

NewWorld SA

Livre Bleu

Projet réalisé par SCAFFIDI FONTI Mathis et PERDIGON Théo
modification : 6 mai 2022



Sommaire

Serveur DCWebDev	3
1. Service Apache/PHP	3
2. Service FTP	4
3. Utilisateurs	4
4. Envoie de courriel	5
5. Génération d'utilisateur automatique	6
Configuration des routeurs	10
1. Lardier	10
2. Sisteron	15
Configuration des switch	21
1. Lardier	21
2. Sisteron	23
Service DHCP	25
1. Configuration Master	25
2. Configuration Slave	28
Service DNS	31
1. Configuration Master	31
2. Configuration Slave	34
Central DB	36
Serveur SNMP	36
Serveur RADIUS	37
Serveur PROXY	38
Serveur Rebond	45
Serveur NAS	47
Serveur Syslog	50

- Serveur DCWebDev

1. Service Apache/PHP

Configuration de php

On va paramétrer php pour qu'il affiche les erreurs.

dans le fichier:

```
#nano /etc/php/7.3/apache2/php.ini
```

On modifie les lignes suivantes:

```
date.timezone = Europe/Paris
```

Cette option définit la timezone pour l'heure et la date.

```
upload_max_filesize = 20M
```

On augmente la limite max de l'upload à 20M

```
max_execution_time = 300
```

On augmente la limite max d'exécution à 300s

```
display_errors = On
```

Cette option permet d'activer l'affichage des erreurs

```
error_reporting = E_ALL
```

Affiche toutes les erreurs

Module userdir

On va tout d'abord activer ce module qui est présent par défaut dans apache.

```
#a2enmod userdir
```

On va ensuite modifier la configuration pour qu'apache détecte le dossier www présent dans les répertoires personnels comme répertoire web.

```
#nano /etc/apache2/mods-available/userdir.conf
```

Dans ce fichier, on va modifier les lignes:

```
UserDir www #précédemment : UserDir public_html
```

Et

```
<Directory /home/*/www> #précédemment : <Directory /home/*/public_html>
```

2. Service FTP

Configuration de proFTPD

On modifie la configuration en éditant le fichier:

```
#nano /etc/proftpd/proftpd.conf
```

On modifie le nom du serveur.

```
ServerName "DCWebDev"
```

On désactive l'ipv6.

```
UseIPv6 off
```

On décommente la ligne:

```
DefaultRoot ~
```

Cela permet de bloquer les clients ftp dans leurs dossier personnel.

3. Utilisateurs

Afin de faciliter la création des utilisateurs ainsi que des compte mariadb et base de donnée associé, on utilisera un script permettant leurs création en envoyant le nom d'utilisateur et le mot de passe en paramètre.

Pour exécuter la commande mkpasswd présente dans le script, le paquet **whois** est nécessaire.

Script

```
#!/bin/bash

if [ -z $1 ]
then
    read -p 'Saisir le nom : ' nom
    read -p 'Saisir le mot de passe : ' mdp
else
    nom=$1
    mdp=$2
fi

if $(useradd $nom -m -s /bin/bash -p $(mkpasswd -m sha-512 $mdp)) &&
$(echo "CREATE DATABASE $nom; GRANT ALL ON $nom.* TO '$nom'@'localhost'
IDENTIFIED BY '$mdp';" | mariadb -u mntnnc -proot)
then
    echo Création du compte $nom réussie
else
    echo Erreur
fi
```

Exécution du script

On exécute le script avec les paramètres. (./script <user> <mdp>)

```
#!/createUserAndDB.sh mscaffidi elini01
```

Le script renvoie:

```
Création du compte mscaffidi réussie
```

4. Envoie de courriel

On modifie les fichiers de configuration d'exim4 pour l'envoi de mail par un smarthost.

Fichiers à modifier:

Fichier /etc/exim4/update-exim4.conf.conf

```
dc_eximconfig_configtype='smarthost'  
dc_other_hostnames=''  
dc_local_interfaces='127.0.0.1'  
dc_readhost=''  
dc_relay_domains=''  
dc_minimaldns='false'  
dc_relay_nets=''  
dc_smarthost='smtp.gmail.com::587'  
CFILEMODE='644'  
dc_use_split_config='false'  
dc_hide_mailname='false'  
dc_mailname_in_oh='true'  
dc_localdelivery='mail_spool'
```

Fichier /etc/exim4/passwd.client

```
smtp.gmail.com:coeursi.newworld@gmail.com:passf202
```

5. Génération d'utilisateur automatique

Fichier google sheet:

<https://docs.google.com/spreadsheets/d/1rIKOTpqnP7rjVhNEs1yiSyy7Xfed4MiKO-Ye4oEGdCw/edit#gid=0>

Prérequis à l'exécution :

- paquet whois
- exim4

Script bash:

```
#!/bin/bash  
#Créé par SCAFFIDI FONTI Mathis pour le projet NewWorldSA  
  
#Script à exécuter en root  
  
#Initialisation des variables  
usersFailed=''
```

```

usersCreated=''
sqlFailed=''

#Telechargement du fichier csv
wget -q -O user.csv.tmp
https://docs.google.com/spreadsheets/d/1rIKOTpqnP7rjVhNEs1yiSyy7Xfed4MiK
0-Ye4oEGdCw/export?format=csv&id=1rIKOTpqnP7rjVhNEs1yiSyy7Xfed4MiK0-Ye4o
EGdCw&gid=0 && sleep 5

if [ -s user.csv.tmp ]; then
    #Suppression de la première ligne
    sed -i '1d' user.csv.tmp
    #Ajout d'une ligne à la fin
    echo -ne ".\n" >> user.csv.tmp

    #On lit le fichier csv ligne par ligne
    for ligne in `cat ./user.csv.tmp`
    do
        #Suppression du dernier caractere de la ligne
        ligne=${ligne::-1}

        #On recupere les elements de la ligne
        prenom=`echo $ligne | awk -F"," '{ print $2 }'`
        mail=`echo $ligne | awk -F"," '{ print $3 }'`
        user=`echo $ligne | awk -F"," '{ print $4 }'`

        existe=$(cat /etc/passwd | grep $(echo "$user:x:"))
        #Si l'utilisateur n'existe pas
        if [ -z "$existe" ]; then
            #Generation du mot de passe
            mdp=$(cat /dev/urandom | tr -dc 'a-zA-Z0-9' | fold -w 5 |
head -n 1)

            #Si la création de l'utilisateur est OK
            if $(useradd "$user" -m -s /bin/bash -p $(mkpasswd -m
sha-512 $mdp)); then
                #On complète les logs avec "succes"
                echo "`date +%Y/%m/%d`      `date +%H:%M:%S`
Création de l'utilisateur $user réussie" >> /var/log/gestUsers.log

                #Forcer le changement du mdp à la première connexion
                chage -d0 $user

                #Creation du compte sql

```

```

        if $(echo "CREATE DATABASE $user; GRANT ALL ON
$user.* TO '$user'@'localhost' IDENTIFIED BY '$mdp';" | mariadb -u
mntnc -poot); then
            #Envoi du mail a l'utilisateur contenant le mot
de passe
            echo -e "Bonjour $prenom, \nLa création de votre
compte sur le serveur de développement DCWebDev a été créé avec succès.
\nVos identifiants de connexion sont les suivants. \n\nConnexion
SSH:\n\tid: $user\n\tmdp: $mdp \n\nConnexion SQL:\n\tid: $user\n\tmdp:
$mdp \n\nIP intranet: 172.28.14.102 \n\n\nNB: Il vous seras demandé de
changer votre mot de passe à la première connexion. \nVous pourrez le
changer à tout moment avec la commande 'passwd'." | mail -s 'Serveur
DCWebDev' $(echo $mail)

            #Liste des utilisateurs créé
usersCreated=$usersCreated"\t$user\n"
        else
            #On complète les logs avec "erreur"
            echo "`date +%Y/%m/%d`      `date +%H:%M:%S`
Erreur: une erreur est survenue lors de la création du compte sql pour
$user" >> /var/log/gestUsers.log
            #Liste compte sql non créé
            sqlFailed=$sqlFailed"\t$user\n"
        fi
    else
        #Sinon on complète les logs avec "erreur"
        echo "`date +%Y/%m/%d`      `date +%H:%M:%S`      Erreur:
une erreur est survenue lors de la création de l'utilisateur $user" >>
/var/log/gestUsers.log

        #Liste des utilisateurs non créé
        usersFailed=$usersFailed"\t$user\n"
    fi
done
rm user.csv.tmp
else
    echo "`date +%Y/%m/%d`      `date +%H:%M:%S`      Erreur: une erreur est
survenue lors du téléchargement de la liste des utilisateurs" >>
/var/log/gestUsers.log
fi
if [ -n "$usersFailed" ];then

