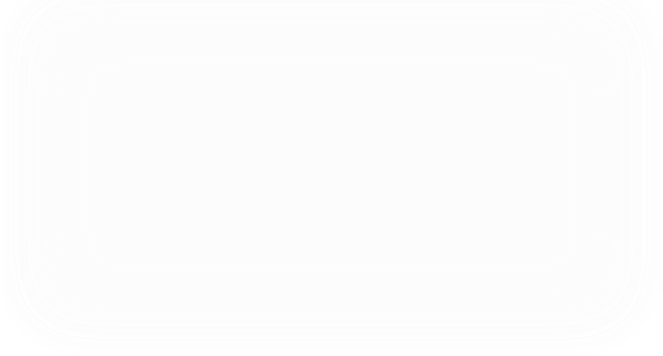


© 2022 NTT DATA, Inc. All rights reserved.



NTT and HSBC API & Core Services SRE Collaboration

Show & Tell

–

Sprint 9

7

Oct 20, 2022



Prepared by: NTT DATA

* Recap previous Show & Tell sessions
* Findings & Recommendations from previous Sprints

© 2022 NTT DATA, Inc. All rights reserved.

2



PUBLIC

Agenda

* Questions and Suggestions

© 2022 NTT DATA, Inc. All rights reserved.

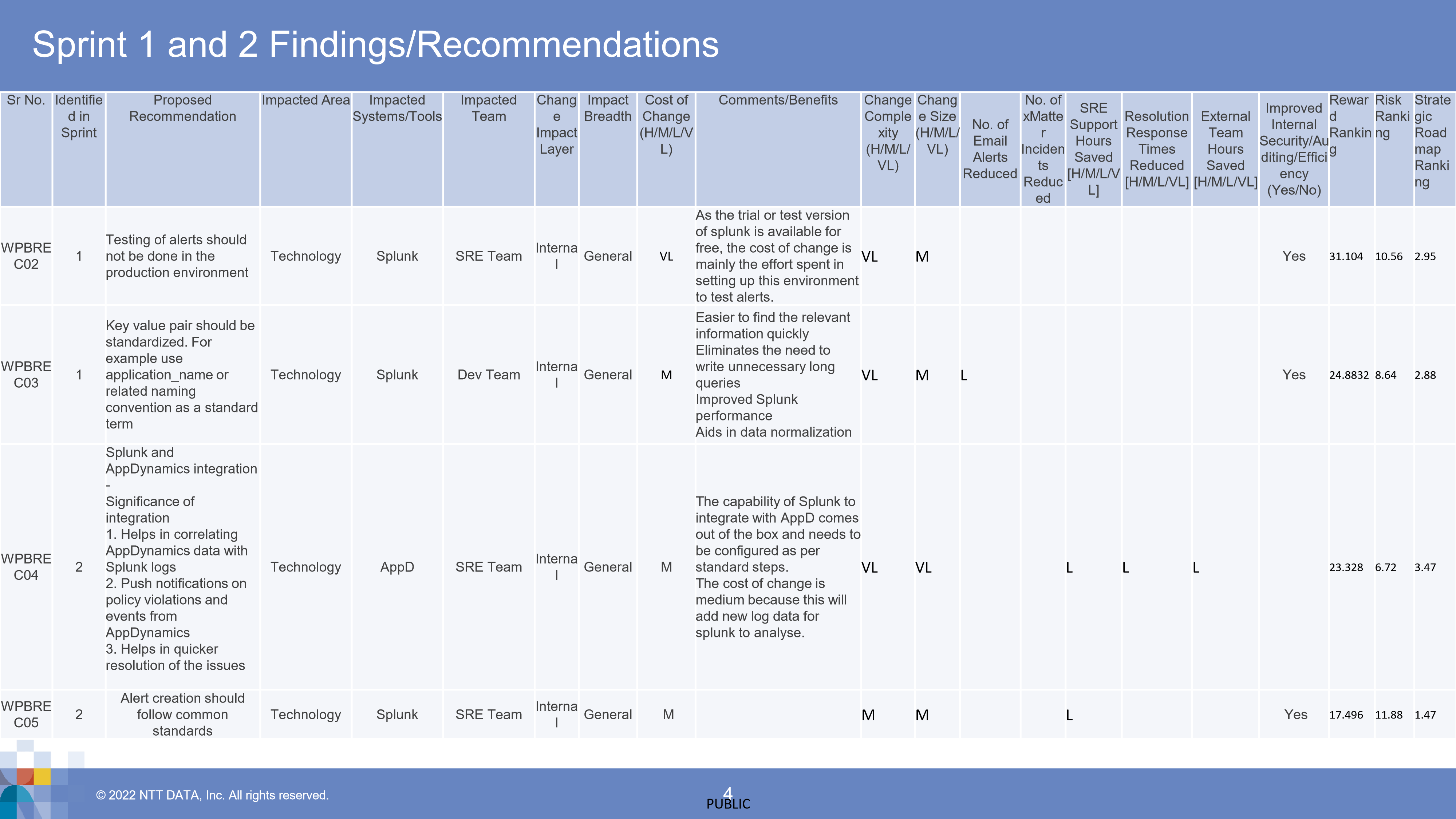
3

Findings & Recommendations

–

Previous

Sprints



© 2022 NTT DATA, Inc. All rights reserved.

5

Findings & Recommendations

–

Sprint 3

© 2022 NTT DATA, Inc. All rights reserved.

WPBREC01

-

Disabled alerts should be

removed from production environment

© 2022 NTT DATA, Inc. All rights reserved.

7

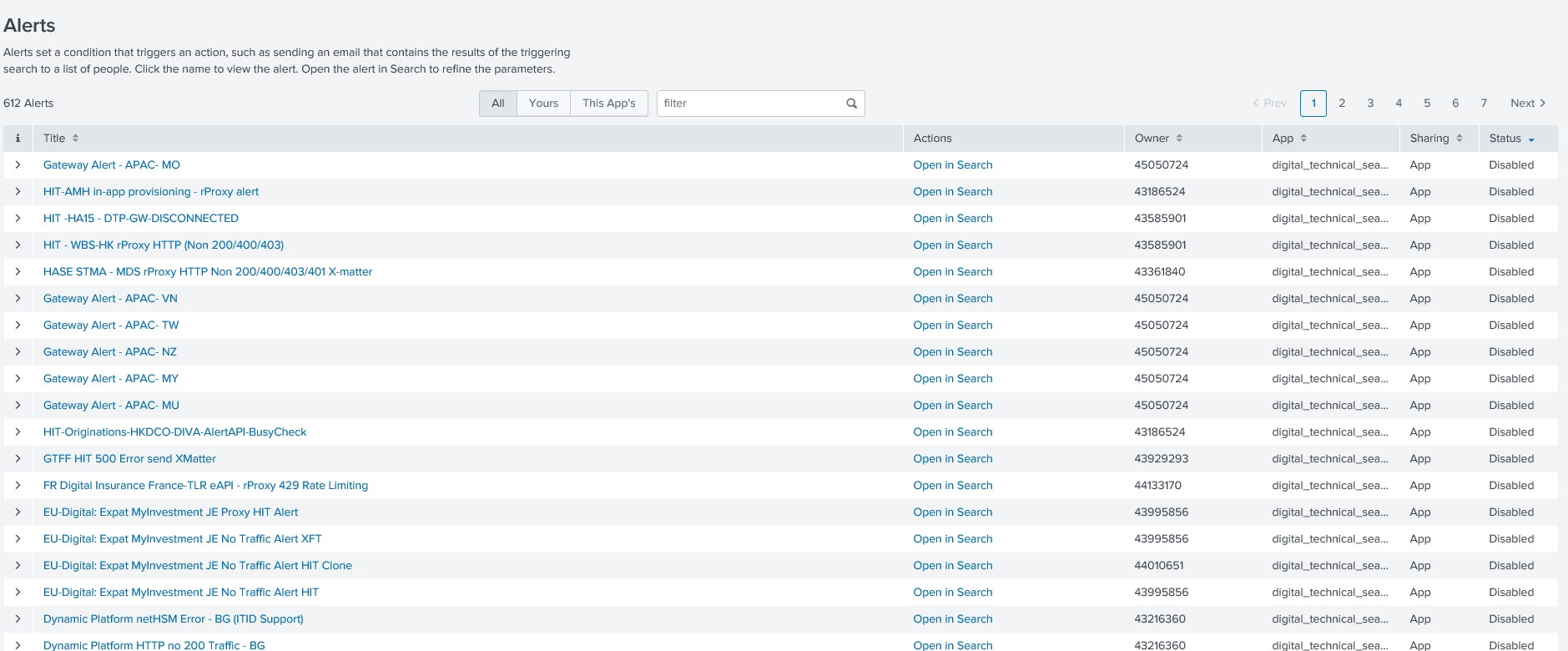


PUBLIC

Recommendation

Details

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | | | | | Issue Targeted | | | Impacted Area | Impacted Systems/Tools | Impacted Team |
| House cleansing activity for  Alerts | Disabled alerts should be removed from production environment | | | | | Best practice | | | Standards | Splunk | SRE Team |
| Comments/Benefits | | | | | |
| This will prevent accidental enablement of the alerts  Cleaner production environment | | | | | |
| Reward Ranking | Risk  Ranking | Strategic  Roadmap  Ranking | |
| 29.0304 | 4.8 | 6.05 | |



▪

**Total Splunk alerts**

-

499

UK / 611 HK / 172 US

▪

**Total Disabled Splunk alerts**

-

231

UK /226 HK / 56 US

© 2019 NTT DATA, Inc. All rights reserved.

