

Forward-Looking Statements



This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2022 Splunk Inc. All rights reserved.

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





Jonathan Fair

Professional Services Lead Architect
Global Services ITops and Observability

Marco Stadler

Professional Services Architect
EMEA ITops and Observability

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

1

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!



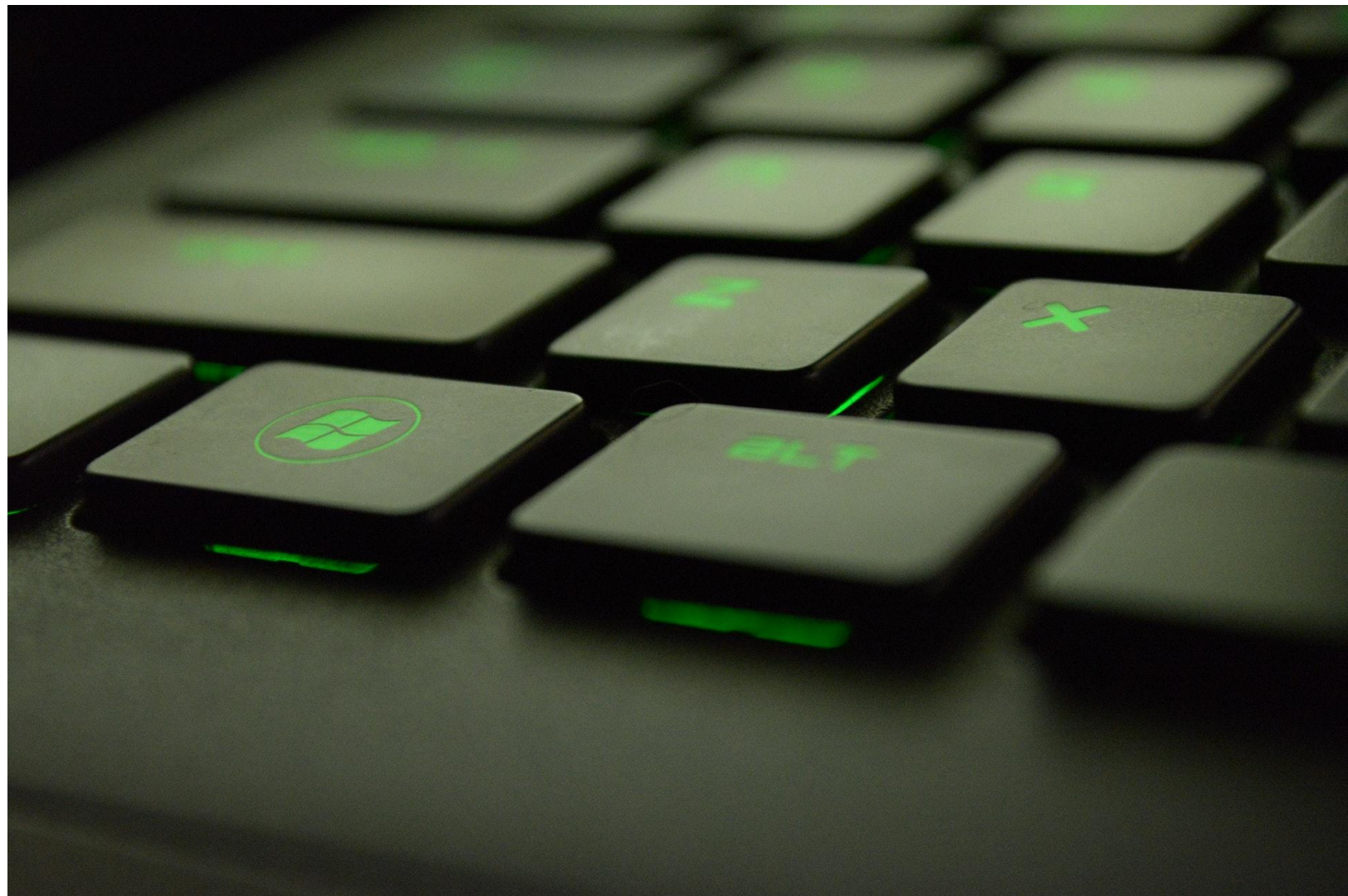
You did it!

Windows Dashboards and Reports

New Home + Some
New Updates!

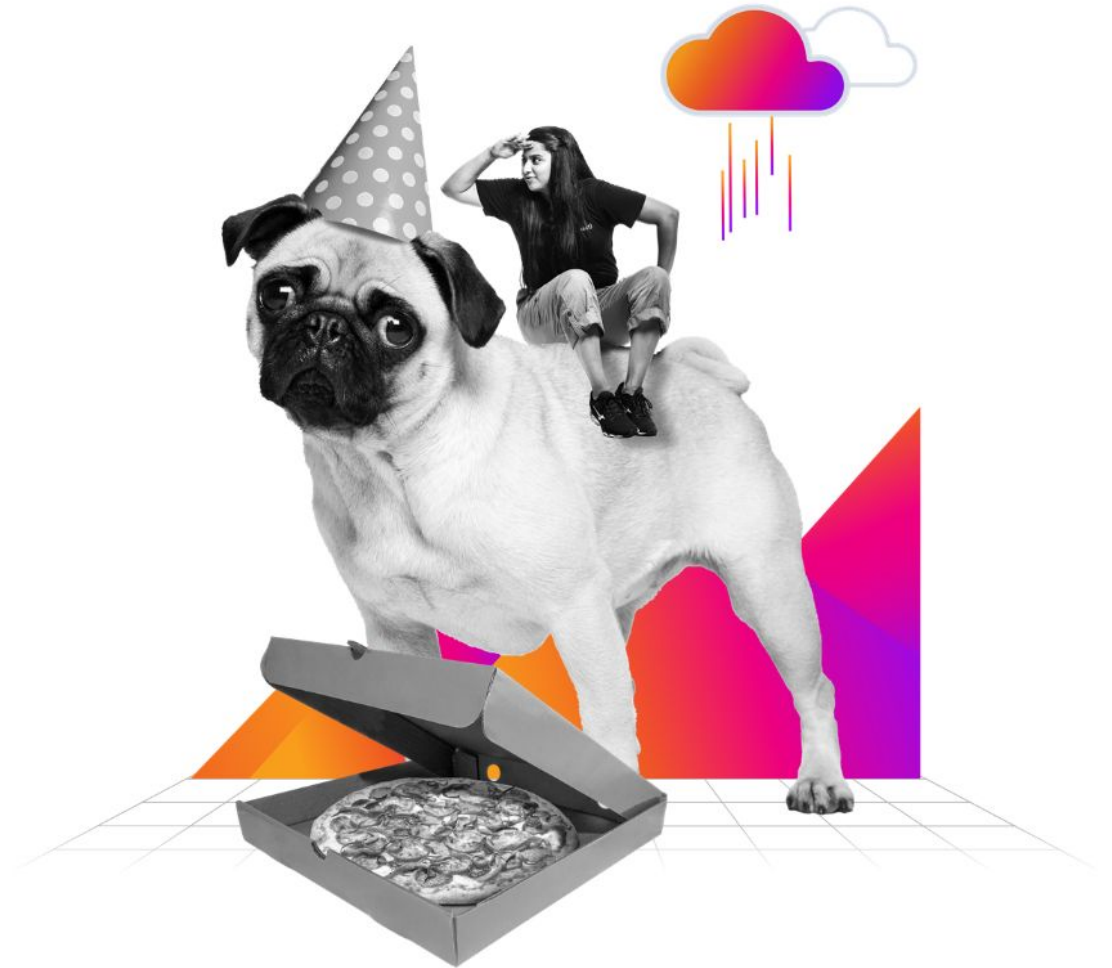
Content Pack focused on OS
Monitoring

- 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

Event types	
Showing 1-25 of 25 items	
App	Content Pack for Wind... ▾
Owner	Any ▾
Created in the App	▾
Search string	<input type="text" value="_index_windows"/> 🔍
Name ▾	Search string ▾
wineventlog_index_windows	index=wineventlog
wineventlog_common	eventtype=wineventlog_index_windows eventtype=wineventlog_windows OR source = "WinEventLog:DFS Replication" OR source = "WinEventLog:Directory Service" OR source = "WinEventLog:File Replication Service" OR source = "WinEventLog:Key Management Service" OR source="WinEventLog:DNS Server" OR source="WinEventLog:Exchange Auditing"
windows_index_windows	index=windows
perfmon_index_windows	index=perfmon
msad_index_windows	index=msad

