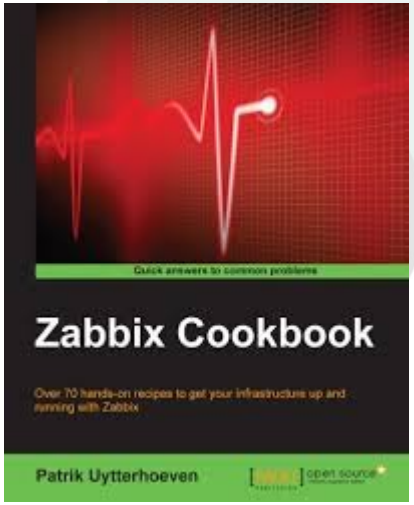
Hardening Zabbix

Who am I

- Name: Patrik Uytterhoeven
- Company: Open-Future
- Job: Open-Source Consultant
- Author: Zabbix Cookbook



Why This Talk ?

- Too many guides on the internet saying: ignore SELinux
- People ignore to check there distro for updates
- Lazy SYSadmins (sometimes not bad :-))

What can we do to improve Security

- Configure Apache, Nginx, … to make use of HTTPS instead of HTTP
- Do not connect to the internet (use vpn !)
- Disable the GUEST user !
- Enable and configure SELinux
- Check for security updates on your OS. (remember hearthbleed,Ghost, …)

Wrong ideas about SELinux

- SELinux is too difficult to configure . It is easier to disable.
- Some people think it has NSA backdoors because it is developed by the NSA.

The Truth

- SELinux is developed to protect us. Adding a backdoor would also put American companies at risk.
- The Kernel code is free available. Feel free to have a look and let me know if you can find some backdoor …
- SELinux was difficult to use but has been improved over the years. Since RedHat 6 SELinux is very easy to debug. No excuse to not use it anymore.

How to Activate SELinux ?

- Check the SELinux status with: getenforce
  - This should return “Enforcing”
- Edit SELinux Config: /etc/selinux/config
  - SELINUX=enforcing
  - Run “setenforce 1”

Some SELinux Settings for Zabbix

- On the Agent Side
  - setsebool -P zabbix_can_network 1
- On the Server Side
  - setsebool -P httpd_can_network_connect on
  - setsebool -P httpd_can_network_connect_db on
- getsebool -a “This will list all booleans”

More Advanced troubleshooting

Fping will always return 0 in Zabbix with SELinux active. How to resolve this ?

Install setroubleshoot-server package:

- Yum install setroubleshoot-server

Run sealert

- sealert -a /var/log/audit/audit.log to check the errors in selinux. (-a is the option to analyze the file)

SELinux will try to propose a solution when possible

fping example

```
:SELinux is preventing /usr/sbin/fping from 'create' accesses on the rawip_socket
.
:
:*****  Plugin catchall (100. confidence) suggests  **************************
:
:If you believe that fping should be allowed create access on the  rawip_socket
by default.
:Then you should report this as a bug.
:You can generate a local policy module to allow this access.
:Do
:allow this access for now by executing:
:# grep fping /var/log/audit/audit.log | audit2allow -M mypol
:# semodule -i mypol.pp
```

Solutions

- Run “setenforce 0” temporary to test if SELinux is blocking access.
- Check /var/log/messages
- Make use of sealert
- Ls -Z (to see selinux context of files)
- restorecon
  - will restore the original context.
- chcon --reference <source> <destination>
  - To copy context from source to destination

Now that you know more about SeLinux

I hope that you will not disable it anymore.

This Zabbix extension will check if SELinux is active and if there are any security updates available on your rhel 6/7 system

- https://github.com/Open-Future-Belgium/zabbix/tree/master/check-yum-updates
- https://share.zabbix.com/operating-systems/redhat-centos/check-yum-updates

Thank You for you time.

Questions ?