WPBREC06

-

Logging should be part of the

acceptance criteria

Since we have lots of logs for API and Platforms, and those logs are being ingested into Splunk; so expectation is that the logging messages must be tested and should follow industry standard

When we search logs with Splunk query index=digital\_\*

Splunk result should display meaningful fields, but in reality there are around 500 fields; many of them can be avoided by writing better logs. Additional fields will unnecessarily eat up support team’s time to analyse the logs.



When we search logs with Splunk query index=digital\_\* | transaction ReqCorrelationId maxspan=30s

Result of this query should display each completed or failed transactions in a group of events for that correlation id.

But in reality multiple correlation ids are used:

correlationId

Jwt correlation Id

Session Correlation ID

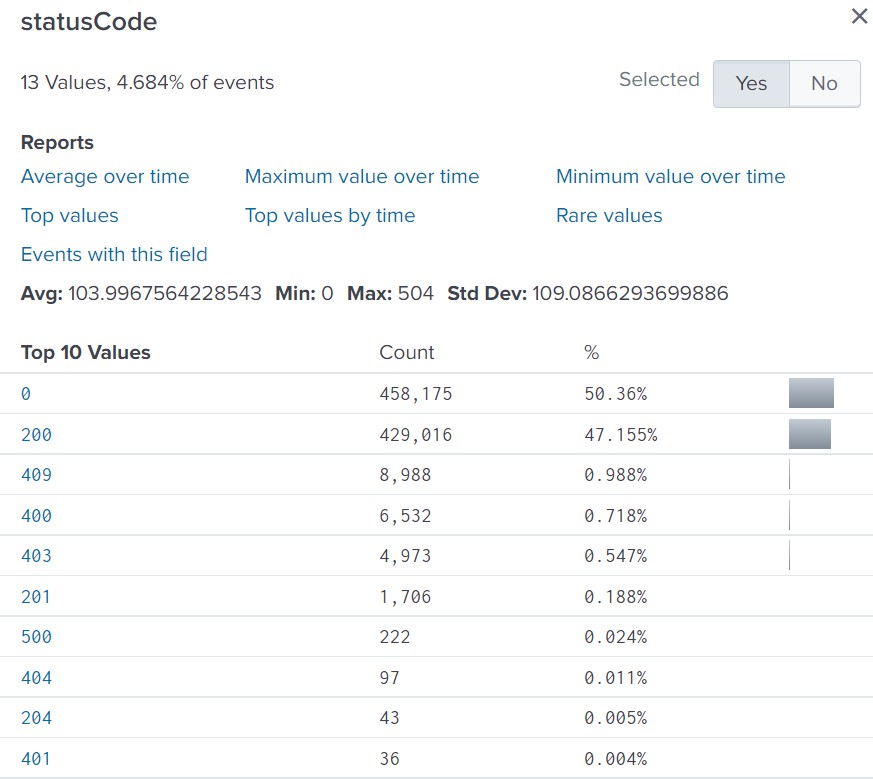
Request correlation id

X-Hsbc-Session-Correlation-Id for SESSION\_TOKEN

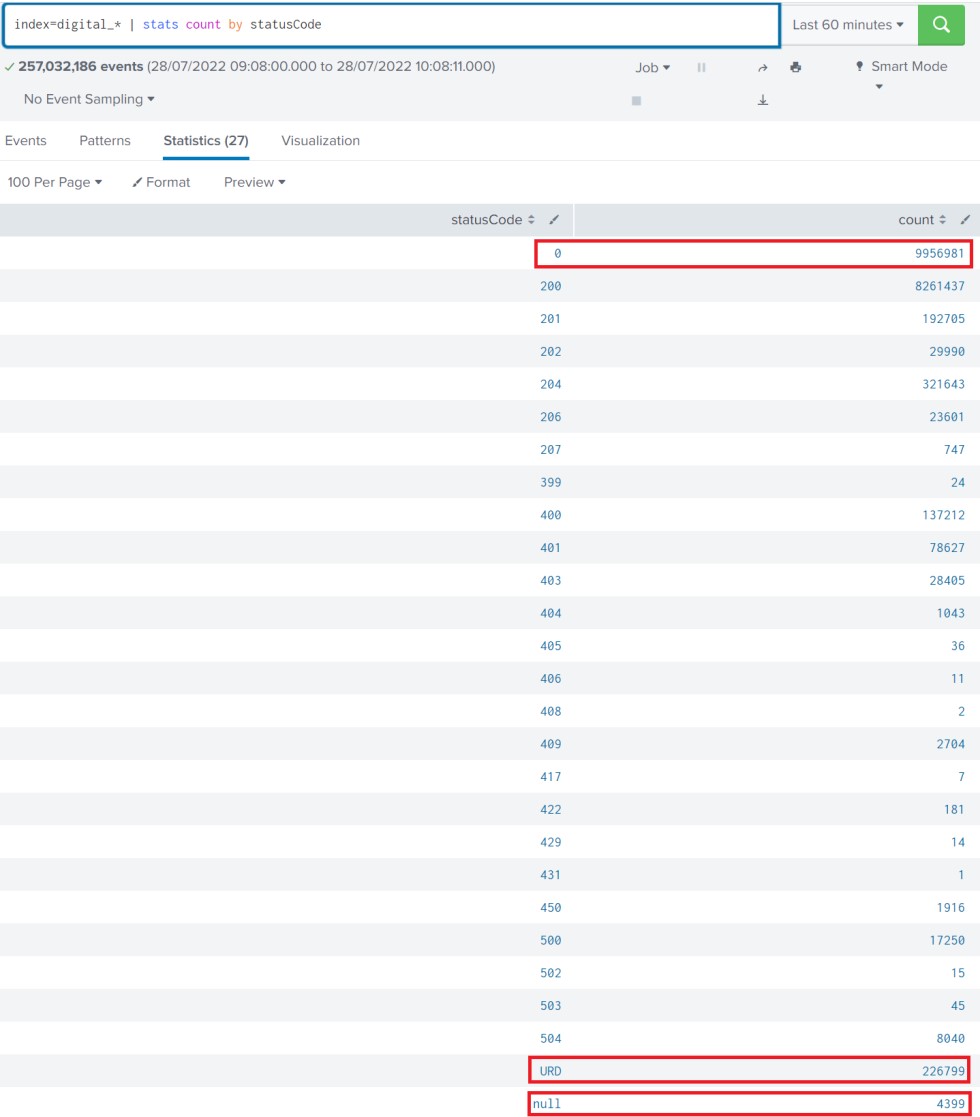
X-Hsbc-Session-Correlation-Id for ACCESS\_TOKEN

X-HSBC-Request-Correlation-Id

HTTP Status code / API Name is inconsistent, some of the status codes are invalid.



