EventTracker

Actionable Security Intelligence

Integrate HAProxy

EventTracker v8.x and above

Publication Date: July 20, 2017

Abstract

This guide provides instructions to configure HAProxy to send the syslog to EventTracker Enterprise. Once syslog is configured to send to EventTracker Manager, alerts and reports can be configured into EventTracker.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 8.x and later, **HAProxy 1.7.5** and later.

Audience

Administrators who are responsible for monitoring **HAProxy** which are running the operating system using EventTracker Manager.

Table of Contents

HAProxy

HAProxy is a free, very fast and reliable solution offering high availability, load balancing, and proxying for TCP and HTTP-based applications. It is particularly suited for very high traffic web sites and powers quite a number of the world's most visited ones. Over the years, it has become the de-facto standard open source load balancer. Since it does not advertise itself, we only know it's used when the admins report it. Its mode of operation makes its integration into existing architectures very easy and riskless, while still offering the possibility not to expose fragile web servers to the net.

Prerequisites

- EventTracker v8.x should be installed.
- HAProxy is known to reliably run on the following OS/Platforms:
  - Linux 2.4 on x86, x86_64, Alpha, Sparc, MIPS, PARISC
  - Linux 2.6 / 3.x on x86, x86_64, ARM, Sparc, PPC64
  - Solaris 8/9 on UltraSPARC 2 and 3
  - Solaris 10 on Opteron and UltraSPARC
  - FreeBSD 4.10 - 10 on x86
  - OpenBSD 3.1 to -current on i386, amd64, mac pc, alpha, sparc64 and VAX (check the ports)
  - AIX 5.1 - 5.3 on Power™ architecture

Configure HAProxy to send syslog to EventTracker

To configure HAProxy to log in syslog,

- Edit the HAProxy server configuration file **(/etc/haproxy/haproxy.cfg)** and include the following lines:
  1. global
  2. log “EventTracker IP address” local0
  3. option httplog

```
global
    # to have these messages end up in /var/log/haproxy.log you will
    # need to:
    #
    # 1) configure syslog to accept network log events.  This is done
    #    by adding the '-r' option to the SYSLOGD_OPTIONS in
    #    /etc/sysconfig/syslog
    #
    # 2) configure local2 events to go to the /var/log/haproxy.log
    #   file. A line like the following can be added to
    #   /etc/sysconfig/syslog
    #
    #    local2.*                       /var/log/haproxy.log
    #
    log         192.168.1.99 local2

    chroot      /var/lib/haproxy
    pidfile     /var/run/haproxy.pid
    maxconn     4000
    user        haproxy
    group       haproxy
    daemon

    # turn on stats unix socket
```

EventTracker Knowledge Pack

Once logs are received into EventTracker, Categories and reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Windows.

Flex Reports

- **HAProxy-Allowed traffic -** This report provides details of all the acceptable traffic that is passed through by the HA proxy server.

LogTime	Computer	Client IP Address	Client Port	Remote Hostname	Http Method	Remote Uri Accessed	Status Code	Bytes Used	User Agent
07/13/2017 04:52:58 PM	HAPROXY	172.263.1.27	57204	www.alliance.com	POST	/life/log/_log HTTP/1.1	200	300	Mozilla/5.0 (iPad; CPU OS 10_3_2 like Mac OS X) AppleWebKit/603.2.4 (KHTML, like Gecko)
07/13/2017 04:52:58 PM	HAPROXY	192.1.21.74	19462	api.vitboj.com	GET	/trackables/activity/suggest?count=6 HTTP/1.1	200	617	Java/1.8.0_131
07/13/2017 04:52:58 PM	HAPROXY	172.11.81.47	28423	apibaseinfo.com	GET	https://api.baseinfo.com/identity/auth HTTP/1.1	200	690	spray-can/1.3.2
07/13/2017 04:52:58 PM	HAPROXY	192.168.1.40	47922	api.calibri.com	GET	https://api.calibri.com/identity/application/1009 HTTP/1.1	200	8289	spray-can/1.3.2

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
7/18/2017 12:52:22 PM	5555	NTPLDTBLR38 / HAProx...	N/A	N/A	Syslog

Event Type: Information
Log Type: Application
Category Id: 0

Description:
Jul 18 06:13:20 10.153.14.79 Jul 18 06:13:24 prod-apiproxy.contoso.net haproxy[12204]: 192.1.21.72:58908 [18/Jul/2017:06:13:24.484] 1499858004 api~ TLSv1.2 AES128-GCM-SHA256 prod_services/prod-services-436f 4/0/0/3/7 200 667 - \- ---- 103/103/4/3/0 0/0 {spray-can/1.3.2|api.contoso.com|} "GET https://api.contoso.com/identity/auth HTTP/1.1.

- **HAProxy-Denied traffic -** This report provides details on all the traffic that is denied by the HAProxy server.

LogTime	Computer	Client IP Address	Client Port	Remote Hostname	Http Method	Remote Uri Accessed	Status Code	Bytes Used	User Agent
07/13/2017 05:32:23 PM	HAPROXY	172.11.14.79	49473	www.contoso.com	POST	/life/journeys/heartbeat HTTP/1.1"	403	713	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like
07/13/2017 05:32:23 PM	HAPROXY	192.33.50.110	52974	www.acme.com	GET	/life/portalConstants.js HTTP/1.1	404	4340	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
07/13/2017 05:32:23 PM	HAPROXY	172.163.11.54	26797	api.alliance.com	PUT	https://api.redbricklabs.com/identity/auth HTTP/1.1	401	376	spray-can/1.3.2
07/13/2017 05:32:23 PM	HAPROXY	192.160.4.111	38697	api.redmond.com	GET	/identity/consumer/2592265/authorize/organization/rbh/creatapplication?	403	441	

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
7/18/2017 12:52:23 PM	5555	NTPLDTBLR38 / HAProx...	N/A	N/A	Syslog

Event Type: Information
Log Type: Application
Category Id: 0

Description:
Jul 18 06:09:16 10.153.14.79 Jul 18 06:09:20 prod-portalproxy-contoso.net haproxy[4568]: 172.163.19.66:49473 [18/Jul/2017:06:09:20.651] 149985 7760 portal~ TLSv1.2 ECDHE-RSA-AES128-SHA256 prod_portallb/prod-portallb-ec84 102/0/0/16/119 403 713 - \- ---- 127/127/3/1/0 0/0 {Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko|www.contoso.com|} "POST /life/journeys/stroke HTTP/1.1

- **HAProxy-Error connections -** This report provides details on all the error connection between the backend and frontend server.

