IT1962 - Using Splunk and its premium solution to accelerate DevOps lifecycle

Scott Lu
Senior Engineering Manager | Splunk

Alfie You
Principal Software Engineer | Splunk

splunk> .conf19

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Agenda

Introduction

DevOps solution using Splunk – ARTS

Problem & Solution

Demo

BETA labs

DevOps solution using Splunk ITSI – InfraWatch Project

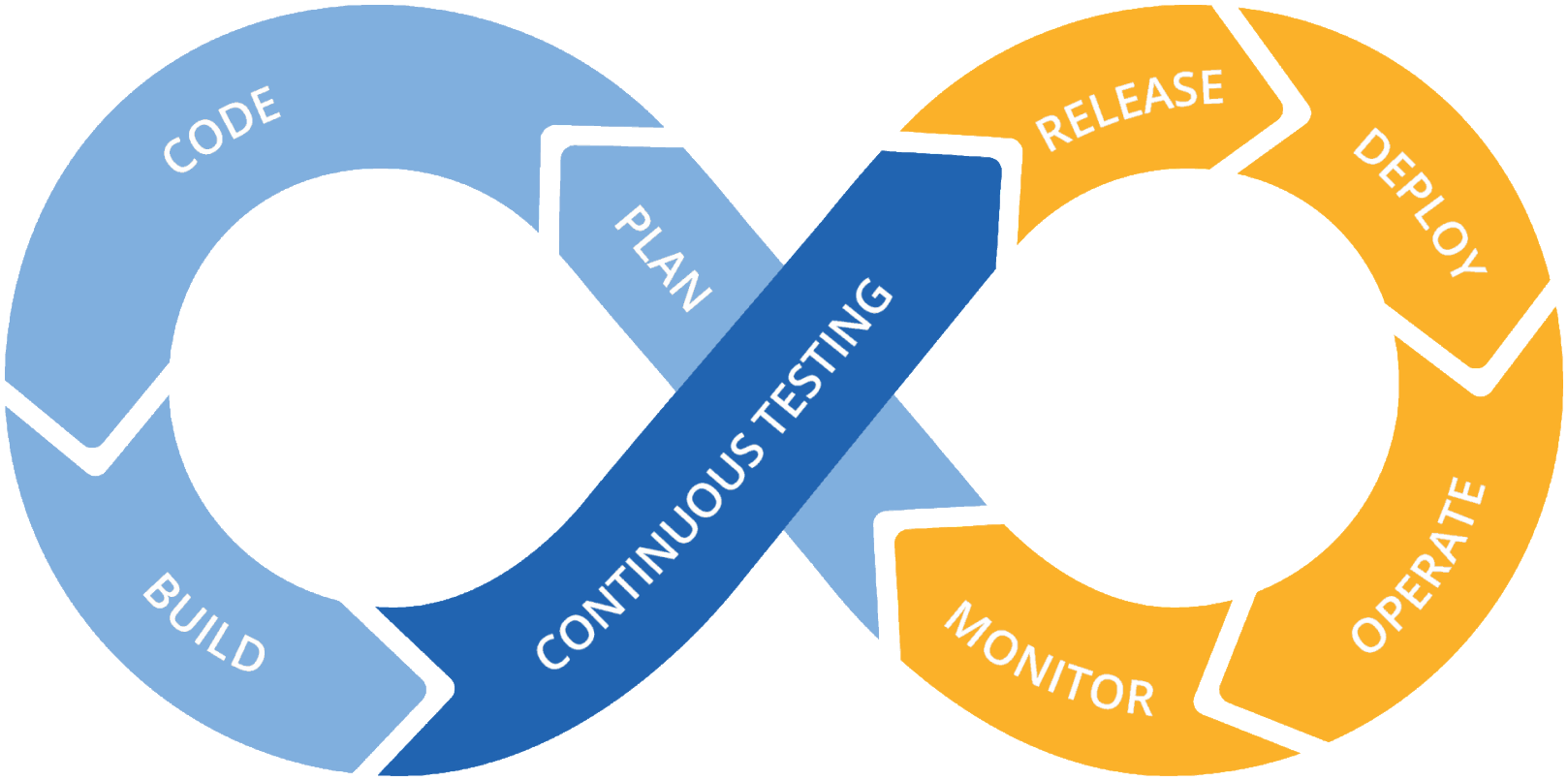
Introduction

Best practices

Q & A

Introduction

DevOps Lifecycle at Splunk



Introduction

Our Solutions for Acceleration

Splunk ARTS

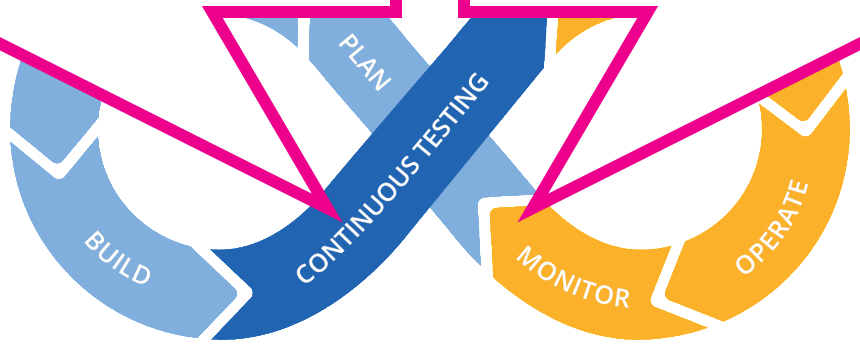