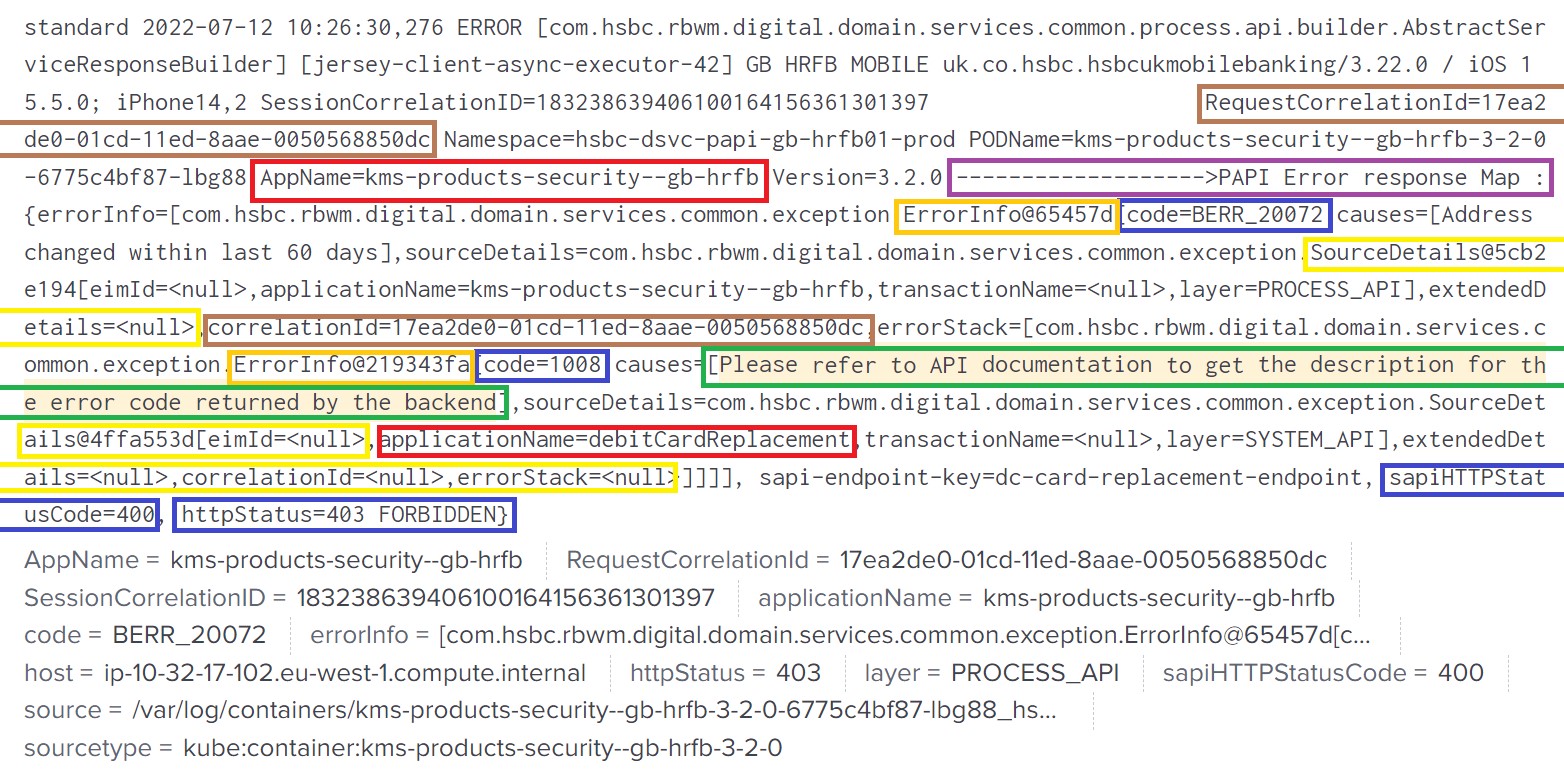
HTTP Status code / API Name is inconsistent, some of the status code are invalid.



# Recommendation Details

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | | Proposed Recommendation Description | | | | | Issue Targeted | | | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| Logging should be part of the acceptance criteria | | 1. Common logging standard to be followed at organisation level 2. Logs should be query-able and make use of key-value pair 3. Log message should be meaningful 4. Avoid unwanted logging 5. In case of error, provide as much as possible information e.g.   service\_name, logged\_user, correlation\_id, method\_name, call\_stack, http\_code, utc\_time   1. Use common field name throughout the system | | | | | 1. Unwanted logging in Splunk leading to potential increase in Splunk cost 2. Due to coding standards not being followed uniformly for writing logs, much   longer time is required to troubleshoot the problems   1. Unnecessary knowledge transfer and documentation is required to understand the logs | | | Technology | Splunk | Dev Team |
|  | | Comments/Benefits | | | | | |
| • | | Faster investigation of problems | | | | | |
| • | | Easier troubleshooting | | | | | |
| • | | Operation and monitoring systems can ingest data easily without any data transformation | | | | | |
| • | | When writing logs to log files, log message output should be tested in Splunk (Splunk testing should be part of acceptance criteria) | | | | | |
| Reward Ranking | Risk  Ranking | Strategic  Roadmap  Ranking | |
| 22.16 | 8.91 | 2.49 | |

# Remediation Steps for Recommendation #WPBREC06



© 2019 NTT DATA, Inc. All rights reserved.

WPBREC07

-

MRDC US\_5XX\_ALERTS

condition is not correct

# Recommendation Details

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | | | | | | Issue Targeted | | | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| MRDC US\_5XX\_ALERTS condition is not correct | updated Syntax :  index=digital\_bankserv\_pcf\_raw  "alogent\_http\_status\_code=\"500\"" | rex   |  | | --- | | **| where totalcount > 0** |   "alogent\_response\_fault\_reason\=(?<reason>[\w\W]+$)" | bucket \_time span=1m | stats count as totalcount | | | | | | SRE team receives alert notification via email for every 30 minutes regardless of the result of the query | | | Technology | Splunk | SRE Team |
|  | Comments/Benefits | | | | | |
| • | Faster investigation of problems | | | | | |
| • | Easier troubleshooting | | | | | |
| • | Operation and monitoring systems can ingest data easily without any data transformation | | | | | |
| Reward Ranking | Risk  Ranking | Strategic  Roadmap  Ranking | |
| 22.46 | 4.68 | 3 | |

© 2019 NTT DATA, Inc. All rights reserved.

WPBREC08

-

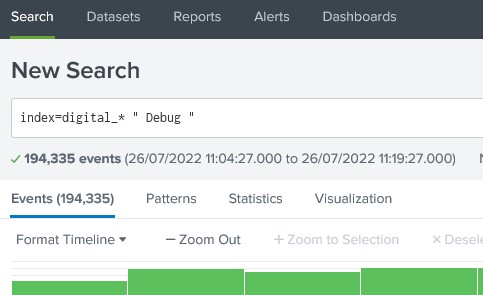
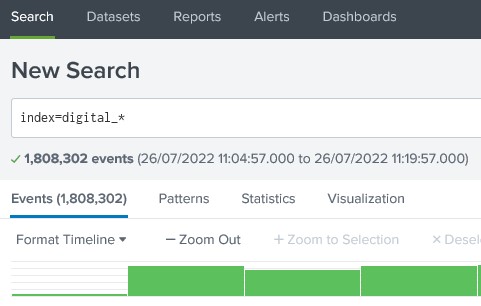
Debug Logs should not be there

in Splunk

# Recommendation Details

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | | | | | | Issue Targeted | | | Impacted Area | Impacted  Systems/Tool s | Impacted Team |
| Debug Logs should not be there in Splunk | As per our observation there is huge amount of debug data to  Splunk, it should be stopped   1. Reduce cost of Splunk 2. Reduce security risk 3. Load on Splunk | | | | | | Large amount of data flow to Splunk due to debug logs (Upwards of 10% of data identified as debug log data) | | | Standards | Splunk | Dev Team |
|  | Comments/Benefits | | | | | |
| • | Significant savings in the amount of data flowing to Splunk and thus potential realisations of cost benefit for the bank overall | | | | | |
| Reward Ranking | Risk  Ranking | Strategic  Roadmap  Ranking | |
| 27.22 | 6.435 | 7 | |

No of debug events: Total number of events (including debug):



© 2019 NTT DATA, Inc. All rights reserved.

