

Chapter 1: Application Logging

```
*** BASIC REND RENDERING org.jdesktop.wonderland.modules.orb.client.cell.OrbCellRenderer@76fe98
*** BASIC REND VISIBLE org.jdesktop.wonderland.modules.orb.client.cell.OrbCellRenderer@76fe9833
Jul 8, 2009 6:15:05 PM org.jdesktop.wonderland.modules.appbase.client.swing.WindowSwing request
WARNING: Focus request for embedded component rejected.
Jul 8, 2009 6:15:06 PM org.jdesktop.wonderland.modules.appbase.client.swing.WindowSwing$1 run
WARNING: Focus request for main canvas rejected.
Jul 8, 2009 6:15:19 PM com.sun.sgs.impl.io.CompleteMessageFilter processReceiveBuffer
WARNING: Exception in message disptach; dropping message
java.lang.NullPointerException
    at org.jdesktop.wonderland.modules.orb.client.cell.OrbMessageHandler.done(OrbMessageHand
    at org.jdesktop.wonderland.modules.orb.client.cell.OrbMessageHandler.processMessage(Orb
    at org.jdesktop.wonderland.modules.orb.client.cell.OrbMessageHandler$1.messageReceived(
    at org.jdesktop.wonderland.client.cell.ChannelComponent.deliverMessage(ChannelComponent
    at org.jdesktop.wonderland.client.cell.ChannelComponent.messageReceived(ChannelComponent
    at org.jdesktop.wonderland.client.cell.ChannelConnection.handleMessage(ChannelConnectio
    at org.jdesktop.wonderland.client.comms.BaseConnection.messageReceived(BaseConnection.j
    at org.jdesktop.wonderland.client.comms.WonderlandSessionImpl$ClientRecord.handleMessag
    at org.jdesktop.wonderland.client.comms.WonderlandSessionImpl.fireSessionMessageReceiv
    at org.jdesktop.wonderland.client.comms.WonderlandSessionImpl$WonderlandClientListene
    at com.sun.sgs.client.simple.SimpleClient$SimpleClientChannel.receivedMessage(SimpleCli
    at com.sun.sgs.client.simple.SimpleClient$SimpleClientConnectionListener.handleChannelMe
    at com.sun.sgs.client.simple.SimpleClient$SimpleClientConnectionListener.handleApplicat
    at com.sun.sgs.client.simple.SimpleClient$SimpleClientConnectionListener.receivedMessage
    at com.sun.sgs.impl.client.simple.SimpleClientConnection.bytesReceived(SimpleClientConn
    at com.sun.sgs.impl.io.SocketConnection.filteredMessageReceived(SocketConnection.java:14
    at com.sun.sgs.impl.io.CompleteMessageFilter.processReceiveBuffer(CompleteMessageFilter
    at com.sun.sgs.impl.io.CompleteMessageFilter.filterReceive(CompleteMessageFilter.java:16
    at com.sun.sgs.impl.io.SocketConnectionListener.messageReceived(SocketConnectionListene
    at org.apache.mina.common.support.AbstractIoFilterChain$TailFilter.messageReceived(Abstr
    at org.apache.mina.common.support.AbstractIoFilterChain.callNextMessageReceived(Abstrac
    at org.apache.mina.common.support.AbstractIoFilterChain.access$1100(AbstractIoFilterCha
    at org.apache.mina.common.support.AbstractIoFilterChain$EntryImpl$1.messageReceived(Abst
    at org.apache.mina.filter.executor.ExecutorFilter.processEvent(ExecutorFilter.java:247)
    at org.apache.mina.filter.executor.ExecutorFilter$ProcessEventsRunnable.run(ExecutorFilt
    at java.util.concurrent.ThreadPoolExecutor$Worker.runTask(ThreadPoolExecutor.java:885)
    at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:907)
    at java.lang.Thread.run(Thread.java:637)
Jul 8, 2009 6:15:19 PM org.jdesktop.wonderland.client.cell.CellCacheBasicImpl unloadCell
WARNING: -----> UNLOADING CELL 50
Jul 8, 2009 6:15:19 PM org.jdesktop.wonderland.client.cell.CellCacheBasicImpl setCellStatus
FINE: Set status of cell 50 to DISK
*** BASIC REND RENDERING org.jdesktop.wonderland.modules.orb.client.cell.OrbCellRenderer@5321d1
*** BASIC REND ACTIVE org.jdesktop.wonderland.modules.orb.client.cell.OrbCellRenderer@5321d174
*** BASIC REND INACTIVE org.jdesktop.wonderland.modules.orb.client.cell.OrbCellRenderer@5321d17
*** BASIC REND DISK org.jdesktop.wonderland.modules.orb.client.cell.OrbCellRenderer@5321d174
Jul 8, 2009 6:15:19 PM org.jdesktop.wonderland.client.cell.CellCacheBasicImpl unloadCell
WARNING: -----> UNLOADING ROOT CELL 50
```

```
17/10/2014 { [-]
16:46:30.000 bytes: 2877
clientip:
duration: 355526
host: www.ezix.org
message: - - [17/Oct/2014:16:46:30 +0200] "GET /project/wiki/AccessJSON HTTP/1.1"
200 2877
method: GET
pname: httpd
port: 443
protocol: HTTP/1.1
referer:
request: /project/wiki/AccessJSON
ssl: 1
sslcipher: ECDHE-RSA-AES128-GCM-SHA256
sslexport: false
sslkeysize: 128
sslprotocol: TLSv1.2
sslvirtualhost:
status: 200
tags: [ [+]
]
time: 2014-10-17T16:46:30+0200
urlpath: /project/wiki/AccessJSON
urlquery: null
user: -
useragent: Mozilla/5.0 (X11; Linux x86_64; rv:32.0) Gecko/20100101 Firefox/32.0
virtualhost: www.ezix.org
```

Show as raw text

host = host = www.ezix.org | source = /var/log/httpd/access.json | sourcetype = json-2 | ssl = 1

```
198.70.37.65, -, 3/31/96, 2:12:09, W3SVC, PAOLO, 198.70.37.65, 2814, 167, 3636, 200, 0, GET, /index.htm, -,
198.70.37.65, -, 3/31/96, 2:12:11, W3SVC, PAOLO, 198.70.37.65, 921, 214, 2360, 200, 0, GET, /Graphics/extra.jpg, -,
198.70.37.65, -, 3/31/96, 2:12:11, W3SVC, PAOLO, 198.70.37.65, 701, 215, 4108, 200, 0, GET, /graphics/events.gif, -,
198.70.37.65, -, 3/31/96, 2:12:11, W3SVC, PAOLO, 198.70.37.65, 871, 216, 2106, 200, 0, GET, /Graphics/WWWSTAT.JPG, -,
198.70.37.65, -, 3/31/96, 2:12:11, W3SVC, PAOLO, 198.70.37.65, 90, 215, 2411, 200, 0, GET, /graphics/public.jpg, -,
198.70.37.65, -, 3/31/96, 2:12:11, W3SVC, PAOLO, 198.70.37.65, 1222, 216, 9335, 200, 0, GET, /graphics/wintugi.jpg, -,
198.70.37.65, -, 3/31/96, 2:12:13, W3SVC, PAOLO, 198.70.37.65, 2113, 216, 3993, 200, 0, GET, /graphics/members.gif, -,
198.70.37.65, -, 3/31/96, 2:12:13, W3SVC, PAOLO, 198.70.37.65, 1742, 216, 2528, 200, 0, GET, /graphics/sponsor.jpg, -,
198.70.37.65, -, 3/31/96, 2:12:13, W3SVC, PAOLO, 198.70.37.65, 2594, 213, 3993, 200, 0, GET, /graphics/NTRC.gif, -,
198.70.37.65, -, 3/31/96, 2:12:13, W3SVC, PAOLO, 198.70.37.65, 2694, 213, 3138, 200, 0, GET, /graphics/join.jpg, -,
198.70.37.65, -, 3/31/96, 2:12:14, W3SVC, PAOLO, 198.70.37.65, 901, 215, 4049, 200, 0, GET, /graphics/roster.gif, -,
198.70.37.65, -, 3/31/96, 2:12:18, W3SVC, PAOLO, 198.70.37.65, 4797, 249, 72, 200, 0, GET, /index.htm, -,
```

sourcetype=iis

570 events (before 10/18/13 12:34:09.000 PM)

Events (570) Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

List Format 20 Per Page

Hide Fields All Fields

Selected Fields

- a c_ip 3
- # cs_bytes 100+
- a cs_Cookie 3
- a cs_host 5
- a cs_method 9
- a cs_uri_query 34
- a cs_uri_stem 100+
- a cs_User_Agent 5
- a cs_version 2
- a host 1
- a s_ip 2
- # s_port 1
- # sc_bytes 12
- # sc_status 5
- # sc_substatus 1
- # sc_win32_status 3
- a source 9
- a sourcetype 1

Interesting Fields

- a date 7
- # date_hour 6
- # date_mday 8
- # date_minute 11

i	Time	Event
▶	10/18/13 11:35:33.000 AM	2013-10-18 18:35:33 ::1 GET /favicon.ico - 80 - ::1 HTTP/1.1 Mozilla/5.0+(compatible; splunkweb_csrftoken_8000=3571848927425522258 localhost 404 0 2 5375 254 46
▶	10/18/13 11:35:33.000 AM	2013-10-18 18:35:33 ::1 GET /welcome.png - 80 - ::1 HTTP/1.1 Mozilla/5.0+(compatible; splunkweb_csrftoken_8000=3571848927425522258 localhost 200 0 0 185196 353 31

sc_status

5 Values, 100% of events Selected Yes No

Reports

Average over time	Maximum value over time	Minimum value over time
Top values	Top values by time	Rare values

Events with this field

Avg: 378.231579 Min: 200 Max: 501 Std Dev: 68.8561

Values	Count	%
404	480	84.21%
200	73	12.807%
405	13	2.281%
501	3	0.526%
304	1	0.175%

Version 1 of RegExr is now deprecated. We will continue to keep it on-line for the foreseeable future. We encourage you to use the new RegExr. Any new patterns you save here, will not be visible in RegExr v2.

Match Replace

global ignoreCase extended dotall multiline

07:02:47 PM all 91.84 2.55 5.61 0.00 0.00 0.00

07:02:49 PM all 29.74 49.74 7.69 0.00 0.00 12.82

07:02:51 PM all 0.50 0.00 1.51 0.00 0.00 97.99

07:02:53 PM all 5.05 0.00 15.15 0.00 0.00 79.80

07:02:55 PM all 19.50 0.00 34.50 4.00 0.00 42.00

07:02:57 PM all 8.59 0.00 10.10 0.00 0.00 81.31

File	Edit	Format	View	Help			
Time stamp	CPU	%user	%nice	%system	%iowait	%steal	%idle

New Search Save As ▾ Close

index=main | convert timeformat="%H:%M:%S" ctime(_time) as timestamp | table timestamp cpu pctUser pctNice
pctSys pctIOWait pctSteal pctIdle All time ▾ 🔍

✓ 1 event (before 1/16/16 2:06:54.000 PM) Job ▾ || ■ ↶ ↷ ⚙️ Smart Mode ▾

Events Patterns Statistics (1) Visualization

20 Per Page ▾ Format ▾ Preview ▾

timestamp ▾	cpu ▾	pctUser ▾	pctNice ▾	pctSys ▾	pctIOWait ▾	pctSteal ▾	pctIdle ▾
07:02:47	all	91.84	2.55	5.61	0	0	0

Time	Thread	Product	Category	EventID	Level	Correlation	Message
01/29/2011 14:...	0x2A50	Share...	Monito...	b4ly	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Leaving Monitored Scope (Creating Web BI). Executi
01/29/2011 14:...	0x2A50	Share...	General	85m6	Medium	a6ea7f59-7b54-46f8-9e68-5be81172704c	Applying web template 'BICenterSite#0' on web url htt
01/29/2011 14:...	0x2A50	Share...	General	85m7	Medium	a6ea7f59-7b54-46f8-9e68-5be81172704c	Actual web template to apply to Uri 'http://atide6510-
01/29/2011 14:...	0x2A50	Share...	General	72h7	Medium	a6ea7f59-7b54-46f8-9e68-5be81172704c	Applying template "BICenterSite#0" to web at URL "h
01/29/2011 14:...	0x2A50	Share...	General	88jb	Medium	a6ea7f59-7b54-46f8-9e68-5be81172704c	Feature Activation: Activating Feature 'Publishing' (ID:
01/29/2011 14:...	0x2A50	Share...	General	75fb	Medium	a6ea7f59-7b54-46f8-9e68-5be81172704c	Calling 'FeatureActivated' method of SPFeatureReceiv
01/29/2011 14:...	0x2A50	Web ...	Publis...	1ght	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Publishing Feature activation event handled.
01/29/2011 14:...	0x2A50	Web ...	Publis...	75ot	Unexpec...	a6ea7f59-7b54-46f8-9e68-5be81172704c	Publishing Feature activation failed. Exception: System
01/29/2011 14:...	0x2A50	Share...	Featur...	88jm	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Feature receiver assembly 'Microsoft.SharePoint.Publi
01/29/2011 14:...	0x2A50	Share...	General	72by	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Feature Activation: Threw an exception, attempting to
01/29/2011 14:...	0x2A50	Share...	Monito...	b4ly	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Leaving Monitored Scope (Feature Activation: Activat
01/29/2011 14:...	0x2A50	Share...	General	8i36	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Failed to activate site-scoped features for template 'BI
01/29/2011 14:...	0x2A50	Share...	Fields	bn3x	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Failed to activate web features when provisioning site
01/29/2011 14:...	0x2A50	Share...	General	72h9	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Failed to apply template "BICenterSite#0" to web at U
01/29/2011 14:...	0x2A50	Share...	General	72k2	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Failed to apply template "BICenterSite#0" to web at U
01/29/2011 14:...	0x2A50	Share...	General	8e1d	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Deleting the web at http://atide6510-as/BI .
01/29/2011 14:...	0x2A50	Share...	Monito...	b4ly	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Leaving Monitored Scope (Render WebPart AddGalle
01/29/2011 14:...	0x2A50	Share...	Monito...	b4ly	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Leaving Monitored Scope (Render WebPart Zone g_
01/29/2011 14:...	0x2A50	Share...	Monito...	b4lv	Medium	a6ea7f59-7b54-46f8-9e68-5be81172704c	Leaving Monitored Scope (Request http://atic
Time	Thread	Product	Category	EventID	Level	Correlation	Message
01/29/2011 14:...	0x2A50	Share...	Monito...	b4ly	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Leaving Monitored Scope (Creating Web BI). Executi
01/29/2011 14:...	0x2A50	Share...	General	85m6	Medium	a6ea7f59-7b54-46f8-9e68-5be81172704c	Applying web template 'BICenterSite#0' on web url htt
01/29/2011 14:...	0x2A50	Share...	General	85m7	Medium	a6ea7f59-7b54-46f8-9e68-5be81172704c	Actual web template to apply to Uri 'http://atide6510-
01/29/2011 14:...	0x2A50	Share...	General	72h7	Medium	a6ea7f59-7b54-46f8-9e68-5be81172704c	Applying template "BICenterSite#0" to web at URL "h
01/29/2011 14:...	0x2A50	Share...	General	88jb	Medium	a6ea7f59-7b54-46f8-9e68-5be81172704c	Feature Activation: Activating Feature 'Publishing' (ID:
01/29/2011 14:...	0x2A50	Share...	General	75fb	Medium	a6ea7f59-7b54-46f8-9e68-5be81172704c	Calling 'FeatureActivated' method of SPFeatureReceiv
01/29/2011 14:...	0x2A50	Web ...	Publis...	1ght	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Publishing Feature activation event handled.
01/29/2011 14:...	0x2A50	Web ...	Publis...	75ot	Unexpec...	a6ea7f59-7b54-46f8-9e68-5be81172704c	Publishing Feature activation failed. Exception: System
01/29/2011 14:...	0x2A50	Share...	Featur...	88jm	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Feature receiver assembly 'Microsoft.SharePoint.Publi
01/29/2011 14:...	0x2A50	Share...	General	72by	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Feature Activation: Threw an exception, attempting to
01/29/2011 14:...	0x2A50	Share...	Monito...	b4ly	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Leaving Monitored Scope (Feature Activation: Activat
01/29/2011 14:...	0x2A50	Share...	General	8i36	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Failed to activate site-scoped features for template 'BI
01/29/2011 14:...	0x2A50	Share...	Fields	bn3x	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Failed to activate web features when provisioning site
01/29/2011 14:...	0x2A50	Share...	General	72h9	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Failed to apply template "BICenterSite#0" to web at U
01/29/2011 14:...	0x2A50	Share...	General	72k2	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Failed to apply template "BICenterSite#0" to web at U
01/29/2011 14:...	0x2A50	Share...	General	8e1d	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Deleting the web at http://atide6510-as/BI .
01/29/2011 14:...	0x2A50	Share...	Monito...	b4ly	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Leaving Monitored Scope (Render WebPart AddGalle
01/29/2011 14:...	0x2A50	Share...	Monito...	b4ly	High	a6ea7f59-7b54-46f8-9e68-5be81172704c	Leaving Monitored Scope (Render WebPart Zone g_
01/29/2011 14:...	0x2A50	Share...	Monito...	b4lv	Medium	a6ea7f59-7b54-46f8-9e68-5be81172704c	Leaving Monitored Scope (Request IPOST:http://atic

```

weblogic.application.utils.StateMachineDriver nextState(StateMachineDriver.java:26)
>
####<Dec 29, 2006 2:14:24 PM IST> <Notice> <Log Management> <svoidyan02> <xbusServer>
<[ACTIVE] ExecuteThread: '0' for queue: 'weblogic.kernel.Default (self-tuning)''> <<WLS
kernel>> <> <> <1167381864275> <BEA-170027> <The server initialized the domain log
broadcaster successfully. Log messages will now be broadcasted to the domain log.>
####<Dec 29, 2006 2:14:24 PM IST> <Notice> <WebLogicServer> <svoidyan02> <xbusServer> <Main
Thread> <<WLS kernel>> <> <> <1167381864976> <BEA-000365> <Server state changed to ADMIN>
####<Dec 29, 2006 2:14:24 PM IST> <Notice> <WebLogicServer> <svoidyan02> <xbusServer> <Main
Thread> <<WLS kernel>> <> <> <1167381864996> <BEA-000365> <Server state changed to RESUMING>
####<Dec 29, 2006 2:14:28 PM IST> <Notice> <Security> <svoidyan02> <xbusServer> <[STANDBY]
ExecuteThread: '5' for queue: 'weblogic.kernel.Default (self-tuning)''> <<WLS kernel>> <> <>
<1167381868541> <BEA-090171> <Loading the identity certificate and private key stored under
the alias DemoIdentity from the jks keystore file
C:\bea2613a\WEBLOG~1\server\lib\DemoIdentity.jks.>
####<Dec 29, 2006 2:14:29 PM IST> <Notice> <Security> <svoidyan02> <xbusServer> <[STANDBY]
ExecuteThread: '5' for queue: 'weblogic.kernel.Default (self-tuning)''> <<WLS kernel>> <> <>
<1167381869643> <BEA-090169> <Loading trusted certificates from the jks keystore file
C:\bea2613a\WEBLOG~1\server\lib\DemoTrust.jks.>
####<Dec 29, 2006 2:14:29 PM IST> <Notice> <Security> <svoidyan02> <xbusServer> <[STANDBY]
ExecuteThread: '5' for queue: 'weblogic.kernel.Default (self-tuning)''> <<WLS kernel>> <> <>
<1167381869713> <BEA-090169> <Loading trusted certificates from the jks keystore file
C:\bea2613a\JROCKI~1\jre\lib\security\cacerts.>
####<Dec 29, 2006 2:15:32 PM IST> <Warning> <Server> <svoidyan02> <xbusServer>
<DynamicSSLListenThread[DefaultSecure[1]]> <<WLS kernel>> <> <> <1167381932743> <BEA-002611>
<Hostname "svoidyan02.apac.bea.com", maps to multiple IP addresses: 192.168.1.5,
172.22.56.120>
####<Dec 29, 2006 2:15:32 PM IST> <Notice> <Server> <svoidyan02> <xbusServer> <[STANDBY]
ExecuteThread: '5' for queue: 'weblogic.kernel.Default (self-tuning)''> <<WLS kernel>> <> <>
<1167381932753> <BEA-002613> <Channel "Default[2]" is now listening on 127.0.0.1:7021 for