```



```

#Mail technicien
mailTech='Création du compte système : \n\tuseradd <user> -m -s
/bin/bash -p $(mkpasswd -m sha-512 <mdp>)\n\n'"Création du compte sql :
\n\tCREATE DATABASE <user>; \n\tGRANT ALL ON <user>.* TO
'<user>'@'localhost' IDENTIFIED BY '<mdp>'; \n\n"
[ -n "$sqlFailed" ] && msgSQL="\n\n\nLa création du compte sql a
échoué pour : \n$sqlFailed\n" || msgSQL="";
echo -e "La création des utilisateurs a échoué pour : \n$usersFailed
\nPour les créé, suivre les indications suivantes : \n\n$mailTech
$msgSQL" | mail -s 'Création utilisateur DCWebDev'
mathis.scaffidi@gmail.com

elif [ -n "$sqlFailed" ];then
#Mail technicien
echo -e "La création du compte sql a échoué pour : \n$sqlFailed
\nPour les créé, suivre les indications suivantes : \n\nCréation du
compte sql : \n\tCREATE DATABASE <user>; \n\tGRANT ALL ON <user>.* TO
'<user>'@'localhost' IDENTIFIED BY '<mdp>'; \n\n" | mail -s 'Création
utilisateur DCWebDev' mathis.scaffidi@gmail.com
fi

if [ -n "$usersCreated" ] || [ -n "$usersFailed" ];then

[ -n "$usersCreated" ] && msgRc="La création des utilisateurs
suivant a été effectué avec succès : \n$usersCreated \n" || msgRc="";
[ -n "$usersFailed" ] && msgRf="\nLa création des utilisateurs
suivant a échoué : \n$usersFailed \n" || msgRf="";

#Mail responsable pôle DevClassique
echo -e "$msgRc $msgRf" | mail -s 'Création utilisateur DCWebDev'
coeursi.webdev.newworld@gmail.com
fi

```

- Configuration des routeurs

1. Lardier

```
Current configuration : 8291 bytes
!
! Last configuration change at 07:09:32 UTC Thu Mar 31 2022 by theo
! NVRAM config last updated at 05:42:46 UTC Thu Mar 31 2022 by theo
! NVRAM config last updated at 05:42:46 UTC Thu Mar 31 2022 by theo
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Routeur_Lardier
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$y23h$HDeyuXR2R4PfdDeVJCX9/
enable password 7 0005170B0D55
!
no aaa new-model
!
no process cpu extended history
no process cpu autoprofile hog
!
no ipv6 cef
ip source-route
ip cef
!
!
!
!
!
ip domain name nw07_btsinfogap.org
!
multilink bundle-name authenticated
!
crypto pki token default removal timeout 0
!
!
license udi pid CISCO1941/K9 sn FCZ1648613K
license accept end user agreement
license boot module c1900 technology-package securityk9
!
!
username theo password 7 082048430017
!
redundancy
!
```

```
!  
!  
!  
ip ftp username p07  
ip ftp password 7 14121E02020D7A7A  
ip ssh version 2  
!  
!  
crypto isakmp policy 100  
  hash md5  
  authentication pre-share  
crypto isakmp key root address 10.14.100.2  
!  
!  
crypto ipsec transform-set TEST esp-aes esp-md5-hmac  
!  
crypto map VPN 10 ipsec-isakmp  
  set peer 10.14.100.2  
  set transform-set TEST  
  match address VPN  
!  
!  
!  
!  
!  
interface Embedded-Service-Engine0/0  
  no ip address  
  shutdown  
  no cdp enable  
!  
interface GigabitEthernet0/0  
  ip address 172.28.13.254 255.255.0.0  
  ip nat outside  
  ip virtual-reassembly in  
  duplex auto  
  speed auto  
  no cdp enable  
  no mop enabled  
!  
interface GigabitEthernet0/1  
  no ip address  
  duplex auto  
  speed auto  
  no cdp enable  
!  
interface GigabitEthernet0/1.10  
  encapsulation dot1Q 10  
  ip address 10.14.10.254 255.255.255.0  
  ip helper-address 192.168.14.20  
  ip helper-address 192.168.14.21  
  ip nat inside  
  ip virtual-reassembly in  
!  
interface GigabitEthernet0/1.20
```

```

encapsulation dot1Q 20
ip address 10.14.20.254 255.255.255.0
ip helper-address 192.168.14.20
ip helper-address 192.168.14.21
ip nat inside
ip virtual-reassembly in
!
interface GigabitEthernet0/1.21
encapsulation dot1Q 21
ip address 10.14.21.254 255.255.255.0
ip helper-address 192.168.14.20
ip helper-address 192.168.14.21
ip nat inside
ip virtual-reassembly in
!
interface GigabitEthernet0/1.22
encapsulation dot1Q 22
ip address 10.14.22.254 255.255.255.0
ip helper-address 192.168.14.20
ip helper-address 192.168.14.21
ip nat inside
ip virtual-reassembly in
!
interface GigabitEthernet0/1.30
encapsulation dot1Q 30
ip address 10.14.30.254 255.255.255.0
ip helper-address 192.168.14.20
ip helper-address 192.168.14.21
ip nat inside
ip virtual-reassembly in
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
no cdp enable
!
interface Serial0/0/1
ip address 10.14.100.1 255.255.255.252
clock rate 2000000
no cdp enable
crypto map VPN
!
interface GigabitEthernet0/1/0
switchport access vlan 100
no ip address
no cdp enable
!
interface GigabitEthernet0/1/1
switchport access vlan 100
no ip address
no cdp enable
!
interface GigabitEthernet0/1/2

```

```

switchport access vlan 101
no ip address
no cdp enable
!
interface GigabitEthernet0/1/3
no ip address
shutdown
no cdp enable
!
interface Vlan1
no ip address
shutdown
!
interface Vlan100
ip address 192.168.14.126 255.255.255.128
ip nat inside
ip virtual-reassembly in
!
interface Vlan101
ip address 192.168.14.254 255.255.255.128
ip nat inside
ip virtual-reassembly in
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip nat inside source list 1 interface GigabitEthernet0/0 overload
ip nat inside source list 2 interface GigabitEthernet0/0 overload
ip nat inside source static tcp 192.168.14.253 80 172.28.13.254 80 extendable
ip nat inside source static tcp 192.168.14.253 443 172.28.13.254 443 extendable
ip nat inside source static tcp 192.168.14.140 22 172.28.13.254 2207 extendable
ip nat inside source static tcp 192.168.14.140 8080 172.28.13.254 8080 extendable
ip route 0.0.0.0 0.0.0.0 172.28.255.254
ip route 10.14.40.0 255.255.255.0 10.14.100.2
!
ip access-list extended VPN
permit ip 192.168.14.0 0.0.0.255 10.14.0.0 0.0.255.255
!
access-list 1 permit 10.14.0.0 0.0.255.255
access-list 2 permit 192.168.14.0 0.0.0.255
!
!
!
!
!
snmp-server community private RO
snmp-server community public RW
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps transceiver all
snmp-server enable traps ds1
snmp-server enable traps call-home message-send-fail server-fail