WPBREC09

-

Splunk Search Improvement

-

DIGITAL SERVICE HK SAPI 5XX Email ALERT

# Recommendation Details

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | | | | | | Issue Targeted | | | Impacted Area | Impacted Systems/Tools | Impacted Team |
| Splunk Search Improvement - DIGITAL SERVICE HK SAPI 5XX Email ALERT | New search query save approx 25 sec. (20% reduction in time to execute)  Details of the change described in the next slide | | | | | | Splunk performance | | | Standards | Splunk | SRE Team |
|  | Comments/Benefits | | | | | |
| • | Best Practice | | | | | |
| Reward Ranking | Risk  Ranking | Strategic  Roadmap  Ranking | |
| 10.37 | 3.24 | 9.5 | |

• **Existing Search Query:** sourcetype=technical\_pcf\_app\_proc\_web\* (index=digital\_technical\_pcf\* OR index= digital\_technical\_authz\_bsplus\_raw OR index= digital\_technical\_sapi\_bsplus\_raw)

|rex field=\_raw "\s(?<sapi\_dc>[\wd]+)(ko100|km100|ko101|km101)-(?<sapi\_org>[\w\d-]\*)\.(?<sapi\_space>[\w\d-]+)\.(?<sapi\_app>[\w\d-]+)\s" |search HTTPStatusCode>= 499

|eval series=1

|fillnull value=NULL

|stats count(HTTPStatusCode) as status5xx values(MainframeErrorCode) as ErrorCode perc95(TotalSAPIResponseTime) as p95ResponseTime by APP\_Name HTTPStatusCode |where status5xx >=25

**New Search Query:**

(index=digital\_technical\_pcf\* OR index= digital\_technical\_authz\_bsplus\_raw OR index= digital\_technical\_sapi\_bsplus\_raw) sourcetype=technical\_pcf\_app\_proc\_web\*

HTTPStatusCode>= 499

|fillnull value=NULL

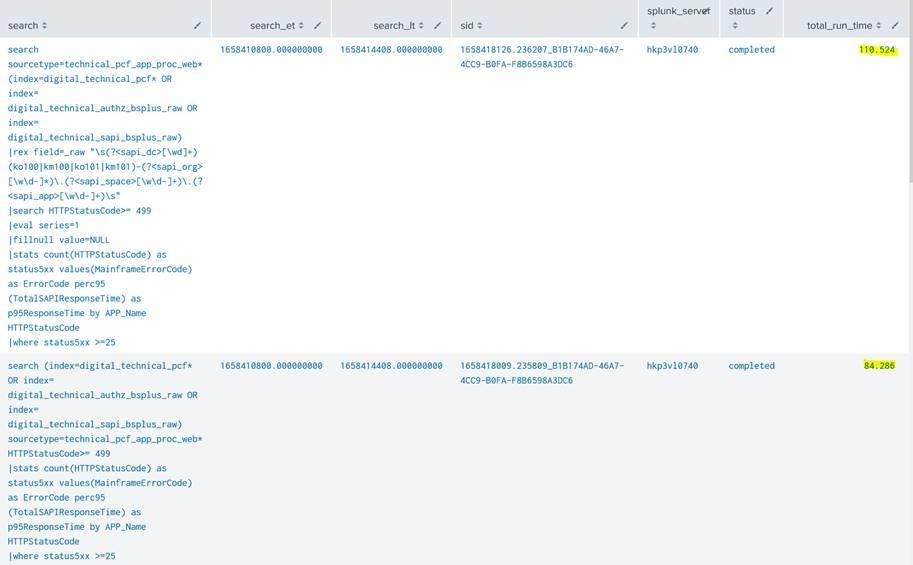
|stats count(HTTPStatusCode) as status5xx values(MainframeErrorCode) as ErrorCode perc95(TotalSAPIResponseTime) as p95ResponseTime by APP\_Name HTTPStatusCode

|where status5xx >=25

* **Change:**
* No use of regex & series in search string – we can remove this o |rex field=\_raw "\s(?<sapi\_dc>[\wd]+)(ko100|km100|ko101|km101)-(?<sapi\_org>[\w\d-]\*)\.(?<sapi\_space>[\w\d-]+)\.(?<sapi\_app>[\w\d-]+)\s"

o |eval series=1

* Wrong placement of HTTPStatusCode>= 499, this should be part of main search



© 2019 NTT DATA, Inc. All rights reserved.

WPBREC10

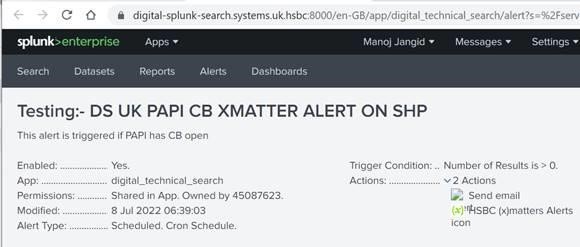
-

Remove Duplicate Alerts

# Recommendation Details

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | | | | | | Issue Targeted | | | Impacted Area | Impacted  Systems/Tool s | Impacted Team |
| Remove Duplicate Alerts | Remove Duplicate for Example:  DIGITAL SERVICE HK SAPI 5XX Email ALERT With Error Code  Testing: DIGITAL SERVICE HK SAPI 5XX Email ALERT With Error Code  Testing:DS UK PAPI CB XMATTER ALERT ON SHP | | | | | | Best practice | | | Standards | Splunk | SRE Team |
|  | Comments/Benefits | | | | | |
| • | This was highlighted when discovered and has since been corrected | | | | | |
| • | Also related to WPBREC02 | | | | | |
| Reward Ranking | Risk  Ranking | Strategic  Roadmap  Ranking | |
| 10.37 | 3.24 | 9.5 | |

Remove duplicate alert:



1. Digital Service - No App Found on US Splunk Authz

Alert

1. Digital Service - No App Found on US Splunk Authz

ALERT

and

1. Digital Service - No App Found on US Splunk Alert

© 2022 NTT DATA, Inc. All rights reserved.

28



PUBLIC

1. Digital Service - No App Found on US Splunk ALERT

e.g. - Digital Service - US/CA/MX Rproxy 503 xMatter Alert

© 2022 NTT DATA, Inc. All rights reserved.

29

Findings & Recommendations

–

Sprint 4

30

© 2019 NTT DATA, Inc. All rights reserved.

WPBREC11

-

CI/CD Pipeline should be

implemented for Splunk

© 2022 NTT DATA, Inc. All rights reserved.

31



PUBLIC

Reward

Ranking

Risk

Ranking

Strategic

Roadmap

Ranking

10.69

9.405

17

Recommendation

Details

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | | | | Issue Targeted | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| CI/CD Pipeline should be implemented for Splunk | All changes should go through a CI/CD automated process that includes the principles and methodologies used across the bank  under the banner of DevSecOps | | | | Industry Standard | Technology | Splunk | SRE Team |
|  | Comments/Benefits |
| • | Aligns to standard Production deployment practices. |
| • | Streamlines the auditing and security aspects of any changes to production Splunk instance. |

32

© 2019 NTT DATA, Inc. All rights reserved.

WPBREC14

–

There should be a separate

Splunk App per sub HSBC Business Unit, e.g.

WPB ACS

© 2022 NTT DATA, Inc. All rights reserved.

33



PUBLIC

Reward

Ranking

Risk

Ranking

Strategic

Roadmap

Ranking

25.92

4.68

2

Recommendation

Details

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | | | | Issue Targeted | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| Every SRE team should have there  Splunk App | There should be a separate Splunk App per sub HSBC Business Unit,  e.g. WPB ACS | | | | Seperation of concerns industry best practices | Standards | Splunk | SRE Team |
|  | Comments/Benefits |
| • | This is connected to the CI/CD pipeline as this is a precursor to implementing  an efficient, traceable and auditable  DevSecOps processes for Splunk |

© 2022 NTT DATA, Inc. All rights reserved.

34



PUBLIC

DNS

NGINX

(

Reverse

Proxy)

Jenkins

VPC (Bare metal)

Minikube

K8s Cluster

Internet

Internet

Security check

Webhook Triggered on Code Check

-

in

Deploy Config &

Refresh Pods

Splunk

Snyk

GIT Repo

POD

POD

Agent Pod

Vulnerability

Check

https://splunk.traderyolo.com

Trusted Certificate

LetsEncrypt

CA

Access K8s cluster resources over

NodePort

OR

LoadBalancer

github.wiqram.splunk

-

hsbc

-

demo

Certificate Issuing

Authority

https://jenkins.traderyolo.com

Splunk Demo Architecture

© 2019 NTT DATA, Inc. All rights reserved.

