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> .conf22

Out With the Old; In With the New! Migrating Your Monitoring From Legacy Windows and *Nix Splunk Apps to ITSI and IT Essentials Work

OBS1493C

Jonathan Fair

Professional Services | Splunk

Marco Stadler

Professional Services | Splunk

splunk> .conf22

Jonathan Fair

Professional Services Lead Architect
Global Services ITOps and Observability

Marco Stadler

Professional Services Architect
EMEA ITOps and Observability

splunk> .conf22

Moving

Moving

- 11 Times!

Moving

- 11 Times!
- In the Summer

Moving Tips!

Moving Tips!

- Be Ready

Moving Tips!

- Be Ready
- Keep all walkways clear

Moving Tips!

- Be Ready
- Keep all walkways clear
- Have a plan for furniture placement

Moving + Splunk = ?

We are here to help

Why the change?

- Legacy Apps moved to ITE-Work / ITSI
- Common Framework for Monitoring
- Metric Index Support
- Entity Types Integration
- Vital Metrics
- New Dashboards

Migration Steps

Disable old

Disable the legacy app

Migration Steps

1

Disable old

Disable the legacy app

2

Install new

Install ITE-Work or ITSI

Install the Splunk App for Content Packs

Migration Steps

1

Disable old

Disable the legacy app

2

Install new

Install ITE-Work or ITSI

Install the Splunk App for Content Packs

3

Configuration

Change settings if needed

Enable Alerts

Migration Steps

1

Disable old

Disable the legacy app

2

Install new

Install ITE-Work or ITSI

Install the Splunk App for Content Packs

3

Configuration

Change settings if needed

Enable Alerts

ITE-Work / ITSI Dashboards / Reports

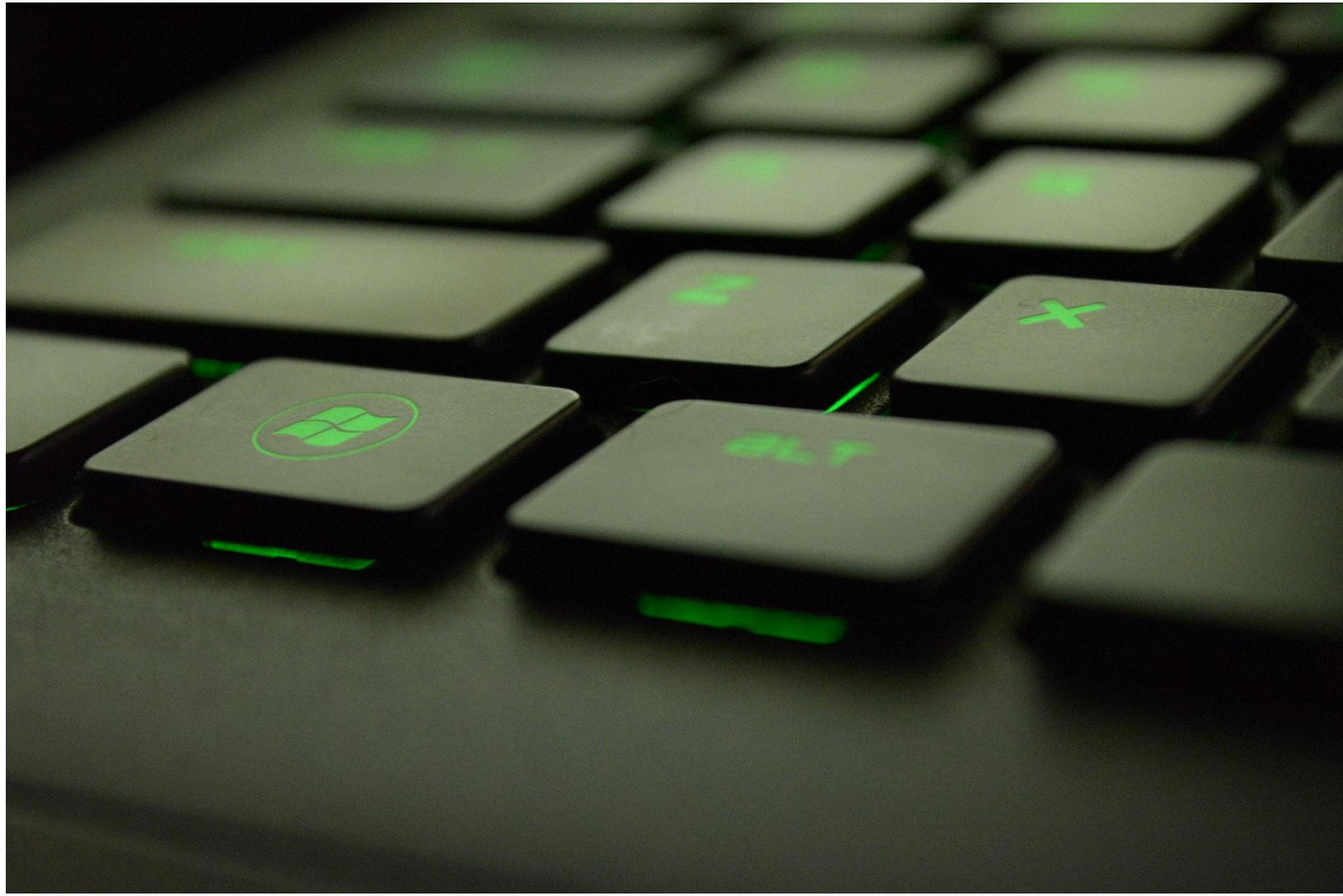
Voila!

You did it!

splunk> .conf22

Windows Dashboards and Reports

New Home + Some New Updates!

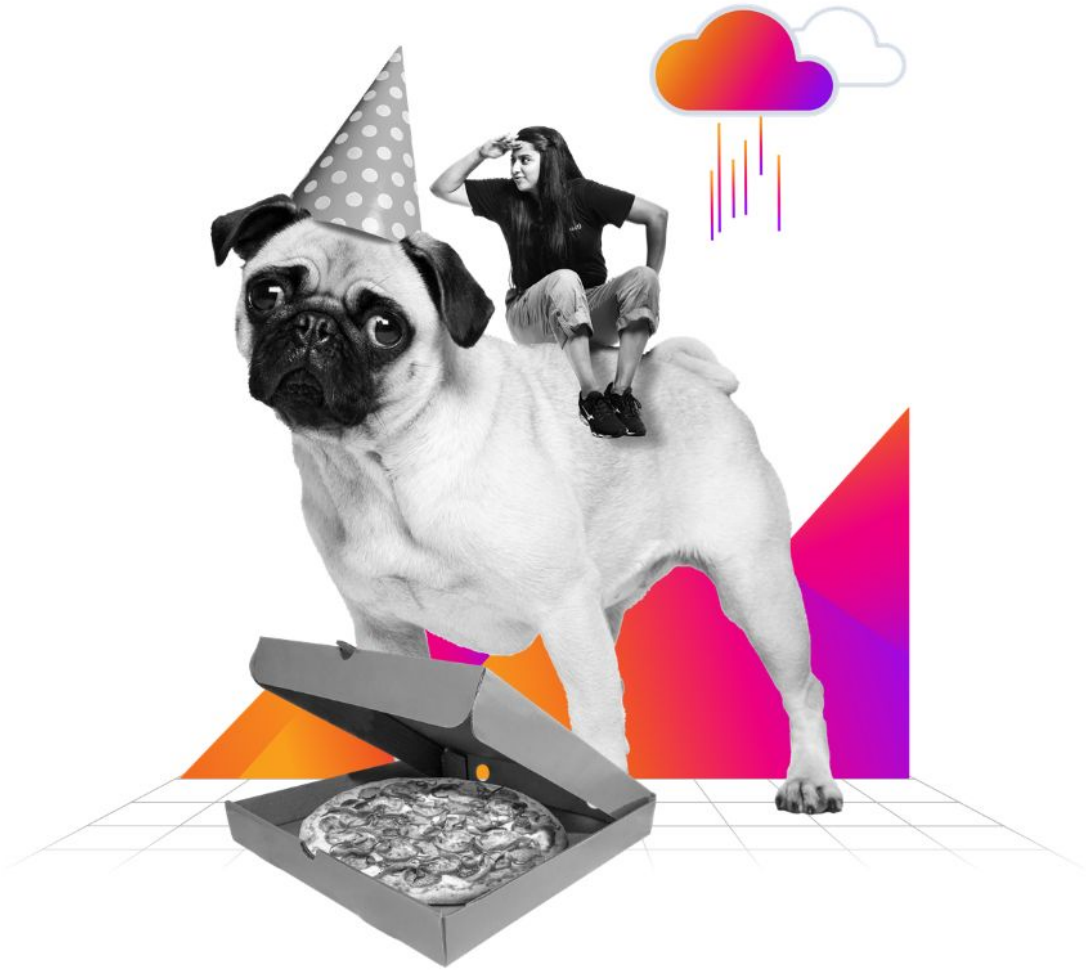


Content Pack focused on OS Monitoring

- All the dashboards have been moved
- Some have been updated since migration

More Information on Active Directory and other IT Essentials Releases:

OBS1373 - IT Essentials - The Fast Pass to Value with Splunk for IT Operations



Before - After

Apps and Add-ons

Splunk® App for Windows Infrastructure

	Data collection node (forwarder)	Indexer	Search head
Splunk Add-on for Windows	✓	✓	✓
Splunk App for Windows Infrastructure			✓
Splunk Supporting Add-on for Active Directory			✓

Before - After

Apps and Add-ons

Splunk® App for Windows Infrastructure

	Data collection node (forwarder)	Indexer	Search head
Splunk Add-on for Windows	✓	✓	✓
Splunk App for Windows Infrastructure			✓
Splunk Supporting Add-on for Active Directory			✓

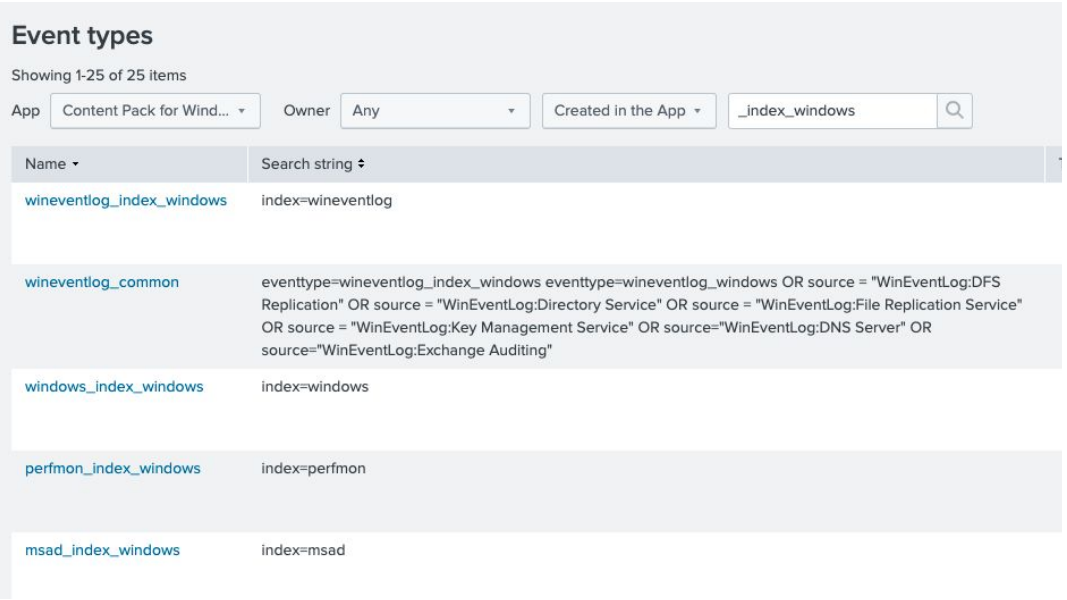
ITE-Work / ITSI with CP

	Data collection node (forwarder)	Indexer	Search head
Splunk Add-on for Windows	✓	✓	✓
ITSI or IT Essentials Work		✓	✓
Splunk App for Windows Infrastructure			Disabled
Splunk App for Content Packs			✓
Splunk Supporting Add on For Active Directory			✓

Update Eventtypes

Either from the UI or Configuration Files

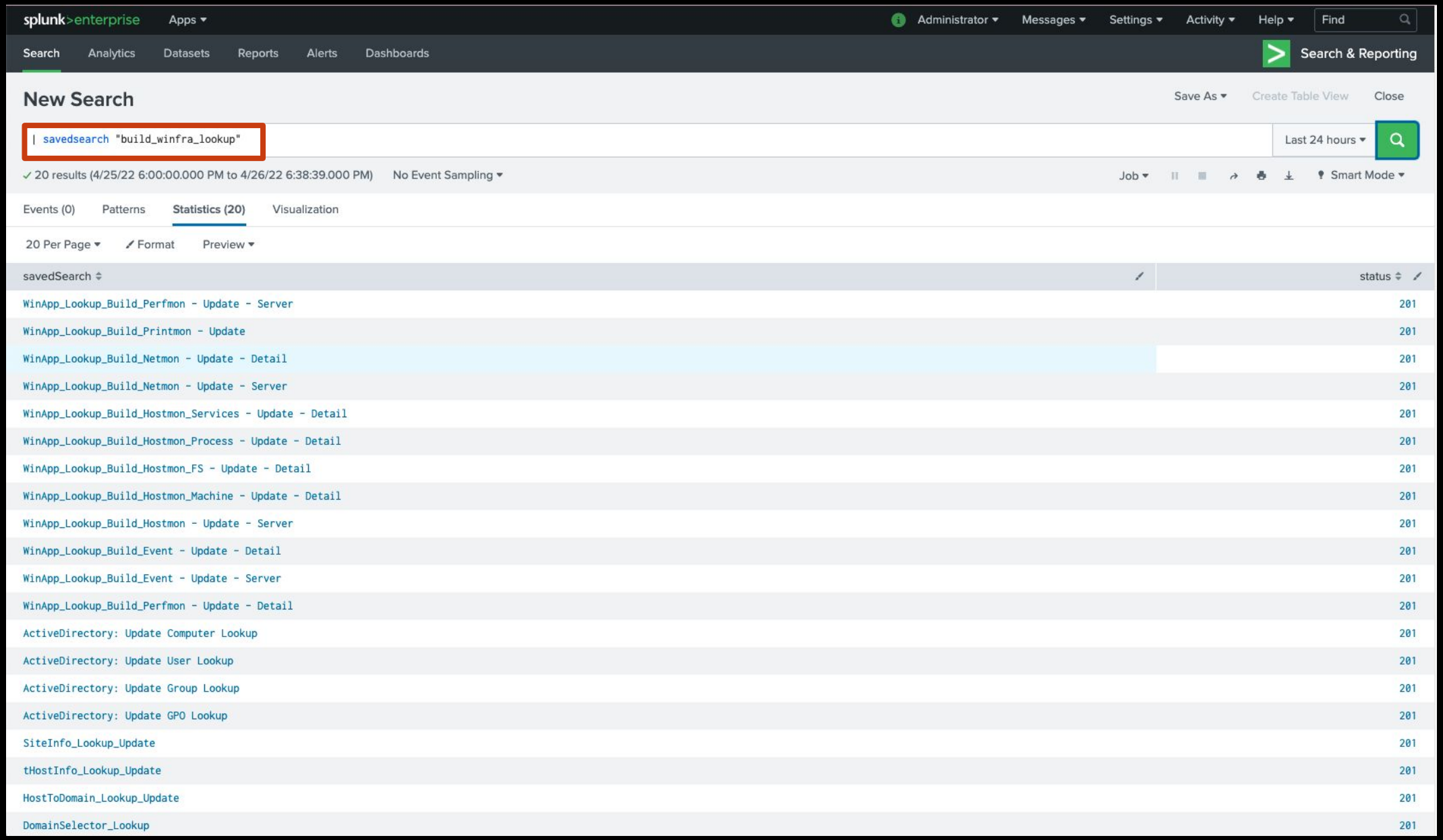
Content Pack for Windows Dashboards and Reports



