

What's New in Splunk 9.0

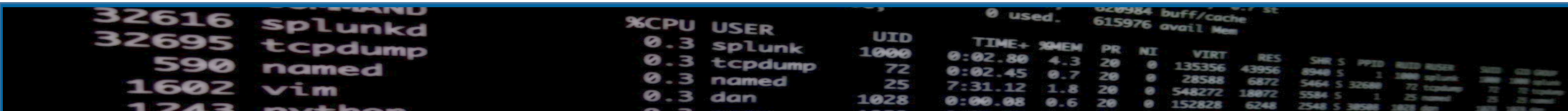
Dave Shpritz, Aplura Director of Services

Baltimore Splunk User Group

July 2022

Some modifications/additions, Ismo Soutamo, Data Findings Oy

Helsinki Splunk User Group, 31.8.2022



A terminal window showing system metrics and a process list. The top part shows memory usage: 0 used, 620984 buff/cache, 615976 avail Mem. Below that is a table with columns: %CPU, USER, UID, TIME+, %MEM, PR, NI, VIRT, RES. The process list includes:

%CPU	USER	UID	TIME+	%MEM	PR	NI	VIRT	RES
0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956
0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872
0.3	named	25	7:31.12	1.8	20	0	548272	18872
0.3	dan	1028	0:00.08	0.6	20	0	152828	6248



Many Solutions, One Goal.

Agenda

- Overview
- Security
- Indexing
- Admin
- Search
- Other stuff

```
020984 buff/cache 0 used, 615976 avail Mem
```

COMMAND	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	PID	PPID	USER	MEM	MEM	MEM
32616 splunkd	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	2880	2880	splunk	2880	2880	splunk
32695 tcpdump	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32680	72	72	tcpdump	72	72	tcpdump
590 named	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	25	25	named	25	25	named
1602 vim	0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38584	1602	1602	dan	1602	1602	dan
1243 other	0.3																	

Overview - Splunk Version 9.0.0

Latest versions are 9.0.1 and Splunk Cloud 9.0.2205.1 (31.8.2022)

- Released at .conf22
- Release Notes:
<https://docs.splunk.com/Documentation/Splunk/9.0.0/ReleaseNotes/MeetSplunk>
- Upgrade:
<https://docs.splunk.com/Documentation/Splunk/9.0.0/Installation/AboutupgradingREADTHISFIRST>
- Known Issues:
<https://docs.splunk.com/Documentation/Splunk/9.0.0/ReleaseNotes/Knownissues>

```
32616 splunkd
32695 tcpdump
590 named
1602 vim
1243 other

%CPU USER      UID      TIME+  %MEM  PR  NI  VIRT  RES  SHR  S  PPID  RSS  RSSD  RSSM  RSSV  RSSO  RSSP  RSSC  RSSM  RSSV  RSSO  RSSP  RSSC
0.3  splunk  1000    0:02.80  4.3  20  0  135356  43956  8940  S  1  2880  splunk  1000  1000  splunk
0.3  tcpdump  72     0:02.45  0.7  20  0  28588  6872  5464  S  32680  72  tcpdump  1000  1000  tcpdump
0.3  named    25     7:31.12  1.8  20  0  548272  18072  5584  S  1  25  named    1000  1000  named
0.3  dan     1028    0:00.08  0.6  20  0  152828  6248  2548  S  38580  1812  dan     1000  1000  dan
```

Security

```
020984 buff/cache 0 used, 615976 avail Mem
%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 8940 S  1  2880 1000 1000 0000
0.3 tcpdump   72     0:02.45 0.7  20  0  28588  6872  5464 S  72  1000  72  72  0000
0.3 named     25     7:31.12 1.8  20  0  548272 18872 5584 S  1  25  1000  25  25  0000
0.3 dan      1028    0:00.08 0.6  20  0  152828  6248  2548 S  38584 1828 0000
```



Security

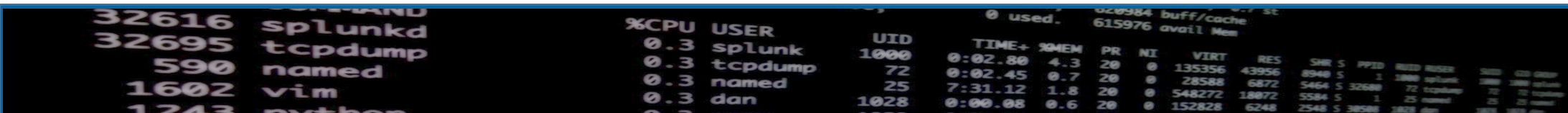
- Security vulnerabilities
- TLS changes
- Audit improvements/Config Tracking
- Universal Forwarder
- Role-based fields

```
020984 buff/cache 0 used, 615976 avail Mem
```

