Automate Your IT! Moving Faster with Puppet and Splunk

Domnick Eger | Global DevOps Practitioner
Chris Barker | Partner Engineering

October 2018 | Version 1.0

Today's Precentors

DOMNICK EGER

Global DevOps Practitioner
from Splunk

CHRIS BARKER

Senior Principal Integration Engineer
from Puppet

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance 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 could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

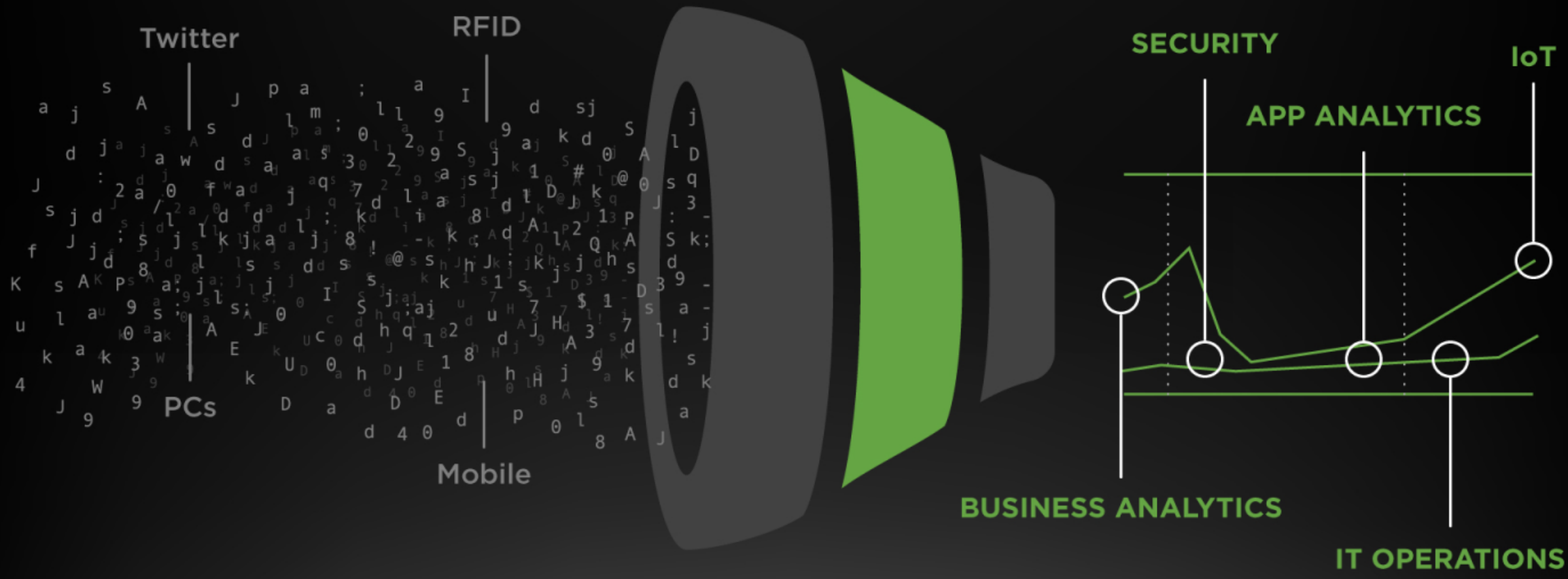
The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. 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 functionality described or to include any such feature or functionality in a future release.

splunk> .conf18

What is Splunk ?

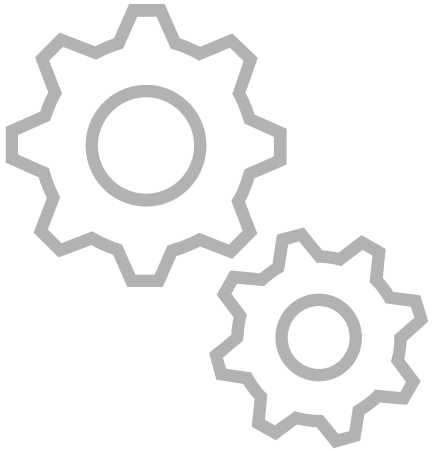
Quick Intro Into the Machine Data Fabric

Splunk Turns Machine Data Into Answers.

