

Triggers and Alerts in Splunk Cloud Services.



Miranda Luna & Declan Shanaghy

Developer Platform | Splunk



Miranda Luna

Product Management | Splunk Developer
Platform



Declan Shanaghy

Architect | Splunk Developer Platform

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.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

Triggers & Alerts in SCS vs Enterprise Scheduled Searches

- Scheduled search for all scenarios, including realtime (poll-based alerting)
 - Consumes resources from the instances on which it runs
 - Searches and actions are tightly coupled
 - Install apps from Splunkbase to expand the out of the box action set
- Scheduled search for some scenarios, DSP pipelines for others (poll- and event-based alerting)
 - Consumes resources from Splunk Cloud Services
 - Searches and actions are decoupled
 - Admin-defined action set

Vision

Conceptually & Architecturally

Conceptually - Data oriented orchestration framework

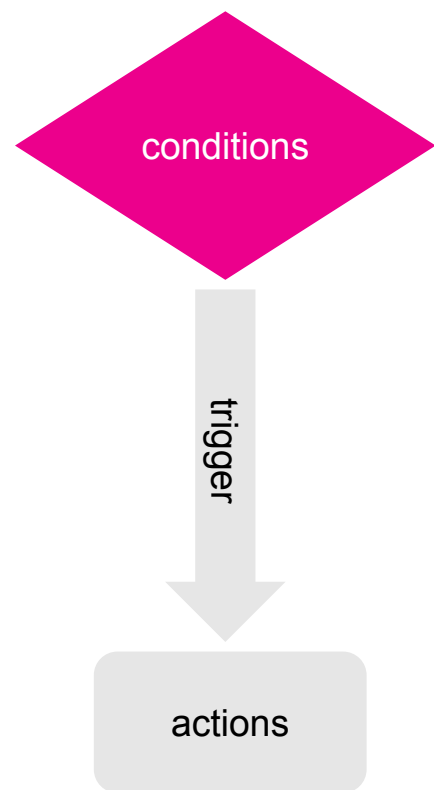
- Look for **signals** in your data
- Take **Action** when the signals appear
- Integrate many **different kinds** of Actions

Architecturally - Decouple Triggers from Alerts

- Triggers fire within the platform
- You define triggers on data insights
- Attach Actions to Triggers

Conditions

Observation of state

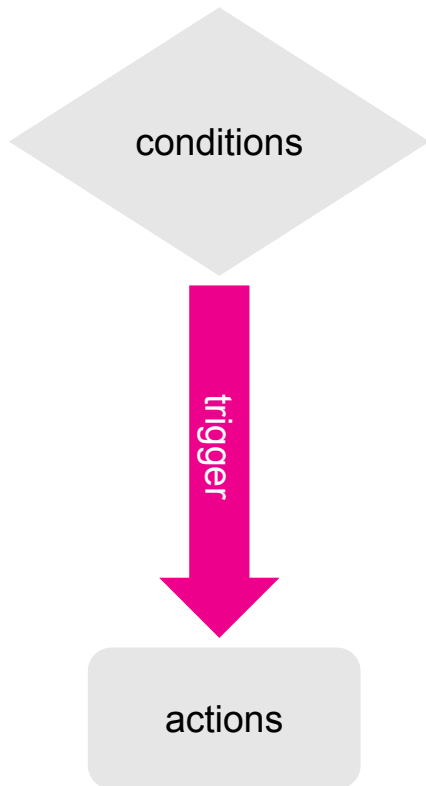


Use Cases

- Notice when...
 - pods thrash memory
 - a new member joins the tenant
 - user shares a workbook
- React when...
 - there are repeated login failures
 - a change needs to be rolled back
 - a service needs to be restarted

Triggers

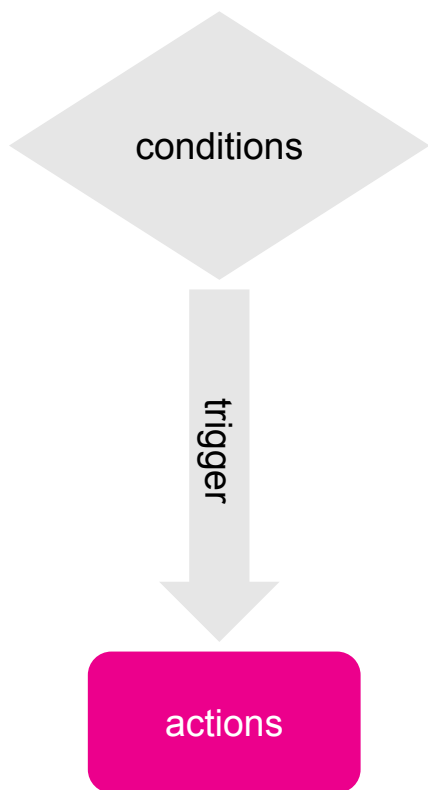
Produced when a condition is met



- Name of service thrashing memory
- How many times it has happened
- Who joined the tenant
- Who added them
- The context of the investigation
- A link to the investigation

