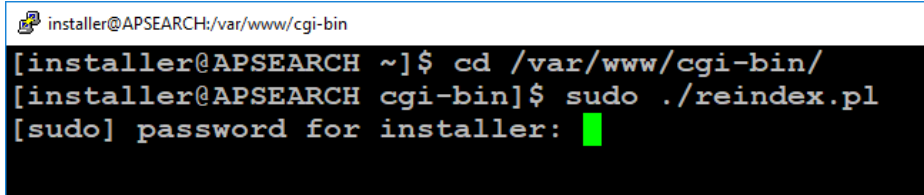


APSearch Tool Admin Guide

Reindexing the data when new invoices are added

- ssh to 192.168.9.9 with username installer and the usual password (see KeePass)
- Run the following commands and enter the password when prompted

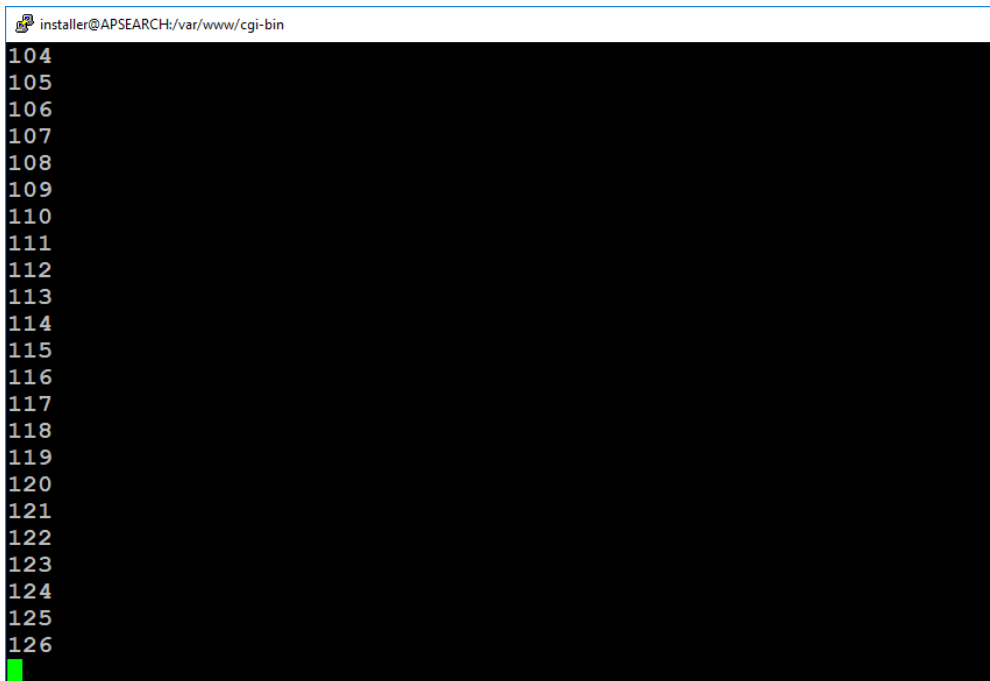
```
# cd /var/www/cgi-bin  
# sudo ./reindex.pl
```



A terminal window showing the execution of the reindexing command. The prompt is 'installer@APSEARCH:~/var/www/cgi-bin'. The user enters 'cd /var/www/cgi-bin/' and then 'sudo ./reindex.pl'. The prompt changes to '[sudo] password for installer:' with a green cursor.

```
installer@APSEARCH:~/var/www/cgi-bin  
[installer@APSEARCH ~]$ cd /var/www/cgi-bin/  
[installer@APSEARCH cgi-bin]$ sudo ./reindex.pl  
[sudo] password for installer: █
```

- The indexing will take some time depending on how much activity is on the LUN where the vm is stored. Usual runtime is around ~30 minutes, the script will count each invoice processed and print the number it is working on to the screen, there are about 42,000 invoices



A terminal window showing the output of the reindexing script. The prompt is 'installer@APSEARCH:~/var/www/cgi-bin'. The output shows a list of numbers from 104 to 126, with a green cursor at the bottom.

```
installer@APSEARCH:~/var/www/cgi-bin  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
█
```

