Considerations when using more than one Allstar server on a LAN

The widespread use of the Raspberry Pi has made it much more likely that you will be using more than one server at a given location on a single public IP address. This document describes what you need to do to implement multiple servers in this way.

When you have more than one server on the same private LAN and you want to connect them locally or connect into them from the Internet there are some special setup considerations. Allstar uses a database that is constantly updated with the public IP addresses and ports of all other active nodes on the network including your own. So if you have two (or more) local nodes on different computers and they try to connect to each other they will not be able to. While many routers have “hairpin loopback” some older routers do not know how to handle their own public IP from within the LAN. The nodes on the LAN need to be aware of each others local IP address and port. The rpt.conf files has a section called [nodes] where the local IP address and port information for other nodes in your network can be stored. The node numbers in this section have priority over any listing in the downloaded database. Here is an example showing how to do this for two or more nodes on the same LAN:

First you need to go to Allstarlink.org and put each of your servers (Raspberry Pi's) on a different port. The default iax port is 4569 and when you define a server that is what is assigned. If you have two servers you need to pick one and change the port, say to 4568, 4567, 4566, etc. You do this in the network tab of the server configuration at Allstarlink.org. Only change the port, do not change or add any IP addresses. The IP address setting should be DHCP in most all cases. If you have more than two servers on the LAN just keep assigning new port numbers for each. The bindport option in /etc/asterisk/iax.conf should match the port selected at allstarlink.org. In addition if you have Hamvoip registrations the port in the registration line also needs to match the bindport.

Here is an example showing the bindport. The servers port is assigned in /etc/asterisk/iax.conf -

[general]
bindport=4569 <<<< change this to the same port that you assigned for this server at Allstarlink.org

The port in Hamvoip registrations looks like this -

register=40000#**4569:ze**fv5dnkRgS3l@register.hamvoip.org

Do this for each server. It is best to write these things down. While you can go back and find all this information again it is much easier to see it written in front of you. Something like this:

System Name	Node#	Node PW	IP Address	Port	Server Name
wa3dsp-40000	**40000**	**123456**	**192.168.1.101**	**4569**	**Demo1**
wa3dsp-40001	**40001**	**654321**	**192.168.1.100**	**4568**	**Demo1**

Then you need to add entries in /etc/asterisk/rpt.conf. Here is an example for two servers:

If you had two nodes, each on a different server and server1 with node 40000 had an IP address of 192.168.1.101 and port of 4569 and server2 with node 40001 had an IP address of 192.168.1.100 with a port of 4568 then you would put the following in nodes section of your rpt.conf file:

[nodes]
; Note, if you are using automatic update for Allstar link nodes,
; no Allstar link nodes should be defined here. Only place a definition
; for your local nodes, and private (off of Allstar link) nodes here.

40000 = radio@127.0.0.1/40000,NONE
40001 = radio@192.168.1.100:4568/40001,NONE <<<< IP and port of other local server

On the other server it would be just reversed with the other nodes IP address and port. 4569 is default and would not need to be entered but shown here for clarity.

[nodes]
; Note, if you are using automatic update for Allstar link nodes,
; no Allstar link nodes should be defined here. Only place a definition
; for your local nodes, and private (off of Allstar link) nodes here.

40001 = radio@127.0.0.1/40001,NONE
40000 = radio@192.168.1.101:4569/40000,NONE <<<< IP and port of other local server

In addition to doing this if you want outside connectivity to your nodes you need to open ports in your router. In this example you would add port 4569 udp to IP address 192.168.1.101 and another entry for port 4568 udp to IP address 192.168.1.100

Also if you want outside ssh access there are two things you can do. If you want direct public ssh access to both servers then you would need to change one servers ssh port since they would both be on port 222. You do this in /etc/ssh/sshd_config on the Raspberry Pi or in /etc/sshd_config on Centos. This can also be done in the admin menu. Change the port number and remember what it is as you will have to use this port to log into this server in the future. One could stay at 222 and the other might be 223. You would then add both entries to your

routers port forwarding. If server1 was port 222 and server2 was 223 then add port 222 tcp 192.168.1.101 and port 223 tcp 192.168.1.100 entries to your router. These port numbers are just examples. You are free to use other port numbers if you desire. ssh is tcp when port forwading.

Another option would be to leave them both at port 222 and then you can log into which ever one is port forwarded. You would only forward one server in your router. Lets say port 222 was routed to 192.168.1.101, server1. When you ssh from the outside to your public IP address at port 222 it would go to that server. But you really want to get to server2. So once you log into server1 you simply type - ssh root@192.168.1.100 -p 222 - Now you get the server2 login, enter your password and you are connected there.

If you only want LAN ssh access not public then you can just connect by local IP address. No port change and no router entries are necessary.

If you are using lsnodes or Allmon/Supermon and you want public access to multiple servers behind a LAN you will need to change the web server ports on the 2nd and subsequent servers and forward them appropriately in your router. The default is port 80 but this could be changed to some more obscure series of ports of your choosing. Again if you just want local access no changes are necessary, just use the servers local IP address in the browser. If you change to other than port 80 you need to specify the domain name or IP address and the port in the URL. Http is tcp when forwarding.

Always restart Asterisk whenever you make any of these changes.

SECURITY NOTE

Port 222 for ssh is well known and often hit by hackers. The best way to ensure you are not compromised is to use good passwords – at least 10 characters of upper/lower case letters, numbers, and special characters. This will prevent logins attacks but not tries which can fill logs. Using a completely and random ssh port can help but even in that case hackers can often find and try to login. Keep an eye on the /var/log/btmp file as this logs login attempts. Do -

last -f /var/log/btmp

This will show login attempts. If this file grows in size and it is not you then you are being hit. In worst cases it will fill your tmp file system. To clear the file do -

>/var/log/btmp

and either change you ssh port, turn off or change port forwarding for ssh, or add a firewall rule for it.