

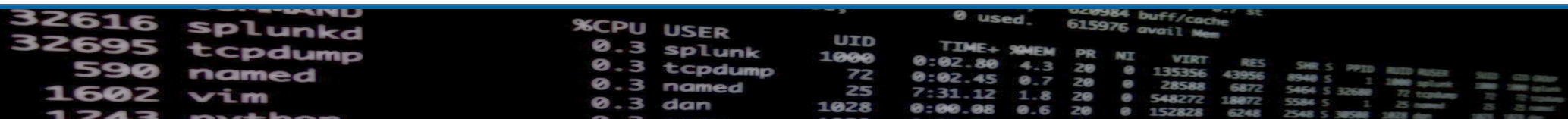
SNMP and You

Kyle Smith, Integration Developer, Aplura, LLC

32616	splunkd	%CPU	USER	UID	TIME+	PMEM	PR	NI	VIRT	RES	SHR	S	PPID	PPID	USER	MEM	GROUP
32695	tcpdump	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	3000	splunk	3000	splunk
590	named	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32680	72	tcpdump	72	tcpdump
1602	vim	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	25	named	25	named
1243	python	0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	30580	1028	dan	1028	dan

Who am I?

- Kyle Smith
- Baltimore UG Co-Lead
- Wrote a Book
- SplunkTrust
- IRC/Slack/Answers/Community



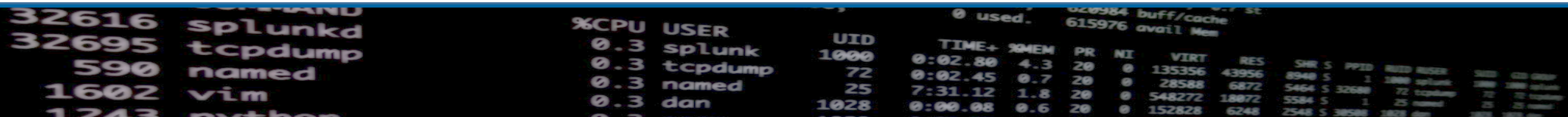
A terminal window screenshot showing system statistics and a list of processes. The top line displays memory usage: 0 used, 620984 buff/cache, 615976 avail Mem. Below this is a table of processes with columns for PID, CPU usage, user, UID, TIME+, MEM, PR, NI, VIRT, RES, SHR, S, PPID, and PGRP. The processes listed are splunkd, tcpdump, named, vim, and python.

PID	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	PGRP
32616	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	3080
32695	0.3	splunk	1000	0:02.45	0.7	20	0	28588	6872	5464	S	1	3080
590	0.3	named	72	7:31.12	1.8	20	0	548272	18872	5584	S	1	25
1602	0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	30584	1828
1243	0.3	python	1028										

What is SNMP?

- Simple Network Management Protocol
 - Collects Information
 - Configures Settings
- 3 Versions
 - SNMP v1
 - Oldest, easiest to configure. Simple protection
 - SNMP v2c
 - Same as v1, but with 64Bit counters
 - SNMP v3
 - Adds encryption and authentication to v2c. Most secure, but complex.

<https://www.logicmonitor.com/blog/whats-with-the-different-snmp-versions-s1-v2c-v3/>



The image shows a terminal window with two sections of output. The top section displays system statistics including CPU usage, memory usage, and swap space. The bottom section displays a list of running processes with columns for PID, PPID, USER, and COMMAND.

System Statistics			
0 used	620984 buff/cache	0 used	615976 avail Mem
32616	splunkd	%CPU	USER
32695	tcpdump	0.3	splunk
590	named	72	1000
1602	vim	0.3	72
1243	python	0.3	25
		0.3	1028

PID	PPID	USER	COMMAND
0.3	0	splunk	0.3 splunk
0.3	0	tcpdump	0.3 tcpdump
0.3	0	named	0.3 named
0.3	0	dan	0.3 dan

