D4Science Infrastructure - Task #98

MongoDB in production: allow only trusted connections

May 14, 2015 05:16 PM - Massimiliano Assante

Status:	Closed	**Start date:**	May 14, 2015
Priority:	High	**Due date:**	
Assignee:	Andrea Dell'Amico	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	System Configuration		
Infrastructure:	Production		

Description

Only allow trusted clients to connect to the port for the mongod instances.
The ports used are: 27017, 28017
Following the list of instances in production:
{{{
node58.p.d4science.research-infrastructures.eu
node67.p.d4science.research-infrastructures.eu
node73.p.d4science.research-infrastructures.eu
node80.p.d4science.research-infrastructures.eu
node84.p.d4science.research-infrastructures.eu
}}}

The networks considered trusted for the storage area are all the networks where gCore nodes or smartgears nodes are deployed.
Follow the list of networks:
fao.org
edu.tw
uoa.gr
vliz.be

History

#1 - May 15, 2015 02:28 PM - Pasquale Pagano

- Target version set to System Configuration

#2 - May 27, 2015 02:22 PM - Luca Frosini

- Assignee changed from Tommaso Piccioli to Andrea Dell'Amico

#3 - May 27, 2015 06:24 PM - Andrea Dell'Amico

Two considerations

1. 28017 is the http port that shows the server status. Is it really needed? even from outside?
2. We need networks and not domain names. It's not possible to obtain complete information about the involved networks from a domain name.

#4 - Jun 03, 2015 11:08 AM - Roberto Cirillo

1. 28017 port should be closed from outside
2. I don't know if is possible to obtain the networks from a domain name. There is a way to do it?

#5 - Jun 03, 2015 11:56 AM - Andrea Dell'Amico

Roberto Cirillo wrote:

> 1. 28017 port should be closed from outside

Ok

> 1. I don't know if is possible to obtain the networks from a domain name. There is a way to do it?

No, there's no connection between domain names and networks. Tommaso produced a networks list some weeks ago, but we don't know if it's complete.

#6 - Jun 10, 2015 05:07 PM - Andrea Dell'Amico

I've found some networks recently used to protect another service on node21.p.d4science.research-infrastructures.eu:

```
ext_nets:
  fao_org_1: 193.43.36.0/24
  uoa_gr_1: 195.134.64.0/18
  uoa_gr_2: 88.197.0.0/17
```

I need to find the networks for vliz.be and edu.tw.
If we do not have a clue I'll sniff the traffic on the mongodb servers.

#7 - Jun 11, 2015 02:39 PM - Andrea Dell'Amico

- File lista-reverse-addresses added

#9 - Jun 11, 2015 03:35 PM - Andrea Dell'Amico

- Status changed from New to In Progress

I did not found any connections from .tw hosts, but I composed a list that includes more that what initially asked:

```
  vliz_be_1: 193.191.134.0/24
  fao_org_1: 193.43.36.0/24
  uoa_gr_1: 195.134.64.0/18
  uoa_gr_2: 88.197.0.0/17
# Greek Research and Technology Network (GRNET) S.A.
  grnet_1: 83.212.96.0/19
# UE
  ue_comm_1: 147.67.0.0/16
  engineering_1: 91.109.57.0/24
  cern_1: 128.141.0.0/16
  cern_2: 128.142.0.0/16
  cern_3: 137.138.0.0/16
# Barcelona Supercomputer Center
  barcelona_sc_1: 84.88.0.0/16
# Barcelona, Politecnico
  barcelona_upc_1: 147.83.0.0/16
# Valencia, Politecnico
  valencia_upv_1: 158.42.0.0/16
```

Talking with Roberto, they all seem legitimate networks.

Let me know how to proceed. Do we want to include all those?

#10 - Jun 11, 2015 03:43 PM - Roberto Cirillo

Yes Andrea. Please, include all these network.

#11 - Jun 11, 2015 04:29 PM - Andrea Dell'Amico

- Status changed from In Progress to Feedback

- % Done changed from 0 to 90

The iptables rules are now active.

#12 - Jun 12, 2015 02:26 PM - Andrea Dell'Amico

- Status changed from Feedback to Closed

- % Done changed from 90 to 100

Files

lista-reverse-addresses	19.7 KB	Jun 11, 2015	Andrea Dell'Amico