

Metrics Onboarding Workshop for IT Ops



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.
© 2024 Splunk Inc. All rights reserved.

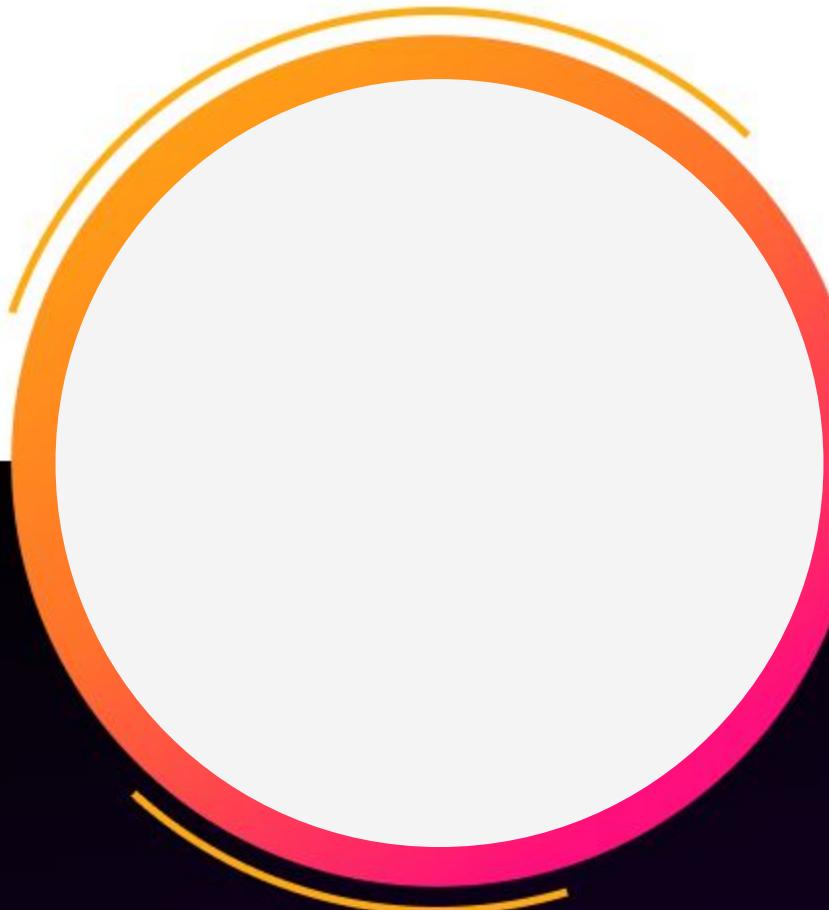


Presenter Name

Job Title

splunk>

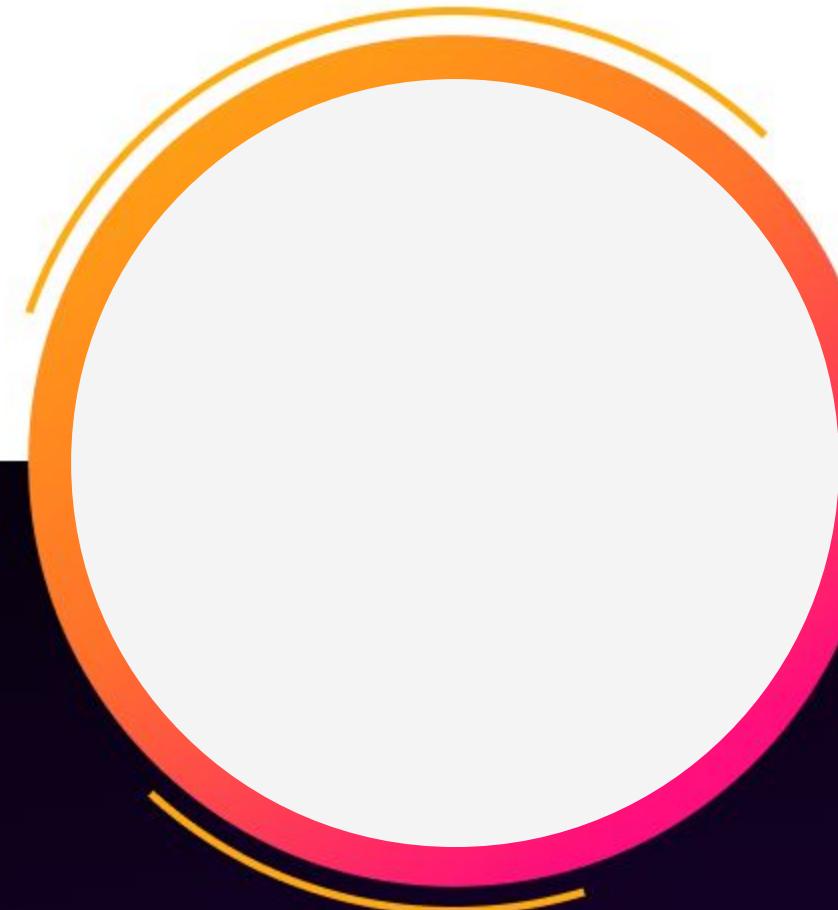
Meet Your Presenters!



Presenter Name

Presenter Name

Job Title



Presenter Name

Presenter Name

Job Title

splunk>

Please introduce yourself!

- Name
- Company/organisation
- Role
- Are you currently using Splunk?
- What are you interested in using Splunk for?





REGISTRATION

5 MINS

Enroll in Today's Workshop

Tasks

1. Get a splunk.com account if you don't have one yet:
<https://splk.it/SignUp>
2. Enroll in the Splunk Show workshop event:
<https://show.splunk.com/event/<eventID>>
3. Download the lab sheet:
<https://splk.it/metrics-lab-sheet>
Contains step-by-step instructions for all of today's exercises!
4. Download a copy of today's slide deck:
<https://splk.it/metrics-attendee>

Goal



PLATFORM

Metrics Onboarding Workshop for IT Ops

⌚ 26/09 14:33 - 26/09 22:24

Enterprise

Metrics Onboarding Workshop...

▶ AVAILABLE

Actions ▾

👤 + Enroll event

Enroll in today's event

What Are Metrics?



Difference Between Metrics and Events

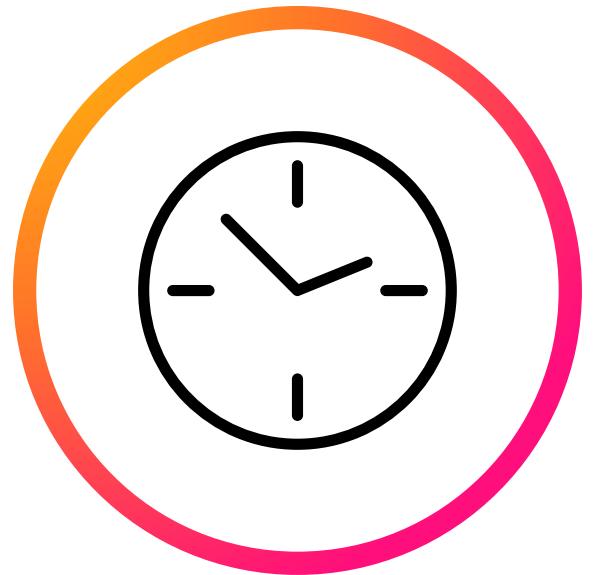
Metrics

- Predict and/or discover “what is happening?”
- Typically know what you want to measure
- Structured data
- Numerical in nature
- Best way to monitor a process or device over time
 - CPU, memory, network latency, disk usage

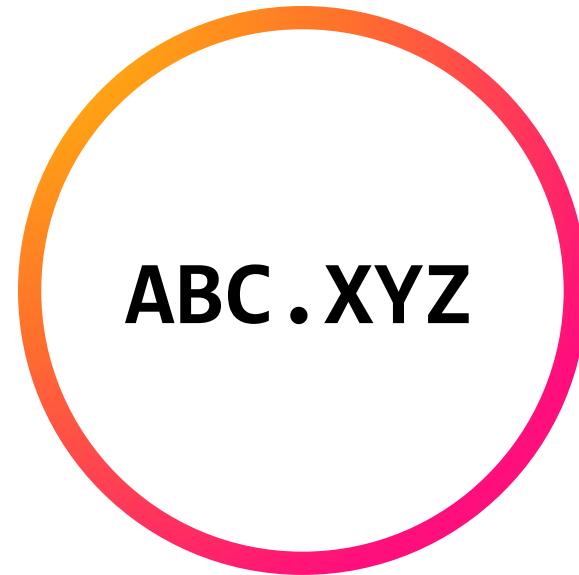
Events

- Tells a story or big picture of “why did this happen?”
- Typically unstructured data (log data)
- Made up of individual events
- Not always numerical

What Metrics Look Like

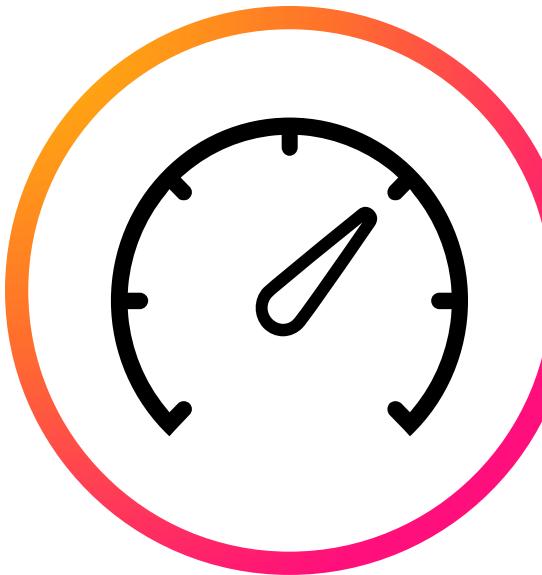


Time



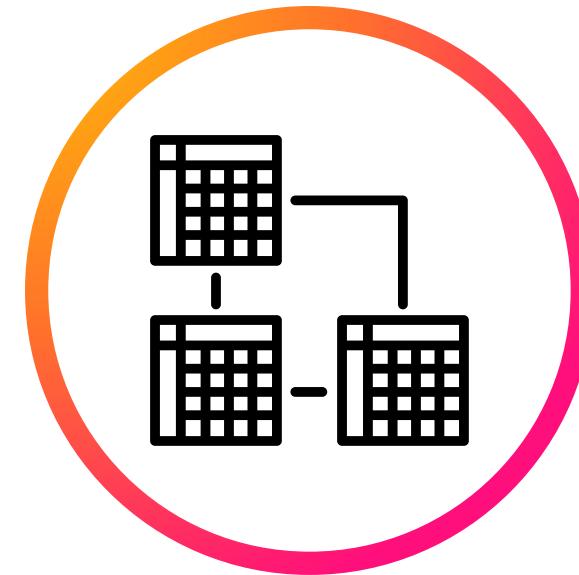
Metric Name

system.cpu.idle



Measure

Numeric data point such as count, gauge, timing, sample, etc.



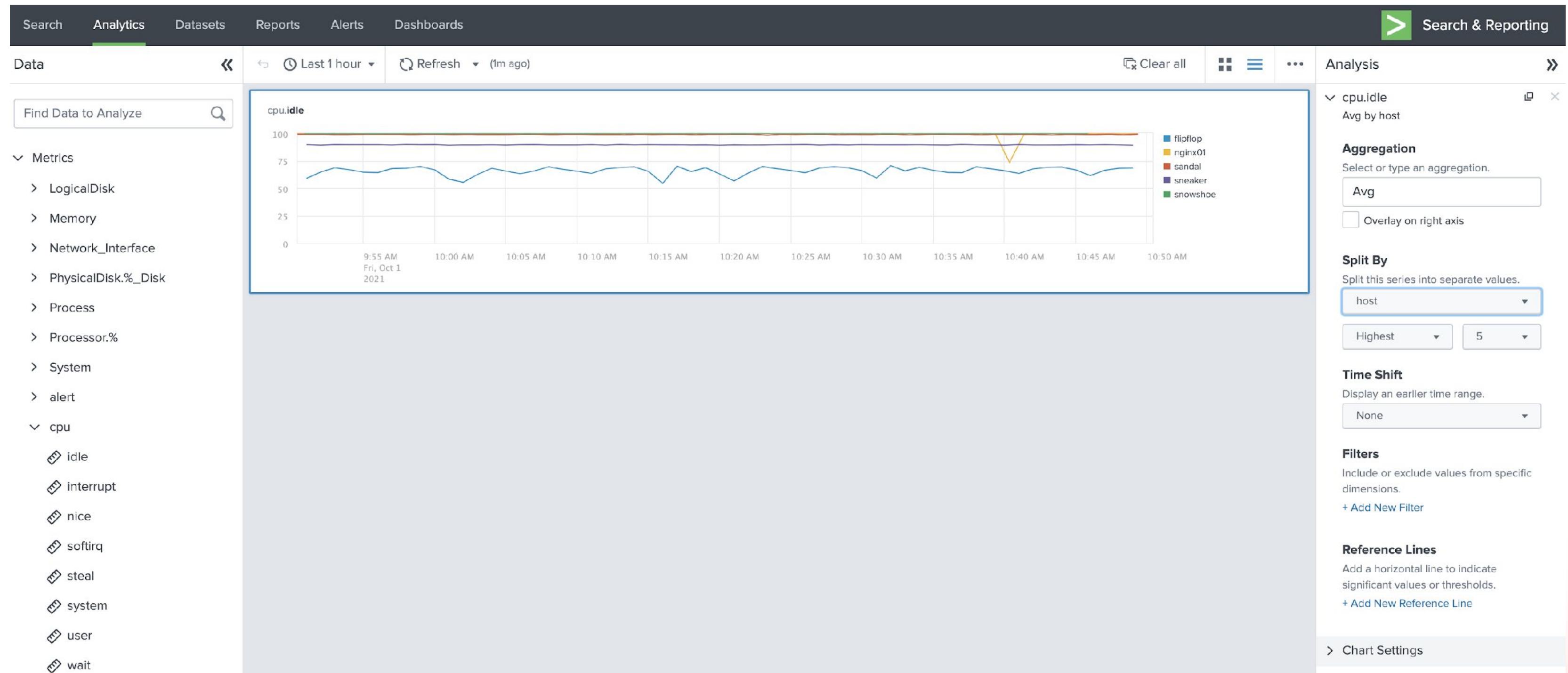
Dimensions

Host (IP address, DNS, hostname)
Region (us-east-1, us-west-1, eu-west-1, ap-southeast-1)
InstanceTypes (t2.medium, t2.large, m3.medium)

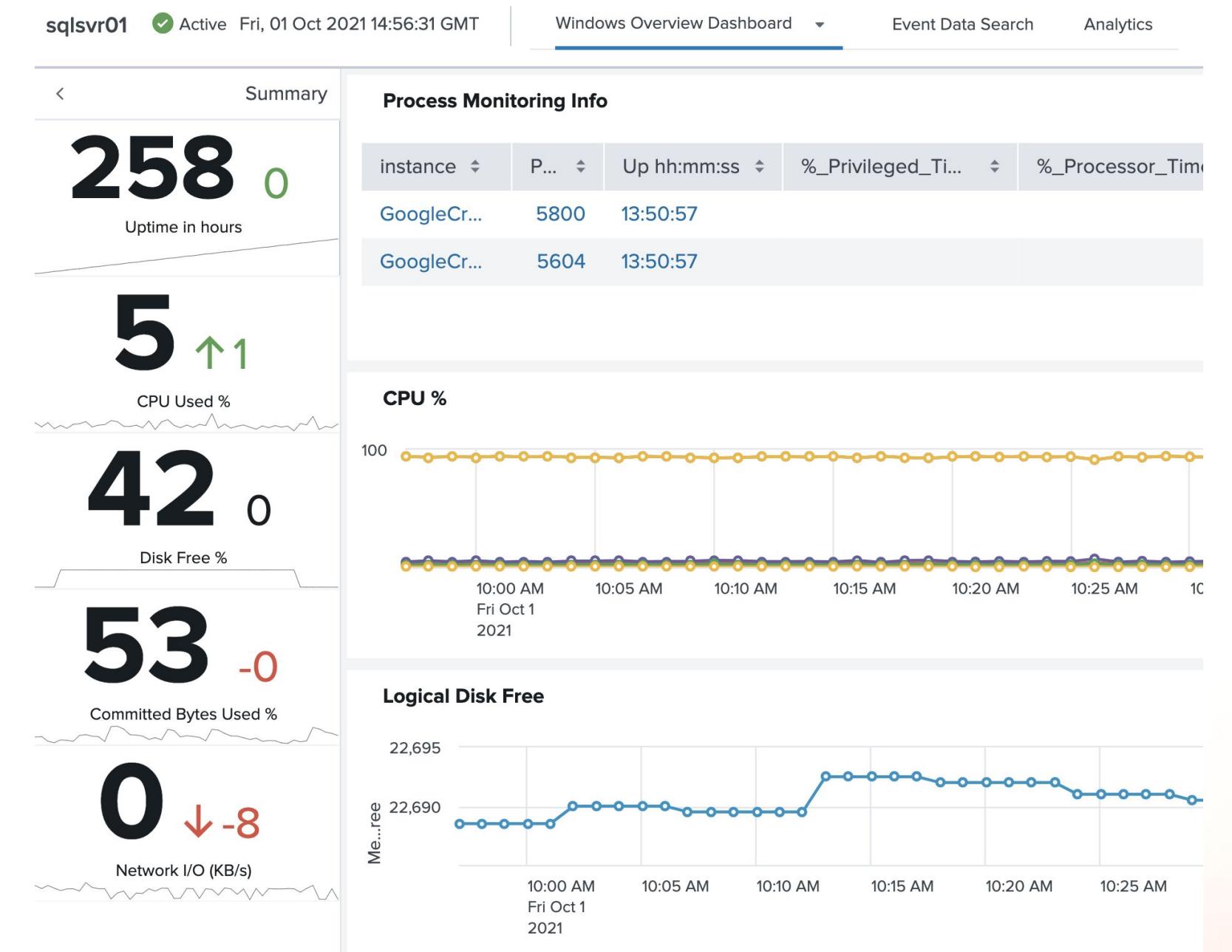
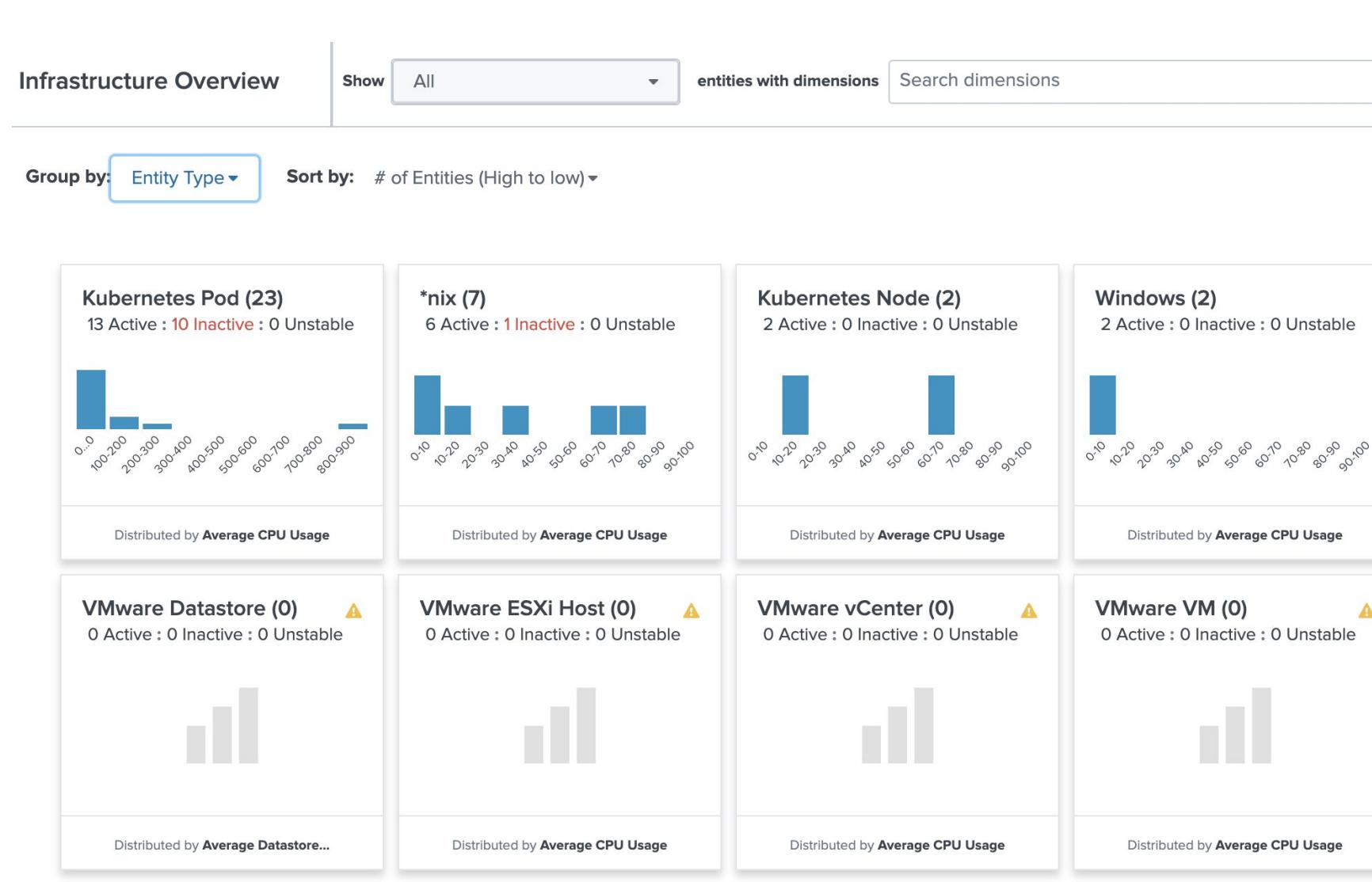
How Do I Use Metrics?



Metrics Analytics Workspace



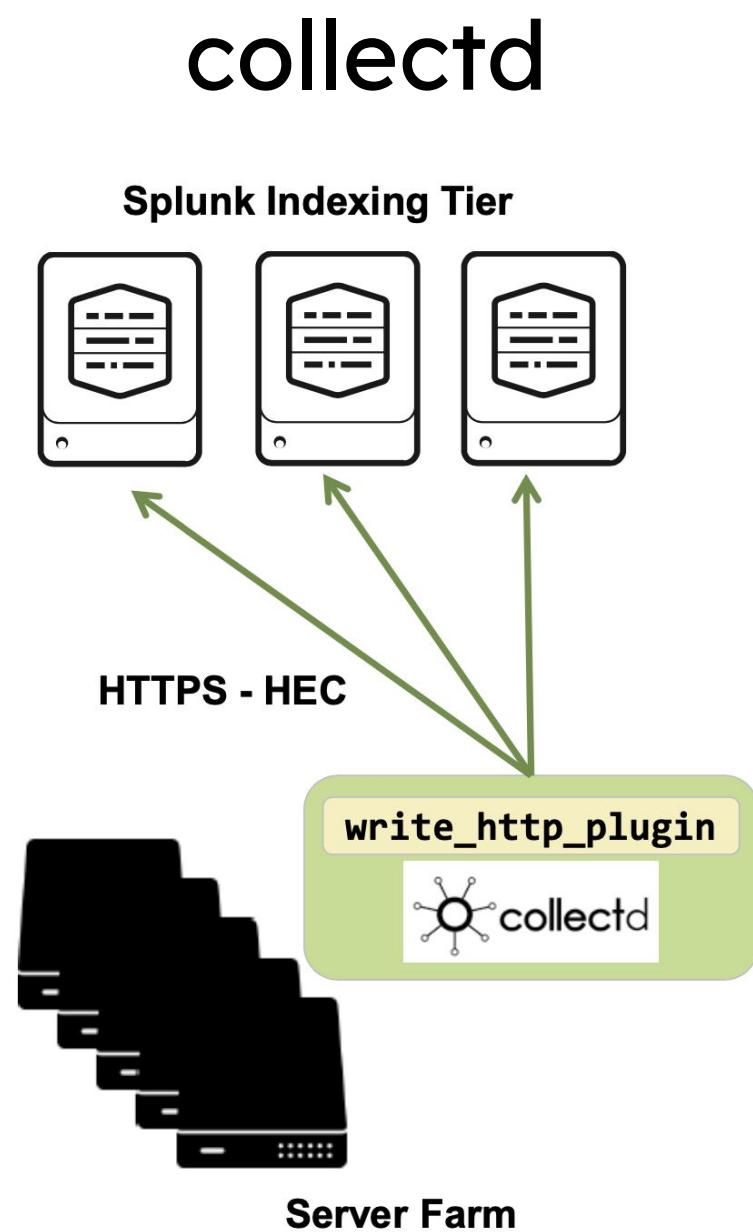
IT Essentials Work & IT Service Intelligence



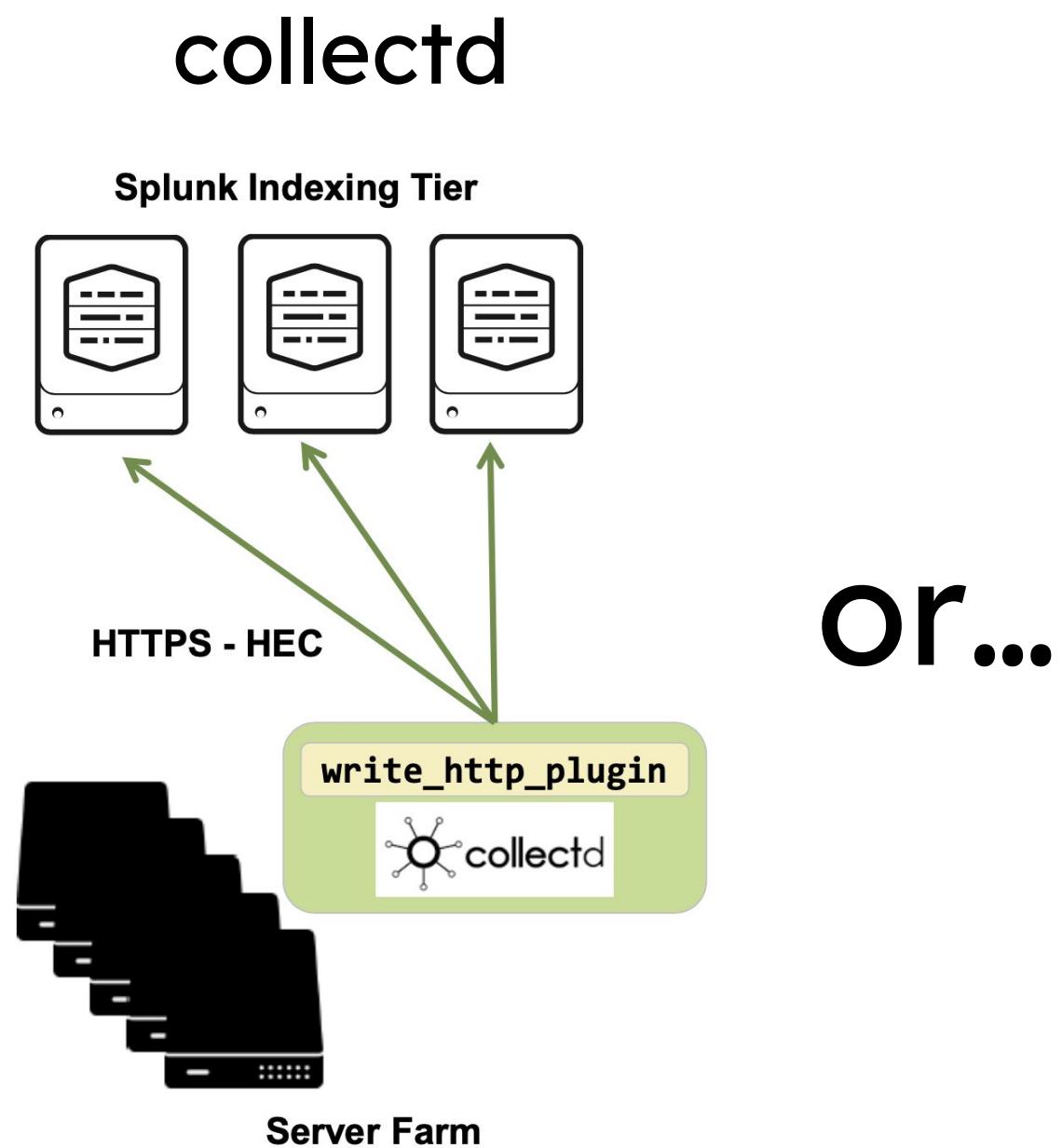
How Do I Get Metrics In?



Gathering Metrics for IT Monitoring

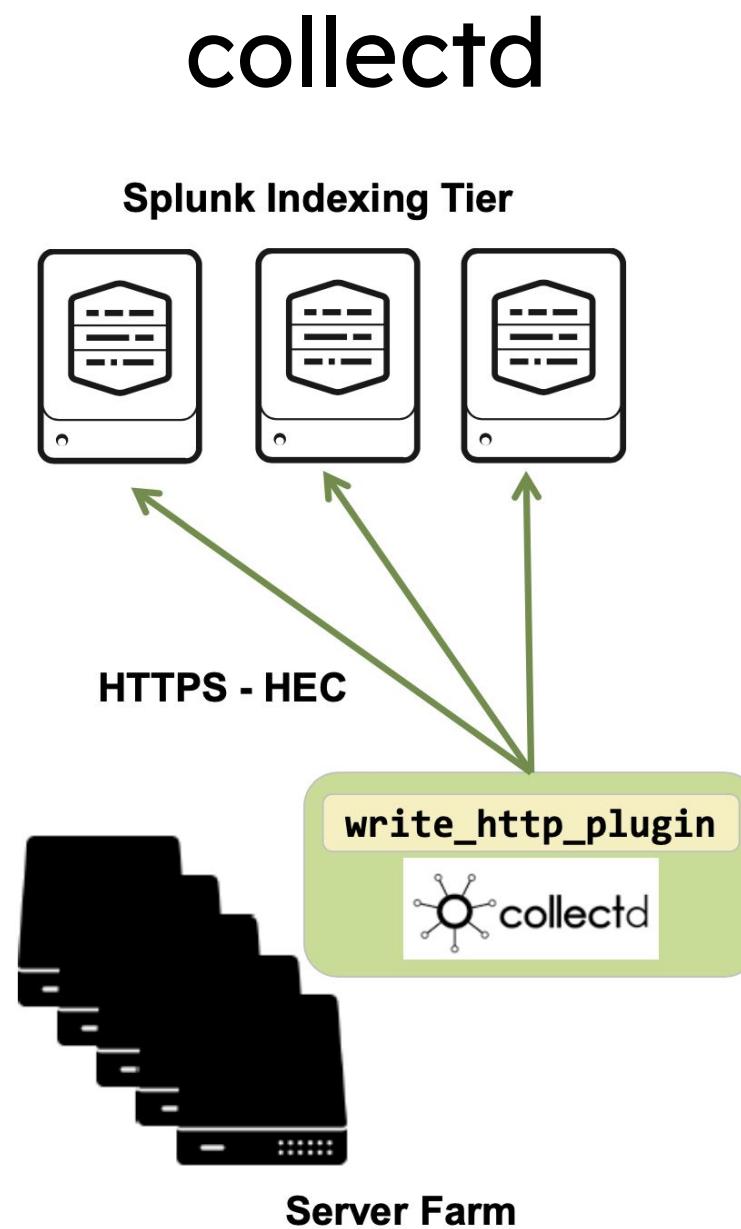


Gathering Metrics for IT Monitoring



or...