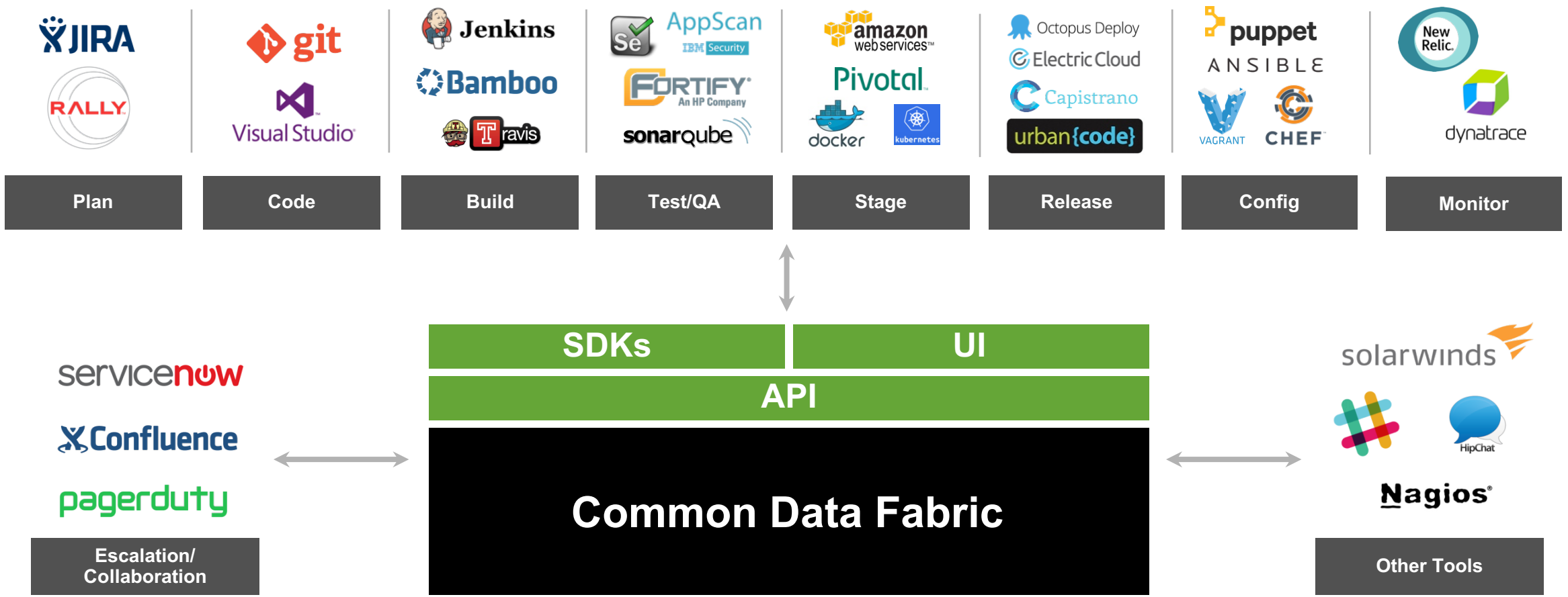


Why Splunk ?

- FAST TIME-TO-VALUE
- ONE PLATFORM, MANY USE CASES
- VISIBILITY ACROSS STACK--NO SILOS
- ASK ANY QUESTION OF DATA
- ANY DATA, ANY SOURCE



The Dev Lifecycle is Complex



Splunk Solutions

Splunk Premium Solutions

- Splunk IT Service Intelligence™
- Splunk Enterprise Security™
- Splunk User Behavior Analytics™

1,000+ Apps and Add-Ons

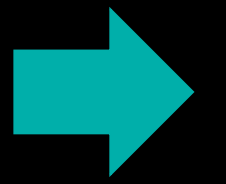
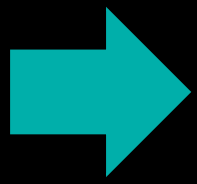
Microsoft .NET, docker, puppet, cisco, kepware, now, NetApp, aws, linux

splunk>enterprise

splunk>cloud

splunk> Platform for Operational Intelligence

splunk> .conf18

Baseline  Analyze  Act

(if you remember only one thing from this talk, this is that thing)


Using Puppet and Splunk independently is good.
But using them together is great!

Splunk + Puppet Complementary Capabilities

Baseline

- System metadata
- Deep system inspection
- Container contents
- Network device interrogation
- APIs
- Community plugins

Analyze

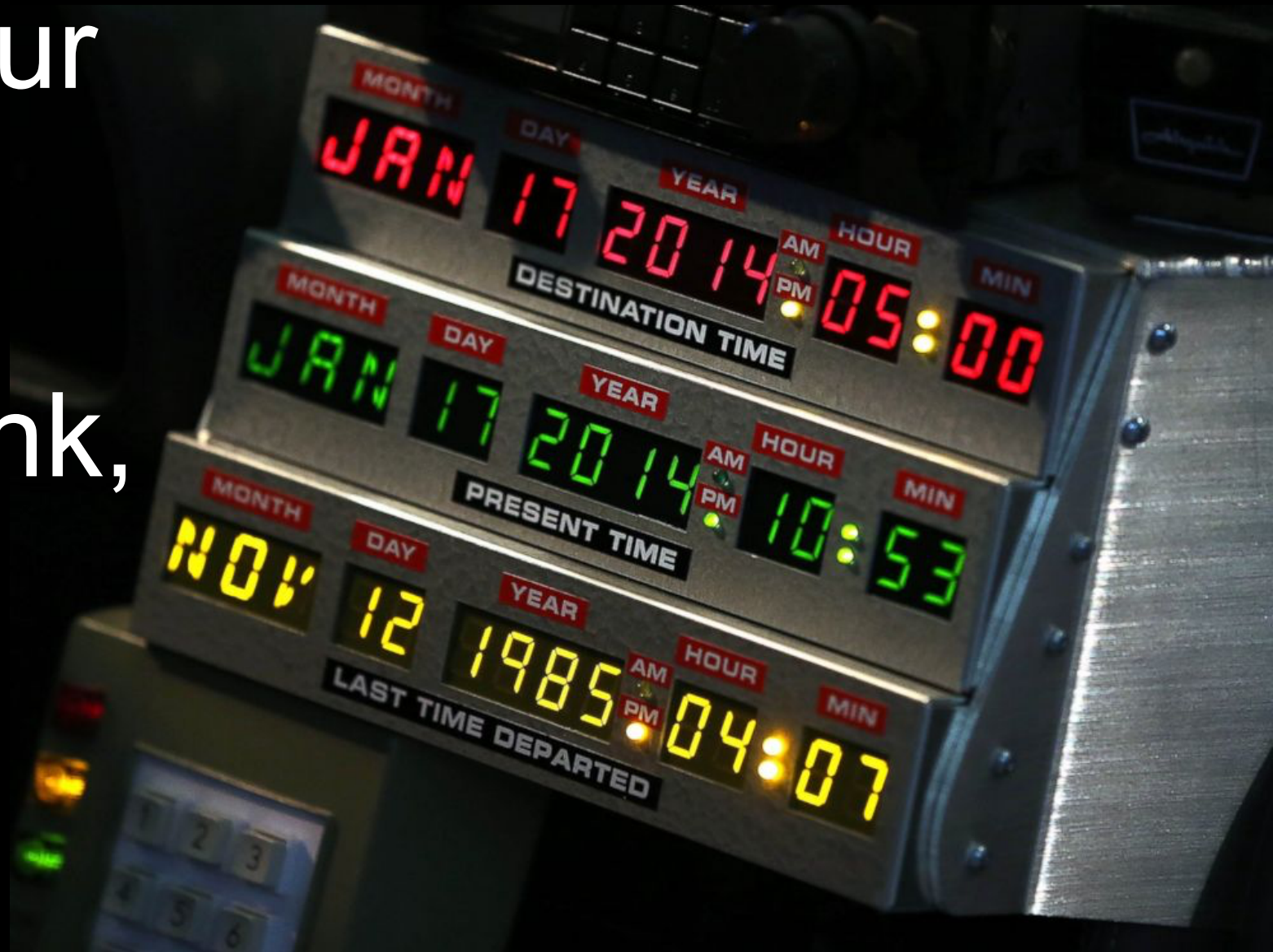
- Splunk server
- Splunk agent
- Bundles
- Modules
- Query language
- Alerts
- Machine learning
- Anomaly detection
- ITSI
- PuppetDB
- PE reporting

Act

- Reconfigure agents
- Puppet agent
- Puppet code / models
- Reconfigure systems
- Re-discovery

Puppet Splunk

Connect all your systems, past, present, and future, to Splunk, automatically!



