

RAPPORT D'ALTERNANCE

STRUCTURE D'ACCUEIL : DSI DE LA MUTUELLE VIASANTE

Eloïse DE PERETTI

INSTITUT LIMAYRAC BTS SIO2 2022/2023

FICHE 1 : PRESENTATION DE LA STRUCTURE D'ACCUEIL

1.1. Présentation générale

ViaSanté est une complémentaire santé française certifiée ISO 9001 appartenant au groupe AG2R La Mondiale. Organisme à but non lucratif, AG2R La Mondiale permet d'assurer la protection sociale et patrimoniale de 15 millions d'adhérents et d'une entreprise sur 4. C'est en 2015 que la mutuelle ViaSanté a rejoint le groupe.

1.2. Cœur de métier

En France, l'Assurance maladie ne rembourse que partiellement les dépenses de santé. Ainsi, le rôle d'une mutuelle telle que ViaSanté est de couvrir les frais restants à charge du bénéficiaire. Le montant remboursé dépend alors du contrat souscrit par l'adhérent. En effet, les fonds des complémentaires santé proviennent principalement des cotisations des membres et permettent d'assurer la protection de ceux-ci contre diverses éventualités.

1.3. Organisation de la structure

La gouvernance de ViaSanté est démocratique. Les membres ont donc la possibilité de participer aux décisions de la mutuelle en élisant des représentants. De plus, tous les bénéfices servent à financer des actions concrètes au profit des adhérents puisque ViaSanté n'a pas d'actionnaires à rémunérer.

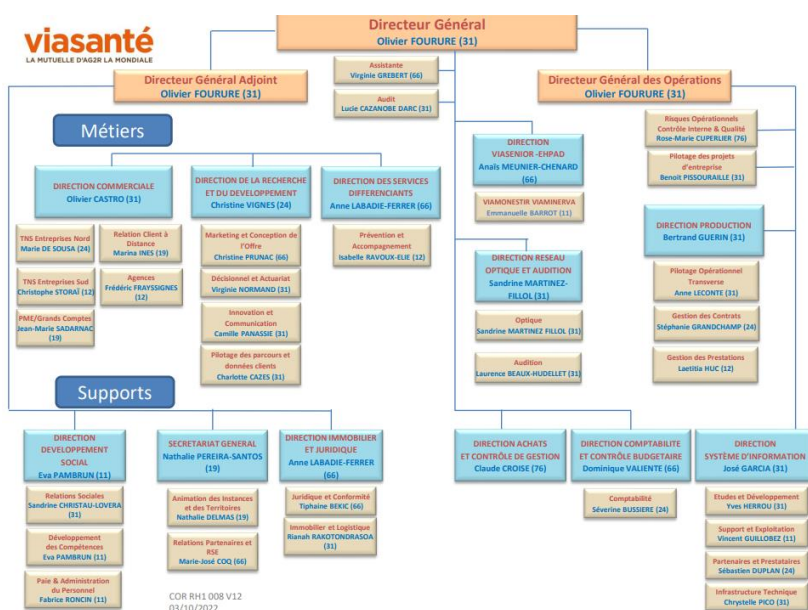


Figure 2: Organigramme général de ViaSanté.



Figure 1: Organigramme la DSI de ViaSanté.

Source des images : livret d'accueil DSI de ViaSanté.

Quelques dates et chiffres

Dates clés

- 2012 : ViaSanté voit le jour à la suite de la fusion de 6 mutuelles interprofessionnelles du grand Sud-Ouest
- 2013 : Entrée en vigueur de l'Accord National Interprofessionnel (A.N.I.)
- 2014 : Intégration de 9 mutuelles supplémentaires
- 2015 : AG2R La Mondiale intègre ViaSanté et REUNICA



Figure 3: Chiffres clés ViaSanté.

Chiffres clés, ViaSanté c'est également ...

- 43 agences sur tout le territoire français
- 1 million de personnes protégées
- 150 délégués mutualistes
- 750 collaborateurs

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	1

FICHE 2 : PRESENTATION DU CONTEXTE DE L'ALTERNANCE

2.1. Tuteur

Mon tuteur pour la durée de l'alternance est Guillaume Ricard, expert Linux au sein du centre de compétence Système du domaine Infrastructure de la D.S.I. ViaSanté. Guillaume est basé sur le site de Rodez et moi sur celui de Labège.

2.2. Positionnement dans l'organisation

Mon alternance a eu lieu principalement sur le site de Labège ainsi que sur celui de Rodez à raison d'une fois par semaine. J'ai intégré l'équipe Système en octobre 2022. La responsable du domaine Infrastructure de la DSI de ViaSanté est Chrystelle Pico.

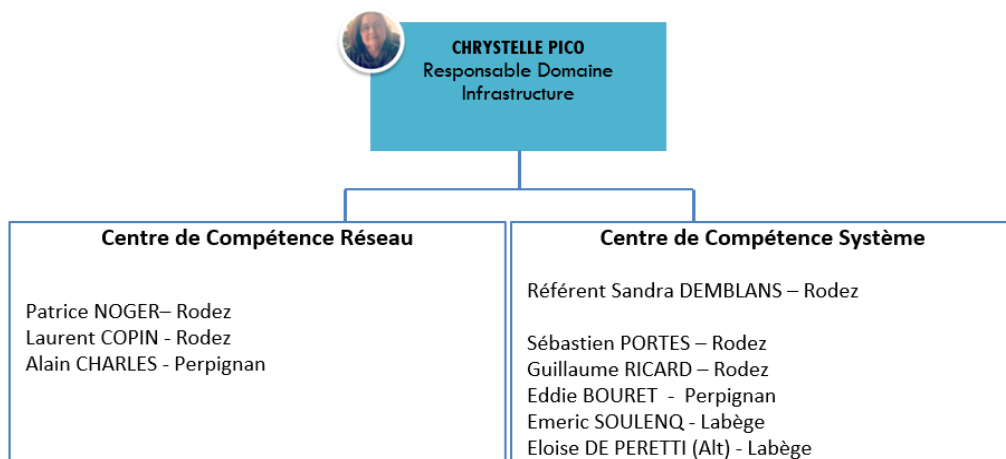


Figure 4: Organigramme du domaine infrastructure.

2.3. Missions réalisées

Au cours de l'alternance, différentes missions m'ont été confiées afin de monter progressivement en compétence sur différents sujets. La liste ci-dessous reprend la plupart des activités qui m'ont été attribuées et que je détaillerai dans des fiches d'activité séparées :

- Mise en place d'un laboratoire sur VirtualBox avec des machines CentOS 7
- Permettre aux machines virtuelles (V.M.) de communiquer entre elles et avec l'hôte physique grâce au protocole SSH
- Installation de BookStack sur CentOS 7, puis passage en connexion sécurisée HTTPS
- Installation et configuration de fail2ban sur le laboratoire et configuration d'une prison SSH
- Création d'un script pour monitorer l'utilisation de l'espace disque au moment de la connexion sur des serveurs de recette Ubuntu et CentOS7
- Amélioration et automatisation du script avec Crontab et envoi de rapports de santé des serveurs de recette et de production

Les différentes missions seront également rattachées aux compétences correspondantes dans le Bloc 1 du référentiel officiel du BTS SIO présenté ci-dessous. Un modèle détaillant chaque activité du B-1 est disponible en annexe.

Bloc n° 1 – Support et mise à disposition de services informatiques

Gérer le patrimoine informatique

Répondre aux incidents et aux demandes d'assistance et d'évolution

Développer la présence en ligne de l'organisation

Travailler en mode projet

Mettre à disposition des utilisateurs un service informatique

Organiser son développement professionnel

Figure 5: Bloc 1 du référentiel officiel SIO.

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	2

FICHE 3 : ENVIRONNEMENT TECHNIQUE

3.1. Ressources matérielles

3.1.1. Architecture

L'architecture globale de ViaSanté est présentée dans le schéma anonymisé ci-dessous. Celle-ci est composée de différents périmètres afin de délimiter les services. Il est intéressant de noter que l'environnement ViaSanté hébergé n'est pas accessible directement depuis internet et qu'il est nécessaire de passer par une DMZ (Zone démilitarisée) pour s'y connecter.

Les différents serveurs de l'environnement de l'infrastructure sont accessibles via un serveur de rebond du Bastion (Wallix). Les connexions au sein du domaine ViaSanté sont soumises aux contrôles d'un pare feu PaloAlto. De même, un pare feu FortiGate est en place à la sortie et à l'entrée de l'environnement interne ViaSanté protégeant les communications avec internet. De plus, tous les échanges vers internet et les fournisseurs sont chiffrés via TLS. Seul un partenaire dispose d'un accès direct à l'environnement hébergé ViaSanté sans passer par la DMZ.

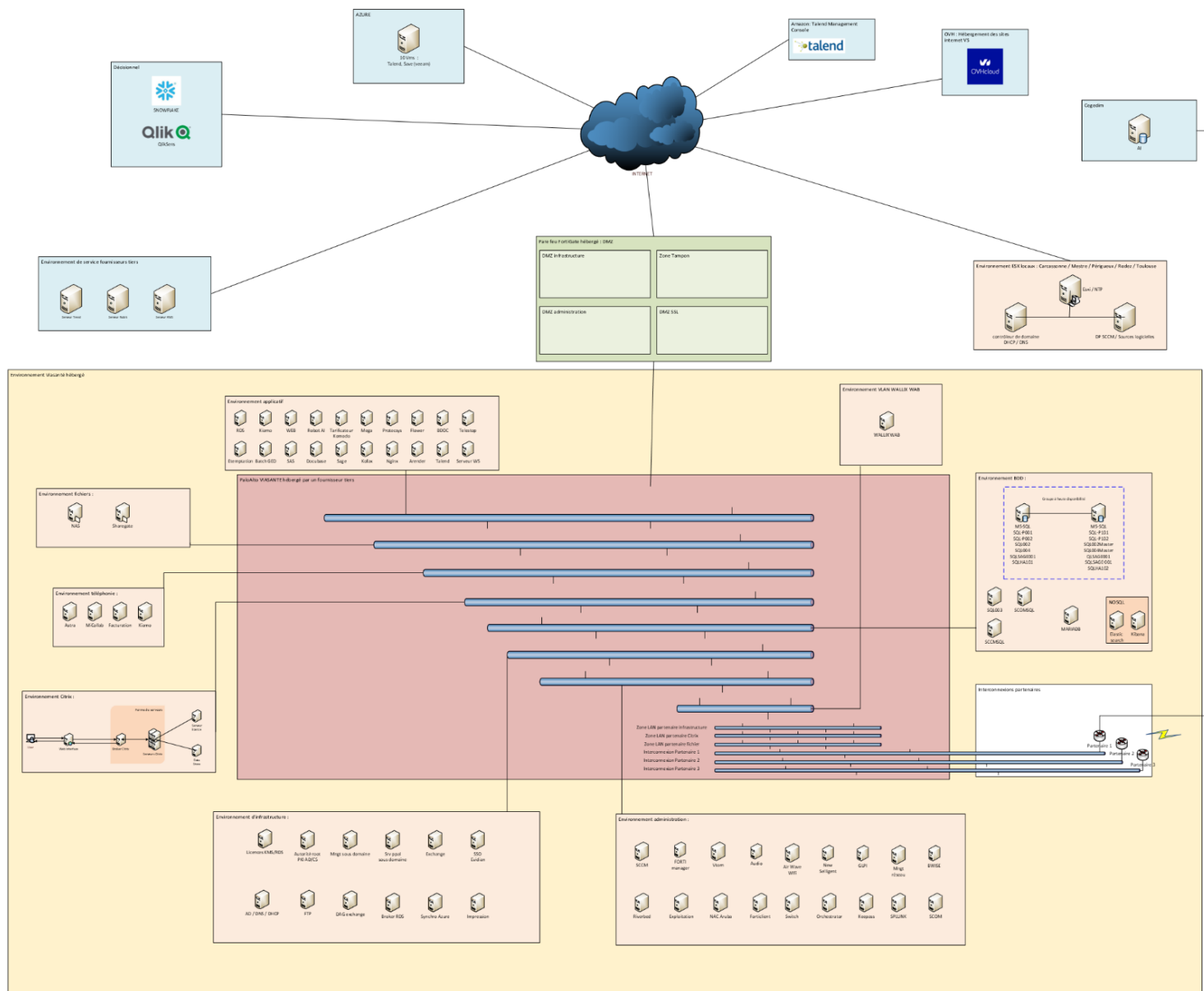


Figure 6: Architecture globale du SI de ViaSanté.