- Once completed, backup the old index then move the new one in place

```
# sudo cp /var/www/html/MHIndex.txt ~/20190325-Index
# sudo cp /var/www/cgi-bin/MHIndex.txt /var/www/html/MHIndex.txt
```

```
[installer@APSEARCH cgi-bin]$ sudo cp /var/www/html/MHIndex.txt ~/20190325-Index
[sudo] password for installer:
[installer@APSEARCH cgi-bin]$ sudo cp /var/www/cgi-bin/MHIndex.txt /var/www/html/MHIndex.txt
```

Adding a computer to the firewall exceptions list

- ssh to the machine and run the following command, substituting the IP address for the machine you are adding. Be sure not to change anything but the IP. Reload the service then check to confirm the machine is in the allow list.

```
# sudo firewall-cmd --permanent --zone=public --add-rich-rule='rule
family=ipv4 source address=192.168.10.25/32 destination
address=192.168.9.9/32 port port=80 protocol=tcp accept'

# sudo firewall-cmd --reload
# sudo firewall-cmd --list-all
```

```
[sudo] password for installer:
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens192
  sources:
  services: ssh dhcpv6-client
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
    rule family="ipv4" source address="192.168.10.25/32"
    rule family="ipv4" source address="192.168.1.67/32"
    rule family="ipv4" source address="192.168.2.73/32"
[installer@APSEARCH cgi-bin]$
```

Removing a computer from the firewall exceptions list

```
# sudo firewall-cmd --permanent --zone=public --remove-rich-  
rule='rule family=ipv4 source address=192.168.2.73/32 destination  
address=192.168.9.9/32 port port=80 protocol=tcp accept'  
  
# sudo firewall-cmd --reload  
# sudo firewall-cmd --list-all
```

Check that the web server is running and restart if necessary

- ssh to the machine and run the following command to check the status of Apache

```
# service httpd status
```

```
[installer@APSEARCH cgi-bin]$ service httpd status  
Redirecting to /bin/systemctl status httpd.service  
• httpd.service - The Apache HTTP Server  
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)  
   Active: active (running) since Fri 2019-03-08 12:53:58 EST; 2 weeks 2 days ago  
     Docs: man:httpd(8)  
           man:apachectl(8)  
  Process: 12749 ExecReload=/usr/sbin/httpd $OPTIONS -k graceful (code=exited, status=0/SUCCESS)  
 Main PID: 9361 (/usr/sbin/httpd)  
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic: 0 B/sec"  
    CGroup: /system.slice/httpd.service  
            └─ 9361 /usr/sbin/httpd -DFOREGROUND  
              └─ 12765 /usr/sbin/httpd -DFOREGROUND  
                └─ 12766 /usr/sbin/httpd -DFOREGROUND  
                  └─ 12767 /usr/sbin/httpd -DFOREGROUND  
                    └─ 12768 /usr/sbin/httpd -DFOREGROUND  
                      └─ 12769 /usr/sbin/httpd -DFOREGROUND  
                        └─ 12770 /usr/sbin/httpd -DFOREGROUND  
                          └─ 14625 /usr/sbin/httpd -DFOREGROUND  
                            └─ 14626 /usr/sbin/httpd -DFOREGROUND  
  
Mar 08 12:53:58 APSEARCH systemd[1]: Starting The Apache HTTP Server...  
Mar 08 12:53:58 APSEARCH systemd[1]: Started The Apache HTTP Server.  
Mar 10 03:42:02 APSEARCH systemd[1]: Reloading The Apache HTTP Server.  
Mar 10 03:42:02 APSEARCH systemd[1]: Reloaded The Apache HTTP Server.  
Mar 17 03:27:02 APSEARCH systemd[1]: Reloading The Apache HTTP Server.  
Mar 17 03:27:02 APSEARCH systemd[1]: Reloaded The Apache HTTP Server.  
Mar 24 03:13:01 APSEARCH systemd[1]: Reloading The Apache HTTP Server.  
Mar 24 03:13:02 APSEARCH systemd[1]: Reloaded The Apache HTTP Server.
```

