

Forward-Looking Statements



This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

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. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

Splunk, Splunk> and Turn Data Into Doing 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. © 2022 Splunk Inc. All rights reserved.

The Developer's App Starter Kit

DEV1127C

Tom West

Senior PS Consultant | Splunk



splunk> .conf22



Tom West

Senior Professional Services Consultant
Splunk

Agenda

1. Splunk App Dev
 - What is Splunk App Dev
2. Add-ons (TA)
 - What they are and how to create them
3. Custom Search Commands
 - SPL™ Friends!!!
4. Packaging & Review
 - The Finish Line?!



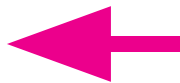
Splunk Dev

The area of Splunk that allows you to create and build solutions for / on the Splunk® Cloud Platform and Splunk® Enterprise.

splunk> .conf22

Resources

- Documentation: [DEV.SPLUNK.COM](https://dev.splunk.com)
- [Dev License](#)
- [.conf Playback](#)
- [Community](#):
 - Slack - splk.it/slack (#AppDev)
 - [User Groups](#)
 - [Answers](#)
- [Splunkbase](#)TM
- [Add-on Builder](#)
- [VS Code Splunk Extension](#)



splunk>dev Developer Guide Reference Tutorials Downloads Examples Splunk platform ▾

Splunk Enterprise developers

Sign up for a free developer license

Use Splunk Enterprise free for six months while you develop your app with our powerful SDKs and helpful online documentation.

[Get your developer license](#)

Splunk Cloud Platform developers

Splunk Cloud Developer Edition: Early Access!

Test your apps for Splunk Cloud Platform readiness with Splunk Cloud Developer Edition. Use in-product guided experiences to install, configure, and test your app's features with sample data.

[Apply today!](#)

Developer Guide

Read about how to develop solutions for Splunk Cloud Platform and Splunk Enterprise.

[→](#)

Resources

- Documentation: [DEV.SPLUNK.COM](https://dev.splunk.com)
- [Dev License](#) 
- [.conf Playback](#)
- [Community](#):
 - Slack - splk.it/slack (#AppDev)
 - [User Groups](#)
 - [Answers](#)
- [Splunkbase](#)TM
- [Add-on Builder](#)
- [VS Code Splunk Extension](#)

splunk>dev

Developer GuideReferenceTutorialsDownloadsExamples

 Splunk platform ▾

Splunk Developer License Signup

With the Splunk developer license, you can use our SDKs and other developer tools to build big data applications that plug into Splunk's map/reduce data-processing pipeline, storage technology, and management facilities. And, you can extend and enhance Splunk Web through our app framework. Just follow a few simple steps below and you'll be on your way.

1. Get Splunk Enterprise:

To build applications that work on top of the Splunk platform, you need a license for Splunk Enterprise, Splunk's flagship core product.

 - [Download Splunk Enterprise](#) and get a license.
 - [Install your Splunk Enterprise license](#).
2. [Request a developer license](#).
3. Get started and stay connected:
 - [Download the Splunk Enterprise SDKs and tools](#).
 - Check out the apps on [Splunkbase](#).
 - Follow us on Twitter for latest updates [@splunkdev](#).
 - Reach out to us on [Slack](#) in the [#appdev](#) channel.

splunk>dev

[Contact](#)Community SlackPrivacyTerms of Service

Resources

- Documentation: [DEV.SPLUNK.COM](https://dev.splunk.com)
- [Dev License](#)
- [.conf Playback](#) 
- [Community](#):
 - Slack - splk.it/slack (#AppDev)
 - [User Groups](#)
 - [Answers](#)
- [Splunkbase™](#)
- [Add-on Builder](#)
- [VS Code Splunk Extension](#)



Agenda Sessions ▾ Speakers Connect Sponsors Partners Event Details [Register Now](#)

Watch

Filters

Clear

"tom west" ×

tom west

Search

24 sessions

conf21 SplunkTrust All Skill Levels

⊕ TRU1053B - Dashboarding Wowzas! Top Tips for Making Your Dashboards Awesome

Tom West, Senior Professional Services Consultant, Splunk

Whether it's a dashboard for a CEO or for a team of developers. Using a dashboard to maximize the value of your data can sometimes be tricky. In this session, I'll share some favorite dashboarding tips and tricks to show you how to easily put...

Session Slides

Session Video

conf20 Splunk Developer Intermediate

⊕ DEV1198C - SPL Rehab: From custom search command to automated delivery

Tom West, Solutions Architect, Converging Data

SPL Rehab is a search debug tool we created to identify problems with our searches by identifying the key lines that may require our attention, primarily via custom search commands and interacting with Splunk at REST. And because we want to...

Session Slides

Session Video

conf21 Splunk4U All Skill Levels

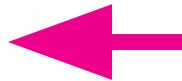
⊕ S4U1049B - Splunk@Home: How To Create Your Own Training Rig Using Data In Your Home!

Tom West, Senior Professional Services Consultant, Splunk

The volume of data available in our homes is significant! Not only can we use this data to save ourselves

Resources

- Documentation: [DEV.SPLUNK.COM](https://dev.splunk.com)
- [Dev License](#)
- [.conf Playback](#)
- [Community](#):
 - Slack - splk.it/slack (#AppDev)
 - [User Groups](#)
 - [Answers](#)
- [Splunkbase](#)TM
- [Add-on Builder](#)
- [VS Code Splunk Extension](#)

