# Transforming ERP Monitoring: Splunk's successful integration of SAP monitoring with PowerConnect

Keith Hontz Global Head of SAP Alliance at Splunk

**Stephen Bangs SAP Solutions Specialist at SoftwareOne**  Las Vegas

2024



1 SAPinsider

# What We'll Cover

- Executive welcome and introductions
- Product overview
- Customer success
- Q&A



# **Executive Welcome and Introductions**



Stephen Bangs SAP Solution Specialist SoftwareOne



Keith Hontz Global Head of SAP Alliance Splunk

# Follow the SAP and cloud pioneers

# 500+

SAP and cloud certified consultants with an average of 15+ years of industry experience serving 30+ countries



600+

SAP client projects with 150+ successful SAP to cloud migrations, SAP S/4HANA conversion engagements,

and RISE with SAP engagements

# 7+ years

of extensive experience in delivering SAP on cloud (Azure, AWS, GCP)

24/7 support in 13 languages 30+

**JUT** countries with local SAP presence

# SAP+

licensing & commercial advisory expertise, covering entire product lifecycle from business need to purchase, adoption and on-going management including negotiation assistance and audits preparation and remediation

# How we help clients achieve their goals



One team and a combined services offerings portfolio to address our clients' business challenges

- SAP on cloud expertise since 2015 (Azure, AWS, GCP)
- 100+ SAP to cloud migrations
- Dual certification SAP and cloud
- Advanced SAP on Azure specialisation
- AWS SAP migration competency

- FinOps
- Contract negotiation
- SAP licensing audits
- Indirect licensing
- BTP licensing
- ECC to SAP S/4HANA license conversion
- operating model
  - RISE with SAP licensing optimisation
    - RISE with SAP or

SAP scopeRISE with SAP

Understand RISE with

- cloud-native
- RISE with SAP authorised resellers

- Prepare SAP S/4HANA conversion
- Expose issues
- Inform preparation program of work
- Experiment SAP S/4HANA on cloud
- Working test and demo environment

- Automate operations
- Unique monitoring solution
- Optimisation across SAP and cloud: technical & commercial



# **SAP Operational and Organizational Changes**





# **Splunk: The Unified Security and Observability Platform**



#### Gartner

Splunk is the only vendor recognized as a leader in the latest Magic Quadrant<sup>™</sup> Reports for SIEM and APM and Observability



GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.



# **PowerConnect Use Cases**

| Business Service<br>Insights | Performance & User<br>Experience | Migrations & Upgrade   | Security & Compliance     | Cloud & SaaS App<br>Observability |
|------------------------------|----------------------------------|------------------------|---------------------------|-----------------------------------|
| E2E process monitoring       | Root Cause Analysis              | Baseline All metrics   | User Behavior Analytics   | Cloud Security                    |
| Cross-System Data validation | End-User Experience              | Comparative monitoring | Automated Audit Reporting | Observability                     |
| Business Process Monitoring  | Correlation to infrastructure    |                        | Access Monitoring         | Authentications                   |
|                              |                                  |                        | Threat Correlation        | Integrations                      |
|                              |                                  |                        |                           | Events Processes                  |

# **Business Service Insights**

#### **Benefits to Business**

- Track integration flows end-to-end between SAP and non-SAP systems
- Provide business context required to prioritize and resolve errors
- Identify if business impact is related to underlying technology or business process

#### **Use Case Examples**

- Outbound Deliveries
- iDoc Error Routing using Business Content
- Batch Jobs
- Web Services
- Number Ranges
- PI/PO Messages
- CPI iFlows