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	3

3.1.2. Schéma réseau

Le schéma réseau représenté ci-dessous reprend une partie des éléments du schéma de l'architecture globale. Sont représentés sur ce graphe les éléments permettant la sécurisation de la communication entre internet, l'environnement interne de ViaSanté et la DMZ. C'est cette dernière qui joue le rôle de pont entre les environnements externe (internet) et interne (périphérie ViaSanté).

Au sein de la DMZ, les pare-feu FortiGate sont redondés et assurent un premier filtrage entre internet et le périmètre Néoclès. Des pare-feu FortiGate redondés sont présents à l'interface entre la DMZ et le périmètre ViaSanté. Les réseaux LAN de ViaSanté ne sont accessibles qu'en passant par une paire de pare-feu PaloAlto redondés.

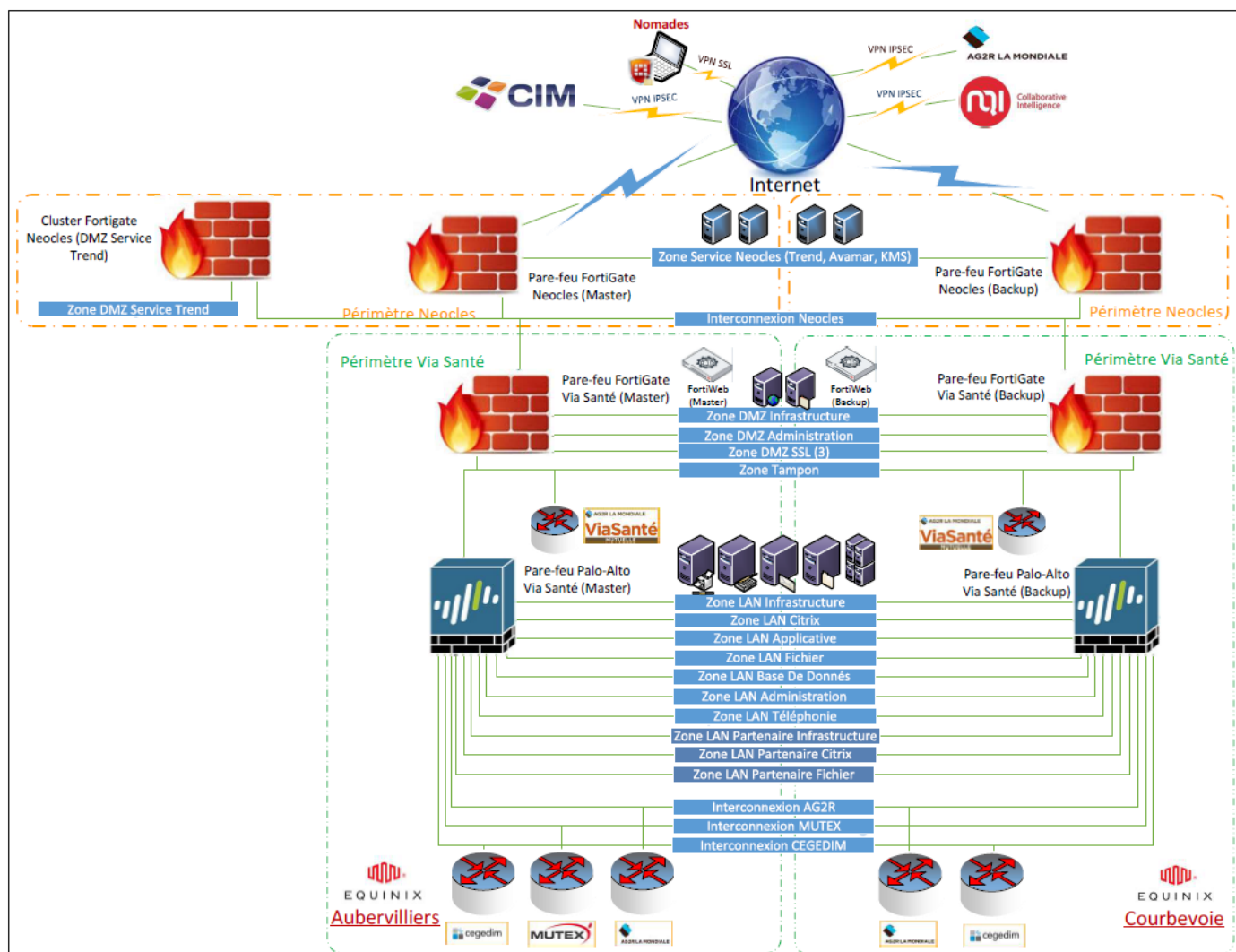


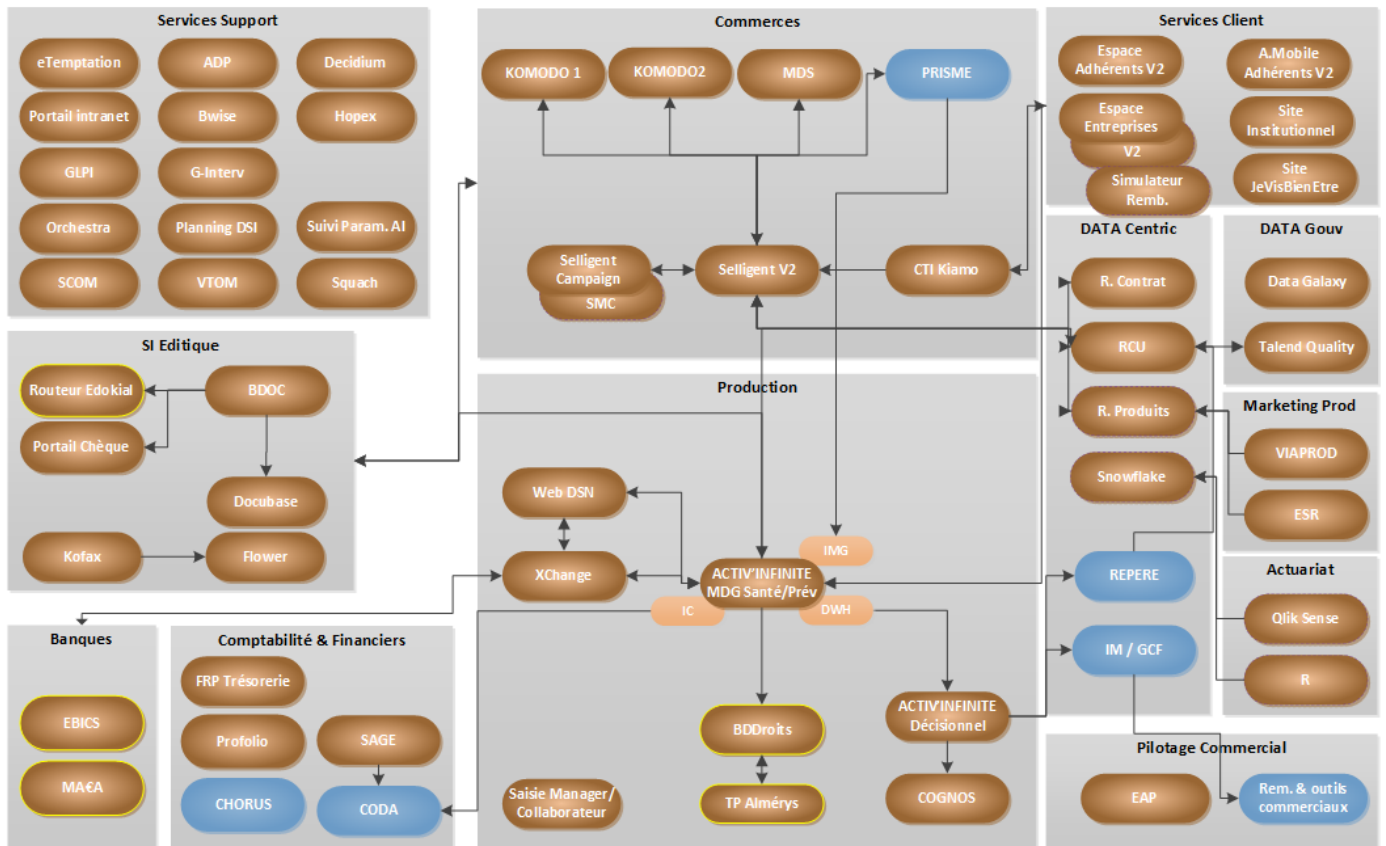
Figure 7: Schéma réseau global du SI de ViaSanté.

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	3

3.2. Ressources logicielles

Les différentes ressources logicielles utilisées par ViaSanté sont présentées dans le schéma ci-dessous. Au cours de mon alternance j'ai principalement interagi avec les briques du service Support et Production.

SI VIASANTE - Régime Complémentaire



Version du 16/11/2021

Figure 8: Cartographie des applications du SI de ViaSanté.

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	3

FICHE 4 : ACTIVITE 1 - Mise en place d'un laboratoire sur VirtualBox avec des machines CentOS 7

4.1. Compétences mises en œuvre

Cette activité a mobilisé les compétences suivantes du module B-1 du référentiel officiel du BTS SIO :

- Gestion du patrimoine informatique
- Organisation de son développement professionnel

4.2. Cahier des charges

A la demande de mon tuteur, j'ai eu à mettre en place un laboratoire sur VirtualBox avec des VM CentOS 7. J'ai configuré le réseau de telle sorte que celles-ci devaient être capables de ping et d'être pingées par la machine physique hôte et de se ping entre elles. Enfin, j'ai mis en place une connexion SSH entre les 2 VM. Voici une liste récapitulative des principales tâches effectuées lors de cette activité :

- Installation de 2 VM CentOS 7 à partir d'une image ISO sans interface graphique
- Configuration rapide des caractéristiques réseau des VM et de VirtualBox
- Jeux de tests de pings

4.3. Démarche/Mode opératoire

Installation des VM CentOS 7

Sous-activité	Etape	Actions
Ajout VM dans VirtualBox	1	Sélectionner « Nouvelle dans le menu VirtualBox »
	2	Après avoir saisi un nom adéquat, mettre le chemin vers l'image ISO
	3	Saisir un nom d'utilisateur et un mot de passe
Installation CentOS 7	1	Lancer la VM et sélectionner « Install CentOS 7 »
	2	Sélectionner « Destination de l'installation »
	3	Sélectionner le disque dur configuré
	4	Cliquer sur « Terminé » puis sur « Démarrer l'installation »
	5	Saisir un mot de passe pour le compte admin
	6	Créer un compte utilisateur (facultatif)