- restart the service if necessary

```
# sudo systemctl reload httpd.service
```

```

Redirecting to /bin/systemctl restart httpd.service
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to manage system services or units.
Authenticating as: installer
Password:
[installer@APSEARCH cgi-bin]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
• httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Fri 2019-03-08 12:53:58 EST; 2 weeks 2 days ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 15030 ExecReload=/usr/sbin/httpd $OPTIONS -k graceful (code=exited, status=0/SUCCESS)
 Main PID: 9361 (/usr/sbin/httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic: 0 B/sec"
    CGroup: /system.slice/httpd.service
            └─ 9361 /usr/sbin/httpd -DFOREGROUND
               └─ 15032 /usr/sbin/httpd -DFOREGROUND
                  └─ 15033 /usr/sbin/httpd -DFOREGROUND
                     └─ 15034 /usr/sbin/httpd -DFOREGROUND
                        └─ 15035 /usr/sbin/httpd -DFOREGROUND
                           └─ 15036 /usr/sbin/httpd -DFOREGROUND
                              └─ 15037 /usr/sbin/httpd -DFOREGROUND

Mar 17 03:27:02 APSEARCH systemd[1]: Reloading The Apache HTTP Server.
Mar 17 03:27:02 APSEARCH systemd[1]: Reloaded The Apache HTTP Server.
Mar 24 03:13:01 APSEARCH systemd[1]: Reloading The Apache HTTP Server.
Mar 24 03:13:02 APSEARCH systemd[1]: Reloaded The Apache HTTP Server.
Mar 25 11:18:33 APSEARCH systemd[1]: Reloading The Apache HTTP Server.
Mar 25 11:18:33 APSEARCH systemd[1]: Reloaded The Apache HTTP Server.
Mar 25 11:18:49 APSEARCH systemd[1]: Reloading The Apache HTTP Server.
Mar 25 11:18:49 APSEARCH systemd[1]: Reloaded The Apache HTTP Server.
Mar 25 11:18:58 APSEARCH systemd[1]: Reloading The Apache HTTP Server.
Mar 25 11:18:58 APSEARCH systemd[1]: Reloaded The Apache HTTP Server.

```

Rebooting or powering down the system

```
# sudo reboot
```

```
# sudo poweroff
```

Checking Audit Logs

- run the following command to create an HTML report with all of the access logs currently on the system. By default, 4 weeks' worth of logs are kept. This can be changed.

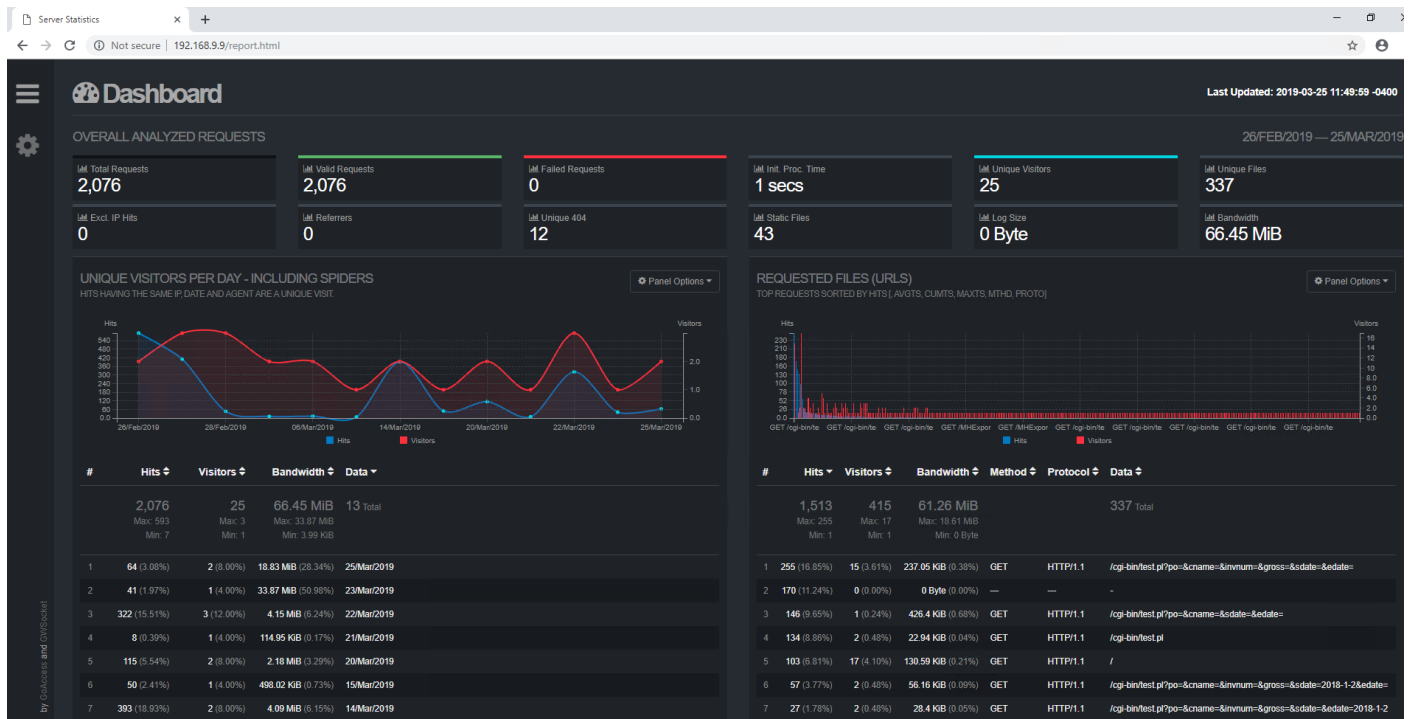
```
# sudo zcat -f /var/log/httpd/access_log* | goaccess -a -o /var/www/html/report.html
```

```

root@APSEARCH:/home/installer
[root@APSEARCH installer]# sudo zcat -f /var/log/httpd/access_log* | goaccess -a -o /var/www/html/report.html
[root@APSEARCH installer]# ]
[root@APSEARCH installer]# █

