Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE CHARGÉ
DE L'EMPLOI

DOSSIER PROFESSIONNEL (DP)

Nom de naissance ▸ LEYSSENE
Nom d'usage ▸ LEYSSENE
Prénom ▸ Loïc
Adresse ▸ Champarnaud
87260 Vicq sur Breuilh

Titre professionnel visé

Technicien supérieur systèmes et réseaux

MODALITE D'ACCES :

☒ Parcours de formation
☐ Validation des Acquis de l'Expérience (VAE)

Présentation du dossier

Le dossier professionnel (DP) constitue un élément du système de validation du titre professionnel. **Ce titre est délivré par le Ministère chargé de l'emploi.**

Le DP appartient au candidat. Il le conserve, l'actualise durant son parcours et le présente **obligatoirement à chaque session d'examen**.

Pour rédiger le DP, le candidat peut être aidé par un formateur ou par un accompagnateur VAE.

Il est consulté par le jury au moment de la session d'examen.

Pour prendre sa décision, le jury dispose :

1. des résultats de la mise en situation professionnelle complétés, éventuellement, du questionnaire professionnel ou de l'entretien professionnel ou de l'entretien technique ou du questionnement à partir de productions.
2. du **Dossier Professionnel** (DP) dans lequel le candidat a consigné les preuves de sa pratique professionnelle.
3. des résultats des évaluations passées en cours de formation lorsque le candidat évalué est issu d'un parcours de formation
4. de l'entretien final (dans le cadre de la session titre).

[Arrêté du 22 décembre 2015, relatif aux conditions de délivrance des titres professionnels du ministère chargé de l'Emploi]

Ce dossier comporte :

- pour chaque activité-type du titre visé, un à trois exemples de pratique professionnelle ;
- un tableau à renseigner si le candidat souhaite porter à la connaissance du jury la détention d'un titre, d'un diplôme, d'un certificat de qualification professionnelle (CQP) ou des attestations de formation ;
- une déclaration sur l'honneur à compléter et à signer ;
- des documents illustrant la pratique professionnelle du candidat (facultatif)
- des annexes, si nécessaire.

Pour compléter ce dossier, le candidat dispose d'un site web en accès libre sur le site.

http://travail-emploi.gouv.fr/titres-professionnels

Sommaire

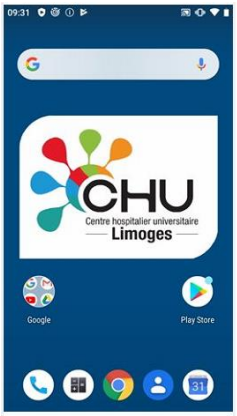
Exemples de pratique professionnelle

EXEMPLES DE PRATIQUE PROFESSIONNELLE

Activité-type 1 Assister les utilisateurs en centre de services

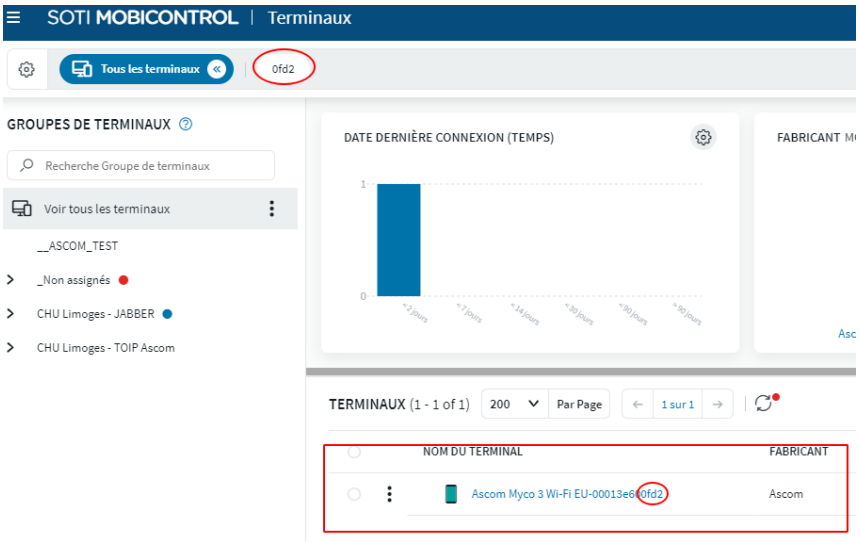
Exemple n°1 ▸ ***MISE EN SERVICE D'UN TELEPHONE MOBILE Myco 3 (wifi)***

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :



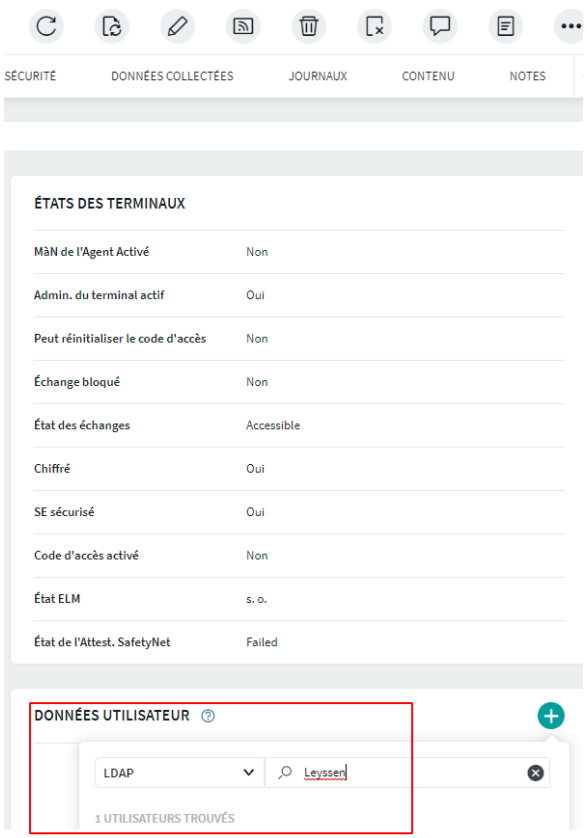
Les téléphones mobile Myco v3 wifi sont fabriqué par "Ascom", eux même sous-traité par "Nxo(nextiraone)".
Nxo développe et vend au CHU la solution logiciel 'Soti one'(serveur pour l'application mobile 'MobiControl') installé sur des machines virtuelle Windows serveur 2016 mise en place par l'équipe système (deux machines acceuillant l'application serveur, la base de données)
Nxo programme et fourni une carte à puce NFC (Near Field Communication) qui contient un script de configuration et installation.

Au premier démarrage du téléphone mobile l'écran de première configuration apparait.
Je présente contre le dos du téléphone la carte NFC, qui contient le script avec les éléments de configuration entre autre langage, le domaine et certificats d'autorité, l'application 'Mobi Control', les identifiants de connexion wifi, qui permettront à l'application MobiControl de communiquer avec le serveur MDM (Mobile Device Manager) : 'Soti one', qui renvoit les informations d'installation d'applications comme 'cisco Jabber', fond d'écran... et d'activation ou désactivation (GPO) de certaines applications et fonctionnalités (exemple: ajout de compte utilisateur téléphone bloqué), et ainsi de lancer les mises à jours du téléphone.



Les mises jour terminées, je relève l'adresse mac du téléphone pour le rechercher facilement dans 'Soti one', qui est accessible via interface web.
Dans 'Sorti One' je recherche le téléphone en renseignant les 4 dernières caractères de son adresse mac, il apparait et le sélectionne en cliquant dessus.

Dans la fenêtre suivante je fais une recherche du nom utilisateur qui sera amené à utiliser le mobile (il faut sélectionner LDAP pour la recherche car Soti est en lien avec l'annuaire du domaine).



L'arborescence des téléphones est organisée par groupe de métiers (professeur, médecin, cadre de santé, Samu), il suffit de faire glisser le mobile précédemment configuré vers le dossier groupe dont l'utilisateur dépend.
Les communications sur les mobiles ne passent que par 'Cisco Jabber' uniquement via connexion wifi, excepté les utilisateurs du Samu qui ont en supplément une carte 4g.
Les numéros de téléphone sont référencés dans un fichier Excel (la plage de numéro va de 48000 à 87000), je recherche de numéro disponible pour l'attribuer au nouvel utilisateur dans l'Active Directory)
Cisco Jabber se connecte via identification/authentification vers des serveurs TOIP du CHU sur le port 443.

2. Précisez les moyens utilisés :

Un Téléphone mobile, un réseau wifi, un pc pour accès au serveur MDM

3. Avec qui avez-vous travaillé ?

En équipe.

