

Version : **2024.01**

Dernière mise-à-jour : 2024/10/18 07:58

LCF606 - Gestion de la Sécurité

Contenu du Module

- **LCF606 - Gestion de la Sécurité**
 - Contenu du Module
 - Le Pare-feu Netfilter/iptables
 - LAB #1 - La Configuration par firewalld
 - La Configuration de Base de firewalld
 - La Commande firewall-cmd
 - La Configuration Avancée de firewalld
 - Le mode Panic de firewalld
 - System Hardening
 - Les compileurs
 - Les paquets
 - Les démons et services
 - Les fichiers .rhosts
 - Les fichiers et les répertoires sans propriétaire
 - Limiter le délai d'inactivité d'une session shell
 - Renforcer la sécurité d'init
 - Les Distributions SysVinit
 - Les Distributions Upstart
 - Renforcer la sécurité du Noyau
 - La commande sysctl
 - Mise en place de SELinux pour sécuriser le serveur
 - Introduction
 - Définitions

- Security Context
- Domains et Types
- Roles
- Politiques de Sécurité
- Langage de Politiques
 - allow
 - type
- type_transition
- Décisions de SELinux
 - Décisions d'Accès
 - Décisions de Transition
- Commandes SELinux
- Les Etats de SELinux
- Booléens
- LAB #2 - Travailler avec SELinux
 - Copier et Déplacer des Fichiers
 - Vérifier les SC des Processus
 - Visualiser la SC d'un Utilisateur
 - Vérifier la SC d'un fichier
 - Troubleshooting SELinux
 - La commande chcon
 - La commande restorecon
 - Le fichier /.autorelabel
 - La commande semanage
 - La commande audit2allow
- Mots de Passe
 - LAB #3 - John the Ripper
 - LAB #4 - Mise en place du Système de Prévention d'Intrusion Fail2Ban
 - Installation
 - Configuration
 - Le répertoire /etc/fail2ban
 - Le fichier fail2ban.conf
 - Le répertoire /etc/fail2ban/filter.d/
 - Le répertoire /etc/fail2ban/action.d/

- Commandes
 - Activer et Démarrer le Serveur
 - Utiliser la Commande Fail2Ban-server
 - Ajouter un Prison
 - Balayage des Ports
 - LAB #5 - Utilisation de nmap et de netcat
 - nmap
 - Installation
 - Utilisation
 - Fichiers de Configuration
 - Scripts
 - netcat
 - Utilisation
 - LAB #6 - Mise en place du Système de Détection et de Prévention d'Intrusion Portsentry
 - Installation
 - Configuration
 - Utilisation
 - Système de Fichiers
 - LAB #7 - Mise en place du File Integrity Checker Afick
 - Présentation
 - Installation
 - Configuration
 - La Section Directives
 - La Section Alias
 - La Section File
 - Utilisation
 - Automatiser Afick
 - LAB #8 - Mise en place de rkhunter
 - Installation
 - Les options de la commande
 - Utilisation
 - Configuration
-

Le Pare-feu Netfilter

Netfilter est composé de 5 *hooks* :

- NF_IP_PRE_ROUTING
- NF_IP_LOCAL_IN
- NF_IP_LOCAL_OUT
- NF_IP_FORWARD
- NF_IP_POSTROUTING

Ces hooks sont utilisés par deux branches, la première est celle concernée par les paquets qui entrent vers des services locaux :

- NF_IP_PRE_ROUTING > NF_IP_LOCAL_IN > NF_IP_LOCAL_OUT > NF_IP_POSTROUTING

tandis que la deuxième concerne les paquets qui traversent la passerelle:

- NF_IP_PRE_ROUTING > NF_IP_FORWARD > NF_IP_POSTROUTING

Si IPTABLES a été compilé en tant que module, son utilisation nécessite le chargement de plusieurs modules supplémentaires en fonction de la situation:

- iptable_filter
- iptable_mangle
- iptable_net
- etc

Netfilter est organisé en **tables**. La commande **iptables** de netfilter permet d'insérer des **politiques** dans les **chaines**:

- La table **FILTER**
 - La chaîne INPUT
 - Concerne les paquets entrants
 - Politiques: ACCEPT, DROP, REJECT
 - La chaîne OUTPUT
 - Concerne les paquets sortants

- Politiques: ACCEPT, DROP, REJECT
- La chaîne FORWARD
 - Concerne les paquets traversant le par-feu.
 - Politiques: ACCEPT, DROP, REJECT

Si aucune table n'est précisée, c'est la table FILTER qui s'applique par défaut.

- La table **NAT**
 - La chaîne PREROUTING
 - Permet de faire la translation d'adresse de destination
 - Cibles: SNAT, DNAT, MASQUERADE
 - La chaîne POSTROUTING
 - Permet de faire la translation d'adresse de la source
 - Cibles: SNAT, DNAT, MASQUERADE
 - Le cas spécifique OUTPUT
 - Permet la modification de la destination des paquets générés localement
- La table **MANGLE**
 - Permet le marquage de paquets générés localement (OUTPUT) et entrants (PREROUTING)

Les **politiques** sont:

- ACCEPT
 - Permet d'accepter le paquet concerné
- DROP
 - Permet de rejeter le paquet concerné sans générer un message d'erreur
- REJECT
 - Permet de rejeter le paquet concerné en générant une message d'erreur

Les **cibles** sont:

- SNAT
 - Permet de modifier l'adresse source du paquet concerné
- DNAT
 - Permet de modifier l'adresse de destination du paquet concerné

- MASQUERADE

- Permet de remplacer l'adresse IP privée de l'expéditeur par un socket public de la passerelle.

IPTABLES peut être configuré soit par des outils tels shorewall, soit en utilisant des lignes de commandes ou un script. Dans ce dernier cas, la ligne prend la forme:

```
# IPTABLES --action CHAINE --option1 --option2
```

Les actions sont:

Action	Abréviation	Déscription
- -append	-A	Ajouter une règle à la fin de la chaîne spécifiée
- -delete	-D	Supprimer une règle en spécifiant son numéro ou la règle à supprimer
- -replace	-R	Permet de remplacer la règle spécifiée par son numéro
- -insert	-I	Permet d'insérer une règle à l'endroit spécifié
- -list	-L	Permet d'afficher des règles
- -flush	-F	Permet de vider toutes les règles d'une chaîne

Les options sont:

Option	Abréviation	Déscription
- -protocol	-p	Permet de spécifier un protocole - tcp, udp, icmp, all
- -source	-s	Permet de spécifier une adresse source
- -destination	-d	Permet de spécifier une adresse de destination
- -in-interface	-i	Permet de spécifier une interface réseau d'entrée
- -out-interface	-o	Permet de spécifier une interface réseau de sortie
- -fragment	-f	Permet de ne spécifier que les paquets fragmentés
- -source-port	-sport	Permet de spécifier un port source ou une plage de ports source
- -destination-port	-dport	Permet de spécifier un port de destination ou une plage de ports de destination
- -tcp-flags	s/o	Permet de spécifier un flag TCP à matcher - SYN, ACK, FIN, RST, URG, PSH, ALL, NONE
- -icmp-type	s/o	Permet de spécifier un type de paquet ICMP
- -mac-source	s/o	Permet de spécifier une adresse MAC

Les options spécifiques à NET sont:

- -to-destination	s/o	Permet de spécifier l'adresse de destination d'une translation
- -to-source	s/o	Permet spécifier l'adresse source d'une translation

Les options spécifiques aux LOGS sont:

- -log-level	s/o	Permet de spécifier le niveau de logs
- -log-prefix	s/o	Permet de spécifier un préfix pour les logs

L'option spécifique au STATEFUL est:

- -state	s/o	Permet de spécifier l'état du paquet à vérifier
----------	-----	---

Ce dernier cas fait référence au STATEFUL. Le STATEFUL est la capacité du par-feu à enregistrer dans une table spécifique, l'état des différentes connexions. Cette table s'appelle une **table d'état**. Le principe du fonctionnement de STATEFUL est simple, à savoir, si le paquet entrant appartient à une communication déjà établie, celui-ci n'est pas vérifié.

Il existe 4 états:

- NEW
 - Le paquet concerne une nouvelle connexion et contient donc un flag SYN à 1
- ESTABLISHED
 - Le paquet concerne une connexion déjà établie. Le paquet ne doit contenir **ni** flag SYN à 1, **ni** flag FIN à 1
- RELATED
 - Le paquet est d'une connexion qui présente une relation avec une autre connexion
- INVALID
 - La paquet provient d'une connexion anormale.

LAB #1 - La Configuration par firewalld

Firewalld utilise des **zones** - des jeux de règles pré-définis dans lesquels sont placés les interfaces :

- **trusted** - un réseau fiable. Dans ce cas tous les ports sont autorisés,
-

- **work, home, internal** - un réseau partiellement fiable. Dans ce cas quelques ports sont autorisés,
- **dmz, public, external** - un réseau non fiable. Dans ce cas peu de ports sont autorisés,
- **block, drop** - tout est interdit. La zone drop n'envoie pas de messages d'erreurs.



Important - Une interface ne peut être que dans une zone à la fois tandis que plusieurs interfaces peuvent être dans la même zone.

Le service firewalld doit toujours être lancé :

```
[root@centos8 ~]# systemctl status firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2024-10-01 12:13:55 CEST; 1h 43min ago
     Docs: man:firewalld(1)
  Main PID: 1079 (firewalld)
    Tasks: 2 (limit: 100949)
   Memory: 32.7M
    CGroup: /system.slice/firewalld.service
            └─1079 /usr/libexec/platform-python -s /usr/sbin/firewalld --nofork --nopid

Oct 01 12:13:53 centos8.ittraining.loc systemd[1]: Starting firewalld - dynamic firewall daemon...
Oct 01 12:13:55 centos8.ittraining.loc systemd[1]: Started firewalld - dynamic firewall daemon.
Oct 01 12:13:56 centos8.ittraining.loc firewalld[1079]: WARNING: AllowZoneDrifting is enabled. This is considered
an insecure configuration option. It will be removed in a future release.
[q]
```

La Configuration de Base de firewalld

La configuration par défaut de firewalld se trouve dans **/usr/lib/firewalld** :

```
[root@centos8 ~]# ls -l /usr/lib/firewalld/
total 16
drwxr-xr-x. 2 root root 224 Mar 6 2022 helpers
drwxr-xr-x. 2 root root 4096 Mar 6 2022 icmptypes
drwxr-xr-x. 2 root root 20 Mar 6 2022 ipsets
drwxr-xr-x. 2 root root 33 Mar 6 2022 policies
drwxr-xr-x. 2 root root 8192 Mar 6 2022 services
drwxr-xr-x. 2 root root 203 Mar 6 2022 zones
```

```
[root@centos8 ~]# ls -l /usr/lib/firewalld/zones
total 44
-rw-r--r--. 1 root root 299 Aug 9 2021 block.xml
-rw-r--r--. 1 root root 293 Aug 9 2021 dmz.xml
-rw-r--r--. 1 root root 291 Aug 9 2021 drop.xml
-rw-r--r--. 1 root root 304 Aug 9 2021 external.xml
-rw-r--r--. 1 root root 397 Aug 9 2021 home.xml
-rw-r--r--. 1 root root 412 Aug 9 2021 internal.xml
-rw-r--r--. 1 root root 809 Nov 26 2019 libvirt.xml
-rw-r--r--. 1 root root 729 Aug 18 2021 nm-shared.xml
-rw-r--r--. 1 root root 343 Aug 9 2021 public.xml
-rw-r--r--. 1 root root 162 Aug 9 2021 trusted.xml
-rw-r--r--. 1 root root 339 Aug 9 2021 work.xml
```

```
[root@centos8 ~]# ls -l /usr/lib/firewalld/services
total 704
-rw-r--r--. 1 root root 399 Aug 9 2021 amanda-client.xml
-rw-r--r--. 1 root root 427 Aug 9 2021 amanda-k5-client.xml
-rw-r--r--. 1 root root 283 Aug 9 2021 amqps.xml
-rw-r--r--. 1 root root 273 Aug 9 2021 amqp.xml
-rw-r--r--. 1 root root 285 Aug 9 2021 apcupsd.xml
-rw-r--r--. 1 root root 301 Aug 9 2021 audit.xml
-rw-r--r--. 1 root root 320 Aug 9 2021 bacula-client.xml
-rw-r--r--. 1 root root 346 Aug 9 2021 bacula.xml
-rw-r--r--. 1 root root 429 Aug 9 2021 bb.xml
```

-rw-r--r--.	1	root	root	339	Aug	9	2021	bgp.xml
-rw-r--r--.	1	root	root	275	Aug	9	2021	bitcoin-rpc.xml
-rw-r--r--.	1	root	root	307	Aug	9	2021	bitcoin-testnet-rpc.xml
-rw-r--r--.	1	root	root	281	Aug	9	2021	bitcoin-testnet.xml
-rw-r--r--.	1	root	root	244	Aug	9	2021	bitcoin.xml
-rw-r--r--.	1	root	root	410	Aug	9	2021	bittorrent-lsd.xml
-rw-r--r--.	1	root	root	294	Aug	9	2021	ceph-mon.xml
-rw-r--r--.	1	root	root	329	Aug	9	2021	ceph.xml
-rw-r--r--.	1	root	root	168	Aug	9	2021	cfengine.xml
-rw-r--r--.	1	root	root	211	Aug	9	2021	cockpit.xml
-rw-r--r--.	1	root	root	296	Aug	9	2021	collectd.xml
-rw-r--r--.	1	root	root	260	Aug	9	2021	condor-collector.xml
-rw-r--r--.	1	root	root	296	Aug	9	2021	ctdb.xml
-rw-r--r--.	1	root	root	305	Aug	9	2021	dhcpx6-client.xml
-rw-r--r--.	1	root	root	234	Aug	9	2021	dhcpx6.xml
-rw-r--r--.	1	root	root	227	Aug	9	2021	dhcpx.xml
-rw-r--r--.	1	root	root	205	Aug	9	2021	distcc.xml
-rw-r--r--.	1	root	root	318	Aug	9	2021	dns-over-tls.xml
-rw-r--r--.	1	root	root	346	Aug	9	2021	dns.xml
-rw-r--r--.	1	root	root	374	Aug	9	2021	docker-registry.xml
-rw-r--r--.	1	root	root	391	Aug	9	2021	docker-swarm.xml
-rw-r--r--.	1	root	root	228	Aug	9	2021	dropbox-lansync.xml
-rw-r--r--.	1	root	root	338	Aug	9	2021	elasticsearch.xml
-rw-r--r--.	1	root	root	304	Aug	9	2021	etcd-client.xml
-rw-r--r--.	1	root	root	304	Aug	9	2021	etcd-server.xml
-rw-r--r--.	1	root	root	224	Aug	9	2021	finger.xml
-rw-r--r--.	1	root	root	270	Aug	9	2021	foreman-proxy.xml
-rw-r--r--.	1	root	root	408	Aug	9	2021	foreman.xml
-rw-r--r--.	1	root	root	709	Aug	9	2021	freeipa-4.xml
-rw-r--r--.	1	root	root	489	Aug	9	2021	freeipa-ldaps.xml
-rw-r--r--.	1	root	root	488	Aug	9	2021	freeipa-ldap.xml
-rw-r--r--.	1	root	root	242	Aug	9	2021	freeipa-replication.xml
-rw-r--r--.	1	root	root	657	Aug	9	2021	freeipa-trust.xml
-rw-r--r--.	1	root	root	361	Aug	9	2021	ftp.xml

-rw-r--r--.	1	root	root	292	Aug	9	2021	galera.xml
-rw-r--r--.	1	root	root	184	Aug	9	2021	ganglia-client.xml
-rw-r--r--.	1	root	root	176	Aug	9	2021	ganglia-master.xml
-rw-r--r--.	1	root	root	212	Aug	9	2021	git.xml
-rw-r--r--.	1	root	root	218	Aug	9	2021	grafana.xml
-rw-r--r--.	1	root	root	119	Aug	9	2021	gre.xml
-rw-r--r--.	1	root	root	608	Aug	9	2021	high-availability.xml
-rw-r--r--.	1	root	root	448	Aug	9	2021	https.xml
-rw-r--r--.	1	root	root	353	Aug	9	2021	http.xml
-rw-r--r--.	1	root	root	372	Aug	9	2021	imaps.xml
-rw-r--r--.	1	root	root	327	Aug	9	2021	imap.xml
-rw-r--r--.	1	root	root	454	Aug	9	2021	ipp-client.xml
-rw-r--r--.	1	root	root	427	Aug	9	2021	ipp.xml
-rw-r--r--.	1	root	root	894	Aug	9	2021	ipsec.xml
-rw-r--r--.	1	root	root	255	Aug	9	2021	ircs.xml
-rw-r--r--.	1	root	root	247	Aug	9	2021	irc.xml
-rw-r--r--.	1	root	root	264	Aug	9	2021	iscsi-target.xml
-rw-r--r--.	1	root	root	358	Aug	9	2021	isns.xml
-rw-r--r--.	1	root	root	213	Aug	9	2021	jenkins.xml
-rw-r--r--.	1	root	root	182	Aug	9	2021	kadmin.xml
-rw-r--r--.	1	root	root	272	Aug	9	2021	kdeconnect.xml
-rw-r--r--.	1	root	root	233	Aug	9	2021	kerberos.xml
-rw-r--r--.	1	root	root	384	Aug	9	2021	kibana.xml
-rw-r--r--.	1	root	root	249	Aug	9	2021	klogin.xml
-rw-r--r--.	1	root	root	221	Aug	9	2021	kpasswd.xml
-rw-r--r--.	1	root	root	182	Aug	9	2021	kprop.xml
-rw-r--r--.	1	root	root	242	Aug	9	2021	kshell.xml
-rw-r--r--.	1	root	root	308	Aug	9	2021	kube-apiserver.xml
-rw-r--r--.	1	root	root	232	Aug	9	2021	ldaps.xml
-rw-r--r--.	1	root	root	199	Aug	9	2021	ldap.xml
-rw-r--r--.	1	root	root	385	Aug	9	2021	libvirt-tls.xml
-rw-r--r--.	1	root	root	389	Aug	9	2021	libvirt.xml
-rw-r--r--.	1	root	root	269	Aug	9	2021	lightning-network.xml
-rw-r--r--.	1	root	root	324	Aug	9	2021	llmnr.xml

-rw-r--r--.	1	root	root	349	Aug	9	2021	managesieve.xml
-rw-r--r--.	1	root	root	432	Aug	9	2021	matrix.xml
-rw-r--r--.	1	root	root	424	Aug	9	2021	mdns.xml
-rw-r--r--.	1	root	root	245	Aug	9	2021	memcache.xml
-rw-r--r--.	1	root	root	343	Aug	9	2021	minidlna.xml
-rw-r--r--.	1	root	root	237	Aug	9	2021	mongodb.xml
-rw-r--r--.	1	root	root	473	Aug	9	2021	mosh.xml
-rw-r--r--.	1	root	root	211	Aug	9	2021	mountd.xml
-rw-r--r--.	1	root	root	296	Aug	9	2021	mqtt-tls.xml
-rw-r--r--.	1	root	root	287	Aug	9	2021	mqtt.xml
-rw-r--r--.	1	root	root	170	Aug	9	2021	mssql.xml
-rw-r--r--.	1	root	root	190	Aug	9	2021	ms-wbt.xml
-rw-r--r--.	1	root	root	242	Aug	9	2021	murmur.xml
-rw-r--r--.	1	root	root	171	Aug	9	2021	mysql.xml
-rw-r--r--.	1	root	root	250	Aug	9	2021	nbd.xml
-rw-r--r--.	1	root	root	342	Aug	9	2021	nfs3.xml
-rw-r--r--.	1	root	root	324	Aug	9	2021	nfs.xml
-rw-r--r--.	1	root	root	293	Aug	9	2021	nmea-0183.xml
-rw-r--r--.	1	root	root	247	Aug	9	2021	nrpe.xml
-rw-r--r--.	1	root	root	389	Aug	9	2021	ntp.xml
-rw-r--r--.	1	root	root	368	Aug	9	2021	nut.xml
-rw-r--r--.	1	root	root	335	Aug	9	2021	openvpn.xml
-rw-r--r--.	1	root	root	260	Aug	9	2021	ovirt-imageio.xml
-rw-r--r--.	1	root	root	343	Aug	9	2021	ovirt-storageconsole.xml
-rw-r--r--.	1	root	root	235	Aug	9	2021	ovirt-vmconsole.xml
-rw-r--r--.	1	root	root	1024	Aug	9	2021	plex.xml
-rw-r--r--.	1	root	root	433	Aug	9	2021	pmcd.xml
-rw-r--r--.	1	root	root	474	Aug	9	2021	pmproxy.xml
-rw-r--r--.	1	root	root	544	Aug	9	2021	pmwebapis.xml
-rw-r--r--.	1	root	root	460	Aug	9	2021	pmwebapi.xml
-rw-r--r--.	1	root	root	357	Aug	9	2021	pop3s.xml
-rw-r--r--.	1	root	root	348	Aug	9	2021	pop3.xml
-rw-r--r--.	1	root	root	181	Aug	9	2021	postgresql.xml
-rw-r--r--.	1	root	root	509	Aug	9	2021	privoxy.xml

-rw-r--r--.	1	root	root	213	Aug	9	2021	prometheus.xml
-rw-r--r--.	1	root	root	261	Aug	9	2021	proxy-dhcp.xml
-rw-r--r--.	1	root	root	424	Aug	9	2021	ptp.xml
-rw-r--r--.	1	root	root	414	Aug	9	2021	pulseaudio.xml
-rw-r--r--.	1	root	root	297	Aug	9	2021	puppetmaster.xml
-rw-r--r--.	1	root	root	273	Aug	9	2021	quassel.xml
-rw-r--r--.	1	root	root	520	Aug	9	2021	radius.xml
-rw-r--r--.	1	root	root	183	Aug	9	2021	rdp.xml
-rw-r--r--.	1	root	root	212	Aug	9	2021	redis-sentinel.xml
-rw-r--r--.	1	root	root	268	Aug	9	2021	redis.xml
-rw-r--r--.	1	root	root	381	Aug	9	2021	RH-Satellite-6-capsule.xml
-rw-r--r--.	1	root	root	556	Aug	9	2021	RH-Satellite-6.xml
-rw-r--r--.	1	root	root	214	Aug	9	2021	rpc-bind.xml
-rw-r--r--.	1	root	root	213	Aug	9	2021	rquotad.xml
-rw-r--r--.	1	root	root	310	Aug	9	2021	rsh.xml
-rw-r--r--.	1	root	root	311	Aug	9	2021	rsyncd.xml
-rw-r--r--.	1	root	root	350	Aug	9	2021	rtsp.xml
-rw-r--r--.	1	root	root	329	Aug	9	2021	salt-master.xml
-rw-r--r--.	1	root	root	371	Aug	9	2021	samba-client.xml
-rw-r--r--.	1	root	root	1298	Aug	9	2021	samba-dc.xml
-rw-r--r--.	1	root	root	448	Aug	9	2021	samba.xml
-rw-r--r--.	1	root	root	324	Aug	9	2021	sane.xml
-rw-r--r--.	1	root	root	283	Aug	9	2021	sips.xml
-rw-r--r--.	1	root	root	496	Aug	9	2021	sip.xml
-rw-r--r--.	1	root	root	299	Aug	9	2021	slp.xml
-rw-r--r--.	1	root	root	231	Aug	9	2021	smtp-submission.xml
-rw-r--r--.	1	root	root	577	Aug	9	2021	smtps.xml
-rw-r--r--.	1	root	root	550	Aug	9	2021	smtp.xml
-rw-r--r--.	1	root	root	308	Aug	9	2021	snmptrap.xml
-rw-r--r--.	1	root	root	342	Aug	9	2021	snmp.xml
-rw-r--r--.	1	root	root	405	Aug	9	2021	spideroak-lansync.xml
-rw-r--r--.	1	root	root	275	Aug	9	2021	spotify-sync.xml
-rw-r--r--.	1	root	root	173	Aug	9	2021	squid.xml
-rw-r--r--.	1	root	root	421	Aug	9	2021	ssdp.xml

```
-rw-r--r--. 1 root root 463 Aug 9 2021 ssh.xml
-rw-r--r--. 1 root root 631 Aug 9 2021 steam-streaming.xml
-rw-r--r--. 1 root root 287 Aug 9 2021 svdrp.xml
-rw-r--r--. 1 root root 231 Aug 9 2021 svn.xml
-rw-r--r--. 1 root root 297 Aug 9 2021 syncthing-gui.xml
-rw-r--r--. 1 root root 311 Aug 9 2021 syncthing.xml
-rw-r--r--. 1 root root 496 Aug 9 2021 synergy.xml
-rw-r--r--. 1 root root 444 Aug 9 2021 syslog-tls.xml
-rw-r--r--. 1 root root 329 Aug 9 2021 syslog.xml
-rw-r--r--. 1 root root 393 Aug 9 2021 telnet.xml
-rw-r--r--. 1 root root 252 Aug 9 2021 tentacle.xml
-rw-r--r--. 1 root root 288 Aug 9 2021 tftp-client.xml
-rw-r--r--. 1 root root 424 Aug 9 2021 tftp.xml
-rw-r--r--. 1 root root 221 Aug 9 2021 tile38.xml
-rw-r--r--. 1 root root 336 Aug 9 2021 tinc.xml
-rw-r--r--. 1 root root 771 Aug 9 2021 tor-socks.xml
-rw-r--r--. 1 root root 244 Aug 9 2021 transmission-client.xml
-rw-r--r--. 1 root root 264 Aug 9 2021 upnp-client.xml
-rw-r--r--. 1 root root 593 Aug 9 2021 vdsml.xml
-rw-r--r--. 1 root root 475 Aug 9 2021 vnc-server.xml
-rw-r--r--. 1 root root 310 Aug 9 2021 wbem-https.xml
-rw-r--r--. 1 root root 352 Aug 9 2021 wbem-http.xml
-rw-r--r--. 1 root root 323 Aug 9 2021 wsmans.xml
-rw-r--r--. 1 root root 316 Aug 9 2021 wsman.xml
-rw-r--r--. 1 root root 329 Aug 9 2021 xdmcp.xml
-rw-r--r--. 1 root root 509 Aug 9 2021 xmpp-bosh.xml
-rw-r--r--. 1 root root 488 Aug 9 2021 xmpp-client.xml
-rw-r--r--. 1 root root 264 Aug 9 2021 xmpp-local.xml
-rw-r--r--. 1 root root 545 Aug 9 2021 xmpp-server.xml
-rw-r--r--. 1 root root 314 Aug 9 2021 zabbix-agent.xml
-rw-r--r--. 1 root root 315 Aug 9 2021 zabbix-server.xml
```

```
[root@centos8 ~]# ls -l /usr/lib/firewalld/icmptypes/
total 180
```

-rw-r--r--.	1	root	root	385	Aug	9	2021	address-unreachable.xml
-rw-r--r--.	1	root	root	258	Aug	9	2021	bad-header.xml
-rw-r--r--.	1	root	root	294	Aug	9	2021	beyond-scope.xml
-rw-r--r--.	1	root	root	279	Aug	9	2021	communication-prohibited.xml
-rw-r--r--.	1	root	root	222	Aug	9	2021	destination-unreachable.xml
-rw-r--r--.	1	root	root	173	Aug	9	2021	echo-reply.xml
-rw-r--r--.	1	root	root	210	Aug	9	2021	echo-request.xml
-rw-r--r--.	1	root	root	261	Aug	9	2021	failed-policy.xml
-rw-r--r--.	1	root	root	280	Aug	9	2021	fragmentation-needed.xml
-rw-r--r--.	1	root	root	266	Aug	9	2021	host-precedence-violation.xml
-rw-r--r--.	1	root	root	257	Aug	9	2021	host-prohibited.xml
-rw-r--r--.	1	root	root	242	Aug	9	2021	host-redirect.xml
-rw-r--r--.	1	root	root	239	Aug	9	2021	host-unknown.xml
-rw-r--r--.	1	root	root	247	Aug	9	2021	host-unreachable.xml
-rw-r--r--.	1	root	root	229	Aug	9	2021	ip-header-bad.xml
-rw-r--r--.	1	root	root	355	Aug	9	2021	neighbour-advertisement.xml
-rw-r--r--.	1	root	root	457	Aug	9	2021	neighbour-solicitation.xml
-rw-r--r--.	1	root	root	250	Aug	9	2021	network-prohibited.xml
-rw-r--r--.	1	root	root	248	Aug	9	2021	network-redirect.xml
-rw-r--r--.	1	root	root	239	Aug	9	2021	network-unknown.xml
-rw-r--r--.	1	root	root	247	Aug	9	2021	network-unreachable.xml
-rw-r--r--.	1	root	root	239	Aug	9	2021	no-route.xml
-rw-r--r--.	1	root	root	328	Aug	9	2021	packet-too-big.xml
-rw-r--r--.	1	root	root	225	Aug	9	2021	parameter-problem.xml
-rw-r--r--.	1	root	root	233	Aug	9	2021	port-unreachable.xml
-rw-r--r--.	1	root	root	256	Aug	9	2021	precedence-cutoff.xml
-rw-r--r--.	1	root	root	249	Aug	9	2021	protocol-unreachable.xml
-rw-r--r--.	1	root	root	185	Aug	9	2021	redirect.xml
-rw-r--r--.	1	root	root	244	Aug	9	2021	reject-route.xml
-rw-r--r--.	1	root	root	241	Aug	9	2021	required-option-missing.xml
-rw-r--r--.	1	root	root	227	Aug	9	2021	router-advertisement.xml
-rw-r--r--.	1	root	root	223	Aug	9	2021	router-solicitation.xml
-rw-r--r--.	1	root	root	248	Aug	9	2021	source-quench.xml
-rw-r--r--.	1	root	root	236	Aug	9	2021	source-route-failed.xml

```
-rw-r--r--. 1 root root 253 Aug 9 2021 time-exceeded.xml
-rw-r--r--. 1 root root 233 Aug 9 2021 timestamp-reply.xml
-rw-r--r--. 1 root root 228 Aug 9 2021 timestamp-request.xml
-rw-r--r--. 1 root root 258 Aug 9 2021 tos-host-redirect.xml
-rw-r--r--. 1 root root 257 Aug 9 2021 tos-host-unreachable.xml
-rw-r--r--. 1 root root 272 Aug 9 2021 tos-network-redirect.xml
-rw-r--r--. 1 root root 269 Aug 9 2021 tos-network-unreachable.xml
-rw-r--r--. 1 root root 293 Aug 9 2021 ttl-zero-during-reassembly.xml
-rw-r--r--. 1 root root 256 Aug 9 2021 ttl-zero-during-transit.xml
-rw-r--r--. 1 root root 259 Aug 9 2021 unknown-header-type.xml
-rw-r--r--. 1 root root 249 Aug 9 2021 unknown-option.xml
```

Ces fichiers sont au format **xml**, par exemple :

```
[root@centos8 ~]# cat /usr/lib/firewalld/zones/home.xml
<?xml version="1.0" encoding="utf-8"?>
<zone>
  <short>Home</short>
  <description>For use in home areas. You mostly trust the other computers on networks to not harm your computer.
Only selected incoming connections are accepted.</description>
  <service name="ssh"/>
  <service name="mdns"/>
  <service name="samba-client"/>
  <service name="dhcpv6-client"/>
  <service name="cockpit"/>
</zone>
```

La configuration de firewalld ainsi que les définitions et règles personnalisées se trouvent dans **/etc/firewalld** :

```
[root@centos8 ~]# ls -l /etc/firewalld/
total 8
-rw-r--r--. 1 root root 2840 Aug 9 2021 firewalld.conf
drwxr-x---. 2 root root 6 Aug 9 2021 helpers
drwxr-x---. 2 root root 6 Aug 9 2021 icmptypes
```

```
drwxr-x---. 2 root root    6 Aug  9 2021 ipsets
-rw-r--r--. 1 root root 283 Aug  9 2021 lockdown-whitelist.xml
drwxr-x---. 2 root root    6 Aug  9 2021 policies
drwxr-x---. 2 root root    6 Aug  9 2021 services
drwxr-x---. 2 root root   46 Aug  9 2021 zones
```

```
[root@centos8 ~]# ls -l /etc/firewalld/zones/
total 8
-rw-r--r--. 1 root root 380 Jun 16 2021 public.xml
-rw-r--r--. 1 root root 343 Jun 16 2021 public.xml.old
```

```
[root@centos8 ~]# ls -l /etc/firewalld/services/
total 0
```

```
[root@centos8 ~]# ls -l /etc/firewalld/icmptypes/
total 0
```

Le fichier de configuration de firewalld est **/etc/firewalld/firewalld.conf** :

```
[root@centos8 ~]# cat /etc/firewalld/firewalld.conf
# firewalld config file

# default zone
# The default zone used if an empty zone string is used.
# Default: public
DefaultZone=public

# Clean up on exit
# If set to no or false the firewall configuration will not get cleaned up
# on exit or stop of firewalld
# Default: yes
CleanupOnExit=yes

# Lockdown
```

```
# If set to enabled, firewall changes with the D-Bus interface will be limited
# to applications that are listed in the lockdown whitelist.
# The lockdown whitelist file is lockdown-whitelist.xml
# Default: no
Lockdown=no

# IPv6_rpfilter
# Performs a reverse path filter test on a packet for IPv6. If a reply to the
# packet would be sent via the same interface that the packet arrived on, the
# packet will match and be accepted, otherwise dropped.
# The rp_filter for IPv4 is controlled using sysctl.
# Note: This feature has a performance impact. See man page FIREWALLD.CONF(5)
# for details.
# Default: yes
IPv6_rpfilter=yes

# IndividualCalls
# Do not use combined -restore calls, but individual calls. This increases the
# time that is needed to apply changes and to start the daemon, but is good for
# debugging.
# Default: no
IndividualCalls=no

# LogDenied
# Add logging rules right before reject and drop rules in the INPUT, FORWARD
# and OUTPUT chains for the default rules and also final reject and drop rules
# in zones. Possible values are: all, unicast, broadcast, multicast and off.
# Default: off
LogDenied=off

# FirewallBackend
# Selects the firewall backend implementation.
# Choices are:
#     - nftables (default)
```

```
# - iptables (iptables, ip6tables, ebtables and ipset)
FirewallBackend=nftables

# FlushAllOnReload
# Flush all runtime rules on a reload. In previous releases some runtime
# configuration was retained during a reload, namely; interface to zone
# assignment, and direct rules. This was confusing to users. To get the old
# behavior set this to "no".
# Default: yes
FlushAllOnReload=yes

# RFC3964_IPv4
# As per RFC 3964, filter IPv6 traffic with 6to4 destination addresses that
# correspond to IPv4 addresses that should not be routed over the public
# internet.
# Defaults to "yes".
RFC3964_IPv4=yes

# AllowZoneDrifting
# Older versions of firewalld had undocumented behavior known as "zone
# drifting". This allowed packets to ingress multiple zones - this is a
# violation of zone based firewalls. However, some users rely on this behavior
# to have a "catch-all" zone, e.g. the default zone. You can enable this if you
# desire such behavior. It's disabled by default for security reasons.
# Note: If "yes" packets will only drift from source based zones to interface
# based zones (including the default zone). Packets never drift from interface
# based zones to other interfaces based zones (including the default zone).
# Possible values; "yes", "no". Defaults to "yes".
AllowZoneDrifting=yes
```

La Commande firewall-cmd

firewalld s'appuie sur netfilter. Pour cette raison, l'utilisation de firewall-cmd est incompatible avec l'utilisation des commandes iptables et system-

config-firewall.



