

Mise en place de la haute disponibilité pour les Serveurs web



Sommaire :

Environnement technique :	3
Description du projet :	3
Contexte :	6
Topologie physique :	7
Solutions possibles :	8
Convention de nommage :	9
Configuration :	10
Plan d'adressage :	10
Physique :	10
Logiciel :	11
Préparation des serveurs Web Debian :	12
Vérification de l'accès à Internet :	12
Ajout des droits super utilisateur :	13
Mise à jour des serveurs Debian :	14
Installation du SSH :	14
Mettre les serveurs dans le domaine :	15
Installation de Apache 2 :	15
Importation de la page web de Dualya :	16
Mise en place de la redondance avec HAProxy :	18
Installation de HAProxy :	18
Configuration du service HAProxy :	19
Configuration de la page de statistique de HAProxy :	21
Difficultés rencontrées :	22
Améliorations possibles :	22
Conclusion :	22
Annexe 1 : Topologie physique.	23
Annexe 2 : Schéma de Gantt.	24
Annexe 3 : Gestionnaire de mot de passe.	25

Environnement technique :

Voici ci-dessous la fiche de l'environnement technique de la maquette.

Environnement Technique pour les deux dossiers E5		
Qui	Quoi	Solution ?
Mise à disposition par le centre de formation	Gestion des incidents	Jira
	Détection et prévention des intrusions	WAZUH
	Chiffrement	Bitlocker
	Analyse de trafic	PFSENSE
Maquette à créer par l'apprenant dans la globalité	Un réseau comportant plusieurs périmètres de sécurité	Sous-réseau Pfsense et fortinate, Vlan sur Switch CISCO
	Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité	GLPI
	Un logiciel d'analyse de trames	Wireshark
	Un logiciel de gestion des configurations	Glpi + Fusion Inventory
	Une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès	VPN
	Une solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes	WAZUH
	Une solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet)	Pfsense + fortigate
	Une solution garantissant la continuité d'un service	SSH, VPN
	Une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion	Raid, Onduleurs
	Une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion	HAPROXY
Une option à choisir par l'apprenant et à intégrer dans sa maquette	Une solution permettant la connexion sécurisée entre deux sites distants	VPN inter-sites
	Une solution permettant le déploiement des solutions techniques d'accès	FOG
	Une solution gérée à l'aide de procédures automatisées écrites avec un langage de scripting	Powershell
	Une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau	Pfsense

Description du projet :

Vous trouverez sur les deux pages suivantes la description de la réalisation professionnelle de mon premier projet proposé. Je vous détaillerai tous les besoins nécessaires pour mener à bien la réalisation de ce projet.

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (recto)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE		N° réalisation : 1
Nom, prénom : HACHET Nicolas		N° candidat : 02203380653
Épreuve ponctuelle <input checked="" type="checkbox"/>	Contrôle en cours de formation <input type="checkbox"/>	Date : ..13 / ..03 / ..2025
Organisation support de la réalisation professionnelle Dans cette situation professionnelle, l'entreprise Dualya fait appel à nos services pour mettre en place la redondance des serveurs web, accessible localement par les collaborateurs.		
Intitulé de la réalisation professionnelle J'ai donc installé trois machine virtuelle (deux serveurs web et un serveur Debian pour la redondance), sur laquelle j'ai configuré les services Apache2 et la haute disponibilité.		
Période de réalisation : ... Du 03/03/2025 au 07/03/2025 Lieu : ... CFA Fab/Academy - La Roche Sur Yon		
Modalité : <input checked="" type="checkbox"/> Seul(e) <input type="checkbox"/> En équipe		
Compétences travaillées <input checked="" type="checkbox"/> Concevoir une solution d'infrastructure réseau <input checked="" type="checkbox"/> Installer, tester et déployer une solution d'infrastructure réseau <input checked="" type="checkbox"/> Exploiter, dépanner et superviser une solution d'infrastructure réseau		
Conditions de réalisation¹ (ressources fournies, résultats attendus) Ressources fournies : Un accès internet, un hyperviseur (machine virtuelles : deux serveurs web, un serveur pour la redondance, Windows 10), un ordinateur portable sous Windows 10 Ressources attendus : Une infrastructure fonctionnelle répondant à la demande du client avec une solution accessible local. Deux serveurs Web virtualisé et un serveurs de redondance virtualisé installé sous Debian et accessible aux utilisateurs Windows 10 via une interface web grâce a l'adresse IP du serveur.		
Description des ressources documentaires, matérielles et logicielles utilisées² Ressources documentaires : documentation technique, documentation utilisateur, schéma réseau de l'entreprise Dualya. Ressources matérielles : un hyperviseur avec des machines virtuelles configurées (Serveurs Web, Serveur de redondance, Windows 10) et un ordinateur portable avec Windows 10 installé. Ressources logicielles : Draw.io, Mozilla Firefox, VMware, Windows 10, debian12, Apache2, WinSCP.		
Modalités d'accès aux productions³ et à leur documentation⁴ Tous les dossiers techniques et le guide des utilisateurs sont accessibles à l'adresse suivante : https://nicolas.hachet.formaton-esiac.fr/		

