D4Science Infrastructure - Task #2508

No firewall on the cassandra hosts

Mar 09, 2016 12:16 PM - Andrea Dell'Amico

Status:	Closed	**Start date:**	Mar 09, 2016
Priority:	Urgent	**Due date:**	
Assignee:	_InfraScience Systems Engineer	**% Done:**	100%
Category:	System Application	**Estimated time:**	0.00 hour
Target version:	System Configuration		
Infrastructure:	Development, Production		

Description

The cassandra hosts are open to the world.

Do we know which hosts can connect and on what ports?

History

#1 - Mar 09, 2016 12:32 PM - Massimiliano Assante

which cassandra hosts are you referring about? dev or production?

#2 - Mar 09, 2016 12:34 PM - Massimiliano Assante

We had firewalls on the previous Production Cassandra Cluster (which was dismissed last month) I assumed we would have the same for the new Production cluster.

As for the 2 dev cassandra hosts it is ok to have them open for me.

#3 - Mar 09, 2016 12:36 PM - Andrea Dell'Amico

Massimiliano Assante wrote:

> which cassandra hosts are you referring about? dev or production?

Both of them.

#4 - Mar 09, 2016 12:39 PM - Andrea Dell'Amico

Massimiliano Assante wrote:

> We had firewalls on the previous Production Cassandra Cluster (which was dismissed last month) I assumed we would have the same for the new Production cluster.

The only firewall rules that I know of on a cassandra cluster of ours are the ones on the social-isti nodes. And are too broad, because it seems that nobody knew what ports needed to be open and to what hosts.

> As for the 2 dev cassandra hosts it is ok to have them open for me.

Hm. Maybe more relaxed rules, but it should be better have them on the dev cluster too. It could be used as a test for the production rules, it seems that we still don't know exactly how to configure them.

#5 - Mar 09, 2016 12:42 PM - Massimiliano Assante

I'm sure @tommaso.piccioli@isti.cnr.it put firewall rules at the time on the dismissed cassandra cluster

#6 - Mar 09, 2016 12:54 PM - Tommaso Piccioli

Don't be so sure, I can't find any firewall rule on the dismissed cluster.

#7 - Mar 09, 2016 12:58 PM - Massimiliano Assante

Tommaso Piccioli wrote:

> Don't be so sure, I can't find any firewall rule on the dismissed cluster.

I remember we discussed about it and you put that in place, also i remember Costantino could not connect to the (dismissed) production cluster from his machine, while I could with my IP.

#8 - Mar 09, 2016 02:04 PM - Andrea Dell'Amico

Some info about the ports used by cassandra:

https://docs.datastax.com/en/cassandra/2.0/cassandra/security/secureFireWall_r.html
https://wiki.apache.org/cassandra/FAQ#ports

About the JMX port: we could need it to monitor the cluster from the monitoring host, but we also can run the checks locally. In the past JMX opened a random port to talk with the clients, but starting from JDK 7.0.25 it's possible to configure the jdk to work using the defined port only.

#9 - Mar 09, 2016 02:11 PM - Tommaso Piccioli

This is the only I can find and was on the old node1.d.cassandra disk:

```
# Generated by iptables-save
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
#
# Allow all on loopback
-A INPUT -i lo -j ACCEPT 
# Allow munin port
-A INPUT -m state --state NEW -s 146.48.122.15 -p tcp -m tcp --dport 4949 -j ACCEPT
-A INPUT -m state --state NEW -s 146.48.87.88 -p tcp -m tcp --dport 4949 -j ACCEPT
# Allow all for me
-A INPUT -s 146.48.87.112 -j ACCEPT
-A INPUT -s 146.48.123.112 -j ACCEPT
# Allow previously established connections
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
# Allow icmp
-A INPUT -p icmp -j ACCEPT
# Allow port 22 (ssh) connections to firewall
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
# Allow cassandra ports
-A INPUT -m state --state NEW -p TCP -s 146.48.122.25 --dport 1024:65535 -j ACCEPT
-A INPUT -m state --state NEW -p TCP -s 146.48.122.106 --dport 1024:65535 -j ACCEPT
-A INPUT -m state --state NEW -p TCP -s 146.48.87.174 --dport 1024:65535 -j ACCEPT
# next only for cassandra inter-node communication
#-A INPUT -m state --state NEW -p TCP -s 146.48.122.106 --dport 7000 -j ACCEPT
#
# Close up firewall. All else blocked.
-A INPUT -j REJECT --reject-with icmp-host-prohibited
#
COMMIT
#
```

#10 - Mar 09, 2016 11:50 PM - Andrea Dell'Amico

Those are similar to the ones installed on the social-isti cluster.
We know which ports are actually used, so my proposal is to try stricter rules on the devel cluster, test them there and then install them on the production cluster.

Is it OK?

#11 - Mar 10, 2016 10:40 AM - Massimiliano Assante

ok

#12 - Mar 14, 2016 03:35 PM - Andrea Dell'Amico

The new rules wil permit traffic between the cluster hosts on the ports: 7000, 7001.
Port 9042 and 9160 will be open to the world (or better to the hosts that need to talk with cassandra. Do we know who they are?)

#13 - Mar 14, 2016 03:36 PM - Andrea Dell'Amico

- Status changed from New to In Progress

#14 - Mar 14, 2016 03:43 PM - Massimiliano Assante

the d4science gateways and the Elastic Search Cluster (Not yet in production, but existing in dev) and a Smart Executor Plugin (Not yet in production, but existing in dev) in charge of indexing social data

#15 - Mar 14, 2016 03:43 PM - Massimiliano Assante

and my IP and Constantino's

#16 - Mar 14, 2016 03:52 PM - Andrea Dell'Amico

Massimiliano Assante wrote:

> the d4science gateways and the Elastic Search Cluster (Not yet in production, but existing in dev) and a Smart Executor Plugin (Not yet in production, but existing in dev) in charge of indexing social data

OK. So at least in dev I can open to the 146.48.122.0/23 and the two desktop IPs. I'm going to deploy the iptables rules in dev in 5 minutes.

#17 - Mar 14, 2016 04:11 PM - Andrea Dell'Amico

The firewall rules are active on cassandra1-d-d4s. cassandra2-d-d4s needs a reboot to activate the firewall, because the running kernel has no iptables support.

#18 - Mar 14, 2016 04:34 PM - Andrea Dell'Amico

cassandra2-d has been restarted.

Let me know if it's all OK on the cluster.

#19 - Mar 14, 2016 04:46 PM - Andrea Dell'Amico

- % Done changed from 0 to 50

#20 - Mar 15, 2016 04:32 PM - Andrea Dell'Amico

- Status changed from In Progress to Feedback

- % Done changed from 50 to 100

Firewall rules deployed on the production cluster too.

#21 - Mar 15, 2016 04:51 PM - Massimiliano Assante

- Status changed from Feedback to Closed