HOWTO – Archiving / Enforcing Retention Policy

Contents

Change Control

Date (DD-MMM-YYYY)	Change Summary
08-JAN-2019	First Release by Dusan Tomic.
10-JAN-2019	Added enforce_policy_at_hour and an example of enforcing policy between two dates

Document Owner: International FortiSIEM CSE Team

Data Retention Policies

Data retention policies are used to manage the way FortiSIEM stores, archives and deletes data.
FortiSIEM is very flexible in this regard as it allows you to define policies based on Organization, Reporting Device and Event Attribute.
By default, the system will manage these defined policies and enforce them at a specific hour of the day defined in the /opt/phoenix/config/phoenix_config.txt file. The parameter that defines at which hour the policy is enforced is **enforce_policy_at_hour** (by default it runs at 22).

If you want to force a retention policy to run at any point in time, you have the option of running the EnforceRetentionPolicy script from the Supervisors SSH console.

EnforceRetentionPolicy

The syntax for this script is EnforceRetentionPolicy DATES, where DATES can be a single day or an interval of days, in unix epoch.

What this means is that in order to enforce the retention policy, you need to transform the date or dates to unix epoch. The easiest way to do this is using the date command in Linux (you can do this from the Supervisor).

Example enforcing a policy only for the day **January 1st 2019**.

Find out number of days since unix epoch (1/1/1970 UTC)

```
expr $(date -u --date="01-JAN-19" +%s) / 86400
```

Result: 17897

Enforce policy for this date:

```
EnforceRetentionPolicy 17897
```

Example enforcing a policy for all days between and including **December 1st 2018** and **January 1st 2019**.

Find out number of days since unix epoch (1/1/1970 UTC)

```
expr $(date -u --date="01-DEC-18" +%s) / 86400
```

Result: 17866

Enforce policy between Dec 1st 2018 and January 1st 2019:

```
EnforceRetentionPolicy 17866-17897
```

How often is the enforce_policy_at_hour attribute read?

This setting from phoenix_config.txt will only be read when the process phDataPurger is restarted.
To restart this process, you can execute the following commands:

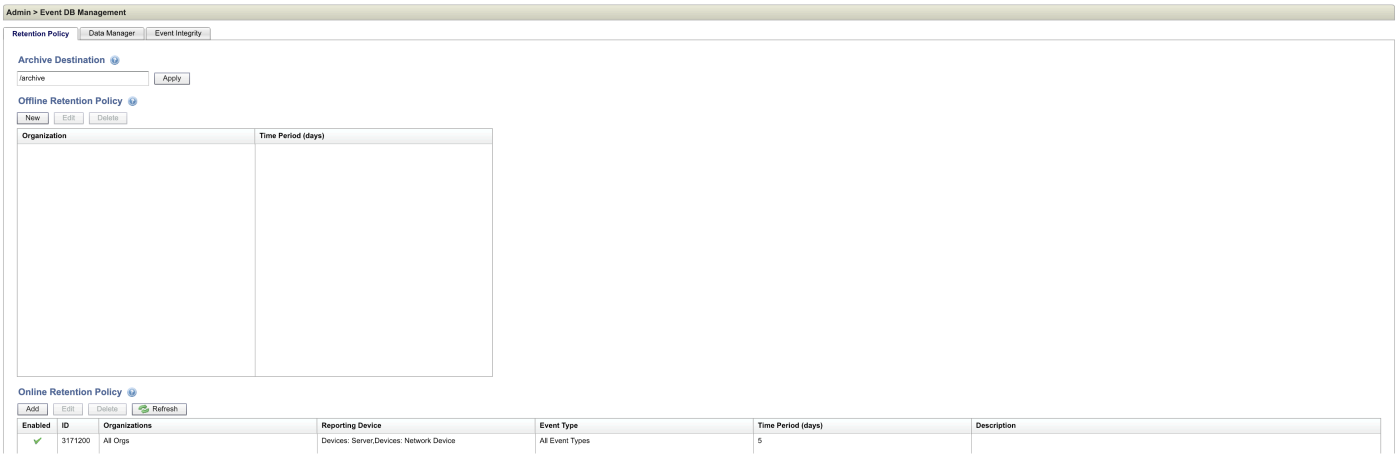
```
phtools --stop phDataPurger
phtools --start phDataPurger
```

You can check the status of your processes with the **phstatus** command.

