NethServer 6 - Bug #3370
Access to graphs and reports from trusted network

03/23/2016 07:57 AM - Filippo Carletti

Status:	CLOSED	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	<multiple packages>		
Target version:	v6.7		
Security class:	low	**Resolution:**	
Affected version:	v6.7	**NEEDINFO:**	No

Description

Even if I limit external httpd-admin access from my ip public address, I can view cgp/collectd graphs and lightsquid reports fro anywhere.
The URL is "obfuscated" and hard to guess, but I'd prefer to enforce access following httpd-admin access control.

Related issues:

Related to NethServer 6 - Bug # 3402: Syntax error in cgp and collectd-web ht...	**CLOSED**

Associated revisions

Revision 7a9fe5cd - 05/06/2016 09:39 AM - Giacomo Sanchietti

Http conf: restrict access if httpd-admin[AllowHosts] is set. Refs #3370

Revision 0531f2b2 - 05/06/2016 09:41 AM - Giacomo Sanchietti

httpd: restrict access if httpd-admin[AllowHosts] is set. Refs #3370

History

#1 - 03/23/2016 08:05 AM - Filippo Carletti

- Status changed from NEW to TRIAGED

- % Done changed from 0 to 20

CGP and collectd-web are missing a Deny directive:

```
# tail -8 /etc/e-smith/templates/etc/httpd/conf.d/cgp.conf/10base
<Directory /var/www/html/cgp>
    Options Indexes FollowSymLinks MultiViews
    AllowOverride all
    Order deny,allow
    Allow from $localAccess
</Directory>
```

We need a "Deny from all" before "Allow from".

I also think that the access prop in /etc/e-smith/templates/etc/httpd/conf.d/cgp.conf/01localAccessString should be changed from ValidFrom to AllowHosts.

#2 - 05/06/2016 06:39 AM - Filippo Carletti

- Tracker changed from Enhancement to Bug

- Category set to <multiple packages>

- Security class set to low

#3 - 05/06/2016 08:41 AM - Giacomo Sanchietti

- Status changed from TRIAGED to ON_DEV

- Assignee set to Giacomo Sanchietti

- % Done changed from 20 to 30

- Affected version set to v6.7

#4 - 05/06/2016 09:27 AM - Giacomo Sanchietti

We should avoid to modify the actual behavior while providing a safe way to allow graphs access only from trusted networks.
Proposed solution:

- if AllowHosts is set, the access must be enable only from listed networks
- otherwise, the access should be enable by all networks

#5 - 05/06/2016 09:45 AM - Giacomo Sanchietti

- Status changed from ON_DEV to MODIFIED

- % Done changed from 30 to 60

#6 - 05/06/2016 09:49 AM - Giacomo Sanchietti

- Status changed from MODIFIED to ON_QA

- Assignee deleted (Giacomo Sanchietti)

- % Done changed from 60 to 70

Packages in nethserver-testing:

- nethserver-lightsquid-1.0.3-1.1.g7a9fe5c.ns6.noarch.rpm
- nethserver-cgp-1.0.0-1.2.g0531f2b.ns6.noarch.rpm
- nethserver-collectd-web-1.0.2-1.noarch.rpm

Test case 1

- Do not set AllowHosts parameter for httpd-admin service inside Network Services page
- Check Lightsquid/CGP/Collected web are accessible from any network

Test case 2

- Set AllowHosts parameter for httpd-admin service inside Network Services page
- Check Lightsquid/CGP/Collected web are accessible only from networks listed inside AllowHosts

#7 - 05/20/2016 05:01 AM - dz0 0te

- Assignee set to dz0 0te

#8 - 05/20/2016 10:57 AM - dz0 0te

- Status changed from ON_QA to TRIAGED

- Assignee deleted (dz0 0te)

- % Done changed from 70 to 20

System and Package Version installed

VM KVM - Clean install of Nethserver 6.7 fully updated

Package Installed:

Other Package installed: DNS and DHCP server
Statistics
Web proxy
Web server

Test Original Problem
Bug

Install Updated Package

yum --enablerepo=nethserver-testing update nethserver-lightsquid-1.0.3-1.1.g7a9fe5c.ns6.noarch nethserver-cgp-1.0.0-1.2.g0531f2b.ns6.noarch nethserver-collectd-web-1.0.2-1.ns6.noarch

Test Results after update
Test Case 1:
ok. access from any network

Test Case 2:
in http-admin service select only from green: access from any network on ip/cgp and ip/collectd-web (lightsquid not tested) in http and https
access to web console is blocked from any network correctly

Test Case 3:
in http-admin service select only from green with Allow Host a single ip: access from any network on ip/cgp and ip/collectd-web (lightsquid not tested) in http and https
access to web console is restricted to the IP correctly

Test Case 4:
in http-admin service select only from localhost : access from any network on ip/cgp and ip/collectd-web (lightsquid not tested) in http and https
access to web console is restricted to all correctly

the only way to vlock access is Set AllowHosts parameter for httpd service
inside Network Services page

Verified or Reopen
Reopen

Note

#9 - 05/24/2016 04:52 AM - Giacomo Sanchietti

When changing the httpd-admin access property the system fires the firewall-adjust event.
The only way to fully automate the configuration changes to lightsquid, cgp, etc is the expansion of all templates and httpd restart inside the firewall adjust event.

I'd like to avoid such an overload for this rare scenario.

#10 - 05/25/2016 10:51 AM - Filippo Carletti

> *I'd like to avoid such an overload for this rare scenario.*

I agree. Given that v7 has solved this "problem" I'd release the updated package which improves the access restrictions.

#11 - 05/26/2016 02:22 AM - Giacomo Sanchietti

- Status changed from TRIAGED to MODIFIED

- % Done changed from 20 to 60

Actual implementation confirmed.

#12 - 05/26/2016 02:22 AM - Giacomo Sanchietti

- Status changed from MODIFIED to ON_QA

- % Done changed from 60 to 70

#13 - 05/26/2016 02:22 AM - Giacomo Sanchietti

- Status changed from ON_QA to VERIFIED

- % Done changed from 70 to 90

#14 - 05/26/2016 02:30 AM - Giacomo Sanchietti

- Status changed from VERIFIED to CLOSED

- % Done changed from 90 to 100

Released in nethserver-updates:

- nethserver-cgp-1.0.1-1.ns6.noarch.rpm
- nethserver-collectd-web-1.0.3-1.ns6.noarch.rpm
- nethserver-lightsquid-1.0.4-1.ns6.noarch.rpm

#15 - 06/07/2016 10:20 AM - Filippo Carletti

- Related to Bug #3402: Syntax error in cgp and collectd-web httpd conf added