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
```




New Search

Save As ▾

Create Table View

Close

| savedsearch "build_winfra_lookup"

Last 24 hours ▾



✓ 20 results (4/25/22 6:00:00.000 PM to 4/26/22 6:38:39.000 PM) No Event Sampling ▾

Job ▾



Smart Mode ▾

Events (0)

Patterns

Statistics (20)

Visualization

20 Per Page ▾

Format

Preview ▾

savedSearch ⬆



status ⬆



WinApp_Lookup_Build_Perfmon - Update - Server

201

WinApp_Lookup_Build_Printmon - Update

201

WinApp_Lookup_Build_Netmon - Update - Detail

201

WinApp_Lookup_Build_Netmon - Update - Server

201

WinApp_Lookup_Build_Hostmon_Services - Update - Detail

201

WinApp_Lookup_Build_Hostmon_Process - Update - Detail

201

WinApp_Lookup_Build_Hostmon_FS - Update - Detail

201

WinApp_Lookup_Build_Hostmon_Machine - Update - Detail

201

WinApp_Lookup_Build_Hostmon - Update - Server

201

WinApp_Lookup_Build_Event - Update - Detail

201

WinApp_Lookup_Build_Event - Update - Server

201

WinApp_Lookup_Build_Perfmon - Update - Detail

201

ActiveDirectory: Update Computer Lookup

201

ActiveDirectory: Update User Lookup

201

ActiveDirectory: Update Group Lookup

201

ActiveDirectory: Update GPO Lookup

201

SiteInfo_Lookup_Update

201

tHostInfo_Lookup_Update

201

HostToDomain_Lookup_Update

201

DomainSelector_Lookup

201



Apps



Search & Reporting



IT Essentials Work

Python Upgrade Readiness
App

Update

Splunk Add-on for Unix and
LinuxSplunk Essentials for Cloud
and Enterprise 8.2

Splunk Secure Gateway

+ Find More Apps

Explore Splunk Enterprise



Product Tours

New to Splunk? Take a tour to help
you on your way.

Add Data

Add or forward data to Splunk
Enterprise. Afterwards, you may
[extract fields](#).Splunk Apps [↗](#)Apps and add-ons extend the
capabilities of Splunk Enterprise.Splunk Docs [↗](#)Comprehensive documentation for
Splunk Enterprise and for all other
Splunk products.

Close



Choose a home dashboard



Infrastructure Overview

All Status ▾

All Severities ▾

Clear
all

Last 60 minutes ▾

Refresh ▾

Group By: Entity Type ▾

Sort By: # of Entities (High to low) ▾

☐ Hide entity type

Windows (2)

2 Active : 0 Inactive : 0 Unstable



Distributed by CPU Utilization

*nix (0)

0 Active : 0 Inactive : 0 Unstable



Distributed by CPU Utilization

Kubern...

0 Active



Distributed by Average CPU Usage

d (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

Predictive Analytics

Event Analytics Monitoring

Event Analytics Audit

ITSI Health Check

ITSI SVC Statistics

Dashboards

Datasets

Reports



Dashboards

[Create New Dashboard](#)

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

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

X

i	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



Dashboards

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

[Create New Dashboard](#)

Latest Resources

☆ Examples for Dashboard Studio

Browse examples of dashboards & visualizations. [Visit Example Hub](#)

Intro to

Learn how to build dashboards with Dashboard Studio. [Learn More](#)

Learn how to build traditional Simple XML dashboards. [Learn More](#)

87 Dashboards

All

Yours

This App's

Windows

X

i	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?**





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



< Back

Windows

All Status ▾

All Severities ▾

Search Entity Dimensions

Clear
all

Last 60 minutes ▾

↻ Refresh

Entity Health

Current Entity Status Breakdown



CPU Utilization

3.34%