MIBs and OIDs

- MIBs

- Management Information Base

- Database that contains entities used in a communication network

- OIDs

- Object Identifiers

- Managed Elements
 - Hierarchical in nature
 - Follows a tree format

- IANA Enterprise Numbers

- Can be registered for any organization.
 - Aplura is 50198

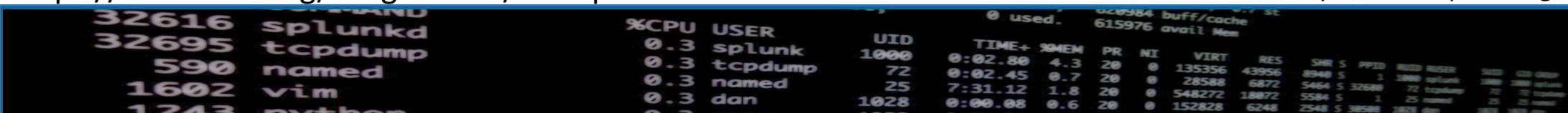
1.3.6.1.4.1.343

and corresponds to the following path through the OID tree:

- 1 ISO
- 1.3 identified-organization,
- 1.3.6 dod,
- 1.3.6.1 internet,
- 1.3.6.1.4 private,
- 1.3.6.1.4.1 IANA enterprise numbers,
- 1.3.6.1.4.1.343 Intel Corporation

<https://www.iana.org/assignments/enterprise-numbers>

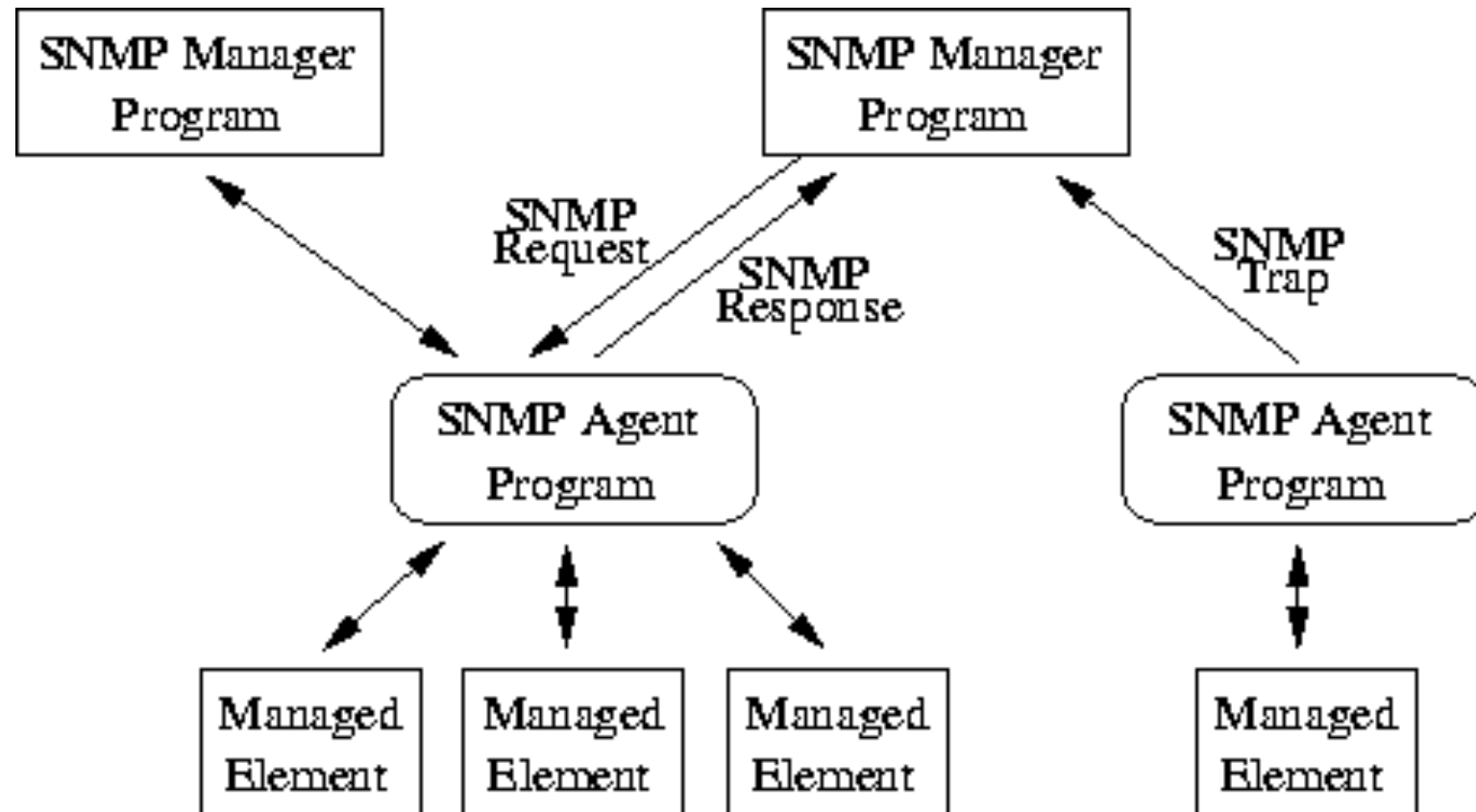
https://en.wikipedia.org/wiki/Object_identifier