```

```

01/08/2016 07:28:54.100 - 1 home 1 New Home Avenue2 dentist
01/08/2016 07:28:54.430 - 1 DDS Avenue3 1a 3 LA shack3 restaurant 3
Hole in the wall 7 dev house
kelld 7 NO fowlerville MPPN November 14
November 22 2015 - Inst 8876.33_v2 filled for Caption at fox 2
01/08/2016 07:29:54.010 - 7 Hacker way dist 55v12bb CANCELLED X11253581 Order From 223
APPT 8874698225
01/08/2016 07:28:54.100 - 1 home 1 New Home Avenue2 dentist
01/08/2016 07:28:54.430 - 1 DDS Avenue3 1a 3 LA shack3 restaurant 3
Hole in the wall 7 dev house
kelld 7 NO fowlerville MPPN November 14
November 22 2015 - Inst 8876.33_v2 filled for Caption at fox 2
01/08/2016 07:29:54.010 - 7 Hacker way dist 55v12bb CANCELLED X11253581 order From 223
APPT 8874698225

```

Add Data Next >

Select Source
Set Source Type
Input Settings
Review
Done

Local Event Logs
Collect event logs from this machine.

Remote Event Logs
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.

Files & Directories
Upload a file, index a local file, or monitor an entire directory. >

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure Splunk to listen on a network port.

Local Performance Monitoring
Collect performance data from this machine.

Remote Performance Monitoring
Collect performance and event information from remote hosts. Requires domain credentials.

Registry monitoring
Have Splunk index the local Windows Registry, and monitor it for changes.

Active Directory monitoring
Index and monitor Active Directory.

Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. Splunk monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. [Learn More](#)

File or Directory?

On Windows: c:\apache\apache.error.log or \hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

Whitelist?

Blacklist?

FAQ

- > What kinds of files can Splunk index?
- > I can't access the file that I want to index. Why?
- > How do I get remote data onto my Splunk instance?
- > Can I monitor changes to files in addition to their content?
- > What is a source type?
- > How do I specify a whitelist or blacklist for a directory?

Add Data

Select Source Set Source Type Input Settings Review Done

< Next >

Set Source Type

This page lets you see how Splunk sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: C:\Users\TRAVIS\Downloads\kv_ht.txt

Source type: Recommended Settings

Event Breaks

Break Type:

> Timestamp

> Advanced

	Time	Event
1	1/8/16 7:28:54.100 AM	01/08/2016 07:28:54.100 - 1home1 New Home Avenue 2dentist
2	1/8/16 7:28:54.430 AM	01/08/2016 07:28:54.430 - 1 DDS Avenue 3la3 LA shack 3restaurant3 Hole in the wall 7dev house Show all 7 lines
3	1/8/16 7:29:54.010 AM	01/08/2016 07:29:54.010 - 7 Hacker way dist 55v12bb CANCELLED X11253581 Order From 223 APPT 8874698225

Save Source Type

Name

Description

Category

App

New Search

source="C:\\Users\\TRAVIS\\Downloads\\kv_ht.txt" host="DT-TMARLETTE" sourcetype="myUnstructured"]

✓ 3 events (before 1/16/16 3:30:00.000 PM)

Events (3) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection x Deselect



List Format 20 Per Page

< Hide Fields

All Fields

Selected Fields

a host 1

a source 1

a sourcetype 1

Interesting Fields

date_hour 1

date_mday 1

date_minute 2

a date_month 1

date_second 1

a date_wday 1

date_year 1

a date_zone 1

a index 1

i	Time	Event
>	1/8/16 7:29:54.010 AM	01/08/2016 07:29:54.010 - 7 Hacker way dist 55v12bb CANCELLED X11253581 Order From 223 APPT 8874698225 host = DT-TMARLETTE ; source = C:\\Users\\TRAVIS\\Downloads\\kv_ht.txt ; sourcetype = myUnstructured
>	1/8/16 7:28:54.430 AM	01/08/2016 07:28:54.430 - 1 DDS Avenue 31a3 LA shack 3restaurant3 Hole in the wall 7dev house Show all 7 lines host = DT-TMARLETTE ; source = C:\\Users\\TRAVIS\\Downloads\\kv_ht.txt ; sourcetype = myUnstructured
>	1/8/16 7:28:54.100 AM	01/08/2016 07:28:54.100 - 1home1 New Home Avenue 2dentist host = DT-TMARLETTE ; source = C:\\Users\\TRAVIS\\Downloads\\kv_ht.txt ; sourcetype = myUnstructured

Computer > MEDIA1 (X:) > Program Files > etc > apps > search > local

Search local

Organize Include in library Share with Burn New folder

Name	Date modified	Type	Size
inputs	1/16/2016 3:26 PM	CONF File	1 KB
props	1/16/2016 3:29 PM	CONF File	1 KB

props - WordPad

```
[myUnstructured]
DATETIME_CONFIG =
NO_BINARY_CHECK = true
category = Custom
pulldown_type = true
```

100%

Distribute Configuration Bundle

Distribute the configuration bundle from the master to the peers. [Learn More](#) ↗

[← Back to Master Node](#)

[Distribute Configuration Bundle](#)

🔍 New Search

sourcetype="web_frontend"

✓ 3 events (before 1/16/16 3:54:51.000 PM)

Events (3) Patterns Statistics Visualization

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



List ▾ ↗ Format ▾ 20 Per Page ▾

← Hide Fields ☰ All Fields		i	Time	Event
Selected Fields a host 1 a sourcetype 1		>	1/8/16 7:29:54.010 AM	01/08/2016 07:29:54.010 - 7 Hacker way dist 55v12bb CANCELLED X11253581 Order From 223 APPT 8874698225 host = lpioud554 sourcetype = web_frontend
Interesting Fields # date_hour 1 # date_mday 1 # date_minute 2 a date_month 1 # date_second 1 a date_wday 1 # date_year 1 a date_zone 1 a index 1 # linecount 3 a punct 3 a source 1		>	1/8/16 7:28:54.430 AM	01/08/2016 07:28:54.430 - 1 DDS Avenue 31a3 LA shack 3restaurant3 Hole in the wall 7dev house Show all 7 lines host = lpioud554 sourcetype = web_frontend
		>	1/8/16 7:28:54.100 AM	01/08/2016 07:28:54.100 - 1home1 New Home Avenue 2dentist host = lpioud554 sourcetype = web_frontend

Chapter 2: Data Inputs


hostname	environment	cluster	serverType	procCount	sockets	cores	uptime	memory	os	osVersion	kernelVersion	osManufacturer	SN	cpuSpeed	cpuType	diskCount	model	manufacturer	installDate
Big Data			Physical	32	2	8	53 days, 18:03,	252	Linux	Red Hat Enterprise Linux Server release 6.6 (Santiago)	2.6.32-504.23.4.el6.x86_64	Red Hat		2401.000	Intel(R) Xeon(R) CPU ES-2665 0 @ 2.40GHz	1	UCSC-C240-M3S	Cisco Systems Inc	Sep 27 2013
Big Data			Physical	32	2	8	95 days, 1:11,	126	Linux	Red Hat Enterprise Linux Server release 6.6 (Santiago)	2.6.32-504.23.4.el6.x86_64	Red Hat		2400.054	Intel(R) Xeon(R) CPU ES-2665 0 @ 2.40GHz	24	UCSC-C240-M3S	Cisco Systems Inc	Sep 29 2014
Big Data			Physical	32	2	8	95 days, 3:23,	126	Linux	Red Hat Enterprise Linux Server release 6.6 (Santiago)	2.6.32-504.23.4.el6.x86_64	Red Hat		2400.264	Intel(R) Xeon(R) CPU ES-2665 0 @ 2.40GHz	24	UCSC-C240-M3S	Cisco Systems Inc	Jun 13 2014
Big Data			Physical	32	2	8	97 days, 1:24,	126	Linux	Red Hat Enterprise Linux Server release 6.6 (Santiago)	2.6.32-504.23.4.el6.x86_64	Red Hat		2400.069	Intel(R) Xeon(R) CPU ES-2665 0 @ 2.40GHz	24	UCSC-C240-M3S	Cisco Systems Inc	Oct 2 2014
Big Data			Physical	32	2	8	53 days, 20:57,	126	Linux	Red Hat Enterprise Linux Server release 6.6 (Santiago)	2.6.32-504.23.4.el6.x86_64	Red Hat		2401.000	Intel(R) Xeon(R)	1	UCSC-C240-M3S	Cisco Systems Inc	Jul 19 2013

EMC XtremIO Add-on for Splunk Enterprise


This technology add-on collects data from EMC XtremIO cluster to be used by the EMC XtremIO App for Splunk Enterprise.

Content: Add-on | **Compatibility:** 6.2 | **Platform:** Platform Independent | **Categories:** IT Operations Management | **Author:** Crest Data Systems | **Downloads:** 85 | **Released:** Jul 31, 2015 | **Updated:** Jul 31, 2015

Administrator Messages Settings Activity Help Find



Add Data



Distributed Management Console

KNOWLEDGE

- Searches, reports, and alerts
- Data models
- Event types
- Tags
- Fields
- Lookups
- User interface
- Alert actions
- Advanced search
- All configurations

DATA

- Data inputs**
- Forwarding and receiving
- Indexes
- Report acceleration summaries
- Source types

DISTRIBUTED ENVIRONMENT

- Indexer clustering
- Forwarder management
- Distributed search

SYSTEM

- Server settings
- Server controls
- Licensing

USERS AND AUTHENTICATION

- Access controls

Local inputs

Set up data inputs from files and directories, network ports, and scripted inputs. If you want to

- Type**

- Files & directories**
Index a local file or monitor an entire directory.

- TCP**
Listen on a TCP port for incoming data, e.g. syslog.

- UDP**
Listen on a UDP port for incoming data, e.g. syslog.

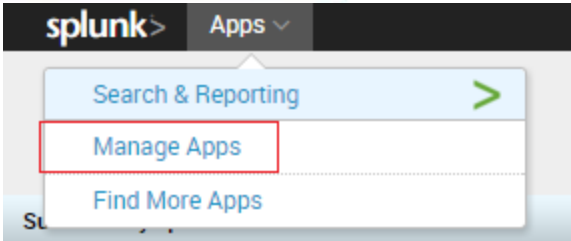
- Scripts**
Run custom scripts to collect or generate more data.

- Automation Testing | Synthetic Transactions**
Perform web automation and synthetic transactions on web pages.

- Splunk Add-on for Cisco UCS**
Enable Cisco UCS inputs

- Splunk Add-on for ServiceNow**
Enable ServiceNow database table inputs

- XtremIO REST Inputs**
REST API input for polling data from EMC XtremIO



Apps

[Browse more apps](#) | [Install app from file](#) | [Create app](#)

Showing 1-21 of 21 items

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SQL config	SQL config		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions	Disabled Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions	Disabled Enable	
Splunk Add-on for Cisco UCS	Splunk_TA_cisco-ucs	2.0.0	Yes	Yes	Global Permissions	Enabled Disable	Launch app Edit properties View objects View details on SplunkApps
Splunk Add-on for *Nix	Splunk_TA_ipc2HeavyForwarder	5.1.0	Yes	Yes	Global Permissions	Enabled Disable	Launch app Edit properties View objects View details on SplunkApps
Splunk Add-on for ServiceNow	Splunk_TA_snow	2.0.0	Yes	No	Global Permissions	Enabled Disable	Set up Edit properties View objects View details on SplunkApps
EMC XtremIO Add-on for Splunk Enterprise	TA-EMC-XtremIO	1.0	Yes	No	Global Permissions	Enabled Disable	Set up Edit properties View objects View details on SplunkApps

XtremIO Configuration

Host

Username

Password

Confirm password

Cancel

Save

splunk> Apps ▾

Data inputs

Local inputs

Set up data inputs from files and directories, network ports, and scripted inputs. If you want to

Type

Files & directories

Index a local file or monitor an entire directory.

TCP

Listen on a TCP port for incoming data, e.g. syslog.

UDP

Listen on a UDP port for incoming data, e.g. syslog.

Scripts

Run custom scripts to collect or generate more data.

Automation Testing | Synthetic Transactions

Perform web automation and synthetic transactions on web pages.

