GSB

Mise en production d'un switch

Version <1.0>

Mise en production d'un switch

Historique des révisions

Date	Version	Description	Auteur
07/09/2015	<1.0>	**Rédaction de la documentation**	**Julien Legrand | Brice Harismendy**

Table des matières

Mise en production d'un switch

1. Introduction

1.1 Contexte du projet

Un nouveau commutateur est arrivé nous allons donc le configurer, de manière à ce que celui-ci soit sécurisé en terme d'accès, etc.

1.2 Objectifs du document

Explique de manière détaillée comment configurer le switch

1.3 Portée

Employés du service informatique

1.4 Définitions, Acronymes et Abréviations

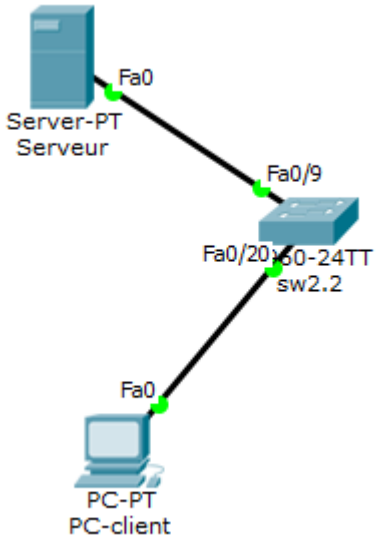
Conf t : configure terminal
int : interface
fa : fastEthernet
gi : gigabitEthernet
sw : switch
sh run : show running-config
sh vlan br : show vlan brief

1.5 Références

Mise en place des mots de passe : http://www.clemanet.com/configuration-base-switch.php
mise en place du serveur tftp : http://doc.ubuntu-fr.org/tftpd
mise en place du time out et du nombre d'essai maximum :
http://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html
configuration du SSH : http://reussirsonccna.fr/configuration-du-ssh-sur-ios/
fermeture des ports et commandes diverses : http://www.actualitix.com/commandes-commutateurs-cisco.html

2. Éléments de configuration

2.1 schéma réseau



2.2 Configuration de base du switch

Entrer dans l'interface de configuration :

```
switch>enable
switch#conf t
switch(config)#
```

Changer le nom du switch :

```
switch(config)#hostname sw2.2
```

2.3 Mise en place du vlan d'administration

```
Sw2.2>enable
sw2.2#conf t
sw2.2(config)#int vlan 29
sw2.2(config-if)#ip address 192.168.29.2 255.255.255.0
sw2.2(config-if)#ip default-gateway 192.168.29.254
```

2.4 Mise en place des Mots de passes robuste

```
Sw2.2>enable
sw2.2#conf t
sw2.2(config)#service password-encryption
sw2.2(config)#enable secret cisco
```

```
sw2.2(config)#line con 0
sw2.2(config-line)#password cisco
sw2.2(config-line)#login
sw2.2(config-line)#exit
sw2.2(config)#line vty 0 15
sw2.2(config-line)#password cisco
sw2.2(config-line)#login
sw2.2(config-line)#end
```

2.5 Mise en place du serveur TFTP

Sur un serveur Debian 8 après avoir configuré le réseau, installer les paquets suivant : xinetd tftpd tftp
vous devez donc faire :

```
apt-get install xinetd
apt-get install tftpd
apt-get install tftp
```

désinstaller openbsd-inetd :

```
apt-get purge openbsd-inetd
```

vérifier que le service fonctionne :

```
netstat -laputen | grep 69
```

Créer le fichier /etc/xinetd.d/tftp puis l'éditer et saisir :

```
service tftp
{
protocol        = udp
port            = 69
socket_type     = dgram
wait            = yes
user            = root
server          = /usr/sbin/in.tftpd
server_args     = /srv/tftpboot
disable         = no
}
```

Créer le répertoire /tftpboot :

```
mkdir /tftpboot
chmod -R 777 /tftpboot
```

créer le fichier concernant le switch (pour des raisons de sécurités nous n'automatisons pas la

création de fichiers de sauvegarde) :
touch /srv/tftpboot/sw2.2-confg

modifiez le fichier /etc/inetd.conf a la ligne 32 remplacer la par :

tftp dgram udp wait nobody /usr/sbin/tcpd /usr/sbin/in.tftpd /srv/tftpboot

si a la place il y a xinet.conf le fichier doit contenir :

```
# Simple configuration file for xinetd
# Some defaults, and include /etc/xinetd.d/
defaults
{
# Please note that you need a log_type line to be able to use log_on_success
# and log_on_failure. The default is the following :
# log_type = SYSLOG daemon info
}
includedir /etc/xinetd.d
$/sbin/in.tftpd /srv/tftpboot
```

