Metrics Onboarding Workshop for IT Ops

splunk>
a CISCO company

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> a CISCO company

splunk>

Presenter Name

Job Title

splunk>

Meet Your Presenters!

Presenter Name

Job Title

Presenter Name

Job Title

Please introduce yourself!

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

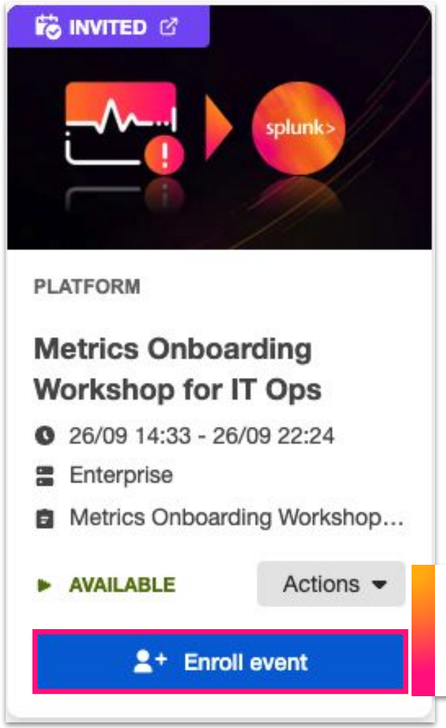
Enroll in Today's Workshop

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



Enroll in today's event

What Are Metrics?

splunk> a CISCO company

Difference Between Metrics and Events

Metrics

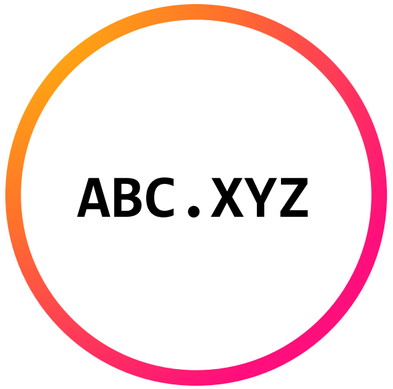
- Predict and/or discover “what is happening?”
- Typically know what you want to measure
- Structured data
- Numerical in nature
- Best way to monitor a process or device over time
    - CPU, memory, network latency, disk usage

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

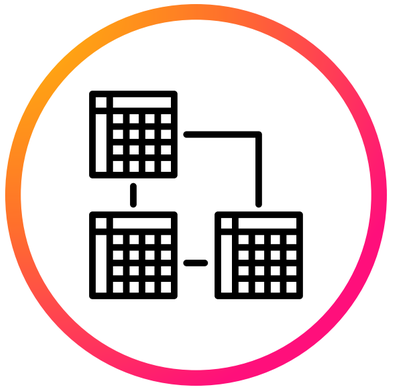


Metric Name

`system.cpu.idle`

Measure

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



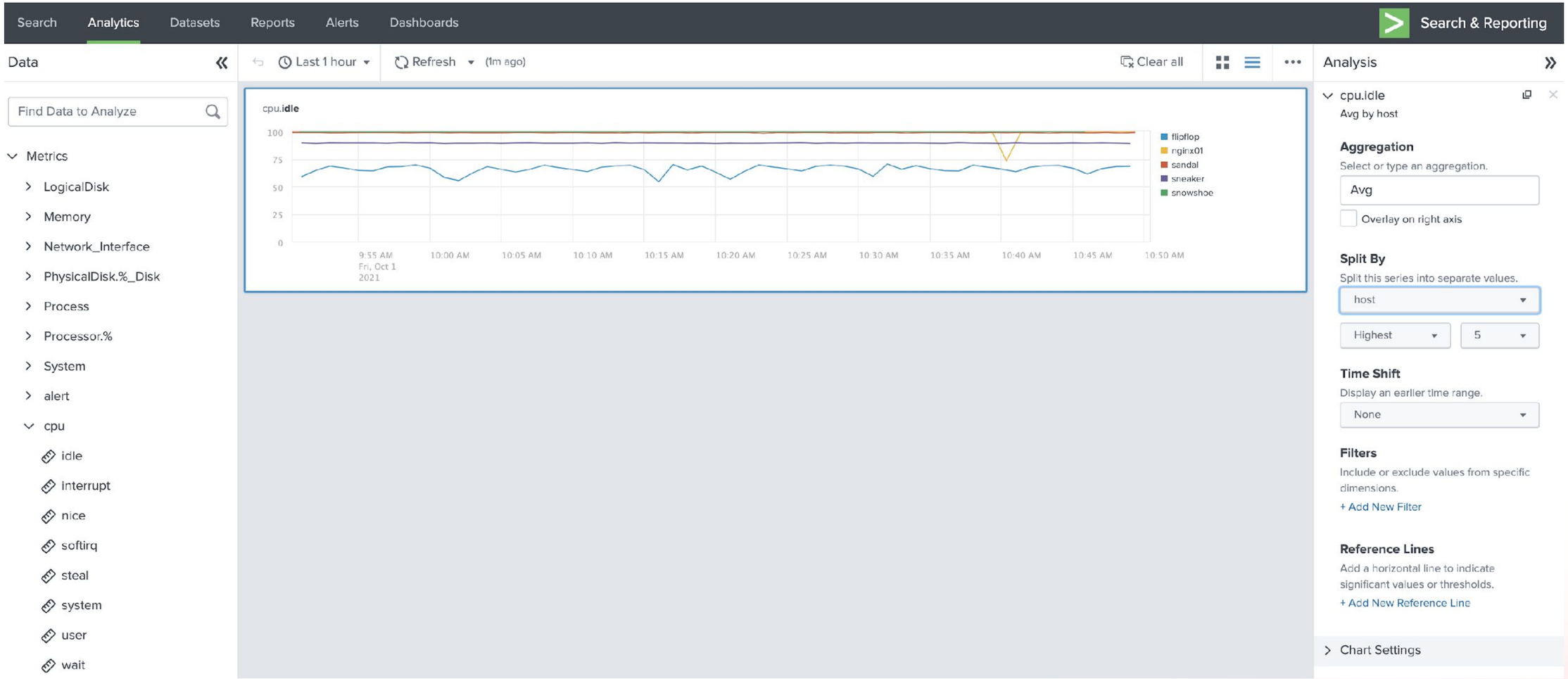
Dimensions

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

How Do I Use Metrics?

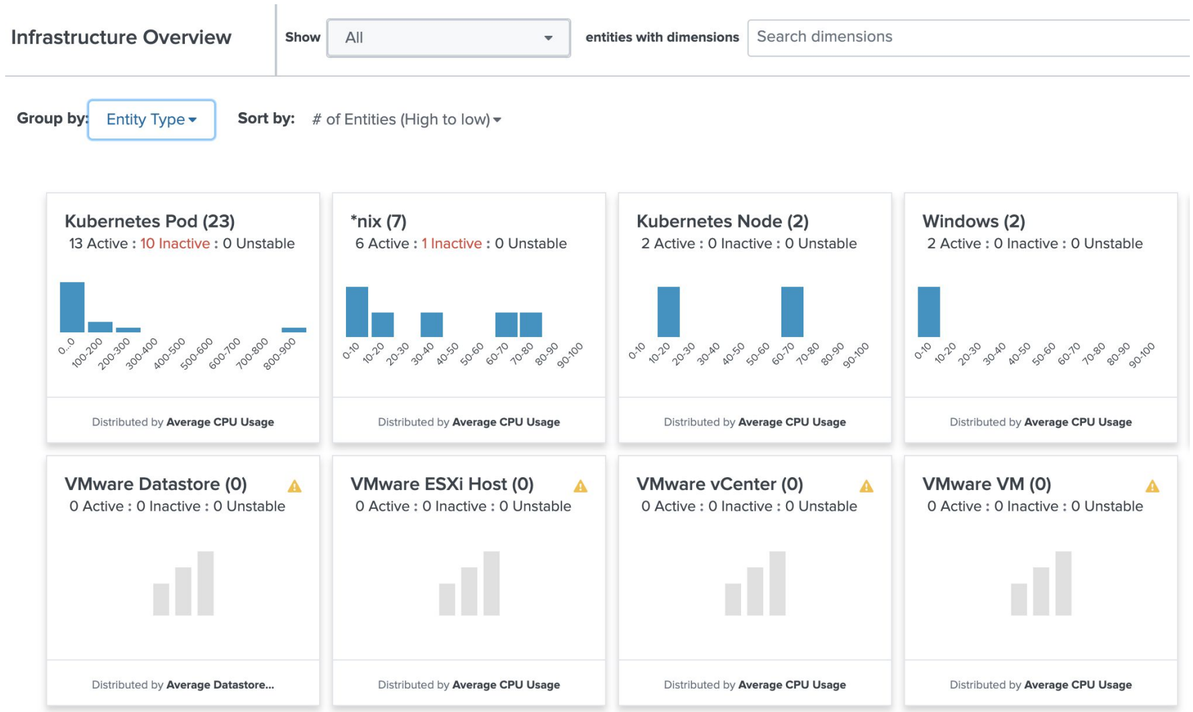
splunk> a CISCO company

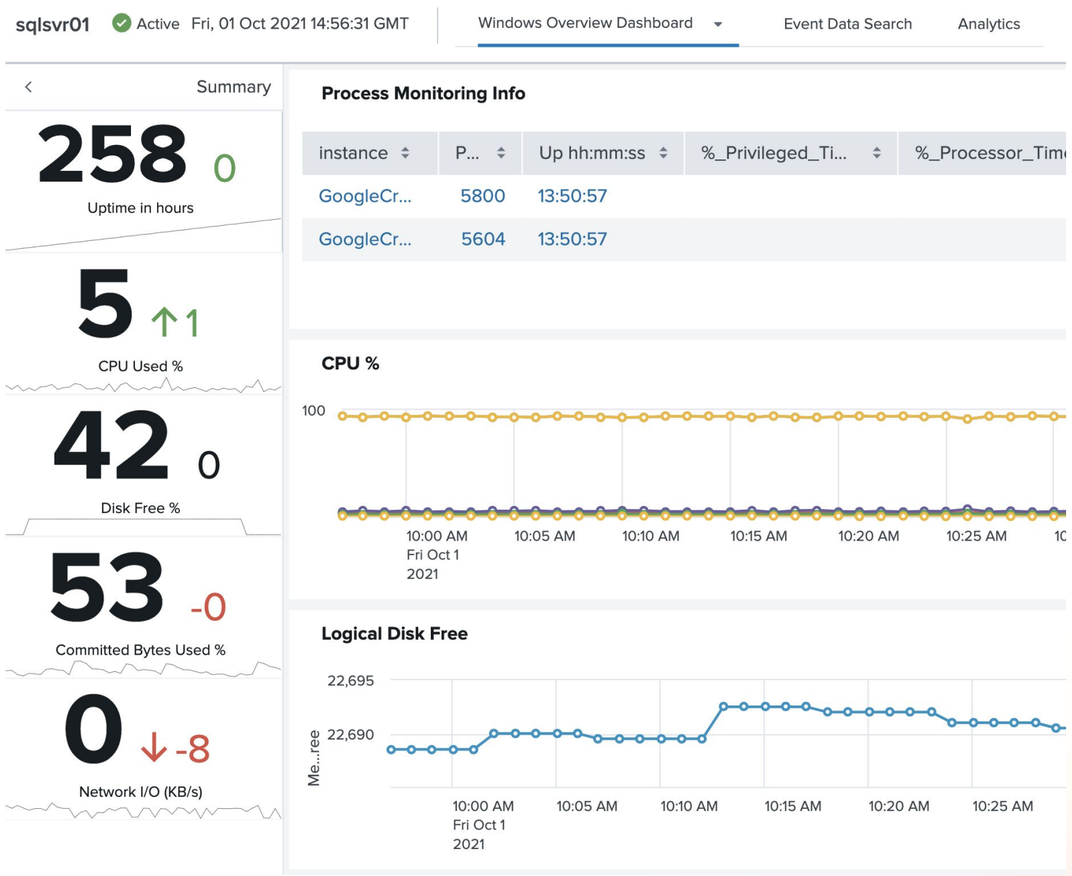
Metrics Analytics Workspace



splunk>
a cisco company

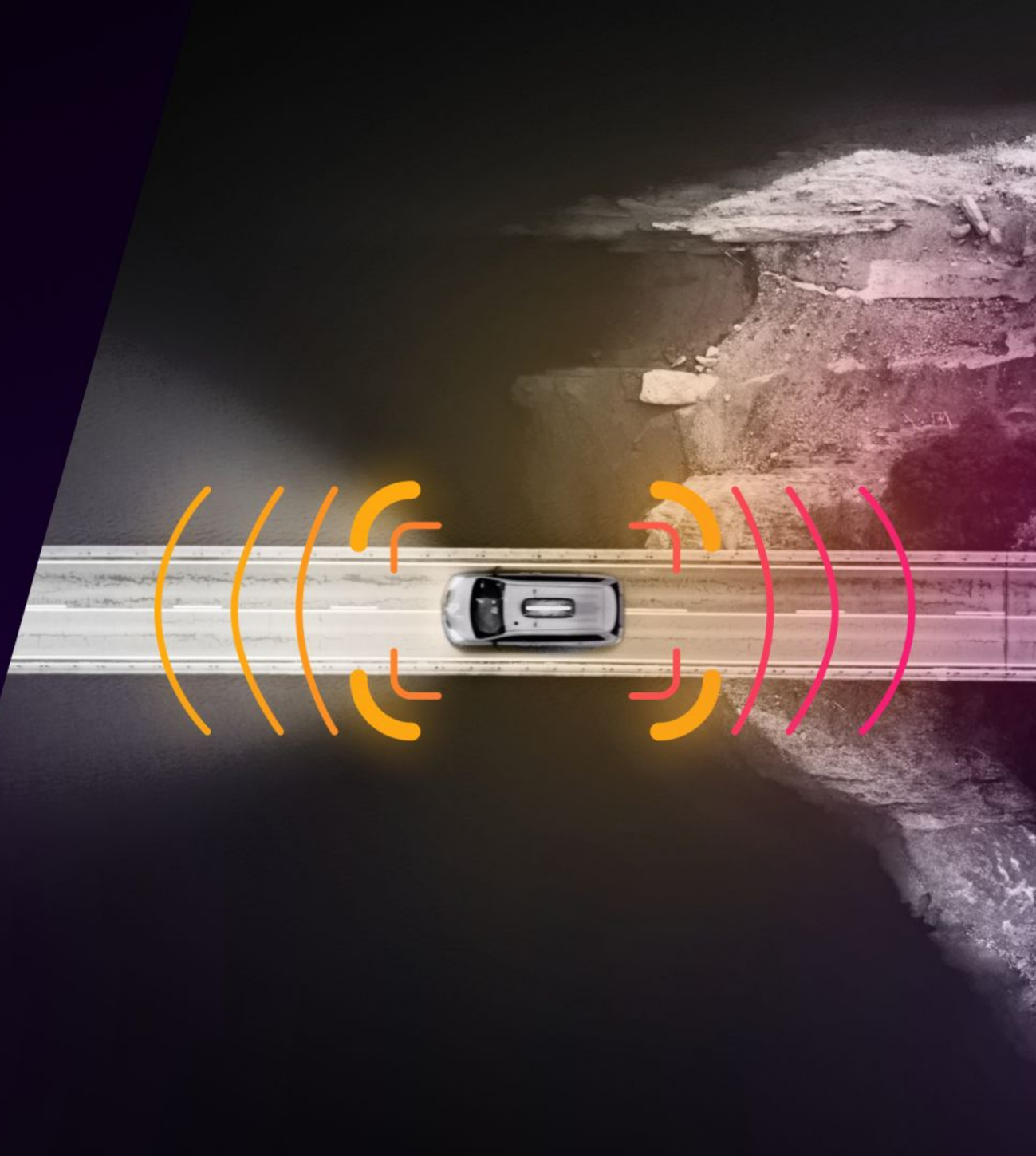
IT Essentials Work & IT Service Intelligence





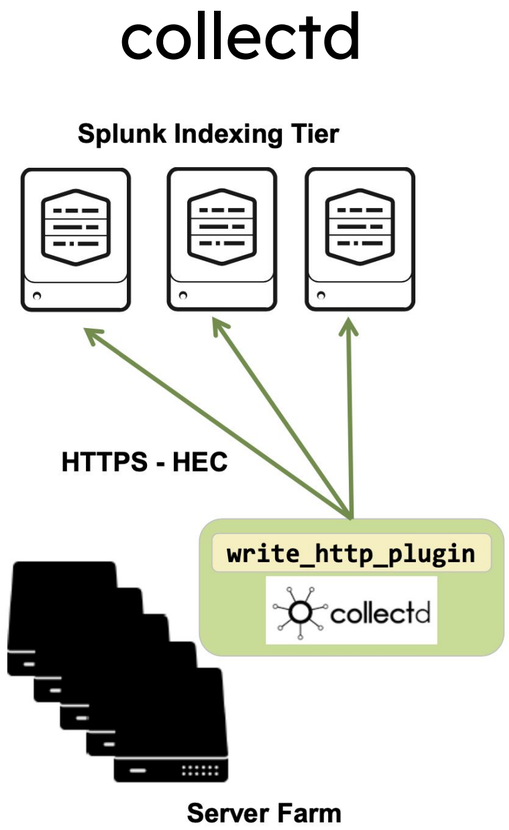
splunk>
a cisco company

How Do I Get Metrics In?



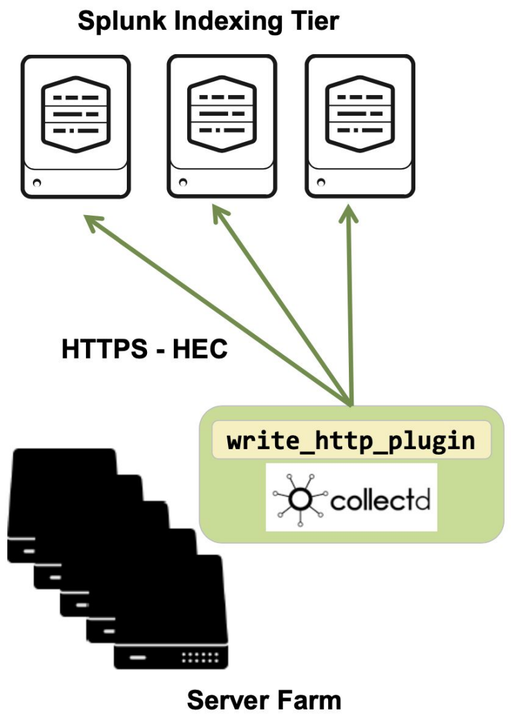
splunk>
a CISCO company

Gathering Metrics for IT Monitoring



Gathering Metrics for IT Monitoring

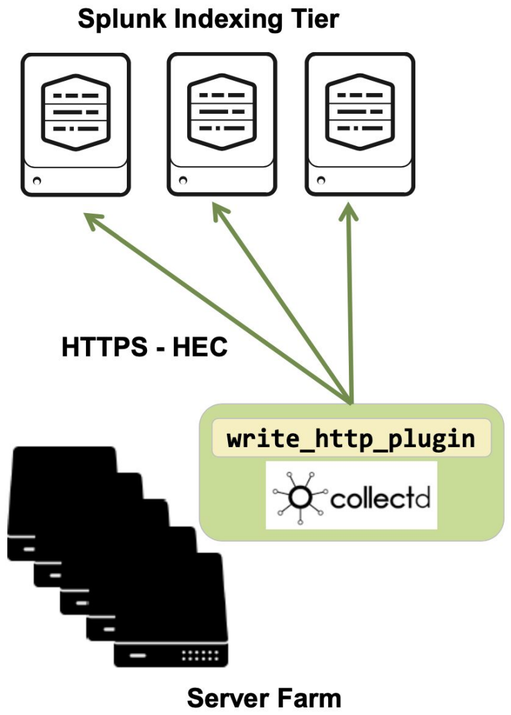
collectd



or…

Gathering Metrics for IT Monitoring

collectd



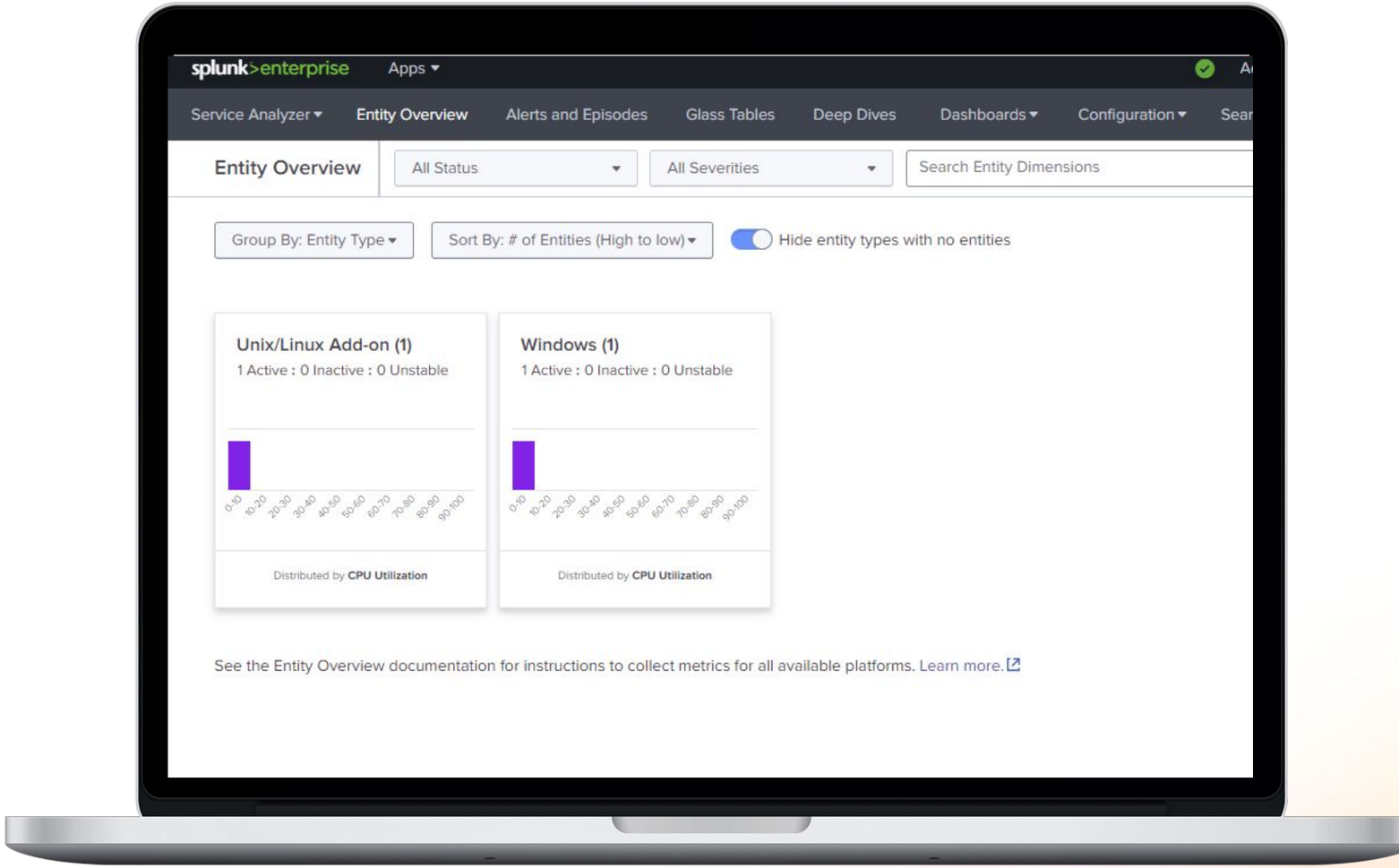
or…

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



splunk>
a cisco company

Activity #1
- current state

splunk>
a CISCO company

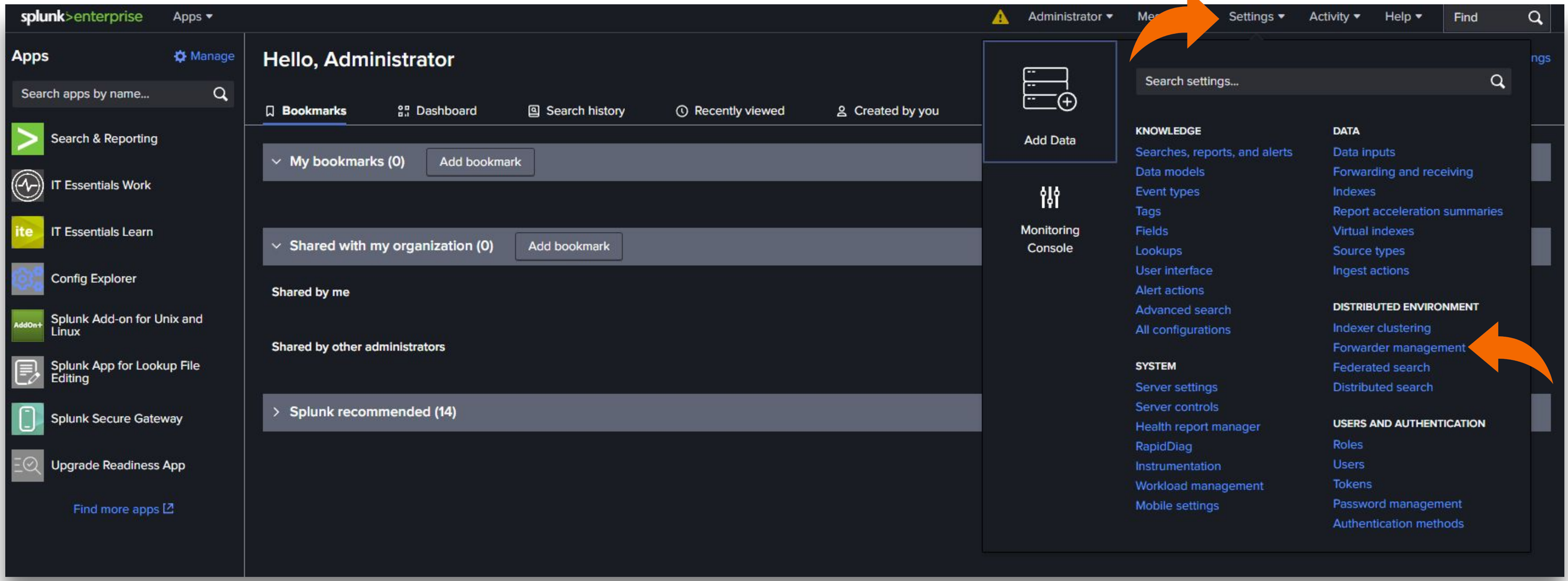
Activity #1 - Splunk Login

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

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

Activity #1 - Current state

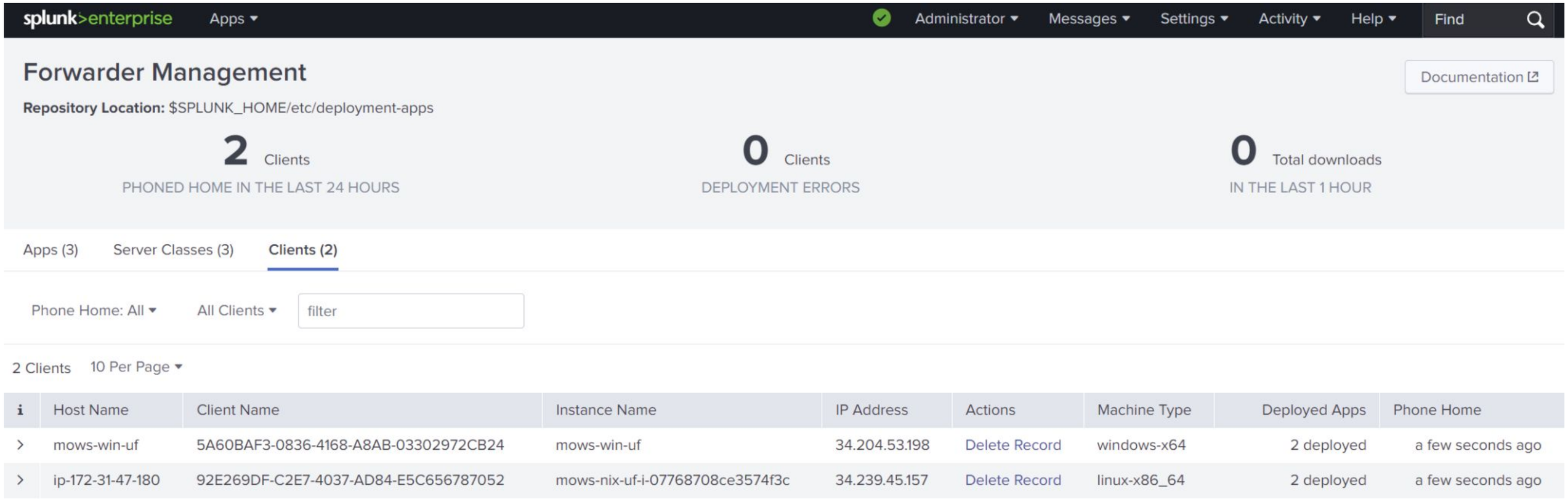
Navigate to Settings - Forwarder management



splunk>
a cisco company

Activity #1 - Forwarder Management

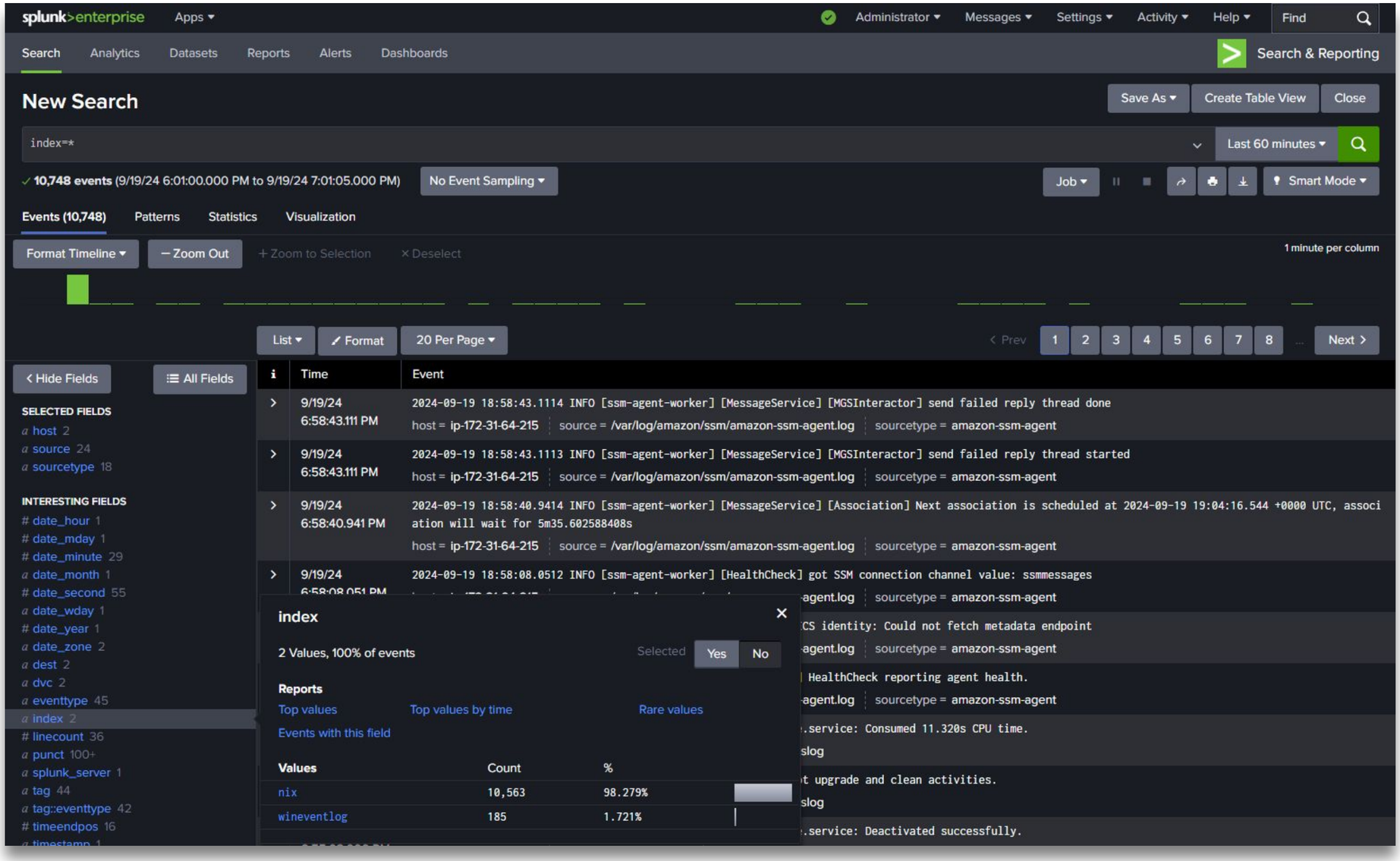
Verify that you have 2 systems **phoning home** to the deployment server.