End to End example of creating, forcing and validating and Event Retention Policy

Create an Online Retention Policy of 5 days for Servers and Network Devices. This policy will run at 10pm (as defined in phoenix_config.txt), but we want to enforce it immediately for January 1st 2019 and not have to wait until 10pm.

The archived data will go into the /archive folder on FortiSIEM.



Admin > Event DB Management

Archive Destination

/archive

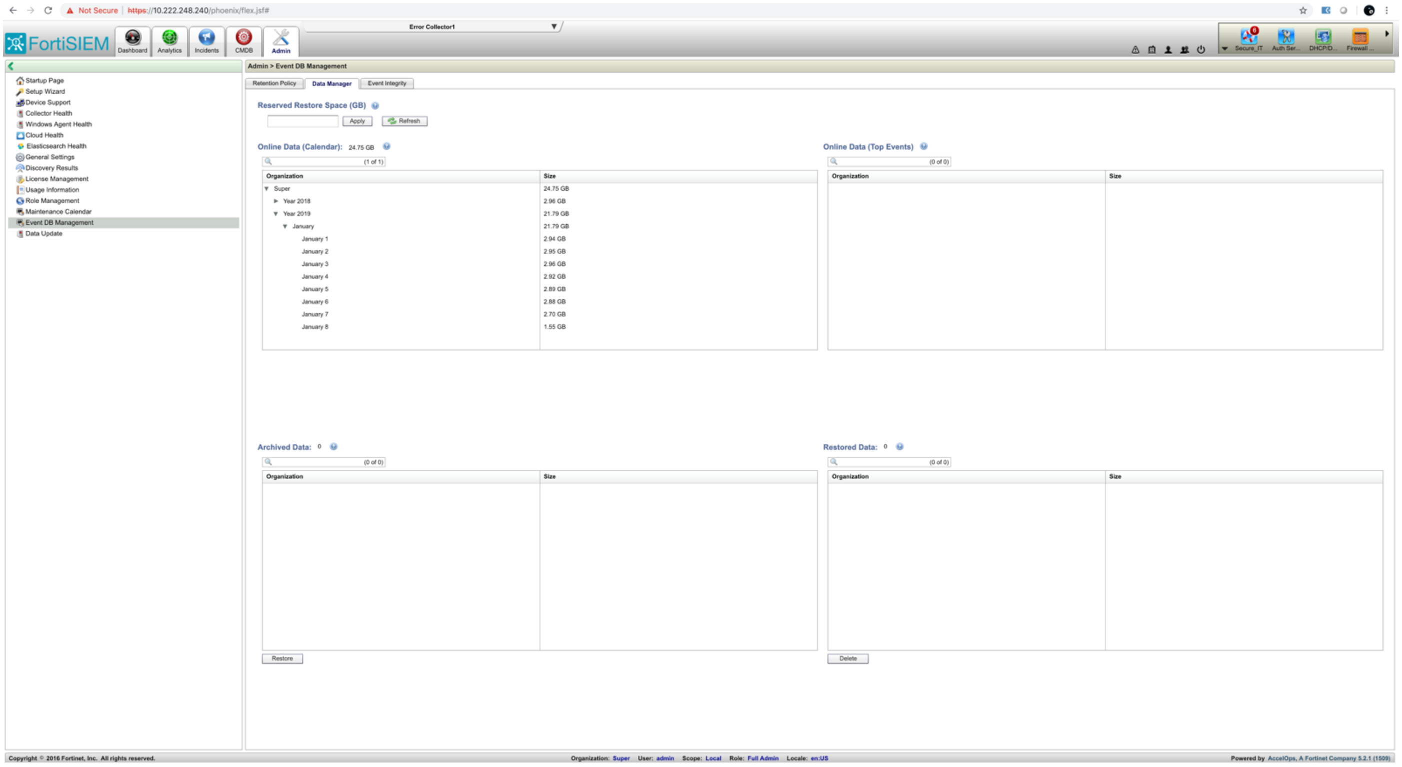
Offline Retention Policy

Organization	Time Period (days)

Online Retention Policy

Enabled	ID	Organizations	Reporting Device	Event Type	Time Period (days)	Description
✓	3171200	All Orgs	Devices: Server,Devices: Network Device	All Event Types	5	

Validate how much data we have on 1st January in the Data Manager tab:



Admin > Event DB Management

Reserved Restore Space (GB)

Online Data (Calendar): 24.75 GB

(1 of 1)