Configurations des réseaux

Sous-activité	Etape	Actions
Configuration réseau dans VirtualBox	1	Sélectionner la VM à configurer
	2	Cliquer sur « Configuration »
	3	Aller dans l'onglet « Réseau »
	4	Dans « Adapter 2 », sélectionner le mode d'accès « Réseau privé hôte » dont le nom correspond à l'adaptateur Ethernet de VirtualBox. Dans les options avancées, mettre le « Mode promiscuité » en « Allow all »
	5	Dans « Adapter 1 », sélectionner cette fois-ci le mode d'accès réseau « NAT », avec le même mode de promiscuité que précédemment
	6	Valider les modifications avec « OK »
Configuration réseau dans CentOS 7	1	Utiliser la commande suivante : nmtui
	2	Dans nmtui, sélectionner « Modifier une connexion »
	3	Choisir l'interface réseau à gérer
	4	Vérifier que la configuration IPv4 est en <Automatique>
	5	Vérifier que la configuration IPv6 est en <Ignorer>
	6	Valider
	7	Sélectionner « Activer une connexion »
	8	Passer l'interface sélectionnée en <Activer>
	9	Lorsque celle-ci sera activée, une astérisque apparaîtra à côté de son nom
	10	Retour vers le menu nmtui
	11	Valider les configurations

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

Jeux de tests

Sous-activité	Etape	Actions	Commandes
Tests de pings	1	Récupération des adresses IP des VM	ip a
	2	Récupération de l'IP de l'hôte physique	ipconfig
	3	Pings des VM entre elles, pings des VM depuis et vers l'hôte physique	ping 192.168.XXX.XXX ping XXX.XXX.XXX.XXX

4.4. Preuves de la réalisation

Sous-activité

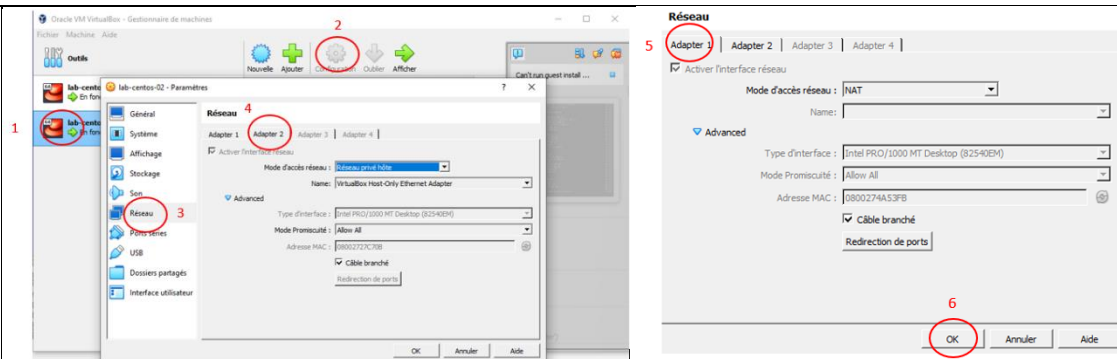
Ajout VM dans VirtualBox

Captures d'écran

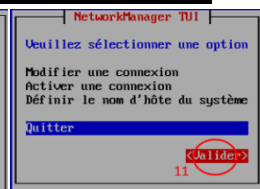
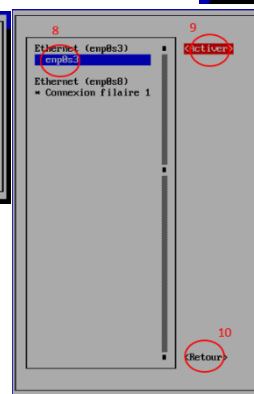
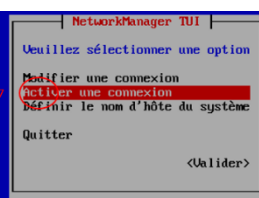
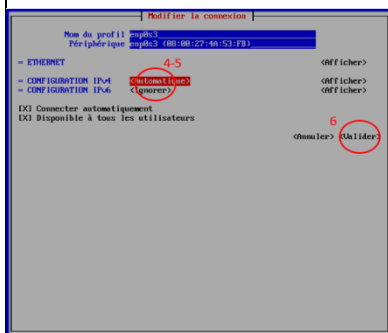
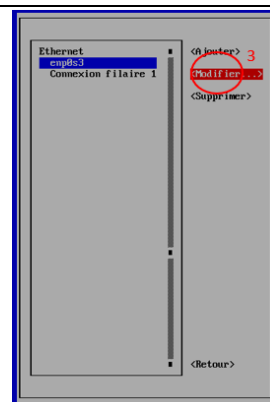
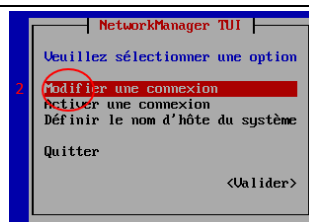
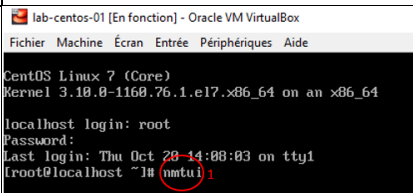
Installation CentOS 7

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

Configuration réseau sous VirtualBox



Configuration réseau dans CentOS 7



Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

Tests de pings

lab-centos-01 [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

```
[root@localhost ~]# ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=0.561 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=0.432 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=0.439 ms
^C
--- 192.168.56.103 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.432/0.477/0.561/0.061 ms
[root@localhost ~]# ping 10.107.131.80
PING 10.107.131.80 (10.107.131.80) 56(84) bytes of data.
64 bytes from 10.107.131.80: icmp_seq=1 ttl=127 time=0.738 ms
64 bytes from 10.107.131.80: icmp_seq=2 ttl=127 time=1.57 ms
64 bytes from 10.107.131.80: icmp_seq=3 ttl=127 time=0.968 ms
^C
--- 10.107.131.80 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 0.738/1.094/1.578/0.356 ms
[root@localhost ~]# _
```

Invite de commandes

```
^C
C:\Users\DEPERETTIE>ping 192.168.56.102

Envoi d'une requête 'Ping' 192.168.56.102 avec 32 octets de données :
Réponse de 192.168.56.102 : octets=32 temps<1ms TTL=64
Réponse de 192.168.56.102 : octets=32 temps<1ms TTL=64
Réponse de 192.168.56.102 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.56.102:
    Paquets : envoyés = 3, recus = 3, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
Ctrl+C
^C
C:\Users\DEPERETTIE>ping 192.168.56.103

Envoi d'une requête 'Ping' 192.168.56.103 avec 32 octets de données :
Réponse de 192.168.56.103 : octets=32 temps<1ms TTL=64
Réponse de 192.168.56.103 : octets=32 temps<1ms TTL=64
Réponse de 192.168.56.103 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.56.103:
    Paquets : envoyés = 3, recus = 3, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
Ctrl+C
^C
C:\Users\DEPERETTIE>
```

lab-centos-02 [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

```
[root@localhost ~]# ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=128 time=0.406 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=128 time=0.620 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=128 time=0.451 ms
^C
--- 192.168.56.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.406/0.492/0.620/0.093 ms
[root@localhost ~]# ping 10.107.131.80
PING 10.107.131.80 (10.107.131.80) 56(84) bytes of data.
64 bytes from 10.107.131.80: icmp_seq=1 ttl=127 time=0.800 ms
64 bytes from 10.107.131.80: icmp_seq=2 ttl=127 time=0.802 ms
64 bytes from 10.107.131.80: icmp_seq=3 ttl=127 time=0.761 ms
^C
--- 10.107.131.80 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.761/0.841/0.802/0.056 ms
[root@localhost ~]# _
```

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

FICHE 4 : ACTIVITE 2 - Mise en place du protocole SSH entre les 2 VM CentOS 7

4.1. Compétences mises en œuvre

Cette activité a mobilisé les compétences suivantes du module B-1 du référentiel officiel du BTS SIO :

- Gestion du patrimoine informatique
- Organisation de son développement professionnel

4.2. Cahier des charges

Afin d'établir une connexion sécurisée entre les 2 VM CentOS 7, le protocole SSH est utilisé car celui-ci permet d'une part de chiffrer les données et d'autre part d'assurer l'authenticité en autorisant uniquement les ordinateurs désignés. Voici une liste récapitulative des principales tâches effectuées lors de cette activité :

- Mise à jour du pare-feu pour autoriser le port 22 (dédié au protocole SSH) sur les VM CentOS 7 et activation du service SSHD
- Génération clé SSH
- Jeux de tests de la connexion SSH

4.3. Démarche/Mode opératoire

Mise à jour du pare-feu et activation SSHD

Sous-activité	Etape	Actions	Commandes
Ajout port 22 et relance du pare-feu	1	Autoriser le port 22 à établir des connexions SSH	<code>sudo firewall-cmd --add-port=22/tcp --permanent</code>
	2	Relancer le pare-feu pour prendre en compte la nouvelle exception	<code>firewall-cmd --reload</code>
Activation et configuration SSH	1	Lancer le démon SSH	<code>systemctl start sshd.service</code>
	2	Dans le fichier <code>sshd_config</code> situé dans le répertoire <code>/etc/ssh</code> , il faut s'assurer que la ligne avec le port est décommentée et que le port renseigné est le 22	
	3	Relancer le service SSH	<code>systemctl restart sshd.service</code>

Génération de la clé SSH

Sous-activité	Etape	Actions	Commandes
Génération de la clé	1	Générer la paire de clé	<code>ssh-keygen</code>
	2	Copier la clé publique et la donner à l'hôte avec lequel on souhaite établir la connexion et saisir le mdp associé au compte utilisateur de l'hôte distant	<code>ssh-copy-id <USER>@<IP></code>

Jeux de tests

Sous-activité	Etape	Actions	Commandes
Connectivité SSH	1	Etablir une connexion SSH avec l'hôte distant	<code>ssh <USER>@<IP></code>
	2	Rendre la connexion automatique et entrer une nouvelle phrase de passe si nécessaire	<code>ssh-keygen -p</code>

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

4.4. Preuves de la réalisation

Sous-activité	Captures d'écran
Ajout port 22 et relance du pare-feu	<pre>[root@localhost ssh]# firewall-cmd --add-port=22/tcp --permanent Warning: ALREADY_ENABLED: 22:tcp success [root@localhost ssh]# firewall-cmd --reload success [root@localhost ssh]# _</pre>
Activation et configuration SSH	<pre># \$OpenBSD: sshd_config,v 1.100 2016/08/15 12:32:04 naddy Exp \$ # This is the sshd server system-wide configuration file. See # sshd_config(5) for more information. # This sshd was compiled with PATH=/usr/local/bin:/usr/bin # The strategy used for options in the default sshd_config shipped with # OpenSSH is to specify options with their default value where # possible, but leave them commented. Uncommented options override the # default value. # If you want to change the port on a SELinux system, you have to tell # SELinux about this change. # semanage port -a -t ssh_port_t -p tcp #PORTNUMBER # #Port 22 #AddressFamily any #ListenAddress 0.0.0.0 #ListenAddress :: # HostKey /etc/ssh/ssh_host_rsa_key #HostKey /etc/ssh/ssh_host_dsa_key HostKey /etc/ssh/ssh_host_ecdsa_key HostKey /etc/ssh/ssh_host_ed25519_key # # Ciphers and keying #RekeyLimit default none # # Logging #SyslogFacility AUTH SyslogFacility AUTHPRIV #LogLevel INFO # # Authentication: "sshd_config" 139L, 3986C ----- [root@localhost ssh]# systemctl restart sshd.service [root@localhost ssh]#</pre>
Génération de la clé	<pre>[root@localhost ssh]# ssh-keygen Generating public/private rsa key pair. Enter file in which to save the key (/root/.ssh/id_rsa): Enter passphrase (empty for no passphrase): Enter same passphrase again: Your identification has been saved in /root/.ssh/id_rsa. Your public key has been saved in /root/.ssh/id_rsa.pub. The key fingerprint is: SHA256:uA06LHsJsc640lSgghEuty0IUW6Tzrs77MrXf87c9c root@localhost.localdomain The key's randomart image is: +----[RSA 2048]-----+ o.o.. +=..+ *o..=o +.o.o. o+. .S. =o * .+o .o . . o =o+.o . + . E o..+++==+ . = . +----[SHA256]-----+ [root@localhost ssh]# [root@localhost ssh]# ssh-copy-id root@192.168.56.103 /bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub" /bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed /bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys root@192.168.56.103's password: Number of key(s) added: 1 Now try logging into the machine, with: "ssh 'root@192.168.56.103'" and check to make sure that only the key(s) you wanted were added. [root@localhost ssh]# _</pre>
Connectivité SSH	<pre>[root@localhost ssh]# ssh 192.168.56.103 Enter passphrase for key '/root/.ssh/id_rsa': Last login: Fri Oct 21 09:12:52 2022 from 192.168.56.102 [root@localhost ~]# _ [root@localhost ssh]# ssh-keygen -p Enter file in which the key is (/root/.ssh/id_rsa): Enter old passphrase: Enter new passphrase (empty for no passphrase): Enter same passphrase again: Your identification has been saved with the new passphrase. [root@localhost ssh]# ssh 192.168.56.103 Last login: Fri Oct 21 09:26:35 2022 from 192.168.56.102 [root@localhost ~]# exit déconnexion Connection to 192.168.56.103 closed. [root@localhost ssh]#</pre>