Important - firewall-cmd est le front-end de firewalld en ligne de commande. Il existe aussi la commande **firewall-config** qui lance un outil de configuration graphique.

Pour obtenir la liste de toutes les zones prédéfinies, utilisez la commande suivante :

```
[root@centos8 ~]# firewall-cmd --get-zones
block dmz drop external home internal libvirt nm-shared public trusted work
```

Pour obtenir la liste de tous les services prédéfinis, utilisez la commande suivante :

```
[root@centos8 ~]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule amanda-client amanda-k5-client amqp amqps apcupsd audit bacula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-mon cfengine cockpit collectd condor-collector ctdb dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git grafana gre high-availability http https imap imaps ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-apiserver ldap ldaps libvirt libvirt-tls lightning-network llmnr managesieve matrix mdns memcache minidlna mongodb mosh mntd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nfs nfs3 nmap-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus proxy-dhcp ptp pulseaudio puppetmaster quassel radius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane sip sips slp smtp smtp-submission smtps snmp snmptrap spideroak-lansync spotify-sync squid ssdp ssh steam-streaming svdrp svn syncthing syncthing-gui synergy syslog syslog-tls telnet tentacle tftp tftp-client tile38 tinc tor-socks transmission-client upnp-client vds vnc-server wbem-http wbem-https wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server
```

Pour obtenir la liste de tous les types ICMP prédéfinis, utilisez la commande suivante :

```
[root@centos8 ~]# firewall-cmd --get-icmptypes
address-unreachable bad-header beyond-scope communication-prohibited destination-unreachable echo-reply echo-request failed-policy fragmentation-needed host-precedence-violation host-prohibited host-redirect host-unknown host-unreachable ip-header-bad neighbour-advertisement neighbour-solicitation network-prohibited network-redirect network-unknown network-unreachable no-route packet-too-big parameter-problem port-unreachable precedence-cutoff protocol-unreachable redirect reject-route required-option-missing router-advertisement router-solicitation source-quench source-route-failed time-exceeded timestamp-reply timestamp-request tos-host-redirect tos-host-unreachable tos-network-redirect tos-network-unreachable ttl-zero-during-reassembly ttl-zero-during-transit unknown-header-type unknown-option
```

Pour obtenir la liste des zones de la configuration courante, utilisez la commande suivante :

```
[root@centos8 ~]# firewall-cmd --get-active-zones
libvirt
  interfaces: virbr0
public
  interfaces: ens18
```

Pour obtenir la liste des zones de la configuration courante pour une interface spécifique, utilisez la commande suivante :

```
[root@centos8 ~]# firewall-cmd --get-zone-of-interface=ens18
public
```

Pour obtenir la liste des services autorisés pour la zone public, utilisez la commande suivante :

```
[root@centos8 ~]# firewall-cmd --zone=public --list-services
cockpit dhcpv6-client ssh
```

Pour obtenir toute la configuration pour la zone public, utilisez la commande suivante :

```
[root@centos8 ~]# firewall-cmd --get-active-zones
libvirt
  interfaces: virbr0
```

```
public
  interfaces: ens18
[root@centos8 ~]# firewall-cmd --get-zone-of-interface=ens18
public
[root@centos8 ~]# firewall-cmd --zone=public --list-services
cockpit dhcpv6-client ssh
[root@centos8 ~]# firewall-cmd --zone=public --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens18
  sources:
  services: cockpit dhcpv6-client ssh
  ports: 5901/tcp
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Pour obtenir la liste complète de toutes les zones et leurs configurations, utilisez la commande suivante :

```
root@centos8 ~]# firewall-cmd --zone=public --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens18
  sources:
  services: cockpit dhcpv6-client ssh
  ports: 5901/tcp
  protocols:
  forward: no
```

```
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
[root@centos8 ~]# firewall-cmd --list-all-zones
block
  target: %%REJECT%%
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

dmz
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: ssh
  ports:
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
```

rich rules:

drop

target: DROP

icmp-block-inversion: no

interfaces:

sources:

services:

ports:

protocols:

forward: no

masquerade: no

forward-ports:

source-ports:

icmp-blocks:

rich rules:

external

target: default

icmp-block-inversion: no

interfaces:

sources:

services: ssh

ports:

protocols:

forward: no

masquerade: yes

forward-ports:

source-ports:

icmp-blocks:

rich rules:

home

target: default

```
icmp-block-inversion: no
interfaces:
sources:
services: cockpit dhcpv6-client mdns samba-client ssh
ports:
protocols:
forward: no
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
```

internal

```
target: default
icmp-block-inversion: no
interfaces:
sources:
services: cockpit dhcpv6-client mdns samba-client ssh
ports:
protocols:
forward: no
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
```

libvirt (active)

```
target: ACCEPT
icmp-block-inversion: no
interfaces: virbr0
sources:
services: dhcp dhcpv6 dns ssh tftp
```

```
ports:
protocols: icmp ipv6-icmp
forward: no
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
    rule priority="32767" reject
```

nm-shared

```
target: ACCEPT
icmp-block-inversion: no
interfaces:
sources:
services: dhcp dns ssh
ports:
protocols: icmp ipv6-icmp
forward: no
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
    rule priority="32767" reject
```

public (active)

```
target: default
icmp-block-inversion: no
interfaces: ens18
sources:
services: cockpit dhcpv6-client ssh
ports: 5901/tcp
protocols:
```

```
forward: no
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
```

trusted

```
target: ACCEPT
icmp-block-inversion: no
interfaces:
sources:
services:
ports:
protocols:
forward: no
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
```

work

```
target: default
icmp-block-inversion: no
interfaces:
sources:
services: cockpit dhcpv6-client ssh
ports:
protocols:
forward: no
masquerade: no
forward-ports:
source-ports:
```

```
icmp-blocks:  
rich rules:
```

Pour changer la zone par défaut de public à work, utilisez la commande suivante :

```
[root@centos8 ~]# firewall-cmd --set-default-zone=work  
success  
  
[root@centos8 ~]# firewall-cmd --get-active-zones  
libvirt  
  interfaces: virbr0  
work  
  interfaces: ens18
```

Pour ajouter l'interface ip_fixe à la zone work, utilisez la commande suivante :

```
[root@centos8 ~]# firewall-cmd --zone=work --add-interface=ip_fixe  
success  
  
[root@centos8 ~]# firewall-cmd --get-active-zones  
libvirt  
  interfaces: virbr0  
work  
  interfaces: ens18 ip_fixe
```

Pour supprimer l'interface ip_fixe à la zone work, utilisez la commande suivante :

```
[root@centos8 ~]# firewall-cmd --zone=work --remove-interface=ip_fixe  
success  
  
[root@centos8 ~]# firewall-cmd --get-active-zones  
libvirt  
  interfaces: virbr0  
work
```

```
interfaces: ens18
```

Pour ajouter le service **http** à la zone **work**, utilisez la commande suivante :

```
[root@centos8 ~]# firewall-cmd --zone=work --add-service=http  
success
```

```
[root@centos8 ~]# firewall-cmd --zone=work --list-services  
cockpit dhcpv6-client http ssh
```

Pour supprimer le service **http** de la zone **work**, utilisez la commande suivante :

```
[root@centos8 ~]# firewall-cmd --zone=work --remove-service=http  
success
```

```
[root@centos8 ~]# firewall-cmd --zone=work --list-services  
cockpit dhcpv6-client ssh
```

Pour ajouter un nouveau bloc ICMP, utilisez la commande suivante :

```
[root@centos8 ~]# firewall-cmd --zone=work --add-icmp-block=echo-reply  
success
```

```
[root@centos8 ~]# firewall-cmd --zone=work --list-icmp-blocks  
echo-reply
```

Pour supprimer un bloc ICMP, utilisez la commande suivante :

```
[root@centos8 ~]# firewall-cmd --zone=work --remove-icmp-block=echo-reply  
success
```

```
[root@centos8 ~]# firewall-cmd --zone=work --list-icmp-blocks
```

```
[root@centos8 ~]#
```

Pour ajouter le port 591/tcp à la zone work, utilisez la commande suivante :

```
[root@centos8 ~]# firewall-cmd --zone=work --add-port=591/tcp  
success
```

```
[root@centos8 ~]# firewall-cmd --zone=work --list-ports  
591/tcp
```

Pour supprimer le port 591/tcp à la zone work, utilisez la commande suivante :

```
[root@centos8 ~]# firewall-cmd --zone=work --remove-port=591/tcp  
success
```

```
[root@centos8 ~]# firewall-cmd --zone=work --list-ports
```

```
[root@centos8 ~]#
```

Pour créer un nouveau service, il convient de :

- copier un fichier existant se trouvant dans le répertoire **/usr/lib/firewalld/services** vers **/etc/firewalld/services**,
- modifier le fichier,
- recharger la configuration de firewalld,
- vérifier que firewalld voit le nouveau service.

Par exemple :

```
[root@centos8 ~]# cp /usr/lib/firewalld/services/http.xml /etc/firewalld/services/filemaker.xml
```

```
[root@centos8 ~]# vi /etc/firewalld/services/filemaker.xml
```

```
[root@centos8 ~]# cat /etc/firewalld/services/filemaker.xml  
<?xml version="1.0" encoding="utf-8"?>
```

```
<service>
  <short>FileMakerPro</short>
  <description>fichier de service firewalld pour FileMaker Pro</description>
  <port protocol="tcp" port="591"/>
</service>
```

```
[root@centos8 ~]# firewall-cmd --reload
success
```

```
[root@centos8 ~]# firewall-cmd --get-services
```

```
RH-Satellite-6 RH-Satellite-6-capsule amanda-client amanda-k5-client amqp amqps apcupsd audit bacula bacula-
client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-mon cfengine
cockpit collectd condor-collector ctdb dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry docker-
swarm dropbox-lansync elasticsearch etcd-client etcd-server filemaker finger foreman foreman-proxy freeipa-4
freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git grafana
gre high-availability http https imap imaps ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin
kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-apiserver ldap ldaps libvirt libvirt-tls lightning-
network llmnr managesieve matrix mdns memcache minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur
mysql nbd nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd
pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus proxy-dhcp ptp pulseaudio puppetmaster
quassel radius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc
sane sip sips slp smtp smtp-submission smtps snmp snmptrap spideroak-lansync spotify-sync squid sssd ssh steam-
streaming svdrp svn syncthing syncthing-gui synergy syslog syslog-tls telnet tentacle tftp tftp-client tile38
tinc tor-socks transmission-client upnp-client vdsd vnc-server wbem-http wbem-https wsman wsmans xdmcp xmpp-bosh
xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-server
```

La Configuration Avancée de firewalld

La configuration de base de firewalld ne permet que la configuration des zones, services, blocs ICMP et les ports non-standard. Cependant firewalld peut également être configuré avec des **Rich Rules** ou **Règles Riches**. Rich Rules ou Règles Riches évaluent des **critères** pour ensuite entreprendre une **action**.

Les **Critères** sont :

- **source address**= "<adresse_IP>"
- **destination address**= "<adresse_IP>",
- **rule port port**= "<numéro_du_port>",
- **service name**= <nom_d'un_sevice_prédéfini>.

Les **Actions** sont :

- **accept**,
- **reject**,
 - une Action reject peut être associée avec un message d'erreur spécifique par la clause **type**= "<type_d'erreur>",
- **drop**.

Saisissez la commande suivante pour ouvrir le port 80 :

```
[root@centos8 ~]# firewall-cmd --add-rich-rule='rule port port="80" protocol="tcp" accept' success
```



Important - Notez que la Rich Rule doit être entourée de caractères '.



Important - Notez que la Rich Rule a créé deux règles, une pour IPv4 et une deuxième pour IPv6. Une règle peut être créée pour IPv4 seul en incluant le Critère **family=ipv4**. De la même façon, une règle peut être créée pour IPv6 seul en incluant le Critère **family=ipv6**.

Cette nouvelle règle est écrite en mémoire mais non pas sur disque. Pour l'écrire sur disque dans le fichier zone se trouvant dans **/etc/firewalld**, il faut ajouter l'option **-permanent** :

```
[root@centos8 ~]# firewall-cmd --add-rich-rule='rule port port="80" protocol="tcp" accept' --permanent success
```

```
[root@centos8 ~]# cat /etc/firewalld/zones/work.xml
<?xml version="1.0" encoding="utf-8"?>
<zone>
  <short>Work</short>
  <description>For use in work areas. You mostly trust the other computers on networks to not harm your computer.
Only selected incoming connections are accepted.</description>
  <service name="ssh"/>
  <service name="dhcpv6-client"/>
  <service name="cockpit"/>
  <rule>
    <port port="80" protocol="tcp"/>
    <accept/>
  </rule>
</zone>
```



Important - Attention ! La règle ajoutée avec l'option `-permanent` n'est pas prise en compte immédiatement mais uniquement au prochain redémarrage. Pour qu'une règle soit appliquée immédiatement **et** être écrite sur disque, il faut saisir la commande deux fois dont une avec l'option `-permanent` et l'autre sans l'option `-permanent`.

Redémarrez le service **firewalld** :

```
[root@centos8 ~]# systemctl restart firewalld.service
```

Pour visualiser cette règle dans la configuration de firewalld, il convient de saisir la commande suivante :

```
[root@centos8 ~]# firewall-cmd --zone=work --list-all
work (active)
  target: default
  icmp-block-inversion: no
```

```
interfaces: ens18
sources:
services: cockpit dhcpv6-client ssh
ports:
protocols:
forward: no
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
    rule port port="80" protocol="tcp" accept
```

Notez que la Rich Rule est créée dans la Zone par Défaut. Il est possible de créer une Rich Rule dans une autre zone en utilisant l'option **-zone=<zone>** de la commande firewall-cmd :

```
[root@centos8 ~]# firewall-cmd --zone=public --add-rich-rule='rule port port="80" protocol="tcp" accept'
success
```

```
[root@centos8 ~]# firewall-cmd --zone=public --list-all
public
target: default
icmp-block-inversion: no
interfaces:
sources:
services: cockpit dhcpv6-client ssh
ports: 5901/tcp
protocols:
forward: no
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
```

```
rule port port="80" protocol="tcp" accept
```

Pour supprimer une Rich Rule, il faut copier la ligne entière la concernant qui se trouve dans la sortie de la commande **firewall-cmd -list-all-zones** :

```
[root@centos8 ~]# firewall-cmd --zone=public --remove-rich-rule='rule port port="80" protocol="tcp" accept'
success
```

Le mode Panic de firewalld

Le mode Panic de firewalld permet de bloquer tout le trafic avec une seule commande. Pour connaître l'état du mode Panic, utilisez la commande suivante :

```
[root@centos8 ~]# firewall-cmd --query-panic
no
```

Pour activer le mode Panic, il convient de saisir la commande suivante :

```
# firewall-cmd --panic-on
```

Pour désactiver le mode Panic, il convient de saisir la commande suivante :

```
# firewall-cmd --panic-off
```

System Hardening

Les compilateurs

Afin d'empêcher un pirate de créer des exécutables sur le serveur vous devez modifier les permissions sur les compilateurs éventuellement présents afin que seulement root puisse les exécuter.

Les paquets

Il convient dans ce cas de passer en revue la liste des paquets installés puis de supprimer ceux qui sont jugés être inutiles :

```
[root@centos8 ~]# rpm -qa | more
librepo-1.14.0-2.el8.x86_64
prefixdevname-0.1.0-6.el8.x86_64
zip-3.0-23.el8.x86_64
gnome-shell-extension-desktop-icons-3.32.1-22.el8_5.noarch
python3-setuptools-wheel-39.2.0-6.el8.noarch
perl-Term-Cap-1.17-395.el8.noarch
accountsservice-libs-0.6.55-2.el8_5.2.x86_64
enchant2-2.2.3-3.el8.x86_64
google-noto-sans-lisu-fonts-20161022-7.el8.1.noarch
ipset-libs-7.1-1.el8.x86_64
pangomm-2.40.1-6.el8.x86_64
anaconda-gui-33.16.5.6-1.el8.x86_64
libibverbs-35.0-1.el8.x86_64
thai-scalable-waree-fonts-0.6.5-1.el8.noarch
libidn-1.34-5.el8.x86_64
tuned-2.16.0-1.el8.noarch
kbd-legacy-2.0.4-10.el8.noarch
NetworkManager-team-1.32.10-4.el8.x86_64
lohit-kannada-fonts-2.5.4-3.el8.noarch
ipxe-roms-qemu-20181214-8.git133f4c47.el8.noarch
openssh-server-8.0p1-10.el8.x86_64
sssd-nfs-idmap-2.5.2-2.el8_5.3.x86_64
cronie-anacron-1.5.2-4.el8.x86_64
libgdither-0.6-17.el8.x86_64
libcanberra-gtk3-0.30-18.el8.x86_64
net-snmp-libs-5.8-22.el8.x86_64
libnl3-3.5.0-1.el8.x86_64
libblockdev-lvm-2.24-7.el8.x86_64
```

```
libjose-10-2.el8.x86_64
jq-1.5-12.el8.x86_64
zenity-3.28.1-1.el8.x86_64
lz4-1.8.3-3.el8_4.x86_64
flatpak-selinux-1.8.5-5.el8_5.noarch
python3-ordered-set-2.0.2-4.el8.noarch
bash-4.4.20-2.el8.x86_64
libpkgconf-1.4.2-1.el8.x86_64
gnome-keyring-3.28.2-1.el8.x86_64
iwl100-firmware-39.31.5.1-103.el8.1.noarch
python3-libstoragemgmt-1.9.1-1.el8.x86_64
libtevent-0.11.0-0.el8.x86_64
gnome-themes-standard-3.22.3-4.el8.x86_64
augeas-libs-1.12.0-6.el8.x86_64
fprintd-pam-1.90.9-2.el8.x86_64
setroubleshoot-plugins-3.3.14-1.el8.noarch
osinfo-db-tools-1.9.0-1.el8.x86_64
libwayland-server-1.19.0-1.el8.x86_64
libvirt-daemon-driver-interface-6.0.0-37.module_el8.5.0+1002+36725df2.x86_64
kernel-modules-4.18.0-305.3.1.el8.x86_64
libbpf-0.4.0-1.el8.x86_64
libexif-0.6.22-5.el8_3.x86_64
python3-simpleline-1.1.1-2.el8.noarch
cockpit-system-251.1-1.el8.noarch
python3-setools-4.3.0-2.el8.x86_64
perl-IO-1.38-420.el8.x86_64
ibus-typing-booster-2.1.0-5.el8.noarch
--More--
[q]
```

Les démons et services

Il convient dans ce cas de passer en revue la liste des démons et services actives puis de supprimer ceux qui sont jugés être inutiles;

- ps aux
- chkconfig -list
- systemctl list-unit-files

```
[root@centos8 ~]# ps aux | more
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.0 241416 14192 ?        Ss   12:13   0:02 /usr/lib/systemd/systemd --switched-root --
system --deserialize 18
root           2  0.0  0.0      0      0 ?        S    12:13   0:00 [kthreadd]
root           3  0.0  0.0      0      0 ?        I<   12:13   0:00 [rcu_gp]
root           4  0.0  0.0      0      0 ?        I<   12:13   0:00 [rcu_par_gp]
root           6  0.0  0.0      0      0 ?        I<   12:13   0:00 [kworker/0:0H-events_highpri]
root           9  0.0  0.0      0      0 ?        I<   12:13   0:00 [mm_percpu_wq]
root          10  0.0  0.0      0      0 ?        S    12:13   0:00 [ksoftirqd/0]
root          11  0.0  0.0      0      0 ?        I    12:13   0:00 [rcu_sched]
root          12  0.0  0.0      0      0 ?        S    12:13   0:00 [migration/0]
root          13  0.0  0.0      0      0 ?        S    12:13   0:00 [watchdog/0]
root          14  0.0  0.0      0      0 ?        S    12:13   0:00 [cpuhp/0]
root          15  0.0  0.0      0      0 ?        S    12:13   0:00 [cpuhp/1]
root          16  0.0  0.0      0      0 ?        S    12:13   0:00 [watchdog/1]
root          17  0.0  0.0      0      0 ?        S    12:13   0:00 [migration/1]
root          18  0.0  0.0      0      0 ?        S    12:13   0:00 [ksoftirqd/1]
root          20  0.0  0.0      0      0 ?        I<   12:13   0:00 [kworker/1:0H-events_highpri]
root          21  0.0  0.0      0      0 ?        S    12:13   0:00 [cpuhp/2]
root          22  0.0  0.0      0      0 ?        S    12:13   0:00 [watchdog/2]
root          23  0.0  0.0      0      0 ?        S    12:13   0:00 [migration/2]
root          24  0.0  0.0      0      0 ?        S    12:13   0:00 [ksoftirqd/2]
root          26  0.0  0.0      0      0 ?        I<   12:13   0:00 [kworker/2:0H-events_highpri]
root          27  0.0  0.0      0      0 ?        S    12:13   0:00 [cpuhp/3]
root          28  0.0  0.0      0      0 ?        S    12:13   0:00 [watchdog/3]
root          29  0.0  0.0      0      0 ?        S    12:13   0:00 [migration/3]
root          30  0.0  0.0      0      0 ?        S    12:13   0:00 [ksoftirqd/3]
root          32  0.0  0.0      0      0 ?        I<   12:13   0:00 [kworker/3:0H-events_highpri]
root          33  0.0  0.0      0      0 ?        S    12:13   0:00 [cpuhp/4]
```

```

root      34  0.0  0.0    0    0 ?      S   12:13   0:00 [watchdog/4]
root      35  0.0  0.0    0    0 ?      S   12:13   0:00 [migration/4]
root      36  0.0  0.0    0    0 ?      S   12:13   0:00 [ksoftirqd/4]
root      38  0.0  0.0    0    0 ?      I<  12:13   0:00 [kworker/4:0H-events_highpri]
root      39  0.0  0.0    0    0 ?      S   12:13   0:00 [cpuhp/5]
root      40  0.0  0.0    0    0 ?      S   12:13   0:00 [watchdog/5]
root      41  0.0  0.0    0    0 ?      S   12:13   0:00 [migration/5]
root      42  0.0  0.0    0    0 ?      S   12:13   0:00 [ksoftirqd/5]
root      44  0.0  0.0    0    0 ?      I<  12:13   0:00 [kworker/5:0H-events_highpri]
root      45  0.0  0.0    0    0 ?      S   12:13   0:00 [cpuhp/6]
root      46  0.0  0.0    0    0 ?      S   12:13   0:00 [watchdog/6]
root      47  0.0  0.0    0    0 ?      S   12:13   0:00 [migration/6]
root      48  0.0  0.0    0    0 ?      S   12:13   0:00 [ksoftirqd/6]
root      49  0.0  0.0    0    0 ?      I   12:13   0:00 [kworker/6:0-mm_percpu_wq]
root      50  0.0  0.0    0    0 ?      I<  12:13   0:00 [kworker/6:0H-events_highpri]
root      51  0.0  0.0    0    0 ?      S   12:13   0:00 [cpuhp/7]
root      52  0.0  0.0    0    0 ?      S   12:13   0:00 [watchdog/7]
root      53  0.0  0.0    0    0 ?      S   12:13   0:00 [migration/7]
root      54  0.0  0.0    0    0 ?      S   12:13   0:00 [ksoftirqd/7]
root      56  0.0  0.0    0    0 ?      I<  12:13   0:00 [kworker/7:0H-events_highpri]
root      65  0.0  0.0    0    0 ?      S   12:13   0:00 [kdevtmpfs]
root      66  0.0  0.0    0    0 ?      I<  12:13   0:00 [netns]
root      67  0.0  0.0    0    0 ?      S   12:13   0:00 [rcu_tasks_trace]
root      68  0.0  0.0    0    0 ?      S   12:13   0:00 [rcu_tasks_rude_]
root      69  0.0  0.0    0    0 ?      S   12:13   0:00 [kauditd]
root      70  0.0  0.0    0    0 ?      S   12:13   0:00 [khungtaskd]
root      71  0.0  0.0    0    0 ?      S   12:13   0:00 [oom_reaper]
--More--
[q]

```

```
[root@centos8 ~]# chkconfig --list
```

Note: This output shows SysV services only and does not include native systemd services. SysV configuration data might be overridden by native

systemd configuration.

If you want to list systemd services use 'systemctl list-unit-files'.
To see services enabled on particular target use
'systemctl list-dependencies [target]'.

```
[root@centos8 ~]# systemctl list-unit-files
UNIT FILE                                STATE
proc-sys-fs-binfmt_misc.automount      static
-.mount                                generated
boot.mount                              generated
dev-hugepages.mount                    static
dev-mqueue.mount                       static
proc-fs-nfsd.mount                     static
proc-sys-fs-binfmt_misc.mount          static
run-vmblock\x2dfuse.mount              disabled
sys-fs-fuse-connections.mount          static
sys-kernel-config.mount                static
sys-kernel-debug.mount                 static
tmp.mount                              disabled
var-lib-machines.mount                 static
var-lib-nfs-rpc_pipefs.mount           static
cups.path                              enabled
ostree-finalize-staged.path             disabled
systemd-ask-password-console.path      static
systemd-ask-password-plymouth.path     static
systemd-ask-password-wall.path         static
session-1.scope                        transient
session-5.scope                        transient
session-cl.scope                       transient
accounts-daemon.service                enabled
alsa-restore.service                  static
alsa-state.service                    static
anaconda-direct.service                static
```

anaconda-fips.service	static
anaconda-nm-config.service	static
anaconda-noshell.service	static
anaconda-pre.service	static
anaconda-shell@.service	static
anaconda-sshd.service	static
anaconda-tmux@.service	static
anaconda.service	static
arp-ethers.service	disabled
atd.service	enabled
auditd.service	enabled
auth-rpcgss-module.service	static
autovt@.service	enabled
avahi-daemon.service	enabled
blivet.service	static
blk-availability.service	disabled
bluetooth.service	enabled
bolt.service	static
brltty.service	disabled
btattach-bcm@.service	static
canberra-system-bootup.service	disabled
canberra-system-shutdown-reboot.service	disabled
canberra-system-shutdown.service	disabled
chrony-dnssrv@.service	static
chrony-wait.service	disabled
chronyd.service	enabled
cockpit-motd.service	static
cockpit-wsinstance-http-redirect.service	static
lines 1-55	
[q]	

Les fichiers .rhosts

Le système rhosts présente une faille de sécurité importante pour un serveur Linux. Pour cette raison, il convient de supprimer les fichiers **.rhosts** des utilisateurs. Utilisez la commande suivante:

```
# find / -name ".rhosts" -exec rm -f {} \; [Entree]
```

Les fichiers et les répertoires sans propriétaire

Afin de dresser la liste des fichiers et des groupes sans propriétaires sur le serveur, il convient d'utiliser les deux commandes suivantes:

```
# find / -nouser -exec ls -l {} \; 2> sans_pro.txt [Entree]
```

```
# find / -nogroup -exec ls -l {} \; 2>> sans_pro.txt[Entree]
```

Ces commandes produiront une liste éventuelle dans le fichier **sans_pro.txt**.

L'examen de cette liste pourrait dévoiler des anomalies au quel cas il conviendrait de:

- modifier le propriétaire a root
- modifier le groupe a root
- modifier les permissions a 700

Limiter le délai d'inactivité d'une session shell

Une session de shell laissée ouverte inutilement et d'une manière sans surveillance est un risque de sécurité. Vérifiez donc le contenu du fichier **/etc/profile** :

```
[root@centos8 ~]# cat /etc/profile  
# /etc/profile
```

```
# System wide environment and startup programs, for login setup
# Functions and aliases go in /etc/bashrc

# It's NOT a good idea to change this file unless you know what you
# are doing. It's much better to create a custom.sh shell script in
# /etc/profile.d/ to make custom changes to your environment, as this
# will prevent the need for merging in future updates.
```

```
pathmunge () {
    case "${PATH}:" in
        *:"$1":*)
            ;;
        *)
            if [ "$2" = "after" ] ; then
                PATH=$PATH:$1
            else
                PATH=$1:$PATH
            fi
    esac
}
```

```
if [ -x /usr/bin/id ]; then
    if [ -z "$EUID" ]; then
        # ksh workaround
        EUID=`/usr/bin/id -u`
        UID=`/usr/bin/id -ru`
    fi
    USER="/usr/bin/id -un`"
    LOGNAME=$USER
    MAIL="/var/spool/mail/$USER"
fi
```

```
# Path manipulation
```

```
if [ "$EUID" = "0" ]; then
    pathmunge /usr/sbin
    pathmunge /usr/local/sbin
else
    pathmunge /usr/local/sbin after
    pathmunge /usr/sbin after
fi

HOSTNAME=`/usr/bin/hostname 2>/dev/null`
HISTSIZE=1000
if [ "$HISTCONTROL" = "ignorespace" ] ; then
    export HISTCONTROL=ignoreboth
else
    export HISTCONTROL=ignoredups
fi

export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE HISTCONTROL

# By default, we want umask to get set. This sets it for login shell
# Current threshold for system reserved uid/gids is 200
# You could check uidgid reservation validity in
# /usr/share/doc/setup-*/uidgid file
if [ $UID -gt 199 ] && [ "`/usr/bin/id -gn`" = "`/usr/bin/id -un`" ]; then
    umask 002
else
    umask 022
fi

for i in /etc/profile.d/*.sh /etc/profile.d/sh.local ; do
    if [ -r "$i" ]; then
        if [ "${-#*i}" != "$-" ]; then
            . "$i"
        else
            . "$i" >/dev/null
        fi
    fi
done
```

```
        fi
    fi
done

unset i
unset -f pathmunge

if [ -n "${BASH_VERSION-}" ] ; then
    if [ -f /etc/bashrc ] ; then
        # Bash login shells run only /etc/profile
        # Bash non-login shells run only /etc/bashrc
        # Check for double sourcing is done in /etc/bashrc.
        . /etc/bashrc
    fi
fi
```

A ce fichier doivent être ajoutées les deux lignes suivantes:

```
readonly TMOUT=300
export TMOUT
```

Par cette action, vous définissez le délai d'inactivité d'une session shell à une durée de 5 minutes.

Dernièrement, afin de se protéger contre des permissions trop permissives lors de la création de fichiers et de répertoires, il convient de passer la valeur d'**umask** à **077** dans le fichier **/etc/profile**.

Renforcer la securite d'init

Les Distributions SysVinit

Le fichier **/etc/inittab** est utilise pour configurer le démarrage de votre serveur.

La première modification à effectuer est de spécifier le niveau d'exécution par défaut a 3 au lieu de 5. Ceci permet de ne pas lancer les sessions graphiques sur une serveur de production. Cherchez donc la ligne suivante:

```
id:5:initdefault:
```

Modifiez-la en:

```
id:3:initdefault:
```

Le mode **single user** de démarrage de Linux n'est pas habituellement protégé par un mot de passe. Afin de remédier a cela, ajoutez les lignes suivantes:

```
# Single user mode
~~:S:wait:/sbin/sulogin
```

Dernièrement, afin d'empêcher une personne a redémarrer le serveur à l'aide des touches **ctrl+alt+supp**, il convient de mettre en commentaire la ligne correspondante:

```
# ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

Les Distributions Upstart

Afin d'empêcher une personne à redémarrer le serveur à l'aide des touches **ctrl+alt+supp**, éditez le fichier **/etc/init/control-alt-delete.conf** en modifiant la ligne suivante :

```
exec /sbin/shutdown -r now "Control-Alt-Delete pressed"
```

en

```
#exec /sbin/shutdown -k now "Control-Alt-Delete pressed"
```

Renforcer la sécurité du Noyau

La commande sysctl

Les fichiers dans le répertoire **/proc/sys** peuvent être administrés par la commande **sysctl** en temps réel.