4. Contexte

Nom de l'entreprise, organisme ou association ▸ *CHU*

Chantier, atelier, service ▸ Service réseau

Période d'exercice ▸ Du : *15/06/2021* au : *28/05/2021*

5. Informations complémentaires *(facultatif)*

Activité-type 1 Assister les utilisateurs en centre de services

Exemple n° 2 ▸ Documenter configuration et mise en service Clickshare

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

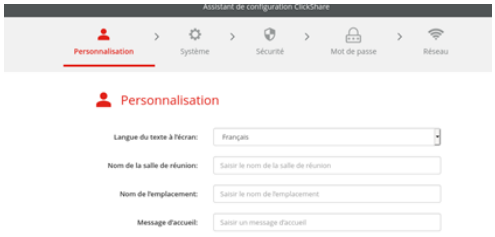
Démarrage et initialisation

Brancher le ClickShare à un écran via HDMI, connecter le en POE grâce à un câble RJ45.

L'adresse IP est affichée en bas à gauche, dans la partie « Wired IP ». Pour accéder à l'interface

web, rentrer cette adresse en https://

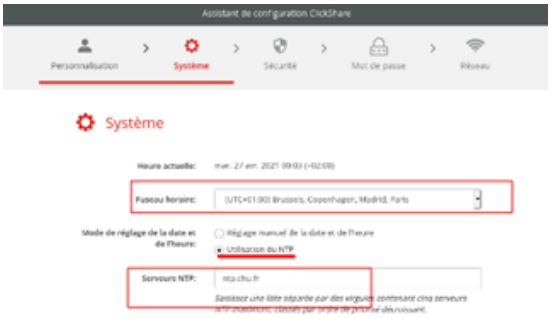
Attention : Le Vlan 324 ne possède pas de DHCP. Il faut le configurer sur un autre vlan que celui-là



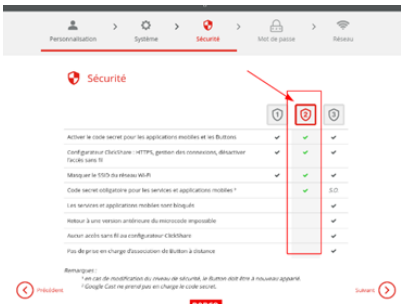
Renseigner :
La langue
(Français) ;
Le nom de la salle
de réunion ;
Son emplacement.

.

Sur la deuxième page, renseigner le bon fuseau horaire (UTC +01 :00), puis régler le mode de réglage de la date et heure sur : Utilisation du NTP.
Adresse du serveur NTP du CHU de Limoges : ntp.chu.fr



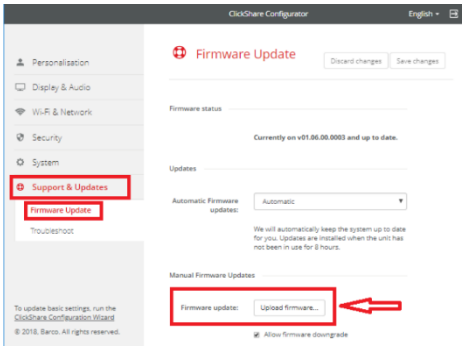
Sur la troisième page, sélectionner le niveau de sécurité «Niveau 2 » dans la section Sécurité, afin d'activer et forcer le code pin de sécurité pour les appareils mobiles.



Mise à Jour

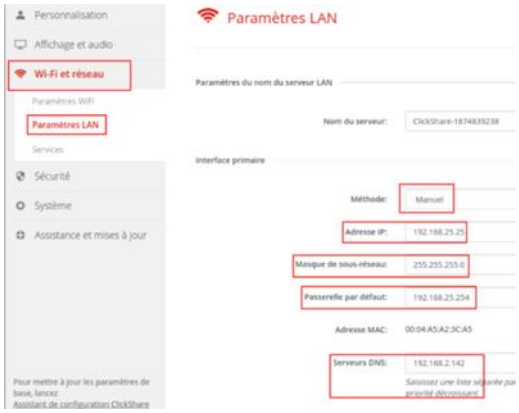
Avant de changer les paramètres du cklickshare et ses boutons, il faut mettre à jour le firmware, disponible ici : https://www.barco.com/fr/clickshare/firmware-update

Une fois téléchargé, il faut charger la mise à jour. Aller dans Assistance et mise à jour > Mise à jour du microcode > Mises à jour manuelles du microcode



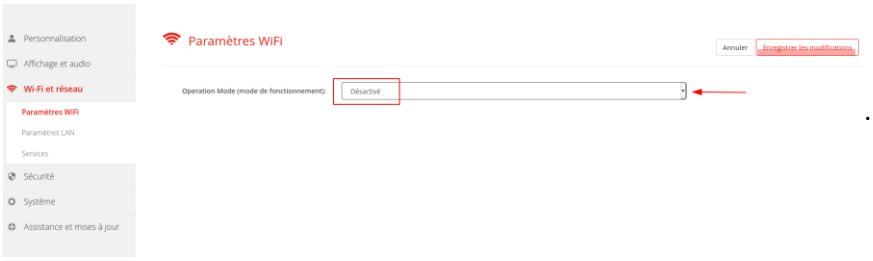
Paramètres

Configuration des paramètres LAN.
Aller dans Wifi et réseau > Paramètre LAN.
Ne pas oublier pas de passer en manuel :
Méthode : Manuel
Adresse IP : 192.168.25.XXX
Masque de sous-réseau : 255.255.255.0
Passerelle par défaut : 192.168.25.254
Serveur DNS : 192.168.2.142



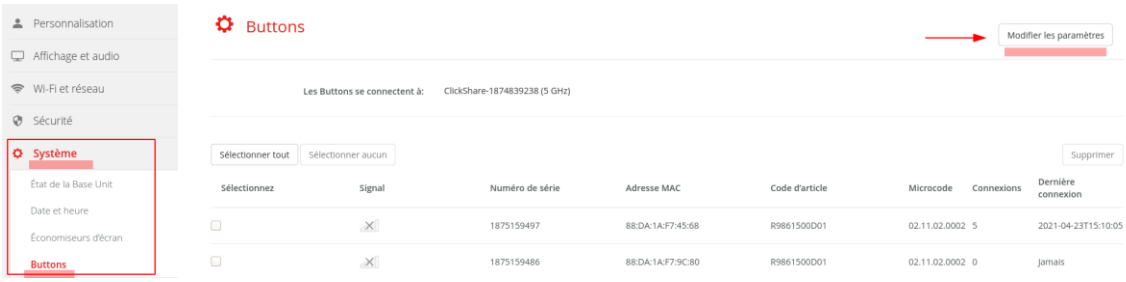
Une fois les modifications effectuées, penser à remettre le vlan 324 sur la prise pour qu'il puisse prendre la nouvelle adresse IP. Une fois reconnecté à l'interface avec la nouvelle adresse IP, configurer les paramètres wifi. Aller dans Wifi et réseau > Paramètre Wifi. Pour commencer, on clique sur modifier les paramètres en haut à droite de la page :

Désactiver le wifi sur le CSE-200, enregistrer les modifications (une fenêtre d'avertissement va s'ouvrir)

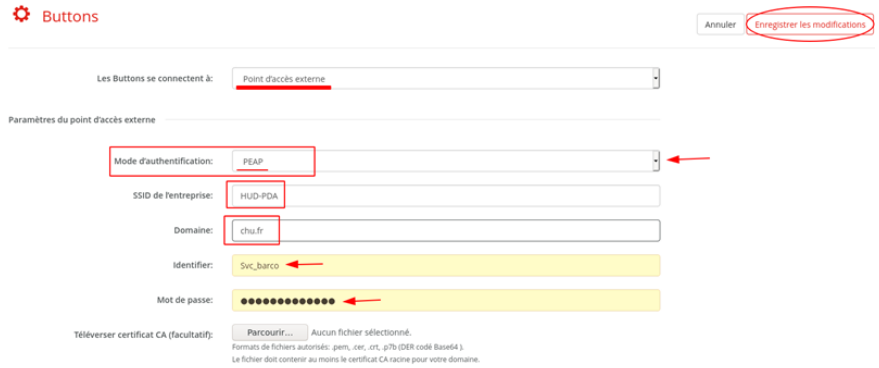


Sur cette fenêtre d'avertissement, sélectionner « Non, procéder à la configuration manuelle des buttons ».

Pour configurer les boutons, aller dans Système > Buttons puis modifier les paramètres en haut à droite.



Les buttons se connectent à : Point d'accès externe
Mode d'authentification : PEAP
SSID de l'entreprise : HUD-PDA
Domaine : chu.fr
Identifier : Svc_barco
Mot de passe : SvcBarco#2021
Ne pas oublier d'enregistrer les modifications en haut à droite.



