Microsoft® SCOM

This document is applicable to **Ironstream for Splunk® only.** For any other platform refer to applicable documents.

Ironstream for Splunk®

Table of Contents

3. Mainframe Data – Introduction

The IBM mainframe is a mature computing environment. This business machine was developed in the 1960s and it has evolved over the decades into an efficient, powerful, and feature-rich platform. It is ready for the latest technologies like Cloud, Mobile and DevOps. It will play an important role in the evolving technologies like Blockchain, Artificial Intelligence (AI), & Machine Learning (ML).

Along with these great technologies, a mainframe can also supply activity logs. These activity logs record what is happening with both hardware and software resources.

3.1. What is Mainframe Log Data?

There are many data sources that are available within the IBM z/OS mainframe system. The data from these sources can give valuable information about the status, new trends, fault diagnosis, the operational health of the system and its applications, etc. The data can also be used to give business-critical information about security and compliance issues of the system.

For example, the System Management Facility (SMF) on z/OS is the component which collects and records a large amount of real-time and historical information on:

- performance,
- security, and
- technical operations.

Terabytes of very useful data can be recorded daily. SMF records every operational event that occurs on the mainframe — from a simple log-in attempt at a workstation to a potential breach of system security — in its one or more SMF record types.

Unix System Services files may contain log records and application information from web-based and other applications that can give very important information.

Though the data is very helpful, understanding and utilizing this log information can be complex. It requires a great mainframe knowledge and some consolidation of information to create a meaningful result. Users, especially those who are less familiar with the mainframe, can often struggle to make a sense of this valuable resource.

Precisely' s Ironstream® for Mainframe was developed to help Splunk® users – typically not mainframe experts – to better understand these logs and how to integrate them with other data for a 360-degree view of their IT Operations.

4. Splunk® - Limitation

To manage today's IT infrastructure, you need a single and complete view of all the systems in your environment. As a result, Splunk® is the IT platform of choice for many companies.

However, Splunk® does not support collection of machine data from traditional IBM mainframe and IBM i systems. Precisely' s Ironstream® makes it easy to collect, transform, and securely stream data from these traditional IBM platforms into Splunk® with no need for mainframe or IBM i expertise.

5. Ironstream® - Introduction

Various organizations have a variety of tools that help them to analyze their mainframe systems and components. For decades, software suppliers provided silo point-based solutions that helped organizations to do deep analysis of their performance, availability, security, and more.

At the same time organizations find that there is less integration between these silo analyzers and there is no integration at all with information from other platforms. This creates a big gap in understanding security issues and service delivery on an enterprise-wide basis for cross-platform IT services.

5.1. Ironstream for Splunk® - The New Solution

Precisely - a global leader in data integration - introduced Ironstream® to the Splunk® market in September 2014. Ironstream® is industry's leading automatic forwarder of z/OS mainframe log data and IBM i machine data to Splunk® Enterprise.

Ironstream® collects data and sends it in machine-readable form to a Splunk® Enterprise or Splunk Cloud™ platform. Then, the data can be merged and analyzed with other machine data from different sources of organization's infrastructure. The combined data can be used to support your strategic enterprise-wide objectives, which can include:

- Security Information and Event Management (SIEM)
- IT Service Intelligence (ITSI)
- IT Operations Analytics (ITOA)
- Compliance for regulations such as PCI-DSS, GDPR, CCPA and HIPAA.

Ironstream® running with Splunk® is an easy, cost-effective way for an organization to get that invaluable 360-degree view of its complete IT infrastructure. You get this view when Ironstream® integrates key performance indicators and events which are available across different logging facilities.

Moreover, you don't need special knowledge and expertise to correlate mainframe data and data from other platforms as Ironstream® is proficient in handling this task.

Ironstream for Splunk®

With extensive support for critical IBM mainframe and IBM i data sources, Ironstream® helps organizations to keep their IT infrastructure secure and helps them to do their best.

To know more about Ironstream for Splunk®, refer the short 4-minute video.