Gathering Metrics for IT Monitoring



Or...

Splunk Universal Forwarder

```
[perfmon://CPU]
disabled=false
counters=% C1 Time;% C2 Time;% Idle Time;% Processor Time;% User
Time;% Reserved Time;% Interrupt Time;% Privileged Time;
instances=*
interval=60
object=Processor
mode=single
sourcetype=PerfmonMetrics:CPU
index=itsi_im_metrics
_meta = entity_type::Windows_Host
```

```
[script://./bin/cpu_metric.sh]
sourcetype = cpu_metric
source = cpu
interval = 60
disabled = 0
index=itsi_im_metrics
```

Hands-on Lab

The image shows a laptop screen displaying the Splunk Enterprise Entity Overview interface. The interface includes a top navigation bar with links for Service Analyzer, Entity Overview, Alerts and Episodes, Glass Tables, Deep Dives, Dashboards, Configuration, and Search. Below the navigation bar, there are filters for Entity Overview, All Status, All Severities, Group By: Entity Type, Sort By: # of Entities (High to low), and a toggle switch for Hide entity types with no entities. Two cards are displayed: one for Unix/Linux Add-on (1) and one for Windows (1). Both cards show a count of active, inactive, and unstable entities, and a histogram of CPU utilization distribution. A note at the bottom of the interface states: "See the Entity Overview documentation for instructions to collect metrics for all available platforms. Learn more." A small Cisco logo is visible in the top right corner of the interface.

Activity #1

- current state



Activity #1 - Splunk Login

In your web browser, go to **https://<your Splunk server>**

Login as **admin**, password **splunk4mows**



Activity #1 - Current state

Navigate to Settings - Forwarder management

The screenshot shows the Splunk Enterprise dashboard. On the left, there's a sidebar titled "Apps" with a search bar and a list of available apps: Search & Reporting, IT Essentials Work, IT Essentials Learn, Config Explorer, Splunk Add-on for Unix and Linux, Splunk App for Lookup File Editing, Splunk Secure Gateway, and Upgrade Readiness App. Below this is a "Find more apps" link. The main content area displays a "Hello, Administrator" message and a "Bookmarks" section with tabs for "My bookmarks (0)", "Shared with my organization (0)", and "Splunk recommended (14)". At the top right, there's a navigation bar with links for "Administrator", "Settings", "Activity", "Help", and "Find". A large orange arrow points from the "Settings" link towards the right-hand sidebar. The sidebar contains several sections: "Add Data" (with a plus icon), "Monitoring Console" (with a monitoring icon), "KNOWLEDGE" (Searches, reports, and alerts, Data models, Event types, Tags, Fields, Lookups, User interface, Alert actions, Advanced search, All configurations), "DATA" (Data inputs, Forwarding and receiving, Indexes, Report acceleration summaries, Virtual indexes, Source types, Ingest actions), "DISTRIBUTED ENVIRONMENT" (Indexer clustering, Forwarder management, Federated search, Distributed search), and "USERS AND AUTHENTICATION" (Roles, Users, Tokens, Password management, Authentication methods). The "Forwarder management" link under the "DISTRIBUTED ENVIRONMENT" section is highlighted with another orange arrow.

Activity #1 - Forwarder Management

Verify that you have 2 systems phoning home to the deployment server.

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

Forwarder Management

Repository Location: \$SPLUNK_HOME/etc/deployment-apps

Documentation ↗

2 Clients
PHONED HOME IN THE LAST 24 HOURS

0 Clients
DEPLOYMENT ERRORS

0 Total downloads
IN THE LAST 1 HOUR

Apps (3) Server Classes (3) **Clients (2)**

Phone Home: All ▾ All Clients ▾ filter

2 Clients 10 Per Page ▾

i	Host Name	Client Name	Instance Name	IP Address	Actions	Machine Type	Deployed Apps	Phone Home
>	mows-win-uf	5A60BAF3-0836-4168-A8AB-03302972CB24	mows-win-uf	34.204.53.198	Delete Record	windows-x64	2 deployed	a few seconds ago
>	ip-172-31-47-180	92E269DF-C2E7-4037-AD84-E5C656787052	mows-nix-uf-i-07768708ce3574f3c	34.239.45.157	Delete Record	linux-x86_64	2 deployed	a few seconds ago

Activity #1 - What data is present?

1. Navigate to the Search & Reporting app
2. Search for `index=*` over the Last 60 minutes.

New Search

index=*

✓ 10,748 events (9/19/24 6:01:00.000 PM to 9/19/24 7:01:05.000 PM) No Event Sampling ▾

Events (10,748) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

1 minute per column

1 2 3 4 5 6 7 8 ... Next >

Time Event

> 9/19/24 2024-09-19 18:58:43.1114 INFO [ssm-agent-worker] [MessageService] [MGSInteractor] send failed reply thread done
host = ip-172-31-64-215 | source = /var/log/amazon/ssm/amazon-ssm-agent.log | sourcetype = amazon-ssm-agent

> 9/19/24 2024-09-19 18:58:43.1113 INFO [ssm-agent-worker] [MessageService] [MGSInteractor] send failed reply thread started
host = ip-172-31-64-215 | source = /var/log/amazon/ssm/amazon-ssm-agent.log | sourcetype = amazon-ssm-agent

> 9/19/24 2024-09-19 18:58:40.9414 INFO [ssm-agent-worker] [Association] Next association is scheduled at 2024-09-19 19:04:16.544 +0000 UTC, association will wait for 5m35.602588408s
host = ip-172-31-64-215 | source = /var/log/amazon/ssm/amazon-ssm-agent.log | sourcetype = amazon-ssm-agent

> 9/19/24 2024-09-19 18:58:08.0512 INFO [ssm-agent-worker] [HealthCheck] got SSM connection channel value: ssmsmessages
agent.log | sourcetype = amazon-ssm-agent

index

2 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
nix	10,563	98.279%
wineventlog	185	1.721%

Activity #1 - IT Essentials Work Install

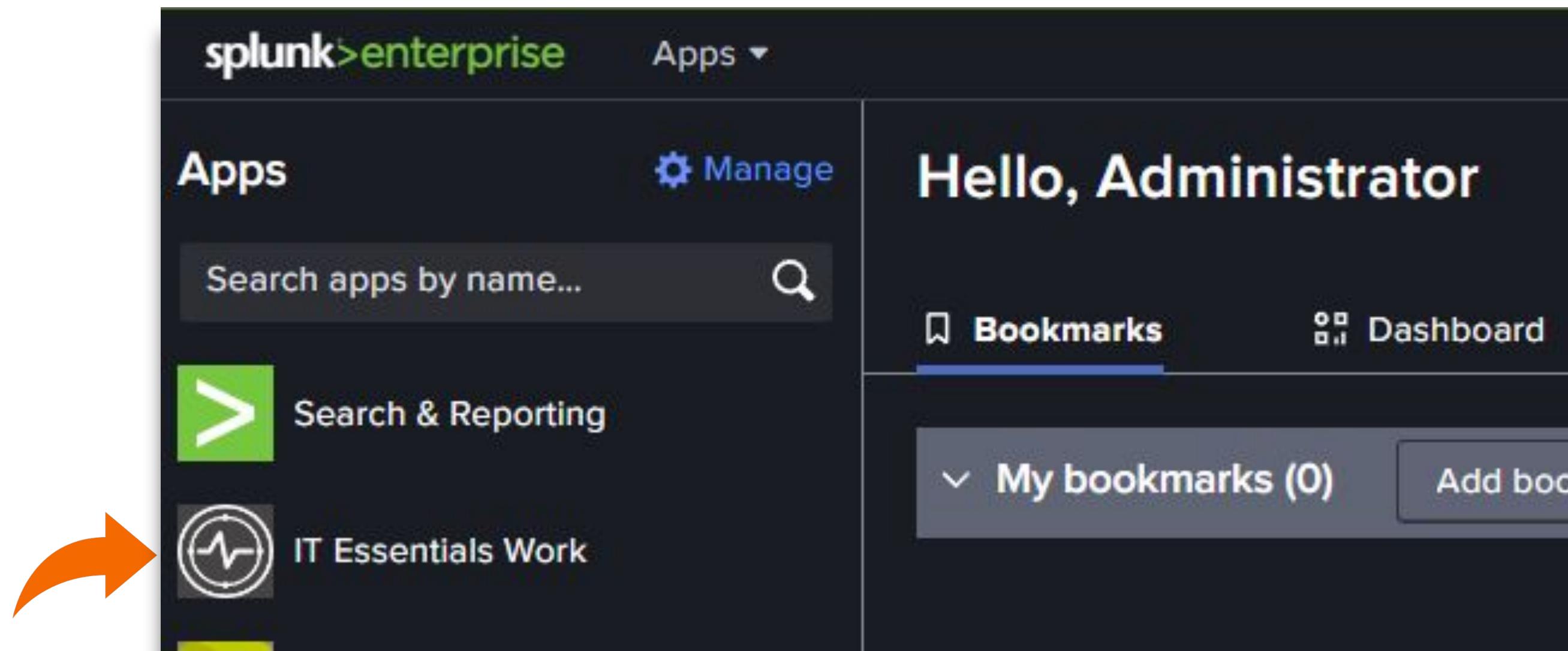
At this time, you can't install Splunk IT Essentials Work from the Splunk Web interface.

<https://docs.splunk.com/Documentation/ITEWork>
<https://splunkbase.splunk.com/app/5403>

1. Stop your Splunk platform
 - `cd /opt/splunk/bin`
 - `./splunk stop`
2. Extract the installation package into `$SPLUNK_HOME/etc/apps`
 - `tar -xvf it-essentials-work_<latest_version>.spl -C /opt/splunk/etc/apps`
3. Restart your Splunk platform
 - `./splunk start`

Activity #1 - IT Essentials Work

Navigate to the IT Essentials Work app



Activity #1 - Entity Overview

Verify that there are no entities found

The screenshot shows the Entity Overview page of the Splunk Enterprise interface. The top navigation bar includes links for Service Analyzer, Entity Overview (which is selected), Alerts and Episodes, Glass Tables, Deep Dives, Dashboards, Configuration, and Search. The right side of the top bar features icons for Administrator, Messages, Settings, Activity, Help, Find, and a search bar. A "IT Essentials Work" icon is also present.

The main content area displays a grid of nine entity types, each represented by a card:

- *nix (0) - Distributed by CPU Utilization
- Kubernetes Node (0) - Distributed by Average CPU Usage
- Kubernetes Pod (0) - Distributed by Average CPU Usage
- Unix/Linux Add-on (0) - Distributed by CPU Utilization
- VMware Cluster (0) - Distributed by Average CPU Usage
- VMware Datastore (0) - Distributed by Average Datastore...
- VMware ESXi Host (0) - Distributed by Average CPU Usage
- VMware vCenter (0) - Distributed by Average CPU Usage
- VMware VM (0) - Distributed by Average CPU Usage
- Windows (0) - Distributed by CPU Utilization

Each card shows a count of 0 for Active, Inactive, and Unstable entities. A yellow warning icon is present in the top right corner of each card. Below the cards, a note states: "See the Entity Overview documentation for instructions to collect metrics for all available platforms. Learn more." with a link icon.

See the Entity Overview documentation for instructions to collect metrics for all available platforms. [Learn more.](#)

Activity #1 - Splunk App for Content Packs

At this time, you can't install Splunk App for Content Packs from the Splunk Web interface.

<https://docs.splunk.com/Documentation/ContentPackApp/latest/Overview/Install>
<https://splunkbase.splunk.com/app/5391>

1. Stop your Splunk platform
 - `cd /opt/splunk/bin`
 - `./splunk stop`
2. Extract the installation package into `$SPLUNK_HOME/etc/apps`
 - `tar -xvf splunk-app-for-content-packs_<latest_version>.spl -C /opt/splunk/etc/apps`
3. Restart your Splunk platform
 - `./splunk start`

Splunk App for Content Packs

What it is

- Curated, prepackaged content for common data sources
- Service maps, dashboards, and correlation searches out-of-the-box

Why it matters

- Quickly set up Splunk ITSI & ITE Work to gain fast time to value

Data Integrations

Start getting value out of Splunk ITSI by integrating data sources to your deployment.
After getting data in, add content packs by installing a content pack.

Getting data in

Content Library

Authored Content

Import Content Pack

Featured Content Packs

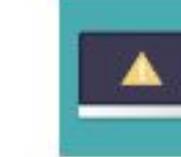
Content packs provide out-of-the-box services, KPIs, and other ITSI objects to help you quickly set up your ITSI environment. [Learn more](#)

All Content Packs ▾

Filter...

Refresh

Splunk Supported Content Packs (22)

 AWS Dashboards and Reports <small>All Saved Searches deactivated</small>	 Example Glass Tables	 ITE Work Alert Routing <small>All Saved Searches deactivated</small>	 ITSI Monitoring and Alerting <small>All Saved Searches activated</small>	 Microsoft 365
 Microsoft Exchange <small>All Saved Searches deactivated</small>	 Monitoring Citrix	 Monitoring Microsoft Windows	 Monitoring Pivotal Cloud Foundry	 Monitoring SOAR as a Service
 NetApp Data ONTAP Dashboards and Reports	 ServiceNow	 *nix	 splunk> SOAR	

Activity #1 - Config Explorer

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

- This app allows changing of files just like you are on the filesystem; it should be used very carefully in any environment that you care about.
- Do not use this app on Search Head clusters to change files because it won't sync changes to cluster
- This app does not automatically update the Splunk running config (except for properties like search-time extractions which Splunk does regularly re-read).
- There are no built-in restrictions on viewing secrets files or passwords. Don't make this app available to users who should not see that sort of thing.
- There are also no restrictions that prevent editing files in default/ folders. You should follow normal Splunk best practices and only edit the **/local/*.conf** files or files in **default/ if you are the developer of that app.**
- If you run Splunk as **root**, this app can allow you to run commands as root which is very dangerous
- **Please don't waste time trying to get this installed on Splunk Cloud**

Activity #2

- enable metrics collection



Activity #2 - Accessing the Splunk Indexer

For this workshop, I have 2 ways to modify the configuration files on the indexer

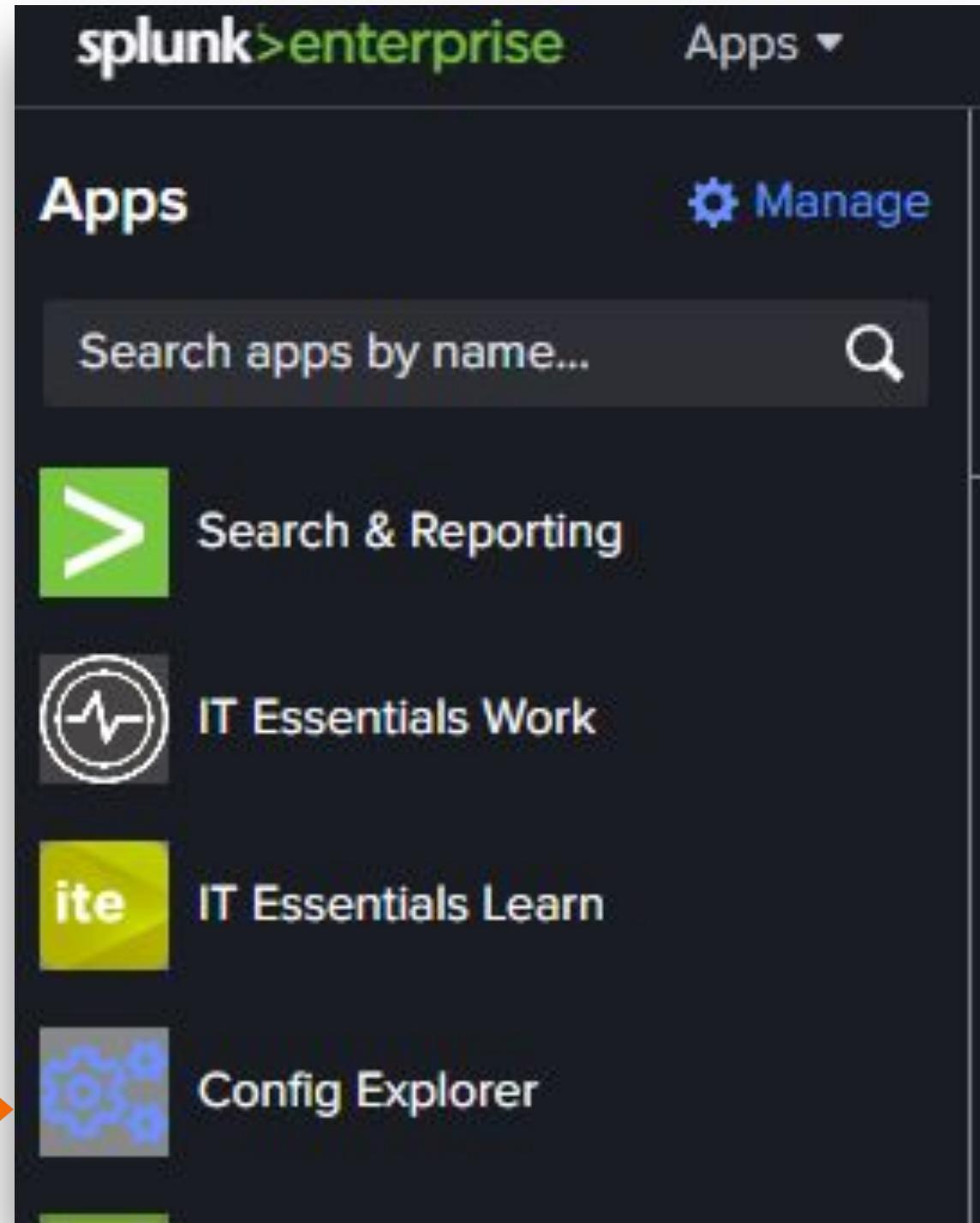
Option 1 - Use Config Explorer

Option 2 - SSH into the Splunk Indexer

Option 1 - Config Explorer

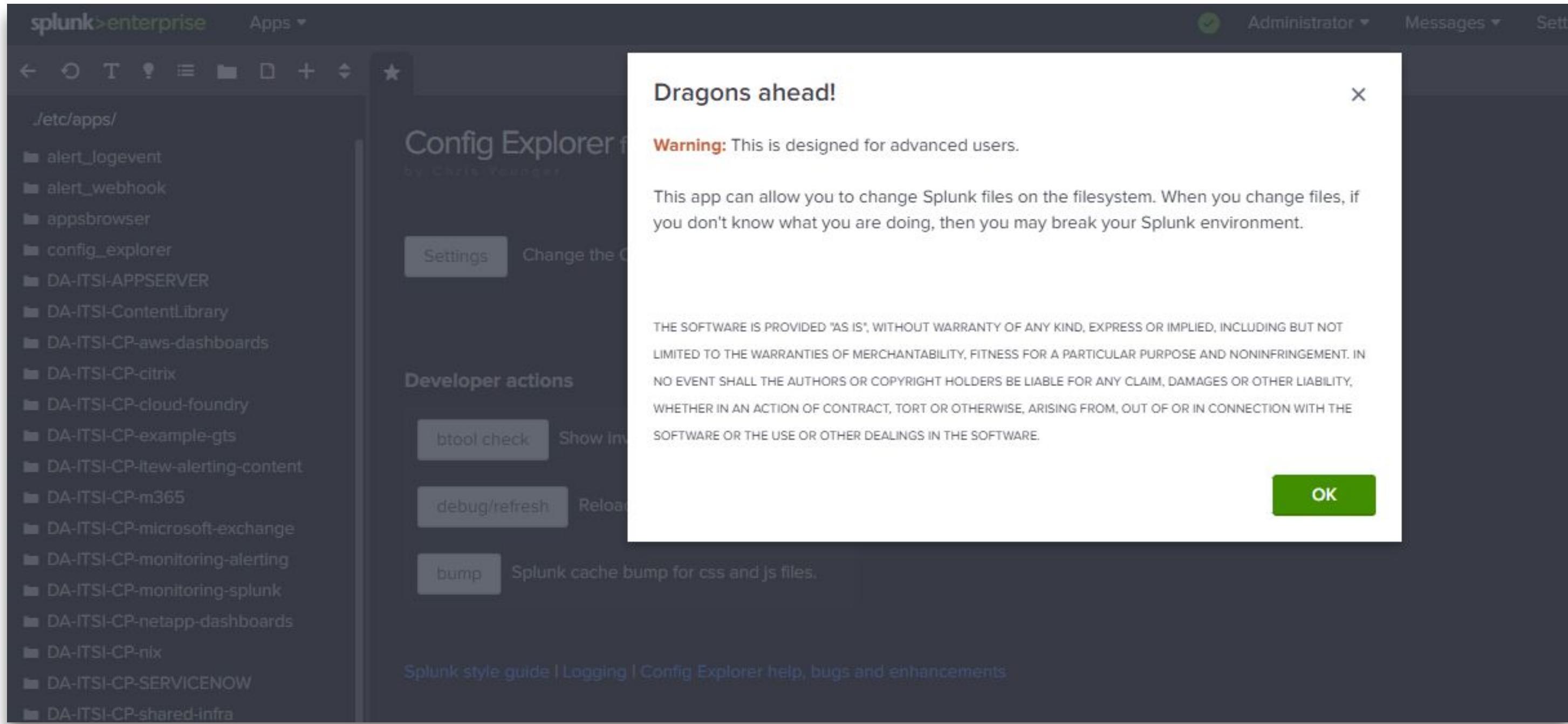
Activity #2 - Config Explorer

Navigate to Config
Explorer



Activity #2 - Config Explorer

Config Explorer warning message upon first opening

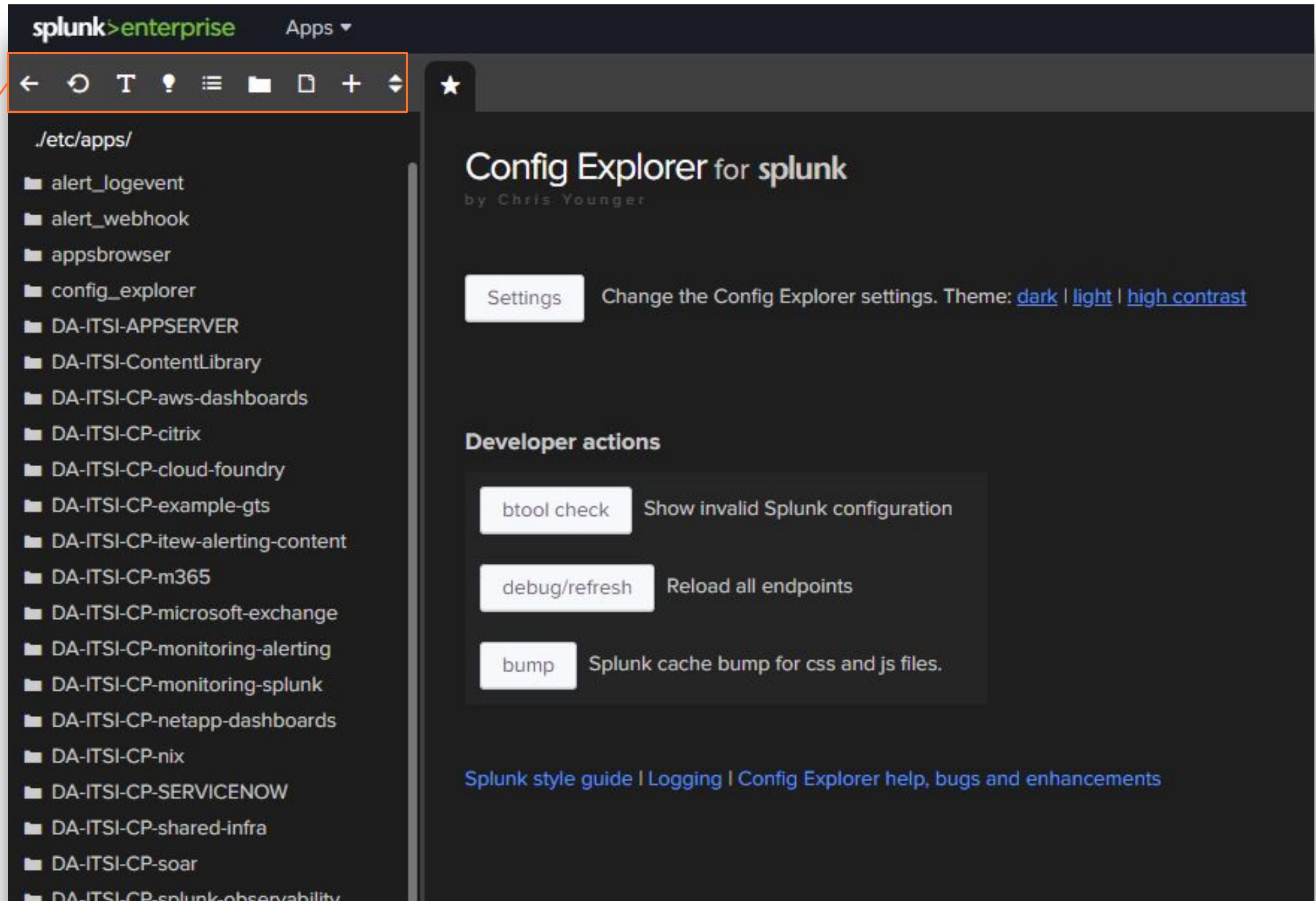


Activity #2 - Config Explorer

When first opening Config Explorer, you should be in the folder:

`./etc/apps`

Here we will use the top navigation menu of Config Explorer to move around.



Activity #2 - Config Explorer

1. Click the back arrow

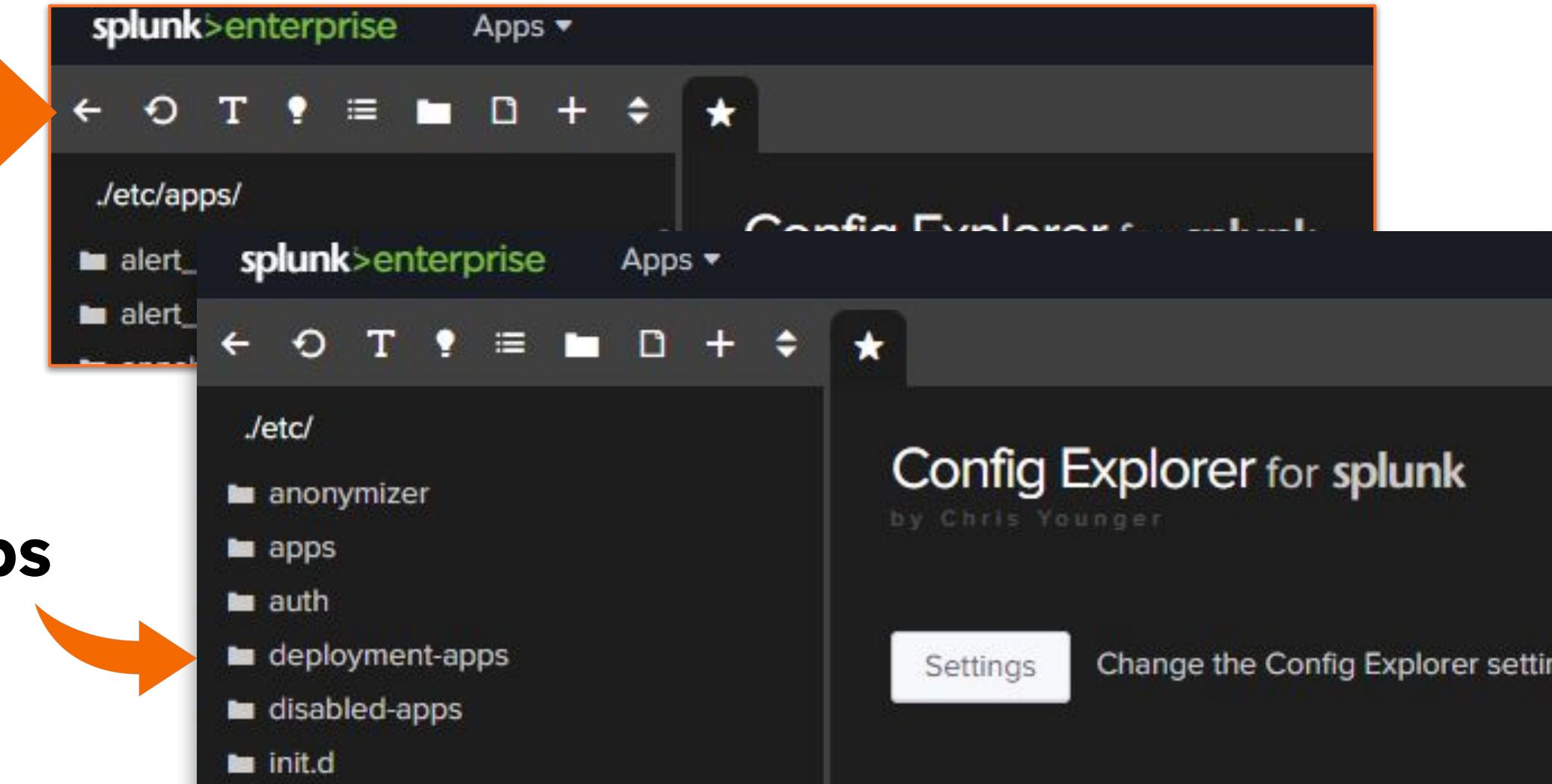
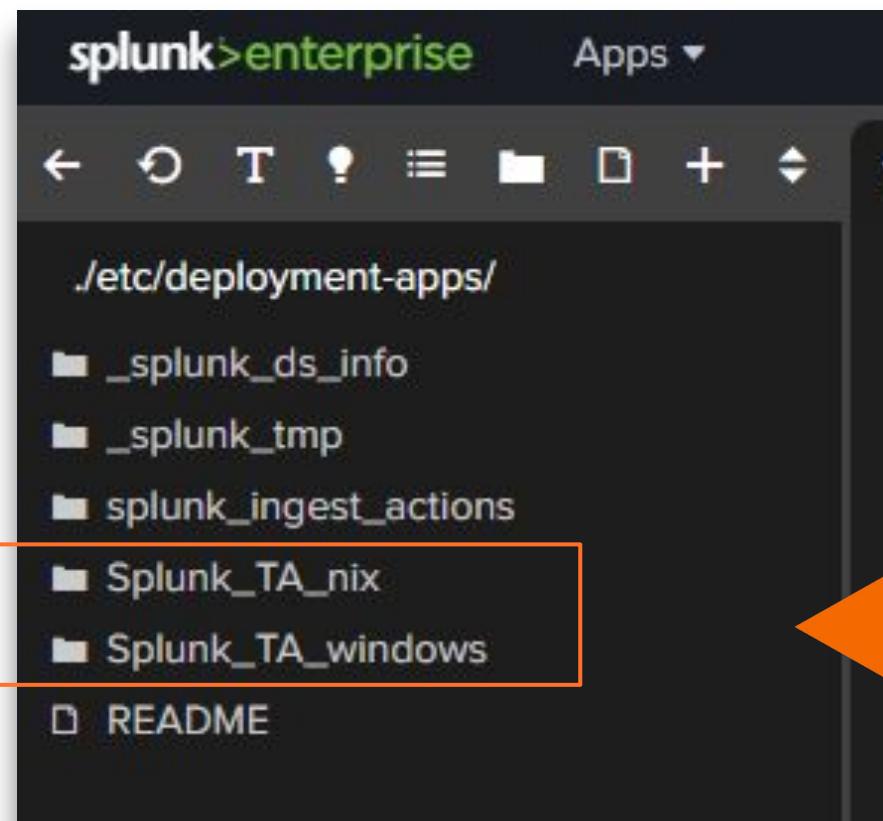


2. Click deployment-apps



3. You should now see the apps

Splunk_TA_nix
Splunk_TA_windows



Activity #2 - Config Explorer

```
...deployment-apps/Splunk_TA_nix/local/
app.conf
inputs.conf
props.conf

disabled = false
sourcetype = bash_history

### scripts
[script://bin/uptime.sh]
disabled = false
interval = 86400
source = Unix:Uptime
sourcetype = Unix:Uptime

[script://bin/version.sh]
disabled = false
interval = 86400
source = Unix:Version
sourcetype = Unix:Version

#####
##### Metric Inputs #####
[script://bin/vmstat_metric.sh]
sourcetype = vmstat_metric
source = vmstat
interval = 60
disabled = 0
index=itsi_im_metrics

[script://bin/iostat_metric.sh]
sourcetype = iostat_metric
source = iostat
interval = 60
disabled = 0
index=itsi_im_metrics

[script://bin/ps_metric.sh]
sourcetype = ps_metric
source = ps
interval = 60
disabled = 0
index=itsi_im_metrics
```

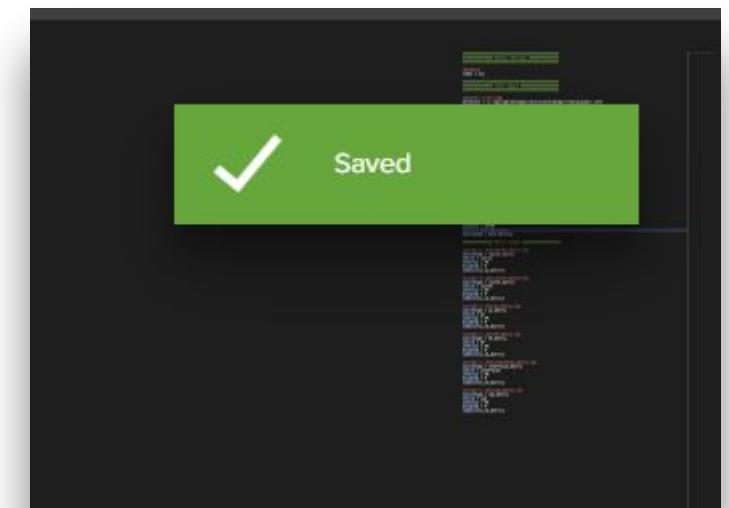
To save any changes made to a file.