Après avoir confirmé les modifications des paramètres Wifi du ClickShare, un message d'erreur va apparaitre

pour vous avertir qu'il faut réassocier les boutons. Cliquer sur « Très bien, je m'en occupe ».

Configuration des boutons

Pour effectuer la configuration des boutons, les connecter aux ports USB-A du CSE-200 à l'arrière. Cette action va re-synchroniser les boutons avec le ClickShare, et ils vont fonctionner en passant par le wifi du CHU plutôt que par le ClickShare directement.

Au moment de brancher le bouton à l'arrière du ClickShare, il va commencer à clignoter en blanc et un message va s'afficher sur l'écran, avec une barre de progression. Une fois la barre de progression terminée, le bouton va arrêter de clignoter pour afficher une lumière rouge fixe.

Le bouton est synchronisé avec le ClickShare.

2. Précisez les moyens utilisés :

Un pc, un Clickshare, un téléviseur, câbles hdmi, rj45

3. Avec qui avez-vous travaillé ?

Seul et en équipe

4. Contexte

Nom de l'entreprise, organisme ou association ▸ *CHU*

Chantier, atelier, service ▸ Service Réseau

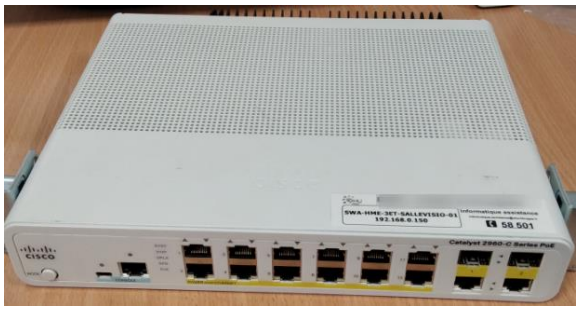
Période d'exercice ▸ Du : *15/04/2021* au : *28/05/2021*

5. Informations complémentaires *(facultatif)*

Activité-type 2 — Maintenir, exploiter et sécuriser une infrastructure centralisée

Exemple n° 1 ▸ ***MISE A JOUR FIRMWARE CISCO WS-C2960C-12PC (tftp)***

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :



Je ne peux pas effectuer de mise à jour avec un support USB (pas de port) sur ces switchs, je vais donc utiliser le protocole TFTP.

Ne pouvant pas installer d'application sur l'OS Windows fourni pour des raisons de sécurité de l'entreprise, j'installe sur une machine un OS client/serveur GNU/Linux (Xubuntu) afin mettre en place un serveur TFTP.
Je procède comme suit :

#apt install tftp tftpd
Je créé un dossier à la racine qui contiendra le fichier image du firware cisco et lui donne les bons droits :
#mkdir /tftpboot
#chmod 777 /tftpboot
#chown loic:loic /tftpboot
J'édite le fichier de configuration de mon tftp pour lui renseigner le bon chemin de stockage:
#nano /etc/inetd.conf
tftp dgram udp wait nobody /usr/sbin/tcpd /usr/sbin/in.tftpd /tftpboot
je redémarre le service: **/etc/init.d openbsd-inetd restart**
Je place l'image du firmware dans le dossier /tftpboot précédemment créé.
il me faut également configurer l'adaptateur USB console pour le rendre fonctionnel avec Linux et putty, je liste les ports USB
et relève les numéros identifiants produit et fabricant,
#lsusb
> Bus 005 Device 003: ID 0403:6001 Future Tech
afin d'activer le module que j'exécute avec modprobe:
#modprobe usbserial vendor=0x0403 product=0x6001
la commande dmesg me donne dans la liste le port com à utiliser dans putty (disponible dans les dépôts xbuntu)
je donne les bons droits au périphérique (sudo chmod 666 /dev/ttyUSB0) pour autoriser la communication avec putty.
Je me connecte via putty au port console du switch.
Pour le transfert du fichier en tftp je dois configurer les adresses IP sur mon pc et sur le switch pour établir une connexion entre les deux.
Je connecte un câble RJ45 sur l'interface Ethernet de mon PC et sur le port FastEthernet0/1 du switch
je renseigne sur le PC via network-manager une adresse IP et un masque de sous réseau (10.0.0.1 255.255.0.0)
je configure sur le switch une adresse IP sur l'interface vlan 1 et active l'interface:
Switch**#conf t**

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#**interface vlan 1**
Switch(config-if)#**ip address 10.0.0.2 255.255.0.0**
Switch(config-if)#**interface FastEthernet0/1**
Switch(config-if)#**switchport mode trunk**
Switch(config-if)#**no shut**

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip address 10.0.0.2 255.255.0.0
Switch(config-if)#interface FastEthernet0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#
Mar 30 01:30:31.602: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
Mar 30 01:30:32.600: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
Mar 30 01:30:35.611: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Switch(config-if)#no shut
Switch(config-if)#
Mar 30 01:31:04.636: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

Je copie ensuite via putty connecté sur le port console l'image du firmware stocké sur mon serveur tftp en lui renseignant son adresse IP vers le nvram dans l'emplacement des images:
Switch#**copy tftp://10.0.0.1/c2960c405-universalk9-mz.152-7.E3.bin flash:**

```
Switch#copy tftp://10.0.0.1/c2960c405-universalk9-mz.152-7.E3.bin flash:
Destination filename [c2960c405-universalk9-mz.152-7.E3.bin]?
Accessing tftp://10.0.0.1/c2960c405-universalk9-mz.152-7.E3.bin...
Loading c2960c405-universalk9-mz.152-7.E3.bin from 10.0.0.1 (via Vlan1): !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 18160640 bytes]

18160640 bytes copied in 290.229 secs (62573 bytes/sec)
Switch#
```

Je lui donne la commande pour lui dire de démarrer sur l'image que je viens de lui envoyer:
boot system flash:c2960c405-universalk9-mz.152-7.E3.bin

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#boot system flash:c2960c405-universalk9-mz.152-7.E3.bin
Switch(config)#end
Switch#
Mar 30 01:43:58.661: %SYS-5-CONFIG_I: Configured from console by console
Switch#wr
Building configuration...
[OK]
Switch#reload
mifs[5]: 587 files, 21 directories
mifs[5]: Total bytes     :   59996160
mifs[5]: Bytes used      :   38175232
mifs[5]: Bytes available :   21820928
mifs[5]: mifs fsck took 18 seconds.
...done Initializing Flash.
done.
Loading "flash:c2960c405-universalk9-mz.152-7.E3.bin"...@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
```

Je liste les anciens firmware pour les supprimer et faire de la place dans la nvram:
Switch#**dir flash:/c2960c405-universalk9-mz.150-2.SE5/**
Et je supprime le dossier :
delete /**recursive** /**force flash:/c2960c405-universalk9-mz.150-2.SE5**

2. Précisez les moyens utilisés :

Un commutateur cisco 2960c12pc, un pc, un câble rj45 et un câble console, accès internet

3. Avec qui avez-vous travaillé ?

seul

4. Contexte

Nom de l'entreprise, organisme ou association ▸ *CHU*

Chantier, atelier, service ▸ Service Réseau

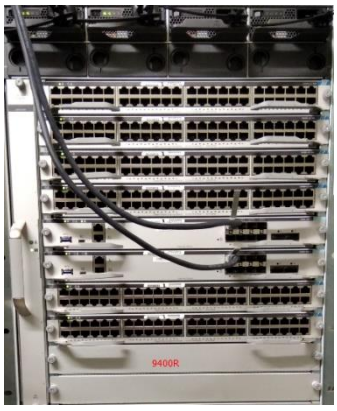
Période d'exercice ▸ Du : *15/04/2021* au : *28/05/2021*

5. Informations complémentaires *(facultatif)*

Activité-type 2 — Maintenir, exploiter et sécuriser une infrastructure centralisée

Exemple n° 2 ▸ MISE A JOUR FIRMWARE ET CONFIGURATION COMMUTATEUR Cisco c9400R

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :



<u>Mise à jour firmware Catalyst c9400R</u>
Réception et déballage de 4 châssis catalyst commutateurs cisco c9400R (gauche) comprenant 10 emplacements permettant d'insérer deux cartes CPU et 8 cartes 48 ports Ethernet, dans le but de remplacer un commutateur 4507(droite) qui ne qui ne contient pas assez de slot de carte 48 ports.

Je dois mettre à jour les firmware (cisco ios) des cartes CPU pour chaque commutateur 9400R. Le fichier image est téléchargeable sur le site cisco avec un compte. Je le copie sur un support USB, me connecte au port console du commutateur via un client comme putty, je rentre dans le mode 'enable', j'insère ma clé dans le port USB, un message m'indique qu'elle est trouvée et montée.

Je vérifie la version du firmware actuellement installé sur le commutateur (#show version), il se trouve qu'elle est plus ancienne. Je liste le contenu des images de démarrage présent dans la mémoire flash (dir flash:) et vérifie sur quelle image il boot (show boot:)