La commande **sysctl** applique les règles consignés dans le fichier **/etc/sysctl.conf** au démarrage de la machine.

Saisissez la commande :

```
[root@centos8 ~]# cat /etc/sysctl.conf
# sysctl settings are defined through files in
# /usr/lib/sysctl.d/, /run/sysctl.d/, and /etc/sysctl.d/.
#
# Vendors settings live in /usr/lib/sysctl.d/.
# To override a whole file, create a new file with the same in
# /etc/sysctl.d/ and put new settings there. To override
# only specific settings, add a file with a lexically later
# name in /etc/sysctl.d/ and put new settings there.
#
# For more information, see sysctl.conf(5) and sysctl.d(5).
```

```
[root@centos8 ~]# ls -la /etc/sysctl.d
total 12
drwxr-xr-x.  2 root root  28 Dec 21  2021 .
drwxr-xr-x. 143 root root 8192 Oct  1 12:13 ..
lrwxrwxrwx.  1 root root  14 Dec 21  2021 99-sysctl.conf -> ../sysctl.conf
```

Options de la commande

Les options de la commande **sysctl** sont :

```
[root@centos8 ~]# sysctl --help
```

Usage:

```
sysctl [options] [variable[=value] ...]
```

Options:

-a, --all	display all variables
-A	alias of -a
-X	alias of -a
--deprecated	include deprecated parameters to listing
-b, --binary	print value without new line
-e, --ignore	ignore unknown variables errors
-N, --names	print variable names without values
-n, --values	print only values of the given variable(s)
-p, --load[=<file>]	read values from file
-f	alias of -p
--system	read values from all system directories
-r, --pattern <expression>	select setting that match expression
-q, --quiet	do not echo variable set
-w, --write	enable writing a value to variable
-o	does nothing
-x	does nothing
-d	alias of -h
-h, --help	display this help and exit
-V, --version	output version information and exit

For more details see `sysctl(8)`.



Important : Consultez la page de la traduction du manuel de **sysctl** [ici](#) pour comprendre la commande.

Mise en place de SELinux pour sécuriser le serveur

Introduction

L'approche SELinux (*Security Enhanced Linux*) à la sécurité est une approche de type **TE**. Elle essaie aussi d'intégrer les notions des approches de type **RBAC**, **MAC** et **MLS** sous la forme de **MCS** : ur

Type de Sécurité	Nom	Description
TE	<i>Type enforcement</i>	Chaque objet a une étiquette appelé <i>type</i> pour un fichier et <i>domaine</i> pour un processus. La politique de sécurité définit l'interaction entre les types et les domaines.
RBAC	<i>Role Based Access Control</i>	Un utilisateur a un ou plusieurs rôles. Les droits sont attribués aux rôles.
MAC	<i>Mandatory Access Control</i>	L'accès aux objets est en fonction de la classification de l'objet (Très secret, Secret, Confidentiel, Public). L'administrateur définit la politique de sécurité et les utilisateurs s'y conforment.
MLS	<i>Multi-Level Security</i>	Les politiques de sécurité imposent que qu'un sujet doit dominer un objet pour pouvoir le lire tandis que l'objet doit dominer le sujet pour que ce dernier puisse y écrire.

Même quand le modèle SELinux de sécurité est actif, la sécurité type DAC est toujours active. Cependant dans le cas où la sécurité du type DAC autorise une action, SELinux va évaluer cette action par rapport à ses propres règles avant de l'autoriser.

SELinux évalue toujours des **actions** tentées par des **sujets** sur des **objets**.

Dans le contexte de SELinux :

- un **sujet** est toujours un **processus**,
- un **objet** peut être un fichier, un répertoire, un autre processus ou une ressource système,
- une **action** est une **permission**.

Chaque **classe d'objet** possède un jeu de permissions possibles ou **actions** qui peuvent être uniques à la classe ou bien **héritées** d'autres classes.

Définitions

Security Context

SELinux associe un *Security Context* (SC) à chaque **objet** et **sujet** du système.

Un SC prend la forme **identité:rôle:type:niveau** :

Nom	Descriptions
Identité	Le nom du propriétaire de l'objet. Une identité est associée à des rôles. Par défaut l'utilisateur à une identité de user_u .
Rôle	Essentiellement appliqué aux processus, le rôle est appelé une domaine. Dans le cas d'un rôle de fichier, celui-ci est toujours object_r . Un rôle se termine généralement par _r .
Type	Définit la classification de sécurité de l'objet. Un type se termine généralement par _t .
Niveau	Un niveau est un attribut de MLS et MCS. Une plage MLS est une paire de niveaux exprimée en utilisant la syntaxe <i>niveaubas-niveauhaut</i> . Chaque niveau est une paire exprimée en tant que sensibilitéhaut-sensibilitébas:catégoriehaut:catégoriebas par exemple s0-s0:c0.c1023. Il est important de noter que s0-s0 s'exprime aussi s0 et c0, c1, c2, c3 est exprimé c0.c3.

Sous RHEL/CentOS 8, le fichier **/etc/selinux/targeted/setrans.conf** contient la correspondance entre les niveaux et leurs valeurs compréhensibles par l'utilisateur :

```
[root@centos8 ~]# cat /etc/selinux/targeted/setrans.conf
#
# Multi-Category Security translation table for SELinux
#
# Uncomment the following to disable translation library
# disable=1
#
# Objects can be categorized with 0-1023 categories defined by the admin.
# Objects can be in more than one category at a time.
# Categories are stored in the system as c0-c1023. Users can use this
# table to translate the categories into a more meaningful output.
# Examples:
# s0:c0=CompanyConfidential
```

```
# s0:c1=PatientRecord
# s0:c2=Unclassified
# s0:c3=TopSecret
# s0:c1,c3=CompanyConfidentialRedHat
s0=SystemLow
s0-s0:c0.c1023=SystemLow-SystemHigh
s0:c0.c1023=SystemHigh
```

Dans le contexte d'un SC pour un **sujet**, le champ **identité** indique les privilèges de l'utilisateur SELinux utilisés par le **sujet**.

Dans le contexte d'un SC pour un **objet**, le champ **identité** indique à quel utilisateur SELinux appartient l'**objet**.

SELinux maintient sa propre liste d'utilisateurs, différente de la liste DAC de Linux. Il existe cependant une correspondance entre les deux listes de façon à ce que les utilisateurs MAC puissent être soumis aux restrictions de SELinux :

```
[root@centos8 ~]# /usr/sbin/semanage login -l
```

Login Name	SELinux User	MLS/MCS Range	Service
__default__	unconfined_u	s0-s0:c0.c1023	*
root	unconfined_u	s0-s0:c0.c1023	*

Domains et Types

Le **Domain** est l'endroit d'exécution d'un processus. Chaque processus a un **Domain**. Le **Domain** détermine les accès du processus.

Le **Domain** contient des **objets** et des **sujets** qui interagissent ensemble. Ce modèle, où chaque **sujet** se voit attribué à un **Domain** et où uniquement certaines opérations sont permises, est appelé **Type Enforcement**.

Dans SELinux on utilise le mot :

- **Domain** pour un processus,
- **Type** pour un fichier.

Roles

Un **Rôle** est comme un utilisateur dans le système de sécurité DAC de Linux. Chaque utilisateur autorisé peut assumer l'identité du **Rôle** afin d'exécuter les commandes liées au **Rôle**.

Politiques de Sécurité

Une politique de sécurité définit les SC de chaque application. Elle définit des droits d'accès des domaines aux types. Il y a deux types de politique possible :

Politique	Description
targeted	Les politiques de sécurité ne s'appliquent qu'à certaines applications
mls	Multi Level Security protection

Les politiques de sécurité se trouvent dans le répertoire **/etc/selinux** :

```
[root@centos8 ~]# ls -lR /etc/selinux/ | more
/etc/selinux/:
total 8
-rw-r--r--. 1 root root  548 Jun 16  2021 config
-rw-r--r--. 1 root root 2647 Feb  3  2021 semanage.conf
drwxr-xr-x. 5 root root  133 Mar  6  2022 targeted

/etc/selinux/targeted:
total 16
-rw-r--r--. 1 root root 2367 Dec 21  2021 booleans.subs_dist
drwxr-xr-x. 4 root root 4096 Mar  6  2022 contexts
drwxr-xr-x. 2 root root    6 Dec 21  2021 logins
drwxr-xr-x. 2 root root   23 Mar  6  2022 policy
-rw-r--r--. 1 root root  607 Dec 21  2021 setrans.conf
-rw-r--r--. 1 root root   73 Mar  6  2022 seusers
```

```
/etc/selinux/targeted/contexts:
```

```
total 68
```

```
-rw-r--r--. 1 root root 262 Mar 6 2022 customizable_types
-rw-r--r--. 1 root root 195 Dec 21 2021 dbus_contexts
-rw-r--r--. 1 root root 1111 Dec 21 2021 default_contexts
-rw-r--r--. 1 root root 114 Dec 21 2021 default_type
-rw-r--r--. 1 root root 29 Dec 21 2021 failsafe_context
drwxr-xr-x. 2 root root 213 Mar 6 2022 files
-rw-r--r--. 1 root root 30 Dec 21 2021 initrc_context
-rw-r--r--. 1 root root 372 Dec 21 2021 lxc_contexts
-rw-r--r--. 1 root root 27 Dec 21 2021 openssh_contexts
-rw-r--r--. 1 root root 33 Dec 21 2021 removable_context
-rw-r--r--. 1 root root 74 Dec 21 2021 securetty_types
-rw-r--r--. 1 root root 1170 Dec 21 2021 sepgsql_contexts
-rw-r--r--. 1 root root 53 Dec 21 2021 snapperd_contexts
-rw-r--r--. 1 root root 57 Dec 21 2021 systemd_contexts
-rw-r--r--. 1 root root 33 Dec 21 2021 userhelper_context
drwxr-xr-x. 2 root root 114 Dec 21 2021 users
-rw-r--r--. 1 root root 62 Dec 21 2021 virtual_domain_context
-rw-r--r--. 1 root root 71 Dec 21 2021 virtual_image_context
-rw-r--r--. 1 root root 2920 Dec 21 2021 x_contexts
```

```
/etc/selinux/targeted/contexts/files:
```

```
total 1008
```

```
-rw-r--r--. 1 root root 407436 Mar 6 2022 file_contexts
-rw-r--r--. 1 root root 574118 Mar 6 2022 file_contexts.bin
-rw-r--r--. 1 root root 14704 Mar 6 2022 file_contexts.homedirs
-rw-r--r--. 1 root root 20149 Mar 6 2022 file_contexts.homedirs.bin
-rw-r--r--. 1 root root 0 Dec 21 2021 file_contexts.local
-rw-r--r--. 1 root root 0 Dec 21 2021 file_contexts.subs
-rw-r--r--. 1 root root 597 Dec 21 2021 file_contexts.subs_dist
-rw-r--r--. 1 root root 139 Dec 21 2021 media
```

```
/etc/selinux/targeted/contexts/users:
```

```
total 28
-rw-r--r--. 1 root root 342 Dec 21 2021 guest_u
-rw-r--r--. 1 root root 724 Dec 21 2021 root
-rw-r--r--. 1 root root 562 Dec 21 2021 staff_u
-rw-r--r--. 1 root root 589 Dec 21 2021 sysadm_u
-rw-r--r--. 1 root root 612 Dec 21 2021 unconfined_u
--More--
[q]
```

Afin d'utiliser SELinux en ligne de commande sous RHEL/CentOS 8, il est nécessaire d'installer le paquet **setools-console** :

```
[root@centos8 ~]# dnf install setools-console
Last metadata expiration check: 0:28:26 ago on Tue 01 Oct 2024 16:11:14 CEST.
Dependencies resolved.
```

```
=====
Package                               Architecture      Version
Repository                            Size
=====
Installing:
setools-console                       x86_64
4.3.0-2.el8                           baseos             42 k
=====
```

Transaction Summary

```
=====
Install 1 Package
```

Total download size: 42 k

Installed size: 122 k

Is this ok [y/N]: y

Downloading Packages:

setools-console-4.3.0-2.el8.x86_64.rpm

```
76 kB/s | 42 kB    00:00
```

```
-----  
Total
```

```
76 kB/s | 42 kB    00:00
```

```
Running transaction check
```

```
Transaction check succeeded.
```

```
Running transaction test
```

```
Transaction test succeeded.
```

```
Running transaction
```

```
  Preparing          :
```

```
1/1
```

```
  Installing          : setools-console-4.3.0-2.el8.x86_64
```

```
1/1
```

```
  Running scriptlet: setools-console-4.3.0-2.el8.x86_64
```

```
1/1
```

```
  Verifying           : setools-console-4.3.0-2.el8.x86_64
```

```
1/1
```

```
Installed products updated.
```

```
Installed:
```

```
  setools-console-4.3.0-2.el8.x86_64
```

```
Complete!
```

Pour consulter les statistiques de la politique, il convient d'utiliser la commande **seinfo** :

```
[root@centos8 ~]# seinfo
```

```
Statistics for policy file: /sys/fs/selinux/policy
```

```
Policy Version:          31 (MLS enabled)
```

```
Target Policy:           selinux
```

```
Handle unknown classes:  allow
```

```
Classes:                 132    Permissions:          464
```

```
Sensitivities:           1      Categories:          1024
```

Types:	4974	Attributes:	255
Users:	8	Roles:	14
Booleans:	342	Cond. Expr.:	391
Allow:	113176	Neverallow:	0
Auditallow:	166	Dontaudit:	10378
Type_trans:	253825	Type_change:	87
Type_member:	35	Range_trans:	6015
Role allow:	38	Role_trans:	423
Constraints:	72	Validatetrans:	0
MLS Constrains:	72	MLS Val. Tran:	0
Permissives:	0	Polcap:	5
Defaults:	7	Typebounds:	0
Allowxperm:	0	Neverallowxperm:	0
Auditallowxperm:	0	Dontauditxperm:	0
Ibendportcon:	0	Ibpkeycon:	0
Initial SIDs:	27	Fs_use:	34
Genfscon:	107	Portcon:	642
Netifcon:	0	Nodecon:	0



Important : Notez ici le grand nombre de la catégorie **Dontaudit**.

Langage de Politiques

Un politique est composé de centaines de directives. Les principales directives sont :

allow

allow autorise l'accès d'un processus d'un domaine à des fichiers appartenant à un type donné. Le format de la directive est :

```
allow user_t domaine_t : file (read execute getattr) ;
```

Dans cette directive :

- user_t est le type de fichier,
- domaine_t est le domaine des processus qui sont autorisés par allow,
- file (droit1 droit2 etc) est la liste des permissions accordées.

Les permissions possibles sont :

- read
- write
- append
- execute
- getattr
- setattr
- lock
- link
- unlink
- rename
- ioctl

type

La directive **type** définit un type SELinux. Le type se termine généralement par **_t**.

auditallow, dontaudit

La directive **auditallow** demande l'écriture d'un message de type **avc** dans les journaux. Elle n'est associée à aucune restriction.

L'inverse peut être obtenue avec **dontaudit**, à savoir, cette directive demande à ce qu'il n'y ait pas de journalisation après une interdiction.

type_transition

Normalement quand un fichier est créé, il hérite du SC du répertoire parent. De même quand un processus SELinux active un nouveau processus, ce dernier s'exécute dans le même domaine que son parent. La directive type_transition permet de modifier ce comportement.

Décisions de SELinux

Il existe deux types de décisions auxquelles SELinux doit faire face :

- **Décisions d'Accès**
- **Décisions de Transition**

Décisions d'Accès

Dans ce type de décision SELinux doit décider d'accorder ou non la permission à :

- un **sujet** de faire quelque chose à un **objet** existant,
- un **sujet** de créer de nouvelles choses dans le **Domain**.

Décisions de Transition

Dans ce type de décision SELinux doit décider d'accorder ou non la permission :

- d'invoquer un processus dans un **Domain** différent du **Domain** courant du **sujet**,
- de créer des **objets** dans différents **Types** que le répertoire parent de l'**objet**.

Commandes SELinux

Commande	Description
chcon	Changer le SC d'un fichier

Commande	Description
audit2allow	Générer la source de la règle de sécurité à l'origine d'une erreur
restorecon	Restaurer le SC par défaut à un ou plusieurs fichiers
setfiles -n	Vérifier si les SC sont corrects
semodule	Gérer les modules de politiques
semodule -i	Installer un module de politiques
checkmodule	Compiler un module
semodule_package	Créer un module installable par semodule
semanage	Administrer une politique
audit2allow -M	Créer un module à partir d'un message d'audit
sesearch	Recherche des règles SELinux
seinfo	Effectuer des recherches dans la politique
getsebool	Affiche l'état d'un booléen
getsebool -a	Affiche l'état de l'ensemble des booléens
sestatus -b	Affiche l'état de l'ensemble des booléens
setsebool	Modifie l'état d'un booléen
togglesebool	Bascule la valeur d'un booléen

Les Etats de SELinux

SELinux connaît trois états :

Etat	Description
disabled	SELinux est inactif.
permissive	SELinux est actif mais tout est permis. Des interdictions ne font que de générer des messages d'erreurs dans les logs.
enforcing	SELinux est actif.

L'examen du contenu du fichier **/selinux/enforce** révèle une de deux valeurs qui correspondent à l'**état** de SELinux :

Valeur	Description
0	SELinux est en mode <i>permissive</i>

Valeur	Description
1	SELinux est en mode <i>enforcing</i>

La configuration de l'activation de SELinux ainsi que son état est effectuée grâce au fichier **/etc/selinux/config** :

```
[root@centos8 ~]# cat /etc/selinux/config

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Afin de connaître l'état de SELinux, il convient d'utiliser la commande **getenforce** :

```
[root@centos8 ~]# getenforce
Enforcing
```

Pour modifier l'état de SELinux, il convient d'utiliser la commande **setenforce** :

```
[root@centos8 ~]# setenforce permissive

[root@centos8 ~]# getenforce
Permissive
```

La commande **sestatus** vous informe sur la configuration de SELinux et notamment sur la version de la politique utilisée :

```
[root@centos8 ~]# sestatus
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:      /etc/selinux
Loaded policy name:           targeted
Current mode:                 permissive
Mode from config file:       enforcing
Policy MLS status:           enabled
Policy deny_unknown status:   allowed
Memory protection checking:   actual (secure)
Max kernel policy version:    33
```

Les différentes versions de politiques évolue en même temps que le noyau Linux.

La commande sestatus peut aussi prendre l'option -v :

```
[root@centos8 ~]# sestatus -v
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:      /etc/selinux
Loaded policy name:           targeted
Current mode:                 permissive
Mode from config file:       enforcing
Policy MLS status:           enabled
Policy deny_unknown status:   allowed
Memory protection checking:   actual (secure)
Max kernel policy version:    33

Process contexts:
Current context:              unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
Init context:                 system_u:system_r:init_t:s0
/usr/sbin/sshd                system_u:system_r:sshd_t:s0-s0:c0.c1023

File contexts:
```

```
Controlling terminal:      unconfined_u:object_r:user_devpts_t:s0
/etc/passwd               system_u:object_r:passwd_file_t:s0
/etc/shadow               system_u:object_r:shadow_t:s0
/bin/bash                 system_u:object_r:shell_exec_t:s0
/bin/login                 system_u:object_r:login_exec_t:s0
/bin/sh                   system_u:object_r:bin_t:s0 -> system_u:object_r:shell_exec_t:s0
/sbin/agetty              system_u:object_r:getty_exec_t:s0
/sbin/init                 system_u:object_r:bin_t:s0 -> system_u:object_r:init_exec_t:s0
/usr/sbin/sshd             system_u:object_r:sshd_exec_t:s0
```

Booléens

Les booléens permettent à des ensembles de règles d'être utilisées d'une manière alternative.

Pour visualiser l'état l'ensemble des booléens, il convient d'utiliser la commande **getsebool -a** :

```
[root@centos8 ~]# getsebool -a | more
abrt_anon_write --> off
abrt_handle_event --> off
abrt_upload_watch_anon_write --> on
antivirus_can_scan_system --> off
antivirus_use_jit --> off
auditadm_exec_content --> on
authlogin_nsswitch_use_ldap --> off
authlogin_radius --> off
authlogin_yubikey --> off
awstats_purge_apache_log_files --> off
boinc_execmem --> on
cdrecord_read_content --> off
cluster_can_network_connect --> off
cluster_manage_all_files --> off
cluster_use_execmem --> off
cobbler_anon_write --> off
```

```
cobbler_can_network_connect --> off
cobbler_use_cifs --> off
cobbler_use_nfs --> off
collectd_tcp_network_connect --> off
colord_use_nfs --> off
condor_tcp_network_connect --> off
conman_can_network --> off
conman_use_nfs --> off
container_connect_any --> off
container_manage_cgroup --> off
container_use_cephfs --> off
cron_can_relabel --> off
cron_system_cronjob_use_shares --> off
cron_userdomain_transition --> on
cups_execmem --> off
cvs_read_shadow --> off
daemons_dump_core --> off
daemons_enable_cluster_mode --> off
daemons_use_tcp_wrapper --> off
daemons_use_tty --> off
dbadm_exec_content --> on
dbadm_manage_user_files --> off
dbadm_read_user_files --> off
deny_bluetooth --> off
deny_execmem --> off
deny_ptrace --> off
dhcpc_exec_iptables --> off
dhcpcd_use_ldap --> off
domain_can_mmap_files --> off
domain_can_write_kmsg --> off
domain_fd_use --> on
domain_kernel_load_modules --> off
entropyd_use_audio --> on
exim_can_connect_db --> off
```

```
exim_manage_user_files --> off
exim_read_user_files --> off
fcron_cron --> off
fenced_can_network_connect --> off
fenced_can_ssh --> off
--More--
[q]
```

ou la commande **sestatus -b** :

```
[root@centos8 ~]# sestatus -b | more
SELinux status:                enabled
SELinuxfs mount:               /sys/fs/selinux
SELinux root directory:        /etc/selinux
Loaded policy name:             targeted
Current mode:                   permissive
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33

Policy booleans:
abrt_anon_write                  off
abrt_handle_event                off
abrt_upload_watch_anon_write     on
antivirus_can_scan_system        off
antivirus_use_jit                off
auditadm_exec_content            on
authlogin_nsswitch_use_ldap      off
authlogin_radius                 off
authlogin_yubikey                off
awstats_purge_apache_log_files  off
boinc_execmem                    on
```

cdrecord_read_content	off
cluster_can_network_connect	off
cluster_manage_all_files	off
cluster_use_execmem	off
cobbler_anon_write	off
cobbler_can_network_connect	off
cobbler_use_cifs	off
cobbler_use_nfs	off
collectd_tcp_network_connect	off
colord_use_nfs	off
condor_tcp_network_connect	off
conman_can_network	off
conman_use_nfs	off
container_connect_any	off
container_manage_cgroup	off
container_use_cephfs	off
cron_can_relabel	off
cron_system_cronjob_use_shares	off
cron_userdomain_transition	on
cups_execmem	off
cvs_read_shadow	off
daemons_dump_core	off
daemons_enable_cluster_mode	off
daemons_use_tcp_wrapper	off
daemons_use_tty	off
dbadm_exec_content	on
dbadm_manage_user_files	off
dbadm_read_user_files	off
deny_bluetooth	off
deny_execmem	off
deny_ptrace	off
dhcpc_exec_iptables	off
--More--	
[q]	

Pour fixer l'état d'un booléen, il convient d'utiliser la commande `setsebool` :

```
[root@centos8 ~]# setsebool antivirus_can_scan_system 1

[root@centos8 ~]# getsebool antivirus_can_scan_system
antivirus_can_scan_system --> on

[root@centos8 ~]# setsebool antivirus_can_scan_system 0

[root@centos8 ~]# getsebool antivirus_can_scan_system
antivirus_can_scan_system --> off
```

LAB #2 - Travailler avec SELinux

Afin reconstruire la politique actuelle **sans** les règles **dontaudit**, utilisez la commande **semodule** :

```
[root@centos8 ~]# semodule -DB
```

Vérifiez qu'il ne reste aucune règle de type **dontaudit** :

```
[root@centos8 ~]# seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:           31 (MLS enabled)
Target Policy:            selinux
Handle unknown classes:   allow
Classes:                  132      Permissions:             464
Sensitivities:            1        Categories:             1024
Types:                   4964     Attributes:              255
Users:                   8         Roles:                   14
Booleans:                338     Cond. Expr.:            386
Allow:                   112733   Neverallow:              0
Auditallow:              166     Dontaudit:               0
```

Type_trans:	252829	Type_change:	87
Type_member:	35	Range_trans:	5781
Role_allow:	38	Role_trans:	421
Constraints:	72	Validatetrans:	0
MLS Constrain:	72	MLS Val. Tran:	0
Permissives:	0	Polcap:	5
Defaults:	7	Typebounds:	0
Allowxperm:	0	Neverallowxperm:	0
Auditallowxperm:	0	Dontauditxperm:	0
Ibendportcon:	0	Ibpkeycon:	0
Initial SIDs:	27	Fs_use:	34
Genfscon:	107	Portcon:	642
Netifcon:	0	Nodecon:	0

Copier et Déplacer des Fichiers

Créez deux fichiers **file1** et **file2** en tant que l'utilisateur **trainee** puis visualisez les SC des fichiers :

```
[root@centos8 ~]# exit
logout
[trainee@centos8 ~]$ touch file1 file2
[trainee@centos8 ~]$ ls -Z file*
unconfined_u:object_r:user_home_t:s0 file1  unconfined_u:object_r:user_home_t:s0 file2
```

Notez que le type des deux fichiers est **user_home_t**.

Copiez maintenant le fichier **file1** vers **/tmp** en utilisant la commande **cp** et visualiser son SC :

```
[trainee@centos8 ~]$ cp file1 /tmp

[trainee@centos8 ~]$ ls -Z /tmp/file1
unconfined_u:object_r:user_tmp_t:s0 /tmp/file1
```

Notez que le fichier ainsi copié a hérité du **type** du répertoire parent, à savoir **tmp_t**.

Déplacez maintenant le fichier **file2** dans le répertoire **/tmp** et contrôlez son SC :

```
[trainee@centos8 ~]$ mv file2 /tmp

[trainee@centos8 ~]$ ls -Z /tmp/file2
unconfined_u:object_r:user_home_t:s0 /tmp/file2
```

Notez que la commande **mv** maintient le **type** d'origine.

Vérifier les SC des Processus

Il convient d'utiliser l'option **Z** avec la commande **ps** :

```
[trainee@centos8 ~]$ ps auxZ | more
```

LABEL	USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
system_u:system_r:init_t:s0	root	1	0.0	0.0	241416	14192	?	Ss	12:13	0:04	
/usr/lib/systemd/systemd --switched-root --system --deserialize 18											
system_u:system_r:kernel_t:s0	root	2	0.0	0.0	0	0	?	S	12:13	0:00	[kthreadd]
system_u:system_r:kernel_t:s0	root	3	0.0	0.0	0	0	?	I<	12:13	0:00	[rcu_gp]
system_u:system_r:kernel_t:s0	root	4	0.0	0.0	0	0	?	I<	12:13	0:00	[rcu_par_gp]
system_u:system_r:kernel_t:s0	root	6	0.0	0.0	0	0	?	I<	12:13	0:00	[kworker/0:0H-events_highpri]
system_u:system_r:kernel_t:s0	root	9	0.0	0.0	0	0	?	I<	12:13	0:00	[mm_percpu_wq]
system_u:system_r:kernel_t:s0	root	10	0.0	0.0	0	0	?	S	12:13	0:00	[ksoftirqd/0]
system_u:system_r:kernel_t:s0	root	11	0.0	0.0	0	0	?	I	12:13	0:00	[rcu_sched]
system_u:system_r:kernel_t:s0	root	12	0.0	0.0	0	0	?	S	12:13	0:00	[migration/0]
system_u:system_r:kernel_t:s0	root	13	0.0	0.0	0	0	?	S	12:13	0:00	[watchdog/0]
system_u:system_r:kernel_t:s0	root	14	0.0	0.0	0	0	?	S	12:13	0:00	[cpuhp/0]
system_u:system_r:kernel_t:s0	root	15	0.0	0.0	0	0	?	S	12:13	0:00	[cpuhp/1]
system_u:system_r:kernel_t:s0	root	16	0.0	0.0	0	0	?	S	12:13	0:00	[watchdog/1]
system_u:system_r:kernel_t:s0	root	17	0.0	0.0	0	0	?	S	12:13	0:00	[migration/1]

system_u:system_r:kernel_t:s0	root	18	0.0	0.0	0	0 ?	S	12:13	0:00	[ksoftirqd/1]
system_u:system_r:kernel_t:s0	root	20	0.0	0.0	0	0 ?	I<	12:13	0:00	[kworker/1:0H-events_highpri]
system_u:system_r:kernel_t:s0	root	21	0.0	0.0	0	0 ?	S	12:13	0:00	[cpuhp/2]
system_u:system_r:kernel_t:s0	root	22	0.0	0.0	0	0 ?	S	12:13	0:00	[watchdog/2]
system_u:system_r:kernel_t:s0	root	23	0.0	0.0	0	0 ?	S	12:13	0:00	[migration/2]
system_u:system_r:kernel_t:s0	root	24	0.0	0.0	0	0 ?	S	12:13	0:00	[ksoftirqd/2]
system_u:system_r:kernel_t:s0	root	26	0.0	0.0	0	0 ?	I<	12:13	0:00	[kworker/2:0H-events_highpri]
system_u:system_r:kernel_t:s0	root	27	0.0	0.0	0	0 ?	S	12:13	0:00	[cpuhp/3]
system_u:system_r:kernel_t:s0	root	28	0.0	0.0	0	0 ?	S	12:13	0:00	[watchdog/3]
system_u:system_r:kernel_t:s0	root	29	0.0	0.0	0	0 ?	S	12:13	0:00	[migration/3]
system_u:system_r:kernel_t:s0	root	30	0.0	0.0	0	0 ?	S	12:13	0:00	[ksoftirqd/3]
system_u:system_r:kernel_t:s0	root	32	0.0	0.0	0	0 ?	I<	12:13	0:00	[kworker/3:0H-events_highpri]
system_u:system_r:kernel_t:s0	root	33	0.0	0.0	0	0 ?	S	12:13	0:00	[cpuhp/4]
system_u:system_r:kernel_t:s0	root	34	0.0	0.0	0	0 ?	S	12:13	0:00	[watchdog/4]
system_u:system_r:kernel_t:s0	root	35	0.0	0.0	0	0 ?	S	12:13	0:00	[migration/4]
system_u:system_r:kernel_t:s0	root	36	0.0	0.0	0	0 ?	S	12:13	0:00	[ksoftirqd/4]
system_u:system_r:kernel_t:s0	root	38	0.0	0.0	0	0 ?	I<	12:13	0:00	[kworker/4:0H-events_highpri]
system_u:system_r:kernel_t:s0	root	39	0.0	0.0	0	0 ?	S	12:13	0:00	[cpuhp/5]
system_u:system_r:kernel_t:s0	root	40	0.0	0.0	0	0 ?	S	12:13	0:00	[watchdog/5]
system_u:system_r:kernel_t:s0	root	41	0.0	0.0	0	0 ?	S	12:13	0:00	[migration/5]
system_u:system_r:kernel_t:s0	root	42	0.0	0.0	0	0 ?	S	12:13	0:00	[ksoftirqd/5]
system_u:system_r:kernel_t:s0	root	44	0.0	0.0	0	0 ?	I<	12:13	0:00	[kworker/5:0H-events_highpri]
system_u:system_r:kernel_t:s0	root	45	0.0	0.0	0	0 ?	S	12:13	0:00	[cpuhp/6]
system_u:system_r:kernel_t:s0	root	46	0.0	0.0	0	0 ?	S	12:13	0:00	[watchdog/6]
system_u:system_r:kernel_t:s0	root	47	0.0	0.0	0	0 ?	S	12:13	0:00	[migration/6]
system_u:system_r:kernel_t:s0	root	48	0.0	0.0	0	0 ?	S	12:13	0:00	[ksoftirqd/6]
system_u:system_r:kernel_t:s0	root	50	0.0	0.0	0	0 ?	I<	12:13	0:00	[kworker/6:0H-events_highpri]
system_u:system_r:kernel_t:s0	root	51	0.0	0.0	0	0 ?	S	12:13	0:00	[cpuhp/7]