Re-charger les fichiers de configuration de xinetd :

sudo /etc/init.d/xinetd restart

2.6 Mise en place d'un timeout de session et d'une limite de tentative de connexion

sw2.2(config)#ip ssh time-out 60
sw2.2(config)#ip ssh authentication-retries 3

2.7 Mise en place d'une connexion SSH

sw2.2(config)# username sw2.2 password P@ssw0rd
sw2.2(config)#ip domain-name cisco.com
sw2.2(config)#crypto key generate rsa modulus 1024

Activer le SSH

sw2.2(config)#line vty 0 4
sw2.2(config-line)#transport input ssh
sw2.2(config-line)#login local
sw2.2(config-line)#exit

2.8 Fermeture des ports SNMP,HTTPS et HTTP

fermer le port snmp :
sw2.2(config)#no snmp-server
fermer le port http :
sw2.2(config)#no ip http server
fermer le port https :
sw2.2(config)#no ip http secure-server

2.9 Mise en place de la journalisation centralisé

sur le serveur debian 8
editer le fichier /etc/rsyslog.conf
et décommenter les lignes suivantes :

provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

dans le bloc rules (a la fin du fichier de configuration) mettez :

$template syslog,"/var/log/clients/%fromhost%/syslog.log"

. ?syslog

sur le switch :

sw2.2(config)#conf t
sw2.2(config)#service timestamps
sw2.2(config)#logging 192.168.20.130
sw2.2(config)#logging facility local6
sw2.2(config)#logging trap informational

2.10 Réglage de l'horloge via NTP

sw2.2(config)#ntp serveur 192.168.2.22
sw2.2(config)#clock timezone GMT + 2

2.11 Sauvegarde des configurations

sur le switch :

```
sw2.2#copy running-config startup-config
```

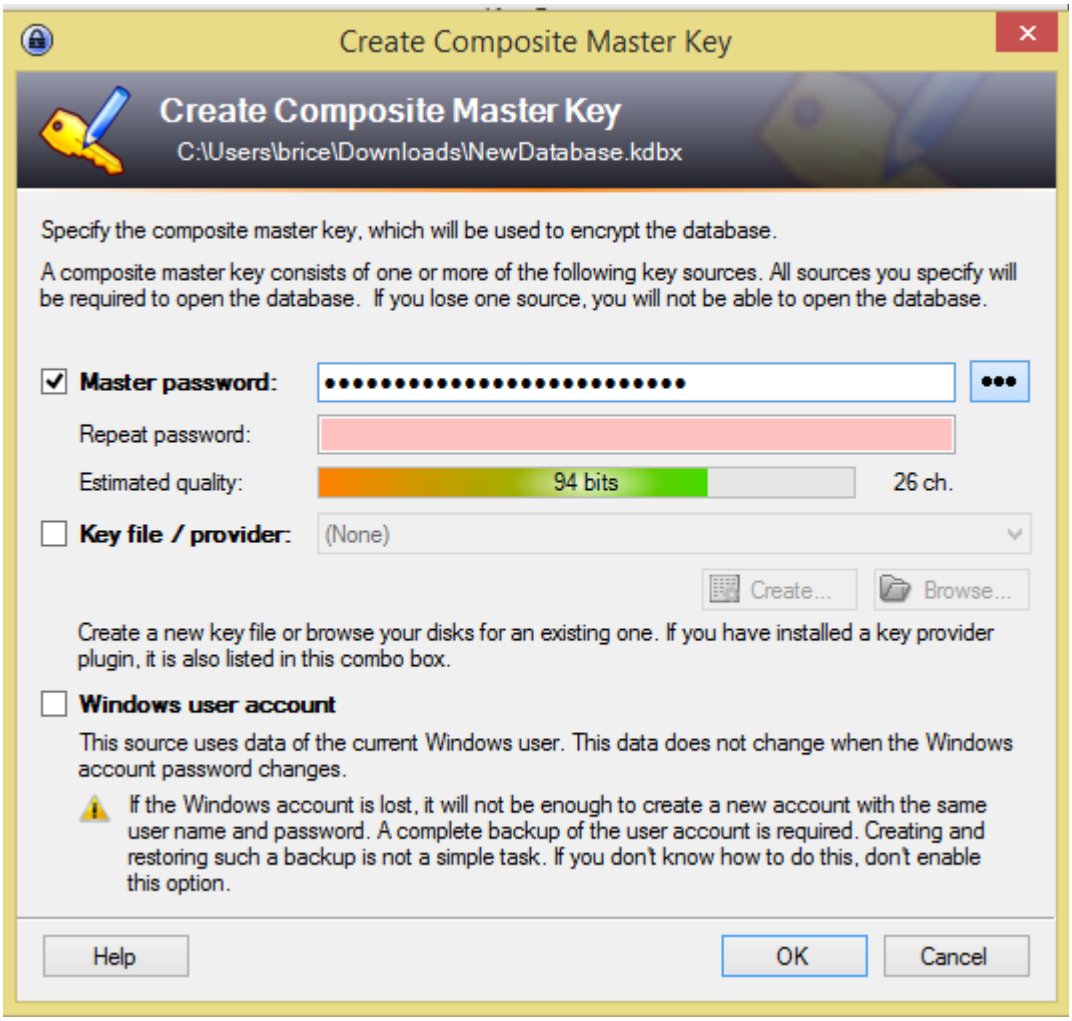
la configuration du switch sur le serveur tftp :

```
sw2.2# copy running-config tftp
sw2.2#copy vlan.dat tftp
```