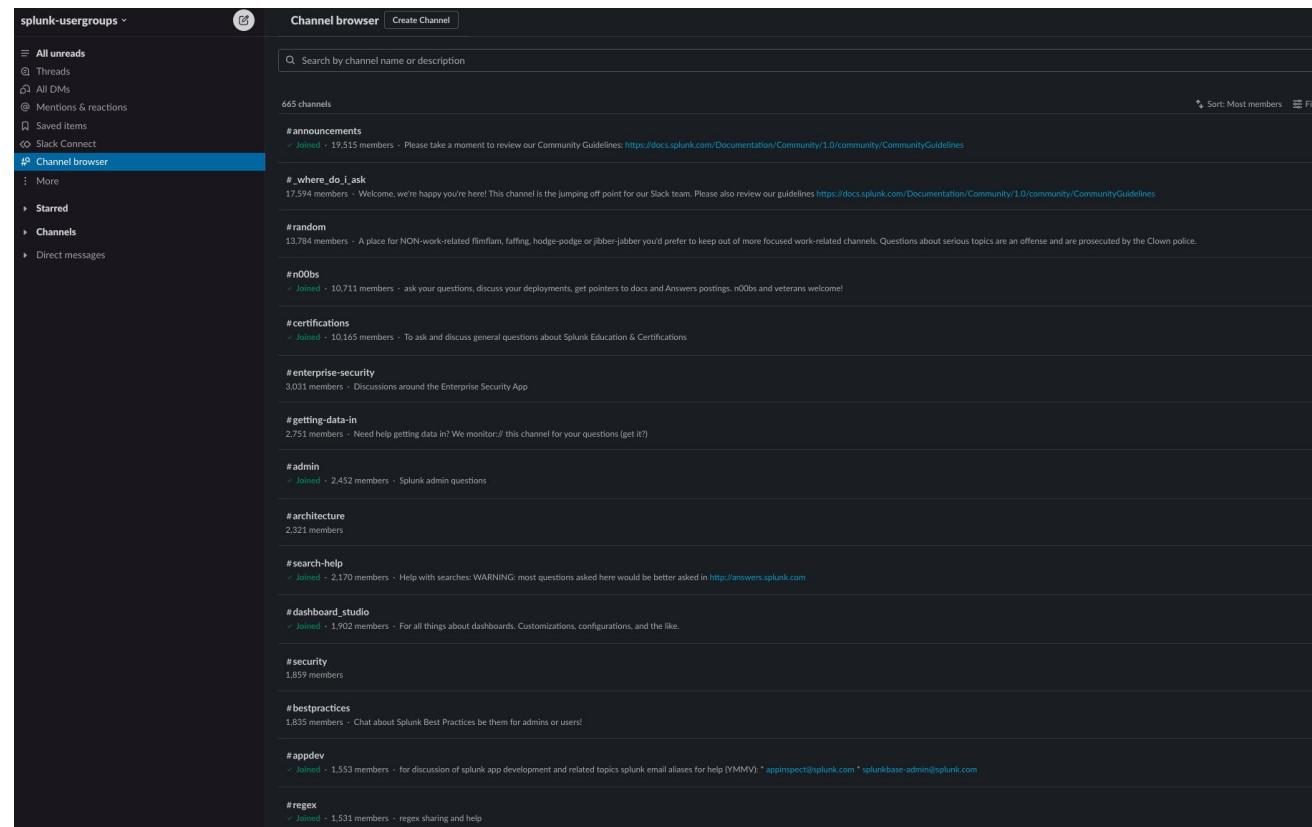


The screenshot shows the Splunk Community homepage. At the top is a navigation bar with the Splunk logo and links to COMMUNITY, SPLUNK ANSWERS, DISCUSSIONS, SPLUNKTRUST, USER GROUPS, SPLUNK LOVE, and IDEAS. A search bar and a 'Sign In' button are on the right. The main section features the headline 'Learn, Give Back, Have Fun' and a subtext: 'Our community members come from around the globe and all walks of life to learn, get inspired, share knowledge and have fun.' To the right of the headline are three statistics: '1,185 Online Now' (with a person icon), '128K Discussions' (with a speech bubble icon), and '53.2K Solutions' (with a checkmark icon). Below this is a search bar with the placeholder 'Search this category' and a 'Search' button, along with a pink 'Ask a Question' button. At the bottom, there are three columns of content, each with an icon, a description, and a 'Sign In' link.

Icon	Description	Sign In Link
	Ask questions. Get answers. Find technical product solutions from passionate experts in the Splunk community.	Sign In to Ask A Question
	Meet virtually or in-person with local Splunk enthusiasts to learn tips & tricks, best practices, new use cases and more.	Sign In to Join A Group
	Search, vote and request new enhancements (ideas) for any Splunk solution - no more logging support tickets.	Sign In to Submit an Idea

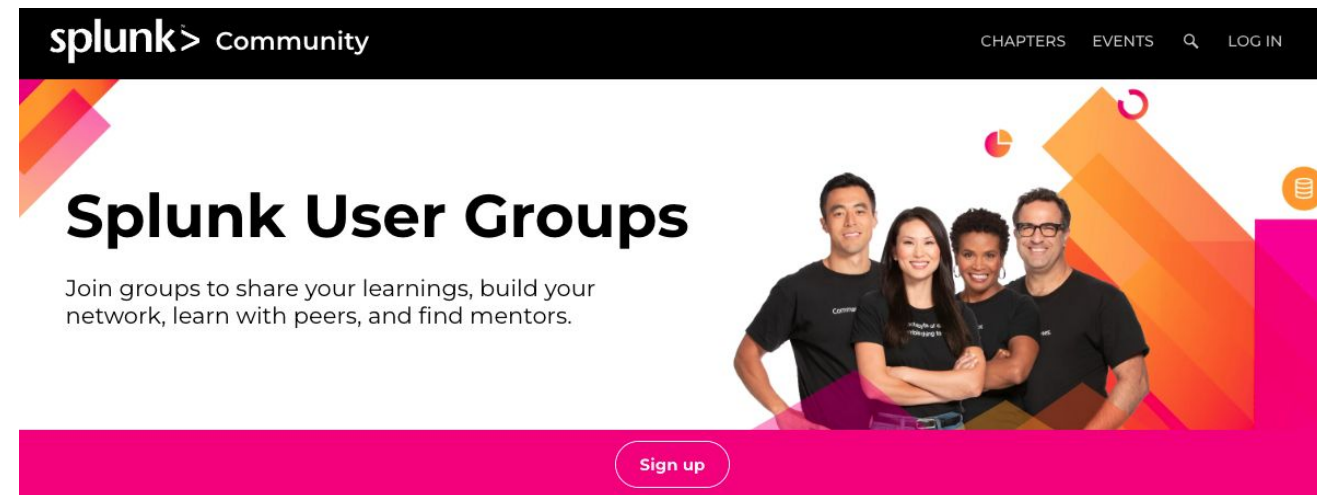
Resources

- Documentation: [DEV.SPLUNK.COM](https://dev.splunk.com)
- [Dev License](#)
- [.conf Playback](#)
- [Community](#):
 - Slack - splk.it/slack (#AppDev)
 - [User Groups](#)
 - [Answers](#)
- [Splunkbase](#)TM
- [Add-on Builder](#)
- [VS Code Splunk Extension](#)



Resources

- Documentation: [DEV.SPLUNK.COM](https://dev.splunk.com)
- [Dev License](#)
- [.conf Playback](#)
- [Community](#):
 - Slack - splk.it/slack (#AppDev)
 - [User Groups](#)
 - [Answers](#)
- [Splunkbase™](#)
- [Add-on Builder](#)
- [VS Code Splunk Extension](#)



Resources

- Documentation: [DEV.SPLUNK.COM](https://dev.splunk.com)
- [Dev License](#)
- [.conf Playback](#)
- [Community](#):
 - Slack - splk.it/slack (#AppDev)
 - [User Groups](#)
 - [Answers](#)
- [Splunkbase™](#)
- [Add-on Builder](#)
- [VS Code Splunk Extension](#)