Proof Of Concept Demo for WPBREC11 and

WPBREC14

WPBREC13

–

Use of Analytics in

AppD

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description |  | Issue Targeted | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| Use of Analytics in AppD | The analytics feature in AppD can be used to create specific metrics and to use it in healthrule | Effective use |  | Technology | AppD | SRE Team |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Comments/Benefits | | | | |
| • | 1. To create dashboards | | | | |
| • | 2. To create metrics to observe | | | | |
| • | 3. to create health rule based on the metrics | | | | |
| Reward Ranking | Risk  Ranking | Strategic  Roadmap  Ranking |
| 17.42 | 7.695 | 14 |

WPBREC12

–

Use alert suppression in

AppD

instead of disabling health rule

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description |  | Issue Targeted | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| Use alert suppression in AppD instead of disabling health rule | Use alert suppression in AppD instead of disabling health rule | Best practice |  | Process | AppD | SRE Team |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Comments/Benefits | | | | |
| • | 1. Best practice | | | | |
| • | 2. Alert suppression can be time bound | | | | |
| • | 3. Health rules disabled for some reasons (e.g. too many alerts on the health rule) not enabled again leads to missing actual alerts | | | | |
| Reward Ranking | Risk  Ranking | Strategic  Roadmap  Ranking |
| 19.01 | 3.96 | 4 |

WPBREC15

–

Use Asynchronous Transaction

Demarcation in

AppD

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description |  | Issue Targeted | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| Use Asynchronous Transaction Demarcation in AppD | Enabling Asynchronous transaction demarcation , helps with endto-end performance metrics determine the total transaction processing time in cases where the response time for the business transaction doesn't reflect the entire logical business flow for the transaction. | Effective use |  | Technology | AppD | SRE Team |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Comments/Benefits | | | | |
| • | When Async Transaction feature of AppD is disabled, it hides the details of any asynchronous calls that are happening within a specific transaction. | | | | |
| • | Enabling this in AppD will provide a detailed view of end-to-end latency for  any particular transaction tracked within  AppD | | | | |
| Reward Ranking | Risk  Ranking | Strategic  Roadmap  Ranking |
| 29.81 | 10.395 | 11 |

WPBREC16

–

Attach Link To Splunk Alert

Details Within Email Alerts From Splunk to

xMatter

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description |  | Issue Targeted | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| Splunk alerts missing URL in xMatters email notification | In xMatters use "flow designer" to set required parameters for notifications | Effective use |  | Technology | xMatter | SRE Team |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Comments/Benefits | | | | |
| • | SRE will be able to quickly log on to the Splunk to understand the alert | | | | |
| Reward Ranking | Risk  Ranking | Strategic  Roadmap  Ranking |
| 36.29 | 4.68 | 1 |

WPBREC17

–

Automation of Restart Runbook

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | Issue Targeted | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| Automation of Restart Runbook | To reduce toil, any repeated tasks that can be automated should be automated.  The Restart runbook at the moment is being handled manually where everytime there is an alert that matches certain criteria, the SRE team manually restarts the problematic, alert generating pod.  This can be automated by existing tools available with the bank. | Automate Everything/ Reduce Toil | Technology | xMatter | SRE Team |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Comments/Benefits | | | | |
| • | Reducing Toil should be one of the key focusses of SRE team and this can be done via automating tasks that can be automated. | | | | |
| • | Restarting of pods is a perfect example for this and a POC will be implemented and demo will be given to the wider team of how it can be achieved. | | | | |
| • | By our rough calculations, today the team approximately undertakes **13680 number of restarts** every year and each renewal requires roughly 9 minutes each time. This means the SRE team spends **roughly 123120 minutes every year on just restarting failed pods** which **equates to 1.16 FTE per year**. This automation will free up that much team time to **focus on innovation and further automation**. | | | | |
| Reward Ranking | Risk  Ranking | Strategic  Roadmap  Ranking |
| 35.28 | 10.395 | 8 |

* <https://social.global.hsbc/stories/view/xVT84YFwp4>
* [**Fred S Seen**](https://social.global.hsbc/stories/author/43344993)talks about SRE and the following is an excerpt from his blog -

*It’s a practice in that it seeks to continuously improve the reliability of systems through engineering practices using software, automation, and data. These practices are necessary in an increasingly complex and dynamic systems landscape as they help to scale the ability to improve observability, reduce toil, more accurately measure risk, and more safely enable business driven change.*

**“Talk is cheap. Show me the code.” ― Linus Torvalds**

# Automation Recovery POC Architecture



DNS

NGINX

Reverse

(

Proxy)

Jenkins

VPC (Bare metal)

Minikube

K8s Cluster

Internet

Internet

Security check

Webhook Triggered on Code Check

-

in

Deploy Config & Refresh Pods

Splunk

Snyk

GIT Repo

POD

POD

Deploy Agents

Vulnerability

Check

https://splunk.traderyolo.com

Trusted Certificate

LetsEncrypt

CA

Access K8s cluster resources over

NodePort

OR

LoadBalancer

github.wiqram.splunk

-

hsbc

-

demo

Certificate Issuing

Authority

https://jenkins.traderyolo.com

Xmatter

Free Trial

XMatter



Problem

App

POD



XAgent

Jenkins Namespace

XAgent

Namespace

Mem

-

Leak

-

Java Namespace

Splunk Namespace

All Pods within Namespace

can only access Pods across

cluster based on their

associated and tagged

Service Accounts and

access given to those SAs

Xmatter

Alert

Xmatter

Workflow

Metrics

Logs

Splunk

-

Connect Namespace

Restart Pod

Command



Data Collectors



© 2019 NTT DATA, Inc. All rights reserved.

Proof Of Concept Demo for WPBREC16 and

WPBREC17

© 2019 NTT DATA, Inc. All rights reserved.

WPBREC18

–

Security Violation Observed

© 2022 NTT DATA, Inc. All rights reserved.

51



PUBLIC

Reward

Ranking

Risk

Ranking

Strategic

Roadmap

Ranking

12.10

3.24

8

Recommendation

Details

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | | | Issue Targeted | | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| Security Violation Observed | Certificate Key printed on logs (example: index=\* "BEGIN CERTIFICATE" , in splunk url: https://digital-splunksearch.systems.uk.hsbc:8000/) | | | Breaks the security policies and exposes bank to threats | | Standards | Engineering  Dev | Dev Team |
|  | Comments/Benefits | |
| • | Goes against every security guideline | |

© 2019 NTT DATA, Inc. All rights reserved.

WPBREC19

–

Merge Alerts where the

differences are insignificant

© 2022 NTT DATA, Inc. All rights reserved.

53



PUBLIC

Reward

Ranking

Risk

Ranking

Strategic

Roadmap

Ranking

10.37

3.24

11

Recommendation

Details

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | | | Issue Targeted | | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| Merge Alerts where the differences are insignificant | Digital service UK Domain PAPI email Alert  Digital service UK Domain PAPI email xMatter Alert | | | High number of Alerts configured in Splunk | | Standards | Splunk | SRE Team |
|  | Comments/Benefits | |
| • | This allows for reducing the number of alerts configured thus doing the bit to simplify the overall alerts management | |

© 2022 NTT DATA, Inc. All rights reserved.

Findings & Recommendations

–

Sprint 7

55

© 2019 NTT DATA, Inc. All rights reserved.

WPBREC20

–

Certificate Auto

-

renewal

–

Part 1

© 2022 NTT DATA, Inc. All rights reserved.

56



PUBLIC

Reward

Ranking

Risk

Ranking

Strategic

Roadmap

Ranking

36.29

4.68

1.5

Recommendation

Details

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | | | Issue Targeted | | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| Certificate Auto-renewal - PART 1 | HSBC currently has Venafi that manages the certificate renewals manually.  We want to automate that to ensure some of the alerts caused by out of date certificates don’t occur again.  This is divided into 2 parts - 1) where certificates are automatically renewed and 2) the renewed certificates are injected into relevant microservices and deployed | | | Manual Cert renewals to be automated. | | Enhance | Technology | Security |
|  | Comments/Benefits | |
| • | Reduces outages caused by out of date certificates. | |

# End-to-End Cert Renewal Automation POC Architecture – PART 1

58

© 2019 NTT DATA, Inc. All rights reserved.

Proof Of Concept Demo for WPBREC20

59

© 2019 NTT DATA, Inc. All rights reserved.

WPBREC21

–

Automated Fetching refreshed

secrets at regular interval

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | Issue Targeted | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| Automated Fetching refreshed secrets every regular interval | To complement WPBREC17 automated restart runbook, we have implemented this POC to showcase how a refreshed token can be retrieved from a secret store vault whenever a command is to be triggered to fix the cause of an alert. | Complementing automation of restart runbook. | Enhance | Technology | Security |

|  |  |
| --- | --- |
|  | Comments/Benefits |
| • | Allows for restart runbook automation to take place keeping in line with hsbc security policies of refreshed tokens every 15 minutes. |

© 2022 NTT DATA, Inc. All rights reserved.

60



PUBLIC

Reward

Ranking

Risk

Ranking

Strategic

Roadmap

Ranking

17.42

6.075

14

Recommendation

Details

# Automated Secrets Fetching POC Architecture – Supplement to WPBREC17

© 2019 NTT DATA, Inc. All rights reserved.

Proof Of Concept Demo for WPBREC21

© 2019 NTT DATA, Inc. All rights reserved.