```
Switch#show boot
BOOT variable = bootflash:cat9k_iosxe.16.06.02.SPA.bin
```

Je liste le contenu de ma clé USB

```
Switch#dir usbflash0:
Switch#..cat9k_iosxe.17.03.03.SPA.bin
```

Je lance la copie et l'installation de la version plus récente vers la mémoire flash
« install add file usbflash0:cat9k_iosxe.17.03.03.SPA.bin activate commit »

```
Switch#install add file usbflash0:cat9k_iosxe.17.03.03.SPA.bin activate commit
install_add_activate_commit: START Tue Apr 29 10:12:44 UTC 2021
System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration....
Downloading file usbflash0:cat9k_iosxe.17.03.03.SPA.bin
Finished downloading file...
install_add_activate_commit: Adding ISSU
```

Ce qui va générer un fichier 'packages.conf' qui est le fichier des informations de l'image de démarrage, je vérifie :

```
Switch#dir flash:*.conf
Directory of bootflash:/*.conf
Directory of bootflash:/
681444   -rw-        7715  Apr 29 2021 12:47:45 +00:00  packages.conf
11250098176 bytes total (9700368384 bytes free)
```

Après la procédure d'installation et redémarrage du commutateur, je vérifie que la nouvelle version du firmware soit installée et que la partition contienne bien les fichier pkg:

```
Switch#show version
Cisco IOS XE Software, Version 17.03.03
Cisco IOS Software [Amsterdam], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.3.3, RELEASE SOFTWARE (fc7)
Technical Support: http://www.cisco.com/techsupport
.................
ROM: IOS-XE ROMMON
BOOTLDR: System Bootstrap, Version 17.3.1r[FC2], RELEASE SOFTWARE (P)"

Switch#dir flash:
Directory of bootflash:/
....
681442  -rw-        47364227  Apr 29 2021 12:42:26 +00:00  cat9k-rpboot.17.03.03.SPA.pkg
681441  -rw-            9220  Apr 29 2021 12:41:46 +00:00  cat9k-wlc.17.03.03.SPA.pkg
```

Et je supprime les anciennes versions (#install remove inactive):

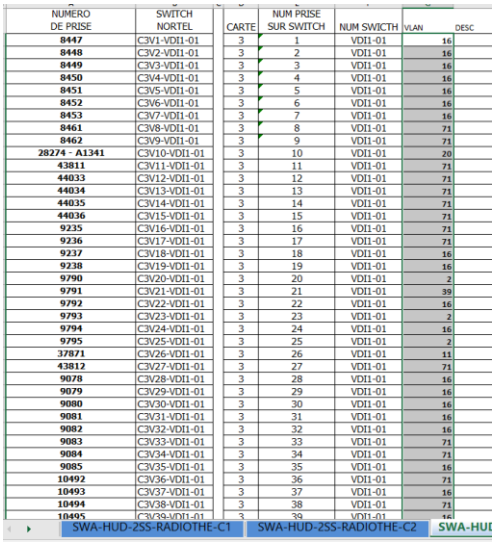
```
Switch#install remove inactive
install_remove: START 09:43:00 UTC 2021
*09:43:00.679: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install removeCleaning up unnecessary package files
No path specified, will use booted path bootflash:packages.conf
Cleaning bootflash:
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    cat9k-cc_srdriver.16.02.03.SPA.pkg
.....
09:43:06.738: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed install remove
```

Je redémarre (#reload), et revérifie la bonne version.
Le firmware du commutateur est à jour.
Je dois à présent insérer 4 cartes 48 ports supplémentaires, deux vis à dévisser pour enlever le cache et les insérer, puis je les clips et revisse.

<u>Configuration du commutateur</u>

N'ayant pas accès aux mots de passe d'authentification des switch on me fournit un fichier (copie de la sortie #sh run, sh vlan et #sh int description) de la configuration de l'ancien switch comprenant pour un, les descriptions des interfaces qui correspondent au numéro de prise, et pour le second les identifiants de vlan correspondant aux interfaces, j'utilise notepad++ et son outil rechercher/remplacer pour ne faire apparaître que les descriptions et vlan afin de me faciliter la tâche.

Je renseigne dans un fichier Excel élaboré par le personnel de l'entreprise, les numéros de prises qui correspondent aux descriptions des interfaces ainsi que les identifiants de vlan sur les interfaces. Chaque onglet du fichier Excel correspond à une carte 48 ports du commutateur (exemple capture droite). Ce fichier contient une formule qui va générer la configuration de chaque interface des cartes du commutateur (1). Les interfaces sont en gigabits et sont nommés pour les identifier : giga1/0/xx
(giga : pour interface gigabite, 1/0/xx : numéro emplacement de carte dans le chassis /0/xx : numéro de port sur la carte).



NUMERO DE PRISE	SWITCH NORTEL	CARTE	NUM PRISE SUR SWITCH	NUM SWITCH	VLAN	DESC
8447	C3V1-VDI1-01	3	1	VDI1-01	16	
8448	C3V2-VDI1-01	3	2	VDI1-01	16	
8449	C3V3-VDI1-01	3	3	VDI1-01	16	
8450	C3V4-VDI1-01	3	4	VDI1-01	16	
8451	C3V5-VDI1-01	3	5	VDI1-01	16	
8452	C3V6-VDI1-01	3	6	VDI1-01	16	
8453	C3V7-VDI1-01	3	7	VDI1-01	16	
8461	C3V8-VDI1-01	3	8	VDI1-01	71	
8462	C3V9-VDI1-01	3	9	VDI1-01	71	
28274 - A1341	C3V10-VDI1-01	3	10	VDI1-01	20	
43811	C3V11-VDI1-01	3	11	VDI1-01	71	
44033	C3V12-VDI1-01	3	12	VDI1-01	71	
44034	C3V13-VDI1-01	3	13	VDI1-01	71	
44035	C3V14-VDI1-01	3	14	VDI1-01	71	
44036	C3V15-VDI1-01	3	15	VDI1-01	71	
9235	C3V16-VDI1-01	3	16	VDI1-01	71	
9236	C3V17-VDI1-01	3	17	VDI1-01	71	
9237	C3V18-VDI1-01	3	18	VDI1-01	16	
9238	C3V19-VDI1-01	3	19	VDI1-01	16	
9790	C3V20-VDI1-01	3	20	VDI1-01	2	
9791	C3V21-VDI1-01	3	21	VDI1-01	39	
9792	C3V22-VDI1-01	3	22	VDI1-01	16	
9793	C3V23-VDI1-01	3	23	VDI1-01	2	
9794	C3V24-VDI1-01	3	24	VDI1-01	16	
9795	C3V25-VDI1-01	3	25	VDI1-01	2	
37871	C3V26-VDI1-01	3	26	VDI1-01	11	
43812	C3V27-VDI1-01	3	27	VDI1-01	71	
9078	C3V28-VDI1-01	3	28	VDI1-01	16	
9079	C3V29-VDI1-01	3	29	VDI1-01	16	
9080	C3V30-VDI1-01	3	30	VDI1-01	16	
9081	C3V31-VDI1-01	3	31	VDI1-01	16	
9082	C3V32-VDI1-01	3	32	VDI1-01	16	
9083	C3V33-VDI1-01	3	33	VDI1-01	71	
9084	C3V34-VDI1-01	3	34	VDI1-01	71	
9085	C3V35-VDI1-01	3	35	VDI1-01	16	
10492	C3V36-VDI1-01	3	36	VDI1-01	71	
10493	C3V37-VDI1-01	3	37	VDI1-01	16	
10494	C3V38-VDI1-01	3	38	VDI1-01	71	
10495	C3V39-VDI1-01	3	39	VDI1-01	16	

SWA-HUD-2SS-RADIOTHE-C1 | SWA-HUD-2SS-RADIOTHE-C2 | SWA-HUI

(1)

C	D	E	F	G
ce giga1/0/1 ıtion 44189 -	authentication event fail action authorize vlan 2	authentication event no-response action authorize vlan 2		interface giga1/0/1 description 44189 - authentication event fail action authorize vlan 2 authentication event no-response action authorize vlan 2
ce giga1/0/2 ıtion 44190 -	authentication event fail action authorize vlan 71	authentication event no-response action authorize vlan 71		interface giga1/0/2 description 44190 - authentication event fail action authorize vlan 71 authentication event no-response action authorize vlan 71
ce giga1/0/3 ıtion 44191 -	authentication event fail action authorize vlan 71	authentication event no-response action authorize vlan 71		interface giga1/0/3 description 44191 - authentication event fail action authorize vlan 71 authentication event no-response action authorize vlan 71
ce giga1/0/4 ıtion 44192 -	authentication event fail action authorize vlan 71	authentication event no-response action authorize vlan 71		interface giga1/0/4 description 44192 - authentication event fail action authorize vlan 71 authentication event no-response action authorize vlan 71

Je modifie dans un document texte le fichier de configuration (startup-config), voici les principales modifications à apporter :

hostname SWA-HUD-2SS-RADIOTHERAPIE-VDI1-01..... ## nom du switch
!.....
spanning-tree vlan 2,3,8,9,11,14,16,20.....## renseigner les vlan pour le spanning-tree
!.....
vlan 2.....## identifiant de vlan
name IMAGERIE.....## nom de vlan
!
vlan 3..... ## identifiant de vlan
name MANAGEMENT.....## nom de vlan.
!.....
interface TenGigabitEthernet5/0/1.....## conf interface10giga carte CPU avec id vlan
desc ** Vers R458(TE2/1/22) ** en mode trunk sur l'interface
switchport trunk allowed vlan 2,3,8,9,11,14,16,20,27,31,34,39,71,74-77,86-89
switchport trunk allowed vlan add 97,219,306-309,407-410
!.....
interface Port-channel.....## conf. du groupe de port
desc ** Vers R458(po38) **
switchport trunk allowed vlan 2,3,8,9,11,14….
!.....
interface range GigabitEthernet1/0/1-48.....## configuration intervalle de port 1 à 48
switchport mode access pour chaque carte
switchport voice vlan 306
authentication event fail action authorize vlan 71.....## si pas de réponse certificat ou mac
authentication event no-response action authorize vlan 71.....##elle est dirigée dans le vlan 71 isolé.
authentication order dot1x mab.....## authentification par certificat (dot1x)
authentication priority dot1x mab.....## authentification par adresse mac (mab)
!.....

Je me connecte au port console pour injecter le fichier de configuration en connectant la clé USB sur lequel se trouve le fichier et exécute la commande : **#copy usbflash0 :fichierconfig startup-config**
Je redémarre le switch (reload), vérifie que le switch ait pris la configuration (sh run). Je passe en mode configuration (#conf t), puis je copie/colle par bloc de 24 pour éviter les erreurs, les descriptions des interfaces pour chaque carte 48 ports (giga1/0/1 à 48,giga2/0/1à48….) , ex :