A terminal window screenshot showing system status and a list of processes. The top part shows system statistics like CPU usage, memory, and disk space. The bottom part shows a list of processes with columns for PID, command, %CPU, USER, and UID.

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

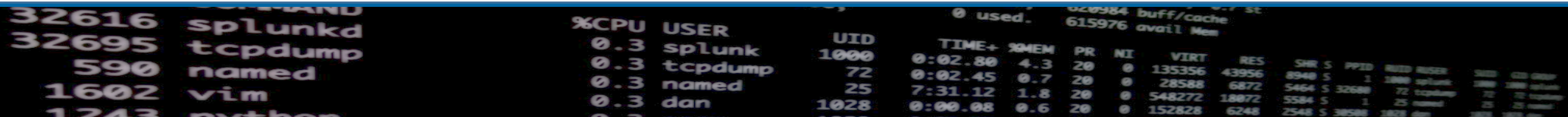
Architecture



	%CPU	USER	UID	TIME+	XMEM	PR	NI	VIRT	RES	SHR	S	PPID	RUDD	MUSER	SWD0	CSD	GROW
32616 splunkd	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	1000	splunk	1000	1000	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	18072	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	30500	1028	dan	1028	1028	dan
1243 python	0.3	python	1000	0:00.00	0.0	20	0	1000	1000	1000	S	1	1000	python	1000	1000	python

SNMP Polling

- Can be done on intervals to collect metrics information
- OIDs of a specific system can be discovered by “walking” the MIB. (as supported)
- Must use an agent to collect the information
- UDP Port 161
- “Pull”
- `snmpwalk -v 1 -c splunk 192.168.1.1 1.3.6.1.4.1.8072`



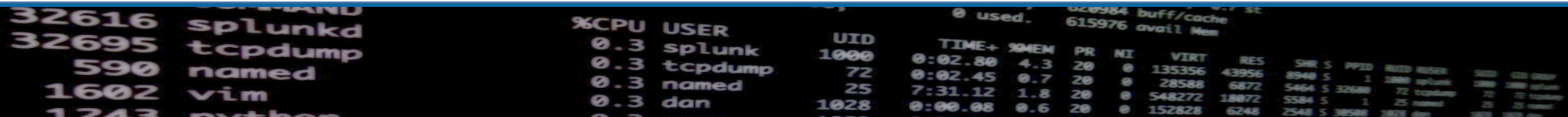
The image shows a terminal window with two main sections. The top section displays a list of processes with their PIDs, names, and PPIDs. The bottom section displays system metrics including CPU usage, memory usage, and process details.