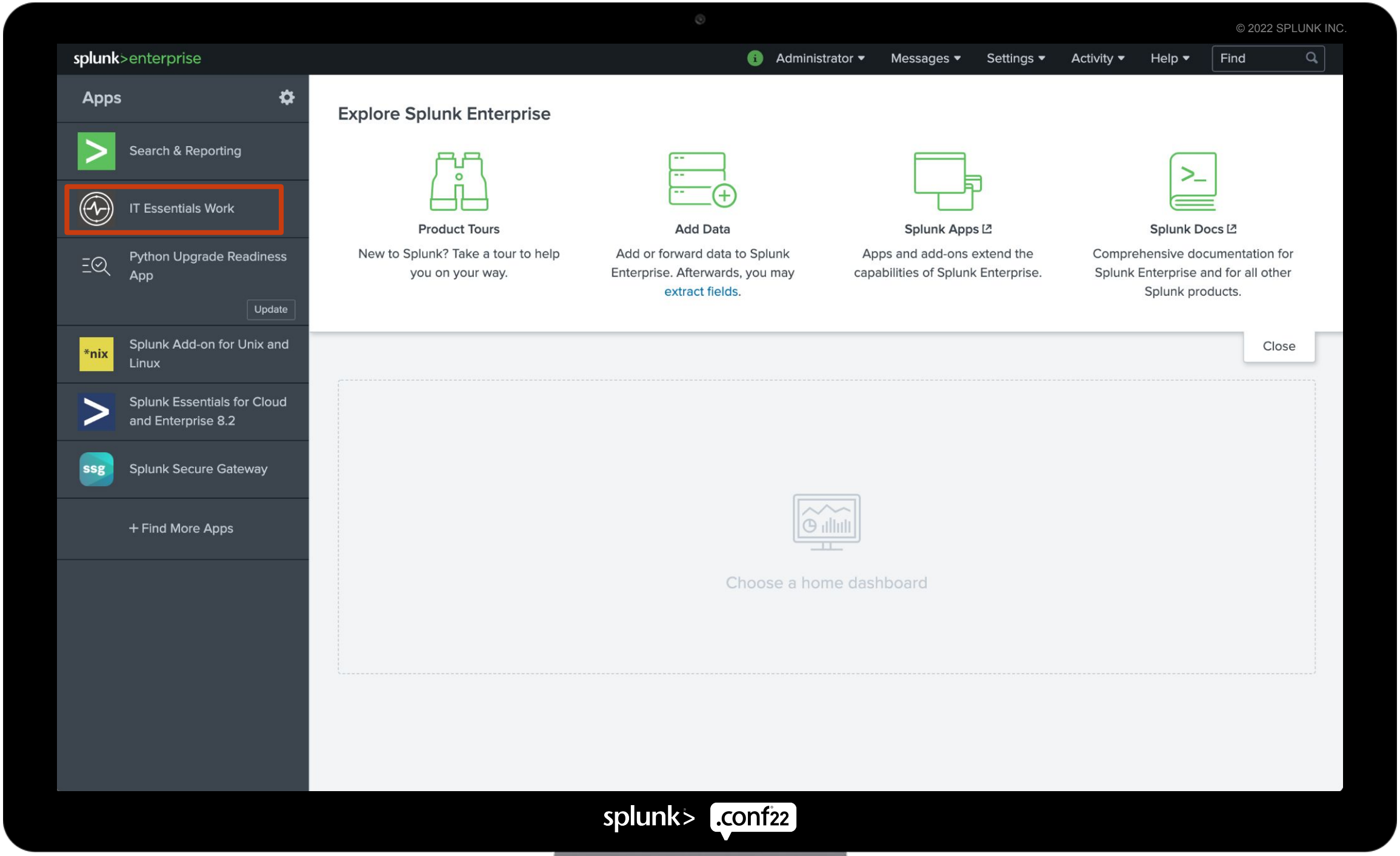
DA-ITSI-CP-windows-dashboards

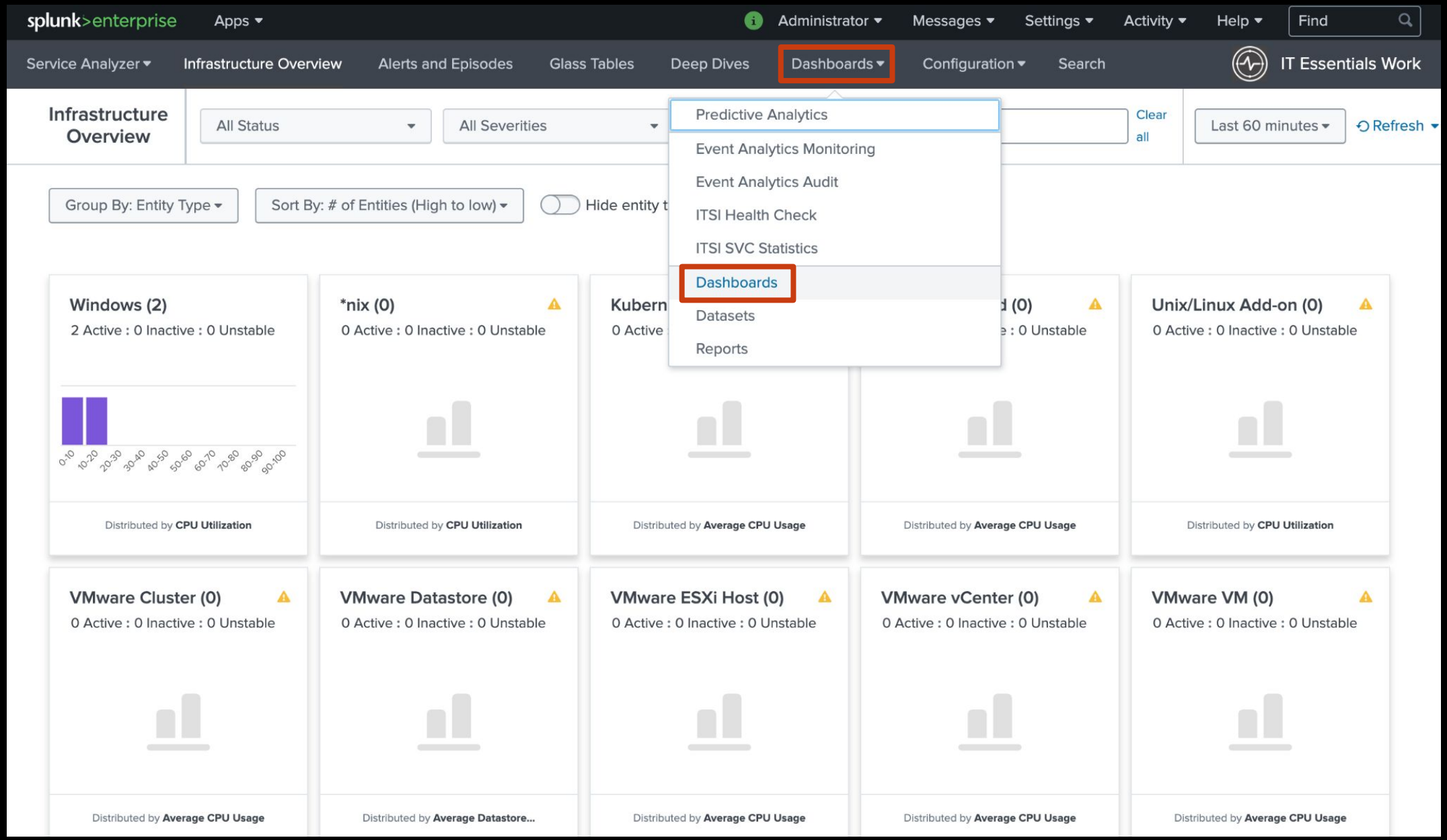
```
eventtypes.conf

[windows_index_windows]
search= index=windows

[perfmon_index_windows]
search= index=perfmon

[wineventlog_index_windows]
search= index=wineventlog

[msad_index_windows]
 search= index=msad
```

splunk> .conf22

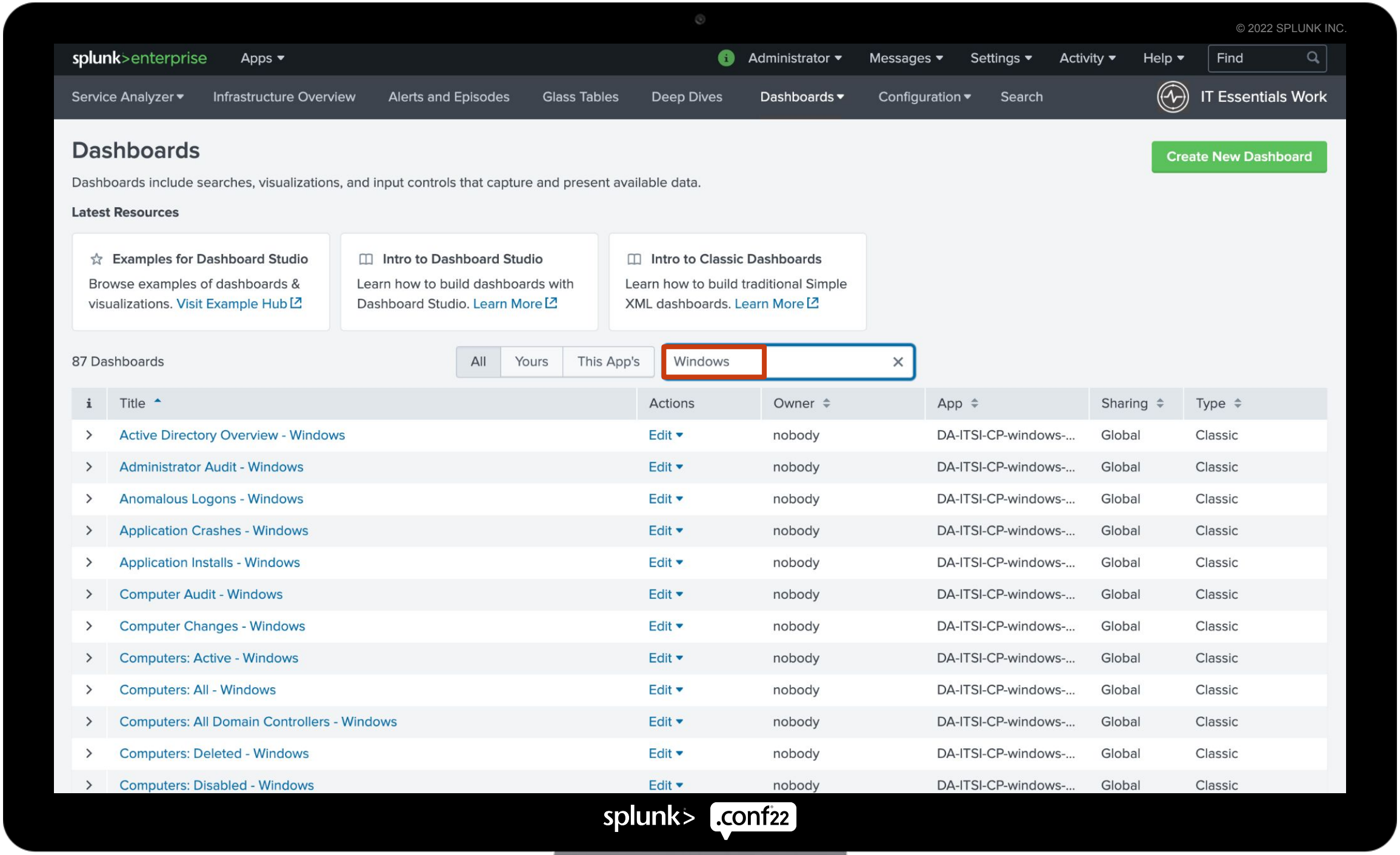


splunk> .conf22





splunk> .conf22



splunk> .conf22

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

Service Analyzer ▾ Infrastructure Overview Alerts and Episodes Glass Tables Deep Dives Dashboards ▾ Configuration ▾ Search IT Essentials Work

Dashboards

Create New Dashboard

Dashboards include searches, visualizations, and input controls that capture and present available data.

87 Dashboards!?

Latest Resources

Examples for Dashboard Studio
Browse examples of dashboards & visualizations. Visit Example Hub

Intro to Dashboard Studio
Learn how to build dashboards with Dashboard Studio. Learn More

Intro to Classic Dashboards
Learn how to build traditional Simple XML dashboards. Learn More

87 Dashboards | All | Yours | This App's | Windows

Title	Actions	Owner	App	Sharing	Type
Active Directory Overview - Windows	Edit	nobody	DA-ITSI-CP-windows-...	Global	Classic
Administrator Audit - Windows	Edit	nobody	DA-ITSI-CP-windows-...	Global	Classic
Anomalous Logons - Windows	Edit	nobody	DA-ITSI-CP-windows-...	Global	Classic
Application Crashes - Windows	Edit	nobody	DA-ITSI-CP-windows-...	Global	Classic
Application Installs - Windows	Edit	nobody	DA-ITSI-CP-windows-...	Global	Classic
Computer Audit - Windows	Edit	nobody	DA-ITSI-CP-windows-...	Global	Classic
Computer Changes - Windows	Edit	nobody	DA-ITSI-CP-windows-...	Global	Classic
Computers: Active - Windows	Edit	nobody	DA-ITSI-CP-windows-...	Global	Classic
Computers: All - Windows	Edit	nobody	DA-ITSI-CP-windows-...	Global	Classic
Computers: All Domain Controllers - Windows	Edit	nobody	DA-ITSI-CP-windows-...	Global	Classic
Computers: Deleted - Windows	Edit	nobody	DA-ITSI-CP-windows-...	Global	Classic
Computers: Disabled - Windows	Edit	nobody	DA-ITSI-CP-windows-...	Global	Classic

8 Dashboards Used by Most

Now with XML Support!

- Application Crashes - Windows
- Application Installs - Windows
- Event Monitoring - Windows
- Host Information - Windows
- Network Activity - Windows
- Processes - Windows
- Services - Windows
- Windows Update - Windows

What about getting some new stuff?

splunk> .conf22

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

Service Analyzer ▾ | Infrastructure Overview | Alerts and Episodes | Glass Tables | Deep Dives | Dashboards ▾ | Configuration ▾ | Search | IT Essentials Work

Infrastructure 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

Windows (2)
2 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**

Unix/Linux Add-on (0)
0 Active : 0 Inactive : 0 Unstable
Distributed by **CPU Utilization**

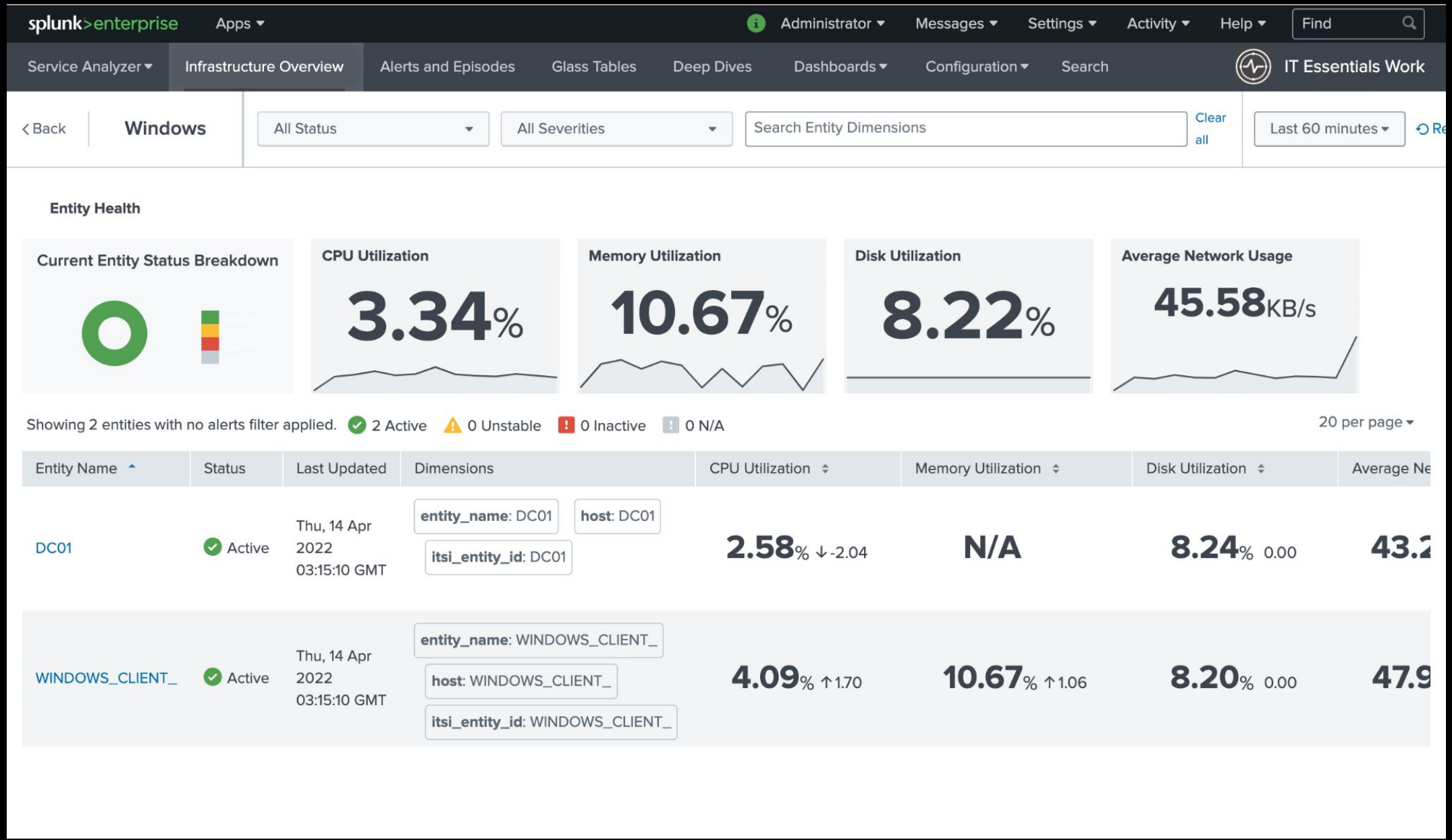
VMware Cluster (0)
0 Active : 0 Inactive : 0 Unstable
Distributed by **Average CPU Usage**

VMware Datastore (0)
0 Active : 0 Inactive : 0 Unstable
Distributed by **Average Datastore...**