Splunk Add-on for Cisco UCS

Enable Cisco UCS inputs

Splunk Add-on for ServiceNow

Enable ServiceNow database table inputs

XtremIO REST Inputs

REST API input for polling data from EMC XtremIO

XtremIO REST Inputs


Settings > Data inputs > XtremIO REST Inputs

New


Showing 1-8 of 8 items

REST input name	Endpoint URL	Polling interval	Source type
imdpzio1gso:bricks	https://imdpzio1gso/api/json/types/bricks/\$get_ids\$	120	emc:xtremio:rest
imdpzio1gso:clusters	https://imdpzio1gso/api/json/types/clusters/\$get_ids\$	120	emc:xtremio:rest
imdpzio1gso:events	https://imdpzio1gso/api/json/types/events	120	emc:xtremio:rest
imdpzio1gso:initiators	https://imdpzio1gso/api/json/types/initiators/\$get_ids\$	120	emc:xtremio:rest
imdpzio1gso:snapshots	https://imdpzio1gso/api/json/types/snapshots/\$get_ids\$	120	emc:xtremio:rest
imdpzio1gso:storage-controllers	https://imdpzio1gso/api/json/types/storage-controllers/\$get_ids\$	120	emc:xtremio:rest
imdpzio1gso:targets	https://imdpzio1gso/api/json/types/targets/\$get_ids\$	120	emc:xtremio:rest
imdpzio1gso:volumes	https://imdpzio1gso/api/json/types/volumes/\$get_ids\$	120	emc:xtremio:rest

he
rise.



Add Data



Distributed Management Console

KNOWLEDGE
Searches, reports, and alerts
Data models
Event types
Tags
Fields
Lookups
User interface
Alert actions
Advanced search
All configurations

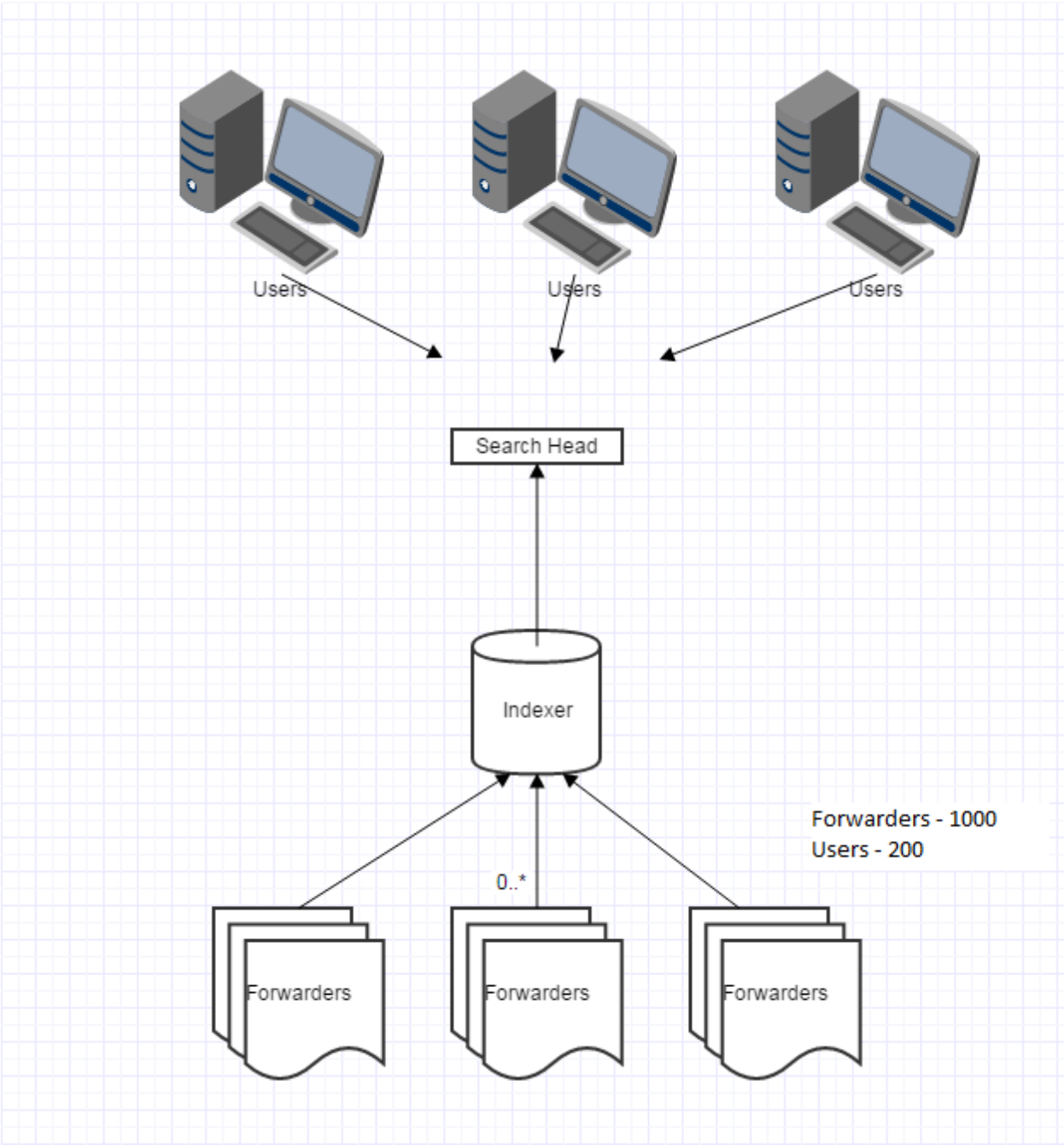
DATA
Data inputs
Forwarding and receiving
Indexes
Report acceleration summaries
Source types

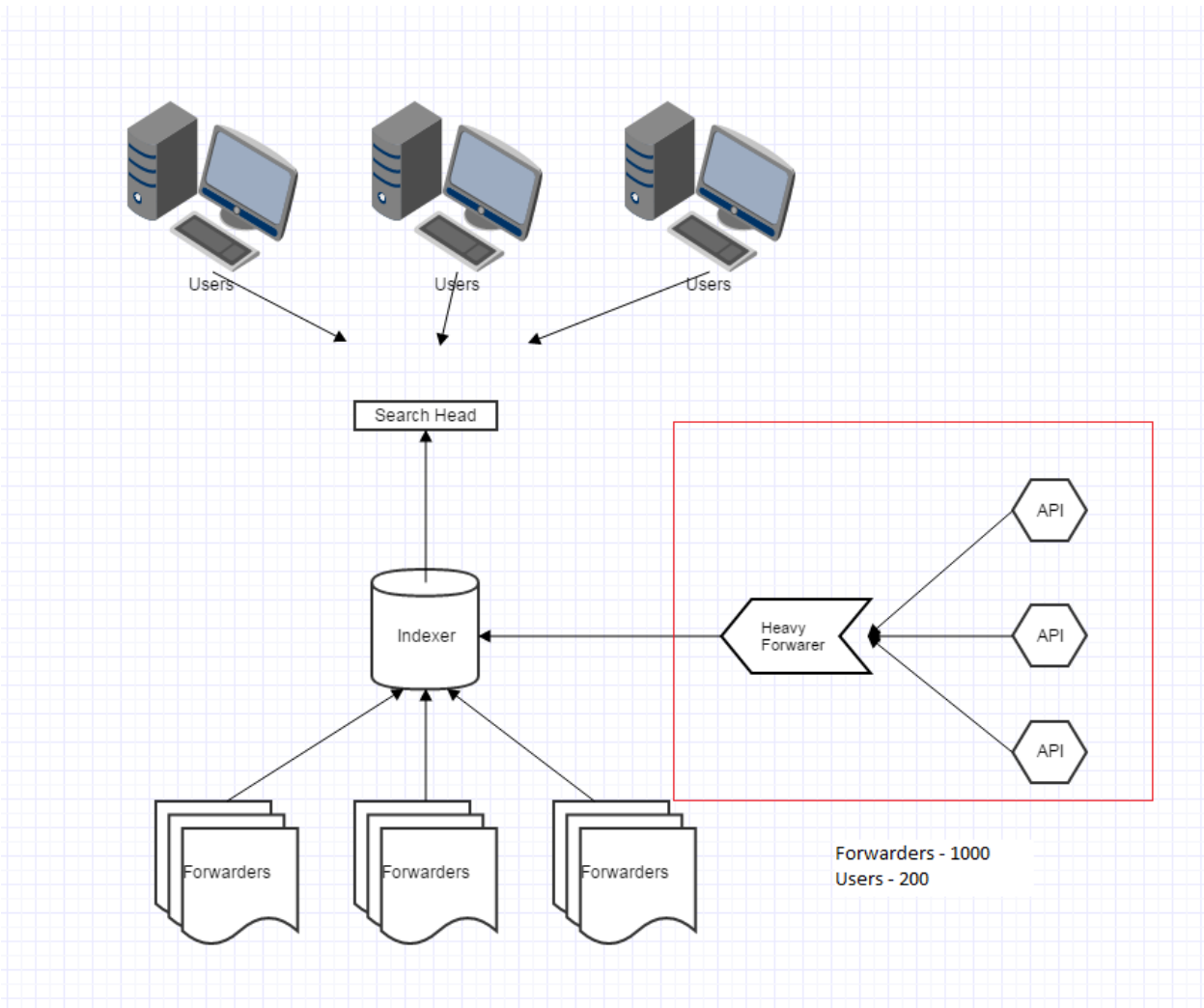
DISTRIBUTED ENVIRONMENT
Indexer clustering
Forwarder management
Distributed search

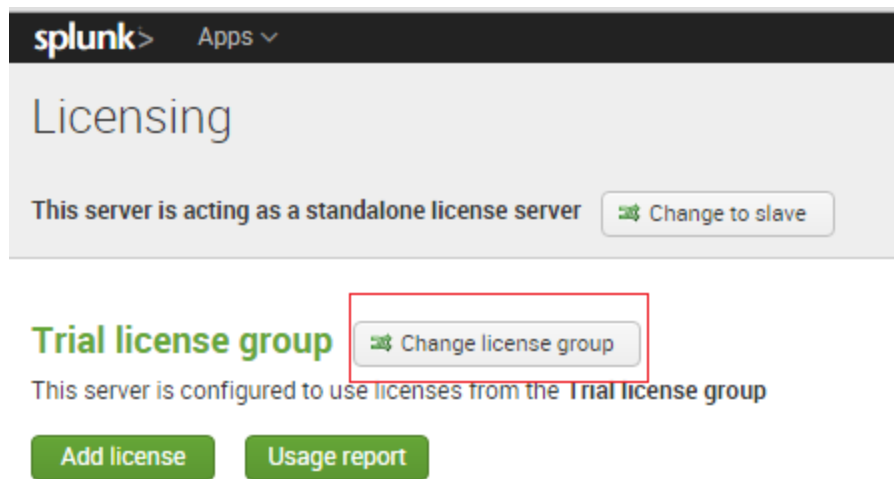
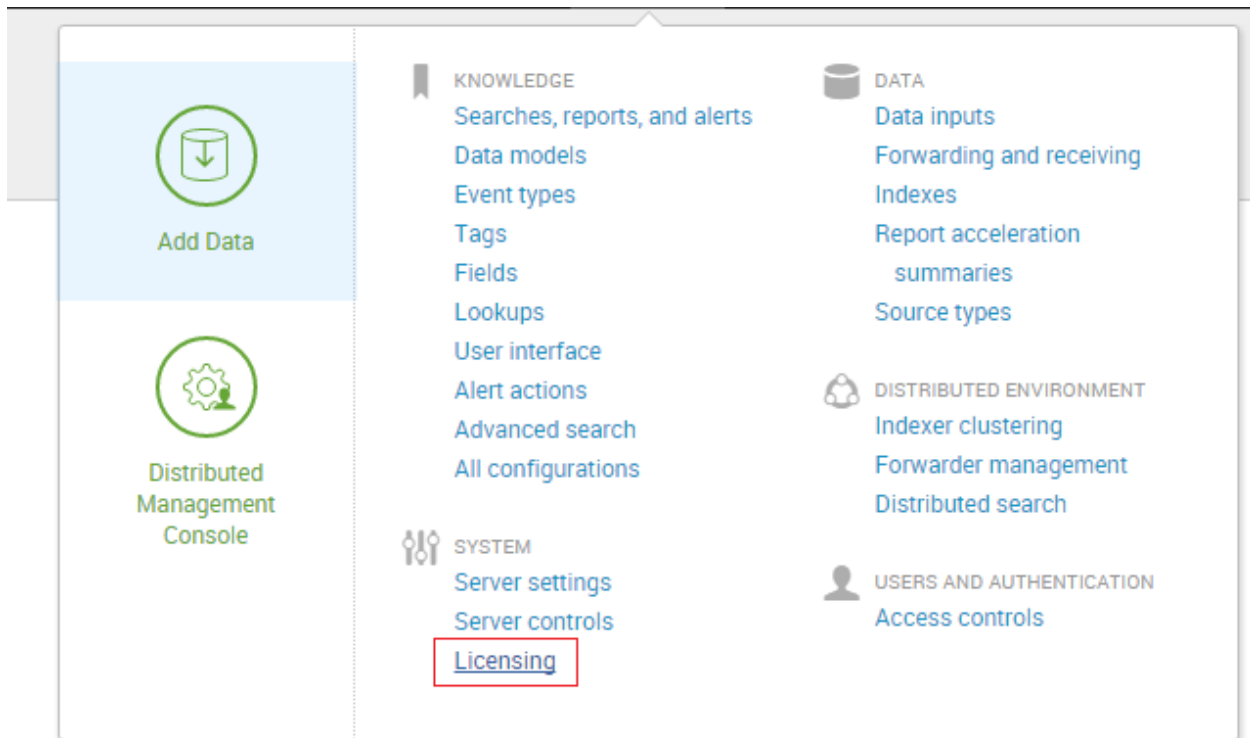
SYSTEM
Server settings
Server controls
Licensing

USERS AND AUTHENTICATION
Access controls

Chapter 3: Data Scrubbing







Change license group

The type of license group determines what sorts of licenses can be used in the pools on this license server.

[Learn more](#)

Enterprise license

This license adds support for multi-user and distributed deployments, alerting, role-based security, single sign-on, scheduled PDF delivery, and unlimited data volumes.

There are no valid Splunk *Enterprise licenses* installed. You will be prompted to install a license if you choose this option.

Forwarder license

Use this group when configuring Splunk as a forwarder. [Learn more](#)

Free license

Use this group when you are running Splunk Free. This license has a 500MB/day daily indexing volume.

[Learn more](#)

Enterprise Trial license

This is your included download trial. **IMPORTANT:** If you switch to another license, you cannot return to the Trial. You must install an Enterprise license or switch to Splunk Free.

Cancel

Save

Forwarding and receiving

Forward data

Set up forwarding between two or more Splunk instances.

[Forwarding defaults](#)

[Configure forwarding](#)

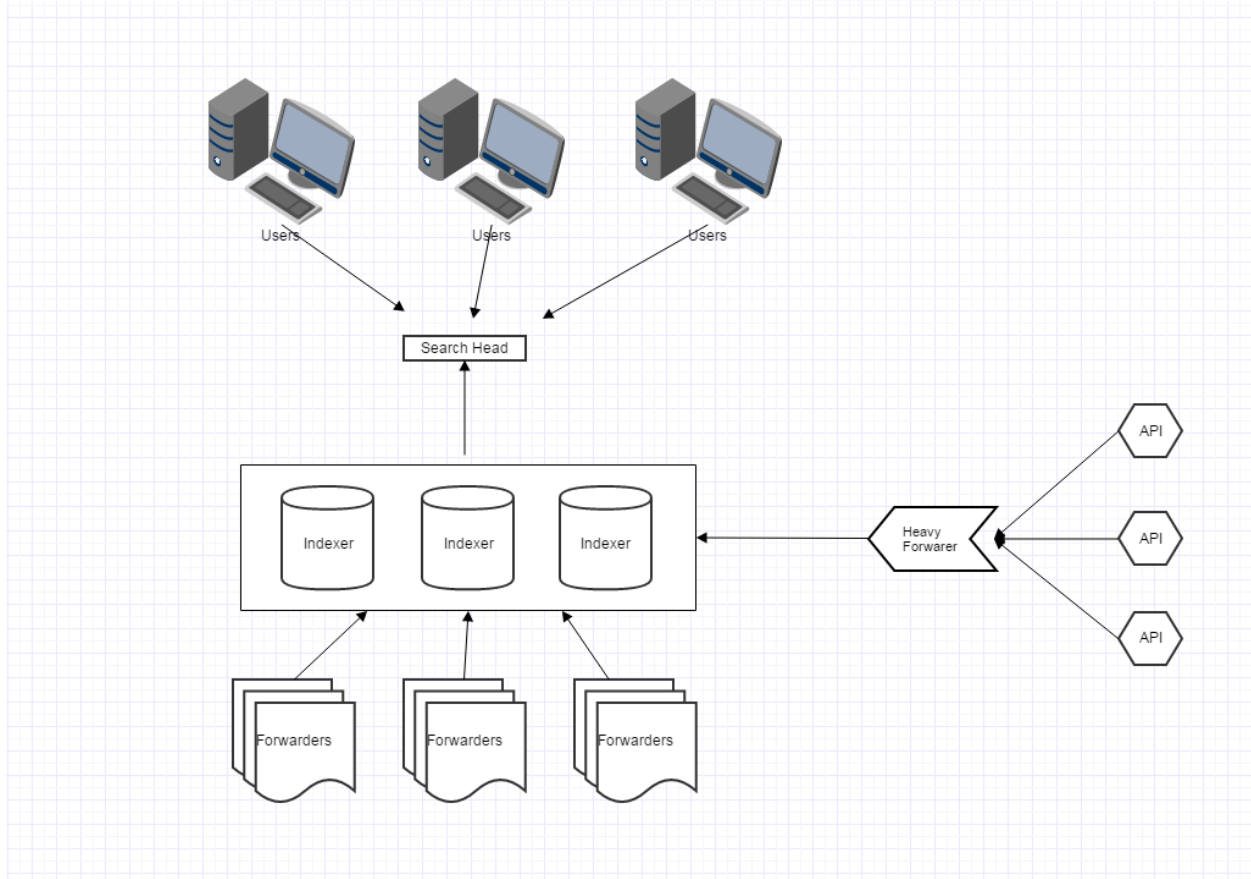
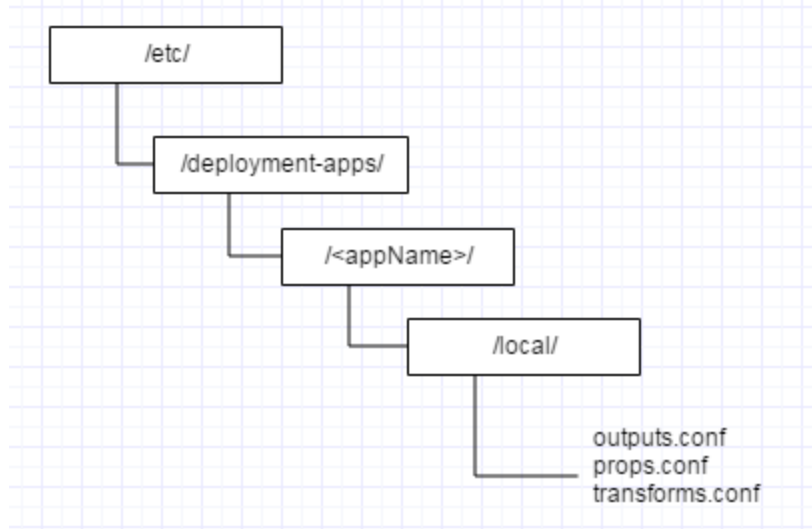
Store a local copy of forwarded events?