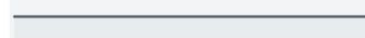
Memory Utilization

10.67%



Disk Utilization

8.22%



Average Network Usage

45.58KB/s

Showing 2 entities with no alerts filter applied. ✓ 2 Active ⚠ 0 Unstable ✖ 0 Inactive ℹ 0 N/A

20 per page ▾

Entity Name ▴	Status	Last Updated	Dimensions	CPU Utilization ▴	Memory Utilization ▴	Disk Utilization ▴	Average Ne
DC01	✓ Active	Thu, 14 Apr 2022 03:15:10 GMT	entity_name: DC01 host: DC01 itsi_entity_id: DC01	2.58% ↓ -2.04	N/A	8.24% 0.00	43.2
WINDOWS_CLIENT_	✓ Active	Thu, 14 Apr 2022 03:15:10 GMT	entity_name: WINDOWS_CLIENT_ host: WINDOWS_CLIENT_ itsi_entity_id: WINDOWS_CLIENT_	4.09% ↑ 1.70	10.67% ↑ 1.06	8.20% 0.00	47.9



< Back

Windows

All Status ▾

All Severities ▾

Search Entity Dimensions

Clear
all

Last 60 minutes ▾

↻ Refresh

Entity Health

Current Entity Status Breakdown



CPU Utilization

3.34%



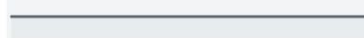
Memory Utilization

10.67%



Disk Utilization

8.22%



Average Network Usage

45.58KB/s

Showing 2 entities with no alerts filter applied. ✓ 2 Active ⚠ 0 Unstable ✖ 0 Inactive ℹ 0 N/A

20 per page ▾

Entity Name ▴	Status	Last Updated	Dimensions	CPU Utilization ▴	Memory Utilization ▴	Disk Utilization ▴	Average Ne
DC01	✓ Active	Thu, 14 Apr 2022 03:15:10 GMT	<div>entity_name: DC01</div> <div>host: DC01</div> <div>itsi_entity_id: DC01</div>	2.58% ↓ -2.04	N/A	8.24% 0.00	43.2
WINDOWS_CLIENT_	✓ Active	Thu, 14 Apr 2022 03:15:10 GMT	<div>entity_name: WINDOWS_CLIENT_</div> <div>host: WINDOWS_CLIENT_</div> <div>itsi_entity_id: WINDOWS_CLIENT_</div>	4.09% ↑ 1.70	10.67% ↑ 1.06	8.20% 0.00	47.9

WINDOWS_CLIENT_ Active Mon, 25 Apr 2022 17:34:09 GMT

Windows Overview Dashboard ▾

Event Data Search

Analytics

Last 1 hour ?

Refresh ▾



< Summary

5 0

Uptime in hours

3 -0

CPU Utilization %

8 0

Disk Utilization %

9 -0

Memory Utilization %

345 ↑8

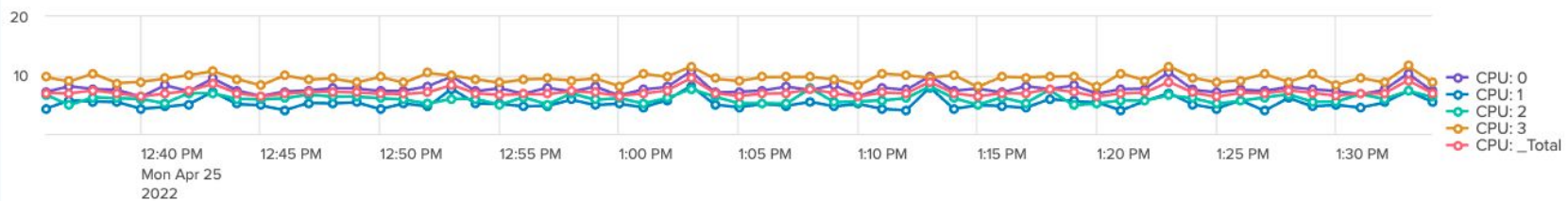
Network I/O (KB/s)

Process Monitoring Info

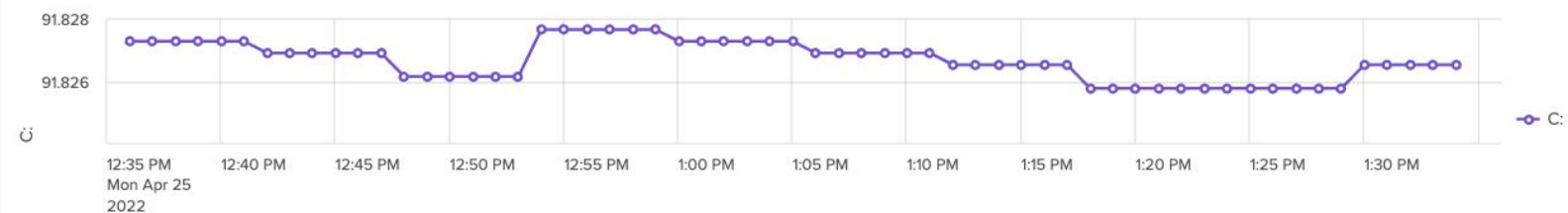
instance ▾	PID ▾	Up hh:mm:ss ▾	%_Privileged_Time ▾	%_Processor_Time ▾	%_User_Time ▾	IO_Read_Bytes/sec ▾	IO_Write_Bytes/sec ▾	Private_MByte
Idle		05:33:05	399.99	399.99				
_Total			399.99	399.99	8.11	206363.69	128069.08	1118
WmiPrvSE	3980	05:32:23	57.57	127.27	45.45	8344888.93		2
WmiPrvSE#2	3292	00:00:57	18.18	30.3	9.09			4
svchost	1508	05:33:01	12.19	29.17	16.98	12.01	10.81	

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

CPU Utilization %



Disk Utilization %



WINDOWS_CLIENT_ Active Mon, 25 Apr 2022 17:34:09 GMT

Windows Overview Dashboard ▾

Event Data Search

Analytics

Last 1 hour ▾ ?

Refresh ▾



< Summary

Process Monitoring Info

instance ▾	PID ▾	Up hh:mm:ss ▾
Idle		05:33:05
_Total		
WmiPrvSE	3980	05:32:23
WmiPrvSE#2	3292	00:00:57
svchost	1508	05:33:01

filter X

Application Crashes - Windows

Application Installs - Windows

Event Monitoring - Windows

Host Information - Windows

Network Activity - Windows

Processes - Windows

Services - Windows

Windows Overview Dashboard

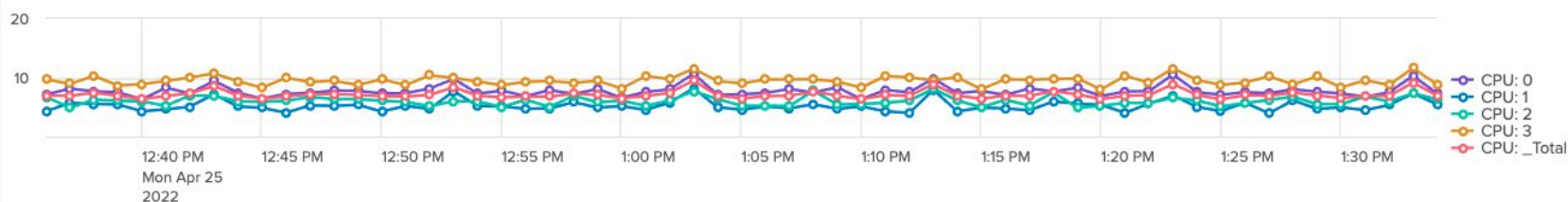
Windows Update - Windows

9 Dashboards of 9

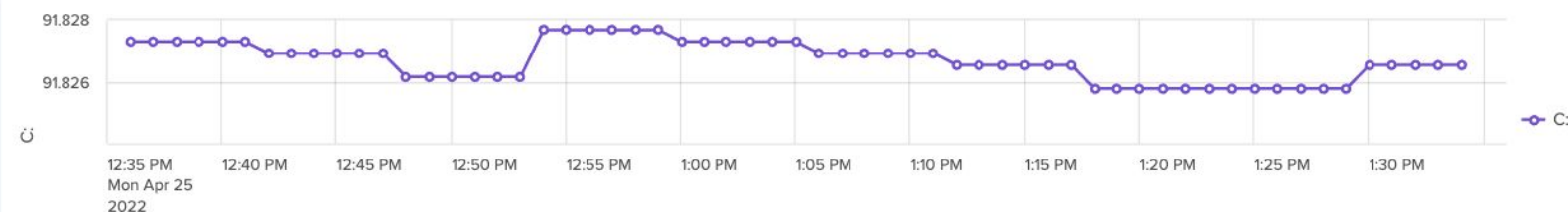
time ▾	%_User_Time ▾	IO_Read_Bytes/sec ▾	IO_Write_Bytes/sec ▾	Private_MByte
399.99				
399.99	8.11	206363.69	128069.08	1118
127.27	45.45	8344888.93		2
30.3	9.09			4
29.17	16.98	12.01	10.81	

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

CPU Utilization %



Disk Utilization %



**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
485 sourcetype=PerfmonMetrics:LogicalDisk
```