PID	Process Name	PPID
32616	splunkd	0
32695	tcpdump	0
590	named	0
1602	vim	0
1243	python	0

%CPU	USER	UID	TIME+	PMEM	PR	NI	VIRT	RES	SHR	S	PPID	NAME	STATE	TIME	TIME	TIME
0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	splunk	0	0	0	0
0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	72	tcpdump	0	0	0	0
0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	named	0	0	0	0
0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	38584	python	0	0	0	0

SNMP Traps

- Allows SNMP-trap enabled equipment to “reach out and touch someone”
- UDP Port 162
- NO ACK, so data loss possible.
- Generally indicate problems/warnings/errors
- “PUSH”

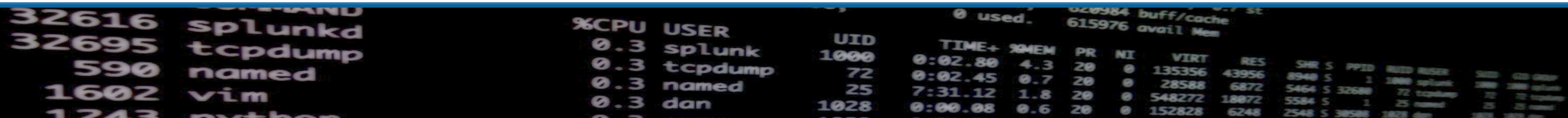


A terminal window screenshot showing system status and process information. The top part displays memory usage: 020984 buff/cache, 615976 avail Mem. Below this is a table of processes with columns for PID, USER, UID, TIME+, MEM, PR, NI, VIRT, RES, SHR, S, PPID, and others. The processes listed are splunkd, tcpdump, named, vim, and python.

PID	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	OTHER
32616	splunkd	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	named
32695	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	72	tcpdump
590	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	named
1602	vim	1028	0:00.08	0.6	20	0	152828	6248	2548	S	30584	vim
1243	python											

Splunk and SNMP

- No native functionality (input) to pull SNMP data.
- Community Apps
 - <https://splunkbase.splunk.com/app/1537/>
- Must have MIBs to perform “OID Translation”
- Pain Points
 - autoresolving oids – gotta have custom MIB
 - anything really around setup is a PITA compared to other tools
 - Modular Input doesn’t die gracefully (or at all)



A terminal window screenshot showing system information. On the left, a list of processes with their PIDs and names: 32616 splunkd, 32695 tcpdump, 590 named, 1602 vim, and 1243 python. On the right, a table of system statistics including CPU usage, memory usage, and network statistics.

%CPU	USER	UID	TIME+	PMEM	PR	NI	VIRT	RES	SHR	S	PPID	PPID	NAME	GROUP
0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	1000	splunk	splunk
0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32680	72	tcpdump	splunk
0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	25	named	splunk
0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	30580	1028	dan	splunk

Many Solutions, One Goal.

Sample SNMP Output

i	Time	Event
>	8/21/17 10:38:54.000 AM	SNMPv2-MIB::sysName."0" = "unifiusr" SNMPv2-MIB::sysDescr."0" = "EdgeOS v4.3.20.4897149.160721.1646" host = 192.168.1.1 source = snmp://unifiusr sourcetype = snmp:unifi
>	8/21/17 10:37:54.000 AM	SNMPv2-MIB::sysName."0" = "unifiusr" SNMPv2-MIB::sysDescr."0" = "EdgeOS v4.3.20.4897149.160721.1646" host = 192.168.1.1 source = snmp://unifiusr sourcetype = snmp:unifi

- No Auto-Extraction of variables/fields
- Possible to have OIDs and not Field names (messy data)

```

0 used.      615976 avail Mem
%CPU USER          UID        TIME+ MEM PR NI    VIRT   RES     SHR S PPID  RSS DUSER  STIO  CIO Group
32616 splunkd         0.3 splunk       1000    0:02.80  4.3 20 0    135356 43956  8940 S 1 1880  splunk  1880 1880 splunk
32695 tcpdump         0.3 tcpdump        72    0:02.45  0.7 20 0    28588  6872  5464 S 32690  tcpdump  72  72 tcpdump
590 named           0.3 named          25    7:31.12  1.8 20 0    548272 18072  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 30500  1028 dan  1028 1028 dan
1243 python

```

- SNMP Mode**

Listen For Traps

The SNMP mode to run this stanza in

☐ IP Version 6

Whether or not this is an IP version 6 address. Defaults to false.

SNMP Version

1

The SNMP Version, 1 / 2C / 3 . Defaults to 2C

Community String

splunk

Community String used for SNMP version 1 and 2C authentication. Defaults to "public"

Custom MIBs

MIB Names

SNMPv2-MIB

0.0.0.0

162

☐ Reverse DNS lookup of trap sources.