PID	PPID	USER	%CPU	MEM	PR	NI	VIRT	RES	SHR	S	PPID	RUSER	RUID	GROUP
32616		splunkd	0.3		20	0	135356	43956	8940	S	1	splunkd	1000	splunk
32695		tcpdump	0.3	4.3	20	0	28588	6872	5464	S	72	tcpdump	72	tcpdump
590		named	0.3	0.7	20	0	548272	18872	5584	S	1	named	25	named
1602		vim	0.3	1.8	20	0	152828	6248	2548	S	38584	vim	1028	vim
1243		python	0.3	0.6	20	0				S				

Vulnerabilities

- Quarterly security patches
- Deployment server/client
 - [SVD-2022-0608](#), [SVD-2022-0607](#)
- TLS
 - [SVD-2022-0606](#), [SVD-2022-0603](#), [SVD-2022-0602](#), [SVD-2022-0601](#)
- UFs
 - [SVD-2022-0605](#)
- Risky commands
 - [SVD-2022-0604](#)
- More info:
 - https://www.splunk.com/en_us/product-security.html
 - https://lantern.splunk.com/Splunk_Platform/Product_Tips/Enterprise/Upgrading_Splunk_Enterprise



A terminal window showing system metrics and a process list. The top part shows memory usage: 0 used, 615976 avail Mem. Below that is a table with columns: %CPU, USER, UID, TIME+, %MEM, PR, NI, VIRT, RES. The table lists several processes including splunkd, tcpdump, named, vim, and dan.

%CPU	USER	UID	TIME+	%MEM	PR	NI	VIRT	RES
0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956
0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872
0.3	named	25	7:31.12	1.8	20	0	548272	18872
0.3	dan	1028	0:00.08	0.6	20	0	152828	6248

Deployment Server/Client

Deployment servers allow client publishing of bundles (SVD-2022-0608)

- Super bad
- Allows anything on your network to tell the DS to publish an app
- No detection searches
- Mitigate yesterday!
- Backported to 8.1 and 8.2 (the only one of these that was)

Deployment servers allow unauthenticated bundle access (SVD-2022-0607)

- Anyone can grab apps
- Previous pass4symmkey implementation not effective
- New pass4symmkey, but requires v9 clients
- Certificate validation

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

%CPU USER      UID      TIME+  %MEM  PR  NI  VIRT  RES  SHR  S  PPID  RSS  RSSD  RSSM  RSSV  RSSO  RSSP  RSSC  RSSD  RSSM  RSSV  RSSO  RSSP  RSSC
0.3  splunk  1000    0:02.80  4.3  20  0  135356  43956  8940  S  1  2888  2888  2888  2888  2888  2888  2888  2888  2888  2888  2888  2888  2888
0.3  tcpdump  72     0:02.45  0.7  20  0  28588  6872  5464  S  1  72  72  72  72  72  72  72  72  72  72  72  72  72  72
0.3  named    25     7:31.12  1.8  20  0  548272  18872  5584  S  1  25  25  25  25  25  25  25  25  25  25  25  25  25  25
0.3  dan     1028    0:00.08  0.6  20  0  152828  6248  2548  S  1  25  25  25  25  25  25  25  25  25  25  25  25  25  25
```

TLS

- [SVD-2022-0606, SVD-2022-0603, SVD-2022-0602, SVD-2022-0601](#)
- All present similar issues, that is, Splunk wasn't validating certificates correctly
- New TLS docs!
- [https://docs.splunk.com/Documentation/Splunk/9.0.0/Security/AboutsecuringyourSplunkconfigurationwithSSL](#)

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

%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	PPID	NAME	MEM	MEM	MEM
0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	2888	splunk	2888	2888	splunk
0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32689	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	1028	dan	1028	1028	dan

Universal Forwarders

- [SVD-2022-0605](#)
- Once you set a password, remote login is allowed by default
- Splunk 9 changes that
- No longer binding to all IPs, just localhost
- You can pull the same trick on older versions

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

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

Risky ~~Business~~ Commands

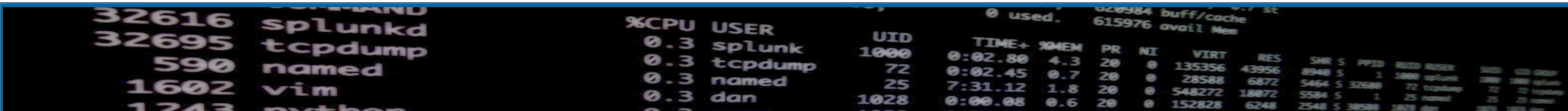
- [SVD-2022-0604](#)
- Attacker using a compromised browser could inject commands
- Turn off your GUIs (indexers, for example, maybe your DS)
- [New capabilities in Splunk 9](#)

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

%CPU USER      UID      TIME+  %MEM  PR  NI  VIRT  RES  SHR  S  PPID  RSS  RSIZE  RUSER  SUID  GID  GROUP
0.3 splunk  1000    0:02.80  4.3  20  0  135356  43956  8940  S  1  2880  splunk  2880  2880  splunk
0.3 tcpdump  72     0:02.45  0.7  20  0  28588  6872  5464  S  32680  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  38580  1628  dan  38580  1628  dan
```