But that's just the beginning of a long list of possibilities!

Demo

Integrations and Technology Preview

Splunk App and Add-On for Puppet Enterprise

Overview and Demo

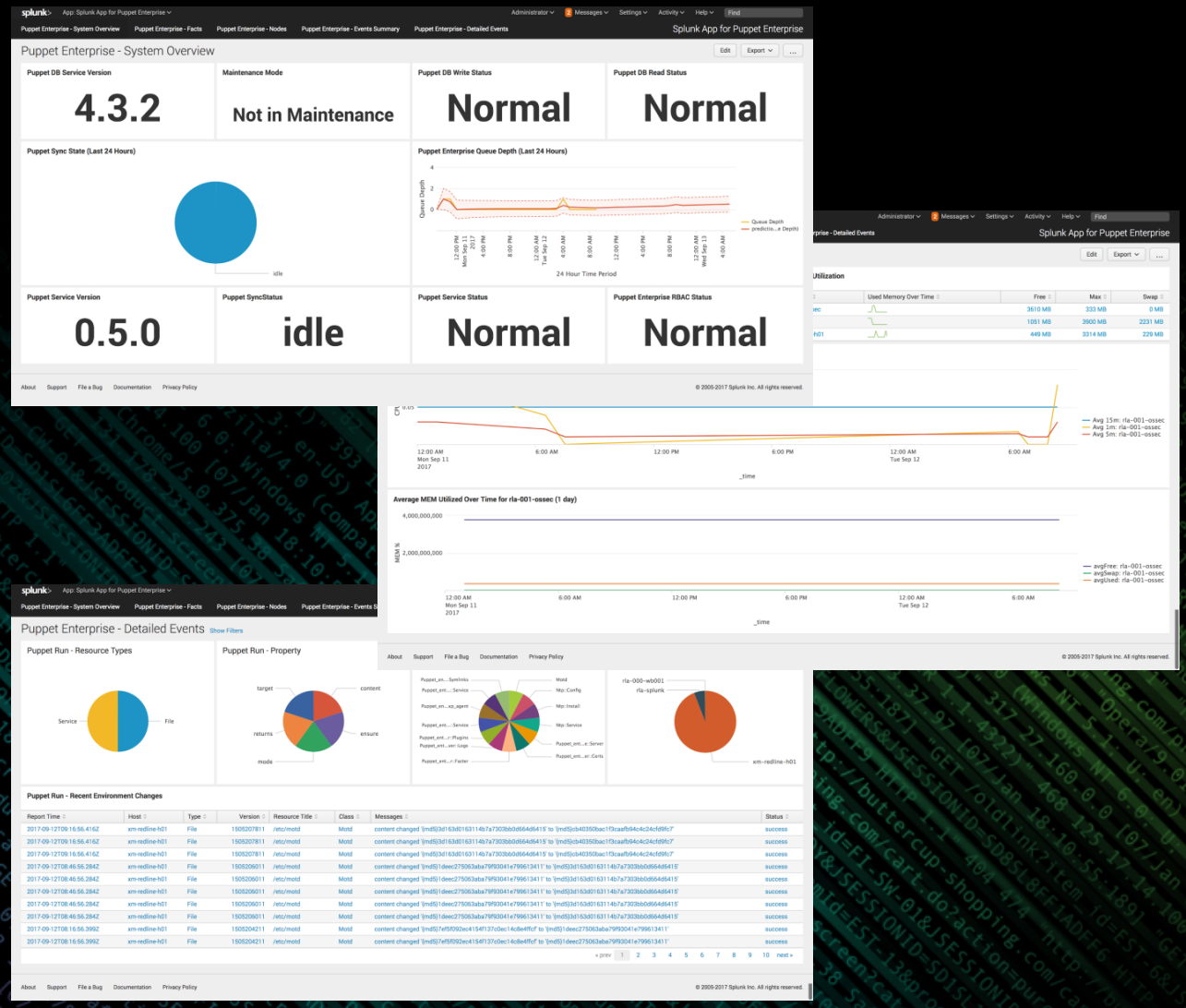
splunk> .conf18

Splunk App for Puppet Enterprise

Discover and monitor the health of all resources under management

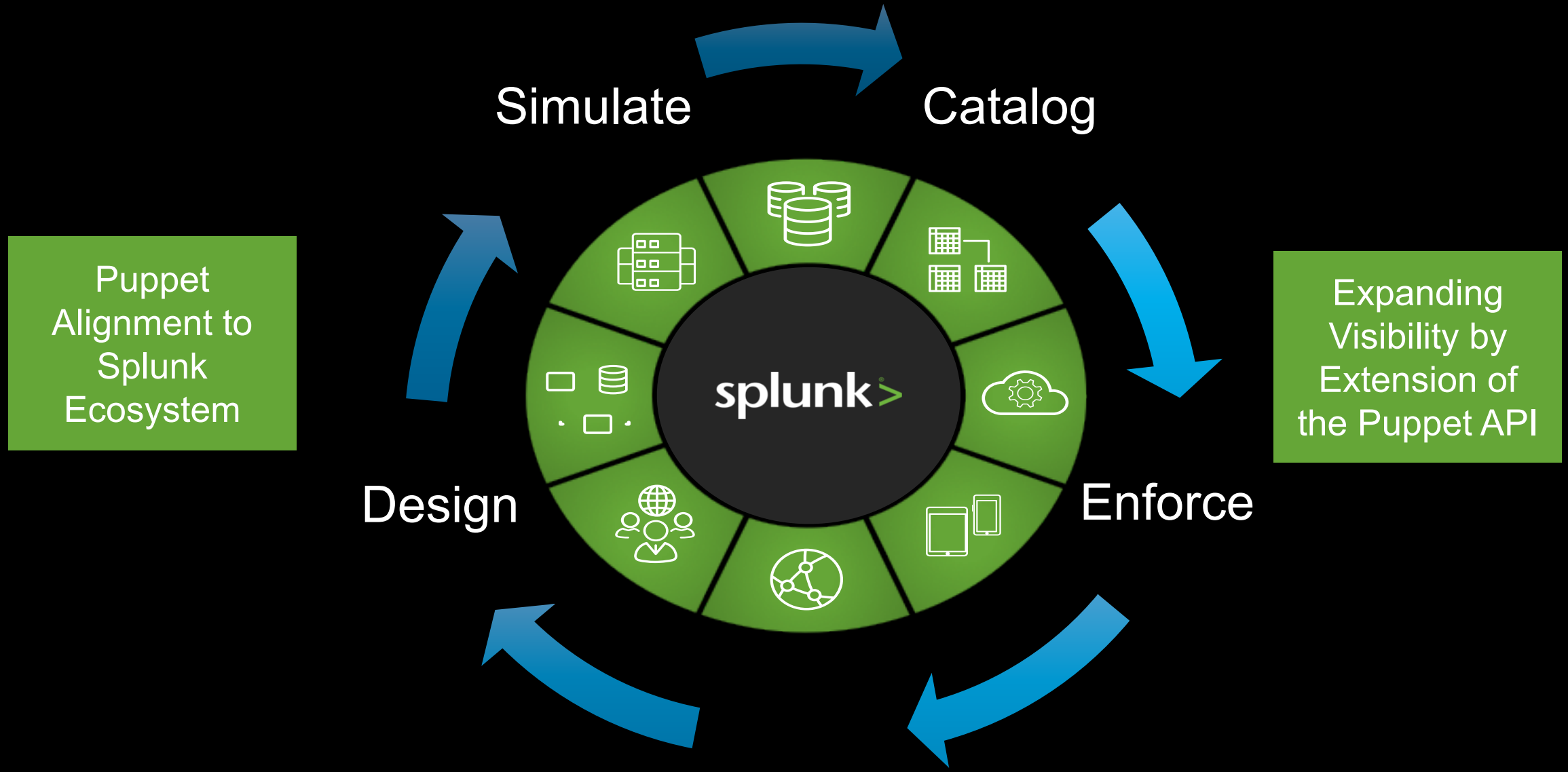
Ingest all data from Puppet Enterprise and correlate that data across your entire tech stack