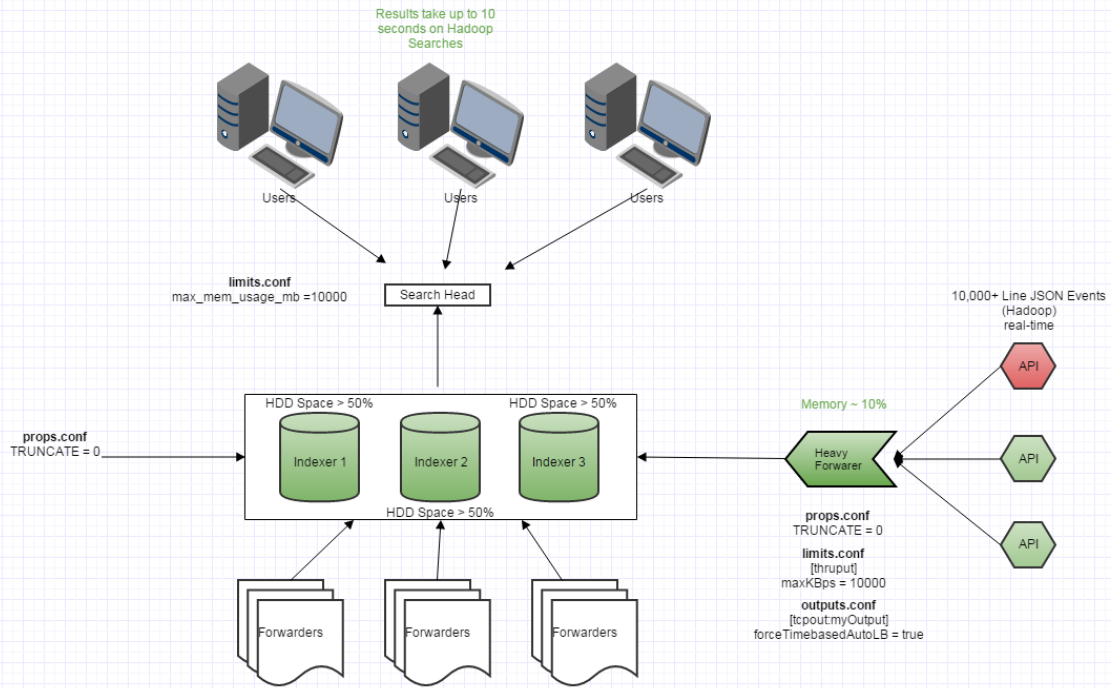
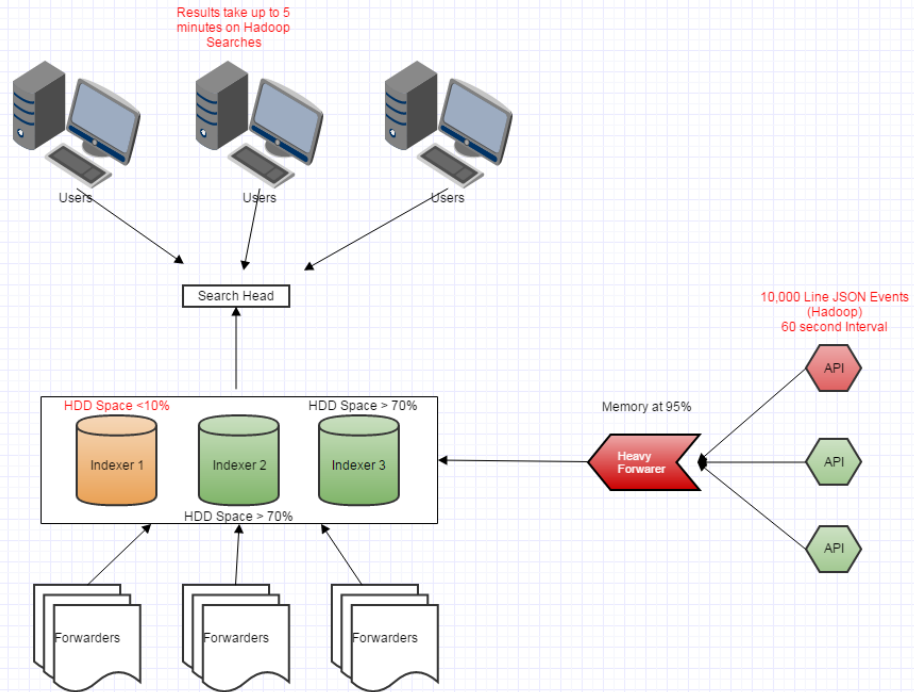
Yes No

This saves a copy of all indexed data on this Splunk instance and forwards copies to other instances.

Cancel

Save





```

root@INTERNET-ROUTER> show log idp-log
Dec  3 06:57:46 INTERNET-ROUTER RT_IDP: IDP_ATTACK_LOG_EVENT: IDP: at 1354543066, SIG Attack log <192.168.1.102/63
279->63.245.215.56/21> for TCP protocol and service SERVICE_IDP application NONE by rule 1 of rulebase IPS in polic
y idp-pol-1. attack: repeat=0, action=CLOSE, threat-severity=INFO, name=custom-ftp, NAT <68.144.56.81:41248->0.0.0.
0:0>, time-elapsed=0, inbytes=0, outbytes=0, inpackets=0, outpackets=0, intf:TRUST:vlan.192->INTERNET:fe-0/0/0.0, p
acket-log-id: 0 and misc-message -

```

```

root@INTERNET-ROUTER>

```

props.conf

```
[sourcetype]
TRANSFORMS = stanzaName
```

transforms.conf

```
[stanzaName]
SOURCE_KEY = ...
REGEX = ...
DEST_KEY = ...
FORMAT = ...
```

List Format 20 Per Page

i	Time	Event
>	1/15/15 10:31:48.000 AM	[01/15/2015:10:31:48] VendorID=67834 ccn: 4929800800059530 purchaseCode=A host = web_server2276 sourcetype = purchasing
>	1/15/15 10:22:34.000 AM	[01/15/2015:10:22:34] VendorID=44562 ccn: 4556727302463532 purchaseCode=G host = web_server2276 sourcetype = purchasing

20 Per Page Format Preview

_time	VendorID	ccn	purchaseCode
2015-01-15 10:31:48	67834	XXXXXXXXXXXX9530	A
2015-01-15 10:22:34	44562	XXXXXXXXXXXX3532	G

Chapter 4: Knowledge Management

```
index=myIndex sourcetype=was:pids earliest_time=0 latest_time=now()
| rex "(?<pid>\d+)"
| stats latest(pid) as pid by jvm_server,host
| join type=inner jvm_server [search index="myIndex" earliest_time=-15m latest_time=now()
sourcetype="iis" website="*" host=host1 OR host=host2 OR host=host3 OR host=host4 OR host=host5
sc_status=5* | lookup status_codes.csv status AS sc_status | rename sc_status AS status | eval
uri=lower(cs_uri_stem) | search uri=*.do | stats count,latest(_time) as Latest_Alert_Time by host
uri | rex field=uri "\/(?<jvm_server>.*?)\./.*" | dedup jvm_server sortby -Latest_Alert_Time | eval
jvm_server=jvm_server."_server" | fields jvm_server,Latest_Alert_Time | search NOT [|inputlookup
Killed_Processes.csv | where return_code==0 | fields jvm_server,Latest_Alert_Time]]
| fields host,pid,jvm_server,Latest_Alert_Time
| eval user="privUser"
| eval command="/usr/local/bin/sudo kill ".pid
| callsshscript host=host user=user command=command
| eval Status=if(return_code==0,"Successfully Killed","Failed")
| outputlookup Killed_Processes.csv
```

```
index=os sourcetype=cpu | eval linuxCPU=100 - pctIdle | lookup
server_inventory.csv nix_host as host | rename linuxCPU as nixUtil |
stats sparkline(avg(linuxCPU)) as averagePCT avg(linuxCPU) as pctCPU by
host cores model | sort - pctCPU | eval pctCPU=round(pctCPU,2) | eval
pctCPU=(pctCPU + "% Used")
```

```
| eval linuxCPU=100 - pctIdle | lookup server_inventory.csv nix_host as
host
```

| rename linuxCPU as nixUtil

```
| stats sparkline(avg(linuxCPU)) as averagePCT avg(linuxCPU) as pctCPU
by host cores model
```

```
index=os sourcetype=cpu | eval linuxCPU=100 - pctIdle | lookup
server_inventory.csv nix_host as host | stats sparkline(avg(linuxCPU))
as averagePCT avg(linuxCPU) as pctCPU by host cores model | sort -
pctCPU | eval pctCPU=round(pctCPU,2) | eval pctCPU=(pctCPU + "% Used")
```

```
index=os sourcetype=cpu | eval linuxCPU=100 - pctIdle | lookup
server_inventory.csv nix_host as host | rename linuxCPU as nixUtil |
stats sparkline(avg(linuxCPU)) as averagePCT avg(linuxCPU) as pctCPU by
host cores model | sort - pctCPU | eval pctCPU=round(pctCPU,2) | eval
pctCPU=(pctCPU + "% Used")
```

New Search Save As ▾ Close

index=nix sourcetype=syslog "SELinux is preventing" Last 15 minutes ▾ 🔍

✓ 30 events (3/28/16 5:50:37.000 PM to 3/28/16 6:05:37.000 PM) Job ▾ || ▢ → ↓ 🗑️ 🔔 Smart Mode ▾

Events (30) | Patterns | Statistics | Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect 1 minute per column

List ▾ Format ▾ 20 Per Page ▾ ◀ Prev 1 2 Next ▶

Hide Fields		All Fields	
i	Time	Event	
>	3/28/16 6:05:11.000 PM	Mar 28 18:05:11 setroubleshoot: SELinux is preventing /sbin/rsyslogd from name_connect access on the tcp_socket . For complete SELinux messages. run sealert -1 ba27e05f-8e2e-49f9-a772-a0e52da5a96c host = ... source = /var/log/messages sourcetype = syslog	
>	3/28/16 6:04:47.000 PM	Mar 28 18:04:47 setroubleshoot: SELinux is preventing /sbin/rsyslogd from name_connect access on the tcp_socket . For complete SELinux messages. run sealert -1 ba27e05f-8e2e-49f9-a772-a0e52da5a96c host = ... source = /var/log/messages sourcetype = syslog	
>	3/28/16 6:04:11.000 PM	Mar 28 18:04:11 setroubleshoot: SELinux is preventing /sbin/rsyslogd from name_connect access on the tcp_socket . For complete SELinux messages. run sealert -1 ba27e05f-8e2e-49f9-a772-a0e52da5a96c host = ... source = /var/log/messages sourcetype = syslog	

Selected Fields
a host 1
a source 1
a sourcetype 1

Interesting Fields
date_hour 2
date_mday 1
date_minute 16
date_month 1
date_second 11

splunk> App: Search & Reporting ▾ Marlette, Travis (Contractor) ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Pivot Reports Alerts Dashboards Search & Reporting

New Search Save As ▾ Close

index=nix sourcetype=syslog "SELinux is preventing" Last 15 minutes ▾ 🔍

✓ 30 events (3/28/16 5:50:37.000 PM to 3/28/16 6:05:37.000 PM) Job ▾ || ▢ → ↓ 🗑️ 🔔 Smart Mode ▾

Events (30) | Patterns | Statistics | Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect 1 minute per column

Report
Dashboard Panel
Alert
Event Type

Save As Event Type

Name

Search index=nix sourcetype=syslog "SELinux is preventing"

Tags

Color

Priority

Determines which style wins, when an event has more than one event type.

New Search Save As ▾ Close

index=nix sourcetype=syslog "SELinux is preventing" Last 15 minutes ▾ 🔍

✓ 30 events (3/28/16 5:50:37.000 PM to 3/28/16 6:05:37.000 PM) Job ▾ || ▢ → ↓ 🗑️ Smart Mode ▾

Events (30) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection x Deselect 1 minute per column

List ▾ Format ▾ 20 Per Page ▾ < Prev 1 2 Next >

< Hide Fields	☰ All Fields	i	Time	Event
Selected Fields a host 1 a source 1 a sourcetype 1 Interesting Fields # date_hour 2 # date_mday 1 # date_minute 16 a date_month 1 # date_second 11		>	3/28/16 6:05:11.000 PM	Mar 28 18:05:11 [redacted] setroubleshoot: SELinux is preventing /sbin/rsyslogd from m_name_connect access on the tcp_socket . For complete SELinux messages. run sealert -l ba27e05f-8e2e-49f9-a772-a0e52da5a96c host = [redacted] source = /var/log/messages sourcetype = syslog
		>	3/28/16 6:04:47.000 PM	Mar 28 18:04:47 [redacted] setroubleshoot: SELinux is preventing /sbin/rsyslogd from m_name_connect access on the tcp_socket . For complete SELinux messages. run sealert -l ba27e05f-8e2e-49f9-a772-a0e52da5a96c host = [redacted] source = /var/log/messages sourcetype = syslog
		>	3/28/16 6:04:11.000 PM	Mar 28 18:04:11 [redacted] setroubleshoot: SELinux is preventing /sbin/rsyslogd from m_name_connect access on the tcp_socket . For complete SELinux messages. run sealert -l ba27e05f-8e2e-49f9-a772-a0e52da5a96c host = [redacted] source = /var/log/messages sourcetype = syslog

```

root@ [redacted] /opt/splunk/etc/apps
[redacted@ [redacted] apps]# pwd
/opt/splunk/etc/apps
[redacted@ [redacted] apps]# ll
total 68
drwx----- 4 root root 4096 Mar 25 14:58 [redacted]_all_heavyforwarder_outputs
drwx----- 4 root root 4096 Mar 25 14:53 [redacted]_all_indexes
drwx----- 4 root root 4096 Mar 25 14:56 [redacted]_search_volume_indexes
drwxr-xr-x 6 root root 4096 Mar 25 12:21 framework
drwxr-xr-x 6 root root 4096 Apr 28 2015 gettingstarted
drwxr-xr-x 4 root root 4096 Apr 28 2015 introspection_generator_addon
drwxr-xr-x 6 root root 4096 Apr 28 2015 launcher
drwxr-xr-x 5 root root 4096 Mar 25 12:21 learned
drwxr-xr-x 3 root root 4096 Apr 28 2015 legacy
drwxr-xr-x 6 root root 4096 Apr 28 2015 sample_app
drwxr-xr-x 10 root root 4096 Mar 25 14:12 search
drwxr-xr-x 4 root root 4096 Apr 28 2015 splunk_datapreview
drwxr-xr-x 4 root root 4096 Apr 28 2015 SplunkForwarder
drwxr-xr-x 4 root root 4096 Apr 28 2015 SplunkLightForwarder
drwxr-xr-x 9 root root 4096 Mar 25 12:21 splunk_management_console
drwx----- 10 root root 4096 Mar 25 14:00 Splunk_TA_nix
drwxr-xr-x 4 root root 4096 Apr 28 2015 user-prefs
[redacted@ [redacted] apps]#
  
```

```
root@ /opt/splunk/etc/apps/search/local
GNU nano 2.0.9 File: eventtypes.conf
[myEventtype]
search = index=nix sourcetype=syslog "SELinux is preventing"

^G Get Help ^C WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

```
Entity refresh control page
=====
...
Forces a refresh on splunkd resources

This method calls a splunkd refresh on all registered EAI handlers that
advertise a reload function. Alternate entities can be specified by appending
them via URI parameters. For example,

    http://localhost:8000/debug/refresh?entity=admin/conf-times&entity=data/ui/manager

will request a refresh on only 'admin/conf-times' and 'data/ui/manager'.