¹ En référence aux conditions de réalisation et ressources nécessaires du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

² Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

³ Conformément au référentiel du BTS SIO « Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve. ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

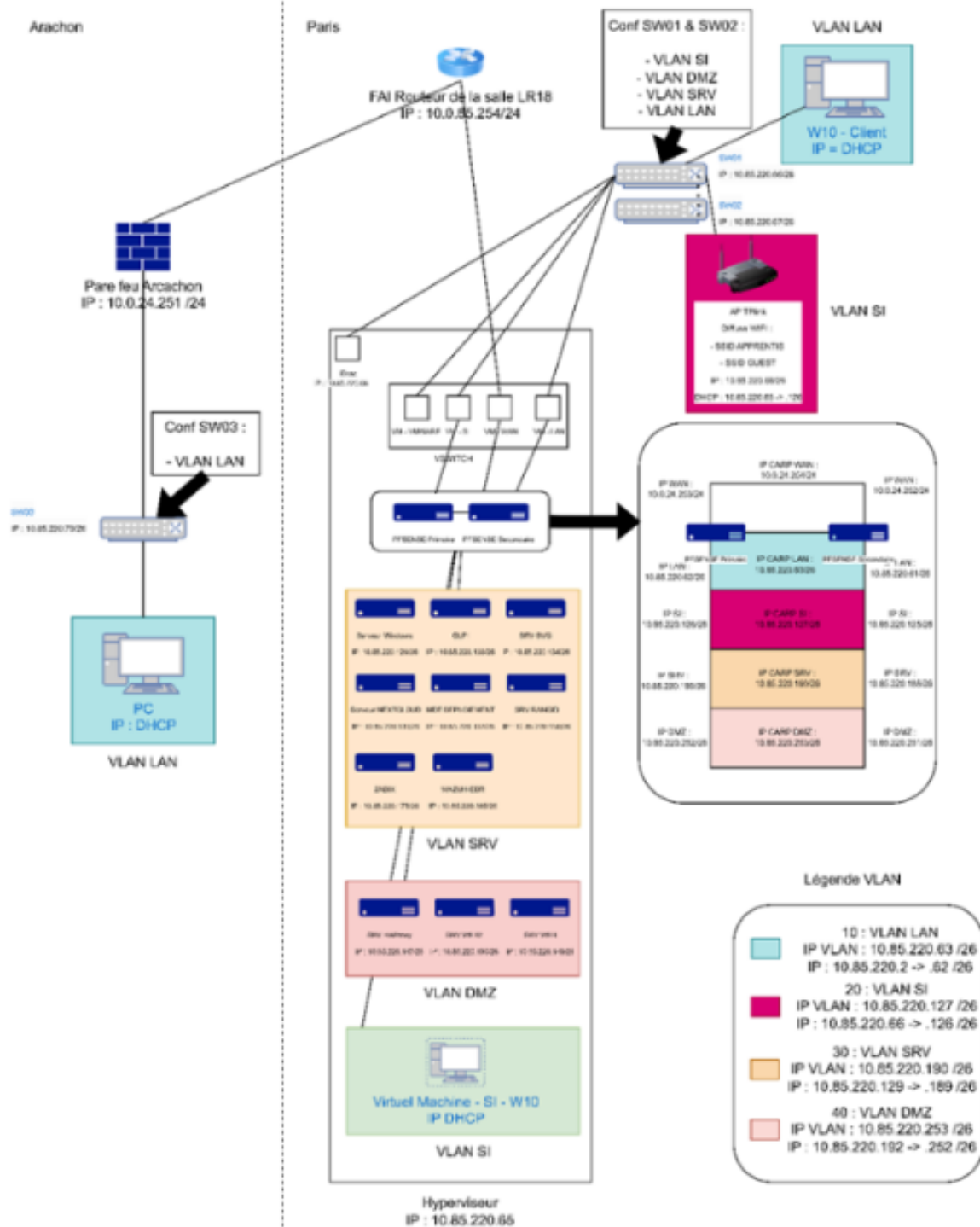
⁴ Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

**ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle
(verso, éventuellement pages suivantes)**

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

Voici le schéma d'infrastructure respectant le schéma réseau, composée des deux serveurs Web et du serveur HAProxy installé sur des machines virtuelle Debian 12, accessible aux clients Windows 10 via une interface web grâce à l'adresse IP du serveur HAProxy.



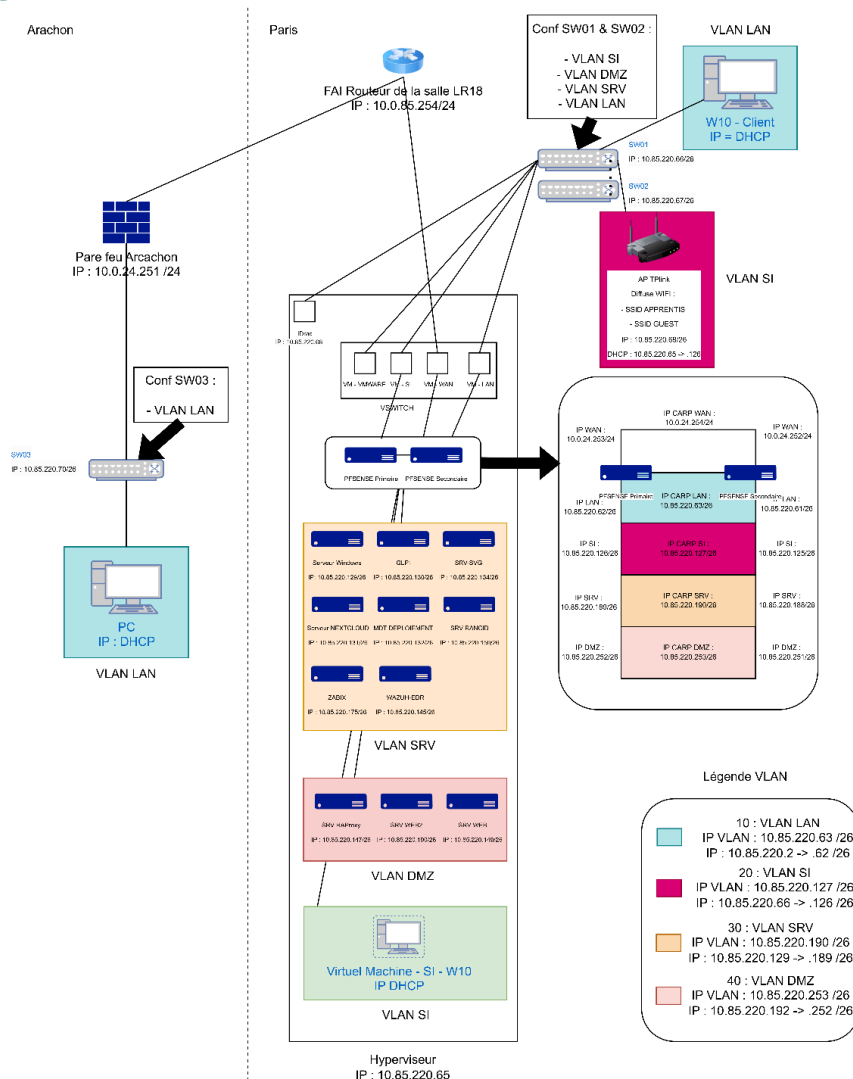
Contexte :

L'entreprise Dualya, spécialisée dans l'art et la rénovation, souhaite renforcer sa visibilité numérique. Pour cela, elle a fait appel au prestataire informatique HAssistance afin de l'accompagner dans la mise en œuvre de sa stratégie digitale.

L'objectif principal de Dualya est de développer sa présence en ligne pour valoriser son savoir-faire et toucher de nouveaux clients potentiels. Il est donc essentiel de garantir un accès fluide, rapide et constant à son site web, y compris en période de forte affluence. L'optimisation de l'expérience utilisateur, notamment à travers la réduction des temps de chargement, est une priorité pour favoriser la fidélisation des visiteurs.