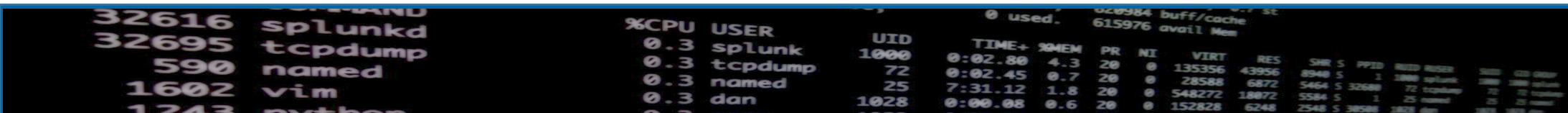
TRAP Generating Host reverse DNS lookup. Forces host field to the DNS looku

[illegible]

Traps Sample

i	Time	Event
>	8/21/17 11:03:01.000 AM	notification_from_address = "192.168.1.128" notification_from_port = "59214" notification_enterprise = "0.0" notification_agent_address = "192.168.1.128" notification_generic_trap = "'authenticationFailure'" notification_specific_trap = "0" notification_uptime = "0" SNMPv2-MIB::sysLocation.0 = ObjectSyntax().setComponentByPosition(0, SimpleSyntax().setComponentByPosition(1, OctetString('Some Location'))) host = 192.168.1.128 source = snmp://snmp_trap sourcetype = snmp:trap
>	8/21/17 11:02:59.000 AM	notification_from_address = "192.168.1.128" notification_from_port = "59214" notification_enterprise = "0.0" notification_agent_address = "192.168.1.128" notification_generic_trap = "'authenticationFailure'" notification_specific_trap = "0" notification_uptime = "0" SNMPv2-MIB::sysLocation.0 = ObjectSyntax().setComponentByPosition(0, SimpleSyntax().setComponentByPosition(1, OctetString('Some Location'))) host = 192.168.1.128 source = snmp://snmp_trap sourcetype = snmp:trap
>	8/21/17 11:02:52.000 AM	notification_from_address = "192.168.1.128" notification_from_port = "59214" notification_enterprise = "0.0" notification_agent_address = "192.168.1.128" notification_generic_trap = "'authenticationFailure'" notification_specific_trap = "0" notification_uptime = "0" SNMPv2-MIB::sysLocation.0 = ObjectSyntax().setComponentByPosition(0, SimpleSyntax().setComponentByPosition(1, OctetString('Some Location'))) host = 192.168.1.128 source = snmp://snmp_trap sourcetype = snmp:trap

- No AutoExtraction of trap OLD Information
- No CIM fields



Collectd and SNMP

- Install collectd
- Enable snmp and write_http plugins (/etc/collectd/collectd.conf)
- Use output plugins (CSV/HEC/Metrics Store)

Shhhh..... <http://docs.splunk.com/Documentation/Splunk/7.0.0/Metrics/GetMetricsInCollectd>

32616	splunkd	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	RATED	MUTEX	INSTR	OUT	CS	GROUP
32695	tcpdump	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43952	8940	5	1	1800	update	1800	1800	0	0
590	named	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	5	32695	72	tcpdump	72	72	0	0
1602	vim	0.3	named	25	7:31.12	1.8	20	0	548272	18072	5584	5	1	25	named	25	25	0	0
1243	python	0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	5	30500	1028	0	1028	1028	0	0

SNMP Config – Collectd - HEC

```
LoadPlugin write_http
<Plugin write_http>
  <Node "node-http-1">
    URL "http://127.0.0.1:8088/services/collector/raw?channel=9E00C924-4408-49A9-AC45-139C3F0B509F"
    Header "Authorization: Splunk 9E00C924-4408-49A9-AC45-139C3F0B509F"
    Format "JSON"
    Metrics true
    StoreRates true
  </Node>
</Plugin>
```

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

%CPU USER      UID      TIME+  MEM PR NI  VIRT  RES  SHR S  PPID  RSS  RUSR  RDSK  RNET  RGRP
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 1828 dan 1828 1828 dan
```


SNMP Config – Collectd SNMP