LogTime	Computer	Client IP Address	Client Port	Frontend Server	Backend Server	Error Message
07/14/2017 04:41:37 PM	HAPROXY	127.0.0.1	56059	api~ TLSv1.2	prod_services/prod-services	Connection error during SSL handshake.
07/14/2017 04:41:37 PM	HAPROXY	192.168.11.14	19452	portal~ TLSv1.2	prod_portallb/prod-portallb	The server closed the transport connection.
07/14/2017 04:41:37 PM	HAPROXY	72.153.12.19	47213	api~ TLSv1.2	prod_services/prod-services	The supplied message is incomplete. The signature was not verified.
07/14/2017 04:41:37 PM	HAPROXY	172.201.18.36	55179	portal~ TLSv1.2	prod_vaultbundle/prod-vaultbundle	The request cannot be fulfilled due to bad syntax.
07/14/2017 04:41:37 PM	HAPROXY	192.168.55.10	56031	portal~ TLSv1.2	prod_portallb/prod-portallb	Access denied.

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
7/18/2017 12:52:23 PM	5555	NTPLDTBLR38 / HAProx...	N/A	N/A	Syslog

Event Type: Information
Log Type: Application
Category Id: 0

Description:
Jul 18 06:09:16 172.163.19.66 Jul 18 06:09:20 prod-portalproxy-acme.net haproxy[6103]: 127.0.0.1:56059 [18/Jul/2017:17:35:10.380] 1499858004 api~ TLSv1.2 AES128-GCM-SHA256 prod_services/prod-services: Connection error during SSL handshake.

Import HAProxy knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Token templates
- Flex Reports

NOTE: Export knowledge pack items in the following sequence:

- Token templates
- Flex Reports

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.

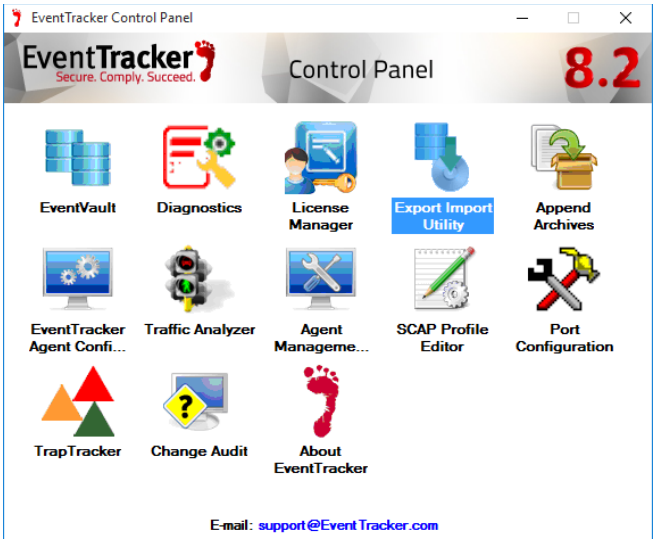


Figure 1

3. Click the **Import** tab.

Token Templates

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab, and then click on ‘**Import**’ option.
3. Click on **Browse** button.

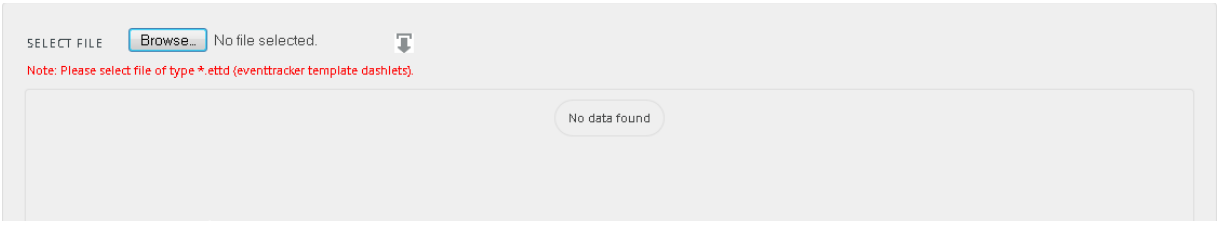


Figure 2

4. Locate **All HAProxy templates.ettd** file, and then click the **Open** button.

Figure 3

5. Now select the check box and then click on ‘**Import**’ option.
   EventTracker displays success message.

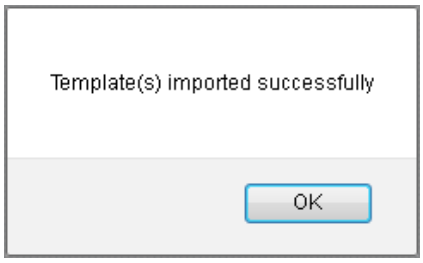


Figure 4

6. Click on **OK** button.

Flex Reports

1. Click **Reports** option, and then click the browse ... button.
2. Locate the **All HAProxy reports.etcrx** file, and then click the **Open** button.