1) not all splunkd endpoints support refreshing.
2) auth-services is excluded from the default set, as refreshing that system will
   logout the current user; use the 'entity' param to force it
...

Refreshing admin/conf-times           OK
Refreshing data/ui/manager            OK
Refreshing data/ui/nav                OK
Refreshing data/ui/views              OK
Refreshing admin/alert_actions        OK
Refreshing admin/citrix_netscaler     OK
Refreshing admin/clusterconfig       OK
Refreshing admin/clustersearchheadconfigOK
Refreshing admin/collections-conf     BadRequest
In handler 'collections-conf': Must use user context of 'nobody' when interacting with collection configurations (used user='admin')
Refreshing admin/commandsconf        OK
Refreshing admin/conf-deploymentclient OK
Refreshing admin/conf-inputs         OK
Refreshing admin/conf-times          OK
Refreshing admin/conf-wmi            OK
Refreshing admin/connections         OK
Refreshing admin/cooked              OK
Refreshing admin/datamodel-files     OK
Refreshing admin/datamodelacceleration OK
Refreshing admin/datamodeledit       OK
Refreshing admin/deploymentsserver   OK
Refreshing admin/dispatch            OK
Refreshing admin/eventtypes          OK
```

Match Replace

duration:\s(?<duration>[^\s]+)

global ignoreCase extended dotall multiline Share Link

Mar 31 17:56:59 wdcpagl05 postgres[13011]: [178005-1] postgres postgres localhost 13011 2016-03-31 17:56:59 EDT SELECTLOG: duration: 0.435 ms

Mar 29 17:14:58 rsyslogd-2177: imuxsock begins to drop messages from pid 31881 due to rate-limiting

Event Actions

Build Event Type	Value	Actions
Extract Fields	/var/log/messages	
Show Source	syslog	
eventtype	nix-all-logs	
index	nix	
linecount	1	
process	rsyslogd-2177	
splunk_server		
splunk_server_group	dmc_group_indexer	
unix_category	all_hosts	
unix_group	All Hosts	
_time	2016-03-29T17:14:58.000-04:00	
punct		

Extract Fields Select fields Validate fields Save < Next >

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 rule.

Mar 29 17:14:58 rsyslogd-2177: imuxsock begins to drop messages from pid 31881 due to rate-limiting

Preview

If you see incorrect results below, click an additional event to add it to the set of sample events.

Events

✓ 1,000 events (before 3/29/16 5:22:32.000 PM)

pid Apply Sample: First 1,000 events

Field Name can r

Sample Value 31881

Extract Require Add Extraction


```

root@\ opt/splunk/etc/apps/search/local
GNU nano 2.0.9 File: props.conf Modified
[syslog]
EXTRACT-pid = pid\s(?<pid>\d+)

```

[^]G Get Help [^]C WriteOut [^]R Read File [^]Y Prev Page [^]K Cut Text [^]C Cur Pos
[^]X Exit [^]J Justify [^]W Where Is [^]V Next Page [^]U UnCut Text [^]T To Spell

- a source 1
- a sourcetype 1

- Interesting Fields
- # date_hour 1
- # date_mday 1
- # date_minute 16
- a date_month 1
- # date_second 60
- a date_wday 1
- # date_year 1
- a date_zone 1
- a eventtype 3
- a index 1
- # linecount 1
- # pid 50
- a process 3
- a punct 6
- a splunk_server 3
- a splunk_server_group 1
- # timeendpos 1
- # timestartpos 1
- a unix_category 1
- a unix_group 1

pid

50 Values, 100% of events

Selected

Reports

Average over time Maximum value over time Minimum value over time
 Top values Top values by time Rare values
 Events with this field

Avg: 11394.468594 Min: 666 Max: 32022 Std Dev: 13912.948028

Top 10 Values	Count	%
31881	300	29.91%
1500	92	9.172%
1338	78	7.777%
1527	70	6.979%
1275	56	5.583%
3776	48	4.786%
1382	42	4.187%
1715	36	3.589%
1393	31	3.091%
1619	25	2.492%

Chapter 5: Alerting

Events | Patterns | Statistics (35) | Visualization

100 Per Page | Format | Preview

host	cpu
myHost	48.491500
myHost	28.408000
myHost	27.212917
myHost	23.612778
myHost	22.213158
myHost	12.753333
myHost	10.662632

Search | Pivot | Reports | Alerts | Dashboards Search & Reporting

New Search

Save As | Close

```
index=nix sourcetype=cpu cpu=all | eval pctCPU=(100 - pctIdle) | stats avg(pctCPU) as cpu by host | eval
host="myHost" | where cpu>25
```

Last 15 minutes | Search

759 events (4/21/16 6:14:44.000 PM to 4/21/16 6:29:44.000 PM)

Job | Stop | Refresh | Download | Print | Smart Mode

Events | Patterns | Statistics (3) | Visualization

100 Per Page | Format | Preview

host	cpu
myHost	33.704091
myHost	25.780417
myHost	38.477368

New Search

Save As | Close

```
index=nix sourcetype=cpu cpu=all startminutesago=30
| eval pctCPU=(100 - pctIdle)
| eval severity=case(pctCPU>=90, "Critical", pctCPU>=70, "Warning", pctCPU>=0, "Normal")
| where severity="Normal"
| stats avg(pctCPU) as cpu count by host severity
| eval host="myHost"
```

Last 15 minutes | Search

1,700 events (4/22/16 5:09:06.000 PM to 4/22/16 5:39:08.290 PM)

Job | Stop | Refresh | Download | Print | Smart Mode

Events | Patterns | Statistics (37) | Visualization

100 Per Page | Format | Preview

host	severity	cpu	count
myHost	Normal	22.250862	58
myHost	Normal	4.224750	40
myHost	Normal	1.045714	35
myHost	Normal	0.666190	42
myHost	Normal	1.766579	38
myHost	Normal	32.225429	35
myHost	Normal	4.179756	41
myHost	Normal	5.847297	37

```
# Shows stats per CPU (useful for SMP machines)
[script://./bin/cpu.sh]
sourcetype = cpu
source = cpu
interval = 30
index = nix
disabled = 0
```

New Search Save As ▾ Close

```
index=nix sourcetype=cpu cpu=all
| eval pctCPU=(100 - pctIdle)
| eval severity=case(pctCPU>=90, "Critical", pctCPU>=70, "Warning", pctCPU>=0, "Normal")
| where severity="Normal"
| stats avg(pctCPU) as cpu count by host severity
| eval host="myHost"
```

Last 15 minutes ▾ 🔍

✓ 1,700 events (4/22/16 5:09:06.000 PM to 4/22/16 5:39:08.290 PM) Job ▾ ⏸ ⏹ ↶ ⏴ ⏵ ⏷ Smart Mode ▾

Events Patterns Statistics (37) Visualization

100 Per Page ▾ Format ▾ Preview ▾

host	severity	cpu	count
myHost	Normal	22.250862	58
myHost	Normal	4.224750	40
myHost	Normal	1.045714	35
myHost	Normal	0.666190	42
myHost	Normal	1.766579	38
myHost	Normal	32.225429	35
myHost	Normal	4.179756	41
myHost	Normal	5.847297	37
myHost	Normal	1.982750	40