Audit improvements/Config Tracking

- New internal index, `_configtracker`, only admin can search by default
- Some fields are ignored, if they are sensitive
- Monitors:
 - `$(SPLUNK_HOME)/etc/system`
 - `$(SPLUNK_HOME)/etc/apps`
 - `$(SPLUNK_HOME)/etc/users`
 - `$(SPLUNK_HOME)/etc/slave-apps`
 - `$(SPLUNK_HOME)/etc/instance.cfg`
- You can add configs you want ignored
- [https://docs.splunk.com/Documentation/Splunk/9.0.0/Troubleshooting/WhatSplunklogsaboutitself#Configuration Change Tracker](https://docs.splunk.com/Documentation/Splunk/9.0.0/Troubleshooting/WhatSplunklogsaboutitself#Configuration%20Change%20Tracker)

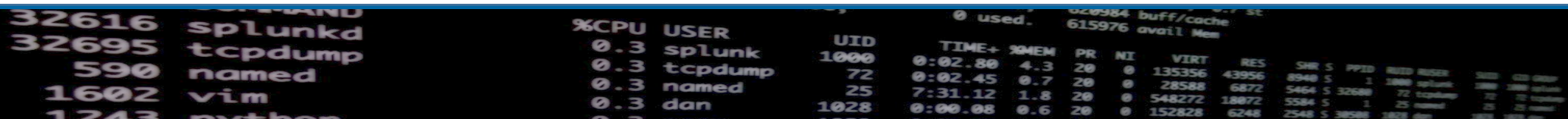


The image shows a terminal window with two sections of output. The top section shows system memory usage: 0 used, 615976 avail Mem. The bottom section shows a list of processes with columns for PID, USER, %CPU, and UID.

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	

Universal Forwarder Security Improvements

- Config changes now monitored by default
- Windows Managed Service Accounts
- Automatic password generation on Windows
- Linux use of capabilities for a least-privilege install
 - <https://docs.splunk.com/Documentation/Forwarder/9.0.0/Forwarder/Install#eastprivileged>
- Management interface now binds to localhost by default
- Native collection of MacOS Unified Logging



A terminal window showing system metrics and a list of processes. The top part shows system statistics like CPU usage and memory. Below that is a table of running processes with columns for PID, command, %CPU, USER, UID, TIME+, %MEM, PR, NI, VIRT, and RES.

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

Role-based fields

- Preview feature. Currently provided “as is”, no support
- Can filter or mask
- Allows you to mask fields using SEDCMD-like syntax for obfuscation
- Can replace with hashes to allow for value-based searches/stats
- <https://docs.splunk.com/Documentation/Splunk/9.0.0/Security/setfilefiltering>

```
0 used, 615976 avail Mem
%CPU USER      UID      TIME+  %MEM  PR  NI  VIRT  RES  SHR  S  PPID  RSS  RSIZE  STATE  CWD  PID  NAME
0.3 splunk    1000    0:02.80  4.3  20  0  135356  43956  8940  S  1  2888  2888  2888  2888  /usr/bin/splunkd
0.3 tcpdump   72      0:02.45  0.7  20  0  28588  6872  5464  S  1  72  72  72  72  /usr/sbin/tcpdump
0.3 named     25      7:31.12  1.8  20  0  548272  18872  5584  S  1  25  25  25  25  /usr/sbin/named
0.3 dan      1028    0:00.08  0.6  20  0  152828  6248  2548  S  1  38588  1828  4000  25  /usr/sbin/dan
```

Indexing

```
020984 buff/cache 0 used, 615976 avail Mem
```

PPID	PID	USER	%CPU	MEM	TIME+	PR	NI	VIRT	RES	SHR	S	PPID	PPID	USER	%CPU	MEM	TIME+	PR	NI	VIRT	RES	SHR	S	
32616	32616	splunkd	0.3		0:02.80	20	0	135356	43956	8940	S	1	3880	splunk	0.3		0:02.45	20	0	548272	18872	5584	S	1
32695	32695	tcpdump	0.3		7:31.12	20	0	28588	6872	5464	S	72	72	tcpdump	0.3		0:00.08	20	0	152828	6248	2548	S	38584
590	590	named	0.3											named	0.3									
1602	1602	vim	0.3											vim	0.3									
1243	1243	python	0.3											python	0.3									