Automation Result Triage System

Automation Result Triage system

InfraWatch Project

Monitoring System for CI/CD Infrastructure

Splunk IT Service Intelligence™ + VictorOps



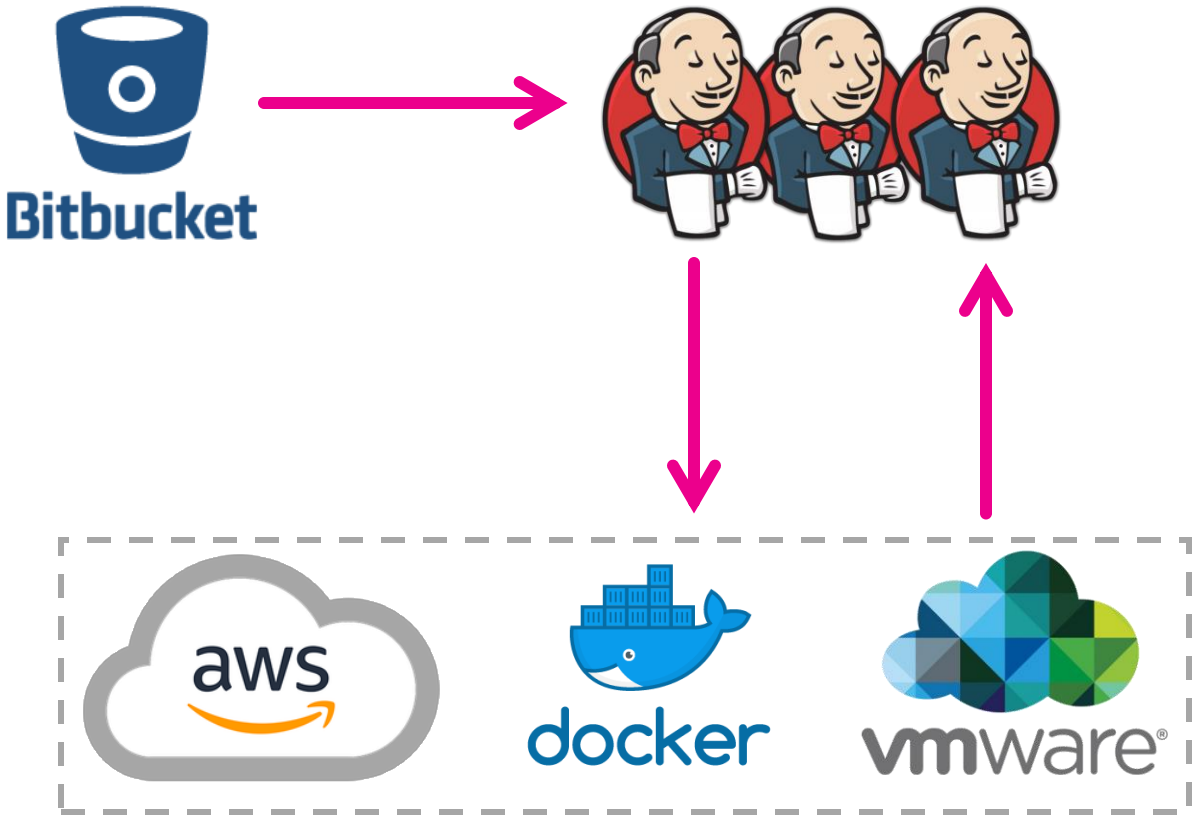
ARTS

Automation Result Triage System

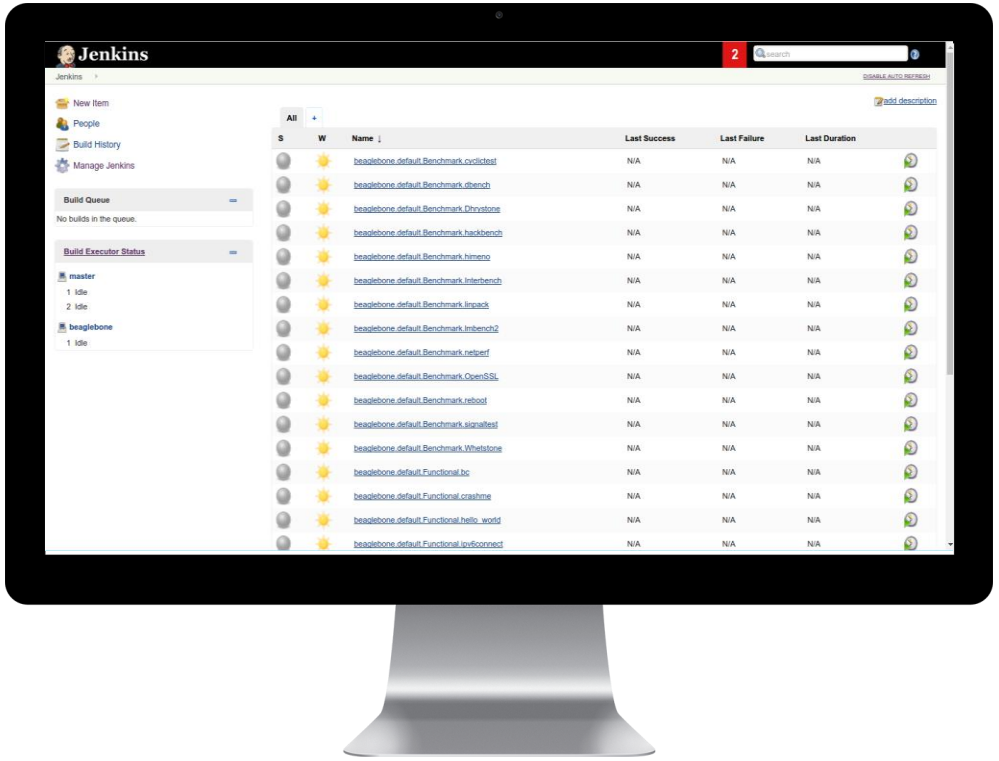
splunk> .conf19

Problem

1

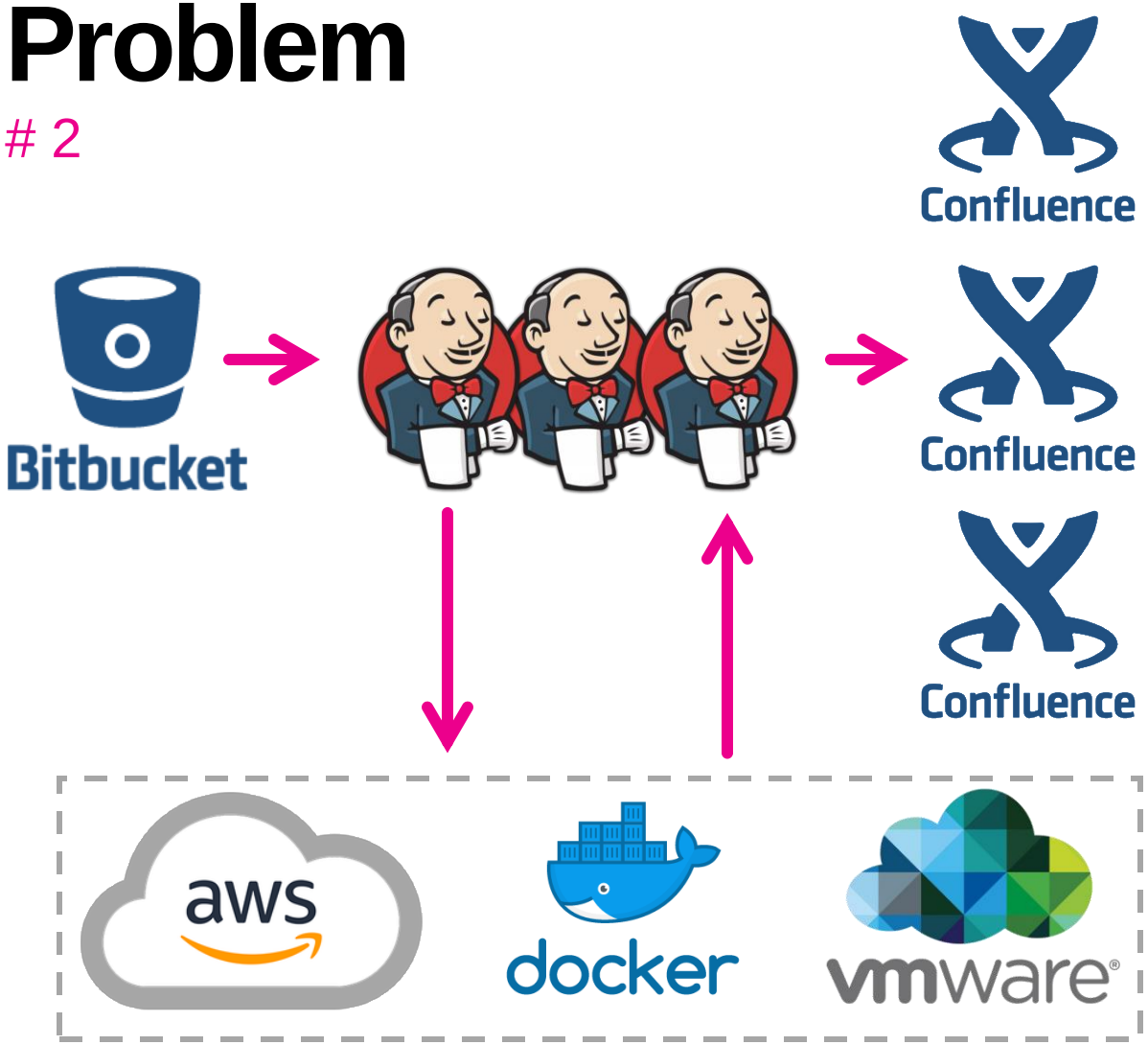


Too much Jenkins data

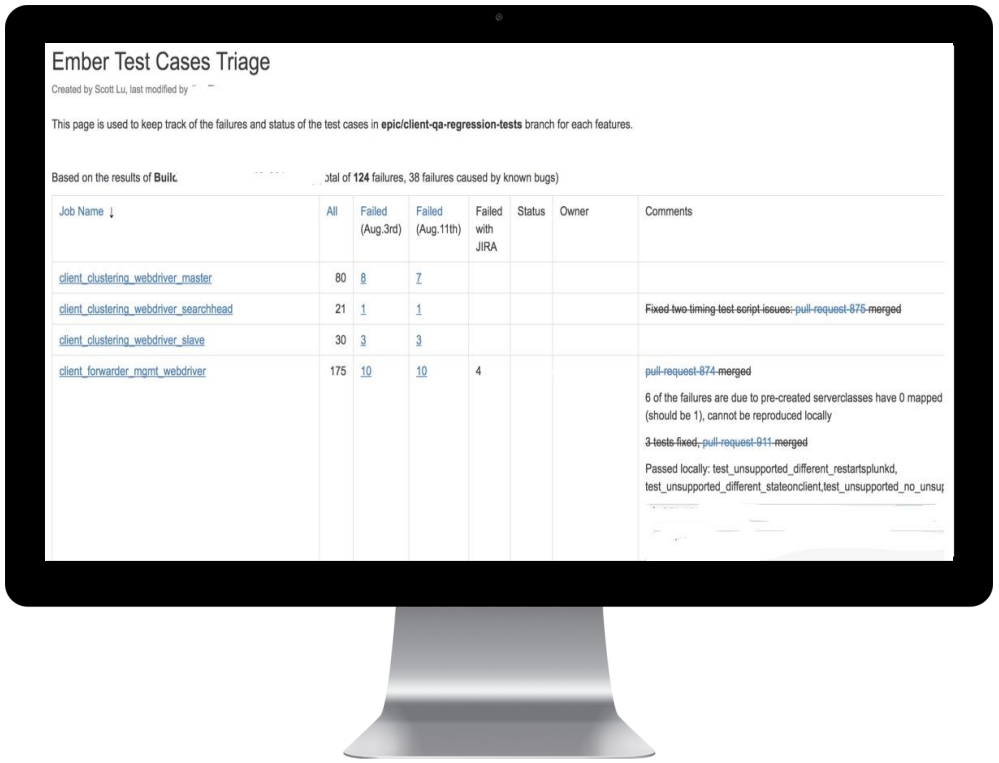


Problem

2

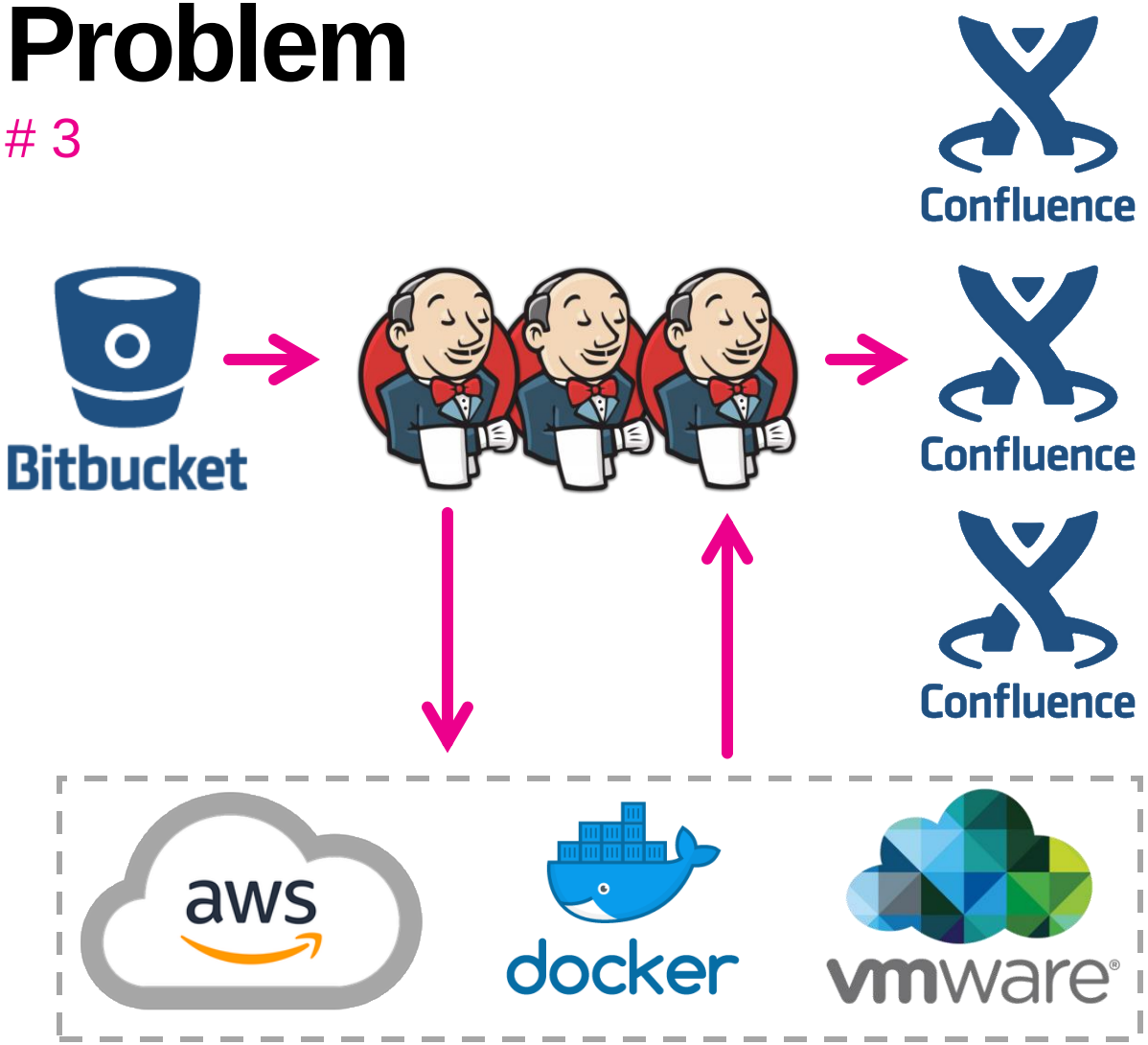


Too much Triage data



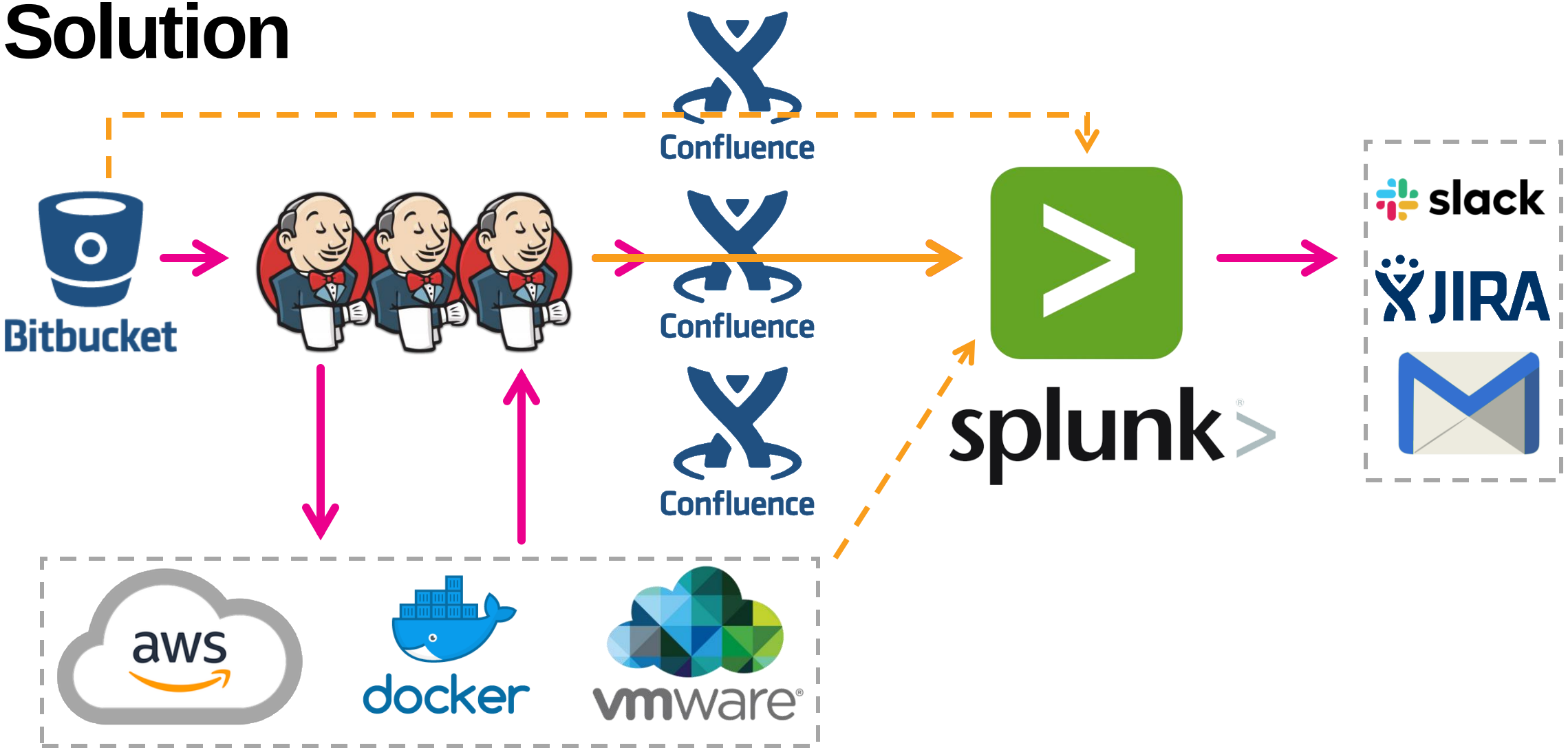
Problem

3

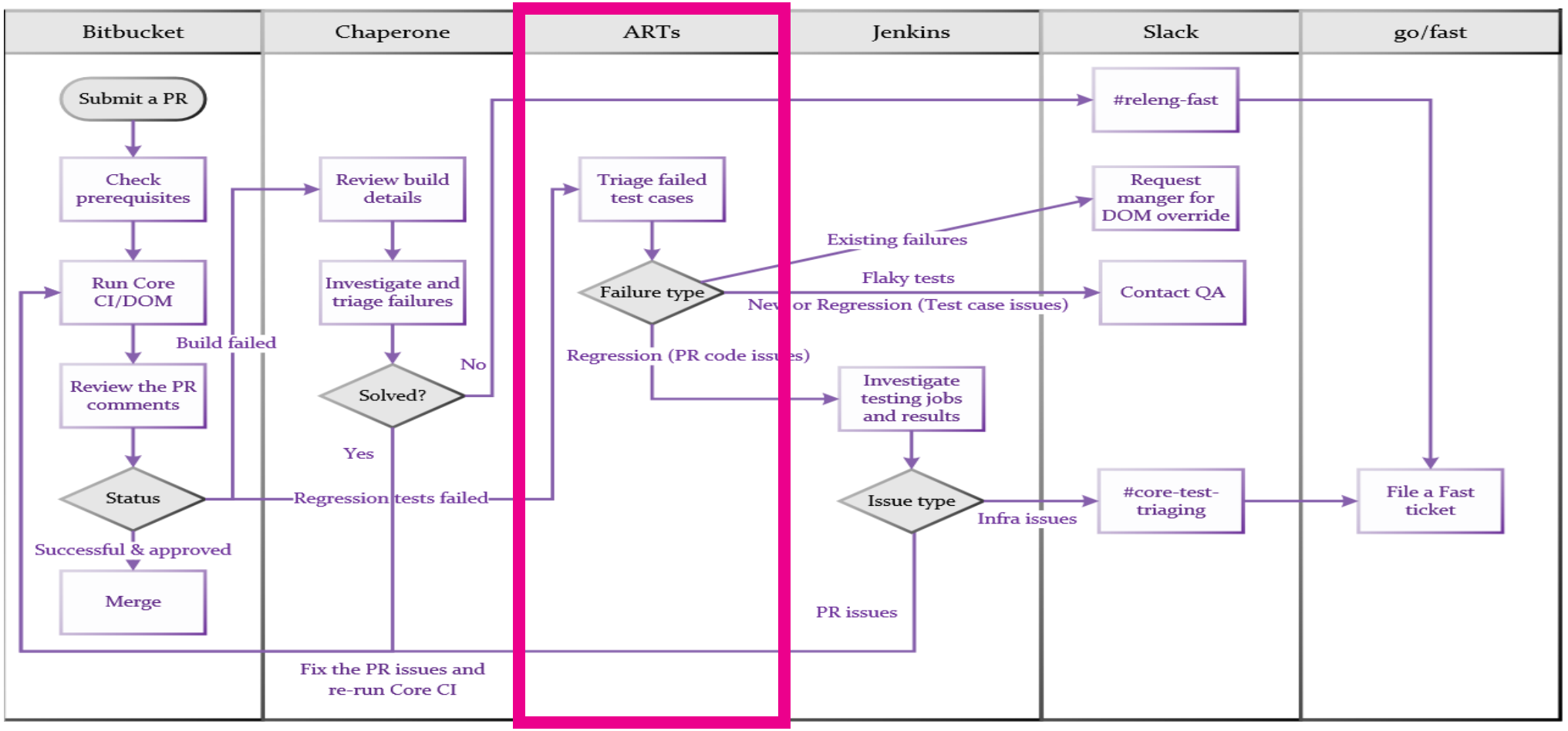


???