Visualize your Puppet data with out of the box dashboards for easy troubleshooting



splunk> .conf18

Current Discussion and Integration



Puppet Tasks for Splunk

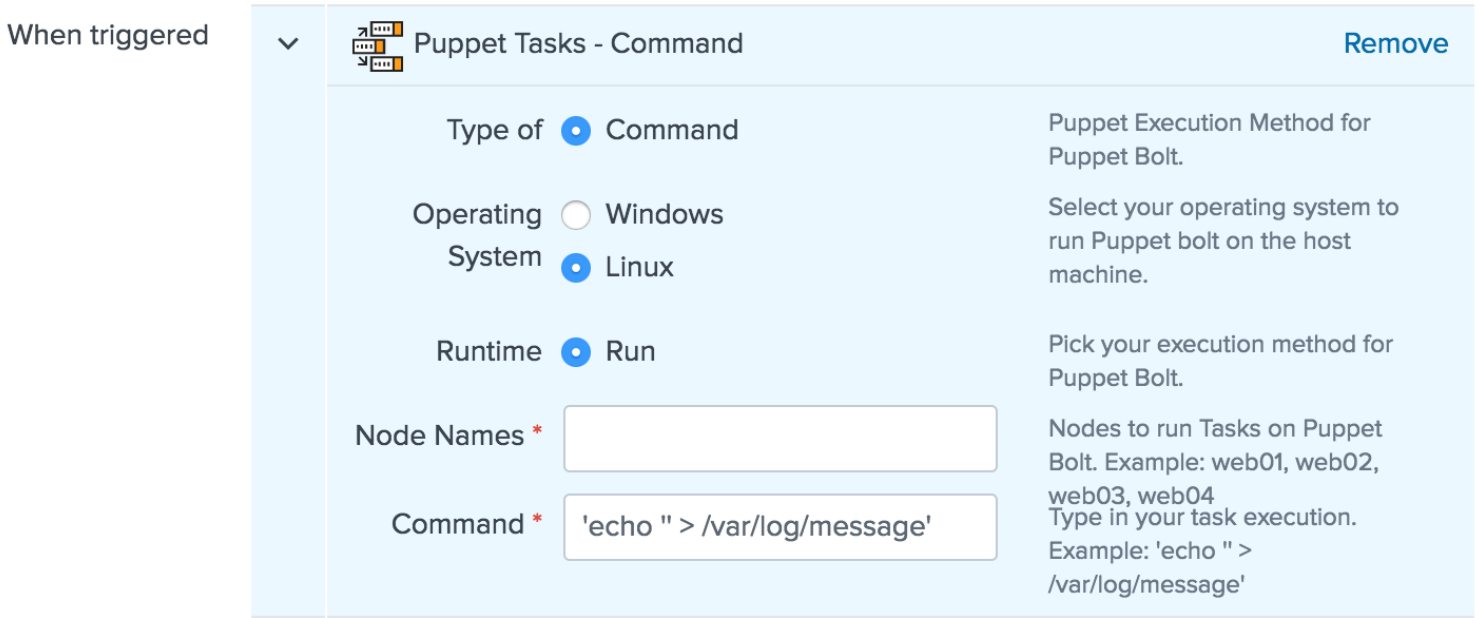
Integration Guide

splunk> .conf18

Puppet Task via Bolt: Commands

Basic Use Case: Disk space on Linux server exceeds 90%. Instead of logging into the server to clear disk space, let chain a few commands together to clear the space on a specific servers when Splunk registers 90% utilization.