Right click in the file.

In the pop-up menu select:

Save file

After saving the file, you will see a green pop-up in the upper right hand corner confirming the changes have been **Saved**.



Option 2 - SSH into the instance

Activity #2 - SSH into the instance

From Windows OS

Open a command prompt as administrator

Run the following command:

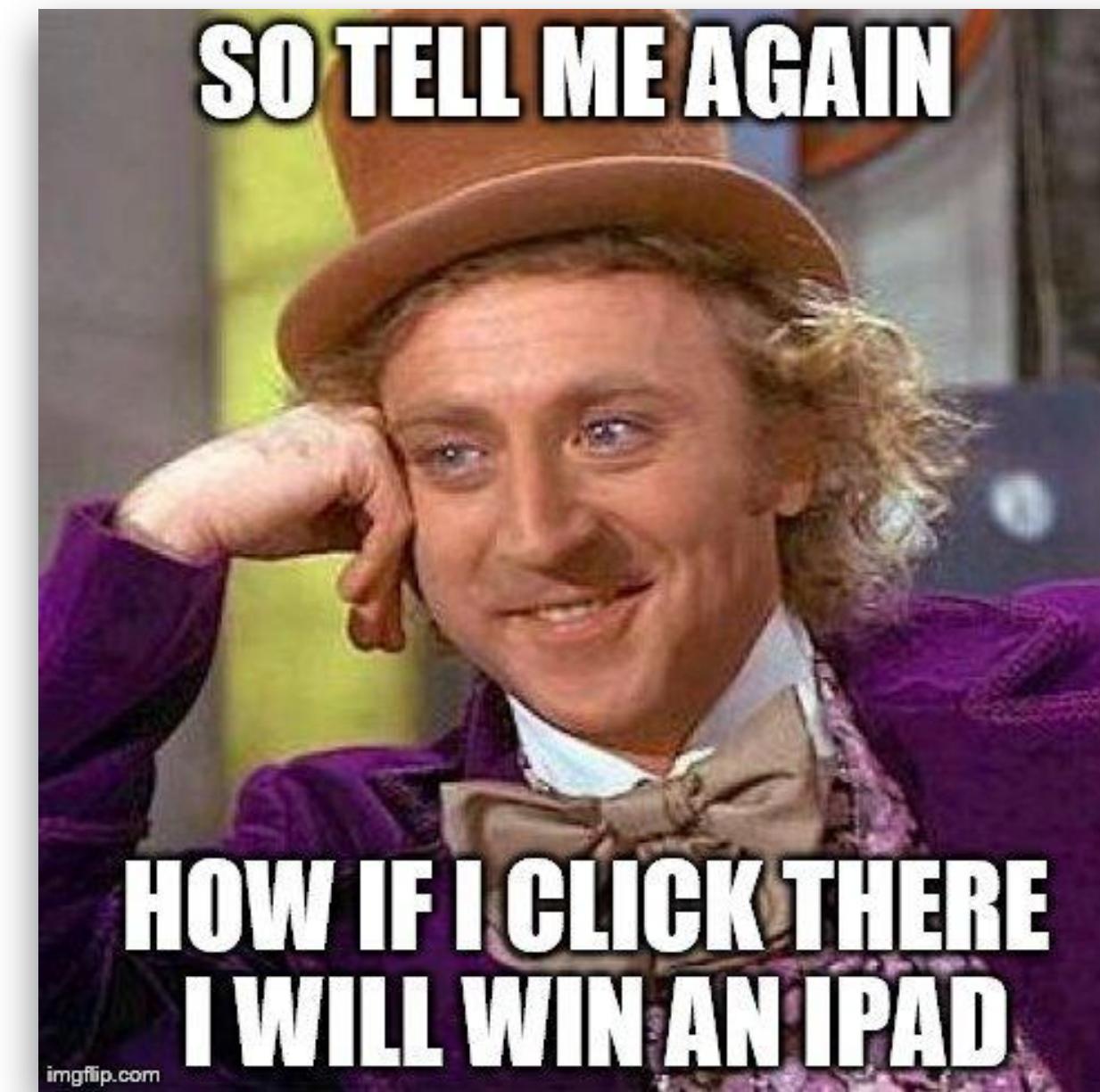
```
ssh -p 2222 splunk@<Your Splunk server>
```

Activity #2 - SSH into the instance

Become super-user:

`sudo -s`

(did I mention we're not following best practices here?)



Activity #2 - SSH into the instance

Navigate to the Splunk deployment apps directory:

/opt/splunk/etc/deployment-apps

Once in that directory execute a ls -ll

Here you'll see a directory for each of the installed TA's.

```
root@show-no-config-i-043bb9e8294d896e9:/opt/splunk/etc/deployment-apps
root@show-no-config-i-043bb9e8294d896e9:/opt/splunk/etc/deployment-apps# ls -ll
total 24
-r--r--r-- 1 10777 10777 307 Jul 19 21:51 README
drwxr-xr-x 11 root root 4096 Sep 11 19:16 Splunk_TA_nix
drwxr-xr-x 11 root root 4096 Sep 11 19:16 Splunk_TA_windows
drwx----- 2 root root 4096 Sep 11 14:42 _splunk_ds_info
drwx----- 2 root root 4096 Sep 11 14:42 _splunk_tmp
drwx----- 4 root root 4096 Sep 12 04:06 splunk_ ingest_actions
root@show-no-config-i-043bb9e8294d896e9:/opt/splunk/etc/deployment-apps#
```

Modify Splunk_TA_windows

Activity #2 - Splunk_TA_windows

Modify the Splunk_TA_windows for metrics collection

/opt/splunk/etc/deployment-apps/Splunk_TA_windows

In the Splunk_TA_windows you will find a **default** folder and a **local** folder

Each folder will contain an **inputs.conf**.

Never edit any **.conf** file in the default folder, however you can copy the stanzas from the **inputs.conf** located in the default folder to the **inputs.conf** file located in the **local** folder.

Pro Tip:

Before editing it's always a good idea to create backup copies of the “inputs.conf” file in case you make an error.

Activity #2 - Splunk_TA_windows

Modify the Splunk_TA_windows for metrics collection:

The next 8 slides will represent the stanzas you need to add to the "local" copy of the "inputs.conf". Ensure you add them exactly as shown in the slides for each stanza.

Here is a link to Splunk documentation with an example of inputs.conf for windows metrics:

https://docs.splunk.com/Documentation/ITEWork/latest/Entity/WindowsMetrics#Example_inputs.conf_file_for_a_universal_forwarder

[perfmon://CPU]

[perfmon://LogicalDisk]

[perfmon://PhysicalDisk]

[perfmon://Memory]

[perfmon://Network]

[perfmon://Process]

[perfmon://System]

Activity #2 - Splunk_TA_windows

Edit “inputs.conf” in the “local” folder of the Splunk_TA_windows:

```
[perfmon://CPU]
counters = % Processor Time; % User Time; % Privileged Time;
Interruptions/sec; % DPC Time; % Interrupt Time; DPCs Queued/sec;
DPC Rate; % Idle Time; % C1 Time; % C2 Time; % C3 Time; C1
Transitions/sec; C2 Transitions/sec; C3 Transitions/sec
disabled = 0
instances = *
interval = 60
mode = single
object = Processor
useEnglishOnly=true
sourcetype=PerfmonMetrics:CPU
index=itsi_im_metrics
```

Activity #2 - Splunk_TA_windows

Edit “inputs.conf” in the “local” folder of the Splunk_TA_windows:

```
[perfmon://LogicalDisk]
counters = % Free Space; Free Megabytes; Current Disk Queue Length; % Disk Time;
Avg. Disk Queue Length; % Disk Read Time; Avg. Disk Read Queue Length; % Disk Write
Time; Avg. Disk Write Queue Length; Avg. Disk sec/Transfer; Avg. Disk sec/Read; Avg.
Disk sec/Write; Disk Transfers/sec; Disk Reads/sec; Disk Writes/sec; Disk Bytes/sec;
Disk Read Bytes/sec; Disk Write Bytes/sec; Avg. Disk Bytes/Transfer; Avg. Disk
Bytes/Read; Avg. Disk Bytes/Write; % Idle Time; Split IO/Sec
disabled = 0
instances = *
interval = 60
mode = single
object = LogicalDisk
useEnglishOnly=true
sourcetype=PerfmonMetrics:LogicalDisk
index=itsi_im_metrics
```

Activity #2 - Splunk_TA_windows

Edit “inputs.conf” in the “local” folder of the Splunk_TA_windows:

```
[perfmon://PhysicalDisk]
counters = Current Disk Queue Length; % Disk Time; Avg. Disk Queue Length; % Disk
Read Time; Avg. Disk Read Queue Length; % Disk Write Time; Avg. Disk Write Queue
Length; Avg. Disk sec/Transfer; Avg. Disk sec/Read; Avg. Disk sec/Write; Disk
Transfers/sec; Disk Reads/sec; Disk Writes/sec; Disk Bytes/sec; Disk Read Bytes/sec;
Disk Write Bytes/sec; Avg. Disk Bytes/Transfer; Avg. Disk Bytes/Read; Avg. Disk
Bytes/Write; % Idle Time; Split IO/Sec
disabled = 0
instances = *
interval = 60
mode = single
object = PhysicalDisk
useEnglishOnly=true
sourcetype=PerfmonMetrics:PhysicalDisk
index=itsi_im_metrics
```

Activity #2 - Splunk_TA_windows

Edit “inputs.conf” in the “local” folder of the Splunk_TA_windows:

```
[perfmon://Memory]
counters = Page Faults/sec; Available Bytes; Committed Bytes; Commit Limit; Write Copies/sec;
Transition Faults/sec; Cache Faults/sec; Demand Zero Faults/sec; Pages/sec; Pages Input/sec;
Page Reads/sec; Pages Output/sec; Pool Paged Bytes; Pool Nonpaged Bytes; Page Writes/sec; Pool
Paged Allocs; Pool Nonpaged Allocs; Free System Page Table Entries; Cache Bytes; Cache Bytes
Peak; Pool Paged Resident Bytes; System Code Total Bytes; System Code Resident Bytes; System
Driver Total Bytes; System Driver Resident Bytes; System Cache Resident Bytes; % Committed
Bytes In Use; Available KBytes; Available MBytes; Transition Pages RePurposed/sec; Free & Zero
Page List Bytes; Modified Page List Bytes; Standby Cache Reserve Bytes; Standby Cache Normal
Priority Bytes; Standby Cache Core Bytes; Long-Term Average Standby Cache Lifetime (s)
disabled = 0
interval = 60
mode = single
object = Memory
useEnglishOnly=true
sourcetype=PerfmonMetrics:Memory
index=itsi_im_metrics
```

Activity #2 - Splunk_TA_windows

Edit “inputs.conf” in the “local” folder of the Splunk_TA_windows:

```
[perfmon://Network]
counters = Bytes Total/sec; Packets/sec; Packets Received/sec; Packets Sent/sec;
Current Bandwidth; Bytes Received/sec; Packets Received Unicast/sec; Packets Received
Non-Unicast/sec; Packets Received Discarded; Packets Received Errors; Packets Received
Unknown; Bytes Sent/sec; Packets Sent Unicast/sec; Packets Sent Non-Unicast/sec;
Packets Outbound Discarded; Packets Outbound Errors; Output Queue Length; Offloaded
Connections; TCP Active RSC Connections; TCP RSC Coalesced Packets/sec; TCP RSC
Exceptions/sec; TCP RSC Average Packet Size
disabled = 0
instances = *
interval = 60
mode = single
object = Network Interface
useEnglishOnly=true
sourcetype=PerfmonMetrics:Network
index=itsi_im_metrics
```

Activity #2 - Splunk_TA_windows

Edit “inputs.conf” in the “local” folder of the Splunk_TA_windows:

```
[perfmon://Process]
counters = % Processor Time; % User Time; % Privileged Time; Virtual Bytes Peak;
Virtual Bytes; Page Faults/sec; Working Set Peak; Working Set; Page File Bytes Peak;
Page File Bytes; Private Bytes; Thread Count; Priority Base; Elapsed Time; ID Process;
Creating Process ID; Pool Paged Bytes; Pool Nonpaged Bytes; Handle Count; IO Read
Operations/sec; IO Write Operations/sec; IO Data Operations/sec; IO Other
Operations/sec; IO Read Bytes/sec; IO Write Bytes/sec; IO Data Bytes/sec; IO Other
Bytes/sec; Working Set - Private
disabled = 0
instances = *
interval = 60
mode = single
object = Process
useEnglishOnly=true
sourcetype=PerfmonMetrics:Process
index=itsi_im_metrics
```

Activity #2 - Splunk_TA_windows

Edit “inputs.conf” in the “local” folder of the Splunk_TA_windows:

```
[perfmon://System]
counters = File Read Operations/sec; File Write Operations/sec; File Control
Operations/sec; File Read Bytes/sec; File Write Bytes/sec; File Control Bytes/sec;
Context
Switches/sec; System Calls/sec; File Data Operations/sec; System Up Time; Processor
Queue Length; Processes; Threads; Alignment Fixups/sec; Exception Dispatches/sec; Fl
oating Emulations/sec; % Registry Quota In Use
disabled = 0
instances = *
interval = 60
mode = single
object = System
useEnglishOnly=true
sourcetype=PerfmonMetrics:System
index=itsi_im_metrics
```

Activity #2 - Splunk_TA_windows

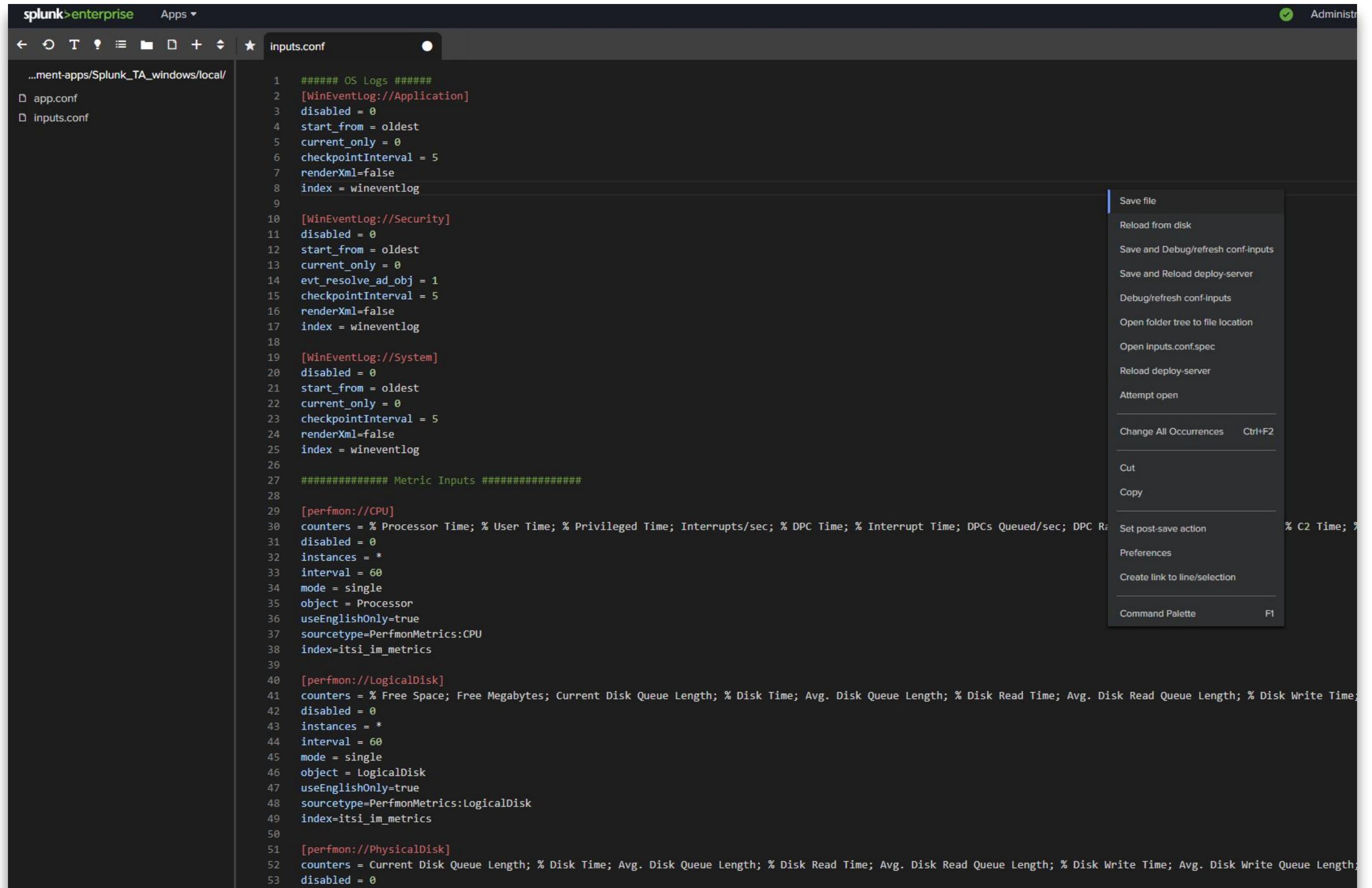
Your
Splunk_TA_windows
inputs.conf file should
look similar to this.

To save any changes
made to a file.

Right click in the file.

In the pop-up menu
select:

Save file



```
...ment-apps/Splunk_TA_windows/local/
  □ app.conf
  □ inputs.conf

1 ##### OS Logs #####
2 [WinEventLog://Application]
3 disabled = 0
4 start_from = oldest
5 current_only = 0
6 checkpointInterval = 5
7 renderXml=false
8 index = wineventlog
9
10 [WinEventLog://Security]
11 disabled = 0
12 start_from = oldest
13 current_only = 0
14 evt_resolve_ad_obj = 1
15 checkpointInterval = 5
16 renderXml=false
17 index = wineventlog
18
19 [WinEventLog://System]
20 disabled = 0
21 start_from = oldest
22 current_only = 0
23 checkpointInterval = 5
24 renderXml=false
25 index = wineventlog
26
27 ##### Metric Inputs #####
28
29 [perfmon://CPU]
30 counters = % Processor Time; % User Time; % Privileged Time; Interrupts/sec; % DPC Time; % Interrupt Time; DPCs Queued/sec; DPC Rate
31 disabled = 0
32 instances = *
33 interval = 60
34 mode = single
35 object = Processor
36 useEnglishOnly=true
37 sourcetype=PerfmonMetrics:CPU
38 index=itsi_im_metrics
39
40 [perfmon://LogicalDisk]
41 counters = % Free Space; Free Megabytes; Current Disk Queue Length; % Disk Time; Avg. Disk Queue Length; % Disk Read Time; Avg. Disk Read Queue Length; % Disk Write Time;
42 disabled = 0
43 instances = *
44 interval = 60
45 mode = single
46 object = LogicalDisk
47 useEnglishOnly=true
48 sourcetype=PerfmonMetrics:LogicalDisk
49 index=itsi_im_metrics
50
51 [perfmon://PhysicalDisk]
52 counters = Current Disk Queue Length; % Disk Time; Avg. Disk Queue Length; % Disk Read Time; Avg. Disk Read Queue Length; % Disk Write Time; Avg. Disk Write Queue Length;
53 disabled = 0
```

The screenshot shows the Splunk Enterprise interface with the 'Inputs' tab selected. A file named 'inputs.conf' is open in the main editor area. The code in the file is a configuration snippet for Splunk_TA_windows, defining inputs from WinEventLog and Perfmon metrics. A context menu is open over the file, with the 'Save file' option highlighted. Other options in the menu include Reload from disk, Save and Debug/refresh conf-inputs, Save and Reload deploy-server, Debug/refresh conf-inputs, Open folder tree to file location, Open inputs.conf.spec, Reload deploy-server, Attempt open, Change All Occurrences (Ctrl+F2), Cut, Copy, Set post-save action, Preferences, Create link to line/selection, Command Palette, and F1.

Activity #2 - Splunk_TA_windows

Now save the changes you have made to the inputs.conf
for the Splunk_TA_windows

Modify Splunk_TA_nix

Activity #2 - Splunk_TA_nix

Next is modify the Splunk_TA_nix for metrics collection

/opt/splunk/etc/deployment-apps/Splunk_TA_nix/local

In the **Splunk_TA_nix** you will find a **default** folder and a **local** folder

Each folder will contain an **inputs.conf**.

Never edit any **.conf** file in the default folder, however you can copy the stanzas from the **inputs.conf** located in the default folder to the **inputs.conf** file located in the **local** folder.

Pro Tip:

Before editing it's always a good idea to create backup copies of the “**inputs.conf**” file in case you make an error.

Activity #2 - Splunk_TA_nix

Modify the Splunk_TA_nix for metrics collection:

The next 6 slides will represent the stanzas you need to add to the **local** copy of the **inputs.conf**. Ensure you add them exactly as shown in the slides for each stanza.

[script://./bin/vmstat_metric.sh]

[script://./bin/iostat_metric.sh]

[script://./bin/ps_metric.sh]

[script://./bin/df_metric.sh]

[script://./bin/interfaces_metric.sh]

[script://./bin/cpu_metric.sh]

Activity #2 - Splunk_TA_nix

Edit **inputs.conf** in the **local** folder of the **Splunk_TA_nix**:

```
[script://./bin/vmstat_metric.  
sh]  
sourcetype = vmstat_metric  
source = vmstat  
interval = 60  
disabled = 0  
index=itsi_im_metrics
```

Activity #2 - Splunk_TA_nix

Edit **inputs.conf** in the **local** folder of the **Splunk_TA_nix**:

```
[script://./bin/iostat_metric.s  
h]  
sourcetype = iostat_metric  
source = iostat  
interval = 60  
disabled = 0  
index=itsi_im_metrics
```

Activity #2 - Splunk_TA_nix

Edit **inputs.conf** in the **local** folder of the **Splunk_TA_nix**:

```
[script://./bin/ps_metric.sh]
sourcetype = ps_metric
source = ps
interval = 60
disabled = 0
index=itsi_im_metrics
```

Activity #2 - Splunk_TA_nix

Edit **inputs.conf** in the **local** folder of the **Splunk_TA_nix**:

```
[script://./bin/df_metric.sh]
sourcetype = df_metric
source = df
interval = 60
disabled = 0
index=itsi_im_metrics
```

Activity #2 - Splunk_TA_nix

Edit **inputs.conf** in the **local** folder of the **Splunk_TA_nix**:

```
[script://./bin/interfaces_metric.s  
h]  
sourcetype = interfaces_metric  
source = interfaces  
interval = 60  
disabled = 0  
index=itsi_im_metrics
```

Activity #2 - Splunk_TA_nix

Edit **inputs.conf** in the **local** folder of the **Splunk_TA_nix**:

```
[script://./bin/cpu_metric.sh]
sourcetype = cpu_metric
source = cpu
interval = 60
disabled = 0
index=itsi_im_metrics
```

Activity #2 - Splunk_TA_nix

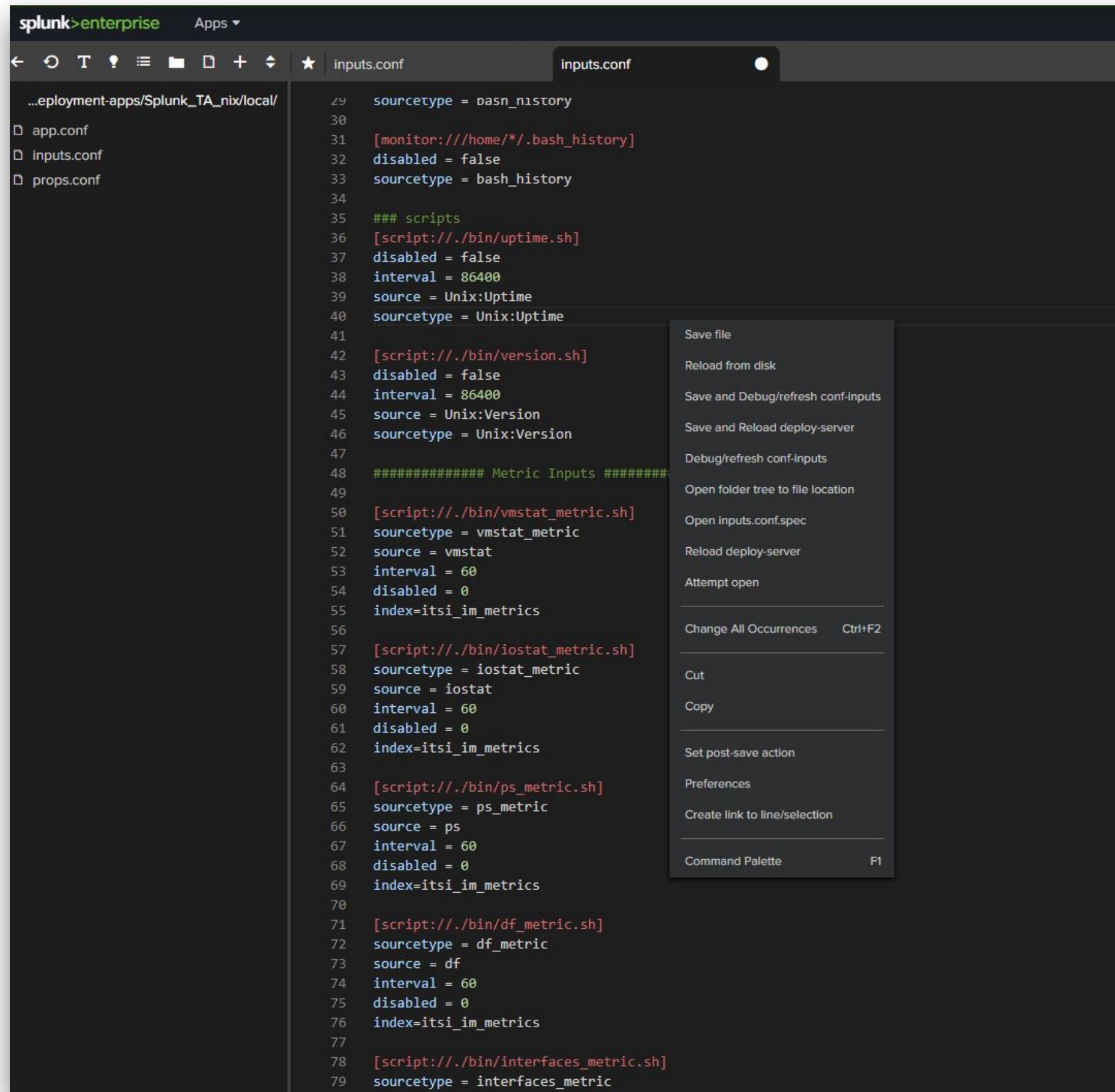
Your Splunk_TA_nix inputs.conf file should look similar to this.

To save any changes made to a file.

Right click in the file.

In the pop-up menu select:

Save file



```
..deployment-apps/Splunk_TA_nix/local/
  □ app.conf
  □ inputs.conf
  □ props.conf

29 sourcetype = bash_history
30 [monitor:///home/*.bash_history]
31 disabled = false
32 sourcetype = bash_history
33
34 ### scripts
35 [script://bin/uptime.sh]
36 disabled = false
37 interval = 86400
38 source = Unix:Uptime
39 sourcetype = Unix:Uptime
40
41 [script://bin/version.sh]
42 disabled = false
43 interval = 86400
44 source = Unix:Version
45 sourcetype = Unix:Version
46
47 ##### Metric Inputs #####
48 [script://bin/vmstat_metric.sh]
49 sourcetype = vmstat_metric
50 source = vmstat
51 interval = 60
52 disabled = 0
53 index=itsi_im_metrics
54
55 [script://bin/iostat_metric.sh]
56 sourcetype = iostat_metric
57 source = iostat
58 interval = 60
59 disabled = 0
60 index=itsi_im_metrics
61
62 [script://bin/ps_metric.sh]
63 sourcetype = ps_metric
64 source = ps
65 interval = 60
66 disabled = 0
67 index=itsi_im_metrics
68
69 [script://bin/df_metric.sh]
70 sourcetype = df_metric
71 source = df
72 interval = 60
73 disabled = 0
74 index=itsi_im_metrics
75
76 [script://bin/interfaces_metric.sh]
77 sourcetype = interfaces_metric
```

Activity #2 - Splunk_TA_nix

Now save the changes you have made to the **inputs.conf** for the
Splunk_TA_nix

Activity #3

- deploy the changes



Activity #3 - deploy the changes

After you edit the content of an app, you must reload the deployment server so that the deployment server learns of the changed app. It then redeploys the app to the mapped set of clients.