Solution

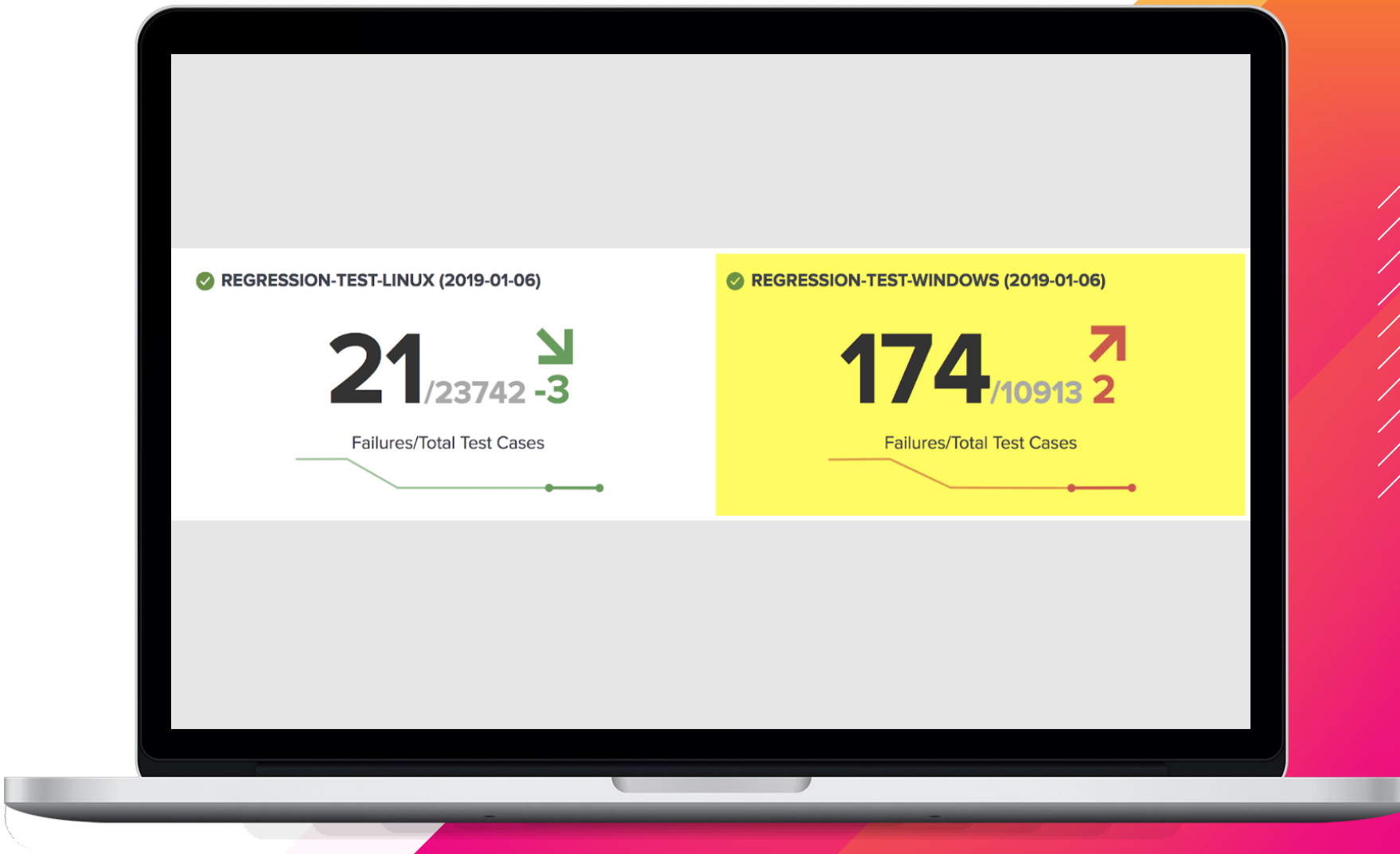


Our CI Workflow



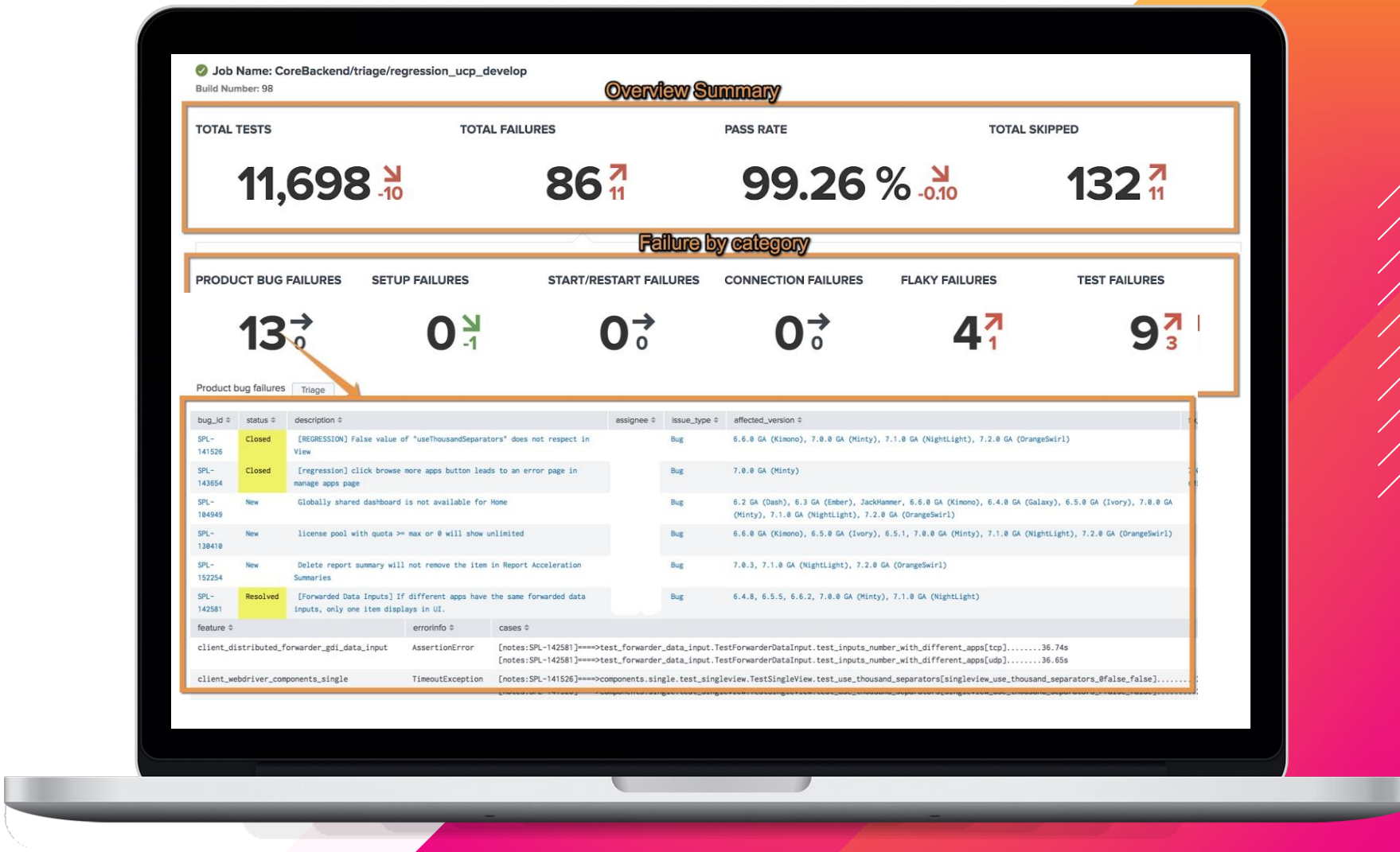
ARTS basic

Overview page



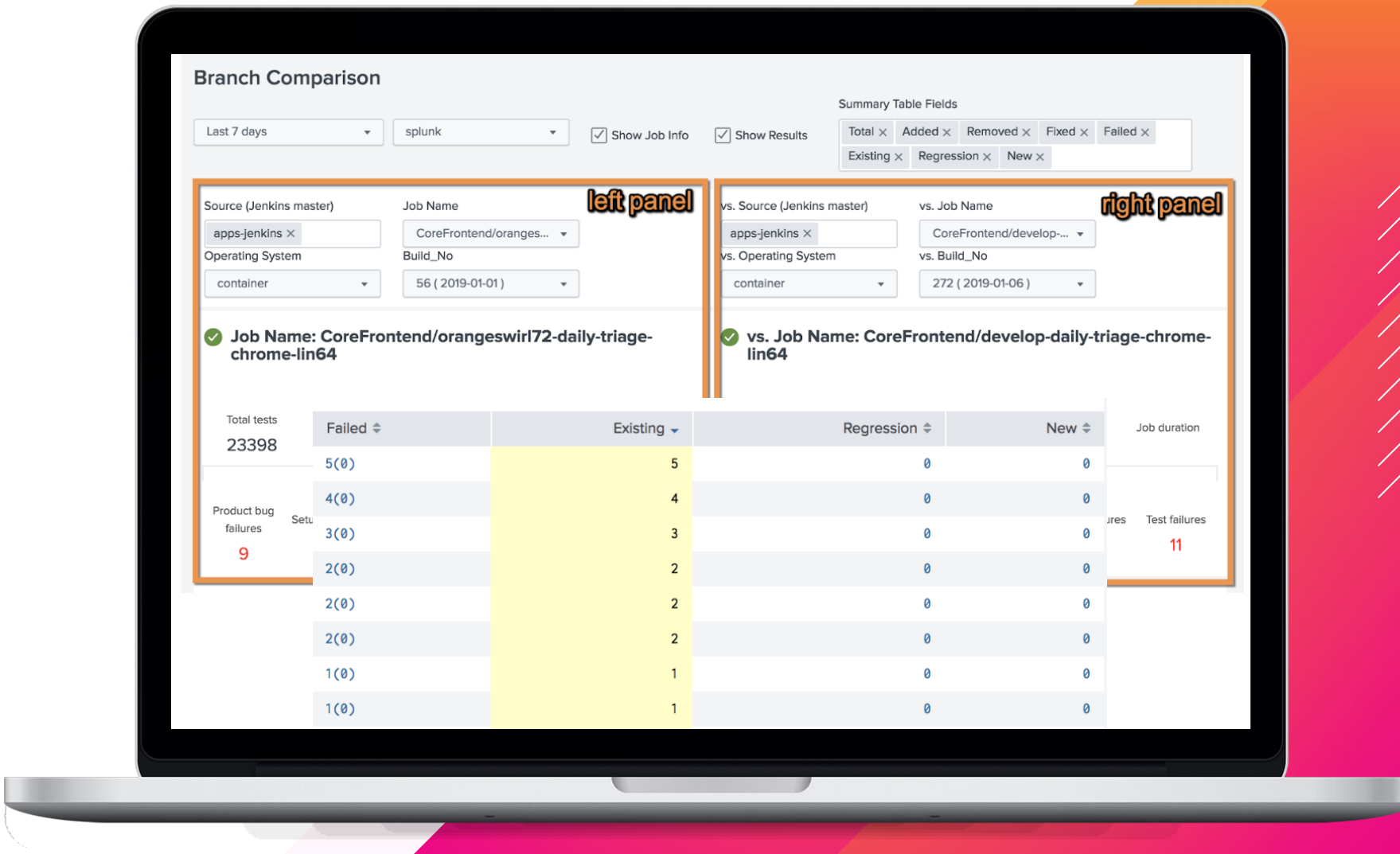
ARTS basic

Trend page



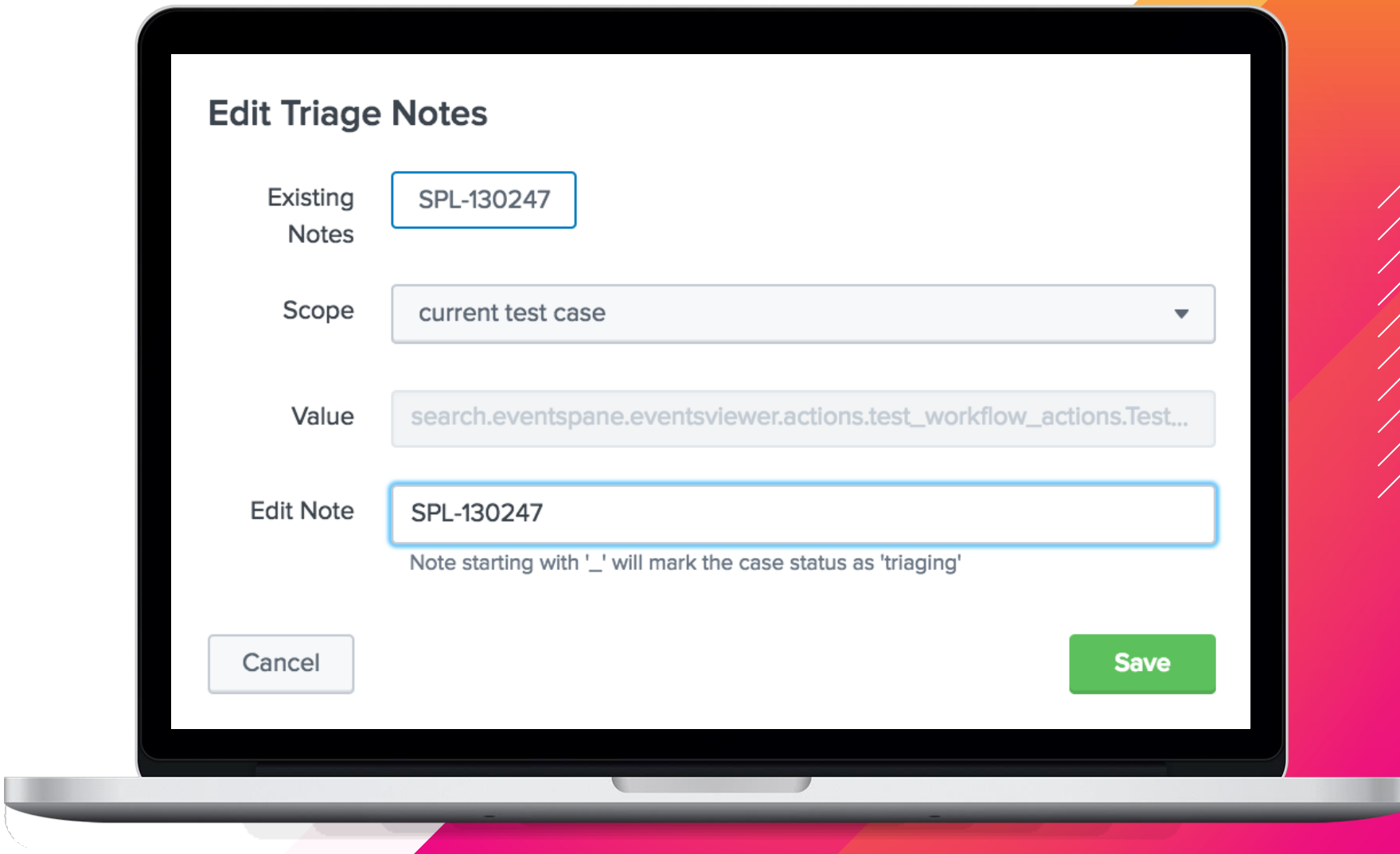