Splunk Search for Alerts: sourcetype=df | multikv | dedup host,Filesystem | search MountedOn="/mnt/sansmount" | rex field=UsePct "(?<usage>\d+)" | where usage>90 | eval _raw="Filesystem "+Filesystem+" (mount point "+MountedOn+") on host "+host+" is "+UsePct+" full!" | fields - *



Puppet Tasks Command:

Splunk triggers Puppet Bolt through Puppet Tasks for Splunk. Admin sets command, operating system and runtime. Types out nodes and command.

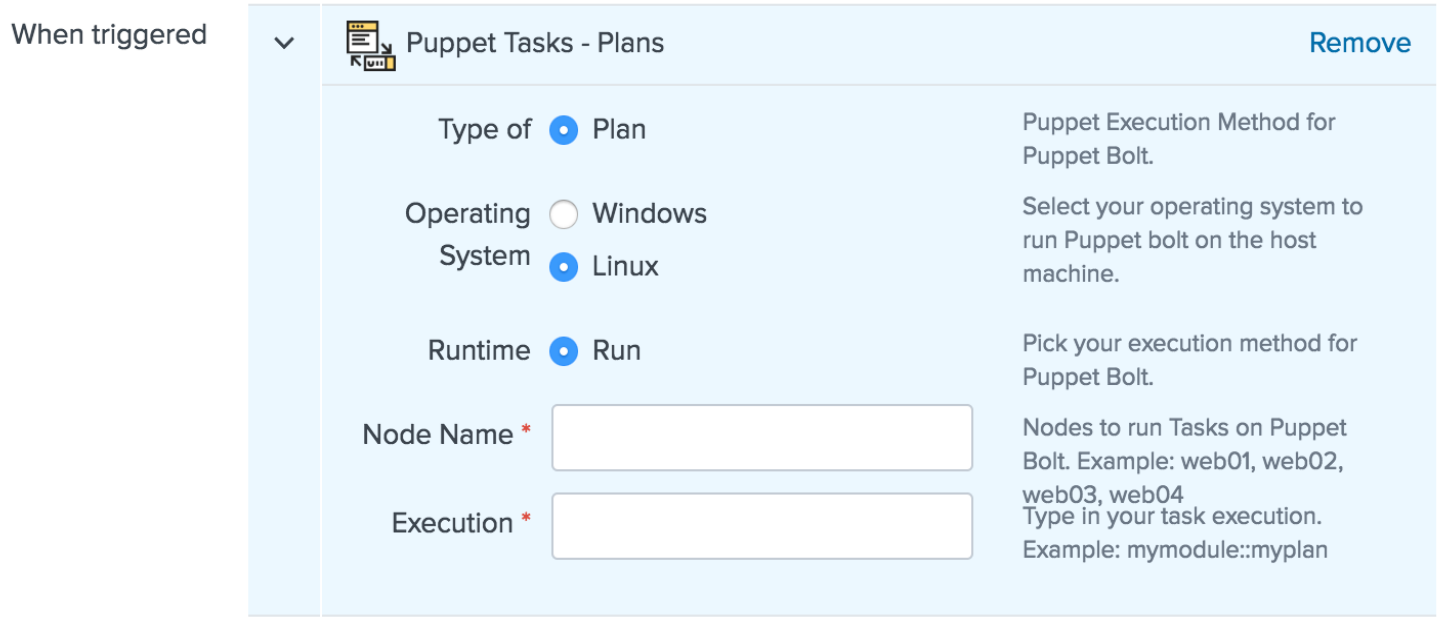
Execution:
'echo '' > /var/log/message && echo '' > /var/log/nginx/access.log

splunk> .conf18

Puppet Task via Bolt: Plans

Basic Use Case: Disk space on Linux server exceeds 90%. Instead of logging into the server to clear disk space, let chain a few commands together to clear the space on a specific servers when Splunk registers 90% utilization.

Splunk Search for Alerts: sourcetype=df | multikv | dedup host,Filesystem | search MountedOn="/mnt/sansmount" | rex field=UsePct "(?<usage>\d+)" | where usage>90 | eval _raw="Filesystem "+Filesystem+" (mount point "+MountedOn+") on host "+host+" is "+UsePct+" full!" | fields - *



Puppet Tasks Command:

Splunk triggers Puppet Bolt through Puppet Tasks for Splunk. Admin sets command, operating system and runtime. Types out nodes and plan name.