Lets cover different ways to reload the Deployment Server.

Activity #3 - deploy the changes

If you do not have access to the command line on the Deployment Server, the below string will reload the deployment server:

Enter the following into your browser, replacing <your Splunk server> :

https://<your Splunk server>:8089/services/deployment/server/serverclasses/_reload

OR

<https://<your Splunk server>:8089/services/deployment/serverclasses/nix/reload>

<https://<your Splunk server>:8089/services/deployment/serverclasses/win/reload>

Activity #3 - deploy the changes

Should have a pop-up asking you to log in

Login as **admin**, password **splunk4mows**

After logging in you should see this screen and Deployment Server should have been reloaded

The screenshot shows a web browser window with a dark header bar. The header bar contains the text "Splunk Atom Feed: serverclasses". Below the header, there is a light-colored content area. At the top of this area, the text "Updated: 2024-09-25T15:32:17+00:00 Splunk build: 9.3.0" is displayed. Below this, the text "Feed links: [create](#) - [reload](#) - [rename](#) -" is shown. The rest of the content area is empty, indicating no feed items are currently listed.

Activity #3 - deploy the changes

Here are the steps to reload the deployment server on a *nix OS when you have access to the command line:

First move to the Splunk bin folder:

```
cd /opt/splunk/bin
```

Reload all apps:

```
./splunk reload deploy-server
```

Reload just one app here are 2 examples:

```
./splunk reload deploy-server -class all-windows
```

```
./splunk reload deploy-server -class all-linux
```

Activity #3 - deploy the changes

Here is example output from CLI reloading the deployment server

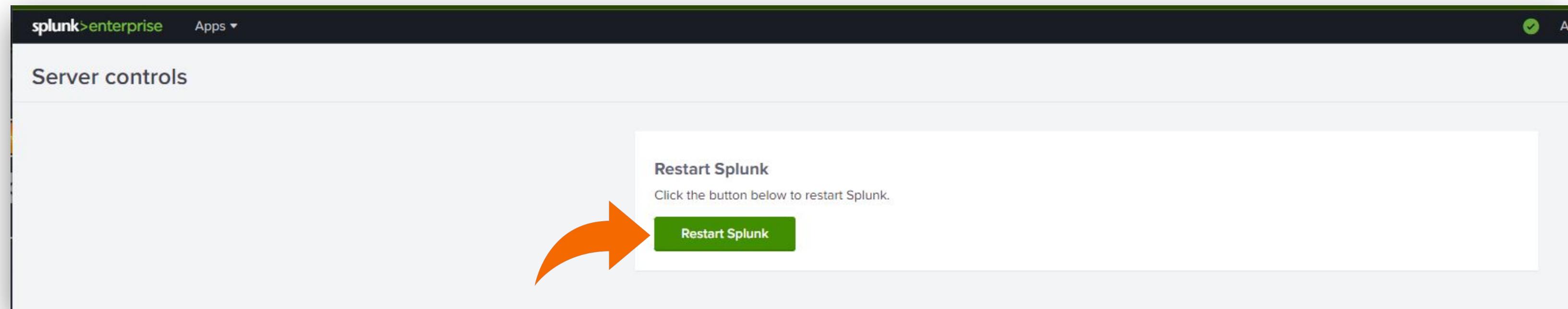
```
root@ip-172-31-13-174:/opt/splunk/etc/deployment-apps/Splunk_TA_nix/local# cd ../../..
root@ip-172-31-13-174:/opt/splunk/etc# cd ..
root@ip-172-31-13-174:/opt/splunk# cd bin
root@ip-172-31-13-174:/opt/splunk/bin# ./splunk reload deploy-server -class all-windows
Splunk username: admin
Password:
Reloading serverclass(es).
root@ip-172-31-13-174:/opt/splunk/bin# ./splunk reload deploy-server -class all-linux
Reloading serverclass(es).
root@ip-172-31-13-174:/opt/splunk/bin# 
```

Activity #3 - deploy the changes

If all else fails during this workshop, just restart Splunk from the GUI.

Navigate to **Settings - Server controls**

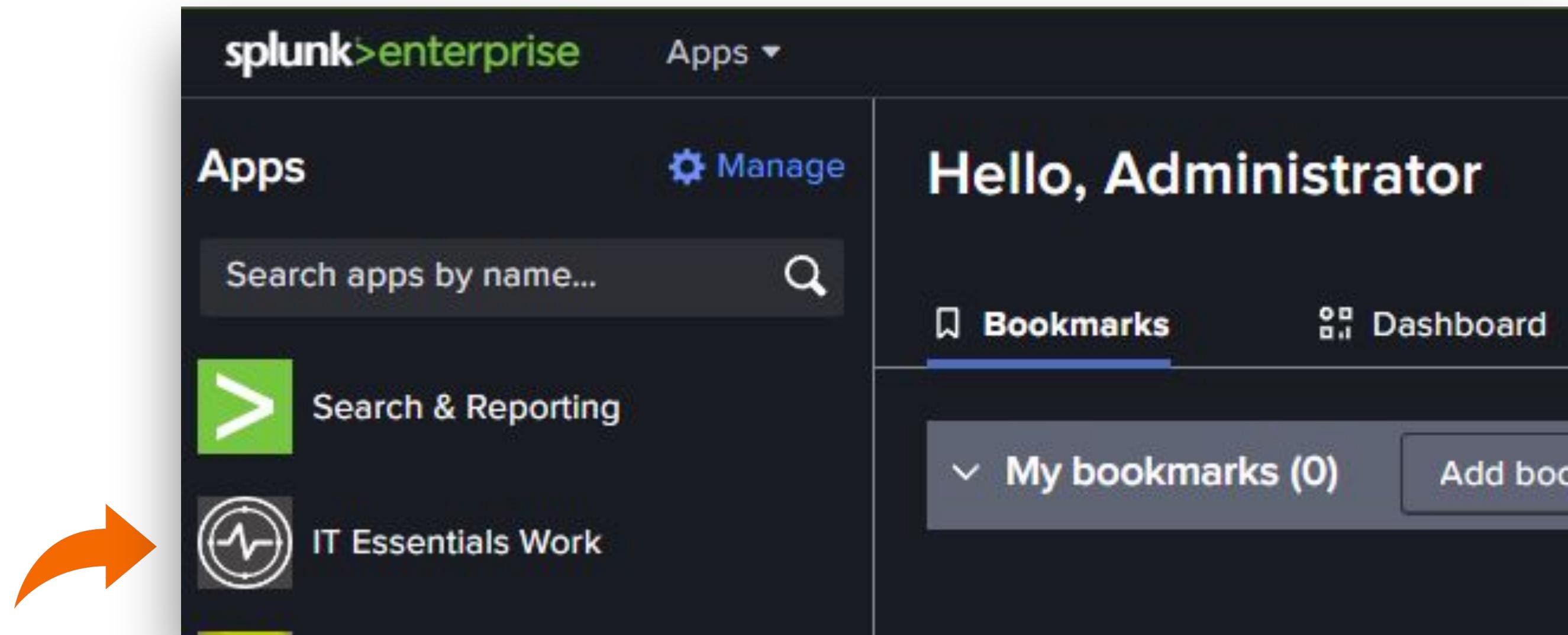
Click Restart Splunk



Activity #3 - deploy the changes

In your browser, navigate again to the IT Essentials Work app and wait for entities to start to appear.

You can set the view to automatically refresh using the refresh button in the upper right corner.



Activity #3 - deploy the changes

May take a few minutes, but you should see 2 entities.

Pro Tip - I clicked **Hide entity types with no entities** for this screenshot

The screenshot shows the Splunk Enterprise interface with the title "splunk>enterprise". The top navigation bar includes "Service Analyzer", "Entity Overview" (which is currently selected), "Alerts and Episodes", "Glass Tables", "Deep Dives", "Dashboards", "Configuration", and a search bar. Below the navigation is a toolbar with filters for "All Status", "All Severities", and a "Search Entity Dimensions" field. Further down are buttons for "Group By: Entity Type" and "Sort By: # of Entities (High to low)". A toggle switch is set to "Hide entity types with no entities". The main content area displays two cards: "Unix/Linux Add-on (1)" and "Windows (1)". Each card shows a count of active, inactive, and unstable entities, followed by a small chart titled "Distributed by CPU Utilization" with a single purple bar at the 0-10% mark. At the bottom of the page is a link: "See the Entity Overview documentation for instructions to collect metrics for all available platforms. Learn more." The Splunk logo and "a CISCO company" text are visible at the bottom left.

Activity #4

- helpful commands to search metrics data**



Activity #4 - helpful commands

How not to search a metrics index.

1. Navigate to the Search & Reporting app
2. Search for `index="itsi_im_metrics"` over the **Last 60 minutes**.

New Search

Save As ▾ Create Table View Close

index="itsi_im_metrics" Last 60 minutes 🔍

! This command only searches event indexes. To search metric indexes, use the mstats command.

✓ 0 events (3/1/22 7:29:00.000 PM to 3/1/22 8:29:28.000 PM) No Event Sampling ▾

Events (0) Patterns Statistics Visualization Job ▾ II ⌂ ⌁ ⌂ Smart Mode ▾

Activity #4 - helpful commands

Overview of Metrics and commands.

A metric is a single measurement at a specific point in time

Metrics in the Splunk platform uses a custom index type that is optimized for metric storage and retrieval.

You can run metrics-specific commands like **mstats**, **mcatalog**, and **mpreview** on the metric data points in those metric indexes.

Activity #4 - mpreview command

Use mpreview to get an idea of the kinds of metric time series that are stored in your metrics indexes and to troubleshoot your metrics data.

mpreview returns a preview of the raw metric data points in a specified metric index that match a provided filter.

By design, mpreview returns metric data points in JSON format

Run the following search:

```
| mpreview  
index=itsi_im_metrics
```

The screenshot shows the Splunk Enterprise search interface. The search bar contains the command: `| mpreview index=itsi_im_metrics`. Below the search bar, it displays `18,848 events (9/18/24 11:00:00.000 PM to 9/19/24 11:59:48.000 PM)`. The search results are presented in a table with columns: `i`, `Time`, and `Event`. The first event is shown in JSON format:

```
i | Time | Event  
> 9/19/24 11:59:41.000 PM { [-]  
| collection: LogicalDisk  
| instance: C:  
| metric_name:LogicalDisk.%_Disk_Read_Time: 0.0015514920783136273  
| object: LogicalDisk  
}  
| Show as raw text  
host = IP-AC1F4070 | source = Perfmon:LogicalDisk | sourcetype = PerfmonMetrics:LogicalDisk
```

The second event is also shown in JSON format:

```
i | Time | Event  
> 9/19/24 11:59:41.000 PM { [-]  
| collection: LogicalDisk  
| instance: _Total  
| metric_name:LogicalDisk.%_Disk_Read_Time: 0.0015514920783136273  
| object: LogicalDisk  
}  
| Show as raw text  
host = IP-AC1F4070 | source = Perfmon:LogicalDisk | sourcetype = PerfmonMetrics:LogicalDisk
```

On the left side of the search results, there are sections for `SELECTED FIELDS` (host, source, sourcetype) and `INTERESTING FIELDS` (collection, instance, object). There are also buttons for `List`, `Format`, and `20 Per Page`.

Activity #4 - mcatalog command

The mcatalog command performs aggregations on the values in the metric_name and dimension fields in the metric indexes.

The mcatalog command is a generating command for reports. Generating commands use a leading pipe character. The mcatalog command must be the first command in a search pipeline, except when append=true.

Run the following search:

```
| mcatalog values(metric_name) WHERE index=itsi_im_metrics
```

The screenshot shows the Splunk Enterprise search interface. The top navigation bar includes 'splunk>enterprise' and 'Administrator'. Below the bar are tabs for 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards', with 'Search' being the active tab. A 'New Search' button is visible. The search bar contains the command: '| mcatalog values(metric_name) WHERE index=itsi_im_metrics'. Below the search bar, it says '10,687 events (9/19/24 12:00:00.000 AM to 9/20/24 12:02:37.000 AM)' and 'No Event Sampling'. There are tabs for 'Events', 'Patterns', 'Statistics (1)', and 'Visualization', with 'Statistics' being the active tab. Below these are buttons for '20 Per Page', 'Format', and 'Preview'. The 'values(metric_name)' field is expanded, showing a list of metric names: LogicalDisk.%_Disk_Read_Time, LogicalDisk.%_Disk_Time, LogicalDisk.%_Disk_Write_Time, LogicalDisk.%_Free_Space, LogicalDisk.%_Idle_Time, LogicalDisk.Avg._Disk_Bytes/Read, LogicalDisk.Avg._Disk_Bytes/Transfer, LogicalDisk.Avg._Disk_Bytes/Write, LogicalDisk.Avg._Disk_Queue_Length, LogicalDisk.Avg._Disk_Read_Queue_Length, LogicalDisk.Avg._Disk_Write_Queue_Length, LogicalDisk.Avg._Disk_sec/Read, and LogicalDisk.Avg._Disk_sec/Transfer.

Activity #4 - mstats command

Use the mstats command to analyze metrics.

This command performs statistics on the measurement, metric_name, and dimension fields in metric indexes

The mstats command is a report-generating command, except when append=true is specified.

Run the following search:

```
| mstats count where  
index=itsi_im_metrics  
metric_name=* by metric_name
```

The screenshot shows the Splunk Enterprise search interface. The search bar contains the command: | mstats count where index=itsi_im_metrics metric_name=* BY metric_name. The results section displays 118,904 events from September 19, 2024, to September 20, 2024. The results are grouped by metric_name, with the following counts:

metric_name	count
LogicalDisk.%_Disk_Read_Time	32
LogicalDisk.%_Disk_Time	46
LogicalDisk.%_Disk_Write_Time	46
LogicalDisk.%_Free_Space	46
LogicalDisk.%_Idle_Time	46
LogicalDisk.Avg._Disk_Bytes/Read	32
LogicalDisk.Avg._Disk_Bytes/Transfer	46
LogicalDisk.Avg._Disk_Bytes/Write	46
LogicalDisk.Avg._Disk_Queue_Length	46
LogicalDisk.Avg._Disk_Read_Queue_Length	32

Activity #4 - mstats command

Use mstats to see average CPU idle:

```
| mstats avg("cpu_metric.pctIdle") WHERE index=itsi_im_metrics by host
```

The screenshot shows the Splunk Enterprise search interface. The top navigation bar includes 'splunk>enterprise', 'Apps ▾', 'Administrator', 'Messages 1', 'Settings', 'Activity', 'Help', 'Find', and a search icon. Below the navigation is a secondary menu with 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', 'Dashboards', and a 'Search & Reporting' button. The main search area is titled 'New Search' with buttons for 'Save As', 'Create Table View', and 'Close'. The search bar contains the command: '| mstats avg("cpu_metric.pctIdle") WHERE index=itsi_im_metrics by host'. Below the search bar, it shows '270 events (9/19/24 11:59:24.000 PM to 9/20/24 12:14:24.000 AM)' and 'No Event Sampling'. The results are displayed in a table with columns 'host' and 'avg(cpu_metric.pctIdle)'. One visible row shows 'ip-172-31-64-215' with a value of '98.68411111111111'. The bottom of the interface features buttons for 'Events', 'Patterns', 'Statistics (1)', 'Visualization', '20 Per Page ▾', 'Format', and 'Preview ▾'.

host	avg(cpu_metric.pctIdle)
ip-172-31-64-215	98.68411111111111

Activity #4 - mstats command

Use mstats to see average CPU idle per host for **Last 15 minutes**:

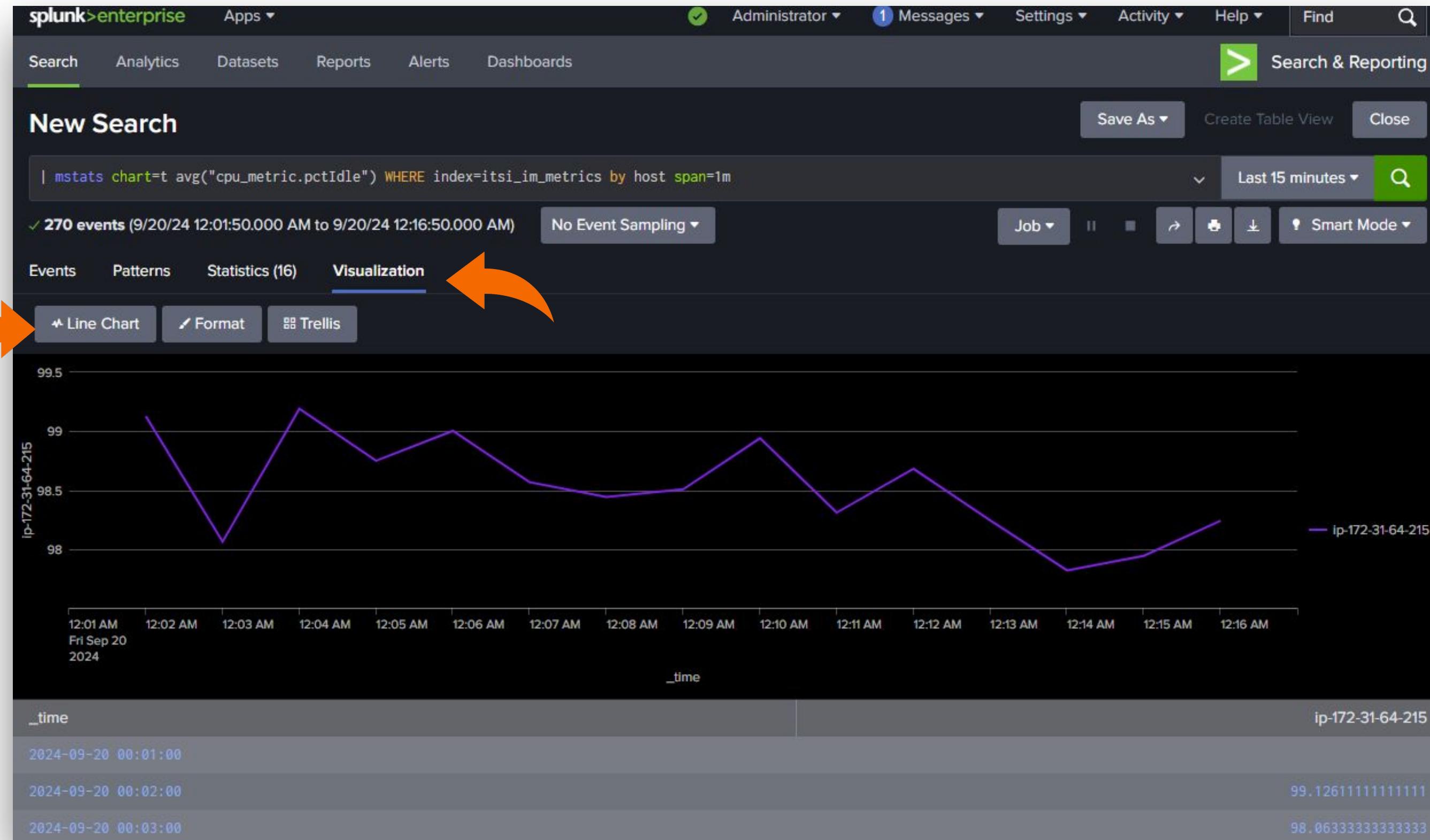
```
| mstats chart=t avg("cpu_metric.pctIdle") WHERE index=itsi_im_metrics by host span=1m
```

The screenshot shows the Splunk Enterprise search interface. The search bar contains the command: `| mstats chart=t avg("cpu_metric.pctIdle") WHERE index=itsi_im_metrics by host span=1m`. The results pane displays 270 events from September 20, 2024, between 00:01:00 and 00:08:00. The data is sorted by _time. The first few rows of the table are:

_time	ip-172-31-64-215
2024-09-20 00:01:00	99.12611111111111
2024-09-20 00:02:00	98.06333333333333
2024-09-20 00:03:00	99.19
2024-09-20 00:04:00	98.75055555555555
2024-09-20 00:05:00	99.00277777777778
2024-09-20 00:06:00	98.56722222222223
2024-09-20 00:07:00	98.44222222222223
2024-09-20 00:08:00	98.44222222222223

Activity #4 - mstats command

Now take that same search and click **Visualization** and select **Line Chart**.



Activity #4 - helpful commands

Try the mstats command with another metric_name

Remember the **mcatalog** & **mpreview** command can help you discover other metric names.

```
| mcatalog values(metric_name) WHERE index=itsi_im_metrics  
| mpreview index=itsi_im_metrics
```

Other **mstats** examples:

```
| mstats chart=t avg("df_metric.UsePct") WHERE index=itsi_im_metrics by host span=1m  
| mstats chart=t avg("Memory.Available_MBytes") WHERE index=itsi_im_metrics by host span=1m
```

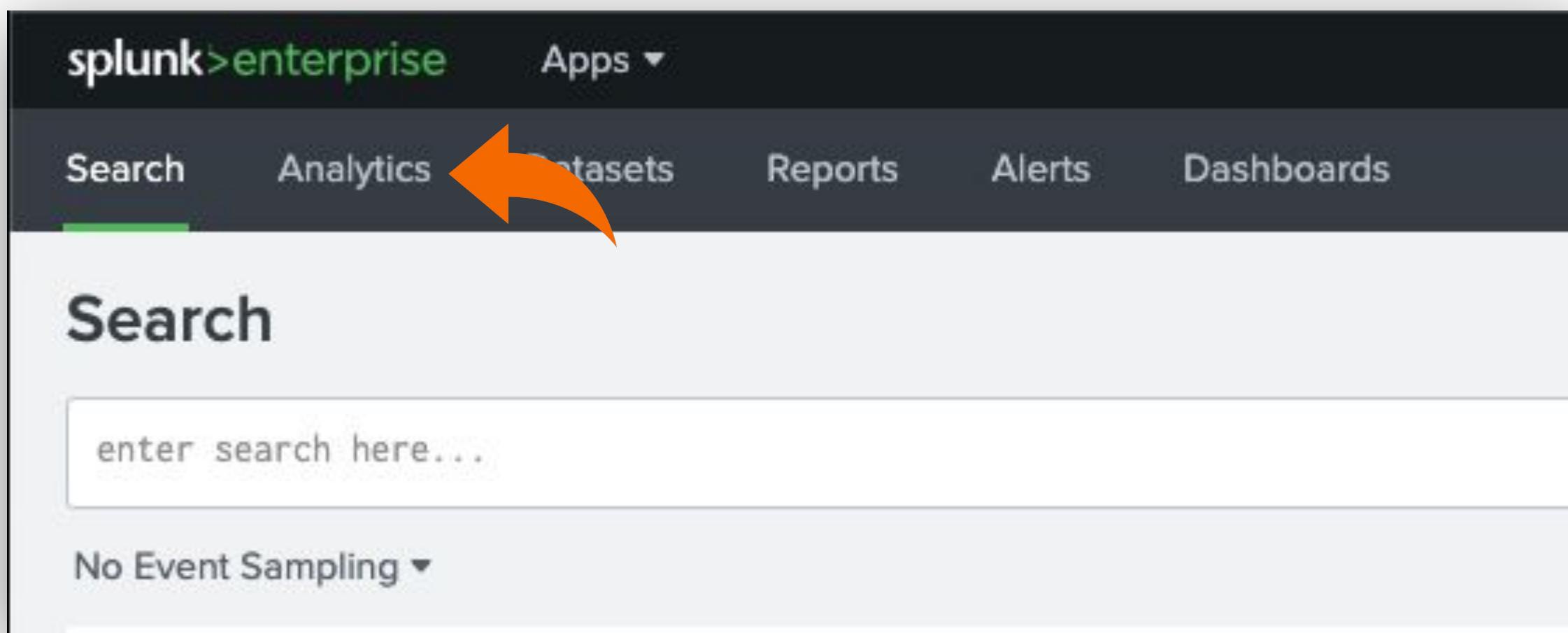
Activity #5
- Use Analytics
Workspace to build
useful reports,
dashboards and alerts



Activity #5 - Analytics Workspace

Navigate to the **Search & Reporting** app

Click the **Analytics** tab



Activity #5 - Analytics Workspace

The Analytics Workspace Data panel contains the data sources that you have available for visualization and analysis.

The screenshot shows the Splunk Analytics Workspace interface. At the top, there's a navigation bar with 'splunk>enterprise' on the left, followed by 'Apps ▾', 'Administrator' (with a green checkmark), 'Messages' (with a blue circle containing '1'), 'Settings ▾', 'Activity ▾', 'Help ▾', 'Find', and a magnifying glass icon. Below the navigation bar is a secondary menu with 'Search', 'Analytics' (which is underlined in green), 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. To the right of this is a 'Search & Reporting' button with a green arrow icon. The main area is titled 'Data' and features a 'Find Data to Analyze' search bar with a magnifying glass icon. On the left, there's a sidebar with a tree view of data sources under 'Metrics': 'LogicalDisk', 'Memory', 'Network_Interface', 'PhysicalDisk', 'Process', 'Processor', 'System', 'cpu_metric', 'df_metric', 'interfaces_metric', 'iostat_metric', 'ps_metric', 'spl', and 'vmstat_metric'. The main panel has a dark background with light-colored text. It displays the message 'Start by selecting data.' and 'Find something interesting? Save it to a dashboard, or create an alert.'

Activity #5 - Analytics Workspace

In the **Find Data to Analyze** box enter:

CPU

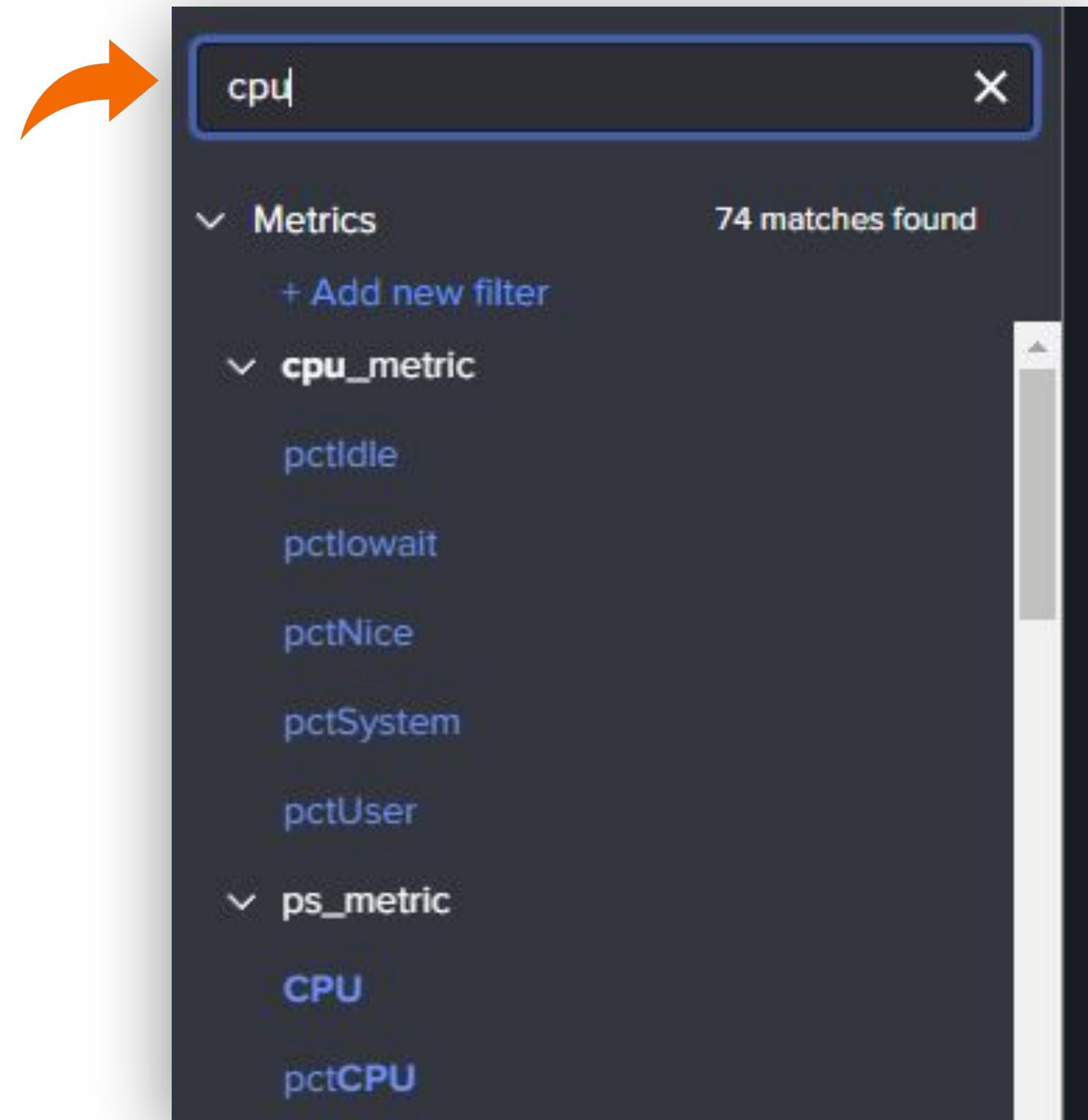
This will filter the metrics data sources to only display metrics related to **CPU**.