ARTS basic

Branch compare page



ARTS basic

Triage notes

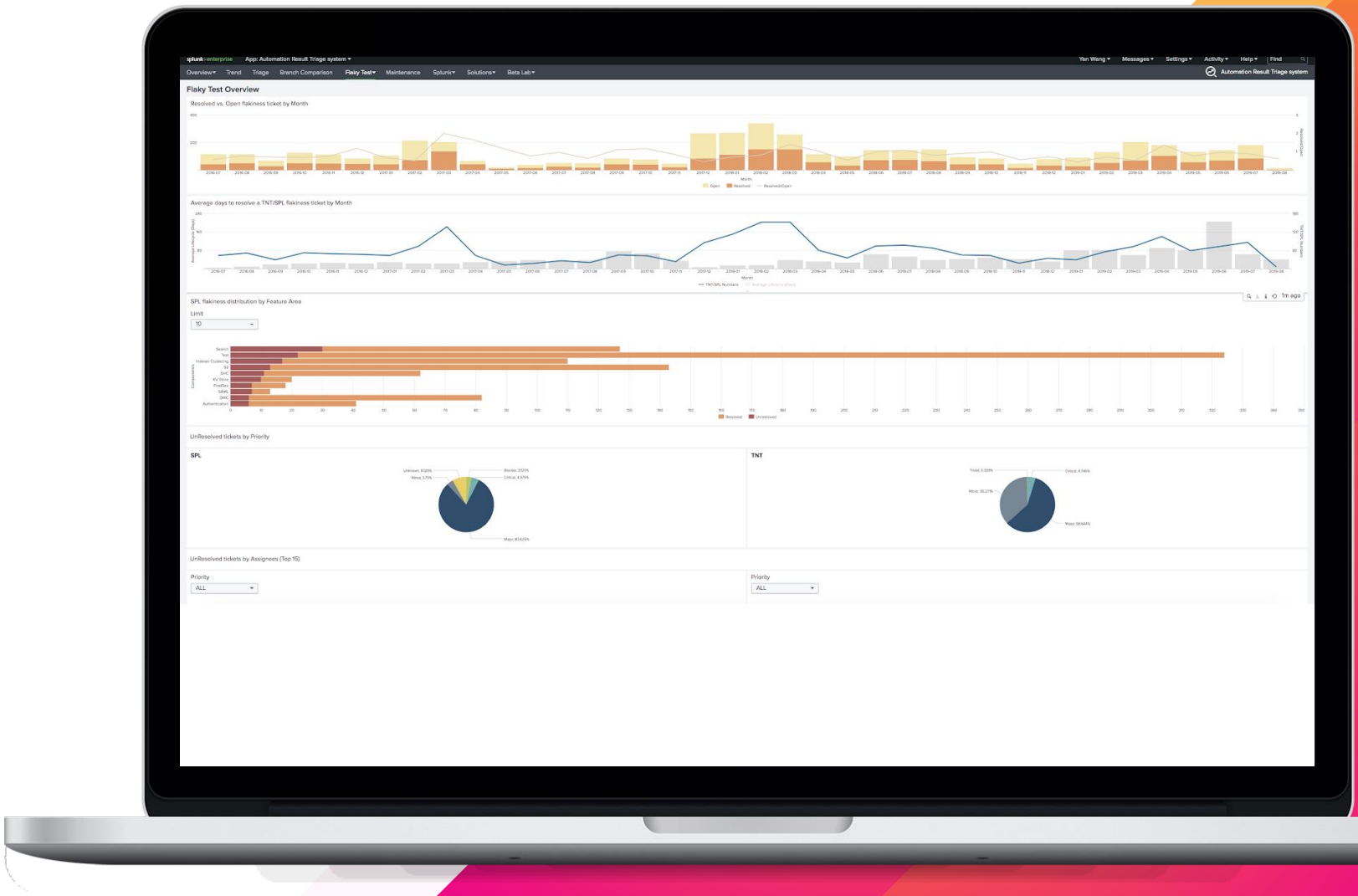


Demo

splunk> .conf19

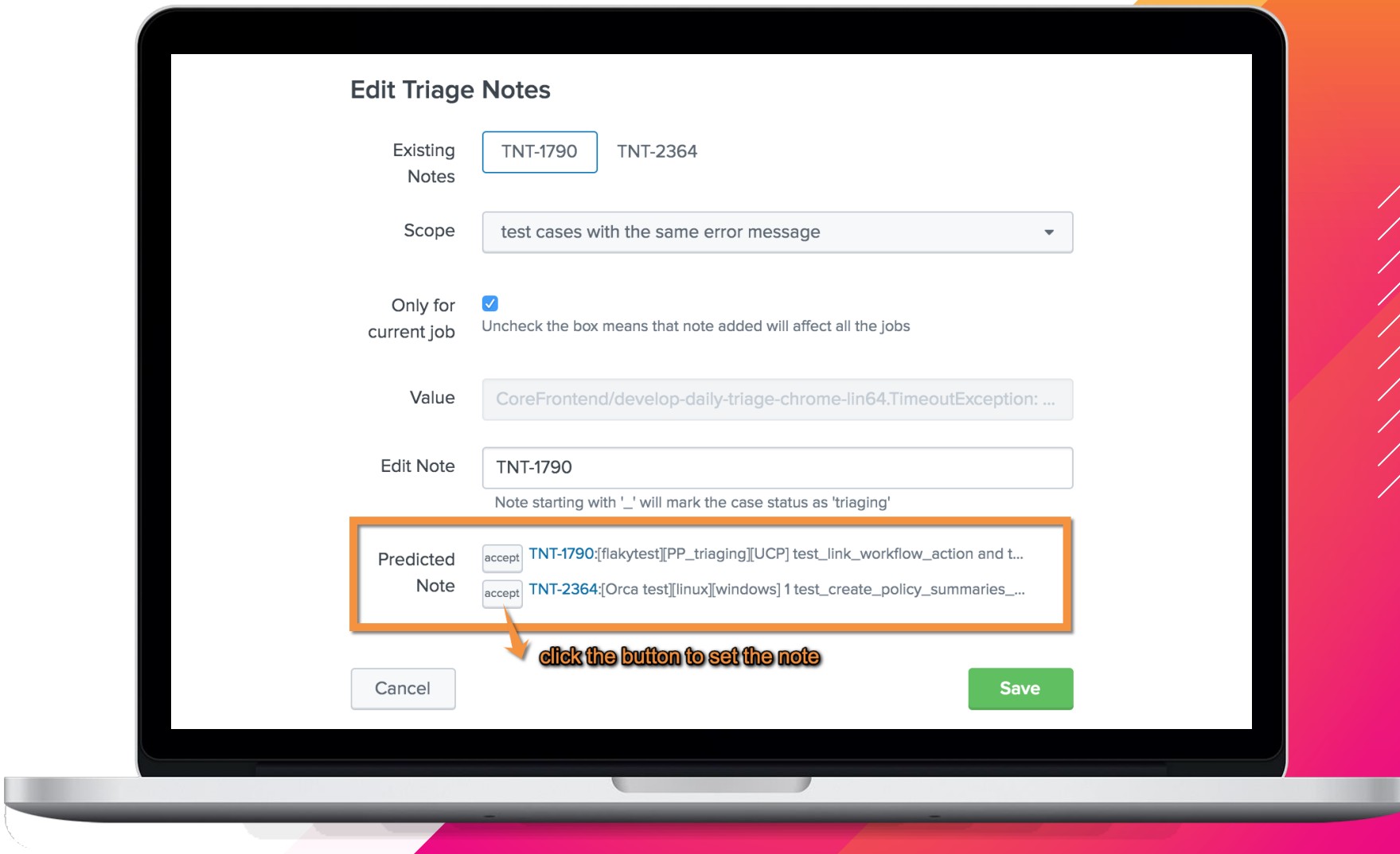
BETA

Flakiness detection



BETA

Predictive Triage