Organization	Size
▼ Super	24.75 GB
► Year 2018	2.96 GB
▼ Year 2019	21.79 GB
▼ January	21.79 GB
January 1	2.94 GB
January 2	2.95 GB
January 3	2.96 GB
January 4	2.92 GB
January 5	2.89 GB
January 6	2.88 GB
January 7	2.70 GB
January 8	1.55 GB

Online Data (Top Events)

(0 of 0)

Organization	Size

Archived Data: 0

(0 of 0)

Organization	Size

Restored Data: 0

(0 of 0)

Organization	Size

Copyright © 2016 Fortinet, Inc. All rights reserved. Organization: Super User: admin Scope: Local Role: Full Admin Locale: en:US Powered by AccelOps, A Fortinet Company 5.2.1 (1509)

January 1st : 2.94GB

Let’s run the EnforceRetentionPolicy script for January 1st.

```
EnforceRetentionPolicy 17897
```

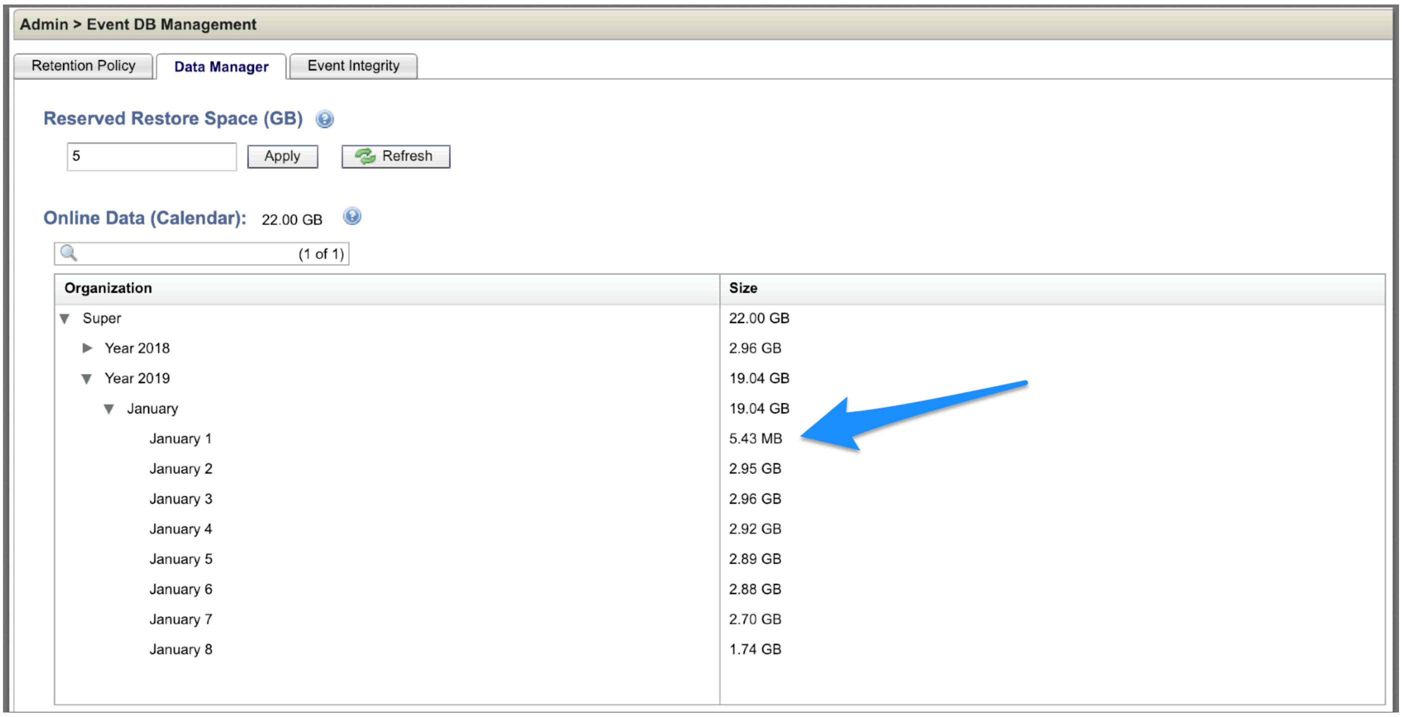
Applying a retention policy may take several minutes (or hours, depending how much data you have).