Go ahead and try a few other keywords:

Memory

User

Bytes



Activity #5 - Analytics Workspace

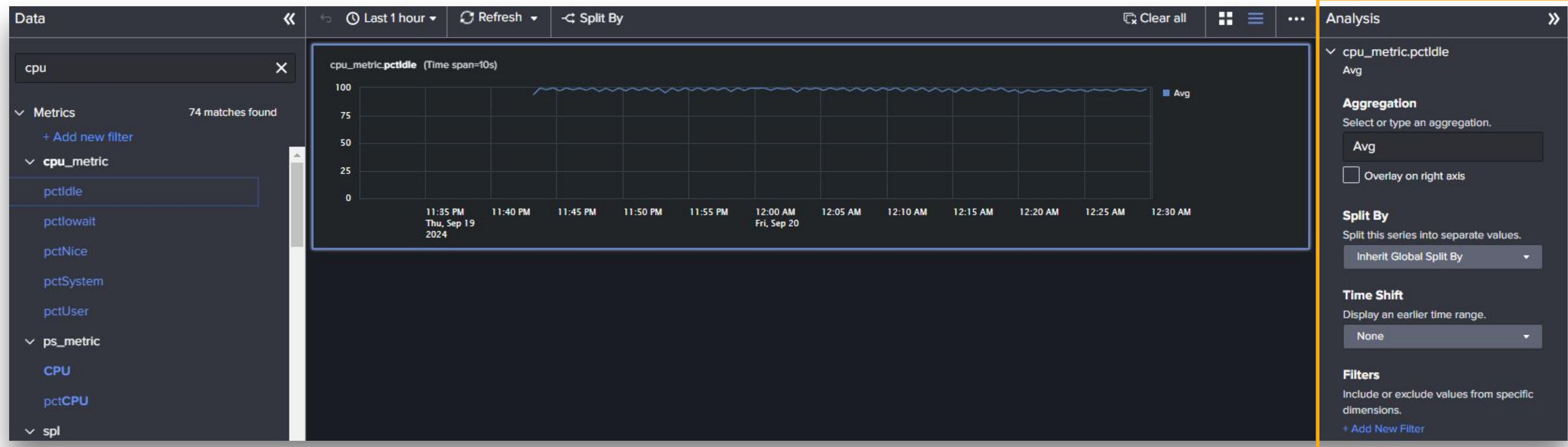
Sticking with CPU, lets click on **pctidle** under **cpu_metric**

Now you should have a chart that shows an aggregate average for **cpu_metric.pctidle**



Activity #5 - Analytics Workspace

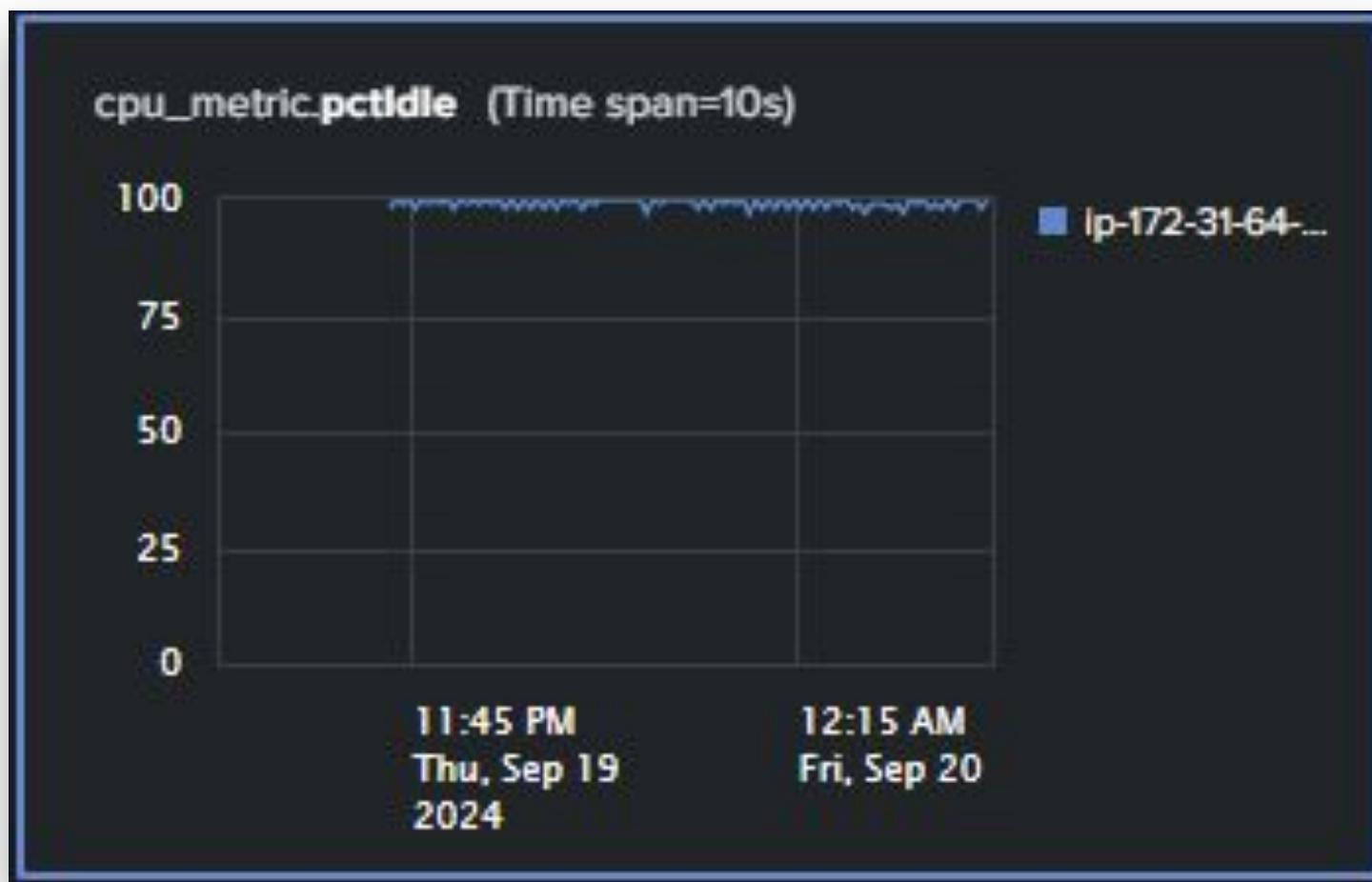
Notice a new navigation menu appeared on the right side called **Analysis** panel.



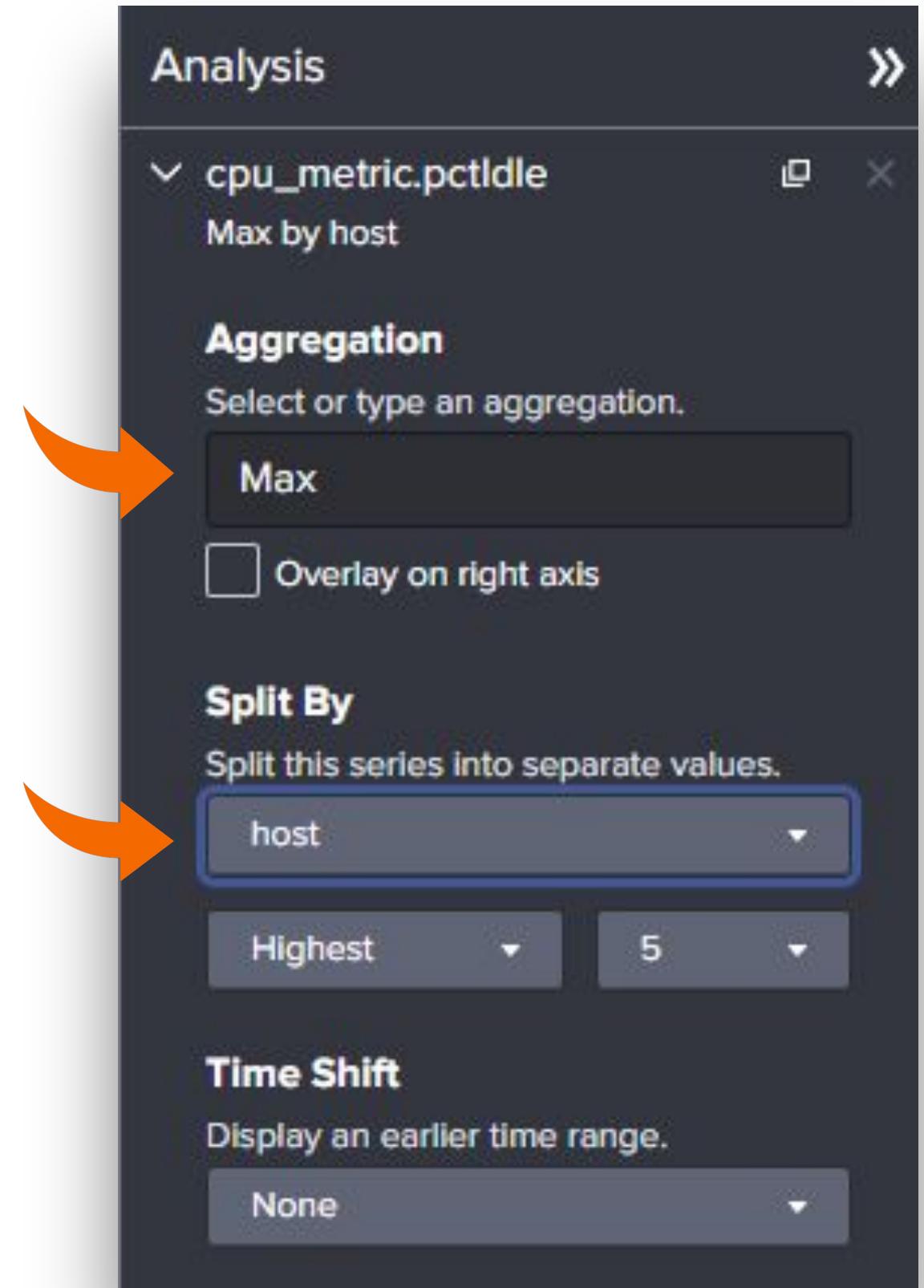
Activity #5 - Analytics Workspace

Analysis panel allows you to perform analytic functions and operations.

1. From **Aggregation** change Avg to Max
2. Under **Split By** select host.



In the chart you should see the Max
cpu_metric.pctidle by
host.



Activity #5 - Analytics Workspace

You can have more than 1 chart.

In the **Find Data to Analyze** box enter **memUsedPct** and click on **memUsedPct** under **vmstat_metric**

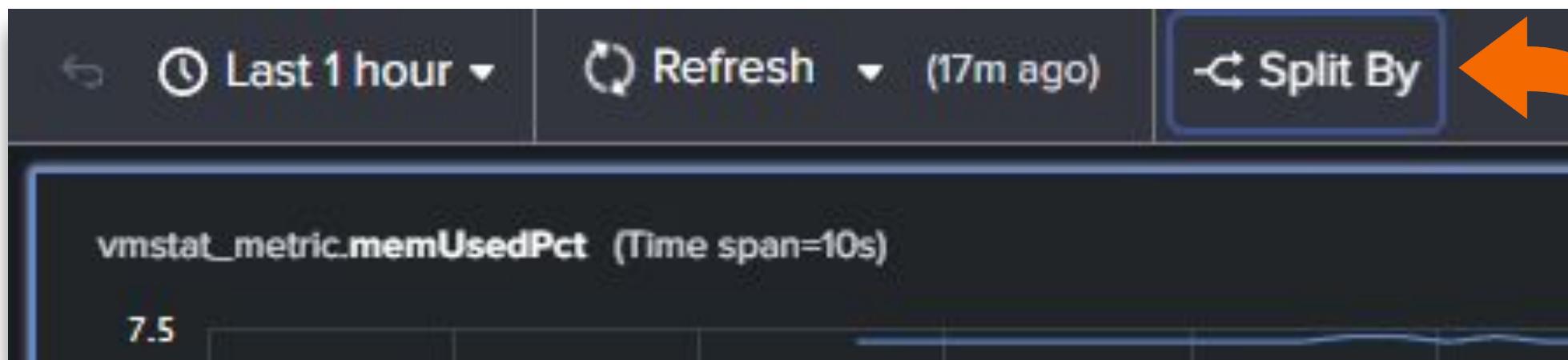


Activity #5 - Analytics Workspace

At this point you will have 2 charts.

However, the newest chart is not Split By host.

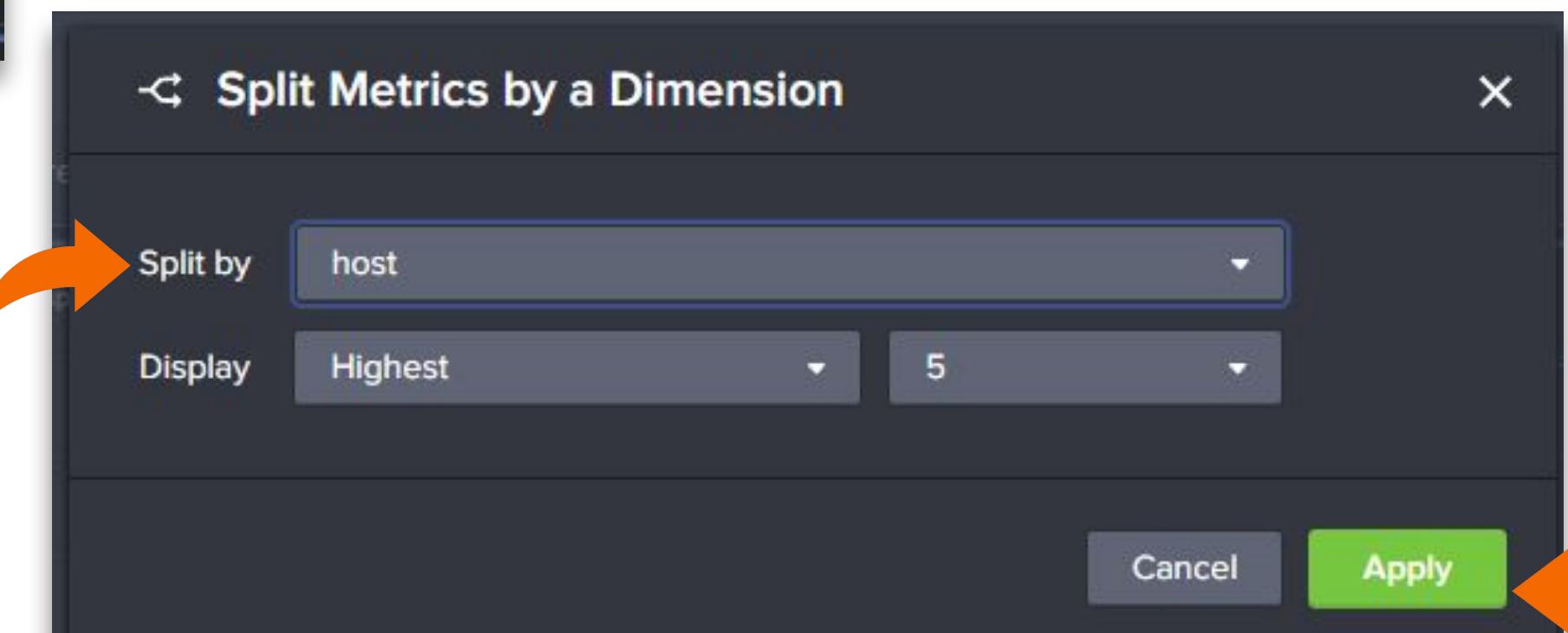
By default, any new chart will inherit the **Global Split By** value and no value has been set.



Click on **Split By** at the top

You will now see a pop-up box where you can select what to Split By.

Select **host** from the dropdown and click **Apply**"



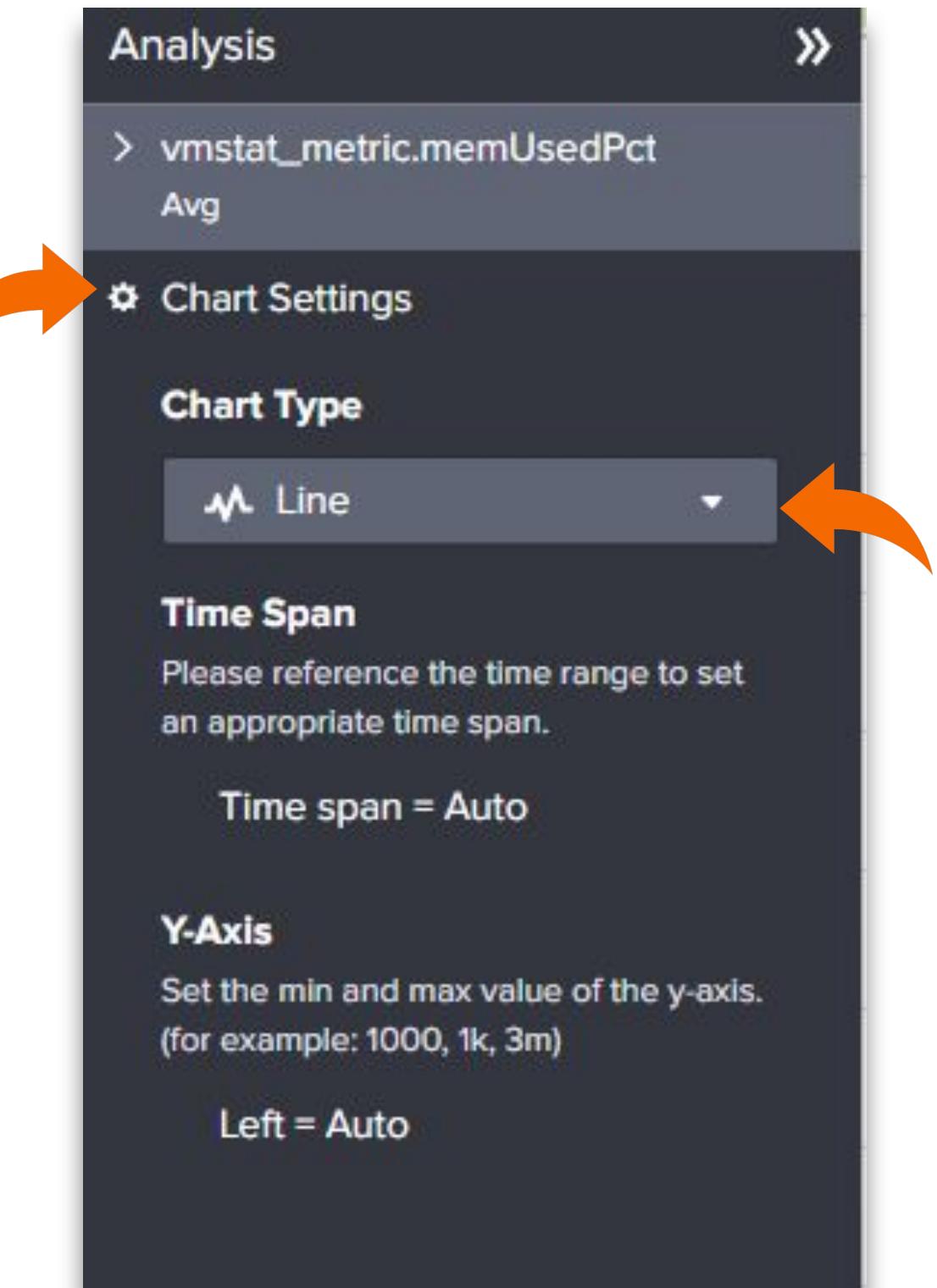
Activity #5 - Analytics Workspace

Analysis panel also has Chart Settings section near the bottom.

Chart Settings allows you to change the chart from **Line** to **Area**, adjust **Time Span** and the **Y-Axis**

Select your top chart and change the Chart Type from **Line** to **Area** or whatever you would like.

Try them all out.

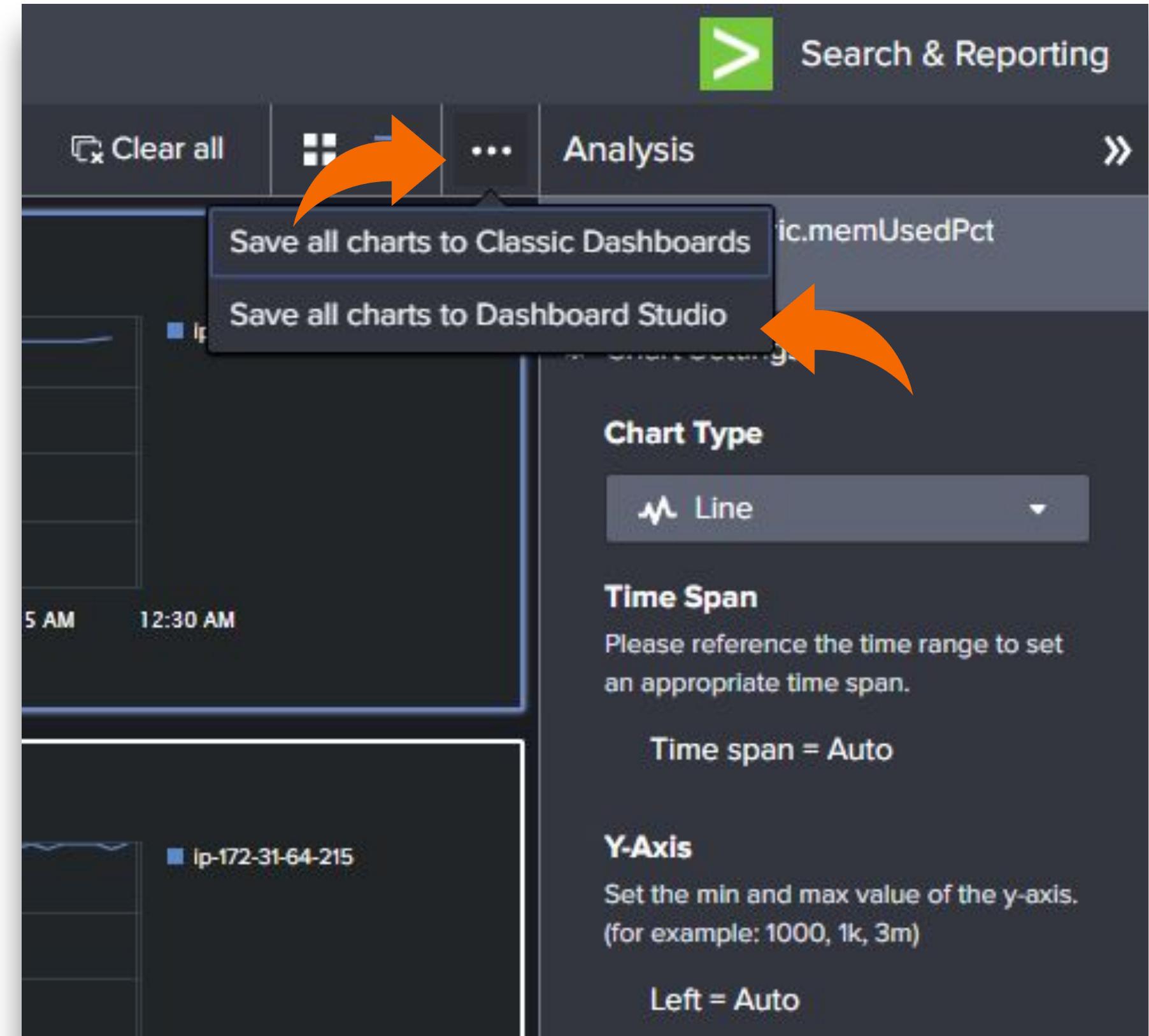


Activity #5 - Analytics Workspace

Save all Charts as a Dashboard.

Global Actions is represented by 3 dots
“...” at the top

Click the “...” and select
Save all charts to Dashboard Studio



Activity #5 - Analytics Workspace

Save all Charts as a Dashboard.

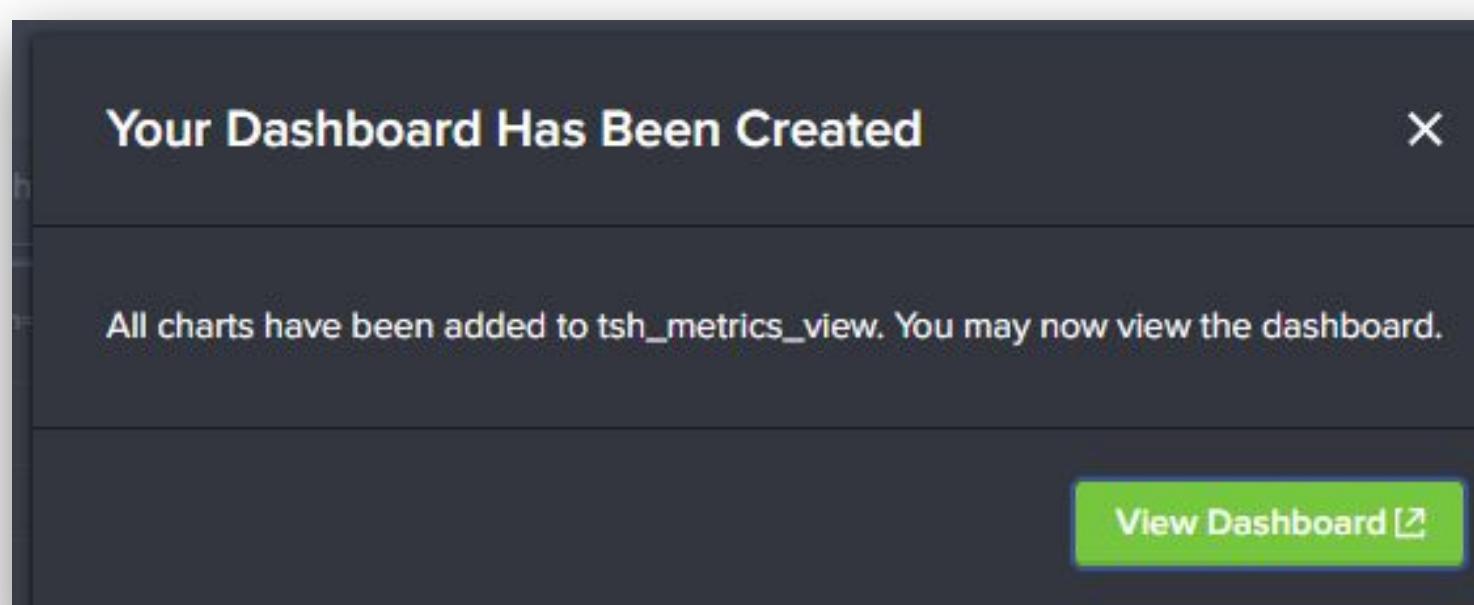
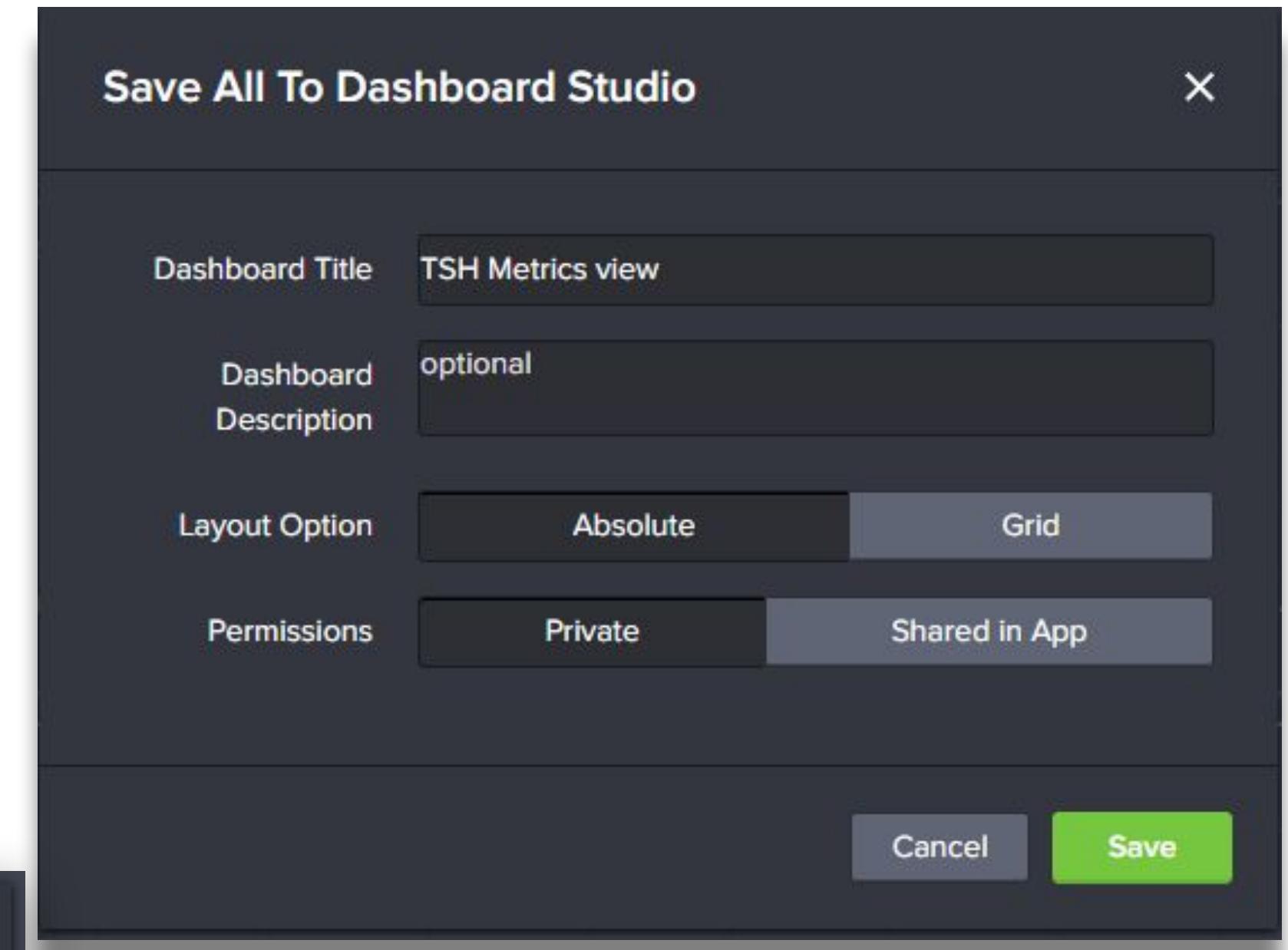
In the pop-up give your dashboard a **Title**

For example: **TSH Metrics view**

You can leave everything else alone.