```

```
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps license
snmp-server enable traps envmon
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps flash insertion removal
snmp-server enable traps c3g
snmp-server enable traps adsl1line
snmp-server enable traps vdsl2line
snmp-server enable traps icsudsu
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps ds0-busyout
snmp-server enable traps ds1-loopback
snmp-server enable traps energywise
snmp-server enable traps vstack
snmp-server enable traps mac-notification
snmp-server enable traps bgp
snmp-server enable traps isis
snmp-server enable traps rf
snmp-server enable traps aaa_server
snmp-server enable traps atm subif
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-change
inconsistency
snmp-server enable traps memory bufferpeak
snmp-server enable traps cnpd
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps fru-ctrl
snmp-server enable traps resource-policy
snmp-server enable traps event-manager
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps msdp
snmp-server enable traps mvpn
snmp-server enable traps nhrp nhs
```

```

snmp-server enable traps nhrp nhc
snmp-server enable traps nhrp nhp
snmp-server enable traps nhrp quota-exceeded
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps pppoe
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps vtp
snmp-server enable traps ipsla
snmp-server enable traps bfd
snmp-server enable traps firewall serverstatus
snmp-server enable traps isakmp policy add
snmp-server enable traps isakmp policy delete
snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
snmp-server host 192.168.14.42 private
snmp-server host 192.168.14.42 public
!
control-plane
!
!
!
line con 0
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  password 7 020700560208
  login local
  transport input ssh
!
scheduler allocate 20000 1000
end

```

2. Sisteron

```
Current configuration : 7402 bytes
!
! Last configuration change at 07:13:32 UTC Thu Mar 31 2022 by admin
! NVRAM config last updated at 08:35:22 UTC Mon Mar 28 2022 by admin
! NVRAM config last updated at 08:35:22 UTC Mon Mar 28 2022 by admin
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Routeur_Sisteron
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$LN2k$S/WSC901LIqTCj7N0FSIN/
enable password 7 011E0710535A
!
no aaa new-model
!
!
no ipv6 cef
ip source-route
ip cef
!
ip dhcp excluded-address 10.14.40.101 10.14.40.254
ip dhcp excluded-address 10.14.20.101 10.14.20.254
!
ip dhcp pool logigot
network 10.14.40.0 255.255.255.0
default-router 10.14.40.254
domain-name nw07-btsinfogap.org
dns-server 192.168.14.22 192.168.14.23
!
ip dhcp pool coeurSI
network 10.14.20.0 255.255.255.0
default-router 10.14.20.252
domain-name nw07-btsinfogap.org
dns-server 192.168.14.22 192.168.14.23
!
!
ip domain name nw07_btsinfogap.org
!
multilink bundle-name authenticated
!
crypto pki token default removal timeout 0
!
!
license udi pid CISCO1941/K9 sn FCZ1648C1SF
license accept end user agreement
```



```
license boot module c1900 technology-package securityk9
!
!
username admin password 7 071D2E435A
!
redundancy
!
ip ftp username p07
ip ftp password 7 00011F0F0A525B57
!
!
crypto isakmp policy 100
  hash md5
  authentication pre-share
crypto isakmp key root address 10.14.100.1
!
!
crypto ipsec transform-set TEST esp-aes esp-md5-hmac
!
crypto map VPN 10 ipsec-isakmp
  set peer 10.14.100.1
  set transform-set TEST
  match address VPN
!
!
interface Embedded-Service-Engine0/0
  no ip address
  shutdown
!
interface GigabitEthernet0/0
  ip address 172.28.14.254 255.255.0.0
  ip nat outside
  ip virtual-reassembly in
  duplex auto
  speed auto
  no mop enabled
!
interface GigabitEthernet0/1
  no ip address
  duplex auto
  speed auto
!
interface GigabitEthernet0/1.20
  encapsulation dot1Q 20
  ip address 10.14.20.251 255.255.255.0
  ip nat inside
  ip virtual-reassembly in
  shutdown
!
interface GigabitEthernet0/1.40
  encapsulation dot1Q 40
  ip address 10.14.40.254 255.255.255.0
  ip nat inside
  ip virtual-reassembly in
```

```
!  
interface Serial0/0/0  
  no ip address  
  shutdown  
  clock rate 2000000  
!  
interface Serial0/0/1  
  ip address 10.14.100.2 255.255.255.252  
  crypto map VPN  
!  
interface GigabitEthernet0/1/0  
  no ip address  
  shutdown  
!  
interface GigabitEthernet0/1/1  
  no ip address  
  shutdown  
!  
interface GigabitEthernet0/1/2  
  no ip address  
  shutdown  
!  
interface GigabitEthernet0/1/3  
  no ip address  
  shutdown  
!  
interface Vlan1  
  no ip address  
  shutdown  
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
!  
ip nat inside source list 1 interface GigabitEthernet0/0 overload  
ip route 0.0.0.0 0.0.0.0 172.28.255.254  
ip route 10.14.10.0 255.255.255.0 10.14.100.1  
ip route 10.14.11.0 255.255.255.0 10.14.100.1  
ip route 10.14.20.0 255.255.255.0 10.14.100.1  
ip route 10.14.21.0 255.255.255.0 10.14.100.1  
ip route 10.14.22.0 255.255.255.0 10.14.100.1  
ip route 10.14.30.0 255.255.255.0 10.14.100.1  
ip route 10.14.31.0 255.255.255.0 10.14.100.1  
ip route 192.168.14.0 255.255.255.128 10.14.100.1  
ip route 192.168.14.128 255.255.255.128 10.14.100.1  
!  
ip access-list extended VPN  
  permit ip 10.14.0.0 0.0.255.255 192.168.14.0 0.0.0.255  
!  
access-list 1 permit 10.14.0.0 0.0.255.255  
!  
snmp-server community public RO  
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
```

```
snmp-server enable traps vrrp
snmp-server enable traps transceiver all
snmp-server enable traps ds1
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps license
snmp-server enable traps envmon
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps flash insertion removal
snmp-server enable traps c3g
snmp-server enable traps adsl1line
snmp-server enable traps vdsl2line
snmp-server enable traps icsudsu
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps ds0-busyout
snmp-server enable traps ds1-loopback
snmp-server enable traps energywise
snmp-server enable traps vstack
snmp-server enable traps mac-notification
snmp-server enable traps bgp
snmp-server enable traps isis
snmp-server enable traps rf
snmp-server enable traps aaa_server
snmp-server enable traps atm subif
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-change
inconsistency
snmp-server enable traps memory bufferpeak
snmp-server enable traps cnpd
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps fru-ctrl
snmp-server enable traps resource-policy
snmp-server enable traps event-manager
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
```

```

snmp-server enable traps ipmulticast
snmp-server enable traps msdp
snmp-server enable traps mvpn
snmp-server enable traps nhrp nhs
snmp-server enable traps nhrp nhc
snmp-server enable traps nhrp nhp
snmp-server enable traps nhrp quota-exceeded
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps pppoe
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps syslog
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps vtp
snmp-server enable traps ipsla
snmp-server enable traps bfd
snmp-server enable traps firewall serverstatus
snmp-server enable traps isakmp policy add
snmp-server enable traps isakmp policy delete
snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
snmp-server host 192.168.14.42 private
snmp-server host 192.168.14.42 public
!
control-plane
!
line con 0
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  password 7 04560A120773
  login local
  transport input ssh
!
scheduler allocate 20000 1000
end