```

system_u:system_r:kernel_t:s0 root 52 0.0 0.0 0 0 ? S 12:13 0:00 [watchdog/7]
system_u:system_r:kernel_t:s0 root 53 0.0 0.0 0 0 ? S 12:13 0:00 [migration/7]
system_u:system_r:kernel_t:s0 root 54 0.0 0.0 0 0 ? S 12:13 0:00 [ksoftirqd/7]
system_u:system_r:kernel_t:s0 root 56 0.0 0.0 0 0 ? I< 12:13 0:00 [kworker/7:0H-
events_highpri]
system_u:system_r:kernel_t:s0 root 65 0.0 0.0 0 0 ? S 12:13 0:00 [kdevtmpfs]
system_u:system_r:kernel_t:s0 root 66 0.0 0.0 0 0 ? I< 12:13 0:00 [netns]
system_u:system_r:kernel_t:s0 root 67 0.0 0.0 0 0 ? S 12:13 0:00
[rcu_tasks_trace]
system_u:system_r:kernel_t:s0 root 68 0.0 0.0 0 0 ? S 12:13 0:00
[rcu_tasks_rude_]
system_u:system_r:kernel_t:s0 root 69 0.0 0.0 0 0 ? S 12:13 0:00 [kauditd]
system_u:system_r:kernel_t:s0 root 70 0.0 0.0 0 0 ? S 12:13 0:00 [khungtaskd]
system_u:system_r:kernel_t:s0 root 71 0.0 0.0 0 0 ? S 12:13 0:00 [oom_reaper]
system_u:system_r:kernel_t:s0 root 72 0.0 0.0 0 0 ? I< 12:13 0:00 [writeback]
--More--
[q]

```

Visualiser la SC d'un Utilisateur

Utilisez l'option **-Z** avec la commande **id** :

```

[trainee@centos8 ~]$ id -Z
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023

```

Notez que vous ne pouvez pas consulter le SC d'un autre utilisateur :

```

[trainee@centos8 ~]$ id root
uid=0(root) gid=0(root) groups=0(root)

[trainee@centos8 ~]$ id -Z root
id: cannot print security context when user specified

```

Vérifier la SC d'un fichier

Il convient d'utiliser la commande ls avec l'option **-Z** :

```
[trainee@centos8 ~]$ cd /etc

[trainee@centos8 etc]$ ls -Z l* -d
unconfined_u:object_r:ld_so_cache_t:s0 ld.so.cache          system_u:object_r:etc_t:s0 libpaper.d
system_u:object_r:etc_t:s0 login.defs                     system_u:object_r:etc_t:s0 libreport
      system_u:object_r:etc_t:s0 ld.so.conf                 system_u:object_r:etc_t:s0 libssh
system_u:object_r:etc_t:s0 logrotate.conf                  system_u:object_r:etc_t:s0 libuser.conf
      system_u:object_r:etc_t:s0 ld.so.conf.d               system_u:object_r:etc_t:s0 libvirt
system_u:object_r:etc_t:s0 logrotate.d                    system_u:object_r:etc_t:s0 libxslt
      system_u:object_r:etc_t:s0 libaudit.conf              system_u:object_r:etc_t:s0 libxml2
system_u:object_r:etc_t:s0 lsm                             system_u:object_r:virt_etc_t:s0 libvirt
      system_u:object_r:etc_t:s0 libblockdev                system_u:object_r:locale_t:s0 locale.conf
system_u:object_r:lvm_etc_t:s0 lvm                         system_u:object_r:locale_t:s0 localtime
      system_u:object_r:etc_t:s0 libibverbs.d
      system_u:object_r:etc_t:s0 libnl
```

Troubleshooting SELinux

L'interprétation des messages journalisés de SELinux est souvent la clef d'un dépannage efficace et rapide.

Si le démon **auditd** est démarré, les messages de SELinux sont consignés dans le fichier **/var/log/audit/audit.log**. Dans le cas contraire, les mêmes messages sont consignés dans le fichier **/var/log/messages**. Dans les deux cas, chaque message de SELinux contient le mot clef **AVC** :

La commande chcon

La commande **chcon** permet de modifier *temporairement* une SC.

```
[trainee@centos8 etc]$ cd ~
```

```
[trainee@centos8 ~]$ chcon --help
```

Usage: chcon [OPTION]... CONTEXT FILE...

or: chcon [OPTION]... [-u USER] [-r ROLE] [-l RANGE] [-t TYPE] FILE...

or: chcon [OPTION]... --reference=RFILE FILE...

Change the SELinux security context of each FILE to CONTEXT.

With --reference, change the security context of each FILE to that of RFILE.

Mandatory arguments to long options are mandatory for short options too.

--dereference	affect the referent of each symbolic link (this is the default), rather than the symbolic link itself
-h, --no-dereference	affect symbolic links instead of any referenced file
-u, --user=USER	set user USER in the target security context
-r, --role=ROLE	set role ROLE in the target security context
-t, --type=TYPE	set type TYPE in the target security context
-l, --range=RANGE	set range RANGE in the target security context
--no-preserve-root	do not treat '/' specially (the default)
--preserve-root	fail to operate recursively on '/'
--reference=RFILE	use RFILE's security context rather than specifying a CONTEXT value
-R, --recursive	operate on files and directories recursively
-v, --verbose	output a diagnostic for every file processed

The following options modify how a hierarchy is traversed when the -R option is also specified. If more than one is specified, only the final one takes effect.

-H	if a command line argument is a symbolic link to a directory, traverse it
-L	traverse every symbolic link to a directory encountered
-P	do not traverse any symbolic links (default)

```
--help      display this help and exit
--version   output version information and exit
```

```
GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Report chcon translation bugs to <https://translationproject.org/team/>
Full documentation at: <https://www.gnu.org/software/coreutils/chcon>
or available locally via: info '(coreutils) chcon invocation'
```

HERE

Prenons le cas de la création d'un répertoire à la racine du système de fichiers afin d'y stocker les pages web du serveur apache :

```
[trainee@centos8 ~]$ su -
Password:fenestros

[root@centos8 ~]# mkdir /www
[root@centos8 ~]# touch /www/index.html
```

Installez maintenant le serveur Apache :

```
[root@centos8 ~]# dnf install httpd -y
```

Modifiez ensuite la directive **DocumentRoot** dans le fichier **/etc/httpd/conf/httpd.conf** :

```
[...]
#DocumentRoot "/var/www/html"
DocumentRoot "/www"
[...]
```

Ajoutez les section **<Directory "/www">**:

```
...
<Directory "/var/www">
    AllowOverride None
```

```
# Allow open access:
Require all granted
</Directory>

<Directory "/www">
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>

# Further relax access to the default document root:
<Directory "/var/www/html">
...
```

Créez le fichier **/www/index.html** :

```
[root@centos8 ~]# cat /www/index.html
<html>
<title>
This is a test
</title>
<body>
www test page
</body>
</html>
```

Modifiez ensuite le propriétaire et le groupe du répertoire **/www** et son contenu :

```
[root@centos8 ~]# chown -R apache:apache /www
```

Dernièrement, créez un fichier index.html **vide** dans le répertoire **/var/www/html/** :

```
[root@centos8 ~]# touch /var/www/html/index.html
```

Redémarrez maintenant le service httpd :

```
[root@centos8 ~]# systemctl restart httpd.service
[root@centos8 ~]# systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Wed 2024-10-02 12:24:15 CEST; 15s ago
     Docs: man:httpd.service(8)
  Main PID: 53680 (httpd)
    Status: "Running, listening on: port 80"
     Tasks: 213 (limit: 100949)
    Memory: 39.3M
    CGroup: /system.slice/httpd.service
            └─53680 /usr/sbin/httpd -DFOREGROUND
              └─53683 /usr/sbin/httpd -DFOREGROUND
                └─53684 /usr/sbin/httpd -DFOREGROUND
                  └─53685 /usr/sbin/httpd -DFOREGROUND
                    └─53686 /usr/sbin/httpd -DFOREGROUND

Oct 02 12:24:14 centos8.ittraining.loc systemd[1]: Starting The Apache HTTP Server...
Oct 02 12:24:15 centos8.ittraining.loc systemd[1]: Started The Apache HTTP Server.
Oct 02 12:24:15 centos8.ittraining.loc httpd[53680]: Server configured, listening on: port 80
```

Passez SELinux en mode enforcing :

```
[root@centos8 ~]# setenforce enforcing

[root@centos8 ~]# getenforce
Enforcing
```

Consultez le site localhost en utilisant **lynx** :

```
[root@centos8 ~]# lynx localhost
bash: lynx: command not found...
```

Install package 'lynx' to provide command 'lynx'? [N/y] y

* Waiting in queue...

* Loading list of packages....

The following packages have to be installed:

lynx-2.8.9-2.el8.x86_64 A text-based Web browser

Proceed with changes? [N/y] y

* Waiting in queue...

* Waiting for authentication...

* Waiting in queue...

* Downloading packages...

* Requesting data...

* Testing changes...

* Installing packages...

HTTP Server Test Page

This page is used to test the proper operation of the HTTP server after it has been installed. If you can read this page it means that this site is working properly. This server is powered by [1]CentOS.

If you are a member of the general public:

The website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting `www.example.com`, you should send e-mail to `"webmaster@example.com"`.

If you are the website administrator:

You may now add content to the webroot directory. Note that until you do so, people visiting your website will see this page, and not your content.

For systems using the Apache HTTP Server: You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

For systems using NGINX: You should now put your content in a location of your choice and edit the root configuration directive in the nginx configuration file `/etc/nginx/nginx.conf`.

[2][Powered by CentOS] [Powered by CentOS]

Important note!

The CentOS Project has nothing to do with this website or its content, it just provides the software that makes the website run.

If you have issues with the content of this site, contact the owner of the domain, not the CentOS project. Unless you intended to visit `CentOS.org`, the CentOS Project does not have anything to do with this website, the content or the lack of it.

For example, if this website is `www.example.com`, you would find the owner of the `example.com` domain at the following WHOIS server:

[3]<http://www.internic.net/whois.html>

© 2021 The CentOS Project | [4]Legal | [5]Privacy

References

1. <http://centos.org/>
2. <https://www.centos.org/>
3. <http://www.internic.net/whois.html>
4. <https://www.centos.org/legal/>
5. <https://www.centos.org/legal/privacy/>

Consultez les messages d'alerte de SELinux dans le fichier **/var/log/messages** :

```
[root@centos8 ~]# grep "SELinux is preventing" /var/log/messages
...
Oct  2 12:44:28 centos8 setroubleshoot[57035]: SELinux is preventing /usr/sbin/httpd from using the net_admin
capability. For complete SELinux messages run: sealert -l a169ef1e-7a43-47d5-ac8f-36d5459c82b6
Oct  2 12:44:28 centos8 setroubleshoot[57035]: SELinux is preventing /usr/sbin/httpd from using the net_admin
capability.#012#012***** Plugin catchall (100. confidence) suggests *****#012#012If you
believe that httpd should have the net_admin capability by default.#012Then you should report this as a
bug.#012You can generate a local policy module to allow this access.#012Do#012allow this access for now by
executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
Oct  2 12:44:38 centos8 setroubleshoot[57035]: SELinux is preventing /usr/sbin/httpd from using the net_admin
capability. For complete SELinux messages run: sealert -l a169ef1e-7a43-47d5-ac8f-36d5459c82b6
Oct  2 12:44:38 centos8 setroubleshoot[57035]: SELinux is preventing /usr/sbin/httpd from using the net_admin
capability.#012#012***** Plugin catchall (100. confidence) suggests *****#012#012If you
believe that httpd should have the net_admin capability by default.#012Then you should report this as a
bug.#012You can generate a local policy module to allow this access.#012Do#012allow this access for now by
executing:#012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule -X 300 -i my-httpd.pp#012
```

La commande **sealert** possède à la fois une interface graphique **et** un mode en ligne de commande.

```
[root@centos8 ~]# sealert -l a169ef1e-7a43-47d5-ac8f-36d5459c82b6
```

SELinux is preventing /usr/sbin/httpd from using the net_admin capability.

***** Plugin catchall (100. confidence) suggests *****

If you believe that httpd should have the net_admin capability 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:
ausearch -c 'httpd' --raw | audit2allow -M my-httpd
semodule -X 300 -i my-httpd.pp

Additional Information:

Source Context	system_u:system_r:httpd_t:s0
Target Context	system_u:system_r:httpd_t:s0
Target Objects	Unknown [capability]
Source	httpd
Source Path	/usr/sbin/httpd
Port	<Unknown>
Host	centos8.ittraining.loc
Source RPM Packages	
Target RPM Packages	
SELinux Policy RPM	selinux-policy-targeted-3.14.3-80.el8_5.2.noarch
Local Policy RPM	selinux-policy-targeted-3.14.3-80.el8_5.2.noarch
Selinux Enabled	True
Policy Type	targeted
Enforcing Mode	Enforcing
Host Name	centos8.ittraining.loc
Platform	Linux centos8.ittraining.loc 4.18.0-348.7.1.el8_5.x86_64 #1 SMP Wed Dec 22 13:25:12 UTC 2021 x86_64 x86_64
Alert Count	110
First Seen	2024-10-02 12:24:14 CEST

```
Last Seen          2024-10-02 12:48:45 CEST
Local ID           a169ef1e-7a43-47d5-ac8f-36d5459c82b6
```

Raw Audit Messages

```
type=AVC msg=audit(1727866125.775:861): avc: denied { net_admin } for pid=53680 comm="httpd" capability=12
scontext=system_u:system_r:httpd_t:s0 tcontext=system_u:system_r:httpd_t:s0 tclass=capability permissive=0
```

```
Hash: httpd,httpd_t,httpd_t,capability,net_admin
```

Ce message a été généré parce que le repertoire /www ainsi que le fichier index.html ne possèdent pas le **type** nécessaire pour que le service apache puisse les utiliser :

```
[root@centos8 ~]# ls -Z /www/index.html
unconfined_u:object_r:default_t:s0 /www/index.html
```

```
[root@centos8 ~]# ls -Z /var/www/html/index.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/index.html
```

L'exemple ci-dessus nous montre clairement que le type pour **/www/index.html** est **default_t** or apache a besoin du type **httpd_sys_content_t** pour pouvoir accéder au fichier.

Pour vérifier la cause de l'erreur, utilisez la commande suivante :

```
[root@centos8 ~]# grep "/www/index.html" /var/log/messages
...
Oct  2 12:44:48 centos8 setroubleshoot[57035]: SELinux is preventing /usr/sbin/httpd from getattr access on the
file /www/index.html. For complete SELinux messages run: sealert -l 874480af-4890-4ae4-a1a2-961f5c528f3e
...
```

Modifiez donc la SC de /www et /www/index.html en utilisant la commande **chcon** :

```
[root@centos8 ~]# chcon -Rv --type=httpd_sys_content_t /www
changing security context of '/www/index.html'
```

```
changing security context of '/www'
```

```
[root@centos8 ~]# ls -Z /www/index.html  
unconfined_u:object_r:httpd_sys_content_t:s0 /www/index.html
```

Afin de maintenir ces SC lors d'une **restauration des SC par défaut**, il convient d'utiliser la commande **semanage** afin d'appliquer la modification d'une manière définitive :

```
[root@centos8 ~]# semanage fcontext -a -t httpd_sys_content_t "/www(/.*)"?"
```

Vérifiez que ces modifications fonctionnent :

```
[root@centos8 ~]# lynx --dump localhost  
www test page
```

La commande restorecon

```
usage:  restorecon [-iFnRv] [-e excludedir ] [-o filename ] [-f filename | pathname... ]
```

Pour illustrer l'utilisation de cette commande, créez les fichiers copy.html et move.html dans le répertoire /tmp :

```
[root@centos8 ~]# cd /tmp ; touch copy.html move.html
```

```
[root@centos8 tmp]# ls -Z | grep html  
unconfined_u:object_r:user_tmp_t:s0 copy.html  
unconfined_u:object_r:user_tmp_t:s0 move.html
```

Copiez le fichier copy.html vers /var/www/html et **déplacez** le fichier move.html vers la même cible :

```
[root@centos8 tmp]# cp copy.html /var/www/html/  
[root@centos8 tmp]# mv move.html /var/www/html/  
[root@centos8 tmp]# ls -Z /var/www/html
```

```
unconfined_u:object_r:httpd_sys_content_t:s0 copy.html  unconfined_u:object_r:httpd_sys_content_t:s0 index.html
unconfined_u:object_r:user_tmp_t:s0 move.html
```



Important : Notez ici que copy.html a pris le type du répertoire de destination tandis que move.html retient le type obtenu lors de sa création.

Restaurez maintenant la SC par défaut de move.html compte tenu de son emplacement en utilisant la commande **restorecon** :

```
[root@centos8 tmp]# restorecon -v /var/www/html/move.html
Relabeled /var/www/html/move.html from unconfined_u:object_r:user_tmp_t:s0 to
unconfined_u:object_r:httpd_sys_content_t:s0

[root@centos8 tmp]# ls -Z /var/www/html
unconfined_u:object_r:httpd_sys_content_t:s0 copy.html  unconfined_u:object_r:httpd_sys_content_t:s0 index.html
unconfined_u:object_r:httpd_sys_content_t:s0 move.html
```

Le fichier /.autorelabel

En cas de besoin il est intéressant de pouvoir restaurer les SC par défaut sur l'ensemble des objets du système. Cette procédure est très simple à mettre en oeuvre. Il convient de créer le fichier **.autorelabel** à la racine et de redémarrer le système :

```
[root@centos8 tmp]# touch /.autorelabel
[root@centos8 tmp]# shutdown -r now
```

```
root@computeXX:~# ssh -l trainee 10.0.2.45
trainee@10.0.2.45's password: trainee
Activate the web console with: systemctl enable --now cockpit.socket
```

```
Last login: Wed Oct  2 11:47:29 2024 from 10.0.2.1
[trainee@centos8 ~]$ su -
```

Password: fenestros

La commande semanage

La commande **semanage** peut prendre plusieurs options :

```
[root@centos8 ~]# semanage --help
usage: semanage [-h]
{import,export,login,user,port,ibpkey,ibendport,interface,module,node,fcontext,boolean,permissive,dontaudit}
...
```

semanage is used to configure certain elements of SELinux policy with-out requiring modification to or recompilation from policy source.

positional arguments:

```
{import,export,login,user,port,ibpkey,ibendport,interface,module,node,fcontext,boolean,permissive,dontaudit}
import          Import local customizations
export          Output local customizations
login           Manage login mappings between linux users and SELinux
                confined users
user            Manage SELinux confined users (Roles and levels for an
                SELinux user)
port            Manage network port type definitions
ibpkey          Manage infiniband ibpkey type definitions
ibendport       Manage infiniband end port type definitions
interface       Manage network interface type definitions
module          Manage SELinux policy modules
node            Manage network node type definitions
fcontext        Manage file context mapping definitions
boolean         Manage booleans to selectively enable functionality
permissive      Manage process type enforcement mode
dontaudit       Disable/Enable dontaudit rules in policy
```

optional arguments:

-h, --help show this help message and exit

Pour illustrer l'utilisation de cette commande, considérez le besoin de mettre le service apache à l'écoute du port **8090** au lieu du port standard.

SELinux gère aussi l'accès aux ports par les différents serveurs. La liste complète des ports autorisés par serveur peut être visualisée à l'aide de la commande **semanage** :

```
[root@centos8 ~]# 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            tcp    7002
afs_pt_port_t            udp    7002
afs_vl_port_t            udp    7003
agentx_port_t            tcp    705
agentx_port_t            udp    705
amanda_port_t            tcp    10080-10083
amanda_port_t            udp    10080-10082
amavisd_recv_port_t      tcp    10024
amavisd_send_port_t      tcp    10025
amqp_port_t              tcp    15672, 5671-5672
amqp_port_t              udp    5671-5672
aol_port_t               tcp    5190-5193
aol_port_t               udp    5190-5193
apc_port_t               tcp    3052
apc_port_t               udp    3052
apcupsd_port_t           tcp    3551
apcupsd_port_t           udp    3551
```

apertus_ldp_port_t	tcp	539
apertus_ldp_port_t	udp	539
appswitch_emp_port_t	tcp	2616
appswitch_emp_port_t	udp	2616
asterisk_port_t	tcp	1720
asterisk_port_t	udp	2427, 2727, 4569
audit_port_t	tcp	60
auth_port_t	tcp	113
babel_port_t	udp	6696
bacula_port_t	tcp	9103
bacula_port_t	udp	9103
bctp_port_t	tcp	8999
bctp_port_t	udp	8999
bfd_control_port_t	tcp	3784
bfd_control_port_t	udp	3784
bgp_port_t	tcp	179, 2605
bgp_port_t	udp	179, 2605
boinc_client_port_t	tcp	1043
boinc_client_port_t	udp	1034
boinc_port_t	tcp	31416
brlp_port_t	tcp	4101
certmaster_port_t	tcp	51235
chronyd_port_t	udp	323
clamd_port_t	tcp	3310
clockspeed_port_t	udp	4041
cluster_port_t	tcp	5149, 40040, 50006-50008
cluster_port_t	udp	5149, 50006-50008
cma_port_t	tcp	1050
cma_port_t	udp	1050
cobbler_port_t	tcp	25151
collectd_port_t	udp	25826
complex_link_port_t	tcp	4331, 5001
complex_link_port_t	udp	5001
complex_main_port_t	tcp	5000

complex_main_port_t	udp	5000
comsat_port_t	udp	512
condor_port_t	tcp	9618
condor_port_t	udp	9618
conman_port_t	tcp	7890
conman_port_t	udp	7890
connlcli_port_t	tcp	1358
connlcli_port_t	udp	1358
conntrackd_port_t	udp	3780
couchdb_port_t	tcp	5984, 6984
couchdb_port_t	udp	5984, 6984
ctdb_port_t	tcp	4379
ctdb_port_t	udp	4379
cvs_port_t	tcp	2401
cvs_port_t	udp	2401
cyphesis_port_t	tcp	6767, 6769, 6780-6799
cyphesis_port_t	udp	32771
cyrus_imapd_port_t	tcp	2005
daap_port_t	tcp	3689
daap_port_t	udp	3689
dbskkd_port_t	tcp	1178
dcc_port_t	udp	6276, 6277
dccm_port_t	tcp	5679
dccm_port_t	udp	5679
dey_keyneg_port_t	tcp	8750
dey_keyneg_port_t	udp	8750
dey_sapi_port_t	tcp	4330
dhcpc_port_t	tcp	68, 546, 5546
dhcpc_port_t	udp	68, 546, 5546
dhcpd_port_t	tcp	547, 548, 647, 847, 7911
dhcpd_port_t	udp	67, 547, 548, 647, 847
dict_port_t	tcp	2628
distccd_port_t	tcp	3632
dns_port_t	tcp	53, 853

dns_port_t	udp	53, 853
dnssec_port_t	tcp	8955
dogtag_port_t	tcp	7390
echo_port_t	tcp	7
echo_port_t	udp	7
efs_port_t	tcp	520
embrace_dp_c_port_t	tcp	3198
embrace_dp_c_port_t	udp	3198
ephemeral_port_t	tcp	32768-60999
ephemeral_port_t	udp	32768-60999
epmap_port_t	tcp	135
epmap_port_t	udp	135
epmd_port_t	tcp	4369
epmd_port_t	udp	4369
fac_restore_port_t	tcp	5582
fac_restore_port_t	udp	5582
fingerd_port_t	tcp	79
firepower_port_t	tcp	2615
firepower_port_t	udp	2615
flash_port_t	tcp	843, 1935
flash_port_t	udp	1935
fmpro_internal_port_t	tcp	5003
fmpro_internal_port_t	udp	5003
freeipmi_port_t	tcp	9225
freeipmi_port_t	udp	9225
ftp_data_port_t	tcp	20
ftp_port_t	tcp	21, 989, 990
ftp_port_t	udp	989, 990
gatekeeper_port_t	tcp	1721, 7000
gatekeeper_port_t	udp	1718, 1719
gdomap_port_t	tcp	538
gdomap_port_t	udp	538
gds_db_port_t	tcp	3050
gds_db_port_t	udp	3050

gear_port_t	tcp	43273
gear_port_t	udp	43273
geneve_port_t	tcp	6080
gifted_port_t	tcp	1213
git_port_t	tcp	9418
git_port_t	udp	9418
glance_port_t	tcp	9292
glance_port_t	udp	9292
glance_registry_port_t	tcp	9191
glance_registry_port_t	udp	9191
gluster_port_t	tcp	38465-38469, 24007-24027
gopher_port_t	tcp	70
gopher_port_t	udp	70
gpsd_port_t	tcp	2947
hadoop_datanode_port_t	tcp	50010
hadoop_namenode_port_t	tcp	8020
hddtemp_port_t	tcp	7634
hi_reserved_port_t	sctp	512-1023
hi_reserved_port_t	tcp	512-1023
hi_reserved_port_t	udp	512-1023
howl_port_t	tcp	5335
howl_port_t	udp	5353
hplip_port_t	tcp	1782, 2207, 2208, 8290, 8292, 9100, 9101, 9102, 9220, 9221, 9222, 9280, 9281, 9282, 9290, 9291, 50000, 50002
http_cache_port_t	tcp	8080, 8118, 8123, 10001-10010
http_cache_port_t	udp	3130
http_port_t	tcp	80, 81, 443, 488, 8008, 8009, 8443, 9000
...		

Notez par exemple que le serveur apache est autorisé d'utiliser les ports suivants :

http_port_t	tcp	80, 81, 443, 488, 8008, 8009, 8443, 9000
-------------	-----	--

Dans le cas où on souhaite qu'apache utilise le port **8090** par exemple, il est nécessaire de créer la règle adéquate avec la commande semanage :

```
[root@centos8 ~]# semanage port -a -t http_port_t -p tcp 8090
```

Vous noterez que le port 8090 a été ajouté à la liste des ports reconnus comme valides par SELinux :

```
[root@centos8 ~]# semanage port -l | grep http
http_cache_port_t      tcp      8080, 8118, 8123, 10001-10010
http_cache_port_t      udp      3130
http_port_t            tcp      8090, 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t    tcp      5988
pegasus_https_port_t   tcp      5989
```

La commande audit2allow

La création d'un module de politique personnalisé se fait en utilisant la commande **audit2allow**. L'administrateur de sécurité à recours à la création de modules quand, et uniquement quand :

- la résolution du problème n'est pas possible en utilisant une des commandes précédemment citées,
- il n'existe pas de booléen capable de régler le problème.

```
[root@centos8 ~]# audit2allow --help
Usage: audit2allow [options]
```

Options:

--version	show program's version number and exit
-h, --help	show this help message and exit
-b, --boot	audit messages since last boot conflicts with -i
-a, --all	read input from audit log - conflicts with -i
-p POLICY, --policy=POLICY	Policy file to use for analysis
-d, --dmesg	read input from dmesg - conflicts with --all and --input
-i INPUT, --input=INPUT	read input from <input> - conflicts with -a

```
-l, --lastreload      read input only after the last reload
-r, --requires        generate require statements for rules
-m MODULE, --module=MODULE
                        set the module name - implies --requires
-M MODULE_PACKAGE, --module-package=MODULE_PACKAGE
                        generate a module package - conflicts with -o and -m
-o OUTPUT, --output=OUTPUT
                        append output to <filename>, conflicts with -M
-D, --dontaudit       generate policy with dontaudit rules
-R, --reference        generate refpolicy style output
-N, --noreference     do not generate refpolicy style output
-v, --verbose         explain generated output
-e, --explain         fully explain generated output
-t TYPE, --type=TYPE  only process messages with a type that matches this
                        regex
--perm-map=PERM_MAP   file name of perm map
--interface-info=INTERFACE_INFO
                        file name of interface information
-x, --xperms          generate extended permission rules
--debug              leave generated modules for -M
-w, --why             Translates SELinux audit messages into a description
                        of why the access was denied
```

Pour illustrer l'utilisation de cette commande, créez un nouveau répertoire pour les documents d'apache ainsi que la page d'accueil :

```
[root@centos8 tmp]# mkdir /www1
[root@centos8 tmp]# touch /www1/index.html
```

Éditez le fichier **/etc/httpd/conf/httpd.conf** :

```
[...]
#DocumentRoot "/var/www/html"
DocumentRoot "/www1"
```

```
[...]
```

Ajoutez les section **<Directory "/www">**:

```
...
<Directory "/var/www">
    AllowOverride None
    # Allow open access:
    Require all granted
</Directory>

<Directory "/www1">
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>

# Further relax access to the default document root:
<Directory "/var/www/html">
    ...
```

Créez le fichier **/www1/index.html** :

```
[root@centos8 ~]# vi /www1/index.html
[root@centos8 ~]# cat /www1/index.html
<html>
<title>
This is a test
</title>
<body>
www1 test page
</body>
</html>
```

Modifiez ensuite le propriétaire et le groupe du répertoire **/www1** et son contenu :

```
[root@centos8 ~]# chown -R apache:apache /www1
```

Redémarrez le service httpd :

```
[root@centos8 ~]# systemctl restart httpd.service
[root@centos8 ~]# systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Wed 2024-10-02 13:17:32 CEST; 12s ago
     Docs: man:httpd.service(8)
  Main PID: 3255 (httpd)
    Status: "Running, listening on: port 80"
     Tasks: 213 (limit: 100949)
    Memory: 49.2M
    CGroup: /system.slice/httpd.service
            └─3255 /usr/sbin/httpd -DFOREGROUND
              └─3256 /usr/sbin/httpd -DFOREGROUND
                └─3257 /usr/sbin/httpd -DFOREGROUND
                  └─3258 /usr/sbin/httpd -DFOREGROUND
                    └─3259 /usr/sbin/httpd -DFOREGROUND

Oct 02 13:17:31 centos8.ittraining.loc systemd[1]: Starting The Apache HTTP Server...
Oct 02 13:17:32 centos8.ittraining.loc systemd[1]: Started The Apache HTTP Server.
Oct 02 13:17:32 centos8.ittraining.loc httpd[3255]: Server configured, listening on: port 80
```

Consultez le site localhost en utilisant **lynx** :

```
[root@centos8 ~]# lynx --dump localhost
HTTP Server Test Page
```

```
This page is used to test the proper operation of the HTTP server after
it has been installed. If you can read this page it means that this
```

site is working properly. This server is powered by [1]CentOS.

If you are a member of the general public:

The website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting `www.example.com`, you should send e-mail to "`webmaster@example.com`".

If you are the website administrator:

You may now add content to the webroot directory. Note that until you do so, people visiting your website will see this page, and not your content.

For systems using the Apache HTTP Server: You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

For systems using NGINX: You should now put your content in a location of your choice and edit the root configuration directive in the nginx configuration file `/etc/nginx/nginx.conf`.

[2][Powered by CentOS] [Powered by CentOS]

Important note!

The CentOS Project has nothing to do with this website or its content, it just provides the software that makes the website run.

If you have issues with the content of this site, contact the owner of the domain, not the CentOS project. Unless you intended to visit CentOS.org, the CentOS Project does not have anything to do with this website, the content or the lack of it.

For example, if this website is www.example.com, you would find the owner of the example.com domain at the following WHOIS server:

[3]<http://www.internic.net/whois.html>

© 2021 The CentOS Project | [4]Legal | [5]Privacy

References

1. <http://centos.org/>
2. <https://www.centos.org/>
3. <http://www.internic.net/whois.html>
4. <https://www.centos.org/legal/>
5. <https://www.centos.org/legal/privacy/>

Le fichier **/var/log/audit/audit.log** contient maintenant des notifications de type **AVC** :