| Outbound D        | Delivery N     | <i>I</i> onitor        |           |               |             |                         |                 |            |                 |                        |          |          |            |          |              | Ð        | tractor Status :       | Edit      | Expor | t 🕶 📖     |
|-------------------|----------------|------------------------|-----------|---------------|-------------|-------------------------|-----------------|------------|-----------------|------------------------|----------|----------|------------|----------|--------------|----------|------------------------|-----------|-------|-----------|
| Range             |                | SAP System             |           | Deliver       | y number    | Name                    | e-of-ship-party | St         | пр То           | N                      | laterial |          | Plant      |          |              | Descript | ion                    |           |       |           |
| Last 24 hours     | •              | ID8                    | • ×       | •             |             |                         |                 |            |                 |                        |          |          |            |          |              |          |                        |           |       |           |
|                   |                |                        |           |               |             |                         |                 |            |                 |                        |          |          |            |          |              |          |                        |           |       |           |
|                   |                |                        |           |               |             |                         |                 |            |                 |                        |          |          |            |          |              |          |                        |           |       |           |
|                   |                | Picking                |           | 1             | Pi          | cking                   |                 | ۵.         | L               | .oading                |          |          |            | Goods    | lssue        |          |                        | Transport | ation |           |
|                   |                |                        |           |               | Co          | onfirmation             |                 |            |                 |                        |          |          |            |          |              | VS I     |                        | Planning  |       |           |
|                   |                | _                      |           |               |             |                         |                 |            |                 |                        |          |          | 00         |          |              |          |                        |           |       |           |
|                   | 55             |                        |           |               | - 7         |                         |                 |            | 476             |                        |          |          | -23        | 5        |              |          | Л                      | 76        |       |           |
|                   |                | -                      |           |               |             | •                       |                 |            |                 |                        |          |          |            |          |              |          | - 4                    | -70       |       |           |
|                   |                |                        |           |               |             |                         |                 |            |                 |                        |          |          |            |          |              |          |                        |           |       |           |
| "Picking" Details |                |                        |           |               |             |                         |                 |            |                 |                        |          |          |            |          |              |          |                        |           |       |           |
| Delivery          |                |                        | Item      | Material      | Material    | Name of the             | Number of       | Overall WM | Pick            | Picking Date           | Plant    | Priority | Processing | Quantity | Ship To      | Shipping |                        | Total     | Unit  | Weight    |
| Number 🗘 🛛        | Description \$ | GI Date 🗢              | Number \$ |               | Available 🗘 | ship-to party 🗢         | items ¢         | status 🗢   | Confirmation \$ |                        |          |          | Time 🗘     |          |              | Point ¢  | Time 🕈                 | Weight \$ |       | Unit ¢    |
| 0080018066        | Schmieröl      | 2020-04-16             | 888918    | T-BW20-       | 20220420    | Software                |                 |            |                 | 2020-04-14             | 1000     |          |            | 3.000    |              | 1000     | 2024-03-06             | 3.600     |       |           |
|                   |                | 00:00:00               |           | 28            |             | Systeme Gmb             |                 |            |                 | 88:00:00               |          |          |            |          | L63B07       |          | 09:12:52               |           |       |           |
| 0080018066        |                | 2020-04-16<br>00:00:00 | 666666    |               | 66666666    | Software<br>Systeme Gmb |                 |            |                 | 2020-04-14<br>00:00:00 |          | 02       | 0          | 8        | T-<br>L63B07 | 1000     | 2024-03-06<br>09:12:52 | 3.600     |       | KG        |
| 0080018065 L      | Lagerträger    | 2022-01-25             | 000010    | T-8W05-       | 20220121    | Software                | 9               |            |                 | 2022-01-21             | 1000     | 02       | 9          | 5,000    |              | 1000     | 2024-03-06             | 11,000    |       | KG        |
|                   |                | 80:00:00               |           |               |             | Systeme Gmb             |                 |            |                 | 88:88:88               |          |          |            |          | L63B07       |          | 09:12:52               |           |       |           |
| 0080018065        |                | 2022-01-25             | 000000    |               | 0000000     | Software                |                 |            |                 | 2022-01-21             |          |          |            |          |              | 1000     | 2024-03-06             | 11.000    |       |           |
|                   |                | 00:00:00               |           |               |             | Systeme Gmb             |                 |            |                 | 00:00:00               |          |          |            |          | L63B07       |          | 09:12:52               |           |       |           |
| 0080018064 L      | Lagerträger    | 2020-04-16<br>00:00:00 | 000010    | T-BW05-<br>20 | 20211229    | Software<br>Systeme Gmb | 0               |            |                 | 2020-04-14<br>00:00:00 | 1000     | 02       | 0          | 4.000    | T-<br>L63B07 | 1000     | 2024-03-06<br>09:12:52 | 8.800     | ST    | KG        |
| 0080018064        |                | 2020-04-16             | 000000    |               | 0000000     | Software                |                 | A          |                 | 2020-04-14             |          | 02       | 9          | 0        |              | 1000     | 2024-03-06             | 8,800     |       | KG        |
|                   |                | 80:00:00               |           |               |             | Systeme Gmb             |                 |            |                 | 00:00:00               |          |          |            |          | L63B07       |          | 09:12:52               |           |       |           |
| 0080018040 E      | Druckdeckel    | 2019-04-26             | 000010    | T-8W04-       | 20190426    | Hallmann                |                 |            |                 | 2019-04-26             | 1000     |          |            | 5.000    |              | 1000     | 2024-03-06             | 9.000     |       |           |
|                   |                | 00:00:00               |           | 28            |             | Anlagenbau              |                 |            |                 | 00:00:00               |          |          |            |          | L69A19       |          | 09:12:52               |           |       |           |
| 0080018040        |                | 2019-04-26<br>00:00:00 | 000000    |               | 0000000     | Hallmann<br>Anlagenbau  |                 |            |                 | 2019-04-26<br>00:00:00 |          | 01       | 0          | 0        | T-<br>L69A19 | 1000     | 2024-03-06<br>09:12:52 | 9.000     |       | KG        |
| 0080018032 H      | High Speed     | 2019-05-06             | 000010    | T-ATT11       | 20190502    | Compu-Soft              | 9               |            |                 | 2019-05-02             | 1200     | 02       | 9          | 7.000    |              | 1201     | 2024-03-06             | 7,700     |       | KG        |
| E                 | Basic          | 80:00:00               |           |               |             |                         |                 |            |                 | 00:00:00               |          |          |            |          | S66D24       |          | 09:12:52               |           |       |           |
| 0080018032        |                | 2019-05-06             | 886668    |               | 0000000     | Compu-Soft              |                 |            |                 | 2019-05-02             |          |          |            |          | T-           | 1201     | 2024-03-06             | 7.700     |       |           |
|                   |                | 00:00:00               |           |               |             |                         |                 |            |                 | 00:00:00               |          |          |            |          | 566024       |          | 09:12:52               |           |       | D. Newton |
|                   |                |                        |           |               |             |                         |                 |            |                 |                        |          |          |            |          |              |          | 2345                   | 6 / 8     | 9 10  | J Next »  |