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**

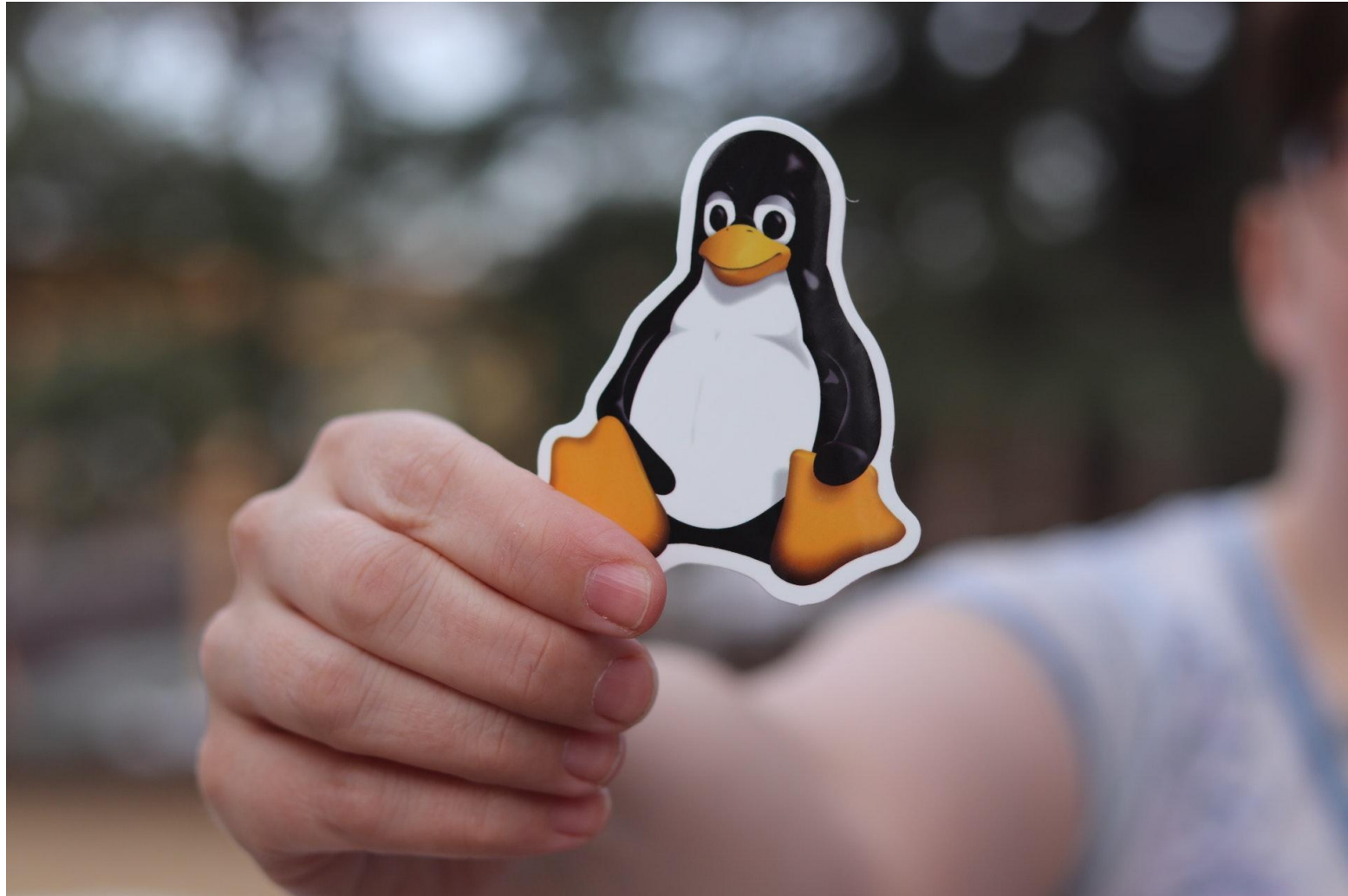
Let's tackle Linux



Unix (and Linux) Dashboards and Reports

What you have is what
you get

Five Hundred Dashboards

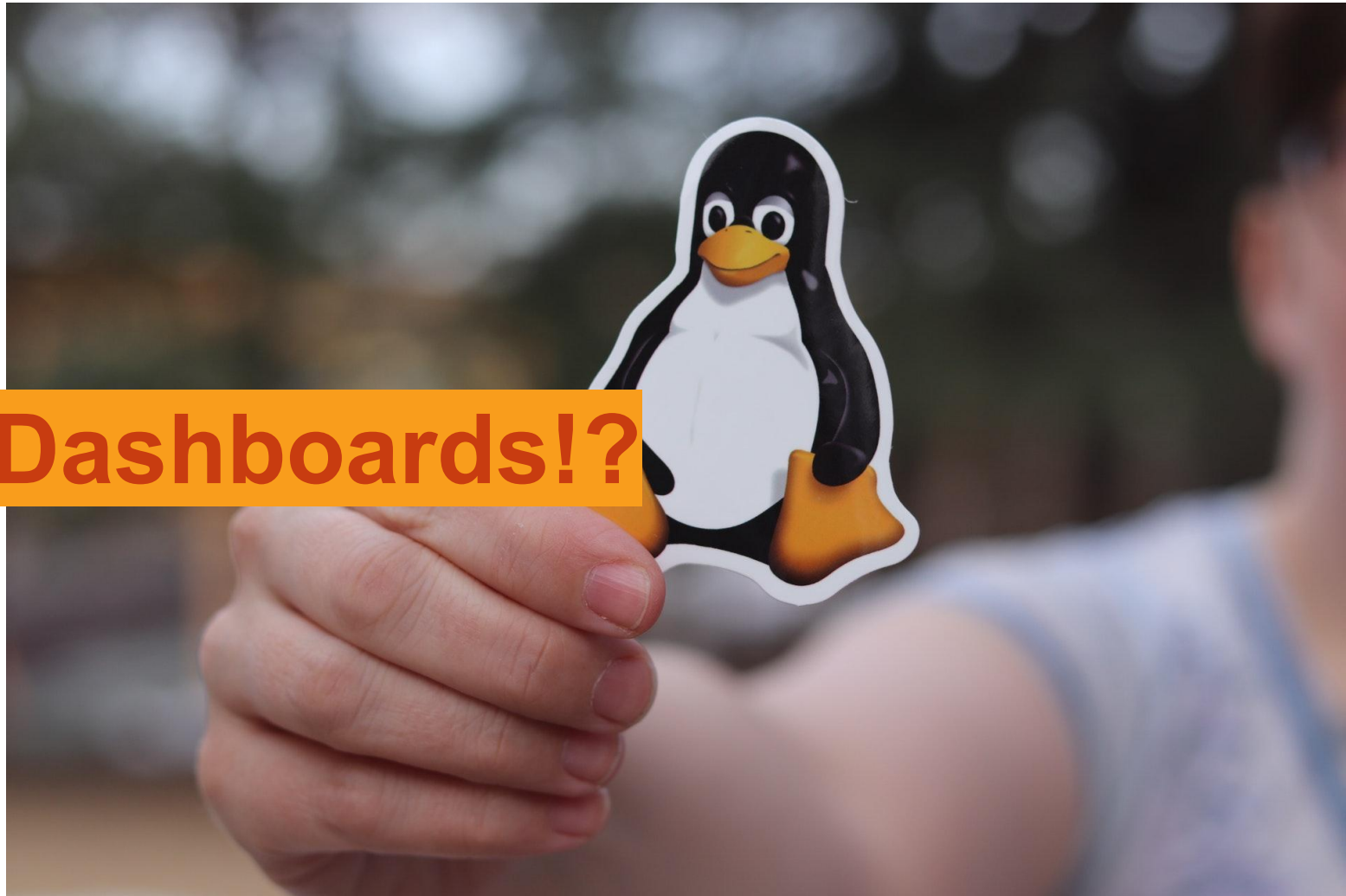


Unix (and Linux) Dashboards and Reports

What you have is what
you get

Five Hundred Dashboards

500 Dashboards!?

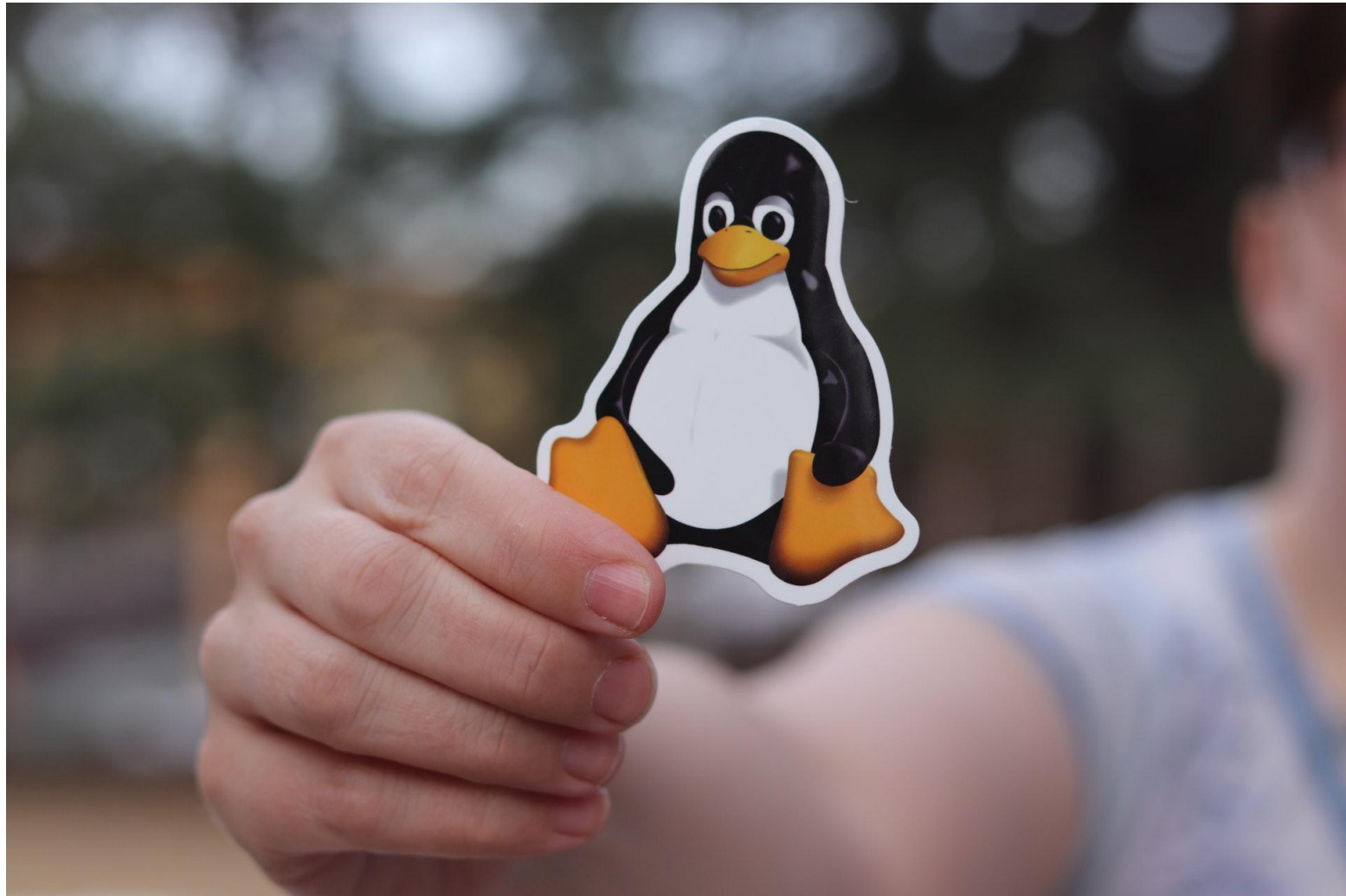


Unix (and Linux) Dashboards and Reports

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			✓



Apps



Search & Reporting



IT Essentials Work

Python Upgrade Readiness
App

Update

Splunk Add-on for Unix and
LinuxSplunk Essentials for Cloud
and Enterprise 8.2

Splunk Secure Gateway

+ Find More Apps

Explore Splunk Enterprise



Product Tours

New to Splunk? Take a tour to help
you on your way.

Add Data

Add or forward data to Splunk
Enterprise. Afterwards, you may
[extract fields](#).Splunk Apps [🔗](#)Apps and add-ons extend the
capabilities of Splunk Enterprise.Splunk Docs [🔗](#)Comprehensive documentation for
Splunk Enterprise and for all other
Splunk products.

Close



Choose a home dashboard



Infrastructure Overview

All Status ▾

All Severities

Clear
all

Last 60 minutes ▾

Refresh ▾

Group By: Entity Type ▾

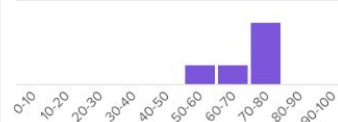
Sort By: # of Entities (High to low) ▾

☐ Hide entity t

Unix/Linux Add-on (10)

10 Active : 0 Inactive : 0 Unstable

⚠ 1 Warning Alerts (+ 29 more)



Distributed by CPU Utilization

*nix (0)

0 Active : 0 Inactive : 0 Unstable



Distributed by CPU Utilization

Kubern

0 Active



Distributed by Average CPU Usage

d (0)

e : 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

Windows (0)

0 Active : 0 Inactive : 0 Unstable



Distributed by CPU Utilization



Dashboards

[Create New Dashboard](#)

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

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](#)

5 Dashboards

All

Yours

This App's

unix



i	Title ^	Actions	Owner ⇅	App ⇅	Sharing ⇅	Type ⇅
>	Alerts - Unix	Edit	nobody	DA-ITSI-CP-unix-dash...	Global	Classic
>	Home - Unix	Edit	nobody	DA-ITSI-CP-unix-dash...	Global	Classic
>	Hosts - Unix	Edit	nobody	DA-ITSI-CP-unix-dash...	Global	Classic