Activity #1 - What data is present?

1. Navigate to the Search & Reporting app

2. Search for `index=*` over the **Last 60 minutes**.



splunk>
a cisco company

Activity #1 - IT Essentials Work Install

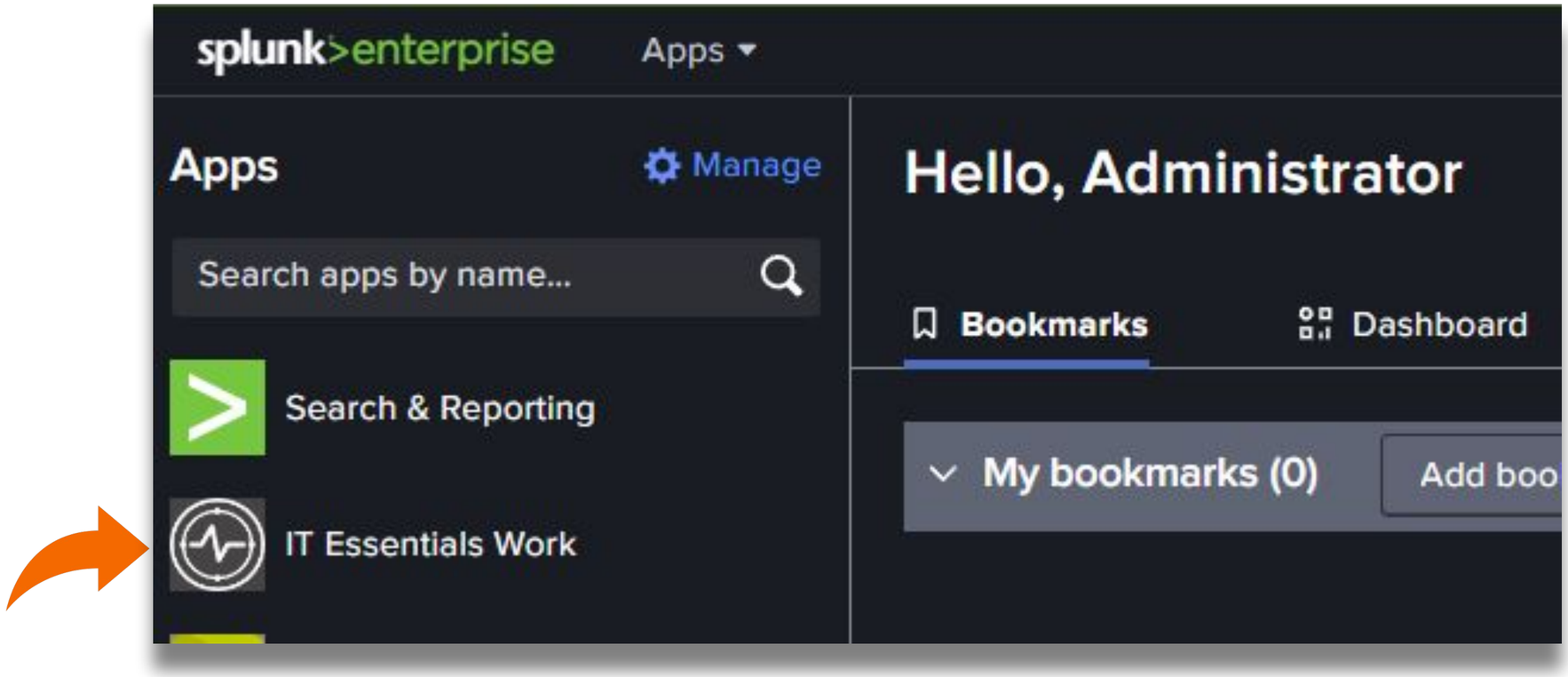
At this time, you can't install Splunk IT Essentials Work from the Splunk Web interface.

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

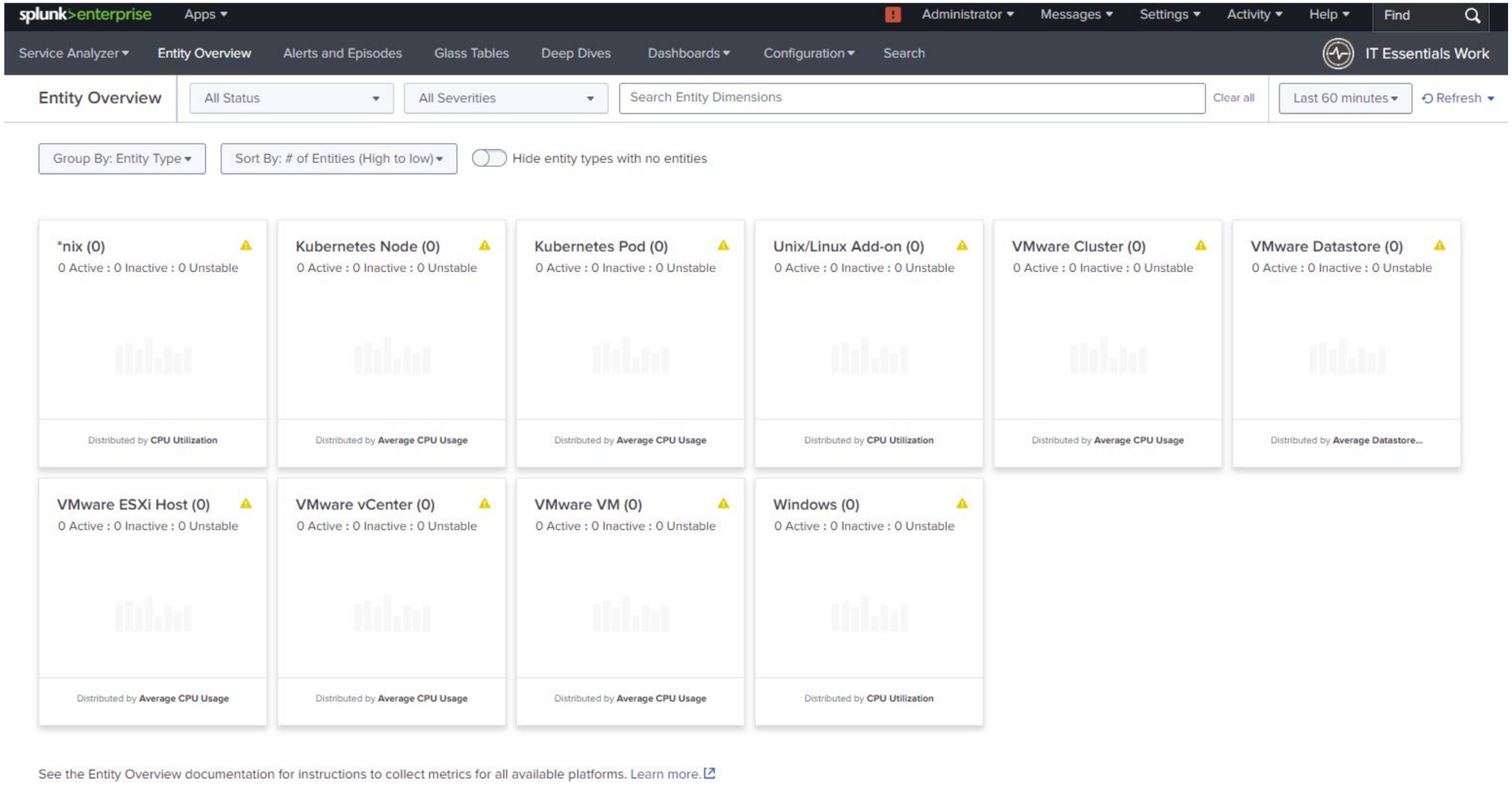
Navigate to the IT Essentials Work app



splunk>
a cisco company

Activity #1 - Entity Overview

Verify that there are no entities found



splunk>
a cisco company

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> a cisco company

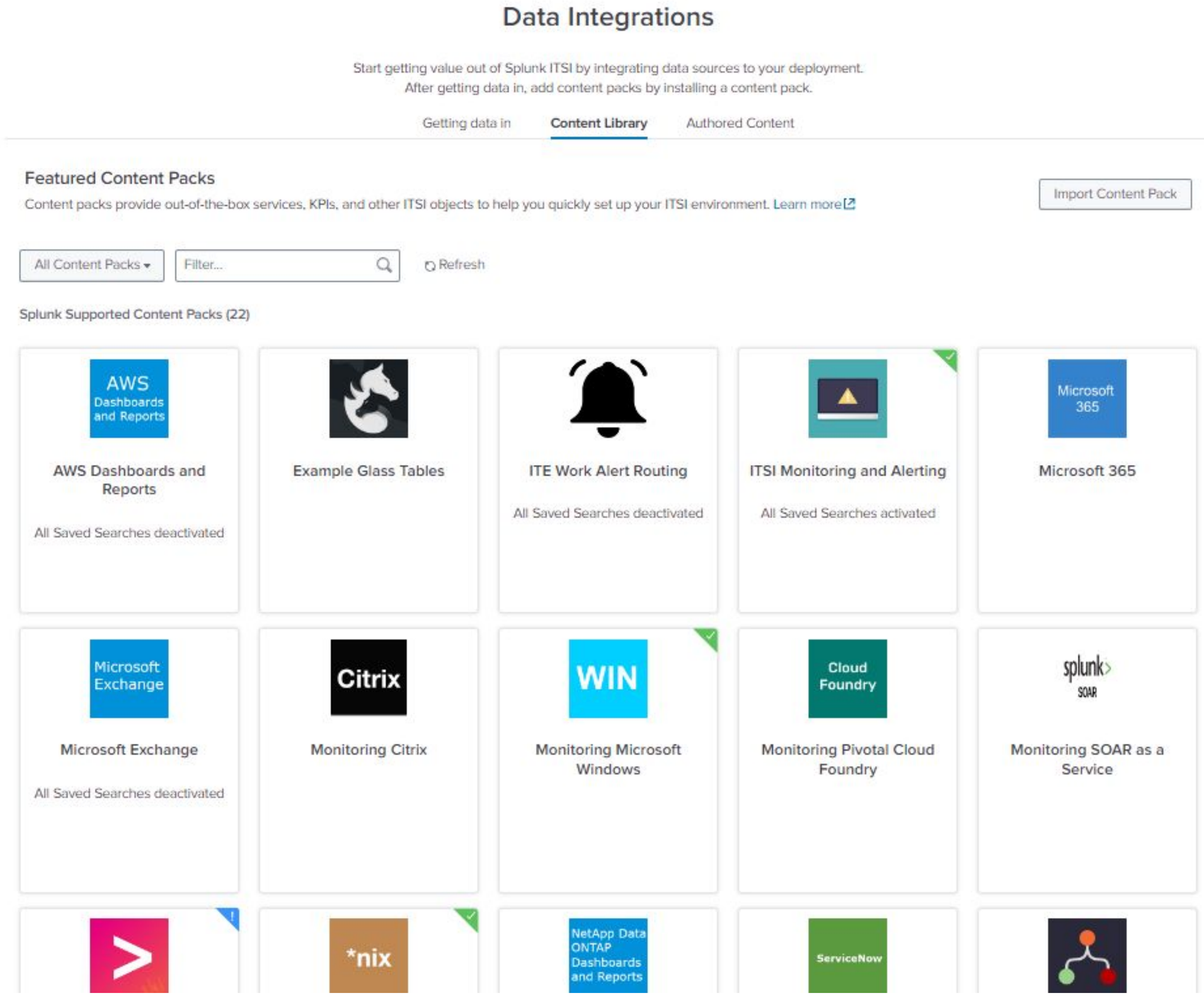
Splunk App for Content Packs

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



splunk>
a cisco company

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

splunk>
a CISCO company

Activity #2 - Accessing the Splunk Indexer

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

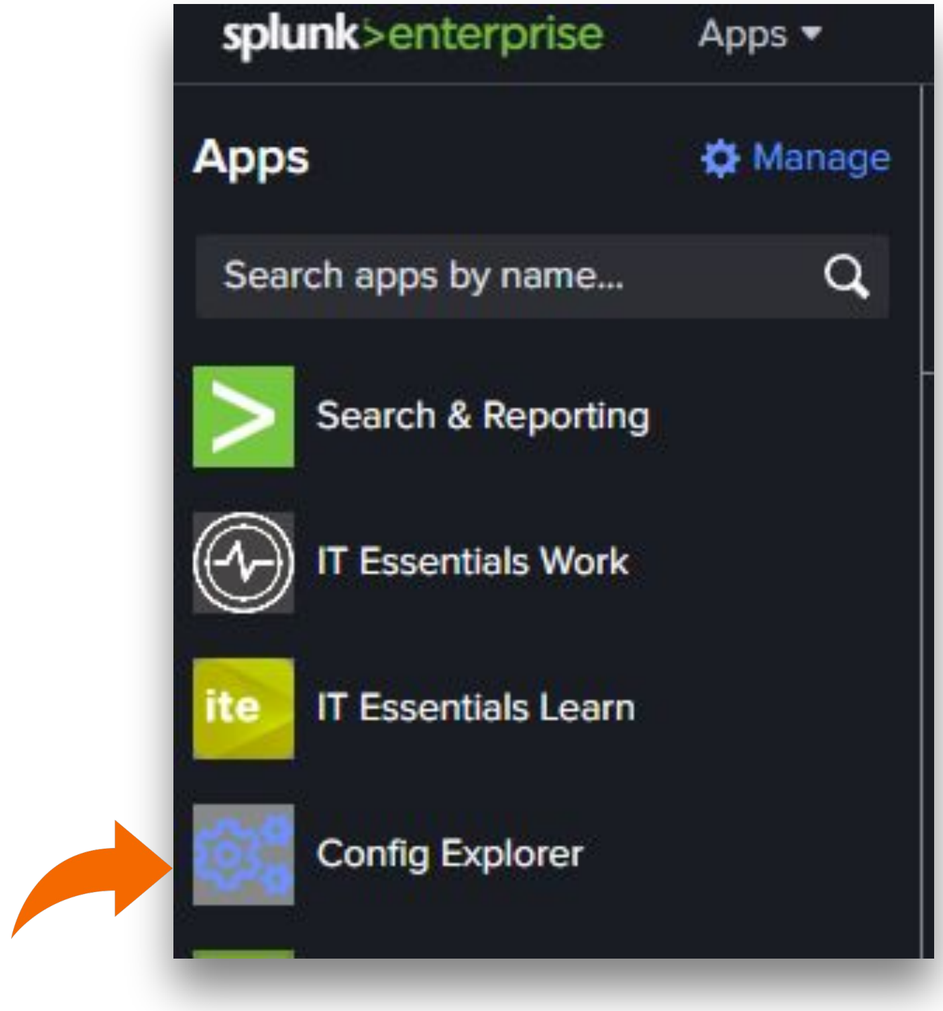
Option 1 - Use Config Explorer

Option 2 - SSH into the Splunk Indexer

Option 1 - Config Explorer

Activity #2 - Config Explorer

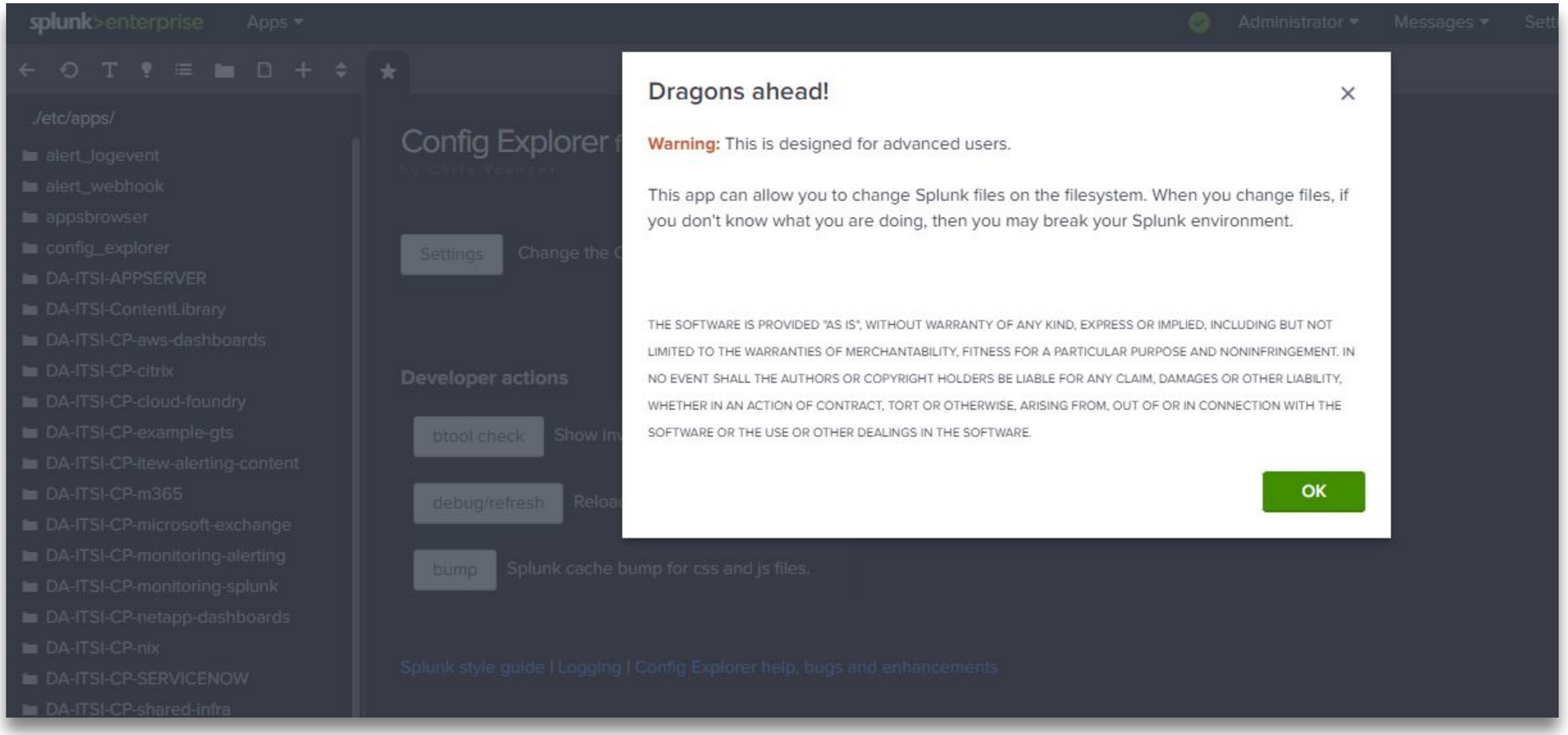
Navigate to **Conifg Explorer**



splunk>
a cisco company

Activity #2 - Config Explorer

Config Explorer warning message upon first opening

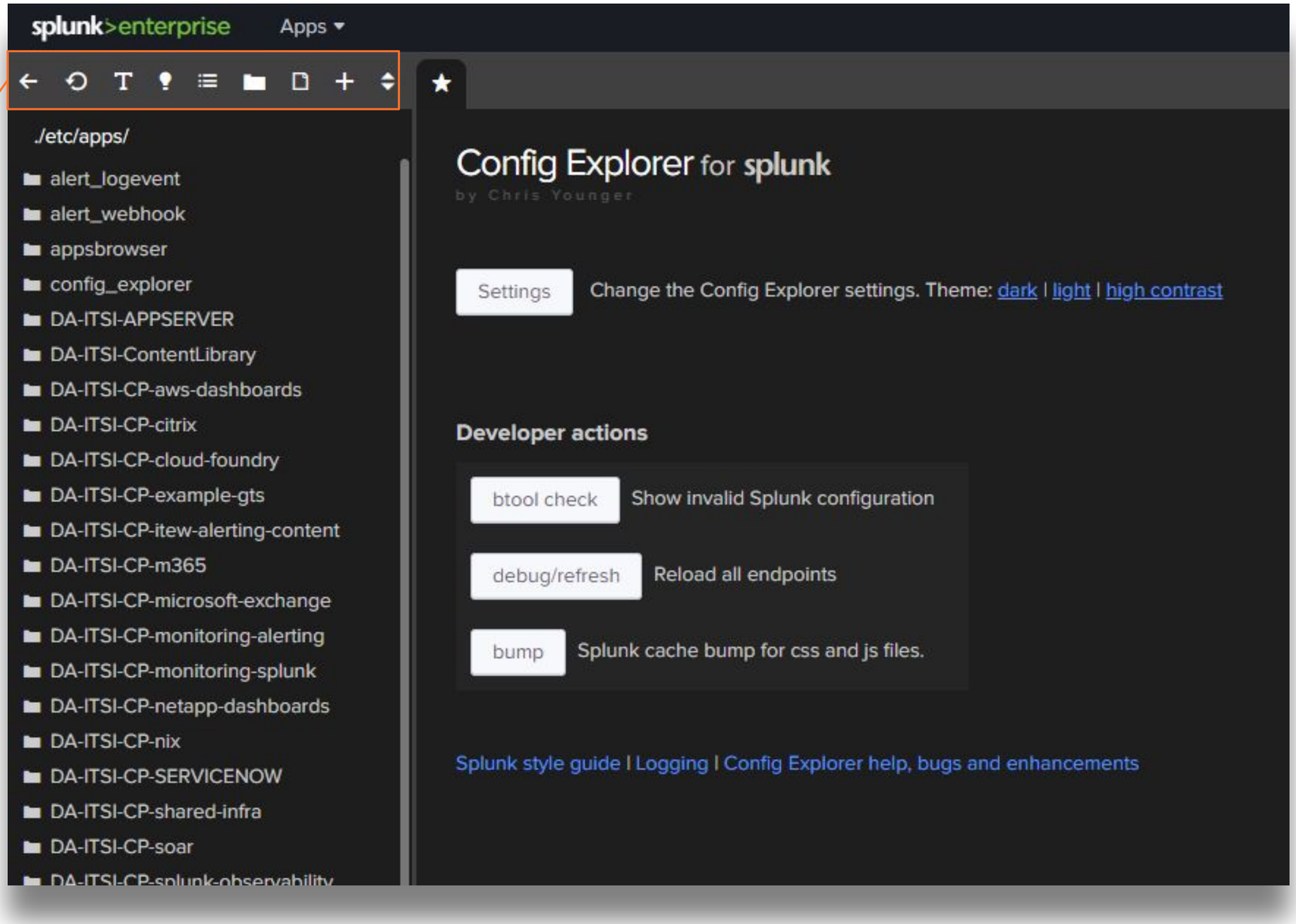


Activity #2 - Config Explorer

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

`./etc/apps`

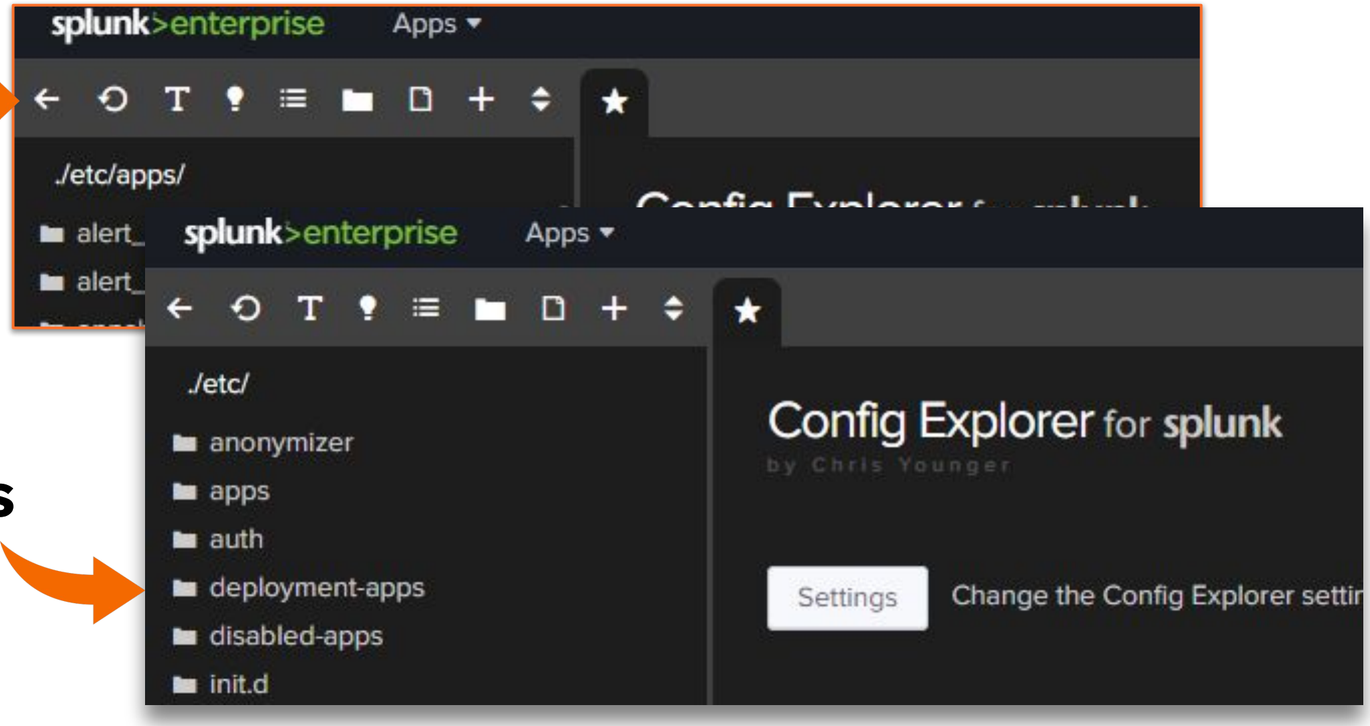
Here we will use the top navigation menu of Config Explorer to move around.



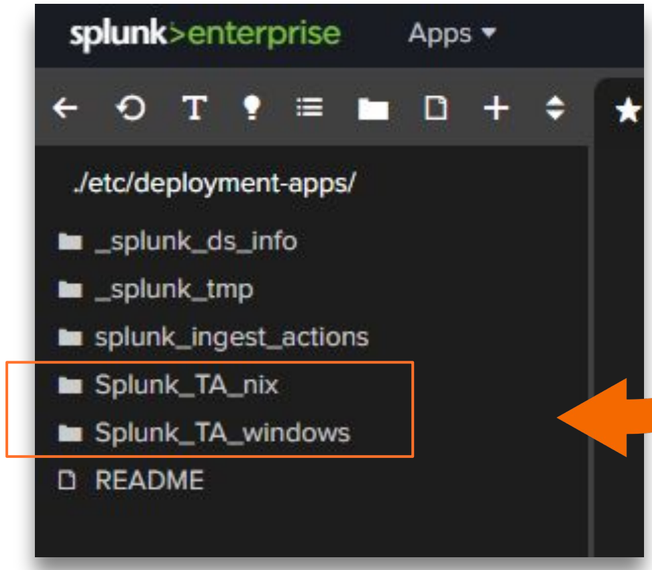
splunk>
a cisco company

Activity #2 - Config Explorer

1. Click the **back arrow**



2. Click **deployment-apps**

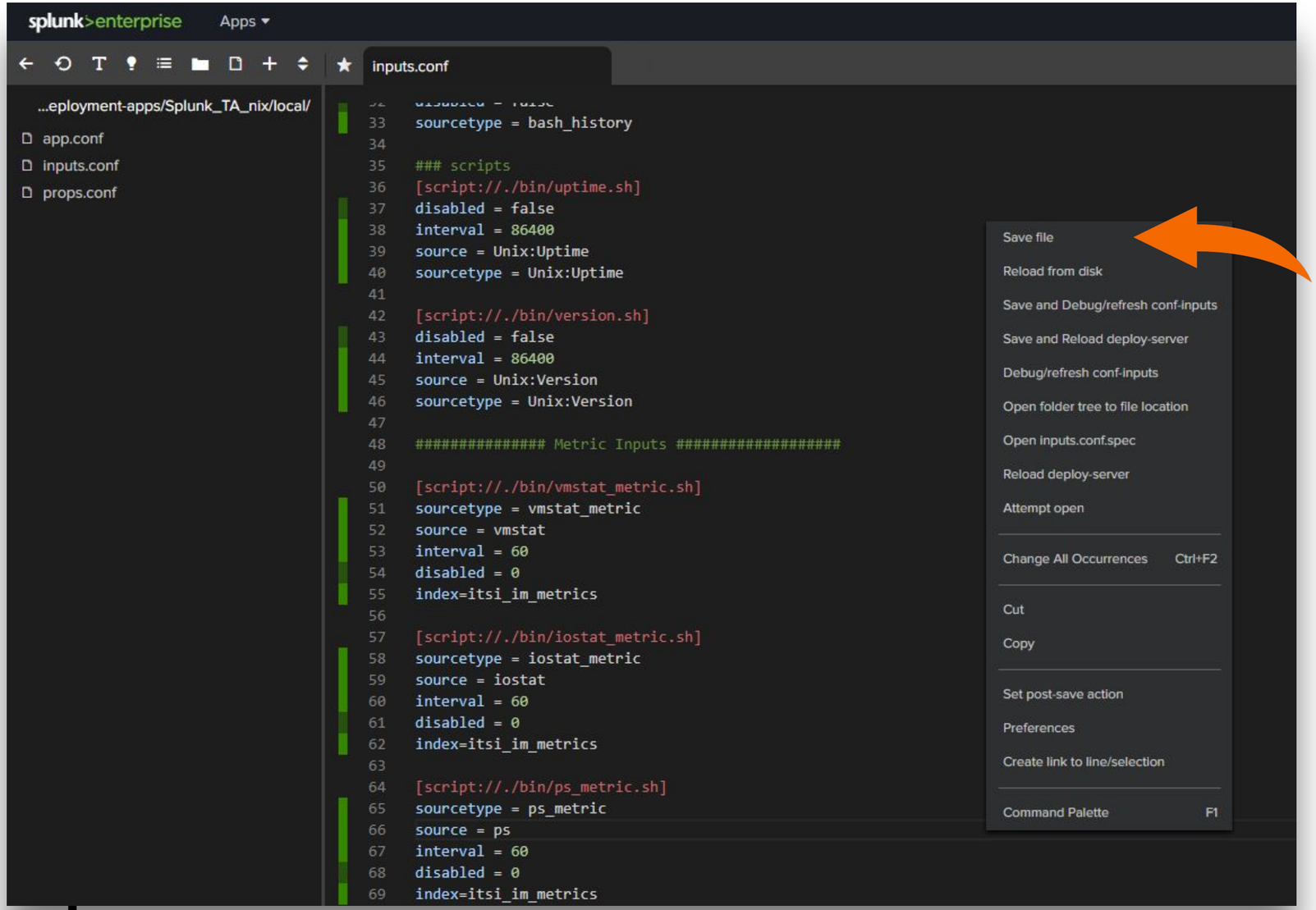


3. You should now see the apps

Splunk_TA_nix
Splunk_TA_windows

splunk>
a cisco company

Activity #2 - Config Explorer



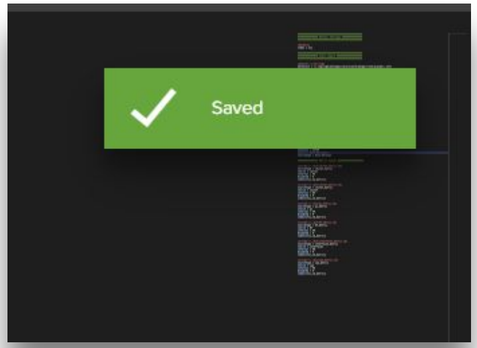
To save any changes made to a file.