Comment concevoir la présence en ligne de l'entreprise Dualya tout en garantissant à ses clients un accès fiable, performant ?

Topologie physique :



La maquette repose sur une architecture réseau conçue pour garantir la connectivité, la sécurité et la haute disponibilité du service web. Le réseau est segmenté en plusieurs VLAN, ce qui permet une isolation logique des différents services et un meilleur contrôle des flux de données.

Afin de renforcer la sécurité, l'infrastructure intègre trois pare-feux : un pare-feu physique Fortinet, ainsi que deux pare-feux virtuels PfSense, chargés de filtrer les accès et de protéger l'ensemble du système contre les menaces externes et internes.

Un serveur DHCP assure l'attribution dynamique des adresses IP aux équipements du réseau, tandis qu'un contrôleur de domaine (Active Directory) gère de manière centralisée les utilisateurs et leurs droits d'accès.

Enfin, un conteneur KeePass, accessible depuis le réseau de la salle BTS, permet de consulter de manière sécurisée les identifiants nécessaires à la connexion aux différentes machines du système.

Solutions possibles :

Choix de l'infrastructure web pour Dualya

Pour héberger le site web de Dualya, plusieurs options sont envisageables, chacune présentant des avantages spécifiques. Les serveurs web Apache et Nginx sont parmi les plus utilisés dans le monde professionnel.

Apache est reconnu pour sa flexibilité, sa large compatibilité avec de nombreux modules (comme `mod_rewrite`, `mod_security`, etc.) et sa documentation abondante, ce qui facilite sa personnalisation. Cependant, son architecture basée sur des processus ou des threads peut le rendre moins performant en cas de forte charge.

Nginx, quant à lui, se distingue par son excellente gestion des connexions simultanées, grâce à une architecture événementielle. Il est donc particulièrement adapté aux environnements à fort trafic, bien que parfois moins personnalisable qu'Apache.

IIS (Internet Information Services) est une alternative solide dans un environnement Windows, mais il reste moins adapté à des infrastructures mixtes ou open source comme celle envisagée pour Dualya.

En complément, pour garantir la haute disponibilité du service web, l'utilisation d'un équilibreur de charge est indispensable. HAProxy s'impose comme une solution de référence, reconnue pour sa robustesse, ses bonnes performances et ses fonctionnalités de monitoring en temps réel. Il prend en charge plusieurs algorithmes de répartition, tels que round-robin ou leastconn, ce qui permet d'optimiser l'utilisation des ressources serveurs.

Choix retenu

Pour répondre aux besoins de Dualya, nous avons retenu une architecture associant :

Apache, pour sa souplesse de configuration et sa richesse fonctionnelle,

HAProxy, pour assurer une répartition de charge efficace et garantir une haute disponibilité du site web.

Cette combinaison permet de mettre en place une infrastructure stable, performante et évolutive, capable de soutenir la croissance de l'entreprise et de garantir une expérience utilisateur optimale.

Convention de nommage :

Nous avons décidé d'utiliser une convention de nommage pour optimiser l'infrastructure de Dualya.

Une convention de nommage dans une infrastructure informatique, c'est un ensemble de règles définies pour nommer de manière cohérente les éléments techniques d'un système.

Machines :

Ex : VM-DMZ-WEB-01

VM → Machine virtuelle

DMZ → Nom du VLAN sur lequel se situe la VM

WEB → Nom du Service

PA → Site où se trouve l'équipement (PA = Paris, AR = Arcachon)

01 → Numéro de la machine en fonction de ses pairs, s'il y a deux serveur WEB le deuxième serait le -02

Utilisateurs :

Les machines seront administrées par l'utilisateur admin (administrateur) et un mot de passe.