2.12 Sauvegarde des mots de passe sous Keepass

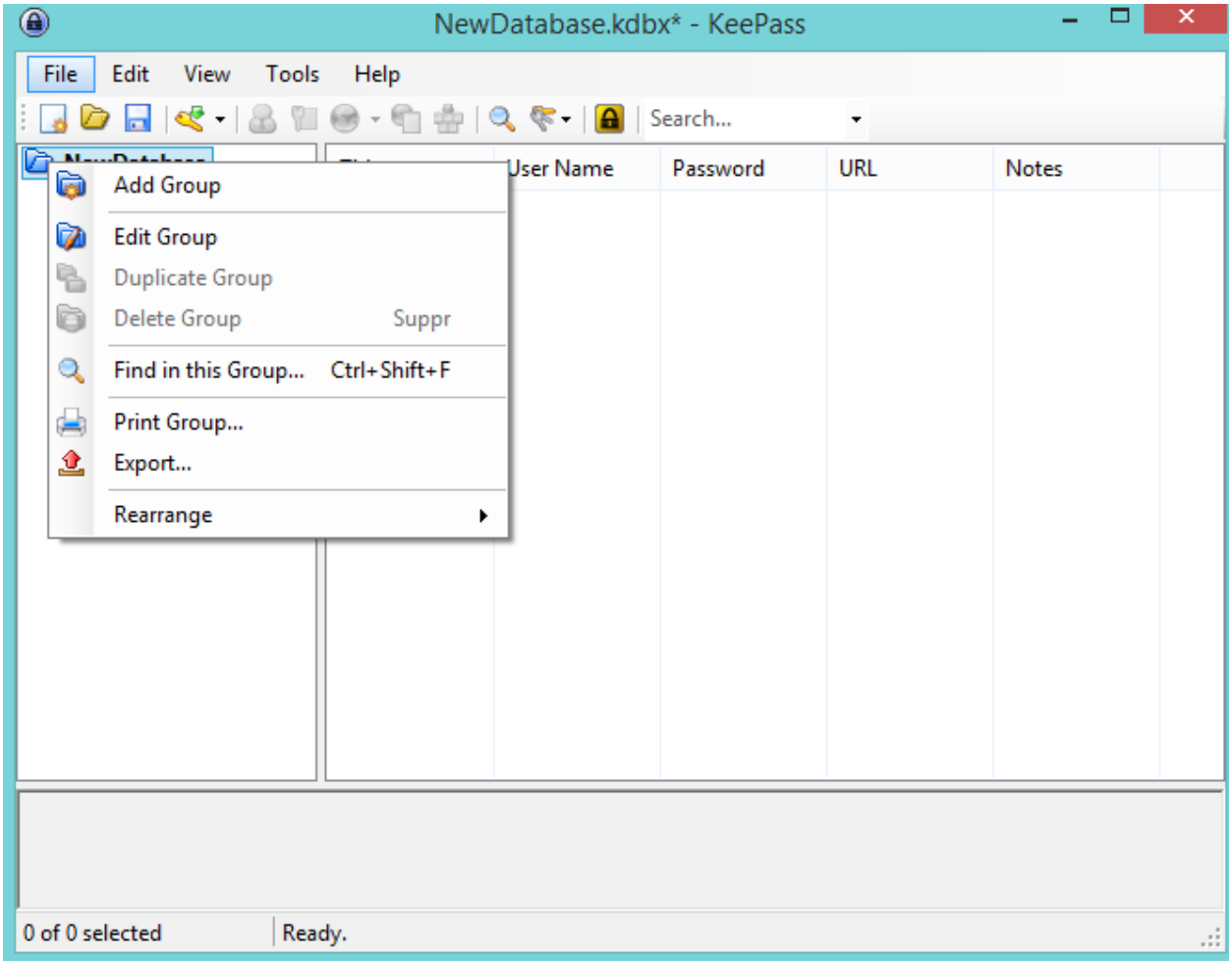
Téléchargez keepass a cette adresse : http://keepass.info/download.html

