close window

Web Exclusive

Print

Secure Your VIO Server

November 2017 | by Jaqui Lynch

Most clients today now have to undergo regular security scans. Those scans will include your server LPARs, HMCs and VIO servers. In order to pass PCI compliance checks it is necessary to take steps to secure your VIO and HMC. In this article we will touch on some of those items.

HMC and Server Security

The HMC should be installed at the latest level—either 8.8.6.0 SP2 MH01722 or 8.8.7. These levels have removed insecure ciphers that triggered SSL alerts and they have also updated SSL to current levels. For older levels of the HMC there are specific patches that need to be installed.

Power Systems servers have one or two FSPs (flexible service processors). Typically these are either direct connected to the HMC (where there is only one server) or they are connected to the HMC via a private network. It's important to use the private network rather than connecting over a public network. Firstly, the HMC provides IP addresses to the FSPs using DHCP. You don't want those packets dropping on your public network. It's possible to provide static IPs to the FSPs but this brings along other issues. POWER7 servers allow SSLv3 connections, which means they can be vulnerable to various SSL exploits. There are several solutions for this: 1.) Update to the latest firmware as many SSL exploits to the FSPs are corrected there. 2.) Keep the FSPs on a private network so no one can get to them anyway—this is best practice, or 3.) For POWER7 you can also go into the security menu once you are at AL770+ firmware and disable SSLv3. In POWER8 SSLv3 is deprecated so there is no security menu. I keep firmware up to date and I also keep the FSPs on a private network. The private network is best practice for setting up HMC to FSP connectivity.

VIO Security

By default the VIO server has some security issues. Specifically, the default levels of SSL and SSH need to be modified along with a few other changes. Before making any of these changes you should use viosbr to take a backup and then take a full mksysb backup of the VIO using backupios. Then you can start making changes.

By default /etc/inetd.conf has ftp and telnet plus several other services enabled. I take a copy of inetd.conf and then remove nearly everything from the running inetd.conf as follows:

```
cp /etc/inetd.conf /etc/inetd.conf.orig Modify inetd.conf so it now only contains: #ftp
stream tcp6 nowait root /usr/sbin/ftpd ftpd #telnet stream tcp6 nowait root /usr/sbin
/telnetd telnetd -a xmquery dgram udp6 wait root /usr/bin/xmtopas xmtopas -p3 caa_cfg
stream tcp6 nowait root /usr/sbin/clusterconf clusterconf >>/var/adm/ras/clusterconf.log
2>&1
Then refresh -s inetd
```

Now your only connectivity options are ssh, sftp and scp

I also go to IBM Fix Central and download the latest Java, SSL and SSH versions. For VIO 2.2.5 java5 is no longer needed so it should be uninstalled. For vio 2.2.6 java6 is no longer needed and should be uninstalled. When you uninstall java5 it may also uninstall cimserver, which is also no longer needed. These are hangovers from older VIO levels.

If java6 is to remain then it should be updated to at least 6.0.0.650. You can download this from FixCentral. If you are

running both 32 bit and 64 bit Java6 then you will need to update both. Once the update is done you should see something like:

```
#lslpp -l | grep ava
Java6.sdk 6.0.0.650 COMMITTED Java SDK 32-bit
Java6.sdk 6.0.0.650 COMMITTED Java SDK 32-bit

If Java7 is installed it needs to be updated to at least 7.0.0.610.
```

Both SSL and SSH need to be updated. The latest SSL is ssl-1.0.2.1100 and the latest SSH is 7.5. You can obtain the latest versions of these at the IBM Web Download Programs Page. Look for OpenSSH Version 7.5 and right below it you will find OpenSSL 1.0.2.x. The radio buttons only allow you to choose one at a time to download. For SSL make sure to choose the VRMF: 1.0.2.1100 which comes down as a tar.Z file.