Actions

What should be done about it



- Open a VictorOps incident
- Message a Slack channel or user
- Customizable webhook
 - Create a ServiceNow ticket
 - Run a Phantom playbook
- Email

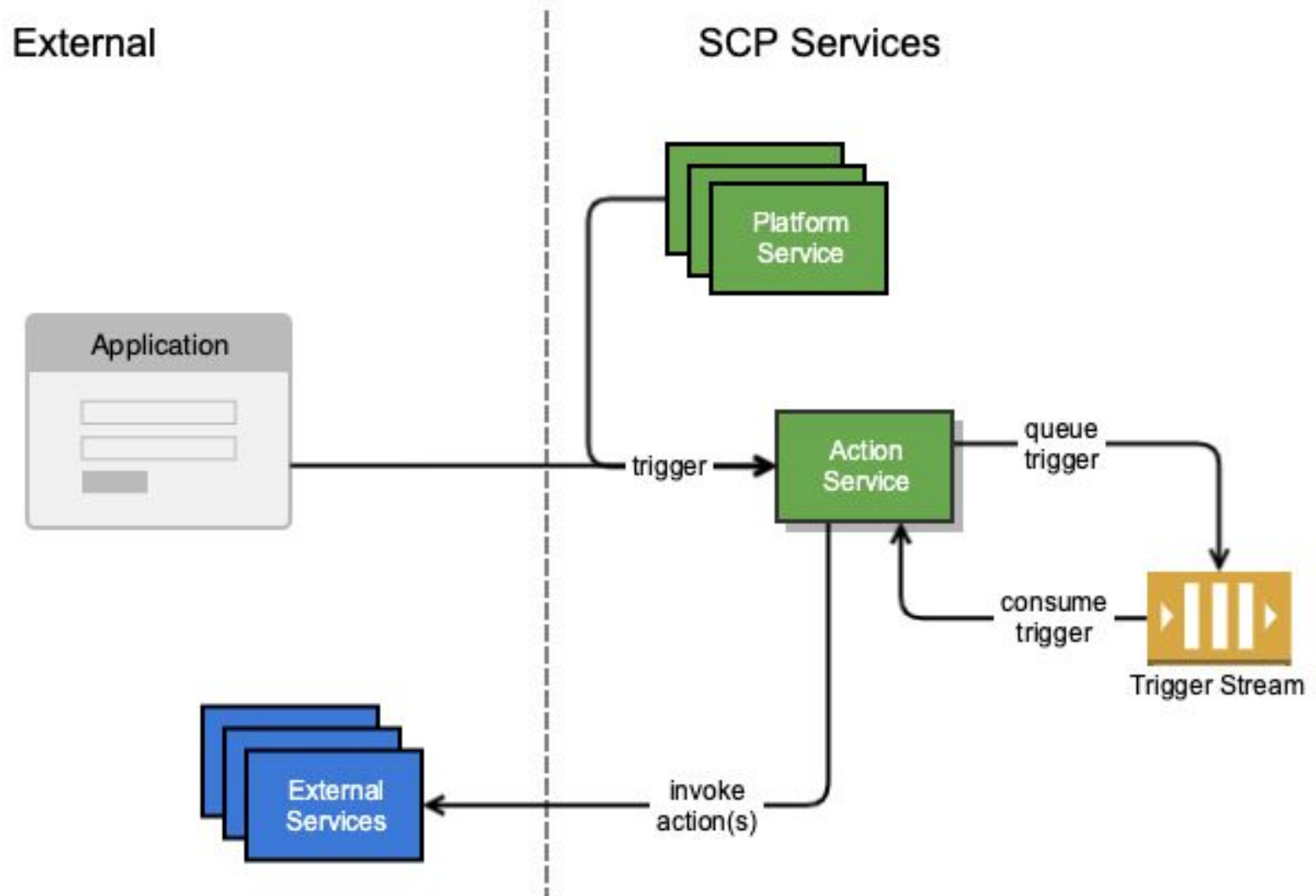
Architectural Overview

Trigger Producers

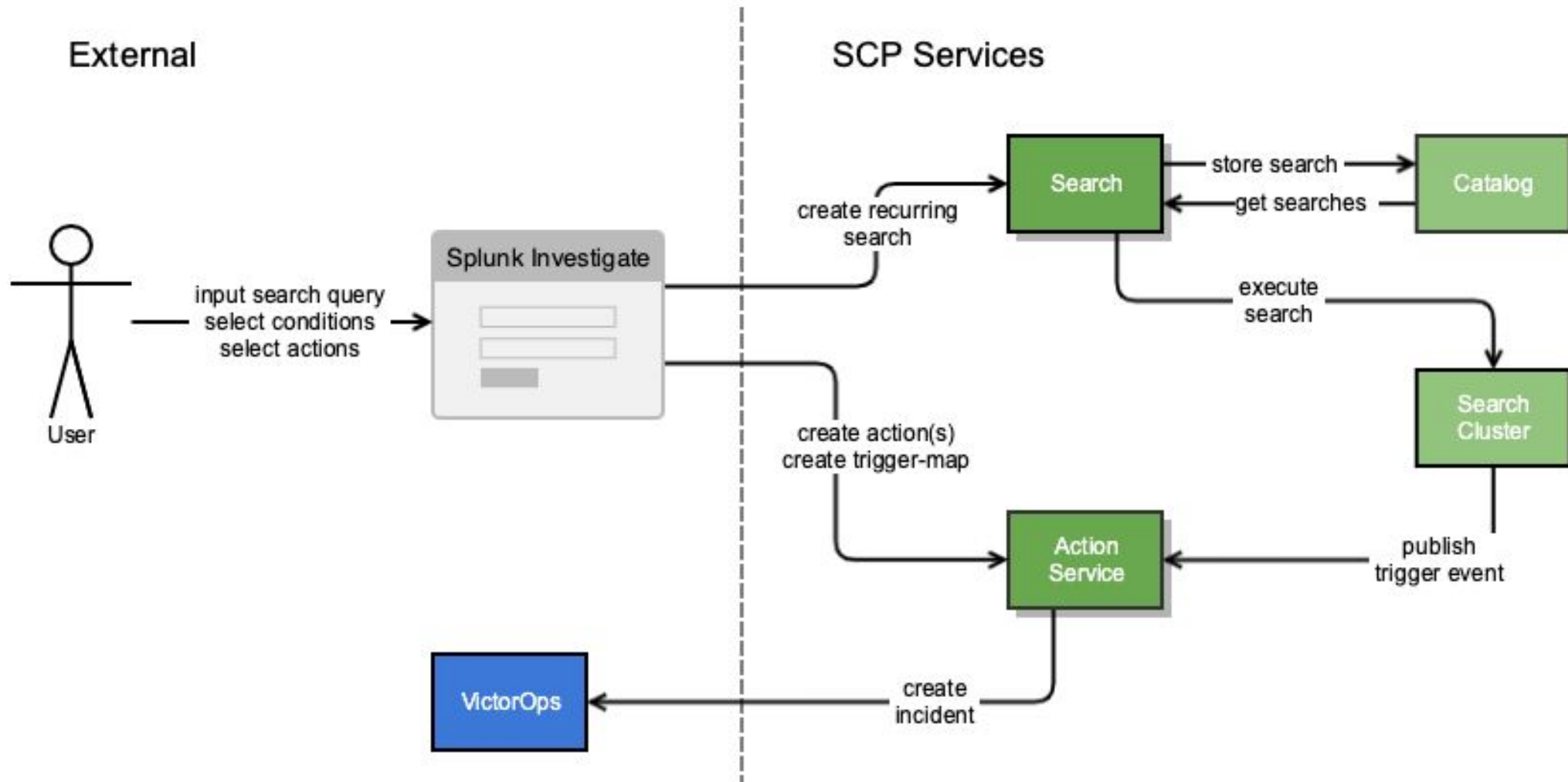
- Recurring Search
- Identity Service
- Apps

