Ironstream for Splunk®

Product Specification Document

precisely

Corporate headquarters
2 Blue Hill Plaza, #1563
Pearl River, NY 10965
info@precisely.com
+1 (877) 700 0970

Table of Contents

1. Objective

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

2. Scope

This document is applicable to Precisely's **Ironstream for Splunk® only**.

Precisely's Ironstream® available for the below platforms:

1. Splunk®
2. ServiceNow®
3. Elastic
4. Kafka
5. Micro Focus®
6. Microsoft® SCOM

To know more about each platform, refer to the specific product specification document.

3. IBM Mainframe

3.1 What is Mainframe?

Mainframes are data servers designed to process up to 1 trillion web transactions daily with the highest levels of security and reliability. Mainframe solutions are robust, resilient, securable, and technologically advanced platforms for hybrid cloud.

3.2 IBM Mainframe

IBM mainframes are high-performance computing environment with large amounts of memory and processors that process billions of simple calculations and transactions in real time. This business machine was developed in 1960 to 1970 and evolved over decades to more efficient, powerful, and rich platform.

The IBM mainframe is critical to commercial databases, transaction servers, and applications that require high resiliency, security, and agility.

IBM mainframes are evolved and ready with IBM mainframe server solutions like Cloud computing, Data & Analytics, Hybrid Cloud, Machine Learning (ML), etc.

3.3 IBM Mainframe Data

There are many valuable data available within the IBM mainframe z/OS (mainframe machine data) that can provide an insight to the system health, applications security, operations, and system compliance.

The System Management Facility (SMF) on IBM z/OS is the primary data source which collects and records a real-time large amount of data and historical information on:

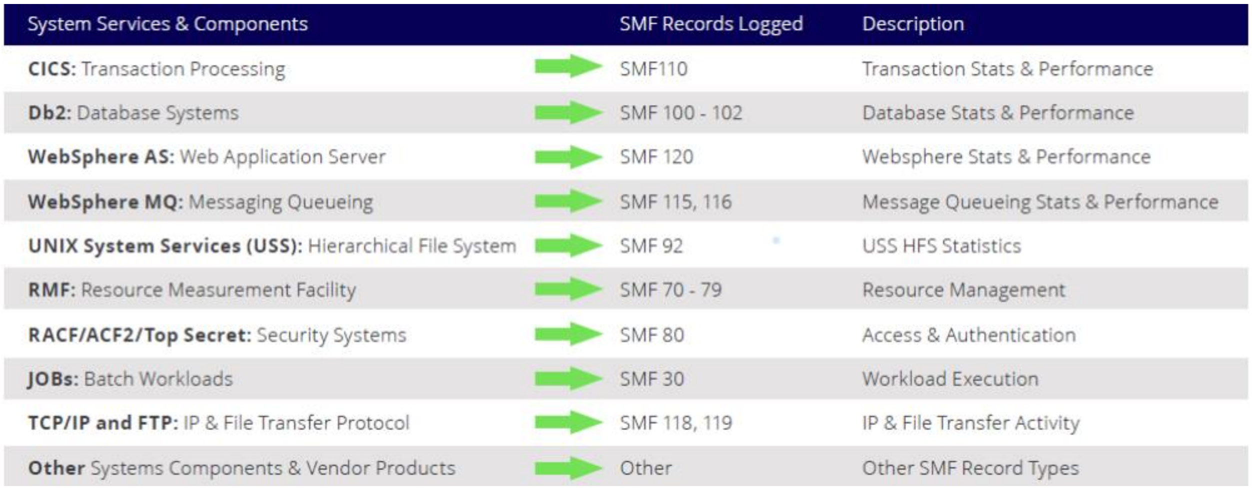
1. Performance
2. Security
3. Technical Operations.

SMF records plenty of information daily. SMF captures every operational event that occurs on the mainframe — from a simple log-in attempt at a particular workstation to a potential breach of system security — is captured and recorded in one or more SMF record types.

SMF is a logging capability provided by IBM z/OS to capture detailed information about every activity within the system. The information includes system-level information, application information, security information and events, transaction information, database information, and virtual anything related to the system's operating environment. The SMF data is the single source of operational and security information on the mainframe.

3.4 SMF Data

SMF data is very complex and collects every aspect of the system operating environment generates a unique record type which is self-describing and can contain thousands of unique fields. The recorded data can be used by anyone for data analytics who is familiar with analytics platform like Splunk. The below image shows the example of SMF records logged by various system components and processes.