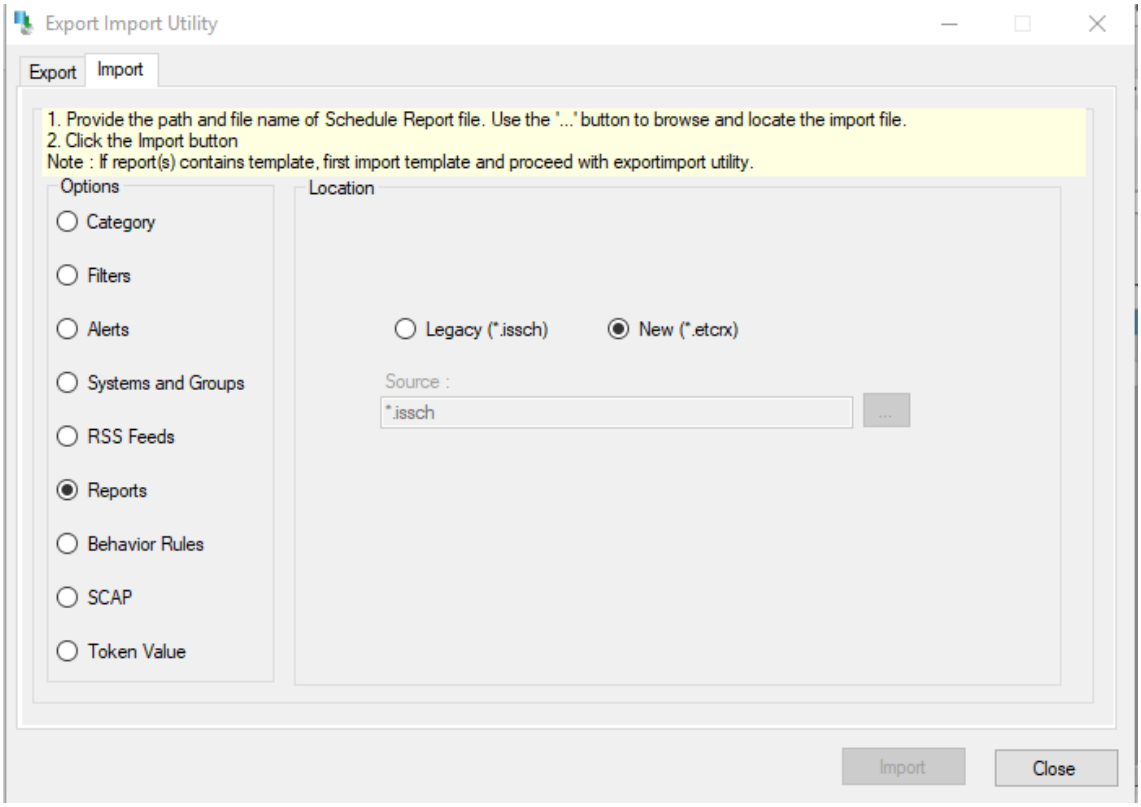


Figure 5

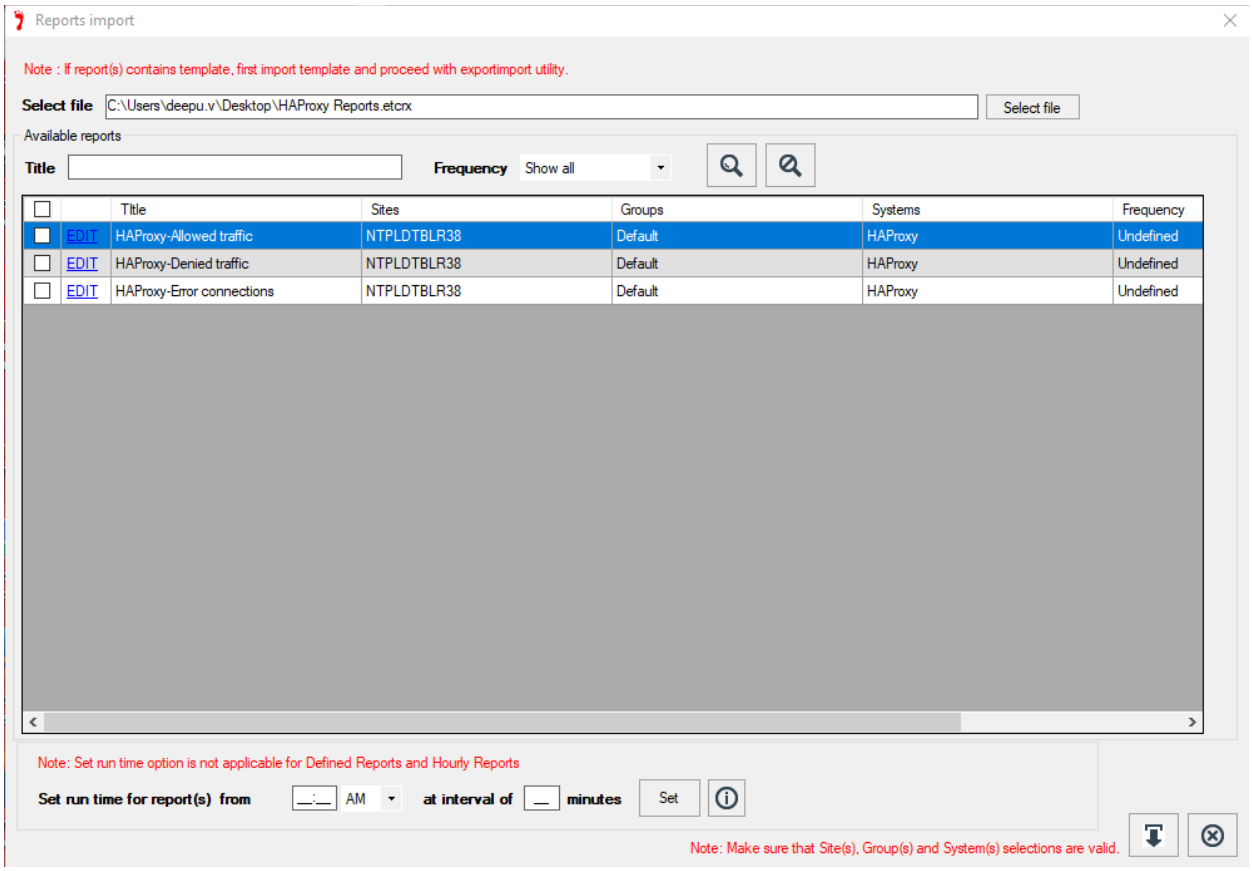


Figure 6

3. Click the **Import** button to import the **scheduled** reports. EventTracker displays success message.

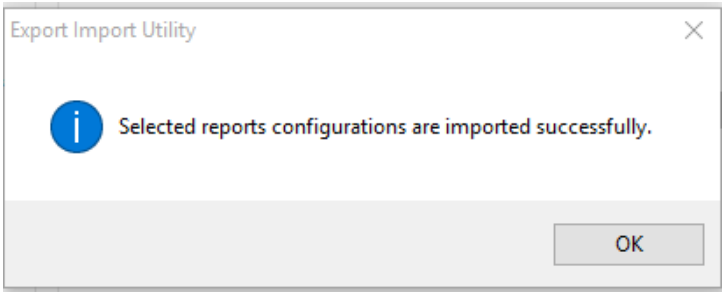


Figure 7

Verify HAProxy knowledge pack in EventTracker

Token Template

1. Logon to **EventTracker Enterprise** web interface.
2. Click the **Admin** menu, and then click **Parsing Rules** and click **Template**.