Machines \ Compte	Identifiant	Mot de passe
VM-DMZ-WEB-01	tech	(Keepass)
VM-DMZ-WEB-02	tech	(keepass)

Configuration :

Plan d'adressage :

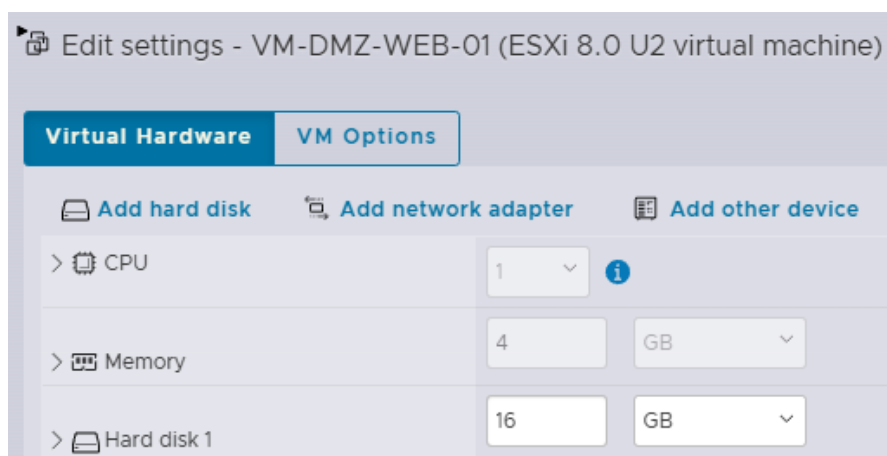
	Adresse IP	Masque	Passerelle
VM-DMZ-WEB-01	10.85.220.193	255.255.255.192	10.85.220.254
VM-DMZ-WEB-02	10.85.220.194	255.255.255.192	10.85.220.254
VM-DMZ-HAPROXY-01	10.85.220.195	255.255.255.192	10.85.220.254

Le plan d'adressage a été conçu de manière à ce que les machines soient intégrées dans le réseau du VLAN DMZ

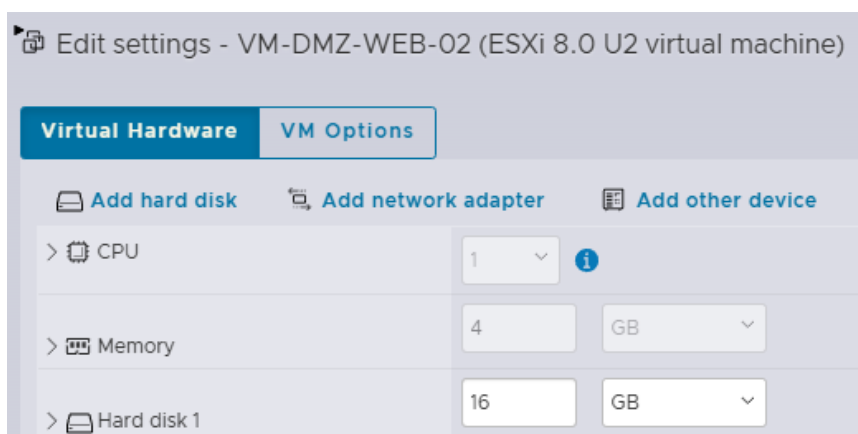
Physique :

Les serveurs possèdent 1 processeurs avec 1 sockets et 1 cœur, 4 Go de mémoire vive et 16 Go d'espace de stockage. Cette configuration choisie permet à la machine d'être rapide et efficace lors de sa configuration.

VM-DMZ-WEB-01 :



VM-DMZ-WEB-02 :



Logiciel :

Les deux serveurs web ont été configurés de manière identique afin d'assurer la haute disponibilité d'un site unique accessible aux clients. Chaque machine virtuelle est équipée du service SSH, permettant une administration à distance simple et sécurisée.

Un utilisateur nommé "tech", doté des droits administrateurs, est utilisé sur l'ensemble des machines afin de faciliter la gestion centralisée par l'équipe informatique de HAssistance.

Le système d'exploitation retenu est Debian 12.10, la dernière version stable. Ce choix offre une meilleure compatibilité matérielle, des performances optimisées et un niveau de sécurité renforcé grâce aux mises à jour récentes — des éléments essentiels pour garantir un service web fiable.

Une fois les configurations de base réalisées, les serveurs ont été intégrés au domaine Active Directory. Cette intégration permet une gestion centralisée des utilisateurs et des autorisations, simplifiant l'authentification, la gestion des droits d'accès, et renforçant la sécurité globale du système.