Once done, you can validate that you have data in the /archive directory, and you can test it to see what kind of logs it contains.

```
[root@FSM_5 ~]# cd /archive/CUSTOMER_1/default/17897/
You have new mail in /var/spool/mail/root
[root@FSM_5 17897]# du -sh
1.8G    .
```

We seem to have 1.8GB of archived logs from January 1st. It is expected to have less storage than we did before due to losing the indexes (total storage was 2.94GB when online in /data)

If we look in the GUI we can also see that the data from January 1st is now gone:



Organization	Size
▼ Super	22.00 GB
▶ Year 2018	2.96 GB
▼ Year 2019	19.04 GB
▼ January	19.04 GB
January 1	5.43 MB
January 2	2.95 GB
January 3	2.96 GB
January 4	2.92 GB
January 5	2.89 GB
January 6	2.88 GB
January 7	2.70 GB
January 8	1.74 GB

We can test the archived data (read its content) using another script called **TestSegmentReader**. The path below is specific to my testing system, you will a different directory, but it will contain the date (in this case 17897) and start with the word seg.

```
[root@FSM_5 data]# TestSegmentReader /archive/CUSTOMER_1/default/17897/429528-429551-
182384880/seg-1-0-600000-1546300800-1546305001/
[PH_MODULE_LOCAL_CONFIG_LOADED]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]=phConfigLoader.cpp,[lineNumber]=161,[configName]=global,[phLogDetail]=Module loaded local config
successfully
[PH_GENERIC_INFO]:[eventSeverity]=LM_INFO,[procName]=<unknown>,[fileName]=phConfigurationThruHttp.cpp,[lineNumber]=105,[phLogDetail]=520-DR: reload agent info in cache.
[PH_GENERIC_DEBUG]:[eventSeverity]=LM_DEBUG,[procName]=<unknown>,[fileName]=phHttpClient.cpp,[lineNumber]=2494,[phLogDetail]=DBG_CACHE_371, cannot get process
[PH_GENERIC_DEBUG]:[eventSeverity]=LM_DEBUG,[procName]=<unknown>,[fileName]=phHttpClient.cpp,[lineNumber]=2494,[phLogDetail]=DBG_CACHE_371, cannot get process
[PH_GENERIC_DEBUG]:[eventSeverity]=LM_DEBUG,[procName]=<unknown>,[fileName]=phHttpClient.cpp,[lineNumber]=2494,[phLogDetail]=DBG_CACHE_371, cannot get process
[PH_GENERIC_DEBUG]:[eventSeverity]=LM_TRACE,[procName]=<unknown>,[fileName]=phHttpClient.cpp,[lineNumber]=1007,[phLogDetail]=Response file of this cache will be located at
/opt/phoenix/cache/10.222.248.240/phoenix/rest/config/systemConfig/default.dat
[PH_GENERIC_DEBUG]:[eventSeverity]=LM_DEBUG,[procName]=<unknown>,[fileName]=phHttpClient.cpp,[lineNumber]=1841,[phLogDetail]=set CURLOPT_SSL_VERIFYPEER to no

[PH_GENERIC_DEBUG]:[eventSeverity]=LM_DEBUG,[procName]=<unknown>,[fileName]=phHttpClient.cpp,[lineNumber]=754,[phLogDetail]=Send req with
https://10.222.248.240:443/phoenix/rest/config/systemConfig
[PH_GENERIC_DEBUG]:[eventSeverity]=LM_DEBUG,[procName]=<unknown>,[fileName]=phHttpClient.cpp,[lineNumber]=2494,[phLogDetail]=DBG_CACHE_371, cannot get process
[PH_GENERIC_DEBUG]:[eventSeverity]=LM_DEBUG,[procName]=<unknown>,[fileName]=phHttpClient.cpp,[lineNumber]=785,[phLogDetail]=Check curl result for
https://10.222.248.240:443/phoenix/rest/config/systemConfig: result: 0
[PH_GENERIC_DEBUG]:[eventSeverity]=LM_DEBUG,[procName]=<unknown>,[fileName]=phHttpClient.cpp,[lineNumber]=2494,[phLogDetail]=DBG_CACHE_371, cannot get process
