While you wait...

Why not let us know what topics you'd like us to cover next?

Take the short survey at:

squaredup.com/topics

SquaredUp

Coffee Break Webinar Series

Integrating Splunk

Topic

Integrating Splunk events into Squared Up via WebAPI

Discussion points:

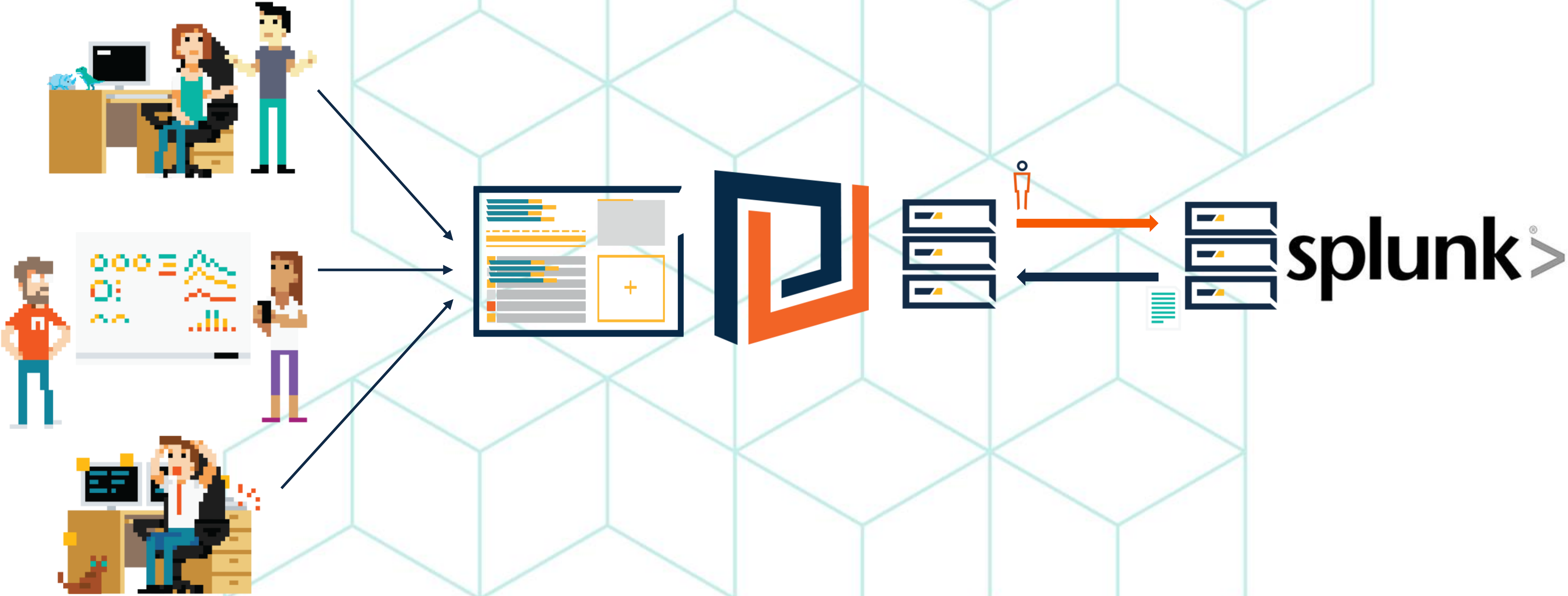
- Connecting to Splunk
- Simple queries
- Perspectives

Web API Integration

Integrate data from external sources alongside SCOM into a single pane of glass

- Queries live API data and displays on your dashboard
- Apply SCOM role-based access control
- No need to setup users in external systems
- Easy to share enterprise-wide
- Results are displayed on demand, so no extra storage, agents etc

How it works



Connecting to Splunk

Creating a provider and sending basic queries

- Create a Web API Provider
- Create a simple dashboard with a WebAPI (Grid) tile
- Send a oneshot query to Splunk

```
download_installer"
log "====> This node is using channel #{node['squared_up_channel']}
log "====> This node is using the package #{node['squared_up_package
irectory "c:/squared_up_temp" do
 action :create
nd

Chef::Recipe.send(:include, Windows::Helper)
ere_is_a_build_installed = is_package_installed?(

_block "check-current-build-time" do
ock do
node.run_state["install_new_build"] = true
node.run_state["ftp_file_time"] = File.mtime(
hef::Log.info("Last modification time: #{node.run_state
 node.attribute?('squared_up_build_last_mod_time')
if node.normal['squared_up_build_last_mod_time']
  node.run_state["install_new_build"] = true
lse
  node.run_state["install_new_build"] = false
nd
```

Summary

- Create a simple provider
  - Add Authorisation header, specifying Basic *APIkey*
  - Enable ignore invalid SSL if using self-signed certs
- Use http post mode
- Set response data key path to results

Query data options

Name	Description
search	search= *Your search query*
exec_mode	Must specify **oneshot**
earliest_time	The earliest result (useful for Last x hours, e.g. -1h)
latest_time	The latest result, usually just **now**
output_mode	Must specify json
timeout	How long Splunk should keep results for (in seconds)
max_time	Query processing timeout limit (in seconds)

Recommendations

When making use of the Web API tile, we'd recommend you keep these best practices in mind

- Get hold of the API Documentation or a Subject Matter expert
- Test your query with PowerShell/Curl/Postman to see the results directly
- Users will need the construct-sensitive-queries permission to be able to create/edit Web API tiles, which should only be given to extremely trusted users

Coffee Break: Resources

Let us know what you'd like us to cover:
squaredup.com/topics

See what's coming up next:
squaredup.com/coffee-break-series

Recordings and slides published via
squaredup.com/blog

YouTube playlist for series
https://www.youtube.com/playlist?list=PLJNXoiGgmTEu3yZRGpPNWQbG9WMyihZFs

Follow up email, inc. resources, sent out after each webinar

Q&A

SquaredUp