System Services & Components		SMF Records Logged	Description
CICS: Transaction Processing	➡	SMF110	Transaction Stats & Performance
Db2: Database Systems	➡	SMF 100 - 102	Database Stats & Performance
WebSphere AS: Web Application Server	➡	SMF 120	Websphere Stats & Performance
WebSphere MQ: Messaging Queueing	➡	SMF 115, 116	Message Queueing Stats & Performance
UNIX System Services (USS): Hierarchical File System	➡	SMF 92	USS HFS Statistics
RMF: Resource Measurement Facility	➡	SMF 70 - 79	Resource Management
RACF/ACF2/Top Secret: Security Systems	➡	SMF 80	Access & Authentication
JOBs: Batch Workloads	➡	SMF 30	Workload Execution
TCP/IP and FTP: IP & File Transfer Protocol	➡	SMF 118, 119	IP & File Transfer Activity
Other Systems Components & Vendor Products	➡	Other	Other SMF Record Types

SMF records logged by various system components and processes

4. Splunk®

Splunk® is the world's first Data-to-Everything Platform designed to remove the barriers between data and action, so that everyone thrives in the Data Age. We are empowering IT, DevOps, and security teams to transform their organizations with data from any source and on any timescale.

To manage today's IT infrastructure, you need to have a single, comprehensive 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 simple to securely collect, transform, and forward log data from these traditional IBM systems to Splunk® with no need for mainframe or IBM i expertise.

5. Ironstream®

There are several platforms that helps organizations to monitor IT security and operations across the enterprise in real-time and act fast. Those platforms help to analyze the data and provided silo-based solutions. Later the organization found there are less integrity between the data and platforms.

This creates a big gap in understanding security issues and service delivery on an enterprise-wide basis for cross-platform IT services. But the major challenge is mainframes or IBM i systems are not natively supported by these modern tools.

Precisely's Ironstream® breaks down those silos, makes it easy and cost-effective for organizations to get a real-time, 360-degree view of their IT infrastructure.

Ironstream® integrates machine data from traditional IBM systems into leading IT analytics platforms for a complete picture of your IT environment to drive better decisions, faster problem resolution and more accurate troubleshooting.

6. Ironstream for Splunk®

Organizations rely on Splunk's IT analytics dashboards to manage IT operations, security, regulatory compliance, and more. But Splunk® does not integrate with mainframe and IBM i systems.

Precisely's Ironstream® is the industry's leading automatic forwarder of z/OS mainframe log data and IBM i machine data to Splunk® Enterprise.

Ironstream® was developed in partnership with Splunk® to solve the challenge of making complex mainframe and IBM i data available for true enterprise-wide analytics. It's a robust and highly scalable solution, yet lightweight and easy to configure, install, and use.

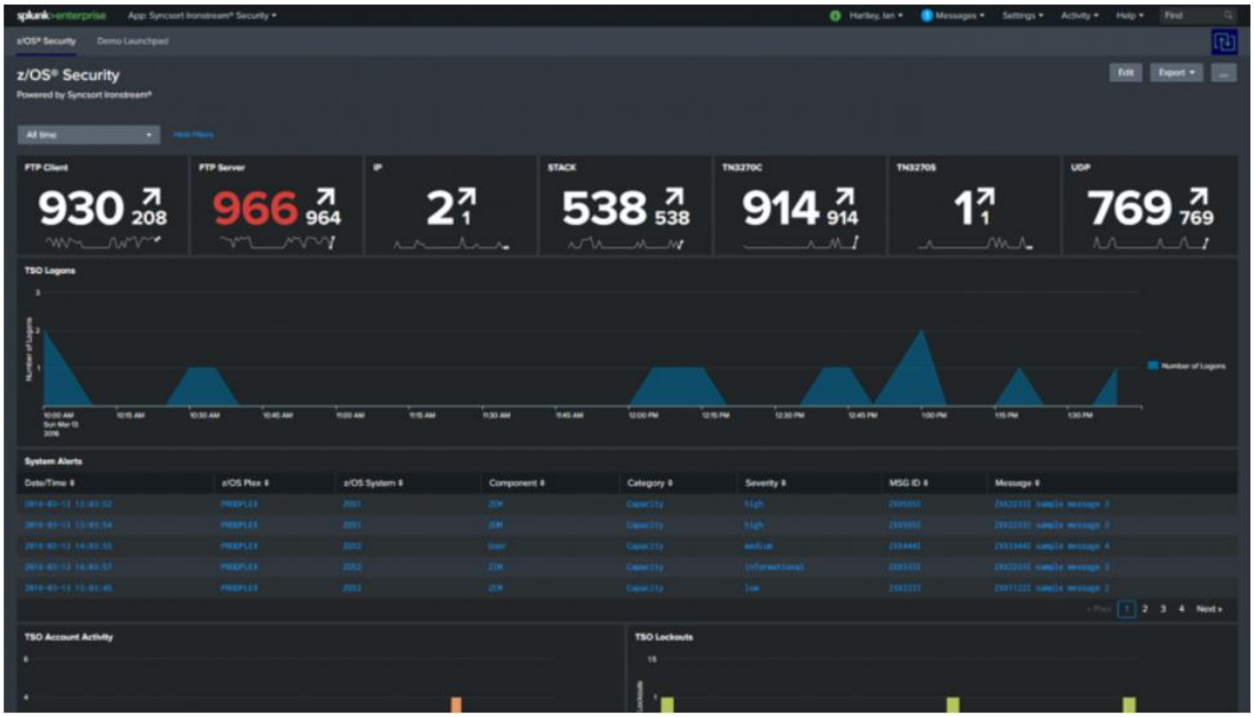
Ironstream for Splunk® provides powerful insights are at hand as users can easily search, analyze, and visualize the data from all your enterprise systems in one location.