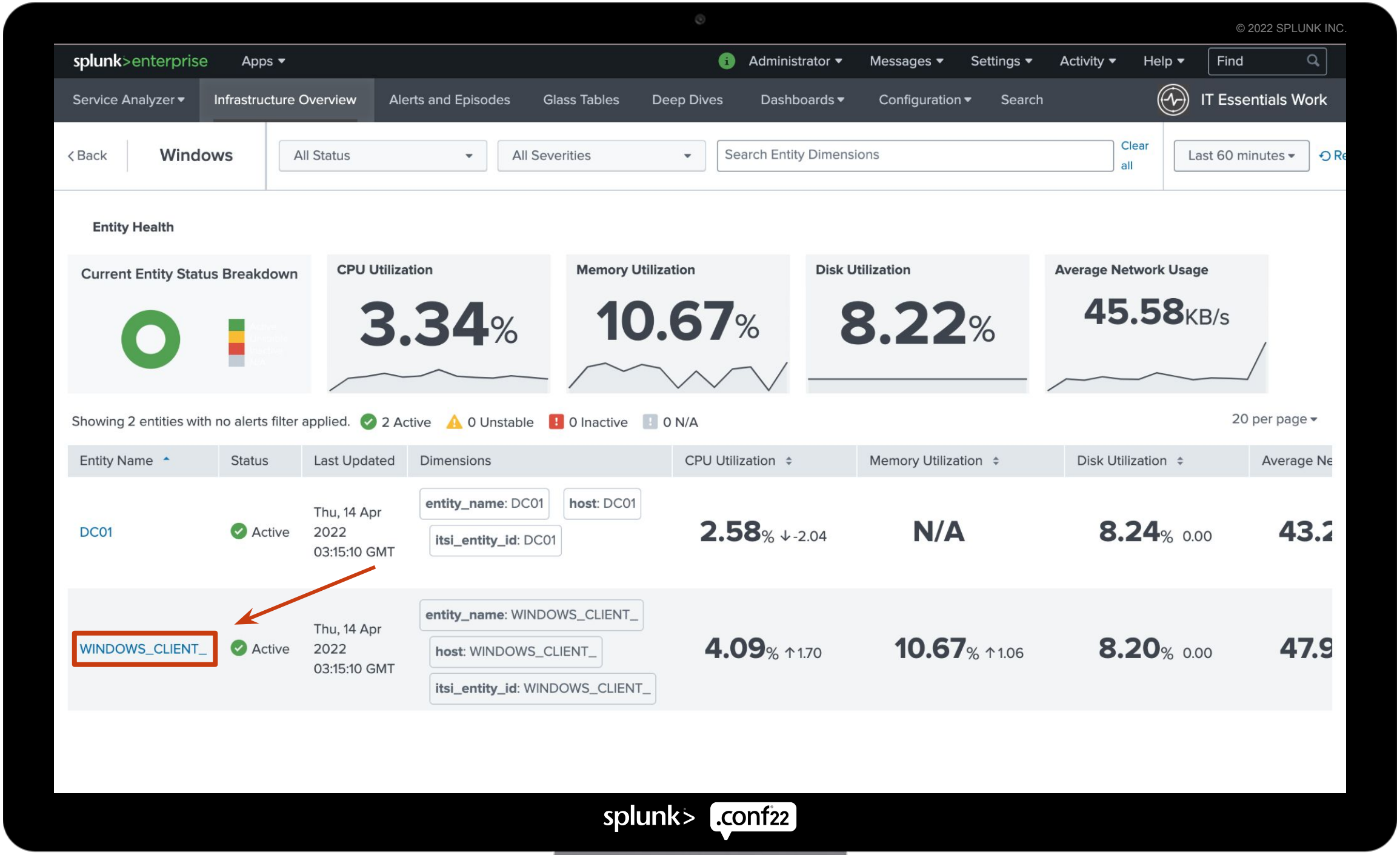
VMware ESXi Host (0)
0 Active : 0 Inactive : 0 Unstable
Distributed by **Average CPU Usage**

VMware vCenter (0)
0 Active : 0 Inactive : 0 Unstable
Distributed by **Average CPU Usage**

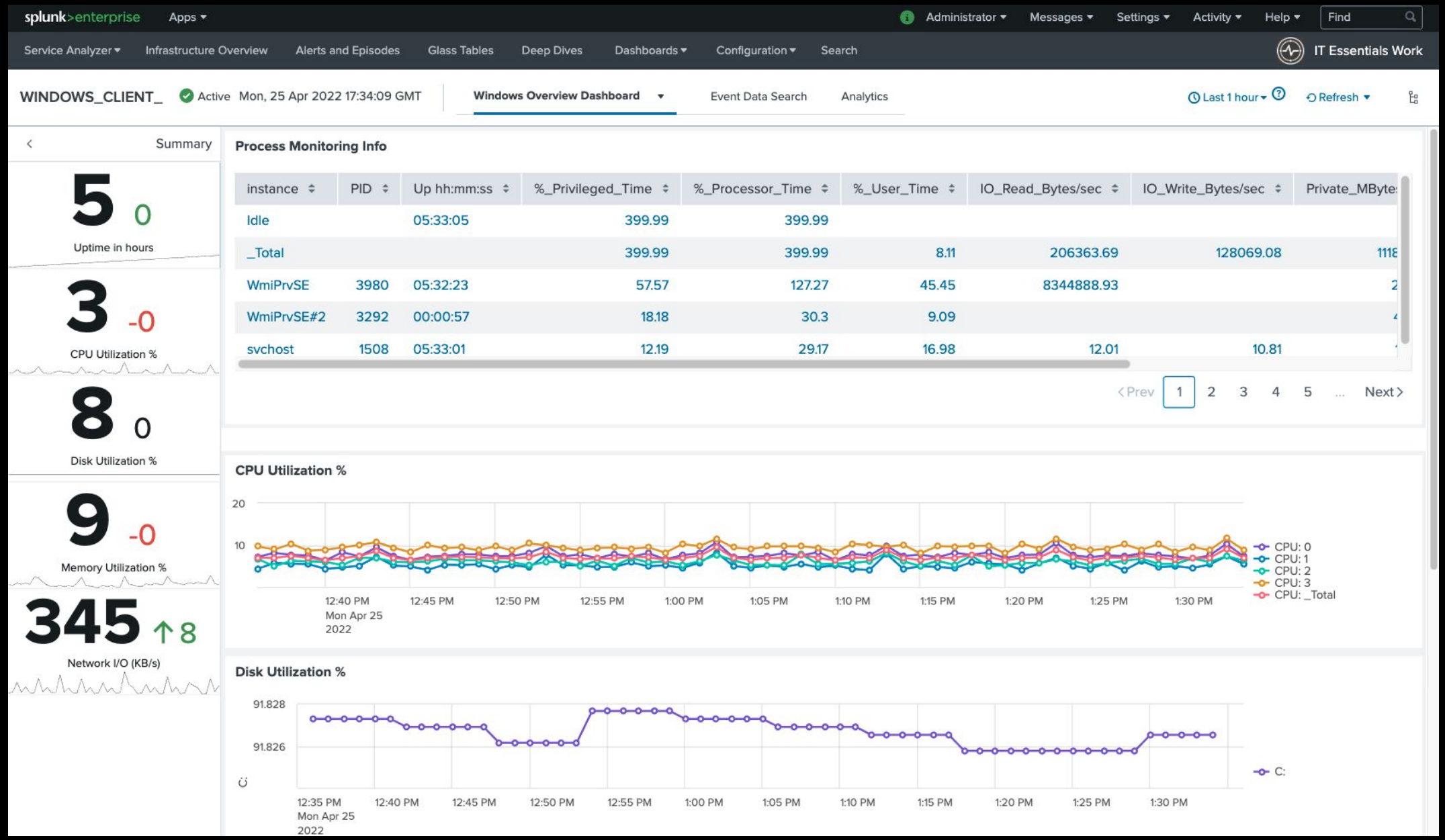
VMware VM (0)
0 Active : 0 Inactive : 0 Unstable
Distributed by **Average CPU Usage**



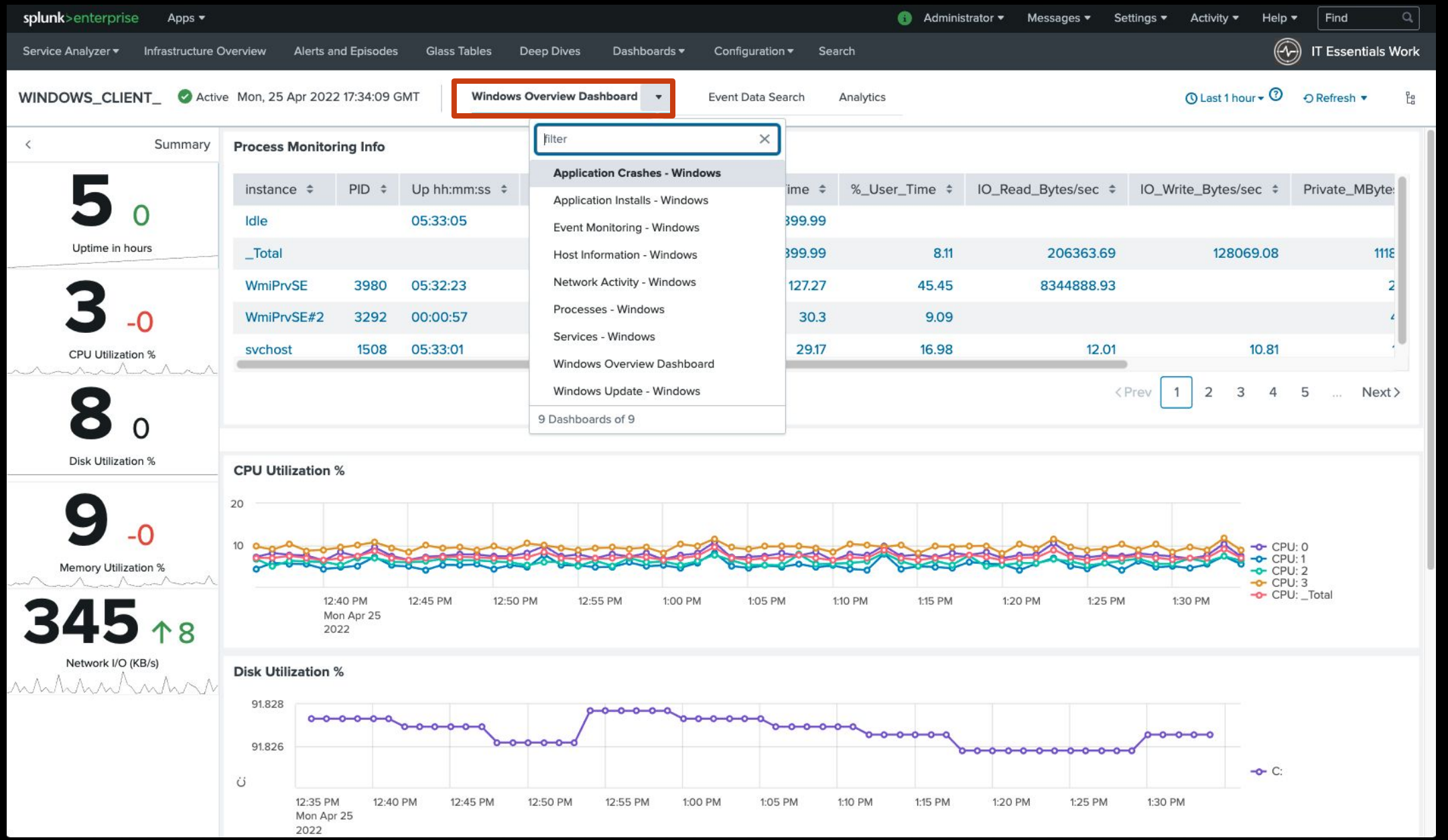
splunk> .conf22



splunk> .conf22



splunk> .conf22



splunk> .conf22

The move is complete, but how did we do it?

Getting Data In

For ITW-Work / ITSI Infrastructure Monitoring

```
464  ########################################
465  ### Metrics Inputs for ITE Work/iTSI ###
466  ########################################
467
468  [perfmon://CPU]
469  counters=% C1 Time;% C2 Time;% Idle Time;% Processor Time;% User Time;% Reserved Time;% Interrupt Time;% Privileged Time;
470  instances=*
471  object=Processor
472  mode=single
473  index=itsi_im_metrics
474  interval=60
475  sourcetype=PerfmonMetrics:CPU
476  disabled = false
477
478  [perfmon://LogicalDisk]
479  counters=Free Megabytes;% Free Space;
480  instances=*
481  object=LogicalDisk
482  mode=single
483  index=itsi_im_metrics
484  interval=60
```

Getting Data In

For ITW-Work / ITSI Infrastructure Monitoring

```
12  ###### OS Logs ######
13  [WinEventLog://Application]
14  disabled = false
15  start_from = oldest
16  current_only = 0
17  checkpointInterval = 5
18  renderXml=true
19  index = wineventlog
20
21  [WinEventLog://Security]
22  disabled = false
23  start_from = oldest
24  current_only = 0
25  evt_resolve_ad_obj = 1
26  checkpointInterval = 5
27  blacklist1 = EventCode="4662" Message="Object Type:(?!\s*groupPolicyContainer)"
28  blacklist2 = EventCode="566" Message="Object Type:(?!\s*groupPolicyContainer)"
29  renderXml=true
30  index = wineventlog
31
32  [WinEventLog://System]
33  disabled = false
```