After you download them you will need to uncompress and untar the files. I combine them into one directory for both ssh and ssl and then use smitty to install them. This should be done using a console through the HMC since you are updating SSH. Prior to updating SSH you may want to copy your /etc/ssh/sshd_config just in case. Once SSH is installed you want to ensure that no backlevel ciphers can be used. This is done by editing your /etc/ssh/sshd_config file and adding the following two lines to the bottom:

Ciphers aes128-ctr,aes192-ctr,aes256-ctr MACs hmac-sha1, mac-64@openssh.com,hmac-ripemd160

Also check the file to make sure that you have it set up for the kind of logins you normally do—password or ssl, etc.

Now you can stop and start SSH:
ps -ef | grep ssh
If no one is logged in then:
stopsrc -s sshd
Once it is down:
startsrc -s sshd
Check that ssh is running again and then try to ssh to the VIO server

Old Director Agents

If you have been upgrading your VIO servers for a while it is possible that the old systems director agent and/or cimserver are running or installed. The process to remove them is as follows:
Remove director agent:
From a padmin shell, run the following command:
oem_setup_env
1. To stop the common and platform agents, run the following command: Stop the common agent, platform agent and SLP /opt/ibm/director/agent/bin/stopagent_vios Stop the cimserver cimserver -s 2. To disable them, do the following: a. Uninstall the nonstop service by running the following command: /opt/ibm/director/agent/runtime/nonstop /bin/installnonstop.sh -uninstallservice b. In /etc/inittab , comment out these lines (using a ':' (colon) character at the beginning of the line, as seen here): :director_agent:2:once:/opt/ibm/director/agent/bin/startagent_vios >/dev/null 2>&1 :climgrcim:23456789:once:/usr/ios/sbin/climgr cimserver start > /dev/null 2>&1

Logging

By default the VIO server does almost no logging. I normally set up a filesystem called /usr/local/logs and I then set up logging on the VIO server. I usually set up something like:

```
Add lines to syslog.conf as follows:
vi /etc/syslog.conf
mail.debug      /usr/local/logs/mailog
*.emerg         /usr/local/logs/syslog
*.alert         /usr/local/logs/syslog
```

```
*.crit          /usr/local/logs/syslog
*.err           /usr/local/logs/syslog
auth.notice     /usr/local/logs/infolog
*.info          /usr/local/logs/messages

cd /usr/local/logs
touch syslog mailog infolog messages


stopsrc -s syslogd
startsrc -s syslogd
```

When you do set up logging make sure to setup and use a separate filesystem—that way if the filesystem fills up it won't take your system down. You can also have the VIO server send logs to remote log servers and so on.

Other

Check /etc/rc.tcpip and make sure sendmail is not being started. If you are not using snmp to monitor the VIO then also comment out all the MIB processes. If you are using SNMP then you should customize it rather than letting it default.

You should also set up NTP to point to time servers so that time is consistent. On a VIO server you need to configure /etc/ntp.conf and also /home/padmin/config/ntp.conf.

I also stop the Xservers running – these are supposed to make an Xwindows interface available at a graphics console. Since we don't have graphics consoles there is no reason to run these.

```
vi  /usr/dt/config/Xservers and comment out :0 line
cp /usr/dt/config/Xservers /etc/dt/config
vi /usr/lib/X11/xdm/Xservers and comment out :0 line
```

Patches

At this point, you've secured most of the things you need to and it is time to check for security and hiper patches using FLRTVC.

FLRTVC is a vulnerability checker. You download the script and run it on the system to be reviewed. It uses wget or curl to try to download a file called apar.csv from IBM and it then checks known issues against your software levels. FLRTVC identifies the efixes and ifixes that need to go on, provides links to the readmes and also to the actual download. You can send the output to a .txt file, download it and open it in Excel (it is in csv format) to make it easier to view. I typically run FLRTVC on my critical systems once a month.

If your VIO does not have outside access then you can still run flrtvc. You need to download the apar.csv file manually and upload it from your desktop. You then edit the flrtvc.ksh and change

```
SKIPDOWNLOAD=0
To SKIPDOWNLOAD=1
```

This tells FLRTVC to use the apar.csv file you already have.