# **Solution Performance**

#### **Benefits to SAP Performance**

- Provide the necessary context to resolve root cause with alerts
- Automate manual health checks
- Correlate multiple components of SAP application and infrastructure in single location
- Create any alert based on full fidelity data provided
- Anomaly detection based on historical telemetry and machine learning

#### **Use Case Examples**

- End User Experience Monitoring (STATS)
- Work Process Utilization (SM51)
- RFC Connection Status (SM59)
- Gateway Utilization and Logs (SMGW)
- JVM Load and Memory



Out-of-the-box content driven by **208 SAP transactions** including SM04, ST03, SM51, SM58, SMC1, SMQ1, ST22, STAD, STATS, SMGW, +++

# **SAP Breaches Create Material Risk**



SAP applications are constrained by historical data parameters and Security datasets are only available for a short period of time. Splunk enables historical analysis and correlation across multiple environments and timeframes to create proactive alerts and mitigate risks before fraud or security breaches occur

# **SAP Cloud Migrations and Upgrades**



## **PowerConnect ABAP & Java Architecture**



# **PowerConnect SAP Cloud Architecture**

SAP SaaS & PaaS

SAP Cloud Platform SAP Cloud Platform Integration SAP Business Technology Platform SAP API Management SAP Sales Cloud / CPQ SAP SuccessFactors SAP Ariba SAP Fieldglass



# splunk > cloud



# splunk>enterprise



# **PowerConnect is 100% Certified**

#### 15 SAP certifications ensure compatibility with SAP products

- SAP certified for SAP S/HANA cloud 2023 extended edition
- SAP certified for SAP S/HANA cloud 2023 (RISE + HEC)
- SAP certified for SAP S/HANA cloud 2022 extended edition
- SAP certified for SAP S/HANA cloud 2022 (RISE + HEC)
- SAP certified for SAP S/HANA cloud 2021 (RISE + HEC)
- SAP certified for SAP S/HANA cloud 1909 (RISE + HEC)
- SAP certified for SAP S/4HANA 2021
- SAP certified for SAP S/4HANA 2020
- SAP certified for SAP S/4HANA 1909
- SAP certified for SAP S/4HANA 1809
- SAP certified for SAP S/4HANA 1709
- SAP certified for SAP S/4HANA 1609
- SAP certified for SAP NetWeaver 7.5 ABAP
- SAP certified for SAP NetWeaver 7.5 ABAP add-on deployment
- SAP certified for SAP NetWeaver 7.5 Java







**SAP**<sup>®</sup> Certified Powered by SAP NetWeaver<sup>®</sup>

**SAP**<sup>®</sup> Certified Integration with SAP S/4HANA<sup>®</sup> Cloud

**SAP** Certified Integration with SAP S/4HANA

# **Customer Success**

10+ Years in Market with 5K+ Installations with Customers in 24 Countries



# **PowerConnect Case Study: Outbound Delivery Processing**

#### **Industry: Consumer Product Goods**

#### **Problem Statement**

- No method to track end-to-end processing time
- No capability to track and alert on delays in delivery processing