>	Metrics - Unix	Edit	nobody	DA-ITSI-CP-unix-dash...	Global	Classic
>	Settings - Unix	Edit	nobody	DA-ITSI-CP-unix-dash...	Global	Classic



Dashboards

[Create New Dashboard](#)

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

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](#)

5 Dashboards

All

Yours

This App's

unix

×

i	Title ^	Actions	Owner ⇅	App ⇅	Sharing ⇅	Type ⇅
>	Alerts - Unix	Edit ▾	nobody	DA-ITSI-CP-unix-dash...	Global	Classic
>	Home - Unix	Edit ▾	nobody	DA-ITSI-CP-unix-dash...	Global	Classic
>	Hosts - Unix	Edit ▾	nobody	DA-ITSI-CP-unix-dash...	Global	Classic
>	Metrics - Unix	Edit ▾	nobody	DA-ITSI-CP-unix-dash...	Global	Classic
>	Settings - Unix	Edit ▾	nobody	DA-ITSI-CP-unix-dash...	Global	Classic



Settings

Your Data

Categories

Alerts

Save

Unix Index(es) ?

index=os

X

Preview

Add New

Syslog Data ?

sourcetype=syslog

X

Preview

Add New

CPU Data ?

sourcetype=cpu

X

Preview

Add New

DF Data ?

sourcetype=df

X

Preview

Add New

Hardware Data ?

sourcetype=hardware

X



Settings

Your Data

Categories

Alerts

Categories



all_hosts

10

Groups



Redhat

5

Ubuntu

5

Hosts in

Redhat

redhat1

redhat2

redhat3

redhat4

redhat5

Hosts not in

Redhat

ubuntu1

Ubuntu

ubuntu2

Ubuntu

ubuntu3

Ubuntu

ubuntu4

Ubuntu

ubuntu5

Ubuntu



Settings

Your Data

Categories

Alerts

Alert

Threshold

Impact

Status

CPU_Exceeds_Percent_by_Host

CPU usage has exceeded a threshold for one or more hosts

more than %

Business Impact:

Enabled

Disable

Info Medium High

Remediation:

Escalation:

Save

CPU_Under_Percent_by_Host

CPU usage is below a threshold for one or more hosts

less than %

Business Impact:

Possible under-utilization of con

Enable

Disabled

Info Medium High

Remediation:

Try balance workloads between

Escalation:

Saved

Disk_Used_Exceeds_Percent_by_Host

Disk used percentage over threshold for one or more hosts

more than %

Business Impact:

Enable

Disabled

Info Medium High

Remediation:

Escalation:

Saved

**Moving is not
always hard.**

**HOW'S EVERYTHING
GOING WITH THE MOVE?**

IT'S GREAT.



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

Unix/Linux Add-on (10)

10 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

Windows (0)