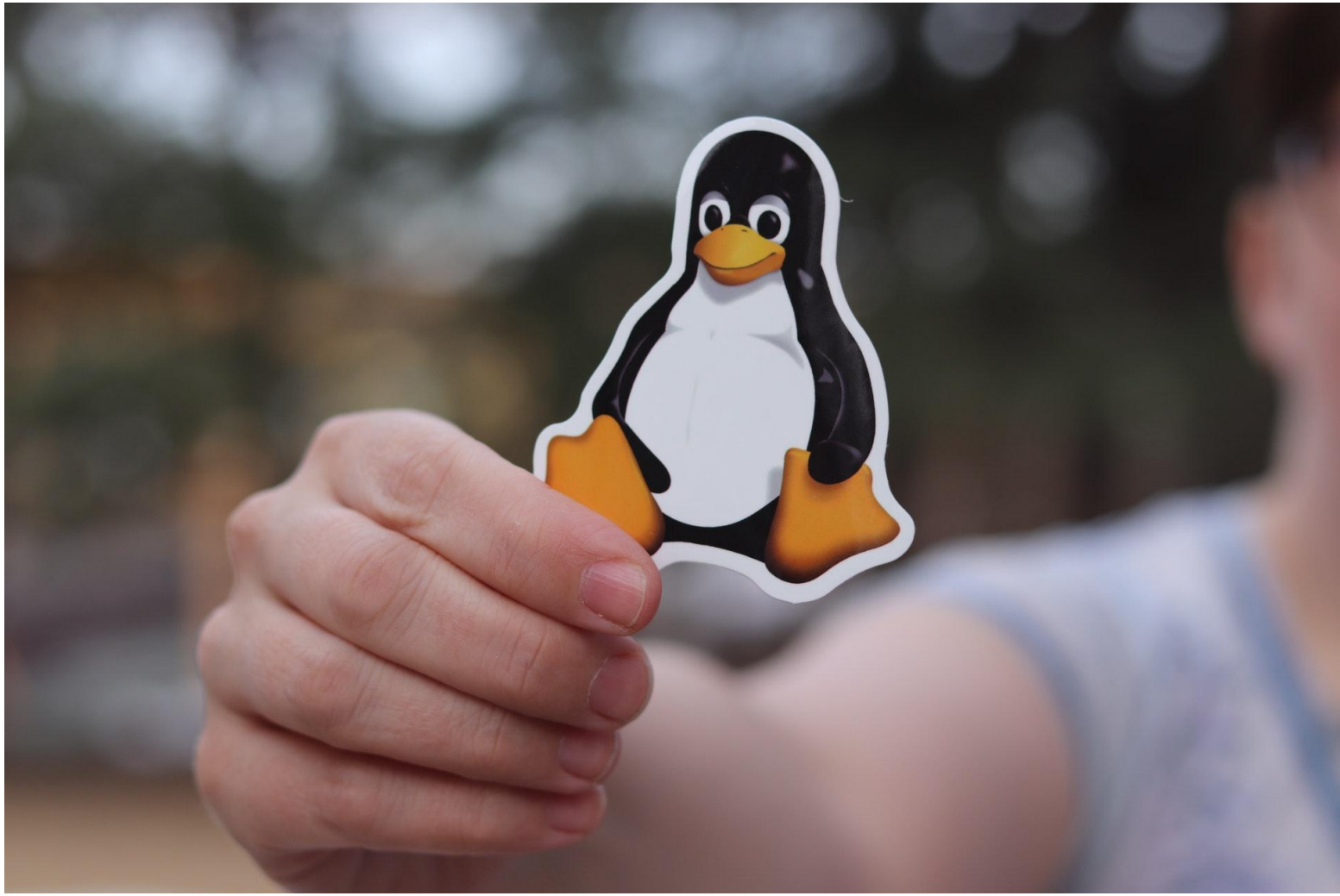
That’s it for Windows

Let’s tackle Linux

Unix (and Linux) Dashboards and Reports

What you have is what you get

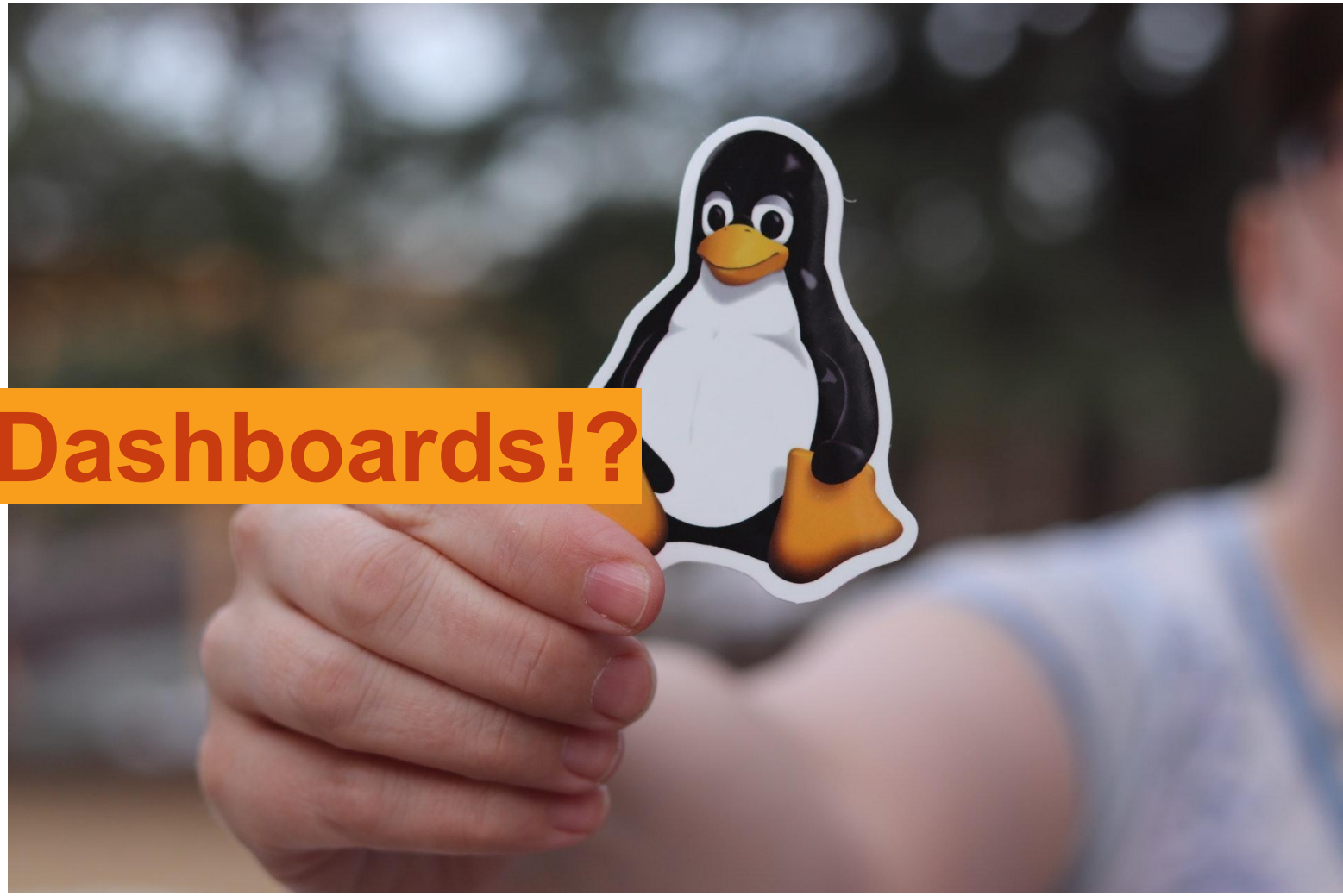
Five Hundred Dashboards



Unix (and Linux) Dashboards and Reports

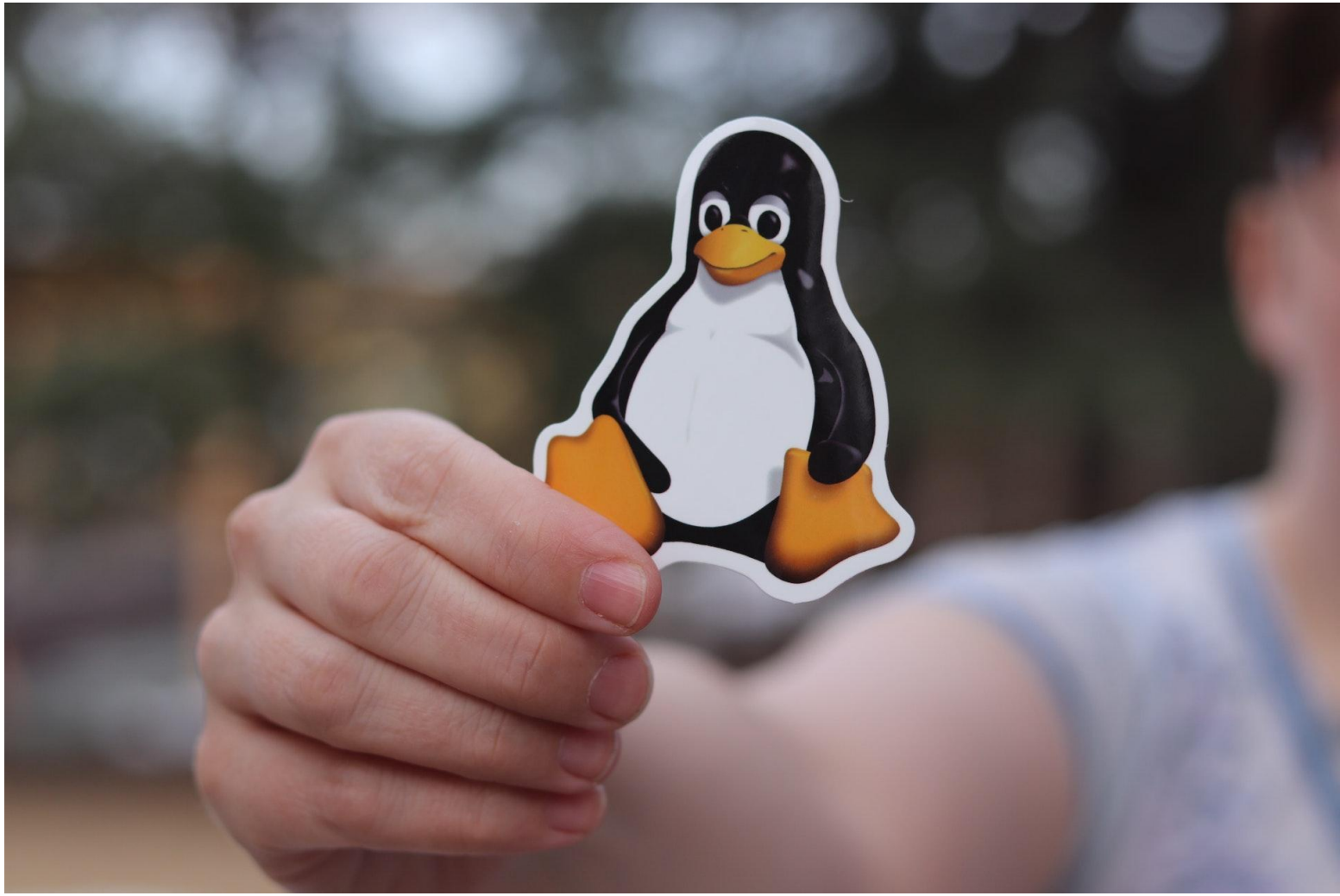
What you have is what you get

Five Hundred Dashboards



Unix (and Linux) Dashboards and Reports

What you have is what you get



Five Dashboards

- Home
- Metrics
- Hosts
- Alerts
- Settings

Ready for the Move?

Migration Steps - Unix App

1

Disable old

Disable the legacy app

2

Install new

Install ITE-Work or ITSI

Install the Splunk App for Content Packs

3

Configure

Open Settings Dashboard

Define indexes and sourcetypes

Create Categories

Enable Alerts

ITE-Work / ITSI Dashboards / Reports

Voila!

Before - After

Apps and Add-ons

Splunk® App for Unix

	Data collection node	Indexer	Search head
Splunk Add-on for Unix and Linux	✓	✓	✓
Splunk App for Unix and Linux			✓

Before - After

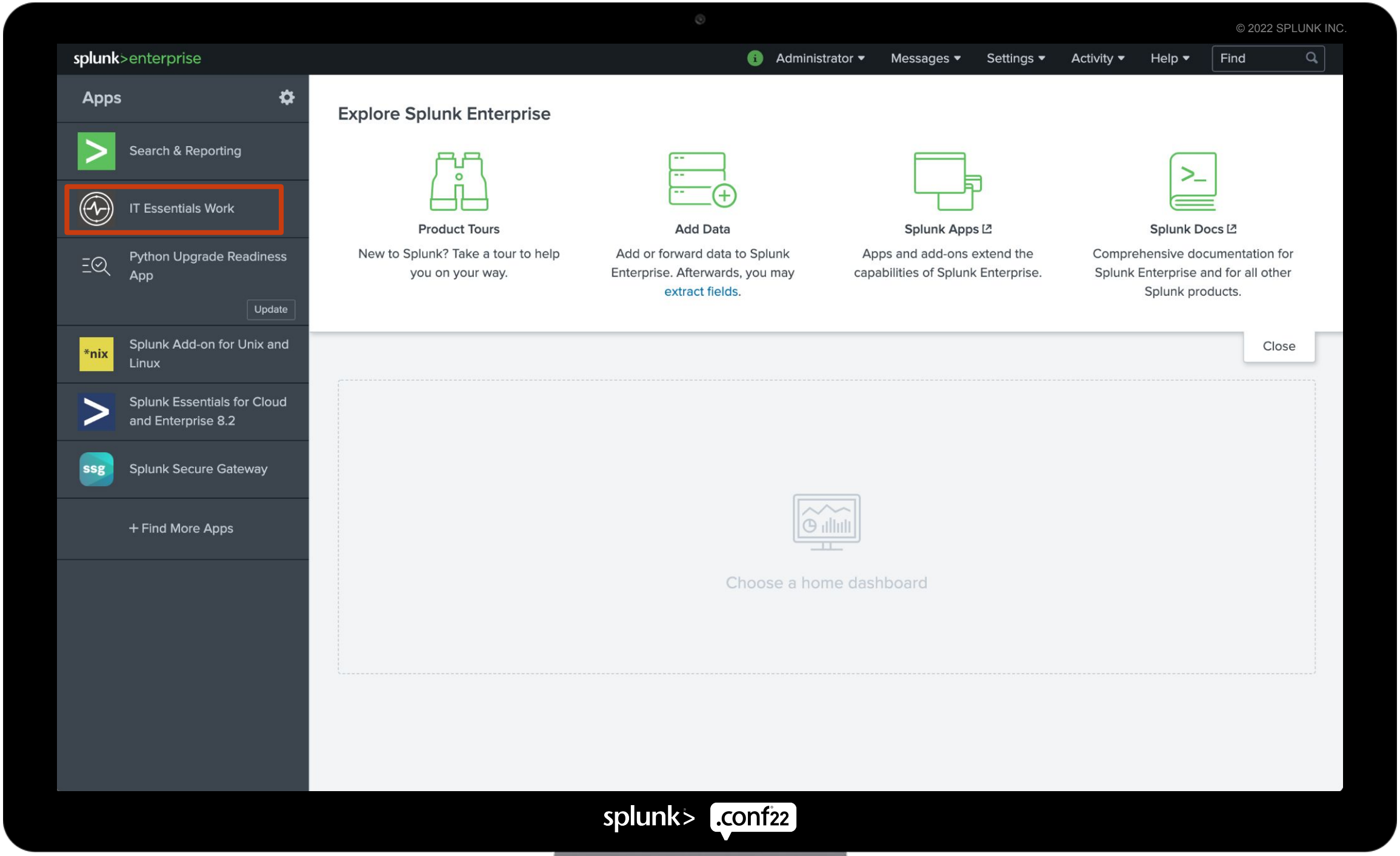
Apps and Add-ons

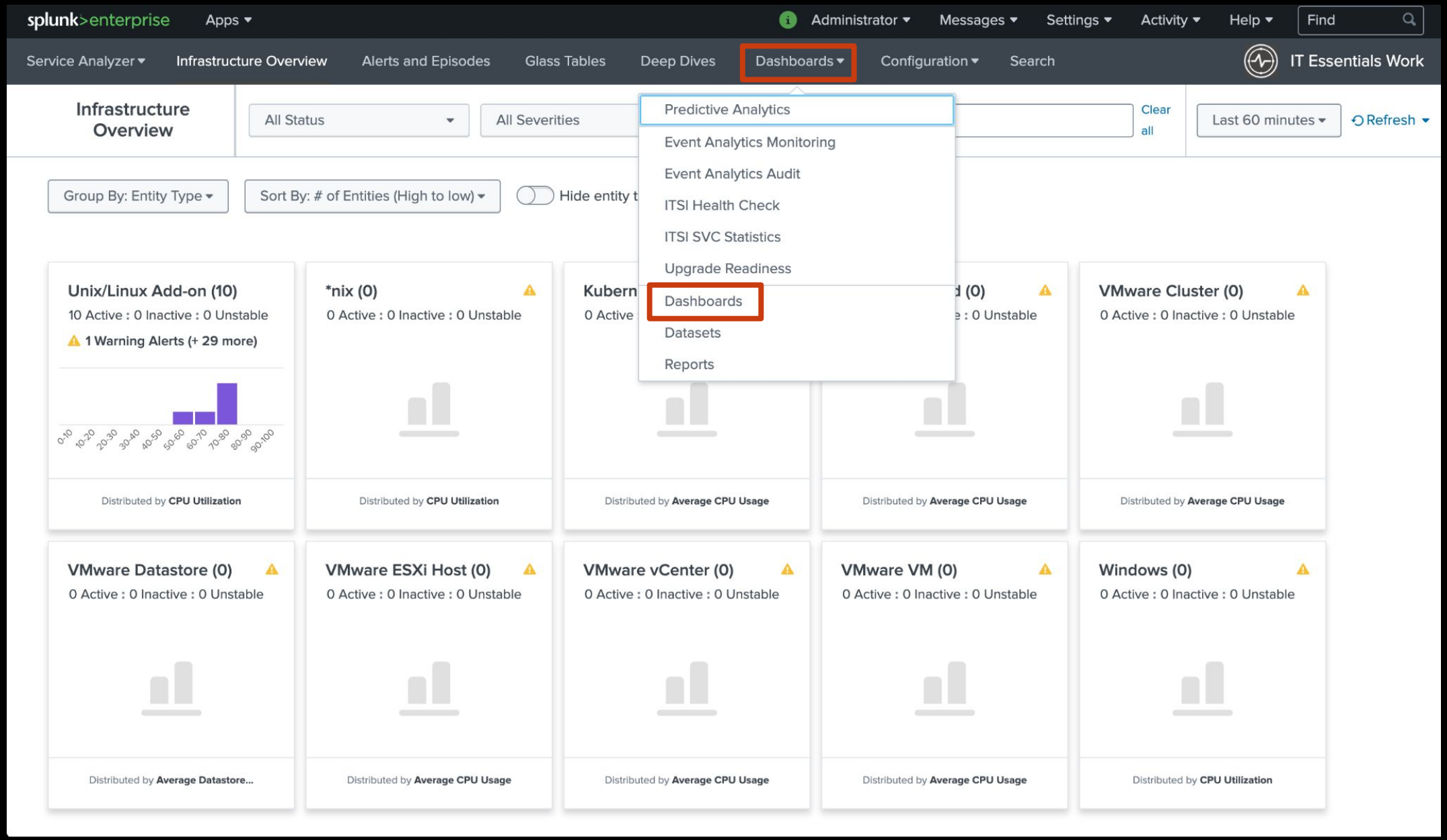
Splunk® App for Unix

	Data collection node	Indexer	Search head
Splunk Add-on for Unix and Linux	✓	✓	✓
Splunk App for Unix and Linux			✓

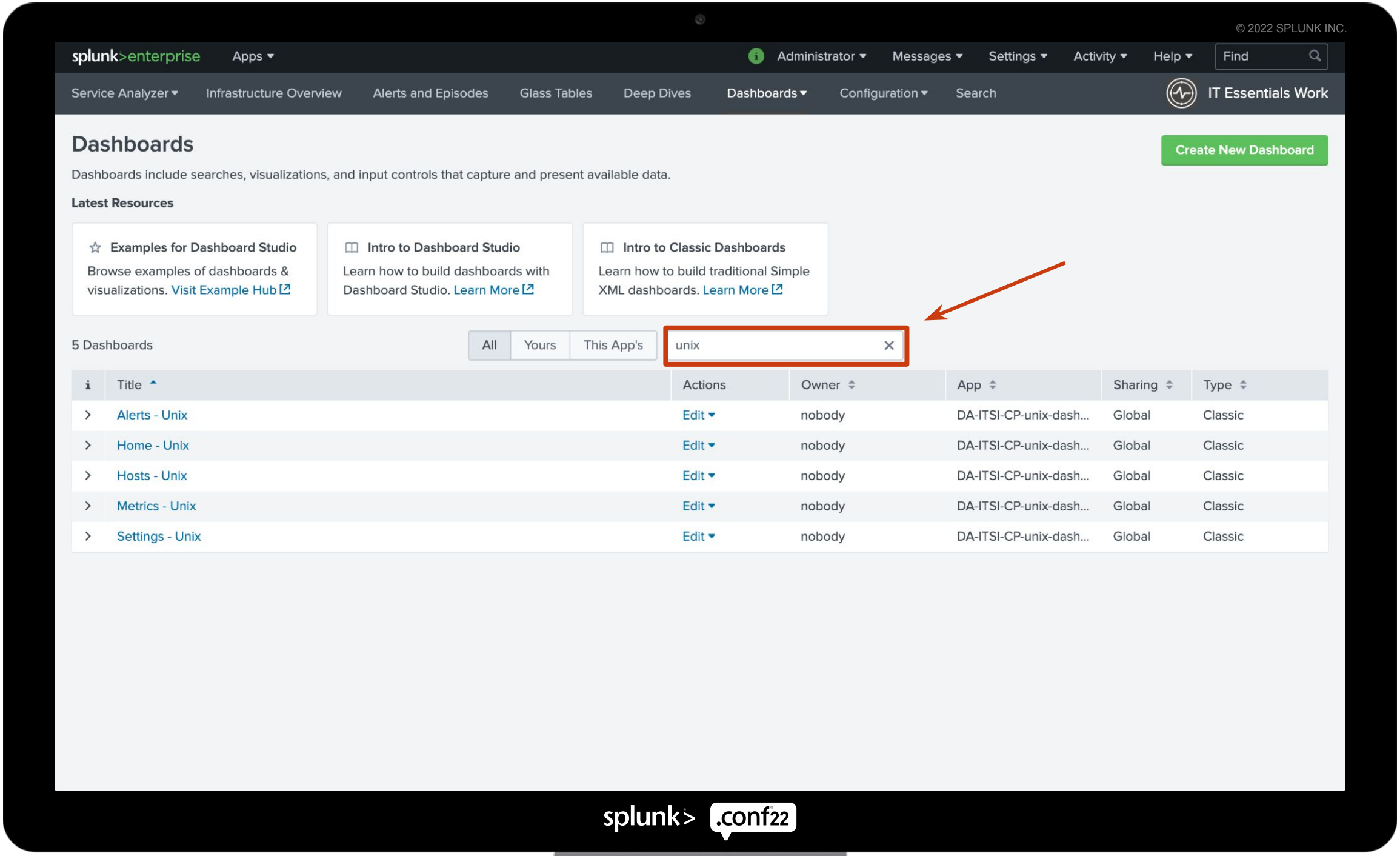
ITE-Work / ITSI with CP

	Data collection node	Indexer	Search head
Splunk Add-on for Unix and Linux	✓	✓	✓
Splunk App for Unix and Linux			Disabled
ITSI or IT Essentials Work		✓	✓
Splunk App for Content Packs			✓