#### Approach

- PowerConnect data used to extract message payload from PI/PO
- Message payload details used to map the endto-end business process at a delivery level
- Provides better visibility to potential processing slowdowns, and trends per distribution center

#### **On-Time Delivery Distribution**

- Alerts sent to business and IT if deliveries didn't abide by SLAs
- Bottlenecks in the outbound delivery process identified based on processing times for individual steps

| Stopped Car Routin<br>Last N Freight Orders<br>5 | E<br>Events Updated in the Last:<br>24 hours. |                         |   |  |                |                   | Ex                         | port *                |
|--|---|-------------------------|---|--|----------------|-------------------|----------------------------|-----------------------|
|  |   |                         |   | Select a Plant                           | • All •        | ×                 |                            |                       |
| AVG Time in Minutes                              |   |                         |   | Total Time Bigger Than 3                 | 20 Minutes     |                   |                            |                       |
| -  |   |                         |   | Last Update ¢                            | Alarms ‡       |                   | Total Time<br>÷            | Completed<br>a        |
|  |   |                         |   | 1 2823-12-26<br>13:51:24                 | States in case |                   | 22m 53                     |                       |
| 2  | 2<br>PalishPor                                | NPC Network to NPAction |   |  |                | Quality of Qrs: 1 |                            |                       |
|  |   |                         |   |  |                |                   | <b>A</b> + <b>B</b>        | oge mt>               |
| AVG Time by Plant in Minutes                     |   |                         |   | Total Time Bigger Than 1                 | 10 Minutes     |                   |                            |                       |
| 4  | 2   |                         |   | Last Update \$<br>2623-12-26<br>11:51:29 | Attention #    |                   | Total Time<br>e<br>18e 28s | Completed<br>•<br>YES |
|  | 2.  | 5                       | 3 |  |                |                   |                            |                       |

# **PowerConnect Case Study: End-to-End Pricing Call Performance**

#### **Industry: Manufacturing**

#### **Problem Statement**

- Customers abandoning their shopping cart because of long-running pricing calls from the e-commerce platform to the back-end SAP system
- No method to identify which application was causing performance bottleneck

### Approach

- End-to-end dashboard created correlating individual pricing calls between the customer's ECC/PO/Hybris environments
- Proactive alerts sent if pricing call performance deteriorated
- Automatic incidents routing to responsible team using statistical thresholds

#### **Permanent Changes to Architecture**

- The existing architecture was reworked based on the pattern of pricing call performance degradation
- The ABAP program responsible for the pricing call
   was modified to improve performance
- Customer satisfaction scores improved as a result for the e-commerce website.



# **PowerConnect Case Study: Material Pricing Reconciliation**

#### **Industry: Retail**

#### **Problem Statement**

- Daily pricing updates transmitting the pricing updates from SAP to a SIDECAR database, and afterwards to the cash registers
- The customer had multiple failing points along the process and was unaware of where the pricing changes were getting lost

#### Approach

- Dashboard created to reconcile the prices transmitted by SAP via iDoc with the recipient system
- Proactive alerts created informing IT and business teams of reconciliation mismatches

#### **Improved Material Pricing Accuracy**

- Reconciliation of the transmission of prices between the SAP and non-SAP systems ensures that the price at the cash register is accurate for the retail customers
- Accurate pricing directly impacts gross profit margin for the business