```
LoadPlugin snmp
<Plugin snmp>
<Data "uptimer">
  Type "uptime"
  Table false
  Instance "system"
  Values "1.3.6.1.2.1.1.3.0"
</Data>

<Host "unifiusr">
  Address "192.168.1.1"
  Version 1
  Community "splunk"
  Collect "uptimer"
  Interval 120
</Host>
<Host "basementap">
  Address "192.168.1.170"
  Version 1
  Community "splunk"
  Collect "uptimer"
  Interval 300
</Host>
</Plugin>
```

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

```
%CPU USER      UID      TIME+  %MEM  PR  NI  VIRT  RES  SHR  S  PPID  RSSD  RSSR  RSSM  RSSV  RSSD  RSSR  RSSM  RSSV
0.3  splunk  1000    0:02.80  4.3  20  0  135356 43956 8940 S   1  1000  uptimer  1000  1000  uptimer
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  30580 1828  dan    1828 1828  dan
```

SNMP Collectd CSV Output

```
more /var/lib/collectd/csv/unifiusr/sntp/uptime-system-2017-08-21
epoch,value
1503332846.320,142340179.0000000
1503332966.314,142352178.0000000
```

- Can then use UF to consume the data
- Filenames/locations configurable

PID	COMMAND	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR S	PPID	RSSD	RSSUS	SZUS	CSS	OSTYPE
32616	splunkd	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8948 S	1	18880	splunkd	18880	18880	to tcpdump
32695	tcpdump	0.3	splunk	72	0:02.45	0.7	20	0	54654	6872	54654 S	32695	72	tcpdump	72	72	to tcpdump
590	named	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584 S	1	25	named	25	25	to tcpdump
1602	vim	0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548 S	38058	1602	vim	1602	1602	to tcpdump
1243	python	0.3	python	1000	0:00.00	0.0	20	0	152828	6248	2548 S	38058	1602	vim	1602	1602	to tcpdump

Tools

- MIB Browser / Trap Sender
 - Solarwinds ToolSet
 - Windows only
 - A large amount of MIBs
 - <http://ireasoning.com/mibbrowser.shtml>
 - Can use custom MIBs as required
 - JAVA – Mac OSX, Windows, etc.
 - Sends /receives Traps
 - Walk the devices

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

Examples and dashboards

PID	COMMAND	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR S	PPID	RSSD	RSSUS	SWP	CSS	OSTYPE
32616	splunkd	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8948 S	1	18880	splunkd	18880	18880	to tcpdump
32695	tcpdump	0.3	splunk	72	0:02.45	0.7	20	0	54654	6872	54654 S	32695	72	tcpdump	72	72	to tcpdump
590	named	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584 S	1	25	named	25	25	to tcpdump
1602	vim	0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548 S	38058	1602	vim	1602	1602	to tcpdump
1243	python	0.3	python	1000	0:00.00	0.0	20	0	152828	6248	2548 S	38058	1243	python	1243	1243	to tcpdump

Questions?

- I'm sure there are some.

32616	splunkd	%CPU	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	PPID	USER	MEM	GROUP
32695	tcpdump	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	3000	splunk	1000	splunk
590	named	0.3	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	32680	72	tcpdump	72	tcpdump
1602	vim	0.3	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	25	named	25	named
1243	python	0.3	dan	1028	0:00.08	0.6	20	0	152828	6248	2548	S	30580	1028	dan	1028	dan