Après l'avoir installé nous allons le configurer pour qu'il stocke nos mots de passe :
cliquez en haut à gauche sur 'file' puis 'new' choisissez un lieu ou serra stocké le fichier contenant vos mots de passe .
Entrez un mot de passe robuste, attention il permettra d'acceder à tout vos mot de passe



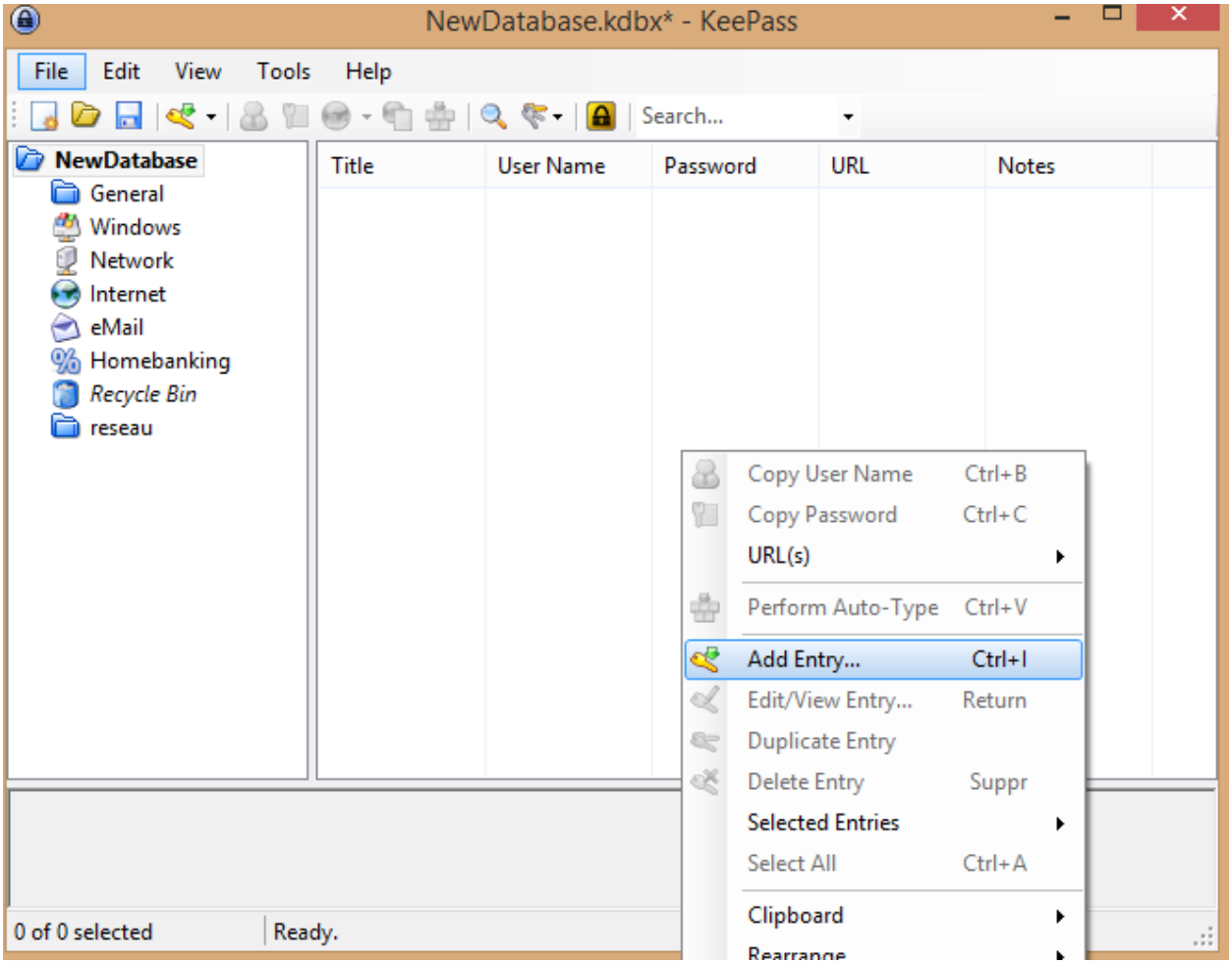
cliquez ensuite 2 fois sur 'ok'