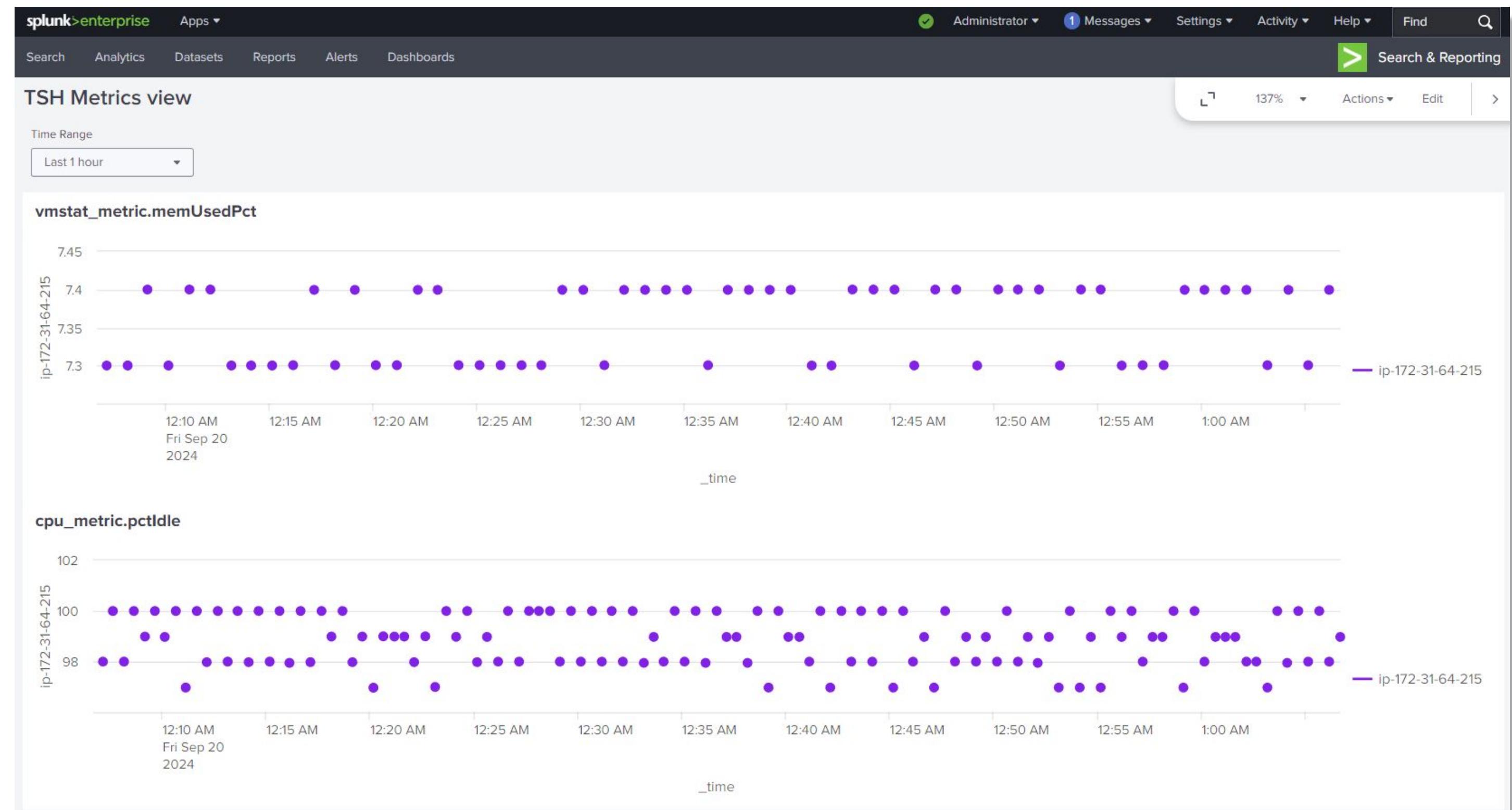
Now click **Save**

You should have another pop-up where you can click **View Dashboard**



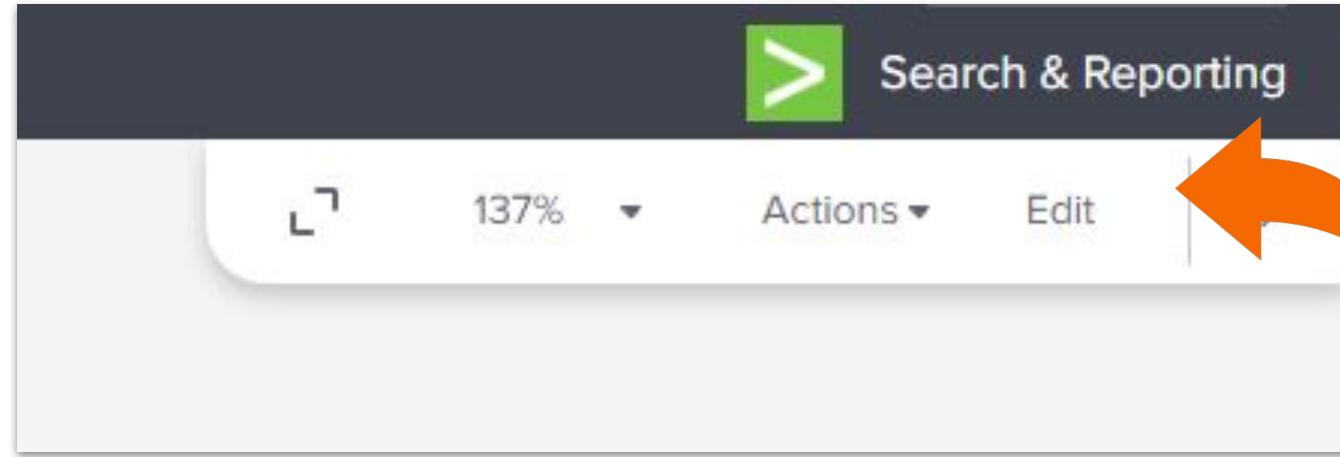
Activity #5 - Analytics Workspace

A dashboard has been born

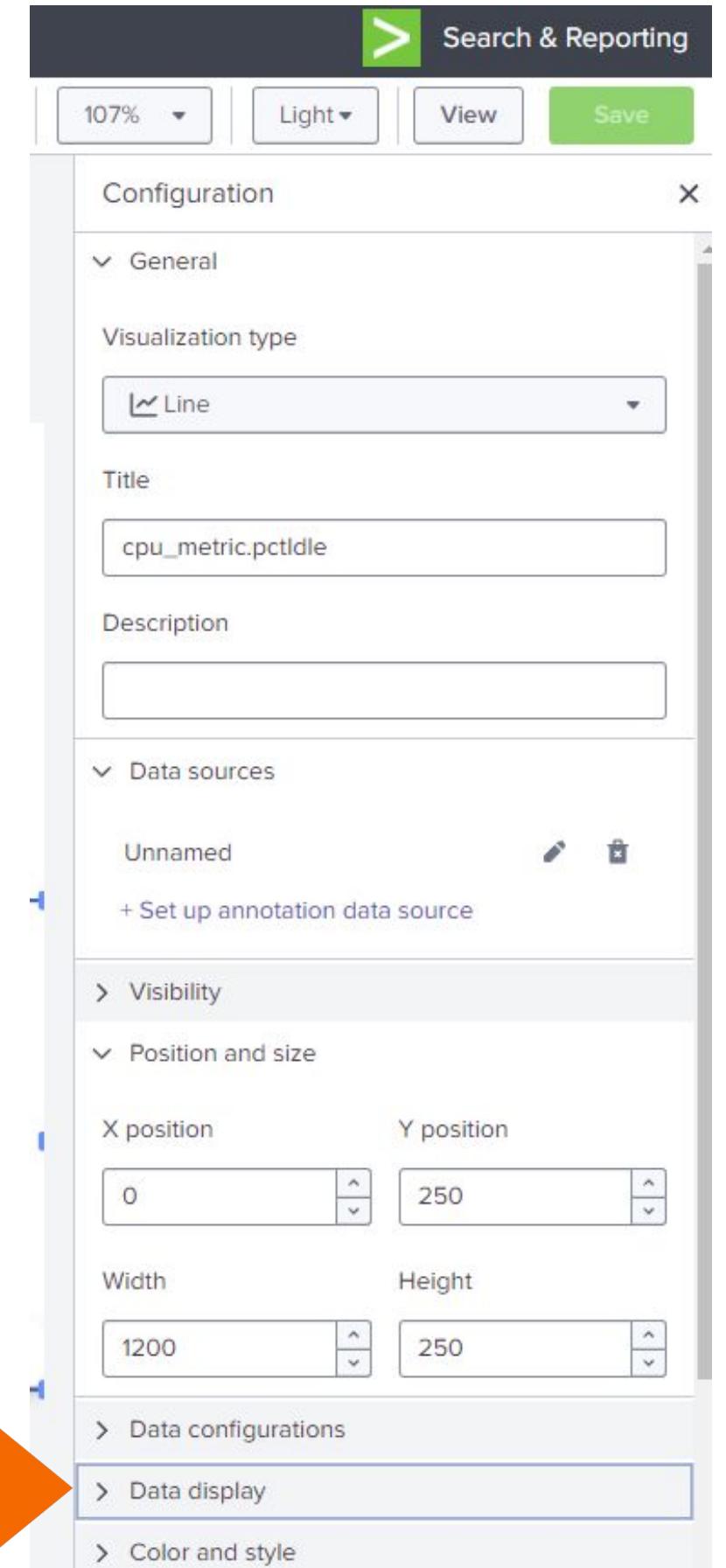


Activity #5 - Analytics Workspace

Adjust the Line chart to connect the “dots”



1. Click **Edit** in the top right corner
2. Next select a chart
3. You should now see the **Configuration** menu on the right side.
4. Find **Data display** and click to expand



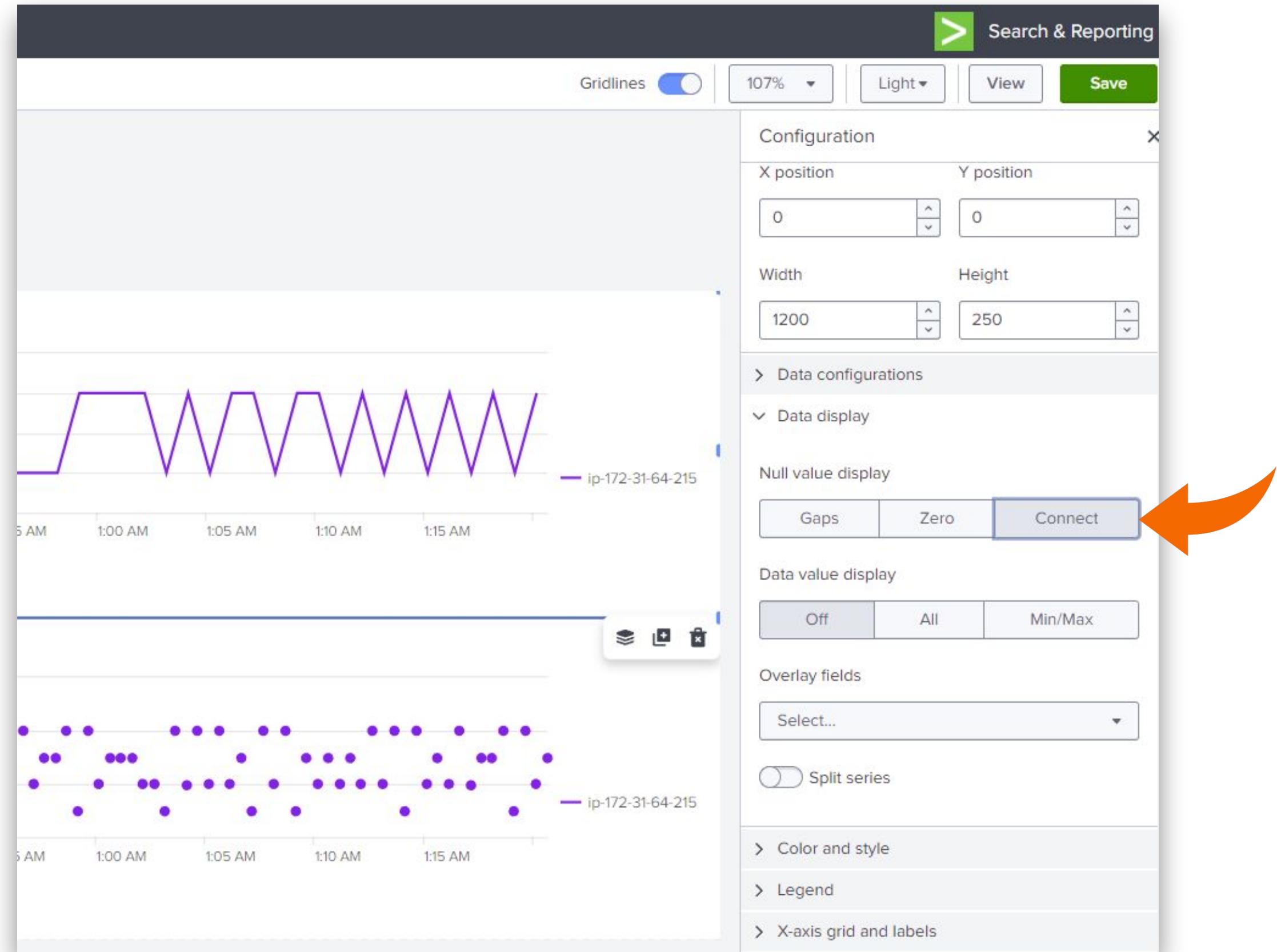
Activity #5 - Analytics Workspace

Select **Connect** under Null value display

You should see the change immediately.

Now you can click **Save** to retain your changes.

Take this time to play around with the different settings or practice again with the other chart.



Activity #5 - Analytics Workspace

BTW, Each chart also has **Chart Actions**



In the chart near the top right, you will see 3 dots “...” appear.

Clicking on the 3 dots “...” will provide a drop down of actions available.

For example, if you would like to see the backend query that is driving the chart. Click **Open in Search**

Or you could save this chart as a report.

Review all available options

Activity #6

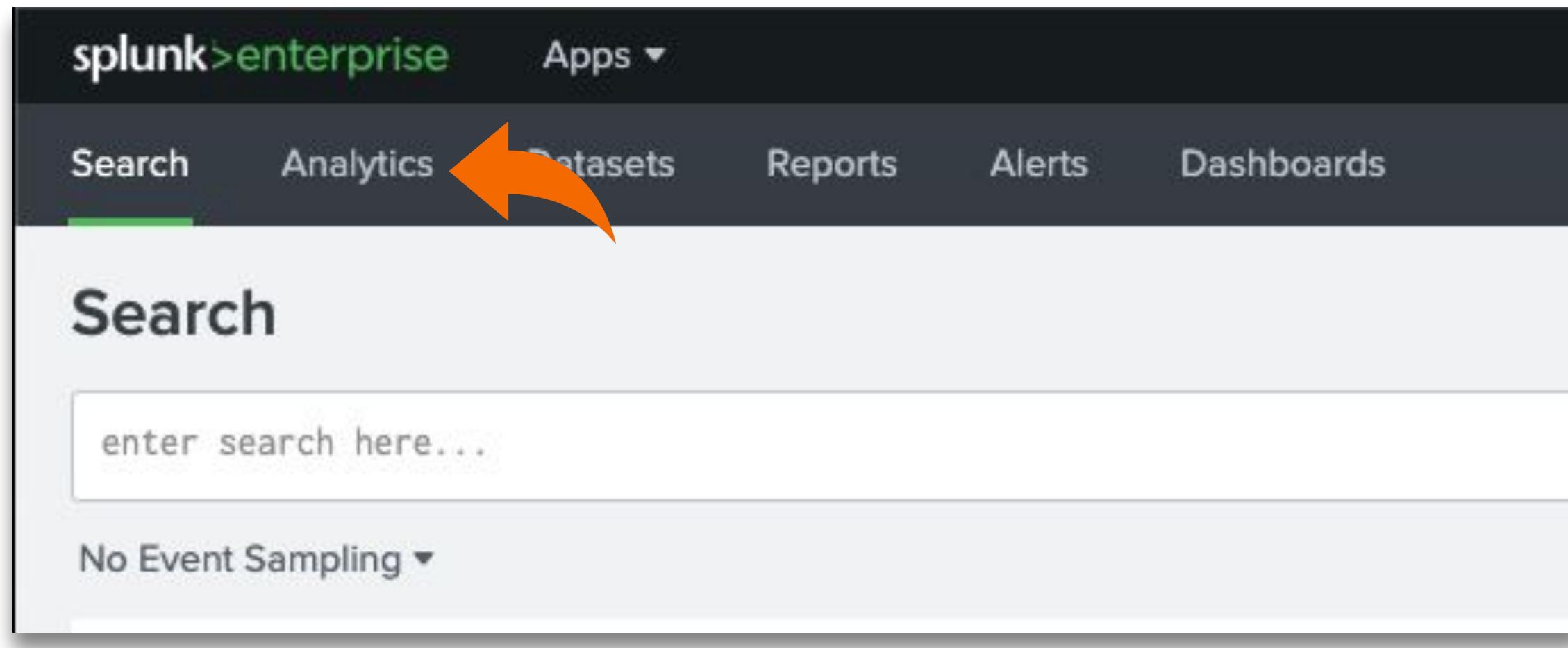
- Use Analytics
Workspace to
build alerts**



Activity #6 - Create an Alert

Navigate to the **Search & Reporting** app

Click the **Analytics** tab

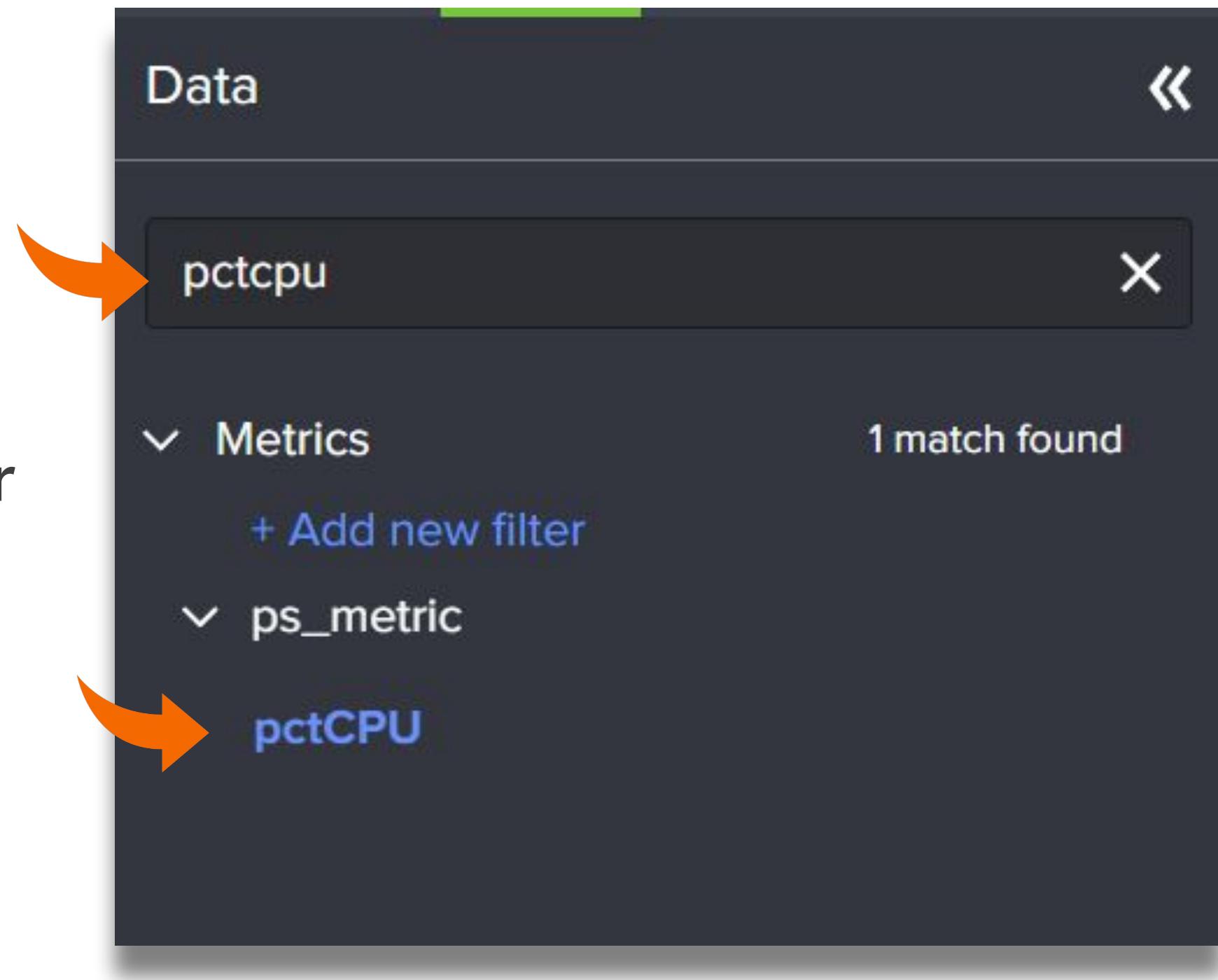


Activity #6 - Create an Alert

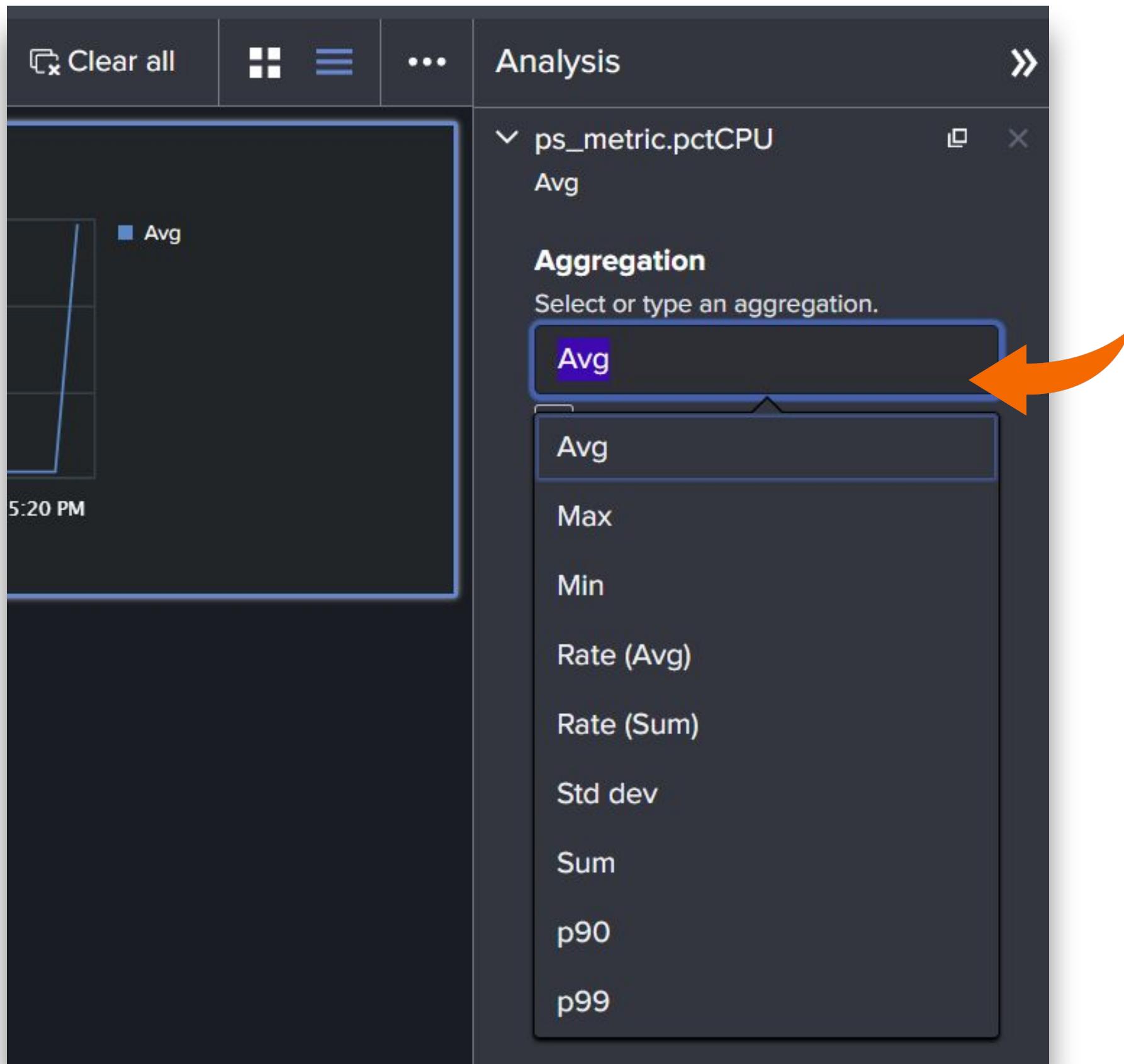
In the **Find Data to Analyze** box enter:

pctCPU

Click on **pctCPU** under **ps_metrics**



Activity #6 - Create an Alert

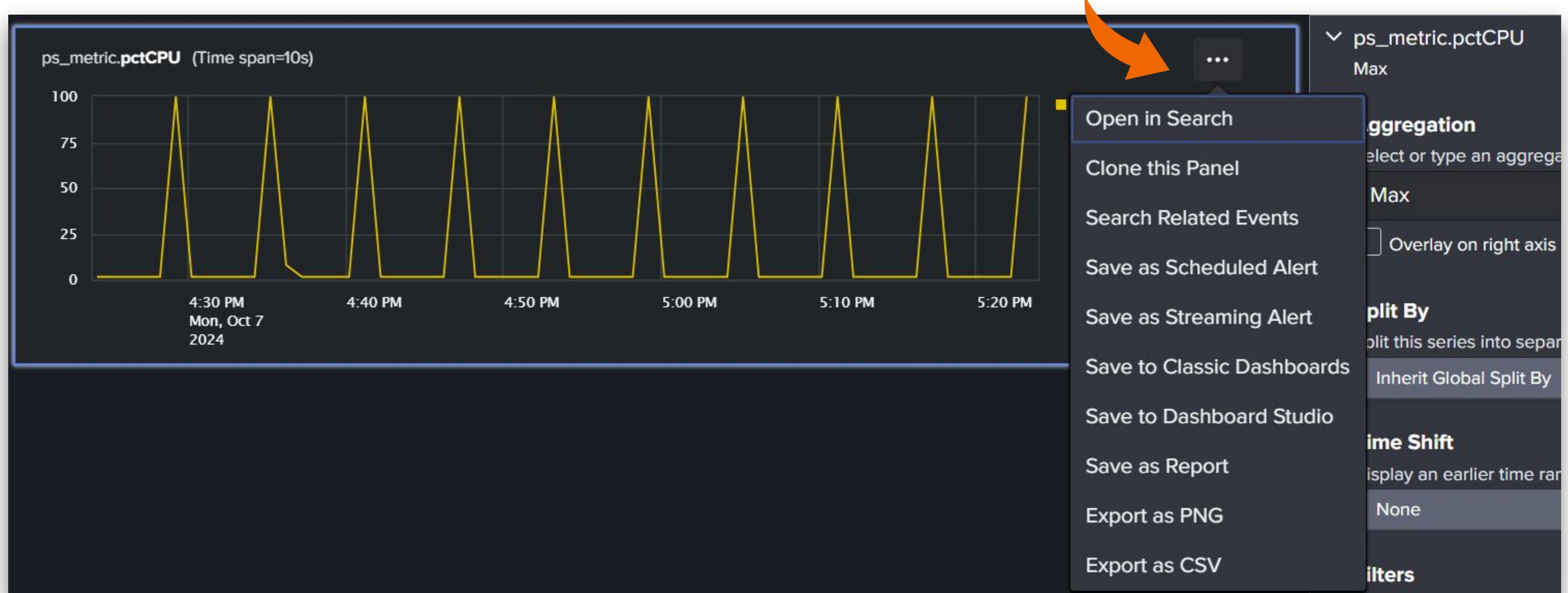


Change the
Aggregation from Avg
to Max

Activity #6 - Create an Alert

In the chart, near the top right, you will see 3 dots “...” appear.

Clicking on the 3 dots “...” will provide a drop down of actions available.

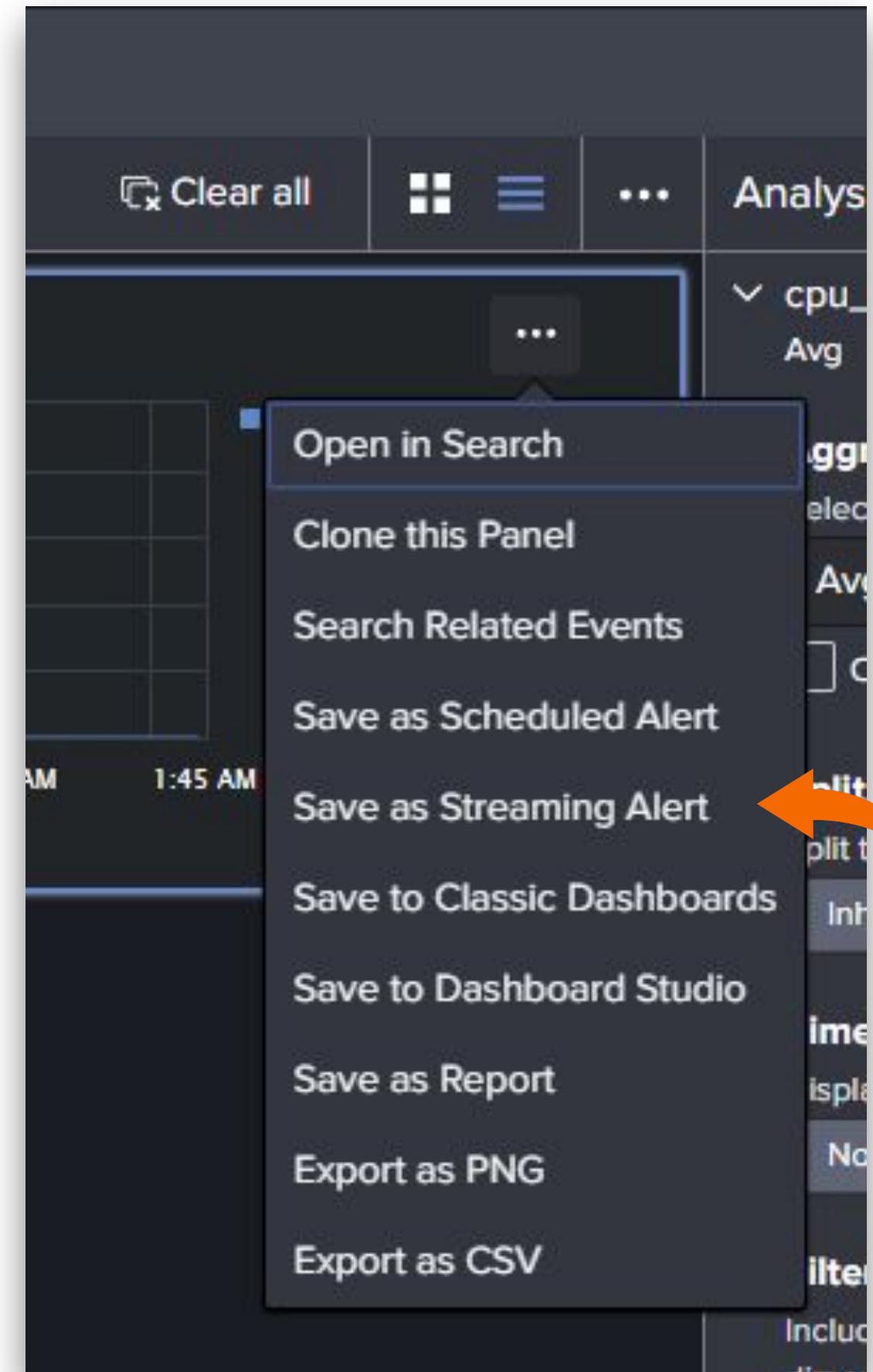


Activity #6 - Create an Alert

You have 2 Alert Types to choose from:

- **Scheduled alerts** periodically search for trigger conditions.
- **Streaming alerts** continuously search for trigger conditions. Streaming alerts can also reduce search processing load by enabling similar alerts to share the same search process.