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**.



splunk>
a cisco company

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://PhysicalDisk]

[perfmon://Network]

[perfmon://System]
```

```
[perfmon://LogicalDisk]

[perfmon://Memory]

[perfmon://Process]
```

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;
Interrupts/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

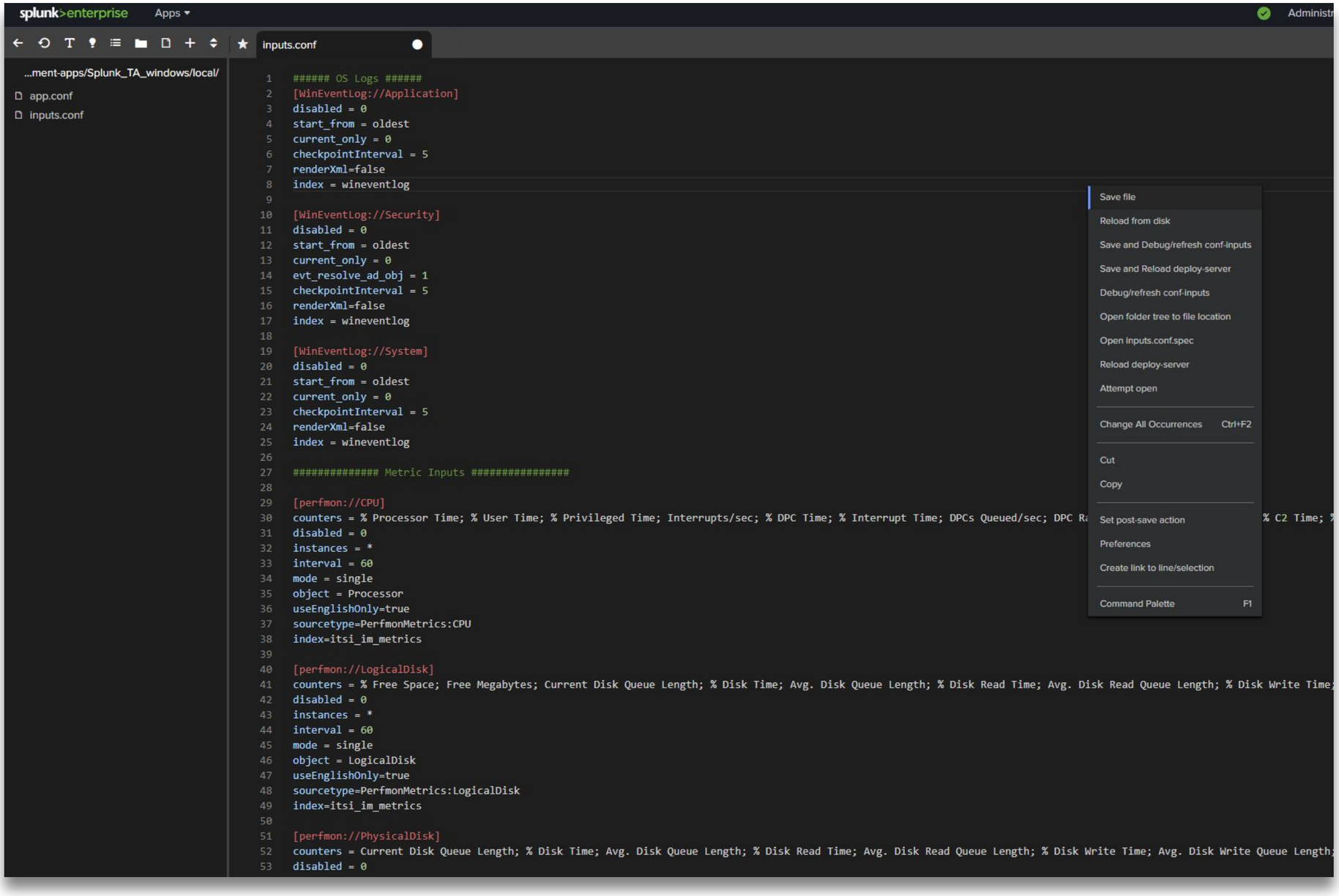
Your Splunk_TA_windows inputs.conf file should look similar to this.

To save any changes made to a file.

Right click in the file.

In the pop-up menu select:

Save file



splunk>
a cisco company

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

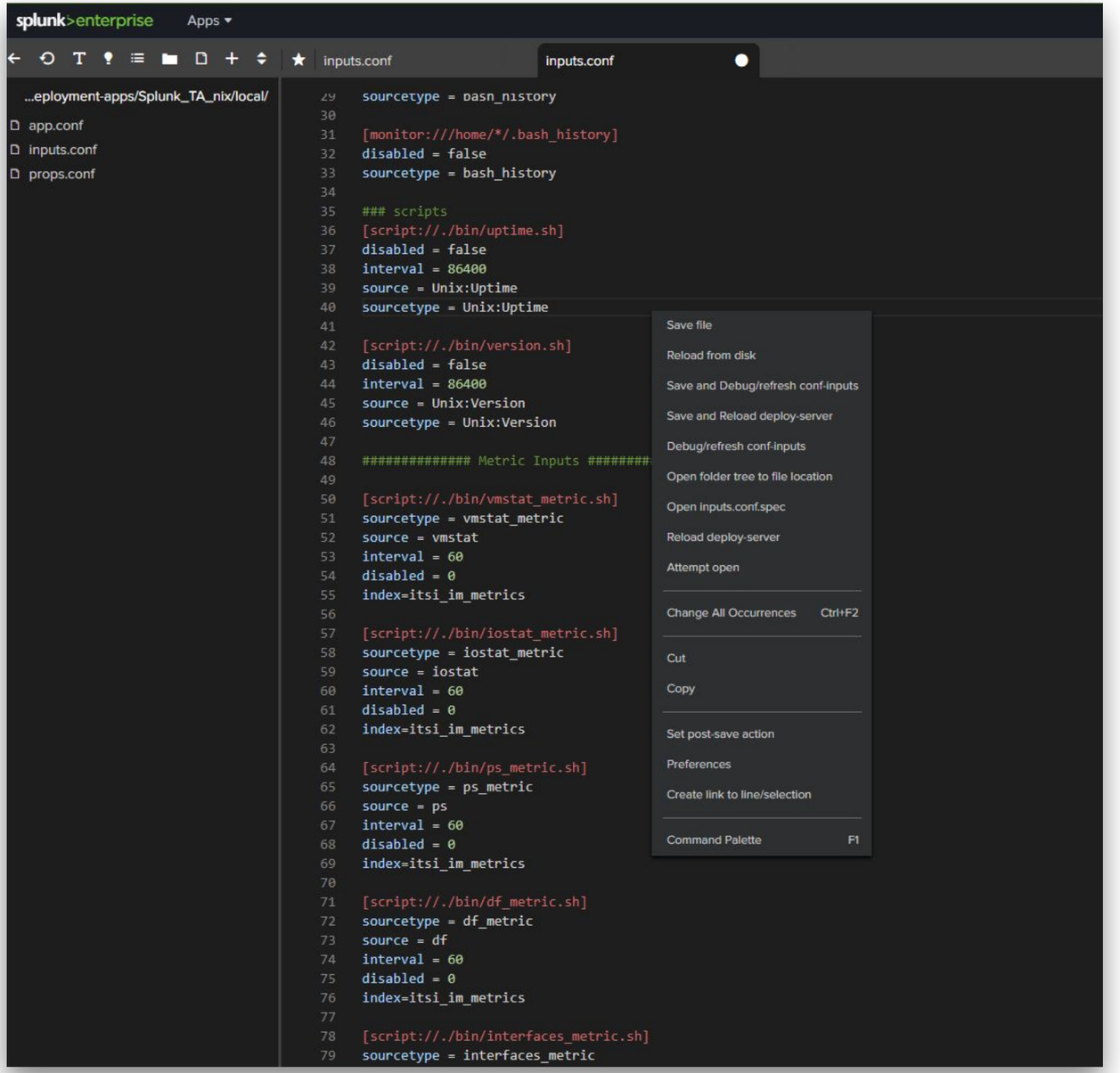
Your Splunk_TA_nix inputs.conf file should look similar to this.

To save any changes made to a file.

Right click in the file.

In the pop-up menu select:

Save file



splunk>
a cisco company

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

splunk>
a CISCO company

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

splunk> a cisco company

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

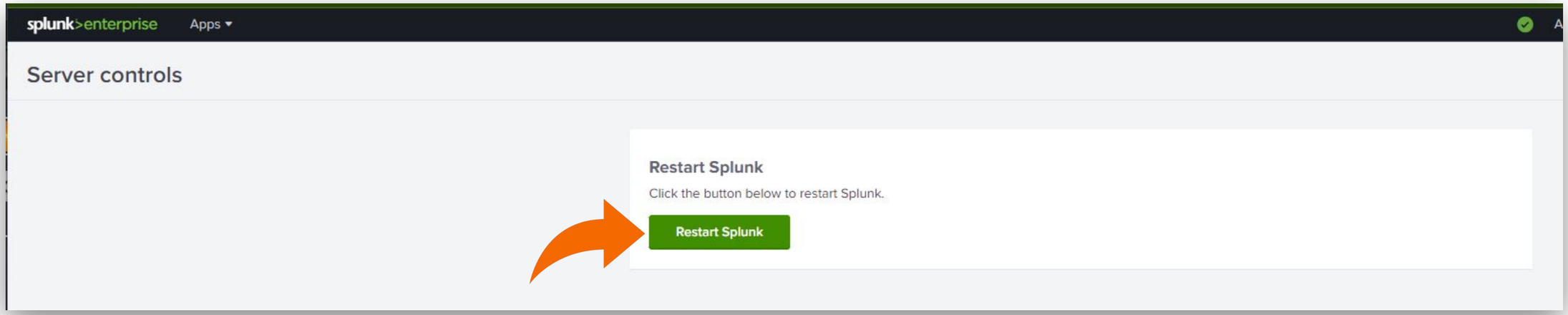
```
root@ip-172-31-13-174:/opt/splunk/etc/deployment-apps/Splunk_TA_nix/local# cd ../../..
root@ip-172-31-13-174:/opt/splunk/etc# cd ..
root@ip-172-31-13-174:/opt/splunk# cd bin
root@ip-172-31-13-174:/opt/splunk/bin# ./splunk reload deploy-server -class all-windows
Splunk username: admin
Password:
Reloading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

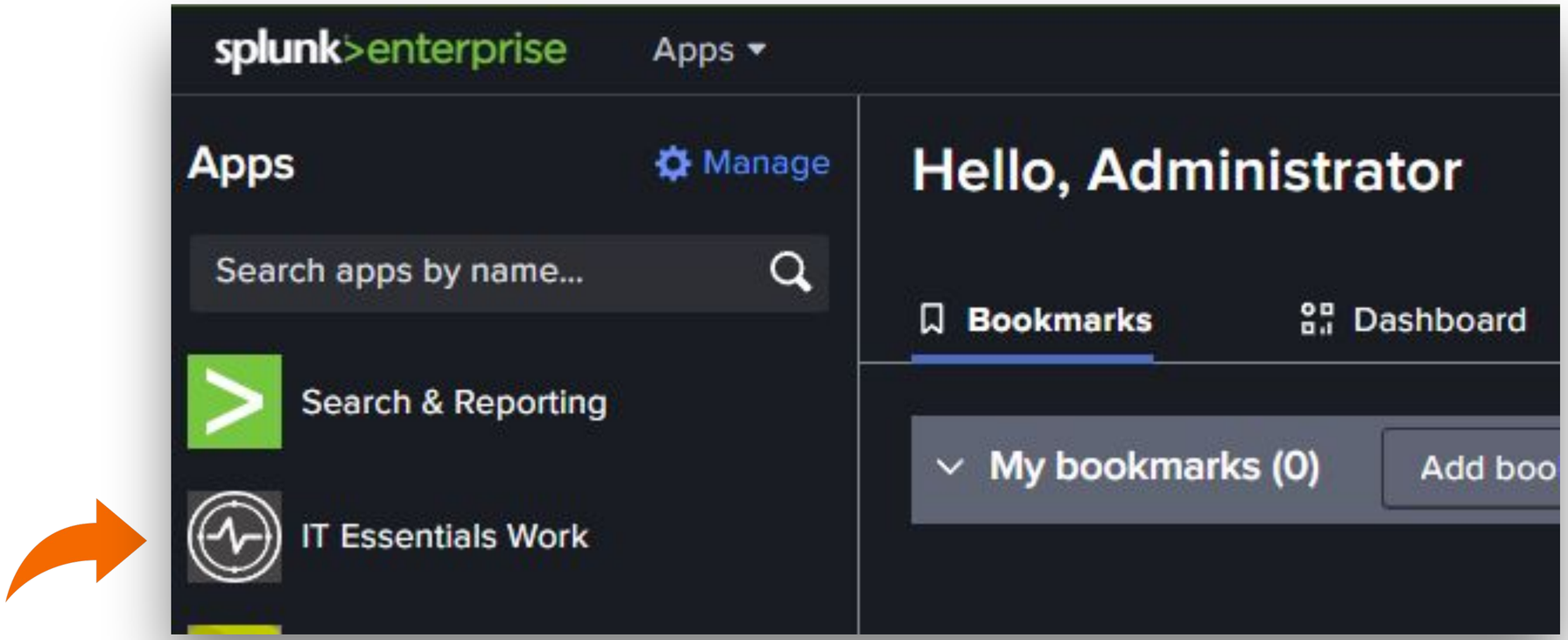
Click **Restart Splunk**



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.

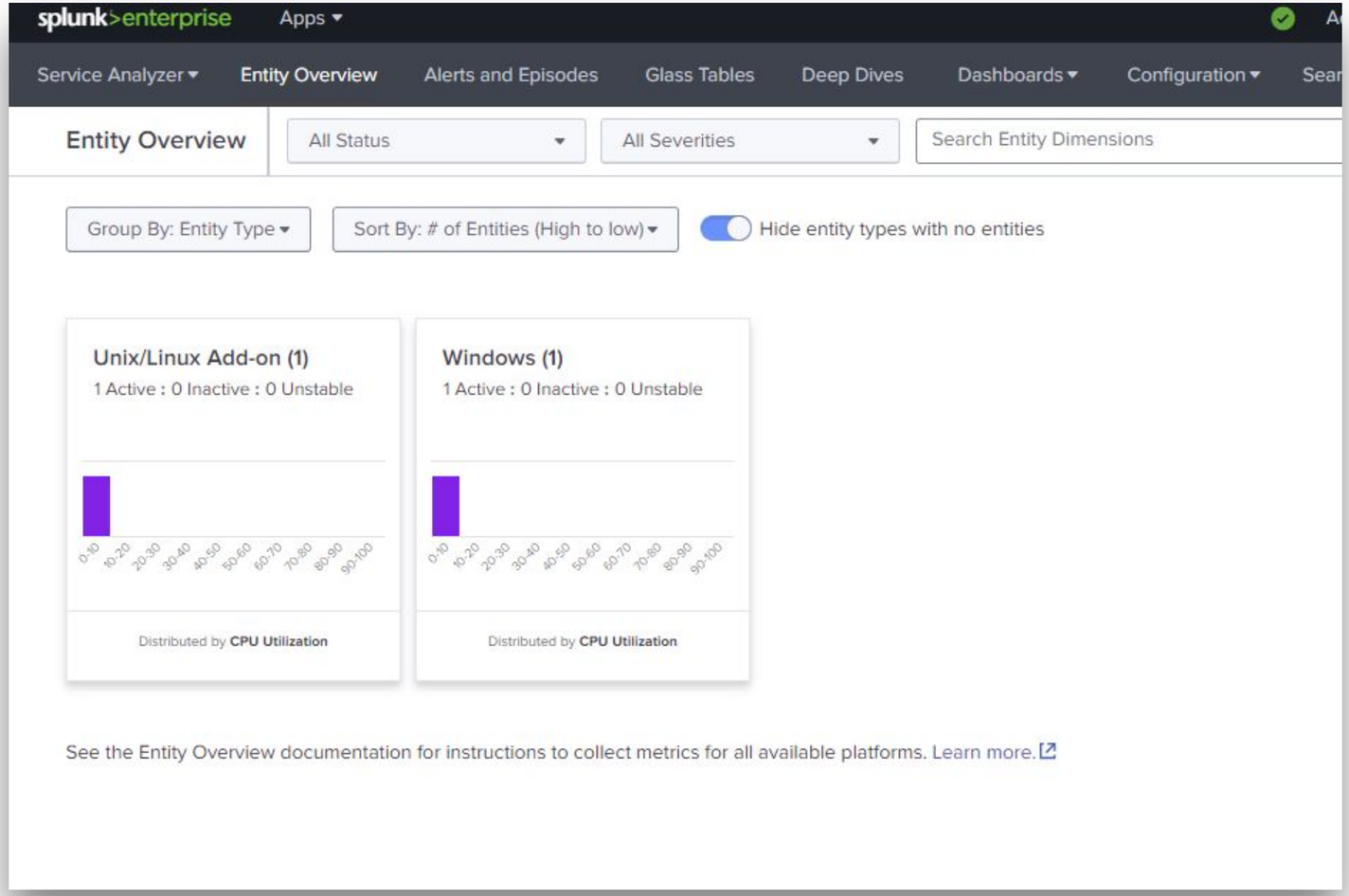


splunk>
a cisco company

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



splunk>
a cisco company

Activity #4 - helpful commands to search metrics data

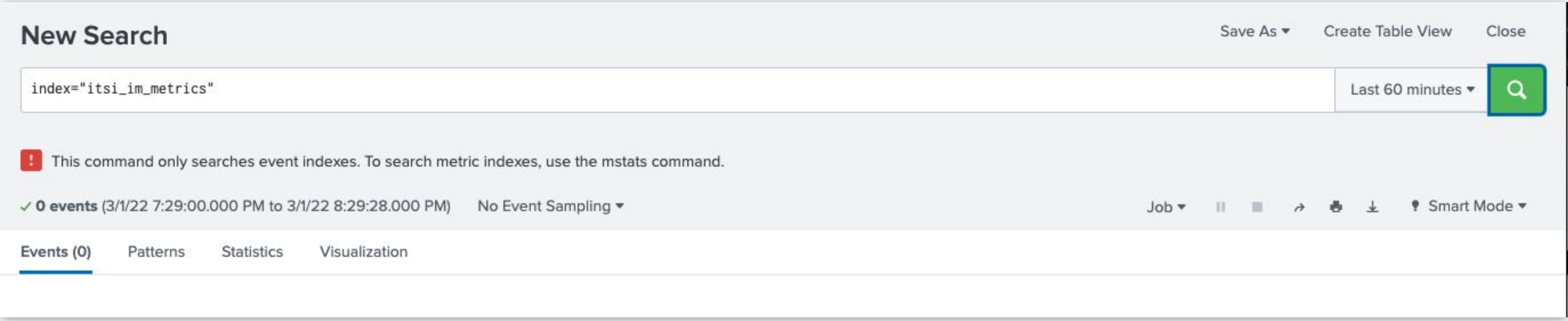
splunk>
a CISCO company

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**.



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

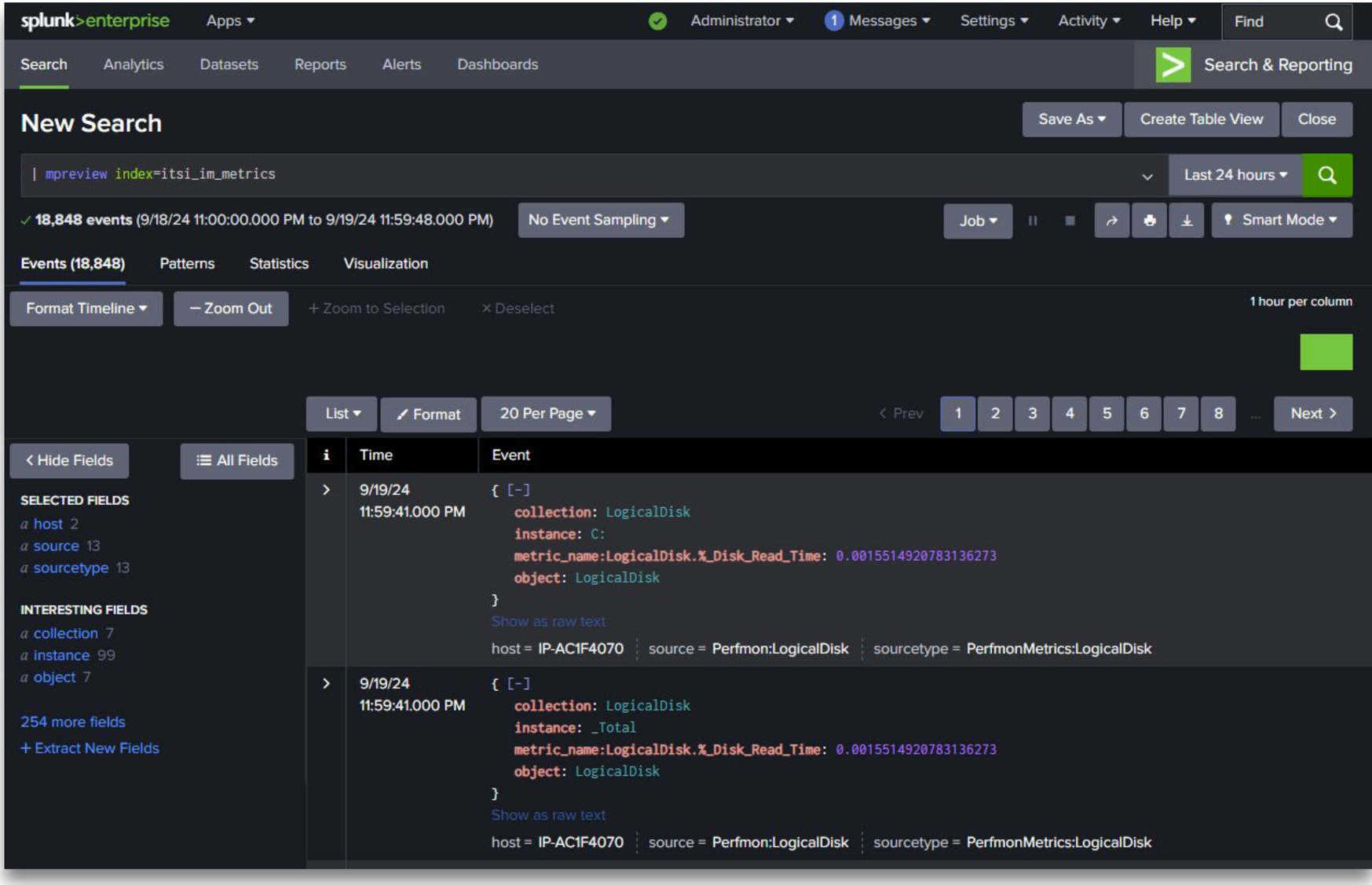
Use mpreview to get an idea of the kinds of metric time series that are stored in your metrics indexes and to troubleshoot your metrics data.

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
```



splunk>
a cisco company

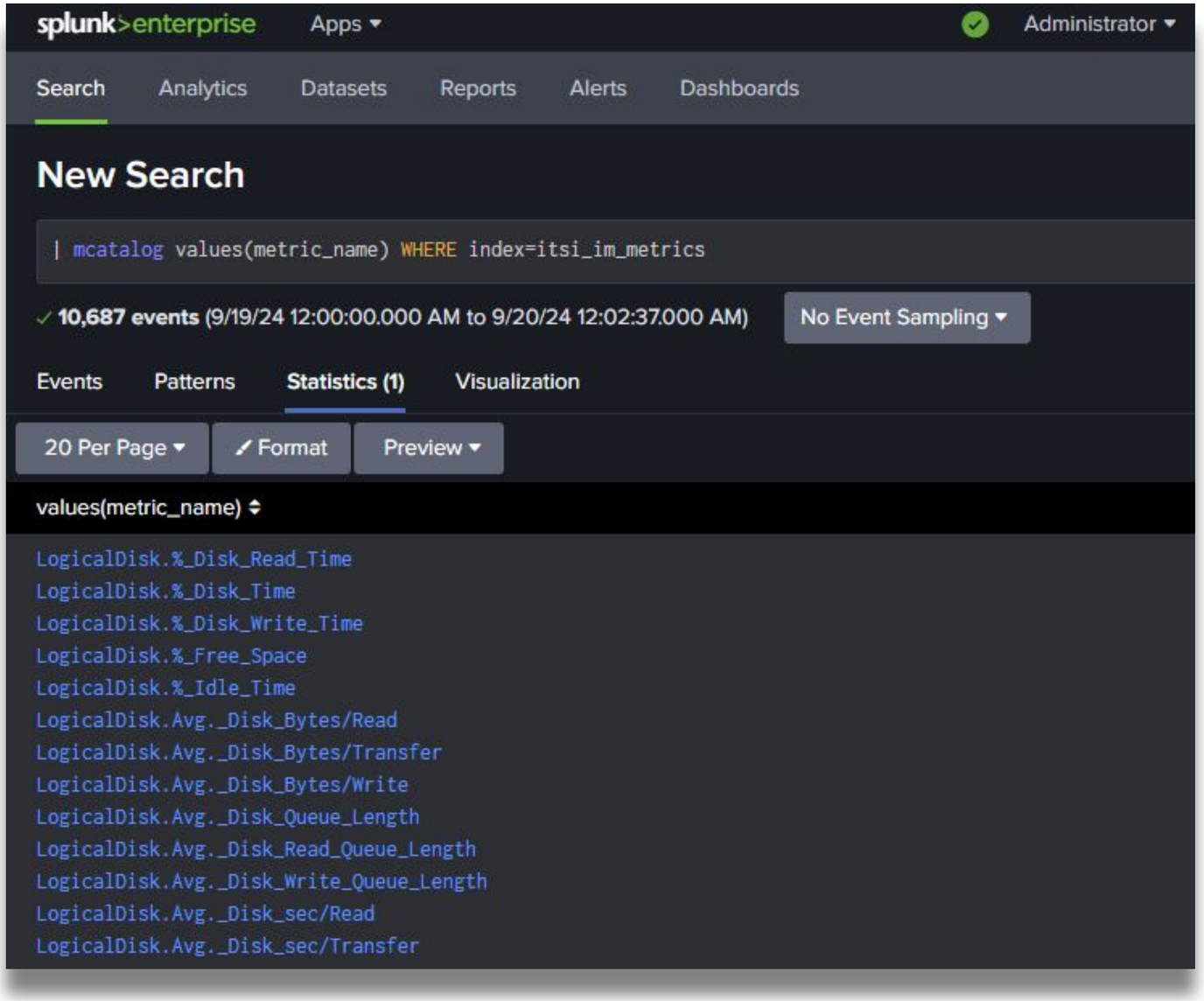
Activity #4 - mcatalog command

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
```



Activity #4 - mstats command

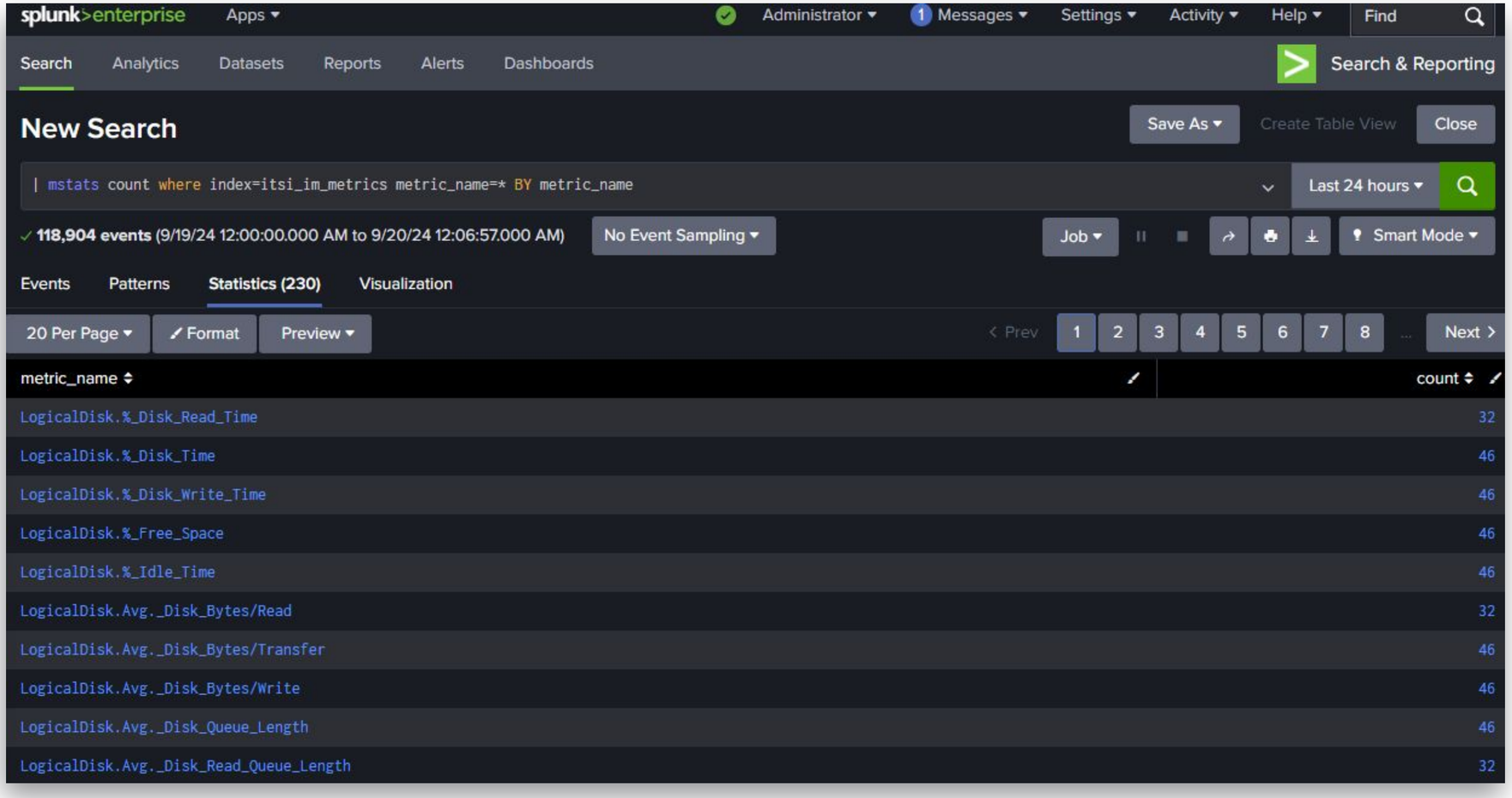
Use the mstats command to analyze metrics.