on va créer un groupe spécial réseaux pour nos mots de passe :
clique droit sur le nom de votre base de donné et clique gauche sur 'add a group' :

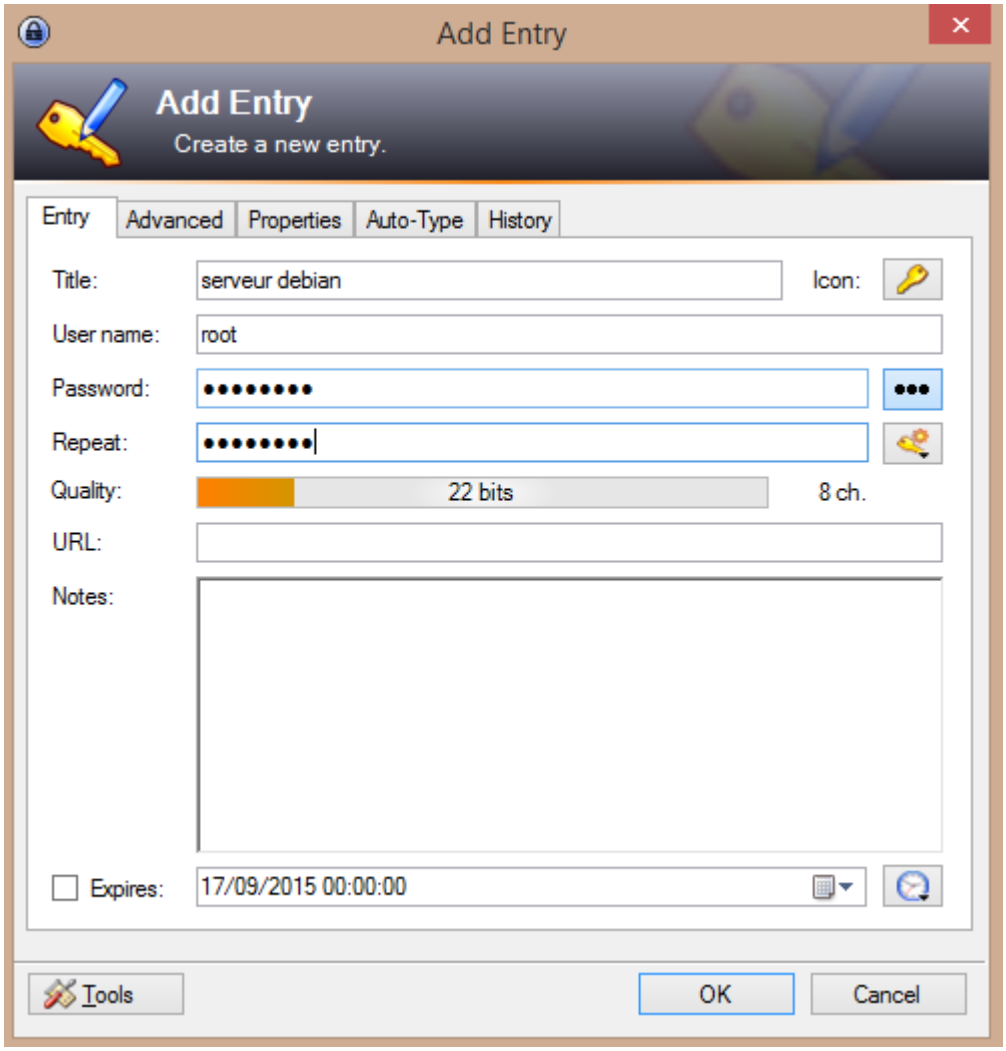


dans le champ 'name' entrez 'reseau' :

faite un clic droit dans la zone de stockage des clés et selectionner 'add entry' :



puis remplissez de manière intuitive les différents champs , voici ce que ça donne pour le serveur par exemple :



2.13 Envoie de la configuration finale dans un autre fichier via tftp

après ajout du fichier secureSWconf dans le fichier tftpboot (touch /srv/tftpboot) et à l'ajout des droits a ce fichier (chmod 777 secureSWconf) on l'envoie depuis le switch au serveur :

```
sw2.2#copy running-config tftp:
Address or name of remote host []? 192.168.20.130
Destination filename [sw2.2-confg]? secureSWconf
!!