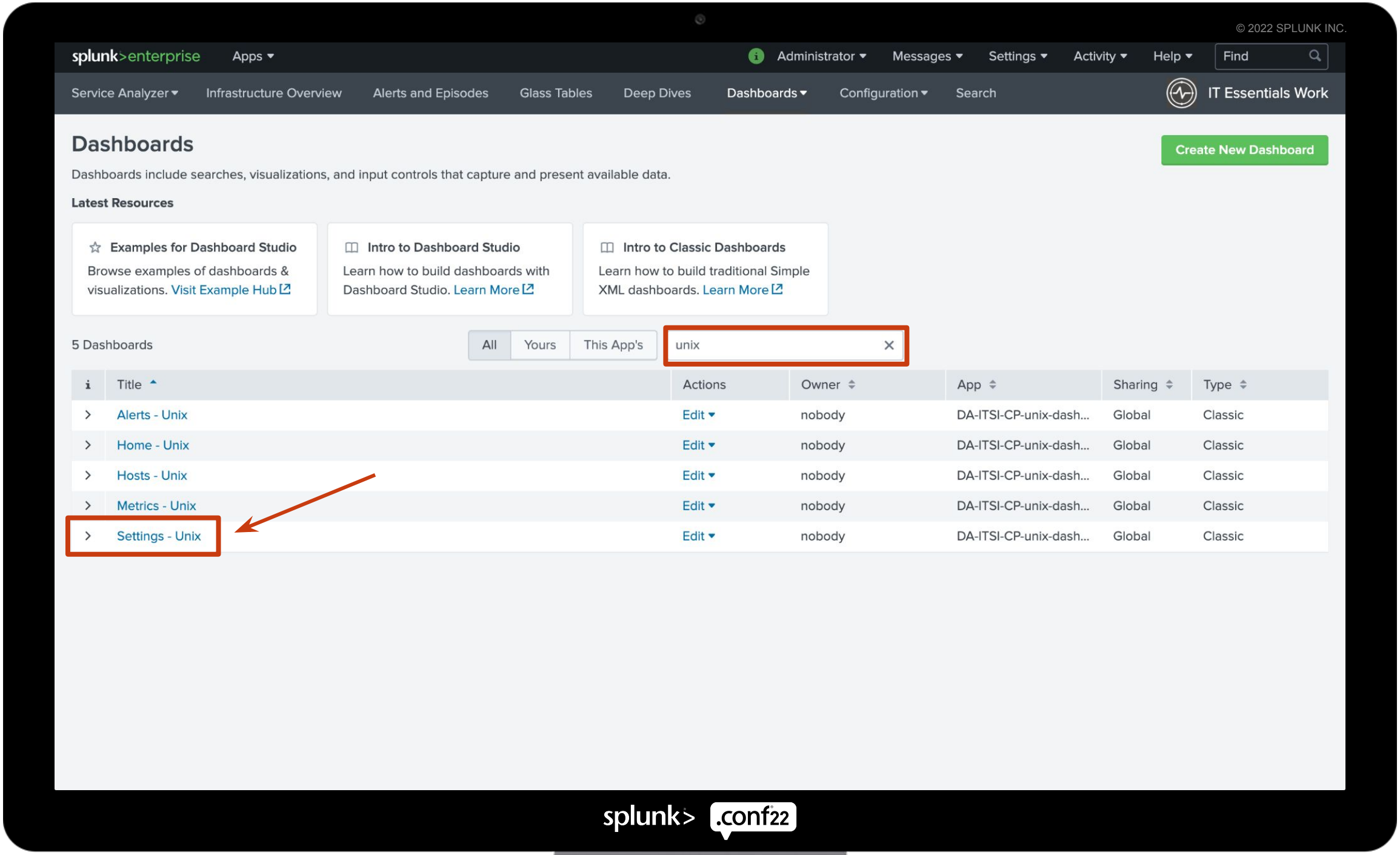




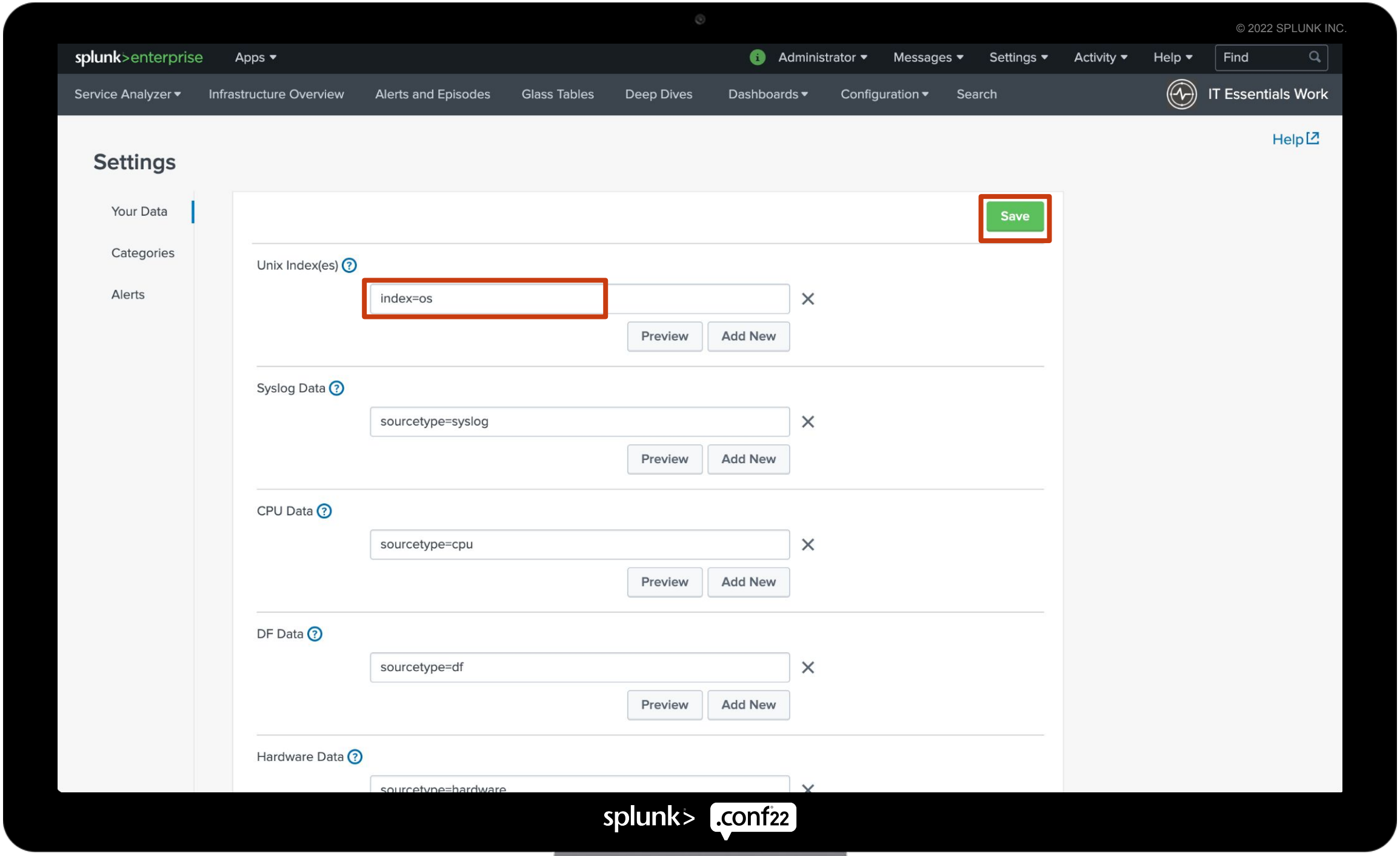
splunk> .conf22

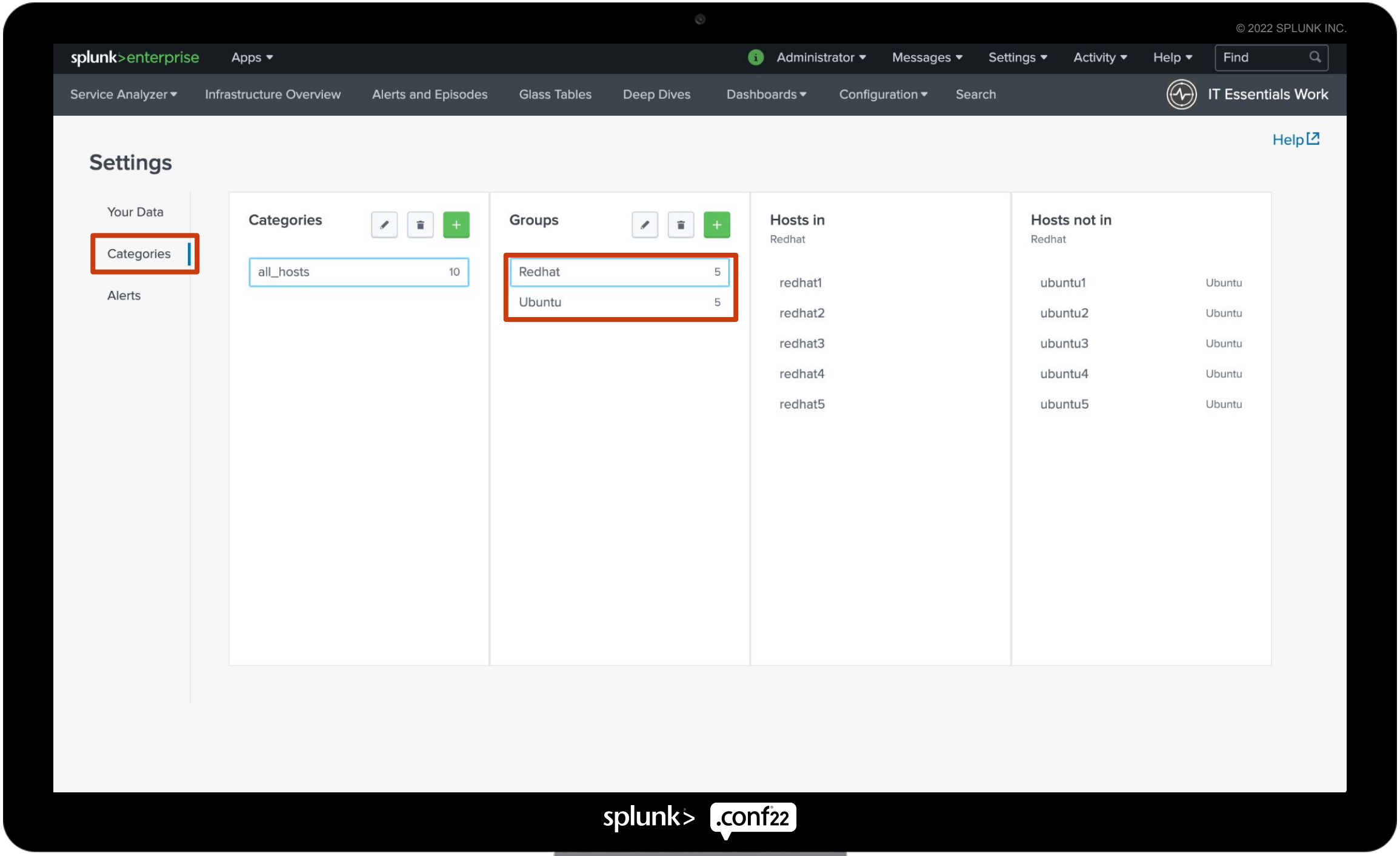


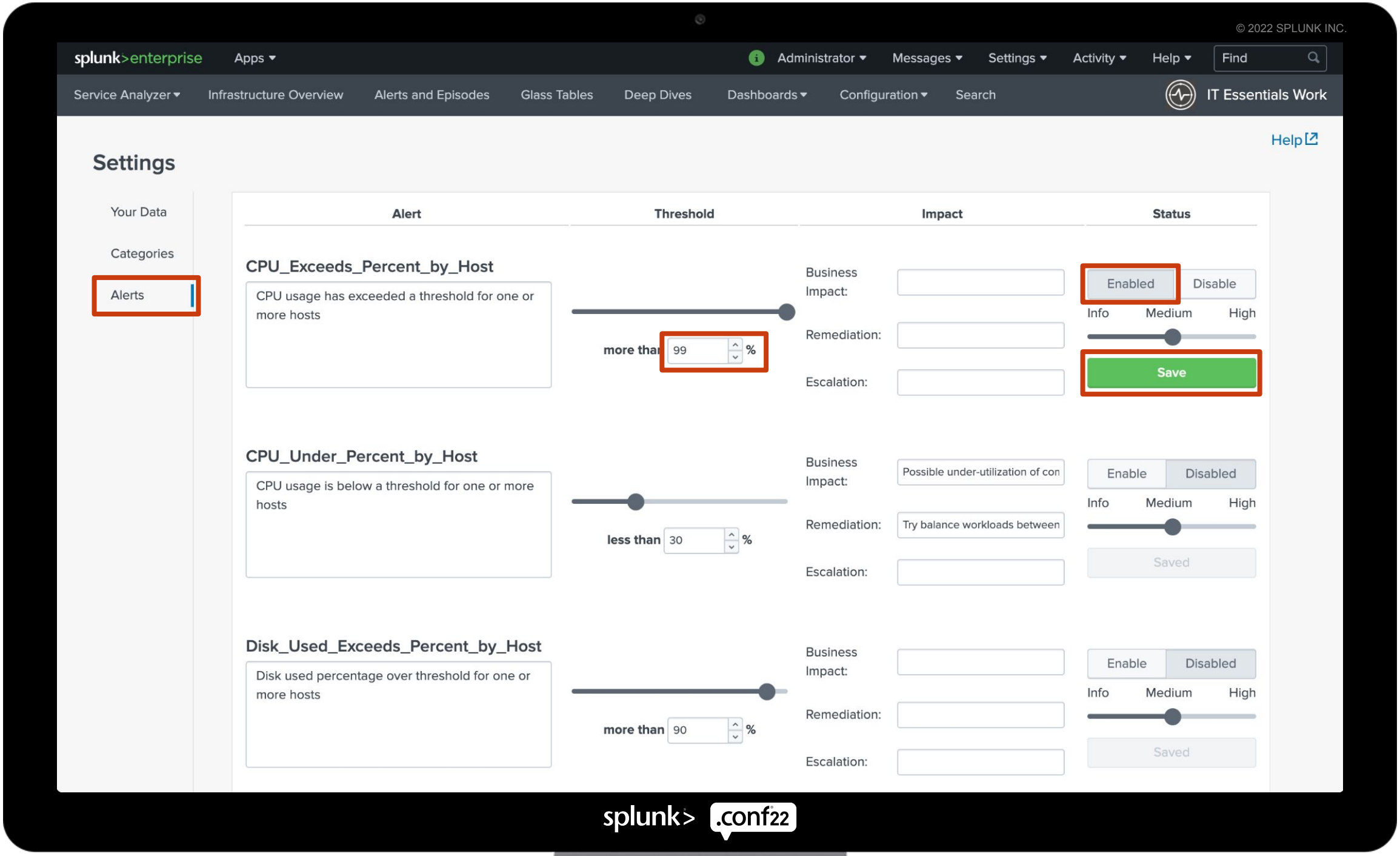
splunk> .conf22



splunk> .conf22

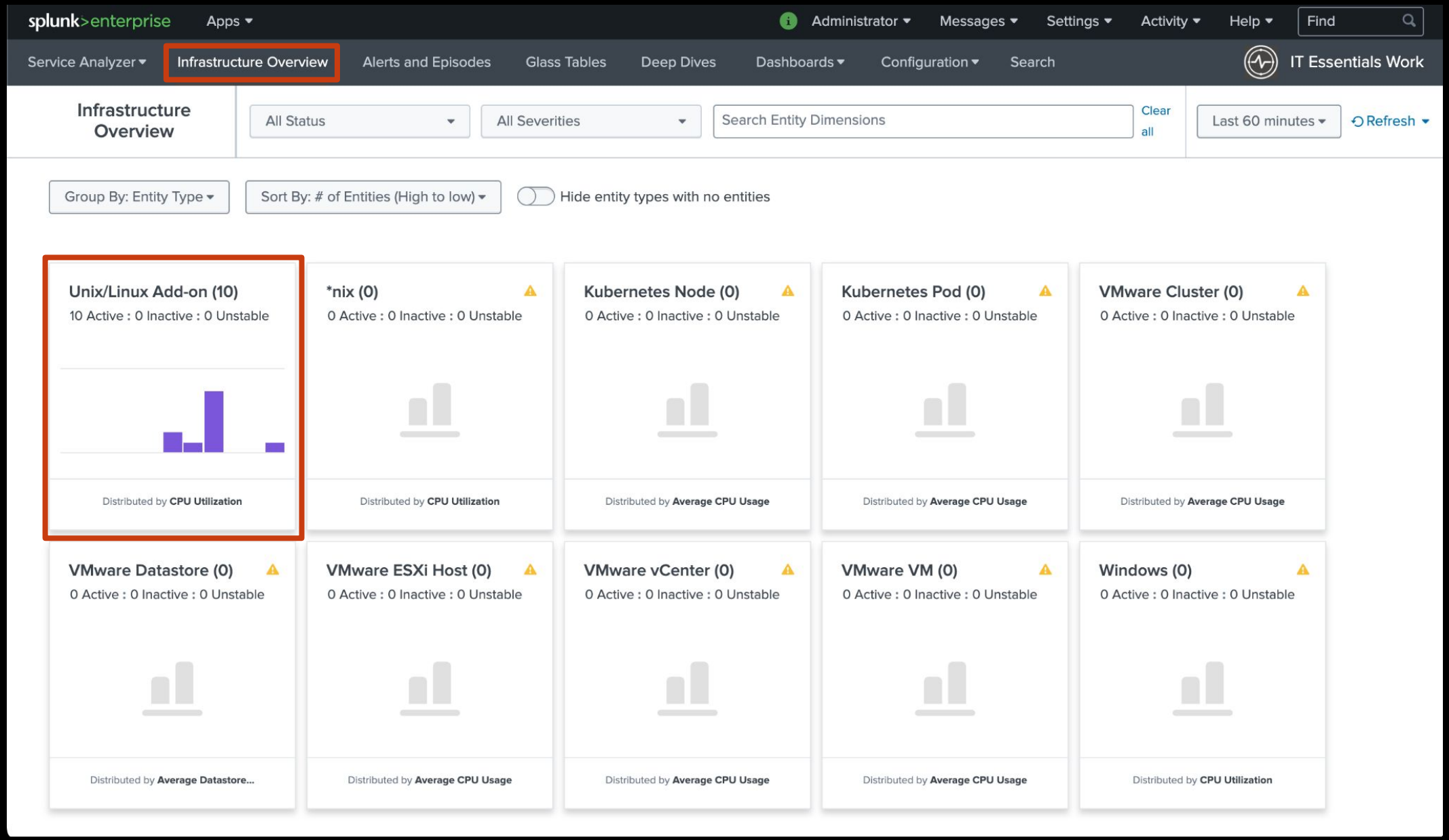




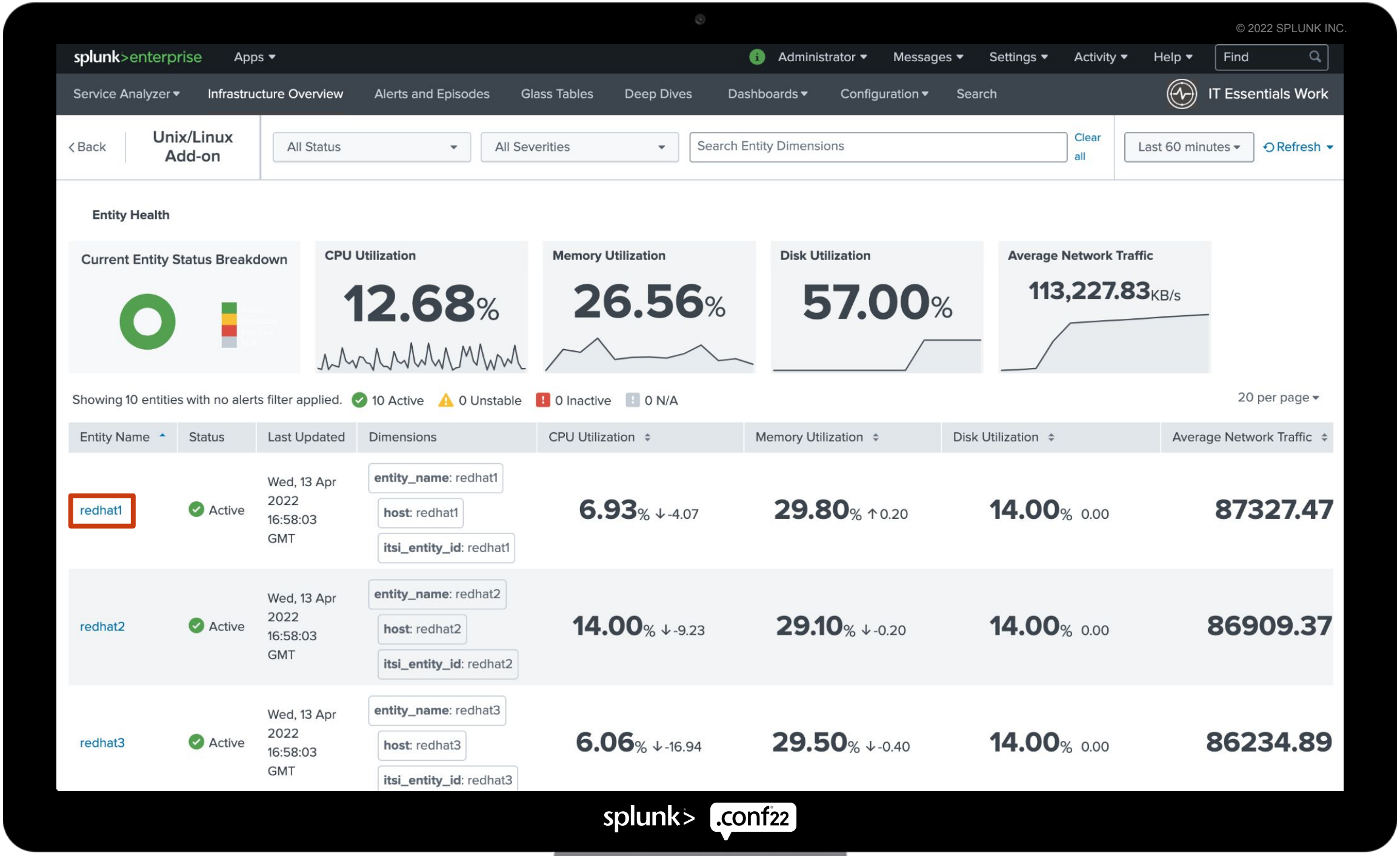


splunk> .conf22

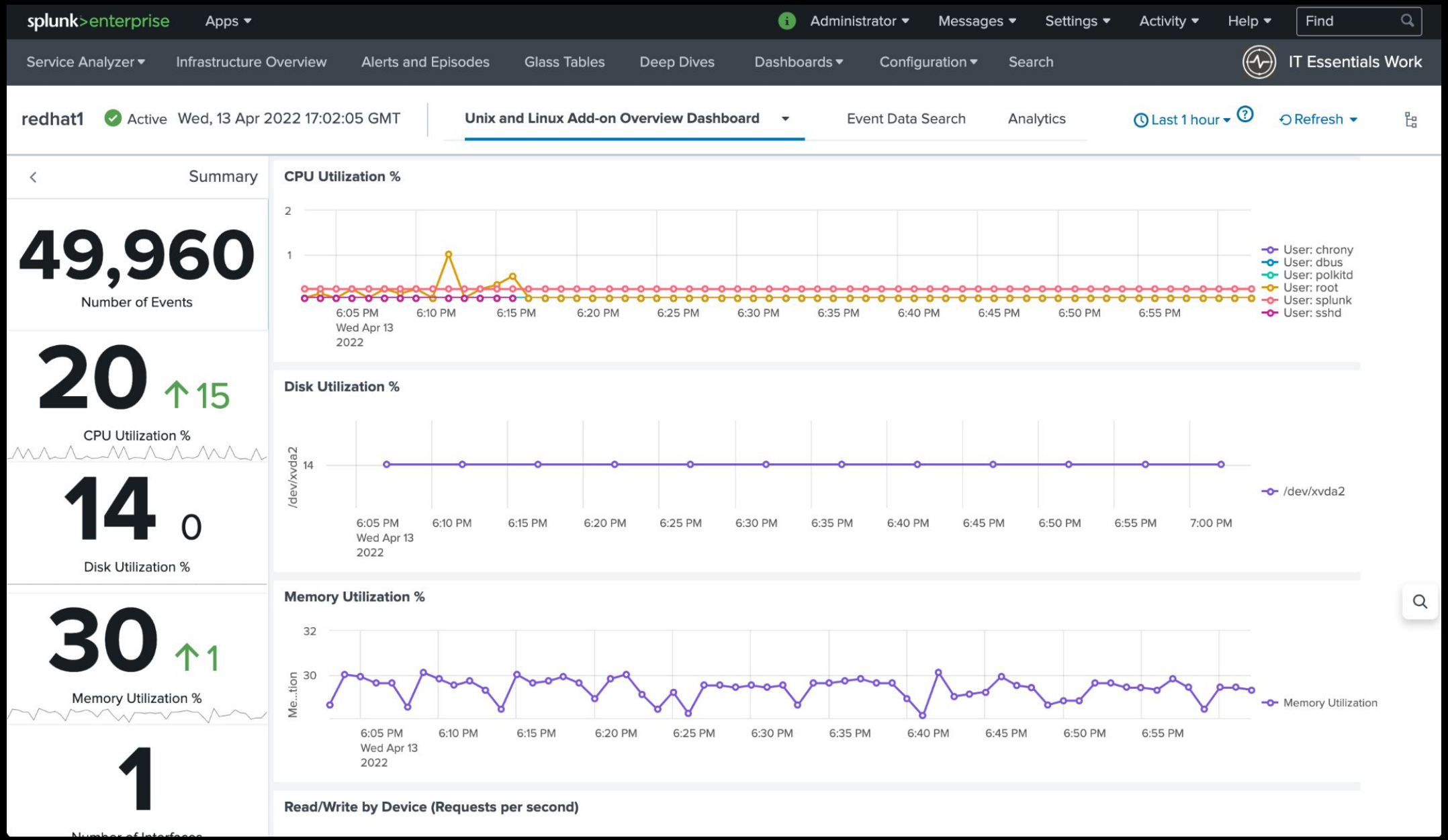
Moving is not always hard.