```

- Configuration des switch

1. Lardier

```
config-file-header
SwitchLardier
v1.3.0.62 / R750_NIK_1_3_647_260
CLI v1.0
set system mode switch

file SSD indicator encrypted
@
ssid-control-start
ssid config
ssid file passphrase control unrestricted
no ssid file integrity control
ssid-control-end cb0a3fdb1f3a1af4e4430033719968c0
!
vlan database
vlan 10,20-22,30
exit
voice vlan oui-table add 0001e3 Siemens_AG_phone_____
voice vlan oui-table add 00036b Cisco_phone_____
voice vlan oui-table add 00096e Avaya_____
voice vlan oui-table add 000fe2 H3C_Aolynk_____
voice vlan oui-table add 0060b9 Philips_and_NEC_AG_phone_____
voice vlan oui-table add 00d01e Pingtel_phone_____
voice vlan oui-table add 00e075 Polycom/Veritel_phone___
voice vlan oui-table add 00e0bb 3Com_phone_____
hostname SwitchLardier
no passwords complexity enable
no passwords complexity not-current
passwords aging 0
username cisco password encrypted
3e59e4c36bd000f997699647404aa1a4ea2c76ef privilege 15
username theo password encrypted
c6ef26d9760939c71cf5a6dd30499a47d1f808ec privilege 15
ip ssh server
ip ssh-client username theo
encrypted ip ssh-client password
k97/Rxnk1sVpmAid7CTYJqf62ripNhX72tSedUjGaro=
ip ssh-client server authentication
snmp-server server
```

```
snmp-server community private ro view Default
snmp-server community public ro view Default
snmp-server host 192.168.14.42 traps version 2c public
!
interface vlan 1
  no ip address dhcp
!
interface vlan 20
  ip address 10.14.20.253 255.255.255.0
!
interface fastethernet1
  switchport mode access
  switchport access vlan 10
!
interface fastethernet2
  switchport mode access
  switchport access vlan 20
!
interface fastethernet3
  switchport mode access
  switchport access vlan 21
!
interface fastethernet4
  switchport mode access
  switchport access vlan 21
!
interface fastethernet5
  switchport trunk allowed vlan add 20,22
!
interface fastethernet6
  switchport mode access
  switchport access vlan 30
!
interface fastethernet7
  switchport trunk allowed vlan add 10,20-22,30
!
interface fastethernet8
  shutdown
  switchport mode access
!
exit
ip default-gateway 10.14.20.254
```

2. Sisteron

```
config-file-header
SWSisteron
v1.3.7.18 / R750_NIK_1_35_647_358
CLI v1.0
set system mode switch

file SSD indicator encrypted
@
ssd-control-start
ssd config
ssd file passphrase control unrestricted
no ssd file integrity control
ssd-control-end cb0a3fdb1f3a1af4e4430033719968c0
!
vlan database
vlan 20,40
exit
voice vlan oui-table add 0001e3 Siemens_AG_phone_____
voice vlan oui-table add 00036b Cisco_phone_____
voice vlan oui-table add 00096e Avaya_____
voice vlan oui-table add 000fe2 H3C_Aolynk_____
voice vlan oui-table add 0060b9 Philips_and_NEC_AG_phone
voice vlan oui-table add 00d01e Pingtel_phone_____
voice vlan oui-table add 00e075 Polycom/Veritel_phone___
voice vlan oui-table add 00e0bb 3Com_phone_____
hostname SWSisteron
no passwords complexity enable
username cisco password encrypted
7a488390a939c4795cc1a801e51751d5f25d800d privilege 15
ip ssh server
ip ssh password-auth
crypto key pubkey-chain ssh
user-key root rsa
key-string row AAAAB3NzaC1yc2EAAAADAQABAAQgQDKifUVqtrc
key-string row c+9AsEXIjhooF2/6T+uGiHu/1kFec7q9LcMVn3Sv
key-string row 50vP7uiXWW5PMWK+HJgi2KUSjRGdlu7RKIqynNXL
key-string row auHqdEWUWhJRdHvFOsAHzVous1+5it/n
key-string row 2Q6fEn88Hy3q02f9BGVHEVxZXXSRGVQY2f+mbF1T
key-string row nz0r7SsibQ==
exit
exit
ip ssh-client server authentication
```

```
snmp-server server
snmp-server community public ro view Default
snmp-server community private ro view Default
snmp-server host 192.168.14.42 traps version 2c public
!
interface vlan 20
 name coeurSI
!
interface vlan 40
 name logigot
 ip address 10.14.40.253 255.255.255.0
 no ip address dhcp
!
interface fastethernet1
 switchport mode access
 switchport access vlan 20
!
interface fastethernet2
 switchport mode access
 switchport access vlan 40
!
interface fastethernet3
 switchport mode access
 switchport access vlan 20
!
interface fastethernet4
 switchport mode access
 switchport access vlan 40
!
interface fastethernet8
 switchport trunk allowed vlan add 20,40
!
exit
ip default-gateway 10.14.40.254
```


- Service DHCP

1. Configuration Master

IP : 192.168.14.106

```
option domain-name "nw07-btsinfogap.org";
option domain-name-servers 192.168.14.108, 192.168.14.109;

ddns-update-style none;

authoritative;

failover peer "DHCP-NWSA"{
primary;
address 192.168.14.106;
port 520;
peer address 192.168.14.107;
peer port 520;
max-response-delay 60 ;
max-unacked-updates 10 ;
mclt 3600;
split 255;
load balance max seconds 3;
}

# POOL SERVEUR
subnet 192.168.14.0 netmask 255.255.255.128 {
    range 192.168.14.1 192.168.14.2;
    option routers 192.168.14.126;
    # Réservations serveurs
    host DCWebDev {
        hardware ethernet B6:A8:AA:63:CA:2C;
        fixed-address 192.168.14.50;
    }
    host ADNWSA {
        hardware ethernet F2:EE:2A:4D:E0:77;
        fixed-address 192.168.14.40;
    }
    host DNS {
        hardware ethernet FE:B4:5B:38:35:5D;
        fixed-address 192.168.14.22;
```

```

}
host DNS2 {
hardware ethernet 86:33:8D:28:26:CB;
fixed-address 192.168.14.23;
}
host CentraleDB {
hardware ethernet E2:5D:A4:93:FB:D1;
fixed-address 192.168.14.25;
}
host RADIUS {
hardware ethernet 0E:5E:8B:ED:3E:61;
fixed-address 192.168.14.24;
}
host NAS {
hardware ethernet FE:ED:E3:0C:3A:E7;
fixed-address 192.168.14.26;
}
host GLPI {
hardware ethernet 0A:98:B6:7D:5D:E3;
fixed-address 192.168.14.41;
}
host PROXY {
hardware ethernet BA:F4:68:32:AA:69;
fixed-address 192.168.14.27;
}
host ZABBIX {
hardware ethernet 12:20:FF:14:C5:23;
fixed-address 192.168.14.42;
}
host SYSLOG {
hardware ethernet 66:F9:D3:DA:9F:86;
fixed-address 192.168.14.43;
}
}

# VLAN 10
subnet 10.14.10.0 netmask 255.255.255.0{
pool {
failover peer "DHCP-NWSA";
option routers 10.14.10.254;
range 10.14.10.1 10.14.10.100;
default-lease-time 21600;
max-lease-time 36000;
}
}

```

```
}
# VLAN 20
subnet 10.14.20.0 netmask 255.255.255.0{
pool {
failover peer "DHCP-NWSA";
option routers 10.14.20.254;
range 10.14.20.1 10.14.20.100;
default-lease-time 21600;
max-lease-time 36000;
}
}
# VLAN 21
subnet 10.14.21.0 netmask 255.255.255.0{
pool {
failover peer "DHCP-NWSA";
option routers 10.14.21.254;
range 10.14.21.1 10.14.21.100;
default-lease-time 21600;
max-lease-time 36000;
}
}
# VLAN 22
subnet 10.14.22.0 netmask 255.255.255.0{
pool {
failover peer "DHCP-NWSA";
option routers 10.14.22.254;
range 10.14.22.1 10.14.22.100;
default-lease-time 21600;
max-lease-time 36000;
}
}
# VLAN 30
subnet 10.14.30.0 netmask 255.255.255.0{
pool {
failover peer "DHCP-NWSA";
option routers 10.14.30.254;
range 10.14.30.1 10.14.30.100;
default-lease-time 21600;
max-lease-time 36000;
}
}
```