Préparation des serveurs Web Debian :

Vérification de l'accès à Internet :

Pour commencer, nous avons vérifié que les machines virtuelles (VM) disposaient bien d'un accès à Internet. Cette étape passe par la vérification de leur configuration réseau, afin de s'assurer qu'elles sont correctement adressées conformément au plan d'adressage défini.

```
tech@VM-DMZ-WEB-01:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:eb:2b:28 brd ff:ff:ff:ff:ff:ff
    altname enp11s0
    inet 10.85.220.193/26 brd 10.85.220.255 scope global noprefixroute ens192
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feeb:2b28/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Nous avons constaté que les machines sont correctement adressées conformément au plan d'adressage. Nous allons donc effectuer un test de connectivité en envoyant une requête ping vers l'adresse IP 8.8.8.8, qui correspond à un serveur DNS public de Google.

Si le ping est réussi, cela confirmera que les machines virtuelles ont bien accès à Internet et peuvent communiquer en dehors du réseau local.

```
tech@VM-DMZ-WEB-01:/$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=12.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=13.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=14.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=117 time=12.9 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 12.628/13.262/14.057/0.539 ms
```

Nous pouvons constater que le test de ping a réussi, car tous les paquets envoyés ont été reçus.

Ensuite, j'ai effectué un test de résolution DNS en lançant un ping vers le nom de domaine *google.fr*. Ce test permet de vérifier si la machine est capable de résoudre un nom de domaine en adresse IP.

L'objectif principal est de s'assurer que la résolution DNS fonctionne correctement. En effet, lorsqu'un utilisateur accède à un site web via son nom de domaine (par exemple *google.fr*), le système doit le traduire en adresse IP pour établir la connexion. Si cette traduction échoue, la machine ne pourra pas accéder au site, même si la connexion Internet est fonctionnelle.

Ce test confirme donc que les serveurs DNS configurés sont opérationnels et que la machine peut résoudre correctement les noms de domaine, ce qui est indispensable pour une navigation Internet efficace.

```
tech@VM-DMZ-WEB-01:/$ ping google.fr
PING google.fr (par21s19-in-x03.1e100.net (2a00:1450:4007:813::2003)) 56 data bytes
64 bytes from par21s19-in-x03.1e100.net (2a00:1450:4007:813::2003): icmp_seq=1 ttl=116 time=12.3 ms
64 bytes from par21s19-in-x03.1e100.net (2a00:1450:4007:813::2003): icmp_seq=2 ttl=116 time=14.0 ms
64 bytes from par21s19-in-x03.1e100.net (2a00:1450:4007:813::2003): icmp_seq=3 ttl=116 time=12.9 ms
64 bytes from par21s19-in-x03.1e100.net (2a00:1450:4007:813::2003): icmp_seq=4 ttl=116 time=12.8 ms
^C
--- google.fr ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 12.330/12.998/13.984/0.606 ms
```

Nous pouvons constater que le test de ping a réussi, car tous les paquets envoyés ont été reçus. J'ai effectué ces actions sur les serveurs VM-SRV-WEB-01, VM-SRV-WEB-02 ainsi que sur le serveur HAProxy VM-SRV-HAPROXY-01.

Ajout des droits super utilisateur :

Pour ajouter l'utilisateur 'tech' au groupe sudo et lui permettre d'avoir des droits d'administration lorsqu'il utilise la commande sudo, je me suis connecté en tant qu'utilisateur root.

```
tech@VM-DMZ-WEB-01:/$ su -
```

Ensuite, j'ai ajouté l'utilisateur 'tech' au groupe sudo.

```
root@VM-DMZ-WEB-01:~# usermod -aG sudo tech
```

Vérification des droits de super utilisateur :

Enfin, j'ai vérifié que l'utilisateur 'tech' avait bien été ajouté au groupe sudo.

```
root@VM-DMZ-WEB-01:~# groups tech
tech : tech cdrom floppy sudo audio dip video plugdev users netdev bluetooth lpadmin scanner
```

Nous pouvons constater que l'utilisateur 'tech' a bien été ajouté au groupe sudo. Un redémarrage est nécessaire pour que le serveur prenne en compte les modifications. J'ai effectué ces actions sur les serveurs VM-SRV-WEB-01, VM-SRV-WEB-02 ainsi que sur le serveur HAProxy VM-SRV-HAPROXY-01.

Mise à jour des serveurs Debian :

Après avoir vérifié l'accès à Internet et ajouté l'utilisateur 'tech' au groupe sudo, j'ai procédé à la mise à jour des serveurs.

```
tech@VM-DMZ-WEB-01:/$ sudo apt update && sudo apt upgrade -y
```

Après avoir mis à jour le serveur, j'ai vérifié qu'il était bien à jour.

Vérification que les serveurs sont à jour :

Pour vérifier que le serveur était à jour, j'ai utilisé la commande « sudo apt update ».