3. Click on **HAProxy** group option.

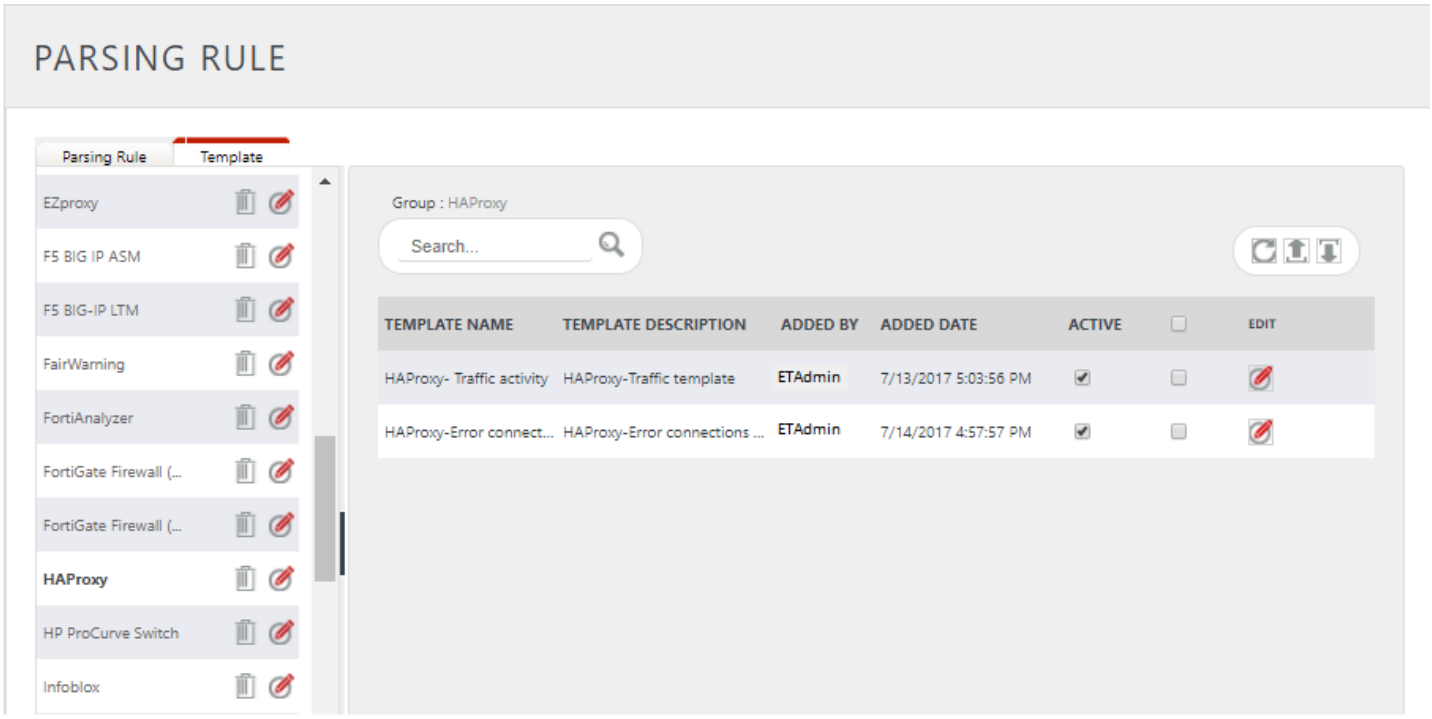


Figure 8

Flex Reports

1. In the **EventTracker Enterprise** web interface, click the **Reports** menu, and then select **Configuration**.
2. In **Reports Configuration** pane, select **Defined** option.
3. In search box enter '**HAProxy**, and then click the **Search** button.
   EventTracker displays Flex reports of '**HAProxy**'.

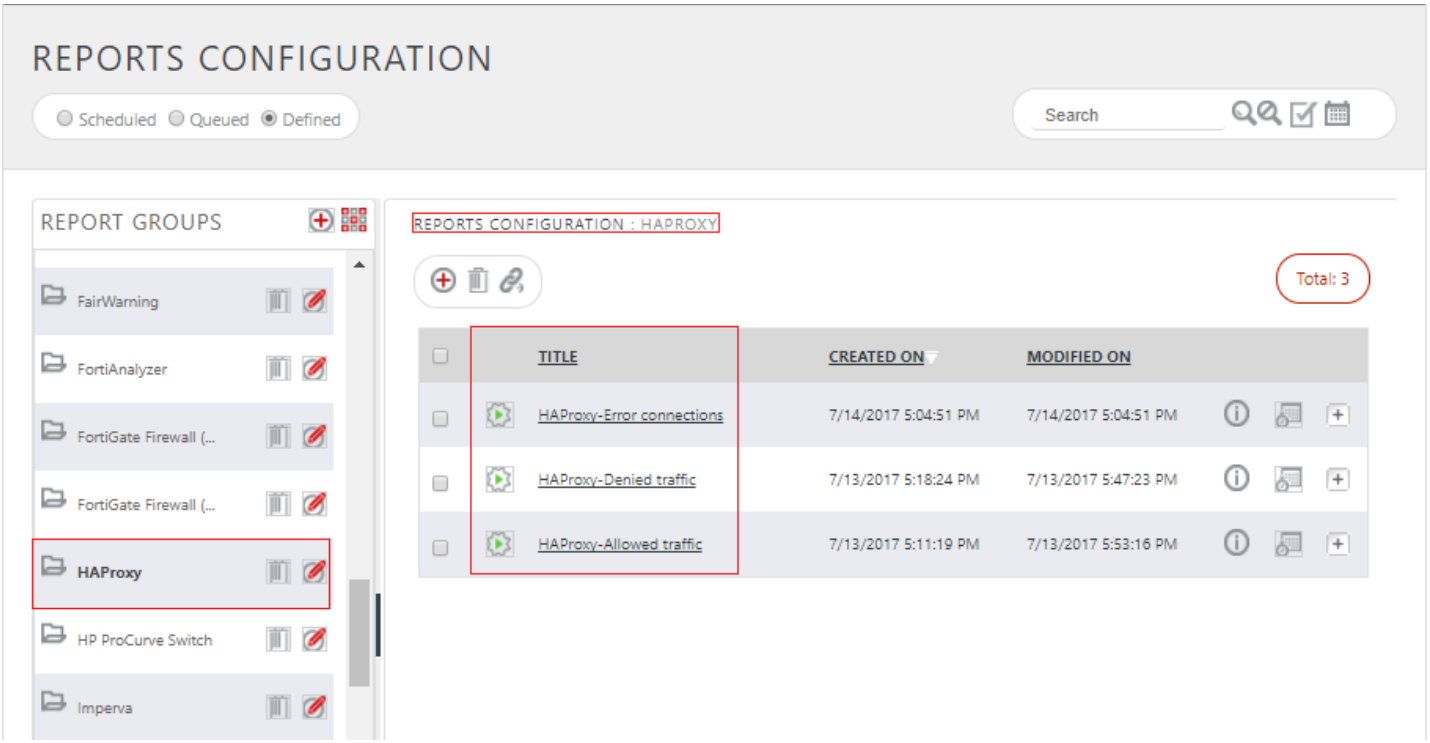


Figure 9

Create Flex Dashboards in EventTracker

NOTE: To configure the flex dashboards, schedule and generate the reports. Flex dashboard feature is available from EventTracker Enterprise v8.0.

