D4Science Infrastructure - Incident #232

node51.p.d4science.research-infrastructures.eu webapp unresponsive. The ajp port is open with connections from China

Jun 06, 2015 12:44 PM - Andrea Dell'Amico

Status:	Closed	**Start date:**	Jun 06, 2015
Priority:	Urgent	**Due date:**	
Assignee:	Roberto Cirillo	**% Done:**	100%
Category:	System Application	**Estimated time:**	0.00 hour
Target version:	UnSprintable		
Infrastructure:	Production		

Description

The 8080 (and 8005) tomcat port has been closed since last night.
The actual 'netstat -na' output is:

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:4949            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5666            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8627            0.0.0.0:*               LISTEN
tcp        0      0 146.48.122.127:22       146.48.123.11:54985     ESTABLISHED
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::45339                :::*                    LISTEN
tcp6       0      0 :::4000                 :::*                    LISTEN
tcp6       0      0 :::4001                 :::*                    LISTEN
tcp6       0      0 146.48.122.127:8009     61.240.144.65:60000     ESTABLISHED
tcp6       0      0 146.48.122.127:8009     61.240.144.67:60000     ESTABLISHED
tcp6       0      0 146.48.122.127:42774    146.48.122.255:6166     ESTABLISHED
udp        0      0 146.48.122.127:55702    239.2.10.67:8627        ESTABLISHED
udp        0      0 146.48.122.127:8627     0.0.0.0:*
udp        0      0 0.0.0.0:8627            0.0.0.0:*
udp6  124860      0 :::4446                 :::*
udp6       0      0 :::4446                 :::*
```

The two IPs connected to the 8009 (ajp) port are from a chinese network.
The 4446 udp port has been opened by tomcat or one of the running apps, but I don't know the reason.
The load average is costantly around 1.00, while there's no memory pressure.

I completely stopped the tomcat container to get rid of the rogue connections.

History

#1 - Jun 08, 2015 11:04 AM - Roberto Cirillo

On node51.p (pre production host) there are the following services:

- executionengineservice-search
- searchsystemservice

I'm going to analyze the logs

#2 - Jun 08, 2015 11:34 AM - Roberto Cirillo

If there isn't an apache frontend on this host, I think is better to disable the 8009 port in the server.xml file. I think someone could abuse of 8009 port as happened in the latest days.
What do you think about it?

#3 - Jun 08, 2015 11:38 AM - Andrea Dell'Amico

It surely needs to be closed.

The ajp port is always of no use on our systems, because we always use the http port even for the apache frontends.
Even if we wanted to use it, it should be configured to bind on localhost only.

I'm more worried about the udp port 4446, is it open by one of the d4science services?

#4 - Jun 08, 2015 11:52 AM - Roberto Cirillo

I don't know this. The d4science services hosted on this VM are related to an elastic search cluster and, maybe, this port is used for this. I've added John to this ticket, maybe John can answer to this question.

#5 - Jun 08, 2015 12:49 PM - John Gerbesiotis

Searchsystem service communicates with elasticsearch, which is on another vm and with pottal.

To my knowledge, elasticsearch does not use the port 4446. Moreover, searchsystem exploits elasticsearch through http rest api, so there is no need for other communication to elasticsearch node. Portal exploits searchsearvice throught resultset which communicates at another port (e.g. 4000-4010).

I searched logs of elasticsearch, searchsystem and portal of the development environment and didn't find 4446 port exploitation.

At least, we could limit access to the production subnet? Otherwise, if there is a change in firewall, we have to check the status of the services.

#6 - Jun 08, 2015 04:03 PM - Roberto Cirillo

as John said, for this VM I think is better to limit access to our subnet. The services hosted on node51.p have to communicate with: DTS, index-service, portal, Information-System and Registry of preproduction environment. All these services are deployed to CNR, so, I think we could try to restrict the access to the CNR net.

#7 - Jun 08, 2015 04:15 PM - John Gerbesiotis

Well, search services should be publicly available for REST APIs also, as such, 8080 should be public at least. We could only protect irrelevant ports with the services, such as 8009. Correct me if I am wrong.

#8 - Jun 08, 2015 04:23 PM - Andrea Dell'Amico

Port 8009 is now closed. What's worrying me is udp 4446, it's opened by one of the tomcat webapps but I don't know if it's used by some services.

#9 - Jun 08, 2015 04:26 PM - John Gerbesiotis

I suggest limiting 4446 to subnet only.

#10 - Jun 08, 2015 04:44 PM - Roberto Cirillo

I've notice on node51.p there are the ehcache jars. I don't know how the ehcache is configured but I've seen that a kind of setting is:

```
<cacheManagerPeerProviderFactory
class="net.sf.ehcache.distribution.RMICacheManagerPeerProviderFactory"
properties="peerDiscovery=automatic, multicastGroupAddress=230.0.0.1,
multicastGroupPort=4446, timeToLive=32"/>
```

with multicastGroupPort=4446....
Maybe the 4446 port is used by ehcache ?

#11 - Jun 09, 2015 12:21 PM - John Gerbesiotis

Yes searchsystem uses ehcache and the default port of ehcache is 4446.

#12 - Jun 09, 2015 12:24 PM - Roberto Cirillo

- *% Done changed from 0 to 100*

I think we can close the ticket now

#13 - Jun 09, 2015 12:26 PM - Roberto Cirillo

- *Status changed from New to In Progress*
- *% Done changed from 100 to 90*

Andrea, do you want to add an iptables rule for this port?

#14 - Jun 09, 2015 12:37 PM - Andrea Dell'Amico

John Gerbesiotis wrote:

> Yes searchsystem uses ehcache and the default port of ehcache is 4446.

And that port is effectively used to talk with other instances?
In a tcpdump session I've seen only broadcast traffic from other - completely unrelated - servers that happen to live on the same network.

> Andrea, do you want to add an iptables rule for this port?

Yes. I'd limit it to localhost only if it does not need to talk to anyone else.

#15 - Jun 09, 2015 12:42 PM - John Gerbesiotis

No it is a feature of ehcache that is not being exploited. Searchsystem's ehcache does not talk with other service instances. It is enabled by default.

#16 - Jun 09, 2015 01:16 PM - Andrea Dell'Amico

- Status changed from In Progress to Closed

- % Done changed from 90 to 100

The iptables rules are active.