```
Oct  2 13:20:57 centos8 setroubleshoot[3502]: SELinux is preventing /usr/sbin/httpd from getattr access on the
file /www1/index.html. For complete SELinux messages run: sealert -l 874480af-4890-4ae4-ala2-961f5c528f3e
Oct  2 13:20:57 centos8 setroubleshoot[3502]: SELinux is preventing /usr/sbin/httpd from getattr access on the
file /www1/index.html.#012#012***** Plugin catchall_labels (83.8 confidence) suggests
*****#012#012If you want to allow httpd to have getattr access on the index.html file#012Then you
need to change the label on /www1/index.html#012Do#012# semanage fcontext -a -t FILE_TYPE
'/www1/index.html'#012where FILE_TYPE is one of the following: NetworkManager_exec_t, NetworkManager_log_t,
NetworkManager_tmp_t, abrt_dump_oops_exec_t, abrt_etc_t, abrt_exec_t, abrt_handle_event_exec_t,
```

abrt_helper_exec_t, abrt_retrace_coredump_exec_t, abrt_retrace_spool_t, abrt_retrace_worker_exec_t, abrt_tmp_t, abrt_upload_watch_tmp_t, abrt_var_cache_t, abrt_var_log_t, abrt_var_run_t, accountsd_exec_t, acct_data_t, acct_exec_t, admin_crontab_tmp_t, admin_passwd_exec_t, afs_logfile_t, aide_exec_t, aide_log_t, alsa_exec_t, alsa_tmp_t, amanda_exec_t, amanda_log_t, amanda_recover_exec_t, amanda_tmp_t, amtu_exec_t, anacron_exec_t, anon_inodefs_t, antivirus_exec_t, antivirus_log_t, antivirus_tmp_t, apcupsd_cgi_content_t, apcupsd_cgi_htaccess_t, apcupsd_cgi_ra_content_t, apcupsd_cgi_rw_content_t, apcupsd_cgi_script_exec_t, apcupsd_log_t, apcupsd_tmp_t, apm_exec_t, apmd_log_t, apmd_tmp_t, arpwatch_tmp_t, asterisk_log_t, asterisk_tmp_t, audisp_exec_t, auditadm_sudo_tmp_t, auditctl_exec_t, auditd_tmp_t, auth_cache_t, authconfig_exec_t, automount_tmp_t, avahi_exec_t, awstats_content_t, awstats_htaccess_t, awstats_ra_content_t, awstats_rw_content_t, awstats_script_exec_t, awstats_tmp_t, bacula_admin_exec_t, bacula_log_t, bacula_tmp_t, bacula_unconfined_script_exec_t, bin_t, bitlbee_log_t, bitlbee_tmp_t, blueman_exec_t, blueman_tmp_t, bluetooth_helper_exec_t, bluetooth_helper_tmp_t, bluetooth_helper_tmpfs_t, bluetooth_tmp_t, boinc_log_t, boinc_project_tmp_t, boinc_tmp_t, boot_t, bootloader_exec_t, bootloader_tmp_t, brctl_exec_t, brlty_log_t, bugzilla_content_t, bugzilla_htaccess_t, bugzilla_ra_content_t, bugzilla_rw_content_t, bugzilla_script_exec_t, bugzilla_tmp_t, calamaris_exec_t, calamaris_log_t, calamaris_www_t, callweaver_log_t, canna_log_t, cardctl_exec_t, cardmgr_dev_t, ccs_tmp_t, ccs_var_lib_t, ccs_var_log_t, cdcc_exec_t, cdcc_tmp_t, cdrecord_exec_t, cert_t, certmaster_var_log_t, certmonger_tmp_t, certmonger_unconfined_exec_t, certwatch_exec_t, cfengine_log_t, cgroup_log_t, cgroup_t, checkpc_exec_t, checkpc_log_t, checkpolicy_exec_t, chfn_exec_t, chkpwd_exec_t, chrome_sandbox_exec_t, chrome_sandbox_nacl_exec_t, chrome_sandbox_tmp_t, chronyc_exec_t, chronyd_tmp_t, chronyd_var_log_t, cinder_api_tmp_t, cinder_backup_tmp_t, cinder_log_t, cinder_scheduler_tmp_t, cinder_volume_tmp_t, cloud_init_tmp_t, cloud_log_t, cluster_conf_t, cluster_tmp_t, cluster_var_lib_t, cluster_var_log_t, cluster_var_run_t, cobbler_etc_t, cobbler_tmp_t, cobbler_var_lib_t, cobbler_var_log_t, cockpit_tmp_t, cockpit_tmpfs_t, collectd_content_t, collectd_htaccess_t, collectd_log_t, collectd_ra_content_t, collectd_rw_content_t, collectd_script_exec_t, collectd_script_tmp_t, colord_exec_t, colord_tmp_t, comsat_tmp_t, condor_log_t, condor_master_tmp_t, condor_schedd_tmp_t, condor_startd_tmp_t, conman_log_t, conman_tmp_t, conman_unconfined_script_exec_t, conntrackd_log_t, consolehelper_exec_t, consolekit_exec_t, consolekit_log_t, container_file_t, container_log_t, container_runtime_tmp_t, couchdb_log_t, couchdb_tmp_t, courier_exec_t, cpu_online_t, cpucontrol_exec_t, cpufreqselector_exec_t, cpuspeed_exec_t, crack_exec_t, crack_tmp_t, cron_log_t, crond_tmp_t, crontab_exec_t, crontab_tmp_t, ctddb_log_t, ctddb_tmp_t, cups_pdf_tmp_t, cupsd_config_exec_t, cupsd_log_t, cupsd_lpd_tmp_t, cupsd_tmp_t, cvs_content_t, cvs_data_t, cvs_exec_t, cvs_htaccess_t, cvs_ra_content_t, cvs_rw_content_t, cvs_script_exec_t, cvs_tmp_t, cyphesis_exec_t, cyphesis_log_t, cyphesis_tmp_t, cyrus_tmp_t, dbadm_sudo_tmp_t, dbskkd_tmp_t, dbusd_etc_t, dbusd_exec_t, dcc_client_exec_t, dcc_client_tmp_t, dcc_dbclean_exec_t, dcc_dbclean_tmp_t, dccd_tmp_t, dccifd_tmp_t, dccm_tmp_t, ddclient_log_t, ddclient_tmp_t, debuginfo_exec_t, deltacloud_log_t, deltacloud_tmp_t, denyhosts_var_log_t,

devicekit_disk_exec_t, devicekit_exec_t, devicekit_power_exec_t, devicekit_tmp_t, devicekit_var_log_t, dhcpd_exec_t, dhcpd_tmp_t, dhcpd_tmp_t, dirsrv_config_t, dirsrv_share_t, dirsrv_snmp_var_log_t, dirsrv_tmp_t, dirsrv_var_log_t, dirsrv_var_run_t, dirsrvadmin_config_t, dirsrvadmin_content_t, dirsrvadmin_htaccess_t, dirsrvadmin_ra_content_t, dirsrvadmin_rw_content_t, dirsrvadmin_script_exec_t, dirsrvadmin_tmp_t, dirsrvadmin_unconfined_script_exec_t, disk_munin_plugin_exec_t, disk_munin_plugin_tmp_t, dkim_milter_tmp_t, dlm_controld_var_log_t, dmesg_exec_t, dmesgcode_exec_t, dnsmasq_tmp_t, dnsmasq_var_log_t, dnssec_trigger_tmp_t, dovecot_auth_tmp_t, dovecot_deliver_tmp_t, dovecot_tmp_t, dovecot_var_log_t, drbd_tmp_t, dspam_content_t, dspam_htaccess_t, dspam_log_t, dspam_ra_content_t, dspam_rw_content_t, dspam_script_exec_t, efivarfs_t, etc_runtime_t, etc_t, evtchnd_var_log_t, exim_exec_t, exim_log_t, exim_tmp_t, fail2ban_client_exec_t, fail2ban_log_t, fail2ban_tmp_t, fail2ban_var_lib_t, faillog_t, fenced_tmp_t, fenced_var_log_t, fetchmail_exec_t, fetchmail_log_t, file_context_t, fingerd_log_t, firewalld_exec_t, firewalld_tmp_t, firewalld_var_log_t, firewallgui_exec_t, firewallgui_tmp_t, firstboot_exec_t, flatpak_helper_exec_t, foghorn_var_log_t, fonts_cache_t, fonts_t, fprintd_exec_t, fprintd_tmp_t, freqset_exec_t, fsadm_exec_t, fsadm_log_t, fsadm_tmp_t, fsdaemon_tmp_t, ftpd_tmp_t, ftpdctl_exec_t, ftpdctl_tmp_t, fwupd_exec_t, games_exec_t, games_tmp_t, games_tmpfs_t, gconf_tmp_t, gconfd_exec_t, gconfdefaultsm_exec_t, geoclue_exec_t, geoclue_tmp_t, getty_exec_t, getty_log_t, getty_tmp_t, gfs_controld_var_log_t, git_content_t, git_htaccess_t, git_ra_content_t, git_rw_content_t, git_script_exec_t, git_script_tmp_t, git_sys_content_t, gitd_exec_t, gitosis_exec_t, gitosis_var_lib_t, gkeyringd_exec_t, gkeyringd_tmp_t, glance_log_t, glance_registry_tmp_t, glance_tmp_t, gnomesystemmm_exec_t, gpg_agent_exec_t, gpg_agent_tmp_t, gpg_agent_tmpfs_t, gpg_exec_t, gpg_helper_exec_t, gpg_pinentry_tmp_t, gpg_pinentry_tmpfs_t, gpm_tmp_t, gpsd_exec_t, groupadd_exec_t, groupd_var_log_t, gssd_tmp_t, haproxy_var_log_t, hostname_etc_t, hostname_exec_t, hsldb_tmp_t, httpd_cache_t, httpd_config_t, httpd_exec_t, httpd_helper_exec_t, httpd_keytab_t, httpd_lock_t, httpd_log_t, httpd_modules_t, httpd_passwd_exec_t, httpd_php_exec_t, httpd_php_tmp_t, httpd_rotatelogd_exec_t, httpd_squirrelmail_t, httpd_suexec_exec_t, httpd_suexec_tmp_t, httpd_sys_content_t, httpd_sys_htaccess_t, httpd_sys_ra_content_t, httpd_sys_rw_content_t, httpd_sys_script_exec_t, httpd_tmp_t, httpd_tmpfs_t, httpd_unconfined_script_exec_t, httpd_user_htaccess_t, httpd_user_ra_content_t, httpd_user_rw_content_t, httpd_user_script_exec_t, httpd_var_lib_t, httpd_var_run_t, hugetlbfs_t, hwclock_exec_t, hwloc_dhwd_exec_t, ibacm_log_t, iceauth_exec_t, icecast_exec_t, icecast_log_t, ifconfig_exec_t, inetd_child_tmp_t, inetd_log_t, inetd_tmp_t, init_tmp_t, initrc_tmp_t, initrc_var_log_t, innd_log_t, install_exec_t, iotop_exec_t, ipsec_log_t, ipsec_mgmt_exec_t, ipsec_tmp_t, iptables_exec_t, iptables_tmp_t, irc_exec_t, irssi_exec_t, iscsi_log_t, iscsi_tmp_t, iso9660_t, iwhd_log_t, jetty_cache_t, jetty_log_t, jetty_tmp_t, jetty_unit_file_t, jetty_var_lib_t, jetty_var_run_t, jockey_exec_t, jockey_var_log_t, journalctl_exec_t, kadmind_log_t, kadmind_tmp_t, kdump_exec_t, kdumpctl_tmp_t, kdumpgui_exec_t, kdumpgui_tmp_t, keepalived_tmp_t, keepalived_unconfined_script_exec_t, keystone_cgi_content_t, keystone_cgi_htaccess_t, keystone_cgi_ra_content_t, keystone_cgi_rw_content_t, keystone_cgi_script_exec_t, keystone_log_t, keystone_tmp_t,

```
kismet_exec_t, kismet_log_t, kismet_tmp_t, kismet_tmpfs_t, klogd_tmp_t, kmod_exec_t, kmod_tmp_t, kpatch_exec_t,
krb5_conf_t, krb5_host_rcache_t, krb5_keytab_t, krb5kdc_conf_t, krb5kdc_log_t, krb5kdc_tmp_t, ksmtuned_log_t,
ktalkd_log_t, ktalkd_tmp_t, l2tpd_tmp_t, lastlog_t, ld_so_cache_t, ld_so_t, ldconfig_exec_t, ldconfig_tmp_t, lib
```

A l'aide de la commande `grep`, il convient maintenant d'envoyer les messages d'erreurs en provenance du fichier **/var/log/audit/audit.log** sur l'entrée standard de la commande **audit2allow** afin de permettre celle-ci de créer des règles permettant l'autorisation de ce qui a été précédemment interdit par SELinux :

```
[root@centos8 ~]# grep httpd_t /var/log/audit/audit.log | audit2allow -m httpdlocal > httpdlocal.te
```

L'examen du fichier **httpdlocal.te** révèle la création de ces règles :

```
[root@centos8 ~]# cat httpdlocal.te

module httpdlocal 1.0;

require {
    type httpd_t;
    type default_t;
    class capability net_admin;
    class file { getattr map open read };
}

#===== httpd_t =====

#!!!! This avc can be allowed using the boolean 'domain_can_mmap_files'
allow httpd_t default_t:file map;
allow httpd_t default_t:file { getattr open read };

#!!!! This avc has a dontaudit rule in the current policy
allow httpd_t self:capability net_admin;
```

L'audit du fichier terminé, il faut maintenant utiliser `audit2allow` pour fabriquer un module de politique :

```
[root@centos8 ~]# grep httpd_t /var/log/audit/audit.log | audit2allow -M httpdlocal
```

***** IMPORTANT *****

To make this policy package active, execute:

```
semodule -i httpdlocal.pp
```

Chargez maintenant le module dans la politique SELinux :

```
[root@centos8 ~]# semodule -i httpdlocal.pp
```

Vérifiez que le module est chargé :

```
[root@centos8 ~]# semodule -l | grep httpd
httpdlocal
```

Redémarrez le service httpd :

```
[root@centos8 ~]# systemctl restart httpd.service
```

```
[root@centos8 ~]# systemctl status httpd.service
```

- `httpd.service` - The Apache HTTP Server

```
Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
```

Active: active (running) since Wed 2024-10-02 13:28:09 CEST; 8s ago

Docs: `man:httpd.service(8)`

Main PID: 3620 (httpd)

```
Status: "Started, listening on: port 80"
```

Tasks: 213 (limit: 100949)

Memory: 42.7M

CGroup: /system.slice/httpd.service

```
|—3620 /usr/sbin/httpd -DFOREGROUND
```

```
|—3622 /usr/sbin/httpd -DFOREGROUND
```

```
|—3623 /usr/sbin/httpd -DFOREGROUND
```

```
|—3624 /usr/sbin/httpd -DFOREGROUND
```

```
└─3625 /usr/sbin/httpd -DFOREGROUND
```

```
Oct 02 13:28:09 centos8.ittraining.loc systemd[1]: Starting The Apache HTTP Server...
Oct 02 13:28:09 centos8.ittraining.loc systemd[1]: Started The Apache HTTP Server.
Oct 02 13:28:09 centos8.ittraining.loc httpd[3620]: Server configured, listening on: port 80
```

Consultez le site localhost :

```
[root@centos8 ~]# lynx --dump localhost
www1 test page
```

Mots de Passe

Un pirate peut utiliser un logiciel de **crackage** pour tenter de découvrir un mot de passe. Le plus connu est [John The Ripper](#).

Le principe de ces logiciels est simples - le logiciel utilise des dictionnaires de mots de passe qui sont utilisés le uns après les autres à une vitesse qui peut atteindre des milliers par seconde.

LAB #3 - John the Ripper

Installation

Créez le script suivant dans un terminal de RHEL/CentOS 7 en tant que root :

```
[root@centos8 ~]# vi john.sh
[root@centos8 ~]# cat john.sh
#!/bin/bash
# Centos 7 John the Ripper Installation
yum -y install wget gpgme
yum -y group install "Development Tools"
cd
wget http://www.openwall.com/john/j/john-1.8.0.tar.xz
```

```
wget http://www.openwall.com/john/j/john-1.8.0.tar.xz.sign
wget http://www.openwall.com/signatures/openwall-signatures.asc
gpg --import openwall-signatures.asc
gpg --verify john-1.8.0.tar.xz.sign
tar xvfJ john-1.8.0.tar.xz
cd john-1.8.0/src
make clean linux-x86-64
cd ../run/
./john --test
#password dictionary download
wget -O - http://mirrors.kernel.org/openwall/wordlists/all.gz | gunzip -c > openwall.dico
```

Rendez-le exécutable :

```
[root@centos8 ~]# chmod u+x john.sh
```

Exécutez le script :

```
[root@centos8 ~]# ./john.sh
```

Utilisation

Placez-vous dans le répertoire **/root/john-1.8.0/run** :

```
[root@centos8 ~]# cd john-1.8.0/run/
```

Utilisez l'utilitaire **unshadow** pour créer le fichier des mots de passe :

```
[root@centos8 run]# ./unshadow /etc/passwd /etc/shadow > mypasswd
```

Consultez le fichier **myspasswd** :

```
[root@centos8 run]# cat mypasswd
root:$6$ZagUzfR879NQxAks$hgN8rjBjwk90/Bd6fsjQ9p5DPSw3ZoeJVz1SXahzeWsnov3VKn93WNHrqUsqmTqKV.jqza4Jdym7t5jzTA2ez.:0
:0:root:/root:/bin/bash
bin:*:1:1:bin:/bin:/sbin/nologin
daemon:*:2:2:daemon:/sbin:/sbin/nologin
adm:*:3:4:adm:/var/adm:/sbin/nologin
lp:*:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:*:5:0:sync:/sbin:/bin/sync
shutdown:*:6:0:shutdown:/sbin:/sbin/shutdown
halt:*:7:0:halt:/sbin:/sbin/halt
mail:*:8:12:mail:/var/spool/mail:/sbin/nologin
operator:*:11:0:operator:/root:/sbin/nologin
games:*:12:100:games:/usr/games:/sbin/nologin
ftp:*:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:*:65534:65534:Kernel Overflow User:/:/sbin/nologin
dbus:!!:81:81:System message bus:/:/sbin/nologin
systemd-coredump:!!:999:997:systemd Core Dumper:/:/sbin/nologin
systemd-resolve:!!:193:193:systemd Resolver:/:/sbin/nologin
tss:!!:59:59:Account used for TPM access:/dev/null:/sbin/nologin
polkitd:!!:998:996:User for polkitd:/:/sbin/nologin
geoclue:!!:997:995:User for geoclue:/var/lib/geoclue:/sbin/nologin
rtkit:!!:172:172:RealtimeKit:/proc:/sbin/nologin
pipewire:!!:996:992:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
libstoragemgmt:!!:995:991:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
qemu:!!:107:107:qemu user:/:/sbin/nologin
clevis:!!:994:990:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/sbin/nologin
usbmuxd:!!:113:113:usbmuxd user:/:/sbin/nologin
unbound:!!:993:989:Unbound DNS resolver:/etc/unbound:/sbin/nologin
gluster:!!:992:988:GlusterFS daemons:/run/gluster:/sbin/nologin
rpc:!!:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
avahi:!!:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
dnsmasq:!!:987:987:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
radvd:!!:75:75:radvd user:/:/sbin/nologin
saslauth:!!:986:76:Saslauthd user:/run/saslauthd:/sbin/nologin
```

```
sssd:!!:985:986:User for sssd:/:/sbin/nologin
cockpit-ws:!!:984:984:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:!!:983:983:User for cockpit-ws instances:/nonexisting:/sbin/nologin
chrony:!!:982:982::/var/lib/chrony:/sbin/nologin
colord:!!:981:981:User for colord:/var/lib/colord:/sbin/nologin
rpcuser:!!:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
pulse:!!:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
setroubleshoot:!!:980:977::/var/lib/setroubleshoot:/sbin/nologin
flatpak:!!:979:976:User for flatpak system helper:/:/sbin/nologin
gdm:!!:42:42::/var/lib/gdm:/sbin/nologin
gnome-initial-setup:!!:978:975::/run/gnome-initial-setup:/sbin/nologin
sshd:!!:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:!!:72:72:::/sbin/nologin
trainee:$6$g0ugY2dcMmHB1AIX$/JB80G1MD.ExKh0Tvm3.SZWAyr5w3jJLVeT9cu4sENvGcCQAnJjKWQIAEug1K5HGcNk5RGr.RGYzbJn60m/4L
.:1000:1000:trainee:/home/trainee:/bin/bash
apache:!!:48:48:Apache:/usr/share/httpd:/sbin/nologin
pesign:!!:977:974:Group for the pesign signing daemon:/var/run/pesign:/sbin/nologin
```

Lancez **john** pour craquer le fichier **mypasswd** :

```
[root@centos8 run]# ./john mypasswd
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
trainee          (trainee)
[q] <-----appuyez sur la touche
q
lg 0:00:00:27 5% 2/3 0.03650g/s 282.4p/s 282.4c/s 282.4C/s Notta1..Notused
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

Consultez la liste des mots de passe craqués :

```
[root@centos8 run]# ./john --show mypasswd
trainee:trainee:1000:1000:trainee:/home/trainee:/bin/bash
```

1 password hash cracked, 1 left

LAB #4 - Mise en place du Système de Prévention d'Intrusion Fail2Ban



Important - Pour continuer, il faut travailler sur un CentOS 8 Stream.

Fail2Ban est un **S**ystème de **P**révention d'**I**ntrusion. Fail2Ban lit les logs de divers services (SSH, Apache, FTP...) à la recherche d'erreurs d'authentification répétées et ajoute une règle à iptables pour bannir l'adresse IP de la source.

Installation

Installez Fail2Ban :

```
[root@centos8 run]# cd ~  
[root@centos8 ~]# dnf install fail2ban
```

Configuration

La configuration de Fail2Ban se trouve dans le fichier **/etc/fail2ban/jail.conf** :

```
[root@centos8 ~]# more /etc/fail2ban/jail.conf  
#  
# WARNING: heavily refactored in 0.9.0 release. Please review and  
#           customize settings for your setup.  
#  
# Changes:  in most of the cases you should not modify this  
#           file, but provide customizations in jail.local file,  
#           or separate .conf files under jail.d/ directory, e.g.:
```

```
#
# HOW TO ACTIVATE JAILS:
#
# YOU SHOULD NOT MODIFY THIS FILE.
#
# It will probably be overwritten or improved in a distribution update.
#
# Provide customizations in a jail.local file or a jail.d/customisation.local.
# For example to change the default bantime for all jails and to enable the
# ssh-iptables jail the following (uncommented) would appear in the .local file.
# See man 5 jail.conf for details.
#
# [DEFAULT]
# bantime = 1h
#
# [sshd]
# enabled = true
#
# See jail.conf(5) man page for more information

# Comments: use '#' for comment lines and ';' (following a space) for inline comments

[INCLUDES]

#before = paths-distro.conf
before = paths-fedora.conf

# The DEFAULT allows a global definition of the options. They can be overridden
# in each jail afterwards.

[DEFAULT]
```

```
#
# MISCELLANEOUS OPTIONS
#

# "bantime.increment" allows to use database for searching of previously banned ip's to increase a
# default ban time using special formula, default it is banTime * 1, 2, 4, 8, 16, 32...
#bantime.increment = true

# "bantime.rndtime" is the max number of seconds using for mixing with random time
# to prevent "clever" botnets calculate exact time IP can be unbanned again:
#bantime.rndtime =

# "bantime.maxtime" is the max number of seconds using the ban time can reach (doesn't grow further)
#bantime.maxtime =

# "bantime.factor" is a coefficient to calculate exponent growing of the formula or common multiplier,
--More-- (6%)
[q]
```

Dans ce fichier se trouvent des sections pour configurer l'action de Fail2Ban pour chaque service :

```
...
[sshd]

# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and details.
#mode    = normal
port     = ssh
logpath  = %(sshd_log)s
backend  = %(sshd_backend)s
...
```

Ces sections, appelées des Prisons (*jails* en anglais), peuvent contenir des directives telles que :

Directive	Description
enabled	Indique si oui (true) ou non (false) le prison est activé.
port	Le port à bloquer dans iptables.
filter	Le nom du filtre, une expression régulière, associé au prison et utilisé pour trouver une activité suspect. Le nom dans ce champs, sans l'extention .conf, fait référence à un fichier dans le répertoire /etc/fail2ban/filter.d/ . Par exemple la valeur sshd fait référence au fichier /etc/fail2ban/filter.d/sshd.conf .
logpath	Le nom et le chemin du journal à examiner.
maxretry	Le nombre maximal de tentatives.
action	Spécifie l'action à entreprendre lors d'une correspondance du filter . Le nom dans ce champs, sans l'extention .conf, fait référence à un fichier dans le répertoire /etc/fail2ban/action.d/ . Par exemple la valeur iptables fait référence au fichier /etc/fail2ban/action.d/iptables.conf .

Il n'est pas recommandé de modifier ce fichier afin de ne pas voir ses modifications écrasées lors de la prochaine mise-à-jour de Fail2Ban. Fail2Ban nous donne la possibilité de créer le fichier **/etc/fail2ban/jail.local** pour contenir nos modifications. Créez donc ce fichier avec le contenu ci-dessous :

```
[root@centos8 ~]# vi /etc/fail2ban/jail.local
[root@centos8 ~]# cat /etc/fail2ban/jail.local
[DEFAULT]
ignoreip = 127.0.0.1 172.YY+20.0.3
findtime = 3600
bantime = 86400
maxretry = 5

[sshd]
enabled = true
```

Il est à noter que les directives dans le fichier **jail.conf** sont surchargées par celles dans les fichiers suivantes et dans l'ordre suivant :

- **/etc/fail2ban/jail.d/*.conf** dans l'ordre alphabétique,
- **/etc/fail2ban/jail.local**,
- **/etc/fail2ban/jail.d/*.local** dans l'ordre alphabétique.



Important - Notez que la définition des variables dans la section



[DEFAULT] du fichier **/etc/fail2ban/jail.local** s'appliquent à toutes les sections de prisons actives dans les fichiers **/etc/fail2ban/jail.local** et **/etc/fail2ban/jail.conf** sauf si dans la section du prison elle-même, la variable est redéfinie.

Dans ce fichier, les directives sont donc :

Directive	Description
ignoreip	Liste des adresses IP, séparées par un espace , qui ne sont pas concernées par l'action de Fail2Ban ou une liste d'adresses de réseaux, exprimées au format CIDR.
findtime	L'intervalle de temps en secondes, avant l'heure actuelle, pendant laquelle des authentifications infructueuses sont prises en compte pour le calcul de banir l'adresse IP ou non.
bantime	La durée de vie des règles, en secondes, inscrites dans le pare-feu iptables.
maxretry	Le nombre maximal de tentatives. La règle sera donc inscrite dans le pare-feu lors de la sixième tentative.

Le répertoire **/etc/fail2ban**

Le répertoire **/etc/fail2ban/** contient des fichiers et répertoires importants pour le fonctionnement de Fail2Ban :

```
[root@centos8 ~]# ls -l /etc/fail2ban/
total 56
drwxr-xr-x. 2 root root 4096 Oct 2 16:19 action.d
-rw-r--r--. 1 root root 3017 Apr 1 2023 fail2ban.conf
drwxr-xr-x. 2 root root 6 Apr 1 2023 fail2ban.d
drwxr-xr-x. 3 root root 4096 Oct 2 16:19 filter.d
-rw-r--r--. 1 root root 25607 Apr 1 2023 jail.conf
drwxr-xr-x. 2 root root 31 Oct 2 16:19 jail.d
-rw-r--r--. 1 root root 114 Oct 2 16:26 jail.local
-rw-r--r--. 1 root root 2728 Apr 1 2023 paths-common.conf
-rw-r--r--. 1 root root 930 Apr 1 2023 paths-fedora.conf
```

Le fichier fail2ban.conf

Ce fichier définit les configurations globales de Fail2Ban, telles le **pidfile**, le **socket** et le niveau syslog de journalisation :

```
[root@centos8 ~]# cat /etc/fail2ban/fail2ban.conf
# Fail2Ban main configuration file
#
# Comments: use '#' for comment lines and ';' (following a space) for inline comments
#
# Changes:  in most of the cases you should not modify this
#           file, but provide customizations in fail2ban.local file, e.g.:
#
# [DEFAULT]
# loglevel = DEBUG
#
[DEFAULT]

# Option: loglevel
# Notes.: Set the log level output.
#         CRITICAL
#         ERROR
#         WARNING
#         NOTICE
#         INFO
#         DEBUG
# Values: [ LEVEL ]  Default: INFO
#
loglevel = INFO

# Option: logtarget
# Notes.: Set the log target. This could be a file, SYSTEMD-JOURNAL, SYSLOG, STDERR or STDOUT.
#         Only one log target can be specified.
```

```
#      If you change logtarget from the default value and you are
#      using logrotate -- also adjust or disable rotation in the
#      corresponding configuration file
#      (e.g. /etc/logrotate.d/fail2ban on Debian systems)
# Values: [ STDOUT | STDERR | SYSLOG | SYSOUT | SYSTEMD-JOURNAL | FILE ] Default: STDERR
#
logtarget = /var/log/fail2ban.log

# Option: syslogsocket
# Notes: Set the syslog socket file. Only used when logtarget is SYSLOG
#       auto uses platform.system() to determine predefined paths
# Values: [ auto | FILE ] Default: auto
syslogsocket = auto

# Option: socket
# Notes.: Set the socket file. This is used to communicate with the daemon. Do
#         not remove this file when Fail2ban runs. It will not be possible to
#         communicate with the server afterwards.
# Values: [ FILE ] Default: /var/run/fail2ban/fail2ban.sock
#
socket = /var/run/fail2ban/fail2ban.sock

# Option: pidfile
# Notes.: Set the PID file. This is used to store the process ID of the
#         fail2ban server.
# Values: [ FILE ] Default: /var/run/fail2ban/fail2ban.pid
#
pidfile = /var/run/fail2ban/fail2ban.pid

# Option: allowipv6
# Notes.: Allows IPv6 interface:
#         Default: auto
# Values: [ auto yes (on, true, 1) no (off, false, 0) ] Default: auto
#allowipv6 = auto
```

```
# Options: dbfile
# Notes.: Set the file for the fail2ban persistent data to be stored.
#         A value of ":memory:" means database is only stored in memory
#         and data is lost when fail2ban is stopped.
#         A value of "None" disables the database.
# Values: [ None :memory: FILE ] Default: /var/lib/fail2ban/fail2ban.sqlite3
dbfile = /var/lib/fail2ban/fail2ban.sqlite3

# Options: dbpurgeage
# Notes.: Sets age at which bans should be purged from the database
# Values: [ SECONDS ] Default: 86400 (24hours)
dbpurgeage = 1d

# Options: dbmaxmatches
# Notes.: Number of matches stored in database per ticket (resolvable via
#         tags <ipmatches>/<ipjailmatches> in actions)
# Values: [ INT ] Default: 10
dbmaxmatches = 10

[Definition]

[Thread]

# Options: stacksize
# Notes.: Specifies the stack size (in KiB) to be used for subsequently created threads,
#         and must be 0 or a positive integer value of at least 32.
# Values: [ SIZE ] Default: 0 (use platform or configured default)
#stacksize = 0
```

Le répertoire `/etc/fail2ban/filter.d/`

Ce répertoire contient les fichiers appelés par les directives **filter** dans les sections des prisons :

```
[root@centos8 ~]# ls -l /etc/fail2ban/filter.d/
total 380
-rw-r--r--. 1 root root 467 Apr 1 2023 3proxy.conf
-rw-r--r--. 1 root root 3228 Apr 1 2023 apache-auth.conf
-rw-r--r--. 1 root root 2831 Apr 1 2023 apache-badbots.conf
-rw-r--r--. 1 root root 1265 Apr 1 2023 apache-botsearch.conf
-rw-r--r--. 1 root root 1619 Apr 1 2023 apache-common.conf
-rw-r--r--. 1 root root 403 Apr 1 2023 apache-fakegooglebot.conf
-rw-r--r--. 1 root root 511 Apr 1 2023 apache-modsecurity.conf
-rw-r--r--. 1 root root 596 Apr 1 2023 apache-nohome.conf
-rw-r--r--. 1 root root 1246 Apr 1 2023 apache-noscript.conf
-rw-r--r--. 1 root root 2187 Apr 1 2023 apache-overflows.conf
-rw-r--r--. 1 root root 362 Apr 1 2023 apache-pass.conf
-rw-r--r--. 1 root root 1020 Apr 1 2023 apache-shellshock.conf
-rw-r--r--. 1 root root 3492 Apr 1 2023 assp.conf
-rw-r--r--. 1 root root 2386 Apr 1 2023 asterisk.conf
-rw-r--r--. 1 root root 427 Apr 1 2023 bitwarden.conf
-rw-r--r--. 1 root root 522 Apr 1 2023 botsearch-common.conf
-rw-r--r--. 1 root root 307 Apr 1 2023 centreon.conf
-rw-r--r--. 1 root root 2776 Apr 1 2023 common.conf
-rw-r--r--. 1 root root 244 Apr 1 2023 counter-strike.conf
-rw-r--r--. 1 root root 463 Apr 1 2023 courier-auth.conf
-rw-r--r--. 1 root root 512 Apr 1 2023 courier-smtp.conf
-rw-r--r--. 1 root root 444 Apr 1 2023 cyrus-imap.conf
-rw-r--r--. 1 root root 338 Apr 1 2023 directadmin.conf
-rw-r--r--. 1 root root 2107 Apr 1 2023 domino-smtp.conf
-rw-r--r--. 1 root root 2647 Apr 1 2023 dovecot.conf
-rw-r--r--. 1 root root 1730 Apr 1 2023 dropbear.conf
-rw-r--r--. 1 root root 547 Apr 1 2023 drupal-auth.conf
-rw-r--r--. 1 root root 1572 Apr 1 2023 ejabberd-auth.conf
-rw-r--r--. 1 root root 534 Apr 1 2023 exim-common.conf
-rw-r--r--. 1 root root 2875 Apr 1 2023 exim.conf
-rw-r--r--. 1 root root 2158 Apr 1 2023 exim-spam.conf
-rw-r--r--. 1 root root 1922 Apr 1 2023 freeswitch.conf
```