Benefit

Fully automated

Faster response time

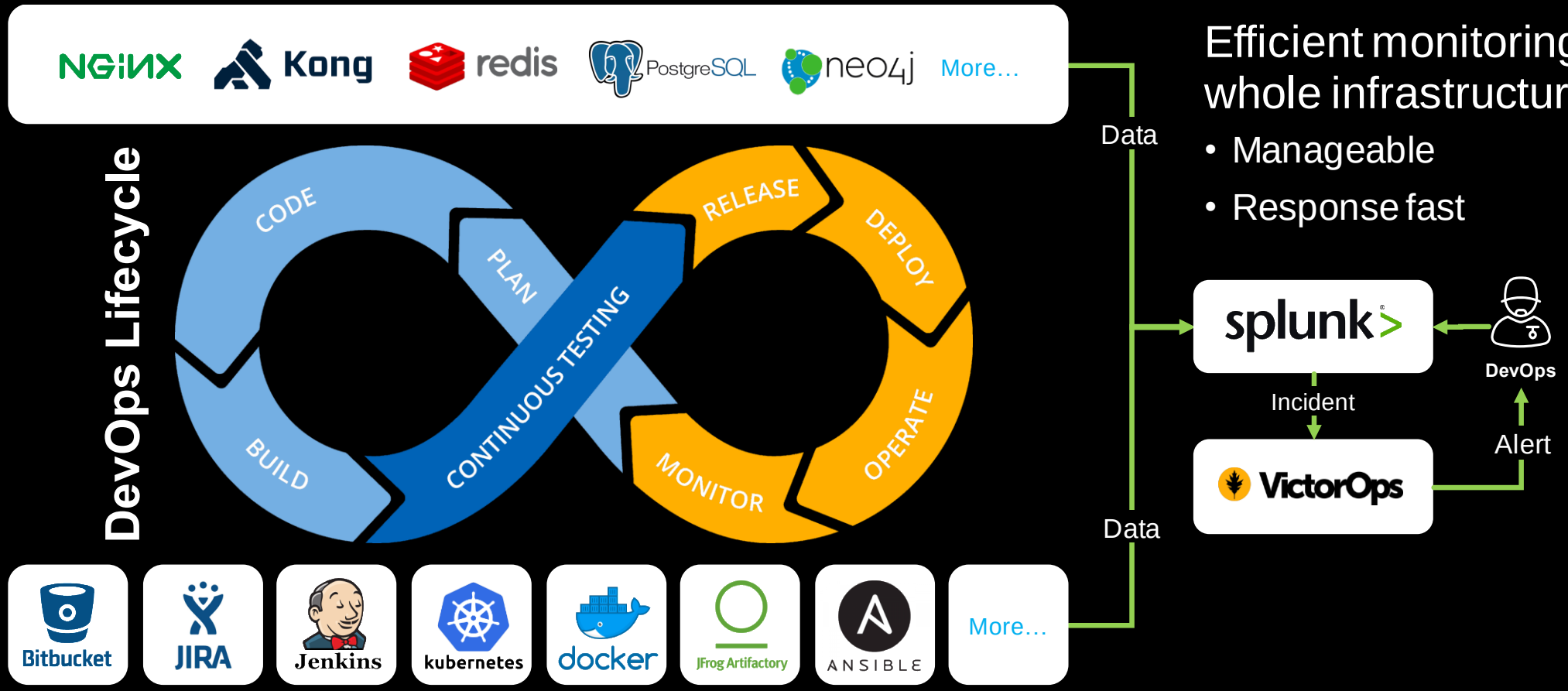
Connected experience

InfraWatch Project

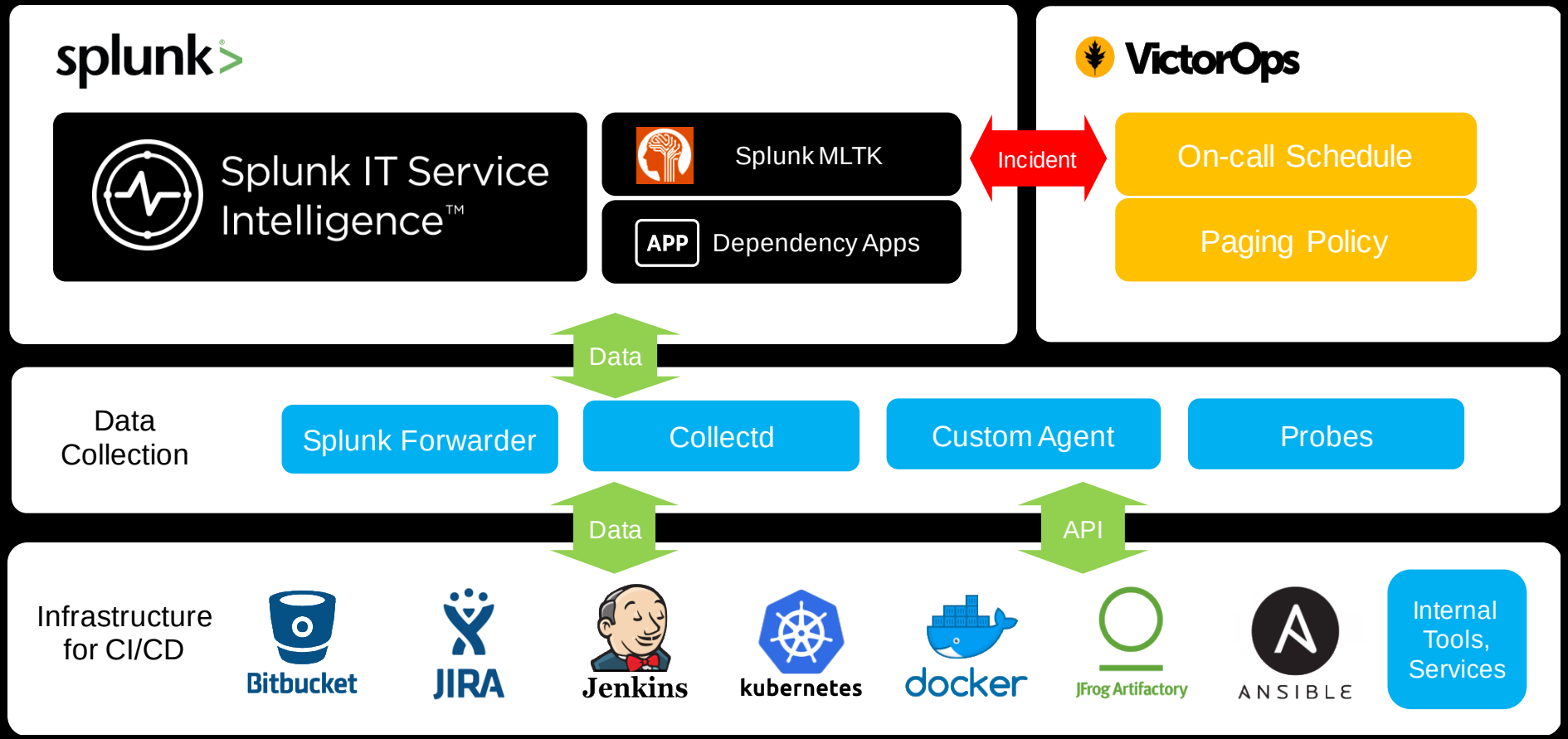
Monitoring the CI/CD Infrastructure Based on Splunk ITSI & VictorOps