Schedule Reports

1. Open **EventTracker** in browser and logon.

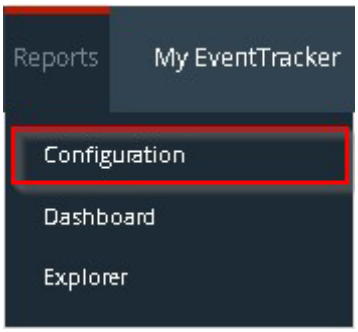


Figure 10

2. Navigate to **Reports>Configuration**.
3. Select **HAProxy** in report groups. Check **Defined** dialog box.

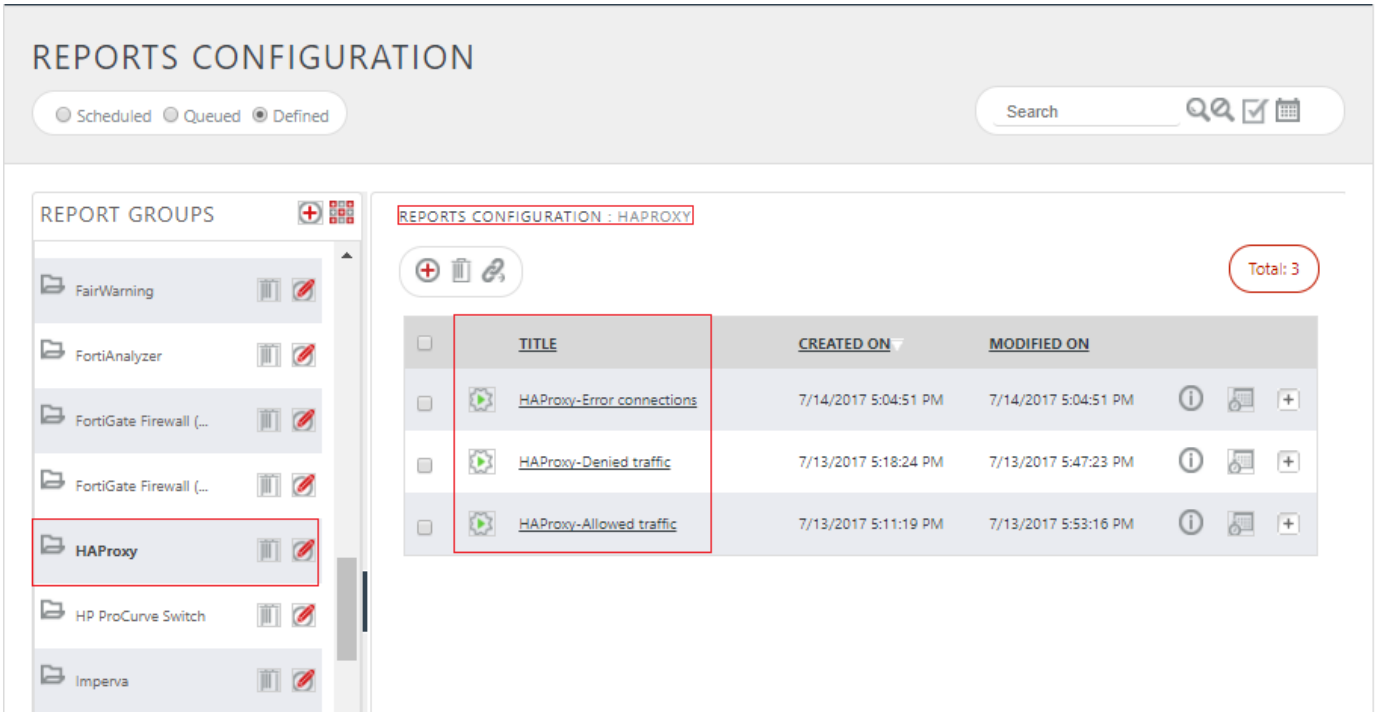


Figure 11

4. Click on '**schedule**'  to plan a report for later execution.
5. Click **Next** button to proceed.
6. In review page, check **Persist data in EventVault Explorer** option.