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

FICHE 4 : ACTIVITE 3 - Installation de BookStack sur CentOS 7

4.1. Compétences mises en œuvre

Cette activité a mobilisé les compétences suivantes du module B-1 du référentiel officiel du BTS SIO :

- Gestion du patrimoine informatique
- Réponse aux incidents et aux demandes d'assistance et d'évolution
- Organisation de son développement professionnel

4.2. Cahier des charges

BookStack est un logiciel gratuit et open-source de type Wiki. Disponible sous licence M.I.T. et basé sur le framework Laravel, il permet d'organiser les informations sous forme d'étagères, de livres, de chapitres et de pages. Comme nous avons fait le choix d'installer BookStack sur une VM sans interface graphique CentOS 7, il a fallu dans un premier temps installer les dépendances nécessaires, sous forme de paquets, et configurer une bdd de type MariaDB. Dans un second temps, un serveur web Nginx a été mis en place pour héberger l'application. Ensuite, il a fallu rediriger le port 80 de la VM vers la machine physique, afin de visualiser BookStack. Enfin, la connexion a été améliorée en HTTPS pour plus de sécurité et pour chiffrer les informations. Voici une liste récapitulative des principales tâches effectuées lors de cette activité :

- Installation et configuration des prérequis : EPEL, Nginx, PHP, PHP-FPM, Composer, MariaDB etc.
- Installation et configuration de BookStack et de Nginx
- Configuration du fichier hosts de l'hôte physique
- Première connexion à BookStack
- Première connexion à BookStack en HTTPS

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

4.3. Démarche/Mode opératoire

Installation et configuration des prérequis

Sous-activité	Etape	Actions	Commandes
Installation des répertoires EPEL et Webtatic	1	Récupérer le paquet EPEL	<code>sudo yum -y install epel-release</code>
	2	Récupérer le paquet Wabtatic	<code>sudo rpm -Uvh https://mirror.webtatic.com/yum/el7/webtatic-release.rpm</code>
Installation et lancement Nginx	1	Installer Nginx	<code>sudo yum -y install nginx</code>
	2	Lancer Nginx	<code>sudo systemctl start nginx</code>
	3	Vérifier que le port affecté à Nginx est le 80	<code>netstat -plntu</code>
Autoriser HTTP	1	Autoriser le service HTTP	<code>firewall-cmd --add-service=http --permanent</code>
	2	Recharger la configuration du pare-feu	<code>firewall-cmd --reload</code>
Vérifier SELinux	1	Vérifier le statut de SELinux	<code>sestatus</code>
	2	Mettre SELinux en « permissive » ou « disabled » dans /etc/selinux/config	<code>vim /etc/selinux/config</code>
Installation de PHP-FPM	1	Installer le paquet PHP-FPM	<code>sudo yum -y install php-fpm</code>
	2	Ouvrir et modifier le fichier php.ini dans /etc	<code>sudo vim /etc/php.ini</code>
	3	Décommenter la ligne cgi.fix_pathinfo et mettre sa valeur à 0	<code>cgi.fix_pathinfo=0</code>
	4	Démarrer le service PHP-FPM	<code>systemctl start php-fpm</code>
	5	Vérifier que le port dédié est à l'écoute de PHP-FPM	<code>netstat -pl grep php</code>
Installation de MariaDB	1	Télécharger et lancer MariaDB	<code>sudo yum -y install mariadb-server</code> <code>systemctl start mariadb</code>
	2	Lancer l'installation sécurisée de MariaDB et suivre les différentes étapes	<code>mysql_secure_installation</code>
Création de la base de données et de l'utilisateur associé	1	Lancer MariaDB	<code>mysql -u root -p</code>
	2	Créer la bdd de BookStack	<code>create database bookstackdb ;</code>
	3	Créer l'utilisateur bookstack et lui donner les droits sur la base	<code>create user bookstack@localhost identified by 'bookstack@';</code> <code>grant all privileges on bookstackdb.* to bookstack@localhost identified by 'bookstack@';</code>
	4	Sortir de MariaDB	<code>exit;</code>

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

Installation et configuration de BookStack et de Nginx

Sous-activité	Etape	Actions	Commandes
Installation et configuration de BookStack	1	Créer le répertoire /var/www/html	sudo mkdir -p /var/www/html
	2	Récupérer le repo BookStack dans /var/www/html	cd /var/www/html git clone https://github.com/BookStackApp/BookStack.git --branch release --single-branch
	3	Dans le répertoire BookStack, utiliser Composer pour installer l'appli	cd BookStack/ composer install
Récupération et édition du fichier .env BookStack	1	Dans le répertoire de BookStack, éditer le fichier .env dans la section #Database details	# Database details DB_HOST=localhost DB_USERNAME=bookstackdb DB_PASSWORD=bookstack@
	2	Editer l'URL d'accès à l'application	APP_URL=http://bookstack.centos7.vm01
	3	Donner les droits d'écriture à Nginx	chown -R nginx :nginx /var/www/html/BookStack
	4	Toujours dans le répertoire BookStack, générer la clé unique de l'application, qui sera par la suite stockée dans le .env	php artisan key :generate
Configuration de Nginx	1	Dans le répertoire de Nginx, créer un fichier bookstack.conf	cd /etc/nginx vim conf.d/bookstack.conf
	2	Vérifier que le chemin vers la socket PHP-FPM est le bon et renseigner le nom du serveur ainsi que le répertoire root soit le bon	
	3	Vérifier le statut de Nginx et relancer le service	systemctl restart nginx systemctl status nginx -l

Configuration du fichier hosts de l'hôte physique

Sous-activité	Etape	Actions
Ajout manuel d'une entrée locale	1	Ouvrir le fichier hosts situé dans C:\Windows\System32\drivers\etc
	2	Ajouter l'adresse IP de la VM sur laquelle tourne le serveur web Nginx et l'application BookStack et la faire correspondre au nom de domaine renseigné dans le .env et dans bookstack.conf

Première connexion à BookStack

Sous-activité	Etape	Actions
Connexion à l'application	1	Depuis la machine physique, se rendre sur l'URL suivante : http://bookstack.centos7.vm01
	2	Renseigner les identifiants suivants : admin@admin.com , password

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

Connexion à BookStack en HTTPS

Sous-activité	Etape	Actions	Commandes
Ajout d'une règle dans le firewall	1	Autoriser le port 443 associé à HTTPS dans le pare-feu	firewall-cmd -permanent -add-port=443/tcp
	2	Recharger la configuration du pare-feu	firewall-cmd --reload
Génération d'une clé et d'un certificat avec OpenSSL	1	Installer OpenSSL	sudo yum install openssl
	2	Créer le répertoire ssl-certs dans le dossier nginx	mkdir /etc/nginx/ssl-certs
	3	Générer une clé privée et un certificat auto-signé et renseigner les informations demandées	sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/nginx/ssl-certs/nginx.key -out /etc/nginx/ssl-certs/nginx.crt
Ajout du certificat auto-signé et connexion en HTTPS	1	Editer le fichier bookstack.conf	vim /etc/nginx/conf.d/bookstack.conf
	2	Ajouter les lignes ci-après dans la configuration du serveur	listen 443 ssl ; ssl on ; ssl_certificate /etc/nginx/ssl-certs/nginx.crt ; ssl_trusted_certificate /etc/nginx/ssl-certs/nginx.crt ; ssl_certificate_key /etc/nginx/ssl-certs/nginx.key ;
	3	Redémarrer le service nginx	sudo systemctl restart nginx
	4	Se rendre sur l'URL suivante : https://bookstack.centos7.vm01	

4.4. Preuves de la réalisation

Sous-activité	Captures d'écran
Installation et lancement Nginx	<pre>[root@hakase-labs ~]# [root@hakase-labs ~]# systemctl start nginx [root@hakase-labs ~]# systemctl enable nginx Created symlink from /etc/systemd/system/multi-user.target.wants/nginx.service to /usr/lib/systemd/system/nginx.service. [root@hakase-labs ~]# [root@hakase-labs ~]# netstat -plntu Active Internet connections (only servers) Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name tcp 0 0 0.0.0.0:111 0.0.0.0:* LISTEN 1/systemd tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN 3188/nginx: master tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 903/sshd tcp6 0 0 :::111 :::* LISTEN 1/systemd tcp6 0 0 :::80 :::* LISTEN 3188/nginx: master tcp6 0 0 :::22 :::* LISTEN 903/sshd tcp6 0 0 :::1:25 :::* LISTEN 1018/master udp 0 0 127.0.0.1:323 0.0.0.0:* 571/chronyd udp 0 0 0.0.0.0:18396 0.0.0.0:* 713/dhclient udp 0 0 0.0.0.0:68 0.0.0.0:* 713/dhclient udp6 0 0 :::1:323 :::* 571/chronyd udp6 0 0 :::17966 :::* 713/dhclient [root@hakase-labs ~]#</pre>
Vérifier SELinux	<pre>/etc/selinux/config # This file controls the state of SELinux on the system. # SELINUX= can take one of these three values: # enforcing - SELinux security policy is enforced. # permissive - SELinux prints warnings instead of enforcing. # disabled - No SELinux policy is loaded. SELINUX=disabled # SELINUXTYPE= can take one of these two values: # targeted - Targeted processes are protected, # mls - Multi Level Security protection. SELINUXTYPE=targeted</pre>

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

Installation de PHP-FPM	<pre> [root@localhost BookStack]# netstat -pl grep php unix 2 [ACC] STREAM LISTENING 18371 989/php-fpm: master /var/run/php-fpm/php-fpm sock [root@localhost BookStack]# </pre>
Installation de MariaDB	<pre> [root@hakase-labs ~]# [root@hakase-labs ~]# <u>systemctl start mariadb</u> [root@hakase-labs ~]# <u>systemctl enable mariadb</u> Created symlink from /etc/systemd/system/multi-user.target.wants/mariadb.service to /usr/lib/systemd/system/mariadb.service. [root@hakase-labs ~]# [root@hakase-labs ~]# <u>mysql_secure_installation</u> NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY! In order to log into MariaDB to secure it, we'll need the current password for the root user. If you've just installed MariaDB, and you haven't set the root password yet, the password will be blank, so you should just press enter here. Enter current password for root (enter for none): OK, successfully used password, moving on... Setting the root password ensures that nobody can log into the MariaDB root user without the proper authorisation. Set root password? [Y/n] Y New password: Re-enter new password: Password updated successfully! Reloading privilege tables.. ... Success! Set root password? [Y/n] Y Remove anonymous users? [Y/n] Y Disallow root login remotely? [Y/n] Y Remove test database and access to it? [Y/n] Y Reload privilege tables now? [Y/n] Y </pre>
Récupération et édition du fichier <code>.env</code> BookStack	<pre> # All URLs in BookStack will be generated using this value # to ensure URLs generated are consistent and secure. # If you change this in the future you may need to run a com mand # to update stored URLs in the database. Command example: # php artisan bookstack:update-url https://old.example.com h ttps://new.example.com APP_URL=http://bookstack.centos7.vm01 # Database details DB_HOST=localhost DB_DATABASE=bookstackdb DB_USERNAME=bookstack DB_PASSWORD=bookstack@ </pre>

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

```

[root@hakase-labs BookStack]#
[root@hakase-labs BookStack]# cp .env.example .env
[root@hakase-labs BookStack]# vim .env
[root@hakase-labs BookStack]#
[root@hakase-labs BookStack]# chown -R nginx:nginx /var/www/BookStack
[root@hakase-labs BookStack]#
[root@hakase-labs BookStack]# php artisan key:generate
*****
*      Application In Production!      *
*****

Do you really wish to run this command? (yes/no) [no]:
> yes

Application key [base64:dCyt+xi8+mvJelYA1ttcrpxXnMyZeYYMctz+aKmk3Uk=] set successfully.
[root@hakase-labs BookStack]#
[root@hakase-labs BookStack]# php artisan migrate
*****
*      Application In Production!      *
*****

Do you really wish to run this command? (yes/no) [no]:
> yes

Migration table created successfully.

