

'enp2s0' weliswaar een hoge belasting heeft, maar dat het aantal swapouts per seconde waarschijnlijk een nog zwaardere impact had gedurende de 10-minuten interval, die eindigt om 16:55 uur.

We kunnen diezelfde interval met atop verder analyseren en vragen daarbij om het geheugengebruik per proces te tonen (optie '-m', analoog aan de 'm' toets binnen atop) voor het specifieke tijdstip 16:55:

```
atop -m -r y -b 16:55
```

De uitvoer in **Figuur 4** toont in de MEM regel, dat dit systeem 7.6 GiB geheugen heeft ('tot'), waarvan 4.4 GB gebruikt wordt als page cache ('cache'+ 'buff') en 425 MB als dynamisch kernelgeheugen ('slab'). In de proceslijst zien we dat het commando grep 1 GB fysiek geheugen gebruikt ('RSIZE') en de daaropvolgende vier processen samen meer dan 1 GB fysiek geheugen gebruiken. Daarmee hebben we al een groot deel van het geheugengebruik in kaart gebracht. Opvallend is natuurlijk dat het commando grep bij het doorspitten van grote hoeveelheden data zelf een behoorlijke omvang krijgt (1 GB). Daarnaast zorgt het doorzoeken van vele bestanden voor een forse groei van de page cache. In dit geval veroorzaken deze factoren dat delen van andere processen uitgeswapt worden, waardoor de gebruikers van die processen het systeem als traag ervaren.

VERDWENEN PROCESSEN TRACEREN

Atop is niet alleen nuttig voor performance-analyse, maar ook voor troubleshooting. Stel dat je ontdekt dat de systeemtijd niet meer accuraat is, omdat het daemon-proces 'chronyd' verdwenen is. Dan wil je kunnen achterhalen wanneer dat proces geëindigd is en op welke wijze (uit vrije wil of door ontvangst van een dodelijk signaal). Je kunt eerst kijken of het proces eerder vandaag is geëindigd:

```
atop -r | egrep '^ATOP|chronyd'
```

De optie '-r' zorgt voor het lezen van de gegevens sinds middernacht. Als het gezochte proces al eerder dan vandaag is geëindigd, kun je een of meer 'y'-tekens meegeven bij de optie '-r' om telkens een dag verder terug te doorzoeken. De zoekstring voor egrep zorgt dat we niet alleen de regel vinden met het gezochte proces 'chronyd', maar ook de kopregel van iedere interval (regels die beginnen met ATOP) om het tijdstip te kunnen bepalen. Na enige zoeken zou je de volgende uitvoer kunnen krijgen (zie **Listing 15**).

File Edit View Search Terminal Help										
ATOP - robin		2018/05/29 16:55:32		-----				10m0s elapsed		
PRC	sys	95.59s	user	1m45s	#proc	552	#zombie	0	#exit	246
CPU	sys	11%	user	18%	irq	1%	idle	269%	wait	100%
CPL	avg1	1.06	avg5	1.13	avg15	0.98	csw	9569310	intr	6449651
MEM	tot	7.6G	free	123.5M	cache	4.4G	buff	4.5M	slab	425.2M
SWP	tot	10.0G	free	9.7G			vmcom	7.9G	vmlim	13.8G
PAG	scan	1672893	steal	1562e3	stall	7	swin	8	swout	54803
LVM	tos_ssd-home	busy	0%	read	13337		write	268	avio	0.19 ms
LVM	ntos_hdd-var	busy	0%	read	12		write	147	avio	12.8 ms
DSK	sda	busy	1%	read	13		write	1715	avio	2.65 ms
NFM	/nfs/Public	srv	nasi	read	5.8G		write	0K	nread	5.0G
NFC	rpc	206048	read	192952	write	0	retxmit	0	autref	206e3
NET	transport	tcpi	4109180	tcpo	2187246		udpi	43	udpo	43
NET	network	ipo	4109399	ipo	2187315		ipfrw	0	deliv	4109e3
NET	enp2s0	86%	pcki	4353364	pcko	2187328	si	86 Mbps	so	2264 Kbps

PID	VSTACK	VSIZE	RSIZE	PSIZE	VGROW	RGROW	SWAPSZ	MEM	CMD	1/111
16606	132K	2.1G	1.0G	1.0G	2.0G	1.0G	0K	13%	grep	
3778	144K	3.0G	463.9M	440.2M	-8196K	-960K	0K	6%	4. Uitvoer van atop	
16371	140K	2.7G	266.0M	250.7M	-12K	-800K	0K	3%	voor traag systeem	
9977	132K	2.0G	235.7M	214.7M	0K	-384K	0K	3%		
3231	140K	2.0G	187.1M	170.5M	-5832K	-9.8M	10620K	2%	gnome-shell	

LISTING 15

```
atop -r yyyy | egrep '^ATOP|chronyd'
....
ATOP - robin 2018/05/25 15:49:01 ... 10m0s elapsed
1124 0.00s 0.01s 0K 0K 0K 0K 2 3 0% chronyd
ATOP - robin 2018/05/25 15:59:01 ... 10m0s elapsed
1124 0.00s 0.00s 0K 0K - - 1 3 0% <chronyd>
ATOP - robin 2018/05/25 16:09:01 ... 10m0s elapsed
ATOP - robin 2018/05/25 16:19:01 ... 10m0s elapsed
```

LISTING 17

```
PID ... ENDDATE ENDTIME ST EXC S CPU CMD
1124 ... 2018/05/25 15:56:41 -S 9 E 0% <chronyd>
```

In een interactieve atop sessie kun je vervolgens bepalen waarom chronyd er de brui aan gegeven heeft:

```
atop -v -r yyyy -b 15:59
```

De optie '-v' (of toetsaanslag 'v') zorgt dat atop per proces de start- en eindtijd, én de manier van eindigen toont. Als je binnen atop zoekt naar proces 'chonyd' (/chronyd), dan zou je de volgende uitvoer kunnen krijgen (zie **Listing 17**).

We zien dat chronyd om 15:56:41 is geëindigd. Als reden zien we de letter 'S' als tweede teken in de kolom ST: getermineerd door een signal en wel signal 9 (kolom EXC). Dat tweede teken zou ook een 'E' kunnen zijn, bij een vrijwillig einde met de exitcode in de kolom EXC. Maar de cliffhanger na deze workshop blijft: wie vermoordde chronyd?

Het package 'atop' vind je voor de meeste distributies in de standaard repository. In dat geval kun je 'atop' installeren via commando's als yum of apt-get (afhankelijk van de distro). De meest-courante versie vind je altijd op de website www.atoptool.nl als RPM en als tar-ball.

OVER DE AUTEUR

Gerlof Langeveld is de maker van atop, atopsar en kernel module netatop. Hij werkt inmiddels 21 jaar als docent/consultant bij AT Computing. Hij doceert o.a. de vijfdaagse master class "Linux performance analysis and tuning" voor systeembeheerders, waarin ruim aandacht wordt geschonken aan de werking van de kernel en de interpretatie van performance-gegevens, die door tools als atop worden getoond.