

What's New in 6.6

The other cool stuff!

```
COMMAND
32616 splunkd
32695 tcpdump
590 named
1602 vim
1243 python

%CPU USER      UID      TIME+  %MEM  PR  NI  VIRT  RES  SHR  S  PPID  RSS  RUSR  RDSR  ST
0.3 splunk  1000    0:02.80 4.3  20  0  135356 43956 8948 S  1  2888  splunk  2888  2888  splunk
0.3 tcpdump  72     0:02.45 0.7  20  0  28588  6872  5464 S  32688  72  tcpdump  72  72  tcpdump
0.3 named    25     7:31.12 1.8  20  0  548272 18872 5584 S  1  25  named    25  25  named
0.3 dan     1028   0:00.08 0.6  20  0  152828  6248  2548 S  38588 1828  dan     38588 1828  dan
```

New SPL commands, and extensions to others!

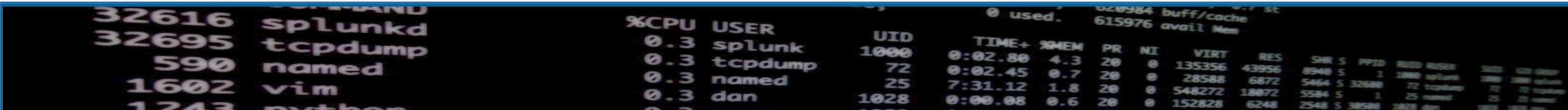
- Union: Used with datasets to merge them together:
<http://docs.splunk.com/Documentation/Splunk/6.6.0/SearchReference/Union>
- The SQL-like “IN” operator
<http://docs.splunk.com/Documentation/Splunk/6.6.0/SearchReference/ConditionalFunctions#in.28VALUE-LIST.29>
 - Used with “eval”, “where” command, against a list of values
 - ... | where status in("400", "401", "403", "404")

A terminal window showing system statistics and a process list. The top part shows memory usage: 0 used, 615976 avail Mem. Below that is a table of processes with columns for PID, COMMAND, %CPU, USER, and UID. The processes listed are splunkd (PID 32616), tcpdump (PID 32695), named (PID 590), vim (PID 1602), and others (PID 1243).

PID	COMMAND	%CPU	USER	UID
32616	splunkd	0.3	splunk	1000
32695	tcpdump	0.3	tcpdump	72
590	named	0.3	named	25
1602	vim	0.3	dan	1028
1243	others	0.3		

Search Head Clustering Improvements

- Outputlookup improvements
 - Can now allow for multi-value fields
- A GUI!
 - Available on all members
 - Only shows up when using a cluster
 - Allows for rolling restarts, captain transfer
 - All members must be on 6.6
- Deployment
 - Captain first
 - No .index on large lookups are replicated
 - Warnings on built-in apps
- Message Improvements
 - Now propagate to all members
- Replication Improvements
 - Avoids some bugs related to JSON object length
 - Available as a config item



The image shows a terminal window with two sections of output. The top section shows system memory usage: 0 used, 615976 avail Mem. The bottom section shows a process list with columns for PID, USER, %CPU, and UID.

PID	USER	%CPU	UID
32616	splunkd	0.3	1000
32695	tcpdump	0.3	72
590	named	0.3	25
1602	vim	0.3	1028
1243	python	0.3	1028

Indexer Clustering Improvements

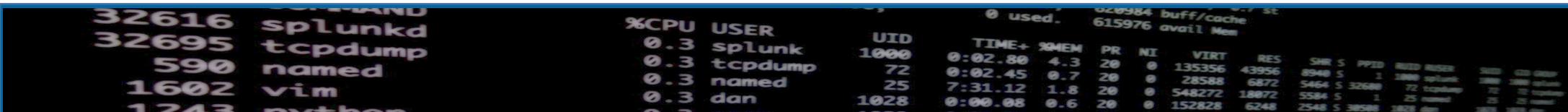
- Take a node offline without search disruption
- Faster indexer recovery
- Avoid data coming in to indexers in manual detention
- Bundle rollback
 - http://docs.splunk.com/Documentation/Splunk/6.6.0/Indexer/Updatepeerconfigurations#Rollback_the_configuration_bundle
- No restart on new app deployment on indexers
- Phased bundle downloads

A terminal window showing system statistics and a list of processes. The top part shows memory usage: 0 used, 620984 buff/cache, 615976 avail Mem. Below that is a table of processes with columns for PID, CPU, USER, UID, TIME+, MEM, PR, NI, VIRT, RES, SHR, S, PPID, PWD, RUSER, RGROUP, RSESSION, RUID, and RUSER.

PID	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	PWD	RUSER	RGROUP	RSESSION	RUID	RUSER
32616	0.3	splunkd	1000	0:02.80	4.3	20	0	135356	43956	8948	S	1	/usr/bin/splunk	splunk	splunk	1000	splunk	
32695	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32689	/usr/bin/tcpdump	tcpdump	tcpdump	72	tcpdump	
590	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	/usr/sbin/named	named	named	25	named	
1602	0.3	vim	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38588	/usr/bin/vim	vim	vim	1028	vim	
1243	0.3	python																

Forwarding Improvements

- Multi-site aware forwarding
 - Failover between sites for forwarders
 - Must be using indexer discovery
 - Only forward to the same site, unless the targets are unavailable
 - http://docs.splunk.com/Documentation/Splunk/6.6.0/Indexer/indexerdiscovery#Configure_the_forwarder_site_failover_capability
- Volume-based forwarding
 - You can balance by time (autoLB) or by volume (autoLBVolume) from outputs.conf
 - Or both! If the autoLBVolume has been reached, move to the next target, otherwise, stay until autoLBFrequency
 - Both should be used with EVENT_BREAKER
 - Don't set this or the frequency too low!
- S2S v2
 - Not as chatty with the indexers
 - Gets better notification of indexer shutdowns
- Force local processing
 - Only for parts of the pipeline
 - NOT RECOMMENDED
 - Forces it through the existing structured data pipeline



A terminal window showing system metrics and process information. The top part shows memory usage: 0 used, 615976 avail Mem. Below that is a table of processes with columns for PID, USER, %CPU, and UID. The processes listed are splunkd, tcpdump, named, vim, and dan.