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
```

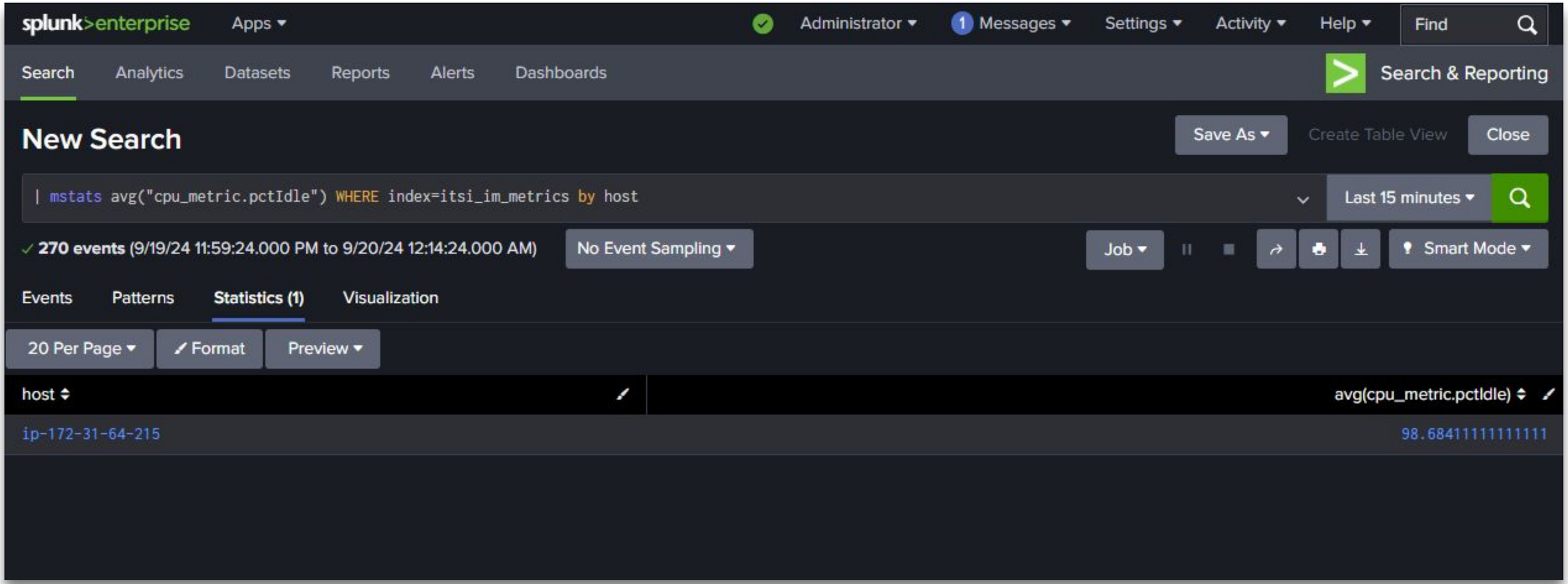


splunk>
a cisco company

Activity #4 - mstats command

Use mstats to see average CPU idle:

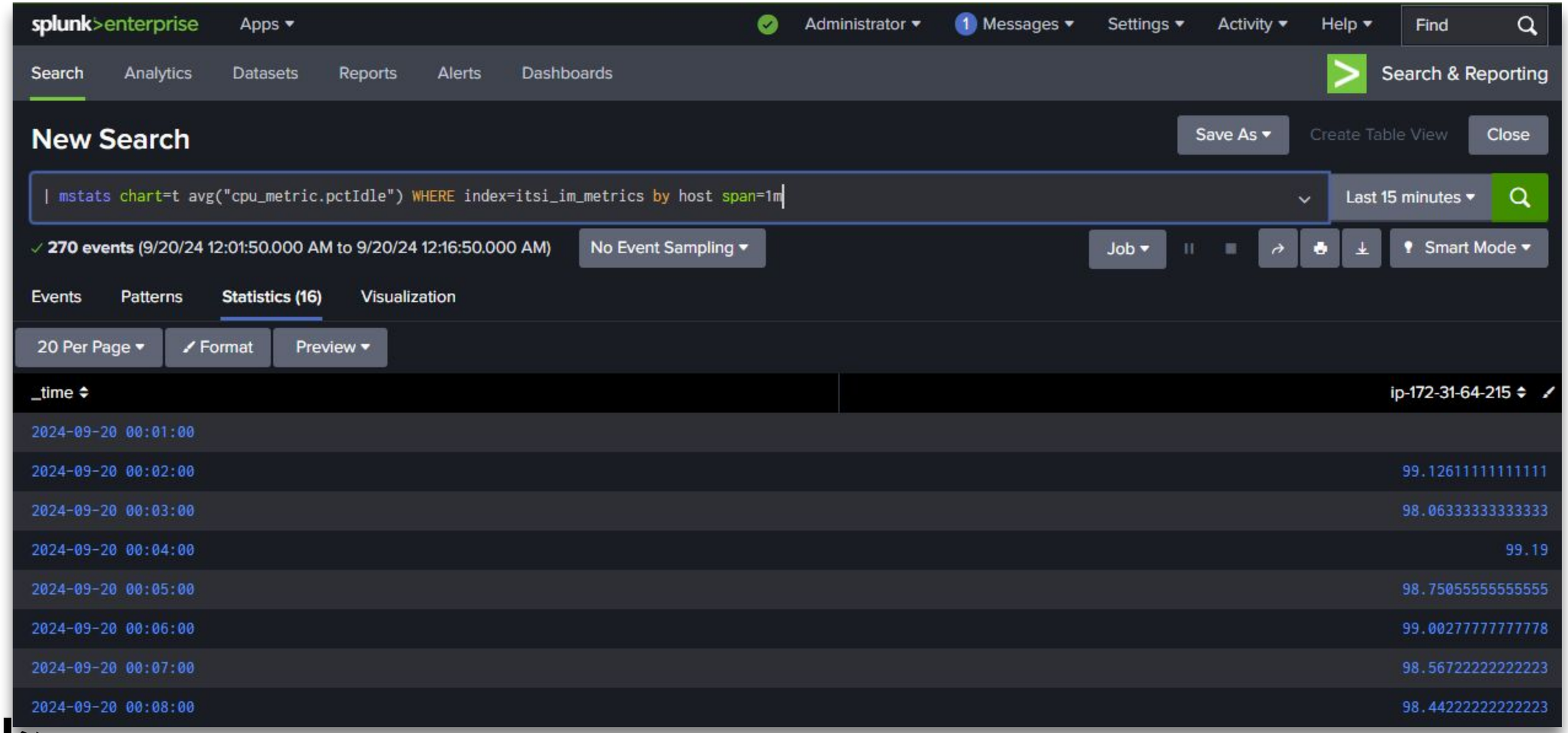
```
| mstats avg("cpu_metric.pctIdle") WHERE index=itsi_im_metrics by host
```



Activity #4 - mstats command

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

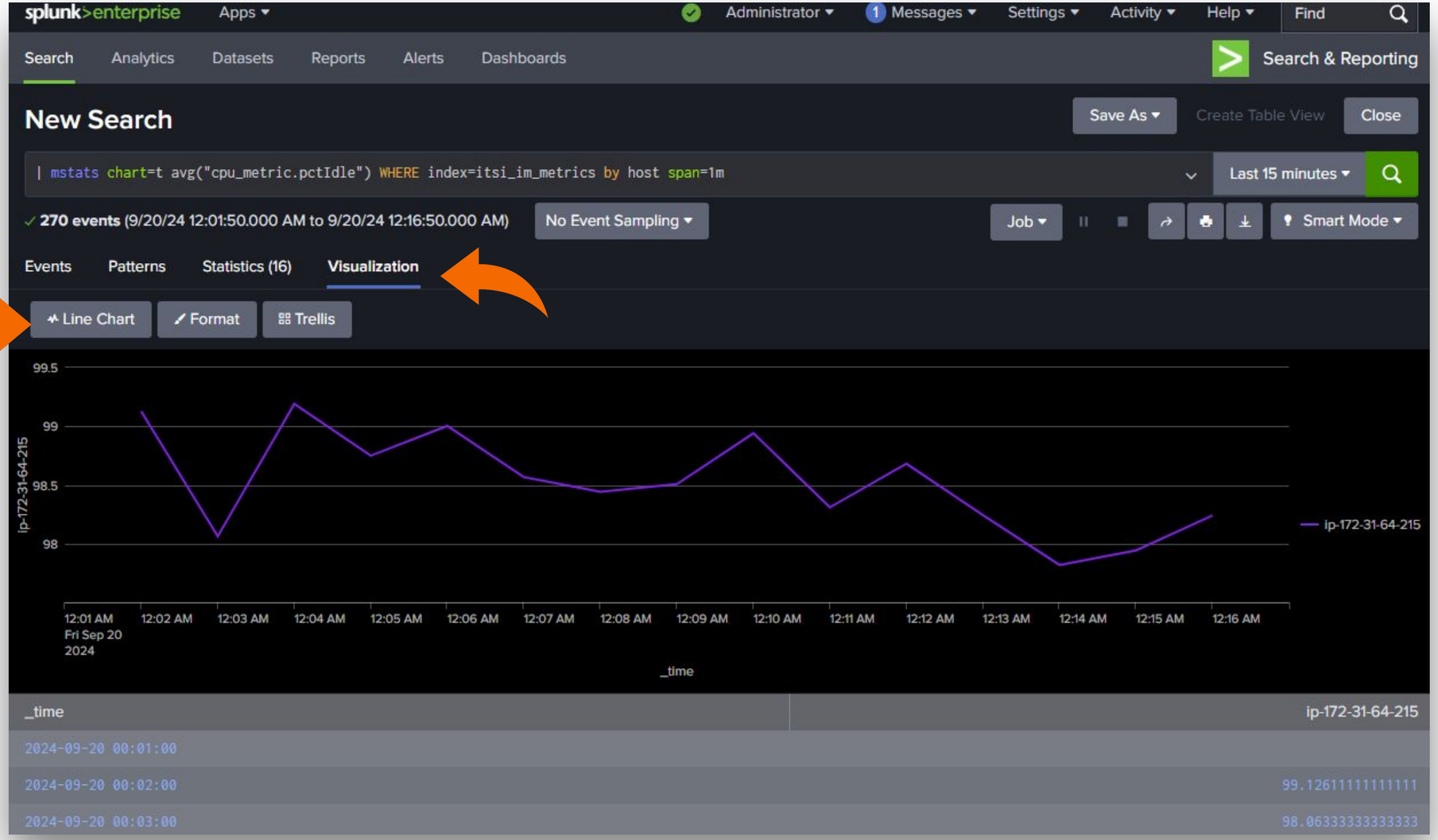
```
| mstats chart=t avg("cpu_metric.pctIdle") WHERE index=itsi_im_metrics by host span=1m
```



splunk>
a cisco company

Activity #4 - mstats command

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



splunk>
a cisco company

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
```

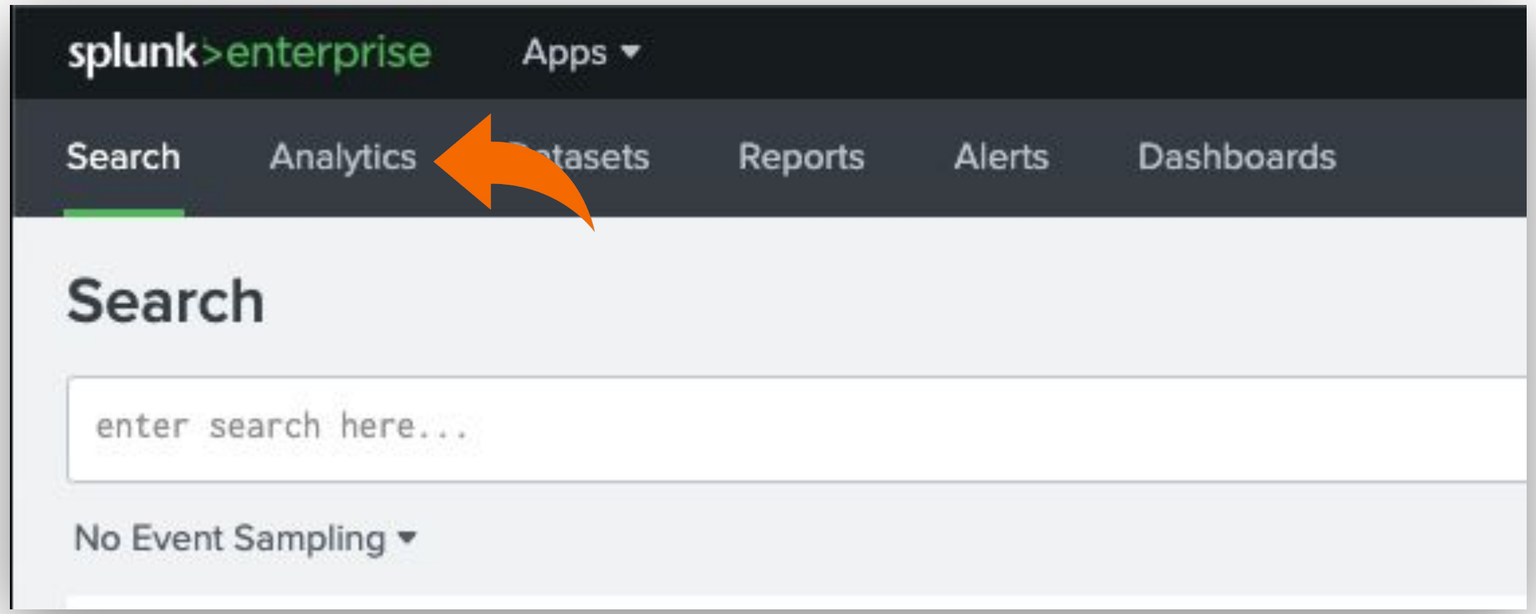
Activity #5
- Use Analytics Workspace to build useful reports, dashboards and alerts

splunk>
a CISCO company

Activity #5 - Analytics Workspace

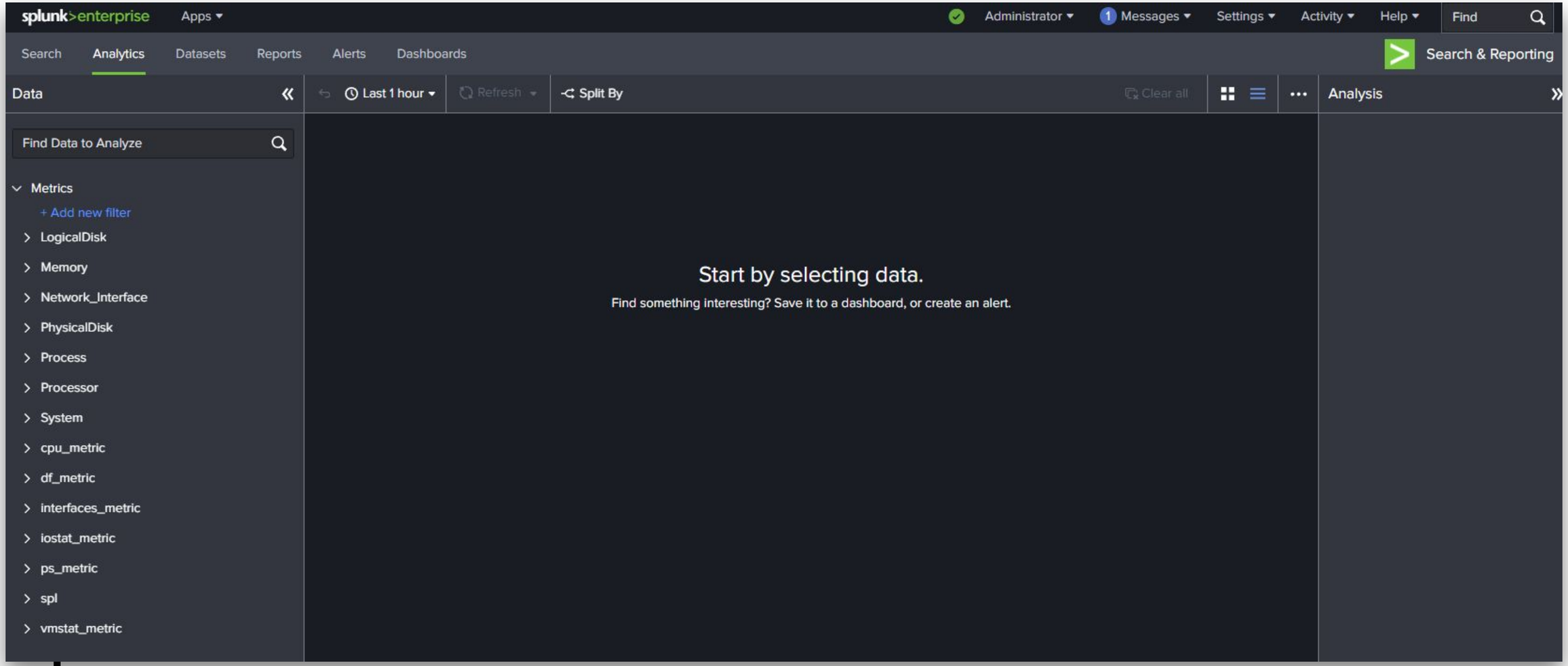
Navigate to the **Search & Reporting** app

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.



splunk>
a cisco company

Activity #5 - Analytics Workspace

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

CPU

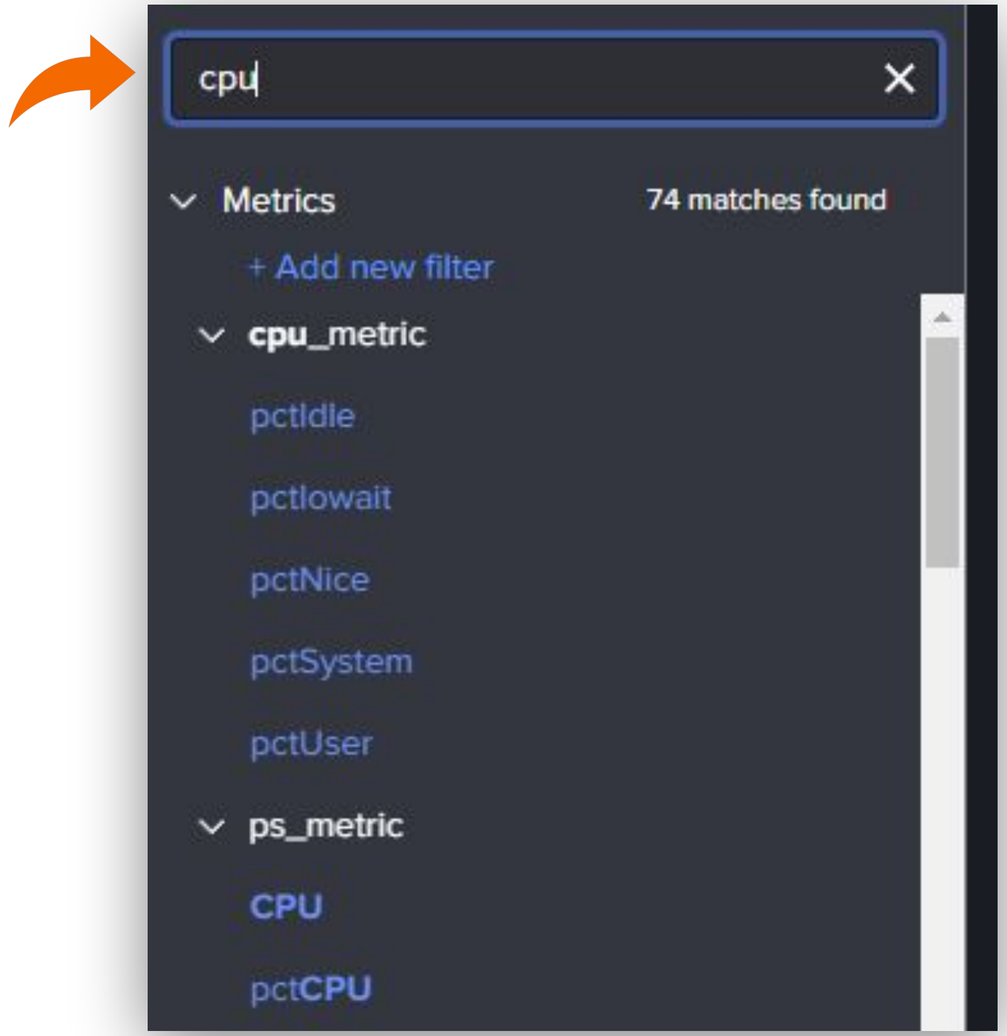
This will filter the metrics data sources to only display metrics related to **CPU**.

Go ahead and try a few other keywords:

Memory

User

Bytes



splunk>
a cisco company

Activity #5 - Analytics Workspace

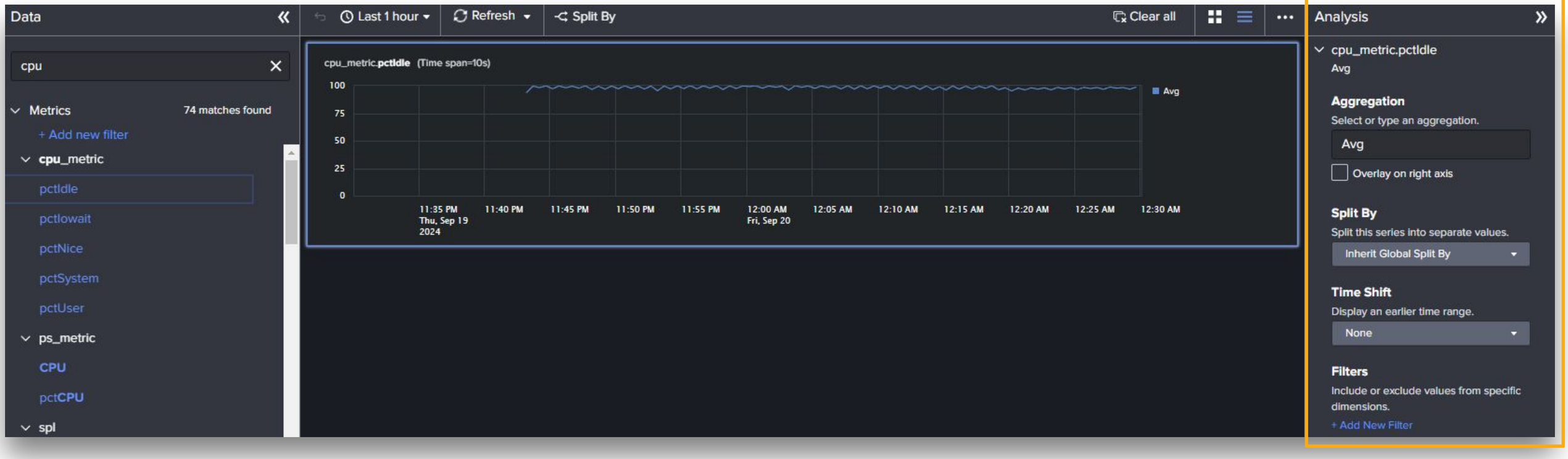
Sticking with **CPU**, lets click on **pctidle** under **cpu_metric**

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

splunk>
a cisco company

Activity #5 - Analytics Workspace

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

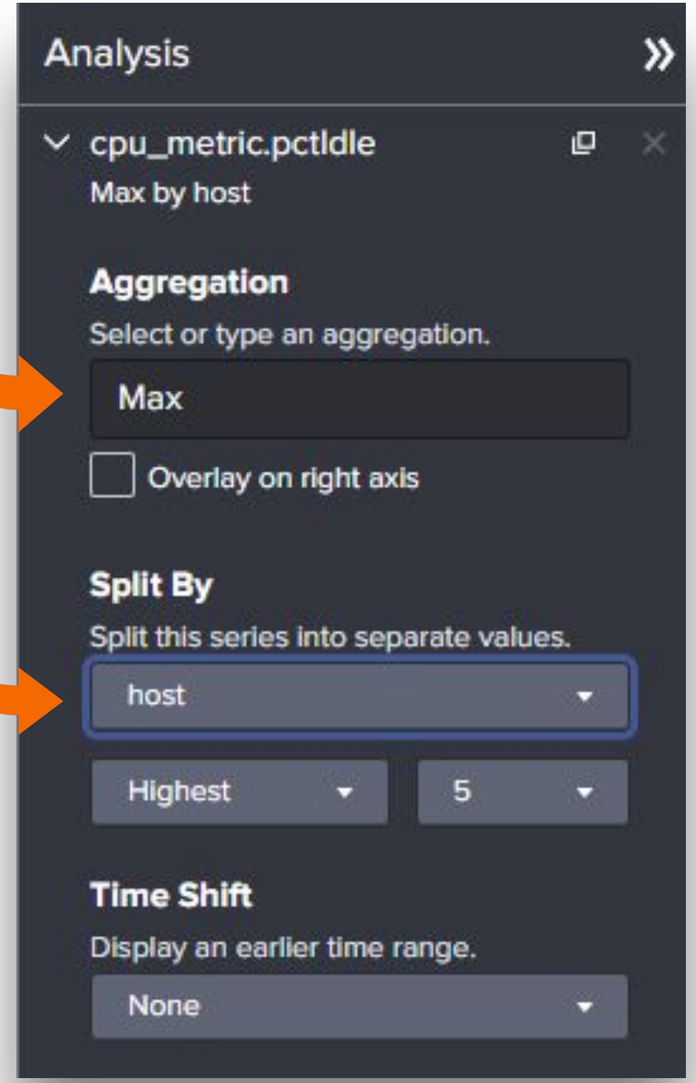


splunk> a cisco company

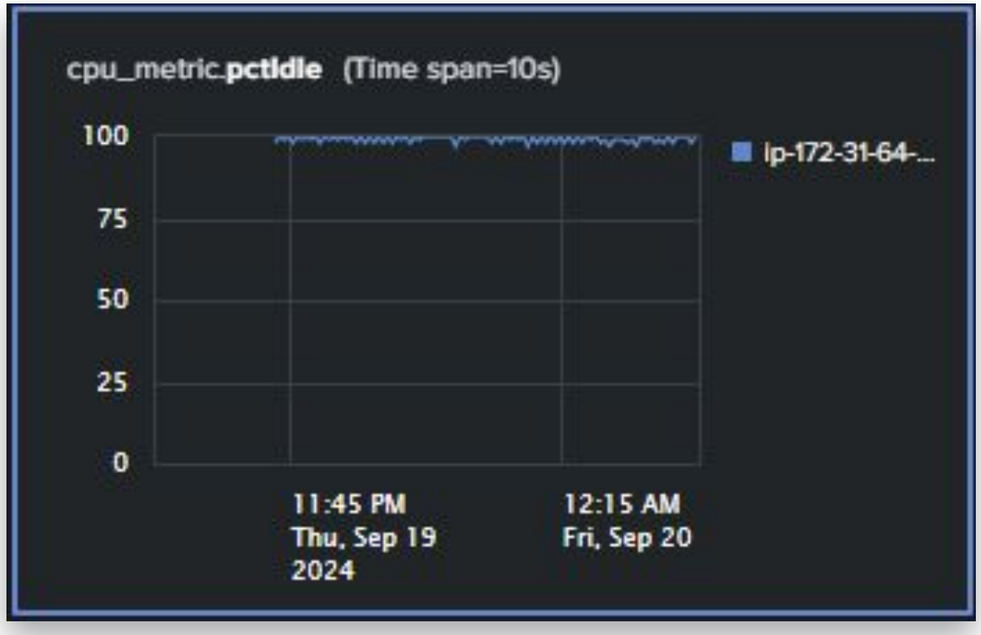
Activity #5 - Analytics Workspace

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.

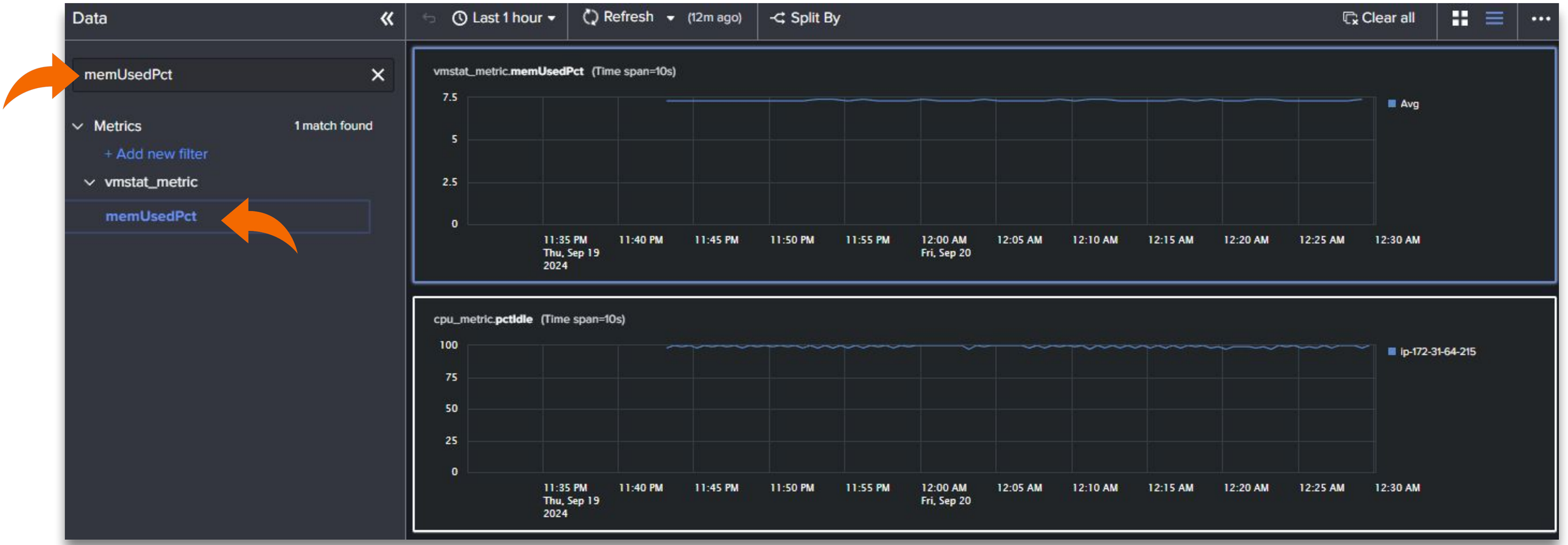


splunk>
a cisco company

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



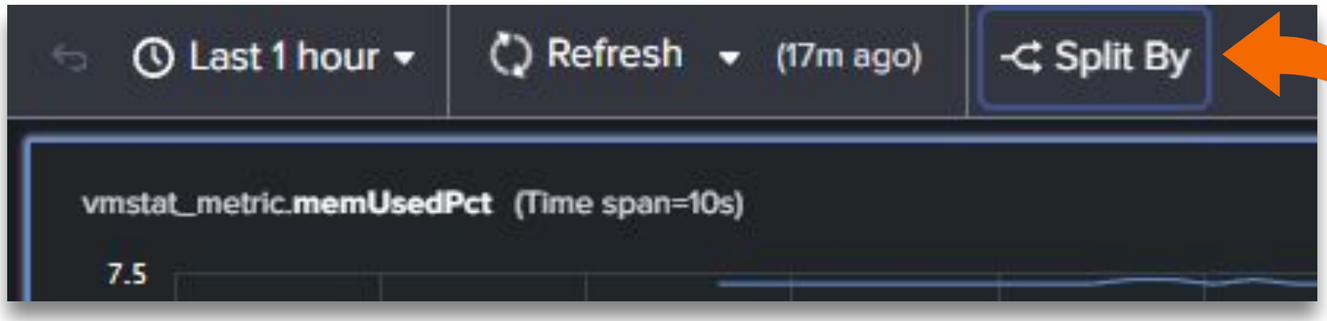
splunk> a cisco company

Activity #5 - Analytics Workspace

At this point you will have 2 charts.

However, the newest chart is not Split By host.

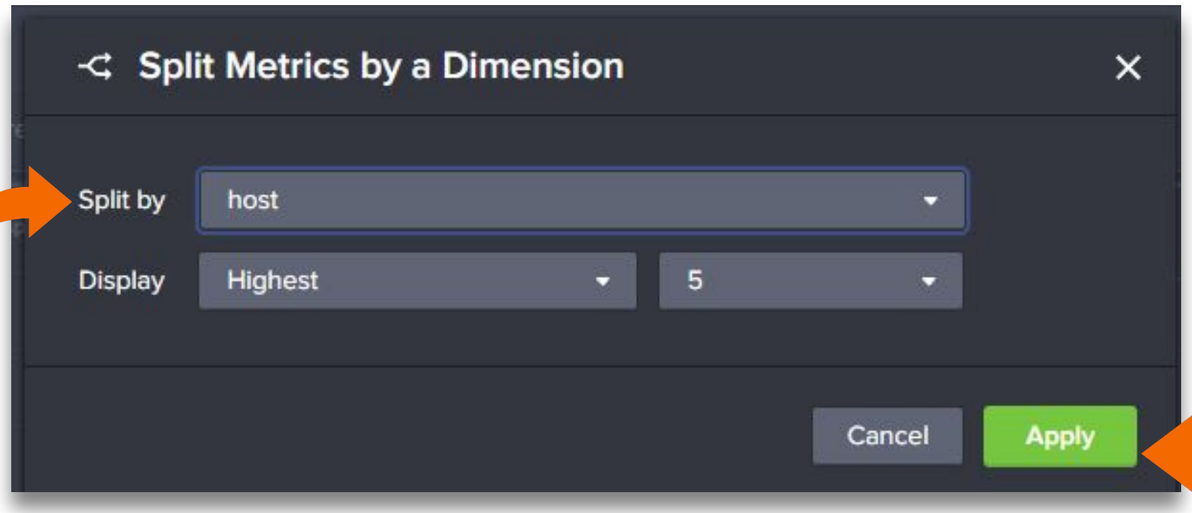
By default, any new chart will inherit the **Global Split By** value and no value has been set.



