#CR3

Limitation de la disponibilité des commandes

configuration et attibution de niveaux de privilège

on peut le réaliser par 3 étapes

1. modifier level privilège de la commande qu'on veut. 'privilege exrc level 5 ping'
2. créer un MDP pour change l'exec level pour l'user temporellement. 'enable algorithm_type scrypt secret level 5 cisco5' pour accéder au level on veut: 'enable 15' et saisir le MDP pour avoir le level on veut.
3. créer un compte ayant un level privilege on le donne. 'username support privilege 5 algorithm_type scrypt secret cisco5'

configuration de view et superview

mode view est un autre façon pour distribuer le droits aux users. la différence estle mode view distribue les droits de commande à un ou plusieur groupe. Si une commande n'a pas configuré dans un view, elle ne peut pas être exécuté.

système log de routeur

une autre VM est nécessaire pour stocker le syslog. dans ce cas-ci, on installe un système linux 'net-toolbox'

sur routeur: 'logging host *IP_Address*'

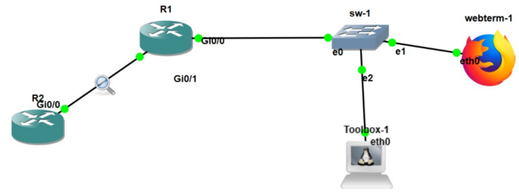
'logging trap *level*' usuellement 7- debugging

'logging on' activer logging

service NTP POUR SYNCRONISER LE LOG

un horloge synchronisé est demandé pour le système log.

Les secondes comptent lorsqu'ils'agit d'une attaque, car il est important d'identifier l'ordre dans lequel une attaque spécifiée s'est produite.



- syntax

1. 'ntp master *stratum*' *stratum* est l'hop de routage.
2. 'ntp server ip' désigner le serveur ntp par l'adress IP.
3. 'ntp broadcast client' configuré sur des interfaces routeur.

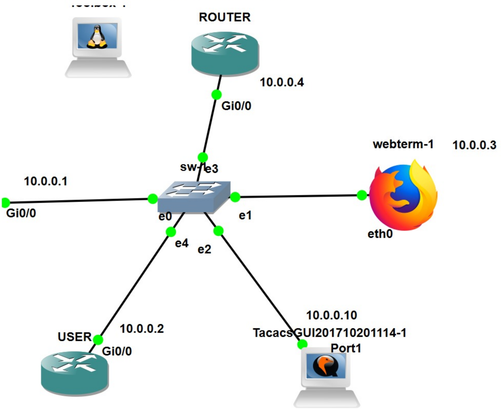
apres la configuration, on peut voir le resultat par 'show ntp status'

```
R2#sh ntp sta
Clock is synchronized, stratum 3, reference is 10.0.0.1
nominal freq is 1000.0003 Hz, actual freq is 999.9613 Hz, precision is 2**14
ntp uptime is 395200 (1/100 of seconds), resolution is 1001
reference time is E3A98EFD.3DF3230A (15:23:41.241 UTC Wed Jan 13 2021)
clock offset is -1633.3061 msec, root delay is 5.47 msec
root dispersion is 2873.33 msec, peer dispersion is 2.24 msec
loopfilter state is 'SPIK' (Spike), drift is 0.000038959 s/s
system poll interval is 256, last update was 70 sec ago.
R2#
```

serveur tacacs/radius

preparation

installation des machines TACACS, WEBTERM, deux ROUTEUR(user et ROUTER).



Configurations:

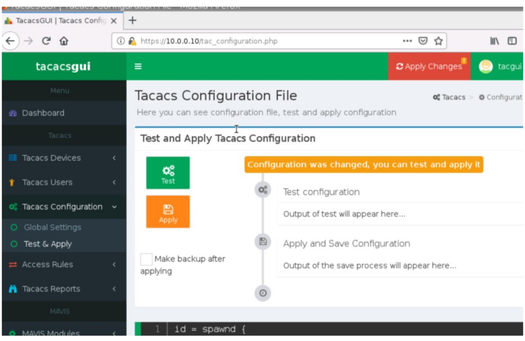
```
(sur le routeur)
username wuqi password cisco5
aaa new-model
!
aaa groupe server tacacs+ gns3group
  server name tacacsgui
!
aaa authentication login default group gns3group local

!
tacacs server tacacsgui
  address ipv4 10.0.0.10
  key cisco

!
enable password cisco ###pour  activer mode enable pour la connexion AAA
```

DANS gui tacacs(sur webterm)

- Ajoute un group devices
- Ajoute device ROUTER
- Ajoute un user avec un banner gentil
- atttention: tous les MDPs sont clair-text
- Après chaque modification, il faut bien 'apply changes' déchochant 'make backup after applying'. En ravanche, il ne marche pas et faut tout refaire.



Aller sur ROUTER

```
line vty 0 4
  tranport input telnet
!
'#'debug tacacs
```

aller sur Router user

```
telnet 10.0.0.4 (utiliser ID et MDP enregistrés sur TACACS GUI)
```

aller sur ROUTER puis d'analyser les logs

blocage de la connection serveur tacacs

si l'on déconnecte le serveur tacacs, USER peut encore acceder au serveur par vty. c'est a dire que l'authetication ne marche que le première fois. Et il n'est nécessaire ensuite.