-rw-r--r--.	1	root	root	1210	Apr	1	2023	froxlор-auth.conf
-rw-r--r--.	1	root	root	236	Apr	1	2023	gitlab.conf
-rw-r--r--.	1	root	root	388	Apr	1	2023	grafana.conf
-rw-r--r--.	1	root	root	236	Apr	1	2023	groupoffice.conf
-rw-r--r--.	1	root	root	322	Apr	1	2023	gssftpd.conf
-rw-r--r--.	1	root	root	1447	Apr	1	2023	guacamole.conf
-rw-r--r--.	1	root	root	1170	Apr	1	2023	haproxy-http-auth.conf
-rw-r--r--.	1	root	root	404	Apr	1	2023	horde.conf
drwxr-xr-x.	2	root	root	34	Oct	2	16:19	ignorecommands
-rw-r--r--.	1	root	root	938	Apr	1	2023	kerio.conf
-rw-r--r--.	1	root	root	459	Apr	1	2023	lighttpd-auth.conf
-rw-r--r--.	1	root	root	2279	Apr	1	2023	mongodb-auth.conf
-rw-r--r--.	1	root	root	787	Apr	1	2023	monit.conf
-rw-r--r--.	1	root	root	640	Apr	1	2023	monitorix.conf
-rw-r--r--.	1	root	root	441	Apr	1	2023	mssql-auth.conf
-rw-r--r--.	1	root	root	927	Apr	1	2023	murmur.conf
-rw-r--r--.	1	root	root	953	Apr	1	2023	mysqld-auth.conf
-rw-r--r--.	1	root	root	400	Apr	1	2023	nagios.conf
-rw-r--r--.	1	root	root	1600	Apr	1	2023	named-refused.conf
-rw-r--r--.	1	root	root	474	Apr	1	2023	nginx-bad-request.conf
-rw-r--r--.	1	root	root	740	Apr	1	2023	nginx-botsearch.conf
-rw-r--r--.	1	root	root	1048	Apr	1	2023	nginx-http-auth.conf
-rw-r--r--.	1	root	root	1513	Apr	1	2023	nginx-limit-req.conf
-rw-r--r--.	1	root	root	779	Apr	1	2023	nsd.conf
-rw-r--r--.	1	root	root	452	Apr	1	2023	openhabs.conf
-rw-r--r--.	1	root	root	495	Apr	1	2023	openwebmail.conf
-rw-r--r--.	1	root	root	1937	Apr	1	2023	oracleims.conf
-rw-r--r--.	1	root	root	947	Apr	1	2023	pam-generic.conf
-rw-r--r--.	1	root	root	568	Apr	1	2023	perdition.conf
-rw-r--r--.	1	root	root	278	Apr	1	2023	phpmyadmin-syslog.conf
-rw-r--r--.	1	root	root	891	Apr	1	2023	php-url-fopen.conf
-rw-r--r--.	1	root	root	242	Apr	1	2023	portsentry.conf
-rw-r--r--.	1	root	root	3222	Apr	1	2023	postfix.conf
-rw-r--r--.	1	root	root	1163	Apr	1	2023	proftpd.conf

```
-rw-r--r--. 1 root root 2409 Apr 1 2023 pure-ftpd.conf
-rw-r--r--. 1 root root 795 Apr 1 2023 qmail.conf
-rw-r--r--. 1 root root 1374 Apr 1 2023 recidive.conf
-rw-r--r--. 1 root root 1499 Apr 1 2023 roundcube-auth.conf
-rw-r--r--. 1 root root 354 Apr 1 2023 scanlogd.conf
-rw-r--r--. 1 root root 821 Apr 1 2023 screensharingd.conf
-rw-r--r--. 1 root root 538 Apr 1 2023 selinux-common.conf
-rw-r--r--. 1 root root 570 Apr 1 2023 selinux-ssh.conf
-rw-r--r--. 1 root root 790 Apr 1 2023 sendmail-auth.conf
-rw-r--r--. 1 root root 2970 Apr 1 2023 sendmail-reject.conf
-rw-r--r--. 1 root root 371 Apr 1 2023 sieve.conf
-rw-r--r--. 1 root root 706 Apr 1 2023 slapd.conf
-rw-r--r--. 1 root root 451 Apr 1 2023 softethervpn.conf
-rw-r--r--. 1 root root 722 Apr 1 2023 sogo-auth.conf
-rw-r--r--. 1 root root 1094 Apr 1 2023 solid-pop3d.conf
-rw-r--r--. 1 root root 260 Apr 1 2023 squid.conf
-rw-r--r--. 1 root root 191 Apr 1 2023 squirrelmail.conf
-rw-r--r--. 1 root root 7879 Apr 1 2023 sshd.conf
-rw-r--r--. 1 root root 363 Apr 1 2023 stunnel.conf
-rw-r--r--. 1 root root 649 Apr 1 2023 suhosin.conf
-rw-r--r--. 1 root root 890 Apr 1 2023 tine20.conf
-rw-r--r--. 1 root root 2390 Apr 1 2023 traefik-auth.conf
-rw-r--r--. 1 root root 374 Apr 1 2023 uwimap-auth.conf
-rw-r--r--. 1 root root 637 Apr 1 2023 vsftpd.conf
-rw-r--r--. 1 root root 444 Apr 1 2023 webmin-auth.conf
-rw-r--r--. 1 root root 520 Apr 1 2023 wuftp.conf
-rw-r--r--. 1 root root 521 Apr 1 2023 xinetd-fail.conf
-rw-r--r--. 1 root root 912 Apr 1 2023 znc-adminlog.conf
-rw-r--r--. 1 root root 1146 Apr 1 2023 zoneminder.conf
```

Le répertoire `/etc/fail2ban/action.d/`

Ce répertoire contient les fichiers appelés par les directives **action** dans les sections des prisons :

```
[root@centos8 ~]# ls -l /etc/fail2ban/action.d/
total 228
-rw-r--r--. 1 root root 3748 Apr  1 2023 abuseipdb.conf
-rw-r--r--. 1 root root  587 Apr  1 2023 apf.conf
-rw-r--r--. 1 root root 1413 Apr  1 2023 apprise.conf
-rw-r--r--. 1 root root 2715 Apr  1 2023 blacklist_de.conf
-rw-r--r--. 1 root root 3037 Apr  1 2023 cloudflare.conf
-rw-r--r--. 1 root root 3004 Apr  1 2023 cloudflare-token.conf
-rw-r--r--. 1 root root 7684 Apr  1 2023 dshield.conf
-rw-r--r--. 1 root root 1717 Apr  1 2023 dummy.conf
-rw-r--r--. 1 root root 1501 Apr  1 2023 firewallcmd-allports.conf
-rw-r--r--. 1 root root 2649 Apr  1 2023 firewallcmd-common.conf
-rw-r--r--. 1 root root 3669 Apr  1 2023 firewallcmd-ipset.conf
-rw-r--r--. 1 root root 1270 Apr  1 2023 firewallcmd-multiport.conf
-rw-r--r--. 1 root root 1898 Apr  1 2023 firewallcmd-new.conf
-rw-r--r--. 1 root root 1021 Apr  1 2023 firewallcmd-rich-logging.conf
-rw-r--r--. 1 root root 1753 Apr  1 2023 firewallcmd-rich-rules.conf
-rw-r--r--. 1 root root  592 Apr  1 2023 helpers-common.conf
-rw-r--r--. 1 root root  291 Apr  1 2023 iptables-allports.conf
-rw-r--r--. 1 root root 4790 Apr  1 2023 iptables.conf
-rw-r--r--. 1 root root 2576 Apr  1 2023 iptables-ipset.conf
-rw-r--r--. 1 root root 1980 Apr  1 2023 iptables-ipset-proto4.conf
-rw-r--r--. 1 root root  814 Apr  1 2023 iptables-ipset-proto6-allports.conf
-rw-r--r--. 1 root root  773 Apr  1 2023 iptables-ipset-proto6.conf
-rw-r--r--. 1 root root  232 Apr  1 2023 iptables-multiport.conf
-rw-r--r--. 1 root root 2163 Apr  1 2023 iptables-multiport-log.conf
-rw-r--r--. 1 root root  332 Apr  1 2023 iptables-new.conf
-rw-r--r--. 1 root root 2842 Apr  1 2023 iptables-xt_recent-echo.conf
-rw-r--r--. 1 root root 4292 Apr  1 2023 ipthreat.conf
-rw-r--r--. 1 root root 1051 Apr  1 2023 mail-whois-common.conf
-rw-r--r--. 1 root root 5321 Apr  1 2023 mynetwatchman.conf
-rw-r--r--. 1 root root 1493 Apr  1 2023 netscaler.conf
-rw-r--r--. 1 root root  383 Apr  1 2023 nftables-allports.conf
-rw-r--r--. 1 root root 6318 Apr  1 2023 nftables.conf
```

```
-rw-r--r--. 1 root root 384 Apr 1 2023 nftables-multiport.conf
-rw-r--r--. 1 root root 4010 Apr 1 2023 nginx-block-map.conf
-rw-r--r--. 1 root root 1524 Apr 1 2023 npf.conf
-rw-r--r--. 1 root root 3234 Apr 1 2023 nsupdate.conf
-rw-r--r--. 1 root root 1023 Apr 1 2023 route.conf
-rw-r--r--. 1 root root 2806 Apr 1 2023 sendmail-buffered.conf
-rw-r--r--. 1 root root 1938 Apr 1 2023 sendmail-common.conf
-rw-r--r--. 1 root root 829 Apr 1 2023 sendmail.conf
-rw-r--r--. 1 root root 1761 Apr 1 2023 sendmail-geoip-lines.conf
-rw-r--r--. 1 root root 950 Apr 1 2023 sendmail-whois.conf
-rw-r--r--. 1 root root 1055 Apr 1 2023 sendmail-whois-ipjailmatches.conf
-rw-r--r--. 1 root root 1036 Apr 1 2023 sendmail-whois-ipmatches.conf
-rw-r--r--. 1 root root 1299 Apr 1 2023 sendmail-whois-lines.conf
-rw-r--r--. 1 root root 1000 Apr 1 2023 sendmail-whois-matches.conf
-rw-r--r--. 1 root root 3521 Apr 1 2023 shorewall-ipset-proto6.conf
-rw-r--r--. 1 root root 6277 Apr 1 2023 smtp.py
-rw-r--r--. 1 root root 1503 Apr 1 2023 symbiosis-blacklist-allports.conf
-rw-r--r--. 1 root root 6443 Apr 1 2023 xarf-login-attack.conf
```

Commandes

Fail2Ban est constitué de deux commandes :

```
[root@centos8 ~]# which fail2ban-client
/usr/bin/fail2ban-client

[root@centos8 ~]# which fail2ban-server
/usr/bin/fail2ban-server
```

L'exécutable **fail2ban-server** est responsable de l'examen des fichiers de journalisation ainsi que les commandes de blocage/déblocage. La commande fail2ban-client est utilisée pour configurer le **fail2ban-server**.

Les options de la commande **fail2ban-server** sont :

```
[root@centos8 ~]# fail2ban-server --help
```

```
Usage: fail2ban-server [OPTIONS]
```

Fail2Ban v1.0.2 reads log file that contains password failure report and bans the corresponding IP addresses using firewall rules.

Options:

-c, --conf <DIR>	configuration directory
-s, --socket <FILE>	socket path
-p, --pidfile <FILE>	pidfile path
--pname <NAME>	name of the process (main thread) to identify instance (default fail2ban-server)
--loglevel <LEVEL>	logging level
--logtarget <TARGET>	logging target, use file-name or stdout, stderr, syslog or sysout.
--syslogsocket auto <FILE>	
-d	dump configuration. For debugging
--dp, --dump-pretty	dump the configuration using more human readable representation
-t, --test	test configuration (can be also specified with start parameters)
-i	interactive mode
-v	increase verbosity
-q	decrease verbosity
-x	force execution of the server (remove socket file)
-b	start server in background (default)
-f	start server in foreground
--async	start server in async mode (for internal usage only, don't read configuration)
--timeout	timeout to wait for the server (for internal usage only, don't read configuration)
--str2sec <STRING>	convert time abbreviation format to seconds
-h, --help	display this help message
-V, --version	print the version (-V returns machine-readable short format)

Report bugs to <https://github.com/fail2ban/fail2ban/issues>

Les options de la commande **fail2ban-client** sont :

```
[root@centos8 ~]# fail2ban-client --help
```

Usage: fail2ban-client [OPTIONS] <COMMAND>

Fail2Ban v1.0.2 reads log file that contains password failure report and bans the corresponding IP addresses using firewall rules.

Options:

-c, --conf <DIR>	configuration directory
-s, --socket <FILE>	socket path
-p, --pidfile <FILE>	pidfile path
--pname <NAME>	name of the process (main thread) to identify instance (default fail2ban-server)
--loglevel <LEVEL>	logging level
--logtarget <TARGET>	logging target, use file-name or stdout, stderr, syslog or sysout.
--syslogsocket auto <FILE>	
-d	dump configuration. For debugging
--dp, --dump-pretty	dump the configuration using more human readable representation
-t, --test	test configuration (can be also specified with start parameters)
-i	interactive mode
-v	increase verbosity
-q	decrease verbosity
-x	force execution of the server (remove socket file)
-b	start server in background (default)
-f	start server in foreground
--async	start server in async mode (for internal usage only, don't read configuration)
--timeout	timeout to wait for the server (for internal usage only, don't read configuration)
--str2sec <STRING>	convert time abbreviation format to seconds
-h, --help	display this help message
-V, --version	print the version (-V returns machine-readable short format)

Command:

	BASIC
start	starts the server and the jails
restart	restarts the server
restart [--unban] [--if-exists] <JAIL>	restarts the jail <JAIL> (alias for 'reload --restart ... <JAIL>')

reload [--restart] [--unban] [--all]	reloads the configuration without restarting of the server, the option '--restart' activates completely restarting of affected jails, thereby can unban IP addresses (if option '--unban' specified)
reload [--restart] [--unban] [--if-exists] <JAIL>	reloads the jail <JAIL>, or restarts it (if option '--restart' specified)
stop	stops all jails and terminate the server
unban --all	unbans all IP addresses (in all jails and database)
unban <IP> ... <IP>	unbans <IP> (in all jails and database)
banned	return jails with banned IPs as dictionary
banned <IP> ... <IP>]	return list(s) of jails where given IP(s) are banned
status	gets the current status of the server
ping	tests if the server is alive
echo	for internal usage, returns back and outputs a given string
help	return this output
version	return the server version
LOGGING	
set loglevel <LEVEL>	sets logging level to <LEVEL>. Levels: CRITICAL, ERROR, WARNING, NOTICE, INFO, DEBUG, TRACEDEBUG, HEAVYDEBUG or corresponding

get loglevel	numeric value (50-5)
set logtarget <TARGET>	gets the logging level
	sets logging target to <TARGET>.
	Can be STDOUT, STDERR, SYSLOG,
	SYSTEMD-JOURNAL or a file
get logtarget	gets logging target
set syslogsocket auto <SOCKET>	sets the syslog socket path to
	auto or <SOCKET>. Only used if
	logtarget is SYSLOG
get syslogsocket	gets syslog socket path
flushlogs	flushes the logtarget if a file
	and reopens it. For log rotation.
DATABASE	
set dbfile <FILE>	set the location of fail2ban
	persistent datastore. Set to
	"None" to disable
get dbfile	get the location of fail2ban
	persistent datastore
set dbmaxmatches <INT>	sets the max number of matches
	stored in database per ticket
get dbmaxmatches	gets the max number of matches
	stored in database per ticket
set dbpurgeage <SECONDS>	sets the max age in <SECONDS> that
	history of bans will be kept
get dbpurgeage	gets the max age in seconds that
	history of bans will be kept
JAIL CONTROL	
add <JAIL> <BACKEND>	creates <JAIL> using <BACKEND>
start <JAIL>	starts the jail <JAIL>
stop <JAIL>	stops the jail <JAIL>. The jail is
	removed
status <JAIL> [FLAVOR]	gets the current status of <JAIL>,

with optional flavor or extended info

JAIL CONFIGURATION

set <JAIL> idle on off	sets the idle state of <JAIL>
set <JAIL> ignoreself true false	allows the ignoring of own IP addresses
set <JAIL> addignoreip <IP>	adds <IP> to the ignore list of <JAIL>
set <JAIL> delignoreip <IP>	removes <IP> from the ignore list of <JAIL>
set <JAIL> ignorecommand <VALUE>	sets ignorecommand of <JAIL>
set <JAIL> ignorecache <VALUE>	sets ignorecache of <JAIL>
set <JAIL> addlogpath <FILE> ['tail']	adds <FILE> to the monitoring list of <JAIL>, optionally starting at the 'tail' of the file (default 'head').
set <JAIL> dellogpath <FILE>	removes <FILE> from the monitoring list of <JAIL>
set <JAIL> logencoding <ENCODING>	sets the <ENCODING> of the log files for <JAIL>
set <JAIL> addjournalmatch <MATCH>	adds <MATCH> to the journal filter of <JAIL>
set <JAIL> deljournalmatch <MATCH>	removes <MATCH> from the journal filter of <JAIL>
set <JAIL> addfailregex <REGEX>	adds the regular expression <REGEX> which must match failures for <JAIL>
set <JAIL> delfailregex <INDEX>	removes the regular expression at <INDEX> for failregex
set <JAIL> addignoreregex <REGEX>	adds the regular expression <REGEX> which should match pattern to exclude for <JAIL>
set <JAIL> delignoreregex <INDEX>	removes the regular expression at

set <JAIL> findtime <TIME>	<INDEX> for ignoreregex sets the number of seconds <TIME> for which the filter will look back for <JAIL>
set <JAIL> bantime <TIME>	sets the number of seconds <TIME> a host will be banned for <JAIL>
set <JAIL> datepattern <PATTERN>	sets the <PATTERN> used to match date/times for <JAIL>
set <JAIL> usedns <VALUE>	sets the usedns mode for <JAIL>
set <JAIL> attempt <IP> [<failure1> ... <failureN>]	manually notify about <IP> failure
set <JAIL> banip <IP> ... <IP>	manually Ban <IP> for <JAIL>
set <JAIL> unbanip [--report-absent] <IP> ... <IP>	manually Unban <IP> in <JAIL>
set <JAIL> maxretry <RETRY>	sets the number of failures <RETRY> before banning the host for <JAIL>
set <JAIL> maxmatches <INT>	sets the max number of matches stored in memory per ticket in <JAIL>
set <JAIL> maxlines <LINES>	sets the number of <LINES> to buffer for regex search for <JAIL>
set <JAIL> addaction <ACT>[<PYTHONFILE> <JSONKWARGS>]	adds a new action named <ACT> for <JAIL>. Optionally for a Python based action, a <PYTHONFILE> and <JSONKWARGS> can be specified, else will be a Command Action
set <JAIL> delaction <ACT>	removes the action <ACT> from <JAIL>
COMMAND ACTION CONFIGURATION	
set <JAIL> action <ACT> actionstart <CMD>	sets the start command <CMD> of

```
set <JAIL> action <ACT> actionstop <CMD> the action <ACT> for <JAIL>
sets the stop command <CMD> of the
action <ACT> for <JAIL>
set <JAIL> action <ACT> actioncheck <CMD>
sets the check command <CMD> of
the action <ACT> for <JAIL>
set <JAIL> action <ACT> actionban <CMD> sets the ban command <CMD> of the
action <ACT> for <JAIL>
set <JAIL> action <ACT> actionunban <CMD>
sets the unban command <CMD> of
the action <ACT> for <JAIL>
set <JAIL> action <ACT> timeout <TIMEOUT>
sets <TIMEOUT> as the command
timeout in seconds for the action
<ACT> for <JAIL>
```

GENERAL ACTION CONFIGURATION

```
set <JAIL> action <ACT> <PROPERTY> <VALUE>
sets the <VALUE> of <PROPERTY> for
the action <ACT> for <JAIL>
set <JAIL> action <ACT> <METHOD>[ <JSONKWARGS>]
calls the <METHOD> with
<JSONKWARGS> for the action <ACT>
for <JAIL>
```

JAIL INFORMATION

```
get <JAIL> banned
return banned IPs of <JAIL>
get <JAIL> banned <IP> ... <IP>]
return 1 if IP is banned in <JAIL>
otherwise 0, or a list of 1/0 for
multiple IPs
get <JAIL> logpath
gets the list of the monitored
files for <JAIL>
get <JAIL> logencoding
gets the encoding of the log files
for <JAIL>
```

get <JAIL> journalmatch	gets the journal filter match for <JAIL>
get <JAIL> ignoreself	gets the current value of the ignoring the own IP addresses
get <JAIL> ignoreip	gets the list of ignored IP addresses for <JAIL>
get <JAIL> ignorecommand	gets ignorecommand of <JAIL>
get <JAIL> failregex	gets the list of regular expressions which matches the failures for <JAIL>
get <JAIL> ignoreregex	gets the list of regular expressions which matches patterns to ignore for <JAIL>
get <JAIL> findtime	gets the time for which the filter will look back for failures for <JAIL>
get <JAIL> bantime	gets the time a host is banned for <JAIL>
get <JAIL> datepattern	gets the pattern used to match date/times for <JAIL>
get <JAIL> usedns	gets the usedns setting for <JAIL>
get <JAIL> banip [<SEP> --with-time]	gets the list of of banned IP addresses for <JAIL>. Optionally the separator character ('<SEP>', default is space) or the option '--with-time' (printing the times of ban) may be specified. The IPs are ordered by end of ban.
get <JAIL> maxretry	gets the number of failures allowed for <JAIL>
get <JAIL> maxmatches	gets the max number of matches stored in memory per ticket in <JAIL>
get <JAIL> maxlines	gets the number of lines to buffer

get <JAIL> actions	for <JAIL> gets a list of actions for <JAIL>
COMMAND ACTION INFORMATION	
get <JAIL> action <ACT> actionstart	gets the start command for the action <ACT> for <JAIL>
get <JAIL> action <ACT> actionstop	gets the stop command for the action <ACT> for <JAIL>
get <JAIL> action <ACT> actioncheck	gets the check command for the action <ACT> for <JAIL>
get <JAIL> action <ACT> actionban	gets the ban command for the action <ACT> for <JAIL>
get <JAIL> action <ACT> actionunban	gets the unban command for the action <ACT> for <JAIL>
get <JAIL> action <ACT> timeout	gets the command timeout in seconds for the action <ACT> for <JAIL>
GENERAL ACTION INFORMATION	
get <JAIL> actionproperties <ACT>	gets a list of properties for the action <ACT> for <JAIL>
get <JAIL> actionmethods <ACT>	gets a list of methods for the action <ACT> for <JAIL>
get <JAIL> action <ACT> <PROPERTY>	gets the value of <PROPERTY> for the action <ACT> for <JAIL>

Report bugs to <https://github.com/fail2ban/fail2ban/issues>

Activer et Démarrer le Serveur

Pour prendre en compte la configuration dans le fichier **/etc/fail2ban/jail.local**, activez et démarrez le server :

```
[root@centos8 ~]# systemctl status fail2ban
```

- fail2ban.service - Fail2Ban Service

Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; disabled; vendor preset: disabled)

Active: inactive (dead)

Docs: man:fail2ban(1)

```
[root@centos8 ~]# systemctl enable fail2ban
```

Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /usr/lib/systemd/system/fail2ban.service.

```
[root@centos8 ~]# systemctl start fail2ban
```

```
[root@centos8 ~]# systemctl status fail2ban
```

- fail2ban.service - Fail2Ban Service

Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; vendor preset: disabled)

Active: active (running) since Wed 2024-10-02 16:31:33 CEST; 16s ago

Docs: man:fail2ban(1)

Process: 8319 ExecStartPre=/bin/mkdir -p /run/fail2ban (code=exited, status=0/SUCCESS)

Main PID: 8321 (fail2ban-server)

Tasks: 5 (limit: 100483)

Memory: 12.7M

CGroup: /system.slice/fail2ban.service

└─8321 /usr/bin/python3.6 -s /usr/bin/fail2ban-server -xf start

Oct 02 16:31:33 centos8.ittraining.loc systemd[1]: Starting Fail2Ban Service...

Oct 02 16:31:33 centos8.ittraining.loc systemd[1]: Started Fail2Ban Service.

Oct 02 16:31:34 centos8.ittraining.loc fail2ban-server[8321]: Server ready

```
[root@centos8 ~]# ps aux | grep fail2ban-server
```

```
root          8321  0.5  0.1 512900 24400 ?        Ssl  16:31   0:00 /usr/bin/python3.6 -s /usr/bin/fail2ban-server  
-xf start
```

```
root          8341  0.0  0.0  12216   1048 pts/0    S+   16:32   0:00 grep --color=auto fail2ban-server
```

Utiliser la Commande Fail2Ban-server

Pour connaître le status de Fail2Ban-server, saisissez la commande suivante :

```
[root@centos8 ~]# fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:  sshd
```

Il est aussi possible de se renseigner sur le statut d'un prison particulier :

```
[root@centos8 ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|   |- Currently failed: 0
|   |- Total failed:     0
|   `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
    |- Currently banned: 0
    |- Total banned:     0
    `-- Banned IP list:
```

La commande **fail2ban-client** peut être utilisée pour contrôler un prison :

```
[root@centos8 ~]# fail2ban-client stop sshd
Jail stopped

[root@centos8 ~]# fail2ban-client status sshd
2024-10-02 16:33:54,336 fail2ban [8353]: ERROR    NOK: ('sshd',)
Sorry but the jail 'sshd' does not exist

[root@centos8 ~]# fail2ban-client reload
OK
```

```
[root@centos8 ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|   |- Currently failed: 0
|   |- Total failed:     0
|   `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
    |- Currently banned: 0
    |- Total banned:     0
    `-- Banned IP list:
```

Ajouter un Prison

Modifiez maintenant votre fichier **/etc/fail2ban/jail.local** :

```
[root@centos8 ~]# vi /etc/fail2ban/jail.local
[root@centos8 ~]# cat /etc/fail2ban/jail.local
[DEFAULT]
ignoreip = 127.0.0.1 10.0.2.15
findtime = 3600
bantime = 86400
maxretry = 5

[sshd]
enabled = true

[apache-auth]
enabled = true
```

Appliquez la nouvelle configuration et constatez le résultat :

```
[root@centos8 ~]# fail2ban-client reload
```

OK

```
[root@centos8 ~]# fail2ban-client status
Status
|- Number of jail:      2
`- Jail list:  apache-auth, sshd
```

Balayage des Ports

LAB #5 - Utilisation de nmap et de netcat

nmap

Installation

Sous RHEL/CentOS 8, **nmap** n'est pas installé par défaut :

```
[root@centos8 ~]# which nmap
/usr/bin/which: no nmap in (/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/root/bin)
```

Installez donc nmap en utilisant yum :

```
[root@centos8 ~]# dnf install nmap
```

Options de la commande

Les options de cette commande sont :

```
[root@centos8 ~]# nmap --help
Nmap 7.92 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}

TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file

HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host

SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan

PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
```

- F: Fast mode - Scan fewer ports than the default scan
- r: Scan ports consecutively - don't randomize
- top-ports <number>: Scan <number> most common ports
- port-ratio <ratio>: Scan ports more common than <ratio>

SERVICE/VERSION DETECTION:

- sV: Probe open ports to determine service/version info
- version-intensity <level>: Set from 0 (light) to 9 (try all probes)
- version-light: Limit to most likely probes (intensity 2)
- version-all: Try every single probe (intensity 9)
- version-trace: Show detailed version scan activity (for debugging)

SCRIPT SCAN:

- sC: equivalent to --script=default
- script=<Lua scripts>: <Lua scripts> is a comma separated list of directories, script-files or script-categories
- script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
- script-args-file=filename: provide NSE script args in a file
- script-trace: Show all data sent and received
- script-updatedb: Update the script database.
- script-help=<Lua scripts>: Show help about scripts.
<Lua scripts> is a comma-separated list of script-files or script-categories.

OS DETECTION:

- O: Enable OS detection
- osscan-limit: Limit OS detection to promising targets
- osscan-guess: Guess OS more aggressively

TIMING AND PERFORMANCE:

- Options which take <time> are in seconds, or append 'ms' (milliseconds), 's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
- T<0-5>: Set timing template (higher is faster)
 - min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
 - min-parallelism/max-parallelism <numprobes>: Probe parallelization
 - min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies probe round trip time.
 - max-retries <tries>: Caps number of port scan probe retransmissions.

```
--host-timeout <time>: Give up on target after this long
--scan-delay/--max-scan-delay <time>: Adjust delay between probes
--min-rate <number>: Send packets no slower than <number> per second
--max-rate <number>: Send packets no faster than <number> per second
```

FIREWALL/IDS EVASION AND SPOOFING:

```
-f; --mtu <val>: fragment packets (optionally w/given MTU)
-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
-S <IP_Address>: Spoof source address
-e <iface>: Use specified interface
-g/--source-port <portnum>: Use given port number
--proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
--data <hex string>: Append a custom payload to sent packets
--data-string <string>: Append a custom ASCII string to sent packets
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
```

OUTPUT:

```
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
    and Grepable format, respectively, to the given filename.
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--noninteractive: Disable runtime interactions via keyboard
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
```

MISC:

- 6: Enable IPv6 scanning
- A: Enable OS detection, version detection, script scanning, and traceroute
- datadir <dirname>: Specify custom Nmap data file location
- send-eth/--send-ip: Send using raw ethernet frames or IP packets
- privileged: Assume that the user is fully privileged
- unprivileged: Assume the user lacks raw socket privileges
- V: Print version number
- h: Print this help summary page.