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**”



splunk>
a cisco company

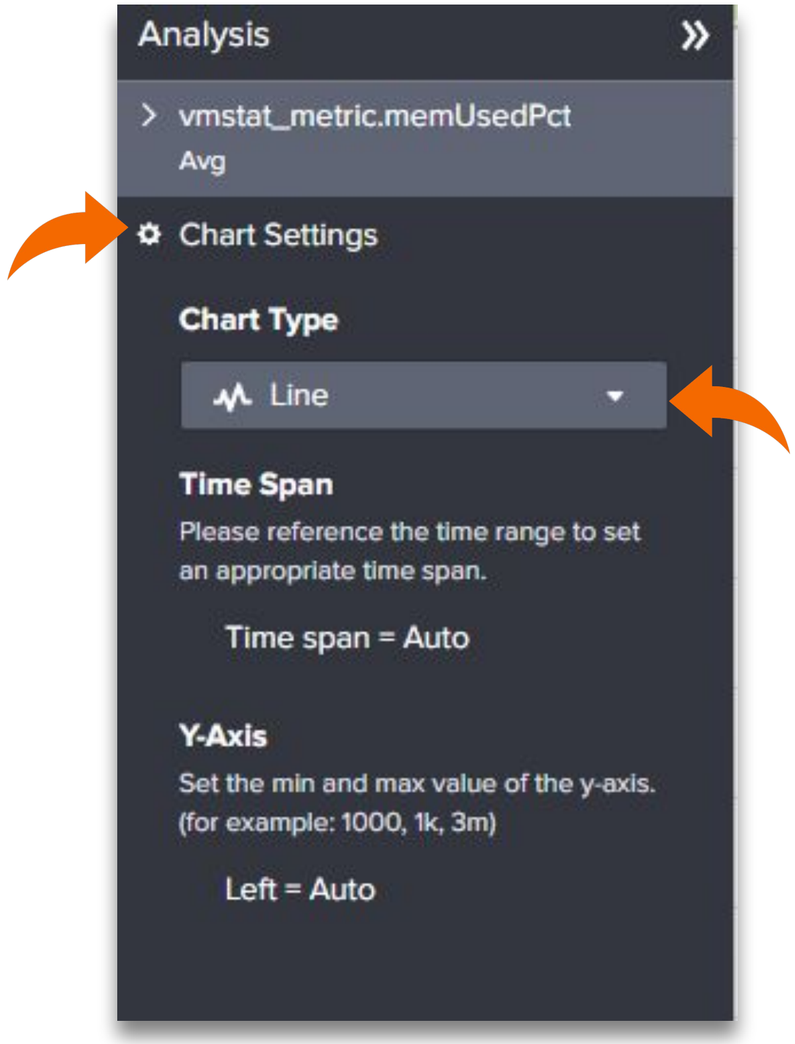
Activity #5 - Analytics Workspace

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.

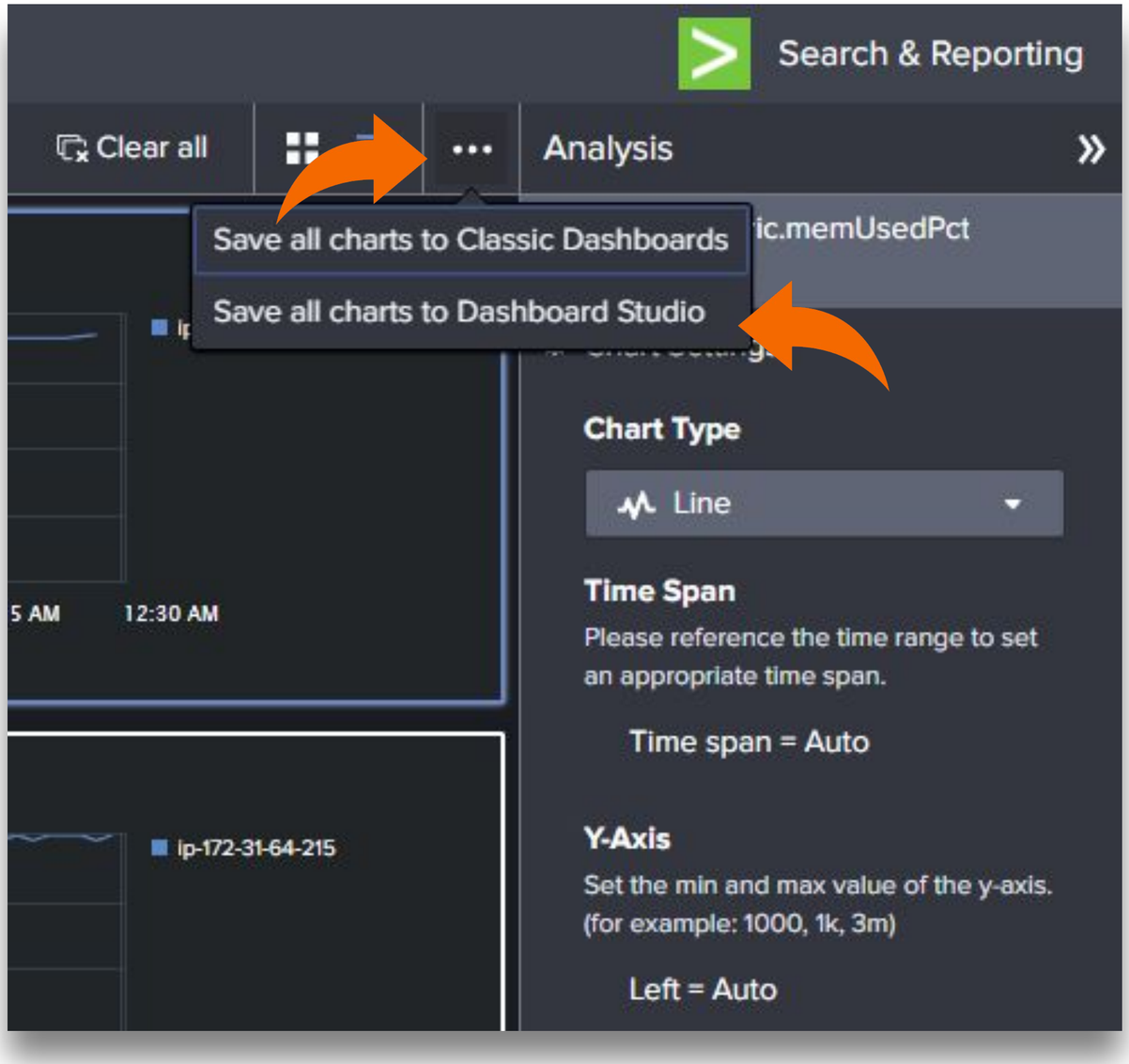


Activity #5 - Analytics Workspace

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



splunk>
a cisco company

Activity #5 - Analytics Workspace

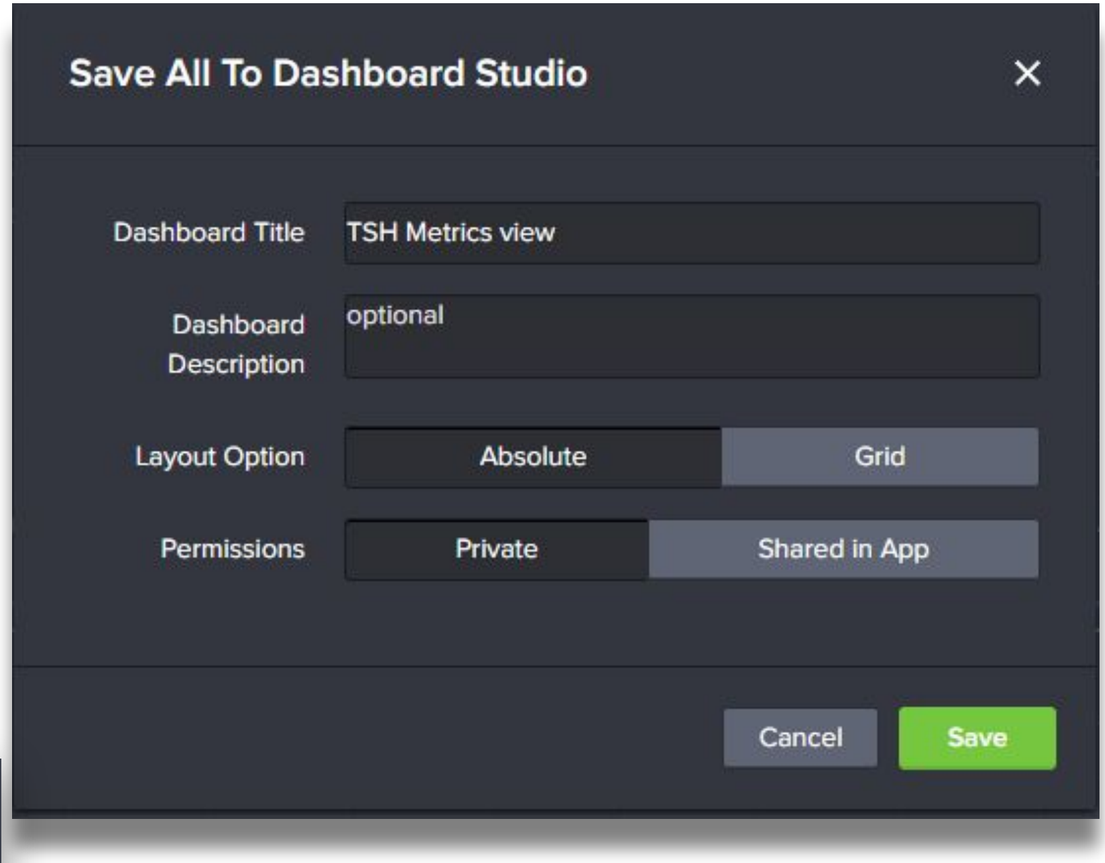
Save all Charts as a Dashboard.

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

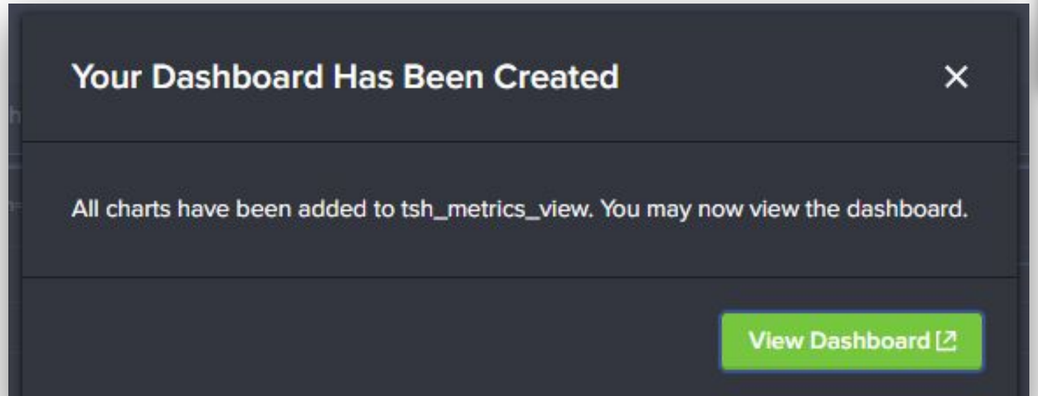
For example: **TSH Metrics view**

You can leave everything else alone.

Now click **Save**



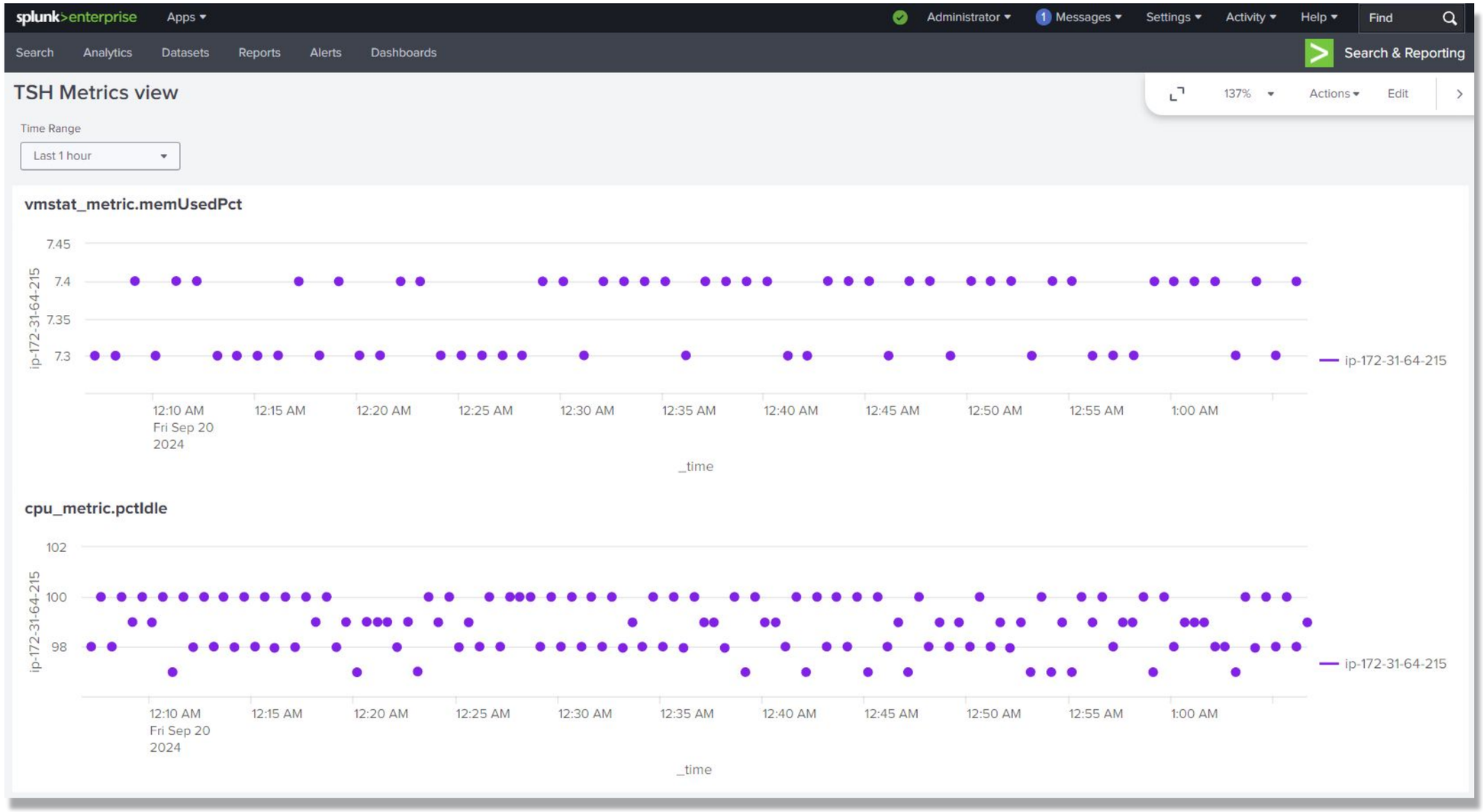
You should have another pop-up where you can click **View Dashboard**



splunk> a cisco company

Activity #5 - Analytics Workspace

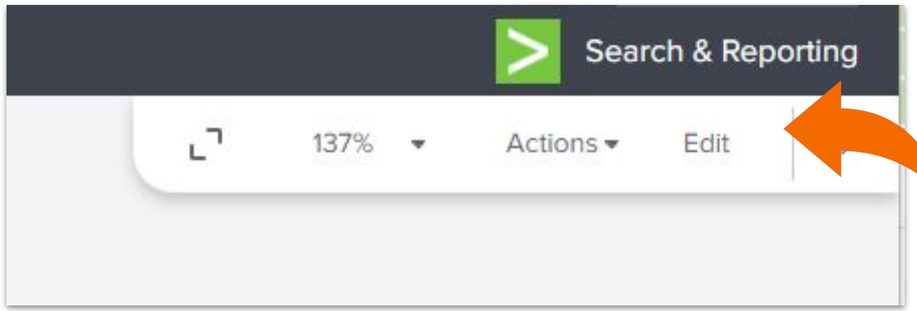
A dashboard has been born



splunk>
a cisco company

Activity #5 - Analytics Workspace

Adjust the Line chart to connect the “dots”

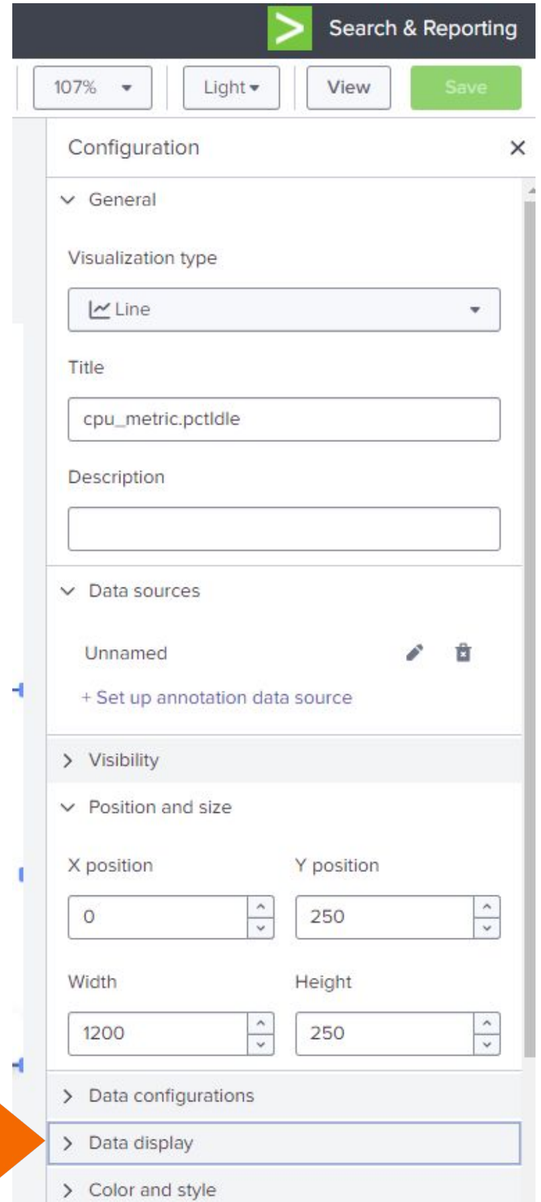


1. Click **Edit** in the top right corner

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



splunk> a cisco company

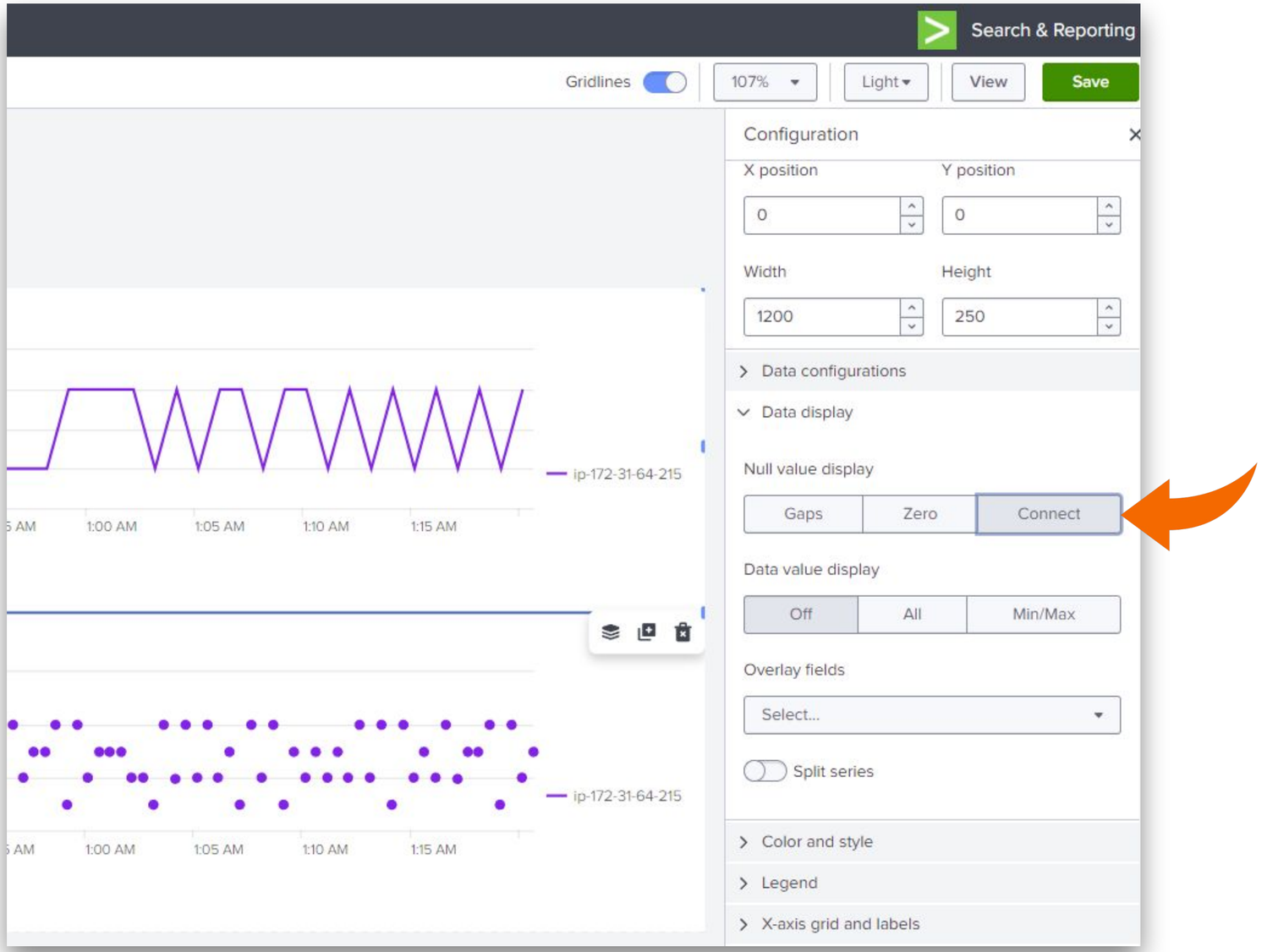
Activity #5 - Analytics Workspace

Select **Connect** under Null value display

You should see the change immediately.

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

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



splunk> a cisco company

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 the 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

splunk> a cisco company

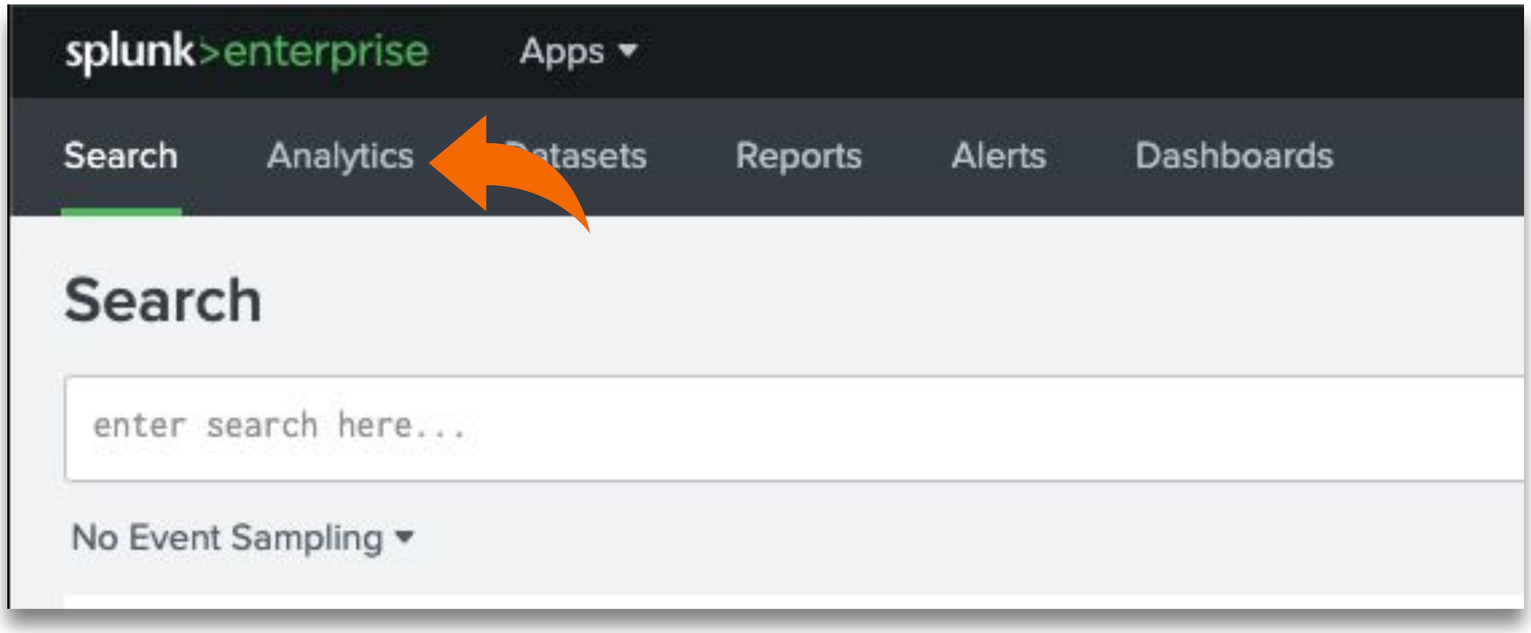
Activity #6 - Use Analytics Workspace to build alerts

splunk>
a CISCO company

Activity #6 - Create an Alert

Navigate to the **Search & Reporting** app

Click the **Analytics** tab



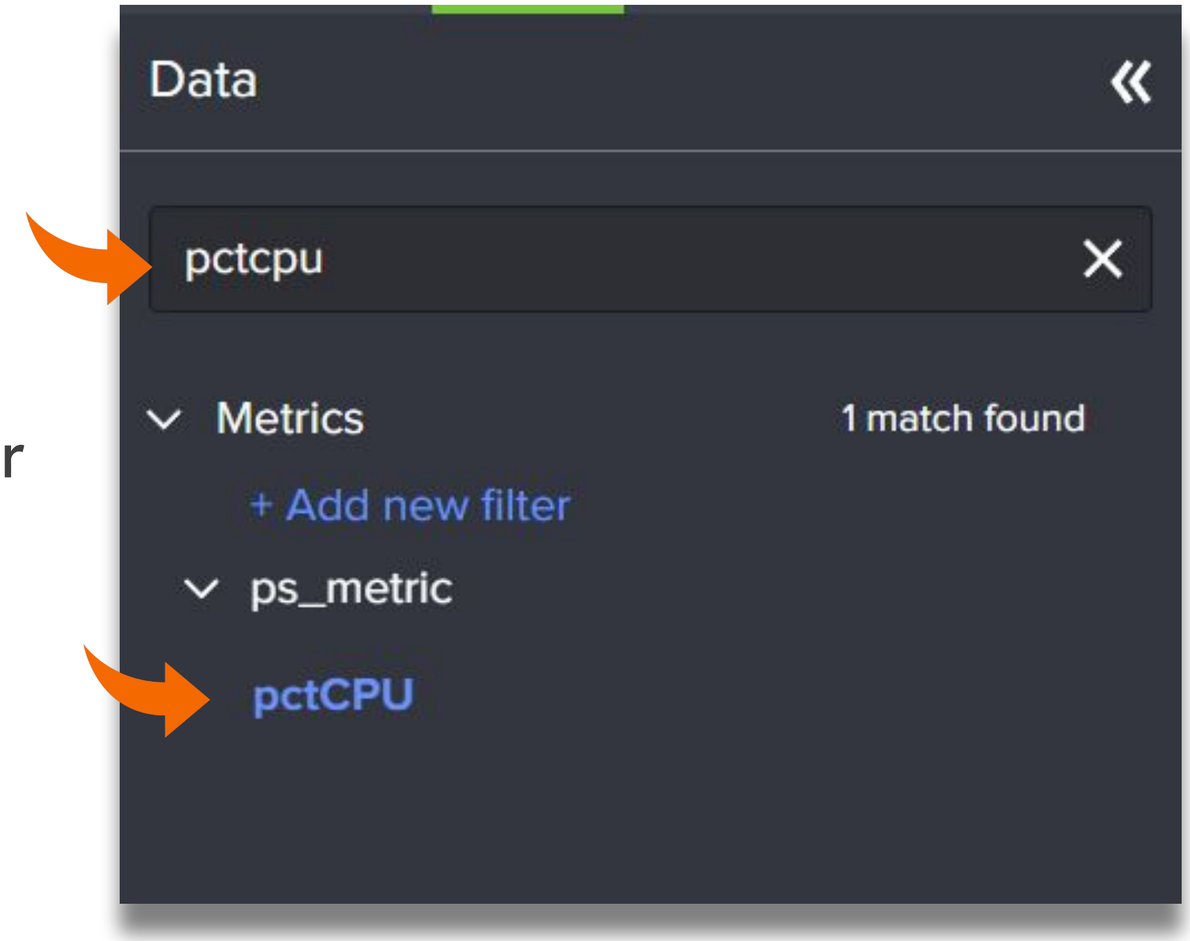
splunk>
a cisco company

Activity #6 - Create an Alert

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

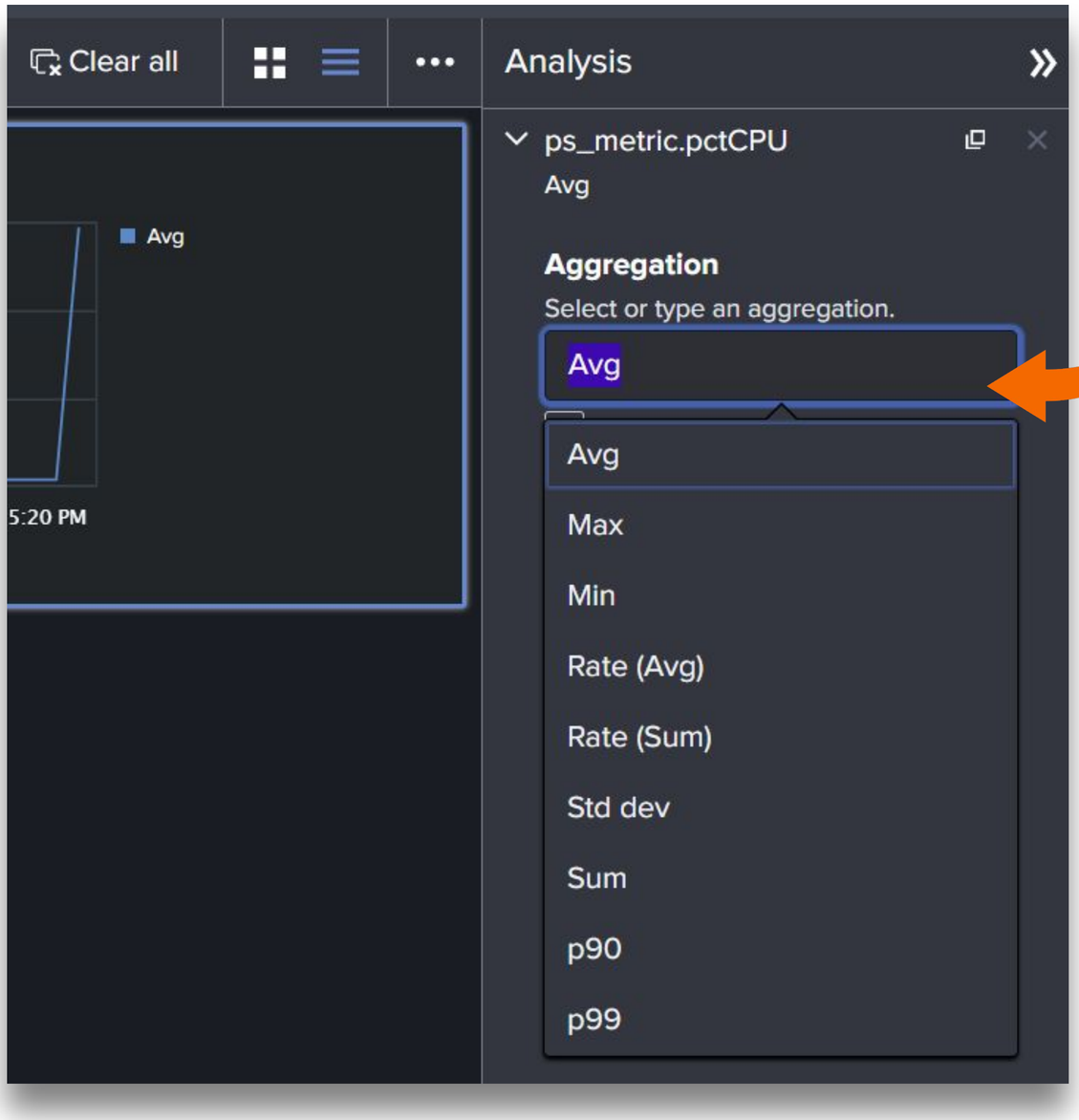
pctCPU

Click on **pctCPU** under ps_metrics



splunk>
a cisco company

Activity #6 - Create an Alert

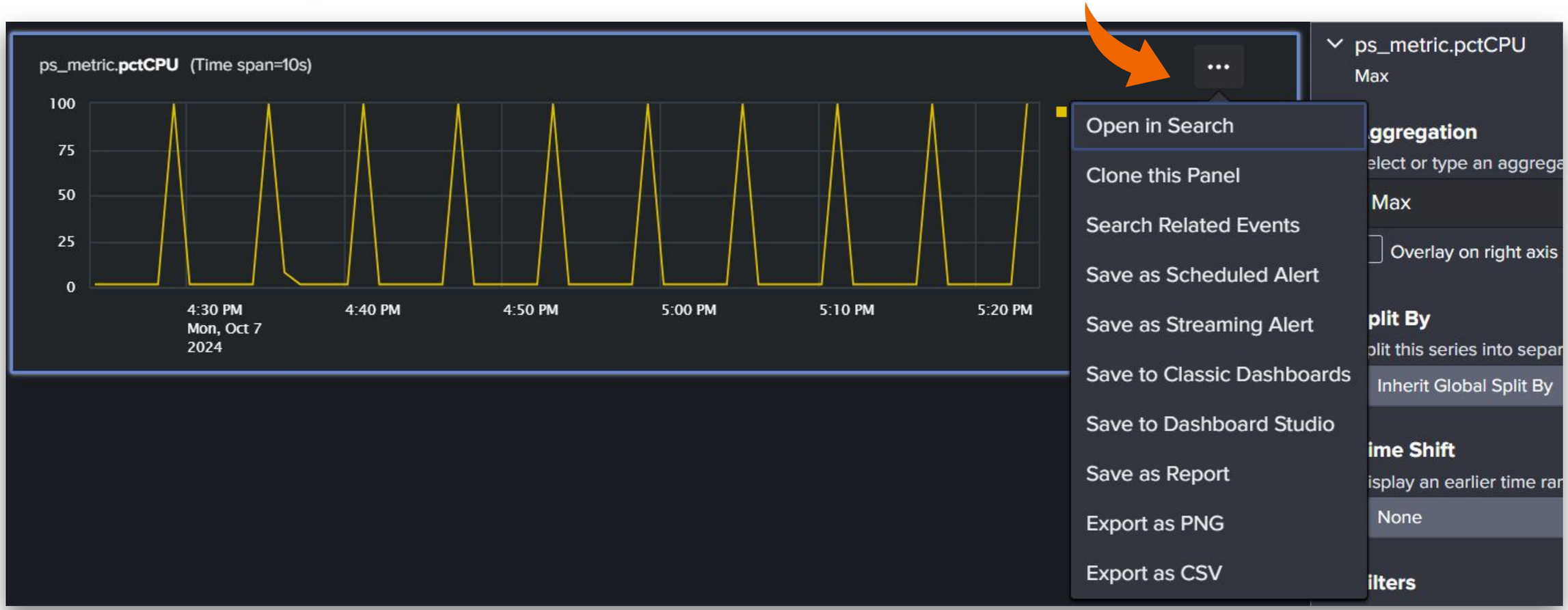


Change the **Aggregation** from **Avg** to **Max**

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.