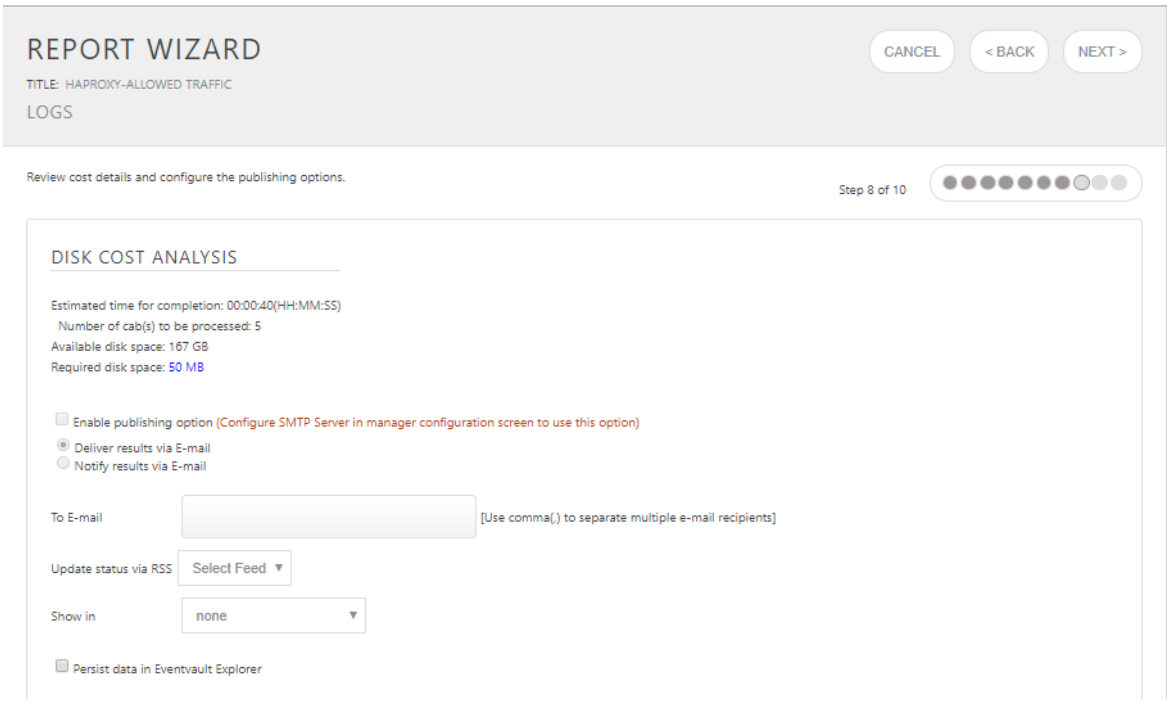


Figure 12

7. In next page, check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.

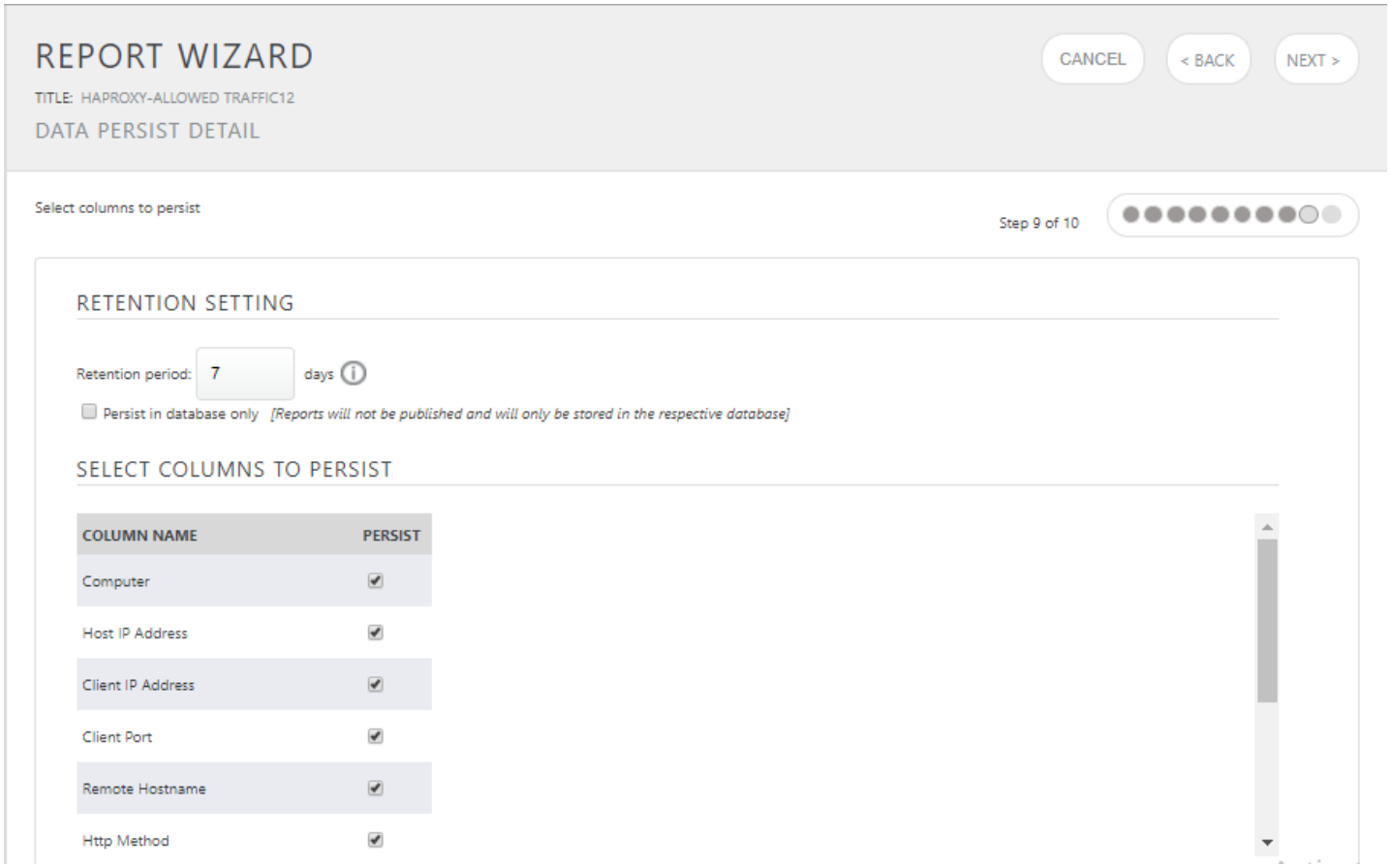


Figure 13

8. Proceed to next step and click **Schedule** button.
9. Wait till the reports get generated.

Create Dashlets

1. Open **EventTracker Enterprise** in browser and logon.

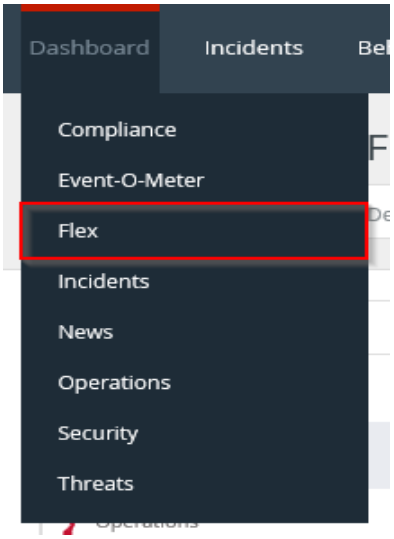


Figure 14

2. Navigate to **Dashboard>Flex**.
   Flex Dashboard pane is shown.

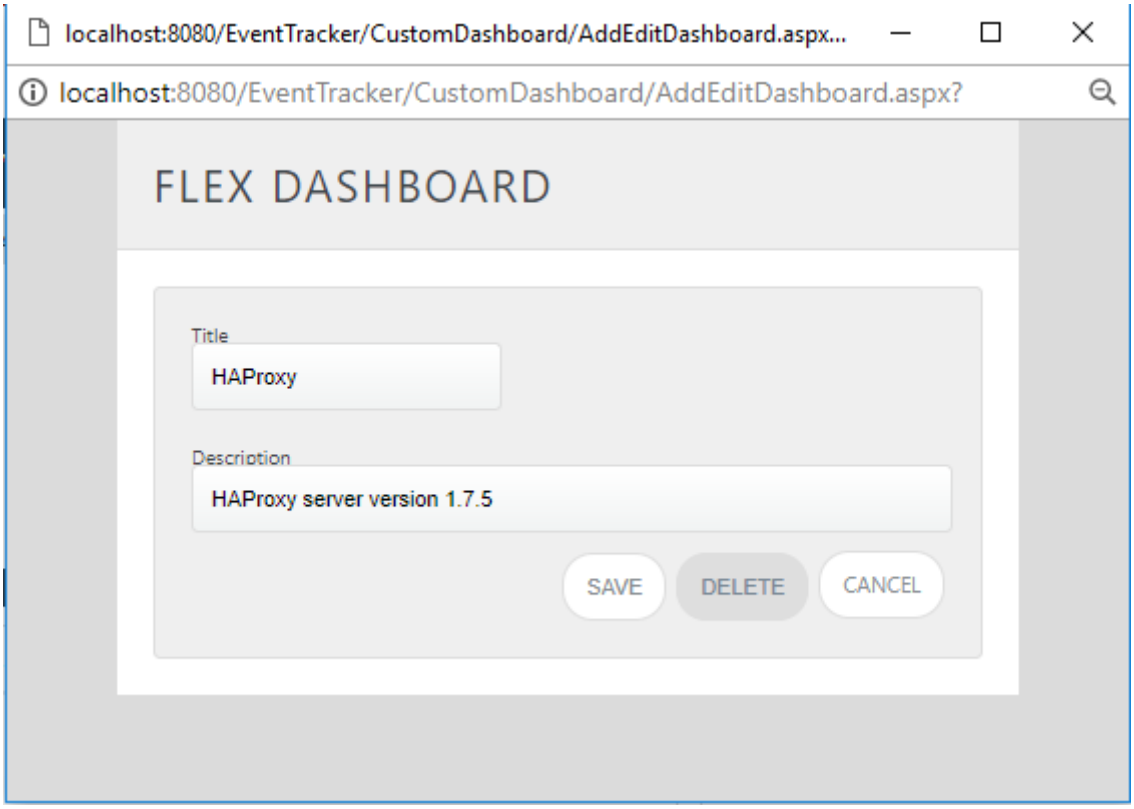


Figure 15

3. Fill suitable title and description and click **Save** button.