Ironstream® seamlessly integrates the IBM mainframe and IBM i data sources to Splunk® platform and helps the organizations to perform enterprise-wide objective which includes:

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

Ironstream® continually collects security data from a wide range of IBM mainframe and IBM i sources, transforms it, and forwards it to Splunk® in real-time. You could be able to analyze the information in the context of your overall enterprise IT infrastructure.

With Ironstream for Splunk®, you can quickly and easily identify the security metrices and can keep the data for auditing purpose.



System Alerts

Date/Time	z/OS Plex	z/OS System	Component	Category	Severity	MSG ID	Message
[illegible]	PRODPLEX	[illegible]	[illegible]	Capacity	high	[illegible]	[illegible] sample message 3
[illegible]	PRODPLEX	[illegible]	[illegible]	Capacity	high	[illegible]	[illegible] sample message 3
[illegible]	PRODPLEX	[illegible]	User	Capacity	medium	[illegible]	[illegible] sample message 4
[illegible]	PRODPLEX	[illegible]	[illegible]	Capacity	informational	[illegible]	[illegible] sample message 3
[illegible]	PRODPLEX	[illegible]	[illegible]	Capacity	low	[illegible]	[illegible] sample message 2

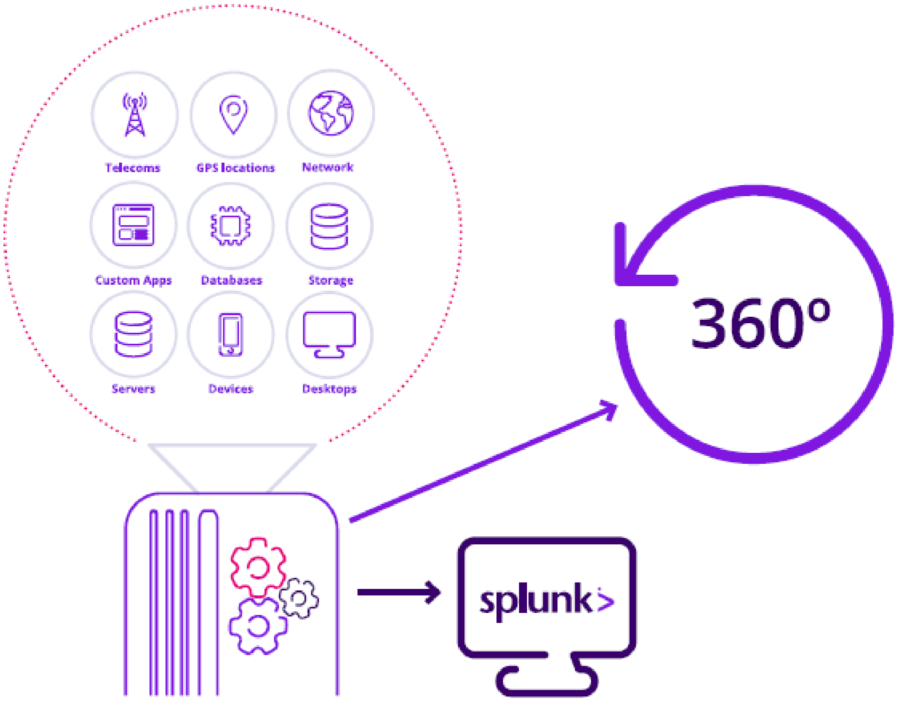
« Prev 1 2 3 4 Next »

Standard Splunk dashboard – Security Metrices

With Ironstream for Splunk®, you can focus on the most significant insights for your organization, with simple but powerful data type, subtype, and field-level filtering.