```
index=nix sourcetype=cpu cpu=all
| eval pctCPU=(100 - pctIdle)
| eval severity=case(pctCPU>=90, "Critical", pctCPU>=70, "Warning", pctCPU>=0, "Normal")
| where severity="Normal"
| stats avg(pctCPU) as cpu count by host severity
| eval host="myHost"
| where count>30
| eval cpu=round(cpu,1)
| sort - cpu
| eval cpu=(cpu + "%")
| fields - count
```

Last 15 minutes ▾ 🔍

✓ 1,711 events (4/22/16 5:17:20.000 PM to 4/22/16 5:47:22.790 PM) Job ▾ ⏸ ⏹ ↶ ⏴ ⏵ ⏷ Smart Mode ▾

Events Patterns Statistics (36) Visualization

100 Per Page ▾ Format ▾ Preview ▾

host	severity	cpu
myHost	Normal	43.4%
myHost	Normal	31.5%
myHost	Normal	29.3%
myHost	Normal	26.7%
myHost	Normal	25.2%
myHost	Normal	23.0%
myHost	Normal	21.8%
myHost	Normal	11.6%
myHost	Normal	9.9%

Save As ▾ Close

- Report
- Dashboard Panel
- Alert
- Event Type

Save As Alert ✕

Title

Description

Alert type Scheduled Real Time

Time Range

Earliest: e.g. -1h@h (1 hour ago, to the hour). [Learn More](#)
4/22/16 5:47:00.000 PM

Latest: e.g. -1h@h (1 hour ago, to the hour). [Learn More](#)
4/22/16 5:55:44.000 PM

Cron Expression e.g. 00 18 * * * (every day at 6PM). [Learn More](#)

Trigger condition

Trigger if number of results

Save As Alert



Send Email

Email must be configured in System Settings > Alert Email Settings. [Learn More](#)

To

Comma separated list of email addresses.
[Show CC and BCC](#)

Priority

Subject

The email subject and message can include tokens that insert text based on the results of the search. [Learn More](#)

Message

- Include
- Link to Alert
 - Link to Results
 - Search String
 - Inline
 - Trigger Condition
 - Attach CSV
 - Trigger Time
 - Attach PDF

Run a Script

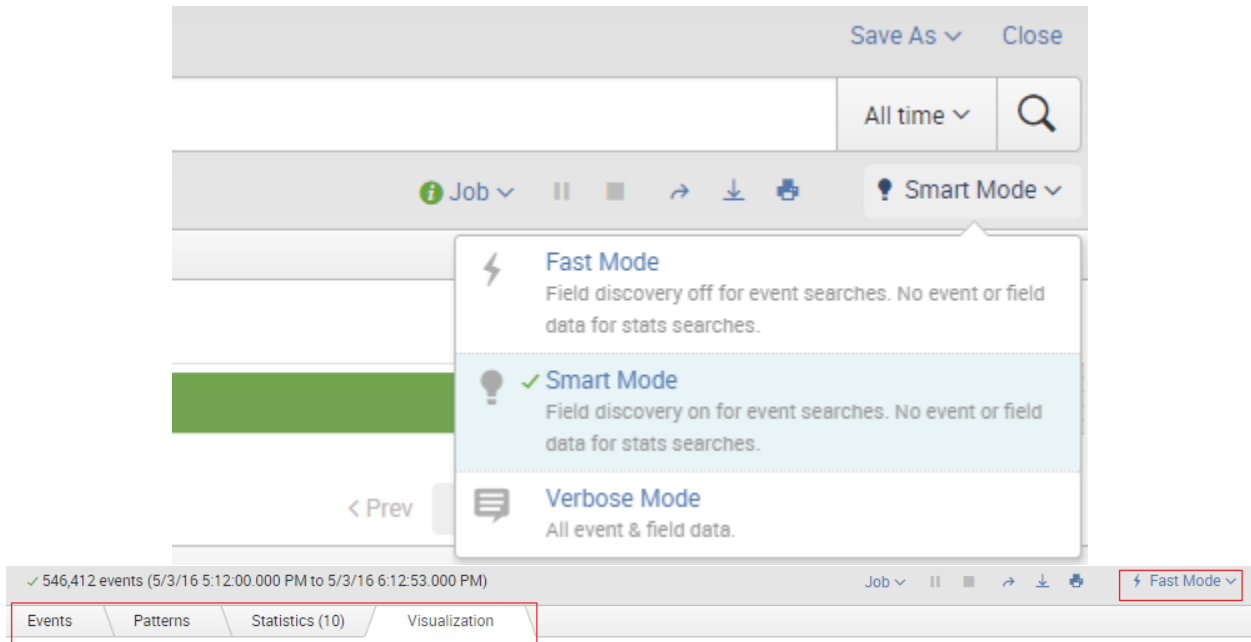
Action Options

When triggered, execute actions

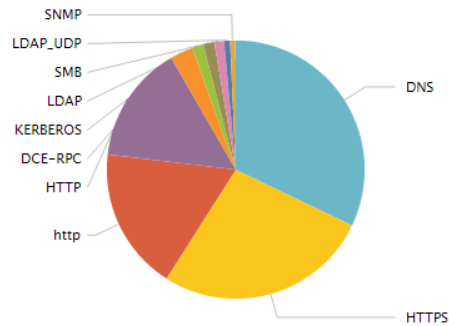
Throttle ?

Suppress triggering for

Chapter 6: Searching and Reporting



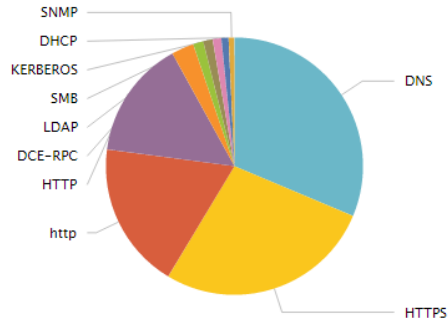
Pie Format



Search job inspector

This search has completed and has returned **10** results by scanning **546,412** events in **8.475** seconds.

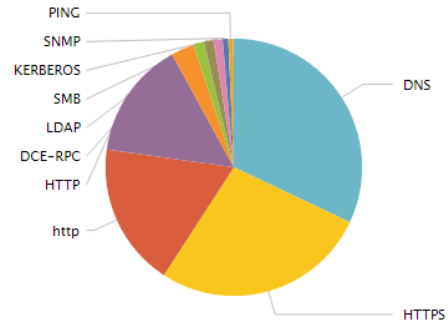
Pie ▾ Format ▾



Search job inspector

This search has completed and has returned **10** results by scanning **543,064** events in **48.115** seconds.

Pie ▾ Format ▾



Search job inspector

This search has completed and has returned **10** results by scanning **538,980** events in **8.196** seconds.

✓ 45 events (5/4/16 5:44:14.000 PM to 5/4/16 5:59:14.000 PM)

Events (45) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection x Deselect

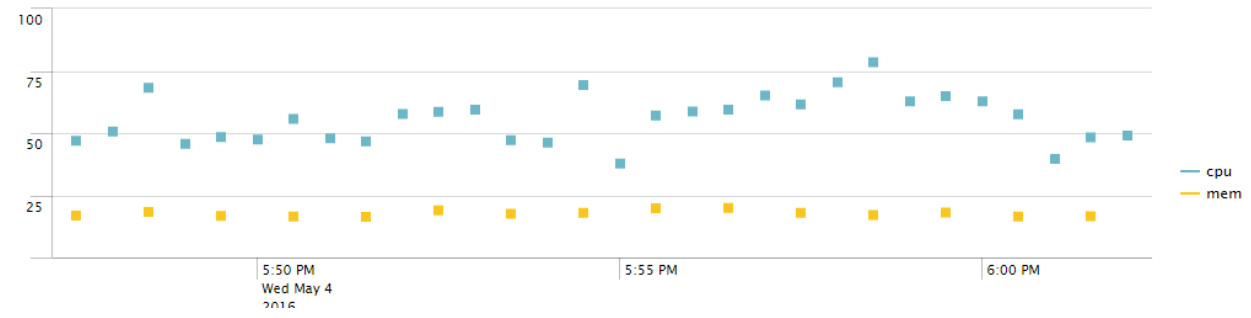


List Format 50 Per Page

Hide Fields		All Fields	i	Time	Event						
			>	5/4/16 5:59:01.000 PM	a11 source = cpu ; sourcetype = cpu	57.59	0.00	5.11	0.00	37.30	
Selected Fields			>	5/4/16 5:58:31.000 PM	a11 source = cpu ; sourcetype = cpu	69.29	0.00	9.12	0.08	21.51	
Interesting Fields			>	5/4/16 5:58:30.000 PM	totMemory 32876372 usedMemory 30452660 source = free.sh ; sourcetype = freeMem		freeMemory 2423712	bufMemory 1293928	cacheMemory 23547752	realusedMem 5610980	realfreeMem 27265392
			>	5/4/16 5:58:01.000 PM	a11 source = cpu ; sourcetype = cpu	66.36	0.00	4.02	0.00	29.62	
			>	5/4/16 5:57:31.000 PM	a11 source = cpu ; sourcetype = cpu	57.14	0.00	4.26	0.08	38.51	
			>	5/4/16 5:57:30.000 PM	totMemory 32876372 usedMemory 30320236 source = free.sh ; sourcetype = freeMem		freeMemory 2556136	bufMemory 1288356	cacheMemory 23148768	realusedMem 5883112	realfreeMem 26993260
			>	5/4/16 5:57:01.000 PM	a11 source = cpu ; sourcetype = cpu	60.79	0.00	4.26	0.00	34.95	
			>	5/4/16 5:56:31.000 PM	a11 source = cpu ; sourcetype = cpu	55.35	0.00	4.10	0.00	40.55	
			>	5/4/16 5:56:30.000 PM	totMemory 32876372 usedMemory 30734672 source = free.sh ; sourcetype = freeMem		freeMemory 2141700	bufMemory 1287060	cacheMemory 22895196	realusedMem 6552416	realfreeMem 26323956
			>	5/4/16	a11	55.22	0.00	3.43	0.00	41.35	

Events Patterns Statistics (91) Visualization


Line Format



✓ 75,213 events (5/5/16 5:31:42.000 PM to 5/5/16 5:46:42.000 PM)

Events Patterns Statistics (0) Visualization

100 Per Page ▾ Format ▾ Preview ▾

 No results found.

✓ 73,490 events (5/5/16 5:33:44.000 PM to 5/5/16 5:48:44.000 PM)

Job ▾ || ■ ↶ ↷ ⌵ ⌶ ⚙ Smart Mode ▾

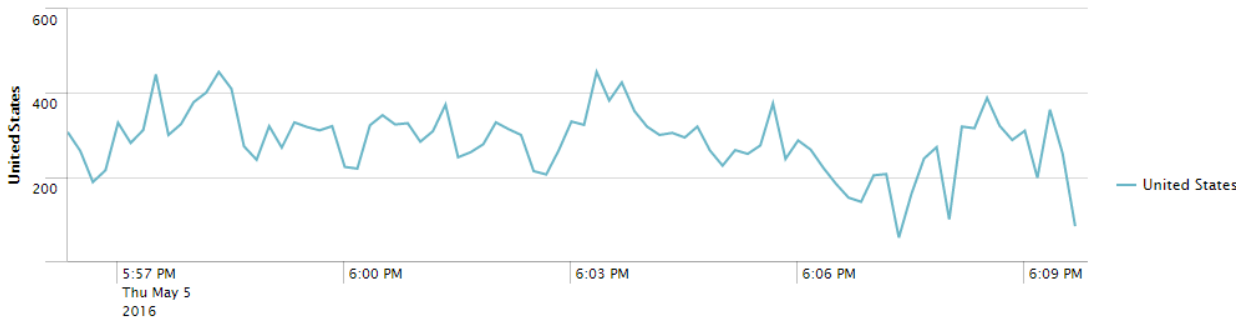
Events Patterns Statistics (18) Visualization

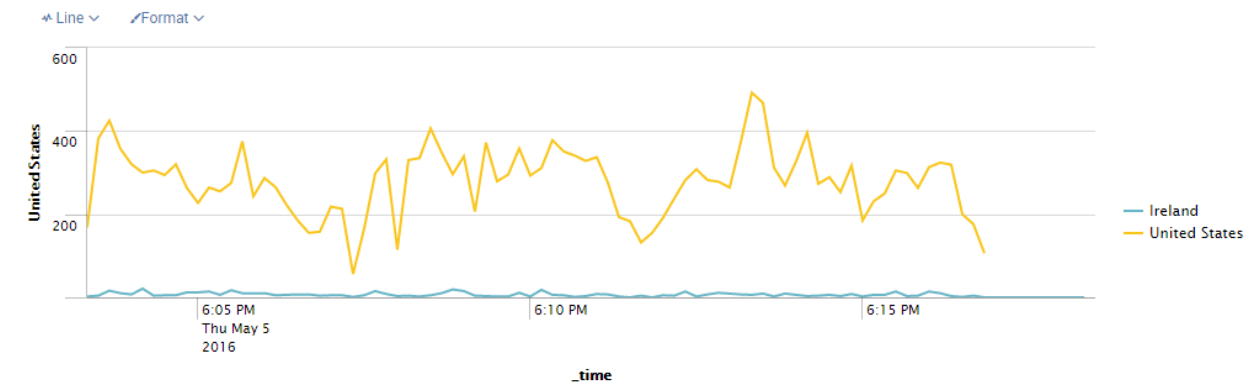
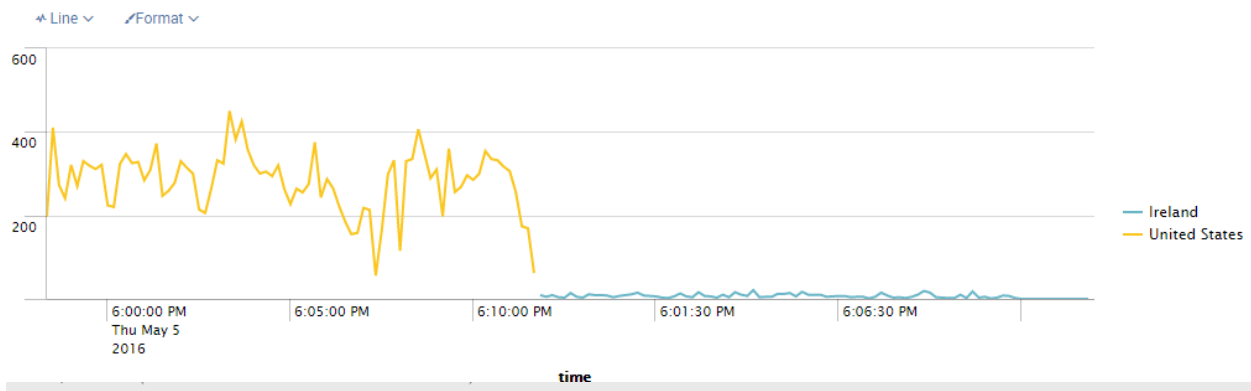
100 Per Page ▾ Format ▾ Preview ▾

catdesc ▾	Ireland ▾	United Kingdom ▾	United States ▾
Advertising	16	-	1357
Business	-	-	116
Content Servers	-	-	69
Entertainment	-	-	23
Finance and Banking	-	-	60
Government and Legal Organizations	-	-	57
Information Technology	-	12	623
Internet Radio and TV	-	-	28
Meaningless Content	-	-	223
News and Media	-	-	135

Events Patterns Statistics (81) Visualization

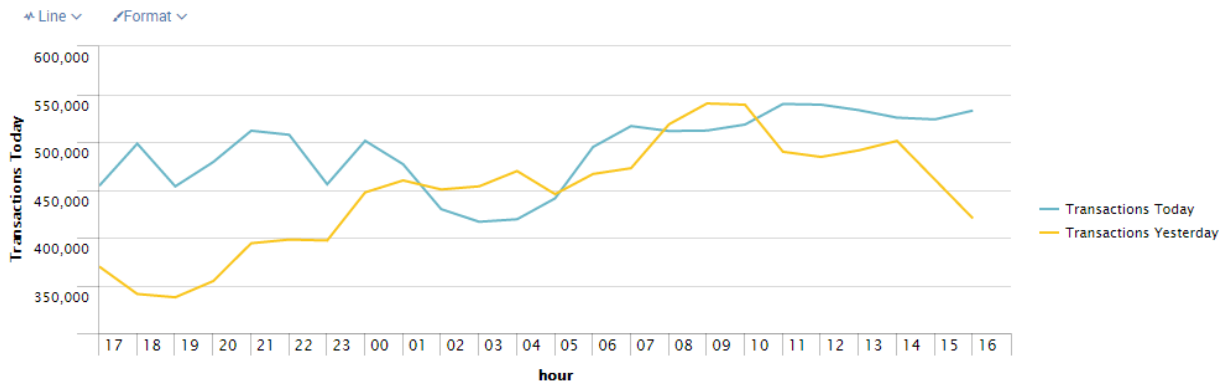
Line ▾ Format ▾





dstcountry ◊	Last Hour ◊	Last 15 Minutes ◊
Australia	35	1
Austria	1	
Belgium	1	
Brazil	3	1
Canada	308	66
Chile	56	
China	23	1
Costa Rica	6	
Denmark	3	
Europe	20	4
France	30	1
Germany	68	23
Greece	1	
Hong Kong	10	1
India	11	2
Ireland	2610	739
Italy	1	
Japan	111	58
Lithuania	3	
Luxembourg	2	
Netherlands	95	11
Norway	4	
Poland	3	2
Reserved	237557	53087
Russian Federation	5	1
Singapore	193	33
Sweden	52	7
Switzerland	11	6
Taiwan	1	
United Kingdom	405	63
United States	117517	24083

dstcountry	Last Hour	Last 15 Minutes
Austria	1	1
Belgium	1	57
Brazil	3	1
Canada	308	2
Chile	56	3
China	23	9
Costa Rica	6	1
Denmark	3	2
Europe	20	621
France	30	1
Germany	68	72
Greece	1	1
Hong Kong	10	6
India	11	2
Ireland	2610	55371
Italy	1	2
Japan	111	21
Lithuania	3	6
Luxembourg	2	9
Netherlands	95	76
Norway	4	23135
Poland	3	
Reserved	237557	
Russian Federation	5	
Singapore	193	
Sweden	52	
Switzerland	11	
Taiwan	1	
United Kingdom	405	
United States	117517	



Chapter 7: Form-Based Dashboards

Events (1,389) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection × Deselect 1 minute per column

List Format 50 Per Page < Prev 1 2 3 4 5 6 7 8 9 ... Next >

Hide Fields		All Fields	i	Time	Event				
Selected Fields			>	5/16/16 1:28:52.000 PM	/dev/mapper/rootvg-root 7G 1.9G 60% / host = . ; source = df ; sourcetype = df	ext4	4.8G	2.	
Interesting Fields			>	5/16/16 1:28:52.000 PM	/dev/sda1 6M 194M 45% /boot host = \ ; source = df ; sourcetype = df	ext4	368M	15	
			>	5/16/16 1:28:52.000 PM	/dev/mapper/rootvg-home 7M 1.8G 2% /home host = ' ; source = df ; sourcetype = df	ext4	2.0G	2	
			>	5/16/16 1:28:52.000 PM	/dev/mapper/rootvg-tmp 2M 1.9G 1% /tmp host = ; source = df ; sourcetype = df	ext4	2.0G	3.	
			>	5/16/16 1:28:52.000 PM	/dev/mapper/rootvg-local 5M 924M 1% /usr/local host = ; source = df ; sourcetype = df	ext4	976M	1.	
			>	5/16/16 1:28:52.000 PM	/dev/mapper/rootvg-var 9M 376M 60% /var host = ; source = df ; sourcetype = df	ext4	976M	54	

✓ 1,380 events (5/16/16 1:44:51.000 PM to 5/16/16 1:59:51.000 PM) Job || ↶ ↷ ↵ ↴ Smart Mode

Events Patterns Statistics (36) Visualization

100 Per Page Format Preview

mount	host	pctSpace
/home/archive		100
		100
/var/log		100
		99
		99
		99
		99
		99
		99
		99
		99
		99
		98
		98
		98
		98
		98
		98
		98

Save Save As View

- Report
- Dashboard Panel
- Alert
- Event Type

Save As Report ×

Title

Description

Visualization

Time Range Picker

splunk> App: Search & Reporting ▾

Search Pivot Reports Alerts Dashboards

> myDiskSpaceReport

Edit Acceleration ×

Report myDiskSpaceReport

Accelerate Report

Acceleration may increase storage and processing costs.

Summary Range ?

T Text General

Label host

Search on Change

Token Options

Token host

Default *

Seed

Token Prefix host-

Token Suffix

Cancel Apply

Edit Search

Title

Search String

```
Index=nix sourcetype=dfshosts | stats
avg(PercentUsedSpace) AS pctSpace
by mount host | eval
pctSpace=round(pctSpace) | where
pctSpace > 90 | sort - pctSpace
```

Run Search

Time Range Scope Shared Time Picker (hist)

Cancel Save

```
index=nix sourcetype=dfs host=myHost
| stats avg(PercentUsedSpace) AS pctSpace
by mount host
| eval pctSpace=round(pctSpace)
| where pctSpace > 90
| sort - pctSpace
```

100 Per Page Format Preview

mount	host	pctSpace
myMount	myHost	100

Edit More Info Add to Dashboard

Job || [] ↺ ↻ ⬇️ 🖨️

< Prev 1 2 Next >

Save As Dashboard Panel



Dashboard

New

Existing

Dashboard Title

myFirstDashboard

Dashboard ID ?

myfirstdashboard

Can only contain letters, numbers and underscores.

Dashboard Description

optional

Dashboard Permissions

Private

Shared in App

Panel Title

optional

Panel Powered By

🔍 Inline Search

📄 Report

Panel Content

📊 Statistics

➕ Line

Cancel

Save

+ Add Panel + Add Input ▾

- T Text
- ⊙ Radio
- ▾ Dropdown
- ☑ Checkbox
- ▾ Multiselect
- ⌚ Time
- 🔍 Submit

Edit: myFirstDashboard

✎ ✕

T Text	General
⊙ Radio	Label <input type="text" value="Select Time Range"/>
▾ Dropdown	Search on Change <input type="checkbox"/>
☑ Checkbox	Token Options
▾ Multiselect	Token ? <input type="text" value="hist"/>
⌚ Time	Default <input type="text" value="Last 24 hours ▾"/>

Cancel Apply

Search bar with icons for search, table, and edit.

- INLINE SEARCH
- Edit Title
- Edit Search String
- Convert to Report
- Delete

Edit Search

Title

Search String

```
index=nix sourcetype=df | stats avg(PercentUsedSpace) AS pctSpace by mount host | eval pctSpace=round(pctSpace) | where pctSpace > 90 | sort - pctSpace
```

Run Search [↗](#)

Time Range Scope

Shared Time Picker (hist) ▾

- ✓ Shared Time Picker (hist)
- Explicit Selection
- Tokens

Cancel

+ Add Panel

+ Add Input ▾

T Text

Radio

▾ Dropdown

Checkbox

▾ Multiselect

🕒 Time

🔍 Submit

field2

T Text General

Radio

▼ Dropdown

Checkbox

▼ Multiselect

Time

Label

Search on Change

Token Options

Token ?

Default ?

Seed ?

Token Prefix ?

Token Suffix ?

Cancel Apply

Edit Search ×

Title

Search String `|index=nix sourcetype=df $host$ | stats avg(PercentUsedSpace) AS pctSpace by mount host | eval pctSpace=round(pctSpace) | where pctSpace > 90 | sort - pctSpace`

Run Search [↗](#)

Time Range Scope

Edit Search ×

Title CPU

Search String `index=nix sourcetype=cpu cpu=all $host$ | eval cpu=(100 - pctidle) | timechart avg(cpu) by host`

Run Search [↗](#)

Time Range Scope

Edit Search ✕

Title Memory

Search String