| Time Range<br>Last 24 hours + | System<br>ECP       | • ×     | Hide Filters |          |                   |                   |         |                   |         |            |            |         |                   |                       |
|-------------------------------|---------------------|---------|--------------|----------|-------------------|-------------------|---------|-------------------|---------|------------|------------|---------|-------------------|-----------------------|
| IDoc Completion               |                     |         |              |          |                   |                   | SID     | ECAR Match        |         |            |            |         |                   |                       |
|                               |                     | 10      | 00.0         | 00 %     |                   |                   |         |                   |         |            | No results | found.  |                   |                       |
| IDoc Statuses                 |                     |         |              |          |                   |                   | SID     | ECAR Counts       |         |            |            |         |                   |                       |
| SAP IDoc Status #             |                     |         |              |          | Count # Percent # |                   | Visi    | ble in SIDECAR? 0 |         |            |            |         | Count #           | Percent #             |
|                               |                     |         |              |          | 5 100.00%         |                   |         | Found             |         |            |            |         |                   | 100.005               |
|                               |                     |         |              |          |                   |                   |         |                   |         |            |            |         |                   |                       |
| Overview<br>SAP Status<br>ALL | Visible in SIDECAR? |         |              |          |                   | Q . I O 3ma       | 90      |                   |         |            |            |         |                   |                       |
| Not Successful                | Not Found           |         |              |          |                   |                   |         |                   |         |            |            |         |                   |                       |
| SAP IDoc Number #             | VTWEG 0             | WERKS 0 | KSCHL 0      | DATBI #  | DATAB 0           | MATNR 0           | KZUST Ø | VKORG 0           | KBETR 0 | KNUMH 0    | KOTABNR 0  | KAPPL # | SAP IDoc Status # | Visible in SIDECAR? 0 |
| 0000001811056742              |                     |         |              |          |                   | 00000000001824595 |         |                   |         |            |            |         |                   |                       |
| 0000001811056744              |                     | 0578    | VKP0         | 20240205 | 20231214          | 00000000001024595 | 010     | HERC              | 38.10   | 4495341226 |            |         | Successful        | Nat Found             |
| 000001811056741               |                     |         | VICPIE       | 99991231 | 20240215          | 00000000001024595 |         | HERC              |         | 4495341226 |            |         | Successful        |                       |
| 0000001811056743              |                     | 9578    | VICPO        | 20248208 | 20240208          | 00000000001024595 | 010     | HERC              | 38.99   | 4495341226 | 071        |         | Successful        | Not Found             |
| 000001811056745               |                     |         |              |          |                   | 00000000001024555 |         | HERC              |         | 4495341226 |            |         |                   |                       |

# **North American Implementation Partner: RHONDOS**



- First-line 24/7 P1 Support
- Certified Implementation Services
- On-Demand SAP Monitoring Experts







- Reduced SAP Monitoring Costs by **50%**
- Expedited Compliance Audits
- Enhanced SAP Security Posture
- Reduced MTTR & RCA by 70%
- Eliminate 30% of P1/P2 Tickets

# Splunk Runs SAP Globally



# Splunk's Landscape



# SAP & Integration Applications Monitoring in the Splunk Observability Platform – Availability Dashboard

| splunk>    | Dashboards<br>FinTech Site Avail | ability / | Solution Overview                                  |   |                                 |                          |                               |               | Q +   | Д |
|------------|----------------------------------|-----------|--|---|---------------------------------|--------------------------|-------------------------------|---------------|-------|---|
|            | FinTech Site Avail               | ability   | ••• EXECUTIVE OVERVIEW S                           | COMPONENT OV                              | ERVIEW                          |                          |                               |               |       | 1 |
| م<br>م     | Override                         | s: Con    | ponent onesource-login, hana, 11 more ×            | Vendor thomson-reuters, sap, 2 more ×     | Solution payments, taxes, erp × | Environment production × | Owner FinTech × Filter Option | a/ Save F     | Reset |   |
| ឹ          |                                  |           |  |   |                                 | Time -1d                 | Chart resolution 💮 👻          | Event overlay |       |   |
| E,         | Availability Tre                 | ends by s | solution   component   🌼 🚥                         | Current Availability by solution   compor | nent   environment 1m           |                          |                               |               | ф ··· |   |
| <b>—</b>   | 1                                | 00        | erp   digital-payments  <br>production             |   |                                 |                          |                               |               |       | ľ |
| (!)        |                                  | 00        | erp   cloudhub-cm-ffpsa  <br>production            |   |                                 |                          |                               |               |       |   |
| Ů          | 1                                | 00        | erp   ariba   production                           |   |                                 |                          |                               |               |       |   |
| 87         | 1                                | 00        | erp   hana   production                            | erp                                       |                                 |                          | taxes                         |               |       |   |
| Ē          | 1                                | 00        | erp   concur   production                          | ariba                                     | cloudhub-cm-ecomm               | digital-payments         | onesource-login               | onesource-tax |       |   |
| 1          | 1                                | 00        | erp   cloudhub-cm-<br>ecomm   production           |   | -                               | -                        |                               |               |       |   |
| ¢ <b>3</b> | 1                                | 00        | erp   web-dispatcher  <br>production               | cloudhub-cm-ffpsa                         | concur                          | fiori                    | payments                      |               |       |   |
|            | 1                                | 00        | erp   fiori   production                           |   | _                               | _                        | stripe-payments-api           |               |       |   |
|            | 1                                | 00        | erp   multi-bank-<br>connectivity   production     | hana                                      | multi-bank-connectivity         | web-dispatcher           |                               |               |       |   |
|            | 1                                | 00        | payments   stripe-<br>payments-api  <br>production |   |                                 |                          |                               |               |       |   |
|            | 1                                | 00        | taxes   onesource-tax  <br>production              |   |                                 |                          |                               |               |       |   |
|            | 1                                | 00        | taxes   onesource-login  <br>production            |   |                                 |                          |                               |               |       |   |