2. Configuration Slave

IP : 192.168.14.107

```
/etc/dhcp/dhcpd.conf

option domain-name "nw07-btsinfogap.org";
option domain-name-servers 192.168.14.108, 192.168.14.109;

# have support for DDNS.)
ddns-update-style none;

#authoritative;

# Paramétrage du failover du DHCP Slave
failover peer "DHCP-NWSA"{
secondary;
address 192.168.14.107;
port 520;
peer address 192.168.14.106;
peer port 520;
max-response-delay 60;
max-unacked-updates 10;
load balance max seconds 3;
}

# POOL SERVEUR
subnet 192.168.14.0 netmask 255.255.255.128 {
    range 192.168.14.1 192.168.14.2;
    option routers 192.168.14.126;
    # Réservations serveurs
    host DCWebDev {
        hardware ethernet B6:A8:AA:63:CA:2C;
        fixed-address 192.168.14.50;
    }
    host ADNWSA {
        hardware ethernet F2:EE:2A:4D:E0:77;
        fixed-address 192.168.14.40;
    }
    host DNS {
        hardware ethernet FE:B4:5B:38:35:5D;
        fixed-address 192.168.14.22;
    }
    host DNS2 {
```

```

    hardware ethernet 86:33:8D:28:26:CB;
    fixed-address 192.168.14.23;
  }
  host CentraleDB {
    hardware ethernet E2:5D:A4:93:FB:D1;
    fixed-address 192.168.14.25;
  }
  host RADIUS {
    hardware ethernet 0E:5E:8B:ED:3E:61;
    fixed-address 192.168.14.24;
  }
  host NAS {
    hardware ethernet FE:ED:E3:0C:3A:E7;
    fixed-address 192.168.14.26;
  }
  host GLPI {
    hardware ethernet 0A:98:B6:7D:5D:E3;
    fixed-address 192.168.14.41;
  }
  host PROXY {
    hardware ethernet BA:F4:68:32:AA:69;
    fixed-address 192.168.14.27;
  }
  host ZABBIX {
    hardware ethernet 12:20:FF:14:C5:23;
    fixed-address 192.168.14.42;
  }
  host SYSLOG {
    hardware ethernet 66:F9:D3:DA:9F:86;
    fixed-address 192.168.14.43;
  }
}

# VLAN 10
subnet 10.14.10.0 netmask 255.255.255.0{
  pool {
    failover peer "DHCP-NWSA";
    option routers 10.14.10.254;
    range 10.14.10.1 10.14.10.100;
    default-lease-time 21600;
    max-lease-time 36000;
  }
}
# VLAN 20

```

```
subnet 10.14.20.0 netmask 255.255.255.0{
pool {
failover peer "DHCP-NWSA";
option routers 10.14.20.254;
range 10.14.20.1 10.14.20.100;
default-lease-time 21600;
max-lease-time 36000;
}
}
# VLAN 21
subnet 10.14.21.0 netmask 255.255.255.0{
pool {
failover peer "DHCP-NWSA";
option routers 10.14.21.254;
range 10.14.21.1 10.14.21.100;
default-lease-time 21600;
max-lease-time 36000;
}
}
# VLAN 22
subnet 10.14.22.0 netmask 255.255.255.0{
pool {
failover peer "DHCP-NWSA";
option routers 10.14.22.254;
range 10.14.22.1 10.14.22.100;
default-lease-time 21600;
max-lease-time 36000;
}
}
# VLAN 30
subnet 10.14.30.0 netmask 255.255.255.0{
pool {
failover peer "DHCP-NWSA";
option routers 10.14.30.254;
range 10.14.30.1 10.14.30.100;
default-lease-time 21600;
max-lease-time 36000;
}
}
```

- Service DNS

1. Configuration Master

/etc/bind/named.conf.local :

```
zone "nw07-btsinfogap.org" IN {
    type master;
    file "/etc/bind/nw07-btsinfogap.org";
    allow-update {none;};
    allow-transfer {192.168.14.109;};
    notify yes;
    also-notify {192.168.14.109;};
};

zone "14.168.192.in-addr.arpa" IN {
    type master;
    file "/etc/bind/nw07-btsinfogap.org.rev";
    allow-update {none;};
    allow-transfer {192.168.14.109;};
    notify yes;
    also-notify {192.168.14.109;};
};
```

/etc/bind/name.conf.options :

```
options {
    directory "/var/cache/bind";

    forwarders {
        172.17.63.131;
        194.250.200.153;
    };

    dnssec-enable yes;
    dnssec-validation auto;

    listen-on-v6 { none; };

    allow-query {192.168.14.0/25; 10.14.0.0/16;};
};
```

/etc/bind/nw07-btsinfogap.org :

```
$TTL      604800
@         IN      SOA      DNS.nw07-btsinfogap.org. root.nw07-btsinfogap.org. (
                        1          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Negative Cache TTL
;

; Informations DNS

@         IN      NS       DNS.nw07-btsinfogap.org.
@         IN      NS       DNS2.nw07-btsinfogap.org.
DNS       IN      A        192.168.14.22
DNS2      IN      A        192.168.14.23
;@        IN      A        192.168.14.22
;@        IN      A        192.168.14.23

; Contrôleur de domaine

_ldap._tcp.nw07-btsinfogap.org. SRV 0 0 389 ADNWSA.nw07-btsinfogap.org.
_kerberos._tcp.nw07-btsinfogap.org. SRV 0 0 88 ADNWSA.nw07-btsinfogap.org.
_ldap._tcp.dc._msdcs.nw07-btsinfogap.org. SRV 0 0 389 ADNWSA.nw07-btsinfogap.org.
_kerberos._tcp.dc._msdcs.nw07-btsinfogap.org. SRV 0 0 88
ADNWSA.nw07-btsinfogap.org.

ADNWSA   IN      A        192.168.14.40

; Serveurs

DCWebDev      IN      A        192.168.14.50
DHCP          IN      A        192.168.14.20
DHCP2        IN      A        192.168.14.21
CentraleDB   IN      A        192.168.14.25
RADIUS       IN      A        192.168.14.24
GLPI         IN      A        192.168.14.41
NAS          IN      A        192.168.14.26
PROXY        IN      A        192.168.14.27
ZABBIX       IN      A        192.168.14.42
SYSLOG       IN      A        192.168.14.43

; VLANs

Direction    IN      A        10.14.10.254
CoeurSI      IN      A        10.14.20.254
ToIP         IN      A        10.14.21.254
Wifi         IN      A        10.14.22.254
DC           IN      A        10.14.30.254
Logigot      IN      A        10.14.40.254

; Materiels
TAP          IN      A        10.14.22.253
DC           IN      A        10.14.30.254
Logigot      IN      A        10.14.40.254
```


