**Use SELinux port labelling to allow services to use non-standard ports.**

**Presentation**

Because of **SELinux** policy, a service is normally allowed to run on a restricted list of well-known ports. For example, in the case of the **httpd** service, this list is **80**, **443**, **488**, **8008**, **8009**, **8443**.

To allow a service to use non-standard ports, you need to follow a specific procedure to change the **SELinux** policy.

**Prerequisites**

Install the **setroubleshoot-server** (to get the **semanage** command) and, optionally, the **selinux-policy-devel** (to get the **sepolicy** command) packages:

# **yum install -y setroubleshoot-server selinux-policy-devel**

Install the service (here **httpd**) that you want to run (if it’s not already done):

# **yum install -y httpd**

**SELinux procedure**

To get the list of all restricted ports by service, type:

# **semanage port -l**

SELinux Port Type              Proto    Port Number

afs3\_callback\_port\_t           tcp      7001

afs3\_callback\_port\_t           udp      7001

afs\_bos\_port\_t                 udp      7007

afs\_fs\_port\_t                  tcp      2040

afs\_fs\_port\_t                  udp      7000, 7005

afs\_ka\_port\_t                  udp      7004

afs\_pt\_port\_t                  udp      7002

afs\_vl\_port\_t                  udp      7003

...

http\_port\_t                    tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000

...

zookeeper\_client\_port\_t        tcp      2181

zookeeper\_election\_port\_t      tcp      3888

zookeeper\_leader\_port\_t        tcp      2888

zope\_port\_t                    tcp      8021

To get the list of well-known ports for the **httpd** service, type:

# **semanage port -l | grep -w http\_port\_t**

http\_port\_t tcp 80, 81, 443, 488, 8008, 8009, 8443, 9000

**Alternatively**, you can also use the **sepolicy** command to get the same result:

# **sepolicy network -t http\_port\_t**

http\_port\_t: tcp: 80,81,443,488,8008,8009,8443,9000

To check if a port is already used (here **8001**), type:

# **sepolicy network -p 8001**

8001: tcp unreserved\_port\_t 1024-32767

8001: udp unreserved\_port\_t 1024-32767

To allow the **httpd** service to run on the **8001 tcp** port (**-a** for add), type:

# **semanage port -a -t http\_port\_t -p tcp 8001**

Note1: Use the **-d** option instead of the **-a** option to remove a port from the list.  
Note2: In case the **8001** **tcp** port is already assigned to an other service, use the **-m** option (see [Sander van Vugt RHCE FAQ](http://rhatcertification.com/index.php?site=pagina&site_id=6) for more information): a port can only be used by one service at a time.

To check the list is updated, type:

# **semanage port -l | grep -w http\_port\_t**

http\_port\_t **tcp 8001**, 80, 81, 443, 488, 8008, 8009, 8443, 9000

**Alternatively**, you can check the new status of the port (here **8001**):

# **sepolicy network -p 8001**

8001: tcp unreserved\_port\_t 1024-32767

8001: udp unreserved\_port\_t 1024-32767

**8001: tcp http\_port\_t 8001**

**Additional specific service configuration**

In addition to the **SELinux** policy change, you may need to adjust the service configuration.  
For example, with the **httpd** service, you will need to update the **Listen** directive or, if it’s a virtual host, the **<VirtualHost>** directive in the **/etc/httpd/conf/httpd.conf** file to take into account the new port.