splunk> .conf22

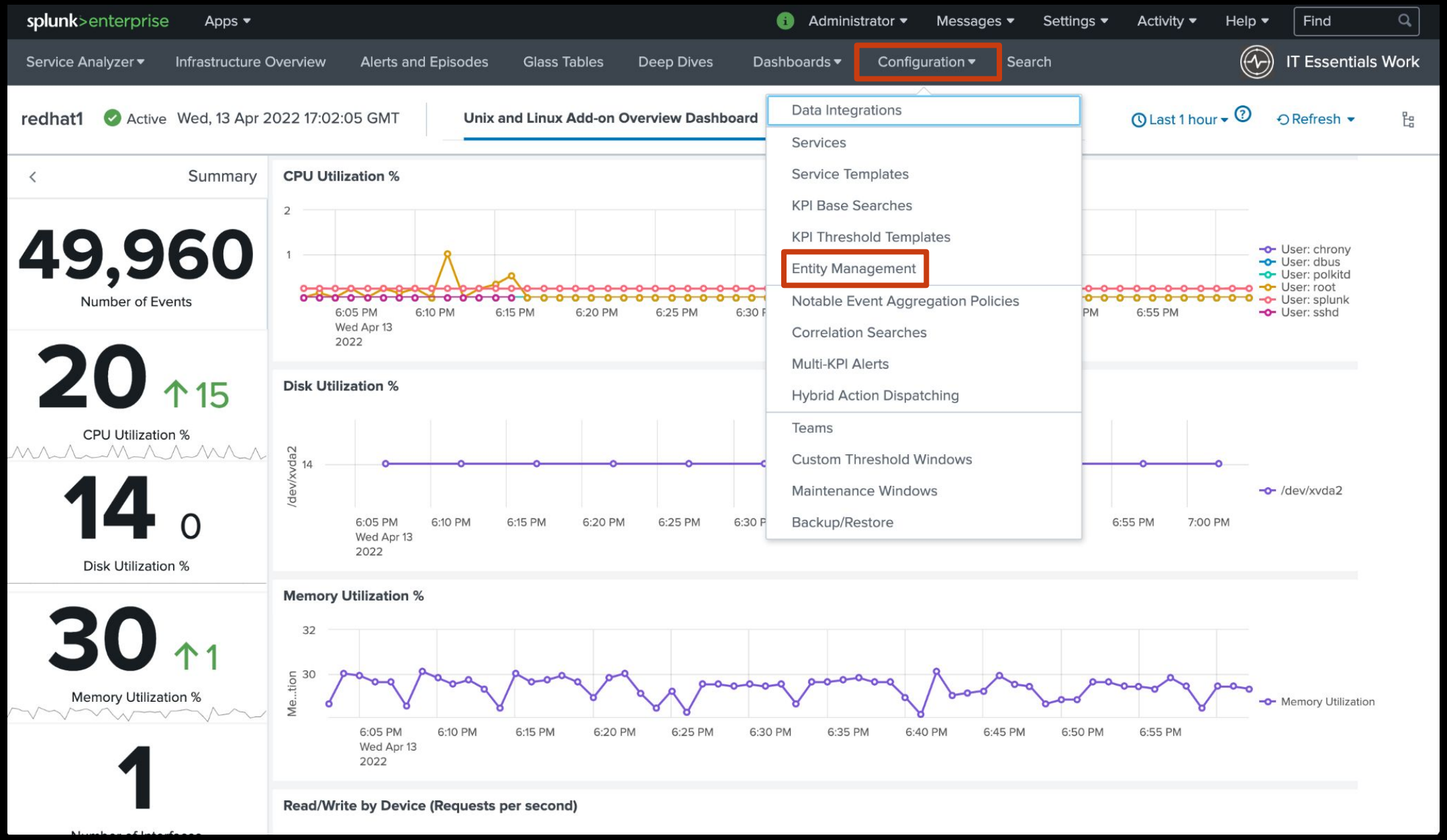


splunk> .conf22

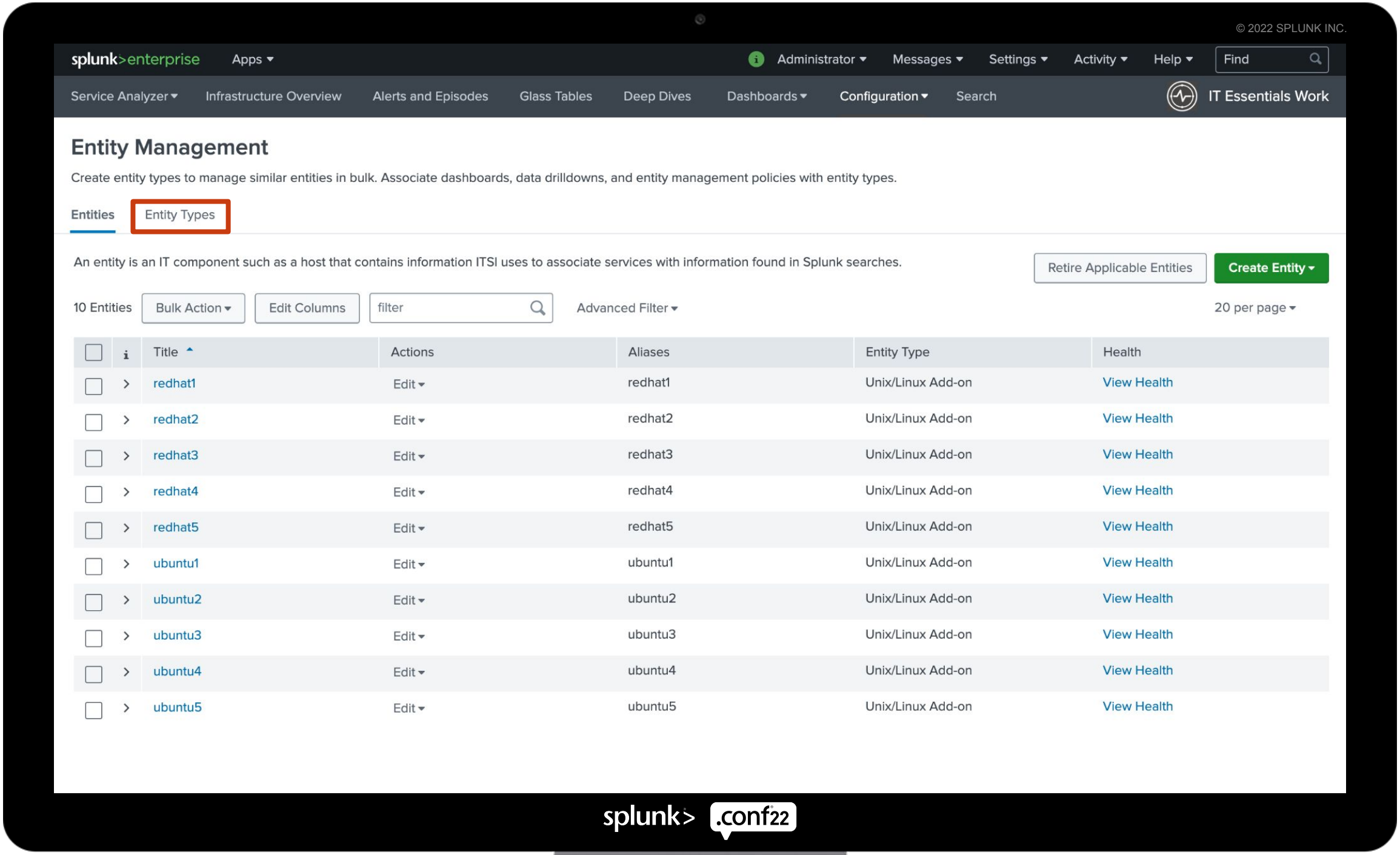


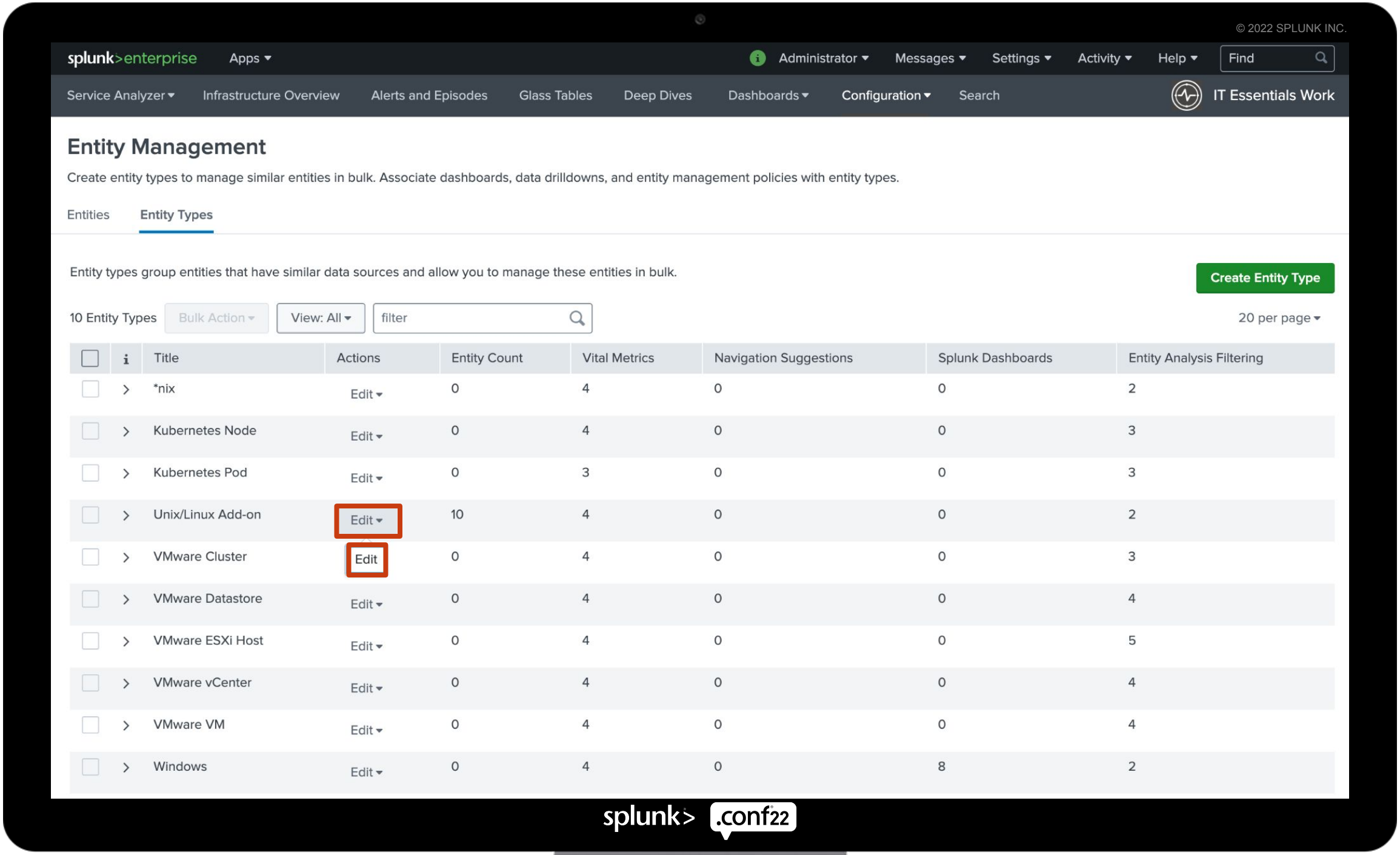
splunk> .conf22

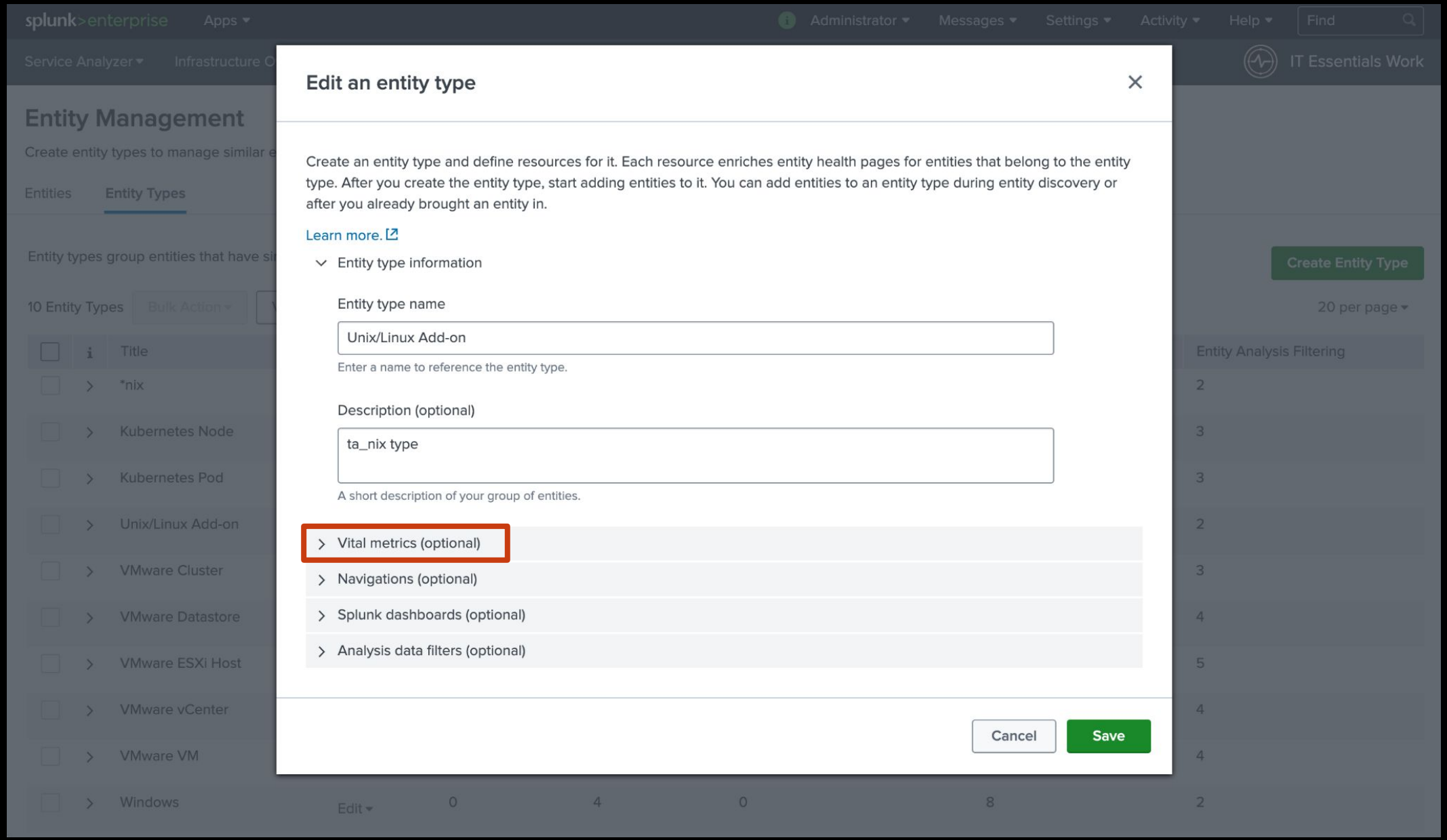
Are we done now?