SNMP TA – Check for MIBS

- Follow documentation to see what MIBs are supported by default
- Add new MIBs (not working yet)
 - Find new MIBS (we are using Ubiquiti as our test)
 - Performed in “snmp_ta/bin”
 - Pip install -lv pysnmp==4.2.5
 - build-pysnmp-mib -o UBNT-MIB.py ./UBNT-MIB
 - build-pysnmp-mib -o UBNT-UniFi-MIB.py ./UBNT-UniFi-MIB
 - Build an Egg

	%CPU	USER	UID	TIME+	XMEM	PR	NI	VIRT	RES	SHR	S	PPID	RUDD	MUSER	SWD0	CSD	GROW
32616 splunkd	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	1000	splunk	1000	1000	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	18072	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	30500	1028	dan	1028	1028	dan
1243 python	0.3	python	1028	0:00.08	0.6	20	0	152828	6248	2548	S	30500	1028	dan	1028	1028	dan

SNMP App by Aplura

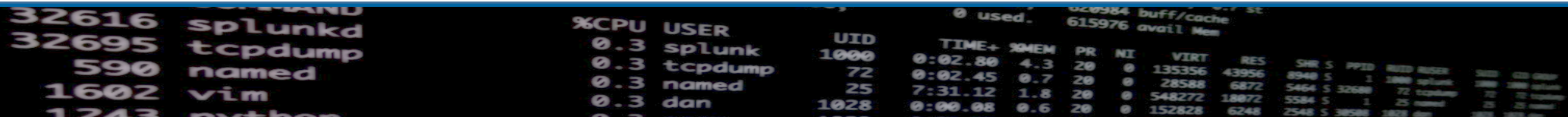
- Requirements:

- Setup wizard (<https://openui5.hana.ondemand.com/#/entity/sap.m.Wizard>)
- Net-snmp for setup wizard
- Collectd
- SNMP plugin for collectd (<https://collectd.org/wiki/index.php/Plugin:SNMP>)
- Write_http plugin for collectd (send to HEC on HF)
- Massive fucking MIB List.
- REST endpoint to read/write the collectd.conf file.

	%CPU	USER	UID	TIME+	XMEM	PR	NI	VIRT	RES	SHR	S	PPID	RUSED	MUSED	SWD	CSD	GROUP
32616 splunkd	0.3	splunk	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	1000	splunk	1000	1000	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	18072	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	30500	1028	dan	1028	1028	dan

SNMP App by Aplura Steps

- Check for and configure HEC. Store Token securely
- Use Wizard:
 - “Data Elements”: query specific host to pull MIBs/OIDs supported.
 - Create “DataSet”, allow name by user.
 - Whitelist/blacklist
 - Allow IP ranges (iterate and make host stanzas for collectd.conf)

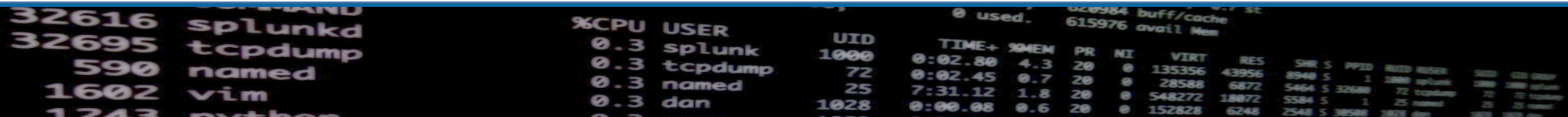


A terminal window screenshot showing system statistics and a list of processes. The top part displays memory usage (0 used, 615976 avail Mem) and system statistics (020984 buff/cache, 0-1 st). Below this is a table of processes with columns for PID, USER, UID, TIME+, MEM, PR, NI, VIRT, RES, SHR, S, PPID, and other details. The processes listed are splunkd, tcpdump, named, vim, and python.

PID	USER	UID	TIME+	MEM	PR	NI	VIRT	RES	SHR	S	PPID	OTHER
32616	splunkd	1000	0:02.80	4.3	20	0	135356	43956	8940	S	1	named
32695	tcpdump	72	0:02.45	0.7	20	0	28588	6872	5464	S	72	tcpdump
590	named	25	7:31.12	1.8	20	0	548272	18872	5584	S	1	named
1602	vim	1028	0:00.08	0.6	20	0	152828	6248	2548	S	30584	vim
1243	python											

Add additional MIB

- Some steps and examples here.



A terminal window screenshot showing system statistics and a list of processes. The top part of the image shows memory usage statistics: 0 used, 620984 buff/cache, and 615976 avail Mem. Below this 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 python (PID 1243). The bottom part of the image shows a detailed view of the system statistics, including CPU usage, memory usage, and network statistics.

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