5244 bytes copied in 0.923 secs (5681 bytes/sec)
```

3. Tests / Validations

[Le client s'attend à ce que vous démontriez que votre installation a été validée et est fonctionnelle. Cela protège aussi la STESIO contre des réclamations du client].

3.1 envoie de la configuration sur le switch et envoi sur le serveur

envoi de la config du switch :

```
sw2.2#copy running-config tftp:
Address or name of remote host []? 192.168.20.130
Destination filename [sw2.2-confg]?
!!
5317 bytes copied in 1.812 secs (2934 bytes/sec)
sw2.2#
```

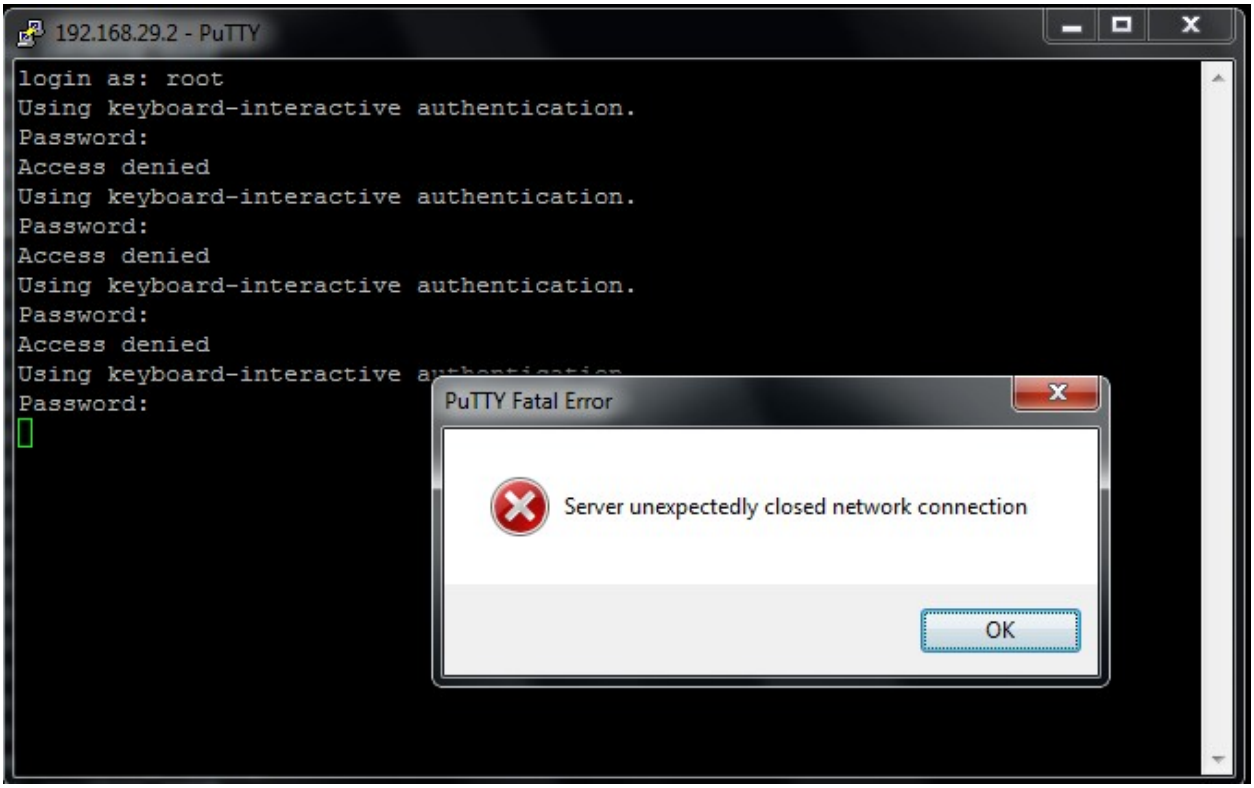
récupération :

```
sw2.2#copy tftp running-config
Address or name of remote host []? 192.168.20.130
Source filename []? sw2.2-confg
Destination filename [running-config]?
Accessing tftp://192.168.20.130/sw2.2-confg...
Loading sw2.2-confg from 192.168.20.130 (via Vlan29): !
[OK - 5317 bytes]
```