Indexing

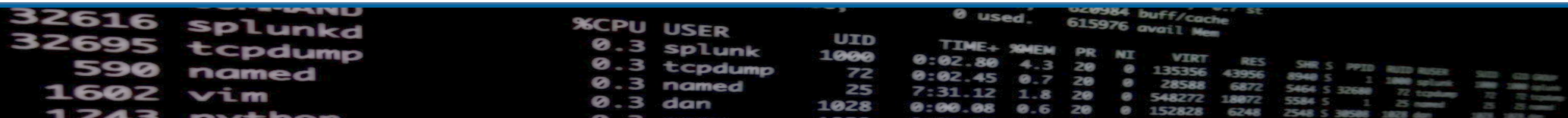
- Ingest Actions
- Indexer Manager HA
- Bucket Merging
- Azure SmartStore
- TSIDX compression in SmartStore
- TSIDX writing level

```
020984 buff/cache 0 used, 615976 avail Mem
```

COMMAND	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	RUID	RUSER	ST	ST	ST	ST
32616 splunkd	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	2880	splunk	2880	2880	splunk	
32695 tcpdump	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32680	72	tcpdump	72	72	tcpdump	
590 named	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	25	named	25	25	named	
1602 vim	0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38584	1028	dan	1028	1028	dan	
1243 python	0.3																	

Ingest Actions

- Biggest change to the Splunk pipelines since 7.3
- Allows you more flexibility with data
- Only in Linux
- You can drop, mask, route (including S3!)
- Competes with Cribl, sort of
- Like TRANSFORMS, SEDCMD, but with a shiny interface (with previews, sometimes)
- Index Manager and Deployment Server deployment methods
- Even works on cooked events!
- <https://docs.splunk.com/Documentation/Splunk/latest/Data/DataIngest>

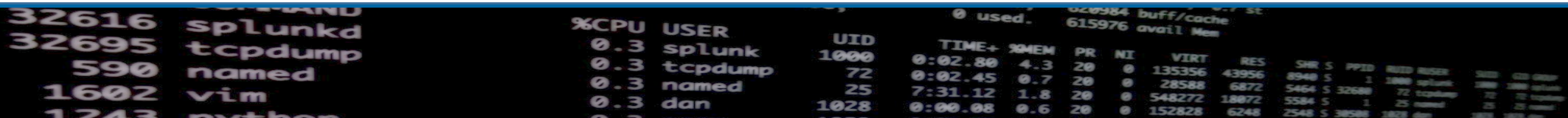


A terminal window showing system metrics and a process list. The top part shows memory usage: 0 used, 615976 avail Mem. Below that is a table with columns: %CPU, USER, UID, TIME+, %MEM, PR, NI, VIRT, RES. The table lists processes like splunkd, tcpdump, named, vim, and others.

%CPU	USER	UID	TIME+	%MEM	PR	NI	VIRT	RES
0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956
0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872
0.3	named	25	7:31.12	1.8	20	0	548272	18872
0.3	dan	1028	0:00.08	0.6	20	0	152828	6248

Ingest Actions - pipeline changes

- Uses the existing regexreplace processor
- Also hooked up from the TCP in for cooked events
- Applies after other transforms
- New DestinationKey in indexing pipelines for output to S3
- S3 only works on AWS, saves to a format called "HEC json"
- Can be used for re-ingest, but no index-time fields other than standard metadata (minus index)
- New metrics (disabled by default, can enable per ruleset)

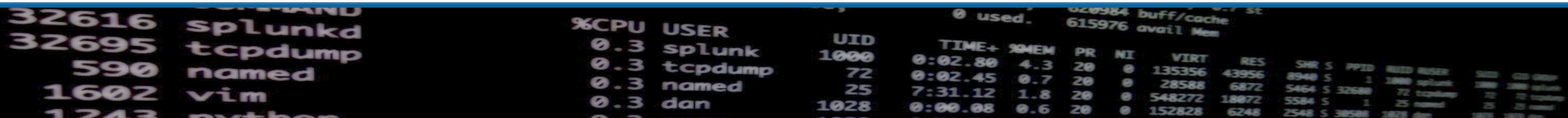


A terminal window showing system metrics and a process list. The top part shows memory usage: 0 used, 615976 avail Mem. Below that is a table with columns: %CPU, USER, UID, TIME+, %MEM, PR, NI, VIRT, RES, SHR, S, PPID, RSS, RSS_MAX, VSZ, VSZ_MAX. The process list includes:

%CPU	USER	UID	TIME+	%MEM	PR	NI	VIRT	RES	SHR	S	PPID	RSS	RSS_MAX	VSZ	VSZ_MAX
0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8948	S	1	2888	2888	3280	3280
0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32688	72	12288	72	12288
0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	25	25	25	25
0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38588	1828	1828	25	25

Ingest Actions – Deployment (CM)

- Interface on Cluster Manager allows for preview and deployment
- Interface allows S3 config
- Deployment is just the standard bundle push, so look out for undeployed changes!
- New rulesets don't require rolling restart, but change/remove does (right now)
- New app: splunk_ingest_actions
- New capabilities: list_ingest_ruleset, edit_ingest_ruleset

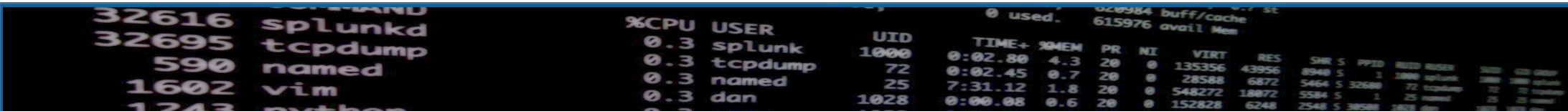


A terminal window showing system metrics and a process list. The top part shows memory usage: 0 used, 615976 avail Mem. Below that is a table of processes with columns for PID, COMMAND, %CPU, USER, UID, TIME+, %MEM, PR, NI, VIRT, RES, SHR, S, PPID, PWD, RUSER, RGROUP, RSESSION, RUID, RUSERGROUP, RUSERSESSION.

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

Ingest Actions – Deployment (DS)

- No configuration of S3
- Only supports Linux HF (pipelines may be on UFs, but not tested)
- Currently only supports 10 HFs
- **Dedicated DS!**
 - The deployment server must be dedicated to the ingest actions function and cannot be used for other types of deployment client configurations. The deployment server cannot service any other deployment clients.
- Even visiting the UI creates a new serverclass “IngestAction_AutoGenerated”
- Careful adding rulesets to a TA and then deploying it from your normal DS or to everywhere. Double processing is a thing.

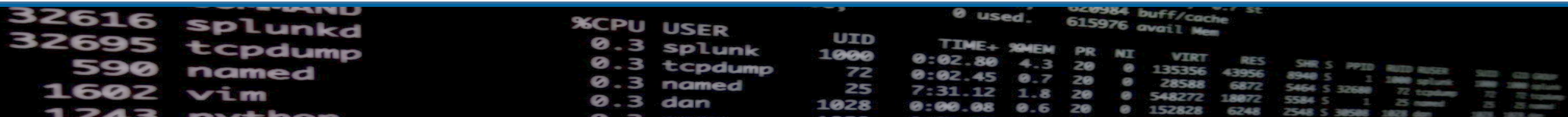


A terminal window showing system metrics and a process list. The top part shows memory usage: 0 used, 615976 avail Mem. Below that is a table with columns: %CPU, USER, UID, TIME+, %MEM, PR, NI, VIRT, RES, SHR, S, PPID, PWD, NAME. The process list includes:

%CPU	USER	UID	TIME+	%MEM	PR	NI	VIRT	RES	SHR	S	PPID	PWD	NAME
0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8948	S	1	/usr/bin	splunk
0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32688	/usr/bin	tcpdump
0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	/usr/sbin	named
0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38588	/usr/bin	vim

Cluster Manager HA

- CM was a single point of failure
- Used to have to sync/failover manually, but some things were in memory, so left behind
- Uses an active/passive topology
- Bundles, generation, peers get synced (bucket list not included)
- Configurable heartbeat
- With a load balancer in front of your CM, this can be automated
- Can also be done with DNS entries, but that would be manual
- New tab in the Indexer Clustering dashboard shows status (in a passive node, that is all you get)
- <https://docs.splunk.com/Documentation/Splunk/9.0.0/Indexer/CMredundancy>



The image shows a terminal window with system status information and a process list. The top part shows memory usage: 0 used, 620984 buff/cache, 615976 avail Mem. Below that is a process list with columns for PID, USER, %CPU, and UID. The processes listed are splunkd (32616), tcpdump (32695), named (590), vim (1602), and others (1243).