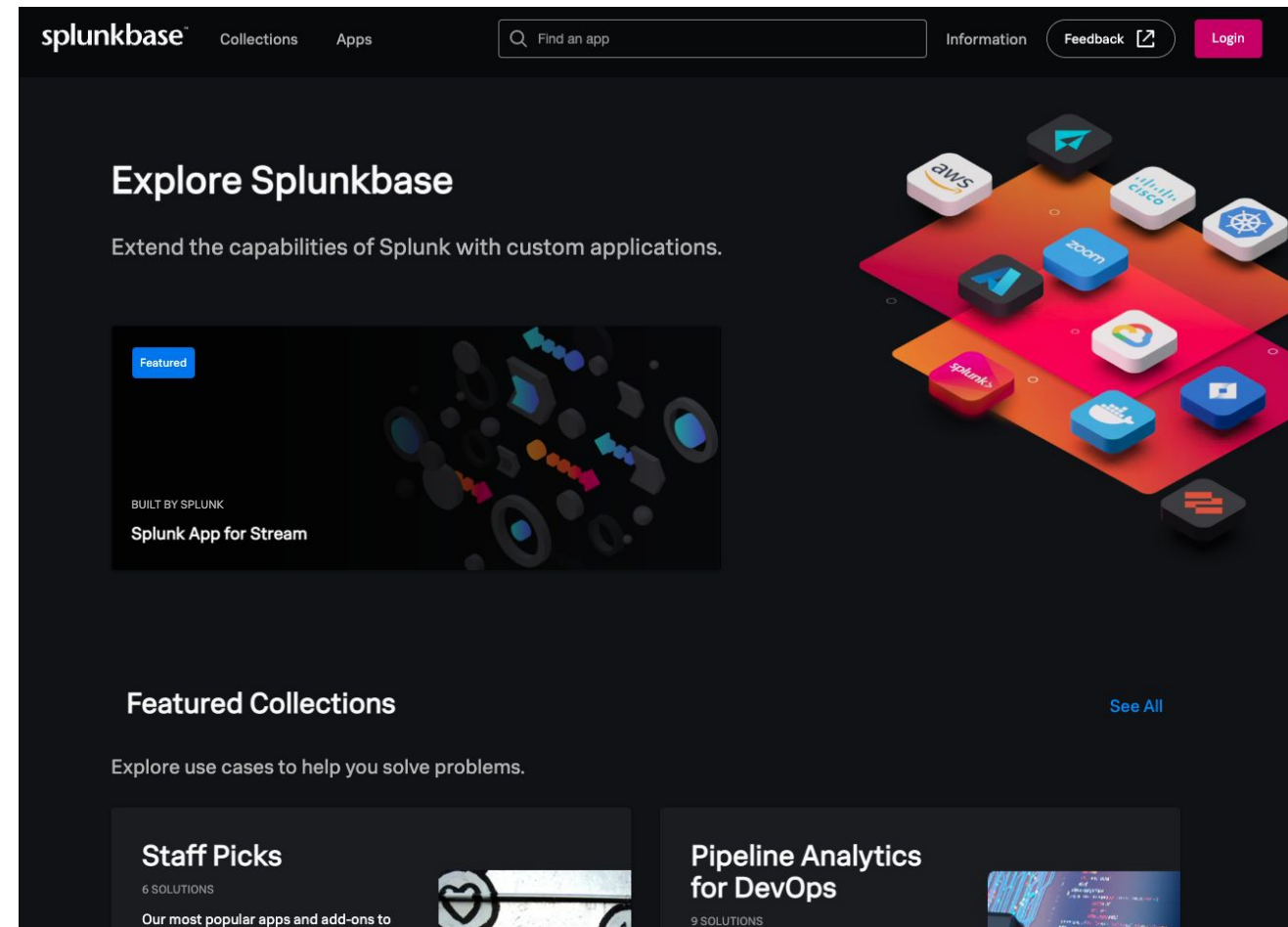


The screenshot shows the Splunk Answers website. The header includes the Splunk logo and navigation links: COMMUNITY, SPLUNK ANSWERS, DISCUSSIONS, SPLUNKTRUST, USER GROUPS, SPLUNK LOVE, and IDEAS. A search bar and a 'Sign In' button are on the right. The main heading is 'Splunk Answers' with the tagline 'Ask questions. Get answers. Find technical product solutions from passionate members of the Splunk community.' Below this is a search bar with the placeholder 'Search this category' and buttons for 'Search' and 'Ask a Question'. The main content area is titled 'Browse the Community' and displays a grid of 16 categories, each with an eye icon, a count, and a speech bubble icon. A pink arrow points to the 'Answers' link in the left-hand list.

Category	Views	Answers
All Apps and Add-ons	76209470	18867
Security Premium Solutions	14700009	3287
Deployment Architecture	31599984	5910
IT Ops Premium Solutions	3239834	771
Reporting	13470587	2637
Splunk SOAR (f.k.a. Phantom)		
Splunk On-Call	40307	9
Splunk Enterprise	9391546	3322
Splunk Administration	216471006	39237
Splunk User Behavior Analytics	56259	16
Using Splunk	335113769	58692
Splunk Data Stream Processor		
Splunk IT Service Intelligence	3239168	770
Developing for Splunk Enterprise	10460931	2401
Splunk Observability Cloud	65090	25
Splunk Cloud Platform	1411436	426
Installation	13519876	2653
Splunk Development		
Splunk Enterprise Security	13294531	3014
Splunk Search	248282813	42264
Splunk Business Flow	865	1
Developing for Splunk Cloud Services	434745	197
DevOps Premium Solutions	105397	34
Alerting		

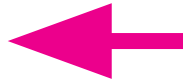
Resources

- Documentation: [DEV.SPLUNK.COM](https://dev.splunk.com)
- [Dev License](#)
- [.conf Playback](#)
- [Community](#):
 - Slack - splk.it/slack (#AppDev)
 - [User Groups](#)
 - [Answers](#)
- [Splunkbase™](#) 
- [Add-on Builder](#)
- [VS Code Splunk Extension](#)



Resources

- Documentation: [DEV.SPLUNK.COM](https://dev.splunk.com)
- [Dev License](#)
- [.conf Playback](#)
- [Community](#):
 - Slack - splk.it/slack (#AppDev)
 - [User Groups](#)
 - [Answers](#)
- [Splunkbase™](#)
- [Add-on Builder](#)
- [VS Code Splunk Extension](#)



The screenshot shows the Splunk Add-on Builder app page. At the top, there's a green gear icon and the title 'Splunk Add-on Builder'. Below the title, a description states: 'The Splunk Add-on Builder is a Splunk app that helps you build and validate technology add-ons for your Splunk Enterprise deployment. The goals of the Splunk Add-on Builder are to: * Guide you through all of the necessary steps of creating an add-on * Build alert actions and adaptive...'. It also says 'Built by Splunk Inc.'.