3.2 vérification du chiffrement des mots de passe

```
no logging console
enable secret 5 $1$quSI$4PbUXZb4PV0X98eytu8Ok0
!
username sw2.2 password 7 046B2B151C361C5C0D
```

3.3 connexion en SSH /time out /nombre d'essai




```
line con 0
 password 7 13061E010803
 login
line vty 0 4
 password 7 045802150C2E
 login local
 transport input ssh
line vty 5 15
 password 7 045802150C2E
 login
!
```

3.4 Port SNMP et HTTP fermé

http :

```
no ip http server
```

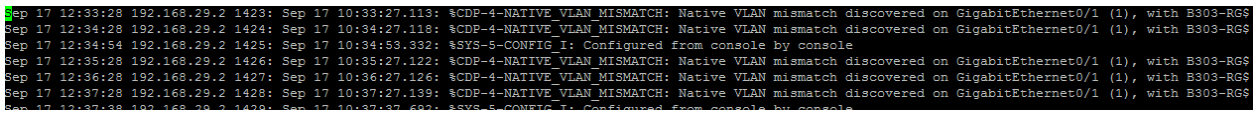
via nmap depuis le serveur debian :

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-09-18 13:02 CEST
Nmap scan report for 192.168.29.2
Host is up (0.0019s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 73.55 seconds
```

3.5 Centralisation des logs

log sur le serveur :



3.6 Heure du switch

```
sw2.2#sh clock
12:46:51.595 GMT Thu Sep 17 2015
```

3.7 Vérification de la bannière

```
login as: sw2.2
Using keyboard-interactive authentication.
Password:
odt
acces reserve aux personnes autorisees, vos actions sont sauvegardee
```

3.8 Journalisation des echecs de login :

(extrait du fichier de log)

```
Sep 18 13:39:19 192.168.29.2 47: Sep 18 11:39:18.413: %SSH-5-SSH2_SESSION:
SSH2 Session request from 192.168.2.44 (tty = 1) using crypto cipher 'aes256-
```

```
cbc', hmac 'hmac-sha1' Succeeded

Sep 18 13:39:29 192.168.29.2 48: Sep 18 11:39:28.337: %CDP-4-
NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1
(1), with B3O3-RG-296O-01.sio-savary-85.local FastEthernet0/9 (99).

Sep 18 13:39:40 192.168.29.2 49: Sep 18 11:39:39.6O3: %SSH-5-SSH2_USERAUTH:
User 'modsfjhqfqpoishfd' authentication for SSH2 Session from 192.168.2.44
(tty = 1) using crypto cipher 'aes256-cbc', hmac 'hmac-sha1' Failed

Sep 18 13:40:29 192.168.29.2 5O: Sep 18 11:40:28.366: %CDP-4-
NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1
(1), with B3O3-RG-296O-01.sio-savary-85.local FastEthernet0/9 (99).
```

4. Conclusion

Maintenant que notre switch est configuré de manière sécurisé on peut sauvegarder cette configuration afin de pouvoir l'utiliser par défaut sur les futurs switchs a déployer.