splunk> .conf19

Why InfraWatch Project?



Architecture

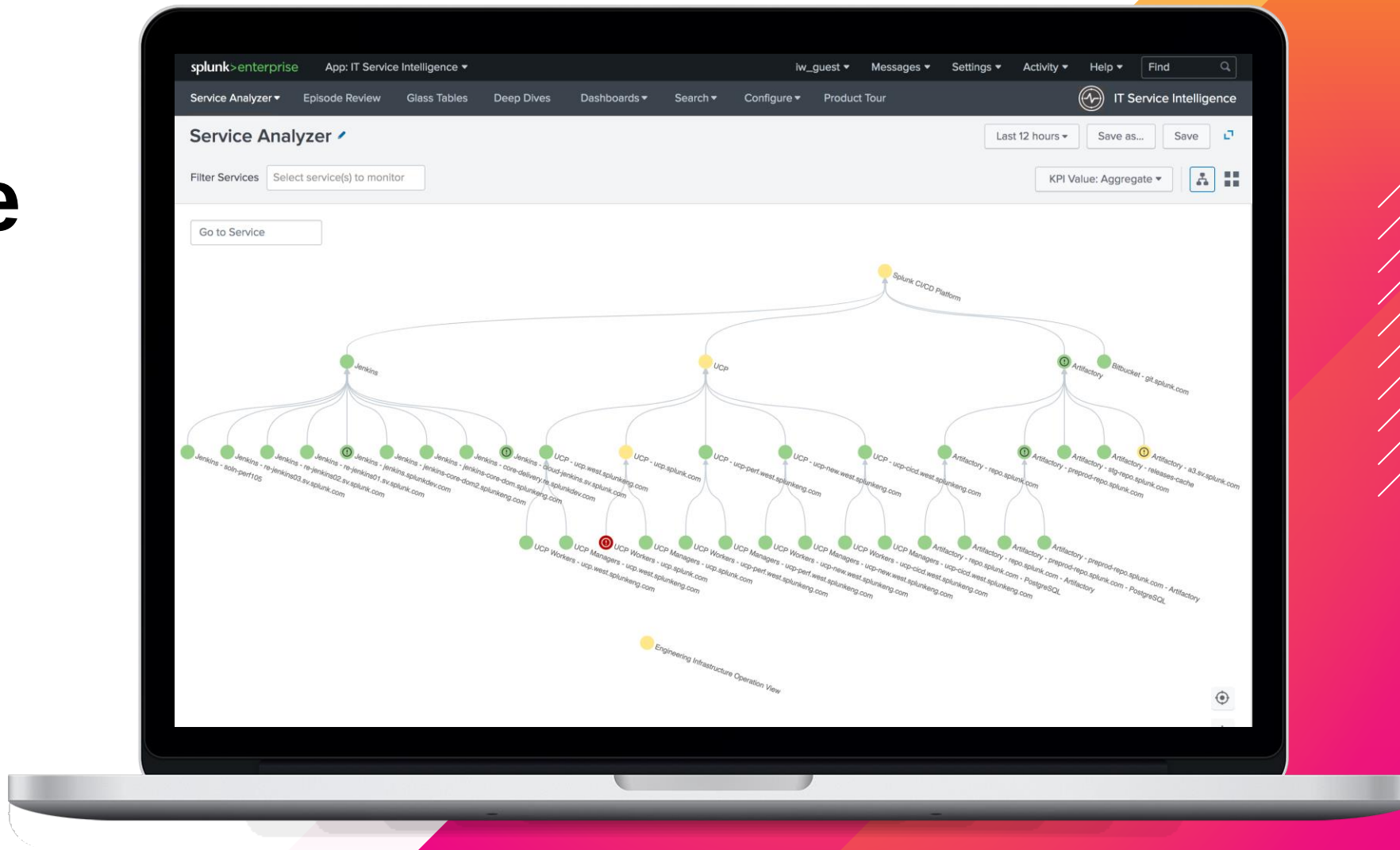


Infrastructure Under Monitoring

In Splunk ITSI

Overview in Splunk ITSI

- Hierarchy of infrastructure
- Health status of services



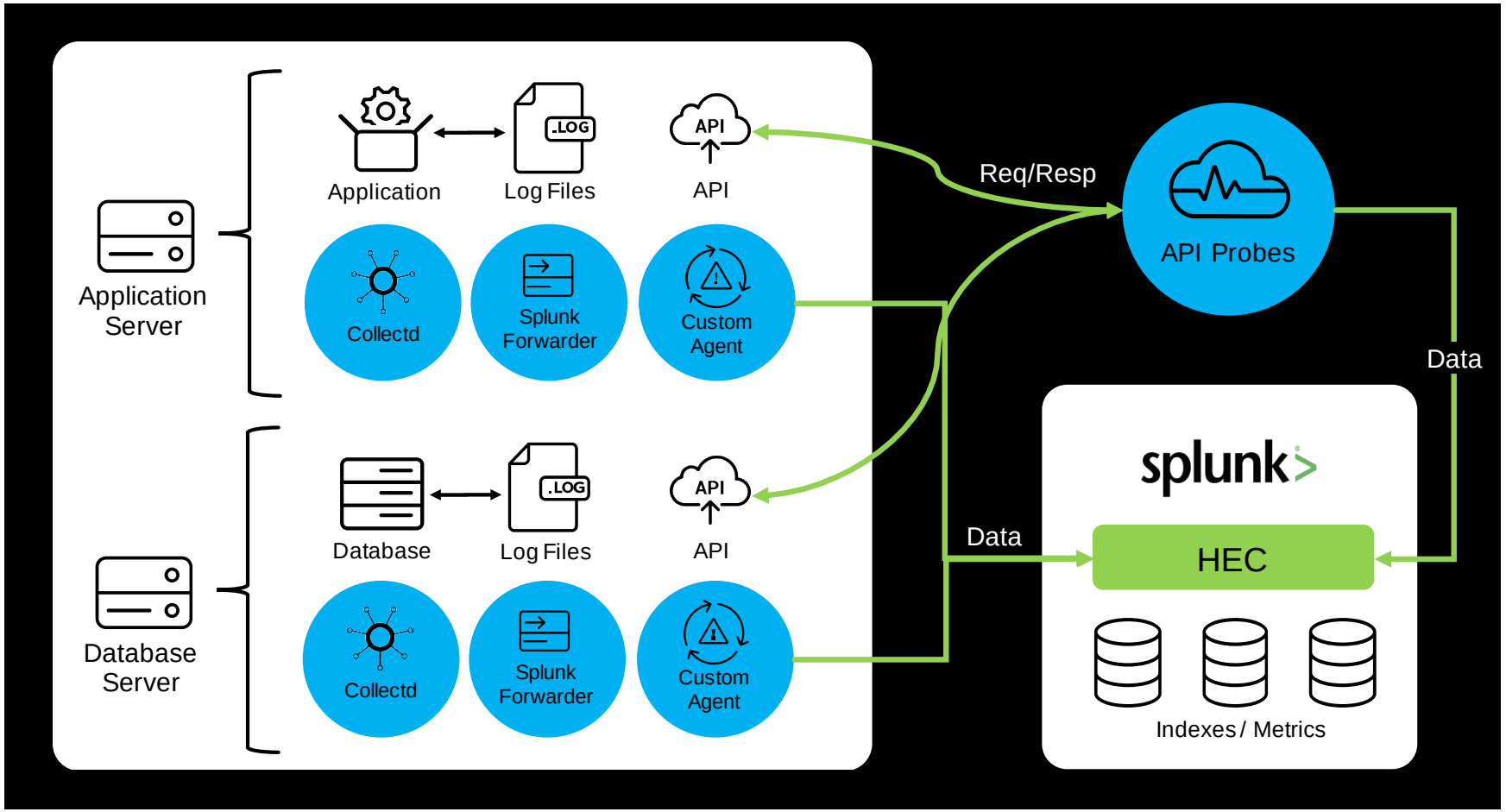
Data Collection

Splunk forwarder
- Log files

Collectd
- Metrics

Custom agent
- Custom data

Custom API probe
- Health check

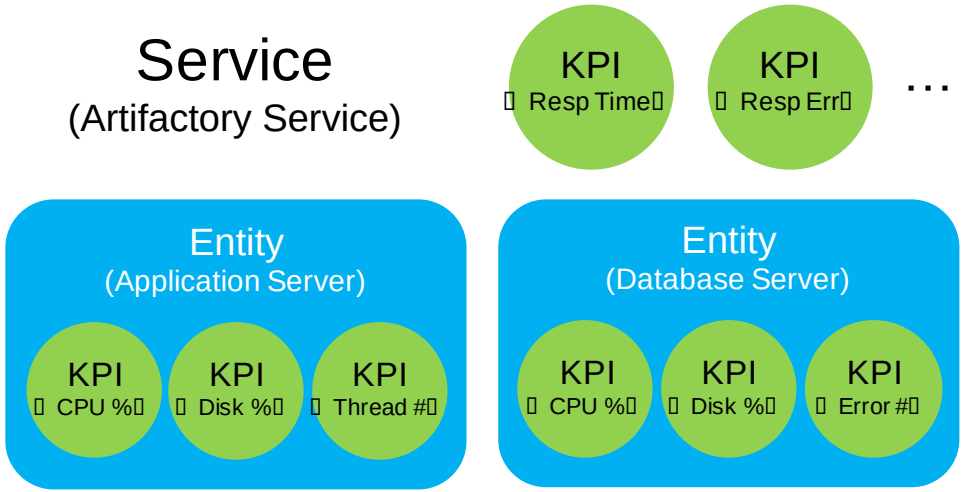


Service Model Setup

In Splunk ITSI

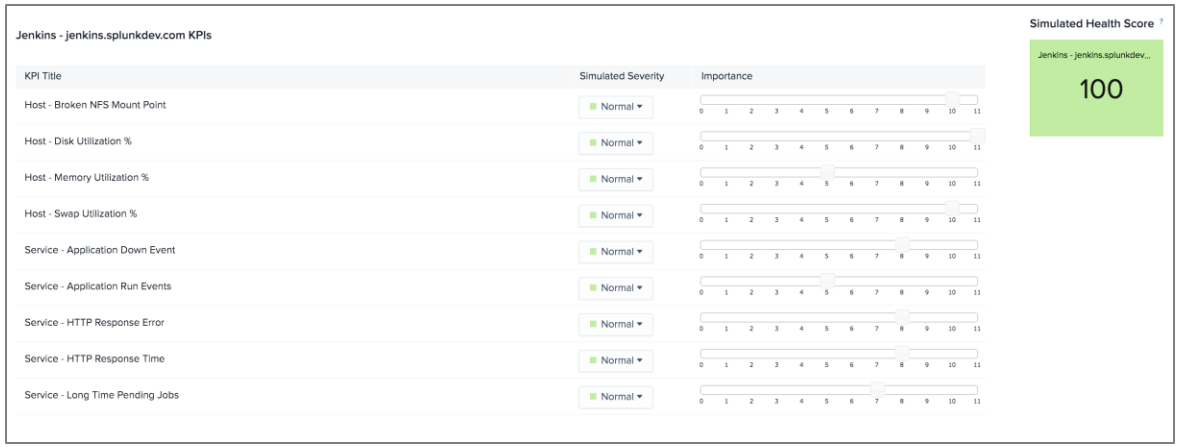
Model used by Splunk ITSI for service status insight