/etc/bind/nw07-btsinfogap.org.rev :

```
$TTL 604800
@      IN      SOA    DNS.nw07-btsinfogap.org. root.nw07-btsinfogap.org. (
                                1          ; Serial
                                604800    ; Refresh
                                86400     ; Retry
                                2419200   ; Expire
                                604800 )  ; Negative Cache TTL
;

; Informations DNS
@      IN      NS     DNS.nw07-btsinfogap.org.
@      IN      NS     DNS2.nw07-btsinfogap.org.
22     IN      PTR    DNS.nw07-btsinfogap.org.
23     IN      PTR    DNS2.nw07-btsinfogap.org.

; Serveurs
50     IN      PTR    DCWebDev.nw07-btsinfogap.org.
40     IN      PTR    ADNWSA.nw07-btsinfogap.org.
20     IN      PTR    DHCP.nw07-btsinfogap.org.
21     IN      PTR    DHCP2.nw07-btsinfogap.org.
25     IN      PTR    CentraleDB.nw07-btsinfogap.org.
24     IN      PTR    RADIUS.nw07-btsinfogap.org.
41     IN      PTR    GLPI.nw07-btsinfogap.org.
26     IN      PTR    NAS.nw07-btsinfogap.org.
27     IN      PTR    PROXY.nw07-btsinfogap.org.
42     IN      PTR    ZABBIX.nw07-btsinfogap.org.
43     IN      PTR    SYSLOG.nw07-btsinfogap.org.

; VLANs
254    IN      PTR    Direction.nw07-btsinfogap.org.
254    IN      PTR    CoeurSI.nw07-btsinfogap.org.
254    IN      PTR    ToIP.nw07-btsinfogap.org.
254    IN      PTR    Wifi.nw07-btsinfogap.org.
254    IN      PTR    DC.nw07-btsinfogap.org.
254    IN      PTR    Logigot.nw07-btsinfogap.org.

; Matériels
253    IN      PTR    TAP.nw07-btsinfogap.org.
```

2. Configuration Slave

/etc/bind/named.conf.local :

```
zone "nw07-btsinfogap.org" IN {
  type slave;
  file "/var/cache/bind/nw07-btsinfogap.org";
  masters {192.168.14.108;};
};

zone "14.168.192.in-addr.arpa" IN {
  type slave;
  file "/var/cache/bind/nw07-btsinfogap.org.rev";
  masters {192.168.14.108;};
};
```

/etc/bind/named.conf.options :

```
options {
  directory "/var/cache/bind";

  forwarders {
    172.17.63.131;
    194.250.200.153;
  };

  dnssec-enable yes;
  dnssec-validation auto;

  listen-on-v6 { none; };

  allow-query {192.168.14.0/25; 10.14.0.0/16;};
};
```

Les configurations nw07-btsinfogap.org et nw07-btsinfogap.org.rev sont récupérées automatiquement sur le serveur master et sont stockées dans /var/cache/bind. Elles sont donc identiques.

Script de synchronisation des fichiers de configuration :

```
#!/bin/bash
# By Théo PERDIGON

# Test de ping du serveur MASTER
ping -c 4 192.168.14.108

if [ "$?" -ne 0 ]
then # Si ca ne ping pas, aucune action n'est à réaliser
    echo "`date`      Le serveur MASTER ne répond pas" >> .failover.log
else # Si le serveur répond, il faut alors faire une sauvegarde des
    fichiers de configuration

    # Suppression des fichiers de configurations présents
    rm /var/cache/bind/nw07*

    # Redémarrage du service bind9
    service bind9 restart

    # Logs
    echo "`date`      Sauvegarde des fichiers de configuration réussie"
>> .failover.log
fi
```

- **Central DB**

/etc/mysql/mariadb.conf.d/50-server.cnf :

```
bind-address          = 0.0.0.0
```

- **Serveur SNMP**

/etc/zabbix/zabbix_server.conf

```
DBHost=centraledb.nw07-btsinfogap.org  
DBname=zabbix  
DBUser=zabbix  
DBPassword=a***n
```

- Serveur RADIUS

/etc/samba/smb.conf :

```
[global]
# workgroup = NT-Domain-Name or Workgroup-Name
workgroup = nw07-btsinfogap

# Security mode. Most people will want user level
# security. See security_level.txt for details.
security = ads

winbind use default domain = no
password server = ADNWSA.nw07-btsinfogap.org
realm = nw07-btsinfogap.org
```

/etc/krb5.conf :

```
NW07-BTSINFOGAP.ORG = {
    kdc = ADNWSA.nw07-btsinfogap.org
}
```

/etc/freeradius/3.0/clients.conf :

```
client 10.14.22.253 {
    secret          = secret
    shortname       = 10.14.22.253
    nastype         = cisco
}
```

/etc/freeradius/3.0/mods-available/mschap :

```
with_ntdomain_hack = yes
#
#
ntlm_auth = "/usr/bin/ntlm_auth --request-nt-key
--username=%{%{Stripped-User-Name}:-%{%{User-Name}:-None}}
--challenge=%{%{mschap:Challenge}:-00}
--nt-response=%{%{mschap:NT-Response}:-00} --domain=%{mschap:NT-Domain}"
```

/etc/freeradius/3.0/mods-available/eap :

```
default_eap_type = peap
```

- Serveur PROXY

/etc/squid/squid.conf :

```
visible_hostname PROXY
append_domain .nw07-btsinfogap.org

# Sites bloqués
url_rewrite_program /usr/bin/squidGuard -c /etc/squidguard/squidGuard.conf

# AD
auth_param ntlm program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-ntlmssp
auth_param ntlm children 5

auth_param basic program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-basic
auth_param basic children 5
auth_param basic realm Squid AD
auth_param basic credentialsttl 2 hours

acl ntlm proxy_auth REQUIRED

# ACL pour le réseau
http_access allow ntlm

forwarded_for off

# Utilisateur faisant les requêtes sur le serveur
cache_effective_user proxy
cache_effective_group winbindd_priv

# Acces par default squid
cache_access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
cache_store_log /var/log/squid/store.log

# Emplacement de stockage des données et réglage des niveaux
cache_mem 16 MB
cache_dir ufs /var/spool/squid 120 16 128

# algorithme utilisé pour gérer le remplacement des objets stockés en cache
cache_replacement_policy heap LFUDA

# pourcentage d'usage du cache à partir duquel squid commence à supprimer des objets
cache_swap_low 80

# pourcentage d'usage du cache à partir duquel squid devient plus restrictif
cache_swap_high 90

acl localnet src 10.0.0.0/8          # RFC 1918 local private network (LAN)
acl localnet src 169.254.0.0/16    # RFC 3927 link-local (directly plugged)
machines
acl localnet src 192.168.0.0/16    # RFC 1918 local private network (LAN)
acl SSL_ports port 443
acl Safe_ports port 80             # http
```

```

acl Safe_ports port 21          # ftp
acl Safe_ports port 443        # https
acl Safe_ports port 70         # gopher
acl Safe_ports port 210        # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280        # http-mgmt
acl Safe_ports port 488        # gss-http
acl Safe_ports port 591        # filemaker
acl Safe_ports port 777        # multiling http
acl CONNECT method CONNECT

http_access allow localhost

include /etc/squid/conf.d/*

http_access allow localhost
http_access allow localnet
http_access deny all
http_port 3128

coredump_dir /var/spool/squid

refresh_pattern ^ftp:          1440    20%    10080
refresh_pattern ^gopher:      1440    0%     1440
refresh_pattern -i (/cgi-bin/|\?) 0     0%     0
refresh_pattern .              0      20%    4320

# proxy parent
acl localDomain dstdomain allow .nw07-btsinfo.org
cache_peer 172.16.63.130 parent 3128 0 no-query default
never_direct deny localDomain
never_direct allow all

```

/etc/squidguard/squidguard.conf :

```

dbhome /var/lib/squidguard/db
logdir /var/log/squidguard

#
# DESTINATION CLASSES:
#
# [see also in file dest-snippet.txt]