4. Click ⚙ to configure a new flex dashlet. Widget configuration pane is shown.

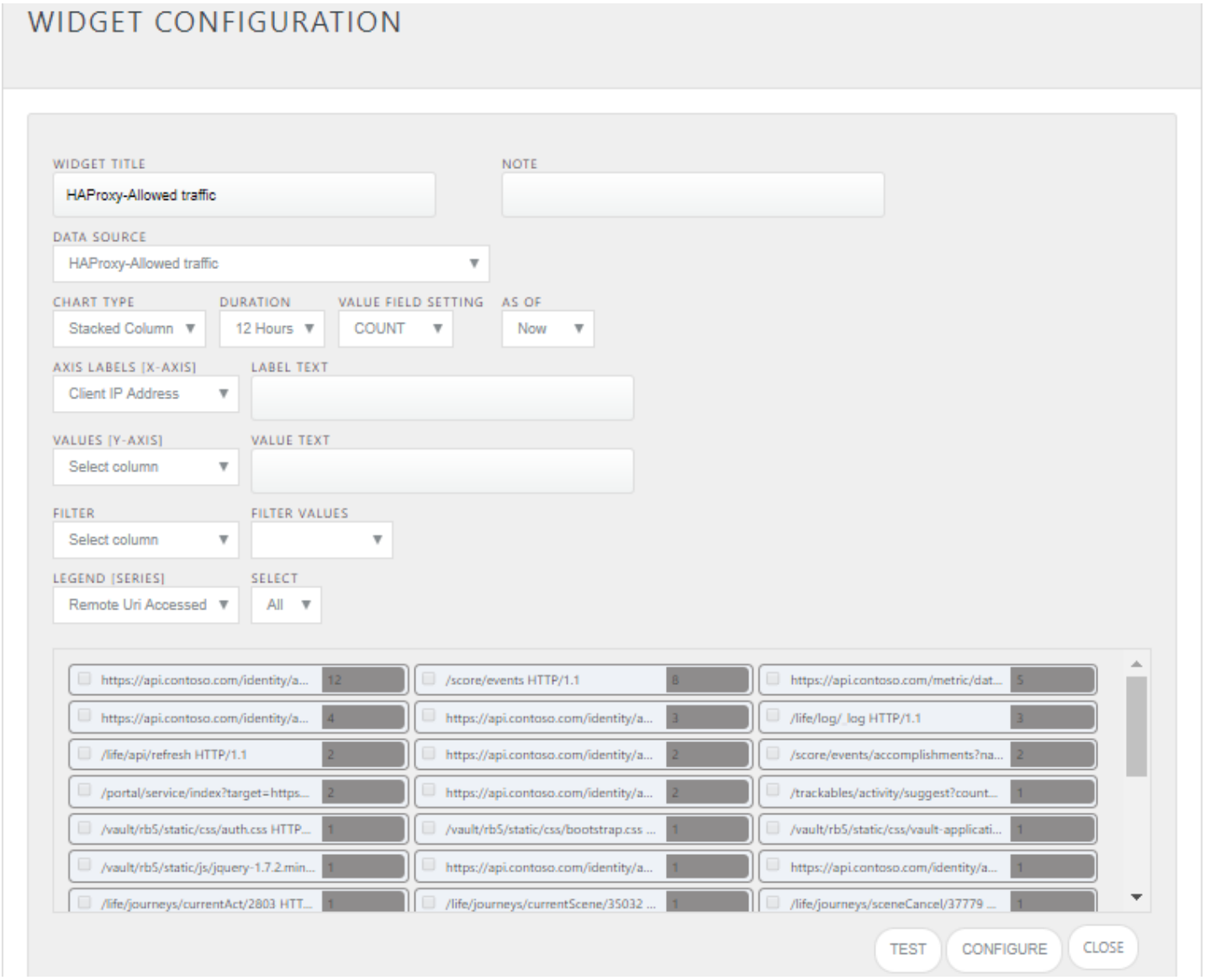


Figure 16

5. Locate earlier scheduled report in **Data Source** dropdown.
6. Select **Chart Type** from dropdown.
7. Select extent of data to be displayed in **Duration** dropdown.
8. Select computation type in **Value Field Setting** dropdown.
9. Select evaluation duration in **As Of** dropdown.
10. Select comparable values in **X Axis** with suitable label.
11. Select numeric values in **Y Axis** with suitable label.
12. Select comparable sequence in **Legend**.
13. Click **Test** button to evaluate. Evaluated chart is shown.