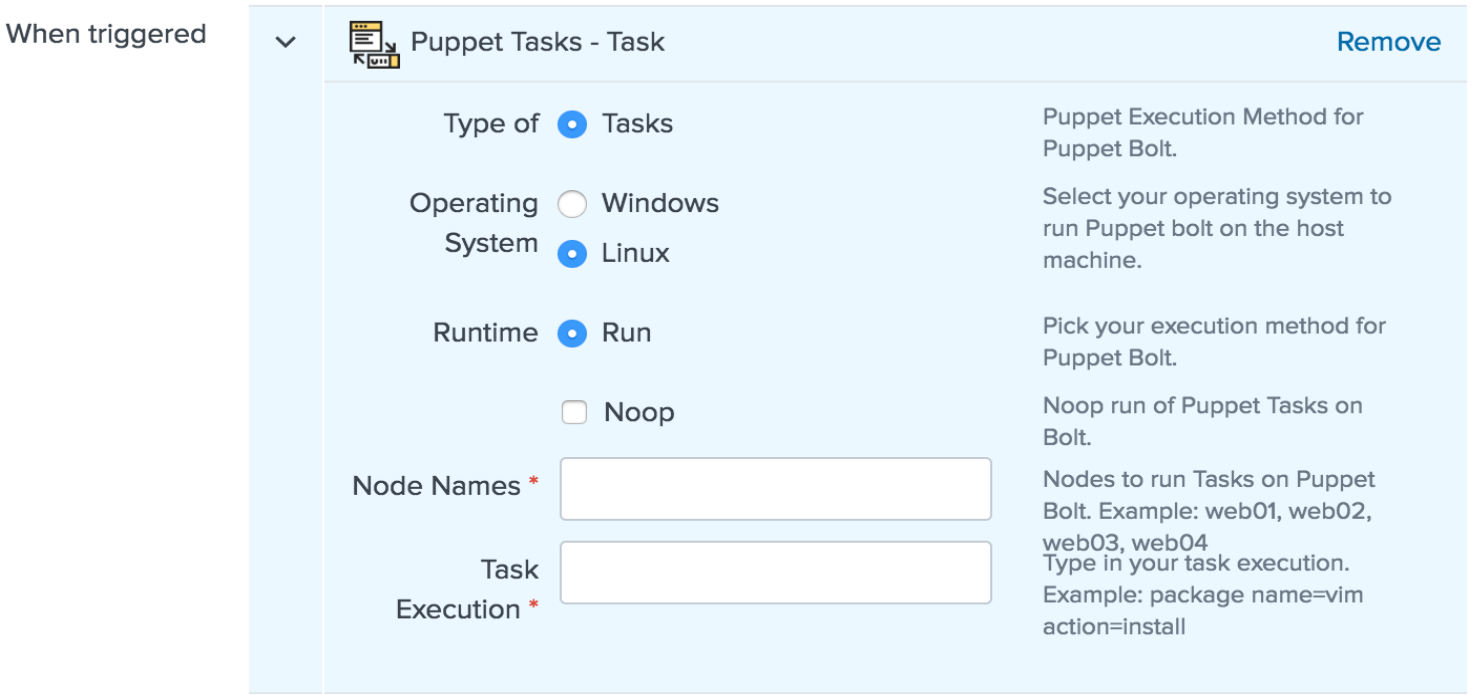
Execution:
“webserver::cleanupmess”

splunk> .conf18

Puppet Task via Bolt: Tasks

Basic Use Case: Disk space on Linux server exceeds 90%. Instead of logging into the server to clear disk space, let chain a few commands together to clear the space on a specific servers when Splunk registers 90% utilization.

Splunk Search for Alerts: sourcetype=df | multikv | dedup host,Filesystem | search MountedOn="/mnt/sansmount" | rex field=UsePct "(?<usage>\d+)" | where usage>90 | eval _raw="Filesystem "+Filesystem+" (mount point "+MountedOn+") on host "+host+" is "+UsePct+" full!" | fields - *

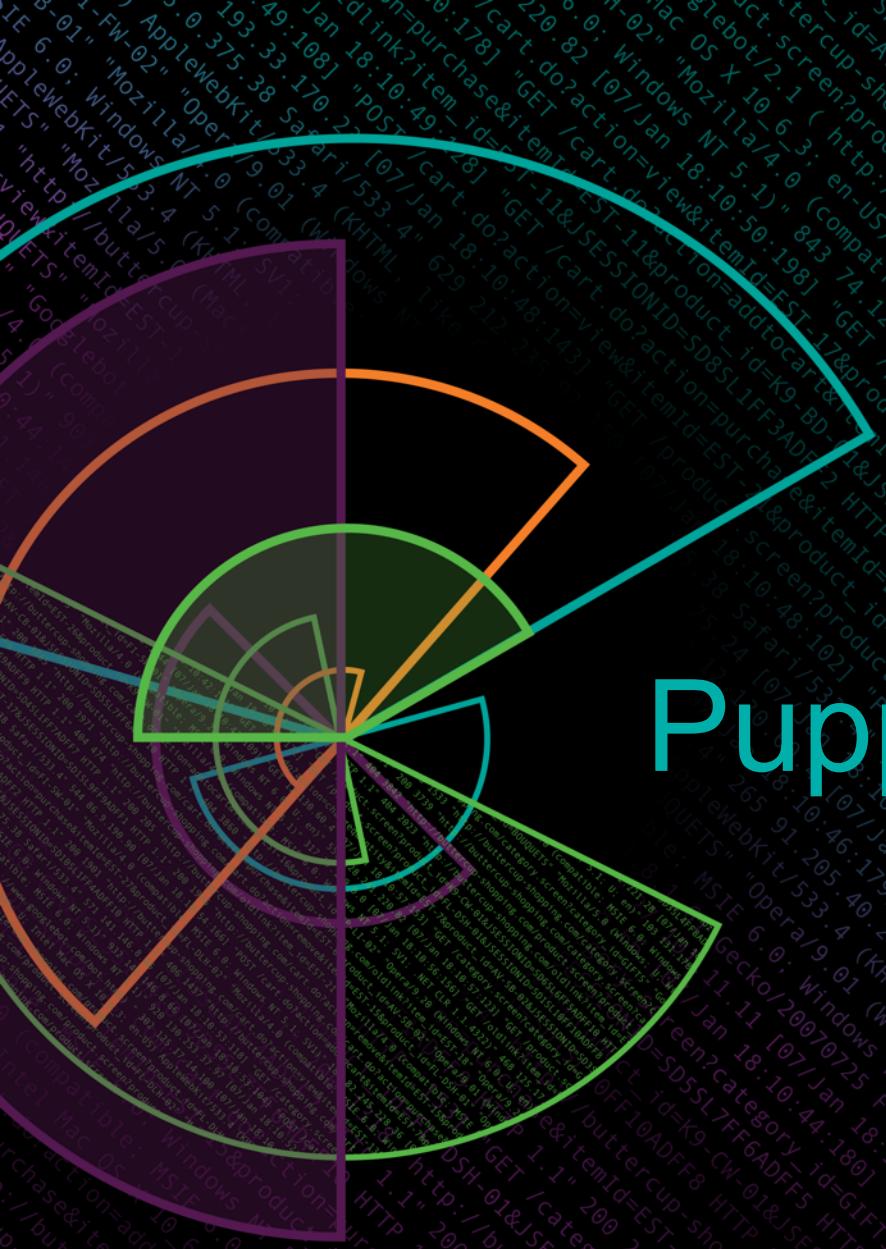


Puppet Tasks Command:

Splunk triggers Puppet Bolt through Puppet Tasks for Splunk. Admin sets command, operating system and runtime. Types out nodes and plan name.