```

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

Configuration de Nginx

```
server {
    listen 80;
    server_name bookstack.centos7.vm01;
    root /var/www/BookStack/public;

    access_log /var/log/nginx/bookstack_access.log;
    error_log /var/log/nginx/bookstack_error.log;

    client_max_body_size 1G;
    fastcgi_buffers 64 4K;

    index index.php;

    location / {
        try_files $uri $uri/ /index.php?$query_string;
    }

    location ~ ^/(?:\.htaccess|data|config|db_structure\.xml|README) {
        deny all;
    }

    location ~ \.php(?:$|/) {
        fastcgi_split_path_info ^(.+\.php)(/.+)$;
        include fastcgi_params;
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
        fastcgi_param PATH_INFO $fastcgi_path_info;
        fastcgi_pass unix:/var/run/php-fpm/php-fpm.sock;
    }

    location ~* \.(?:jpg|jpeg|gif|bmp|ico|png|css|js|swf)$ {
        expires 30d;
        access_log off;
    }
}
```

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

Ajout manuel
d'une entrée
locale

Nom	Modifié le	Type	Taille
hosts	03/01/2023 09:23	Fichier	1 Ko
lmhosts.sam	07/12/2019 10:12	Fichier SAM	4 Ko
networks	07/12/2019 10:12	Fichier	1 Ko
protocol	07/12/2019 10:12	Fichier	2 Ko
services	07/12/2019 10:12	Fichier	18 Ko

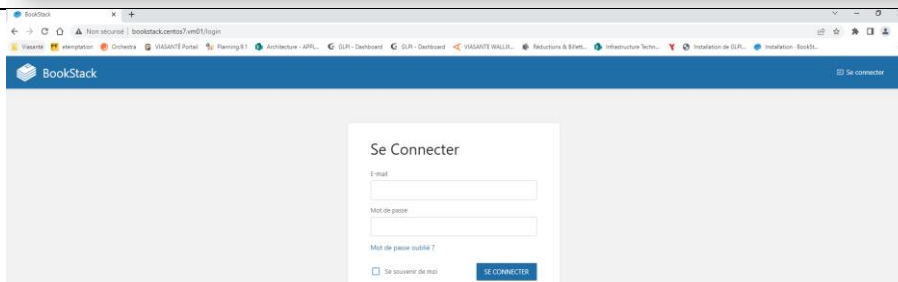
```

hosts - Bloc-notes
Fichier Edition Format Affichage Aide
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com       # source server
#       38.25.63.10       x.acme.com          # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
192.168.56.102           bookstack.centos7.vm01
Ln 1, Col 1    100%  Windows (CRLF)  UTF-8

```

Connexion à
l'application



Génération
d'une clé et
d'un
certificat
avec OpenSSL

```

[root@localhost ~]# mkdir /etc/nginx/ssl-certs/
[root@localhost ~]# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/nginx/ssl-certs/nginx
x.key -out /etc/nginx/ssl-certs/nginx.crt
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/etc/nginx/ssl-certs/nginx.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:FR
State or Province Name (full name) []:Toulouse
Locality Name (eg, city) [Default City]:Labège
Organization Name (eg, company) [Default Company Ltd]:labo
Organizational Unit Name (eg, section) []:infra
Common Name (eg, your name or your server's hostname) []:bookstack.centos7.vm01
Email Address []:laboinfra@gmail.com
[root@localhost ~]#

```

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

Ajout du
certificat
auto-signé et
connexion en
HTTPS

```
server {
    listen 80;
    listen 443 ssl;
    listen [::]:443 ssl;

    ssl on;
    ssl_certificate /etc/nginx/ssl-certs/nginx.crt;
    ssl_trusted_certificate /etc/nginx/ssl-certs/nginx.crt;
    ssl_certificate_key /etc/nginx/ssl-certs/nginx.key;

    server_name bookstack.centos7.vm01;
    root /var/www/html/BookStack/public;

    access_log /var/log/nginx/bookstack_access.log;
    error_log /var/log/nginx/bookstack_error.log;

    client_max_body_size 1G;
    fastcgi_buffers 64 4K;

    index index.php index.html;

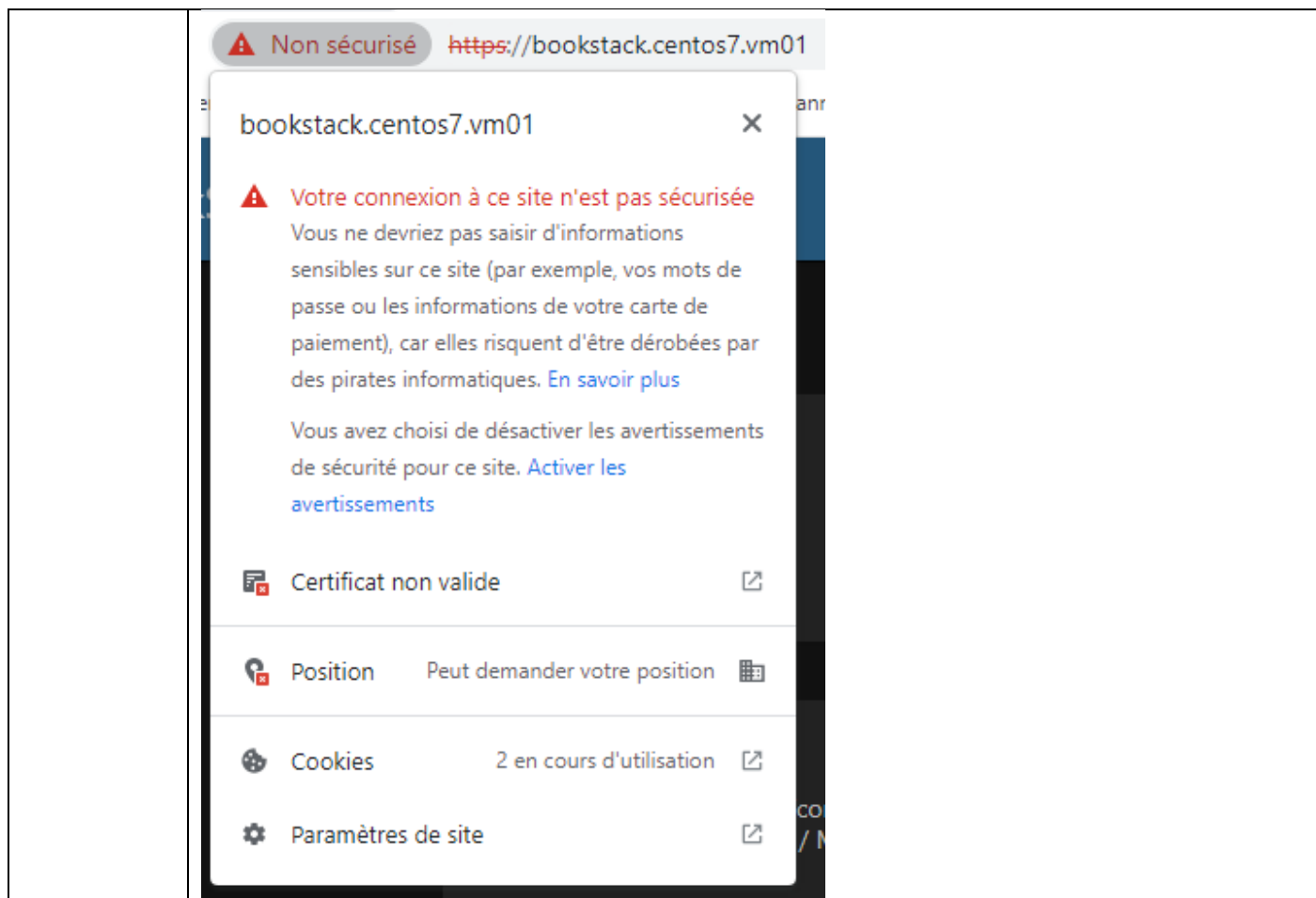
    location / {
        try_files $uri $uri/ /index.php?$query_string;
    }

    # location ~ ^/(?:\.htaccess|data|config|db_structure\.xml|README) {
    #     deny all;
    # }

    location ~ \.php(?:$|/) {
        fastcgi_split_path_info ^(.+\.(php))(/.+)$;
        include fastcgi_params;
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
        fastcgi_param PATH_INFO $fastcgi_path_info;
        fastcgi_pass unix:/var/run/php-fpm/php-fpm.sock;
    }

    # location ~* \.(?:jpg|jpeg|gif|bmp|ico|png|css|js|swf)$ {
    #     expires 30d;
    #     access_log off;
    # }
}
```

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4



Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

FICHE 4 : ACTIVITE 4 - Installation et configuration de prison SSHD avec fail2ban

4.1. Compétences mises en œuvre

Cette activité a mobilisé les compétences suivantes du module B-1 du référentiel officiel du BTS SIO :

- Gestion du patrimoine informatique
- Organisation de son développement professionnel

4.2. Cahier des charges

L'application fail2ban permet, à l'aide de l'analyse de logs de divers services, de mettre en place des actions préventives pour la prévention d'intrusions. Fail2ban a par exemple pour rôle de bannir les adresses IP à l'origine de tentatives répétées d'authentification en erreur. Cet outil renforce la sécurité du système en permettant d'établir des prisons spécifiques. Voici une liste récapitulative des principales tâches effectuées lors de cette activité :

- Installation de fail2ban et activation du service fail2ban
- Activation de la prison SSHD
- Essai de connexion en SSH et analyse des logs de fail2ban
- Visualiser les adresses IP bannies et les « débanir »

4.3. Démarche/Mode opératoire

Installation et activation du service fail2ban

Sous-activité	Etape	Actions	Commandes
Installation et activation de fail2ban	1	Installer fail2ban	sudo yum install fail2ban
	2	Activer le service fail2ban	sudo systemctl start fail2ban

