Setting up Supermon2 on the Internet

Note that Supermon2 version 2.0 still uses the AMI method of accessing local and remote server data. This will change in upcoming versions to use memcache as the primary means of transferring data. Using memcache will make Supermon2 more secure and much more efficient. It will also eliminate the AMI security issue that exists in current versions.

Accessing Supermon2 Locally or Remotely

Supermon2 is a web application that uses the Apache server running on your Hamvoip Pi. As shipped Hamvoip uses the default port 80 http for web access. So locally you will be able to just type the IP address of your Hamvoip Pi and supermon2. This would look like the following:

192.168.1.120/supermon2 or 10.0.0.50/supermon2

Of course your local IP addresses will differ.

Outside of your LAN or coming in from the Internet you would need to use your public IP or domain name. Since public IP addresses can change you would typically use a dyndns (ddns) to equate a name to the current public IP address. If your public IP address changes the ddns service would update so that using the name would always equate to your public IP. Here is an example of using both:

12.64.128.27/supermon2 or my.ddns.name/supermon2

Again these examples are fictitious. You would have to register a name with a ddns service and setup the script in your router or a computer that notifies the ddns service if your IP address changes. If you are lucky enough to have a static public IP that would not change you could use the IP address.

Hamvoip offers a service that allows you to determine the IP address by node number from the Internet. Essentially this is a free ddns but it requires you to have a registered Allstar node running at the site you want to access. Here is how it is used assuming your node number is 78000 the domain name would be:

78000.ip.hamvoip.org - This would resolve as the public IP address where node 78000 is located.

So the complete string would be:

78000.ip.hamvoip.org/supermon2

All of these examples assume the default port 80 is being used and that if access outside of your LAN is desired you must port forward port 80 TCP to the local IP address of your Supermon2 Pi.

Setting a Different Apache HTTP Port

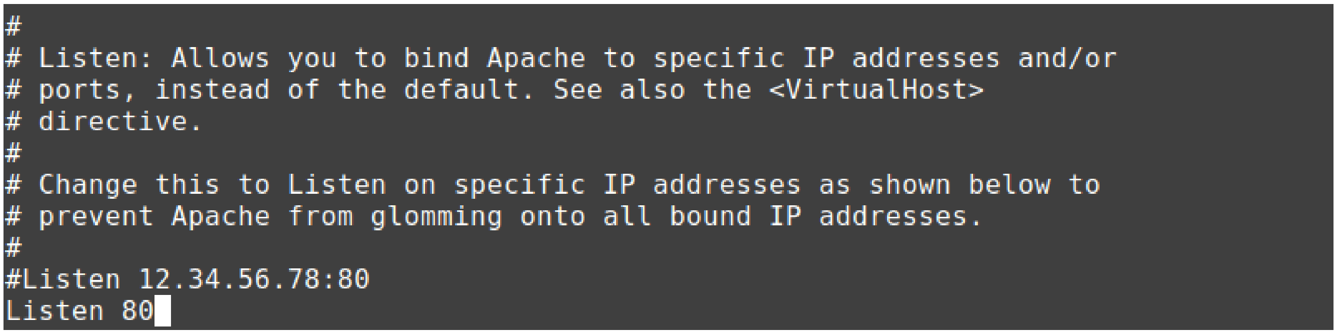
In many cases you may want to change the http port 80 to a different port. This may be because port 80 is being used by some other device or just to add a level of security as the world knows port 80 as the http port and hackers will hit on it just to see what returns. Of course you will have a good login password for you Supermon2 but why expose it to possible abuse.

To change the port you will need to login to your Pi and select the bash prompt from the admin menu. You are then at the linux prompt. Type the following:

cd /etc/httpd/conf/

nano httpd.conf

Scroll down a couple of screens and find these lines:



```
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80
```

The line you are looking to change is the Listen 80. Change the 80 to the port you want to use for http. Any lines with beginning #’s are comments. Typically this is greater than 1024 and less than 65535 so you have a lot to choose from. Just make sure the port you select is not being used by anything else on your LAN.

Once you have changed it type Control X and then yes and enter to save.

You then need to either reboot or restart the httpd process. To do this without rebooting type:

systemctl restart httpd

You can then test by typing your Pi’s local IP address:port in a browser like this:

192.168.1.30:23456

Assuming in this case your IP address is 192.168.1.30 and the port you selected is 23456. You should get this response from your Pi:

THIS IS A TEST !

If you see this the web server is working.