Execution:
webserver::logs::cleanup

splunk> .conf18

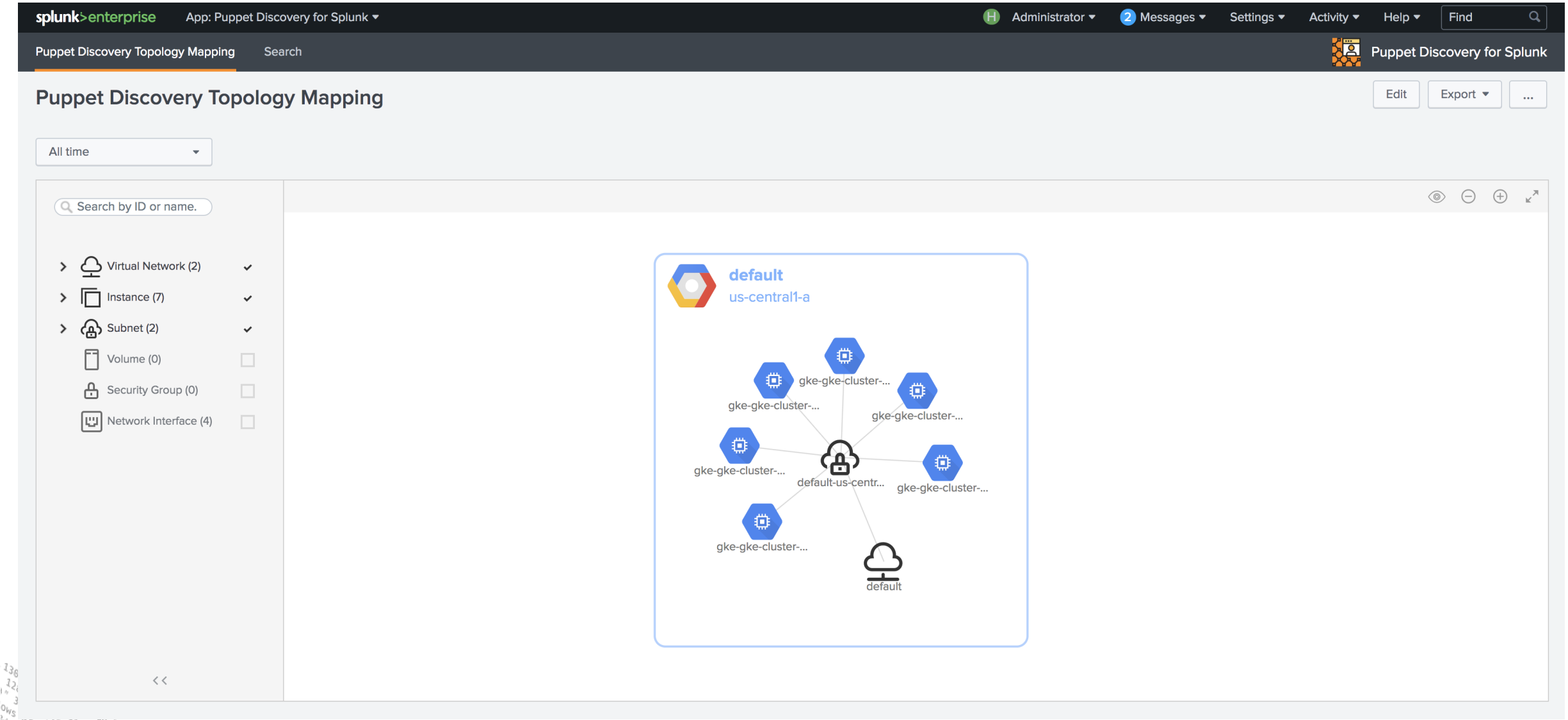


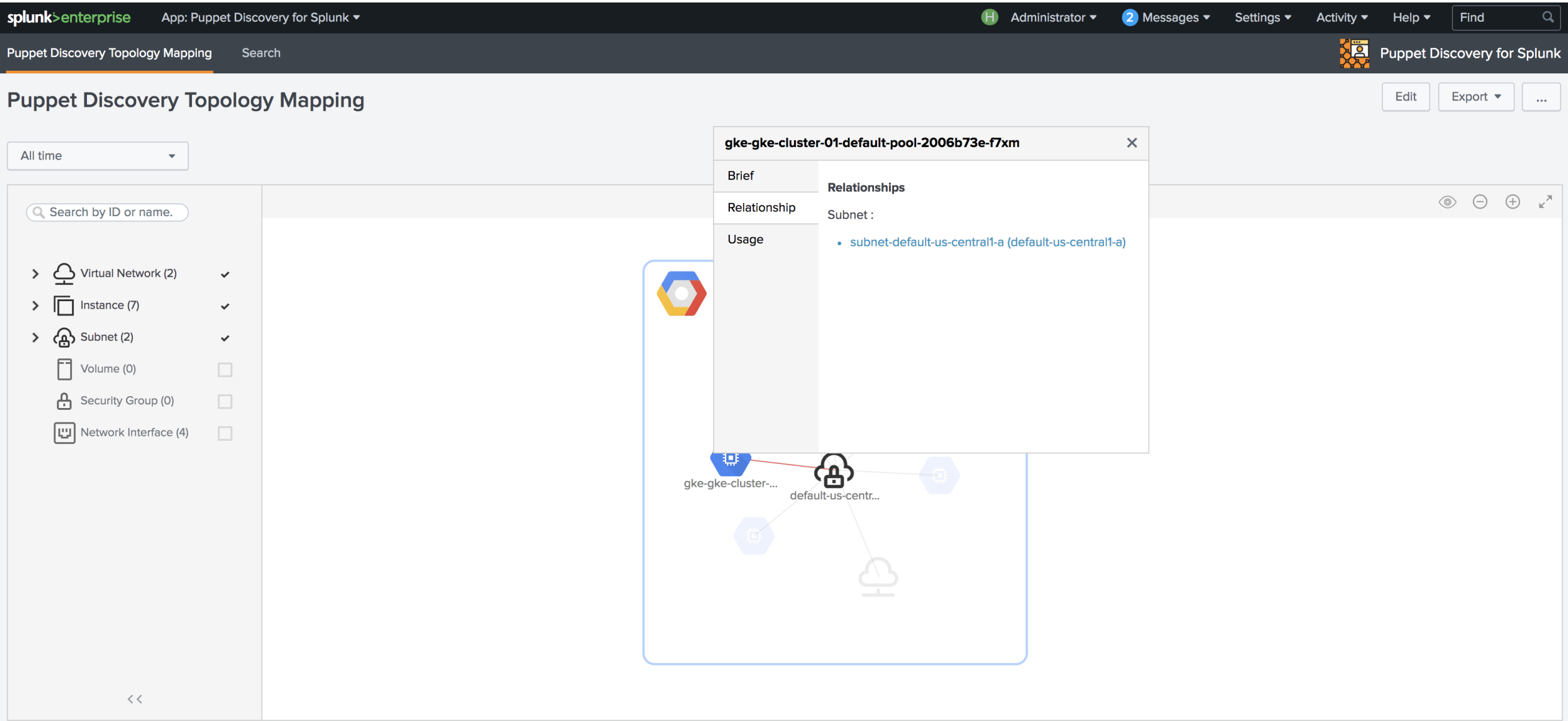
Puppet Discovery for Splunk

Technology Preview

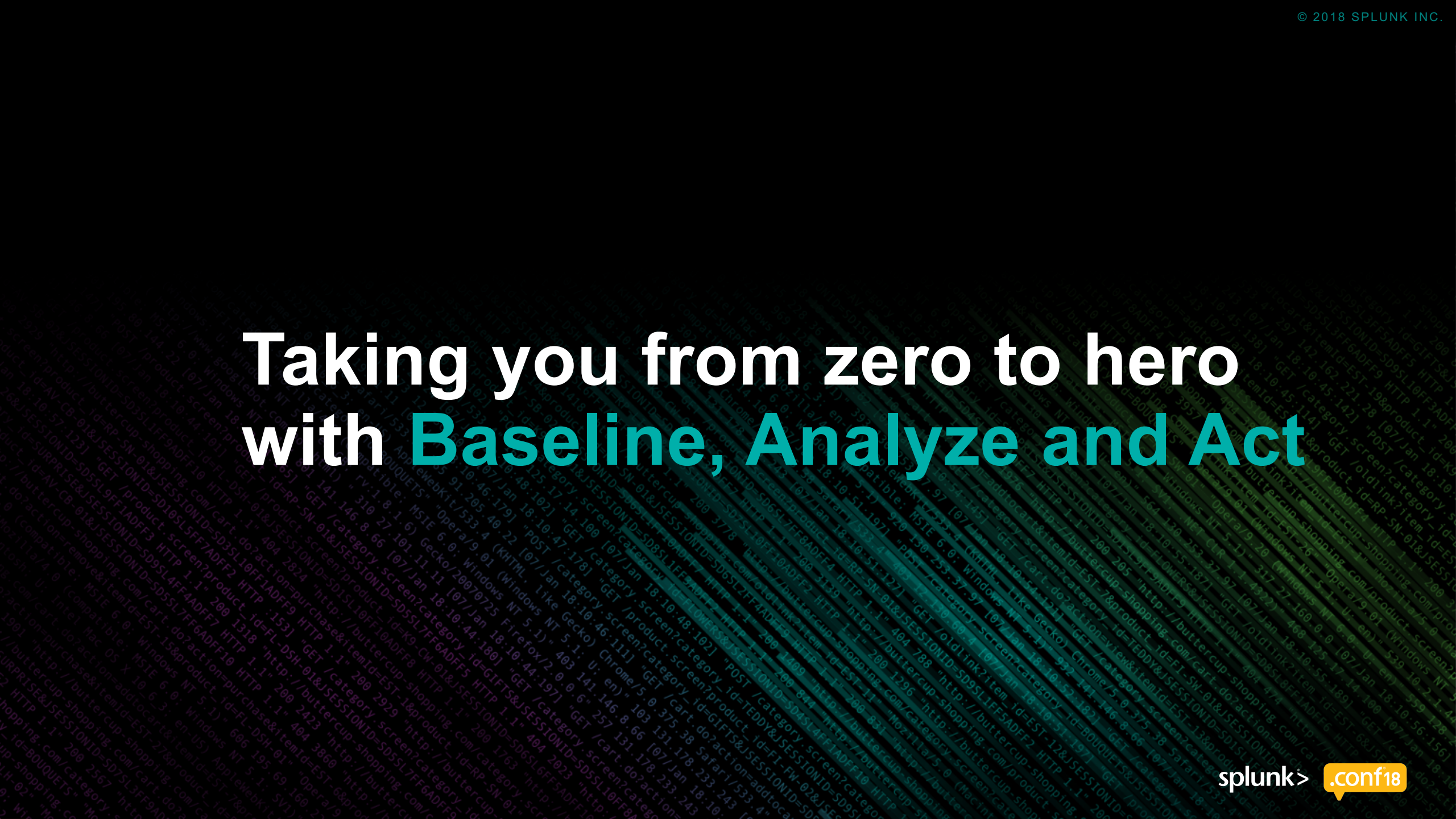
splunk> .conf18

Puppet Discovery for Splunk





Taking you from zero to hero with Baseline, Analyze and Act



splunk> .conf18

“Q&A”

splunk> .conf18

Thank You

Don't forget to rate this session in the .conf18 mobile app