0 Active : 0 Inactive : 0 Unstable



Distributed by CPU Utilization



< Back

Unix/Linux
Add-on

All Status ▾

All Severities ▾

Search Entity Dimensions

Clear
all

Last 60 minutes ▾

Refresh ▾

Entity Health

Current Entity Status Breakdown



CPU Utilization

12.68%



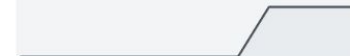
Memory Utilization

26.56%



Disk Utilization

57.00%



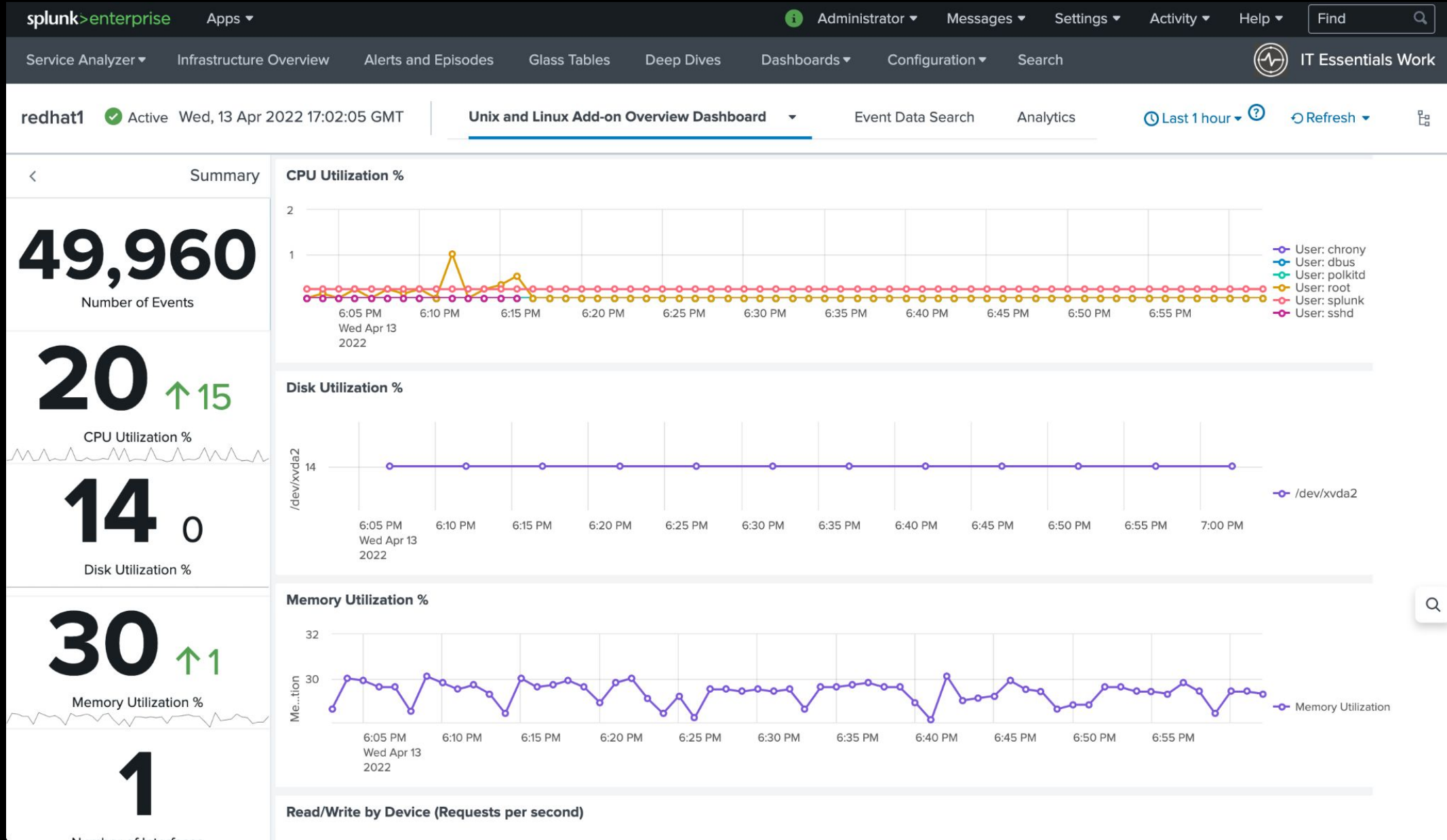
Average Network Traffic

113,227.83 KB/s

Showing 10 entities with no alerts filter applied. ✓ 10 Active ⚠ 0 Unstable ✖ 0 Inactive ! 0 N/A

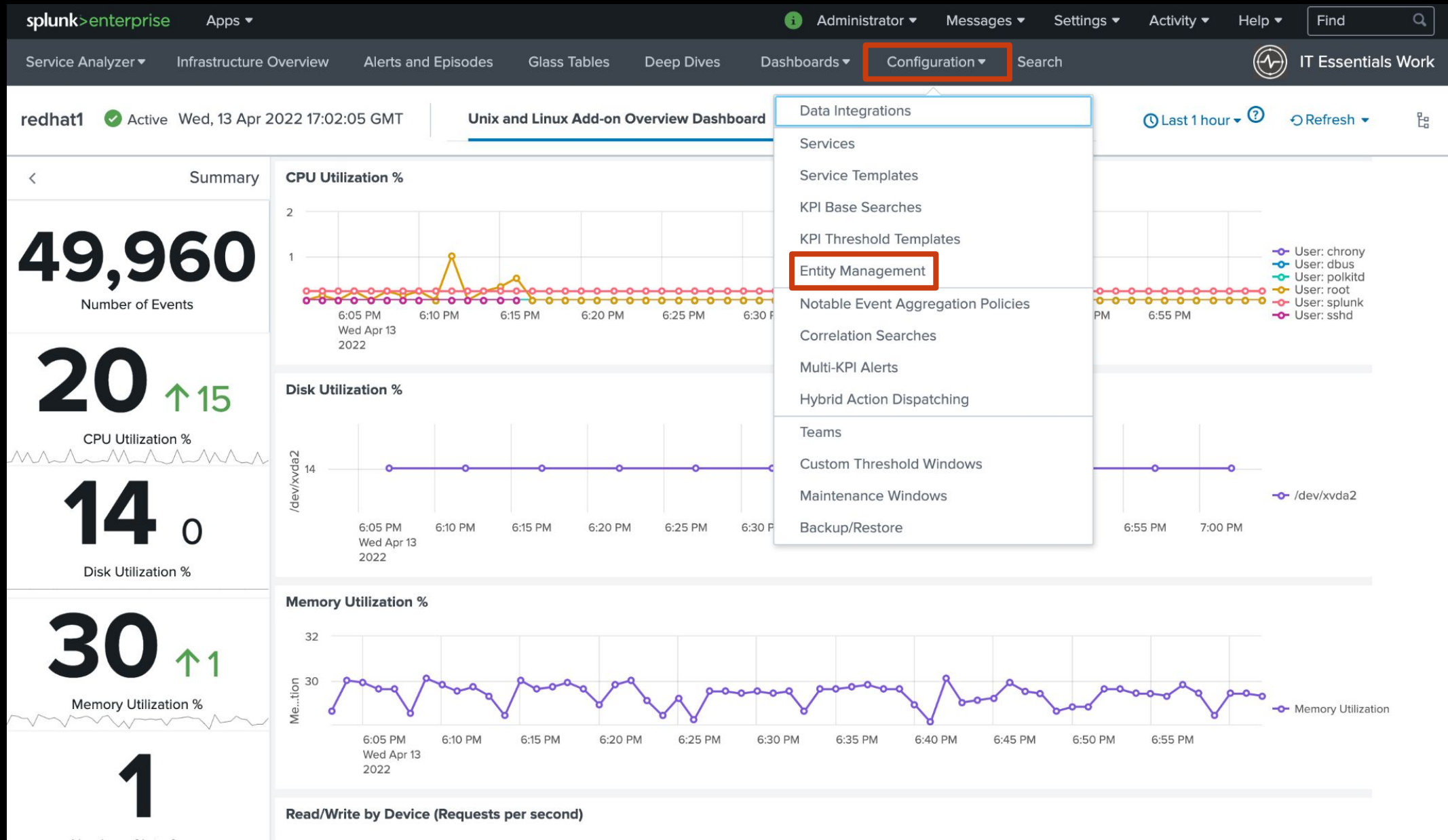
20 per page ▾

Entity Name ▴	Status	Last Updated	Dimensions	CPU Utilization ▴	Memory Utilization ▴	Disk Utilization ▴	Average Network Traffic ▴
redhat1	✓ Active	Wed, 13 Apr 2022 16:58:03 GMT	entity_name: redhat1 host: redhat1 itsi_entity_id: redhat1	6.93% ↓ -4.07	29.80% ↑ 0.20	14.00% 0.00	87327.47
redhat2	✓ Active	Wed, 13 Apr 2022 16:58:03 GMT	entity_name: redhat2 host: redhat2 itsi_entity_id: redhat2	14.00% ↓ -9.23	29.10% ↓ -0.20	14.00% 0.00	86909.37
redhat3	✓ Active	Wed, 13 Apr 2022 16:58:03 GMT	entity_name: redhat3 host: redhat3 itsi_entity_id: redhat3	6.06% ↓ -16.94	29.50% ↓ -0.40	14.00% 0.00	86234.89



Are we done now?







Entity Management

Create entity types to manage similar entities in bulk. Associate dashboards, data drilldowns, and entity management policies with entity types.

[Entities](#)[Entity Types](#)

An entity is an IT component such as a host that contains information ITSI uses to associate services with information found in Splunk searches.