Figure 17

14. If satisfied, click **Configure** button.

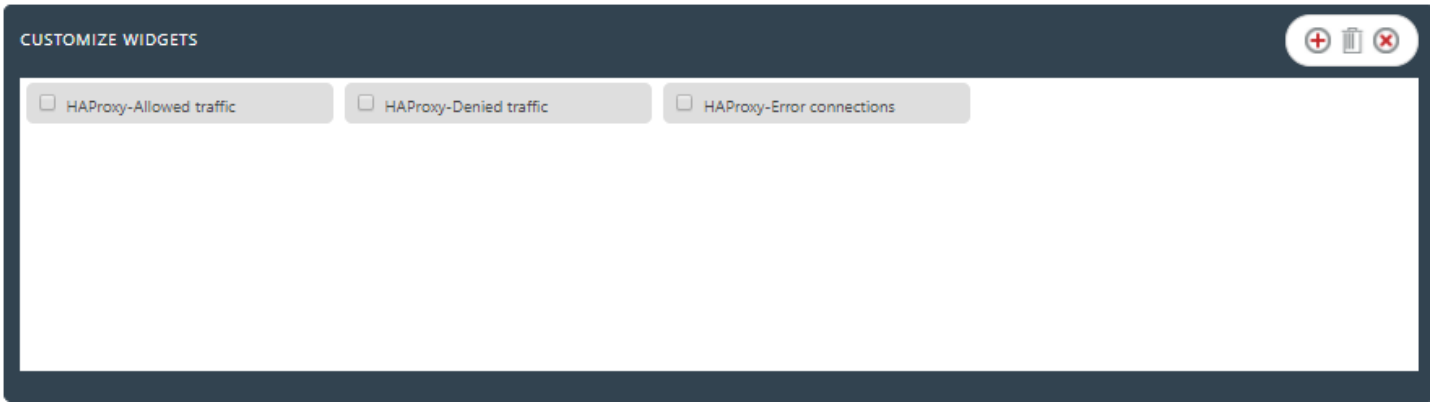
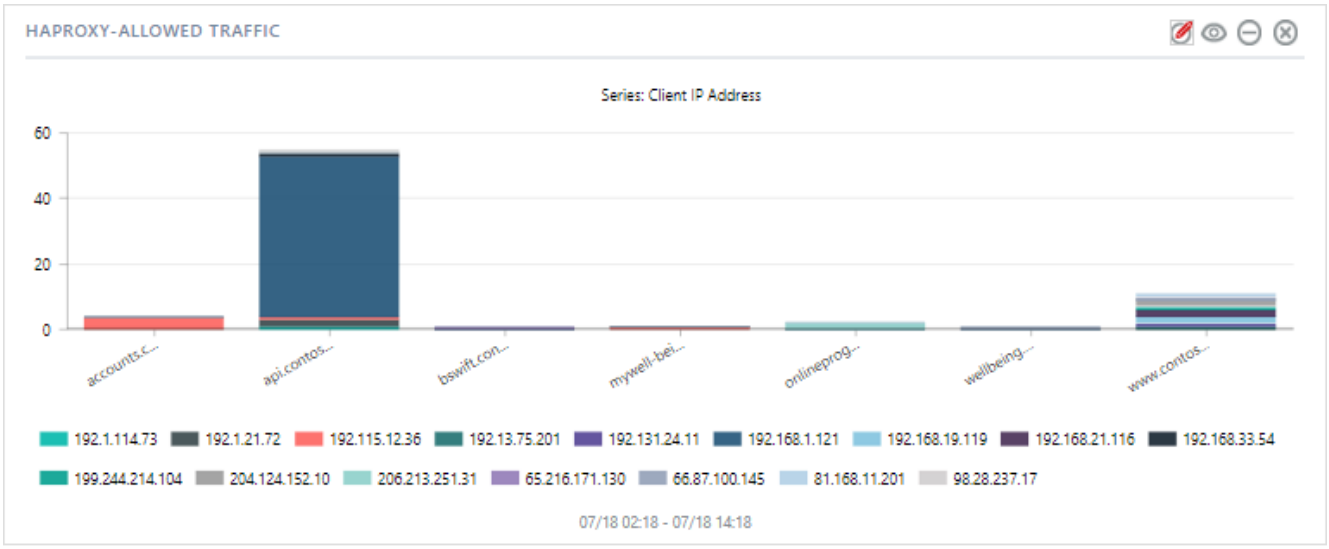


Figure 18

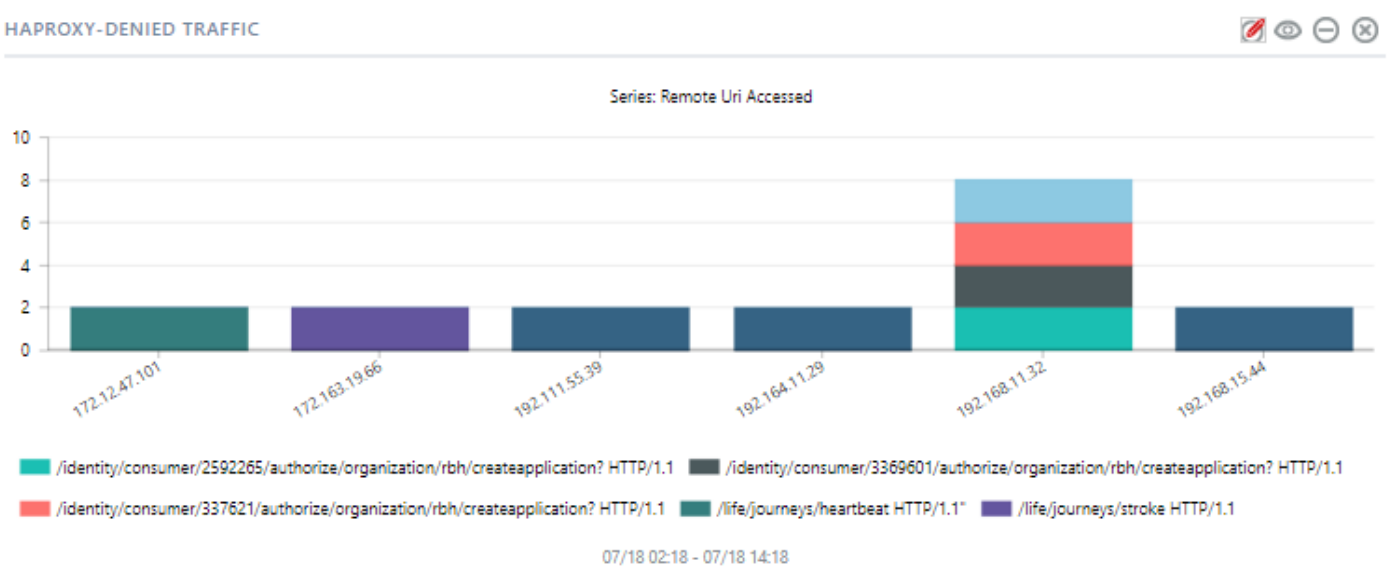
15. Click 'customize' to locate and choose created dashlet.
16. Click to add dashlet to earlier created dashboard.

Sample Flex Dashboards

- **REPORT: HAProxy-Allowed traffic**
  WIDGET TITLE: HAProxy- Allowed traffic
  CHART TYPE: Stacked Column
  AXIS LABELS [X-AXIS]: Remote Uri Accessed
  LEGEND [SERIES]: Client IP Address



- **REPORT: HAProxy-Denied traffic**
  WIDGET TITLE: HAProxy-Denied traffic
  CHART TYPE: Stacked column
  AXIS LABELS [X-AXIS]: Client IP Address
  LEGEND[SERIES]: Uri Accessed



- **REPORT: HAProxy-Error connections**
  WIDGET TITLE: HAProxy-Error connections
  CHART TYPE: Stacked Column
  AXIS LABELS [X-AXIS]: Error Message
  LEGEND[SERIES]: Client IP Address