[PH_GENERIC_DEBUG]:[eventSeverity]=LM_DEBUG,[procName]=<unknown>,[fileName]=phHttpClient.cpp,[lineNumber]=2494,[phLogDetail]=DBG_CACHE_371, cannot get process
[PH_GENERIC_DEBUG]:[eventSeverity]=LM_DEBUG,[procName]=<unknown>,[fileName]=phHttpClient.cpp,[lineNumber]=2494,[phLogDetail]=DBG_CACHE_371, cannot get process
[PH_GENERIC_DEBUG]:[eventSeverity]=LM_TRACE,[procName]=<unknown>,[fileName]=phHttpClient.cpp,[lineNumber]=1007,[phLogDetail]=Response file of this cache will be located at
/opt/phoenix/cache/10.222.248.240/phoenix/rest/config/eventAttributeType/default.dat
[PH_GENERIC_DEBUG]:[eventSeverity]=LM_DEBUG,[procName]=<unknown>,[fileName]=phHttpClient.cpp,[lineNumber]=1841,[phLogDetail]=set CURLOPT_SSL_VERIFYPEER to no

[PH_GENERIC_DEBUG]:[eventSeverity]=LM_DEBUG,[procName]=<unknown>,[fileName]=phHttpClient.cpp,[lineNumber]=754,[phLogDetail]=Send req with
https://10.222.248.240:443/phoenix/rest/config/eventAttributeType
[PH_GENERIC_DEBUG]:[eventSeverity]=LM_DEBUG,[procName]=<unknown>,[fileName]=phHttpClient.cpp,[lineNumber]=2494,[phLogDetail]=DBG_CACHE_371, cannot get process
[PH_GENERIC_DEBUG]:[eventSeverity]=LM_DEBUG,[procName]=<unknown>,[fileName]=phHttpClient.cpp,[lineNumber]=785,[phLogDetail]=Check curl result for
https://10.222.248.240:443/phoenix/rest/config/eventAttributeType: result: 0
```

```
[PH_GENERIC_DEBUG]:[eventSeverity]=LM_DEBUG,[procName]=<unknown>,[fileName]=phHttpClient.cpp,[lineNumber]=2494,[phLogDetail]=DBG_CACHE_371, cannot get process
Attr_1: FortiGate-traffic-denied
Attr_2: 3
Attr_5: 1
Attr_6: 2018-01-01 10:46:30
Attr_7: 2019-01-01 00:00:01
Attr_8: IPV4: 10.1.1.1
Attr_9: IPV4: 10.1.1.1
Attr_11: Fortigate90D
Attr_12: 1
Attr_13: <181>Jan  1 00:00:01 time=10:46:30 devname=Fortigate90D devid=FGT90D3Z13006177 logid=0000000013 type=traffic
subtype=forward level=notice vd=root srcip=10.1.1.19 srcname="mac-server" srcport=58892 srcintf="internal" dstip=10.1.1.151
dstname="10.1.1.151" dstport=3283 dstintf="IPsec_VPN" sessionid=3919220 status=deny policyid=0 dstcountry="Reserved"
srccountry="Reserved" trandisp=noop service=3283/tcp proto=6 duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 devtype="Mac"
osname="Mac OS X" mastersrcmac=0c:4d:e9:99:66:e6 srcmac=0c:4d:e9:99:66:e6 crscore=2432696350 craction=131072
Attr_15: 2913688221740755180
Attr_16: 4
Attr_17: 1
Attr_21: 1
Attr_24: LOW
Attr_43: Fortinet
Attr_44: FortiOS
Attr_53: Super
Attr_110: 1
Attr_122: FortiGateParser
Attr_128: 31497211
Attr_129: 1
Attr_1000: IPV4: 10.1.1.19
Attr_1001: IPV4: 10.1.1.151
Attr_1002: 10.1.1.151
Attr_1007: 0c:4d:e9:99:66:e6
Attr_1008: 00:11:22:3a:4b:5c
Attr_1010: 6
Attr_1011: 58892
Attr_1012: 3283
Attr_1022: internal
Attr_1023: IPsec_VPN
Attr_1032: 0
Attr_1035: 0
Attr_1036: 0
Attr_1037: 0
Attr_1038: 0
Attr_1100: 1
Attr_1121: mac-server
Attr_1150: 0
Attr_1186: Mac
Attr_1200: deny
Attr_1346: 0c:4d:e9:99:66:e6
Attr_2004: Mac OS X
Attr_2582: noop
Attr_2800: notice
Attr_3513: forward
Attr_3523: 0000000013
Attr_3916: 3919220
Attr_4171: root
Attr_4188: Syslog
Attr_4562: deny
Attr_4683: 2432696350
Attr_4685: 131072
Attr_9016: 3283/tcp
```

As you can see, the archived log is from January 1st, which means our policy was enforced successfully.