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	others	0.3	

Bucket Merging

- cluster-merge-buckets command
- Can be used to merge smaller buckets for a reduced overall bucket count
- Covers DMA
- Dry run, backup, runtime limitations
- <https://docs.splunk.com/Documentation/Splunk/9.0.0/Troubleshooting/CommandlinetoolsforusewithSupport#:~:text=cluster%2Dmerge%2Dbuckets,the%20old%20buckets%20are%20removed>

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

%CPU USER      UID      TIME+  MEM PR NI  VIRT  RES
0.3 splunk  1000  0:02.80 4.3 20 0 135356 43956
0.3 tcpdump  72    0:02.45 0.7 20 0 28588  6872
0.3 named    25    7:31.12 1.8 20 0 548272 18872
0.3 dan     1028  0:00.08 0.6 20 0 152828  6248
```

Azure SmartStore

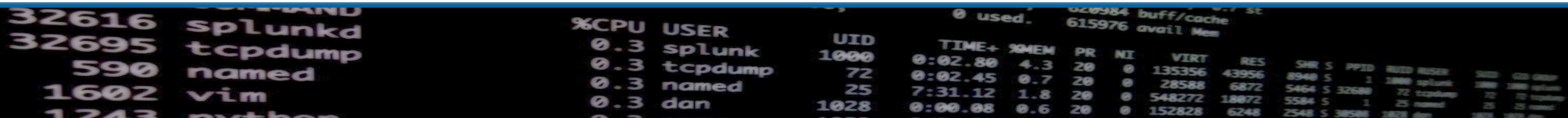
- SmartStore (S2) now can be done natively in Azure
- Uses Azure Blobs
- Not a ton of docs
- [https://docs.splunk.com/Documentation/Splunk/9.0.0/Indexer/ConfigureAzureremotestoreforSmartStore#Configure an Azure Blob remote store](https://docs.splunk.com/Documentation/Splunk/9.0.0/Indexer/ConfigureAzureremotestoreforSmartStore#Configure%20an%20Azure%20Blob%20remote%20store)

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

%CPU USER      UID      TIME+  %MEM  PR  NI  VIRT  RES  SHR  S  PPID  RSSZ  RUSER  STATE  ADDR
0.3 splunk  1000    0:02.80 4.3  20  0  135356 43956 8940 S  1  2888  splunk  2888  splunk
0.3 tcpdump  72     0:02.45 0.7  20  0  28588  6872  5464 S  1  72  tcpdump  72  tcpdump
0.3 named    25     7:31.12 1.8  20  0  548272 18872 5584 S  1  25  named    25  named
0.3 dan     1028    0:00.08 0.6  20  0  152828  6248  2548 S  1  25  dan      25  dan
```

TSIDX compression in SmartStore

- Save storage space/transit for S3
- Compression/decompress is transparent, done on the wire
- Average compression ratio is 50%
- Basic config, just need to turn it on
- Only works on AWS S3
- Once you have turned it on, you cannot turn it off, no backing down (remember, downgrade isn't a supported thing)
- "Talk to support first"
- https://docs.splunk.com/Documentation/Splunk/9.0.0/Indexer/ConfigureSmartStore#Compress_tsidx_files_upon_upload_to_S3

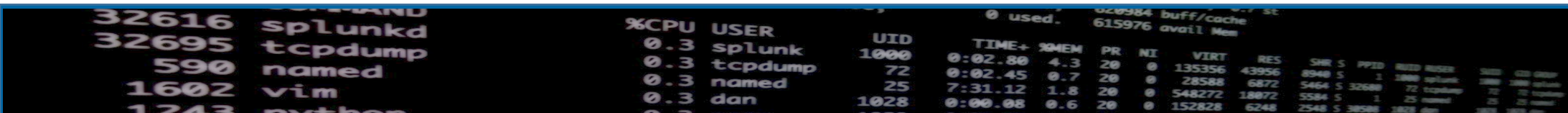


The image shows a terminal window with system metrics and a process list. The top part of the terminal displays memory usage: '0 used' and '615976 avail Mem'. Below this, a table lists system processes with columns for PID, CPU usage, user, UID, TIME+, MEM, PR, NI, VIRT, and RES. The processes listed are splunkd, tcpdump, named, vim, and other.

PID	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES
32616	0.3	splunkd	1000	0:02.80	4.3	20	0	135356	43956
32695	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872
590	0.3	named	25	7:31.12	1.8	20	0	548272	18872
1602	0.3	vim	1028	0:00.08	0.6	20	0	152828	6248
1243	0.3	other							

TSIDX writing level

- Controls the format of the TSIDX files
- Enhancements have been made over the years, version dependent
- Now defaults to 3 (was 2)
- Max is 4
- Older indexers can't read the newer levels
 - Some exceptions, if older indexer support same level than a new one
- Check the chart in docs for version compatibility
- https://docs.splunk.com/Documentation/Splunk/9.0.0/Indexer/Reductsidxdiskusage#The_tsidx_writing_level



A terminal window showing system metrics and a process list. The top part shows memory usage: 0 used, 615976 avail Mem. Below that is a table with columns: %CPU, USER, UID, TIME+, %MEM, PR, NI, VIRT, RES. The process list includes:

%CPU	USER	UID	TIME+	%MEM	PR	NI	VIRT	RES
0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956
0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872
0.3	named	25	7:31.12	1.8	20	0	548272	18872
0.3	dan	1028	0:00.08	0.6	20	0	152828	6248

Admin

```
020984 buff/cache 0 used, 615976 avail Mem
%CPU USER      UID      TIME+  %MEM  PR  NI  VIRT  RES  SHR  S  PPID  RSS  RUSR  RDSR  ...
32616 splunkd    1000     0:02.80 4.3   20  0  135356 43956 8940 S  1  2880 splunkd 1000 1000 splunkd
32695 tcpdump    72      0:02.45 0.7   20  0  28588  6872  5464 S  72  tcpdump  72  72  tcpdump
590   named      25      7:31.12 1.8   20  0  548272 18872 5584 S  1  25  named    25  25  named
1602  vim        1028    0:00.08 0.6   20  0  152828  6248  2548 S  38584 1828 vim    1602 1602 vim
1243  pytho...
```



Readiness App and Python 3

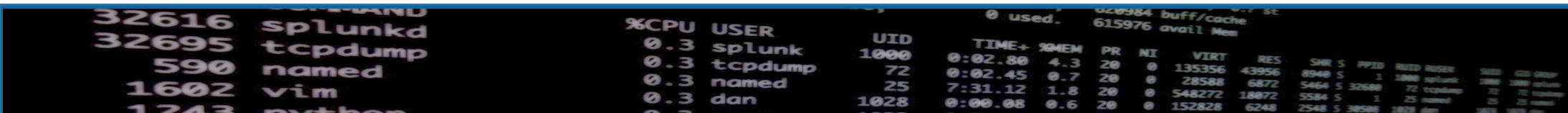
- Splunk Upgrade Readiness App now at version 4
- Prepares for Python 3 and jQuery framework changes
- Can scan for issues
- *There is no Python 2 in Splunk 9*
- Checks TLS configurations (inbound and outbound in Python)
- <https://docs.splunk.com/Documentation/Splunk/9.0.0/UpgradeReadiness/About>

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

%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	PPID	NAME	STATE	TIME	MEM
0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	2888	splunk	2888	2888	splunk
0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32689	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	1028	dan	1028	1028	dan

Health Report and Monitoring Console

- Better descriptions of indicators and what they mean
- New forwarder latency indicator
- Also looks for potential config issues
- Alerts can now be snoozed
- Alerts can be emailed to admins
 - [https://docs.splunk.com/Documentation/Splunk/9.0.0/DMC/Configurealerts#Set up health report alert actions](https://docs.splunk.com/Documentation/Splunk/9.0.0/DMC/Configurealerts#Set_up_health_report_alert_actions)
- Monitoring Console now can automatically build your asset list
 - [https://docs.splunk.com/Documentation/Splunk/9.0.0/DMC/Configureindistributedmode#Enable automatic distributed mode configuration](https://docs.splunk.com/Documentation/Splunk/9.0.0/DMC/Configureindistributedmode#Enable_automatic_distributed_mode_configuration)

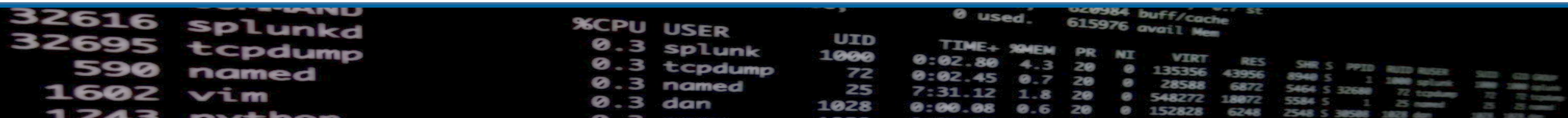


A terminal window showing system metrics and a process list. The top part shows memory usage: 0 used, 615976 avail Mem. Below that is a table with columns: %CPU, USER, UID, TIME+, %MEM, PR, NI, VIRT, RES. The process list includes:

%CPU	USER	UID	TIME+	%MEM	PR	NI	VIRT	RES
0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956
0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872
0.3	named	25	7:31.12	1.8	20	0	548272	18872
0.3	dan	1028	0:00.08	0.6	20	0	152828	6248

Biased Language

- This has been a long running project at Splunk
- Started a few releases ago
- IDXC, Licensing, allow and deny lists
- There is backwards compatibility, but older config directives may be removed, there are a lot of notes in the docs around this
- Note that you can't use both
- Path changes: master-apps -> manager-apps, slave-apps -> peer-apps
 - https://docs.splunk.com/Documentation/Splunk/9.0.0/Indexer/Updatepeerconfigurations#Which_directory_to_use:_manager-apps_or_master-apps.3F
- The old terms still remain in logs as there are customers that use them in multiple ways. Logging may change once more of the effort is complete
- In MC, there are server roles that may need to be updated