```
interface giga1/0/1
description 44189 -
authentication event fail action authorize vlan 2      #ici le passage dans le vlan 2 sur la prise 44189 est forcé
authentication event no-response action authorize vlan 2      "
interface giga1/0/2
description 44190 -
authentication event fail action authorize vlan 71      #tout ce qui n'est pas certifié par l'ise est dirigé dans
authentication event no-response action authorize vlan 71      le vlan 71 (« poubelle »)
…
```

C'est donc dans « l'ISE (Identity Service Engine) » avec la fonction d'authentification IEEE 802.1X et le protocole aaa Radius (synchroniser avec ldap) que sont filtrées les authentification aux ports par certificats (pc client avec anyconnect) et adresses mac (bornes wifi, téléphones, tablettes), toutes machines non authentifiées sera dirigées et isolées vers le vlan « poubelle » (71) . Les autorisations se font au travers de « l'ISE » en fonction de la localisation du bâtiment, l'emplacement (étage) dans le bâtiment du switch, de l'id de vlan via certificat ou adresse mac.

2. Précisez les moyens utilisés :

Un pc, commutateurs Cisco, câble usb air console, clé usb

3. Avec qui avez-vous travaillé ?

Seul et en équipe

4. Contexte

Nom de l'entreprise, organisme ou association ▸ *CHU*

Chantier, atelier, service ▸ Service réseau

Période d'exercice ▸ Du : *15/04/2021* au : *28/05/2021*

5. Informations complémentaires *(facultatif)*

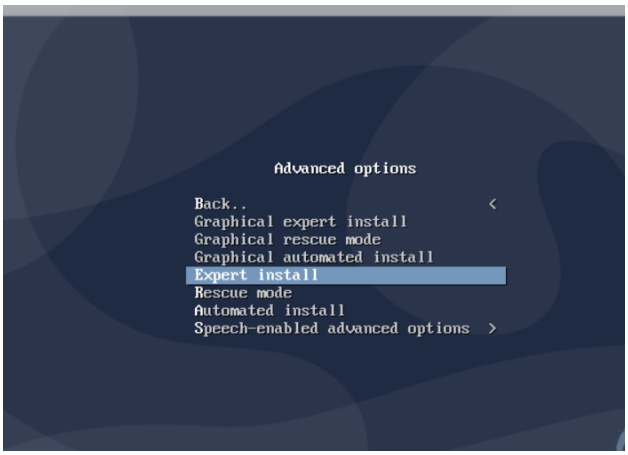
Activité-type 2 — Maintenir, exploiter et sécuriser une infrastructure centralisée

Exemple n° 3 ▸ ***Installation DEBIAN serveur web et GLPI***

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

DEBIAN serveur web et GLPI

INSTALLATION DU SERVEUR (DEBIAN) création de deux machines virtuelles



Je démarre sur l'iso situé dans la banque de donnée (voir Vsphere activité 3).
L'écran de démarrage de d'installeur Debian s'affiche, Je sélectionne les menus en surbrillance valide par entrée mes choix. Je choisi le mode « Expert install » et les fenêtres d'installation démarre, je sélectionne et valide par 'entrée' : Choix de la langue, français, pays, France, jeux de paramètres régionaux (locales) France-fr_FR.UTF-8 qui correspond à l'affichage des nombres, des dates (mois, jours, devises …), configuration du clavier, français. Puis l'installateur va proposer de charger les composants d'installation à partir du support, et de choisir des composants supplémentaires à charger, je choisis un miroir (lien http, qui contient les fichiers relatifs à l'installation), je coche également "network-console: Continue installation remotely using SSH" afin de continuer l'installation depuis un PC client distant avec un logiciel tel que putty ou mobaxterm... à condition que le client et le serveur soit sur le même réseau, ou un réseau accessible de l'un vers l'autre (je renseignerai plus loin un mot de passe pour l'utilisateur 'installer', pour l'accès ssh). L'installateur me propose de configurer le réseau via dhcp ou manuellement, je connais l'adresse IP qui sera attribuée en statique au serveur et la lui renseigne ainsi que le masque de sous réseau (complet ou format CIDR), la passerelle, ainsi que les serveurs dns, ce qui évitera de configurer par la suite la carte réseau via le fichier/etc/network/interfaces.
Je donne un nom à la machine, renseigne un domaine s'il y a lieu. Je choisi l'adresse miroir (lien http basé en France) pour récupérer les paquets d'archives nécessaires à l'installation du système.
Je créé les noms et mots de passe utilisateur(s), ainsi que le mot de passe Root.
Je configure le disque en choisissant la taille voulue, je choisis le noyau à installer (la couche de base du système d'exploitation, le noyau gère la mémoire, l'accès aux périphériques, la circulation des données sur le bus, les droits d'accès, les multiples processus qui correspondent aux multiples tâches que l'ordinateur doit exécuter en même temps) ...
J'active la liste des dépôts (qui sera renseignée dans /etc/apt/sources.list) et coche les accès aux dépôts non-free (pilotes propriétaires) et rétro porté (backports) qui contient des paquets 'dépassés' et recompilés pour les branches stables de Debian (phpmyadmin par exemple que j'utilise).
Je ne coche ici, dans l'installation de logiciels, que le serveur ssh, afin d'avoir accès par la suite.
J'installe Grub, le programme de démarrage du système, sur le disque dur puis confirme l'heure universelle utc.
L'Installation est terminée, le système redémarre.
J'aurai accès à la machine via ssh avec l'utilisateur créé durant l'installation, pas d'accès root en ssh et pourrai passer en root (super utilisateurs) avec la commande 'su -' afin d'obtenir les droits root et les bonnes variables

d'environnement.
(Pour la sécurité pas d'accès root en ssh, seul des comptes autorisés auront des accès super utilisateurs via sudo en les renseignant temporairement dans /etc/sudoers (l'installation du paquet sudo est nécessaire : apt install sudo). L'installation terminée, j'exécute une mise à jour de la liste des paquets (#apt update), afin de vérifier s'il existe des mises à jours disponibles. (#apt upgrade, en cas de mises à jour).

INSTALLATION DE SERVEUR WEB ET GLPI POUR GESTION MATERIEL ET TICKETS DE DEMANDE D'AIDE ET DEPANNAGE

J'utilise apache2 comme serveur web http. Je l'installe en root: apt install apache2.
Deux fichiers de configuration (000-default.conf qui écoute sur le port 80 :http et default-ssl.conf qui écoute sur le port 443 :https sécurisé par certificats CA), sont créés dans /etc/apache2/sites-available, qui servent d'exemple de configuration ou peuvent servir de fichiers de configuration.
Pour l'installation de glpi je copie le lien de l'adresse URL de téléchargement sur le site de GLPI puis l'utilise pour télécharger GLPI sur le serveur via le paquet wget et décompresse l'archive téléchargée dans l'emplacement /var/www/, en renommant le dossier décompressé (mv glpi glpi.mondomaine). Je change le propriétaire du dossier et son contenu par www-data (chown www-data:www-data –R glpi.mondomaine). J'installe les paquets nécessaires au bon fonctionnement de GLPI à savoir les paquets php nécessaires (apt install php-7.3 php-mysqli php-mbstring php-curl php-gd php-intl php-simplexml php-ldap php-apcu php-xmlrpc php-cas php-zip php-bz2).
Pour la configuration de l'hôte virtuel (virtualhosts) dans apache2 je copie et colle en changeant le nom pour glpi.mondomaine du fichier 000-default.conf (cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/glpi.mondomaine), j'édite le fichier renseignant dans les directives, le nom du serveur (glpi.mondomaine) et l'emplacement du répertoire du site /var/www/glpi.mondomaine