<https://docs.splunk.com/Documentation/Splunk/latest/Analytics/Alerts>



Select
**Save as Streaming
Alert**

Activity #6 - Create an Alert

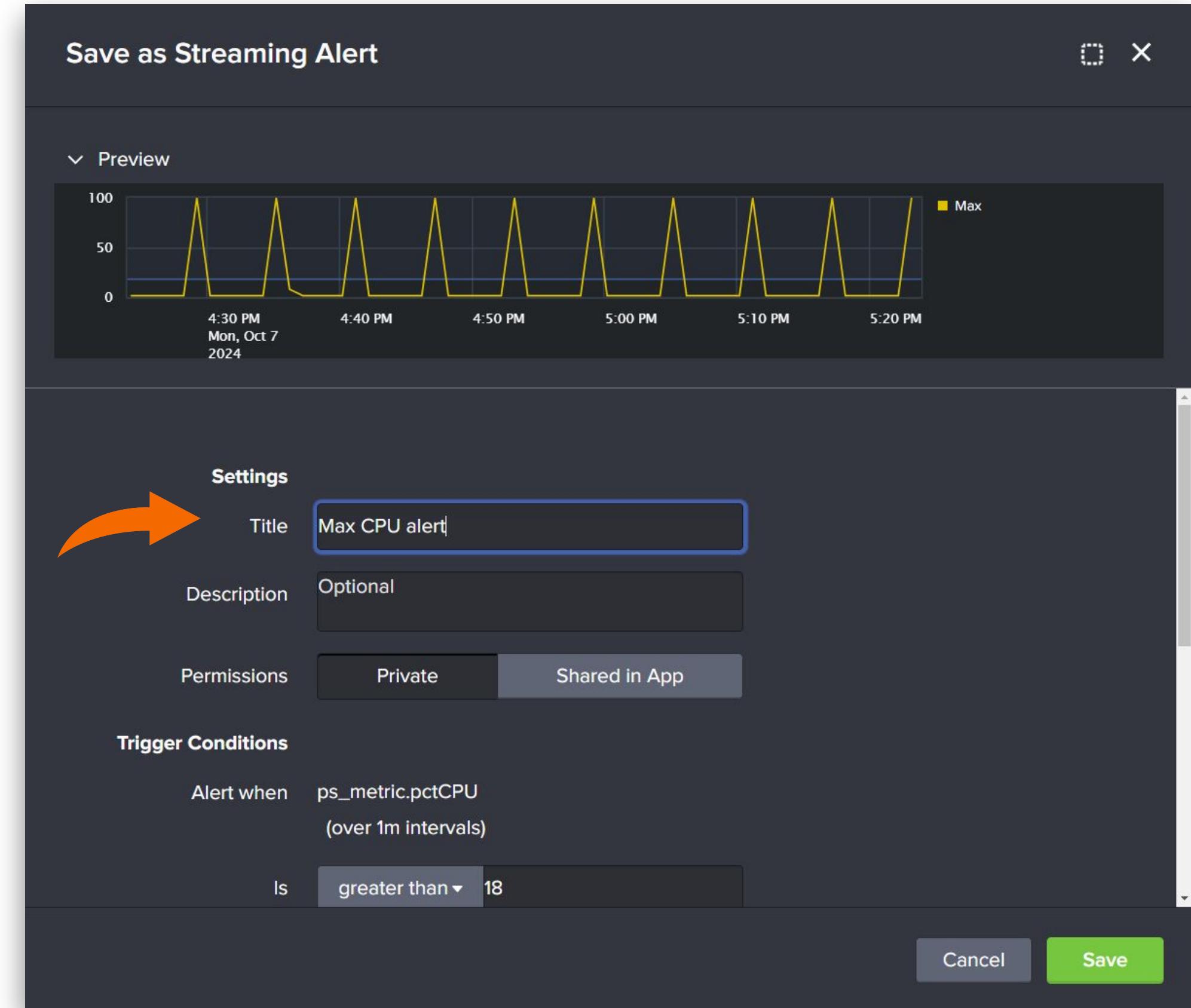
You should now have a **Save as Streaming Alert** pop-up

Near the top you will see **Preview** panel.

When making changes to **Trigger Conditions** the **Preview** panel will update automatically.

Give your alert a **Title**:

For example: **Max CPU alert**



Activity #6 - Create an Alert

Under **Trigger Conditions** adjust the **greater than** value to **80**

Next, Click on **Severity** and chose **High**

The **Preview** panel should have updated automatically with the new values.

Try different values and settings to see how it changes the alert. You can even change **greater than** to **less than**.

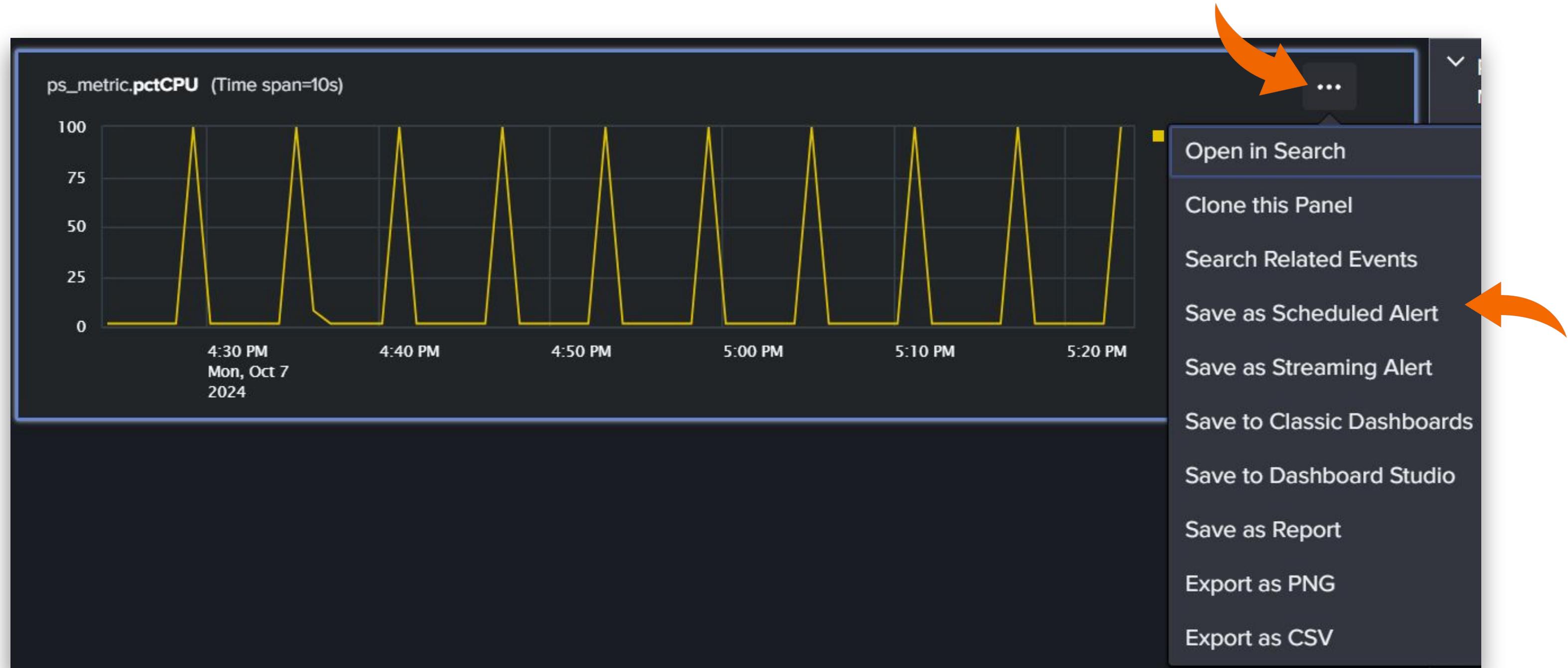
By default the only **Action** will be to send the alert to the **Triggered Alerts** page.

Go ahead and click **Save** to create the alert.

The screenshot shows the 'Save as Streaming Alert' dialog box. In the 'Trigger Conditions' section, the 'Alert when' field is set to 'ps_metric.pctCPU (over 1m intervals)', 'Is' is set to 'greater than' with a value of '80' (highlighted by an orange arrow), and 'Throttle' is checked. In the 'Trigger Actions' section, 'When triggered' includes an 'Add to Triggered Alerts' action with 'Severity' set to 'High' (also highlighted by an orange arrow). Both sections have a 'Save' button at the bottom right.

Activity #6 - Create an Alert

Let's go back through the same process and create a **Scheduled Alert** to see the difference between Streaming Alert.



Activity #6 - Create an Alert

You should now have a **Save as Scheduled Alert** pop-up

Just as before, we have some of the same options for settings

Give you're alert a Title:

For example: **Max CPU scheduled alert**

Notice now we have **Evaluate every** option

Let's change **Hours** to **Minutes**

Set **greater than** to **95**

Set **In the last** to **1**



Save as Scheduled Alert

Preview

Settings

Title: Max CPU Scheduled alert

Description: Optional

Permissions: Private Shared in App

Evaluate every: 1 Minutes

Trigger Conditions

Alert when: ps_metric.pctCPU (over 10s intervals)

Is: greater than 95

In the last: 1 Minutes

Throttle:

Suppress Triggering for: 10 Seconds

Trigger Actions

Activity #6 - Create an Alert

Now click on **+ Add Actions** under **Trigger Actions** to see the available options.

We are going to leave the default of **Add to Triggered Alerts** and change **Severity** to **Critical**

The screenshot shows the Splunk alert configuration interface. At the top, it says "Alert when" followed by the search query "cpu_metric.pctlowait". Below this, a dropdown menu titled "+ Add Actions" is open, displaying five options:

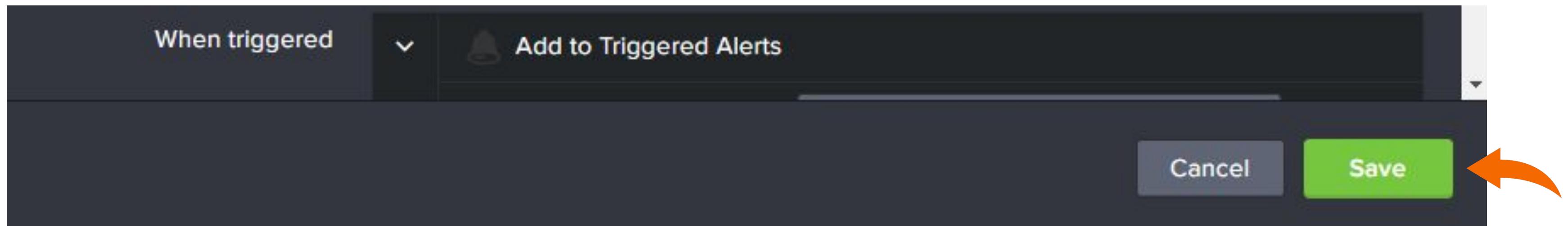
- Add reference link**: Link an episode to an external URL.
- Clear Splunk Infrastructure Monitoring incidents**: Given an ITSI episode, clear the Splunk Infrastructure Monitoring incidents within it.
- Create ServiceNow incident**: Given an ITSI episode, create a ServiceNow incident and link it to the episode.
- ITSI Alert Generator**: Send an ITSI alert to the summary index.
- ITSI Import Objects**

Below the dropdown, there are two sections: "When triggered" and "Add to Triggered Alerts". The "When triggered" section has a dropdown menu currently set to "Add to Triggered Alerts". The "Add to Triggered Alerts" section includes a "Severity" dropdown set to "Critical".

Activity #6 - Create an Alert

Once you're finished reviewing all the options of **Scheduled Alert**

Go ahead and click **Save** to create the alert.



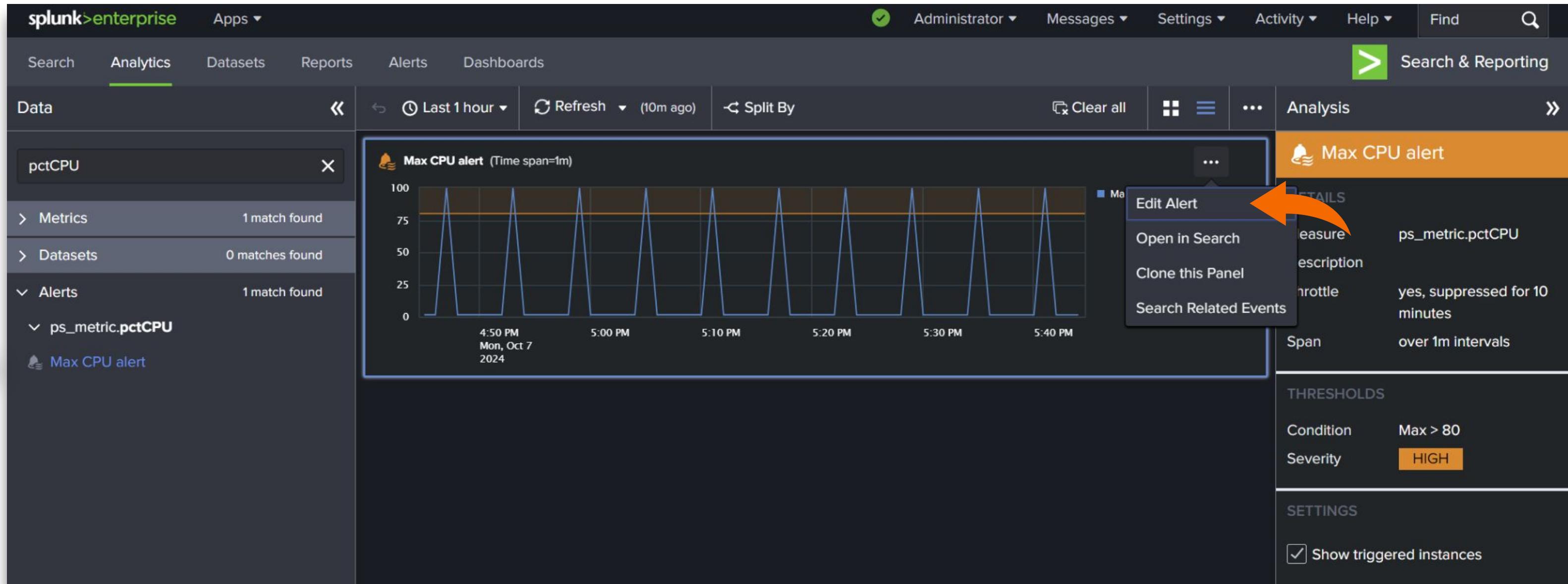
Activity #6 - Create an Alert

After saving the alert, that popup should go away and you will be back in the Analytics workspace.

You may be asking yourself, how do I find those alerts.



Activity #6 - Create an Alert



From the **Analytics Workspace** you can find the alert you created under **Alerts** in the left side menu.

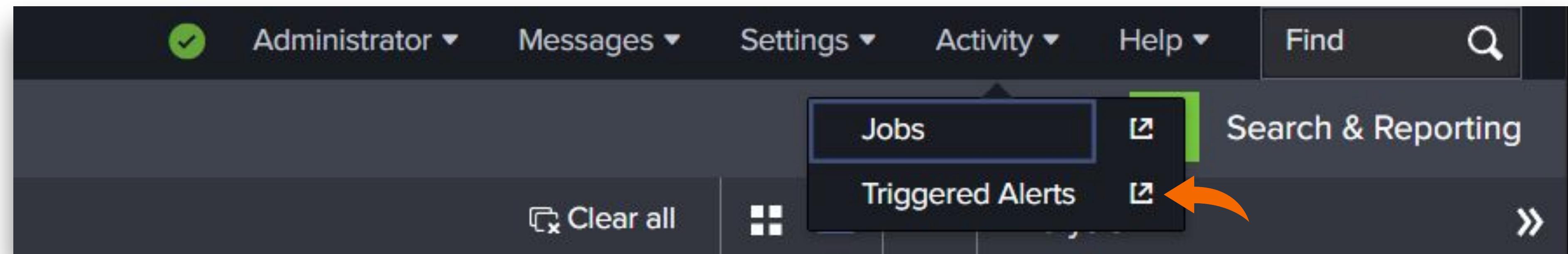
Click on the alert you created and review the information presented.

In **Chart Actions** you can now edit the alert if needed.

Activity #6 - Create an Alert

To find the **Triggered Alerts** page, Click on **Activity** from the top menu.

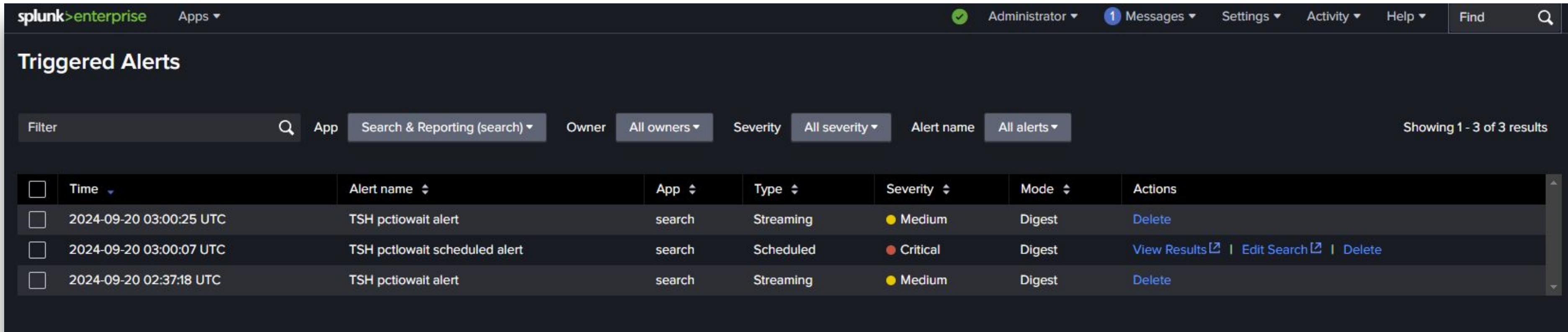
Here you will see a drop down menu with **Triggered Alerts**



Click the icon next to **Triggered Alerts** to open in a new window

Activity #6 - Create an Alert

Examples of alerts that have fired



The screenshot shows the Splunk Enterprise web interface with the title "Triggered Alerts". The top navigation bar includes links for "splunk>enterprise", "Apps", "Administrator", "Messages", "Settings", "Activity", "Help", "Find", and a search icon. The main table has columns for "Time", "Alert name", "App", "Type", "Severity", "Mode", and "Actions". There are three results listed:

Time	Alert name	App	Type	Severity	Mode	Actions
2024-09-20 03:00:25 UTC	TSH pctiowait alert	search	Streaming	Medium	Digest	Delete
2024-09-20 03:00:07 UTC	TSH pctiowait scheduled alert	search	Scheduled	Critical	Digest	View Results Edit Search Delete
2024-09-20 02:37:18 UTC	TSH pctiowait alert	search	Streaming	Medium	Digest	Delete

Activity #6 - Create an Alert

Differences I have noticed between Scheduled and Streaming alerts when creating this workshop

- On the **Triggered Alerts** page, additional **Actions** options are available for a **Scheduled Alert**.

The screenshot shows the Splunk Enterprise web interface with the following details:

- Header:** splunk>enterprise, Apps ▾, Administrator, 1 Messages ▾, Settings ▾, Activity ▾, Help ▾, Find, and a search icon.
- Title:** Triggered Alerts
- Filter Bar:** Filter, Time ▾, App, Search & Reporting (search) ▾, Owner, All owners ▾, Severity, All severity ▾, Alert name, All alerts ▾, and Showing 1 - 3 of 3 results.
- Table:** A grid of alert details with columns: Time, Alert name, App, Type, Severity, Mode, and Actions.
- Data:**

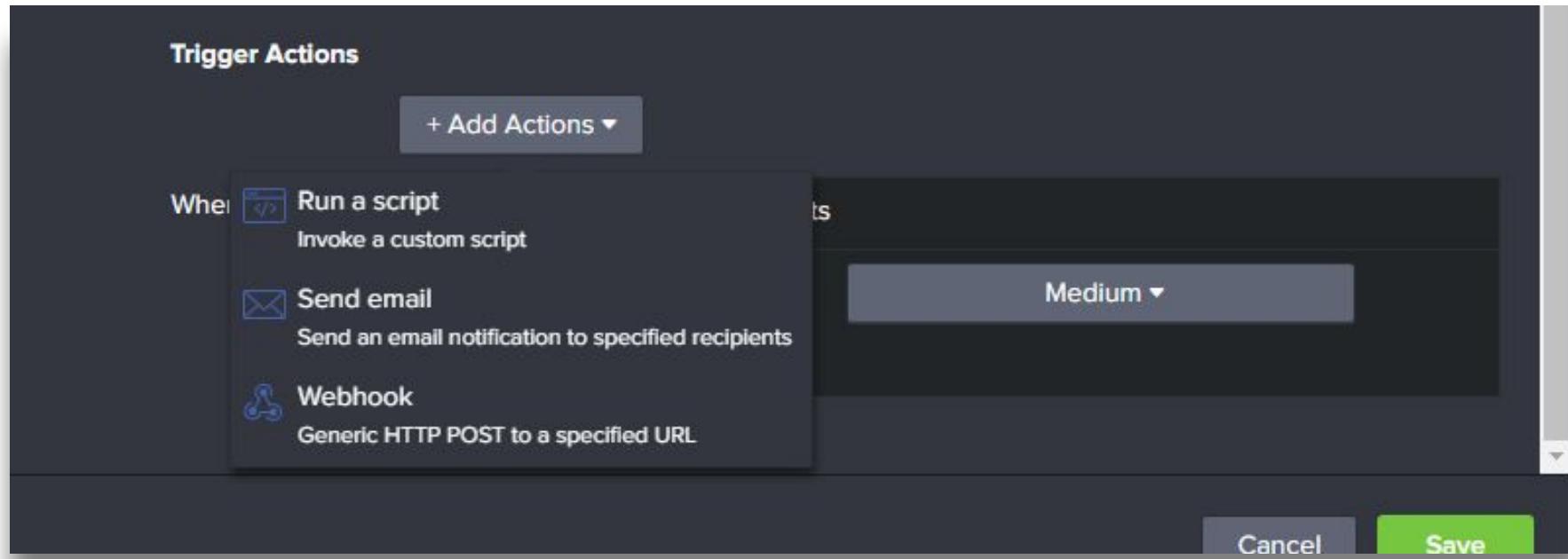
Time	Alert name	App	Type	Severity	Mode	Actions
2024-09-20 03:00:25 UTC	TSH pctiowait alert	search	Streaming	Medium	Digest	Delete
2024-09-20 03:00:07 UTC	TSH pctiowait scheduled alert	search	Scheduled	Critical	Digest	View Results Edit Search Delete
2024-09-20 02:37:18 UTC	TSH pctiowait alert	search	Streaming	Medium	Digest	Delete

Activity #6 - Create an Alert

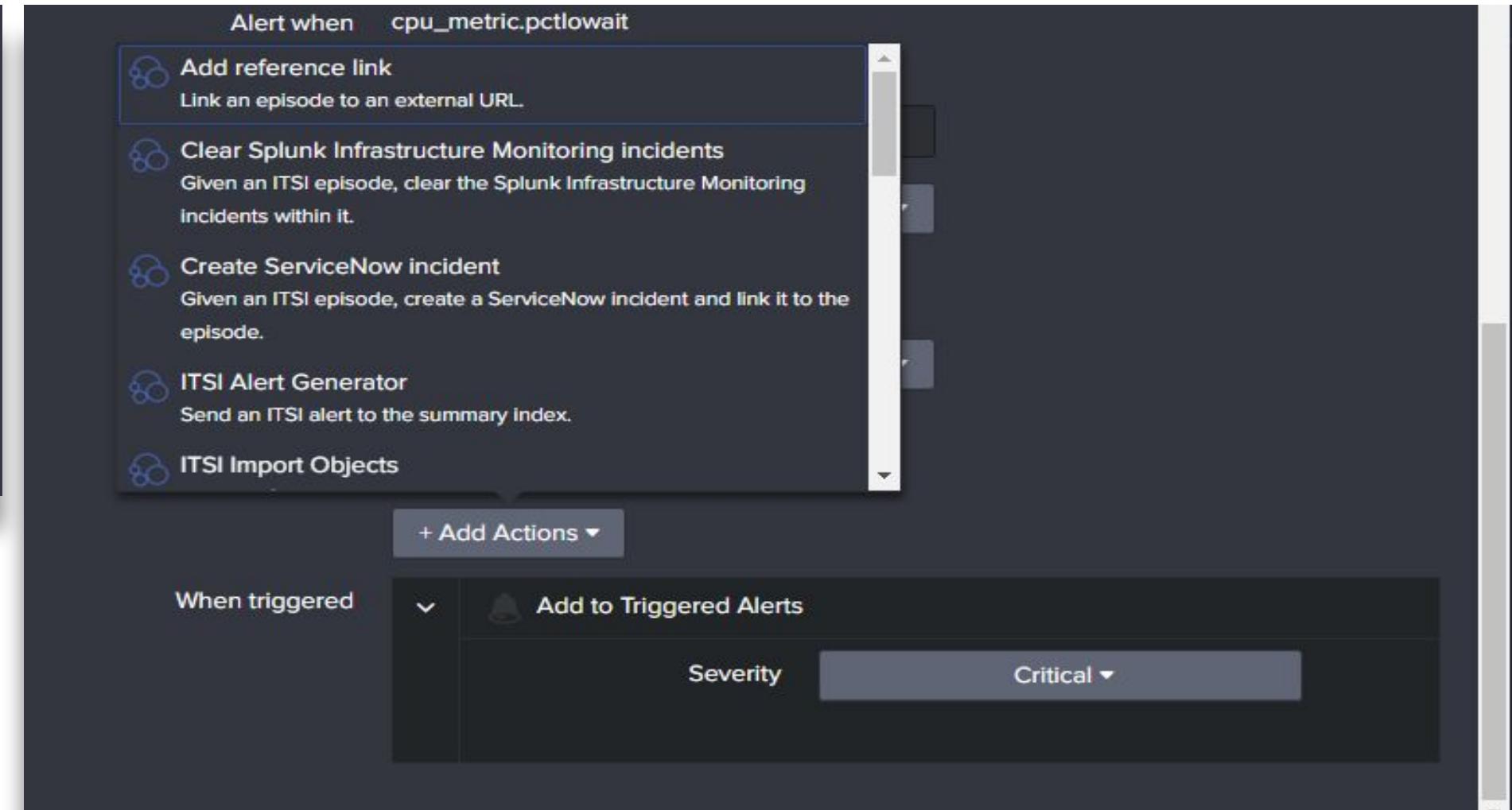
Differences I have noticed between Scheduled and Streaming alerts when creating this workshop

- **Streaming alerts** do not show up in **Settings - Searches, Reports and Alerts**
 - you will need to use the Analytics Workspace to find and edit Streaming alerts
- Out of the box, there seems to be more options under **Add Actions** when creating a **Scheduled Alert**

Streaming Alert options



Scheduled Alert options



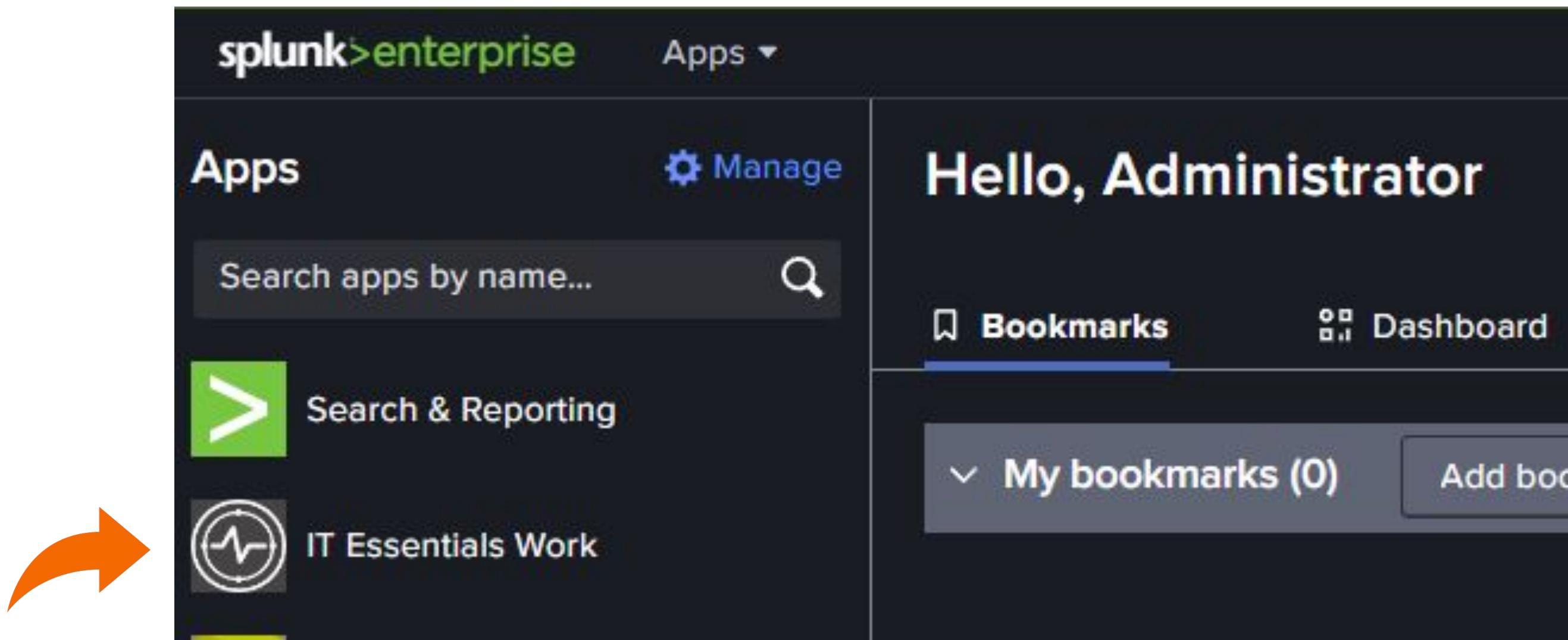
Activity #7

- Exploring IT Essentials Work



Activity #7 - ITE Works

In your browser, navigate again to the IT Essentials Work app



Activity #7 - ITE Works

Entity Overview grouped by entity types

Splunk > enterprise Apps ▾

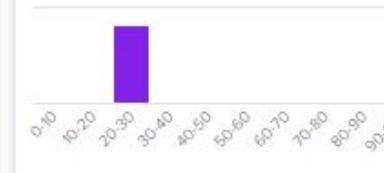
Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Search

Service Analyzer ▾ Entity Overview Alerts and Episodes Glass Tables Deep Dives Dashboards ▾ Configuration ▾ Search

IT Essentials Work

Entity Overview All Status All Severities Search Entity Dimensions Clear all Last 60 minutes Refresh ▾

Group By: Entity Type ▾ Sort By: # of Entities (High to low) ▾ Hide entity types with no entities

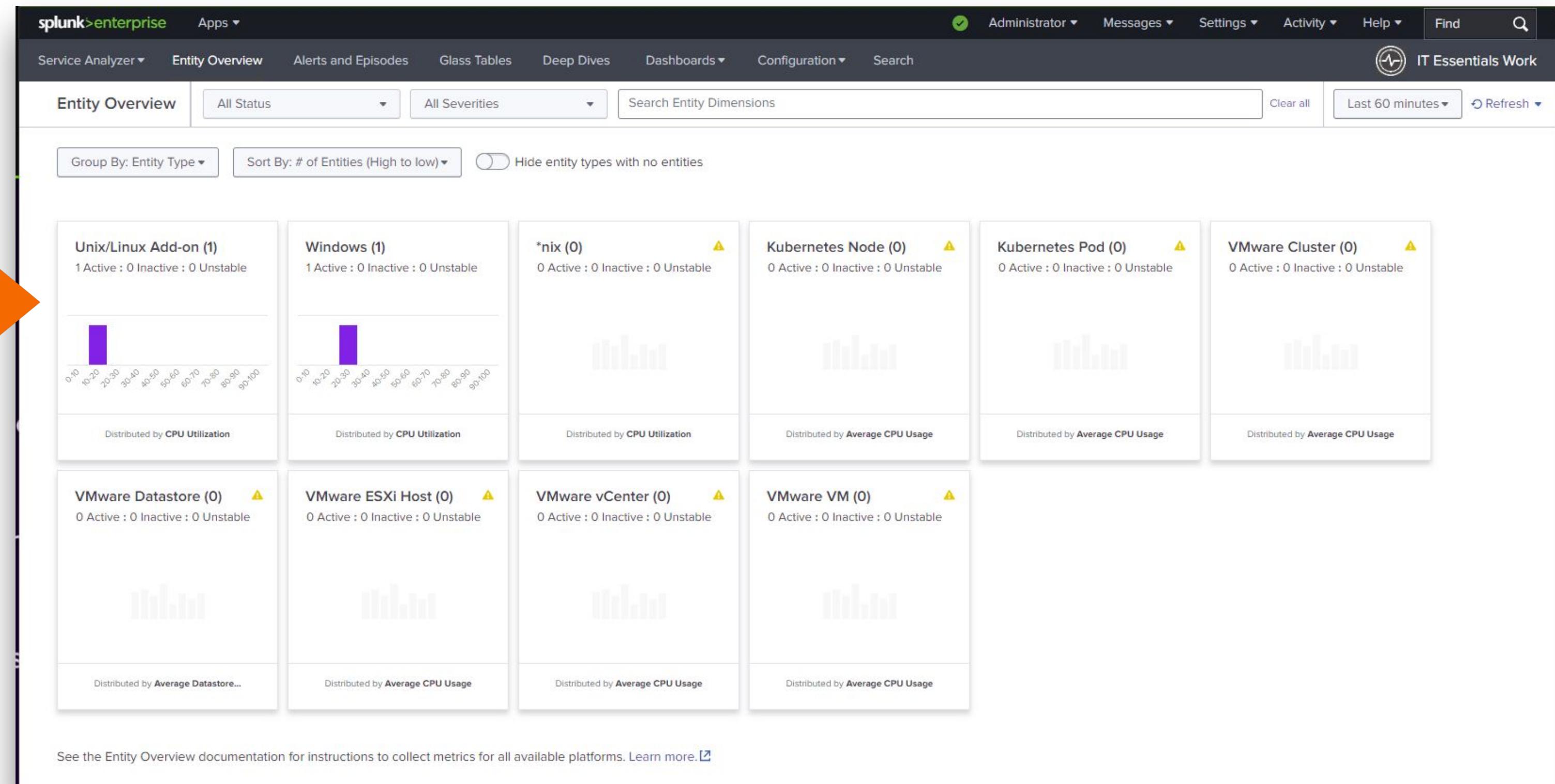
Unix/Linux Add-on (1) 1 Active : 0 Inactive : 0 Unstable  Distributed by CPU Utilization	Windows (1) 1 Active : 0 Inactive : 0 Unstable  Distributed by CPU Utilization	*nix (0) 0 Active : 0 Inactive : 0 Unstable  Distributed by CPU Utilization	Kubernetes Node (0) 0 Active : 0 Inactive : 0 Unstable  Distributed by Average CPU Usage	Kubernetes Pod (0) 0 Active : 0 Inactive : 0 Unstable  Distributed by Average CPU Usage	VMware Cluster (0) 0 Active : 0 Inactive : 0 Unstable  Distributed by Average CPU Usage
VMware Datastore (0) 0 Active : 0 Inactive : 0 Unstable  Distributed by Average Datastore...	VMware ESXi Host (0) 0 Active : 0 Inactive : 0 Unstable  Distributed by Average CPU Usage	VMware vCenter (0) 0 Active : 0 Inactive : 0 Unstable  Distributed by Average CPU Usage	VMware VM (0) 0 Active : 0 Inactive : 0 Unstable  Distributed by Average CPU Usage		

See the Entity Overview documentation for instructions to collect metrics for all available platforms. Learn more.