- Service
  - Entity
  - KPI



Health score of service

- 100 in maximum which stands for 100% healthy
- KPI_1 * weight_1 + KPI_2 * weight_2 + …

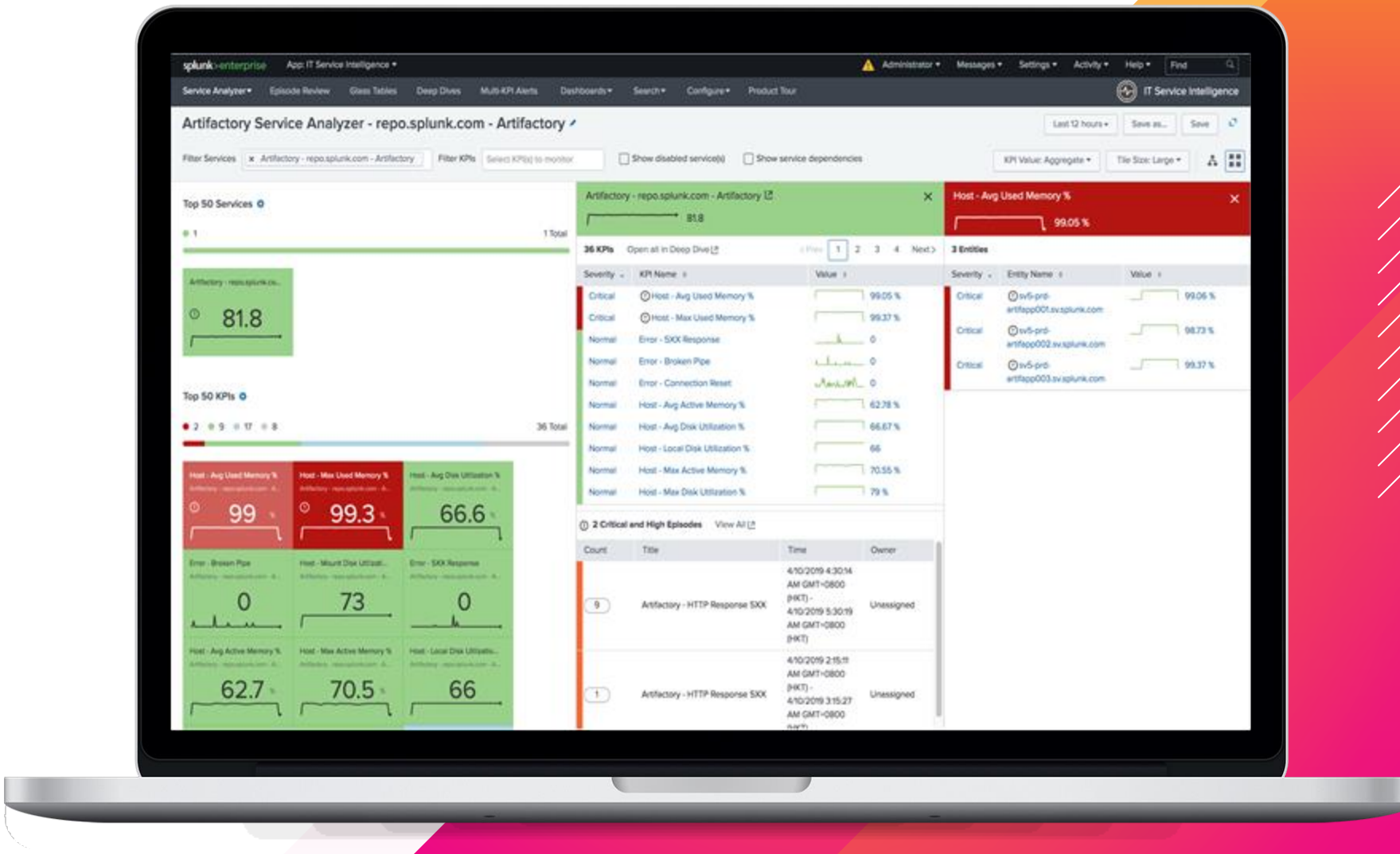


Monitor Model Setup

In Splunk ITSI

Service Analyzer

- Visualize the data model
  - Service, Entity and KPI

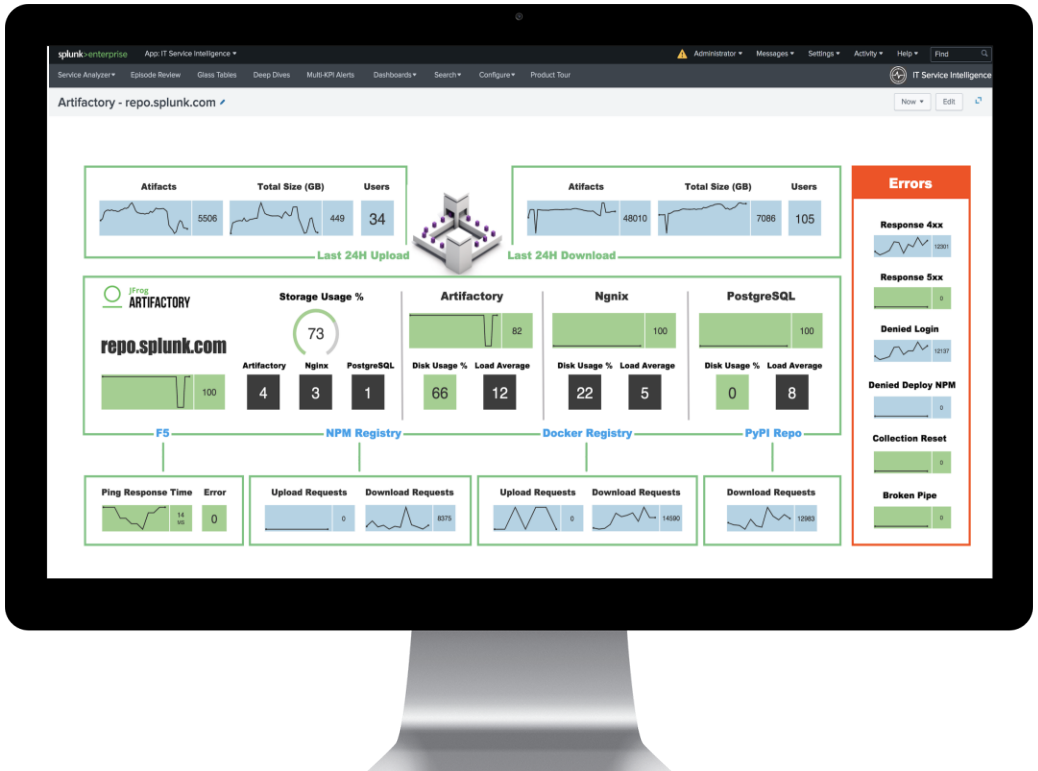


Efficient Visualization

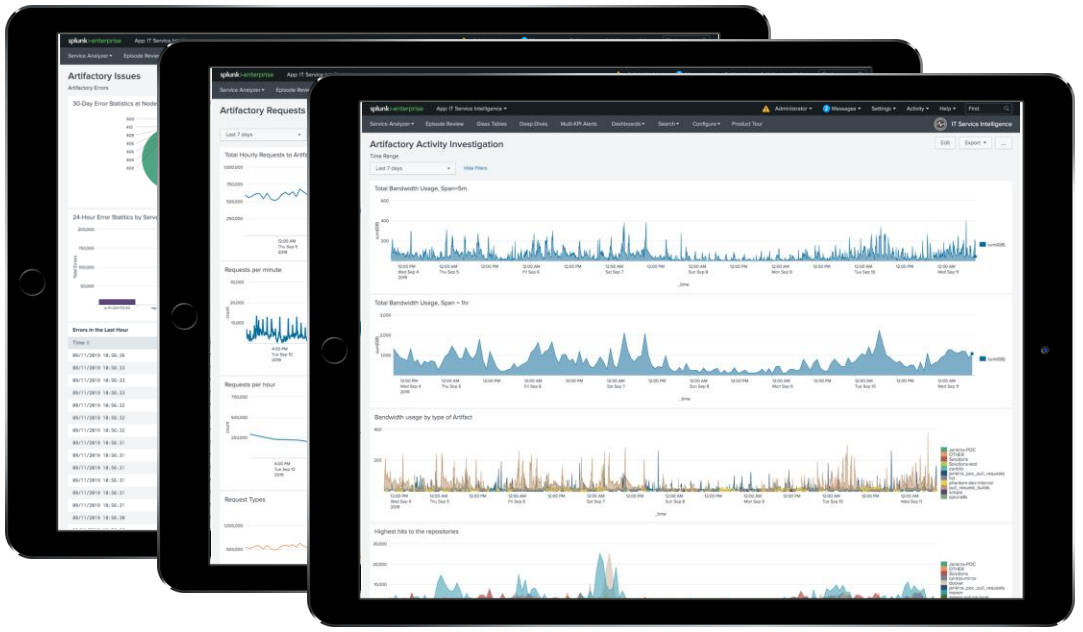
Example for Artifactory in Splunk ITSI

Glass Table

- Custom overview with KPI and non-KPI metrics



Dashboards approachable via drill down from glass table



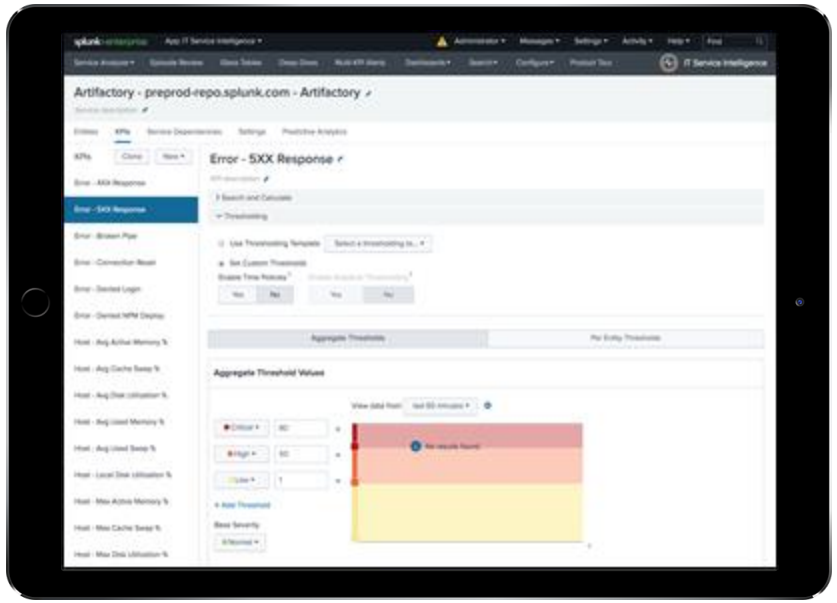
splunk> .conf19

Incident Alert Setup

In Splunk ITSI

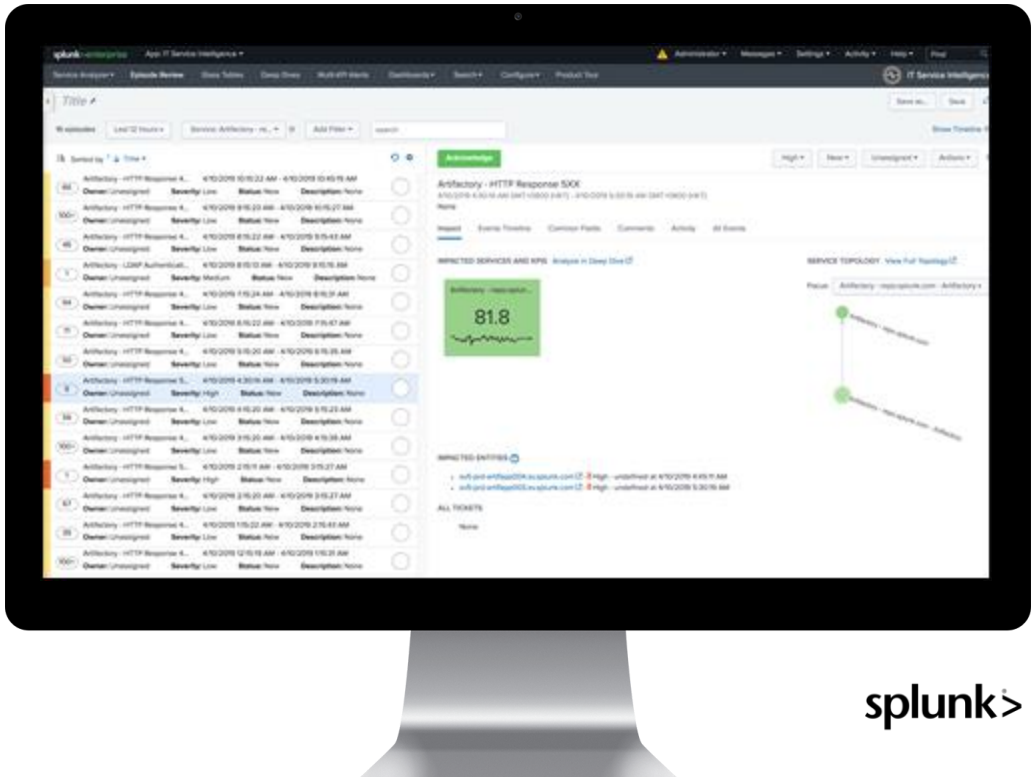
Source of incident

- Ad-hoc SPL query
- KPI



Aggregation Policy

- Aggregate by time, title, etc.
- Trigger necessary alerts in severity levels
- Send alerts to VictorOps



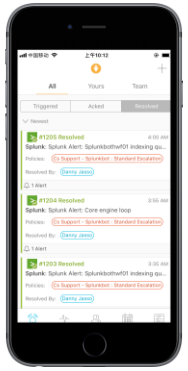
Incident Alert Management

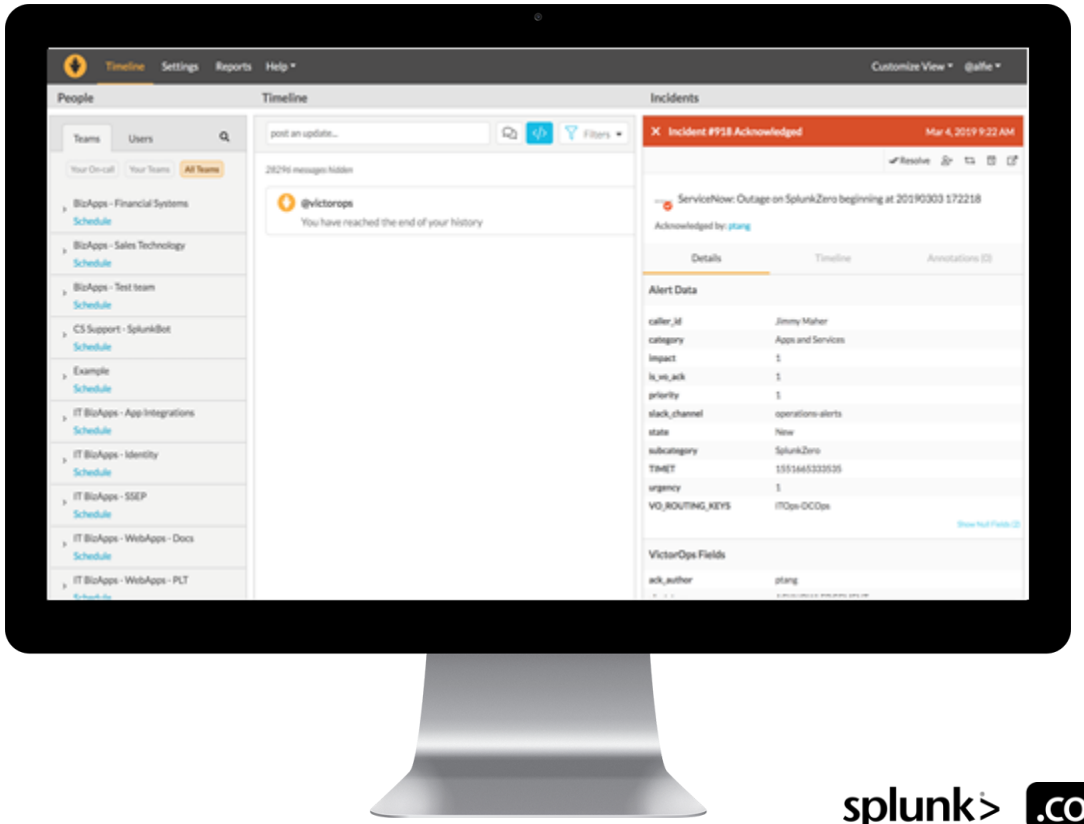