WPBREC22

–

Object validations missing in API

# Recommendation Details

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | | | | | | Issue Targeted | | | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| Object Validation should be included within the app code. | object must be validated in the code.  Example: dcc-gb-hrfb-credit-card-installment-papi  Search String: index=digital\_\* "dcc-gb-hrfb-credit-card-installmentpapi" "Exception occurred while parsing json data :A JSONObject" | | | | | | Not following coding standards | | | Fix | Technology | Engineering  Dev |
|  | Comments/Benefits | | | | | |
| • | There are many errors that could be avoided just by adding the right validation rules for each API attribute within the microservice code itself. | | | | | |
| • | There is not significant savings for this but it is just best practice and reduces the amount of data in splunk (however minor) | | | | | |
| Reward Ranking | Risk  Ranking | Strategic  Roadmap  Ranking | |
| 12.96 | 3.96 | 11 | |

# WPBREC22 – Object validations missing in API

Splunk Query: index=digital\_\* "dcc-gb-hrfb-credit-card-installment-papi" "Exception occurred while parsing json data :A JSONObject" Result:

## Solution

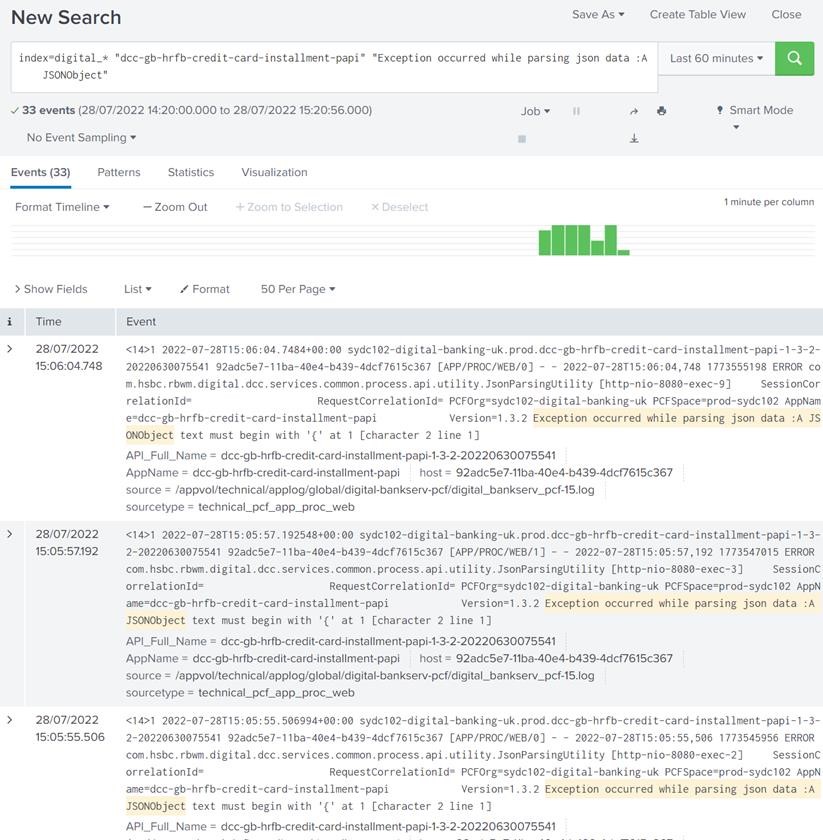
Object must be validated in code e.g.

class ModelObject {​



}

​



@NotBlank(message = 'someString should not be

empty or null') final String someString;

}​

void call\_this\_appi(ModelObject someObject) {​

// All the validation must be covered by unit test verifyValidation(someObject); // If invalid model then this will throw exception

# WPBREC22 – Object validations missing in API



© 2022 NTT DATA, Inc. All rights reserved.

Findings & Recommendations

–

Sprint 8

© 2019 NTT DATA, Inc. All rights reserved.

WPBREC23

–

End

-

to

-

End Certificate Auto

-

renewal

-

PART 2

© 2022 NTT DATA, Inc. All rights reserved.

69



PUBLIC

Reward

Ranking

Risk

Ranking

Strategic

Roadmap

Ranking

26.37

10.395

19

Recommendation

Details

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | | | Issue Targeted | | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| Certificate Auto-renewal - PART 2 | This is part 2 of the WPBREC20 that automates the runbook where end-to-end certificate renewal and push into microservices steps take place. | | | Manual Cert renewals to be automated. | | Enhance | Technology | Security |
|  | Comments/Benefits | |
| • | By our rough calculations, today the team approximately undertakes >2000 cert renewals every year (sometimes one renewals processes includes more than 1 cert) and each renewal requires roughly 60 minutes each time. This means the SRE team spends **roughly 120000 minutes every year** on just cert renewal which equates to **1.13 FTE per year**. This automation will **free up** that much team time **to focus on innovation and further automation**. | |

# End-to-End Cert Renewal Automation POC Architecture – Supplement to WPBREC20

Proof Of Concept Demo for WPBREC23

© 2022 NTT DATA, Inc. All rights reserved.

72

Findings & Recommendations

–

Sprint 9

WPBREC24

–

Efficient use of Summary and

Internal Index

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | Issue Targeted | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| Efficient use of Summary and Internal Index | Benefits are -   1. SLA Based suppressing of alerts 2. historical statistical data saved in a separate index   If all data is accessed via COLLECT command within Splunk then it doesn’t count towards license costs. | Effective use of Splunk | Enhance | Technology | Splunk |

|  |  |
| --- | --- |
|  | Comments/Benefits |
| • | 1) Alert suppression can be targeted for specific alerts for specific APIs thus reducing noise for those alerts that are already in work and well within the SLA to be fixed. |
| • | 2)Effective report generation based on data within summary index, e.g.  resolution times for alerts, alerts that went over SLA, etc. |
| • | 3)Internal Index allows for security and auditing by providing data for all changes/executions,etc. that occur in splunk. |

© 2022 NTT DATA, Inc. All rights reserved.

74



PUBLIC

Reward

Ranking

Risk

Ranking

Strategic

Roadmap

Ranking

15.55

9.405

26

Recommendation

Details

Proof Of Concept Demo

for WPBREC24

© 2019 NTT DATA, Inc. All rights reserved.

WPBREC25

–

Grafana to be used as an

overarching single

-

pane

-

of

-

glass dashboard

solution

# Recommendation Details

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | | | | | Issue Targeted | | | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| Grafana to be used as an overarching single-pane-of-glass dashboard solution | Sitting above the monitoring tools such as AppD and Splunk, Grafana can store data points that can go as far behind in time as needed allowing for trend analytics and holistiv view of the IT estate's performance to be visible. | | | | | Single-pane-of-glass view | | | Enhance | Technology | Grafana |
| Comments/Benefits | | | | | |
| POC candidate for next sprint  The advantage of having a separate dashboard outside of the monitoring tools is to allow for a collation of data from various sources and ability to show a holistic view of the entire IT estate.  Ability to store historic data that goes farther out than what is available on monitoring tools due to restrictions of those tools. | | | | | |
| Reward Ranking | Risk  Ranking | Strategic  Roadmap  Ranking | |
| 11.66 | 10.395 | 28 | |

© 2019 NTT DATA, Inc. All rights reserved.

WPBREC26

–

Define Service Level Indicators

(

SLI) for every API

# Recommendation Details

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | | | | | Issue Targeted | | | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| Define Service Level Indicators (SLI) for every API | SLI: a metric that indicate what measurement of performance a customer is receiving at a given time - example:  Proportion of account transaction requests processed < 42calls/sec, as measured from “DIGITAL\_API PAPI SHP STATS” dashboard from Splunk for one month | | | | | SRE Principles | | | Principles | All | SRE Team |
| Comments/Benefits | | | | | |
| Benefit: SLI helps teams to view the performance metrics significate for the consumer | | | | | |
| Reward Ranking | Risk  Ranking | Strategic  Roadmap  Ranking | |
| 26.37 | 10.395 | 19 | |

# Introduction on SLA

* SLA (Service Level Agreement)
* What? – It is an agreement between provider and client about service availability, performance etc.
* Why? – To provide a better service to clients.
* How? – Typically drawn by company’s business and legal team defining promises and consequences if fails to live up to those promises.
* Challenges – Some times the SLA becomes difficult to measure and report as the criteria to measure the performance is not in sync with tech team. Best Practice to include technical people as well while defining the metrics. Also include external factors like response form client or third party

# Introduction on SLI

* SLI (Service Level Indicator)
* What? – It measures compliance with an SLO.
* Why? – Set customer expectations and tell DevOps and SRE team what goals they need to hit and measure themselves against.
* How? – Typically drawn by company’s business and technical team.
* Challenges – Not all metrics to be considered. Best Practice to include most important metrics only.