Trigger Consumers

- Action Service

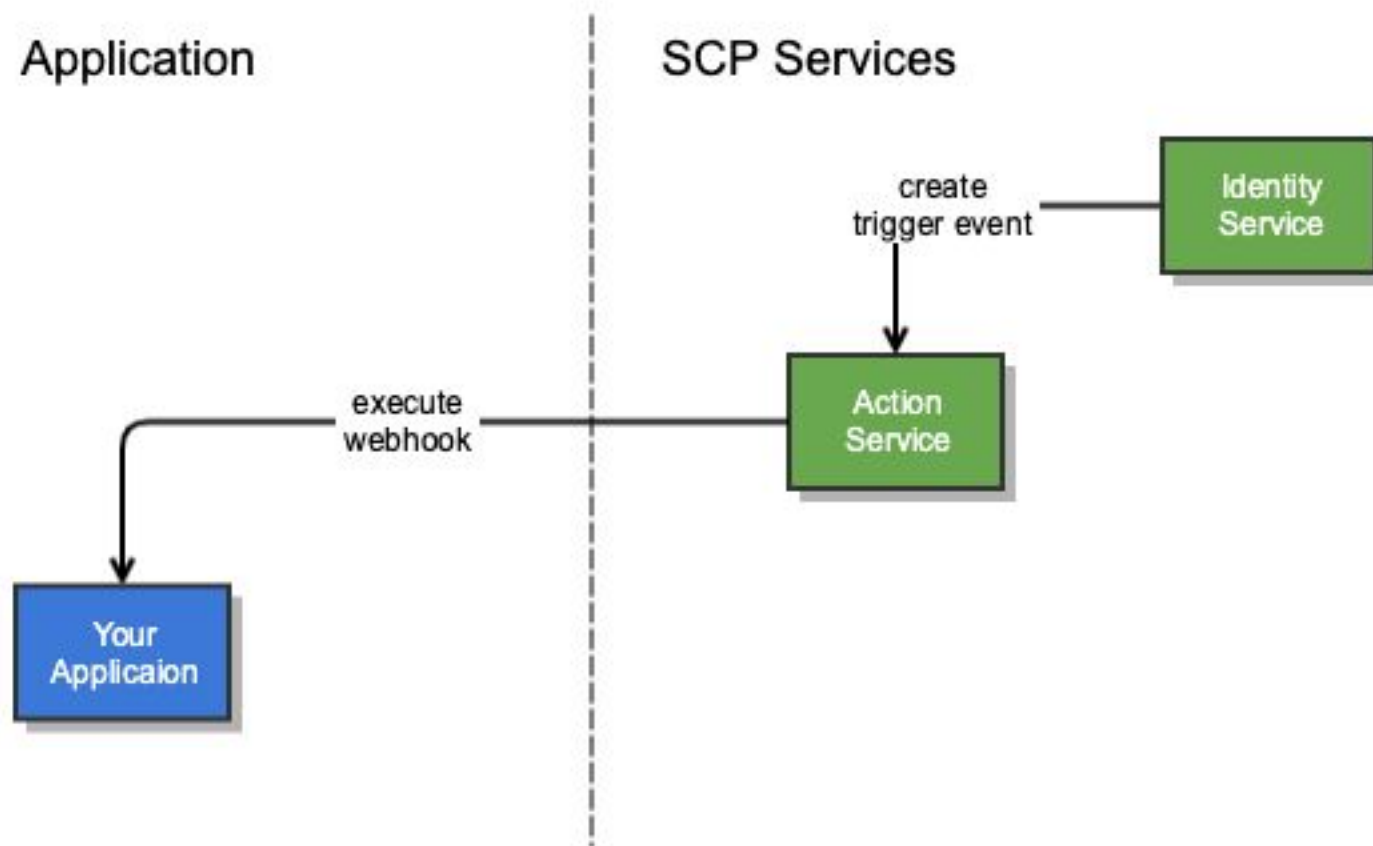


Monitoring your Data



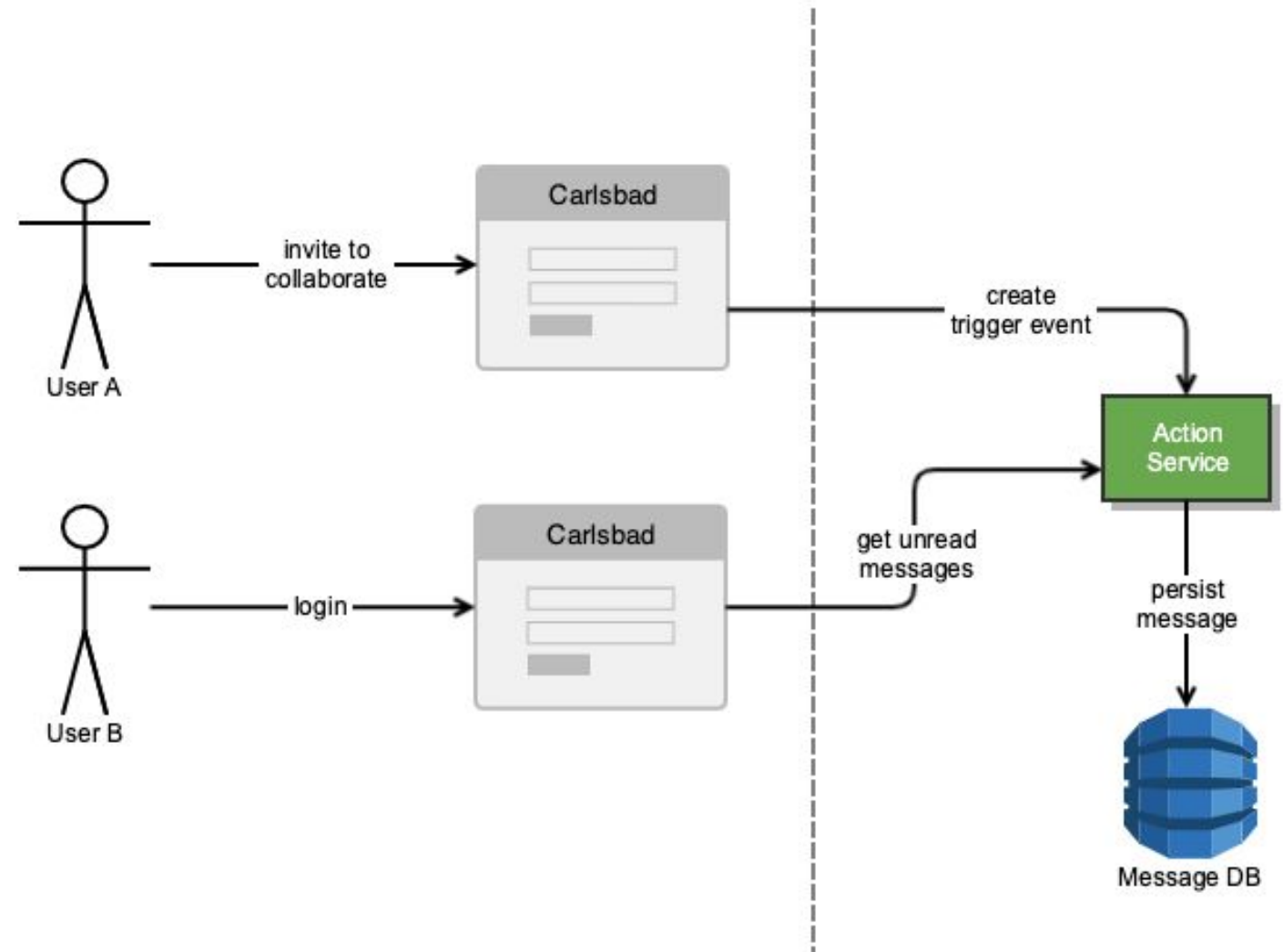
New Member Joins Tenant

- Triggers Produced by the Platform
- Actions defined by an app
- One Time Setup
 - Create webhook action
- Upon Trigger
 - Your webhook is called



Invitation to collaborate

- Triggers produced by an app
- Actions defined produced by an ap
- One Time Setup
 - Create message action
- When invited to collaborate
 - Message is stored
- Upon User B Login
 - Messages are shown



Demo

Priorities for SCS Triggers & Alerts

Today & Tomorrow

Available Today

- Poll-based triggers (recurring searches)
- Numeric condition checks
- Simultaneous Actions
- Generic Webhook
- Webhook Template for VictorOps
- Webhook Template for Slack

Next Priorities

- Event-based triggers (DSP pipelines)
- Sequential Actions
- Admin action configuration
- First class VictorOps & Slack integrations
- Webhook template for Phantom
- Webhook template ServiceNow

We want to hear from you!

Reaching the team

Triggers &. Alerts Usage & Feedback Survey

<to link once finalized>

Booths

Foundations & Platform > Splunk Investigate
Developer > Splunk Cloud Services: Under the Hood

Email

<to add>

Slack

<to add>

Docs

<to add link when finalized>



Q&A



splunk>

Thank

You



Go to the .conf19 mobile app to

RATE THIS SESSION