EXAMPLES:

```
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
```

SEE THE MAN PAGE (<https://nmap.org/book/man.html>) FOR MORE OPTIONS AND EXAMPLES

Utilisation

Pour connaître la liste des ports ouverts sur votre machine virtuelle, saisissez la commande suivante :

```
[root@centos8 ~]# nmap 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-02 16:58 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000011s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
631/tcp   open  ipp

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```



Important - Pour connaître les ports ouverts sur une machine distante, la procédure est identique sauf que vous devez utiliser l'adresse IP de votre cible.

Fichiers de Configuration

nmap utilise un fichier spécifique pour identifier les ports. Ce fichier est **/usr/share/nmap/nmap-services**:

```
[root@centos8 ~]# more /usr/share/nmap/nmap-services
# THIS FILE IS GENERATED AUTOMATICALLY FROM A MASTER - DO NOT EDIT.
# EDIT /nmap-private-dev/nmap-services-all IN SVN INSTEAD.
# Well known service port numbers -*- mode: fundamental; -*-
# From the Nmap Security Scanner ( https://nmap.org/ )
#
# $Id: nmap-services 38272 2021-08-06 18:05:30Z dmiller $
#
# Derived from IANA data and our own research
#
# This collection of service data is (C) 1996-2020 by Insecure.Com
# LLC. It is distributed under the Nmap Public Source license as
# provided in the LICENSE file of the source distribution or at
# https://svn.nmap.org/nmap/LICENSE . Note that this license
# requires you to license your own work under a compatible open source
# license. If you wish to embed Nmap technology into proprietary
# software, we sell alternative licenses (contact sales@insecure.com).
# Dozens of software vendors already license Nmap technology such as
# host discovery, port scanning, OS detection, and version detection.
# For more details, see https://nmap.org/book/man-legal.html
#
```

```
# Fields in this file are: Service name, portnum/protocol, open-frequency, optional comments
#
tcpmux 1/tcp 0.001995 # TCP Port Service Multiplexer [rfc-1078] | TCP Port Service Multiplexer
tcpmux 1/udp 0.001236 # TCP Port Service Multiplexer
compressnet 2/tcp 0.000013 # Management Utility
compressnet 2/udp 0.001845 # Management Utility
compressnet 3/tcp 0.001242 # Compression Process
compressnet 3/udp 0.001532 # Compression Process
unknown 4/tcp 0.000477
rje 5/tcp 0.000000 # Remote Job Entry
rje 5/udp 0.000593 # Remote Job Entry
unknown 6/tcp 0.000502
echo 7/sctp 0.000000
echo 7/tcp 0.004855
echo 7/udp 0.024679
unknown 8/tcp 0.000013
discard 9/sctp 0.000000 # sink null
discard 9/tcp 0.003764 # sink null
discard 9/udp 0.015733 # sink null
unknown 10/tcp 0.000063
sysstat 11/tcp 0.000075 # Active Users
sysstat 11/udp 0.000577 # Active Users
unknown 12/tcp 0.000063
daytime 13/tcp 0.003927
daytime 13/udp 0.004827
unknown 14/tcp 0.000038
netstat 15/tcp 0.000038
unknown 16/tcp 0.000050
qotd 17/tcp 0.002346 # Quote of the Day
qotd 17/udp 0.009209 # Quote of the Day
msp 18/tcp 0.000000 # Message Send Protocol | Message Send Protocol (historic)
msp 18/udp 0.000610 # Message Send Protocol
chargen 19/tcp 0.002559 # ttytst source Character Generator | Character Generator
chargen 19/udp 0.015865 # ttytst source Character Generator
```

```
ftp-data      20/sctp 0.000000      # File Transfer [Default Data] | FTP
--More-- (0%)
[q]
```

Le répertoire **/usr/share/nmap** contient d'autres fichiers importants :

```
[root@centos8 ~]# ls -l /usr/share/nmap
total 9312
-rw-r--r--. 1 root root  10834 Mar 22  2023 nmap.dtd
-rw-r--r--. 1 root root 767503 Mar 22  2023 nmap-mac-prefixes
-rw-r--r--. 1 root root 5033049 Mar 22  2023 nmap-os-db
-rw-r--r--. 1 root root  21253 Mar 22  2023 nmap-payloads
-rw-r--r--. 1 root root   6756 Mar 22  2023 nmap-protocols
-rw-r--r--. 1 root root  43755 Mar 22  2023 nmap-rpc
-rw-r--r--. 1 root root 2498555 Mar 22  2023 nmap-service-probes
-rw-r--r--. 1 root root 1002889 Mar 22  2023 nmap-services
-rw-r--r--. 1 root root  31936 Mar 22  2023 nmap.xsl
drwxr-xr-x. 3 root root   8192 Oct  2 16:57 nselib
-rw-r--r--. 1 root root  48627 Mar 22  2023 nse_main.lua
drwxr-xr-x. 2 root root  28672 Oct  2 16:57 scripts
```

Voici la liste des fichiers les plus importants :

Fichier	Description
/usr/share/nmap/nmap-protocols	Contient la liste des protocols reconnus par nmap .
/usr/share/nmap/nmap-service-probes	Contient les règles de balayage utilisées par nmap pour identifier le service actif sur un port donné.
/usr/share/nmap/nmap-mac-prefixes	Contient une liste de préfix d'adresses MAC par fabricant reconnu par nmap .
/usr/share/nmap/nmap-rpc	Contient une liste des services RPC reconnus par nmap .

Scripts

nmap utilise des scripts pour accomplir certaines tâches allant de la découverte simple de ports ouverts jusqu'à l'intrusion :

```
[root@centos8 ~]# ls /usr/share/nmap/scripts/
acarsd-info.nse          fcrdns.nse             https-redirect.nse
ms-sql-info.nse         smb-flood.nse          http-stored-xss.nse
address-info.nse        finger.nse             http-svn-enum.nse
ms-sql-ntlm-info.nse    smb-ls.nse             http-svn-info.nse
afp-brute.nse           fingerprint-strings.nse http-title.nse
ms-sql-query.nse        smb-mbenum.nse         http-tplink-dir-traversal.nse
afp-ls.nse              firewall.nse           http-trace.nse
ms-sql-tables.nse       smb-os-discovery.nse   http-traceroute.nse
afp-path-vuln.nse       firewall-bypass.nse    http-trane-info.nse
ms-sql-xp-cmdshell.nse  smb-print-text.nse     http-unsafe-output-escaping.nse
afp-serverinfo.nse      flume-master-info.nse  http-useragent-tester.nse
mtrace.nse              smb-protocols.nse      http-userdir-enum.nse
afp-showmount.nse       fox-info.nse           http-vhosts.nse
murmur-version.nse      smb-psexec.nse         http-virustotal.nse
ajp-auth.nse            freelancer-info.nse     http-vlcstreamer-ls.nse
mysql-audit.nse          smb-security-mode.nse  http-vmware-path-vuln.nse
ajp-brute.nse            ftp-anon.nse           http-vuln-cve2006-3392.nse
mysql-brute.nse          smb-server-stats.nse
ajp-headers.nse          ftp-bounce.nse
mysql-databases.nse      smb-system-info.nse
ajp-methods.nse          ftp-brute.nse
mysql-dump-hashes.nse    smb-vuln-conficker.nse
ajp-request.nse          ftp-libopie.nse
mysql-empty-password.nse smb-vuln-cve2009-3103.nse
allseeingeeye-info.nse   ftp-proftpd-backdoor.nse
mysql-enum.nse            smb-vuln-cve-2017-7494.nse
amqp-info.nse            ftp-syst.nse
mysql-info.nse            smb-vuln-ms06-025.nse
asn-query.nse            ftp-vsftpd-backdoor.nse
mysql-query.nse           smb-vuln-ms07-029.nse
auth-owners.nse          ftp-vuln-cve2010-4221.nse
mysql-users.nse           smb-vuln-ms08-067.nse
auth-spoof.nse            ganglia-info.nse
```

mysql-variables.nse	smb-vuln-ms10-054.nse	
backorifice-brute.nse	giop-info.nse	http-vuln-cve2009-3960.nse
mysql-vuln-cve2012-2122.nse	smb-vuln-ms10-061.nse	
backorifice-info.nse	gkrellm-info.nse	http-vuln-cve2010-0738.nse
nat-pmp-info.nse	smb-vuln-ms17-010.nse	
bacnet-info.nse	gopher-ls.nse	http-vuln-cve2010-2861.nse
nat-pmp-mapport.nse	smb-vuln-regsvc-dos.nse	
banner.nse	gpsd-info.nse	http-vuln-cve2011-3192.nse
nbd-info.nse	smb-vuln-webexec.nse	
bitcoin-getaddr.nse	hadoop-datanode-info.nse	http-vuln-cve2011-3368.nse
nbns-interfaces.nse	smb-webexec-exploit.nse	
bitcoin-info.nse	hadoop-jobtracker-info.nse	http-vuln-cve2012-1823.nse
nbstat.nse	smtp-brute.nse	
bitcoinrpc-info.nse	hadoop-namenode-info.nse	http-vuln-cve2013-0156.nse
ncp-enum-users.nse	smtp-commands.nse	
bittorrent-discovery.nse	hadoop-secondary-namenode-info.nse	http-vuln-cve2013-6786.nse
ncp-serverinfo.nse	smtp-enum-users.nse	
bjnp-discover.nse	hadoop-tasktracker-info.nse	http-vuln-cve2013-7091.nse
ndmp-fs-info.nse	smtp-ntlm-info.nse	
broadcast-ataoe-discover.nse	hbase-master-info.nse	http-vuln-cve2014-2126.nse
ndmp-version.nse	smtp-open-relay.nse	
broadcast-avahi-dos.nse	hbase-region-info.nse	http-vuln-cve2014-2127.nse
nessus-brute.nse	smtp-strangeport.nse	
broadcast-bjnp-discover.nse	hddtemp-info.nse	http-vuln-cve2014-2128.nse
nessus-xmlrpc-brute.nse	smtp-vuln-cve2010-4344.nse	
broadcast-db2-discover.nse	hnap-info.nse	http-vuln-cve2014-2129.nse
netbus-auth-bypass.nse	smtp-vuln-cve2011-1720.nse	
broadcast-dhcp6-discover.nse	hostmap-bfk.nse	http-vuln-cve2014-3704.nse
netbus-brute.nse	smtp-vuln-cve2011-1764.nse	
broadcast-dhcp-discover.nse	hostmap-crtsh.nse	http-vuln-cve2014-8877.nse
netbus-info.nse	sniffer-detect.nse	
broadcast-dns-service-discovery.nse	hostmap-robtx.nse	http-vuln-cve2015-1427.nse
netbus-version.nse	snmp-brute.nse	
broadcast-dropbox-listener.nse	http-adobe-coldfusion-apsa1301.nse	http-vuln-cve2015-1635.nse

nexpose-brute.nse	snmp-hh3c-logins.nse	
broadcast-eigrp-discovery.nse	http-affiliate-id.nse	http-vuln-cve2017-1001000.nse
nfs-ls.nse	snmp-info.nse	
broadcast-hid-discoveryd.nse	http-apache-negotiation.nse	http-vuln-cve2017-5638.nse
nfs-showmount.nse	snmp-interfaces.nse	
broadcast-igmp-discovery.nse	http-apache-server-status.nse	http-vuln-cve2017-5689.nse
nfs-statfs.nse	snmp-ios-config.nse	
broadcast-jenkins-discover.nse	http-aspnet-debug.nse	http-vuln-cve2017-8917.nse
nje-node-brute.nse	snmp-netstat.nse	
broadcast-listener.nse	http-auth-finder.nse	http-vuln-misfortune-cookie.nse
nje-pass-brute.nse	snmp-processes.nse	
broadcast-ms-sql-discover.nse	http-auth.nse	http-vuln-wnr1000-creds.nse
nntp-ntlm-info.nse	snmp-sysdescr.nse	
broadcast-netbios-master-browser.nse	http-avaya-ipoffice-users.nse	http-waf-detect.nse
nping-brute.nse	snmp-win32-services.nse	
broadcast-networker-discover.nse	http-awstatstotals-exec.nse	http-waf-fingerprint.nse
nrpe-enum.nse	snmp-win32-shares.nse	
broadcast-novell-locate.nse	http-axis2-dir-traversal.nse	http-webdav-scan.nse
ntp-info.nse	snmp-win32-software.nse	
broadcast-ospf2-discover.nse	http-backup-finder.nse	http-wordpress-brute.nse
ntp-monlist.nse	snmp-win32-users.nse	
broadcast-pc-anywhere.nse	http-barracuda-dir-traversal.nse	http-wordpress-enum.nse
omp2-brute.nse	socks-auth-info.nse	
broadcast-pc-duo.nse	http-bigip-cookie.nse	http-wordpress-users.nse
omp2-enum-targets.nse	socks-brute.nse	
broadcast-pim-discovery.nse	http-brute.nse	http-xssed.nse
omron-info.nse	socks-open-proxy.nse	
broadcast-ping.nse	http-cakephp-version.nse	iax2-brute.nse
openflow-info.nse	ssh2-enum-algos.nse	
broadcast-pppoe-discover.nse	http-chrono.nse	iax2-version.nse
openlookup-info.nse	ssh-auth-methods.nse	
broadcast-rip-discover.nse	http-cisco-anyconnect.nse	icap-info.nse
openvas-otp-brute.nse	ssh-brute.nse	
broadcast-ripng-discover.nse	http-coldfusion-subzero.nse	iec-identify.nse

openwebnet-discovery.nse	ssh-hostkey.nse	
broadcast-sonicwall-discover.nse	http-comments-displayer.nse	ike-version.nse
oracle-brute.nse	ssh-publickey-acceptance.nse	
broadcast-sybase-asa-discover.nse	http-config-backup.nse	imap-brute.nse
oracle-brute-stealth.nse	ssh-run.nse	
broadcast-tellstick-discover.nse	http-cookie-flags.nse	imap-capabilities.nse
oracle-enum-users.nse	sshv1.nse	
broadcast-upnp-info.nse	http-cors.nse	imap-ntlm-info.nse
oracle-sid-brute.nse	ssl-ccs-injection.nse	
broadcast-versant-locate.nse	http-cross-domain-policy.nse	impress-remote-discover.nse
oracle-tns-version.nse	ssl-cert-intaddr.nse	
broadcast-wake-on-lan.nse	http-csrf.nse	informix-brute.nse
ovs-agent-version.nse	ssl-cert.nse	
broadcast-wpad-discover.nse	http-date.nse	informix-query.nse
p2p-conficker.nse	ssl-date.nse	
broadcast-wsdd-discover.nse	http-default-accounts.nse	informix-tables.nse
path-mtu.nse	ssl-dh-params.nse	
broadcast-xdmcp-discover.nse	http-devframework.nse	ip-forwarding.nse
pcanywhere-brute.nse	ssl-enum-ciphers.nse	
cassandra-brute.nse	http-dlink-backdoor.nse	ip-geolocation-geoplugin.nse
pcworx-info.nse	ssl-heartbleed.nse	
cassandra-info.nse	http-dombased-xss.nse	ip-geolocation-ipinfodb.nse
pgsql-brute.nse	ssl-known-key.nse	
cccam-version.nse	http-domino-enum-passwords.nse	ip-geolocation-map-bing.nse
pjl-ready-message.nse	ssl-poodle.nse	
cics-enum.nse	http-drupal-enum.nse	ip-geolocation-map-google.nse
pop3-brute.nse	ssl2-drown.nse	
cics-info.nse	http-drupal-enum-users.nse	ip-geolocation-map-kml.nse
pop3-capabilities.nse	sslv2.nse	
cics-user-brute.nse	http-enum.nse	ip-geolocation-maxmind.nse
pop3-ntlm-info.nse	sstp-discover.nse	
cics-user-enum.nse	http-errors.nse	ip-https-discover.nse
port-states.nse	stun-info.nse	
citrix-brute-xml.nse	http-exif-spider.nse	ipidseq.nse

pptp-version.nse	stun-version.nse	
citrix-enum-apps.nse	http-favicon.nse	ipmi-brute.nse
puppet-naivesigning.nse	stuxnet-detect.nse	
citrix-enum-apps-xml.nse	http-feed.nse	ipmi-cipher-zero.nse
qconn-exec.nse	supermicro-ipmi-conf.nse	
citrix-enum-servers.nse	http-fetch.nse	ipmi-version.nse
qscan.nse	svn-brute.nse	
citrix-enum-servers-xml.nse	http-fileupload-exploiter.nse	ipv6-multicast-mld-list.nse
quake1-info.nse	targets-asn.nse	
clamav-exec.nse	http-form-brute.nse	ipv6-node-info.nse
quake3-info.nse	targets-ipv6-map4to6.nse	
clock-skew.nse	http-form-fuzzer.nse	ipv6-ra-flood.nse
quake3-master-getservers.nse	targets-ipv6-multicast-echo.nse	
coap-resources.nse	http-frontpage-login.nse	irc-botnet-channels.nse
rdp-enum-encryption.nse	targets-ipv6-multicast-invalid-dst.nse	
couchdb-databases.nse	http-generator.nse	irc-brute.nse
rdp-ntlm-info.nse	targets-ipv6-multicast-mld.nse	
couchdb-stats.nse	http-git.nse	irc-info.nse
rdp-vuln-ms12-020.nse	targets-ipv6-multicast-slaac.nse	
creds-summary.nse	http-gitweb-projects-enum.nse	irc-sasl-brute.nse
realvnc-auth-bypass.nse	targets-ipv6-wordlist.nse	
cups-info.nse	http-google-malware.nse	irc-unrealircd-backdoor.nse
redis-brute.nse	targets-sniffer.nse	
cups-queue-info.nse	http-grep.nse	iscsi-brute.nse
redis-info.nse	targets-traceroute.nse	
cvs-brute.nse	http-headers.nse	iscsi-info.nse
resolveall.nse	targets-xml.nse	
cvs-brute-repository.nse	http-hp-ilo-info.nse	isns-info.nse
reverse-index.nse	teamspeak2-version.nse	
daap-get-library.nse	http-huawei-hg5xx-vuln.nse	jdwp-exec.nse
rexec-brute.nse	telnet-brute.nse	
daytime.nse	http-icloud-findmyiphone.nse	jdwp-info.nse
rfc868-time.nse	telnet-encryption.nse	
db2-das-info.nse	http-icloud-sendmsg.nse	jdwp-inject.nse

riak-http-info.nse	telnet-ntlm-info.nse	
deluge-rpc-brute.nse	http-iis-short-name-brute.nse	jdwp-version.nse
rlogin-brute.nse	tftp-enum.nse	
dhcp-discover.nse	http-iis-webdav-vuln.nse	knx-gateway-discover.nse
rmi-dumpregistry.nse	tls-alpn.nse	
dicom-brute.nse	http-internal-ip-disclosure.nse	knx-gateway-info.nse
rmi-vuln-classloader.nse	tls-nextprotoneg.nse	
dicom-ping.nse	http-joomla-brute.nse	krb5-enum-users.nse
rpcap-brute.nse	tls-ticketbleed.nse	
dict-info.nse	http-jsonp-detection.nse	ldap-brute.nse
rpcap-info.nse	tn3270-screen.nse	
distcc-cve2004-2687.nse	http-litespeed-sourcecode-download.nse	ldap-novell-getpass.nse
rpc-grind.nse	tor-consensus-checker.nse	
dns-blacklist.nse	http-ls.nse	ldap-rootdse.nse
rpcinfo.nse	traceroute-geolocation.nse	
dns-brute.nse	http-majordomo2-dir-traversal.nse	ldap-search.nse
rsa-vuln-roca.nse	tso-brute.nse	
dns-cache-snoop.nse	http-malware-host.nse	lexmark-config.nse
rsync-brute.nse	tso-enum.nse	
dns-check-zone.nse	http-mcmp.nse	llmnr-resolve.nse
rsync-list-modules.nse	ubiquiti-discovery.nse	
dns-client-subnet-scan.nse	http-methods.nse	lltd-discovery.nse
rtsp-methods.nse	unittest.nse	
dns-fuzz.nse	http-method-tamper.nse	lu-enum.nse
rtsp-url-brute.nse	unusual-port.nse	
dns-ip6-arpa-scan.nse	http-mobileversion-checker.nse	maxdb-info.nse
rusers.nse	upnp-info.nse	
dns-nsec3-enum.nse	http-ntlm-info.nse	mcafee-epo-agent.nse
s7-info.nse	uptime-agent-info.nse	
dns-nsec-enum.nse	http-open-proxy.nse	membase-brute.nse
samba-vuln-cve-2012-1182.nse	url-snarf.nse	
dns-nsid.nse	http-open-redirect.nse	membase-http-info.nse
script.db	ventrilo-info.nse	
dns-random-srcport.nse	http-passwd.nse	memcached-info.nse

servicetags.nse	versant-info.nse	
dns-random-txid.nse	http-phpmyadmin-dir-traversal.nse	metasploit-info.nse
shodan-api.nse	vmauthd-brute.nse	
dns-recursion.nse	http-phpself-xss.nse	metasploit-msgrpc-brute.nse
sip-brute.nse	vmware-version.nse	
dns-service-discovery.nse	http-php-version.nse	metasploit-xmlrpc-brute.nse
sip-call-spoof.nse	vnc-brute.nse	
dns-srv-enum.nse	http-proxy-brute.nse	mikrotik-routeros-brute.nse
sip-enum-users.nse	vnc-info.nse	
dns-update.nse	http-put.nse	mmouse-brute.nse
sip-methods.nse	vnc-title.nse	
dns-zeustracker.nse	http-qnap-nas-info.nse	mmouse-exec.nse
skypev2-version.nse	voldemort-info.nse	
dns-zone-transfer.nse	http-referer-checker.nse	modbus-discover.nse
smb2-capabilities.nse	vtam-enum.nse	
docker-version.nse	http-rfi-spider.nse	mongodb-brute.nse
smb2-security-mode.nse	vulners.nse	
domcon-brute.nse	http-robots.txt.nse	mongodb-databases.nse
smb2-time.nse	vuze-dht-info.nse	
domcon-cmd.nse	http-robtex-reverse-ip.nse	mongodb-info.nse
smb2-vuln-uptime.nse	wdb-version.nse	
domino-enum-users.nse	http-robtex-shared-ns.nse	mqtt-subscribe.nse
smb-brute.nse	weblogic-t3-info.nse	
dpap-brute.nse	http-sap-netweaver-leak.nse	mrinfo.nse
smb-double-pulsar-backdoor.nse	whois-domain.nse	
drda-brute.nse	http-security-headers.nse	msrpc-enum.nse
smb-enum-domains.nse	whois-ip.nse	
drda-info.nse	http-server-header.nse	ms-sql-brute.nse
smb-enum-groups.nse	wsdd-discover.nse	
duplicates.nse	http-shellshock.nse	ms-sql-config.nse
smb-enum-processes.nse	x11-access.nse	
eap-info.nse	http-sitemap-generator.nse	ms-sql-dac.nse
smb-enum-services.nse	xdmcp-discover.nse	
enip-info.nse	http-slowloris-check.nse	ms-sql-dump-hashes.nse

smb-enum-sessions.nse	xmlrpc-methods.nse	
epmd-info.nse	http-slowloris.nse	ms-sql-empty-password.nse
smb-enum-shares.nse	xmpp-brute.nse	
eppc-enum-processes.nse	http-sql-injection.nse	ms-sql-hasdbaccess.nse
smb-enum-users.nse	xmpp-info.nse	

Les scripts sont regroupés dans des catégories : **auth**, **broadcast**, **brute**, **default**, **discovery**, **dos**, **exploit**, **external**, **fuzzer**, **intrusive**, **malware**, **safe**, **version** and **vuln**.



Important - Pour plus d'informations concernant ces catégories, consultez cette [page](#).

La catégorie la plus utilisée est **default** qui est appelée par l'utilisation de l'option **-sC**. Cette catégorie contient une liste de scripts par défaut.

```
[root@centos8 ~]# nmap -v -sC localhost
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-02 17:02 CEST
NSE: Loaded 125 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:02
Completed NSE at 17:02, 0.00s elapsed
Initiating NSE at 17:02
Completed NSE at 17:02, 0.00s elapsed
Initiating SYN Stealth Scan at 17:02
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 111/tcp on 127.0.0.1
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 631/tcp on 127.0.0.1
Completed SYN Stealth Scan at 17:02, 0.04s elapsed (1000 total ports)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 17:02
```

```
Completed NSE at 17:02, 0.38s elapsed
Initiating NSE at 17:02
Completed NSE at 17:02, 0.00s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000011s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|   3072 11:65:f2:24:6b:e1:f6:dc:31:be:12:28:5a:90:46:84 (RSA)
|   256 9d:99:66:02:fd:cb:cc:58:00:79:38:64:28:55:43:34 (ECDSA)
|_  256 d9:8a:d9:46:96:c1:5a:ad:78:f7:bc:38:d1:d7:06:72 (ED25519)
80/tcp    open  http
| http-methods:
|   Supported Methods: GET POST OPTIONS HEAD TRACE
|_  Potentially risky methods: TRACE
|_http-title: This is a test
111/tcp   open  rpcbind
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp    rpcbind
|   100000  2,3,4        111/udp    rpcbind
|   100000  3,4          111/tcp6   rpcbind
|_  100000  3,4          111/udp6   rpcbind
631/tcp   open  ipp
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Home - CUPS 2.2.6
| ssl-cert: Subject:
commonName=centos8.ittraining.loc/organizationName=centos8.ittraining.loc/stateOrProvinceName=Unknown/countryName
=GB
| Issuer:
commonName=centos8.ittraining.loc/organizationName=centos8.ittraining.loc/stateOrProvinceName=Unknown/countryName
```

```
=GB
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-10-02T15:02:15
| Not valid after: 2034-09-30T15:02:15
| MD5: 3dbd 816b b33c 9bd8 d9f0 f0c4 8204 a60b
|_SHA-1: 9d58 dda8 a024 41db 63cb bb85 fea9 86c1 6238 399b
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ssl-date: TLS randomness does not represent time
```

```
NSE: Script Post-scanning.
Initiating NSE at 17:02
Completed NSE at 17:02, 0.00s elapsed
Initiating NSE at 17:02
Completed NSE at 17:02, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.82 seconds
Raw packets sent: 1000 (44.000KB) | Rcvd: 2004 (84.176KB)
```

Attention - La catégorie par défaut **default** contient certains scripts de la catégorie **intrusive**. Vous ne devez donc jamais utiliser cette option sur un réseau sans avoir obtenu un accord au préalable.

netcat

netcat est un couteau suisse. Il permet non seulement de scanner des ports mais aussi de lancer la connexion lors de la découverte d'un port ouvert.

Options de la commande

Les options de cette commande sont :

```
[root@centos8 ~]# nc --help
Ncat 7.92 ( https://nmap.org/ncat )
Usage: ncat [options] [hostname] [port]

Options taking a time assume seconds. Append 'ms' for milliseconds,
's' for seconds, 'm' for minutes, or 'h' for hours (e.g. 500ms).
  -4                      Use IPv4 only
  -6                      Use IPv6 only
  -U, --unixsock          Use Unix domain sockets only
  --vsock                Use vsock sockets only
  -C, --crlf              Use CRLF for EOL sequence
  -c, --sh-exec <command> Executes the given command via /bin/sh
  -e, --exec <command>    Executes the given command
  --lua-exec <filename>   Executes the given Lua script
  -g hop1[,hop2,...]      Loose source routing hop points (8 max)
  -G <n>                  Loose source routing hop pointer (4, 8, 12, ...)
  -m, --max-conns <n>     Maximum <n> simultaneous connections
  -h, --help              Display this help screen
  -d, --delay <time>      Wait between read/writes
  -o, --output <filename> Dump session data to a file
  -x, --hex-dump <filename> Dump session data as hex to a file
  -i, --idle-timeout <time> Idle read/write timeout
  -p, --source-port port  Specify source port to use
  -s, --source addr       Specify source address to use (doesn't affect -l)
  -l, --listen            Bind and listen for incoming connections
  -k, --keep-open         Accept multiple connections in listen mode
  -n, --nodns             Do not resolve hostnames via DNS
  -t, --telnet            Answer Telnet negotiations
  -u, --udp               Use UDP instead of default TCP
```

--sctp	Use SCTP instead of default TCP
-v, --verbose	Set verbosity level (can be used several times)
-w, --wait <time>	Connect timeout
-z	Zero-I/O mode, report connection status only
--append-output	Append rather than clobber specified output files
--send-only	Only send data, ignoring received; quit on EOF
--recv-only	Only receive data, never send anything
--no-shutdown	Continue half-duplex when receiving EOF on stdin
--allow	Allow only given hosts to connect to Ncat
--allowfile	A file of hosts allowed to connect to Ncat
--deny	Deny given hosts from connecting to Ncat
--denyfile	A file of hosts denied from connecting to Ncat
--broker	Enable Ncat's connection brokering mode
--chat	Start a simple Ncat chat server
--proxy <addr[:port]>	Specify address of host to proxy through
--proxy-type <type>	Specify proxy type ("http", "socks4", "socks5")
--proxy-auth <auth>	Authenticate with HTTP or SOCKS proxy server
--proxy-dns <type>	Specify where to resolve proxy destination
--ssl	Connect or listen with SSL
--ssl-cert	Specify SSL certificate file (PEM) for listening
--ssl-key	Specify SSL private key (PEM) for listening
--ssl-verify	Verify trust and domain name of certificates
--ssl-trustfile	PEM file containing trusted SSL certificates
--ssl-ciphers	Cipherlist containing SSL ciphers to use
--ssl-servername	Request distinct server name (SNI)
--ssl-alpn	ALPN protocol list to use
--version	Display Ncat's version information and exit

See the ncat(1) manpage for full options, descriptions and usage examples

Utilisation

Dans l'exemple qui suite, un scan est lancé sur le port 80 puis sur le port 25 :

```
[root@centos8 ~]# nc 127.0.0.1 80 -w 1 -vv
Ncat: Version 7.92 ( https://nmap.org/ncat )
NCAT DEBUG: Using system default trusted CA certificates and those in /usr/share/ncat/ca-bundle.crt.
NCAT DEBUG: Unable to load trusted CA certificates from /usr/share/ncat/ca-bundle.crt: error:02001002:system
library:fopen:No such file or directory
libnsock nsock_iod_new2(): nsock_iod_new (IOD #1)
libnsock nsock_connect_tcp(): TCP connection requested to 127.0.0.1:80 (IOD #1) EID 8
libnsock nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [127.0.0.1:80]
Ncat: Connected to 127.0.0.1:80.
libnsock nsock_iod_new2(): nsock_iod_new (IOD #2)
libnsock nsock_read(): Read request from IOD #1 [127.0.0.1:80] (timeout: -1ms) EID 18
libnsock nsock_readbytes(): Read request for 0 bytes from IOD #2 [peer unspecified] EID 26
^C

[root@centos8 ~]# nc 127.0.0.1 25 -w 1 -vv
Ncat: Version 7.92 ( https://nmap.org/ncat )
NCAT DEBUG: Using system default trusted CA certificates and those in /usr/share/ncat/ca-bundle.crt.
NCAT DEBUG: Unable to load trusted CA certificates from /usr/share/ncat/ca-bundle.crt: error:02001002:system
library:fopen:No such file or directory
libnsock nsock_iod_new2(): nsock_iod_new (IOD #1)
libnsock nsock_connect_tcp(): TCP connection requested to 127.0.0.1:25 (IOD #1) EID 8
libnsock nsock_trace_handler_callback(): Callback: CONNECT ERROR [Connection refused (111)] for EID 8
[127.0.0.1:25]
Ncat: Connection refused.
```



Important - Notez que **netcat** se connecte au port 25 qui est ouvert.

LAB #6 - Mise en place du Système de Détection et de Prévention d'Intrusion Portsentry

Portsentry est un **Système de Détection et de Prévention** d'Intrusion (SDPI) qui surveille les requêtes entrantes et en cas d'anomalie bloque l'adresse

IP de l'attaquant en inscrivant une règle dans le pare-feu NetFilter (Iptables).

Installation

Sous RHEL/CentOS 8, **portsentry** n'est pas installé par défaut. Qui plus est **portsentry** ne se trouve pas dans les dépôts standards. Installez donc le paquet **portsentry-1.2-1.el5.x86_64.rpm** à partir de l'URL ci-dessous :

```
[root@centos8 ~]# rpm -ivh
https://www.dropbox.com/scl/fi/vliniimmjkvj0kx6xllmt/portsentry-1.2-1.el5.x86_64.rpm?rlkey=zyyvvd2a1ksi27y2v2maf6
fuh&st=kdgnkvfe
[1] 9629
[root@centos8 ~]# Retrieving
https://www.dropbox.com/scl/fi/vliniimmjkvj0kx6xllmt/portsentry-1.2-1.el5.x86_64.rpm?rlkey=zyyvvd2a1ksi27y2v2maf6
fuh
warning: /var/tmp/rpm-tmp.FP6pPg: Header V3 DSA/SHA1 Signature, key ID 4026433f: NOKEY
Verifying... ##### [100%]
Preparing... ##### [100%]
Updating / installing...
  1:portsentry-1.2-1.el5 ##### [100%]
^C
```

Configuration

Téléchargez le fichier **/etc/portsentry/portsentry.conf** :

```
[root@centos8 ~]# wget
https://www.dropbox.com/scl/fi/vaz781ja31t14cd95yc8p/portsentry.conf?rlkey=0bkalz8bjn7zsimp03xine5fz&st=ee9d9vzs
[1] 9676
[root@centos8 ~]#
Redirecting output to 'wget-log'.
^C
```

```
[1]+  Done                  wget
https://www.dropbox.com/scl/fi/vaz781ja31t14cd95yc8p/portsentry.conf?rlkey=0bkalz8bjn7zsimp03xine5fz

[root@centos8 ~]# mv 'portsentry.conf?rlkey=0bkalz8bjn7zsimp03xine5fz' /etc/portsentry/portsentry.conf
mv: overwrite '/etc/portsentry/portsentry.conf'? y
```

Pour rendre le service SysVinit compatible avec Systemd, éditez le fichier **/etc/init.d/portsentry** en supprimant la ligne **11** :

```
[root@centos8 ~]# nl /etc/init.d/portsentry
 1  #!/bin/bash
 2  #
 3  # Startup script for the Portsentry portscan detector
 4  #
 5  # chkconfig: 345 98 02
 6  # description: PortSentry Port Scan Detector is part of the Abacus Project \
 7  #               suite of tools. The Abacus Project is an initiative to release \
 8  #               low-maintenance, generic, and reliable host based intrusion \
 9  #               detection software to the Internet community.
10  # processname: portsentry
11  # pidfile: /var/run/portsentry.pid <-----SUPPRIMEZ cette ligne
12  # config: /etc/portsentry/portsentry.conf
13  # Source function library.