Activity #7 - ITE Works

Entity Overview

Click the tile:
Unix/Linux Add-on



Activity #7 - ITE Works

After clicking on Unix/Linus Add-on tile you will see all the entities in that section.

Here we can see the current status and the health for each entity.

Review the filter boxes



The screenshot shows the Splunk Enterprise interface with the following details:

- Header:** splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾
- Top Navigation:** Service Analyzer ▾ Entity Overview Alerts and Episodes Glass Tables Deep Dives Dashboards ▾ Configuration ▾ Search IT Essentials Work
- Filter Bar:** All Status ▾ All Severities ▾ Search Entity Dimensions Clear all Last 60 minutes ▾ Refresh ▾
- Entity Health:** Current Entity Status Breakdown (Green circle), CPU Utilization (1.50%), Memory Utilization (8.00%), Disk Utilization (13.00%), Average Network Traffic (3.16 KB/s).
- Entity List:** Showing 1 entity with no alerts filter applied.
 - 1 Active, 0 Unstable, 0 Inactive, 0 N/A
 - 20 per page ▾
- Table Headers:** Entity Name ▾ Status ⓘ Last Updated Dimensions CPU Utilization ▾ Memory Utilization ▾ Disk Utilization ▾ Average Network Traffic ▾
- Table Data:** ip-172-31-42-238 (Active, Wed, 25 Sep 2024, 17:12:03 GMT)
 - Dimensions: host: ip-172-31-42-238, itsi_entity_id: ip-172-31-42-238, ip: 172.31.42.238
 - Metrics: CPU Utilization: 1.50% ↑ 0.49, Memory Utilization: 8.00% 0.00, Disk Utilization: 13.00% 0.00, Average Network Traffic: 3.16 KB/s ↓ -0.26

Click the top Entity Name



Activity #7 - ITE Works

Now you should be taken to Entity Information for the selected entity

The screenshot shows the Splunk Enterprise interface with the following details:

- Header:** splunk>enterprise, Apps ▾, Administrator, Messages, Settings, Activity, Help, Find, Search.
- Breadcrumbs:** Service Analyzer ▾, Entity Overview, Alerts and Episodes, Glass Tables, Deep Dives, Dashboards ▾, Configuration ▾, Search, IT Essentials Work.
- Entity Title:** ip-172-31-42-238 (Active, Wed, 25 Sep 2024 17:22:04 GMT).
- Dashboard:** Unix and Linux Add-on Overview Dashboard.
- Summary Metrics:**
 - CPU Utilization %: 2%
 - Disk Utilization %: 10%
 - Memory Utilization %: 8%
 - Number of Interfaces: 1
- Graphs:** CPU Utilization %, Disk Utilization %, Memory Utilization %, Read/Write by Device (Requests per second).
- Entity Information Panel:**
 - Entity Details:** Entity Title: ip-172-31-42-238, Entity Type: Unix/Linux Add-on.
 - Entity Alias/Info:** host: ip-172-31-42-238, itsi_entity_id: ip-172-31-42-238, ip: 172.31.42.238.
 - Navigation Suggestions:** Your entity has no navigation suggestions. Add external data to display navigation suggestions. Learn more. [Add Navigation Suggestions](#).



Click the X
to close the
information
menu

Activity #7 - ITE Works

With the right informational page closed, we can now see all our options for the top menu.

Click Event Data Search

The screenshot shows the Splunk Enterprise web interface. At the top, there is a dark header bar with various links and a search bar. Below this is a secondary navigation bar with tabs like 'Service Analyzer', 'Entity Overview', 'Alerts and Episodes', 'Glass Tables', 'Deep Dives', 'Dashboards', 'Configuration', and 'Search'. A blue box highlights the 'Event Data Search' tab. An orange arrow points from the text 'Click Event Data Search' down to this tab. The main content area displays a dashboard titled 'Unix and Linux Add-on Overview Dashboard'. On the left, there's a summary section with large numbers: '117,392' (Number of Events) and '2 0'. The main part of the dashboard features two line charts: 'CPU Utilization %' and 'Disk Utilization %'. The CPU chart shows utilization over time for several users, with a legend on the right. The Disk chart shows utilization over time. The bottom of the dashboard has a date and time stamp: '4:40 PM Wed Sep 25 2024'.

Activity #7 - ITE Works

Forgot to adjust admin role to include the nix/wineventlog index to be searchable by default

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Service Analyzer ▾ Entity Overview Alerts and Episodes Glass Tables Deep Dives Dashboards ▾ Configuration ▾ Search

ip-172-31-42-238 Active Wed, 25 Sep 2024 17:22:04 GMT Unix and Linux Add-on Overview Dashboard ▾ Event Data Search Analytics Entity Discovery Searches

No search results found. Learn more. Open in Search

Add this to the search:

New Search

index=*> host="ip-172-31-42-238" OR TERM("host::ip-172-31-42-238")

Matching Searches

index=*> host="ip-172-31-42-238..._entity_id::ip-172-31-42...

Click Open in Search

A new tab should have opened

splunk>
a CISCO company

Activity #7 - ITE Works

Now you should be able to see event data for that entity.

The screenshot shows the Splunk Enterprise search interface. The top navigation bar includes 'splunk>enterprise' and 'Apps ▾'. On the right, there are links for 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', 'Find', and a magnifying glass icon. A 'Service Analyzer' dropdown is open, showing 'Entity Overview', 'Alerts and Episodes', 'Glass Tables', 'Deep Dives', 'Dashboards', 'Configuration', and 'Search'. To the right of these is a circular icon with a heart rate line and the text 'IT Essentials Work'. Below the navigation is a search bar containing the query 'index=* host="ip-172-31-42-238" OR TERM("host::ip-172-31-42-238") OR itsi_entity_id="ip-172-31-42-238" OR TERM("itsi_entity_id::ip-172-31-42-238")' and a dropdown for 'Last 60 minutes'. A green search button is highlighted. The main area is titled 'New Search' with options 'Save As ▾', 'Create Table View', and 'Close'. Below the search bar, it says '✓ 399 events (9/25/24 4:58:00.000 PM to 9/25/24 5:58:19.000 PM)' and 'No Event Sampling ▾'. There are buttons for 'Job ▾', 'Smart Mode ▾', and other search controls. The 'Events (399)' tab is selected, followed by 'Patterns', 'Statistics', and 'Visualization'. A timeline at the bottom shows event counts per minute. The event list table has columns for 'Time' and 'Event'. It shows five events from the specified time range. The first event is a cron session closed for user root. The second is a cron command run. The third is a pam_unix session opened for user root. The fourth is an SSM connection message. The fifth is an ECSIdentity agent metadata fetch error. The left sidebar lists 'SELECTED FIELDS' (host 1, source 3, sourcetype 2) and 'INTERESTING FIELDS' (date_hour 2, date_mday 1, date_minute 33, date_month 1, date_second 19, date_wday 1, date_year 1).

Time	Event
Sep 25 17:55:01 5:55:01.000 PM	Sep 25 17:55:01 ip-172-31-42-238 CRON[283301]: pam_unix(cron:session): session closed for user root host = ip-172-31-42-238 source = /var/log/auth.log sourcetype = syslog
Sep 25 17:55:01 5:55:01.000 PM	Sep 25 17:55:01 ip-172-31-42-238 CRON[283302]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1) host = ip-172-31-42-238 source = /var/log/syslog sourcetype = syslog
Sep 25 17:55:01 5:55:01.000 PM	Sep 25 17:55:01 ip-172-31-42-238 CRON[283301]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0) host = ip-172-31-42-238 source = /var/log/auth.log sourcetype = syslog
Sep 25 17:54:47.104 5:54:47.104 PM	2024-09-25 17:54:47.1042 INFO [ssm-agent-worker] [HealthCheck] got SSM connection channel value: ssmmessages host = ip-172-31-42-238 source = /var/log/amazon/ssm/amazon-ssm-agent.log sourcetype = amazon-ssm-agent
Sep 25 17:54:47.103 5:54:47.103 PM	2024-09-25 17:54:47.1031 INFO [ECSIdentity] Agent not taking ECS identity: Could not fetch metadata endpoint host = ip-172-31-42-238 source = /var/log/amazon/ssm/amazon-ssm-agent.log sourcetype = amazon-ssm-agent

Activity #7 - ITE Works

Now go back to the first tab or close that tab.

Click Analytics

The screenshot shows the Splunk Enterprise web interface. At the top, there is a dark header bar with the 'splunk>enterprise' logo, a 'Find' search bar, and several navigation links: 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a magnifying glass icon. Below the header is a secondary navigation bar with links: 'Service Analyzer', 'Entity Overview', 'Alerts and Episodes', 'Glass Tables', 'Deep Dives', 'Dashboards', 'Configuration', and 'Search'. A blue box highlights the 'Configuration' link. An orange arrow points from the text above to this blue box. On the left side of the main content area, there is a sidebar with a timestamp 'Sep 2024 17:22:04' and a status indicator 'Active'. The main content area displays a dashboard titled 'Unix and Linux Add-on Overview Dashboard'. At the bottom of the interface, there are various search and refresh controls.

Activity #7 - ITE Works

This should look familiar and is similar to the Analytics Workspace, except it will only show data for the entity you selected.

The screenshot shows the Splunk Enterprise interface with the following details:

- Top Bar:** splunk>enterprise, Apps, Administrator (logged in), Messages, Settings, Activity, Help, Find, Search icon.
- Secondary Navigation:** Service Analyzer, Entity Overview, Alerts and Episodes, Glass Tables, Deep Dives, Dashboards, Configuration, Search, IT Essentials Work (selected).
- Entity Information:** ip-172-31-42-238, Active, Wed, 25 Sep 2024 17:22:04 GMT.
- Dashboard Title:** Unix and Linux Add-on Overview Dashboard.
- Analytics Tab:** Event Data Search, Analytics (selected), Entity Discovery Searches.
- Left Sidebar:** Find Data to Analyze, Metrics section with options: + Add new filter, cpu_metric, df_metric, interfaces_metric, iostat_metric, ps_metric, spl.mlog, vmstat_metric.
- Central Area:** Start by selecting data. Find something interesting? Save it to a dashboard, or create an alert.

Activity #7 - ITE Works

Click Entity Discover Searches

The screenshot shows the Splunk Enterprise web interface. At the top, there is a dark header bar with the 'splunk>enterprise' logo, user authentication information ('Administrator'), and various navigation links like 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. A magnifying glass icon is also present. Below the header is a secondary navigation bar with links for 'Service Analyzer', 'Entity Overview', 'Alerts and Episodes', 'Glass Tables', 'Deep Dives', 'Dashboards', 'Configuration', and 'Search'. On the far right of this bar is an 'IT Essentials Work' icon. In the bottom left corner, there is a status message for IP '172-31-42-' indicating it is 'Active' since 'Sep 2024 17:22:04'. The main content area features a dashboard titled 'Unix and Linux Add-on Overview Dashboard' which is currently selected. Other visible dashboard cards include 'Event Data Search', 'Analytics', and 'Entity Discovery Searches'. A blue box highlights the 'Entity Discovery Searches' card. To the right of the dashboard cards are filters for time ('Last 1 hour') and refresh ('Refresh'). An orange curved arrow points from the text 'Click Entity Discover Searches' down to the 'Entity Discovery Searches' link in the bottom navigation bar.

Activity #7 - ITE Works

Entity Discovery Search allows you to identify which searches are discovering entities

The screenshot shows the Splunk interface with the following details:

- Top Navigation Bar:** Service Analyzer, Entity Overview, Alerts and Episodes, Glass Tables, Deep Dives, Dashboards, Configuration, Search, and IT Essentials Work.
- Header:** ip-172-31-42-238, Active, Wed, 25 Sep 2024 17:22:04 GMT, Unix and Linux Add-on Overview Dashboard, Event Data Search, Analytics, Entity Discovery Searches (underlined), and a refresh icon.
- Left Sidebar:** Shows a table with columns: Saved search title, Last executed, Entity status last marked active, Search active?, and Tracks status. One entry is listed: "ITSI Import Objects - TA *Nix" (last executed 0 minutes ago, entity status last marked active 0 minutes ago, search active, tracks status active).
- Main Content Area:**
 - Section:** ITSI Import Objects - TA *Nix **Configure search**
 - Entity status last marked active:** 0 minutes ago
 - Number of entities discovered:** 1
 - Search active?**: Yes
 - Tracks status?**: Yes
 - SPL QUERY:**

```
1 | mcatalog values("host") as "dimension.identifier.host"
2 [ mcatalog values(_dims) as info where metric_name=*_metric.* AND
('itsi_entity_type_ta_nix_metrics_indexes') earliest=-90s
```

Activity #8

- Find what caused the alert**



Activity #8 - Find what caused the alert

How do you identify the root cause when a **Max CPU alert** is triggered?

The screenshot shows the Splunk Triggered Alerts interface. At the top, there's a navigation bar with links for Admin..., Messages, Settings, Activity, Help, and a Find button with a magnifying glass icon. Below the navigation is a dark header bar with the title "Triggered Alerts" and a green checkmark icon. On the left, there's a "Filter" section with dropdown menus for App (set to "Search & Reporting (search)"), Owner (All owners), Severity (All severity), Alert name (All alerts), and a search bar with a magnifying glass icon. To the right of the filter, it says "Showing 1 - 1 of 1 results". The main area is a table with columns: Time, Alert name, App, Type, Severity, Mode, and Actions. A single alert is listed:

Time	Alert name	App	Type	Severity	Mode	Actions
2024-10-07 17:48:22 UTC	Max CPU alert	search	Streaming	High	Digest	Delete

Activity #8 - Find what caused the alert

Take this time to see if you can figure out what process is causing the CPU spikes.

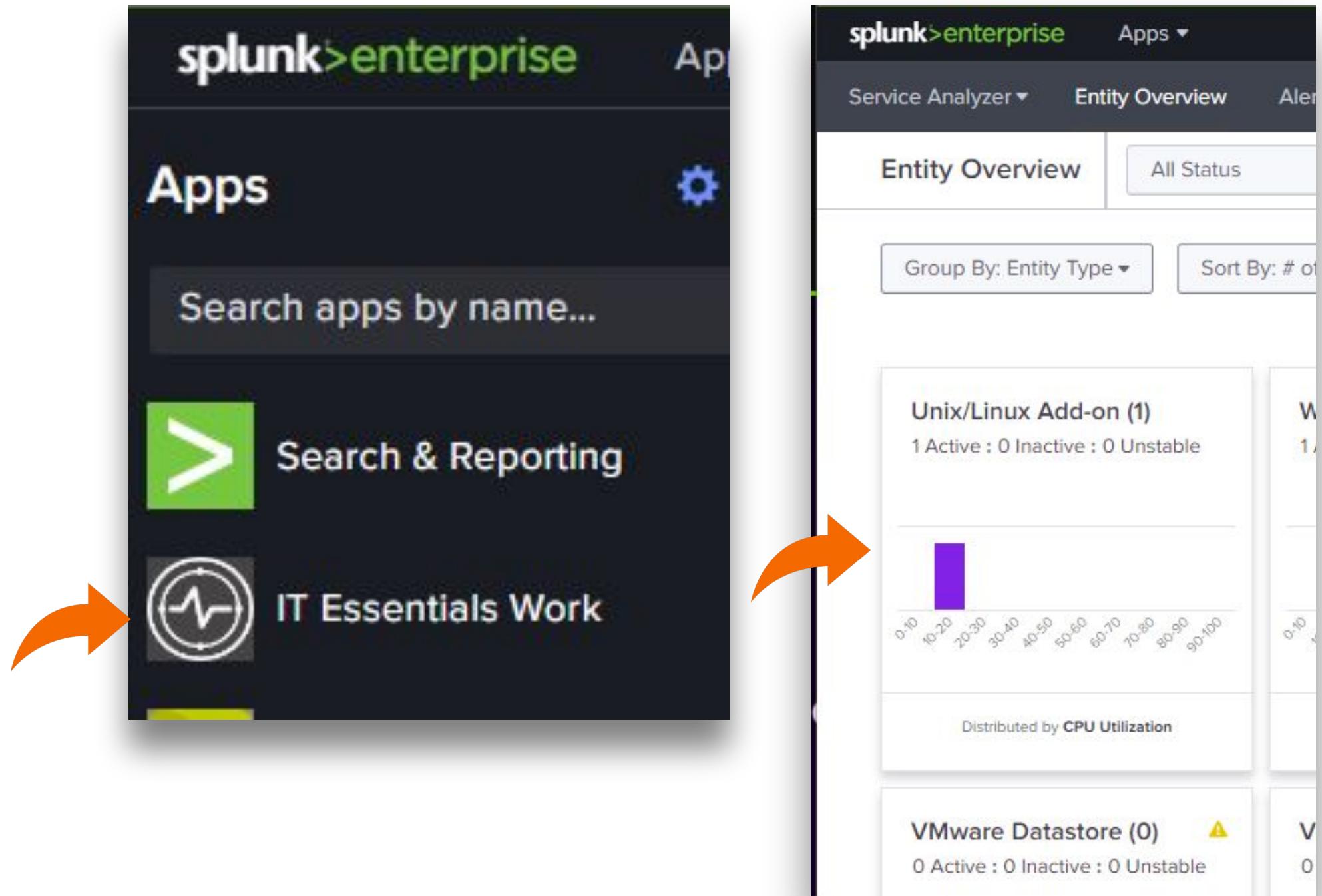


Did anyone find what triggered the alert?

The following slides will go into one method of finding the root cause

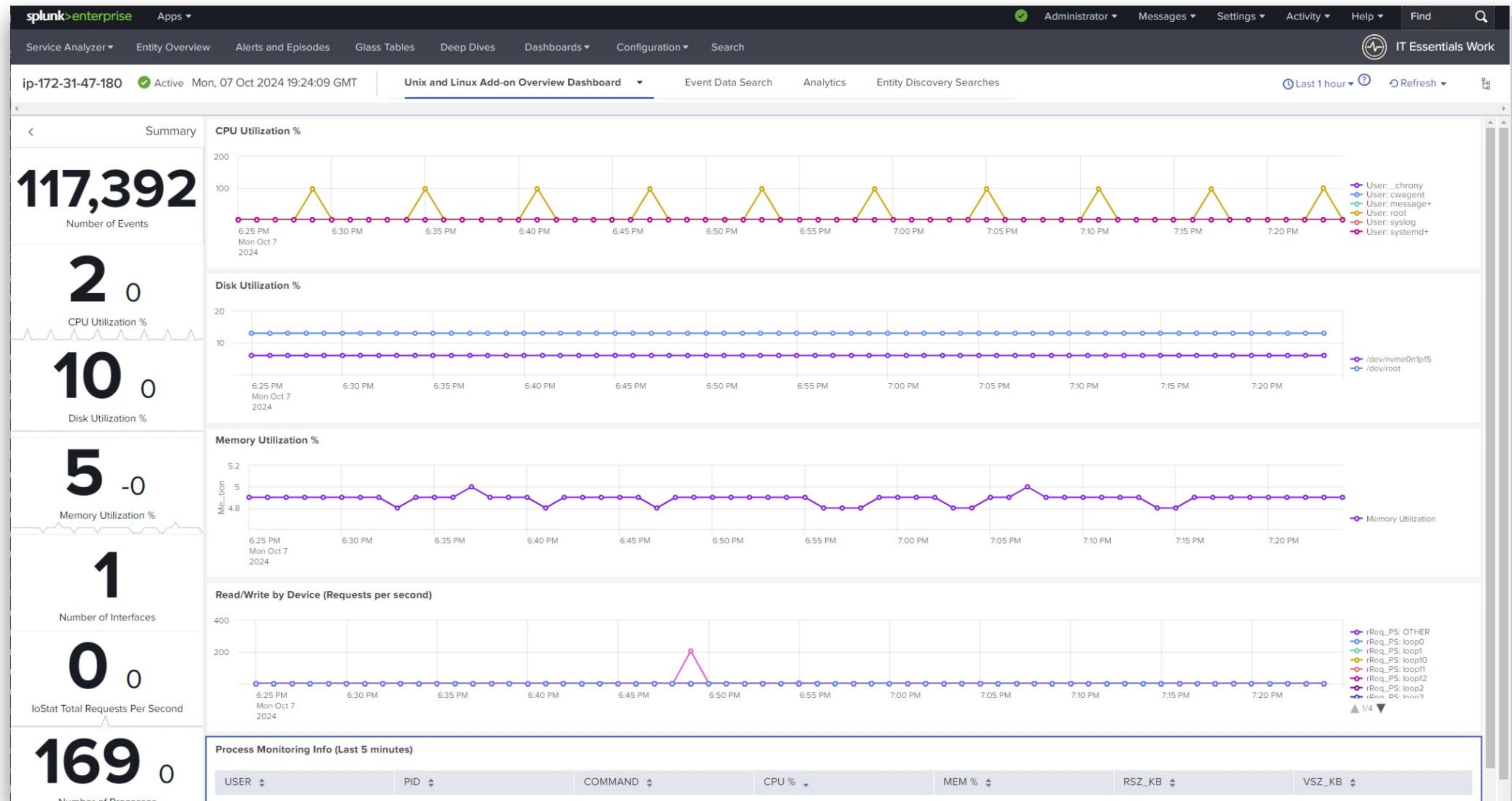
Activity #8 - Find what caused the alert

Lets jump back into **IT Essentials Work** and look at the Unix box with the CPU spikes



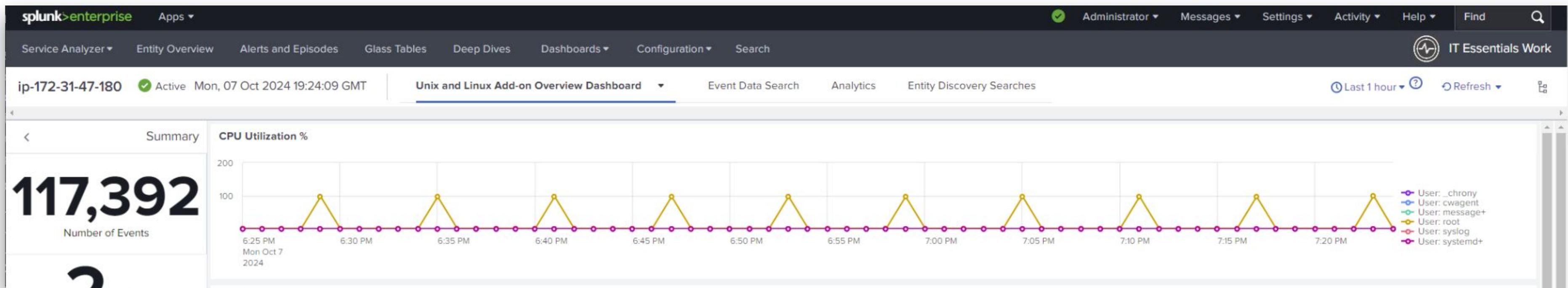
Activity #8 - Find what caused the alert

Now we can see the pre-built dashboard for that entity

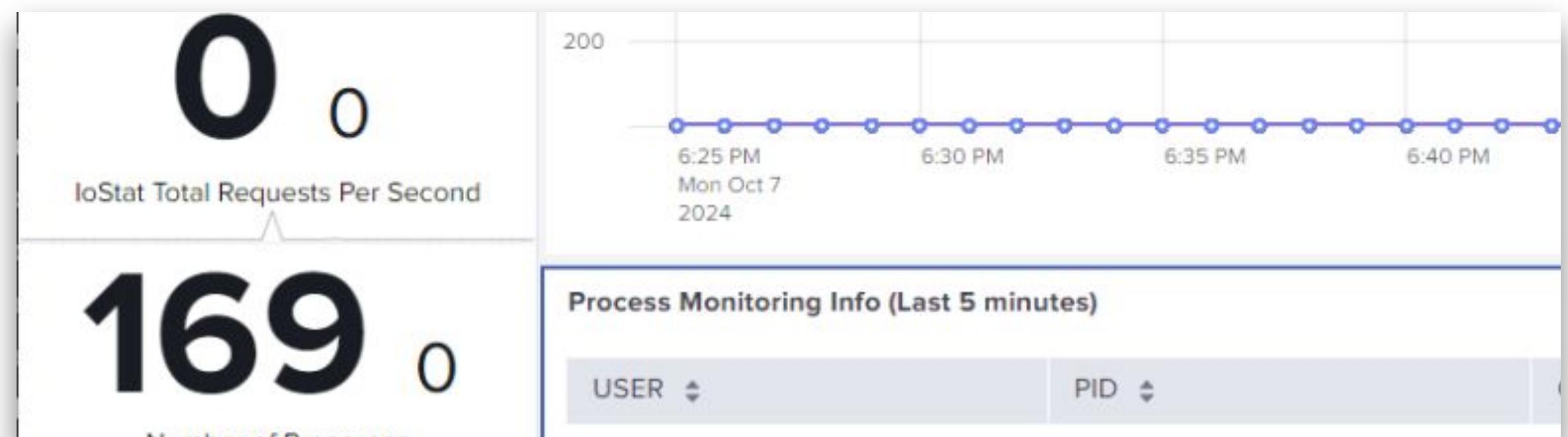


Activity #8 - Find what caused the alert

The top panel shows the CPU Utilization spikes



Did you notice the last panel for
Process Monitoring Info



Activity #8 - Find what caused the alert

Lets sort by **CPU %** and bring the highest value to the top

Process Monitoring Info (Last 5 minutes)

USER	PID	COMMAND	CPU %	MEM %	RSZ_KB	VSZ_KB
_chrony	581	/usr/sbin/chronyd	0	0	3484	18892
_chrony	626	/usr/sbin/chronyd	0	0	1988	10564
cwagent	3288	/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-	0.1	0.5	85320	1348680

< Prev 1 2 3 4 5 ... Next >

Once sorted we can see
stress-ng-cpu
command at the top of the list.

Process Monitoring Info (Last 5 minutes)

USER	PID	COMMAND	CPU %
root	123260	stress-ng-cpu	100
root	339	falcon-sensor-bpf	1.3
root	587	/usr/sbin/collectd	0.2

Activity #8 - Find what caused the alert

Stress-ng is a tool that will stress test a computer system in various selectable ways

If you run the following search you can see the event:

```
| mpreview index=itsi_im_metrics  
| search stress-ng-cpu
```

And if you replace **stress-ng-cpu** with **stress-ng***

You will find an event that has the arguments used in the shell script written to perform the test for 60 seconds.

Yes, I am running this command as **root**

New Search			
mpreview index=itsi_im_metrics search stress-ng-cpu			
✓ 48 events (10/6/24 8:00:00.000 PM to 10/7/24 8:15:15.000 PM) No Event Sampling ▾			
Events (48)	Patterns	Statistics	Visualization
Format Timeline ▾	– Zoom Out	+ Zoom to Selection	✗ Deselect
List ▾ ✓ Format 20 Per Page ▾			
◀ Hide Fields	>All Fields	i	Time
SELECTED FIELDS		i	Event
<i>a host</i> 1		>	10/7/24 6:41:19.000 PM { [-] ARGs: [run] COMMAND: stress-ng-cpu CPUTIME: 0:38 IP_address: 172.31.47.180 OSName: Ubuntu OS_name: Ubuntu OS_version: 22.04 PID: 100499 START: 18:40 STAT: R TTY: ? USER: root entity_type: TA_Nix metric_name:ps_metric.CPU: 97.7 metric_name:ps_metric.MEM: 0 metric_name:ps_metric.RSS: 5724 metric_name:ps_metric.RSZ_KB: 5724 metric_name:ps_metric.VSZ: 76264 metric_name:ps_metric.VSZ_KB: 76264 metric_name:ps_metric.pctCPU: 97.7 metric_name:ps_metric.pctMEM: 0
<i>a source</i> 1			
<i>a sourcetype</i> 1			
INTERESTING FIELDS			
<i>a ARGs</i> 1			
<i>a COMMAND</i> 1			
<i>a CPUTIME</i> 1			
<i>a entity_type</i> 1			
<i>a IP_address</i> 1			
# metric_name:ps_metric.CPU 3			
# metric_name:ps_metric.MEM 1			
# metric_name:ps_metric.pctCPU 3			
# metric_name:ps_metric.pctMEM 1			
# metric_name:ps_metric.RSS 5			
# metric_name:ps_metric.RSZ_KB 5			
# metric_name:ps_metric.VSZ 1			
# metric_name:ps_metric.VSZ_KB 1			
<i>a OS_name</i> 1			
# OS_version 1			
<i>a OSName</i> 1			
# PID 48			

Where do we go from here?



Splunk IT Service Intelligence

KPI-driven, predictive analytics solution for digital services

- Mission & service monitoring
 - Intelligent incident management
 - Machine learning & predictive analytics



**Crushing
metrics,
one
workshop
at a time!**



splunk>
a CISCO company

Thank You