```

```
dest adult {
    domainlist      blacklists/adult/domains
    urllist         blacklists/adult/urls
    expressionlist  blacklists/adult/very_restrictive_expression
}

dest mixed_adult {
    domainlist      blacklists/mixed_adult/domains
    urllist         blacklists/mixed_adult/urls
}

dest porn {
    domainlist      blacklists/porn/domains
    urllist         blacklists/porn/urls
}

# Drogues
dest drogue {
    domainlist      blacklists/drogue/domains
    urllist         blacklists/drogue/urls
}

dest drugs {
    domainlist      blacklists/drugs/domains
    urllist         blacklists/drugs/urls
}

# Violence
dest aggressive {
    domainlist      blacklists/aggressive/domains
    urllist         blacklists/aggressive/urls
}

dest agressif {
    domainlist      blacklists/agressif/domains
    urllist         blacklists/agressif/urls
}

dest violence {
    domainlist      blacklists/violence/domains
    urllist         blacklists/violence/urls
}
```



```

# Triche
dest tricheur {
    domainlist      blacklists/tricheur/domains
    urllist         blacklists/tricheur/urls
}

dest games {
    domainlist      blacklists/games/domains
    urllist         blacklists/games/urls
}

###Forcer la réécriture de https vers http pour les moteurs de recherche
et pouvoir analyser les mots
rew safesearch {
    s@(google..*/search?.*q=.*@ &safe=active@i
    s@(google..*/images.*q=.*@ &safe=active@i
    s@(google..*/groups.*q=.*@ &safe=active@i
    s@(google..*/news.*q=.*@ &safe=active@i
    s@(yandex..*/yandsearch?.*text=.*@ &fyandex=1@i
    s@(search.yahoo..*/search.*p=.*@ &vm=r&v=1@i
    s@(search.live..*/.*q=.*@ &adlt=strict@i
    s@(search.msn..*/.*q=.*@ &adlt=strict@i
    s@(.bing..*/.*q=.*@ &adlt=strict@i
    log block.log
}

#
# ACL RULES:
#

acl {
    default {
        pass !games all
        redirect proxy
    }
}

```

/etc/krb5.conf :

```
[realms]
  NW07-BTSINFOGAP.ORG = {
    kdc = ADNWSA.nw07-btsinfogap.org
    admin_server = ADNWSA.nw07-btsinfogap.org
    default_domain = nw07-btsinfogap.org
  }
[domain_realm]
  .nw07-btsinfogap.org = NW07-BTSINFOGAP.ORG
  nw07-btsinfogap.org = NW07-BTSINFOGAP.ORG
```

/etc/samba/smb.conf :

```
[global]
  workgroup = nw07-btsinfogap
  realm = NW07-BTSINFOGAP.ORG
  security = ads
  encrypt passwords = yes

  password server = ADNWSA.nw07-btsinfogap.org

  idmap uid = 10000-20000
  idmap gid = 10000-20000
  winbind offline logon = false
  winbind enum groups = yes
  winbind enum users = yes
  winbind use default domain = yes

[homes]
  comment = Home Directories
  browseable = no
  writable = yes
```

/etc/nsswitch.conf :

```
passwd:          compat winbind
group:           compat winbind
shadow:         compat winbind
gshadow:        compat winbind

hosts:          files dns
networks:       files
protocols:      db winbind
services:       db winbind
ethers:         db winbind
rpc:            db winbind

netgroup:       nis
```

/etc/squidanalyser/squidanalyser.conf

```
Output      /var/www/html/squidanalyser
WebUrl      /squidreport
LogFile     /var/log/squid/access.log
UseClientDNSName  0
DNSLookupTimeout  100
NetworkAlias  /etc/squidanalyser/network-aliases
UserAlias    /etc/squidanalyser/user-aliases
UrlAlias     /etc/squidanalyser/url-aliases
OrderNetwork  bytes
OrderUser    bytes
OrderUrl     bytes
OrderMime    bytes
UrlReport    1
UrlHitsOnly  0
UserReport   1
QuietMode    1
CostPrice    0
Currency     &euro;
TopNumber    100
TopDenied    100
TopStorage   0
Exclude      /etc/squidanalyser/excluded
Include      /etc/squidanalyser/included
DateFormat   %y-%m-%d
AnonymizeLogin  0
SiblingHit   1
TransfertUnit  BYTES
MinPie       2
WriteDelay   3600
TopUrlUser   10
RefreshTime  5
StoreUserIp  0
```

Script blacklist :

```
#!/bin/bash
# By TPSCAFF
# Exportation du proxy parent
export http_proxy="http://172.16.63.130:3128"

# Téléchargement de la blacklist
cd /var/lib/squidguard/db/
if wget cri.univ-tlse1.fr/blacklists/download/blacklists.tar.gz
then
    echo "`date` Téléchargement de la blacklist effectué" >>
/var/log/maj.log
else
    echo "`date` Erreur lors du téléchargement de la blacklist" >>
/var/log/maj.log
fi

# Décompression de la blacklist
tar xzf blacklists.tar.gz

# Suppression de l'archive
rm blacklists.tar.gz

# Génération des bases de données de SquidGuard
if squidGuard -C all -d /var/lib/squidguard/db/blacklists
then
    echo "`date` Génération de la base de données effectué" >>
/var/log/maj.log
else
    echo "`date` Erreur lors de la génération de la base de données"
>> /var/log/maj.log
fi

# Redémarrage de squid
if systemctl restart squid.service
then
    echo "`date` Redémarrage de Squid effectué" >> /var/log/maj.log
else
    echo "`date` Erreur lors du redémarrage de Squid" >>
/var/log/maj.log
fi
```

- Serveur Rebond

Script de connexion

```
#!/bin/bash
# By PERDIGON Théo

# Boucle infinie permettant l'exécution continue du programme
while [ 1 -eq 1 ]
do
    clear
    echo " _____ "
    echo " | SCRIPT DE CONNEXION AUX SERVEURS | "
    echo " | _____ | "

    echo "Voici la liste des serveurs : "
    echo -e

    # Affichage de la liste des serveurs depuis le fichier
    serveur.csv
    cut -d : -f 1 serveurs.csv | cat -n
    echo -e

    # Demande à l'utilisateur de saisir une ligne
    read -p 'Sur quel serveur voulez-vous vous connecter (Ctrl+C pour
    quitter) : ' ligne

    # Sélection de la ligne en fonction de la saisie de l'utilisateur
    qui détermine donc l'identi
    ant et l'ip de connexion
    serveur=`awk NR==$ligne serveurs.csv | cut -d : -f 2`
    Nomserveur=`awk NR==$ligne serveurs.csv | cut -d : -f 1`

    # Connexion au serveur en SSH
    clear
    echo " _____ "
    echo " CONNEXION AU SERVEUR $Nomserveur "
    echo " | _____ | "
    ssh $serveur

    # Si l'utilisateur saisie 99, il peut modifier le fichier
    contenant la liste des serveurs (pour
```

```
dev)
    if [ $ligne -eq '99' ]
    then
        nano serveurs.csv
    fi
done
```

Serveurs.csv

```
DNS:mntnnc@192.168.14.22
DNS2:mntnnc@192.168.14.23
DHCP:mntnnc@192.168.14.20
DHCP2:mntnnc@192.168.14.21
DCWebDev:mntnnc@192.168.14.50
CentraleDB:mntnnc@192.168.14.25
NAS:mntnnc@192.168.14.26
RADIUS:mntnnc@192.168.14.24
GLPI:mntnnc@192.168.14.41
PROXY:mntnnc@192.168.14.27
ZABBIX:mntnnc@192.168.14.42
```

/etc/fail2band/jail.conf

```
[DEFAULT]
...
ignoreip = 127.0.0.1/8 ::1 10.14.0.0/16
...
bantime = 10m
findtime = 10m
maxretry = 3
...
[sshd]
enabled = true
port = 22
```

- Serveur NAS

Scripts :