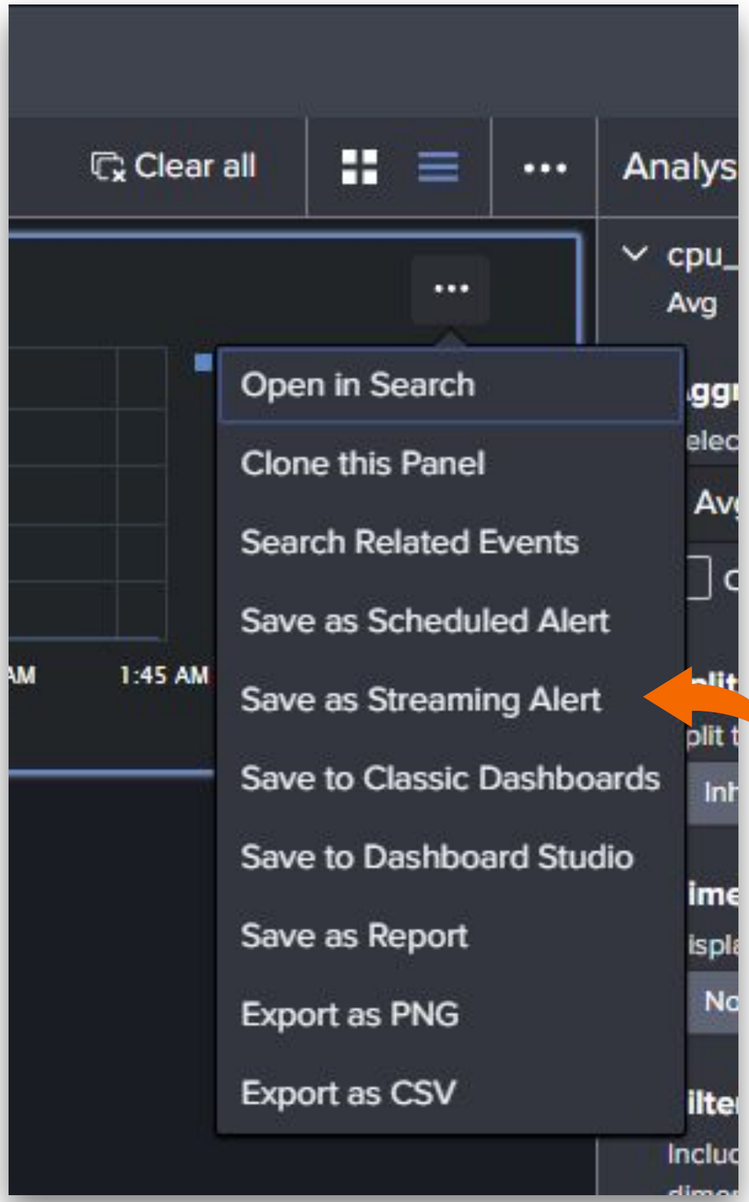
splunk> a cisco company

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**

splunk> a cisco company

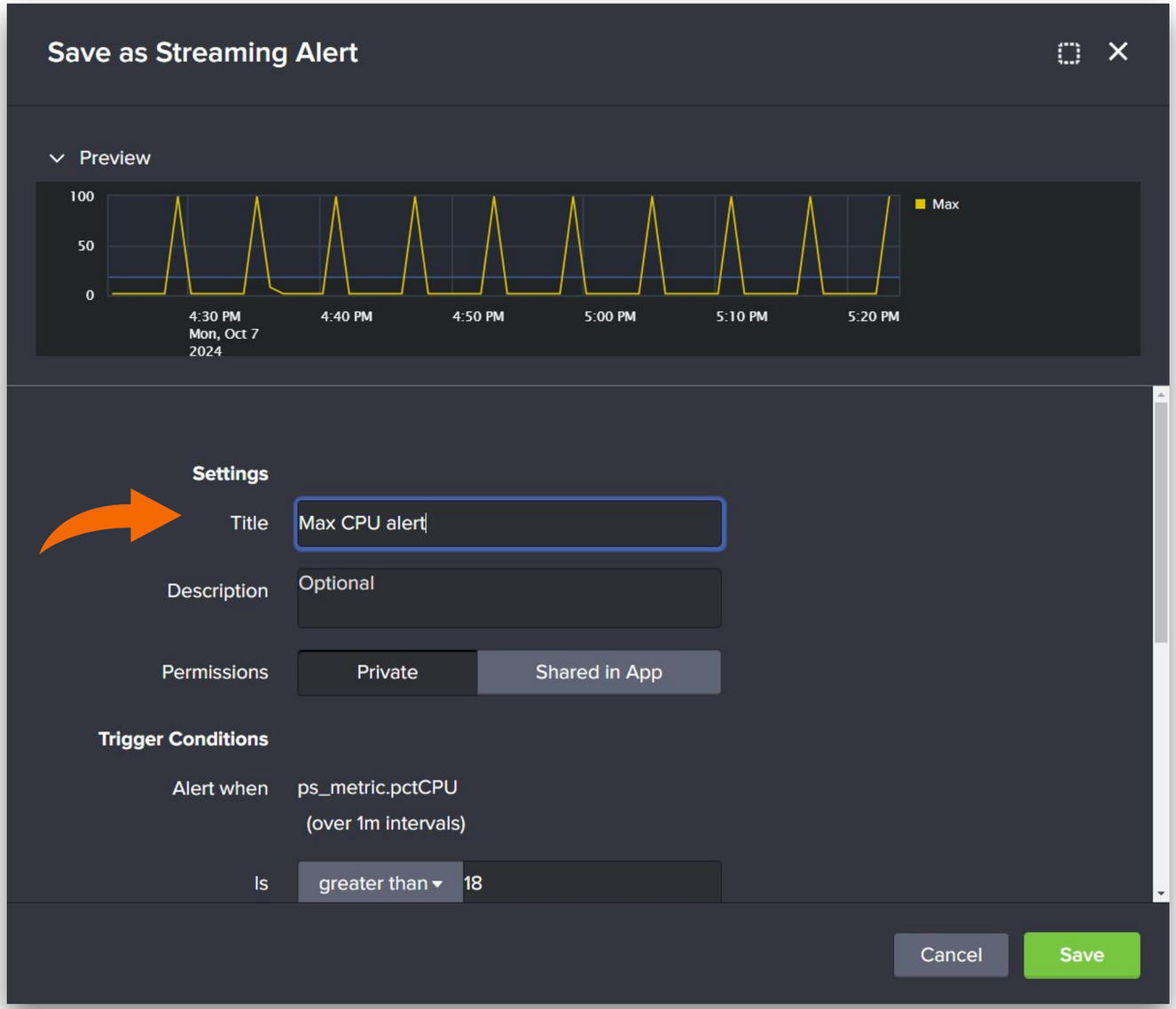
Activity #6 - Create an Alert

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 you're alert a Title:
For example: **Max CPU alert**



splunk>
a cisco company

Activity #6 - Create an Alert

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

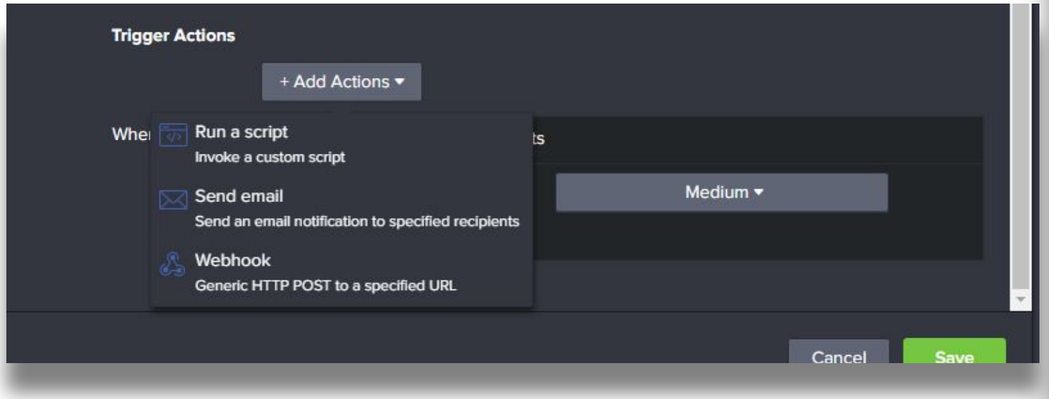
Next, Click on **Severity** and chose **High**

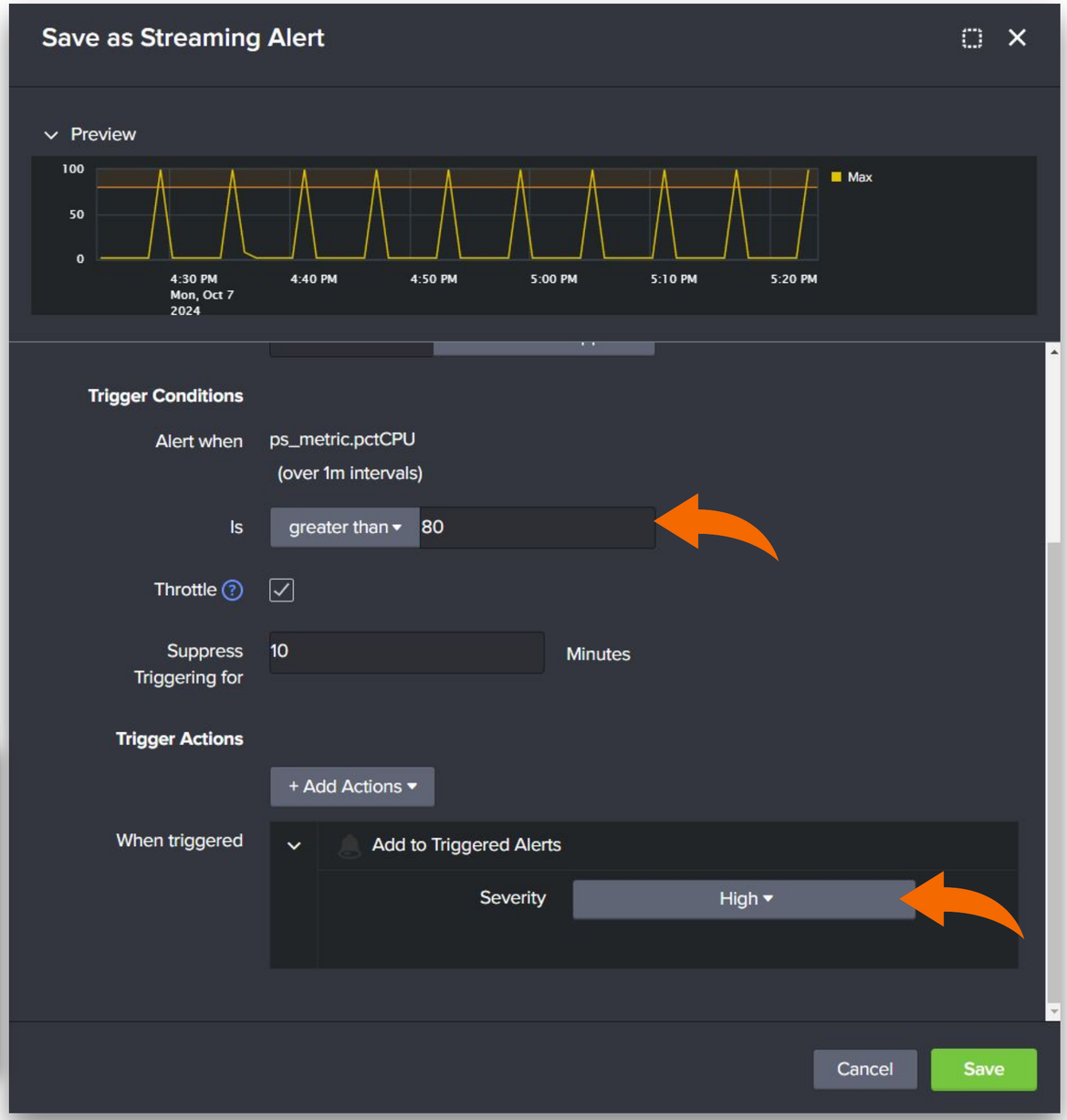
The **Preview** panel should have updated automatically with the new values.

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.





splunk>
a cisco company

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.

splunk> a cisco company

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

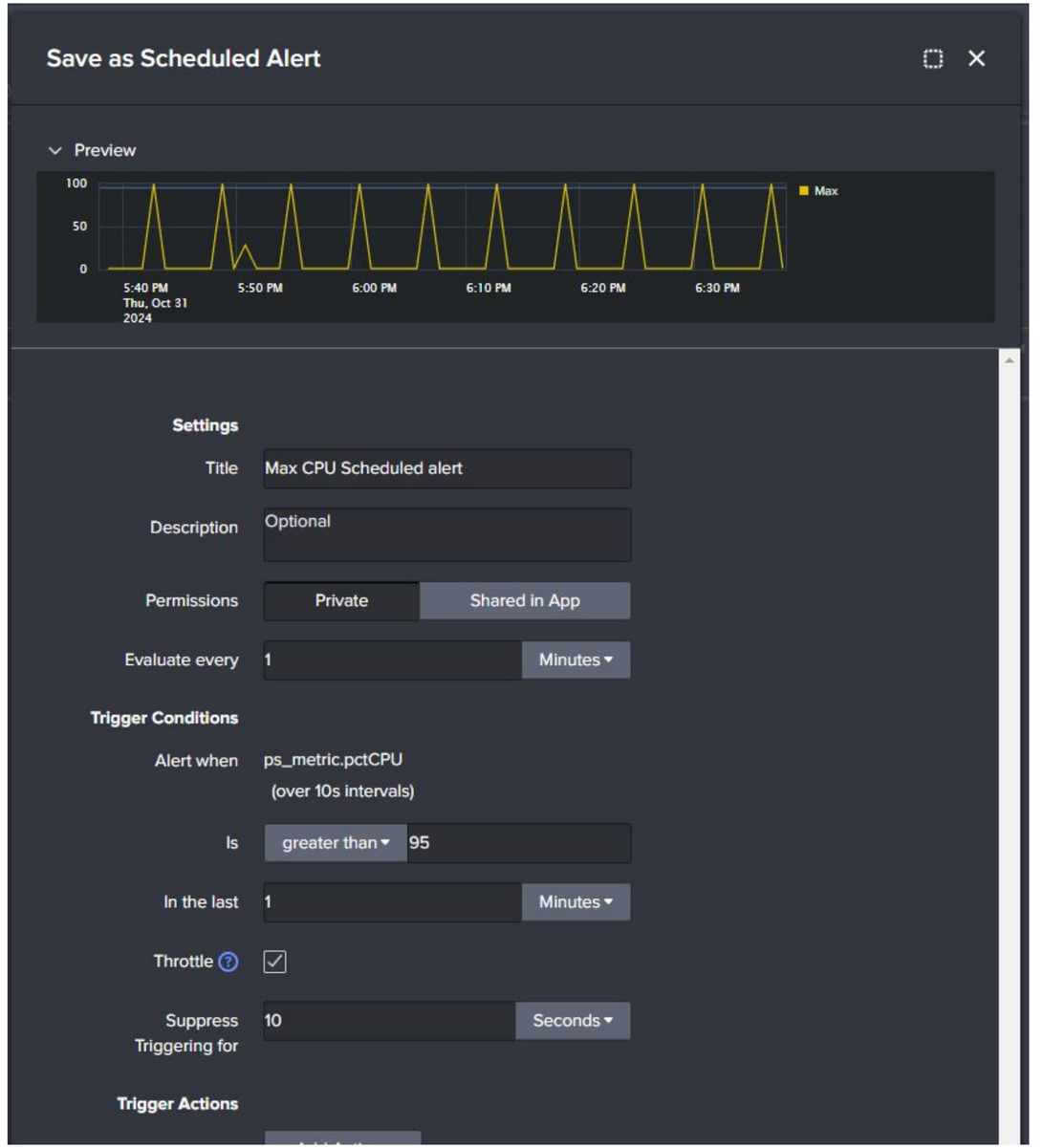
Give you're alert a Title:
For example: **Max CPU scheduled alert**

Notice now we have **Evaluate every** option

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

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

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

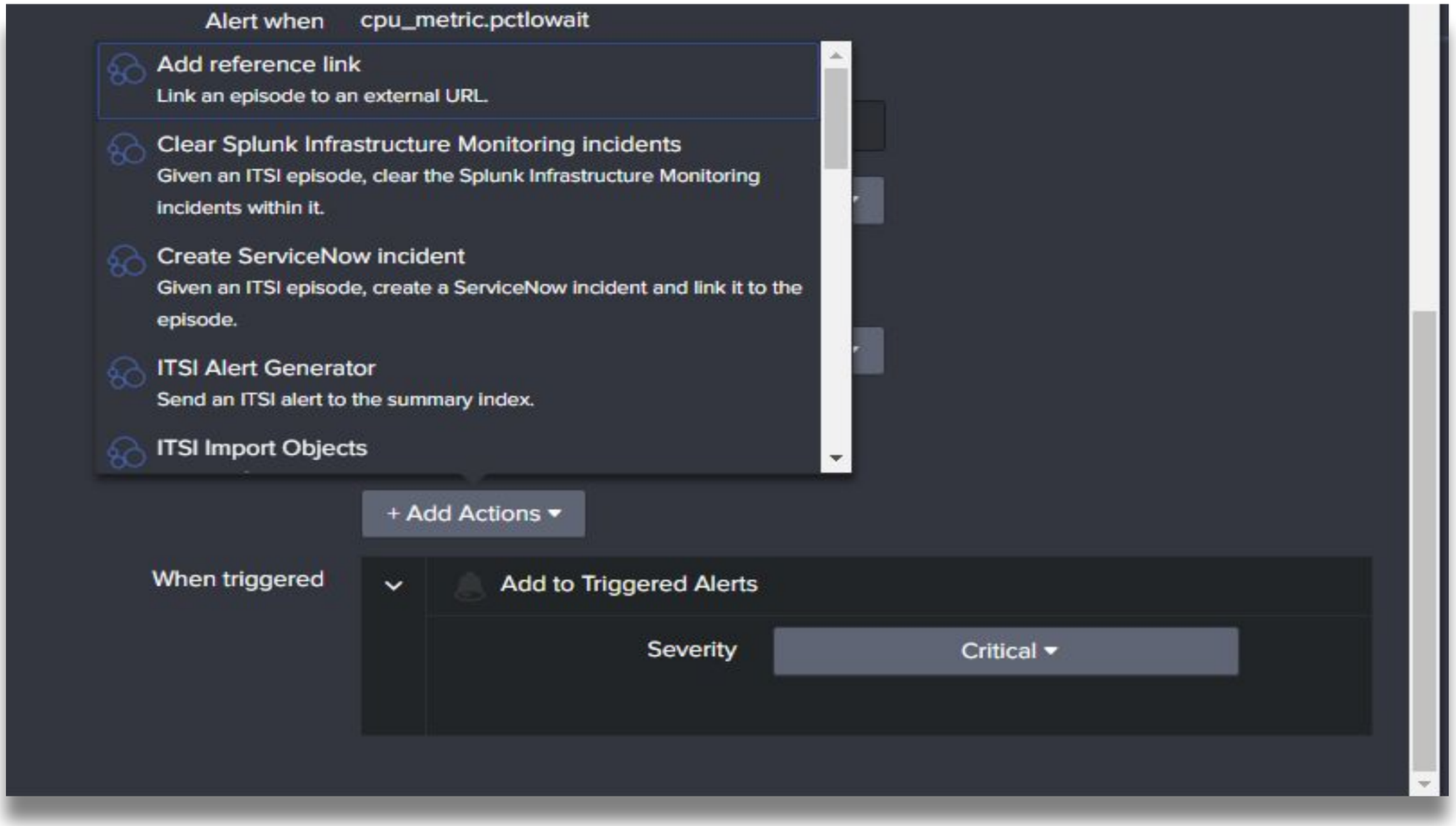


splunk> a cisco company

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**

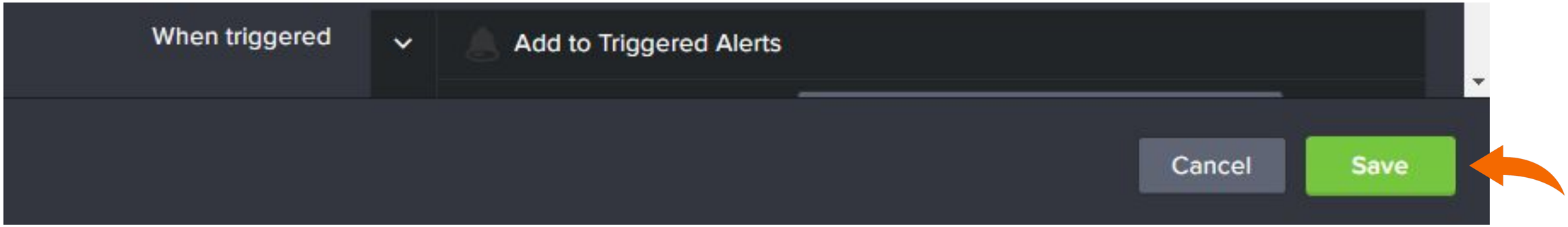


splunk> a cisco company

Activity #6 - Create an Alert

Once your finished reviewing all the option of **Scheduled Alert**

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



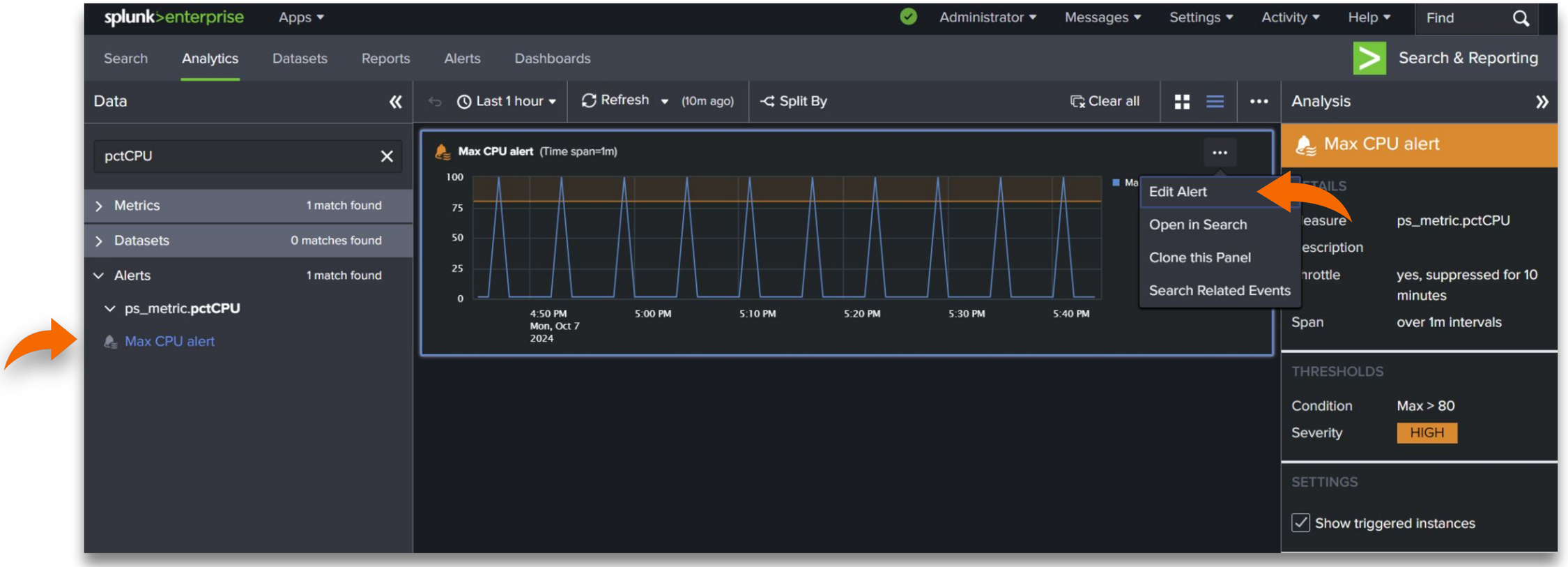
splunk>
a cisco company

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 A**nalytics Workspace** you can find the alert you created under **Alerts** in the left side menu.

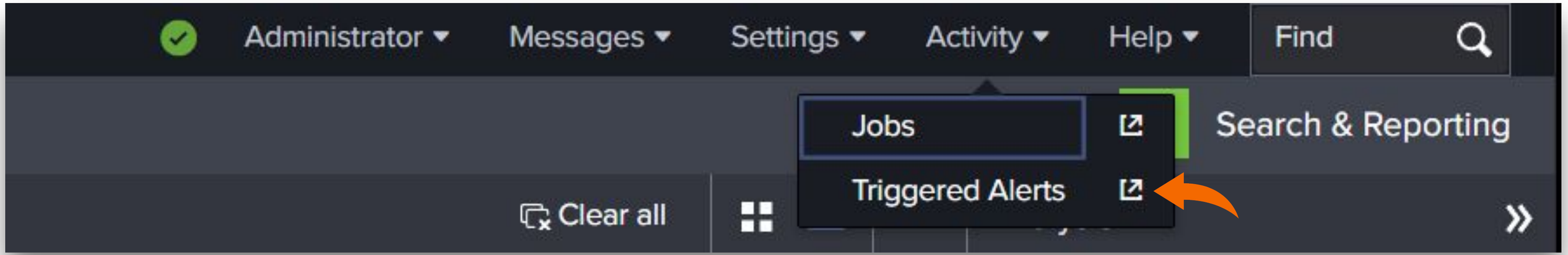
Click on the alert you created and review the information presented.