...
```

Puis ajoutez la ligne **80** :

```
...
77  stop() {
78      echo -n "Stopping $prog: "
79      killproc portsentry
80      killall portsentry <-----AJOUTEZ cette ligne
81      RETVAL=$?
82      echo
83      [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/portsentry
```

```
84 }
85 # See how we were called.
...
```

Exécutez la commande suivante pour prendre en compte les modifications :

```
[root@centos8 ~]# systemctl daemon-reload
```

Utilisation

Démarrez le service **portsentry** :

```
[root@centos8 ~]# systemctl restart portsentry
```

```
[root@centos8 ~]# systemctl status portsentry
```

● portsentry.service - SYSV: PortSentry Port Scan Detector is part of the Abacus Project suite of tools. The Abacus Project is an initiative to release low-maintenance, generic, and reliable host based intrusi>

Loaded: loaded (/etc/rc.d/init.d/portsentry; generated)

Active: active (running) since Wed 2024-10-02 17:37:33 CEST; 4s ago

Docs: man:systemd-sysv-generator(8)

Process: 10142 ExecStart=/etc/rc.d/init.d/portsentry start (code=exited, status=0/SUCCESS)

Tasks: 6 (limit: 100483)

Memory: 1.5M

CGroup: /system.slice/portsentry.service

```
├─ 9907 /usr/sbin/portsentry -atcp
├─ 9909 /usr/sbin/portsentry -audp
├─10086 /usr/sbin/portsentry -atcp
├─10088 /usr/sbin/portsentry -audp
├─10169 /usr/sbin/portsentry -atcp
└─10171 /usr/sbin/portsentry -audp
```

```
Oct 02 17:37:33 centos8.ittraining.loc portsentry[10169]: adminalert: Advanced Stealth scan detection mode
```

```
activated. Ignored TCP port: 25
Oct 02 17:37:33 centos8.ittraining.loc portsentry[10169]: adminalert: Advanced Stealth scan detection mode
activated. Ignored TCP port: 53
Oct 02 17:37:33 centos8.ittraining.loc portsentry[10169]: adminalert: Advanced Stealth scan detection mode
activated. Ignored TCP port: 80
Oct 02 17:37:33 centos8.ittraining.loc portsentry[10169]: adminalert: Advanced Stealth scan detection mode
activated. Ignored TCP port: 110
Oct 02 17:37:33 centos8.ittraining.loc portsentry[10169]: adminalert: Advanced Stealth scan detection mode
activated. Ignored TCP port: 113
Oct 02 17:37:33 centos8.ittraining.loc portsentry[10169]: adminalert: Advanced Stealth scan detection mode
activated. Ignored TCP port: 137
Oct 02 17:37:33 centos8.ittraining.loc portsentry[10169]: adminalert: Advanced Stealth scan detection mode
activated. Ignored TCP port: 138
Oct 02 17:37:33 centos8.ittraining.loc portsentry[10169]: adminalert: Advanced Stealth scan detection mode
activated. Ignored TCP port: 139
Oct 02 17:37:33 centos8.ittraining.loc portsentry[10169]: adminalert: Advanced Stealth scan detection mode
activated. Ignored TCP port: 443
Oct 02 17:37:33 centos8.ittraining.loc portsentry[10169]: adminalert: PortSentry is now active and listening.
```

```
[root@centos8 ~]# ps aux | grep portsentry
root      9907  0.0  0.0   4468   100 ?        Ss   17:23   0:00 /usr/sbin/portsentry -atcp
root      9909  0.0  0.0   4468   100 ?        Ss   17:23   0:00 /usr/sbin/portsentry -audp
root     10086  0.1  0.0   4468    96 ?        Ss   17:35   0:00 /usr/sbin/portsentry -atcp
root     10088  0.1  0.0   4468   100 ?        Ss   17:35   0:00 /usr/sbin/portsentry -audp
root     10169  0.2  0.0   4468   100 ?        Ss   17:37   0:00 /usr/sbin/portsentry -atcp
root     10171  0.2  0.0   4468    96 ?        Ss   17:37   0:00 /usr/sbin/portsentry -audp
root     10192  0.0  0.0  12216  1208 pts/0    S+   17:39   0:00 grep --color=auto portsentry
```

Editez le fichier **/etc/portsentry/portsentry.ignore** en supprimant la ligne contenant votre adresse IP 10.0.2.45 :

```
[root@centos8 ~]# vi /etc/portsentry/portsentry.ignore
```

```
[root@centos8 ~]# cat /etc/portsentry/portsentry.ignore
# Put hosts in here you never want blocked. This includes the IP addresses
```

```
# of all local interfaces on the protected host (i.e virtual host, mult-home)
# Keep 127.0.0.1 and 0.0.0.0 to keep people from playing games.
#
# PortSentry can support full netmasks for networks as well. Format is:
#
# <IP Address>/<Netmask>
#
# Example:
#
# 192.168.2.0/24
# 192.168.0.0/16
# 192.168.2.1/32
# Etc.
#
# If you don't supply a netmask it is assumed to be 32 bits.
#
#

127.0.0.1/32
0.0.0.0
#####
# Do NOT edit below this line, if you      #
# do, your changes will be lost when      #
# portsentry is restarted via the          #
# initscript. Make all changes above      #
# this box.                                #
#####

# Exclude all local interfaces
fe80::8af3:5782:3598:aa0f
127.0.0.1
::1
192.168.122.1
```

```
# Exclude the default gateway(s)
10.0.2.1

# Exclude the nameservers
8.8.8.8

# And last but not least...
0.0.0.0
```

Installez maintenant le paquet **mailx** :

```
[root@centos8 ~]# dnf install mailx
```

Sans re-démarrez le service portsentry, lancez un scan des ports avec nmap :

```
[root@centos8 ~]# nmap -sC 10.0.2.45
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-02 17:45 CEST
^C
[root@centos8 ~]#
```



Important - Notez l'utilisation de la combinaison de touches **CtrlC** pour arrêter nmap.

Consultez les règles d'iptables :

```
[root@centos8 ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
DROP       all  --  centos8.ittraining.loc anywhere <-----REGARDEZ cette ligne.
LIBVIRT_INP all  --  anywhere              anywhere
```

Chain FORWARD (policy ACCEPT)

target	prot	opt	source	destination
LIBVIRT_FWX	all	--	anywhere	anywhere
LIBVIRT_FWI	all	--	anywhere	anywhere
LIBVIRT_FW0	all	--	anywhere	anywhere

Chain OUTPUT (policy ACCEPT)

target	prot	opt	source	destination
LIBVIRT_OUT	all	--	anywhere	anywhere

Chain LIBVIRT_INP (1 references)

target	prot	opt	source	destination	
ACCEPT	udp	--	anywhere	anywhere	udp dpt:domain
ACCEPT	tcp	--	anywhere	anywhere	tcp dpt:domain
ACCEPT	udp	--	anywhere	anywhere	udp dpt:bootps
ACCEPT	tcp	--	anywhere	anywhere	tcp dpt:bootps

Chain LIBVIRT_OUT (1 references)

target	prot	opt	source	destination	
ACCEPT	udp	--	anywhere	anywhere	udp dpt:domain
ACCEPT	tcp	--	anywhere	anywhere	tcp dpt:domain
ACCEPT	udp	--	anywhere	anywhere	udp dpt:bootpc
ACCEPT	tcp	--	anywhere	anywhere	tcp dpt:bootpc

Chain LIBVIRT_FW0 (1 references)

target	prot	opt	source	destination	
ACCEPT	all	--	192.168.122.0/24	anywhere	
REJECT	all	--	anywhere	anywhere	reject-with icmp-port-unreachable

Chain LIBVIRT_FWI (1 references)

target	prot	opt	source	destination	
ACCEPT	all	--	anywhere	192.168.122.0/24	ctstate RELATED,ESTABLISHED
REJECT	all	--	anywhere	anywhere	reject-with icmp-port-unreachable

```
Chain LIBVIRT_FWX (1 references)
target      prot opt source                destination
ACCEPT      all  --  anywhere              anywhere
```

Pour nettoyer la règle, re-démarrez le service **firewalld** :

```
[root@centos8 ~]# systemctl restart firewalld
```

Système de Fichiers

LAB #7 - Mise en place du File Integrity Checker Afick

Présentation

Afick (Another File Intergrity Checker) est un programme “contrôleur d'intégrité des fichiers” : un logiciel dédié à la sécurité informatique, analogue au très connu **tripwire**. Il permet de suivre les modifications des systèmes de fichiers, et en particulier de détecter les intrusions. Il fonctionne en créant une base de données stockant des informations concernant le système de fichiers d'un serveur puis en vérifiant périodiquement le système de fichiers contre cette base afin de vous prévenir de toute modification éventuelle. Pour cette raison, il convient d'installer afick sur le serveur au plus tôt.

Installation

Téléchargez la dernière version d'Afick :

```
[root@centos8 ~]# wget https://sourceforge.net/projects/afick/files/afick/3.8.1/afick-3.8.1-1.noarch.rpm
```

Pour installer **Afick**, utilisez la commande suivante :

```
[root@centos8 ~]# dnf localinstall afick-3.8.1-1.noarch.rpm --nogpgcheck
```

Configuration

La configuration d'Afick est contenu dans le fichier **/etc/afick.conf**.

Dans ce fichier, plusieurs sections nous intéressent :

La Section Directives

```
#####  
# directives section  
#####  
# binary values can be : yes/1/true or no/0/false  
# database : name with full path to database file  
database:=/var/lib/afick/afick  
# history : full path to history file  
history := /var/lib/afick/history  
# archive : full path to directory for archived results  
archive := /var/lib/afick/archive  
# report_url : where to send the result : stdout/stderr/null  
report_url := stdout  
# report_syslog : send output to syslog ?  
report_syslog := no  
# mask_sysupdate : report packages update  
mask_sysupdate := no  
# verbose : (obsolete) boolean value for debugging messages  
# use debug parameter below  
verbose := no  
# debug : set a level of debugging messages, from 0 (none) to 4 (full)  
debug := 0  
# warn_dead_symlinks : boolean : if set, warn about dead symlinks  
warn_dead_symlinks := no  
# follow_symlinks : boolean : if set, do checksum on target file (else on target file name)
```

```
follow_symlinks := no
# allow_overload : boolean : if set, allow to overload rules (the last rule wins), else put a warning
allow_overload := yes
# report_context : boolean : if set, display all changed attributes, not just those selected by rules
report_context := no
# report_full_newdel : boolean : if set, report all changes, if not set, report only a summary on top directories
report_full_newdel := no
# report_summary : boolean ; if set, report the summary section
report_summary := yes
# warn_missing_file : boolean : is set, warn about selected files (in this config), which does not exist
warn_missing_file := no
# running_files : boolean : if set, warn about files changed during a program run
running_files := yes
# timing : boolean : if set, print timing statistics about the job
timing := yes
# ignore_case : boolean : if set, ignore case on file name
ignore_case := no
# max_checksum_size : numeric : only compute checksum on first max_checksum_size bytes ( 0 means unlimited)
max_checksum_size := 10000000
# allow_relativepath : boolean : if set, afick files, config and databases are stored as relative path
allow_relativepath := 0
# utc_time : boolean; if set display date in utc time, else in local time
utc_time := 0

# only_suffix : list of suffix to scan (and just this ones) : is empty (disabled) by default
# not very usefull on unix, but is ok on windows
# this will speed up the scan, but with a lesser security
# only_suffix :=

# the 3 next directives : exclude_suffix exclude_prefix exclude_re
# can be written on several lines
# exclude_suffix : list of suffixes to ignore
# text files
exclude_suffix := log LOG html htm HTM txt TXT xml
```

```
# help files
exclude_suffix := hlp pod chm
# old files
exclude_suffix := tmp old bak
# fonts
exclude_suffix := fon ttf TTF
# images
exclude_suffix := bmp BMP jpg JPG gif png ico
# audio
exclude_suffix := wav WAV mp3 avi
# python
exclude_suffix := pyc

# exclude_prefix : list of prefixes to ignore
exclude_prefix := __pycache__

# exclude_re : a file pattern (using regex syntax) to ignore (apply on full path)
# one pattern by line
#exclude_re :=
```

Cette section définit les directives globales et notamment :

- l'emplacement de la base de données

```
database:=/var/lib/afick/afick
```



Important - Veuillez à sauvegarder régulièrement votre base de données. En effet, dans le cas où votre système est compromis, sans sauvegarde de votre base, vous ne serez plus certain de l'exactitude de cette dernière.

- l'exclusion de certaines extensions de la vérification

```
exclude_suffix := log LOG html htm HTM txt TXT xml
```

La Section Alias

```
#####  
# alias section  
#####  
# action : a list of item to check :  
# md5 : md5 checksum  
# sha1 : sha-1 checksum  
# sha256 : sha-256 checksum  
# sha512 : sha-512 checksum  
# d : device  
# i : inode  
# p : permissions  
# n : number of links  
# u : user  
# g : group  
# s : size  
# b : number of blocks  
# m : mtime  
# c : ctime  
# a : atime  
# acl : acl  
  
#all:    p+d+i+n+u+g+s+b+m+c+md5+acl  
#R:      p+d+i+n+u+g+s+m+c+md5  
#L:      p+d+i+n+u+g  
#P:      p+n+u+g+s+md5  
#E:      ''  
  
# action alias may be configured with
```

```
# your_alias = another_alias|item[+item][-item]
# all is a pre-defined alias for all items except "a"
DIR = p+i+n+u+g
ETC = p+d+u+g+s+md5
Logs = p+n+u+g
MyRule = p+d+n+u+g+s+b+md5
```

Cette partie du fichier de configuration détaille les combinaisons de vérifications de fichiers à réaliser :

```
DIR=p+i+n+u+g
ETC = p+d+i+u+g+s+md5
Logs = p+n+u+g
MyRule = p+d+n+u+g+s+b+md5
```

Les options détaillées sont :

Option	Description
md5	Vérifie la somme de contrôle md5 du contenu du fichier
sha1	Vérifie la somme de contrôle sha1 du contenu du fichier
d	Vérifie pour un périphérique son "major number" et son "minor number"
i	Vérifie le numéro d'inode
p	Vérifie les droits d'accès au fichier
n	Vérifie le nombre de liens
u	Vérifie l'utilisateur propriétaire du fichier
g	Vérifie le groupe propriétaire du fichier
s	Vérifie la taille du fichier
b	Vérifie le nombre de blocs alloués au fichier
m	Vérifie la date de la dernière modification du contenu du fichier
c	Vérifie la date de la dernière modification de l'inode
a	Vérifie la date du dernier accès

La Section File

```
#####
# file section
#####
# 3 syntaxe are available :
# file action
#     to scan a file/directory with "action" parameters
# ! file
#     to remove file from scan
# = directory action
#     to scan the directory but not sub-directories
# file with blank character have to be quoted
#
# action is the list of attribute used to detect a change

= /  DIR

/bin    MyRule

/boot   MyRule
# ! /boot/map
# ! /boot/System.map

/dev p+n
# ! /dev/.udev/db
# ! /dev/.udev/failed
# ! /dev/.udev/names
# ! /dev/.udev/watch
! /dev/bsg
! /dev/bus
! /dev/pts
! /dev/shm
```

```
# to avoid problems with pending usb
# = /dev/scsi p+n

/etc      ETC
/etc/mtab ETC - md5 - s
/etc/adjtime ETC - md5 -s
# /etc/aliases.db ETC - md5 -s
# /etc/mail/statistics ETC - md5 -s
/etc/motd ETC
# /etc/ntp/drift ETC - md5 -s
# /etc/urpmi/urpmi.cfg Logs
# /etc/urpmi/proxy.cfg Logs
# /etc/prelink.cache ETC - md5 - s
! /etc/cups
# ! /etc/map
# ! /etc/postfix/prng_exch
# ! /etc/samba/secrets.tdb
# ! /etc/webmin/sysstats/modules/
# ! /etc/webmin/package-updates/
# ! /etc/webmin/system-status/

/lib      MyRule
/lib64    MyRule
/lib/modules MyRule
# /lib/dev-state MyRule -u

/root     MyRule
! /root/.viminfo
! /root/.bash_history
# ! /root/.mc
# ! /root/tmp
! /root/.cache

/sbin     MyRule
```

```
/usr/bin      MyRule
/usr/sbin     MyRule
/usr/lib      MyRule
! /usr/lib/.build-id/
! /usr/lib/fontconfig/cache/
/usr/lib64    MyRule
/usr/local/bin MyRule
/usr/local/sbin MyRule
/usr/local/lib MyRule

/var/ftp MyRule
/var/log Logs
# ! /var/log/journal
= /var/log/afick Logs
# ! /var/log/ksymoops
/var/www MyRule
# ! /var/www/html/snortsnarf
```

Cette partie du fichier de configuration détaille les vérifications de fichiers à réaliser, en voici un extrait :

```
...
/etc      ETC
/etc/mtab ETC - md5 - s
/etc/adjtime ETC - md5
...
```

Cet extrait indique que :

- le répertoire /etc sera vérifié selon l'alias **ETC**,
- le fichier /etc/mtab sera vérifié selon l'alias **ETC** à l'exception des règles **md5** et **s**,
- le fichier /etc/adjtime sera vérifié selon l'alias **ETC** à l'exception de la règle **md5**.

Utilisation

Commencez par créer la base de données d'afick :

```
[root@centos8 ~]# afick -i
# Afick (3.8.1) init at 2024/10/03 11:16:16 with options (/etc/afick.conf):
# archive:=/var/lib/afick/archive
# database:=/var/lib/afick/afick
# exclude_prefix:=__pycache__
# exclude_suffix:=log LOG html htm HTM txt TXT xml hlp pod chm tmp old bak fon ttf TTF bmp BMP jpg JPG gif png
ico wav WAV mp3 avi pyc
# history:=/var/lib/afick/history
# max_checksum_size:=10000000
# running_files:=1
# timing:=1
# dbm:=Storable
# #####
# MD5 hash of /var/lib/afick/afick => iYqXZ6neFdA/2qBYQPPDcg

# Hash database created successfully. 46551 files entered.
# user time : 18.88; system time : 6.49; real time : 117
```

Au moment où vous souhaitez vérifier l'intégrité de votre système de fichiers, utilisez la commande suivante :

- **afick -k**

En cas de modifications, celles-ci vous seront clairement indiquées.

Il est aussi nécessaire de mettre à jour votre base de données chaque fois que vous installez un nouveau paquet ou que vous mettez à jour un paquet déjà installé. Dans ce cas, utilisez la commande suivante :

- **afick -u**

Automatiser Afick

Lors de l'installation d'afick, le fichier **afick_cron** a été copié dans le répertoire `/etc/cron.daily` :

```
[root@centos8 ~]# cat /etc/cron.daily/afick_cron
#!/usr/bin/env sh
#####
#   afick_cron
#       it's a part of the afick project
#
#   Copyright (C) 2002, 2003 by Eric Gerbier
#   Bug reports to: eric.gerbier@tutanota.com
#   $Id$
#
#   This program is free software; you can redistribute it and/or modify
#   it under the terms of the GNU General Public License as published by
#   the Free Software Foundation; either version 2 of the License, or
#   (at your option) any later version.
#
#   This program is distributed in the hope that it will be useful,
#   but WITHOUT ANY WARRANTY; without even the implied warranty of
#   MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
#   GNU General Public License for more details.
#
#####
# script for cron job
# this script use the "macro" lines of afick configuration file
# the goals are :
# - set the nice priority
# - truncate too long reports to avoid big mails
# - avoid mails if no changes detected
# - sent report to the specicified email adress
# - write reports to /var/log/afick
```

```
# - archive retention management

AFICK="/usr/bin/afick.pl"
PATH="/bin:/usr/bin"
LOGDIR="/var/log/afick"
LOGFILE="$LOGDIR/afick.log"
ERRORLOG="$LOGDIR/error.log"
CONFFILE="/etc/afick.conf"

# the default action is "update" (-u), you can also use "compare" (-k)
ACTION="-u"

#####
treat_log() {
    if [ -n "$VERBOSE_AFICK" ]
    then
        echo "# This is an automated report generated by Another File Integrity Checker on $FQDN $DATE."
    fi

    # "normal" afick output : changes result
    if [ -s $LOGFILE ]; then
        loglines=`wc -l $LOGFILE | awk '{ print $1 }'`
        if [ ${loglines:=0} -gt $LINES ]; then
            echo "# TRUNCATED (!) output of the daily afick run:"
            echo "# Output is $loglines lines, truncated to $LINES."
            head -$LINES $LOGFILE
            echo "# The full output can be found in $LOGFILE."
        else
            echo "# Output of the daily afick run:"
            cat $LOGFILE
        fi
    elif [ -n "$VERBOSE_AFICK" ]
    then
        echo "# afick detected no changes."
    fi
}
```

```
fi

# afick errors
if [ -s $ERRORLOG ]; then
    errorlines=`wc -l $ERRORLOG | awk '{ print $1 }'`
    if [ ${errorlines:=0} -gt $LINES ]; then
        echo "# TRUNCATED (!) output of errors produced:"
        echo "# Error output is $errorlines lines, truncated to $LINES."
        head -$LINES $ERRORLOG
        echo "# The full output can be found in $ERRORLOG."
    else
        echo "# Errors produced:"
        cat $ERRORLOG
    fi
elif [ -n "$VERBOSE_AFICK" ]
then
    echo "# afick produced no errors."
fi

# check end of report (summary)
if [ -s $LOGFILE ]; then
    summary=`grep "MD5 hash of" $LOGFILE`
    if [ -z "$summary" ]
    then
        echo "WARNING: truncated report (no summary)"
    fi
fi

}

#####
# extract macro value from config file
macro () {
    key=$1
    grep -m 1 "^@@define $key" $CONFFILE | sed -e "s/^@@define $key *//"
}
```

```
}
#####
send_mail() {
    echo "$OUTPUT" | mail -s "[AFICK] Daily report for $FQDN" $MAILTO
}
#####
send_nagios() {
    NAGIOS_STATUS=3 # UNKNOWN initial status
    if [ -s $LOGFILE ]
    then
        NAGIOS_MSG=`tail -4 $LOGFILE | head -1 | sed -e "s/^[^0-9]*\(..*changed\) (.*/\1/ "`
        NUM_CHANGES=`echo $NAGIOS_MSG | cut -d " " -f 4`
        if [ $NUM_CHANGES -gt 0 ]
        then
            if [ $NUM_CHANGES -ge $NAGIOS_CRITICAL_CHANGES ]
            then
                NAGIOS_STATUS=2 # CRITICAL
            else
                NAGIOS_STATUS=1 # WARNING
            fi
        else
            NAGIOS_STATUS=0 # OK
        fi
    fi
    HOST=`hostname`
    echo "${HOST}\t${NAGIOS_CHECK_NAME}\t${NAGIOS_STATUS}\t${NAGIOS_MSG}\n" | $NAGIOS_NSCA -H $NAGIOS_SERVER
    -c $NAGIOS_CONFIG >/dev/null
}
#####
# MAIN
#####

[ -x $AFICK ] || exit 0
```

```
# hostname -f only exists on GNU systems,
# on others (HPUX, AIX, Solaris, Tru64), it return an error on stderr
# and a usage message on stdout
FQDN=`( hostname -f || hostname ) 2>/dev/null |tail -1`
DATE=`date +"at %X on %x"`
MAILTO=`macro MAILTO`
LINES=`macro LINES`
VERBOSE=`macro VERBOSE`
REPORT=`macro REPORT`
NICE=`macro NICE`
BATCH=`macro BATCH`
MOUNT=`macro MOUNT`
NAGIOS=`macro NAGIOS`
NAGIOS_SERVER=`macro NAGIOS_SERVER`
NAGIOS_CONFIG=`macro NAGIOS_CONFIG`
NAGIOS_CHECK_NAME=`macro NAGIOS_CHECK_NAME`
NAGIOS_CRITICAL_CHANGES=`macro NAGIOS_CRITICAL_CHANGES`
NAGIOS_NSCA=`macro NAGIOS_NSCA`
ARCHIVE_RETENTION=`macro ARCHIVE_RETENTION`

# default values
[ -z "$FQDN" ] && FQDN=`hostname`
[ -z "$MAILTO" ] && MAILTO="root"
[ -z "$LINES" ] && LINES="1000"
[ -z "$VERBOSE" ] && VERBOSE=0
[ -z "$REPORT" ] && REPORT=1
[ -z "$NICE" ] && NICE=15
[ -z "$BATCH" ] && BATCH=1
[ -z "$NAGIOS" ] && NAGIOS=0
[ -z "$NAGIOS_SERVER" ] && NAGIOS="localhost"
[ -z "$NAGIOS_CONFIG" ] && NAGIOS_CONFIG="/etc/send_nscs.cfg"
[ -z "$NAGIOS_CHECK_NAME" ] && NAGIOS_CHECK_NAME="Another File Integrity Checker"
[ -z "$NAGIOS_CRITICAL_CHANGES" ] && NAGIOS_CRITICAL_CHANGES=2
[ -z "$NAGIOS_NSCA" ] && NAGIOS_NSCA="/usr/sbin/send_nscs"
```

```
[ -z "$ARCHIVE_RETENTION" ] && ARCHIVE_RETENTION=0

#echo "MAILTO=$MAILTO LINES=$LINES VERBOSE=$VERBOSE NICE=$NICE BATCH=$BATCH"

if [ "$BATCH" = "0" ]
then
    exit 0
fi

if [ "$VERBOSE" = "1" ]
then
    # verbose mail
    export VERBOSE_AFICK=1
fi

# the mount point must be already defined in /etc/fstab
if [ -n "$MOUNT" ]
then
    mount $MOUNT
fi

# launch command
nice -n $NICE $AFICK -c $CONFFILE $ACTION > $LOGFILE 2> $ERRORLOG

# archive retention
if [ "$ARCHIVE_RETENTION" != "0" ]
then
    echo "#####" >> $LOGFILE
    echo "# afick_archive" >> $LOGFILE
    /usr/bin/afick_archive.pl -c $CONFFILE -H -k $ARCHIVE_RETENTION >> $LOGFILE 2>> $ERRORLOG
fi

if [ -n "$MOUNT" ]
then
```

```
        umount $MOUNT
    fi

# nagios ?
if [ "$NAGIOS" = "1" ]
then
    send_nagios
fi

if [ "$REPORT" = "0" ]
then
    # no report
    exit
fi

# filter output to send by mail
OUTPUT=`treat_log`
if [ "$VERBOSE" = "1" ]
then
    send_mail
else
    # skip comments and empty lines
    OUTPUT_FILTRE=`echo "$OUTPUT" | grep -v "^#" | grep -v "^$"`
    if [ -n "$OUTPUT_FILTRE" ]
    then
        send_mail
    fi
fi
fi
```

Ce fichier permet d'intégrer Afick dans les tâches gérées par **cron**. Entre autre, il envoie un résumé par email à **root**.

L'adresse email à utiliser peut être modifiée dans la section **macros section** du fichier **/etc/afick.conf** :

```
#####
```

```
# macros section
#####
# used by cron job (afick_cron)
# define the mail adress to send cron job result
@@define MAILTO root@localhost
# truncate the result send by mail to the number of lines (avoid too long mails)
@@define LINES 1000
# REPORT = 1 to enable mail reports, =0 to disable report
@@define REPORT 1
# VERBOSE = 1 to have one mail by run, =0 to have a mail only if changes are detected
@@define VERBOSE 0
# define the nice value : from 0 to 19 (priority of the job)
@@define NICE 18
# = 1 to allow cron job, = 0 to suppress cron job
@@define BATCH 1
# (optionnal, for unix) specify a file system to mount before the scan
# it must be defined in /etc/fstab
#@define MOUNT /mnt/dist
# if set to 0, keep all archives, else define the number of days to keep
# with the syntaxe nS , n for a number, S for the scale
# (d for day, w for week, m for month, y for year)
# ex : for 5 months : 5m
@@define ARCHIVE_RETENTION 0

# send nagios messages by NSCA (= 1 to allow, = 0 to block)
@@define NAGIOS 0
# address of the nagios server to send messages to
@@define NAGIOS_SERVER my.nagios.server.org
# NSCA configuration file
# @@define NAGIOS_CONFIG /etc/send_nsca.cfg
# name used for nagios passive check on the nagios server side
@@define NAGIOS_CHECK_NAME Another File Integrity Checker
# number c of the changes that are considered critical => nagios state CRITICAL
# (0 changes => nagios state OK; 0> and <c changes => nagios state WARNING)
```

```
@@define NAGIOS_CRITICAL_CHANGES 2
# path to nsca binary
# @@define NAGIOS_NSCA /usr/sbin/send_nsca
```

Root Kits

Un **rootkit** est un paquet logiciel qui permet à un utilisateur non-autorisé d'obtenir les droits de **root**.

Les rootkits sont essentiellement de deux types, voire un mélange des deux :

- des modules du noyau,
- des paquets logiciels d'un utilisateur qui prennent la place de binaires système.

Les rootkits de type modules du noyau insèrent des modules qui remplacent des appels systèmes et cachent des informations concernant certains processus spécifiques.

Les rootkits de type paquets logiciels remplacent en règle générale des binaires système tels **ps**, **login** etc. Les binaires de remplacement cachent des processus et des répertoires de l'attaquant.

LAB #8 - Mise en place de rkhunter

rkhunter est un logiciel utilisé pour détecter les rootkits présents sur votre machine.

Installation

L'installation de rkhunter se fait simplement en utilisant yum :

```
[root@centos8 ~]# dnf install rkhunter
```

Les options de la commande

Les options de cette commande sont :

```
[root@centos8 ~]# rkhunter --help
```

```
Usage: rkhunter [--check | --unlock | --update | --versioncheck |  
               --propupd [{filename | directory | package name},...] |  
               --list [{tests | {lang | languages} | rootkits | perl | propfiles}] |  
               --config-check | --version | --help] [options]
```

Current options are:

--append-log	Append to the logfile, do not overwrite
--bindir <directory>...	Use the specified command directories
-c, --check	Check the local system
-C, --config-check	Check the configuration file(s), then exit
--cs2, --color-set2	Use the second color set for output
--configfile <file>	Use the specified configuration file
--cronjob	Run as a cron job (implies -c, --sk and --nocolors options)
--dbdir <directory>	Use the specified database directory
--debug	Debug mode (Do not use unless asked to do so)
--disable <test>[,<test>...]	Disable specific tests (Default is to disable no tests)
--display-logfile	Display the logfile at the end
--enable <test>[,<test>...]	Enable specific tests (Default is to enable all tests)
--hash {MD5 SHA1 SHA224 NONE <command>}	SHA256 SHA384 SHA512 Use the specified file hash function (Default is SHA256)
-h, --help	Display this help menu, then exit
--lang, --language <language>	Specify the language to use

	(Default is English)
--list [tests languages rootkits perl propfiles]	List the available test names, languages, rootkit names, perl module status or file properties database, then exit
-l, --logfile [file]	Write to a logfile (Default is /var/log/rkhunter.log)
--noappend-log	Do not append to the logfile, overwrite it
--nocf	Do not use the configuration file entries for disabled tests (only valid with --disable)
--nocolors	Use black and white output
--nolog	Do not write to a logfile
--nomow, --no-mail-on-warning	Do not send a message if warnings occur
--ns, --nosummary	Do not show the summary of check results
--novl, --no-verbose-logging	No verbose logging
--pkgmgr {RPM DPKG BSD BSDng SOLARIS NONE}	Use the specified package manager to obtain or verify file property values. (Default is NONE)
--propupd [file directory package]...	Update the entire file properties database, or just for the specified entries
-q, --quiet	Quiet mode (no output at all)
--rwo, --report-warnings-only	Show only warning messages
--sk, --skip-keypress	Don't wait for a keypress after each test
--summary	Show the summary of system check results (This is the default)
--syslog [facility.priority]	Log the check start and finish times to syslog (Default level is authpriv.notice)
--tmpdir <directory>	Use the specified temporary directory
--unlock	Unlock (remove) the lock file
--update	Check for updates to database files
--vl, --verbose-logging	Use verbose logging (on by default)
-V, --version	Display the version number, then exit
--versioncheck	Check for latest version of program
-x, --autox	Automatically detect if X is in use
-X, --no-autox	Do not automatically detect if X is in use

Utilisation

Lancez **rkhunter** simplement en appelant son exécutable. A l'issu de son exécution, vous observerez un résumé :

```
[root@centos7 ~]# rkhunter -c
...
System checks summary
=====

File properties checks...
    Required commands check failed
    Files checked: 137
    Suspect files: 4

Rootkit checks...
    Rootkits checked : 498
    Possible rootkits: 0

Applications checks...
    All checks skipped

The system checks took: 2 minutes and 10 seconds

All results have been written to the log file: /var/log/rkhunter/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter/rkhunter.log)
```

Configuration

rkhunter peut être configuré soit par des options sur la ligne de commande soit par l'édition de son fichier de configuration **/etc/rkhunter.conf**.

Copyright © 2024 Hugh Norris.