© 2019 NTT DATA, Inc. All rights reserved.

WPBREC27

–

Define Service Level Objectives

(

SLO) for every API

# Recommendation Details

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | | | | | Issue Targeted | | | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| Define Service Level Objectives (SLO) for every API | SLO: defining the objective that the team can achieve and agreed up on for API's services - example:  99% of account transactions request processed in past 28 days served in < 2500calls/min (42calls/Sec) | | | | | SRE Principles | | | Principles | All | SRE Team |
| Comments/Benefits | | | | | |
| Benefit: SLO help teams to identify whether the API is of high impact (example: SLO of  99.999) and alert/incident related to it. is of highest priority and need to fix it first | | | | | |
| Reward Ranking | Risk  Ranking | Strategic  Roadmap  Ranking | |
| 26.37 | 10.395 | 19 | |

* SLO (Service Level Objective)
* What? – It is an agreement within an SLA about specific goals that that company want to reach.
* Why? – Set customer expectations and tell DevOps and SRE team what goals they need to hit and measure themselves against.

© 2022 NTT DATA, Inc. All rights reserved.

84



PUBLIC

Introduction on SLO

* How? – Typically drawn by company’s business and technical team.
* Challenges – Not all metrics to be considered. Best Practice to include most important metrics only.

© 2019 NTT DATA, Inc. All rights reserved.

WPBREC28

–

Define Error Budget for every

API

© 2022 NTT DATA, Inc. All rights reserved.

86



PUBLIC

Reward

Ranking

Risk

Ranking

Strategic

Roadmap

Ranking

26.37

10.395

19

Recommendation

Details

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | | Issue Targeted | | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| Define Error Budget for every API | Error Budget : the maximum amount of time that a technical system can fail with out contractual consequence - example:  1% of requests acceptable to process beyond 42calls/Sec. (Yearly allowed 87 hours, 39 minutes or monthly allowed 7 hours, 18 minutes) | | SRE Principles | | Principles | All | SRE Team |
| Comments/Benefits | |
| Benefit: Error budget helps PM and team, in identifying whether the API need some attention like fixing it (depleted Error Budget) or it can handle more frequent feature release | |

* Error Budget
* What? – An error budget is the maximum amount of time that a technical system can fail without contractual consequences.
* Why? – Helps the product team to:

**Case1:** If met or exceeded the error budget, then all launches are frozen until they reduce number of errors to a level that allows the launch to proceed

**Case2:** If no to very low consumption of error budget, then product team can launch whatever they want, whenever they want.

© 2022 NTT DATA, Inc. All rights reserved.

87



PUBLIC

Introduction on Error Budget

* How? – Defined via SLO. For example, if SLO for a service is 99.9% then error budget is 0.1% (100-99.9)
* Challenges – Lower the error budget, more difficult to manage the system. For example, 0.001% ER (99.999% SLO) means 25 seconds of downtime is allowed for a month.

© 2022 NTT DATA, Inc. All rights reserved.

88

Findings & Recommendations

–

Sprint 10 and

11

89

© 2019 NTT DATA, Inc. All rights reserved.

WPBREC29

–

SLI/SLO and Error Budget

Documentation

© 2022 NTT DATA, Inc. All rights reserved.

90



PUBLIC

Reward

Ranking

Risk

Ranking

Strategic

Roadmap

Ranking

25.52

8.415

16

Recommendation

Details

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | | Issue Targeted | | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| SLI/SLO and Error Budget Documentation | A document defining SLIs, SLOs and Error Budget for a single API. All the metrics documented are collected from AppDynamics and Splunk configured in HSBC environment. | | SRE Principles | | Principles | All | SRE Team |
| Comments/Benefits | |
| Documented the format to help defining the SLIs, SLOs , error budget and User journey required for an API | |

© 2022 NTT DATA, Inc. All rights reserved.

91



PUBLIC

**Service Level**

**Metric Type**

**Description**

**SLI**

**Specification**

Availability

-

Proportion of account transaction requests that were served successfully

**SLI**

**Implementation**

The success of the request is based on HTTP status code. 5XX

responses count against SLO, while all other requests are considered

successful.

•

Total account transaction requests

(

–

5

XX error response)/ All

transactions

•

i.e. (13547516

-

435)

/ (13547516

-

435) =

0.9999, as measured

from “analytics search” from AppDynamics for a week

•

(

Total account transaction requests

–

5

XX error response)/ (All

transactions)

•

i.e. (63621552+2844

-

12201)/ (63621552+2844+12201) = 0.9996

,

as measured from “DIGITAL\_API PAPI SHP STATS” dashboard for

Days

30

•

(13720761+ 568

-

501)/(13720761+ 568 + 501) = 0.9999

for 7

Days

**SLO**

**Implementation**

>99.99

% of account transactions requests served successfully in a 28 day period

**Error Budget**

**Implementation**

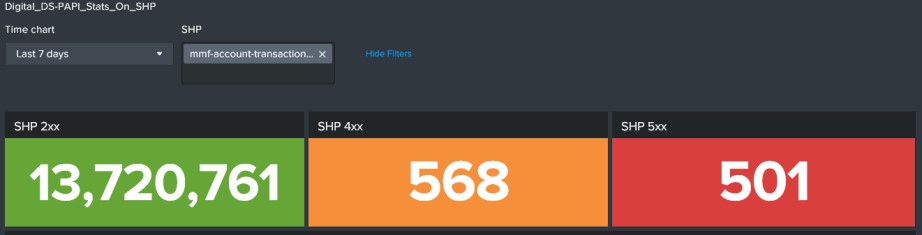
(100

%

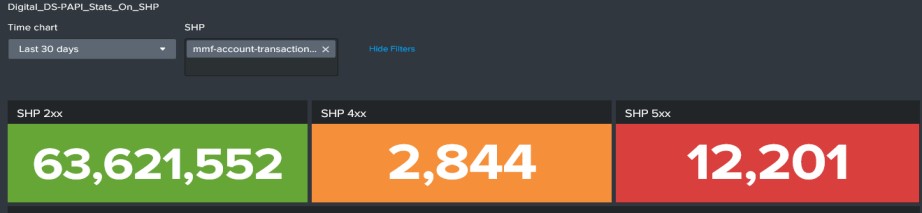
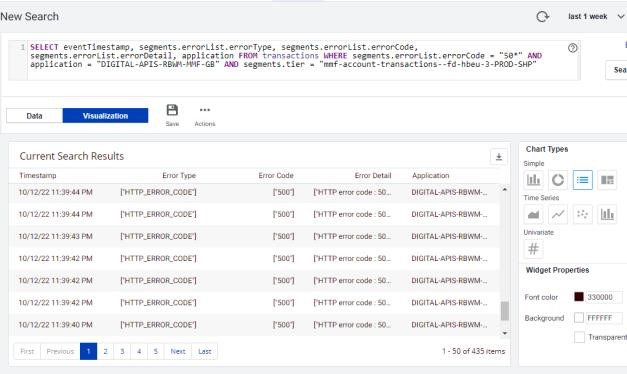
–

99.99%)

**Yearly allowed & budgeted downtime of <5 minutes or monthly allowed downtime <25 seconds**



Sample Template of SLI, SLO and Error Budget for an API



92

© 2019 NTT DATA, Inc. All rights reserved.

WPBREC30

–

Grafana

Current Architecture

Review

© 2022 NTT DATA, Inc. All rights reserved.

93



PUBLIC

Reward

Ranking

Risk

Ranking

Strategic

Roadmap

Ranking

36.74

10.395

10

Recommendation

Details

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | | | Issue Targeted | Impacted Area | Impacted  Systems/T ools | Impacted Team |
| Grafana Current  Architecture Review | Overcome the below shortcomings in current architecture of Grafana in HSBC environment:   1. Dashboard and data source data wipes out when Grafana restarts - The current setup of Grafana, missing a persistent volume where the can be retained. With persistent disk, once the instance restart Grafana pick up its configuration files and loads the dashboards 2. Configuration as code for Grafana - Loading and migration of configuration can be done via CI/CD pipeline for Grafana 3. Limited data in databases - Current databases, contains limited data like alert related information or metrics related to APIs like org, hosts, types regions etc 4. InfluxDB is older version - Current version in HSBC is 1.7 whereas latest is 2.5. A great improvement done in 2.x series on query with flux 5. Data sent to InfluxDB are of string format - The data sent to InfluxDB are not properly type casts. The values like response time, error counts etc. are string type. Arithmetic operations like sum, mean does not work. Either update on the source where data is being pushed or update DB so that type casts can work properly. | | | Grafana  architectural improvement | Technology | Grafana | SRE Team |
| Comments/Benefits |
| Benefit: Helps team to be on sync of any change made to the monitoring system like alert suppressions and configurations |

© 2022 NTT DATA, Inc. All rights reserved.