For VIO 2.2.5.20 I end up installing the following fixes that FLRTVC identifies:

```
emgr -p -e IV95102s9a.VIOS2.2.5.20.170526.epkg.Z
emgr -p -e IV95372s9a.VIOS2.2.5.20.170427.epkg.Z
emgr -p -e IV96351s9d.170525.VIOS2.2.5.20.epkg.Z
emgr -p -e IV96553s9b.170725.VIOS2.2.5.20.epkg.Z
```

```
emgr -p -e IV97135s9a.170714.VIOS2.2.5.20.epkg.Z
Patch for BIND
emgr -p -e IV98826m9a.170809.epkg.Z
Patch for BELLMAIL
emgr -p -e IV92238m8a.170112.epkg.Z
Patch for NTP
emgr -p -e IV96306m9a.170519.epkg.Z
Patch for TCPDUMP
emgr -p -e IV94728s9c.170420.epkg.Z
```

The -p flag says run it in test mode. When you are ready to actually install them then you remove the -p. Some of these require a reboot so you will need to run bosboot and set the bootlist and reboot the VIO after. Once all of them are installed you can run emgr to see what they look like:

```
# emgr -l

ID  STATE LABEL      INSTALL TIME      UPDATED BY ABSTRACT
=== ===== ========== ================= ========== ====================================
1    S    IV95372s9a 07/16/17 15:57:37            Ifix for APAR IV95372
2    S    IV96351s9d 07/16/17 15:58:13            iFix for APAR IV96351
3    S    IV94728s9c 07/16/17 16:00:24            ifix for IV94728
4    S    IV95102s9a 07/16/17 16:10:04            efix for IV95102
5   *Q*   IV96553s9b 11/29/17 15:54:20            Undetected data loss
6   *Q*   IV97135s9a 11/29/17 15:55:10            LACP PORT MAY NOT AGGREGATE.
7    S    IV98826m9a 11/29/17 15:55:43            IV98826 for AIX 7.1 TL 9
8    S    IV96306m9a 11/29/17 15:56:17            Multi Ifix for apar IV96306
```

After the reboot you have done most of the things you need to do. This is the point at which I would take a backup so that the updated VIO server is also backed up.

Summary

Securing your HMC and VIO servers is an important part of any security plan. I include all of these steps in my installation document for VIO servers. I will update it shortly once I upgrade to 2.2.6.10 for the VIO. Taking these steps will help you pass PCI compliance and other security checks. There may be other changes or fixes that you need as they will be technology and service pack level specific. When in doubt you can also open a proactive PMR with IBM to ensure you are catching everything.

References

FLRTVC
https://www14.software.ibm.com/support/customercare/sas/f/flrt/flrtvc.html

HMC SSL Poodle
http://www-01.ibm.com/support/docview.wss?uid=nas8N1020593
http://www-01.ibm.com/support/docview.wss?uid=nas8N1020021

FSP Security
https://www.ibm.com/developerworks/community/wikis/home?lang=en_us#!/wiki/Power%20Systems/page/Power%20Systems%20Flexible%20Service%20Processor%20(FSP)%20Security

IBM Web Download Pack Programs
https://www-01.ibm.com/marketing/iwm/iwm/web/reg/pick.do?source=aixbp&lang=en_US

Disable Director Agents on VIOS
http://www-01.ibm.com/support/docview.wss?uid=nas704b5d1161dceea4386257dc5007b9ab7

References

< Return to main article

Print Email

FLRTVC: https://www14.software.ibm.com/support/customercare/sas/f/flrt/flrtvc.html

HMC SSL Poodle:

http://www-01.ibm.com/support/docview.wss?uid=nas8N1020593

http://www-01.ibm.com/support/docview.wss?uid=nas8N1020021

FSP Security: https://www.ibm.com/developerworks/community/wikis/home?lang=en_us#!/wiki/Power%20Systems/page/Power%20Systems%20Flexible%20Service%20Processor%20(FSP)%20Security

IBM Web Download Pack Programs: https://www-01.ibm.com/marketing/iwm/iwm/web/reg/pick.do?source=aixbp&lang=en_US

Disable Director Agents on VIOS: http://www-01.ibm.com/support/docview.wss?uid=nas704b5d1161dceea4386257dc5007b9ab7

< Return to main article