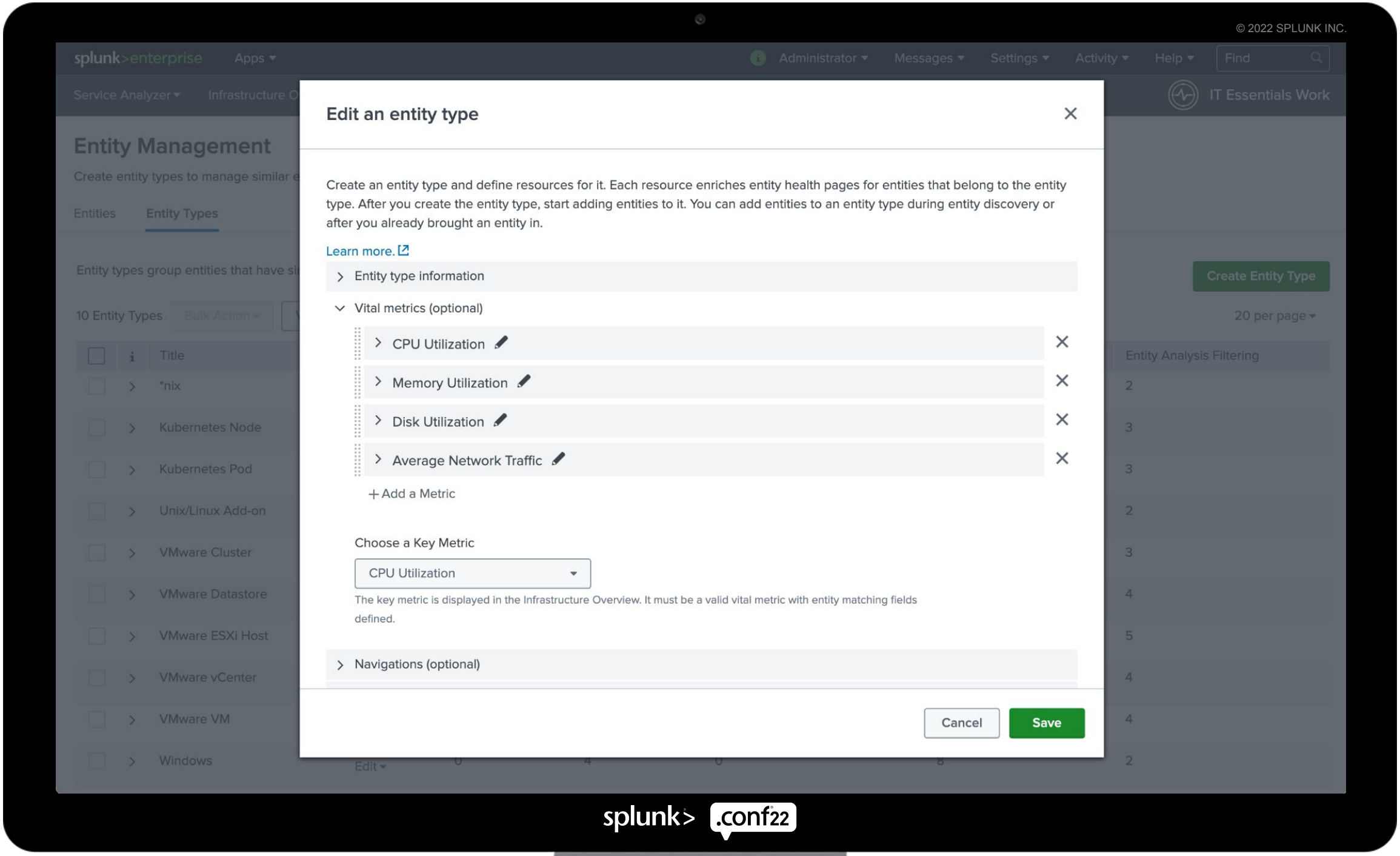


splunk> .conf22

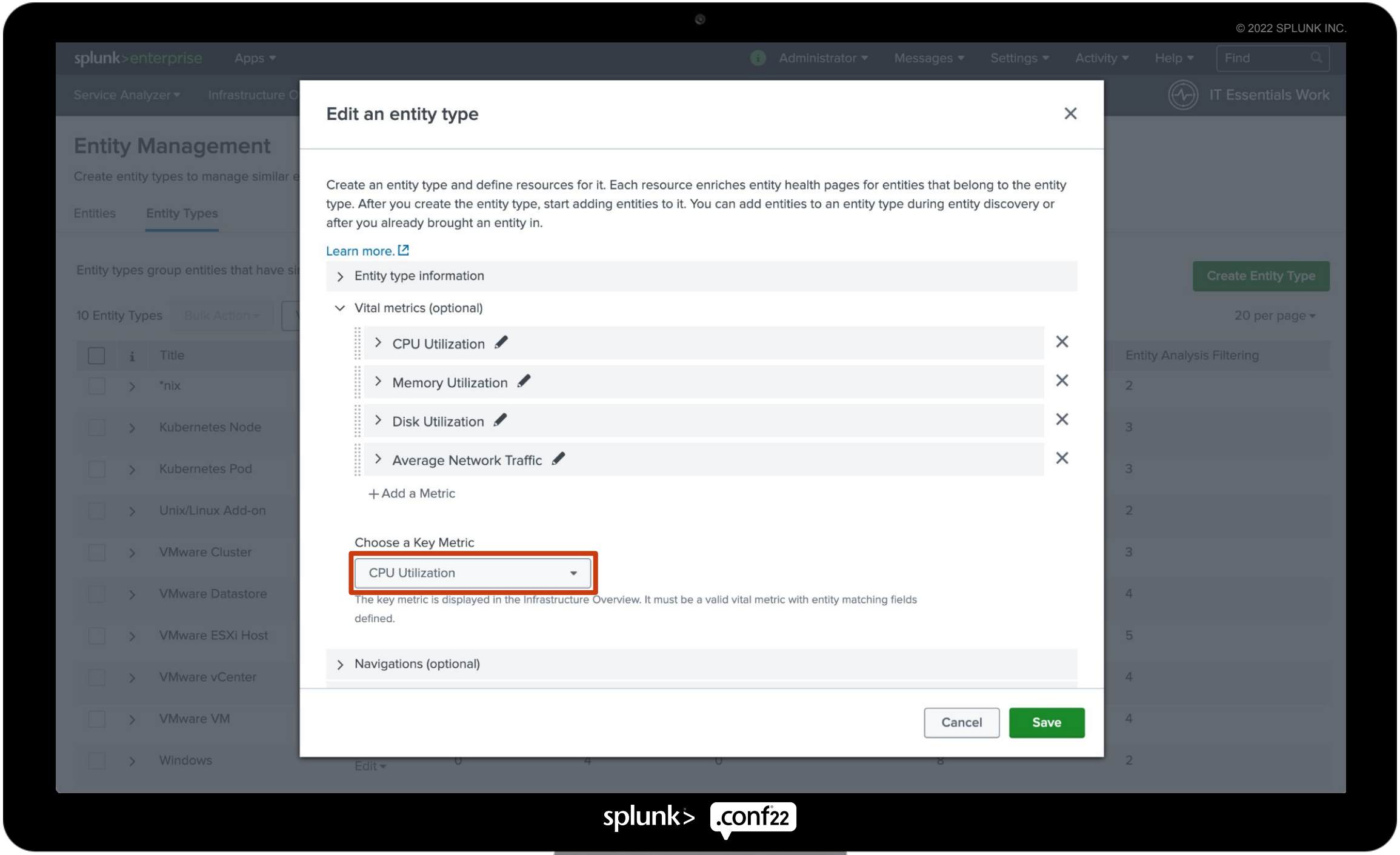




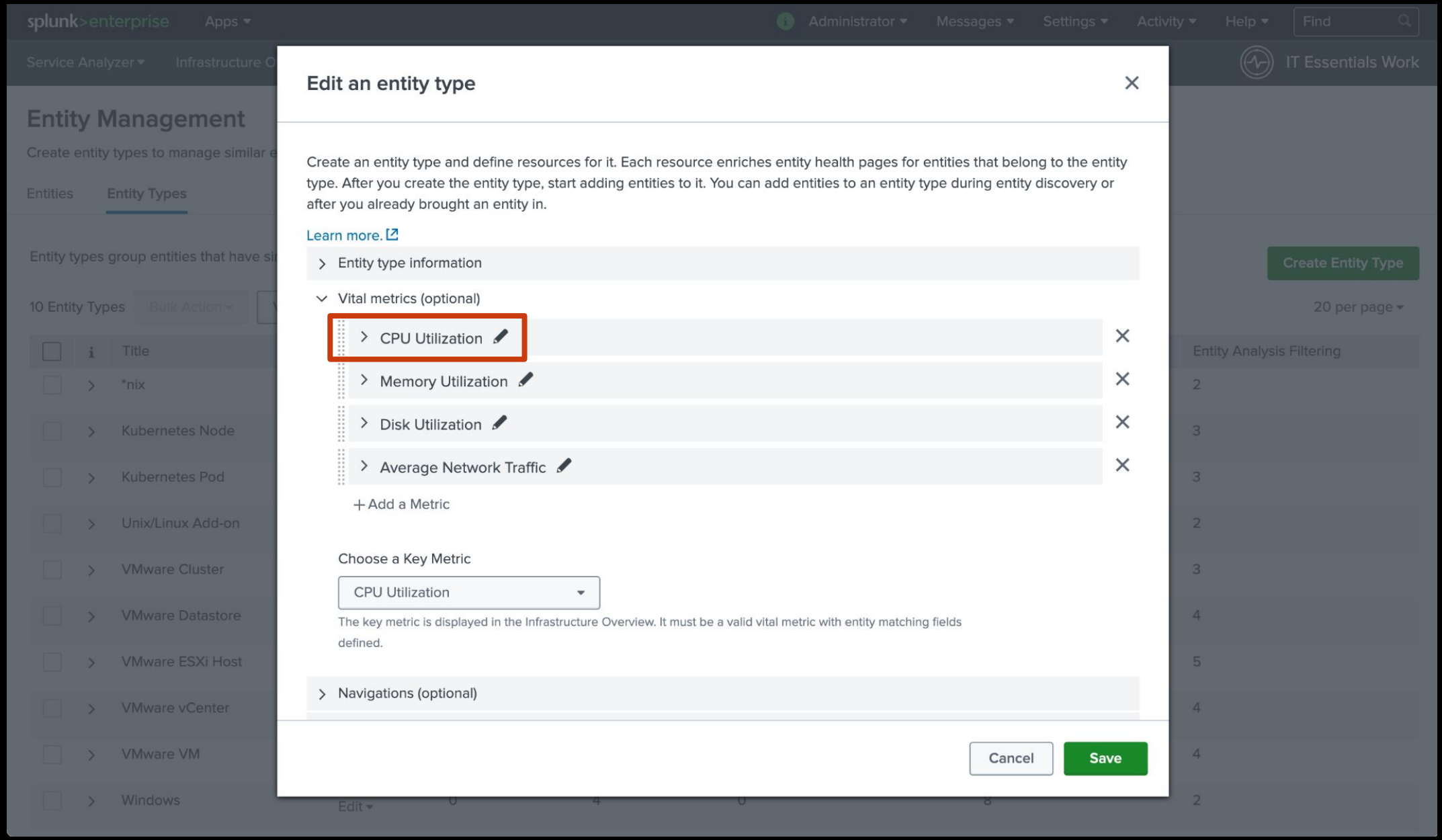


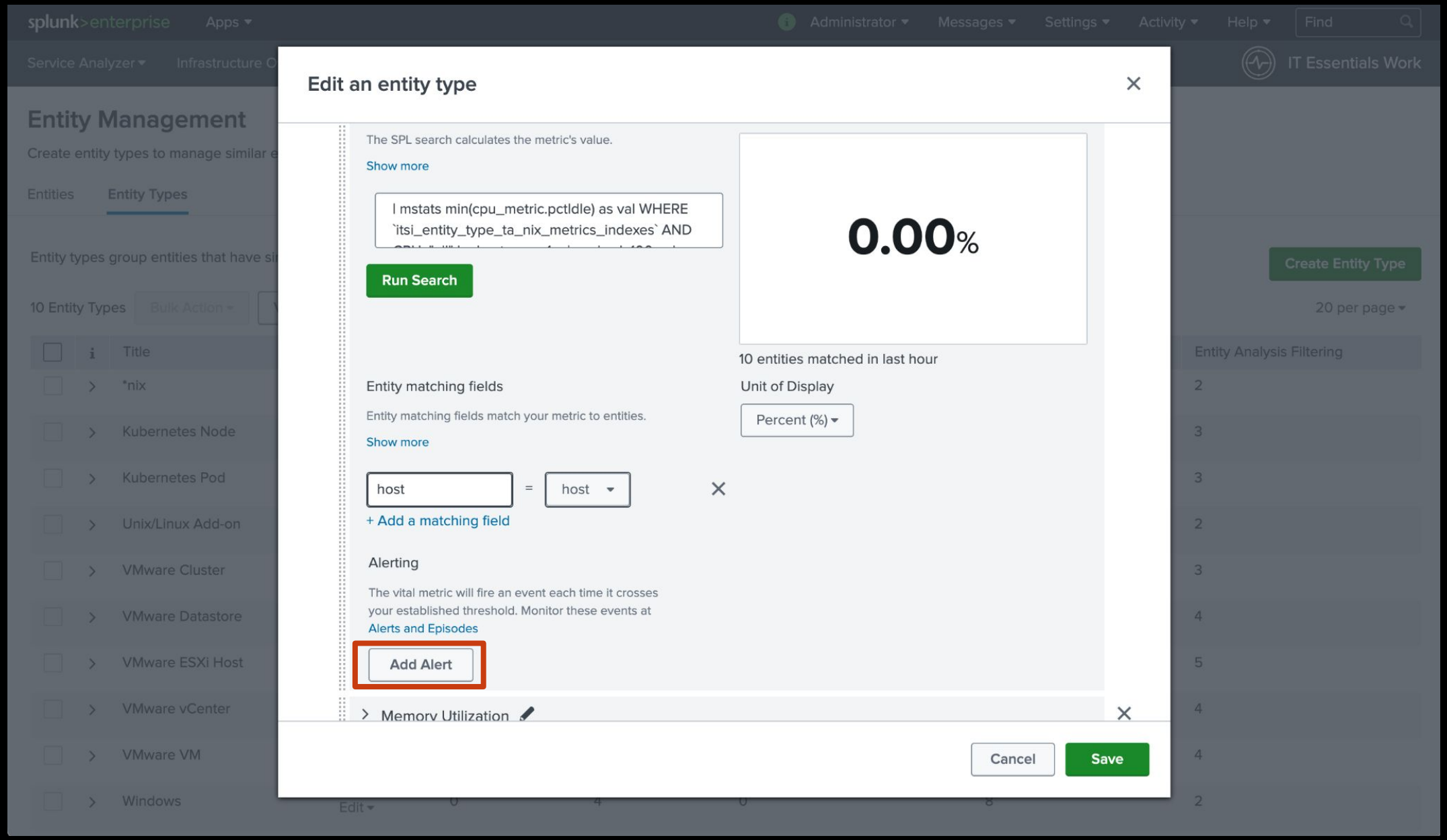


splunk> .conf22

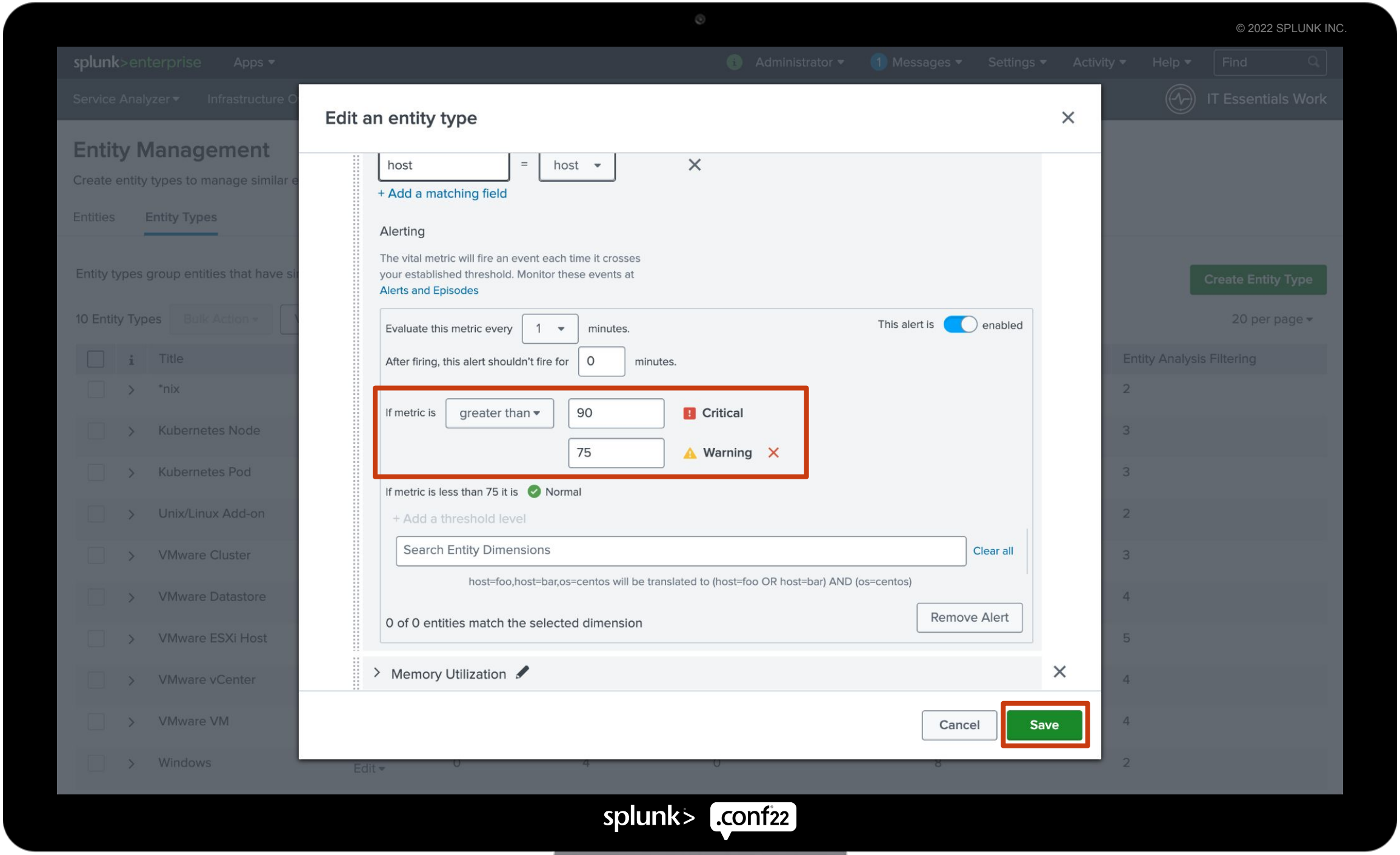


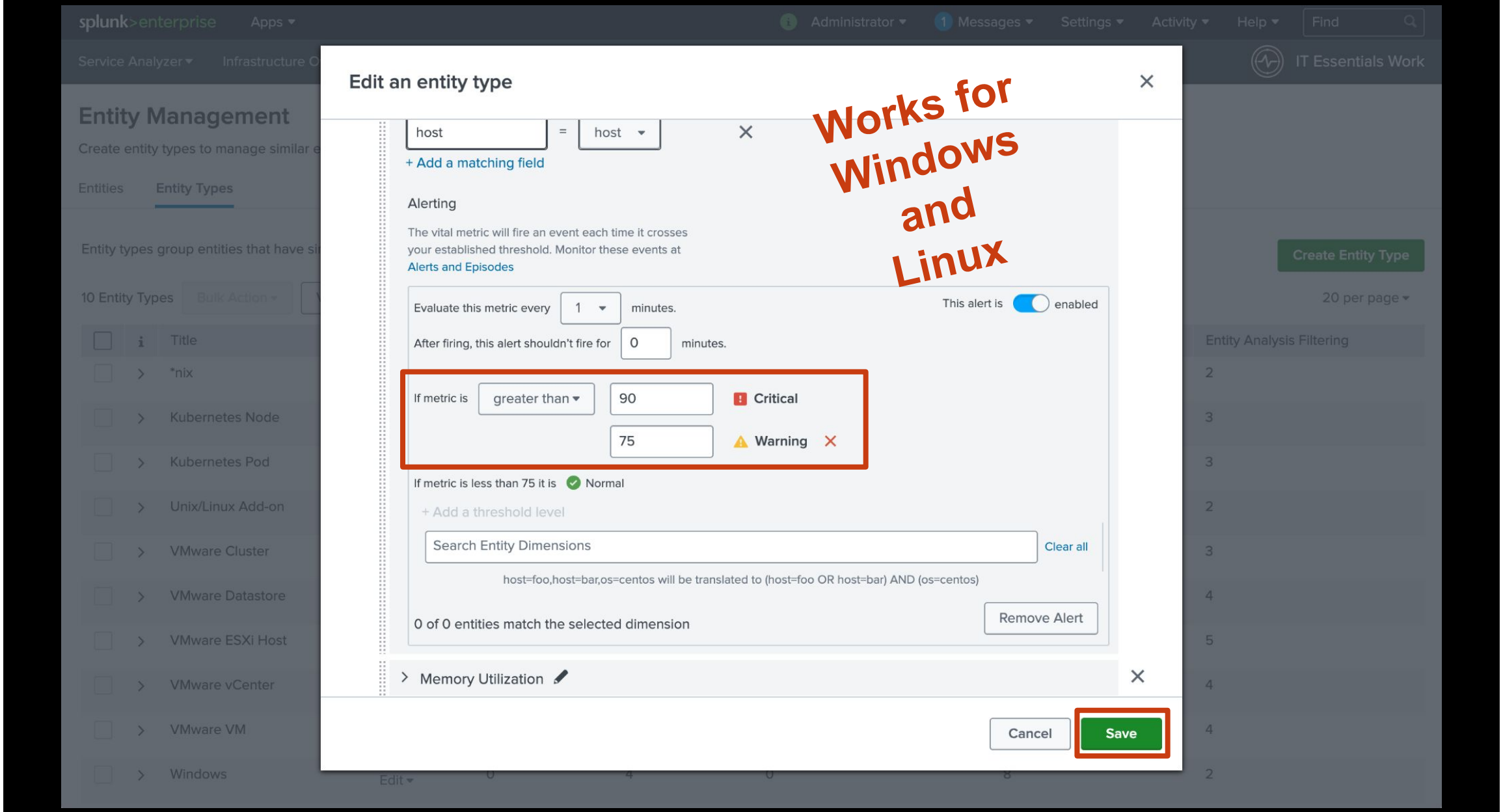
splunk> .conf22



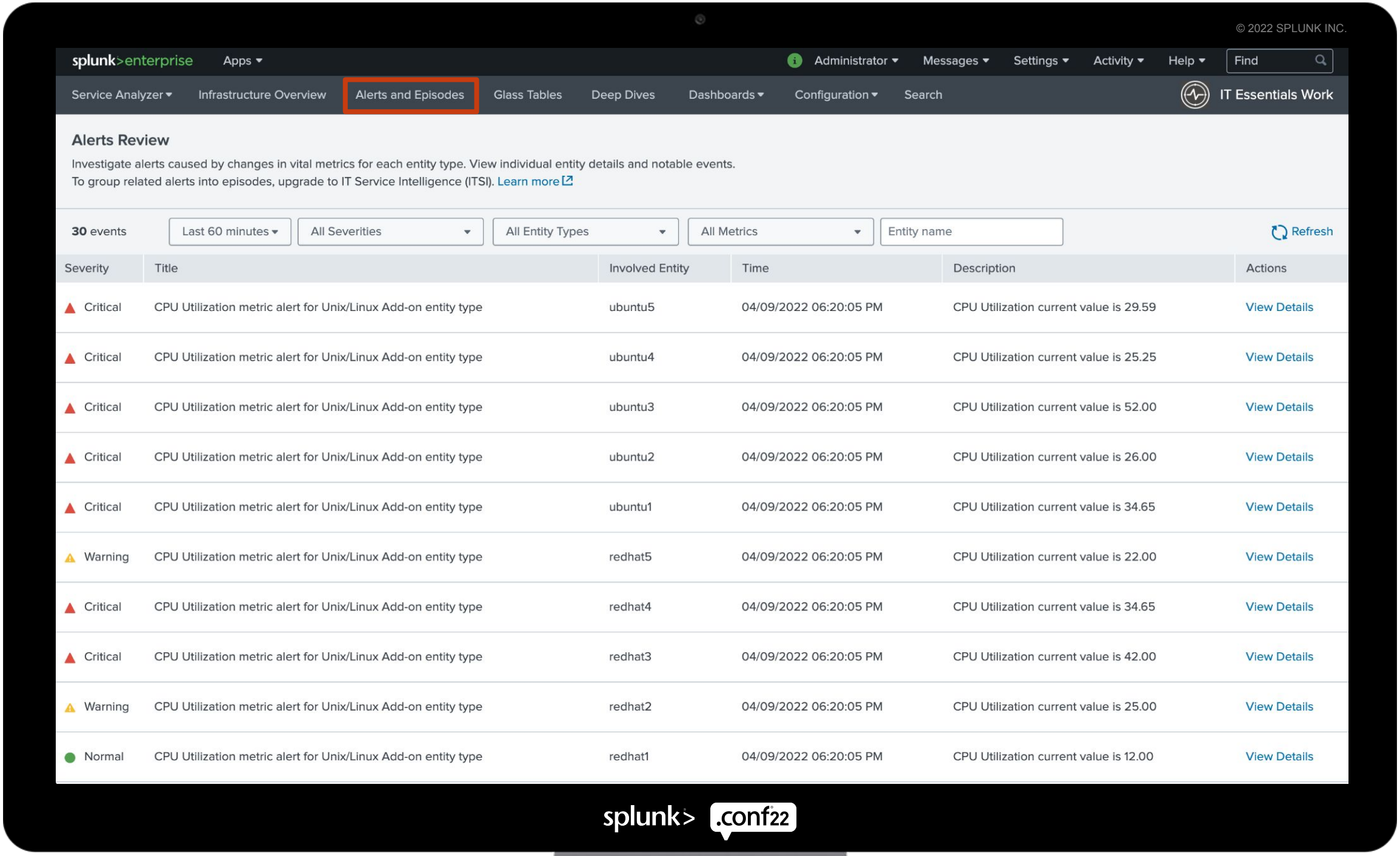


splunk> .conf22





splunk> .conf22



splunk> .conf22

Getting Data In

For ITW-Work / ITSI Infrastructure Monitoring

```
[script://./bin/cpu_metric.sh]
index = itsi_im_metrics
disabled = 0
```

```
[script://./bin/df_metric.sh]
index = itsi_im_metrics
disabled = 0
```

```
[script://./bin/interfaces_metric.sh]
index = itsi_im_metrics
disabled = 0
```

```
[script://./bin/iostat_metric.sh]
index = itsi_im_metrics
disabled = 0
```

```
[script://./bin/ps_metric.sh]
index = itsi_im_metrics
disabled = 0
```

```
[script://./bin/vmstat_metric.sh]
index = itsi_im_metrics
disabled = 0
```

You did it!

Where to go next?

Let's get migrating!

With this instruction and our Splunk Documentation you will be migrated in no time!

1) Splunk Documentation
   - https://docs.splunk.com/Documentation/CPWindowsDash/latest/CP/About
   - https://docs.splunk.com/Documentation/CPUnixDash/latest/CP/About

2) Github link for preset inputs.conf
   - https://github.com/splunk/conf22_OBS1493C

3) OBS1373 - IT Essentials - The Fast Pass to Value with Splunk for IT Operations
   - Session about all new things in IT Essentials, including Active Directory Entity Type

Special Thanks

Thank you to all who helped make this happen!

Thomas Booth

Director of Observability Strategy for Public Sector

Jenny Hollfelder

Global Services ITOps and Observability Architect

Tony Nesavich

Staff Consulting Sales Engineer

Bryan Pluta

Security Consulting Sales Engineer

Tapan Shah

ITSI Principal Product Manager

splunk> .conf22

Special Thanks

Thank you to our Cat Models

Bigfoot

Owner: Marco

Chewbacca

Owner: Marco

Black Cat

Owner: Jonathan

Sam

Owner: Jonathan

Bagheera

Owner: Jonathan

Thank You

splunk> .conf22