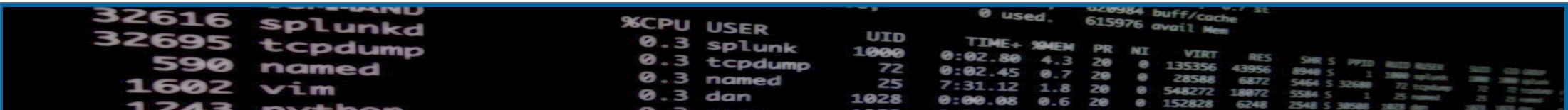
What’s New in 6.6

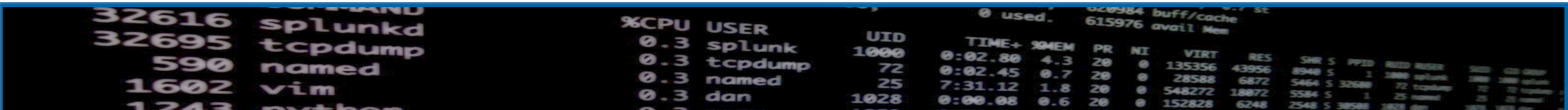
The other cool stuff!



Many Solutions, One Goal.

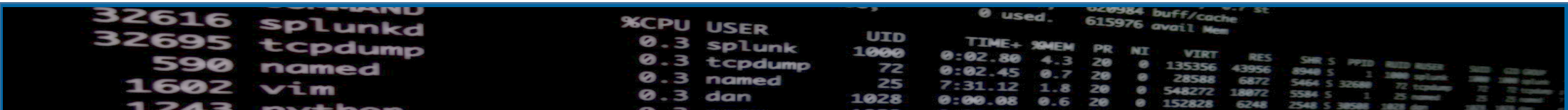
New SPL commands, and extensions to others!

- 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")



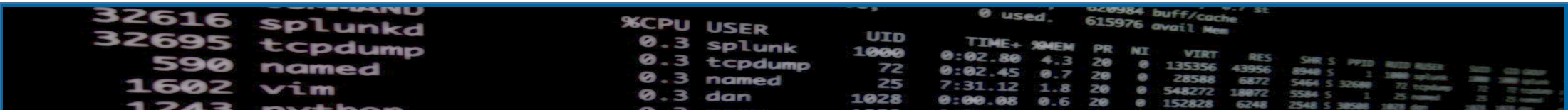
Search Head Clustering Improvements

- 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



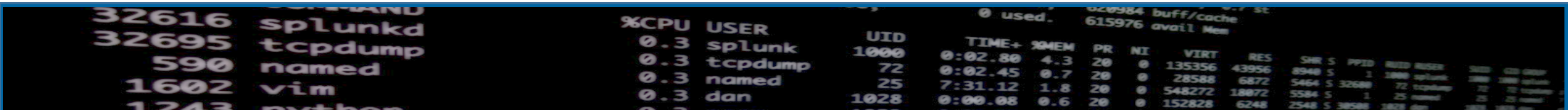
Indexer Clustering Improvements

- 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



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

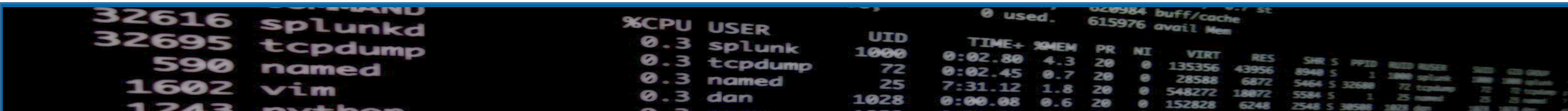


Distributed Search Improvements

- 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
```

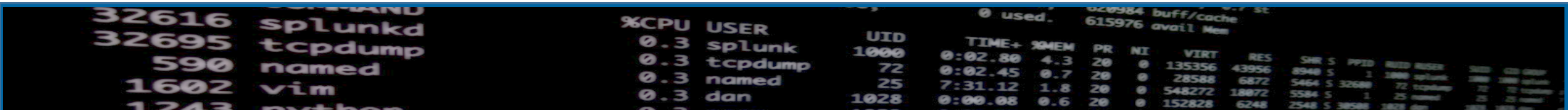
- Large lookup improvements
  - Transforms.conf, index_fields_list



Pipeline Debugging Improvements

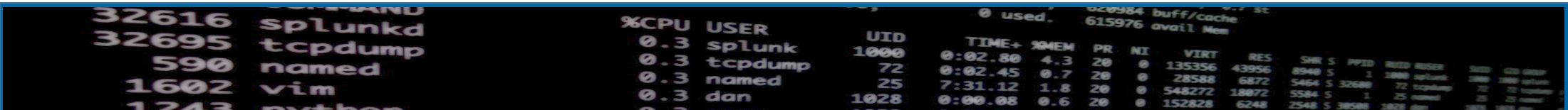
- regex_cpu_profiling
- Should only show on non-UF nodes

```
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
```



Data Model Acceleration Improvements

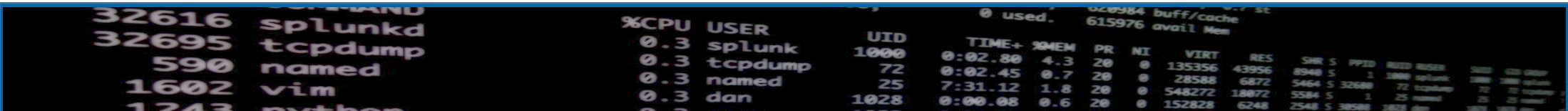
- Even if max_time was set, DMA used bucket boundries
- ”More” respect of max_time
- tags_whitelist
  - Datamodels.conf
  - http://docs.splunk.com/Documentation/Splunk/6.6.0/Knowledge/Designdatamodelobjects#Set_a_tag_whitelist_for_better_data_model_search_performance
  - Improves/prevents KO Explosion



Many Solutions, One Goal.

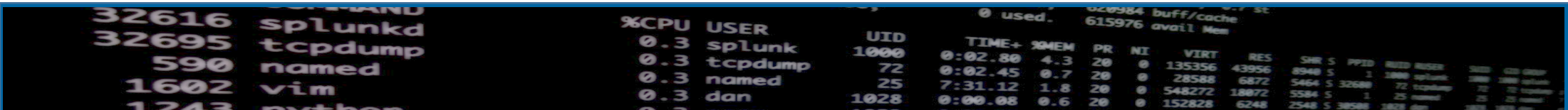
Better Outbound Proxy Support

- 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



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.
```

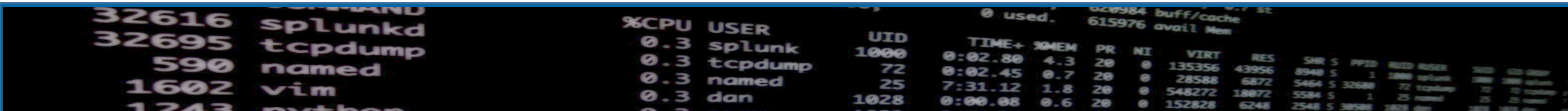


APLURA

Many Solutions, One Goal.

The default time range for Search is now "Last 24 hours". The previous default was "All time".

http://docs.splunk.com/Documentation/Splunk/6.6.0/ReleaseNotes/MeetSplunk



APLURA
Many Solutions, One Goal.