# SAP & Integration Applications Monitoring in the Splunk Observability Platform – Response Time Dashboard



# SAP & Integration Applications Monitoring in the Splunk Observability Platform – Alerts/Detectors

| splunk>   | Alerts<br>Detectors  |  |                     | ۹ + ۲        |
|---|--|--|---------------------|--------------|
| ()<br>()<br>()<br>()<br>()<br>()<br>()<br>()<br>()<br>()<br>()<br>()<br>()<br>( | Get the Most Out of Alerts         Get alerted when cirtical issues arise. Splunk Observability Cloud helps you respond to problems in seconds.         Documentation C Developer docs C | Image: Create a Detector to get Allerted     →   | Getting Notified    |              |
| (!)<br>•  | Filter <b>I sf_severityMajor</b> × + Group By None Team  | FinTech         APM Filters         Any Service/Endpoint         Any Business Workflow         Any Environment   |                     |              |
| 67<br>67<br>68  | Search detectors   | All detectors •<br>1 29 0 0 0<br>1 Critical 29 Major Minor Warning Info  |                     | New Detector |
|   | Detector   | Active Alerts  | Duration            |              |
|   | > FinTech production erp ariba availability alert  | 0000   |                     |              |
|   | > FinTech production taxes onesource-tax availability alert  | 0 0 0 0 0  |                     |              |
|   | > FinTech production erp concur availability alert   |  |                     |              |
|   | <ul> <li>FinTech production erp fiori availability alert</li> </ul>  |  |                     |              |
| >>  |  | <ul> <li>production.erp.fiori.missing-data-points.10 - FinTech GET linux https://fiori.sap.splunkopen</li> <li>production.erp.fiori.missing-data-points.10 - FinTech GET linux https://fiori.sap.splunkopen</li> </ul> | 12 days<br>3 months |              |

"BRIM has standard credit card processing. When a customer has a recently expired credit card, their account goes on block. Customer Service takes 3-4 days to resolve. Splunk for S/4 alert looks at CC expiration events, to proactively decrease our turnaround from 4 days to 10 mins."

# SAP & Integration Applications Monitoring in the Splunk Observability Platform – Critical Alert Example

| ggered 6 days ago, on 06/02/2022 at 12:46:0 | 00 PM (UTC -07:00) |       |          |           | Time 06/02/2022 06:46:00 am to 06/02/2022 06:46 |
|---|--------------------|-------|----------|-----------|---|
| ploratory view 5m                           |                    |       |          |           | Detail View Im                                  |
| 00  |                    |       |          |           | 80  |
| 60  |                    |       |          |           | 60  |
| 40  |                    |       |          |           | 20  |
| 08:00 09:00 10:00 11:0                      | 10 12:00 13:00     | 14:00 | 15:00 16 | :00 17:00 | 12:30 12:46:00 13:00                            |
| — D: (value: 0)                             |                    |       |          |           |   |

"We had an issue a few months back with GCP, our Fiori RFCs were not working and we needed to restart Fiori server. Splunk Alert Monitoring enabled us to resolve in 10 mins, versus 4 hrs in the past."

# **PowerConnect For Splunk – SAP System Overview**



Provides an overview on real-time System Availability, Background and Dialog work processes load and CPU and Memory Consumption.

# **PowerConnect For Splunk – Health Checks**



Provides an overview on some of the most important benchmarks like CPU and Memory Usage, ABAP Dumps, Dialog Response time and failed jobs etc.

# **PowerConnect For Splunk – Weekly Usage**



Weekly Total User Logins, RFC and HTTP calls made, Number of background jobs executed and total number of iDocs created can be monitored on a weekly basis.