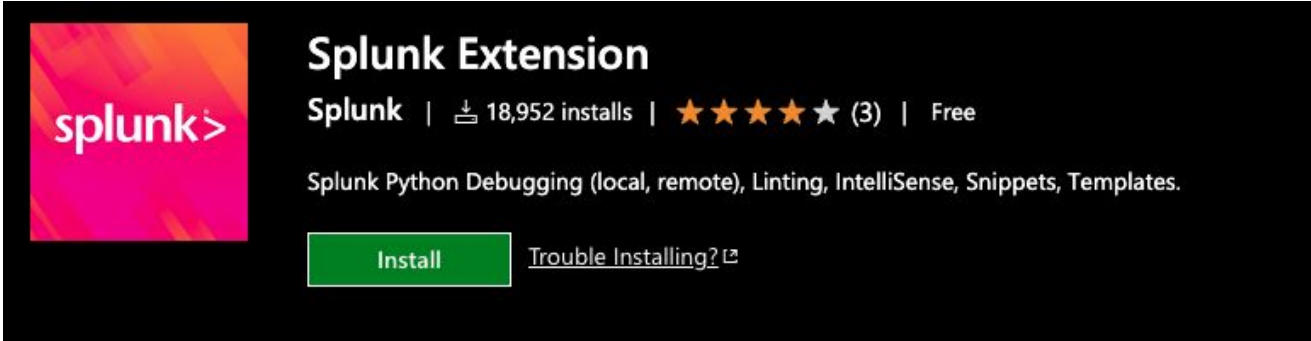
Below the description, there's a 'Login to Download' button and a 'splunk' logo. To the right, there are icons for a link and a notification.

The main content area features four screenshots of the app's interface. Below these, there's a section with metadata: 'Version 4.1.0' (with a dropdown arrow and an info icon), 'March 4, 2022', 'Product: Splunk Enterprise', 'Rating: 4 stars (32)' (with a 'Log in to rate this app' link), and 'Support: Splunk Supported App' (with an info icon).

At the bottom, there are tabs for 'About' and 'Details'. The 'About' tab is active, showing the same description as at the top. The 'Details' tab is also visible. On the right side of the bottom section, there's a box with 'March 4, 2022 - Version 4.1.0', 'Release Notes', and a 'Read More' link.

Resources

- Documentation: [DEV.SPLUNK.COM](https://dev.splunk.com)
- [Dev License](#)
- [.conf Playback](#)
- [Community](#):
 - Slack - splk.it/slack (#AppDev)
 - [User Groups](#)
 - [Answers](#)
- [Splunkbase](#)TM
- [Add-on Builder](#)
- [VS Code Splunk Extension](#)



Splunk Extension
Splunk | 18,952 installs | ★★★★★ (3) | Free
Splunk Python Debugging (local, remote), Linting, IntelliSense, Snippets, Templates.
[Install](#) [Trouble Installing?](#)

[Overview](#) [Version History](#) [Q & A](#) [Rating & Review](#)

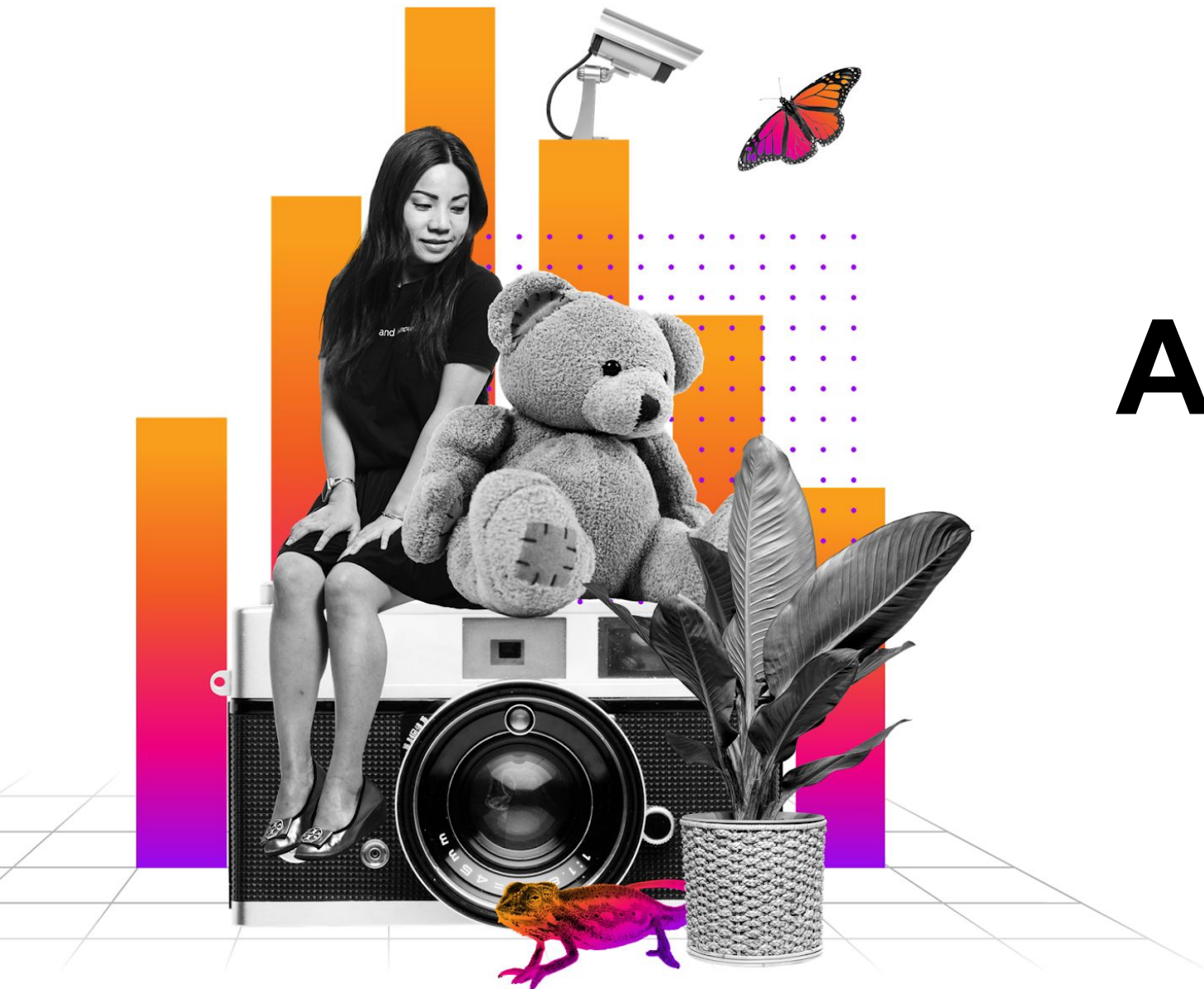
Visual Studio Code Extension for Splunk

The Visual Studio Code Extension for Splunk helps developers create, test, and debug Splunk Enterprise apps, add-ons, custom commands, REST handlers, etc. The extension helps Splunk administrators edit Splunk .conf files by providing stanza and setting completions as well as setting checking. For individuals living in Visual Studio Code, integrations are built in to run Splunk searches and display Splunk visualizations in Visual Studio Code.

Working with .conf files



Note: Screenshot is from Microsoft Marketplace.