```
index=nix sourcetype=freeMem $host$ |  
eval mem=(realfreeMem / totMemory) *  
100 | timechart avg(mem) by host
```

[Run Search](#)

Time Range Scope Shared Time Picker (hist) ▾

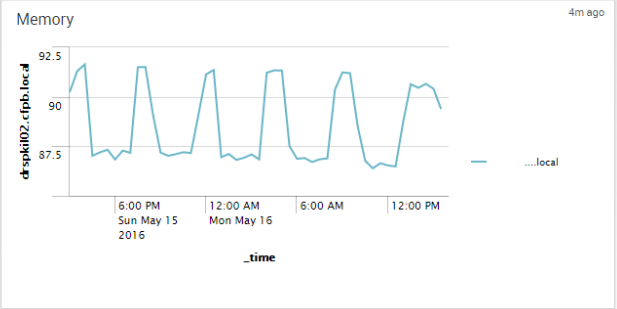
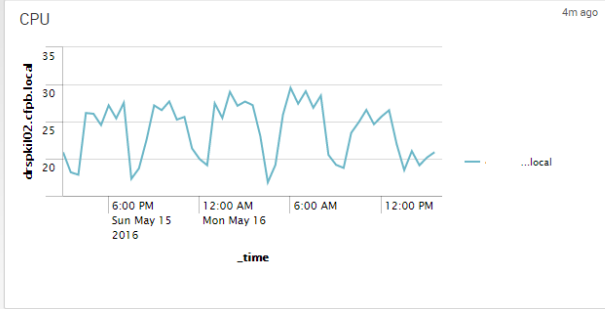
Cancel

Save

myFirstDashboard

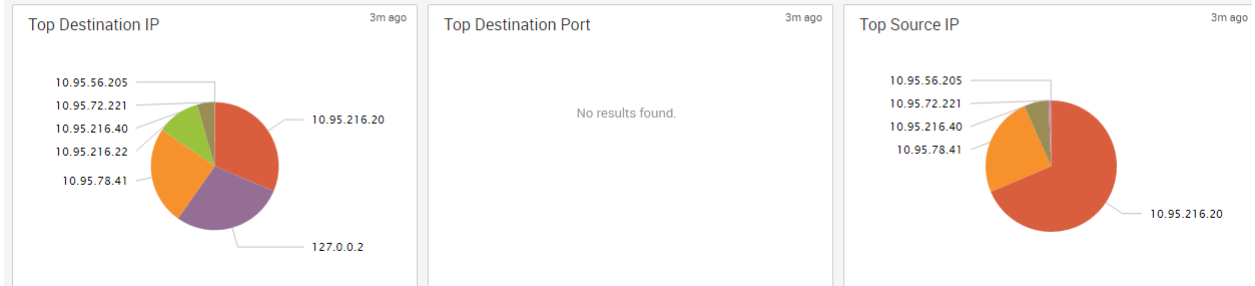
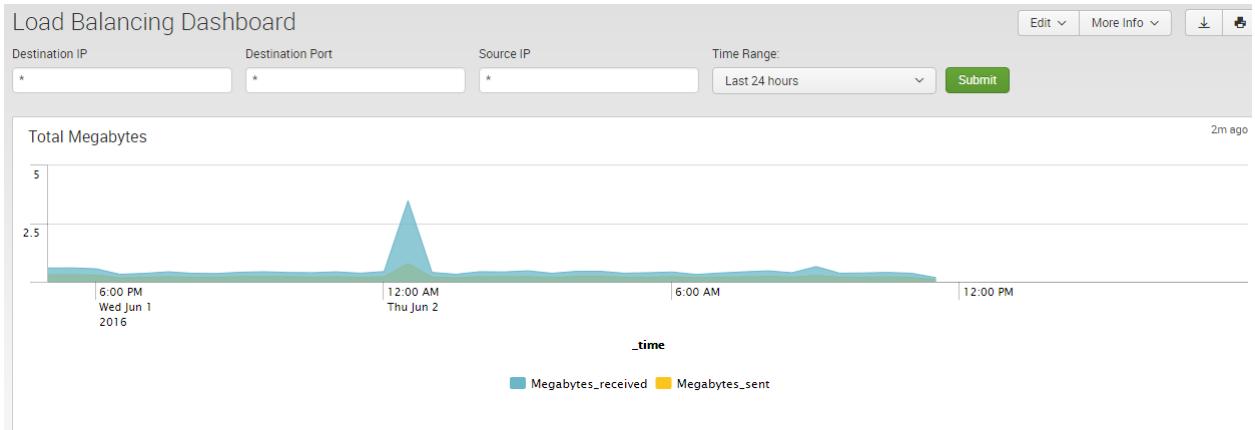
[Edit](#) [More Info](#) [↓](#) [🗑](#)

Select Time Range host
Last 24 hours 2*



mount	host	pctSpace	4m ago
/	dspk102.cfbp.local	100	

Chapter 8: Search Optimization



T Text

- Radio
- Dropdown
- Checkbox
- Multiselect
- Time

General

Label:

Search on Change:

Token Options

Token ?

Default ?

Seed ?

Token Prefix ?

Token Suffix ?

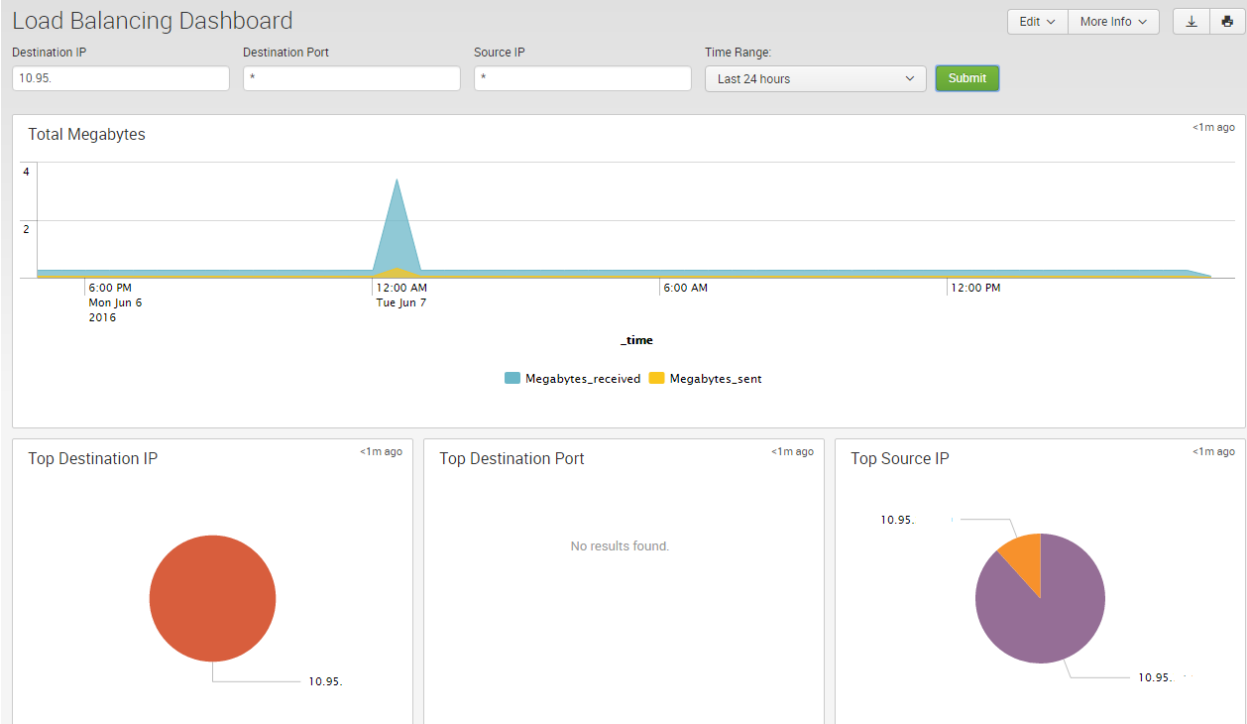
Edit Search ✕

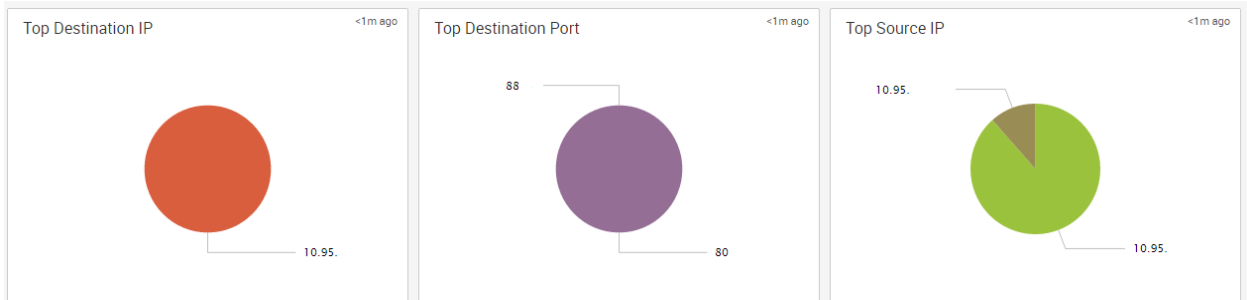
Title	Total Megabytes
Search String	<pre>eventtype=netscaler TCP \$dst_ip\$ \$src_ip\$ bin _time span=5m eval tbrmb=Total_bytes_rcv/(1024*1024) eval tbsmb=Total_bytes_send/(1024*1024) timechart sum(tbrmb) as Megabytes_received sum(tbsmb) as Megabytes_sent</pre>

[Run Search](#)

Time Range Scope: Shared Time Picker (global) ▾

Cancel
Save



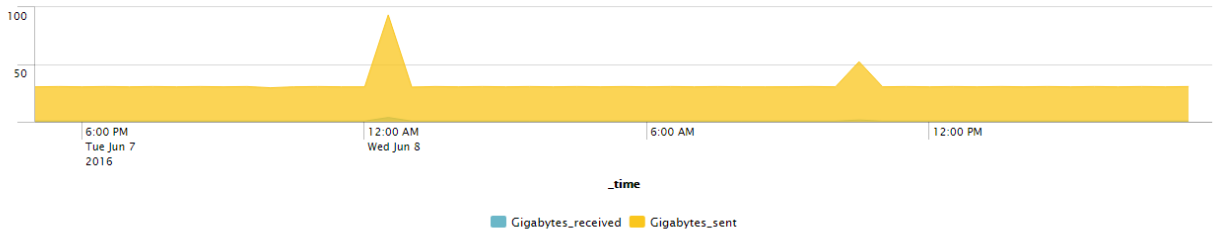


Load Balancing Dashboard

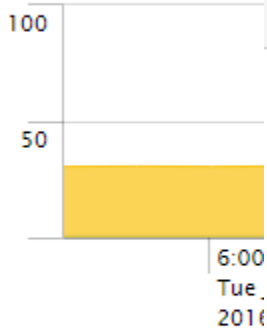
Edit More Info

Destination IP: *
 Destination Port: *
 Source IP: *
 Time Range: Last 24 hours
 Submit

Total Gigabytes



Total Gigabytes



Save As Report

Title:
 Description:
 Visualization: Line None
 Time Range Picker: Yes No

Open in Search



Cancel

Save

Edit Acceleration ✕

Report `netScaler:loadbalancer:throughput`

Accelerate Report
Acceleration may increase storage and processing costs.

Summary Range ? 1 Month ▾

Cancel Save

Edit Search ✕

Title	Total Gigabytes
Search String	<pre> search \$src_ip\$ \$dst_ip\$ timechart sum(tbrmb) as Gigabytes_received sum(tbsmb) as Gigabytes_sent</pre>

[Run Search](#)

Time Range Scope Explicit Selection ▾

Time Range All time ▶

Cancel Save



42



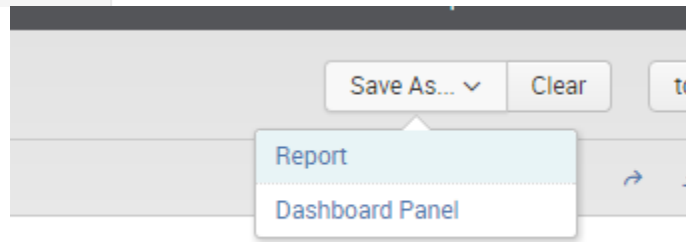
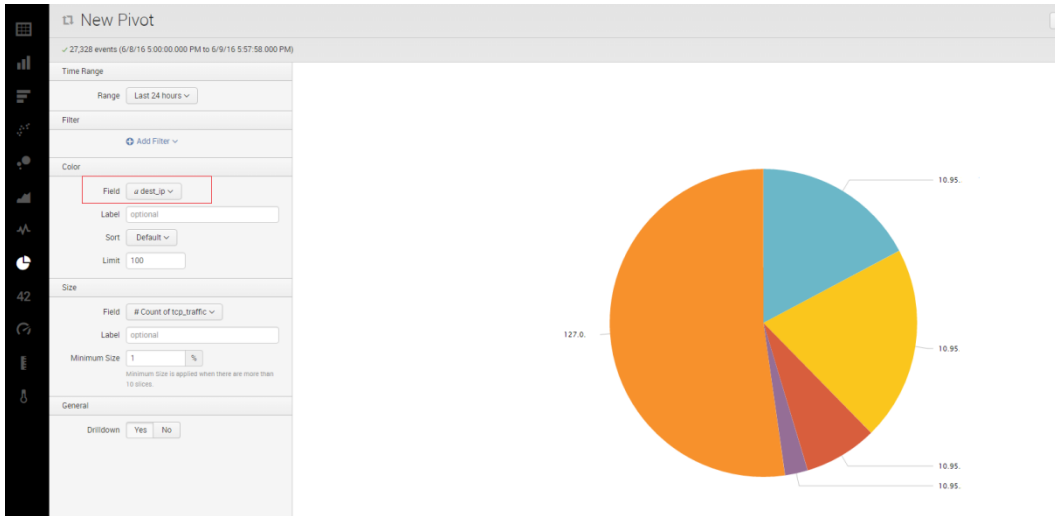
Select a Data Object

[< Back](#)

i 2 Objects in Top Stats

> [netscaler_events](#)

> [tcp_traffic](#)

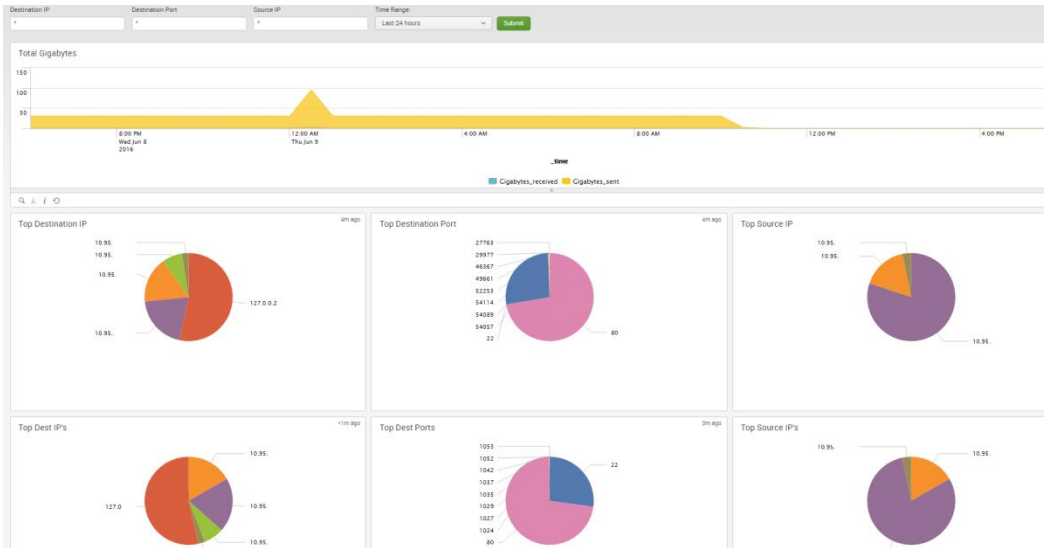


Save As Dashboard Panel

Dashboard:

Panel Title:

Panel Powered By:



Edit Search ✕

Title Top Dest IP's

Search String