/home/mntnnc/save.sh

```
#!/bin/bash
# By TPSCAFF
#Script de sauvegarde de configuration automatique

date=`date +%d-%m-%Y_%H%M`

# DHCP
if scp mntnnc@DHCP:/etc/dhcp/dhcpd.conf /home/mntnnc/DHCP/dhcpd.conf; then echo ""; else
echo "$date : Erreur, DHCP1 : Echec de la sauvegarde." >> /var/log/save.log; fi
if scp mntnnc@DHCP2:/etc/dhcp/dhcpd.conf /home/mntnnc/DHCP/dhcpd.conf.2; then echo "";
else echo "$date : Erreur, DHCP2 : Echec de la sauvegarde." >> /var/log/save.log; fi

# DNS
if scp mntnnc@DNS:/etc/bind/{named.conf*,nw07-btsinfogap.org*} /home/mntnnc/DNS/1/; then
echo ""; else echo "$date : Erreur, DNS1 : Echec de la sauvegarde." >>
/var/log/save.log; fi
if scp mntnnc@DNS2:/etc/bind/named.conf* /home/mntnnc/DNS/2/; then echo ""; else echo
"$date : Erreur, DNS2 : Echec de la sauvegarde." >> /var/log/save.log; fi

# RADIUS
if scp -r mntnnc@RADIUS:/etc/freeradius /home/mntnnc/RADIUS/ && scp
mntnnc@RADIUS:/etc/krb5.conf /home/mntnnc/RADIUS/ && scp
mntnnc@RADIUS:/etc/nsswitch.conf /home/mntnnc/RADIUS/ && scp
mntnnc@RADIUS:/etc/samba/smb.conf /home/mntnnc/RADIUS/; then echo ""; else echo "$date :
Erreur, RADIUS : Echec de la sauvegarde." >> /var/log/save.log; fi

# ZABBIX
if scp mntnnc@ZABBIX:/etc/zabbix/zabbix_server.conf /home/mntnnc/ZABBIX/; then echo "";
else echo "$date : Erreur, DHCP1 : Echec de la sauvegarde." >> /var/log/save.log; fi

# PROXY
if scp mntnnc@PROXY:/etc/squid/squid.conf /home/mntnnc/PROXY/ && scp
mntnnc@PROXY:/etc/squidguard/squidGuard.conf /home/mntnnc/PROXY/ && scp
mntnnc@PROXY:/etc/krb5.conf /home/mntnnc/PROXY/ && scp mntnnc@PROXY:/etc/nsswitch.conf
/home/mntnnc/PROXY/ && scp mntnnc@PROXY:/etc/samba/smb.conf /home/mntnnc/PROXY/; then
echo ""; else echo "$date : Erreur, PROXY : Echec de la sauvegarde." >>
/var/log/save.log; fi

#CentraleDB
if ssh mntnnc@CentraleDB mysqldump -u gestion -padmin glpi >
/home/mntnnc/CentraleDB/glpi.sql; then echo ""; else echo "$date : Erreur, CentraleDB :
Echec de la sauvegarde de la base glpi." >> /var/log/save.log; fi
if ssh mntnnc@CentraleDB mysqldump -u gestion -padmin zabbix >
/home/mntnnc/CentraleDB/zabbix.sql; then echo ""; else echo "$date : Erreur, CentraleDB
: Echec de la sauvegarde de la base zabbix." >> /var/log/save.log; fi
if ssh mntnnc@CentraleDB mysqldump -u gestion -padmin dcwebdev >
/home/mntnnc/CentraleDB/dcwebdev.sql; then echo ""; else echo "$date : Erreur,
```

```

CentraleDB : Echec de la sauvegarde de la base dcwebdev." >> /var/log/save.log; fi

#Routeur
if wget -m ftp://p07:elini01@172.28.200.100/NWSA_R_Lardier -O
/home/mntnnc/ROUTEURS/NWSA_R_Lardier; then echo ""; else echo "$date : Erreur,
ROUTEUR_Lardier : Echec de la sauvegarde." >> /var/log/save.log; fi
if wget -m ftp://p07:elini01@172.28.200.100/NWSA_R_Sisteron -O
/home/mntnnc/ROUTEURS/NWSA_R_Sisteron; then echo ""; else echo "$date : Erreur,
ROUTEUR_Sisteron : Echec de la sauvegarde." >> /var/log/save.log; fi

#Switch
if wget -m ftp://p07:elini01@172.28.200.100/NWSA_S_Lardier.txt -O
/home/mntnnc/SWITCHS/NWSA_S_Lardier; then echo ""; else echo "$date : Erreur,
SWITCH_Lardier : Echec de la sauvegarde." >> /var/log/save.log; fi
if wget -m ftp://p07:elini01@172.28.200.100/NWSA_S_Sisteron.txt -O
/home/mntnnc/SWITCHS/NWSA_S_Sisteron; then echo ""; else echo "$date : Erreur,
SWITCH_Sisteron : Echec de la sauvegarde." >> /var/log/save.log; fi

# Syslog
if scp mntnnc@syslog:/etc/graylog/server/server.conf /home/mntnnc/SYSLOG/ && scp
mntnnc@syslog:/etc/elasticsearch/elasticsearch.yml /home/mntnnc/SYSLOG/; then echo "";
else echo "$date : Erreur, SYSLOG : Echec de la sauvegarde." >> /var/log/save.log; fi

# Récupération des erreurs
erreurs=`cat /var/log/save.log | grep $date`

if [[ -n $erreurs ]]
then
    # Envois d'un mail aux administrateurs si erreur(s)
    echo "$erreurs" | mail -s "NAS : Erreur de sauvegarde"
tperdigon@btsinfogap.org,mscaffidi@btsinfogap.org
fi

# Suppression du dossier créer par la commande FTP
rm -r /home/mntnnc/172.28.200.100

```

/home/mntnnc/archiveJ.sh

```

#!/bin/bash
# By TPSCAFF
# Script d'archivage journalier

# Récupération du jour de la semaine
jour=`date | cut -d . -f 1`
# Récupération de la date
date=`date +%d-%m-%Y_%H%M`

# Création de l'archive dans le dossier correspondant à la semaine
if tar cvzf /home/mntnnc/BACKUPS_J/$jour'_'$date.tar.gz
/home/mntnnc/{CentraleDB,DNS,DHCP,PROXY,ROUTEURS,SWITCHS,ZABBIX,RADIUS}
then

```



```

        echo ""
else
    echo "`date` Archivage journalier : Une erreur est survenue lors de l'archivage
des fichiers" >> /var/log/save.log
    echo "`date` Archivage journalier : Une erreur est survenue lors de l'archivage
des fichiers" | mail -s "NAS : Erreur lors de l'archivage journalier "
tperdigon@btsinfogap.org,mscaffidi@btsinfogap.org
fi

```

/home/mntnnc/archiveH.sh

```

#!/bin/bash
# By TPSCAFF
# Script d'archivage hebdomadaire

# Récupération de la date
date=`date +%d-%m-%Y_%H%M`

# Création de l'archive dans le dossier correspondant à la semaine
if tar cvzf /home/mntnnc/BACKUPS_H/$date.tar.gz /home/mntnnc/BACKUPS_J/*
then
    echo ""
    # Suppression du contenu du répertoire Journalier
    rm /home/mntnnc/BACKUP_J/*
else
    echo "`date` Archivage hebdomadaire : Une erreur est survenue lors de l'archivage
des dossiers"
>> /var/log/save.log
    echo "`date` Archivage hebdomadaire : Une erreur est survenue lors de l'archivage
des dossiers"
| mail -s "NAS : Erreur lors de l'archivage hebdomadaire"
tperdigon@btsinfogap.org,mscaffidi@btsinfoga
p.org
fi

```

Crontab :

user : mntnnc

```

# Save
0 21 * * * /home/mntnnc/save.sh

# ArchiveJ
0 22 * * * /home/mntnnc/archiveJ.sh

# ArchiveH
0 23 * * 5 /home/mntnnc/archiveH.sh

```

- Serveur Syslog

/etc/graylog/server/server.conf

```
is_master = true
password_secret = U***W**1*A***W***9
root_username = admin
root_password_sha2=689286a7ea04bfd94513bb8db1ca94d9df46c0add422d464d4927d5d31a176c
http_bind_address = 192.168.14.43:9000
http_enable_cors = true
http_enable_gzip = true
http_max_header_size = 8192
http_thread_pool_size = 16
```

/etc/elasticsearch/elasticsearch.yml

```
cluster.name: graylog
path.data: /var/lib/elasticsearch
path.logs: /var/log/elasticsearch
action.auto_create_index: false
```