PID	USER	%CPU	UID
32616	splunkd	0.3	1000
32695	tcpdump	0.3	72
590	named	0.3	25
1602	vim	0.3	1028
1243	dan	0.3	1028

Distributed Search Improvements

- SSL Session Reuse

```
useSslClientSessionCache = <bool>  
* Whether to re-use client session.  
* When set to true, client sessions are stored in memory for session re-use.  
  This reduces handshake time, latency and computation time to improve SSL performance.  
* When set to false, each ssl connection will perform full ssl handshake.  
* Defaults to false
```

- Large lookup improvements
 - Transforms.conf, index_fields_list

A terminal window showing system statistics and a process list. The top part shows memory usage: 0 used, 615976 avail Mem. Below that is a table of processes with columns for PID, COMMAND, %CPU, USER, UID, TIME+, MEM, PR, NI, VIRT, RES, SHR, S, PPID, PWD, RUSER, and other fields. The processes listed include splunkd, tcpdump, named, vim, and others.

PID	COMMAND	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	PWD	RUSER
32616	splunkd	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	/usr/local/splunk	splunk
32695	tcpdump	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32680	/72	tcpdump
590	named	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	/25	named
1602	vim	0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38588	/1028	vim

Pipeline Debugging Improvements

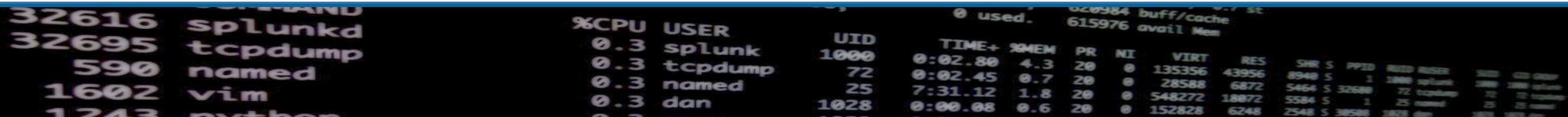
- regex_cpu_profiling
- Should only show on non-UF nodes

```
regex_cpu_profiling = <bool>
```

```
* Enable CPU time metrics for RegexProcessor. Output will be in the  
metrics.log file.
```

```
Entries in metrics.log will appear per_host_regex_cpu, per_source_regex_cpu,  
per_sourcetype_regex_cpu, per_index_regex_cpu.
```

```
* Default: false
```



PID	COMMAND	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	PPID	USER	MEM	MEM
32616	splunkd	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8948	S	1	2880	splunk	2880	2880
32695	tcpdump	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32680	72	tcpdump	72	72
590	named	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	25	named	25	25
1602	vim	0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38588	1602	dan	1602	1602
1243	python																

Better Outbound Proxy Support

- New config options
- If you use apps or add-ons that reach out to the internet
- proxyConfig in server.conf
- https://docs.splunk.com/Documentation/Splunk/6.6.0/Admin/Serverconf#Splunkd_http_proxy_configuration

```
02:09:84 buff/cache 0 used, 615976 avail Mem
```

	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	PPID	PPID	PPID	PPID	PPID	PPID	PPID
32616	0.3	splunkd	1000	0:02.80	4.3	20	0	135356	43956	8948	S	1	2888	splunkd	2888	2888	splunkd	2888	
32695	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32688	72	tcpdump	72	72	tcpdump	72	
590	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	25	named	25	25	named	25	
1602	0.3	vim	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38588	1602	vim	1602	1602	vim	1602	
1243	0.3	python																	

RemotePath in indexes.conf?

```
remotePath = <root path for remote volume, prefixed by a URI-like scheme>
```

- * Optional.
- * Presence of this parameter means that this index uses remote storage, instead of the local file system, as the main repository for bucket storage. The index processor works with a cache manager to fetch buckets locally, as necessary, for searching and to evict them from local storage as space fills up and they are no longer needed for searching.
- * This setting must be defined in terms of a storageType=remote volume definition. See the volume section below.
- * The path portion that follows the volume reference is relative to the path specified for the volume. For example, if the path for a volume "v1" is "s3://bucket/path" and "remotePath" is "volume:v1/idx1", then the fully qualified path will be "s3://bucket/path/idx1". The rules for resolving the relative path with the absolute path specified in the volume can vary depending on the underlying storage type.
- * If "remotePath" is specified, the "coldPath" and "thawedPath" attributes are ignored. However, they still must be specified.

COMMAND	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	PPID	PPID	PPID	PPID	PPID	PPID	PPID
32616 splunkd	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	3880	splunk	3880	3880	3880	3880	3880
32695 tcpdump	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32680	72	tcpdump	72	72	72	72	72
590 named	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	25	named	25	25	25	25	25
1602 vim	0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38588	1602	vim	1602	1602	1602	1602	1602
1243 python	0.3	python	1000	0:00.00	0.0	20	0	152828	6248	2548	S	38588	1243	python	1243	1243	1243	1243	1243