Activation de la prison SSHD

Sous-activité	Etape	Actions	Commandes
Création du fichier jail.local	1	Créer une nouvelle prison locale	sudo vim /etc/fail2ban/jail.local
Paramètres généraux et activation de la prison sshd	1	Mettre la durée de bannissement à 1 heure, le nombre d'essai de connexions maximum à 3 et mettre le localhost comme adresse IP ignorée par les actions de fail2ban	[DEFAULT] # Ban hosts for one hour: bantime = 3600 maxretry=3 Ignoreip = 127.0.0.1
		La méthode de ban choisie est iptables-multiport : on interdit tous les ports	# Override banaction = iptables-multiport
		Activer la prison SSH en précisant le port concerné	[sshd] enabled = true port=ssh
		Activer la récidive et définir la durée du ban sur 1 semaine	[recidive] enabled = true bantime = 1w
	2	Recharger fail2ban pour appliquer la nouvelle prison	sudo systemctl restart fail2ban
	3	Vérifier que la prison est bien active	sudo fail2ban-client status

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

Essai de connexion en SSH et analyse des logs fail2ban

Sous-activité	Etape	Actions	Commandes
Simulation connexion SSH depuis une VM du laboratoire	1	Depuis une autre VM du laboratoire, essayer de se connecter à la machine avec le fail2ban sshd de configuré	ssh <IP CIBLE>
	2	Observer que la connexion est bien impossible	
Analyse des logs fail2ban	1	Ouvrir les logs fail2ban sur la machine concernée par la prison	sudo tail -f fail2ban.log
	2	Observer l'activité de la prison et comparer l'IP bannie avec celle de la VM utilisée pour le test précédent	

Visualiser les adresses IP bannies et les « débanir »

Sous-activité	Etape	Actions	Commandes
Visualisation de la prison sshd	1	Afficher la prison sshd ainsi que la liste des adresses bannies	sudo fail2ban-client status sshd
Deban d'une adresse IP	1	A l'aide de la commande ci-contre, débannir manuellement les adresses IP souhaitées	sudo fail2ban-client set sshd unbanip <IP CIBLE>

4.4. Preuves de la réalisation

Sous-activité	Capture d'écran
Installation et activation de fail2ban	<pre>[root@localhost ~]# systemctl enable fail2ban Created symlink from /etc/systemd/system/multi-user.target.wants/fail2ban.service to /usr/lib/systemd/system/fail2ban.service. [root@localhost ~]# systemctl start fail2ban [root@localhost ~]# sudo fail2ban-client status Status - Number of jail: 0 `- Jail list: [root@localhost ~]#</pre>
Paramètres généraux et activation de la prison sshd	<pre>[DEFAULT] #overwrite le fail2bab.conf !! # Ban hosts for one hour: bantime = 3600 maxretry=3 ignoreip=127.0.0.1 # Override /etc/fail2ban/jail.d/00-firewalld.conf: banaction = iptables-multiport [sshd] enabled = true port = ssh [recidive] enabled = true bantime = 1w</pre>

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

Simulation connexion SSH depuis une VM du laboratoire	<pre> eloise@Ubuntu:~\$ ssh 192.168.56.102 eloise@192.168.56.102's password: Permission denied, please try again. eloise@192.168.56.102's password: Permission denied, please try again. eloise@192.168.56.102's password: eloise@192.168.56.102: <u>Permission denied (publickey,gssapi-keyex,gssapi-with-mi c,password).</u> eloise@Ubuntu:~\$ eloise@Ubuntu:~\$ eloise@Ubuntu:~\$ eloise@Ubuntu:~\$ ssh 192.168.56.102 eloise@192.168.56.102's password: ^[[A ^C eloise@Ubuntu:~\$ ssh 192.168.56.102 ssh: connect to host 192.168.56.102 port 22: <u>Connection refused</u> eloise@Ubuntu:~\$ █ </pre>
Analyse des logs fail2ban	<pre> [root@localhost log]# tail -f fail2ban.log 2022-12-22 14:51:48,269 fail2ban.jail [3651]: INFO Creating new jail 'sshd' 2022-12-22 14:51:48,293 fail2ban.jail [3651]: INFO Jail 'sshd' uses systemd {} 2022-12-22 14:51:48,293 fail2ban.jail [3651]: INFO Initiated 'systemd' backend 2022-12-22 14:51:48,295 fail2ban.filter [3651]: INFO maxLines: 1 2022-12-22 14:51:48,295 fail2ban.filtersystemd [3651]: INFO [sshd] Added journal match for: '_SYSTEMD UNIT=sshd.service + _COMM=sshd' 2022-12-22 14:51:48,348 fail2ban.filter [3651]: INFO maxRetry: 5 2022-12-22 14:51:48,348 fail2ban.filter [3651]: INFO encoding: UTF-8 2022-12-22 14:51:48,348 fail2ban.filter [3651]: INFO findtime: 600 2022-12-22 14:51:48,348 fail2ban.actions [3651]: INFO banTime: 3600 2022-12-22 14:51:48,350 fail2ban.jail [3651]: INFO Jail 'sshd' started 2022-12-22 15:02:39,104 fail2ban.filter [3651]: INFO [sshd] Found 192.168.56.105 - 2022-12-22 15:02:39 2022-12-22 15:02:42,472 fail2ban.filter [3651]: INFO [sshd] Found 192.168.56.105 - 2022-12-22 15:02:42 2022-12-22 15:02:44,140 fail2ban.filter [3651]: INFO [sshd] Found 192.168.56.105 - 2022-12-22 15:02:44 2022-12-22 15:02:45,102 fail2ban.filter [3651]: INFO [sshd] Found 192.168.56.105 - 2022-12-22 15:02:45 2022-12-22 15:02:51,305 fail2ban.filter [3651]: INFO [sshd] Found 192.168.56.105 - 2022-12-22 15:02:51 2022-12-22 15:02:52,065 fail2ban.actions [3651]: NOTICE [sshd] Ban 192.168.56.105 </pre>
Visualisatio n de la prison sshd	<pre> [root@localhost ~]# sudo fail2ban-client status sshd Status for the jail: sshd - Filter - Currently failed: 0 - Total failed: 5 `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd `- Actions - Currently banned: 1 - Total banned: 1 `-- Banned IP list: 192.168.56.105 [root@localhost ~]# █ </pre>

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

Deban d'une
adresse IP

```
[root@localhost ~]# fail2ban-client set sshd unbanip 192.168.56.105
1
[root@localhost ~]# sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|   |- Currently failed: 0
|   |- Total failed: 5
|   `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
    |- Currently banned: 0
    |- Total banned: 1
    `-- Banned IP list:
[root@localhost ~]#
```

2022-12-22 15:07:14,258 fail2ban.actions [3651]: NOTICE [sshd] Unban 192.168.56.105

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

FICHE 4 : ACTIVITE 5 - Réalisation d'un script pour monitorer l'utilisation de l'espace disque et l'état des services de serveurs de recette

4.1. Compétences mises en œuvre

Cette activité a mobilisé les compétences suivantes du module B-1 du référentiel officiel du BTS SIO :

- Gestion du patrimoine informatique
- Réponse aux incidents et aux demandes d'assistance et d'évolution
- Mise à disposition des utilisateurs d'un service informatique
- Travail en mode projet
- Organisation de son développement professionnel

4.2. Cahier des charges

Il est possible d'accéder aux différents serveurs de recette via un serveur de rebond, lui-même accessible via un Bastion, WALLIX. Une fois la session établie avec SYSMGMT, MobaXterm, qui est un émulateur de terminal Linux pour Windows, est utilisé pour établir les connexions SSH aux différents serveurs de test. A la demande de mon tuteur, j'ai réalisé un script permettant de suivre l'utilisation de l'espace disque de 2 serveurs de recette, ainsi que d'afficher l'état de 2 services : nginx et httpd. Dans un premier temps j'ai identifié les commandes et expressions régulières à mettre en place pour récupérer les informations pertinentes. Puis j'ai extrapolé ces scripts en un script plus global, applicable aux 2 serveurs et exécutable depuis SYSMGMT en SSH. Voici une liste récapitulative des principales tâches effectuées lors de cette activité :

- Etablissement et enregistrement des connexions SSH depuis SYSMGMT vers les serveurs de recette
- Identification des commandes pertinentes
- Réalisation d'un script pour chaque serveur
- Extrapolation en un script unique à lancer depuis le serveur de rebond SYSMGMT

4.3. Démarche/Mode opératoire

Enregistrement des sessions SSH depuis SYSMGMT vers les serveurs de recette

Sous-activité	Etape	Actions	Commandes
Editer le fichier .bashrc et y ajouter les connexions SSH	1	Depuis le MobaXterm de SYSMGMT, éditer le fichier .bashrc	vim .bashrc
	2	Enregistrer les différents aliases utilisés	alias site_web= « ssh <IP> »
Recharger le fichier .bashrc	1	Toujours depuis le terminal MobaXterm de SYSMGMT, appliquer les modifications apportées au fichier .bashrc	source .bashrc

Identification des commandes pertinentes

Sous-activité	Etape	Actions	Commandes
Vérification de l'espace disque utilisé et du statut du service	1	A l'aide de la commande df -kh, il est possible d'afficher l'espace disque disponible restant par partition	df -kh
	2	A l'aide de la commande systemctl status, il est possible d'afficher le statut du service	systemctl status httpd.service
Filtrer les sorties des commandes	1	Seule la partition /dev/sda1 résultant de la commande df -kh nous intéresse, il faudra donc utiliser une expression régulière pour n'avoir que la première ligne et la ligne /dev/sda1	df -kh awk 'NR == 1 /\\$/'
	2	Seul le statut du service nous intéresse, il faudra donc utiliser une expression régulière pour n'avoir que cette ligne, lorsque le service est actif	systemctl status service sed '1p ;/Active/ !d'

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

Réalisation d'un script pour chaque serveur

Sous-activité	Etape	Actions	Commandes et script
Création du script shell et vérification du bon fonctionnement	1	Sur un des serveurs de test, créer le script et y faire figurer les commandes accompagnées des expressions régulières pour filtrer les résultats. Ne pas oublier le Shebang au début	vim script.sh #!/bin/bash httpd=\$(systemctl status httpd.service sed '1p;/Active/!d') echo "\$httpd" df=\$(df -kh awk 'NR == 1 /\\$/') echo "\$df"
	2	Lancer le script sur le serveur concerné, en utilisant MobaXterm depuis SYSMGMT et s'assurer que le résultat est conforme	sh script.sh

Réalisation d'un script plus global, applicable aux 2 serveurs de recette

Sous-activité	Etape	Actions	Commandes et script
Corps du script	1	Dans un terminal MobaXterm de SYSMGMT, créer le fichier qui va contenir le script	sudo vim script.sh
	2	Mettre le Shebang en début de script	# !bin/bash
	3	On déclare une variable service, qui prendra une certaine valeur en fonction de l'Hostname de la machine sur laquelle le script s'exécute	if [\$HOSTNAME = "<HOSTNAME>"]; then service=nginx else if [\$HOSTNAME = "<HOSTNAME>"]; then service=httpd fi fi
	4	On intègre la commande systemctl status, qui renverra le statut du service en fonction du serveur	if (systemctl is-active --quiet \$service.service) then echo "\$service is running!" else echo "\$service is not running!" fi
	5	Le script se termine par l'utilisation du disque et l'expression régulière précédemment établie	\$var df -kh awk 'NR == 1 /\\$/' echo "\$var"