```
  GNU nano 4.8

<VirtualHost *:80>
        # The ServerName directive sets the request scheme.
        ServerName glpi.mondomaine
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/glpi.mondomaine
```

J'active le site avec la commande 'a2ensite', ce qui va créer un lien symbolique dans /etc/ap ache2/sites-enabled/.
Dans le cas de cette configuration et pour joindre le site glpi.mondomaine par son nom, un serveur DNS (windows serveur,bind9,unbound….) est obligatoire pour résoudre l'adresse IP au nom du site glpi.mondomaine. En effet le serveur web dans cette configuration écoute sur le port 80 (http), lorsque le nom est renseigné dans le navigateur, le serveur dns résout l'IP du serveur, et le serveur répond sur le port 80 avec le fichier hosts qui répond au nom (ServerName glpi.mondomaine) puis ouvre la page du site qui se trouve dans le répertoire (DocumentRoot /var/www/glpi .mondomaine).
J'installe sur une seconde machine un deuxième serveur Debian qui va me servir à stocker les bases de données, j'installe donc ici les paquets du serveur web : apache2, un serveur SQL : défaut-mysql-server, php en version 7.3 : php-7.3, ainsi que phpmyadmin pour la gestion des utilisateurs SQL. J'édite le fichier /etc/mysql/mariadb.conf.d/50-server.cnf avec nano et fais le changement :
bind-address = 127.0.0.1 par bind-address = 0.0.0.0 afin d'autoriser les connexions de mon serveur GLPI vers le serveur de base de données, puis je redémarre le service (/etc/init.d/mysql restart). Pour plus de sécurité il est conseillé d'établir des règles iptables ou ufw sur le serveur SQL en n'autorisant que l'ip du serveur GLPI sur le port 3306 (sql) et le port 22 (ssh pour les machines admin clients autorisées).
J'installe phpmyadmin via les dépôts backports, et l'installe pour une configuration avec apache2, je créé un mot de passe pour l'utilisateur phpmyadmin et donne tous les privilèges:

```
mysql>
GRANT ALL PRIVILEGES ON *.* TO 'phpmyadmin'@'localhost' WITH GRANT OPTION;
Query ok
```

Afin de me connecter à l'interface et pouvoir créer des utilisateurs et base de données sql.
J'ouvre un navigateur sur un PC client tape l'adresse IP du serveur sql (http://ipserver/phpmyadmin) pour me connecter à l'interface web phpmyadmin et créer l'utilisateur, mot de passe et base de données GLPI.
Je saisis ensuite l'adresse http://glpi.mondomaine pour lancer la première configuration et création de la base de données de GLPI. Dans les fenêtres qui apparaissent je sélectionne français puis suivant, Une page me montre que les tous les modules php nécessaires sont installés avec succès, au moment de rentrer l'adresse et le nom d'utilisateur de la base de données mysql, je renseigne l'adresse ip du serveur où est installé mysql. Je patiente le temps que la base de donnée se construise, une fois terminé mon glpi est accessible et utilisable à l'adresse http://glpi.mondomaine.
(À noter que j'utilise le terme 'mysql' mais lorsque l'on installe 'default-mysql-server sur Debian, c'est 'mariadb, qui est installé).

2. Précisez les moyens utilisés :

Un pc, machines virtuelle, iso et application d'installation

3. Avec qui avez-vous travaillé ?

seul

4. Contexte

Nom de l'entreprise, organisme ou association ▸ *Chu et personnel*

Chantier, atelier, service ▸ Service Réseau

Période d'exercice ▸ Du : *15/04/2021* au : *28/06/2021*

5. Informations complémentaires *(facultatif)*

Activité-type 3

Maintenir, exploiter une infrastructure distribuée et contribuer à sa sécurisation

Exemple n° 1 ▸ ***Configuration firewall StormShield SN300 et vpnssl***

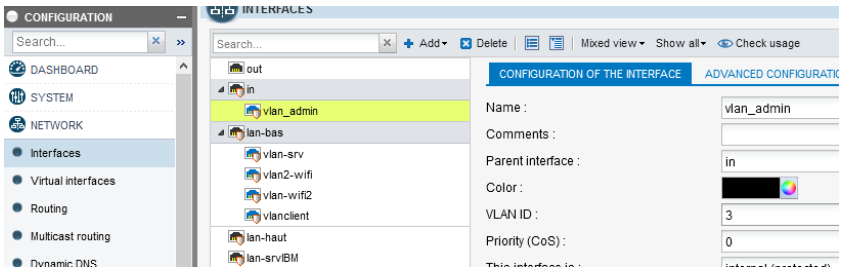
1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

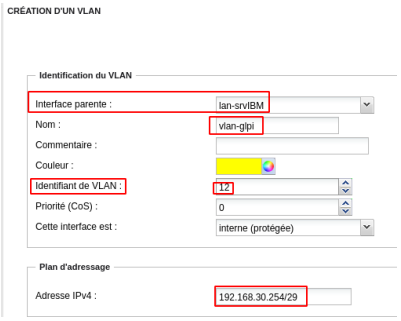
Le pare-feu est un élément essentiel pour la sécurisation d'un réseau. Il permet, entre autre, grâce à un ensemble de règles, de définir des autorisations d'accès entre les différents vlans (utilisateurs, serveurs, impression...), mais également depuis et vers internet. Je connecte un câble RJ45 sur l'interface 2 administration du firewall et sur un PC client, que je configure avec une IP fixe sur le même réseau que cette interface pour avoir un accès à l'interface web d'administration du firewall via le navigateur internet (ici l'adresse ip administration est 10.0.0.254/16 et le pc client 10.0.0.1/16)**.** Je renseigne l'adresse https://10.0.0.254/admin dans le navigateur pour accéder à la page d'identification et d'authentification ou je renseigne le login et mot de passe par défaut. Pour augmenter la sécurité je change le mot de passe admin dans le menu système administrateur onglet compte admin, je crée aussi un objet port d'écoute d'accès à l'interface web, j'active la protection contre les attaques par brute force, avec trois tentatives d'authentification autorisées, un blocage de 5 minutes. J'active l'accès ssh sur un port spécifique et je rajouterai plus tard des autorisations d'accès administration seulement à certaines machines autorisées.

<u>configuration des interfaces</u>

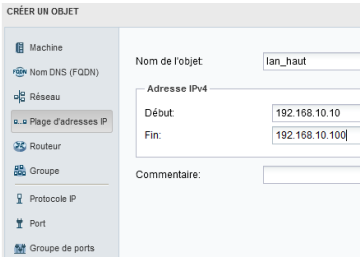
Dans le menu réseau, interfaces, je renseigne un nom et une IP statique aux interfaces qui seront utilisées comme passerelle sur leur réseau.

L'interface out sera externe, et aura une adresse IP sur le réseau du routeur qui donne accès à Internet.
L'interface 2 (in) IP réservée à l'Administration, avec éventuellement un vlan (avec id 3 par exemple) administration lié à cette interface.
Les interfaces DMZ 1, 2, et 3 sont trois réseaux avec une adresse IP statique chacune qui est la passerelle de ces réseaux. (Exemple: interface dmz1 a l'adresse 192.168.10.1/24), des vlan avec leur numéro identifiant et description sont liés à des interfaces.





L'interface DMZ 1 (lan_bas), est connectée à l'interface Gigabit d'un switch HP ProCurve, ou trois vlan sont tagués sur le switch, le vlan serveur, des vlan borne wifi..)
Le firewall peut faire serveur dhcp, auquel cas il faut créer des objets plage d'adresse IP correspondants aux réseaux des interfaces.
(exemple: pour l'interface dmz 2 (lan_haut) je peux définir la plage d'adresse '192.168.10.10 à 192.168.10.100), même chose au besoin pour chaque interface et vlan liés aux interfaces.



Pour les machines ayant besoin d'une adresse IP statique (comme les serveurs), je créé les objets machines en renseignant l'adresse mac de la carte réseau de la machine et une adresse IP sur le réseau où sera connecté la machine, afin de la renseigner dans les réservations d'adresse.

Les règles de filtrage

Les règles de filtrage permettent d'autoriser les communications entre machines vers machines, ou vers réseau, ou réseau vers réseau … en utilisant et autorisant différents services. Elles sont lues de haut en bas et ce qui n'est pas explicitement autorisé est interdit (la dernière règle bloque tout). Pour pouvoir sortir vers internet il faut créer des règles autorisant des ports sortant spécifiques : https (443), http(80), dns(53).

En exemple ici j'autorise le réseau « lan_haut » à communiquer vers internet sur les ports spécifiés :

État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité
on	passer	Network_lan-bas	Internet	https		IPS
on	passer	Network_lan-bas	Internet	dns		IPS
on	passer	Network_lan-bas	Internet	ntp		IPS
on	passer	Network_lan-bas	Internet	http		IPS

(A noter que je pourrais créer un groupe de port pour les services de messagerie.)

Pour que le retour des paquets soit possible il est obligatoire, comme indiqué dans la documentation, de créer une règle de nat (network address translation) pour rediriger les ports ephemeral vers le réseau interne :

État	Trafic original (avant translation)				Trafic après translation			
	Source	Destination	Port dest.		Source	Port src.	Destination	P
on	Network_internals	Internet interface: out	Any	→	Firewall_out	ephemeral_fw	Any	

Les règles sont mises en place et affinées en fonction des besoins.

Pour reprendre ma maquette test du serveur glpi et mysql, la règle est mise en place dans le parefeu, qui n'autorise la connexion du serveur glpi vers le serveur mysql que sur le port 3306 mysql

État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité	Co
règles-serveur-glpi-sql (contient 1 règles, de n° 1 à n° 1)							
on	passer	serveur-glpi	serveur-mysql	mysql		IPS	Cr

Ainsi qu'une règle pour l'administration ssh sur port 22

État	Action	Source	Destination	Port dest.	Protocole	Inspection de s
rveur-glpi (contient 1 règles, de n° 1 à n° 1)						
on	passer	Network_vlan_admin	serveur-glpi serveur-mysql	ssh		IPS