You would then use this port to access the web server on your Pi running Supermon2.

192.168.1.30:23456/supermon2

Browser Selection

Supermon2 works with most browsers like Firefox and Chrome but does NOT work with any Microsoft browsers. Also for security reasons be sure your browser is up to date. Also popups must be activated for the Supermon2 application.

Usernames and Passwords

Supermon2 uses a secure login system. A login is require to perform any actions other than just viewing. Usernames can be anything you want and is often your call or name. Passwords should be random and secure using a combination of at least eight and preferably ten upper/lower case letters, numbers, and special characters. Do not use an exclamation (!) in a password in Supermon2.

Your password is your security in supermon2 so take it seriously if you make your supermon2 accessible to the world. Version 2.0 offers a slew of additional security options that can be put in place as describe in the version 2.0 changes document. This allows you to select by users/pass who can see what buttons and what ini file is used. Selecting an ini file by user means you can select the nodes that user can see and control. This allows a great deal of flexibility if you make Supermon2 available to many users who would have different access restrictions.

Asterisk Manager Setup

The Asterisk Manager Interface or AMI is used to send commands to your various Allstar nodes. Without it Supermon2 would be only a viewing application and not very useful. The AMI setup is detailed in the setup instructions but I will remind you here what needs to be done. The **/etc/asterisk/manager.conf** file needs to be configured with the user/password that you use in your allmon.ini file (or special ini file) for the host (server) you are accessing. The allmon.ini file or any ini file you establish is located in the user_files directory.

So your allmon.ini file would have lines like this assuming node 78000:

```
[78000]
host=127.0.0.1:5038
user=admin
passwd=mypassword
….additional lines
```

and to match this your /etc/asterisk/manager.conf file would look like this:

```
;
; AMI - The Asterisk Manager Interface
;
```

```
; Third party application call management support and PBX event supervision
;
; This configuration file is read every time someone logs in
;
; Use the "manager list commands" at the CLI to list available manager commands
; and their authorization levels.
;
; "manager show command <command>" will show a help text.
;
;
; --------------------------- SECURITY NOTE -------------------------------
; Note that you should not enable the AMI on a public IP address. If needed,
; block this TCP port with iptables (or another FW software) and reach it
; with IPsec, SSH, or SSL vpn tunnel.  You can also make the manager
; interface available over http if Asterisk's http server is enabled in
; http.conf and if both "enabled" and "webenabled" are set to yes in
; this file.  Both default to no.  httptimeout provides the maximum
; timeout in seconds before a web based session is discarded.  The
; default is 60 seconds.
;
[general]
displaysystemname = yes
enabled = yes
;webenabled = yes
port = 5038

;httptimeout = 60
; a) httptimeout sets the Max-Age of the http cookie
; b) httptimeout is the amount of time the webserver waits
;    on a action=waitevent request (actually its httptimeout-10)
; c) httptimeout is also the amount of time the webserver keeps
;    a http session alive after completing a successful action

;bindaddr = 127.0.0.1   ; Local interface only!
bindaddr = 0.0.0.0    ; Not secure
;
;displayconnects = yes
;
; Add a Unix epoch timestamp to events (not action responses)
;
;timestampevents = yes

[admin]
secret = mypassword
read = all,system,call,log,verbose,command,agent,user,config
write = all,system,call,log,verbose,command,agent,user,config
```

The lines above in bold are the lines you could change. The default port is 5038. You could change this but if you do you must also use the new port when defining your nodes in your allmon.ini file.

The bindaddr can be either 127.0.0.1 for local only access or 0.0.0.0 for access to nodes at other IP addresses. If you only intend to run Supermon2 on a Pi and only manage nodes that are specifically on that Pi then this would remain at 127.0.0.1. If you want to manage nodes with your Supermon2 that are elsewhere on your LAN or out on the Internet then this would be set to 0.0.0.0 Comment the line that does not apply.

The secret entry is your password between allmon.ini and the AMI. The secret here and the passwd in allmon.ini must match.

AMI Security

The AMI is notoriously insecure but there are ways to make it secure. Future versions of Supermon2 will use memcache as the primary data transfer means but until then if you use Supermon2 to access nodes outside of your local LAN out on the Internet you should use a method to ensure security. The firewall method is described in the installation notes. This method works well if you have either a static IP, Dyn DNS, or an access LAN that has Hamvoip installed and registered so you can use the NODE.ip.hamvoip.org lookup method for authorizing the IP address. Using a VPN is another way to provide security.