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

4.4. Preuves de la réalisation

Sous-activité	Captures d'écran
Vérification de l'espace disque utilisé et du statut du service	<pre>deperettieadm@~\$ df -kh Filesystem Size Used Avail Use% Mounted on udev 3.8G 0 3.8G 0% /dev tmpfs 777M 1.1M 776M 1% /run /dev/sda1 155G 15G 141G 10% / tmpfs 3.8G 0 3.8G 0% /dev/shm tmpfs 5.0M 0 5.0M 0% /run/lock tmpfs 3.8G 0 3.8G 0% /sys/fs/cgroup /dev/sda15 105M 7.4M 97M 8% /boot/efi /dev/loop1 64M 64M 0 100% /snap/core20/1738 /dev/loop0 56M 56M 0 100% /snap/core18/2667 /dev/loop2 56M 56M 0 100% /snap/core18/2679 /dev/loop3 50M 50M 0 100% /snap/snapd/17883 /dev/loop4 50M 50M 0 100% /snap/snapd/17950 /dev/loop5 92M 92M 0 100% /snap/lxd/23991 /dev/loop6 64M 64M 0 100% /snap/core20/1778 /dev/loop7 92M 92M 0 100% /snap/lxd/24061 tmpfs 777M 0 777M 0% /run/user/1012 deperettieadm@~\$</pre> <pre>deperettieadm@~\$ systemctl status nginx.service ● nginx.service - A high performance web server and a reverse proxy server Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled) Active: active (running) since Wed 2023-02-01 10:51:05 CET; 23h ago Docs: man:nginx(8) Process: 748 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS) Process: 776 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS) Main PID: 832 (nginx) Tasks: 5 (limit: 9279) Memory: 68.2M CGroup: /system.slice/nginx.service └─832 nginx: master process /usr/sbin/nginx -g daemon on; master_process on; └─834 nginx: worker process └─835 nginx: worker process └─836 nginx: worker process └─837 nginx: worker process Warning: some journal files were not opened due to insufficient permissions.</pre>
Filtrer les sorties des commandes	<pre>deperettieadm@~\$ df -kh awk 'NR == 1 /^\$/' Filesystem Size Used Avail Use% Mounted on /dev/sda1 155G 15G 141G 10% / deperettieadm@~\$ systemctl status nginx.service sed '1p;/Active/!d' ● nginx.service - A high performance web server and a reverse proxy server Active: active (running) since Wed 2023-02-01 10:51:05 CET; 23h ago</pre>
Création du script shell et vérification du bon fonctionnement	<pre>#!/bin/bash nginx=\$(systemctl status nginx.service sed '1p;/Active/!d') echo "\$nginx" df=\$(df -kh awk 'NR == 1 /^\$/') echo "\$df" deperettieadm@~\$ sh ngxindf.sh ● nginx.service - A high performance web server and a reverse proxy server Active: active (running) since Wed 2023-02-01 10:51:05 CET; 23h ago Filesystem Size Used Avail Use% Mounted on /dev/sda1 155G 15G 141G 10% / #!/bin/bash httpd=\$(systemctl status httpd.service sed '1p;/Active/!d') echo "\$httpd" df=\$(df -kh awk 'NR == 1 /^\$/') echo "\$df" [deperettieadm@~]\$ sh httpdddf.sh ● httpd.service - The Apache HTTP Server Active: active (running) since Wed 2023-02-01 10:53:37 CET; 23h ago Filesystem Size Used Avail Use% Mounted on /dev/sda1 40G 4.0G 37G 10% /</pre>

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

Corps du script

```
#!/bin/bash

if [ $HOSTNAME = "internet_rec" ]; then
    service=nginx
else
    if [ $HOSTNAME = "extranet_rec" ]; then
        service=httpd
    fi
fi

if (systemctl is-active --quiet $service.service)
then
    echo "$service is running!"
else
    echo "$service is not running!"
fi

$var df -kh | grep -Ew "Filesystem|/dev/sda1"
echo "$var"
```

```
02/02/2023 10:46.05 /home/mobaxterm internet_rec < ~/espace_libre.sh
stty: standard input: Inappropriate ioctl for device
Pseudo-terminal will not be allocated because stdin is not a terminal.
X11 forwarding request failed on channel 0
nginx is running!
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda1       155G   15G  141G  10% /

02/02/2023 10:46.15 /home/mobaxterm extranet_rec < ~/espace_libre.sh
stty: standard input: Inappropriate ioctl for device
Pseudo-terminal will not be allocated because stdin is not a terminal.
X11 forwarding request failed on channel 0
httpd is running!
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda1       40G   4.0G   37G  10% /
```

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

FICHE 4 : ACTIVITE 6 - Amélioration du script pour monitorer l'utilisation de l'espace disque et l'état des services de serveurs de recette et de production

4.1. Compétences mises en œuvre

Cette activité a mobilisé les compétences suivantes du module B-1 du référentiel officiel du BTS SIO :

- Gestion du patrimoine informatique
- Réponse aux incidents et aux demandes d'assistance et d'évolution
- Mise à disposition des utilisateurs d'un service informatique
- Travail en mode projet
- Organisation de son développement professionnel

4.2. Cahier des charges

Guillaume a souhaité que les rapports générés par le script précédemment créé puissent être envoyés par mail tous les matins. Il m'a également demandé d'étendre le monitoring aux 2 serveurs de production. L'envoi de mail étant déjà configuré sur le site internet de production, c'est le serveur que nous avons choisi pour exécuter le script à distance en SSH sur les 3 autres serveurs. Après analyse du besoin et des spécifications, je me suis rendu compte qu'il était plus judicieux de créer en parallèle un script de lancement, dans lequel les hôtes sont précisément indiqués. Lorsque toutes ces actions ont été validées en recette, j'ai déployé mes 2 scripts sur le serveur internet de production et ai ajouté une tâche récurrente via Crontab afin de lancer tous les matins le script « lanceur », qui à son tour lance le script « cœur » sur les machines indiquées dans le script de lancement. Les rapports ainsi générés sont alors stockés dans un répertoire spécifique et envoyé par mail à Guillaume et à moi-même tous les matins. A l'aide de Crontab j'ai également mis en place un archivage des rapports tous les 2 mois, afin de ne pas surcharger le serveur de production. Voici une liste récapitulative des principales tâches effectuées lors de cette activité :

- Réalisation du script de lancement
- Optimisation du script principal
- Envoi de mail contenant le rapport généré
- Planification des tâches via Crontab et archivage

4.3. Démarche/Mode opératoire

Réalisation du script de lancement

Le script de lancement, présenté ci-dessous, se compose de deux différentes parties :

- Les variables USERNAME et HOSTS : respectivement le nom de l'utilisateur qui sera utilisé pour effectuer les connexions SSH aux différents serveurs, et HOSTS, qui contient les FQDN des serveurs cibles.
- Une boucle *for*, qui permet de faire en sorte grâce à l'instruction *do* que pour chaque machine présente dans la variable HOSTS, une connexion SSH est établie.

Nous allons nous intéresser plus en détails à la commande présente dans le bloc conditionnel *for* et la décomposer :

- `ssh USERNAME@HOSTNAME` : une connexion SSH est ouverte avec la machine HOSTNAME
- `ssh USERNAME@HOSTNAME < ~/statut_serveurs.sh` : '`<`' permet d'exécuter la commande située à gauche de l'opérateur en passant le contenu du membre de droite dans son entrée standard. Ainsi dès que la session SSH est établie, le script `statut_serveurs.sh` est lancé.
- `ssh USERNAME@HOSTNAME < ~/statut_serveurs.sh >> « rapport_statut_serveurs/rapport-statut-serveurs-$(date + « %Y-%m-%d »).txt »` : '`>>`' exécute la commande située à sa gauche et redirige le résultat au format demandé
- La redirection se fait vers le dossier *rapport-statut-serveurs*, sous forme d'un fichier en .txt et dont le nom comportera la date du jour au format ANNEE-mois-jour.

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

Ainsi, pour chaque hôte présent dans la variable HOSTS, ici au nombre de 4, une connexion en SSH sera faite, suivie de l'exécution du script principal, puis le résultat de celui-ci sera stocké dans un fichier texte sur le serveur local, le serveur internet de production.

```
#!bin/bash

#USERNAME=renseigner ici le nom d'utilisateur utilisé pour lancer le script de connexion aux machines
#CHANGER ICI LE NOM DE L'UTILISATEUR
USERNAME=""

#HOSTS=Liste des machines sur lesquelles va s'exécuter le script
#CHANGER ICI LA LISTE DES MACHINES
#vps-1.vps.ovh.net : serveur internet production
#vps-2.vps.ovh.net : serveur extranet production
#vps-3.vps.ovh.net : serveur internet recette
#vps-4.vps.ovh.net : serveur extranet recette
HOSTS="vps-1.vps.ovh.net vps-2.vps.ovh.net vps-3.vps.ovh.net vps-4.vps.ovh.net"

#pour chaque machine renseignée dans HOSTS, on exécute le script statut_serveurs.sh et on met les résultats dans le fichier rapport-statut-serveurs.DATE.txt
#CHANGER ICI LE NOM DU SCRIPT
for HOSTNAME in ${HOSTS}; do
    ssh ${USERNAME}@${HOSTNAME} < ~/statut_serveurs.sh >> "rapport-statut-serveurs/rapport-statut-serveurs-$(date +%Y-%m-%d).txt"
done
```

Figure 9: Script de lancement.

Optimisation du script principal

Le script principal, appelé par le script de lancement, se décompose également en deux grandes parties :

- La déclaration des différentes variables et des fonctions
- L'affichage des résultats

Les variables sont au nombre de trois et permettent de récupérer les résultats de simples commandes :

- dt : permet de récupérer la date ainsi que l'heure du jour au format jour mois année et heures :minutes :secondes. Elle servira pour horodater le rapport généré.
- mydstat : permet de récupérer la charge actuelle du serveur à l'aide de la commande *dstat -l*. La commande *awk* suivie d'une expression régulière permet de ne récupérer ici que les 4 premières lignes.
- mydf : permet de récupérer l'utilisation des espaces de stockage des serveurs à l'aide de la commande *df -kh*, suivie d'un *grep* de la partition qui nous intéresse, ici */dev/sda1*.

Pour plus de facilité j'ai créé deux fonctions, l'une permet d'assigner des alias aux différentes machines, pour rendre la lecture du rapport plus aisée mais également pour choisir les services à monitorer en fonction du serveur. La deuxième fonction permet de récupérer le statut du service et d'indiquer simplement dans le rapport si celui-ci est OK ou KO :

- myname() : cette fonction, à l'aide de *case...esac*, vérifie si le nom de la machine récupéré via *\$HOSTNAME* correspond exactement aux différents cas. Ainsi un alias et un ou des services sont définis et stockés dans les variables correspondantes.
- myservice() : cette fonction permet pour chaque service de vérifier s'il tourne à l'aide d'une condition *if*. Si le service est en cours d'exécution alors une phrase sera renvoyée avec le *\$service* en question, suivi de OK. A l'inverse si le service ne tourne pas, alors on aura *\$service* KO.

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4


```
#!/bin/bash

#dt: fonction pour récupérer la date et l'heure afin d'horodater le rapport
dt=$(date '+%d/%m/%Y %H:%M:%S');

#mydstat: fonction qui permet grâce à une regex d'afficher les 4 premières lignes de lors de l'utilisation de la commande dstat
mydstat=$(dstat -l 1 1 | awk 'NR < 4');

#mydf: fonction qui permet de récupérer l'utiliastion de l'espace disque à l'aide d'un grep
mydf=$(df -kh | grep -Ew "Filesystem|dev/sda1");

#fonction permettant d'assigner un alias à la machine en fonction de son nom
#CHANGER L ALIAS SOUHAITE ICI
#CHANGER LES SERVICES SOUHAITES ICI
myname(){
    case $HOSTNAME in
        "██████████")
            ALIAS="SERVEUR INTERNET DE PROD"
            SERVICES="nginx mysql"
            ;;
        "██████████")
            ALIAS="SERVEUR EXTRANET DE PROD"
            SERVICES="httpd"
            ;;
        "██████████")
            ALIAS="SERVEUR INTERNET DE RECETTE"
            SERVICES="nginx mysql"
            ;;
        "██████████")
            ALIAS="SERVEUR EXTRANET DE RECETTE"
            SERVICES="httpd"
            ;;
    esac
}

#myservice: fonction pour récupérer le statut d'un service
myservice(){
    for service in ${SERVICES}; do
        if (systemctl is-active --quiet $service = 0)
        then
            echo "$service OK"
        else
            echo "$service KO"
        fi
    done
}

#invocation des fonctions pour initialiser l'alias et les services monitorés
myname
myservice
```

Figure 10: Script principal.