# **PowerConnect For Splunk – Security Essentials**

| SAP Security Essentials                             |                            |                              |   |                        | Edit Export •                            |
|---|----------------------------|------------------------------|---|------------------------|--|
| Range SAP System                                    | n 🗸 Hide Pitters           |                              |   |                        | Extractor Status : 🛑                     |
|   |                            |                              |   |                        |  |
| å SAP User Behavior Ana                             | lysis 🏖 Logins, Permission | is and Change Events 📗 😤 📑   | Risk Assessment Dashboard                                     |                        |  |
| Standard users with initial well-<br>known password | Client open for change     | Namespace open for change    | Dialog users not compliant with<br>password expiration policy | Certificate Status     |  |
|   | 4                          | ~                            |   | Expired                | Soon to be expired                       |
| Ο   | 1                          | U                            | Ο   | 27                     | 0  |
|   |                            |                              |   |                        | -  |
| User type change - System to<br>Dialog              | Password expiration policy | Security Audit Log Parameter | RFC callback security mode                                    | OS commands prohibited | Logical Path Access Failed               |
| •   | Set                        | Fnabled                      | 3: Most Secure  | No                     | 0  |
| U   |                            | Enabled                      | 5. Most Secure  |                        | le l |
| Password complexity                                 |                            |                              | Unsecured external commands executed                          | (sapxpg)               |  |
| Parameter Name \$                                   |                            | Status \$                    |   |                        |  |
| Atleast one lowercase                               |                            |                              |   |                        |  |
| Atleast one special character                       |                            | 8                            |   |                        |  |
| Atleast one uppercase                               |                            |                              |   | No results found.      |  |
|   |                            |                              |   |                        |  |

Security dashboard for IT General controls which can help in monitoring the access to the SAP system and staying in compliance within the organization policies.

# **Splunk Integration With Slack – System Alerts**



Provides detailed information on audit logs Automated Slack and Email Alerts can be easily configured to be triggered at regular intervals and based on various trigger conditions, for example:

- ABAP Short Dumps Splunk query can be configured to run every 3 hours and trigger alerts if the number of dumps are more than the set threshold.
- Critical Batch Job Failure Splunk query running every 1 hour on the target system data to check if any critical batch job had failed and raise alert.
- RFC Connection Failure Splunk query configured to keep on pinging RFC destinations every minute and raise an alert if any RFC destination fails.

