

# SAV & SCS Sizing Tips Doc

## Sizing Scripts

### Tips for Sizing:

1. Obtain the largest file possible and run the logcount.pl script on it.
  - 1a. Take results from logcount.pl and divide by 24 hours. 60 minutes 60 seconds to get events per second.
  - 1b. To create a worst case scenario take the results from logcount.pl and divide by 8 hours, 60 minutes, 60 seconds.
2. Run either the filterevents.pl or directory\_recurse.pl and determine average across a month's time.
3. Use these numbers as guides not absolutes.

### Scripts Included in this package:

1. logcount.pl
2. filterevents
2. directory\_recurse.pl

### Requirements:

PERL  
Download: [www.activestate.com](http://www.activestate.com)

**Script:** logcount.pl  
**Description:** Used to count number of lines in one file.  
**Usage:** perl count.pl d:\logs\server01\11022004.log  
**Usage Notes:** d:\logs\server01\datestamp.log is the one file that count.pl will count.

### Output:

```
#####  
#  
#      File Counted: d:\log\11022004.log  
#  
#      No. of Lines = 2300  
#  
#####
```

## SAV & SCS Sizing Tips Doc

**Script:** Filterevents.pl  
**Description:** Used to count number of lines in a number of files located in the same directory.  
**Usage:** perl count.pl d:\logs\server01  
**Usage Notes:** d:\logs\server01 contains the collection of DATESTAMP.log files.

### Output:

```
-----# Events -----Percentage-----
SAV Event Scan Stops_____ : 366 : 0.46%
SAV Event Scan Starts_____ : 451 : 0.57%
SAV Event Pattern Update_____ : 7528 : 9.44%
SAV Event Infection_____ : 7106 : 8.91%
SAV Event File Not Open_____ : 112 : 0.14%
SAV Event Load Pattern_____ : 45470 : 56.99%
SAV Event Trap_____ : 6 : 0.01%
SAV Event Config Change_____ : 4929 : 6.18%
SAV Event Shutdown_____ : 4 : 0.01%
SAV Event Startup_____ : 3 : 0.00%
SAV Event Pattern Download_____ : 39 : 0.05%
SAV Event Too Many Viruses_____ : 0 : 0.00%
SAV Event FWD to Quarantine Server: 0 : 0.00%
SAV Event Scan and Deliver_____ : 0 : 0.00%
SAV Event Backup_____ : 0 : 0.00%
SAV Event Scan Abort_____ : 51 : 0.06%
SAV Event RTS Load Error_____ : 35 : 0.04%
SAV Event RTS Load_____ : 3 : 0.00%
SAV Event RTS Unload_____ : 0 : 0.00%
SAV Event UNKNOWN_____ : 13207 : 16.55%
SCF Event IMPLICIT BLOCK_____ : 0 : 0.00%
SCF Event EVENT CONFIG CHANGE_____ : 0 : 0.00%
SCF Event POLICY UPDATE_____ : 380 : 0.48%
SCF Event IDS MONITORING_____ : 0 : 0.00%
SCF Event Firewall Violation_____ : 0 : 0.00%
SCF Event Intrusion Attempted_____ : 0 : 0.00%
SCF Event LiveUpdate_____ : 0 : 0.00%
```

```
TOTAL EVENTS for Directory d:\logs\server01 : 79787 Events
Number of Files Processed: 31
Average Number of Events per Day: 2573.77
Average Number of Events per Hour: 107.24
Average Number of Events per Minute: 1.79
Average Number of Events per Second: 0.03
-----
```

## SAV & SCS Sizing Tips Doc

**Script:** directory\_recurse.pl  
**Description:** Used to count number of lines in a number of files located in a number of directories.  
**Usage:** perl direcoty\_rrecurse.pl d:\logs\  
**Usage Notes:** d:\logs contains the collection of server directories each with corresponding list of logs in each directory.

### OUTPUT:

```
-----# Events -----Percentage-----
SAV Event Scan Stops_____: 610 : 0.36%
SAV Event Scan Starts_____: 757 : 0.45%
SAV Event Pattern Update_____: 8321 : 4.97%
SAV Event Infection_____: 11192 : 6.69%
SAV Event File Not Open_____: 36384 : 21.75%
SAV Event Load Pattern_____: 82963 : 49.60%
SAV Event Trap_____: 6 : 0.00%
SAV Event Config Change_____: 7179 : 4.29%
SAV Event Shutdown_____: 379 : 0.23%
SAV Event Startup_____: 672 : 0.40%
SAV Event Pattern Download_____: 143 : 0.09%
SAV Event Too Many Viruses_____: 0 : 0.00%
SAV Event FWD to Quarantine Server: 0 : 0.00%
SAV Event Scan and Deliver_____: 0 : 0.00%
SAV Event Backup_____: 0 : 0.00%
SAV Event Scan Abort_____: 91 : 0.05%
SAV Event RTS Load Error_____: 69 : 0.04%
SAV Event RTS Load_____: 661 : 0.40%
SAV Event RTS Unload_____: 0 : 0.00%
SAV Event UNKNOWN_____: 17061 : 10.20%
SCF Event IMPLICIT BLOCK_____: 0 : 0.00%
SCF Event EVENT CONFIG CHANGE_____: 0 : 0.00%
SCF Event POLICY UPDATE_____: 598 : 0.36%
SCF Event IDS MONITORING_____: 0 : 0.00%
SCF Event Firewall Violation_____: 2 : 0.00%
SCF Event Intrusion Attempted_____: 0 : 0.00%
SCF Event LiveUpdate_____: 0 : 0.00%
```

```
TOTAL EVENTS for Directory d:\logs : 167272 Events
Number of Files Processed: 1
Average Number of Events per Day: 167272.00
Average Number of Events per Hour: 6969.67
Average Number of Events per Minute: 116.16
Average Number of Events per Second: 1.94
-----
```