La deuxième partie du script est dédiée à l'affichage des résultats qui seront par la suite stockés dans un fichier texte. Les deux fonctions sont invoquées avant l'affichage, afin de récupérer les valeurs des alias, des services et du statut des services.

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

```

#début de l'affichage des résultats
echo
echo "#####"
echo "#####"
echo "RAPPORT DU $dt: $ALIAS"
echo
echo -----
echo -e "STATUT GLOBAL DU $ALIAS\n"
#affichage du résultat de la commande dstat
echo "$mydstat"
echo
echo -----
echo
#affichage du statut des services monitorés
echo -e "STATUT DU SERVICE $SERVICES DU $ALIAS\n"
echo
echo -----
echo -e "UTILISATION ESPACE DISQUE DU $ALIAS\n"
#affichage de la fonction df avec le grep de /dev/sda1
echo "$mydf"
echo
echo "#####"
echo "#####"
echo
#fin de l'affichage des résultats

```

Figure 11: Suite du script principal.

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

Envoi de mail contenant le rapport généré

Le serveur internet de production étant déjà équipé de l'envoi de mails, il faut uniquement utiliser la commande `cat` sur le rapports généré afin de mettre son contenu dans le corps du mail. Pour cela on utilise la ligne suivante :

- `cat rapport-statut-serveurs/rapport-statut-serveurs-$(date +%Y-%m-%d).txt | mail -s « Statut serveurs OVH du $(date +%d-%m-%Y) » eloise.deperetti@viasante.fr`

Planification des tâches via Crontab et archivage

Crontab est un programme permettant de planifier des tâches et des actions à des moments précis. Comme les deux scripts précédents se trouvent sur le serveur internet de production, il est possible à l'aide de quelques tâches planifiées de lancer automatiquement l'exécution des scripts au moment voulu.

Selon la configuration de Crontab ci-dessous, le script de lancement sera exécuté tous les matins à 7h30. De même, le mail contenant le rapport sera envoyé tous les matins à 8h00 à moi-même et à Guillaume.

La dernière tâche planifiée correspond à l'exécution d'un script pour l'archivage des rapports, et est lancée tous les 2 mois.

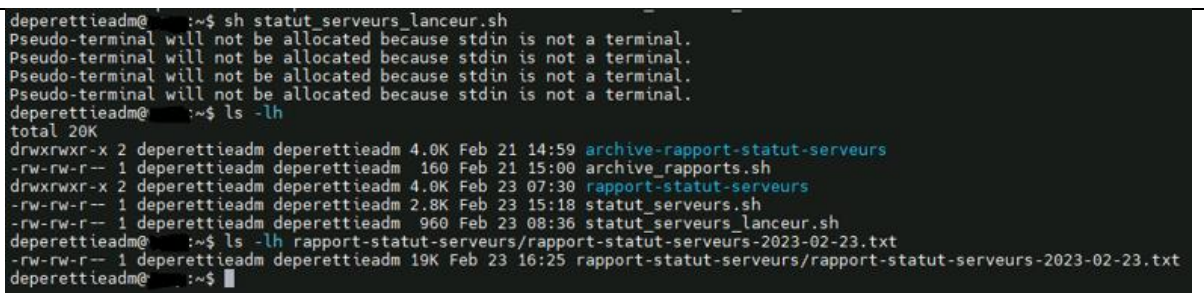
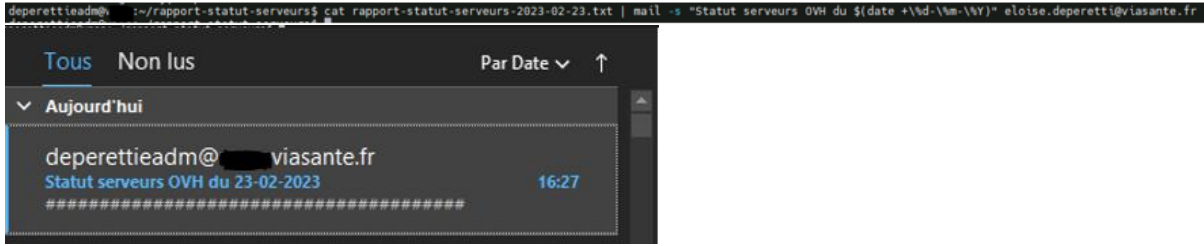
```
GNU nano 4.8 /tmp/crontab.UVjFzW/crontab
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
30 7 * * * sh statut_serveurs_lanceur.sh
0 8 * * * cat rapport-statut-serveurs/rapport-statut-serveurs-$(date +%Y-%m-%d).txt | mail -s "Statut serveurs OVH du $(date +%d-%m-%Y)" eloise.deperetti@viasante.fr guillaume.ricard@viasante.fr
0 1 */2 * sh archive_rapports.sh
```

Figure 12: Crontab des tâches planifiées.

```
#!/bin/bash
TODAY=$(date +%d-%m-%Y)
tar -cvf archive-rapport-statut-serveurs/archives-au-$TODAY.tar.gz rapport-statut-serveurs/*
rm rapport-statut-serveurs/*
```

Figure 13: Script pour l'archivage des rapports.

4.4. Preuves de la réalisation

Sous-activité	Captures d'écran
Réalisation du script de lancement	
Envoi de mail contenant le rapport généré	

Etudiant	DE PERETTI Eloise	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

Planification des tâches
via Crontab
et archivage

```
deperettieadm@ :~$ ls -lh
total 20K
drwxrwxr-x 2 deprerettieadm deprerettieadm 4.0K Feb 21 14:59 archive-rapport-statut-serveur
-rw-rw-r-- 1 deprerettieadm deprerettieadm 160 Feb 21 15:00 archive_rapports.sh
drwxrwxr-x 2 deprerettieadm deprerettieadm 4.0K Feb 24 07:30 rapport-statut-serveurs
-rw-rw-r-- 1 deprerettieadm deprerettieadm 2.8K Feb 24 08:13 statut_serveurs.sh
-rw-rw-r-- 1 deprerettieadm deprerettieadm 960 Feb 23 08:36 statut_serveurs_lanceur.sh
deperettieadm@ :~$ cd archive-rapport-statut-serveurs/
deperettieadm@ ~/archive-rapport-statut-serveurs$ ls
archives-au-21-02-2023.tar.gz
deperettieadm@ ~/archive-rapport-statut-serveurs$
```

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	4

FICHE 5 : RETOUR D'EXPERIENCE

5.1. Remerciements

Je tiens à remercier Chrystelle, qui m'a accueilli chaleureusement au sein de l'équipe et qui a toujours fait en sorte que je sois bien intégrée et à l'aise à ViaSanté. J'ai énormément apprécié passer du temps en sa compagnie, grâce à ses anecdotes captivantes et sa bonne humeur communicative.

Un très grand merci à Guillaume, mon tuteur durant cette alternance. Il a su me transmettre de précieuses connaissances lors de nos rencontres à Labège et à Rodez et ce, toujours dans la bienveillance.

Mes remerciements vont aussi à Alain et Eddie, qui n'ont pas manqué de me faire rire et sourire, aussi bien avec leurs étymologies maison de nos prénoms qu'avec leurs nombreuses plaisanteries, toujours affectueuses.

Un grand merci également à Sandra, qui m'a beaucoup accompagnée au début avec Chrystelle, et qui a toujours été adorable et d'une grande aide tout au long de mon parcours à ViaSanté.

Je tiens à remercier Laurent et Patrice pour leur expertise en réseau et leurs nombreuses explications, toujours dans la bienveillance.

Je veux également remercier Sébastien pour l'aide et les connaissances qu'il a partagé avec moi sur l'environnement Windows.

5.2. Points positifs

Mon alternance au sein de ViaSanté et notamment au sein de l'équipe infrastructure m'a permis de consolider mes connaissances en administration Linux et d'acquérir davantage de rigueur professionnelle. Cela a également été l'occasion pour moi de mettre en application les fondamentaux de mes savoirs en réseau et de faire du Scripting Bash. Mon appétence pour Linux s'en est trouvée confirmée et renforcée.

J'aimerais continuer de monter en compétences sur les systèmes d'exploitation Linux car pour moi ce sont des outils très puissants et polyvalents, couramment employés en entreprise grâce à leur robustesse, fiabilité et sécurité.

5.3. Pistes de progrès

Je pense qu'il me faudrait mettre l'accent sur ma communication afin de rendre celle-ci plus fluide, précise et concise. J'ai en effet parfois du mal à répondre de façon courte à des questions et mon vocabulaire technique est par moment trop vague pour mes interlocuteurs.

Bien que je sois assez réactive, je ne me trouve pas suffisamment proactive et j'aimerais que cela s'améliore. Selon moi cela va de pair avec la confiance en soi, or celle-ci est également à travailler car je doute constamment de moi et me mets en question trop fréquemment.

Enfin, j'aimerais renforcer mes savoirs en réseau. Je me trouve encore trop fragile lorsque des compétences de ce domaine me sont nécessaires : DNS, DHCP, MPLS, pare-feu, proxy, WAF etc.

Etudiant	DE PERETTI Eloïse	Tuteur	RICARD Guillaume	Entreprise	ViaSanté Mutuelle
Année Scolaire	2022/2023	Section	1SIO / 2SIO	Numéro de fiche	5

Référentiel détaillé du bloc 1 - BTS SIO

Domaine d'activité 1 : Support et mise à disposition de services informatiques

En prenant en charge la fonction de support informatique, la personne titulaire du diplôme répond aux attentes des utilisateurs ou des clients en s'assurant de la disponibilité des services existants et de la mise à disposition de nouveaux services. Ainsi, en prenant en compte les besoins métiers de l'organisation, elle accompagne sa transformation numérique tout en maintenant son employabilité.

Pour assurer les missions qui lui sont confiées, la personne titulaire du diplôme est amenée à travailler en mode projet en collaborant avec des membres de l'organisation ou des partenaires.

Activité 1.1. Gestion du patrimoine informatique

- Recensement et identification des ressources numériques
- Exploitation des référentiels, normes et standards adoptés par le prestataire informatique
- Mise en place et vérification des niveaux d'habilitation associés à un service
- Vérification des conditions de la continuité d'un service informatique
- Gestion des sauvegardes
- Vérification du respect des règles d'utilisation des ressources numériques

Activité 1.2. Réponse aux incidents et aux demandes d'assistance et d'évolution

- Collecte, suivi et orientation des demandes
- Traitement des demandes concernant les applicatifs, services réseau et système
- Traitement des demandes concernant les applications

Activité 1.3. Développement de la présence en ligne de l'organisation

- Participation à la valorisation de l'image de l'organisation sur les médias numériques en tenant compte du cadre juridique et des enjeux économiques
- Référencement des services en ligne de l'organisation et mesure de leur visibilité
- Participation à l'évolution d'un site Web exploitant les données de l'organisation

Activité 1.4. Travail en mode projet

- Analyse des objectifs et des modalités d'organisation d'un projet
- Planification des activités
- Évaluation des indicateurs de suivi d'un projet et analyse des écarts

Activité 1.5. Mise à disposition des utilisateurs d'un service informatique

- Test d'intégration et d'acceptation d'un service
- Déploiement d'un service
- Accompagnement des utilisateurs dans la mise en place d'un service

Activité 1.6. Organisation de son développement professionnel

- Mise en place de son environnement d'apprentissage personnel
- Mise en œuvre d'outils et de stratégie veille informationnelle
- Gestion de son identité professionnelle
- Développement de son projet professionnel