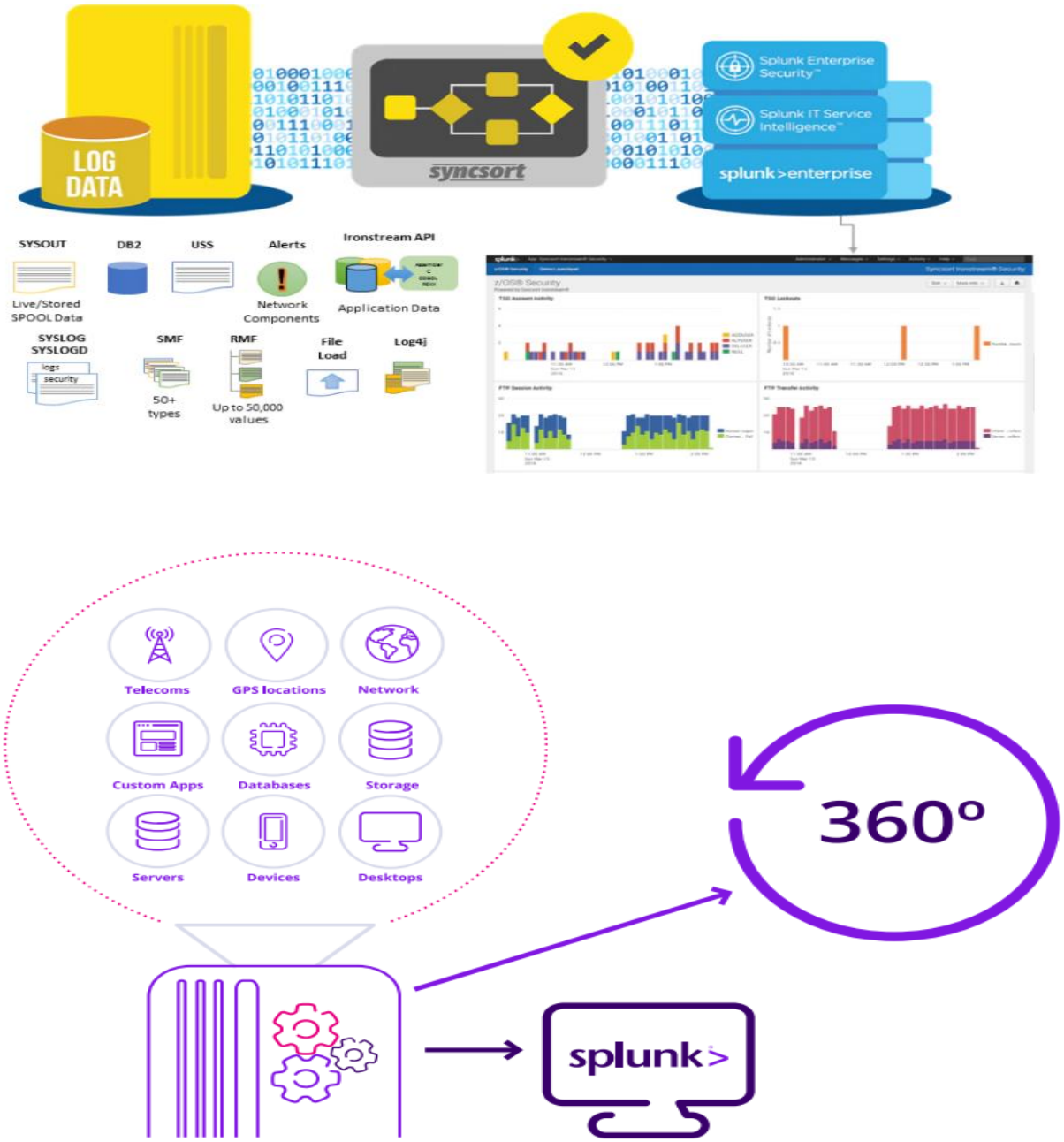

Figure 1: Ironstream for Splunk®

6. Ironstream for Splunk® - Features

6.1. The Key Features

1. Ironstream® can record real-time output from RMF (Resource Measurement Facility) and SMF (System Management Facility) of the mainframe sources. This allows you to see what is happening on the mainframe as it happens, without losing precious time.

2. It gives support for all critical IBM mainframe z/OS data sources which include:

    a. IMS log data

    b. SMF and Syslog records

    c. Security information from RACF, ACF2, and Top Secret

    d. Resource Measurement Facility III data

    e. UNIX Systems Services (USS) and Log4J files

    f. Network-performance data

3. It gives support for all critical IBM i data sources which include:

    a. Operating System

    b. Message Queue Data

    c. System Audit Journal

    d. Custom Data

    e. History Log (QHST)

    f. System Performance Data

    g. Custom Data and many more…

4. It gives advanced filtering options to remove un-necessary data and can forward only critical records to Splunk® for necessary analytics and visualization.

5. It integrates with both Splunk IT Service Intelligence and Splunk Enterprise Security, and gives the benefits that follow:

    a. Mainframe security information is correlated and displayed along with the security data from distributed platforms in all enterprise security dashboards.

    b. KPIs for mainframe components which include CICS and DB2 are mapped to critical business services for total visibility into IT service delivery.

6.2. The Benefits

1. Ironstream® is not complex, it breaks down silos into small chunks and easily integrates with Splunk® for a single view of all your systems. You do not need mainframe expertise.
2. It is accurate and gives clear security information of enterprise wide security alerts and risks for all systems.
3. It creates healthier IT operations because anomalies in the IT environment are easy to find for analytics and diagnosis along with the information from other platforms.
4. It creates a better problem-resolution management with real-time access to data which in turn helps you to act fast.
5. It creates higher operational efficiency with the help of advanced filtering of records, utilization of zIIP processors, and data loss protection.
6. It gives visibility into cross-platform transactions to analyze and improve IT service delivery and application performance.
7. Ironstream® Mainframe Data Model* helps Splunk® users – typically not mainframe experts – better understand mainframe logs and how to integrate them with other data from different platforms. This gives a better view of IT Operations.
8. Ironstream® API* helps COBOL, REXX, and Assembler applications to directly forward application data to an analytics platform for better visualization of application information.
9. zIIP Processors utilized* to reduce CPU consumption and minimize overhead associated with capturing and forwarding data to analytics platforms.
10. Logstream SMF collection* helps in asynchronous collection of SMF data in high transaction rate systems. This in turn gives better application performance and low latency.

* IBM mainframe only

7. References

If you want to learn more about Ironstream for Splunk®, refer the links that follow:

1. Ironstream® Details
2. Ironstream for Splunk® video
3. IBM Ironstream 2.1
4. Splunk®
5. Splunk IT Service Intelligence
6. Splunk Enterprise Security
7. Ironstream® – Customer Story
8. Ironstream®– Webcast

Appendix A – Ironstream® Pre-requisites

To install Ironstream® make sure you have:

- IBM-supported release of z/OS
- Memory: 100MB virtual storage
- Network: TCP/IP or SSL over TCP/IP
- DASD: 10MB
- Authorized library
- Access to CEE.SCEELKED
- Deployed as a JOB or STC

For information on Ironstream z/OS security insights with Splunk Enterprise security:

http://www.syncsort.com/ironstreames.