Integrating Ironstream® with Splunk® enterprise platform is a beneficial for organizations and cost-effective way to perform data analysis and to provide a complete picture of your IT environment.

With extensive support for critical IBM mainframe and IBM i data sources, Ironstream® enables organizations to keep their IT infrastructure secure and performing at its best.



Integration of Ironstream® with Splunk®

6.1 Key Features

1. Ironstream® collects various real-time data from data sources SMF (System Managed Facility) and RMF (Resource Measurement Facility). It provides insight to drive operational performance and business results in an organization.
2. It gives support for all critical IBM mainframe z/OS data sources including:
   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. Also, support for all critical IBM i data sources including:
   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. Ironstream® provides Advanced Filtering which removes the unnecessary data from the mainframes.
5. The Filtering reduces data volume and network traffic ensuring that only critical records and fields required for desired analytics and visualization are forwarded.
6. It helps the **Splunk® Enterprise Security (Splunk ES)** and **IT Service Intelligence (ITSI)** users to add more values by integrating mainframe (IBM mainframe only) data with Ironstream® and helps to get a 360-degree view of your infrastructure and eliminate blind spots.

   a) **Splunk® Enterprise Security** (Splunk ES) is a security information and event management (SIEM) solution that enables security teams to quickly detect and respond to internal and external attacks, to simplify threat management while minimizing risk, and safeguard your business.

   b) **Splunk® IT Service Intelligence (ITSI)** is an analytics and IT management solution that empowers teams to predict incidents before they impact customers. ITSI correlates and applies machine learning intelligence to data collected from monitoring sources for 360° service visibility, predictive analytics and streamlined alert management.
7. Ironstream® delivers real-time, total visibility, without the need for redundant, siloed tools, or specialized IBM mainframe or IBM i expertise.

6.2 Advantages

1. It improves IT Security and Compliance with Mainframe Data in Splunk® platform.
2. It eliminates the manual processes and inefficient tools, and optimize your infrastructure spend.
3. It eradicates the security blind spots with an enterprise-wide view.
4. Makes it easy and cost-effective to integrate machine data from traditional IBM systems into today’s IT analytic platforms.
5. It breaks down the silos and seamlessly integrates with Splunk® for a single view of all your systems, with no mainframe expertise required.

6. It provides you higher operational efficiency enabled by advanced filtering of records, utilization of zIIP processors, and data loss protection.
7. It provides you visibility into cross-platform transactions to monitor and improve IT service delivery and application performance.
8. It provides you better problem-resolution management with real-time access to data so you can act fast.
9. It provides you clearer, more precise security information with complete visibility into enterprise wide security alerts and risks for all systems.
10. Ironstream Mainframe Data Model* helps Splunk® users typically not mainframe experts – better understand mainframe logs and how to integrate them with other data for a more complete view of their IT Operations.
11. Ironstream API* enables COBOL, REXX, and Assembler applications to directly forward application data to an analytics platform for enhanced visualization of application information.
12. zIIP Processors utilized* to reduce CPU consumption and minimize overhead associated with capturing and forwarding data to analytics platforms.
13. Logstream SMF collection* enables asynchronous collection of SMF data in high transaction rate systems to ensure application performance and low latency.
14. It provides enhanced security to protect your organization from enterprise-wide security threats and incidents.
15. It provides improved operations by spot problems before they start, resolve outages quickly, and optimize infrastructure spend.

7. References

To know more about Ironstream for Splunk® refer the below mentioned links:

1. About Ironstream®
2. Ironstream® IBM
3. Mainframe Machine Data: SMF and RMF Data
4. About Splunk®
5. Ironstream for Splunk® and Product Sheet
6. IBM Mainframes
7. Splunk® Enterprise Security (Splunk ES) and Splunk® ES Product Brief
8. Splunk® IT Service Intelligence (Splunk ITSI) and Splunk® ITSI Product Brief
9. IT Security in Splunk®
10. Customer Stories - Ironstream for Splunk®
11. Webcast - Ironstream for Splunk®
12. Syncsort
13. Syncsort Ironstream for Splunk®
14. Precisely-Syncsort
15. Reference Videos: Ironstream® Splunk®