Add-ons (TA)

splunk> .conf22

Apps v Add-ons

Add-ons (TA)

Apps

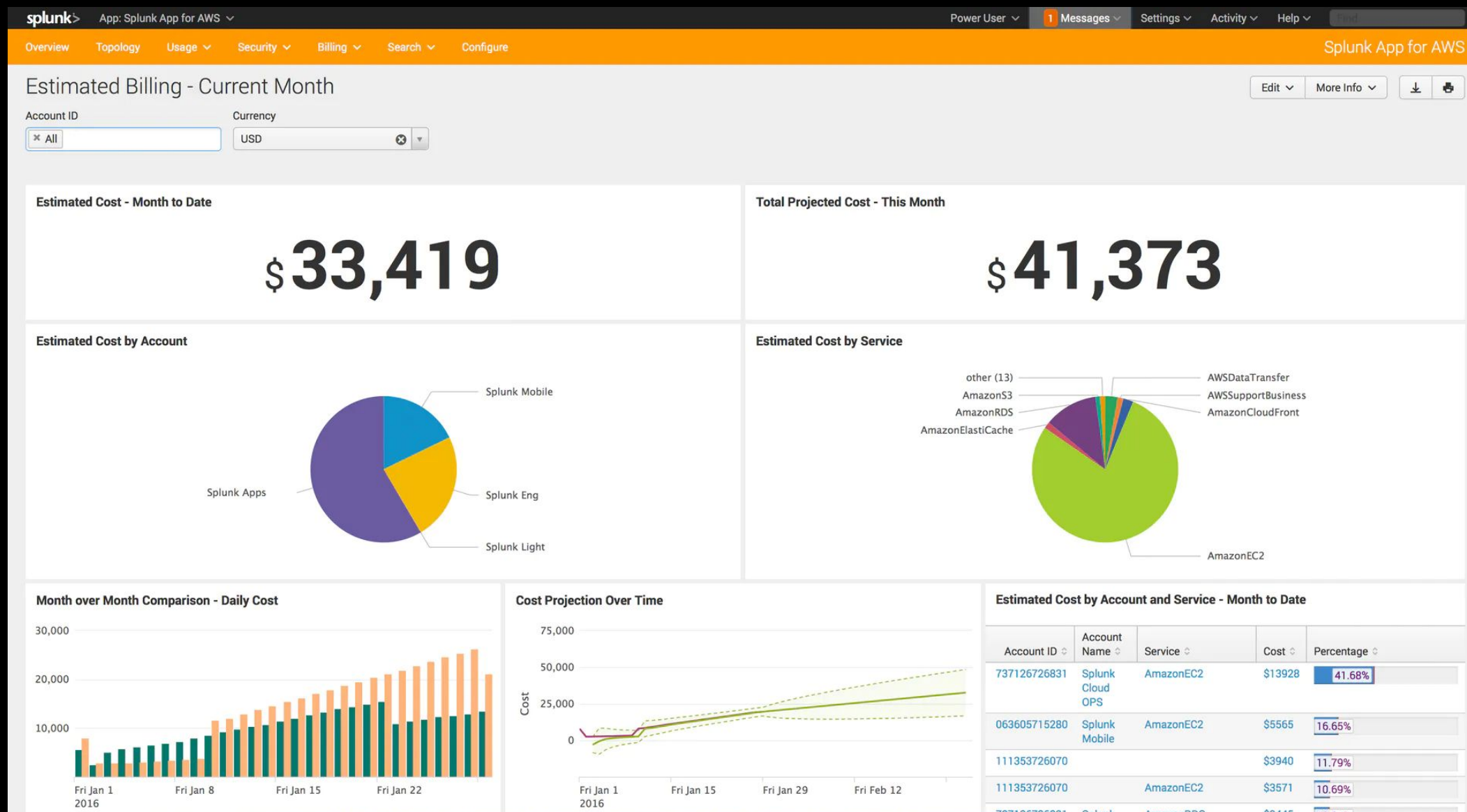
Contains objects which are directly used and interacted with by the user.

- Views
- Saved Searches
- Lookups

Add-ons

To aid with onboarding data and/or enhance the capabilities of other apps within your Splunk system.

Both found in */%SPLUNK_HOME%/etc/apps*

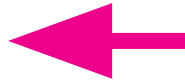


Add-on Builder

Add-ons (TA)

Methods:

- UI
- Script
- Python
 - Allowing for far more advanced data collection (Multiple Endpoints, OAuth, etc)



splunk> App: Splunk Add-on Builder

Administrator Messages Settings Activity Help Find

Create Alert Action

Properties Inputs & Parameters Code & Test

Alert Action Inputs Add-on Setup Parameters

Define the setup parameters that are used by the add-on.
This setup form is displayed to the user the first time the add-on runs. Select the type of parameters to add to the setup form from the list. Drag and drop inputs from the Component Library to add custom parameters. Then, specify the properties for each input in the Property Editor. [Learn More](#)

Add-on Setup Built-in Parameters

☒ Add Proxy
☐ Add Account
☒ Add Logging

Component Library in Panel Setting

ABC

Text Field

SECRET

Password

✓ ABC

Checkbox

API Key

Run time

Ad-Hoc Action

Property Editor

Checkbox

Display Label

Ad-Hoc Action

Internal Name

action

Hints & Help

Optional. Max 120 Characters

splunk>

App: Splunk Add-on Builder

Administrator

Messages

Settings

Activity

Help

Find

Edit Data Input

Inputs & Parameters

Define & Test

Define the data input

Fill out the form below to define your data input, enter variables to pass to the script, then click **Test** to preview the results. [Learn more](#)

Test

Save

Data Input Definition

Output: Done

* REST URL:

http://query.yahooapis.com/v1/public/yql?q=select * from yahoo.finance.quotes where symbol in

* REST method:

GET

REST Request headers:

Name	Value

* Stock (stock)

SPLK

```
{
  "query": {
    "lang": "en-US",
    "results": {
      "quote": {
        "ErrorIndicationReturnedForSymbolChangedInvalid": null,
        "YearRange": "29.85 - 66.90",
        "DividendYield": null,
        "Open": "60.93",
        "LastTradeRealtimeWithTime": null,
        "AfterHoursChangeRealtime": null,
        "Volume": "1795321",
        "PercentChangeFromTwoHundreddayMovingAverage": "+5.87%",
        "HoldingsValue": null,
        "DaysValueChangeRealtime": null,
        "PercentChangeFromFiftydayMovingAverage": "-0.35%",
        "YearLow": "29.85",
        "ChangeFromYearHigh": "-7.27",
        "DaysValueChange": null,
        "FiftydayMovingAverage": "59.84",
        "HoldingsGainPercentRealtime": null,
        "TradeDate": null,
        "ChangeFromFiftydayMovingAverage": "-0.21",
        "PercentChangeFromYearLow": "+99.77%",
        "PEGRatio": "5.47",
        "AverageDailyVolume": "1534010",
        "Symbol": "SPLK",
        "EarningsShare": "-2.61",
        "YearHigh": "66.90",
        "PricePaid": null,
        "LastTradeDate": "10/11/2016",
        "StockExchange": "NMS",
        "PercentChangeFromYearHigh": "-10.87%",
        "Notes": null,
        "ExDividendDate": null,
        "DaysRange": "59.56 - 61.33",
        "DaysHigh": "61.33",
        "LastTradePriceOnly": "59.63",

```

splunk> .conf22

Add-on Builder

Add-ons (TA)

Methods:

- UI
- Script 
- Python
 - Allowing for far more advanced data collection (Multiple Endpoints, OAuth, etc)

Add-on Builder

Add-ons (TA)

Methods:

- UI
- Script
- Python
 - Allowing for far more advanced data collection (Multiple Endpoints, OAuth, etc)

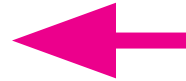


Add-on Builder

Add-ons (TA)

Other Benefits

- Allows for the creation of multiple inputs, easily
- Creates setup pages for users to use
- Enables easy field extraction and aliasing
- Specifically aids in CIM mapping
- Will run validation checks against your app

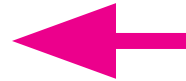


Add-on Builder

Add-ons (TA)

Other Benefits

- Allows for the creation of multiple inputs, easily
- Creates setup pages for users to use
- Enables easy field extraction and aliasing
- Specifically aids in CIM mapping
- Will run validation checks against your app

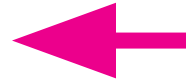


Add-on Builder

Add-ons (TA)

Other Benefits

- Allows for the creation of multiple inputs, easily
- Creates setup pages for users to use
- Enables easy field extraction and aliasing
- Specifically aids in CIM mapping
- Will run validation checks against your app



splunk App: Splunk Add-on Builder Administrator Messages Settings Activity Help Find

My Add-on | Configure Data Collection | Add Sample Data | **Extract Fields** | Map to CIM | Create Alert Actions | Validate & Package **Splunk Add-on Builder**

Extract Fields > Mydata

The summary below shows how your sample data was parsed for the Unstructured Data format. Select the relevant patterns for the fields you want to extract. Select **Show the regular expression** to fine tune the field extraction. When the results look correct, click **Save**. Otherwise, click **Cancel** to return to the previous page to try parsing the data using a different format. [Learn more](#)

705 events in all

- ☒ Enable/Disable All
- ☒ **Pattern1**
181 events, 25.7%
- ☒ **Pattern2**
150 events, 21.3%
- ☒ **Pattern3**
77 events, 10.9%
- ☒ **Pattern4**
52 events, 7.4%
- ☒ **Pattern5**
37 events, 5.2%
- ☐ **Pattern6**
34 events, 4.8%
- ☐ **Pattern7**
19 events, 1.8%
- ☐ **Pattern8**
11 events, 1.6%
- ☐ **Pattern9**
11 events, 1.6%
- ☐ **Pattern10**
9 events, 1.3%
- ☐ **Pattern11**
9 events, 1.3%
- ☐ **Pattern12**
9 events, 1.3%
- ☐ **Pattern13**
7 events, 1%
- ☐ **Pattern14**
6 events, 0.9%
- ☐ **Pattern15**

Pattern: `$[field_1] %ASA-4-722051: Group <GroupPolicy_AcmeFullAccess> User <$[field_2]> IP <$[ipv4_1]> IPv4 Address <$[ipv4_2]> IPv6 address <$[ipv6_1]> assigned to session[us/vnu]*$`

☐ Show the regular expression

Fields:

`field_1` `field_2` `ipv4_1` `ipv4_2` `ipv6_1`

Events:
181 events, 100% matched, 0% unmatched.

1 2 3 4 5 >

```

2016-01-30 00:07:21 68.108.191.72 HOST-003 Oct 10 2014 11:19:35: %ASA-4-722051: Group <GroupPolicy_AcmeFullAccess> User <BradieBee> IP <68.108.191.72> IPv4 Address <68.108.191.72> IPv6 address <966a:170:478b:9bb:7616:9a11:ab59:6736> assigned to session
2016-01-30 00:05:46 37.33.146.25 BUJDEV-006 Oct 10 2014 11:19:35: %ASA-4-722051: Group <GroupPolicy_AcmeFullAccess> User <SimonFurne5290> IP <37.33.146.25> IPv4 Address <37.33.146.25> IPv6 address <d3ac:3f75:b49:a64f:662:df68:fb00:9936> assigned to session
2016-01-30 00:03:27 149.133.251.163 ACME-001 Oct 10 2014 11:19:35: %ASA-4-722051: Group <GroupPolicy_AcmeFullAccess> User <BClementine> IP <149.133.251.163> IPv4 Address <149.133.251.163> IPv6 address <d640:1405:1507:72f6:bd64:5ebe:ae34:d3ed> assigned to session
2016-01-30 00:03:54 120.204.80.141 ACME-001 Oct 10 2014 11:19:35: %ASA-4-722051: Group <GroupPolicy_AcmeFullAccess> User <LuaTodaMinha> IP <120.204.80.141> IPv4 Address <120.204.80.141> IPv6 address <1438:4f41:a6a1:609:f826:5591:48c8:77cc> assigned to session
2016-01-30 00:08:59 75.3.60.200 PROO-POS-002 Oct 10 2014 11:19:35: %ASA-4-722051: Group <GroupPolicy_AcmeFullAccess> User <Contessasosdx> IP <75.3.60.200> IPv4 Address <75.3.60.200> IPv6 address <87d2:37c8:aeb2:c849:7e41:16e6:4df7:31c0> assigned to session
2016-01-30 00:06:47 26.108.17.216 SE-003 Oct 10 2014 11:19:35: %ASA-4-722051: Group <GroupPolicy_AcmeFullAccess> User <Santosyzkir> IP <26.108.17.216> IPv4 Address <26.108.17.216> IPv6 address <909c:17da:e81d:f3ff:f8b2:28e6:e70d:3490> assigned to session
2016-01-30 00:04:02 102.109.126.224 SE-004 Oct 10 2014 11:19:35: %ASA-4-722051: Group <GroupPolicy_AcmeFullAccess> User <SambaLivre> IP <102.109.126.224> IPv4 Address <102.109.126.224> IPv6 address <298e:357e:82fa:1770:5b4d:ca18:c0bf:95d2> assigned to session
2016-01-30 00:05:15 213.52.70.48 PROO-POS-001 Oct 10 2014 11:19:35: %ASA-4-722051: Group <GroupPolicy_AcmeFullAccess> User <onehysoc> IP <213.52.70.48> IPv4 Address <213.52.70.48> IPv6 address <5e56:f560:ff9b:ec4:1fdd:7ac:da:e307> assigned to session
2016-01-30 00:06:19 2.36.1.171 ACME-002 Oct 10 2014 11:19:35: %ASA-4-722051: Group <GroupPolicy_AcmeFullAccess> User <vomafye> IP <2.36.1.171> IPv4 Address <2.36.1.171> IPv6 address <8846:63a5:0b3b:557c:b0d3:9dc5:7d6f:5935> assigned to session

```

Add-on Builder

Add-ons (TA)

Other Benefits

- Allows for the creation of multiple inputs, easily
- Creates setup pages for users to use
- Enables easy field extraction and aliasing
- Specifically aids in CIM mapping
- Will run validation checks against your app



splunk> App: Splunk Add-on Builder

Administrator Messages Settings Activity Help Find

My Add-on | Configure Data Collection Add Sample Data Extract Fields **Map to CIM** Create Alert Actions Validate & Package

 **Splunk Add-on Builder**

Map to CIM

Map fields from your add-on to the Common Information Model. Start by selecting an event type. If the dropdown list doesn't show your event type, click **Add Event Type** to create it. [Learn more](#)

Events

* Select an event type

MyEventType Add Event Type

* Select an event field

Select one event field

CIMs

* Select a CIM data model

Network_Traffic Eval Map

* Select a CIM field

Select a CIM field

Event Type	Event Field	Props.conf Entry	CIM	CIM Field	Actions
MyEventType	Username	FIELDALIAS-user = Username as user	Network_Traffic	user	Delete
MyEventType	IP	FIELDALIAS-src = IP as src	Network_Traffic	src	Delete
MyEventType	nid	FIELDALIAS-dest = nid as dest	Network_Traffic	dest	Delete
MyEventType	bv	FIELDALIAS-channel = bv as channel	Network_Traffic	channel	Delete

Add-on Builder

Add-ons (TA)

Other Benefits

- Allows for the creation of multiple inputs, easily
- Creates setup pages for users to use
- Enables easy field extraction and aliasing
- Specifically aids in CIM mapping
- Will run validation checks against your app



splunk> App: Splunk Add-on Builder

Administrator Messages Settings Activity Help Find

My Add-on | Configure Data Collection Add Sample Data Extract Fields Map to CIM Create Alert Actions **Validate & Package**

Validate & Package
Click **Validate** to validate your add-on against best practices and other rules, and to determine whether your app is ready for Splunk App Certification.
Your add-on package is ready. Click **Download Package** to create and download the SPL package file. [Learn more](#)

Best Practice x CIM Mapping x Field Extraction x APP Pre-certification x **Validate** **Download Package**

Overall Health Report



Ready for certification
Congratulations, your add-on is ready to submit to Splunk App Certification.

0 **Error** **1** **Warning** **97** **Pass**

Validation Rule Details

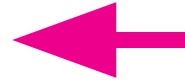
Rule Name	Severity	Category	Description	Solution Suggestion
Validate field coverage	Warning	CIM Mapping Validation	Coverage of the "(network, communicate).action" field in the "MyEventType" event type is 0.0, which is lower than the threshold value of 0.6.	Check whether you should add more regular expressions
Validate field conflicts	Pass	Field Extraction Validation	Pass the field validation for knowledge object "FIELDALIAS-des" in sourcetype "Mydata".	
Validate field conflicts	Pass	Field Extraction Validation	Pass the field validation for knowledge object "FIELDALIAS-user" in sourcetype "Mydata".	
Validate field conflicts	Pass	Field Extraction Validation	Pass the field validation for knowledge object "FIELDALIAS-src" in sourcetype "Mydata".	
Validate app certification	Pass	APP Pre-certification	Check that no duplicate stanzas exist in .conf files.	

Considerations

Add-ons (TA)

Points to be aware of:

- Ensure tokens/secrets are securely stored
- Document your code
- Create your own logs!!!
- If making generally available, how do you enable users to set it up
- User documentation

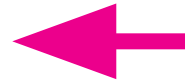


Considerations

Add-ons (TA)

Points to be aware of:

- Ensure tokens/secrets are securely stored
- Document your code
- Create your own logs!!!
- If making generally available, how do you enable users to set it up
- User documentation



Considerations

Add-ons (TA)

Points to be aware of:

- Ensure tokens/secrets are securely stored
- Document your code
- Create your own logs!!!
- If making generally available, how do you enable users to set it up
- User documentation



Considerations

Add-ons (TA)

Points to be aware of:

- Ensure tokens/secrets are securely stored
- Document your code
- Create your own logs!!!
- If making generally available, how do you enable users to set it up
- User documentation



Considerations

Add-ons (TA)

Points to be aware of:

- Ensure tokens/secrets are securely stored
- Document your code
- Create your own logs!!!
- If making generally available, how do you enable users to set it up
- User documentation



HTTP Event Collector

Add-ons (TA)

```
curl -k https://hec.example.com:8088/services/collector/event  
- H "Authorization: Splunk B5A79AAD-D822-46CC-80D1-819F80D7BFB0"  
- d '{"event": "hello world"}'
```

Resources

Add-ons (TA)

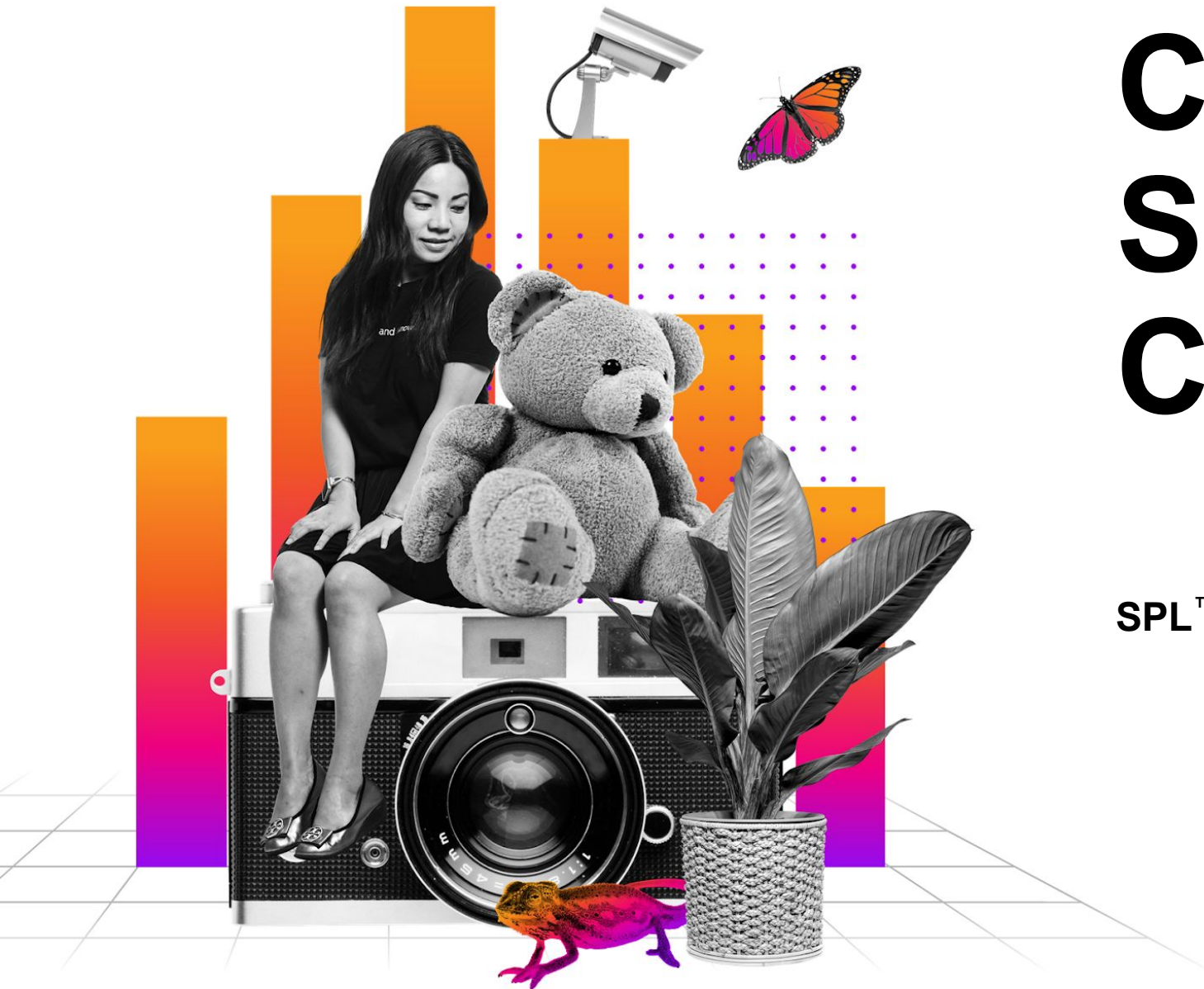
Links:

- [Modular Input Documentation](#)
- [Add-On Builder](#)
 - [User Guide](#)
- HEC
 - [Splunk Enterprise](#)
 - [Splunk Dev](#)

Custom Search Commands

SPL™ Friends!!!!

splunk> .conf22



Custom Search Commands

Build your own search command for use within a splunk search

Types:

- Streaming
 - Distributable (Eval / Fields / Where)
 - Centralized (Head / Streamstats / Dedup)
- Transforming
 - Stats / Chart / Timechart
- Generating
 - search / inputlookup / tstats / makeresults
- Dataset Processing
 - sort / eventstats



Custom Search Commands

Build your own search command for use within a splunk search

Types:

- Streaming
 - Distributable (Eval / Fields / Where)
 - Centralized (Head / Streamstats / Dedup)
- Transforming 
- Stats / Chart / Timechart
- Generating
 - search / inputlookup / tstats / makeresults
- Dataset Processing
 - sort / eventstats

Custom Search Commands

Build your own search command for use within a splunk search

Types:

- Streaming
 - Distributable (Eval / Fields / Where)
 - Centralized (Head / Streamstats / Dedup)
- Transforming
 - Stats / Chart / Timechart
- Generating
 - search / inputlookup / tstats / makeresults
- Dataset Processing
 - sort / eventstats



Custom Search Commands

Build your own search command for use within a splunk search

Types:

- Streaming
 - Distributable (Eval / Fields / Where)
 - Centralized (Head / Streamstats / Dedup)
- Transforming
 - Stats / Chart / Timechart
- Generating
 - search / inputlookup / tstats / makereults
- Dataset Processing
 - sort / eventstats



How To Create One

Custom Search Commands



commands.conf



Your own code

Commands.conf

Custom Search Commands

```
[COMMAND_NAME]  
filename = your_file_here.ext
```

Supported Executable Formats

Custom Search Commands

Extensions

- bat
- cmd
- exe
- js
- pl
- py
- sh

Available SDK

- Python

Resources

Custom Search Commands

Links

- [Overview](#)
- [Non-Python](#)
- [Examples](#)



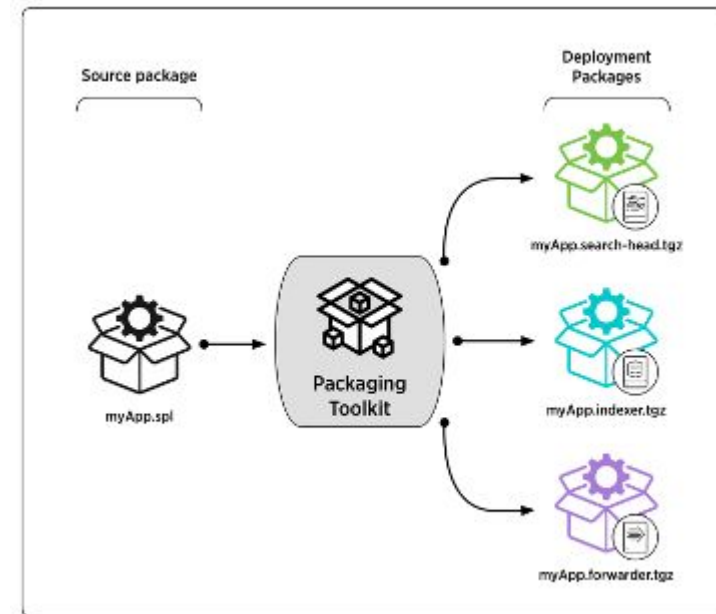
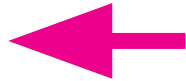
App Packaging and Review

Hello World!

splunk> .conf22

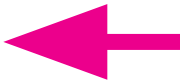
App Packaging

- Splunk® Packaging Toolkit
- Splunk® Enterprise CLI Command
- Manually



App Packaging

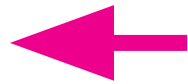
- Splunk® Packaging Toolkit
- Splunk® Enterprise CLI Command
- Manually



```
splunk package app <appname>
```

App Packaging

- Splunk® Packaging Toolkit
- Splunk® Enterprise CLI Command
- Manually



```
COPYFILE_DISABLE=1 tar -cvzf <appname>.tar.gz <appname_directory>
```

AppInspect

Automated App Review

Available In

- CLI



- API

```
pip install splunk-appinspect
```

```
splunk-appinspect inspect <APP-PACKAGE>
```

AppInspect

Automated App Review

Available In

- CLI
- API



```
curl -k -u <USERNAME> \
  --url "https://api.splunk.com/2.0/rest/login/splunk"
```

```
curl -X POST \
  -H "Authorization: bearer <TOKEN>" \
  -H "Cache-Control: no-cache" \
  -F "app_package=@\"/<PATH/APP-PACKAGE>\\\"" \
  --url "https://appinspect.splunk.com/v1/app/validate"
```

Resources

Packaging

Links

- [Deployment Architecture](#)
- [Packaging Apps](#)
- [AppInspect](#)

Resources

More from me

`.conf22`

- PLA1128 - Dashboarding Wowzas! Getting to know Splunk Dashboard Studio
- PLA1455 - Splunk is in the Lobby! How the McLaren Shadow Team Use Splunk to Level Up F1 eSports Performance

[.conf Online Catalog](#)

- DEV1198 - SPL Rehab: From Custom Search Command to Automated Delivery
- TRU1053 - Dashboarding Wowzas! Top Tips for Making Your Dashboards Awesome
- S4U1049 - Splunk@Home: How to Create Your Own Training Rig Using Data In Your Home!

Resources

More @ .conf22

- Builder Bar
- Talks
 - DEV1168 - Best Practices and Better Practices for Splunk Development
 - DEV1385 - Debug Deep Dive: Using Visual Studio Code to Debug Splunk Code Wherever it Runs
 - DEV1160 - Forget Add-On Builder! Build Splunk Platform Apps with Config Explorer!
 - DEV1204 - Making Your Splunk App Look Sweet With SUIT
 - DEV1703 - How Expedia Manages and Deploys Over 2000 Apps Using CI/CD and AppInspect

Thank You