[Retire Applicable Entities](#)[Create Entity ▾](#)

10 Entities

[Bulk Action ▾](#)[Edit Columns](#)[Advanced Filter ▾](#)

20 per page ▾

<input type="checkbox"/>	i	Title ▲	Actions	Aliases	Entity Type	Health
<input type="checkbox"/>	>	redhat1	Edit ▾	redhat1	Unix/Linux Add-on	View Health
<input type="checkbox"/>	>	redhat2	Edit ▾	redhat2	Unix/Linux Add-on	View Health
<input type="checkbox"/>	>	redhat3	Edit ▾	redhat3	Unix/Linux Add-on	View Health
<input type="checkbox"/>	>	redhat4	Edit ▾	redhat4	Unix/Linux Add-on	View Health
<input type="checkbox"/>	>	redhat5	Edit ▾	redhat5	Unix/Linux Add-on	View Health
<input type="checkbox"/>	>	ubuntu1	Edit ▾	ubuntu1	Unix/Linux Add-on	View Health
<input type="checkbox"/>	>	ubuntu2	Edit ▾	ubuntu2	Unix/Linux Add-on	View Health
<input type="checkbox"/>	>	ubuntu3	Edit ▾	ubuntu3	Unix/Linux Add-on	View Health
<input type="checkbox"/>	>	ubuntu4	Edit ▾	ubuntu4	Unix/Linux Add-on	View Health
<input type="checkbox"/>	>	ubuntu5	Edit ▾	ubuntu5	Unix/Linux Add-on	View Health



Entity Management

Create entity types to manage similar entities in bulk. Associate dashboards, data drilldowns, and entity management policies with entity types.

Entities

Entity Types

Entity types group entities that have similar data sources and allow you to manage these entities in bulk.

[Create Entity Type](#)

10 Entity Types

Bulk Action ▾

View: All ▾

filter



20 per page ▾

<input type="checkbox"/>	i	Title	Actions	Entity Count	Vital Metrics	Navigation Suggestions	Splunk Dashboards	Entity Analysis Filtering
<input type="checkbox"/>	>	*nix	Edit ▾	0	4	0	0	2
<input type="checkbox"/>	>	Kubernetes Node	Edit ▾	0	4	0	0	3
<input type="checkbox"/>	>	Kubernetes Pod	Edit ▾	0	3	0	0	3
<input type="checkbox"/>	>	Unix/Linux Add-on	Edit ▾	10	4	0	0	2
<input type="checkbox"/>	>	VMware Cluster	Edit	0	4	0	0	3
<input type="checkbox"/>	>	VMware Datastore	Edit ▾	0	4	0	0	4
<input type="checkbox"/>	>	VMware ESXi Host	Edit ▾	0	4	0	0	5
<input type="checkbox"/>	>	VMware vCenter	Edit ▾	0	4	0	0	4
<input type="checkbox"/>	>	VMware VM	Edit ▾	0	4	0	0	4
<input type="checkbox"/>	>	Windows	Edit ▾	0	4	0	8	2



Entity Management

Create entity types to manage similar entities.

Entities **Entity Types**

Entity types group entities that have similar characteristics.

10 Entity Types

Bulk Action ▾

<input type="checkbox"/>	i	Title
<input type="checkbox"/>	>	*nix
<input type="checkbox"/>	>	Kubernetes Node
<input type="checkbox"/>	>	Kubernetes Pod
<input type="checkbox"/>	>	Unix/Linux Add-on
<input type="checkbox"/>	>	VMware Cluster
<input type="checkbox"/>	>	VMware Datastore
<input type="checkbox"/>	>	VMware ESXi Host
<input type="checkbox"/>	>	VMware vCenter
<input type="checkbox"/>	>	VMware VM
<input type="checkbox"/>	>	Windows

Edit an entity type



Create an entity type and define resources for it. Each resource enriches entity health pages for entities that belong to the entity type. After you create the entity type, start adding entities to it. You can add entities to an entity type during entity discovery or after you already brought an entity in.

[Learn more.](#)

Entity type information

Entity type name

Unix/Linux Add-on

Enter a name to reference the entity type.

Description (optional)

ta_nix type

A short description of your group of entities.

> Vital metrics (optional)

> Navigations (optional)

> Splunk dashboards (optional)

> Analysis data filters (optional)

Cancel

Save

Entity Management

Create entity types to manage similar entities.

Entities Entity Types

Entity types group entities that have similar characteristics.

10 Entity Types

Bulk Action ▾

<input type="checkbox"/>	i	Title
<input type="checkbox"/>	>	*nix
<input type="checkbox"/>	>	Kubernetes Node
<input type="checkbox"/>	>	Kubernetes Pod
<input type="checkbox"/>	>	Unix/Linux Add-on
<input type="checkbox"/>	>	VMware Cluster
<input type="checkbox"/>	>	VMware Datastore
<input type="checkbox"/>	>	VMware ESXi Host
<input type="checkbox"/>	>	VMware vCenter
<input type="checkbox"/>	>	VMware VM
<input type="checkbox"/>	>	Windows

Edit an entity type



Create an entity type and define resources for it. Each resource enriches entity health pages for entities that belong to the entity type. After you create the entity type, start adding entities to it. You can add entities to an entity type during entity discovery or after you already brought an entity in.

[Learn more.](#)

> Entity type information

✓ Vital metrics (optional)

> CPU Utilization



> Memory Utilization



> Disk Utilization



> Average Network Traffic



+ Add a Metric

Choose a Key Metric

CPU Utilization ▾

The key metric is displayed in the Infrastructure Overview. It must be a valid vital metric with entity matching fields defined.

> Navigations (optional)

Cancel

Save



IT Essentials Work

Create Entity Type

20 per page ▾

Entity Analysis Filtering

2

3

3

2

3

4

5

4

4

2

Entity Management

Create entity types to manage similar entities.

Entities Entity Types

Entity types group entities that have similar characteristics.

10 Entity Types

Bulk Action ▾

<input type="checkbox"/>	i	Title
<input type="checkbox"/>	>	*nix
<input type="checkbox"/>	>	Kubernetes Node
<input type="checkbox"/>	>	Kubernetes Pod
<input type="checkbox"/>	>	Unix/Linux Add-on
<input type="checkbox"/>	>	VMware Cluster
<input type="checkbox"/>	>	VMware Datastore
<input type="checkbox"/>	>	VMware ESXi Host
<input type="checkbox"/>	>	VMware vCenter
<input type="checkbox"/>	>	VMware VM
<input type="checkbox"/>	>	Windows

Edit an entity type



Create an entity type and define resources for it. Each resource enriches entity health pages for entities that belong to the entity type. After you create the entity type, start adding entities to it. You can add entities to an entity type during entity discovery or after you already brought an entity in.

[Learn more.](#)

> Entity type information

✓ Vital metrics (optional)

> CPU Utilization ✎ ✕

> Memory Utilization ✎ ✕

> Disk Utilization ✎ ✕

> Average Network Traffic ✎ ✕

+ Add a Metric

Choose a Key Metric

CPU Utilization ▼

The key metric is displayed in the Infrastructure Overview. It must be a valid vital metric with entity matching fields defined.

> Navigations (optional)

Cancel

Save



IT Essentials Work

Create Entity Type

20 per page ▾

Entity Analysis Filtering

2

3

3

2

3

4

5

4

4

2

Entity Management

Create entity types to manage similar entities.

Entities Entity Types

Entity types group entities that have similar characteristics.

10 Entity Types

Bulk Action ▾

<input type="checkbox"/>	i	Title
<input type="checkbox"/>	>	*nix
<input type="checkbox"/>	>	Kubernetes Node
<input type="checkbox"/>	>	Kubernetes Pod
<input type="checkbox"/>	>	Unix/Linux Add-on
<input type="checkbox"/>	>	VMware Cluster
<input type="checkbox"/>	>	VMware Datastore
<input type="checkbox"/>	>	VMware ESXi Host
<input type="checkbox"/>	>	VMware vCenter
<input type="checkbox"/>	>	VMware VM
<input type="checkbox"/>	>	Windows

Edit an entity type



Create an entity type and define resources for it. Each resource enriches entity health pages for entities that belong to the entity type. After you create the entity type, start adding entities to it. You can add entities to an entity type during entity discovery or after you already brought an entity in.