94



PUBLIC

Grafana

Architecture Review

|  |  |  |
| --- | --- | --- |
|  | **Issue** | **Details** |
| 1 | Dashboard and data source data wipes out when Grafana restarts | The current setup of Grafana, missing a persistent volume where the can be retained. With persistent disk, once the instance restart Grafana pick up its configuration files and loads the dashboards |
| 2 | Configuration as code for Grafana | Loading and migration of configuration can be done via CI/CD pipeline for Grafana |
| 3 | Limited data in databases | Current databases, contains limited data like alert related information or metrics related to APIs like org, hosts, types regions etc |
| 4 | InfluxDB is older version | Current version in HSBC is 1.7 whereas latest is 2.5. A great improvement done in 2.x series on query with flux |
| 5 | Data sent to InfluxDB are of string format | The data sent to InfluxDB are not properly type casts. The values like response time, error counts etc. are string type. Arithmetic operations like sum, mean does not work. Either update on the source where data is being pushed or update DB so that type casts can work properly. |

95

© 2019 NTT DATA, Inc. All rights reserved.

WPBREC31

–

Grafana

Dashboard for

SLI/SLO/Error Budget

© 2022 NTT DATA, Inc. All rights reserved.

96



PUBLIC

Reward

Ranking

Risk

Ranking

Strategic

Roadmap

Ranking

32.66

10.395

15

Recommendation

Details

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | | Issue Targeted | | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| Grafana Dashboard for SLI/SLO/Error Budget | A dummy dashboard for SLIs, SLOs and error budget created in Grafana using the existing data source (InfluxDB) | | SRE Principles | | Technology | Grafana | SRE Team |
| Comments/Benefits | |
| Benefit: Helps team to be on sync of any change made to the monitoring system like alert suppressions and configurations | |

© 2022 NTT DATA, Inc. All rights reserved.

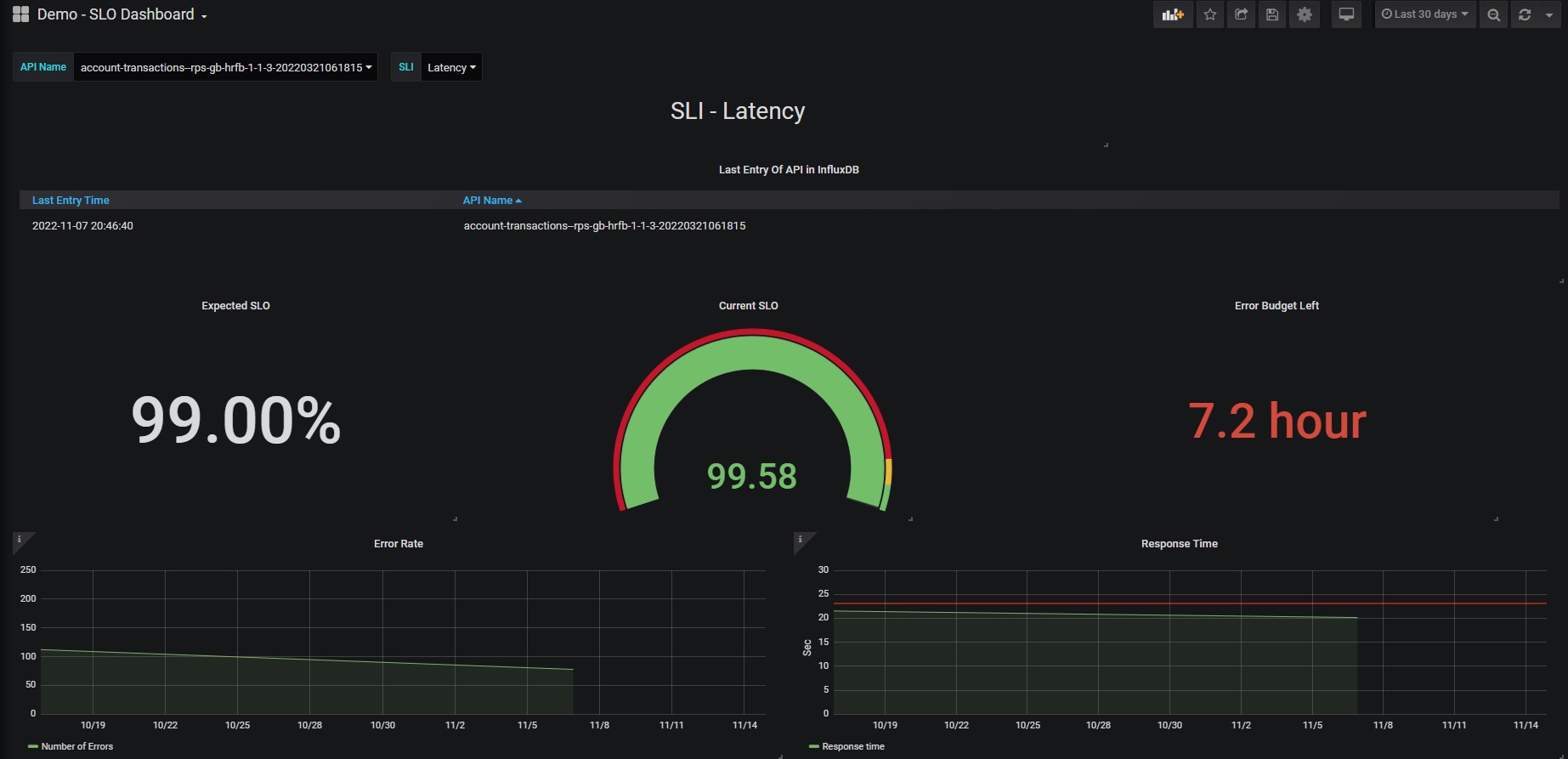
97



PUBLIC

Grafana

Dashboard



98

© 2019 NTT DATA, Inc. All rights reserved.

WPBREC32

–

Automation for configuration

drifts in alerts configurations

© 2022 NTT DATA, Inc. All rights reserved.

99



PUBLIC

Reward

Ranking

Risk

Ranking

Strategic

Roadmap

Ranking

25.52

10.395

22

Recommendation

Details

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Proposed Recommendation | Proposed Recommendation Description | | Issue Targeted | | Impacted Area | Impacted  Systems/Too  ls | Impacted Team |
| Automation for configuration drifts in alerts configurations | Monitor and notify   * Drift in health rules and policies of AppD * Drift in alerts of Splunk * Drift in configurations | | Configuration changes going unnoticed and missing actual alerts | | Technology | Splunk | SRE Team |
| Comments/Benefits | |
| Benefit: Helps team to be on sync of any change made to the monitoring system like alert suppressions and configurations | |

© 2022 NTT DATA, Inc. All rights reserved.

100



PUBLIC



© 2022 NTT DATA, Inc. All rights reserved.

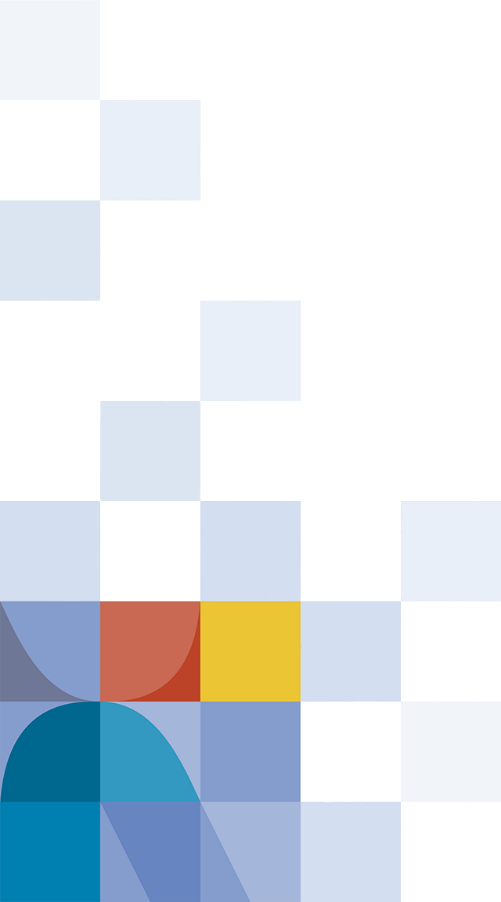
101

Questions

&

Feedback



© 2022 NTT DATA, Inc. All rights reserved.