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**

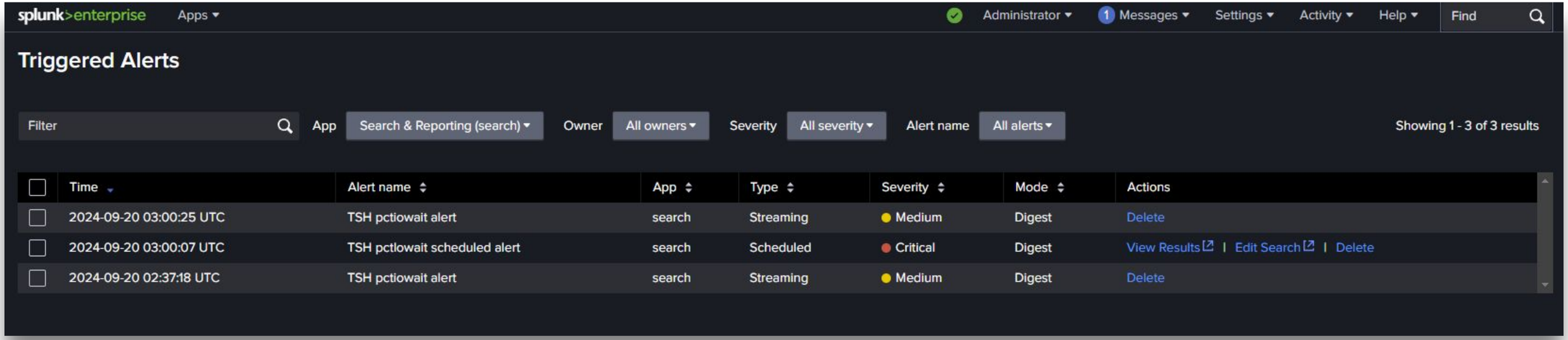


Click the icon next to **Triggered Alerts** to open in a new window

splunk>
a cisco company

Activity #6 - Create an Alert

Examples of alerts that have fired

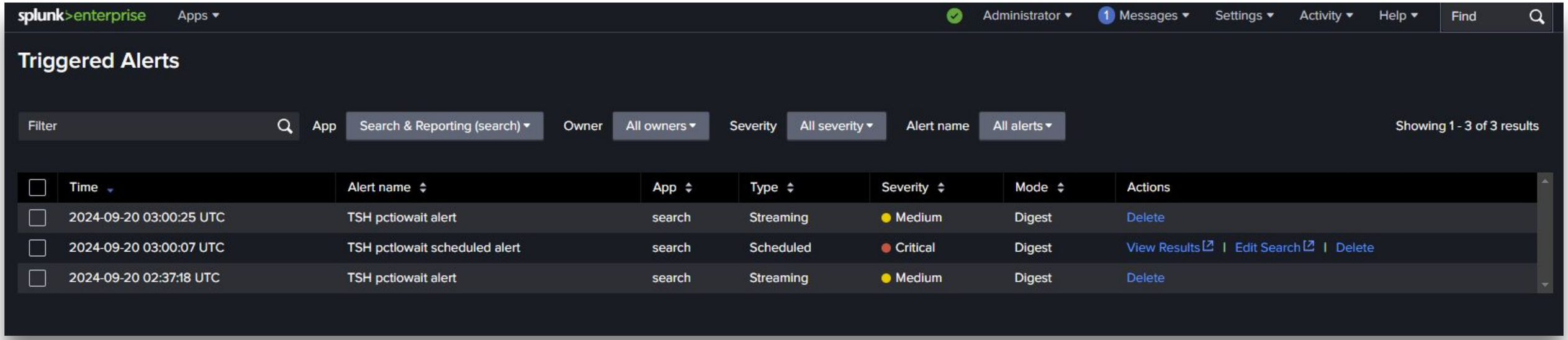


splunk>
a cisco company

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**.



splunk>
a cisco company

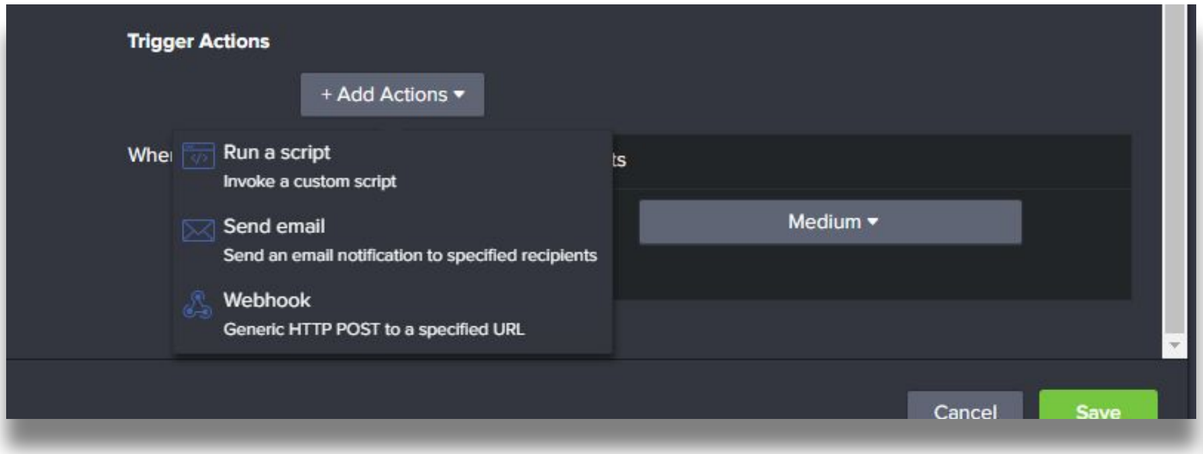
Activity #6 - Create an Alert

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

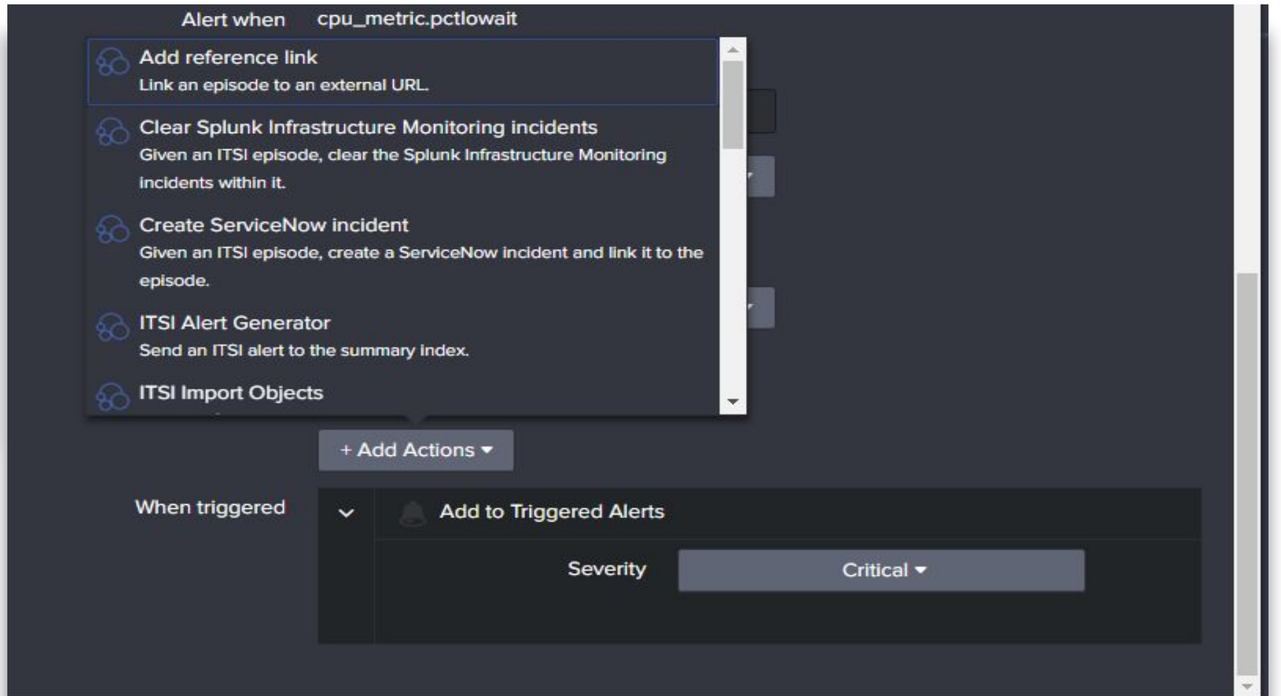
- **Streaming alerts** do not show up in **Settings - Searches,Reports and Alerts**
  - you will need to use the Analytics Workspace to find and edit Streaming alerts

- Out of the box, there seems to be more options under **Add Actions** when creating a **Scheduled Alert**

Streaming Alert options



Scheduled Alert options



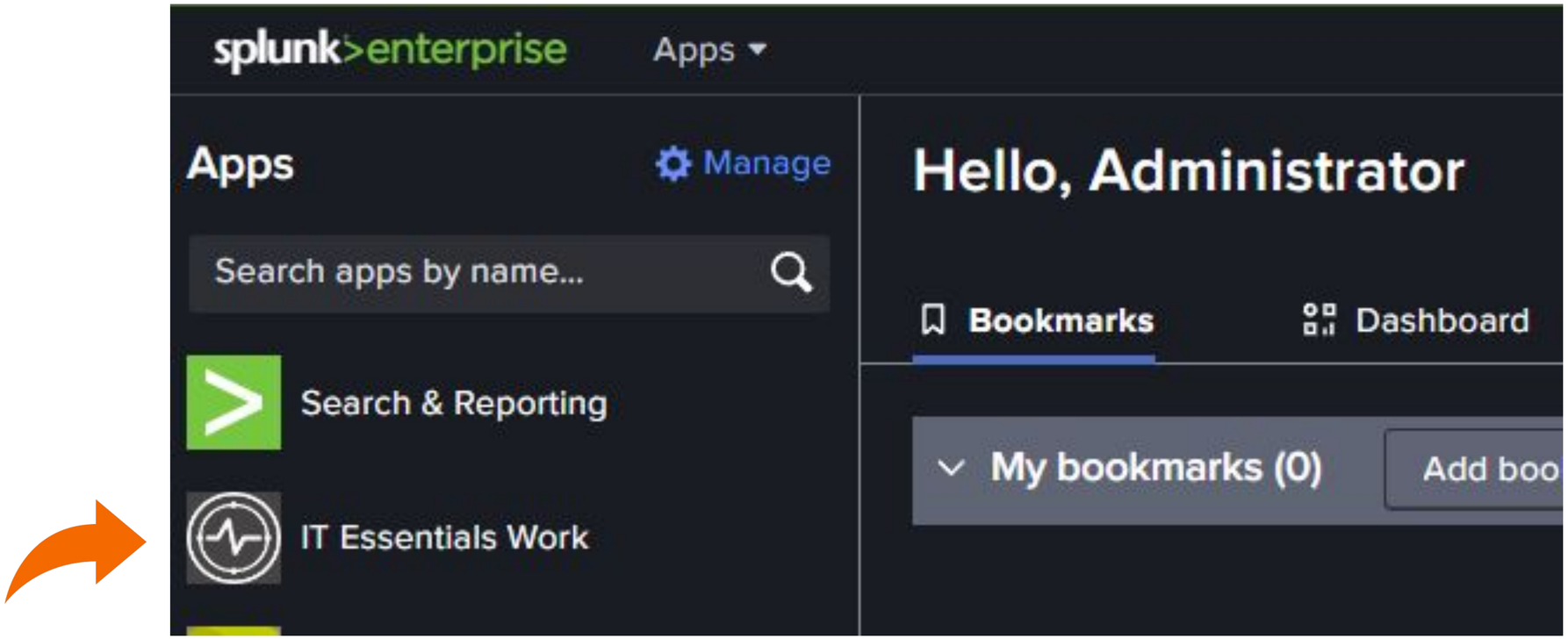
splunk> a cisco company

Activity #7 - Exploring IT Essentials Work

splunk> a CISCO company

Activity #7 - ITE Works

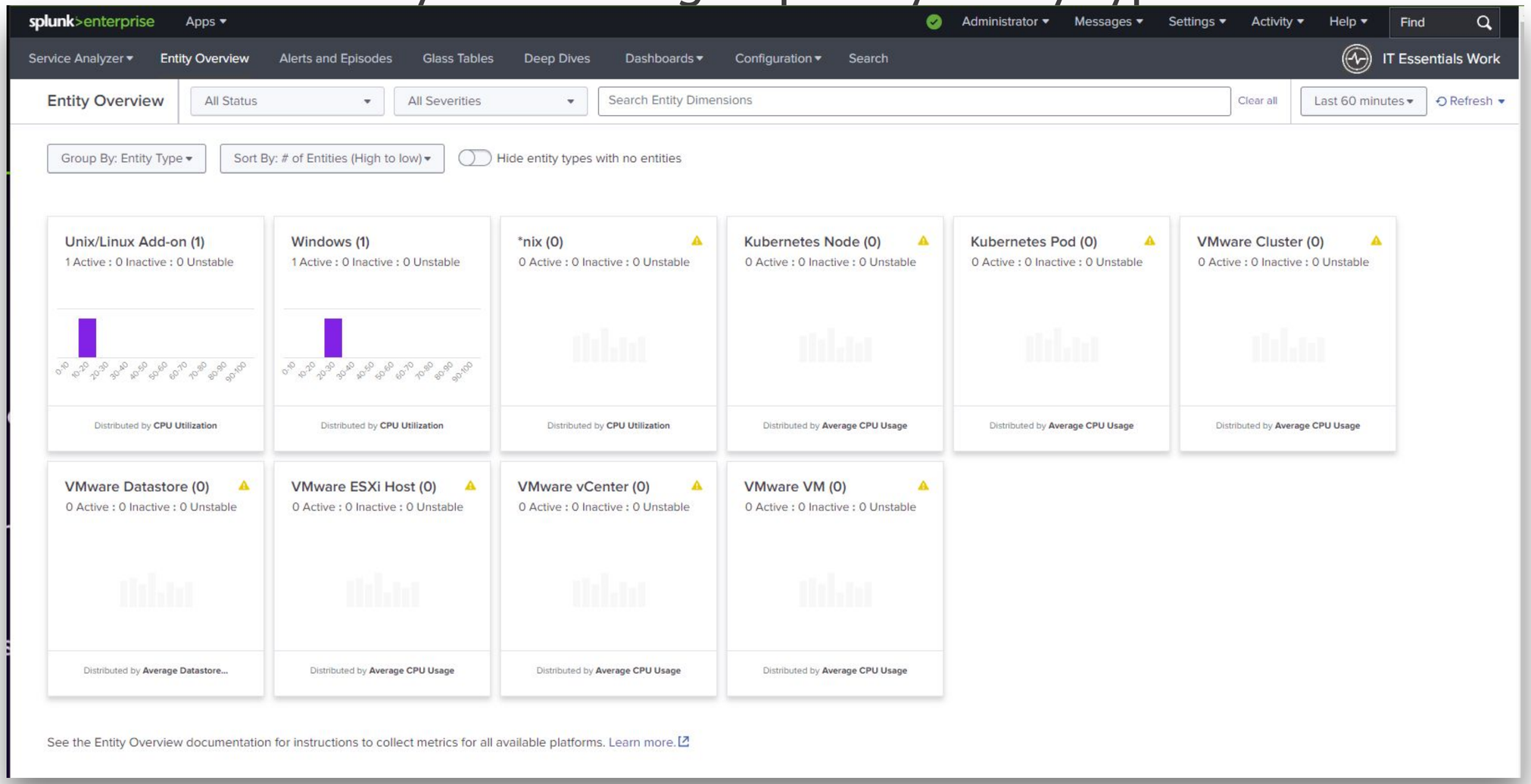
In your browser, navigate again to the IT Essentials Work app



splunk>
a cisco company

Activity #7 - ITE Works

Entity Overview grouped by entity types

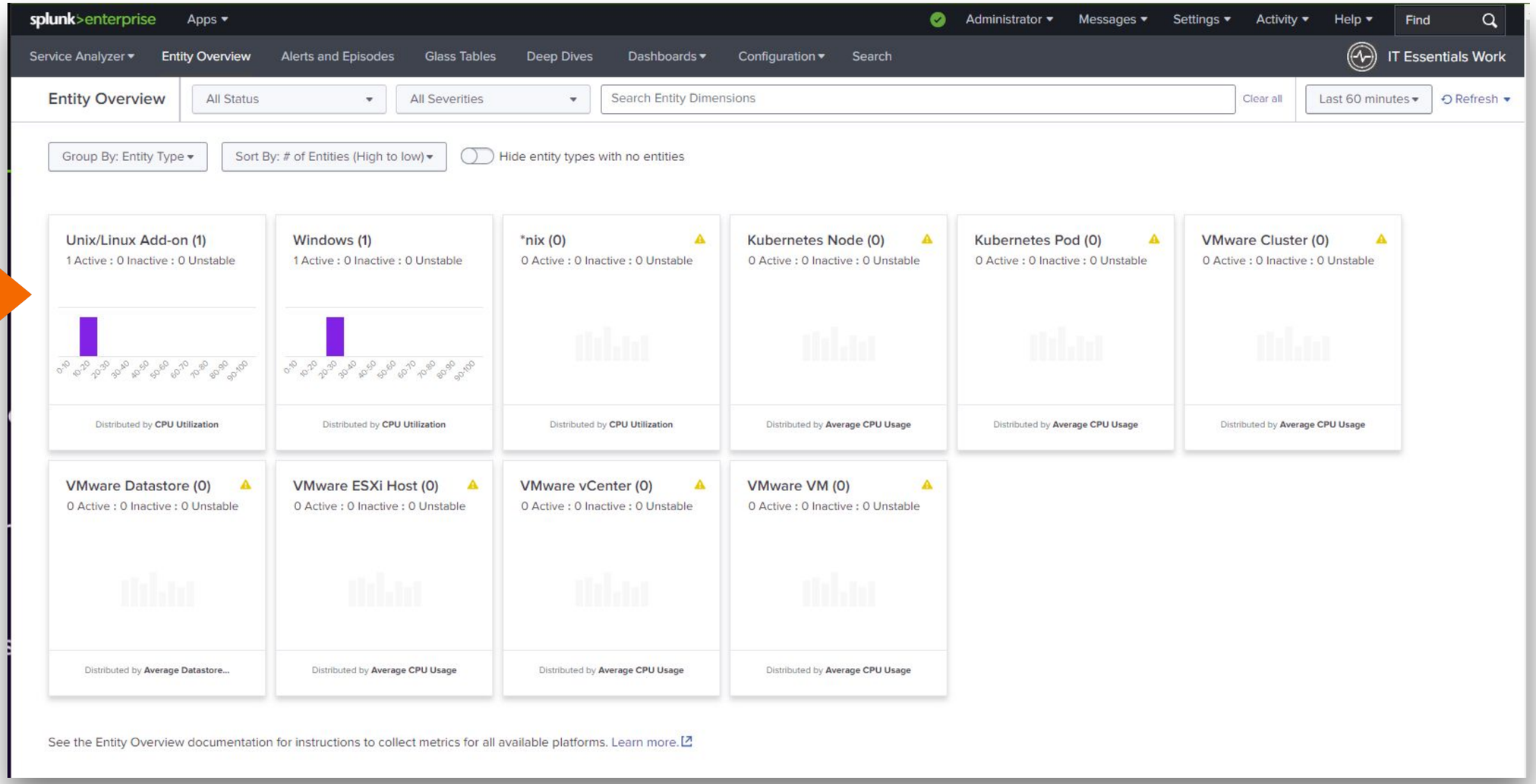


splunk> a cisco company

Activity #7 - ITE Works

Entity Overview

Click the tile:
Unix/Linux Add-on



splunk>
a cisco company

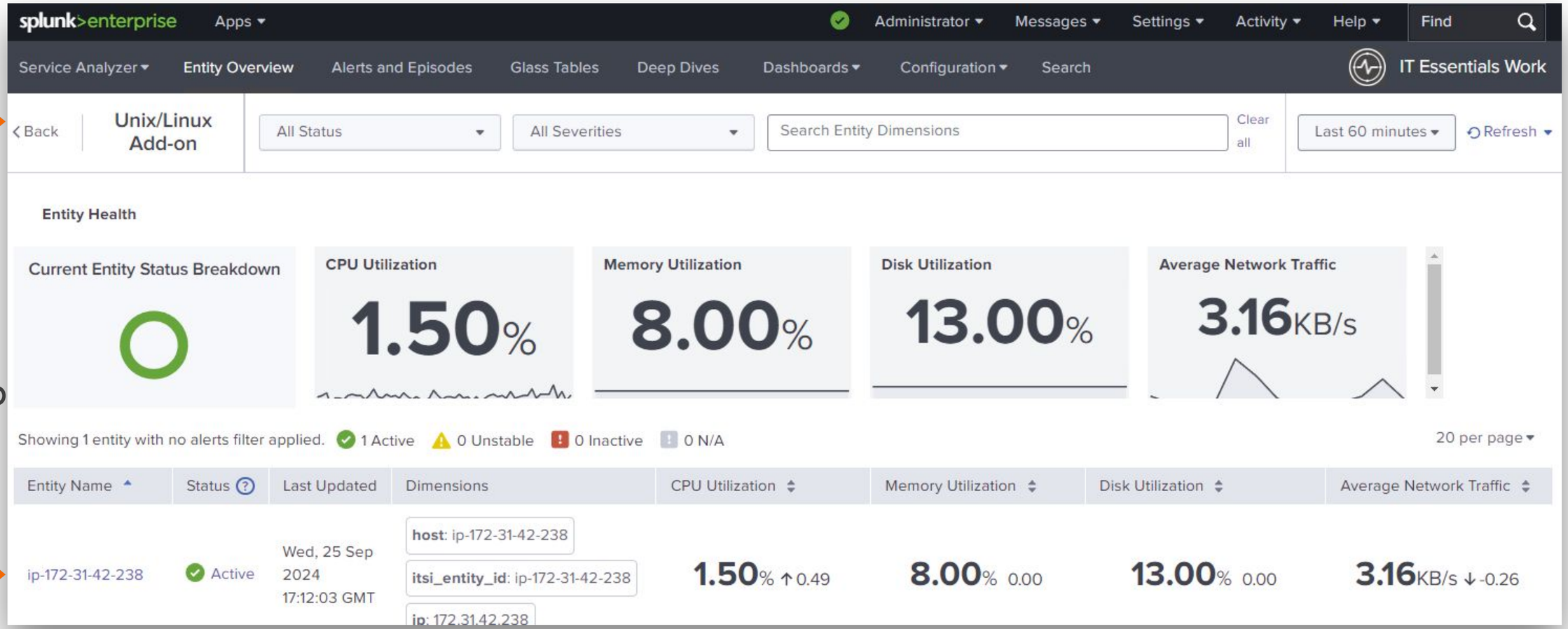
Activity #7 - ITE Works

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

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

Review the filter boxes

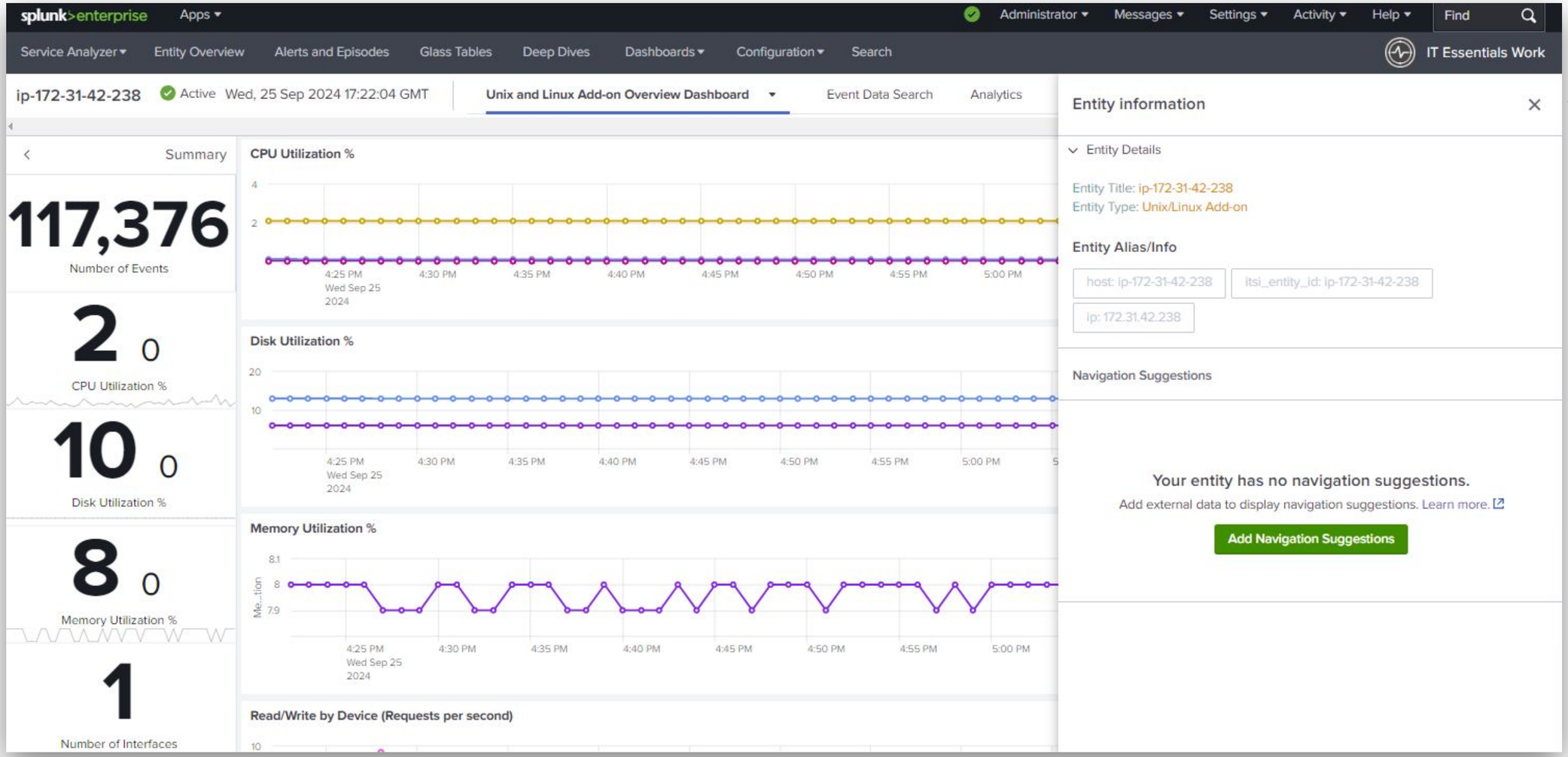
Click the top **Entity Name**



splunk>
a cisco company

Activity #7 - ITE Works

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

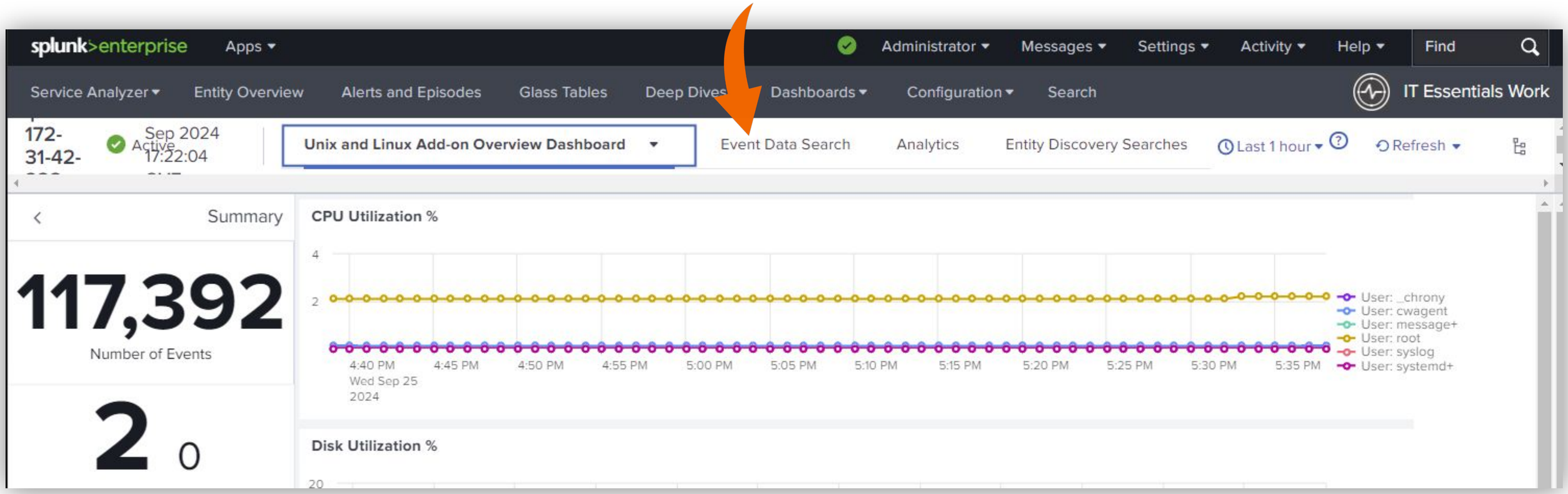


Click the **X** to close the information menu

Activity #7 - ITE Works

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

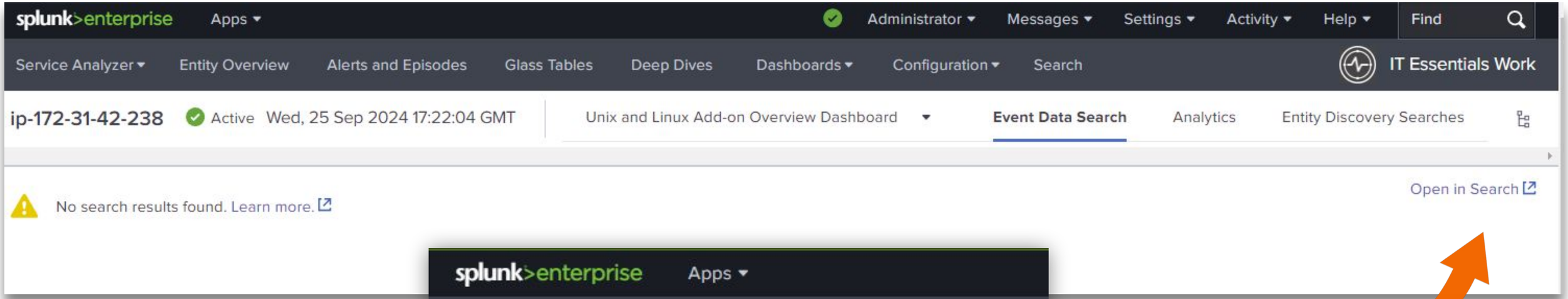
Click **Event Data Search**



splunk>
a cisco company

Activity #7 - ITE Works

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

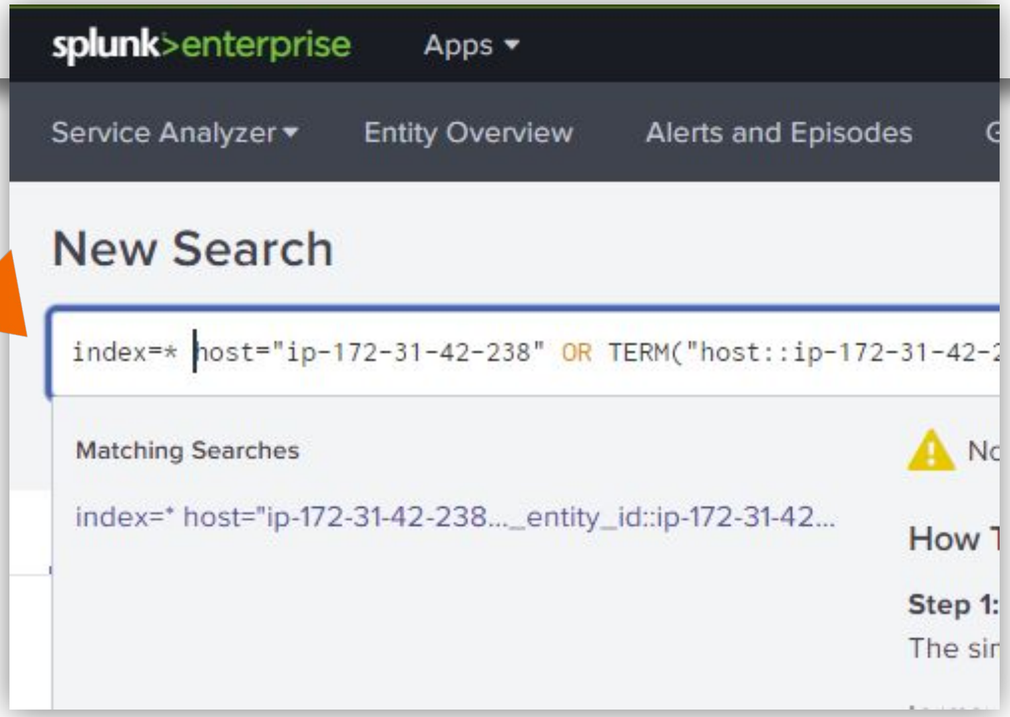


Click **Open in Search**

A new tab should have opened

Add this to the search:

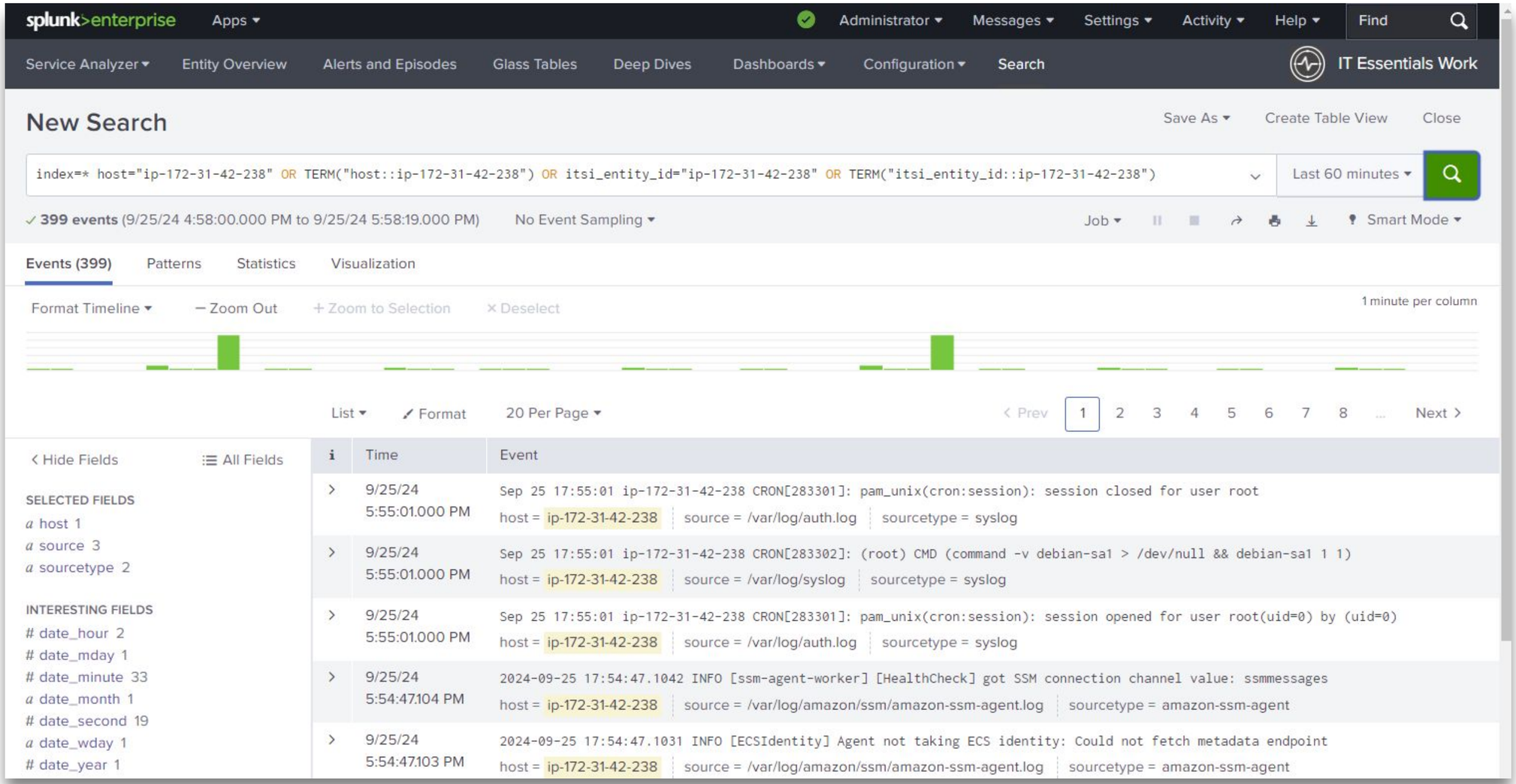
index=*



splunk>
a cisco company

Activity #7 - ITE Works

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

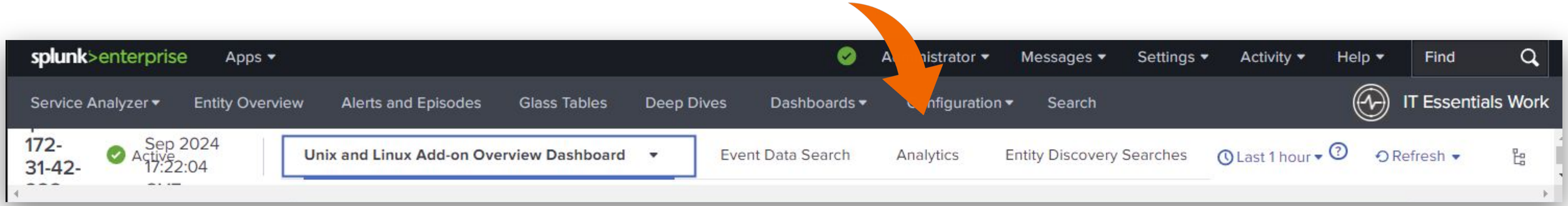


splunk>
a cisco company

Activity #7 - ITE Works

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

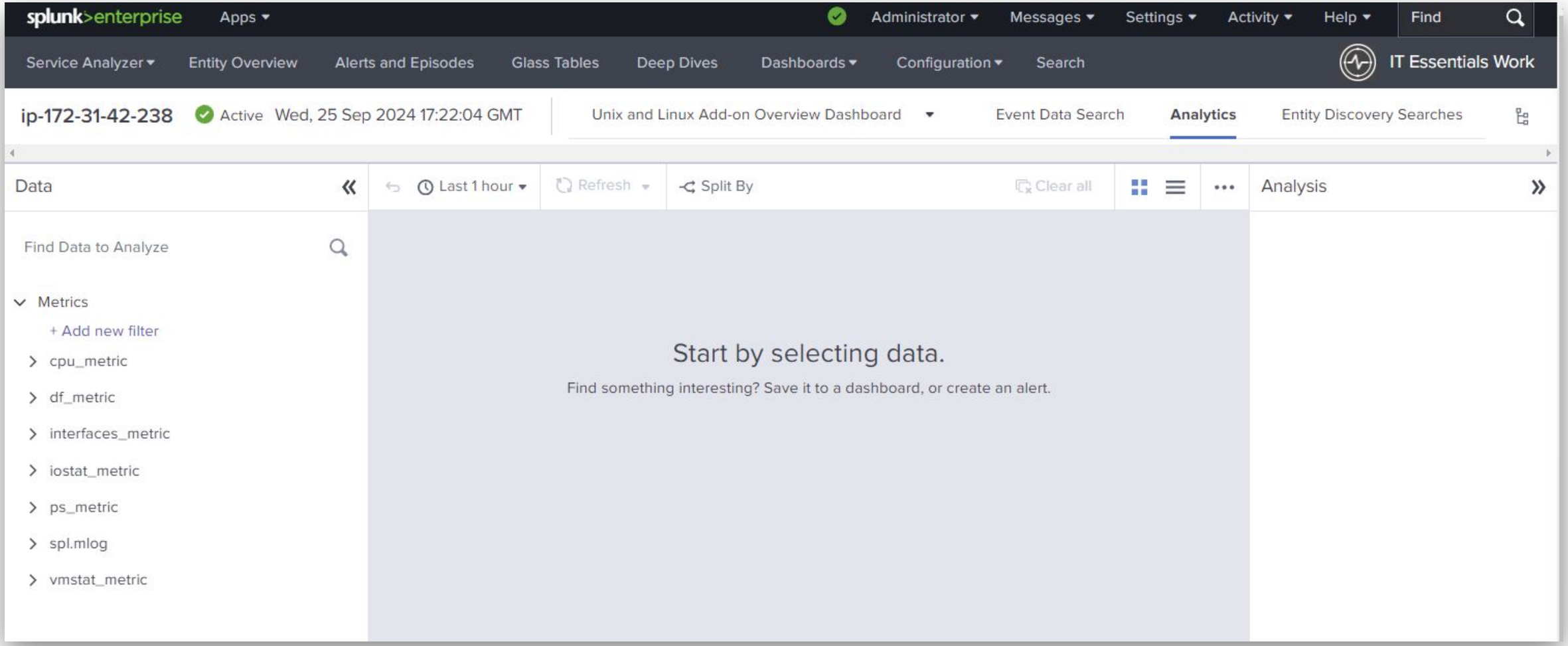
Click **Analytics**



splunk>
a cisco company

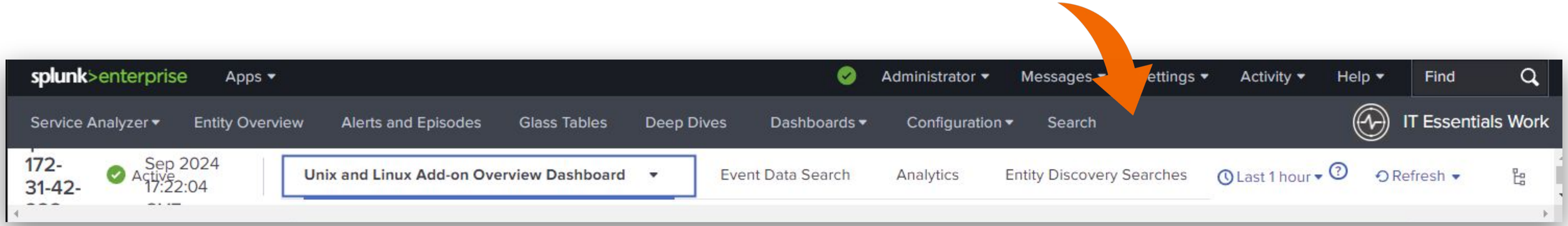
Activity #7 - ITE Works

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



Activity #7 - ITE Works

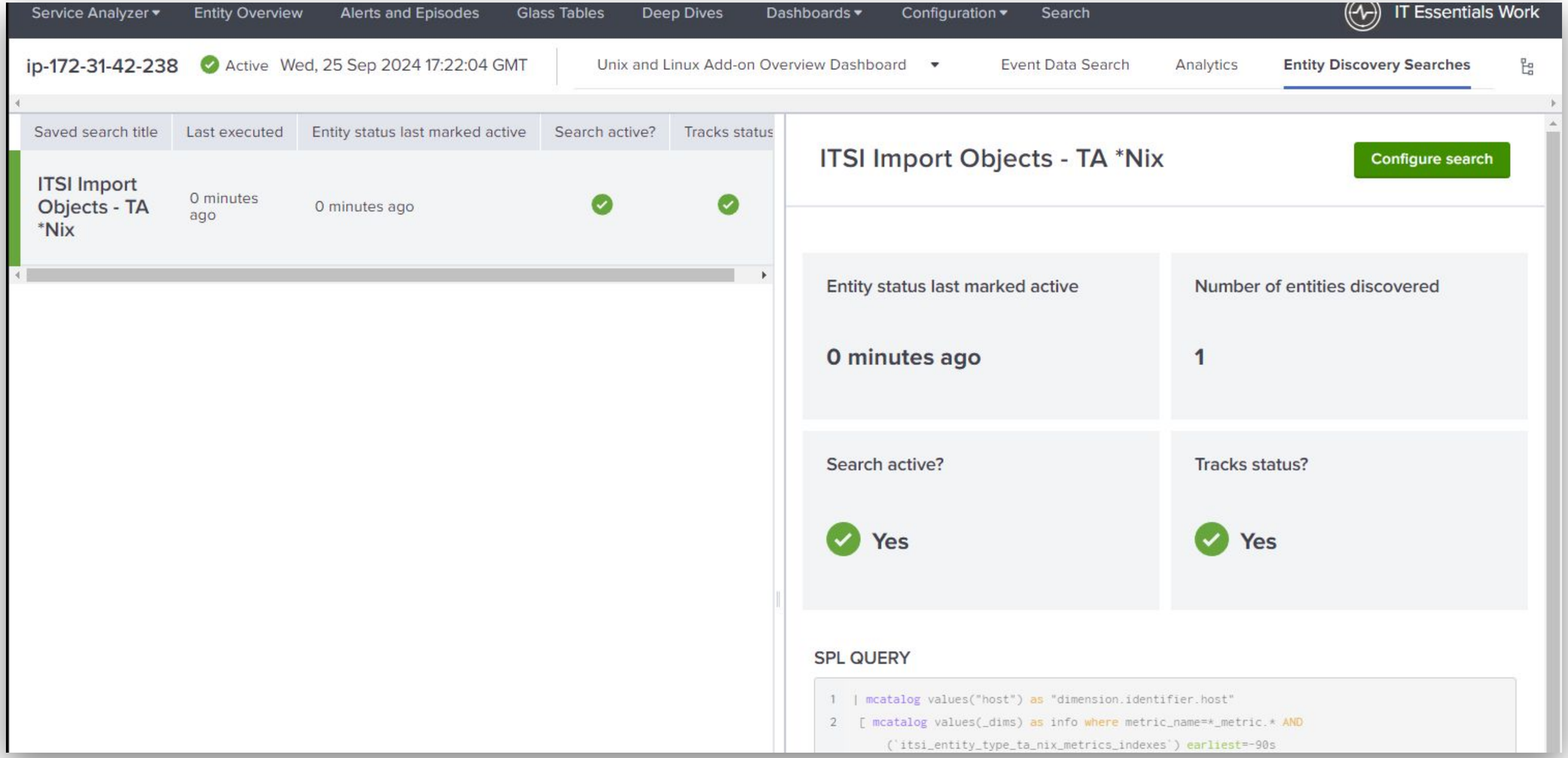
Click **Entity Discover Searches**



splunk>
a cisco company

Activity #7 - ITE Works

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



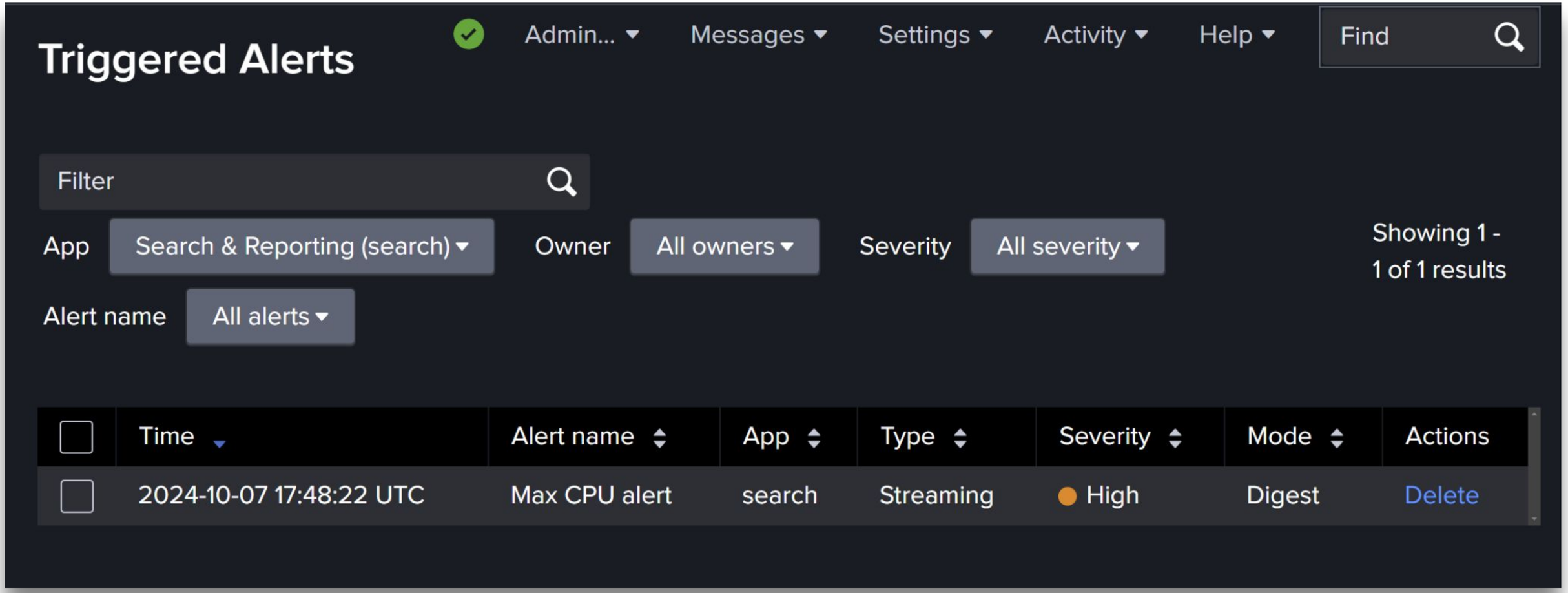
splunk> a cisco company

Activity #8 - Find what caused the alert

splunk>
a CISCO company

Activity #8 - Find what caused the alert

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



splunk>
a cisco company

Activity #8 - Find what caused the alert

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

splunk>
a cisco company

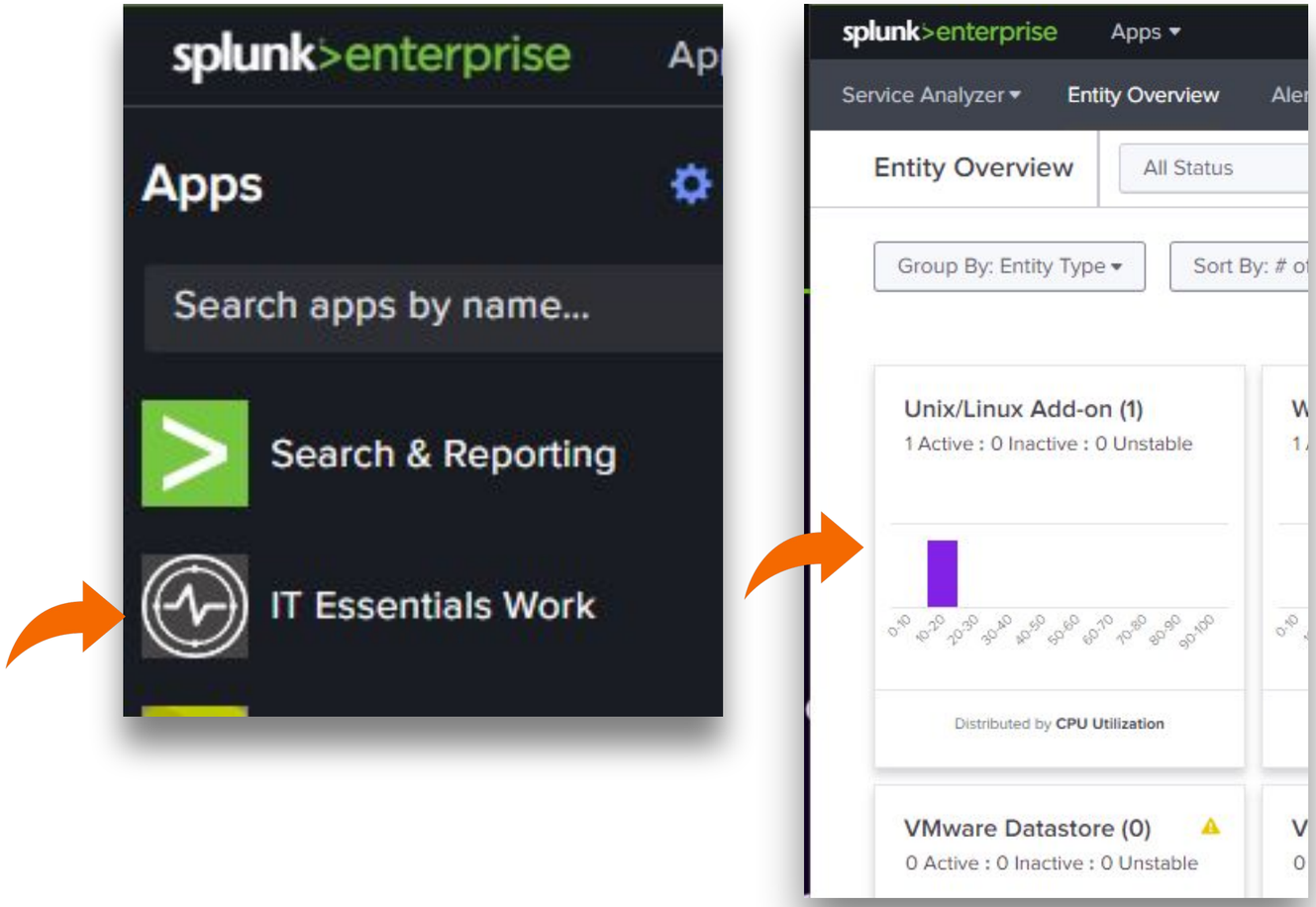
Did anyone find what triggered the alert?

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

splunk> a CISCO company

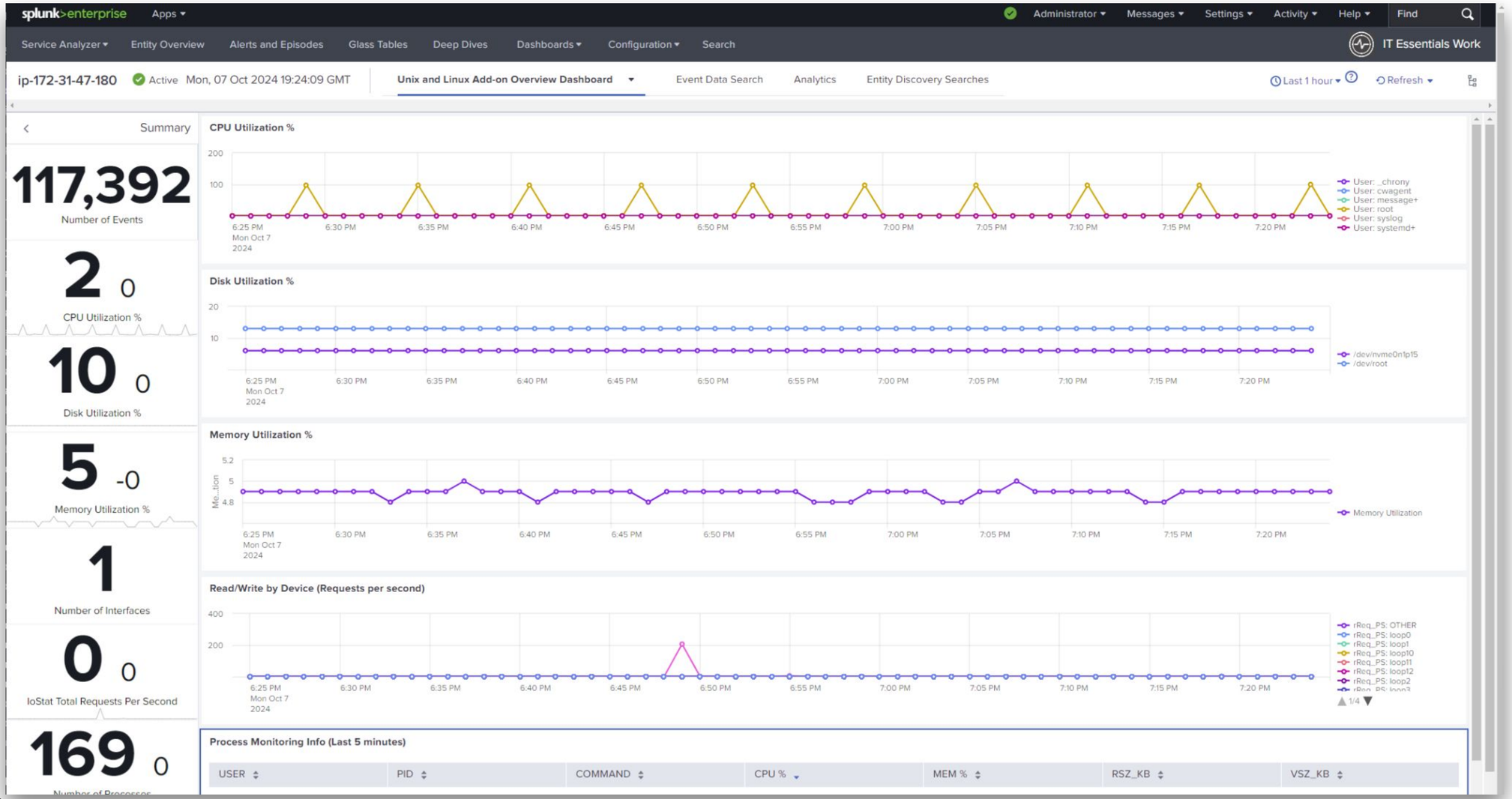
Activity #8 - Find what caused the alert

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



Activity #8 - Find what caused the alert

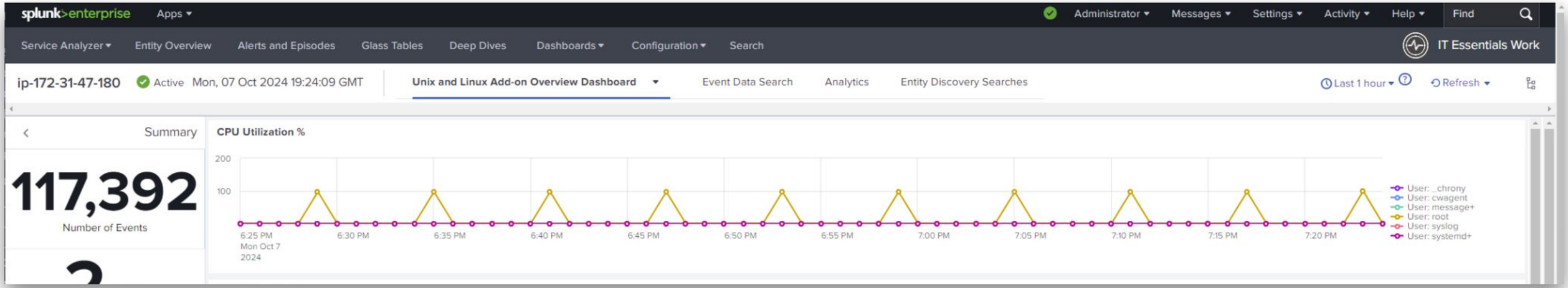
Now we can see the pre-built dashboard for that entity



splunk>
a cisco company

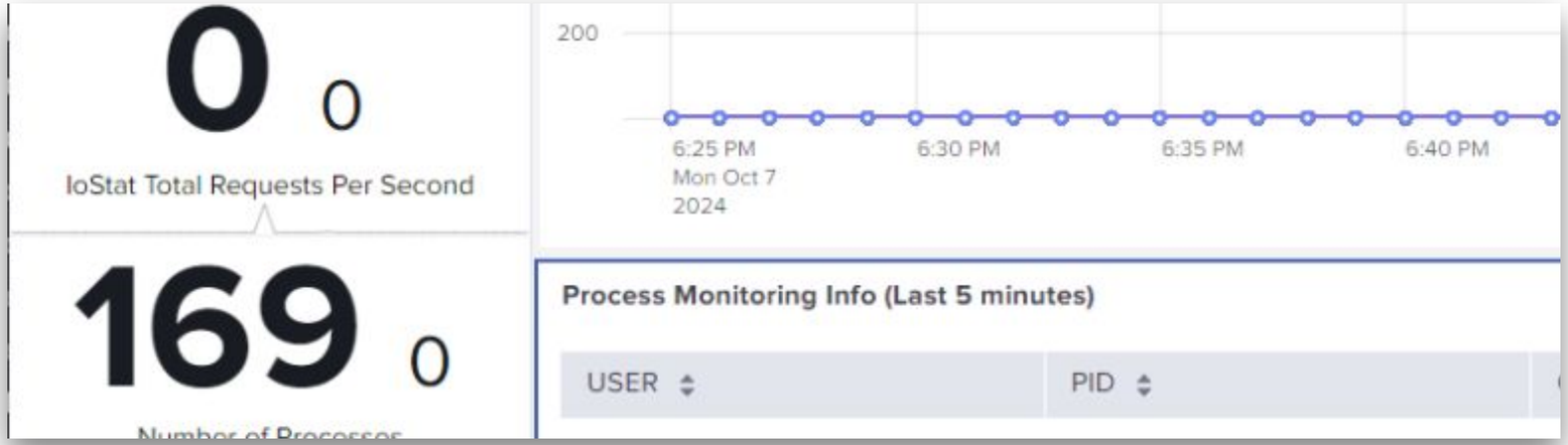
Activity #8 - Find what caused the alert

The top panel shows the **CPU Utilization** spikes



Did you notice the last panel for

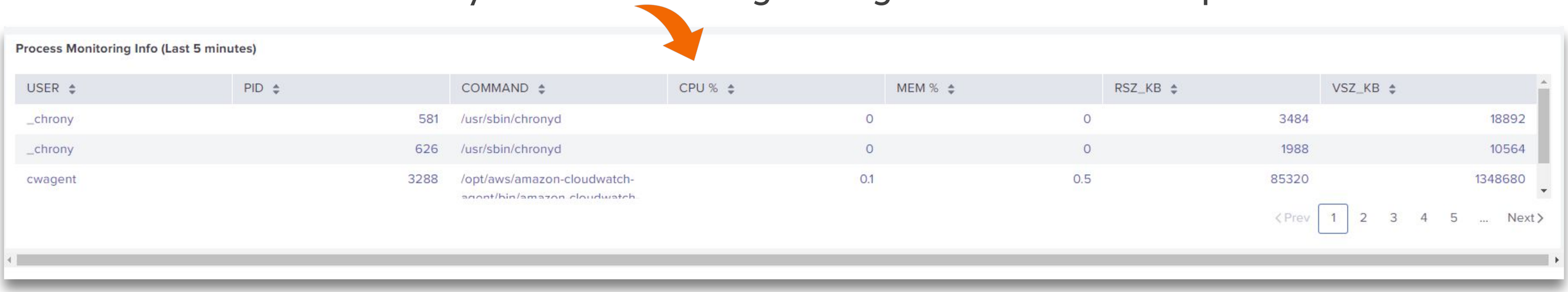
Process Monitoring Info



splunk>
a cisco company

Activity #8 - Find what caused the alert

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

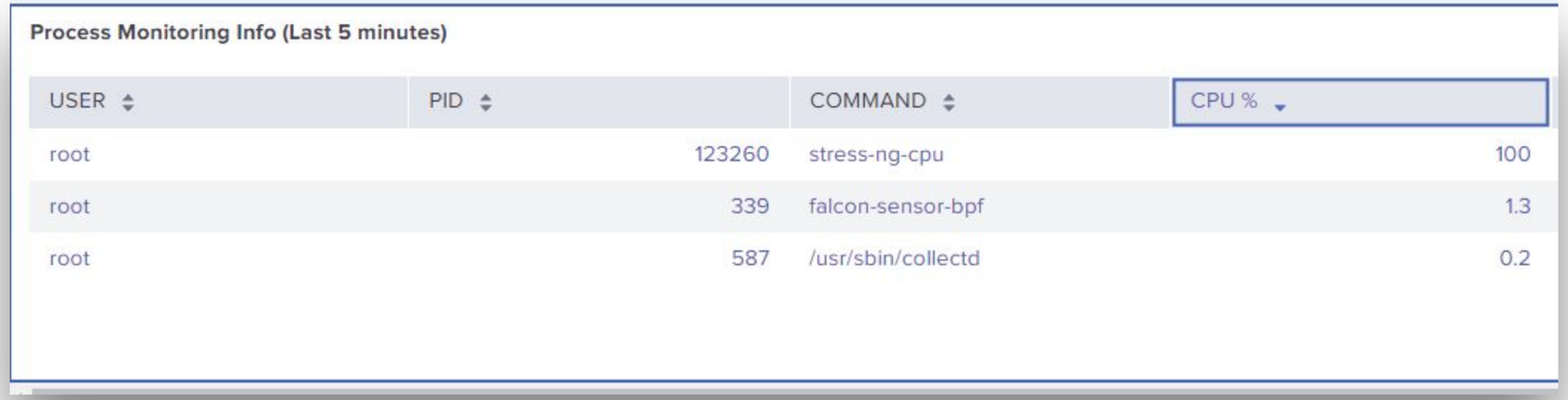


Process Monitoring Info (Last 5 minutes)

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

splunk> a cisco company

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:

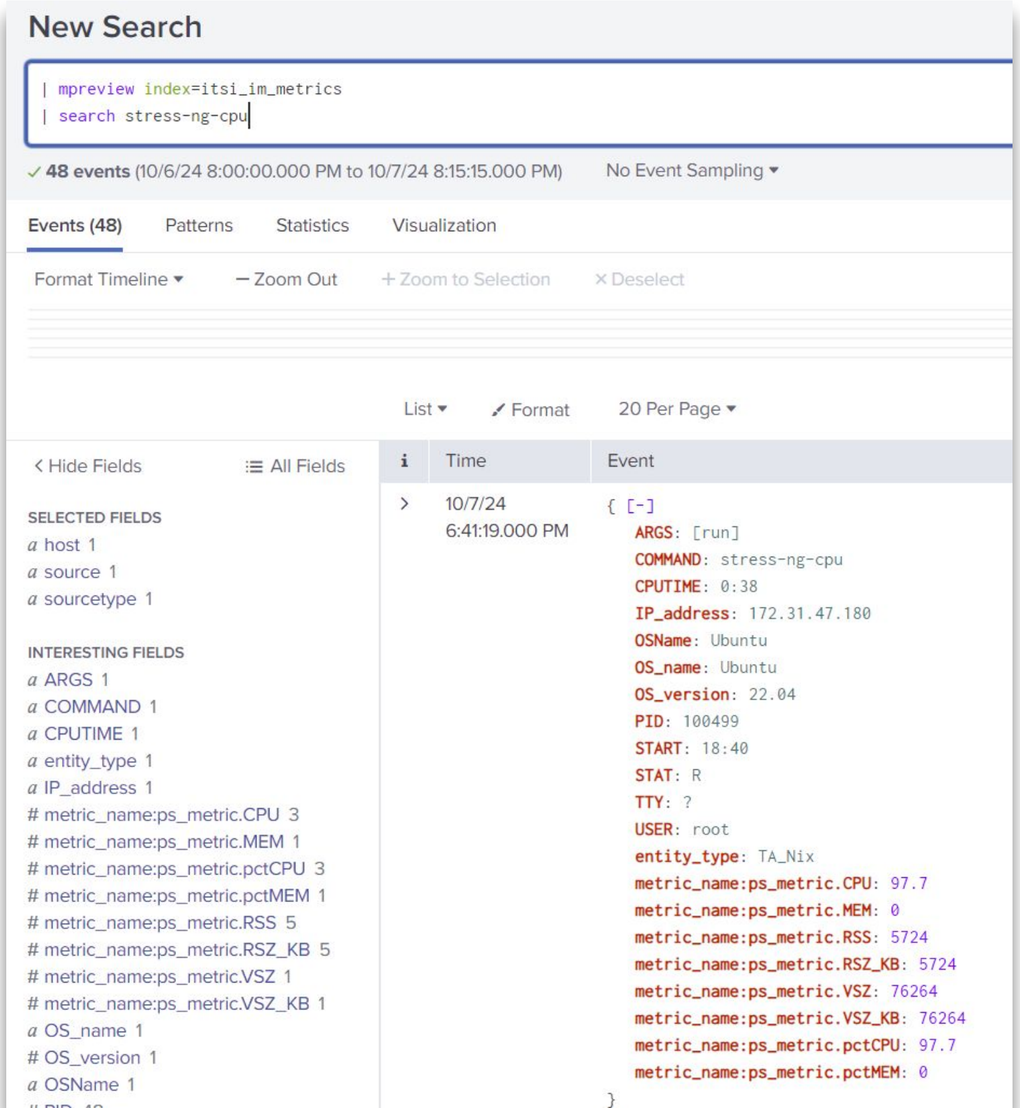
| mpreview index=itsi_im_metrics

| 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**



splunk>
a cisco company

Where do we go from here?

splunk> a CISCO company

Splunk IT Service Intelligence

KPI-driven, predictive analytics solution for digital services

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

splunk> a CISCO company

Crushing metrics, one workshop at a time!

splunk> a cisco company

Thank You