Engineers response alerts in VictorOps

- For incident management via browser or mobile app

Splunk IT Service Intelligence™

INCIDENT





splunk> .conf19

VictorOps Highlights

Incident handling

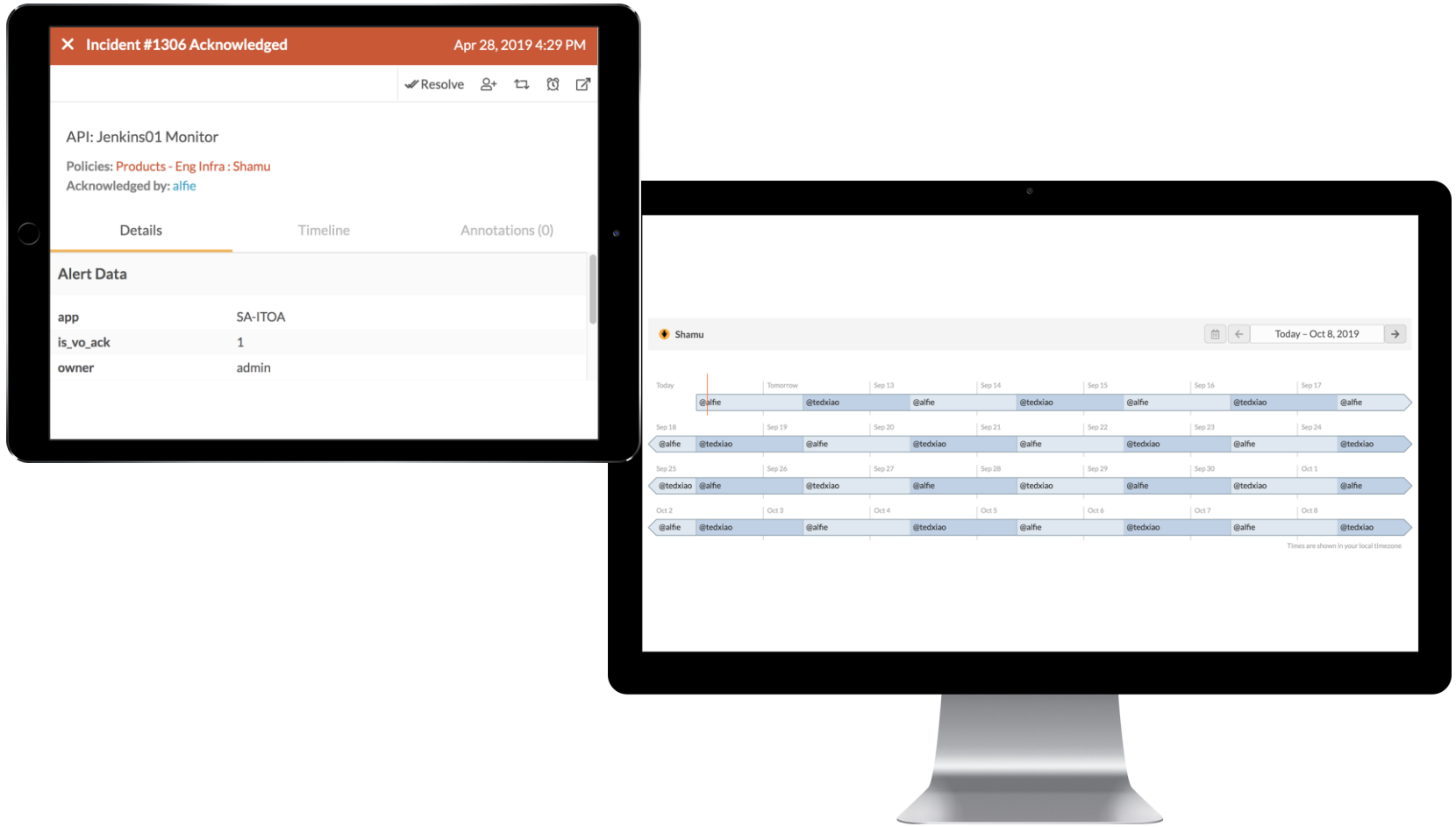
- Acknowledge / snooze / resolve an incident
- Route to other engineers

On-call schedule

- For example, follow-the-sun model

Escalation policy

- For example, notifying tier 2 engineer if an alert is not acknowledged by tie 1 in 10 minutes



Benefits

Centralize monitoring/alerting for the whole infrastructure

Setup monitoring for broader applications/services/tools in two steps

- Step #1, Collect data into Splunk
- Step #2, Define Service/Entity/KPI model in Splunk ITSI

Shorten MTTR efficiently

- Get insight on the whole infrastructure in time
- Collaborate efficiently on solving incidents

Q&A

tyou@splunk.com
slu@splunk.com

splunk> .conf19

.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION