

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.

Forget Add-on Builder! Build Splunk Platform Apps with Config Explorer!

DEV1160B

Brett Adams

Cyber Analytics Specialist | Deloitte



splunk> .conf22



Brett Adams

Cyber Analytics Specialist | Deloitte

Why not Splunk® Add-on Builder?

Is a great starting point for small projects and first time developers.

Has limited checkpointing capabilities.

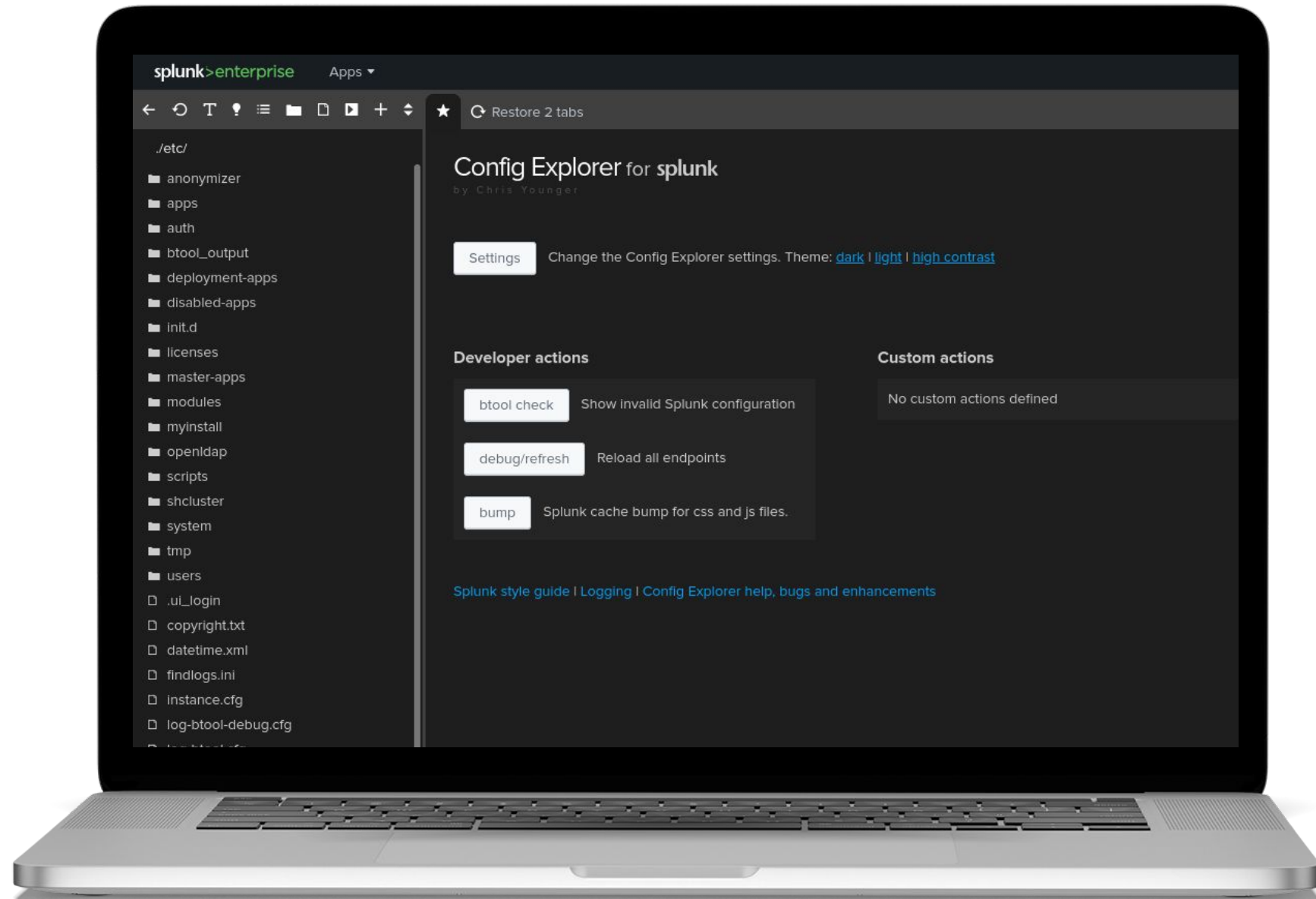
Creates large applications with multiple python dependencies.

By not using Add-on builder, you learn how Splunk apps actually work.

Config Explorer

Built by Chris Younger

Provides an editor interface for viewing and editing Splunk files.





Chris Younger

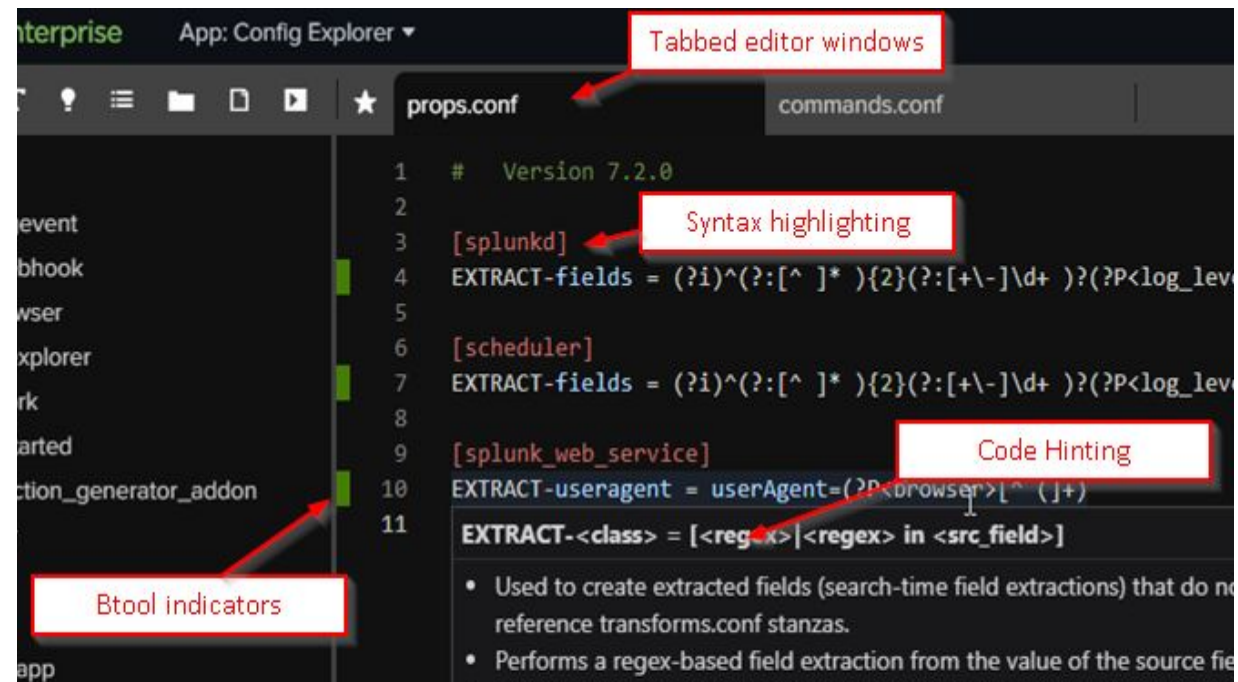
The Man, The Myth,
The Splunkbase Legend

[https://splunkbase.splunk.com/apps/#!/product/all/
author/chrisyoungerjds](https://splunkbase.splunk.com/apps/#!/product/all/author/chrisyoungerjds)

What is Config Explorer

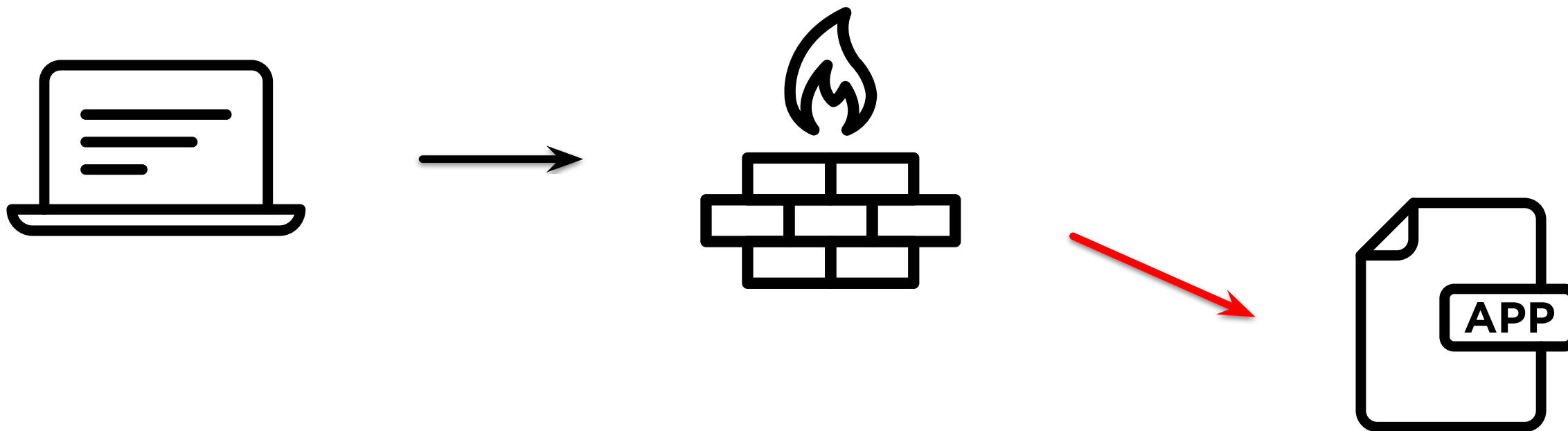
<https://splunkbase.splunk.com/app/4353/>

- Embeds the excellent Microsoft Monaco editor (VS Code)
- Code completion and tooltips
- Code gutter highlights using btool
- Displays the local spec files
- Diff files
- Works on Linux and Windows
- **Provides useful developer hooks (bump, debug refresh etc.) that can be customised and extended**
- **Optional version control of all changes by committing them to a git repository before and after changes**



The Magic

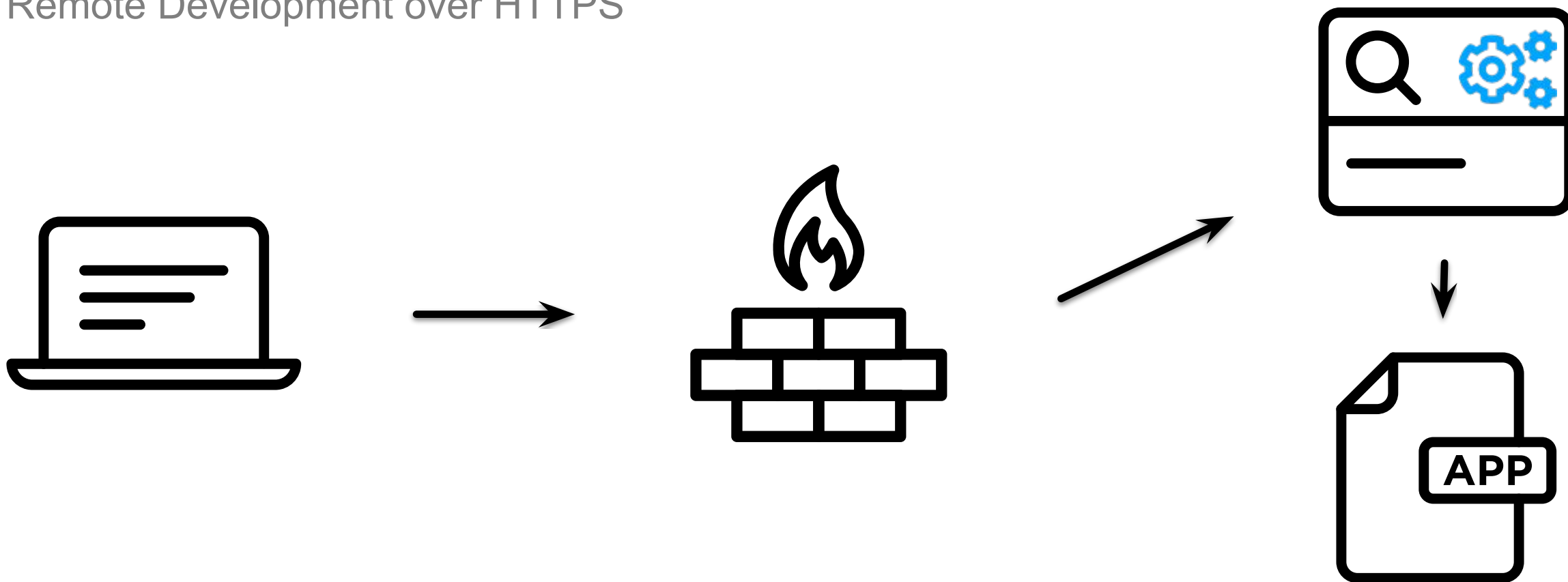
Remote Development over HTTPS



To learn more about developing with Visual Studio Code instead, check out **DEV1385** with Jason Conger.

The Magic

Remote Development over HTTPS



To learn more about developing with Visual Studio Code instead, check out **DEV1385** with Jason Conger.

Build in Enterprise

Run in Cloud & Enterprise





Development Resources

<https://dev.splunk.com/view/SP-CAAER3>

https://github.com/splunk/splunk-sdk-python/tree/master/examples/github_commits

<https://github.com/LukeMurphey/splunk-modular-input>

I recommend
developing
Splunk Apps with
Splunk[®] Enterprise
running on Linux.



Let's Build an App!



Back button

Current directory

/etc/apps/TA_prismacloud_audit/

bin		08/04/2022, 09:58:32
default		08/04/2022, 10:01:10
lib		08/04/2022, 09:57:55
local		09/04/2022, 09:56:31
metadata		09/04/2022, 10:32:17
README		08/04/2022, 09:57:56
static		08/04/2022, 09:57:55
.gitignore	35 B	08/04/2022, 09:57:55
app.manifest	1.01 KB	08/04/2022, 10:46:27
README.md	230 B	08/04/2022, 10:04:01
splunkbaseid	0 B	08/04/2022, 10:04:05

Files and Folders

Config Explorer for splunk

by Chris Younger

Settings

Change the Config Explorer settings. Theme: [dark](#) | [light](#) | [high contrast](#)

Developer actions

btool check

Show invalid Splunk configuration

debug/refresh

Reload all endpoints

bump

Splunk cache bump for css and js files.

Custom actions

No custom actions defined

[Splunk style guide](#) | [Logging](#) | [Config Explorer help, bugs and enhancements](#)

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

← ↺ T ⓘ ≡ 📁 📄 ▶ + ⇅

./etc/apps/TA_prismacloud_audit/

bin		08/04/2022, 09:58:32
default		08/04/2022, 10:01:10
lib		08/04/2022, 09:57:55
local		09/04/2022, 09:56:31
metadata		09/04/2022, 10:32:17
README		08/04/2022, 09:57:56
static		08/04/2022, 09:57:55
.gitignore	35 B	08/04/2022, 09:57:55
app.manifest	1.01 KB	08/04/2022, 10:46:27
README.md	230 B	08/04/2022, 10:04:01
splunkbaseid	0 B	08/04/2022, 10:04:05

Config Explorer for splunk

by Chris Younger

Settings Change the Config Explorer settings. Theme: [dark](#) | [light](#) | [high contrast](#)

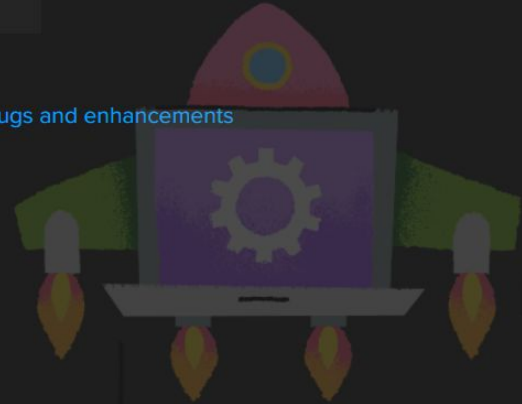
Developer actions

- btool check** Show invalid Splunk configuration
- debug/refresh** Reload all endpoints
- bump** Splunk cache bump for css and js files.

Custom actions

No custom actions defined

[Splunk style guide](#) | [Logging](#) | [Config Explorer help, bugs and enhancements](#)



splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

← ↻ T ⓘ ≡ 📁 📄 ▶ + ⚙️ ★ Settings

./etc/apps/TA_prismacloud_audit/

- bin
- default
- lib
- local
- metadata
- README
- static
- .gitignore
- app.manifest
- README.md
- splunkbaseid

Change both to 'true' then save with CTRL+S

```
1 [global]
2
3 write_access = true
4
5 # Creating new files/folders, deleting and renaming. This
6 # is obviously very dangerous and just like having filesystem access through
7 # the operating system, will make it very easy to destroy your Splunk
8 # environment if you don't know what you are doing.
9 # Defaults to false
10
11 run_commands = true
12
13 # Use with caution.
14 # Defaults to false
15
16 hide_settings = false
17
18 # Hide the "Settings" link from the home screen. Note that if write_access
19 # is true then settings can still be changed at
20 # etc/apps/config_explorer/local/config_explorer.conf. When the Settings link
21 # is displayed, it can be changed even when write_access is off. To
22 # prevent all editing, set hide_settings = true and write_access = false .
23 # Defaults to false.
24
25 #max_file_size = 10
26 # The maximum file size in megabytes that can be opened.
27
28 #cache_file_depth = 6
29 # Cache the list of files and folders for the left pane to this many levels deep.
30 # This makes navigation much faster (especially on windows) but uses more memory,
31 # causes slightly slower startup, and will not follow symbolic links. Set to 0 to
32 # disable cache but allow caching of visited directories. Set -1 to disable all caching.
33 # Defaults to 5
34
35 #conf_validate_on_save = true
```

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

← ↻ T ⓘ ≡ 📁 📄 + ⚙️ ★ prismacloud_audit.py

Click a file in the file browser

Opens as a new tab

```
1 import os
2 import sys
3 import json
4 import hashlib
5 import requests
6 import dateutil.parser
7 from datetime import datetime, timedelta
8 import time
9
10 sys.path.insert(0, os.path.join(os.path.dirname(__file__), "..", "lib"))
11 from splunklib.modularinput import *
12
13 class Input(Script):
14     MASK = "<encrypted>"
15     APP = __file__.split(os.sep)[-3]
16
17     def get_scheme(self):
18
19         scheme = Scheme("Prisma Cloud Audit")
20         scheme.description = ("Grab Audit data from the Prisma Cloud API")
21         scheme.use_external_validation = False
22         scheme.streaming_mode_xml = True
23         scheme.use_single_instance = False
24
25         scheme.add_argument(Argument(
26             name="api_key",
27             title="API Key",
28             data_type=Argument.data_type_string,
29             required_on_create = True,
30             required_on_edit = False
31         ))
32         scheme.add_argument(Argument(
33             name="history"
```




Hooks

Being lazy for maximum productivity

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

← ↻ T ⓘ ≡ 📁 📄 + ⌵ ★

prismacloud_audit.py Settings

Open Home, then Settings

Add these Stanzas

```
146 [hook:python_scheme]
147 # when editing .py files in bin, have an option to run them as 'splunk cmd'
148 # This will only show if run_commands=true in the config file
149 match = ./bin/*.py$
150 label = Run Scheme in Splunk env
151 action = run:splunk cmd python ${FILE} --scheme
152
153 [hook:python2_scheme]
154 # when editing .py files in bin, have an option to run them as 'splunk cmd'
155 # This will only show if run_commands=true in the config file
156 match = ./bin/*.py$
157 label = Run Scheme with Python 2
158 action = run:splunk cmd python2 ${FILE} --scheme
159
160 # when editing .conf files in "deployment-apps", have
161 # this is also useful on search head deployers. See "
162 # [hook:btool-deployment-apps-for-btool]
163 # match = /deployment-apps.*(?:local|default)/[^\/*\
164 # label = [deployment-apps-for-btool] Run btool on ${
165 # action = btool:${BASEFILE}:/opt/splunk/etc/deployme
166 # showWithSave = false
167
168 #####
169 # Custom home-tab actions
170 #####
171
172 # Actions are buttons on the home tab that can be used
173 # the run_commands option must be enabled. Read the s
174 # uses the same command options.
175
176 # Examples below:
177
```

Save file

- Open documentation (.spec file)
- Show out-of-the-box hooks
- Change All Occurrences **Ctrl+F2**
- Cut
- Copy
- Set post-save action
- Preferences
- Create link to line/selection
- Command Palette **F1**

Don't forget to save with the right click menu or CTRL+S

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

← ↻ T ? ☰ 📁 📄 + ⚙️ ★ prismacloud_audit.py Settings

./etc/apps/TA_prismacloud_audit/

- bin
- default
- lib
- local
- metadata
- README
- static
- .gitignore
- app.manifest
- README.md
- splunkbaseid

```
1 import os
2 import sys
3 import json
4 import math
5 import requests
6 import dateutil.parser
7 from datetime import datetime, timedelta
8 import time
9
10 sys.path.insert(0, os.path.dirname(__file__))
11 from splunklib.modularinput import Input
12
13 class Input(Script):
14     MASK = "<encrypted>"
15     APP = __file__.split('.')[0]
16
17     def get_scheme(self, scheme_name):
18
19         scheme = Scheme(scheme_name)
20         scheme.description = "Prisma Cloud Audit"
21         scheme.use_external_streaming = True
22         scheme.use_splunk_scheme = True
23
24         scheme.add_argument(
25             name="api_key",
26             title="API Key",
27             data_type="text",
28             required_on_all_inputs=True,
29             required_for_post_save=True,
30         )
31
32         scheme.add_argument(
33             name="history",
```

Save file

Reload from disk

Save and \$Run in Splunk env

Save and \$Run Scheme in Splunk env

Save and \$Run Scheme with Python 2

\$Run in Splunk env

\$Run Scheme in Splunk env

\$Run Scheme with Python 2

Change All Occurrences Ctrl+F2

Cut

Copy

Set post-save action

Preferences

Create link to line/selection

Hooks appear in the context menu depending on their configuration

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

← ↻ T ? ☰ 📁 📄 + ⇅ ★ prismacloud_audit.py Settings

./etc/apps/TA_prismacloud_audit/

- bin
- default
- lib
- local
- metadata
- README
- static
- .gitignore
- app.manifest
- README.md
- splunkbaseid

```
1 import os
2 import sys
3 import json
4 import math
5 import requests
6 import dateutil.parser
7 from datetime import datetime, timedelta
8 import time
9
10 sys.path.insert(0, os.path.dirname(__file__), "..", "lib"))
11 from splunklib.modular import ScriptInput
12
13 class Input(ScriptInput):
14     MASK = "<encrypted>"
15     APP = __file__.split('.')[0]
16
17     def get_scheme(self, scheme_name):
18
19         scheme = Scheme(scheme_name, "Prisma Cloud Audit", "Prisma Cloud Audit", "Prisma Cloud Audit")
20         scheme.description = "Prisma Cloud Audit"
21         scheme.use_extensions = True
22         scheme.stream_type = "text"
23         scheme.use_splunklib = True
24
25         scheme.add_argument(
26             name="api_key",
27             title="API Key",
28             data_type="text",
29             required_on_create=True,
30             required_on_update=True,
31         )
32         scheme.add_argument(
33             name="history",
```

Save file

Reload from disk

Save and \$Run in Splunk env

Save and \$Run Scheme in Splunk env

Save and \$Run Scheme with Python 2

\$Run in Splunk env

\$Run Scheme in Splunk env

\$Run Scheme with Python 2

Change All Occurrences Ctrl+F2

Cut

Copy

Set post-save action

Preferences

Create link to line/selection

Saves the file before running the hook

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

← ↻ T ⓘ ≡ 📁 📄 ▶ + ⇅ ★ prismacloud_audit.py Settings \$ splunk cmd python ./etc/apps/TA

./etc/apps/TA_prismacloud_audit/

- bin
- default
- lib
- local
- metadata
- README
- static
- .gitignore
- app.manifest
- README.md
- splunkbaseid

```
1 File "./etc/apps/TA_prismacloud_audit/bin/prismacloud_audit.py", line 110
2     Intentional Typo
3     ^
4 IndentationError: unexpected indent
5
6
```

Use the right click menu to run the hook again

Rerun

Change All Occurrences Ctrl+F2

Cut

Copy

Preferences

Command Palette F1

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

prismacloud_audit.py Settings \$ splunk cmd python ./etc/apps/TA

./etc/apps/TA_prismacloud_audit/

- bin
- default
- lib
- local
- metadata
- README
- static
- .gitignore
- app.manifest
- README.md
- splunkbaseid

```
1 <scheme><title>Prisma Cloud Audit</title><description>Grab Audit data from the Prisma Cloud API</description>
2
```

This is the expected XML output

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

← ↶ T ? ≡ 📁 📄 ▶ + ⇅ ★ prismacloud_audit.py

./etc/apps/TA_prismacloud_audit/bin/
prismacloud_audit.py

```
1 import os
2 import sys
3 import json
4 import math
5 import requests
6 import dateutil.parser
7 from datetime import datetime, timedelta
8 import time
9
10 sys.path.insert(0, os.path.join(os.path.dirname(__file__),
11 from splunklib.modularinput import *
12
13 class Input(Script):
14     MASK = "<encrypted>"
15     APP = __file__.split(os.sep)[-3]
16
17     def get_scheme(self):
18
19         scheme = Scheme("Prisma Cloud Audit")
20         scheme.description = ("Grab Audit data from Prisma Cloud")
21         scheme.use_external_validation = False
22         scheme.streaming_mode_xml = True
23         scheme.use_single_instance = False
24
25         # Set post-save action
26
27         string,
28
29         required_on_create = True,
30         required_on_edit = False
31     ))
32     scheme.add_argument(Argument(
33         name="history"
```

Save file
Reload from disk
Save and \$Run in Splunk env
Save and \$Run Scheme in Splunk env
Save and \$Run Scheme with Python 2
\$Run in Splunk env
\$Run Scheme in Splunk env
\$Run Scheme with Python 2
Change All Occurrences Ctrl+F2
Cut
Copy
Set post-save action
Create link to line/selection
Command Palette F1

Sets a post-save action for the open file

splunk>enterprise

Apps ▾

Administrator ▾

Messages ▾

Settings ▾

Activity ▾

Help ▾

Find

← ↻ T ? ☰ 📄

/etc/apps/TA_prismacloud_audit/bin

prismacloud_audit.py

Set post-save action

✕

Enter a command to automatically run after successful save of this file only. This action will be saved in your browser local storage (it will not affect other users or other browsers you use, but it will be remembered after browser refresh). Run commands will be executed from the SPLUNK_HOME directory.

File: `./etc/apps/TA_prismacloud_audit/bin/prismacloud_audit.py`Suggest: `run:splunk cmd python2 ./etc/apps/TA_prismacloud_audit/bin/prismacloud_audit.py --scheme`Suggest: `run:splunk cmd python ./etc/apps/TA_prismacloud_audit/bin/prismacloud_audit.py --scheme`

Run command ▾

`splunk cmd python ./etc/apps/TA_prismacloud_audit/bin/prismacloud_auc`

Run in background tab:

Yes ▾

The following options will check the returned content from a post-save action for a specific string and will show a success or failure icon to be displayed.

Content match for success: Content match for failure:

Save

Cancel

Click a
suggestion to
auto populate

Add success
and failure
strings

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

← ↶ T ? ≡ 📁 📄 ▶ + ⇅ ★ prismacloud_audit.py \$ splunk cmd python ./etc/apps/TA_prismacloud_audit/bin/prismacloud_audit.py ✓

Shows post save action was successful

```
./etc/apps/TA_prismacloud_audit/bin/
└─ prismacloud_audit.py

1  import os
2  import sys
3  import json
4  import math
5  import requests
6  import dateutil.parser
7  from datetime import datetime, timedelta
8  import time
9
10 sys.path.insert(0, os.path.join(os.path.dirname(__file__), "..", "lib"))
11 from splunklib.modularinput import *
12
13 class Input(Script):
14     MASK = "<encrypted>"
15     APP = __file__.split(os.sep)[-3]
16
17     def get_scheme(self):
18
19         scheme = Scheme("Prisma Cloud Audit")
20         scheme.description = ("Grab Audit data from the Prisma Cloud API")
21         scheme.use_external_validation = False
22         scheme.streaming_mode_xml = True
23         scheme.use_single_instance = False
24
25         scheme.add_argument(Argument(
26             name="api_key",
27             title="API Key",
28             data_type=Argument.data_type_string,
29             required_on_create = True,
30             required_on_edit = False
31         ))
32         scheme.add_argument(Argument(
33             name="history"
```

✓ Saved



Spec Files

Better than typing inputs.conf.spec into Google

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

← ↻ T ⓘ ≡ 📁 📄 + ⇅ ★ app.conf

./etc/apps/TA_prismacloud_audit/default/

- app.conf
- inputs.conf
- props.conf

```
1 [install]
2 state = enabled
3 is_configured = 0
4
5 [launcher]
6 author = splunkbase@ba.id.au
7 version = 0.1.0
8 description = Prisma Cloud Audit Data Input
9
10 [package]
11 id = TA_prismacloud_audit
12
13 [ui]
14 label = Prisma Cloud Audit Data Input
15 is_visible = 0
16
17
```

Opens the .spec file for the current .conf file

Save file

Open app.conf.spec

Change All Occurrences Ctrl+F2

Cut

Copy

Set post-save action

Preferences

Create link to line/selection

Command Palette F1

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

← ↻ T ⓘ ≡ 📁 📄 + ⇅ ★ app.conf spec: app

./etc/apps/TA_prismacloud_audit/default/

- app.conf
- inputs.conf
- props.conf

```
90
91 [package]
92 * This stanza defines upgrade-related metadata that streamlines app upgrade
93   to future versions of Splunk Enterprise.
94
95 id = <string>
96 * Omit this setting for apps that are for internal use only and not intended
97   for upload to Splunkbase.
98 * id is required for all new apps that you upload to Splunkbase. Future
99   Splunk Enterprise will use appid to correlate locally-installed apps with
100  same app on Splunkbase (e.g. to notify users about app updates).
101 * id must be the same as the folder name in which your app lives in
102   $SPLUNK_HOME/etc/apps.
103 * id must adhere to these cross-platform folder name restrictions:
104   * must contain only letters, numbers, "." (dot), and "_" (underscore)
105     characters.
106   * must not end with a dot character.
107   * must not be any of the following names: CON, PRN, AUX, NUL,
108     COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9,
109     LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, LPT9
110
111 check_for_updates = <boolean>
112 * Determines whether Splunk Enterprise checks for updates for this
113   app.
114 * Default: true
115
116 show_upgrade_notification = <boolean>
117 * Determines whether Splunk Enterprise shows an upgrade notification in Splunk
118   Web for this app.
119 * Default: false
120
121 [install]
122 * This stanza defines install settings for this app.
```

> check_for_updates Aa AbI_* 1 of 1 ↑ ↓ ≡ ×

Open Find with CTRL+F

Matches are highlighted

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

← ↻ T ⓘ ≡ 📁 📄 ▶ + ⚙️ ★ props.conf

./etc/apps/TA_prismacloud_audit/default/

- app.conf
- inputs.conf
- props.conf

1 [prisma:cloud:audit]
2 DATETIME_CONFIG = NONE
3 SHOULD_LINEMERGE = False
4
5 KV_MODE = JSON
6
7 KV_MODE = [none|auto|auto_escaped|multi|json|xml]
8

Shows if the configuration is in the btool output

Hover over an attribute to show its .spec entry

- Used for search-time field extractions only.
- Specifies the field/value extraction mode for the data.
- Set KV_MODE to one of the following:
 - none: if you want no field/value extraction to take place.
 - auto: extracts field/value pairs separated by equal signs.
 - auto_escaped: extracts fields/value pairs separated by equal signs and honors \" and \\ as escaped sequences within quoted values, e.g field="value with \"nested\" quotes"
 - multi: invokes the multikv search command to expand a tabular event into multiple events.
 - xml : automatically extracts fields from XML data.

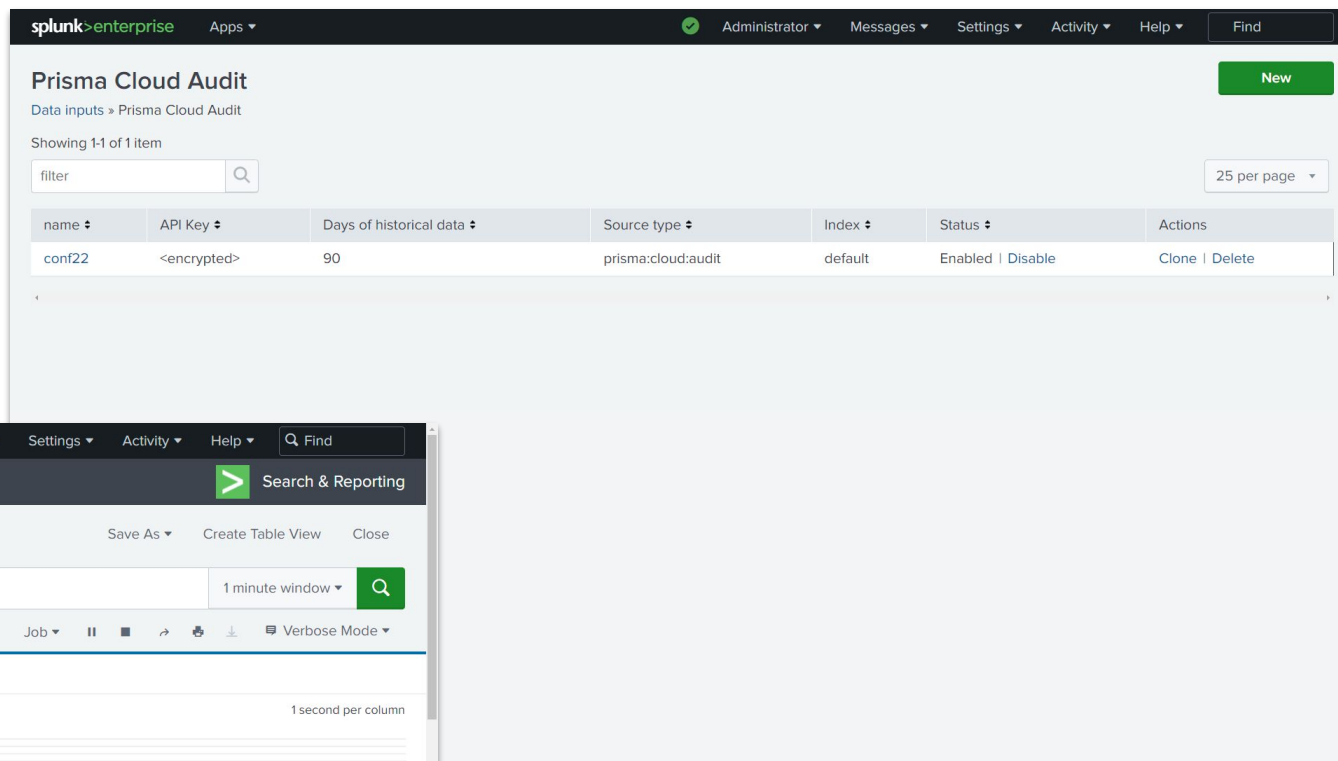


Testing

Finding your faults, just like mom

Testing

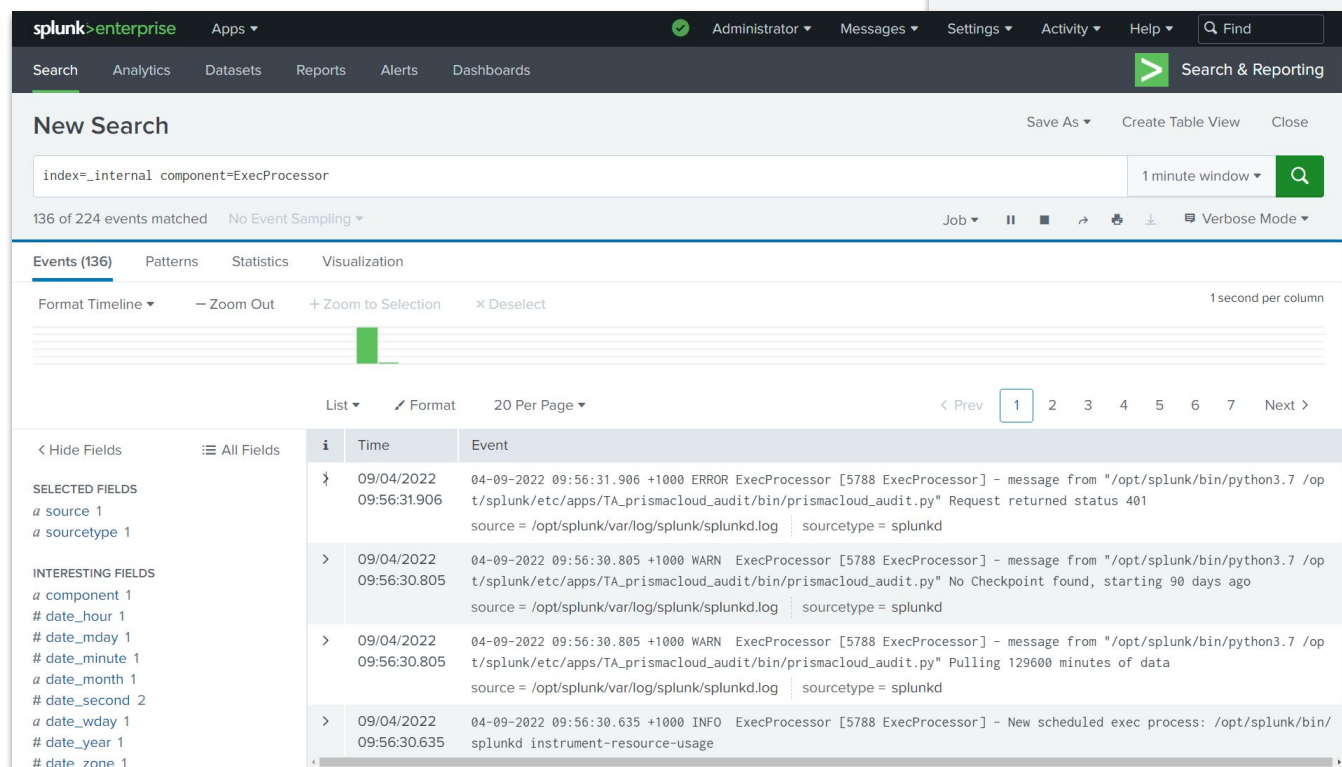
Outside Config Explorer



The screenshot shows the Splunk Enterprise interface for configuring a data input. The top navigation bar includes 'splunk>enterprise', 'Apps', and user options like 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a 'Find' button. The main heading is 'Prisma Cloud Audit' with a 'Data inputs > Prisma Cloud Audit' breadcrumb. Below this, it says 'Showing 1-1 of 1 item'. A search filter box is present. A table lists the configuration details:

name	API Key	Days of historical data	Source type	Index	Status	Actions
conf22	<encrypted>	90	prisma:cloud:audit	default	Enabled Disable	Clone Delete

A 'New' button is located in the top right corner.



The screenshot shows the Splunk Enterprise interface for a search results page. The top navigation bar includes 'splunk>enterprise', 'Apps', and user options like 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a 'Find' button. The main heading is 'New Search' with a 'Search & Reporting' button. The search query is 'index=_internal component=ExecProcessor' with a '1 minute window' and a search button. Below the search bar, it says '136 of 224 events matched' and 'No Event Sampling'. The results are displayed in a table view with columns for 'Time' and 'Event'.

Selected Fields:

- a source 1
- a sourcetype 1

Interesting Fields:

- a component 1
- # date_hour 1
- # date_mday 1
- # date_minute 1
- a date_month 1
- # date_second 2
- a date_wday 1
- # date_year 1
- # date_zone 1

Events (136):

Time	Event
09/04/2022 09:56:31.906	04-09-2022 09:56:31.906 +1000 ERROR ExecProcessor [5788 ExecProcessor] - message from "/opt/splunk/bin/python3.7 /opt/splunk/etc/apps/TA_prismacloud_audit/bin/prismacloud_audit.py" Request returned status 401 source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
09/04/2022 09:56:30.805	04-09-2022 09:56:30.805 +1000 WARN ExecProcessor [5788 ExecProcessor] - message from "/opt/splunk/bin/python3.7 /opt/splunk/etc/apps/TA_prismacloud_audit/bin/prismacloud_audit.py" No Checkpoint found, starting 90 days ago source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
09/04/2022 09:56:30.805	04-09-2022 09:56:30.805 +1000 WARN ExecProcessor [5788 ExecProcessor] - message from "/opt/splunk/bin/python3.7 /opt/splunk/etc/apps/TA_prismacloud_audit/bin/prismacloud_audit.py" Pulling 129600 minutes of data source = /opt/splunk/var/log/splunk/splunkd.log sourcetype = splunkd
09/04/2022 09:56:30.635	04-09-2022 09:56:30.635 +1000 INFO ExecProcessor [5788 ExecProcessor] - New scheduled exec process: /opt/splunk/bin/splunkd instrument-resource-usage

Perfect Packaging

The shell script way

Remove compiled and cached python files

Remove metadata/local.meta

Remove any boilerplate files and Lookup Editor backups

Set all files to 644 (Owner Read & Write, Others Read)

Add execute permission to folders and files in bin

Compress to tar gzip archive with .spl extension

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

\$ bash /opt/splunk/etc/scripts/pack

./etc/apps/TA_prismacloud_audit/

- bin
- default
- lib
- local
- metadata
- README
- static
- .gitignore
- app.manifest
- README.md
- splunkbaseid

\$App Inspect

\$Package

\$Package New

\$Promote

\$Slim Validate

\$Upload

\$Git status

Show change log

Run the 'Package' hook on the current folder

```
remove '/opt/splunk/etc/apps/TA_prismacloud_audit/bin/**/*.pyc': No such file or directory
remove '/opt/splunk/etc/apps/TA_prismacloud_audit/bin/**/*.so': No such file or directory
remove '/opt/splunk/etc/apps/TA_prismacloud_audit/bin/__pycache__': No such file or directory
remove '/opt/splunk/etc/apps/TA_prismacloud_audit/lib/**/*.so': No such file or directory
remove '/opt/splunk/etc/apps/TA_prismacloud_audit/lib/__pycache__': No such file or directory
stat '/opt/splunk/etc/apps/TA_prismacloud_audit/.git': No such file or directory
prismacloud_audit' is packaged.
Location: /opt/splunk/share/splunk/app_packages/TA_prismacloud_audit.spl
stat '/opt/splunk/etc/tmp/.git': No such file or directory
```

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

← ↻ T ⓘ ≡ 📁 📄 ➕ ⚙️ ★ \$ splunk cmd python ./etc/scripts/a

./etc/apps/TA_prismacloud_audit

- \$App Inspect
- \$Package
- \$Package New
- \$Promote
- \$Slim Validate
- \$Upload
- \$Git status
- Show change log

bin
default
lib
local
metadata
README
static
.gitignore
app.manifest
README.md
splunkbaseid

```
1 TA_prismacloud_audit
2 {'request_id': '1c209be3-da12-46...', 'links': 'Validation request submitted.', 'links
3 PROCESSING
4 SUCCESS
5 {'error': 0, 'failure': 0, 'skipped': 0, 'manual_check': 25, 'not_applicable': 130, 'warning': 3, 'succes
6
7 cloud
8 [{ 'result': 'warning', 'message': "28 Python files found. Update these Python scripts to be cross-compatil
9 [{ 'result': 'manual_check', 'message': "Python script is not well formed, syntax error found in python sc
10 [{ 'result': 'manual_check', 'message': 'The following lines should be inspected during code review, Possi
11 [{ 'result': 'manual_check', 'message': 'The following line will be inspected during code review. The `__b
12 [{ 'result': 'manual_check', 'message': 'The following lines should be inspected during code review, `gzip
13 [{ 'result': 'manual_check', 'message': 'The following line will be inspected during code review. The `os.
14 [{ 'result': 'manual_check', 'message': 'The following lines should be inspected during code review. `sock
15 [{ 'result': 'warning', 'message': 'Bias language is found in the app. ent.<<<WHITELIST>>> (lib/splunklib/
16 [{ 'result': 'manual_check', 'message': 'Environment variable being used in lib/splunklib/searchcommands/v
17 [{ 'result': 'manual_check', 'message': 'The executable will be inspected during code review: File: lib/sp
18
19 self-service
20 [{ 'result': 'warning', 'message': "Json Schema version of 2.0.0 is not yet compatible with any versions o
21
22 future
23
24
25
```

High level outcome from AppInspect

Results from each specific tag

splunk>enterprise

Apps ▾



Administrator ▾

Messages ▾

Settings ▾

Activity ▾

Help ▾

Find



./etc/build/

array2object.spl

array2object.spl.json

TA_prismacloud_audit.spl

TA_prismacloud_audit.spl.json

Config Explorer for splunk

by Chris Younger

Change the Config Explorer settings. Theme: [dark](#) | [light](#) | [high contrast](#)

\$App Inspect

\$Upload

Rename

Delete

View file history

Download

Mark for comparison

debug/refresh

Reload all endpoints

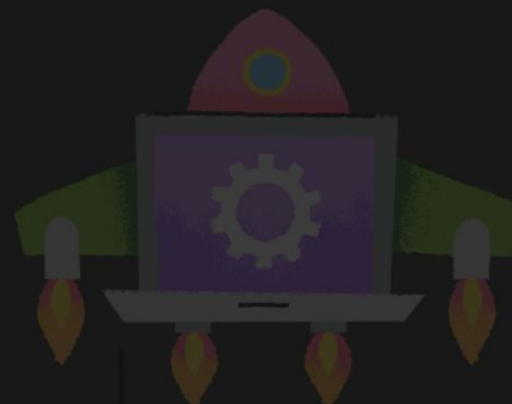
restart splunk

bump

Splunk cache bump for css and js files.

Download any file using
the right click menu

[Splunk style guide](#) | [Logging](#) | [Config Explorer help, bugs and enhancements](#)



splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

splunkbaseid

6379

bin
default
lib
local
metadata
README
static
.gitignore
app.manifest
README.md
splunkbaseid

- \$App Inspect
- \$Package
- \$Package New
- \$Promote
- \$Slim Validate
- \$Upload**
- \$On status
- Show change log



Source Control

Keeping a permanent record of every mistake

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

← ↶ T ? ≡ 📁 📄 ▶ + ⏴ ★ Settings

./etc/apps/TA_prismacloud_audit/

- bin
- default
- lib
- local
- metadata
- README
- static
- .gitignore
- app.manifest
- README.md
- splunkbaseid

```
50
51 git_autocommit = true
52 # Track all file changes by autom
53 # Note you must first configure
54 # Autocommitting is a 'best effort
55 # Defaults to false
56
57 #git_autocommit_show_output = auto
58 # When autocommit is enabled, when should we show the commit log
59 # true = Always show git messages
60 # false = Never show git output
61 # auto = Only show git messages when there is a non-zero status code
62 # Defaults to auto
63
64 #git_autocommit_dir =
65 # Force specific git repository location, relative to SPLUNK_HOME directory.
66 # Defaults to empty, meaning normal git rules will apply (search up from current directory)
67
68 #git_autocommit_work_tree =
69 # Force root location from where changes are tracked, relative to SPLUNK_HOME directory
70 # Set to "etc/" to track all changes beneath etc folder.
71 # Defaults to empty, meaning the normal git behavior will apply.
72
73 #detect_changed_files = true
74 #* Check if files that are open have changed on the filesystem and warn if so.
75 #* Defaults to true
76
77 #####
78 # Custom action hooks #
79 #####
80
81 # Custom hooks create right-click actions for files that match a regular expression
82 # See etc/apps/config-explorer/default/config-explorer.conf for many examples
```

Change to true and don't forget to save

with a generic message. Please see the documentation.

.gitignore

```
local/  
local.meta  
__pycache__  
*.pyc
```

splunk> **.conf22**



splunk>enterprise



Administrator ▾

Messages ▾

Settings ▾

Activity ▾

Help ▾

Find



Refresh button

★ Settings

\$ git init

/etc/apps/TA_prismacloud_audit/

└─ .git

└─ default

└─ lib

└─ local

└─ metadata

└─ README

└─ static

└─ .gitignore

└─ app.manifest

└─ README.md

└─ splunkbaseid

```
1 Initialized empty Git repository in /opt/splunk/etc/apps/TA_prismacloud_audit/.git/
2
3
```

Output from the
run command

splunk> .conf22

splunk>enterprise

Apps ▾



Administrator ▾

Messages ▾

Settings ▾

Activity ▾

Help ▾

Find

← ↻ T ⓘ ≡ 📁 📄 ▶ + ⇅ ★ app.conf

\$ git log

./etc/apps/TA_prismacloud_audit/default/

📄 app.conf

📄 inputs.conf

📄 props.conf

```
1  commit 9010e54f2230fca7657ef4f36dca50ec14b0c763
2  Author: Brett [redacted]@gmail.com>
3  Date:   Sun Apr 17 12:09:59 2022 +1000
4
5  |   admin save
6
7  commit 221c7ceafcffd32b803bb12b030d304c2010c355
8  Author: Brett [redacted]@gmail.com>
9  Date:   Sun Apr 17 12:08:49 2022 +1000
10
11 |   admin save
12
13
```

splunk> .conf22

<> Code

Issues

Pull requests

Actions

Projects

Wiki

Security

Insights

Settings

main

Commits on Jan 20, 2022

admin save



Bre77 committed on 20 Jan



a7c98ae



admin save



Bre77 committed on 20 Jan



bbb0423



admin save



Bre77 committed on 20 Jan



2c4a33c



admin save



Bre77 committed on 20 Jan



15f44d1



admin save



Bre77 committed on 20 Jan



e9d1672



admin save



Bre77 committed on 20 Jan



51ea89b



admin save



Bre77 committed on 20 Jan



bd8a217



admin save



Bre77 committed on 20 Jan



29ae06b



admin save



Bre77 committed on 20 Jan



9abac9c



admin save

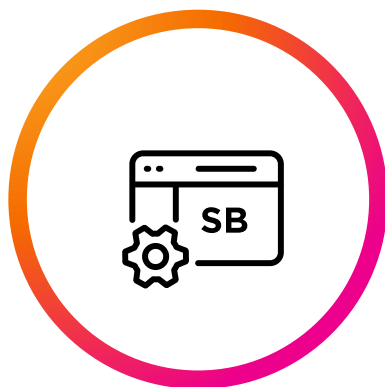
Recap

Create and Use Hooks



Speed up repetitive tasks

Reference the Spec & Btool



Avoid simple mistakes and write perfect conf

Test Fast and AppInspect



Using hooks, realtime search, and AppInspect

Easy Source Control



Publish your source (but not your passwords)



Git Hooked

On Config Explorer

<https://github.com/Bre77/DEV1160B>

Thank You