The image shows a terminal window with a process list on the left and system statistics on the right. The process list includes:

PPID	PID	USER
32616	splunkd	splunkd
32695	tcpdump	tcpdump
590	named	named
1602	vim	vim
1243	python	python

The system statistics on the right include:

%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	PPID	PPID	PPID	PPID	PPID	PPID	PPID	PPID
0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	2888	splunk	2888	2888	2888	2888	2888	2888
0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32688	72	tcpdump	72	72	72	72	72	72
0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	25	named	25	25	25	25	25	25
0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38588	1028	dan	1028	1028	1028	1028	1028	1028

Search

```
0 used, 615976 avail Mem
```

PID	COMMAND	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	RUSER	RGROUP	ST	TTY	VTID	VTGROUP
32616	splunkd	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	splunk	splunk	S			
32695	tcpdump	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32680	72	tcpdump	S			
590	named	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	named	named	S			
1602	vim	0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38584	1602	vim	S			
1243	python																		

Search

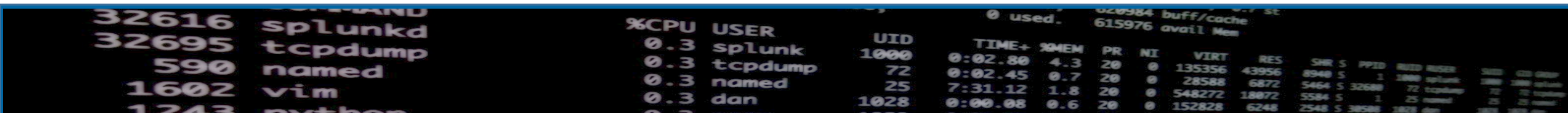
- Federated Search
- Geoip DB

```
020984 buff/cache 0 used, 615976 avail Mem
```

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

Federated Search

- Federated Search != Hybrid Search:
<http://docs.splunk.com/Documentation/Splunk/9.0.0/Search/Hybrid2Federated>
 - Hybrid = peering to other CM/indexers
 - Federated Search = connecting via remote SH
- <https://docs.splunk.com/Documentation/Splunk/9.0.0/Search/Aboutfederatedsearch>
- Better UI with options for restrictions for knowledge objects to limit bundle replication
- Now options for Splunk Cloud -> On prem FS
- Can now use tstats, data models, DMA, lookups
- Transparent Federated Search
 - No more writing in special commands or syntax
 - Only runs in fast mode, so no search-time fields
 - No real-time searching
 - Has to be Transparent or Standard mode, not mixed



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, tcpdump, named, vim, and python.

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	python	0.3	dan	1028

Geoip DB

- No longer using MaxMind as the provider
- The format is the same
- Now using an open source provider
- If you are using a subscription from MaxMind, it will still work

```
020984 buff/cache 0 used, 615976 avail Mem
```

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	8940	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	38584	1602	dan	1602	1602
1243 python	0.3															

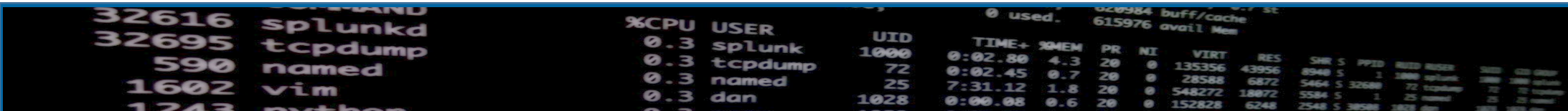
Other stuff

```
020984 buff/cache 0 used, 615976 avail Mem
```

COMMAND	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	RUID	RUSER	SSID	SDIR
32616 splunkd	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	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	38584	1028	vim	1028	1028
1243 python	0.3															

Other stuff

- Dashboards
 - Syntax changes for visualizations
 - No more inline stylesheets
 - Lots of changes to Dashboard Studio:
<https://docs.splunk.com/Documentation/Splunk/9.0.0/DashStudio/WhatNew>
 - Version information is needed on SimpleXML dashboards
- jQuery
 - Admins can disable jQuery 2 access
- Splunk Secure Gateway App
 - New version, lots of changes to make mobile access better
- Semantic versioning of APIs
 - Makes writing things using Splunk APIs easier and more stable, allows for targeting a specific version, and gentle deprecation of older versions
 - <https://semver.org/>



A terminal window showing system metrics 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, USER, %CPU, and UID. The processes listed are splunkd, tcpdump, named, vim, and other.

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	other	0.3	