Gaining visibility into an SAP Basis environment

You work for a large, multinational corporation that uses SAP to manage its business manufacturing and logistical processes. Your job is to manage the performance, operational excellence, and security of the SAP implementation. However, getting the information you need from inside the SAP Basis environment is a difficult challenge.

Previous attempts to solve this challenge have been expensive, complicated and ultimately ineffective. In addition, there are significant challenges to understanding the connections between the closed SAP Basis environment and the supporting operating system, network, database, and other technologies, like virtualization. You are looking for a fresh approach to help your organization be successful in using this tool.

You can use Splunk to gain visibility into both SAP and its supporting infrastructure to understand what's working and what needs attention. You can get a combined view of SAP and its supporting infrastructure for monitoring performance, detecting SAP and infrastructure configuration changes, monitoring SAP and infrastructure processes, automating supporting workflow processes, and monitoring the effect of any changes you make.

Prerequisites

- PowerConnect© for SAP & Splunk
- Data sources onboarded depend on the SAP Modules you have implemented in PowerConnect© for SAP & Splunk.

How to use Splunk software for this use case

You can use Splunk software in many different ways to extract necessary data from SAP Basis and from the supporting infrastructure.

- Security & Compliance
  - SAP Security Essentials
    - Out of the box audit reports
    - Track user authentication activity with location
    - System logs
  - Insights Provided
    - Successful and failed user logins
    - Geographic view of system usage
    - Anomalies in system log, for example, increased message frequency
    - UI details, for example, versions
- Processes Monitoring
- SAP Data Analyzed
  - Batch job execution
  - IDoc and change documents processing
  - PI/PO message – payload, logs
  - BI process chains
  - Number range
- Insights Provided
  - Status of critical business processes
  - Business process context via IDoc content, e.g. sales data or PO without PR
- Solution Performance
  - SAP Data Analyzed
    - SAP transaction STAD
    - Work process utilization
    - SAP server availability
    - JVM load and memory
  - Insights Provided
    - Real-time and historic view of load and response by user, transaction code, or any field in the dataset
    - Availability of SAP solution components
- SAP HANA
  - SAP Data Analyzed
    - HANA SQL Queries collection
    - HANA health and consistency checks
  - Insights Provided
    - HANA database status
    - Real-time and historic performance data
- Supporting Technologies
  - Infrastructure Information Analyzed
    - DB
    - OS
    - Network
    - Virtualization Layers
    - SAP supporting applications from partner vendors
    - All supported by existing Splunk solutions
  - Insights Provided
    - Factual understanding of performance bottlenecks (Infrastructure or SAP)
    - Faster time to mitigate problems with a complete view of the entire SAP environment
Next steps

To maximize their benefit, the concepts in the previous section likely need to tie into existing processes at your organization or become new standard processes. The following people and departments might influence your success with this use case:

- SAP Center of Excellence or SAP Shared Services
- CI, CTO, CISO, or CFO
- VP of Applications or Director of IT
- Director of Business Systems Resiliency
- Manager, Operations Control Center

Measuring impact and benefit is critical to assessing the value of Splunk software and PowerConnect on your SAP implementation. The following are example metrics that can be useful to monitor when implementing this use case:

- SAP downtime: The ability to predict outages more consistently and the overall impact and costs to the business of those outages
- P1 (emergency) and P2 (critical) issues: A reduction in these events and a faster MTTR when they do occur
- Costs associated with root cause analyses: Less cost associated with conducting post-incident analysis
- Resource costs: A reduction in staff costs by giving them a tool that they can more easily use to extract data, as well as a reduction in additional resource expenses, such as war room costs
- Successful SAP MTTD and MTTR reducers:
  - Notifications and alarms due to event storms and noise
  - SAP batch job monitoring and alerting
  - SAP integration document monitoring and alerting
  - QRFC, TRFC, iDoc
  - End to end integration monitoring
  - Problem identification and alerting across SAP and associated applications
  - SAP number range monitoring and alerting
  - SAP System performance monitoring
  - SAP dump analysis and alerting
  - SAP table lock analysis and alerting
  - SAP security auditing and alerting
  - SAP tcode end user experience monitoring and alerting

These additional Splunk resources might help you understand and implement this use case:

- Conf Presentation: AIOps with Splunk
- Conf Presentation: How 3M is transforming SAP ERP operations through AIOps
- Blog: Splunking SAP and turning data into action
- Video: SAP PowerConnect for Splunk
- Tech Talk: Harness the power of machine learning: Driven monitoring and reporting in your SAP infrastructure

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.