Ici je créé une règle qui autorise le réseau vlan des PC client à accéder à la machine serveur d'impression sur le port 9100 :

État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité
veur-impression (contient 1 règles, de n° 1 à n° 1)						
on	passer	Network_vlanclient	srv-impression	port-impression-9100		IPS

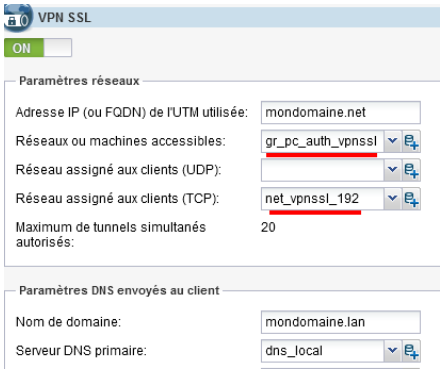
Afin de permettre l'accès à un serveur web hébergé pas l'entreprise sur un vlan serveur (dmz) depuis internet, je dois créer une règle de filtrage autorisant les adresses IP publiques venant d'internet à accéder à l'interface publique (Firewall_out) du pare-feu sur le port https (443, port d'écoute du serveur apache) :

État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité
on	passer	Any	Firewall_out	https		IPS

Je dois également créer une règle de NAT (port forwarding) pour rediriger le flux https arrivant sur le pare-feu vers mon serveur web local situé sur la zone serveur (dmz) :

État	Source	Destination	Port dest.		Source	Port src.	Destination	Port dest.
on	Any interface: out	Firewall_out	https	→			server-wwweb	https

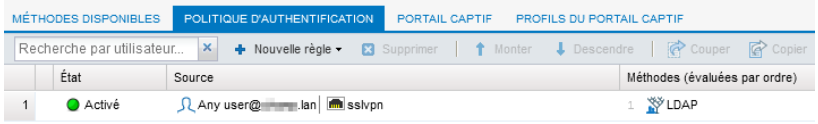
Les règles sont mises en place en fonction des besoins.
Activation du vpn ssl sur le stormshield, pour permettre des accès depuis internet à des machines locales (bureau à distance) ou des serveurs en établissant une connexion sécurisée entre un client et le pare-feu.

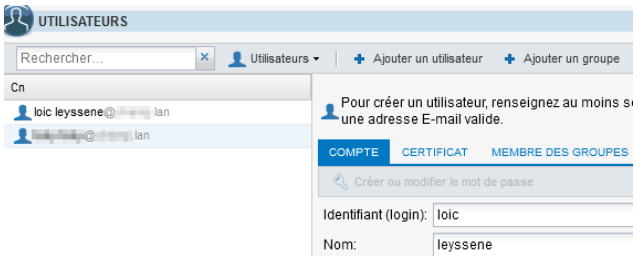


Je créé l'objet réseau net_vpnssl_192 : 192.168.222.0/24 qui est le réseau assigné aux clients connecté via le vpn, je créé un groupe de machines qui devra être accessible par les clients : gr_ pc_etab_vpnssl, je renseigne le nom de domaine public qui permet d'accéder à la connexion vpn sur l'interface out (extérieur) et renseigne le serveur dns local en premier.
J'active le vpn ssl (on).

J'active le portail captif sur l'interface out

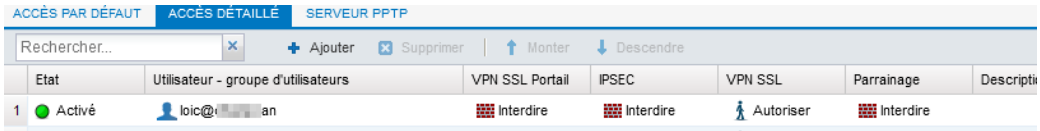
Je créé une règle standard de politique d'authentification, utilisant l'annuaire ldap local du stormshield



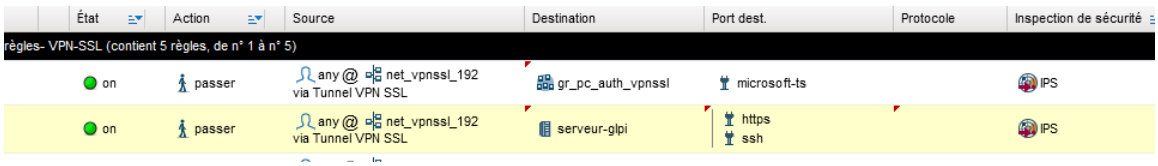


Je créé alors les utilisateurs dans l'annuaire ldap du stormshield

Enfin j'autorise la politique d'accès par défaut au vpn ssl, ainsi que les accès détaillés par utilisateur



Je créé les règles autorisant les clients à se connecter à des sessions sur les machines renseignées dans le groupe de PC autorisés.



Les clients se connectent via un client vpn ssl pour PC ou mobile qui se télécharge en s'identifiant sur le portail du stormshield.

2. Précisez les moyens utilisés :

Un pc, un firewall Stormshield, un câble RJ45, un commutateur hp pro curve

3. Avec qui avez-vous travaillé ?

seul

4. Contexte

Nom de l'entreprise, organisme ou association ▸ *Domicile*

Chantier, atelier, service ▸ domicile

Période d'exercice ▸ Du : *01/05/2021* au : *Cliquez ici*

5. Informations complémentaires *(facultatif)*

Activité-type 3

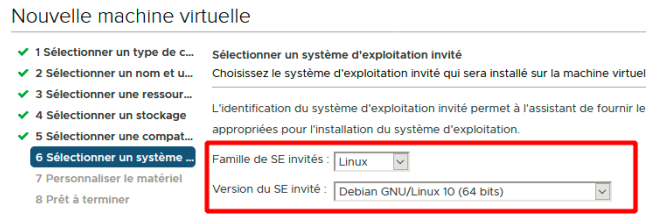
Maintenir, exploiter une infrastructure distribuée et contribuer à sa sécurisation

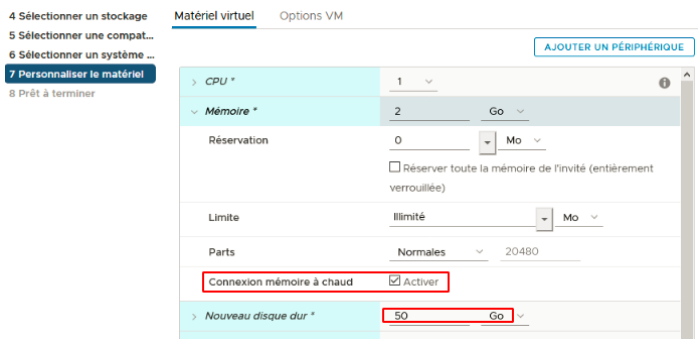
Exemple n° 1 ▸ ***Vsphere : création machine virtuelle***

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Dans l'entreprise, les hôtes esxi (~63) et vsphere sont installés sur des serveurs UCS (Unified Cisco System) situés dans des châssis de huit emplacements, le san est installé sur des serveurs Dell (emc vplex xtremio) avec 26,26To de stockage physique ; avec un ratio de 1,6 de compression et 2,0 de déduplication, on attend 86,50To utilisable. Les LUN (unité de stockage) du san, accueil environ 1119 VM. Je vais créer deux vm test afin d'installer deux serveurs Debian, un pour glpi et un pour la base de données en vue d'une migration d'un serveur glpi fonctionnant sur Windows.
Dans cette infrastructure il existe deux cluster principaux : toip pour les serveurs de téléphonie et UCS pour les esxi en production, je créé une vm dans le dossier test du cluster ucs dans vsphere qui se chargera de déterminer l'emplacement sur les hôtes par rapport à la charge. Le stockage des vm se fait sur le san. Je prends une lun qui a le plus grand espace de stockage.

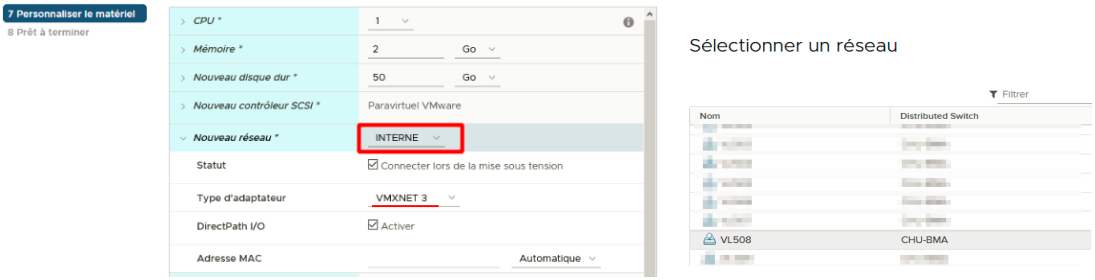
Au moment de sélectionner un système d'exploitation invité, je sélectionne bien la famille de système Linux en version Debian 10 64 bits.



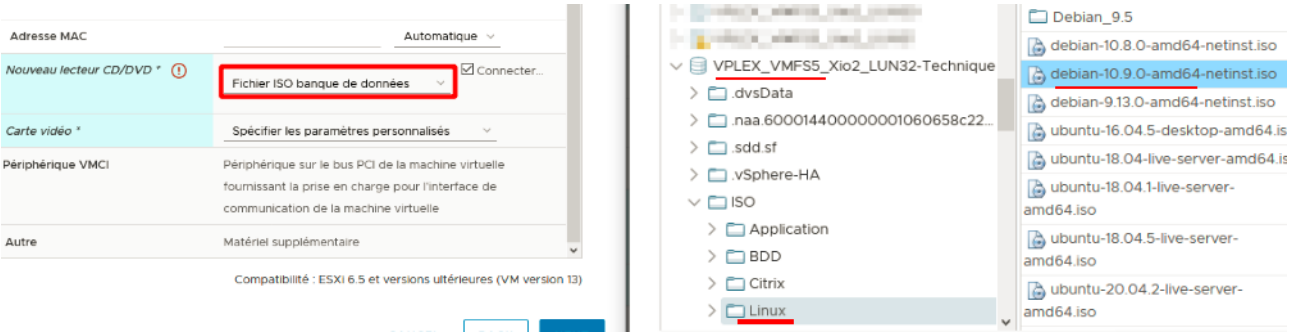


Pour la personnalisation du matériel, je coche pour le cpu « activer les modifications à chaud » et pour la mémoire je coche « activer » pour les « connexions de mémoire à chaud » et renseigne une taille de 50 Go pour disque dur qui accueillera le serveur glpi, et sélectionne réseau interne.

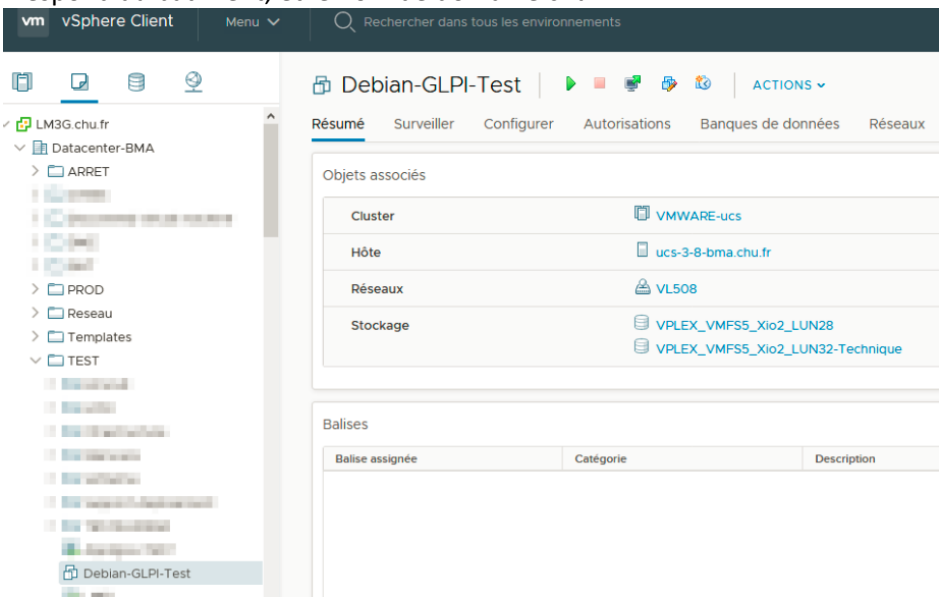
Concernant la partie réseau, je sélectionne réseau interne, sur l'adaptateur virtuel « vmxnet3 » et sélectionne le vlan (508) dédier au serveur intranet sur le réseau.



Pour l'installation du système je sélectionne « Fichier iso banque de données » car les fichiers images sont stockés sur une LUN du san.



La machine virtuelle est donc créée dans le dossier d'organisation test, du cluster vmware-ucs, connecté au réseau sur le vlan508, elle est stockée sur le san vplex_vmfs5_xio2_lun28.
L'hôte esxi est l'ucs-3-8-bma.chu.fr (en ce qui concerne les noms de machines, 'ucs' est le nom du matériel,' 3' est le châssis numéro trois dans la baie, '8' est l'emplacement du serveur numéro huit dans le châssis, 'bma' correspond au bâtiment, et le nom de domaine chu.fr.



Je créé une seconde machine virtuelle sur le même schéma sauf le disque dur qui a une taille de 100 Go, qui servira à accueillir la base de donnée (Debian,mysql).

2. Précisez les moyens utilisés :

Un pc connecté à l'hyperviseur

3. Avec qui avez-vous travaillé ?

En équipe

4. Contexte

Nom de l'entreprise, organisme ou association ▸ *CHU*

Chantier, atelier, service ▸ Service Système

Période d'exercice ▸ Du : *15/04/2021* au : *28/05/2021*

5. Informations complémentaires *(facultatif)*

Titres, diplômes, CQP, attestations de formation

(facultatif)

Intitulé	Autorité ou organisme	Date
Reprenez le contrôle à l'aide de Linux	**OpenClassroom**	28/02/2017
Titre : Installateur Dépanneur Informatique	**APSAH**	09/2018 au 01/2020

Déclaration sur l'honneur

Je soussigné(e) [prénom et nom] LEYSSENE Loïc ,

déclare sur l'honneur que les renseignements fournis dans ce dossier sont exacts et que je suis l'auteur(e) des réalisations jointes.

Fait à BRIVE la Gaillarde le 01/06/2021

pour faire valoir ce que de droit.

Signature :

Documents illustrant la pratique professionnelle

(facultatif)

Intitulé
Cliquez ici pour taper du texte.

ANNEXES

(Si le RC le prévoit)