```

I pivot top_stats tcp_traffic
count(tcp_traffic) AS "Count of
tcp_traffic" SPLITROW dest_ip AS
dest_ip FILTER dest_ip is "*" SORT 10
dest_ip ROWSUMMARY 0
COLSUMMARY 0 NUMCOLS 0
SHOWOTHER 1
  
```

[Run Pivot](#)

Time Range Scope

Performance Monitoring

Perfmon host: Perfmon Host (text search): Last 15 minutes

CPU Metrics Instance: All Counter: % C1 Time

Host	Trend	Average	Peak	Current
...		94.08	100.00	100
...		95.20	100.00	98
...		95.86	100.00	98
...		96.88	100.00	97
...		94.61	100.00	97
...		91.44	99.98	96
...		92.00	100.00	95
...		93.16	99.18	95
...		93.96	99.21	95
...		92.32	100.00	95

Memory Metrics Counter: % Committed Bytes In Use

Host	Trend	Average	Peak	Current
...		84.35	84.50	84
...		74.46	76.42	74
...		54.59	55.39	53
...		54.01	54.47	53
...		51.92	52.60	52
...		51.68	51.80	51
...		47.94	48.05	47
...		47.30	47.37	47
...		46.93	47.94	46
...		46.07	46.86	45

Performance Monitoring

Perfmon host: Perfmon Host (text search): Last 15 minutes

CPU Metrics Instance: All Counter: % C1 Time

Host	Trend	Average	Peak	Current
...		94.08	100.00	100
...		95.20	100.00	98
...		95.86	100.00	98
...		96.88	100.00	97
...		94.61	100.00	97
...		91.44	99.98	96
...		92.00	100.00	95
...		93.16	99.18	95
...		93.96	99.21	95
...		92.32	100.00	95

Memory Metrics Counter: % Committed Bytes In Use

Host	Trend	Average	Peak	Current
...		84.35	84.50	84
...		74.46	76.42	74
...		54.59	55.39	53
...		54.01	54.47	53
...		51.92	52.60	52
...		51.68	51.80	51
...		47.94	48.05	47
...		47.30	47.37	47
...		46.93	47.94	46
...		46.07	46.86	45

Edit: windows performance

Perfmon Host Perfmon Host (text search) Last 15 minutes

Dynamic Options

Content Type

Search String

[Run Search](#)

Field For Label ?

Field For Value ?

Apply

CPU Metrics

Instance: All Counter: % C1 Time

Host	Trend	Average	Peak	Current	Last Updated
		98.10	100.00	98.52	06/22/2016 15:02:53
		96.60	100.00	98.02	06/22/2016 15:01:20
		97.71	100.00	97.85	06/22/2016 15:02:16
		96.48	100.00	97.61	06/22/2016 15:02:27
		95.94	100.00	97.54	06/22/2016 15:02:25
		95.70	100.00	97.35	06/22/2016 15:03:02
		96.68	99.61	96.17	06/22/2016 15:01:10
		93.83	99.67	95.63	06/22/2016 15:02:56
		95.19	100.00	95.06	06/22/2016 15:03:08
		94.07	95.93	94.78	06/22/2016 15:02:22

« prev 1 2 3 4 next »

Untitled

Instance: All Counter: % C1 Time

CPU

Host	Trend	Average	Peak	Current	Last Updated
1		97.03	100.00	98.18	06/22/2016 15:35:52
2		96.87	100.00	97.83	06/22/2016 15:36:24
3		97.31	100.00	97.61	06/22/2016 15:36:16
4		96.43	100.00	97.23	06/22/2016 15:35:35
5		96.20	99.90	97.14	06/22/2016 15:35:27
6		95.80	99.98	96.70	06/22/2016 15:35:56
7		96.68	100.00	96.64	06/22/2016 15:34:21
8		93.97	98.95	96.57	06/22/2016 15:35:10
9		91.57	98.85	96.34	06/22/2016 15:35:23
10		96.50	99.88	96.03	06/22/2016 15:35:27

« prev 1 2 3 4 next »

General

Token Options

Token Prefix ?

Token Suffix ?

Static Options

Name	Value
<input type="text" value="All"/>	<input type="text" value="*"/>

[Add Option](#)

Dynamic Options

Content Type

Search String

[Run Search](#)

Field For Label ?

T Text

Radio

▼ Dropdown

Checkbox

▼ Multiselect

Time

General

Token Options

Token ?

Default ?

[Clear Selection](#)

Token Prefix ?

Token Suffix ?

Static Options

Name	Value
<input type="text"/>	<input type="text"/>

[Add Option](#)

Dynamic Options

Content Type

Search String

Perfmon Host token=host

Perfmon Host (text search) token=txtsch

token=hist

Instance token=inst1

Counter token=cntr1

Edit Search



Title CPU

Search String

```
index=perfmon object="Processor"  
$host$ $txtsch$ $counter$ $instance$ |  
stats sparkline(avg(Value)) as Trend  
avg(Value) as Average, max(Value) as  
Peak, latest(Value) as Current,  
latest(_time) as "Last Updated" by Host  
| convert ctime("Last Updated") | sort -  
Current | eval Average=round(Average,  
2) | eval Peak=round(Peak, 2) | eval  
Current=round(Current, 2)
```

[Run Search](#)

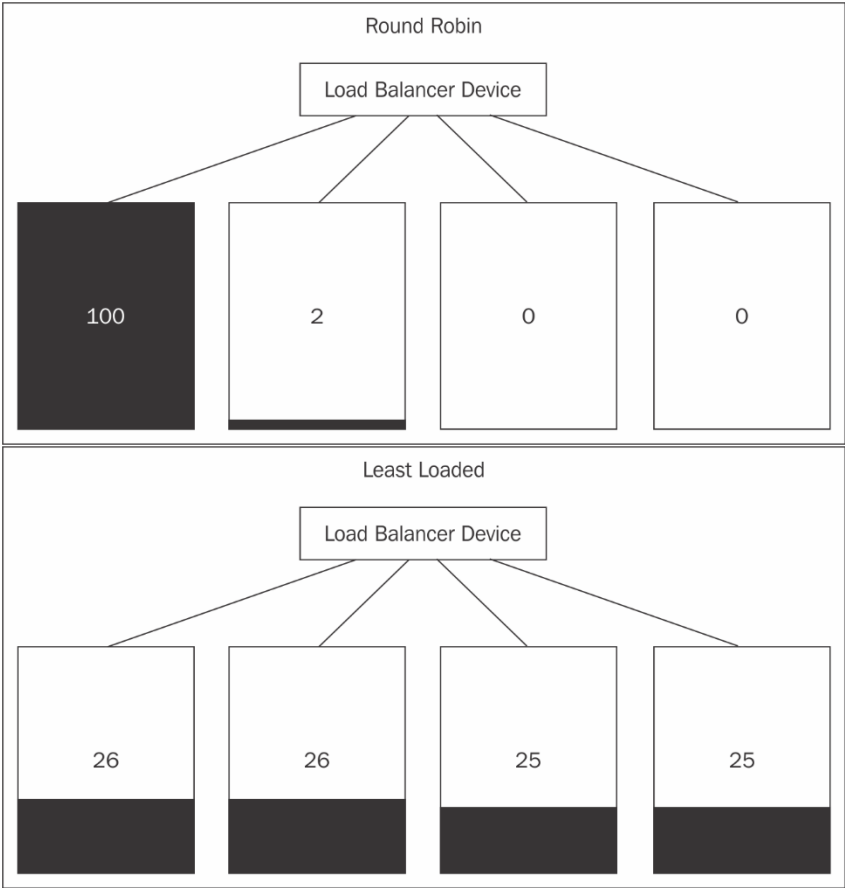
Time Range Scope

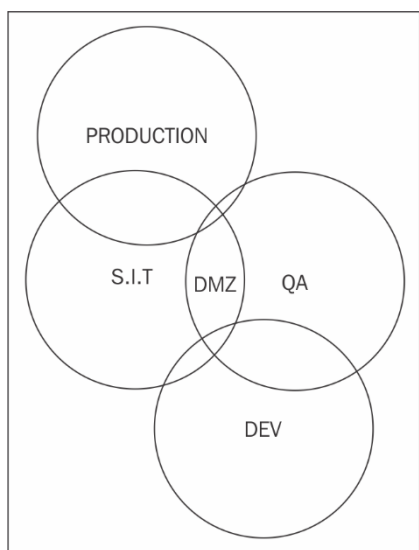
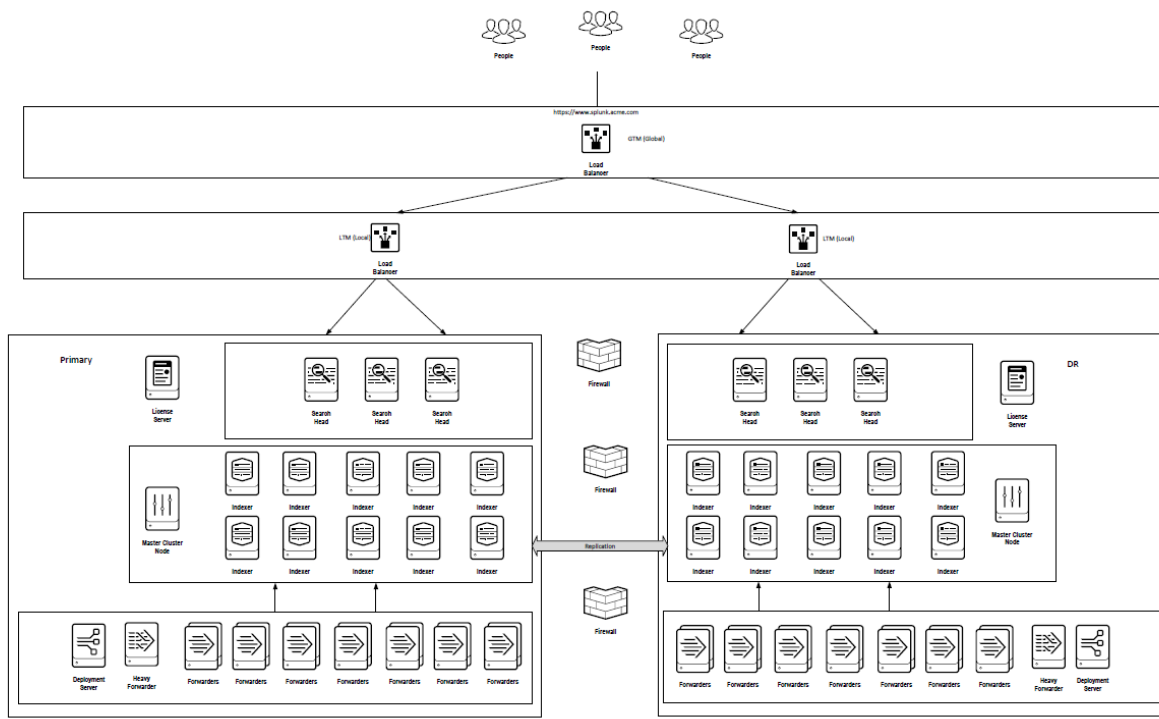
Shared Time Picker (hist) ▾

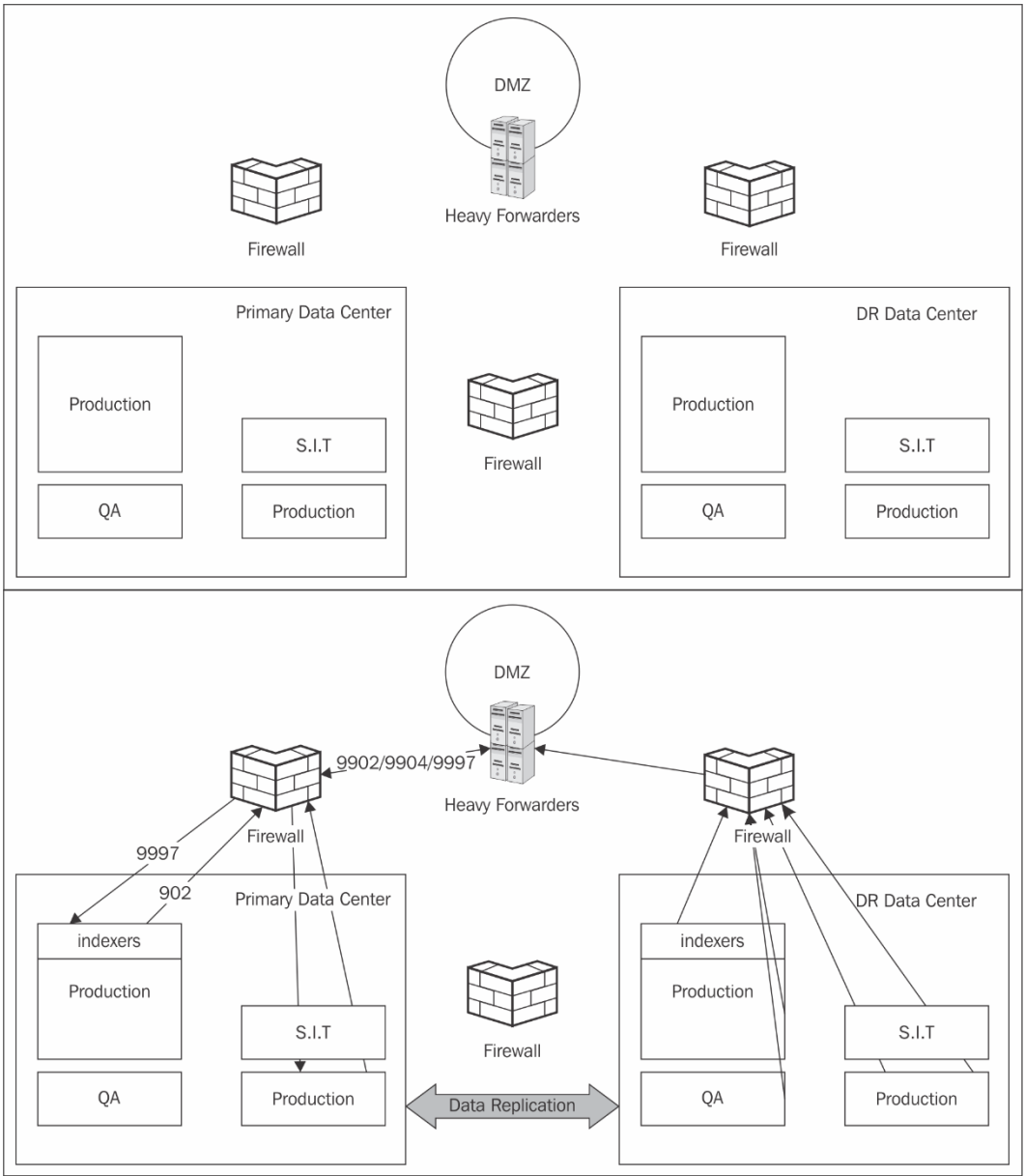
Cancel

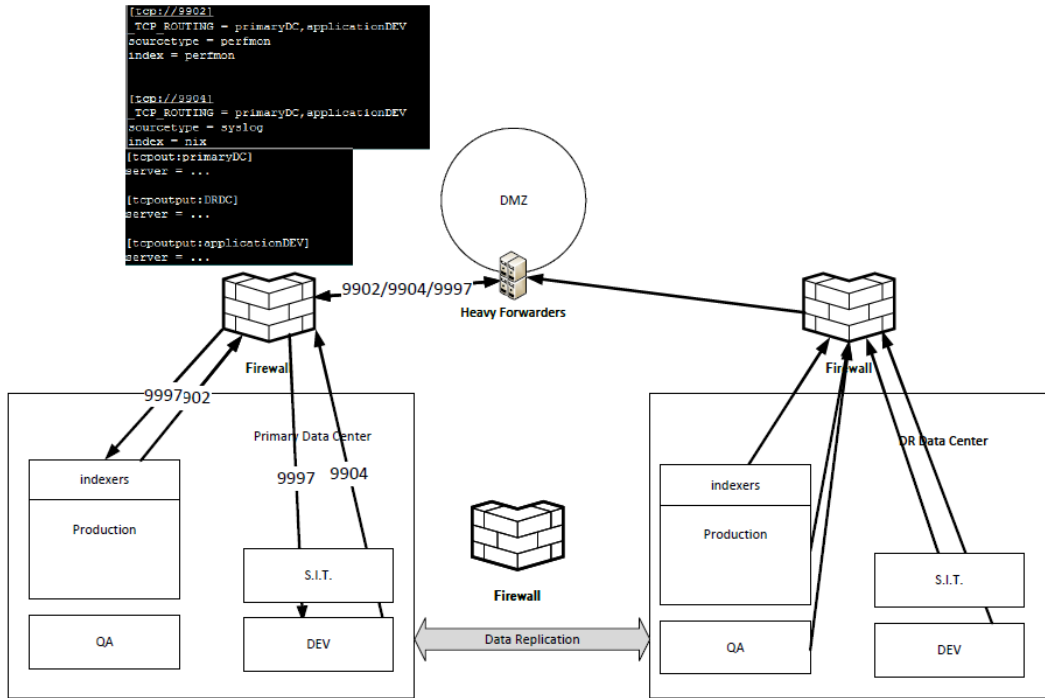
Save

Chapter 10: Advanced Data Routing









```
[top://9902]
TCP_ROUTING = primaryDC,applicationDEV
sourcetype = perfmon
index = perfmon

[top://9904]
TCP_ROUTING = primaryDC,applicationDEV
sourcetype = syslog
index = nix
[tcput:primaryDC]
server = ...

[tcput:DRDC]
server = ...

[tcput:applicationDEV]
server = ...
```

```
Windows perfmon:
[perfmon://CPU]
TCP_ROUTING = dmz_perfmon
counters = *
disabled = 0
instances = *
interval = 60
object = Processor
useEnglishOnly=true

Linux Syslog:
[monitor:///var/log/]
TCP_ROUTING = dmz_nix
whitelist=(messages|secure|auth|mesg|cron$|acpid$)
blacklist=(lastlog|anaconda|.syslog)
disabled = 0

[tcput:dmz_perfmon]
server = ...

[tcput:dmz_nix]
server = ...
```