```

access the report at the following URL: <http://192.168.9.9/report.html>





- If granular logging is required, these logs are kept below **/var/log/httpd**. You can run this command to watch the requests in real-time:

```
# sudo tail -f /var/log/httpd/access_log
```

```
[root@APSEARCH httpd]# tail -f /var/log/httpd/access_log
192.168.1.240 - - [25/Mar/2019:11:35:58 -0400] "GET /MHEXport/ExportData/NGH/ExportData/Page5/exportdetailpage.xsl HTTP/1.1" 200 29884 "http://192.168.9.9/MHEXport/ExportData/NGH/ExportData/Page5/19ff437e2f25445bb9eafda13bc03fb7.xml" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36"
192.168.1.240 - - [25/Mar/2019:11:35:58 -0400] "GET /MHEXport/ExportData/NGH/ExportData/Page5/loc_Invoice.xml HTTP/1.1" 200 65213 "http://192.168.9.9/MHEXport/ExportData/NGH/ExportData/Page5/19ff437e2f25445bb9eafda13bc03fb7.xml" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36"
192.168.1.240 - - [25/Mar/2019:11:35:58 -0400] "GET /MHEXport/ExportData/NGH/ExportData/Page5/exportdetailpage.css HTTP/1.1" 200 2248 "http://192.168.9.9/MHEXport/ExportData/NGH/ExportData/Page5/19ff437e2f25445bb9eafda13bc03fb7.xml" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36"
192.168.1.67 - - [25/Mar/2019:11:36:49 -0400] "-" 408 - "-" "-"
192.168.1.67 - - [25/Mar/2019:11:39:50 -0400] "GET /resources/demos/style.css HTTP/1.1" 404 223 "http://192.168.9.9/cgi-bin/test.pl?po=&cname=mcke&vnum=&invnum=&gross=&sdate=&edate=" "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
192.168.1.67 - - [25/Mar/2019:11:39:50 -0400] "GET /cgi-bin/test.pl?po=&cname=mcke&vnum=&invnum=&gross=&sdate=&edate=" HTTP/1.1" 200 1286726 "http://192.168.9.9/cgi-bin/test.pl?po=&cname=Bell&vnum=&invnum=&gross=&sdate=&edate=" "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
192.168.1.67 - - [25/Mar/2019:11:40:07 -0400] "GET /MHEXport/ExportData/NGH/ExportData/Page7/difb19bd6dd54931aa29160fdc5112d6_IMAGE-10487_16174-652020201-20190206_1_11227_32703481.tif HTTP/1.1" 200 87144 "http://192.168.9.9/cgi-bin/test.pl?po=&cname=mcke&vnum=&invnum=&gross=&sdate=&edate=" "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
192.168.1.67 - - [25/Mar/2019:11:40:14 -0400] "GET /MHEXport/ExportData/WHGH/ExportData/Pagel/27eb45b835744de68faff3c1facc6971.xml HTTP/1.1" 200 16789 "http://192.168.9.9/cgi-bin/test.pl?po=&cname=mcke&vnum=&invnum=&gross=&sdate=&edate=" "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
192.168.1.240 - - [25/Mar/2019:11:53:16 -0400] "GET /report.html HTTP/1.1" 200 446903 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36"
192.168.1.240 - - [25/Mar/2019:11:54:08 -0400] "-" 408 - "-" "-"
```