# **Splunk Integration With Email – System Alerts**

| nk Cioua <alerts@splunkcioua.com><br/>deloittesplunkbasis, gnallapilly, me, csawant,</alerts@splunkcioua.com>  | abhaskara, esanjeevi   | i, mkrupka 👻          |                    | 🔤 12-31AM (13 hours ago) - 🏌  |
|--|--|-----------------------|--------------------|---|
|  |  |                       |                    |   |
| 3110,  |  |                       |                    |   |
| n the past hour, one or more critical bate   | ch jobs have failed  | in the SD2 environm   | nent. For more inf | formation, please refer to the Splunk results link or the attached PDF. |
| he same alert is also published on Slad  | k channelSAP_  | SPLUNKRZ_ALERT        | S_NONPRODUC        | CTION   |
| Chetan Please coordinate and ensure  | that this issue is tr  | racked to closure thr | ough SNOW, Res     | solve, or a Slack thread.   |
| legards,   |  |                       |                    |   |
| plunk for SAP  |  |                       |                    |   |
|  |  |                       |                    |   |
| lert: SAP_ALERT_CRITICAI   | _JOBS_FAILURE  | S_NONPROD_SD2         |                    |   |
| lert: SAP_ALERT_CRITICAI<br>rigger Time: 19:01:33 +0000 on Sep   | L_JOBS_FAILURE   | S_NONPROD_SD2         |                    |   |
| lert: SAP_ALERT_CRITICAI<br>rigger Time: 19:01:33 +0000 on Sep   | L_JOBS_FAILURE   | S_NONPROD_SD2         |                    |   |
| lert: SAP_ALERT_CRITICAI<br>rigger Time: 19:01:33 +0000 on Sep<br>iew results in Splunk  | L_JOBS_FAILURE:<br>tember 20, 2023.  | S_NONPROD_SD2         |                    |   |
| lert: SAP_ALERT_CRITICAI<br>rigger Time: 19:01:33 +0000 on Sep<br>lew results in Splunk<br>JOBNAME   | L_JOBS_FAILURE:<br>tember 20, 2023.<br>JOBCOUNT ST   | S_NONPROD_SD2         | e strttime         |   |
| Iert: SAP_ALERT_CRITICAI<br>rigger Time: 19:01:33 +0000 on Sep<br>iew results in Splunk<br>JOBNAME<br>ZGRAC_SPM_WORKFLOW_SYNC  | L_JOBS_FAILURE<br>tember 20, 2023.<br>JOBCOUNT \$1<br>1030005U A   | TATUS STRTDAT         | e strttime         |   |
| Iert: SAP_ALERT_CRITICAI<br>rigger Time: 19:01:33 +0000 on Sep<br>iew results in Splunk<br>JOBNAME<br>ZGRAC_SPM_WORKFLOW_SYNC<br>ZGRAC_SPM_WORKFLOW_SYNC   | JOBS_FAILURE<br>tember 20, 2023.<br><b>JOBCOUNT S'</b><br>1030005U A<br>1030005Q A   | TATUS STRTDAT         | e strttime         |   |
| Iert: SAP_ALERT_CRITICAI<br>rigger Time: 19:01:33 +0000 on Sep<br>iew results in Splunk<br>JOBNAME<br>ZGRAC_SPM_WORKFLOW_SYNC<br>ZGRAC_SPM_WORKFLOW_SYNC<br>ZGRAC_SPM_WORKFLOW_SYNC  | JOBS_FAILURE<br>tember 20, 2023.<br>1030005U A<br>1030005Q A<br>1030005V A   | TATUS STRTDAT         | e strttime         |   |
| Iert: SAP_ALERT_CRITICAI<br>rigger Time: 19:01:33 +0000 on Sep<br>iew results in Splunk<br>JOBNAME<br>ZGRAC_SPM_WORKFLOW_SYNC<br>ZGRAC_SPM_WORKFLOW_SYNC<br>ZGRAC_SPM_WORKFLOW_SYNC  | JOBS_FAILURE<br>tember 20, 2023.<br>1030005U A<br>1030005Q A<br>1030005V A<br>1030005V A   | TATUS STRTDAT         | e strttime         |   |
| Iert: SAP_ALERT_CRITICAI<br>rigger Time: 19:01:33 +0000 on Sep<br>Iew results in Splunk<br>ZGRAC_SPM_WORKFLOW_SYNC<br>ZGRAC_SPM_WORKFLOW_SYNC<br>ZGRAC_SPM_WORKFLOW_SYNC<br>ZGRAC_SPM_WORKFLOW_SYNC                            | JOBS_FAILURE<br>tember 20, 2023.<br>1030005U A<br>1030005U A<br>1030005V A<br>1030005V A<br>1030005T A                             | TATUS STRTDAT         | e strttime         |   |
| Iert: SAP_ALERT_CRITICAI<br>rigger Time: 19:01:33 +0000 on Sep<br>Iew results in Splunk<br>ZGRAC_SPM_WORKFLOW_SYNC<br>ZGRAC_SPM_WORKFLOW_SYNC<br>ZGRAC_SPM_WORKFLOW_SYNC<br>ZGRAC_SPM_WORKFLOW_SYNC<br>ZGRAC_SPM_WORKFLOW_SYNC | JOBS_FAILURE<br>tember 20, 2023.<br>1030005U A<br>1030005U A<br>1030005V A<br>1030005V A<br>1030005V A<br>1030005T A<br>1030005R A | TATUS STRTDAT         | e strttime         |   |

•••

PowerConnect for Splunk gives flexibility to add custom text for alert messages and can notify a configurable set of users. Here in the above example of alert for critical batch job failures in the SAP system, the email has the list of failed batch jobs which can then be easily tracked.

# **Key Points to Take Home**

- Data siloes within the SAP application and across the broader IT ecosystem can impact business stability
- Monitoring tools needs to span outside of just the SAP environment
- PowerConnect and Splunk provides value across performance, security, business process, and cloud migration use cases for SAP
- Skilled service providers like RHONDOS are available to ensure solution adoption and customer success
- Splunk's use of its own platform with SAP data improved the security and performance of their SAP applications

## Where to Find More Information

How Do You Improve Visibility Into Your SAP Landscape?



Proactively Monitor SAP Systems in the Cloud



Technology Governing Technology



Additional Product Information Available at <u>www.powerconnect.io</u>

# Thank you! Any Questions?

**Keith Hontz** 

Email: <u>khontz@splunk.com</u> LinkedIn: <u>www.linkedin.com/in/keithhontz/</u>

#### **Stephen Bangs**

Email: <a href="mailto:stephen.bangs@softwareone.com">stephen.bangs@softwareone.com</a> LinkedIn: <a href="mailto:www.linkedin.com/in/bangsstephen/">www.linkedin.com/in/bangsstephen/</a> Please remember to complete your session evaluation.

# SAPinsider

#### SAPinsider.org

PO Box 982Hampstead, NH 03841 Copyright © 2024 Wellesley Information Services. All rights reserved.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. Wellesley Information Services is neither owned nor controlled by SAP SE. SAPinsider comprises the largest and fastest growing SAP membership group with more than 800,000 members worldwide.