[Learn more.](#)

> Entity type information

✓ Vital metrics (optional)

> CPU Utilization



> Memory Utilization



> Disk Utilization



> Average Network Traffic



+ Add a Metric

Choose a Key Metric

CPU Utilization ▾

The key metric is displayed in the Infrastructure Overview. It must be a valid vital metric with entity matching fields defined.

> Navigations (optional)

Cancel

Save



IT Essentials Work

Create Entity Type

20 per page ▾

Entity Analysis Filtering

2

3

3

2

3

4

5

4

4

2

Entity Management

Create entity types to manage similar e

Entities Entity Types

Entity types group entities that have si

10 Entity Types

Bulk Action ▾

☐

Title

☐

> *nix

☐

> Kubernetes Node

☐

> Kubernetes Pod

☐

> Unix/Linux Add-on

☐

> VMware Cluster

☐

> VMware Datastore

☐

> VMware ESXi Host

☐

> VMware vCenter

☐

> VMware VM

☐

> Windows

Edit an entity type



The SPL search calculates the metric's value.

[Show more](#)

```
| mstats min(cpu_metric.pctIdle) as val WHERE  
`itsi_entity_type_ta_nix_metrics_indexes` AND
```

Run Search

0.00%

10 entities matched in last hour

Unit of Display

Percent (%) ▾

Entity matching fields

Entity matching fields match your metric to entities.

[Show more](#)

host

=

host ▾

[+ Add a matching field](#)

Alerting

The vital metric will fire an event each time it crosses
your established threshold. Monitor these events at[Alerts and Episodes](#)

Add Alert

> Memory Utilization



Cancel

Save

splunk>enterprise

Apps ▾

Administrator ▾

1 Messages ▾

Settings ▾

Activity ▾

Help ▾

Find



Service Analyzer ▾

Infrastructure C

Entity Management

Create entity types to manage similar e

Entities Entity Types

Entity types group entities that have si

10 Entity Types

Bulk Action ▾

<input type="checkbox"/>	i	Title
<input type="checkbox"/>	>	*nix
<input type="checkbox"/>	>	Kubernetes Node
<input type="checkbox"/>	>	Kubernetes Pod
<input type="checkbox"/>	>	Unix/Linux Add-on
<input type="checkbox"/>	>	VMware Cluster
<input type="checkbox"/>	>	VMware Datastore
<input type="checkbox"/>	>	VMware ESXi Host
<input type="checkbox"/>	>	VMware vCenter
<input type="checkbox"/>	>	VMware VM
<input type="checkbox"/>	>	Windows

Edit an entity type



host

= host ▾

[+ Add a matching field](#)

Alerting

The vital metric will fire an event each time it crosses your established threshold. Monitor these events at [Alerts and Episodes](#)

Evaluate this metric every 1 ▾ minutes.

This alert is ☒ enabled

After firing, this alert shouldn't fire for 0 minutes.

If metric is greater than ▾ 90 Critical

75 Warning

If metric is less than 75 it is Normal

[+ Add a threshold level](#)

Search Entity Dimensions

[Clear all](#)

host=foo,host=bar,os=centos will be translated to (host=foo OR host=bar) AND (os=centos)

0 of 0 entities match the selected dimension

[Remove Alert](#)

> Memory Utilization



Cancel

Save

Create Entity Type

20 per page ▾

Entity Analysis Filtering

2

3

3

2

3

4

5

4

4

2

splunk>enterprise

Apps ▾

Administrator ▾

1 Messages ▾

Settings ▾

Activity ▾

Help ▾

Find



Service Analyzer ▾

Infrastructure C

Entity Management

Create entity types to manage similar e

Entities Entity Types

Entity types group entities that have si

10 Entity Types

Bulk Action ▾

<input type="checkbox"/>	i	Title
<input type="checkbox"/>	>	*nix
<input type="checkbox"/>	>	Kubernetes Node
<input type="checkbox"/>	>	Kubernetes Pod
<input type="checkbox"/>	>	Unix/Linux Add-on
<input type="checkbox"/>	>	VMware Cluster
<input type="checkbox"/>	>	VMware Datastore
<input type="checkbox"/>	>	VMware ESXi Host
<input type="checkbox"/>	>	VMware vCenter
<input type="checkbox"/>	>	VMware VM
<input type="checkbox"/>	>	Windows

Edit an entity type



host

=

host ▾

[+ Add a matching field](#)

Alerting

The vital metric will fire an event each time it crosses your established threshold. Monitor these events at [Alerts and Episodes](#)

Evaluate this metric every

1 ▾

minutes.

This alert is ☒ enabled

After firing, this alert shouldn't fire for

0

minutes.

If metric is

greater than ▾

90

Critical

75

Warning

If metric is less than 75 it is Normal

[+ Add a threshold level](#)

Search Entity Dimensions

[Clear all](#)

host=foo,host=bar,os=centos will be translated to (host=foo OR host=bar) AND (os=centos)

0 of 0 entities match the selected dimension

[Remove Alert](#)

> Memory Utilization



Cancel

Save

Works for
Windows
and
Linux

Create Entity Type

20 per page ▾

Entity Analysis Filtering

2

3

3

2

3

4

5

4

4

2



Alerts Review

Investigate alerts caused by changes in vital metrics for each entity type. View individual entity details and notable events.

To group related alerts into episodes, upgrade to IT Service Intelligence (ITSI). [Learn more](#)

30 events

Last 60 minutes ▾

All Severities ▾

All Entity Types ▾

All Metrics ▾

Entity name

Refresh

Severity	Title	Involved Entity	Time	Description	Actions
▲ Critical	CPU Utilization metric alert for Unix/Linux Add-on entity type	ubuntu5	04/09/2022 06:20:05 PM	CPU Utilization current value is 29.59	View Details
▲ Critical	CPU Utilization metric alert for Unix/Linux Add-on entity type	ubuntu4	04/09/2022 06:20:05 PM	CPU Utilization current value is 25.25	View Details
▲ Critical	CPU Utilization metric alert for Unix/Linux Add-on entity type	ubuntu3	04/09/2022 06:20:05 PM	CPU Utilization current value is 52.00	View Details
▲ Critical	CPU Utilization metric alert for Unix/Linux Add-on entity type	ubuntu2	04/09/2022 06:20:05 PM	CPU Utilization current value is 26.00	View Details
▲ Critical	CPU Utilization metric alert for Unix/Linux Add-on entity type	ubuntu1	04/09/2022 06:20:05 PM	CPU Utilization current value is 34.65	View Details
▲ Warning	CPU Utilization metric alert for Unix/Linux Add-on entity type	redhat5	04/09/2022 06:20:05 PM	CPU Utilization current value is 22.00	View Details
▲ Critical	CPU Utilization metric alert for Unix/Linux Add-on entity type	redhat4	04/09/2022 06:20:05 PM	CPU Utilization current value is 34.65	View Details
▲ Critical	CPU Utilization metric alert for Unix/Linux Add-on entity type	redhat3	04/09/2022 06:20:05 PM	CPU Utilization current value is 42.00	View Details
▲ Warning	CPU Utilization metric alert for Unix/Linux Add-on entity type	redhat2	04/09/2022 06:20:05 PM	CPU Utilization current value is 25.00	View Details
● Normal	CPU Utilization metric alert for Unix/Linux Add-on entity type	redhat1	04/09/2022 06:20:05 PM	CPU Utilization current value is 12.00	View Details

Getting Data In

For ITW-Work / ITSI Infrastructure Monitoring



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

```
index = itsi_im_metrics
```

```
disabled = 0
```

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

```
index = itsi_im_metrics
```

```
disabled = 0
```

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

```
index = itsi_im_metrics
```

```
disabled = 0
```

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

```
index = itsi_im_metrics
```

```
disabled = 0
```

```
[script:///./bin/interfaces_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

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