```
tech@VM-DMZ-WEB-01:/$ sudo apt update
Atteint :1 http://deb.debian.org/debian bookworm InRelease
Atteint :2 http://security.debian.org/debian-security bookworm-security InRelease
Atteint :3 http://deb.debian.org/debian bookworm-updates InRelease
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Tous les paquets sont à jour.
```

On peut constater que le serveur est bien à jour, car il est indiqué que tous les paquets sont à jour. J'ai effectué ces actions sur les serveurs VM-SRV-WEB-01, VM-SRV-WEB-02 ainsi que sur le serveur HAProxy VM-SRV-HAPROXY-01. Ensuite, j'ai installé le service SSH.

Installation du SSH :

Pour installer le service SSH, j'ai utilisé la commande « apt install ssh ».

```
tech@VM-DMZ-WEB-01:/$ sudo apt install ssh
```

Vérification que le service SSH est bien installé :

Pour vérifier que le service SSH est bien installé, j'ai utilisé la commande « systemctl status ssh ».

```
tech@VM-DMZ-WEB-01:/$ sudo systemctl status ssh
• ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Tue 2025-04-22 23:28:22 CEST; 36min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 755 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 783 (sshd)
    Tasks: 1 (limit: 2241)
   Memory: 1.6M
      CPU: 36ms
   CGroup: /system.slice/ssh.service
           └─783 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

avril 22 23:28:22 VM-DMZ-WEB-01 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
avril 22 23:28:22 VM-DMZ-WEB-01 sshd[783]: Server listening on 0.0.0.0 port 22.
avril 22 23:28:22 VM-DMZ-WEB-01 sshd[783]: Server listening on :: port 22.
avril 22 23:28:22 VM-DMZ-WEB-01 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

Nous pouvons constater que SSH est bien installé et actif, car le statut indique 'active'.

J'ai effectué ces actions sur les serveurs VM-SRV-WEB-01, VM-SRV-WEB-02 ainsi que sur le serveur HAProxy VM-SRV-HAPROXY-01.

Mettre les serveurs dans le domaine :

Pour mettre le serveur dans le domaine, j'ai installé le service « realm ».

```
tech@VM-DMZ-WEB-01:/$ sudo apt install realmd
```

Ensuite, j'ai ajouté le serveur Debian dans le domaine.

```
tech@VM-DMZ-WEB-01:/$ sudo realm join --user=Administrateur dualya.local
```

Le mot de passe du compte « Administrateur » sur l'AD doit ensuite être renseigné.

Vérification que les serveurs se trouvent bien dans le domaine :

Pour vérifier que le serveur est bien dans le domaine, j'ai tapé la commande realm list.

```
tech@VM-DMZ-WEB-01:~$ sudo realm list
[sudo] Mot de passe de tech :
dualya.local
  type: kerberos
  realm-name: DUALYA.LOCAL
  domain-name: dualya.local
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
  required-package: samba-common-bin
  login-formats: %U@dualya.local
  login-policy: allow_realm_logins
```

Comme nous pouvons le voir, le serveur est bien dans le domaine, car nous avons les informations du domaine.

J'ai effectué ces actions sur les serveurs VM-SRV-WEB-01, VM-SRV-WEB-02 ainsi que sur le serveur HAProxy VM-SRV-HAPROXY-01.

Après toutes ces vérifications, la préparation des serveurs est terminée.

Installation de Apache 2 :

J'ai installé le service apache2.

```
tech@VM-DMZ-WEB-01:/$ sudo apt install apache2
```

Vérification que le service Apache2 est bien installé :

Pour vérifier que le service apache2 est bien installé et fonctionne, j'ai utilisé la commande « `systemctl status apache2` ».

```
tech@VM-DMZ-WEB-01:/$ sudo systemctl status apache2
• apache2.service - The Apache HTTP Server
  Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
  Active: active (running) since Tue 2025-04-22 23:28:22 CEST; 41min ago
    Docs: https://httpd.apache.org/docs/2.4/
  Process: 750 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 794 (apache2)
   Tasks: 55 (limit: 2241)
  Memory: 10.1M
    CPU: 239ms
  CGroup: /system.slice/apache2.service
          └─794 /usr/sbin/apache2 -k start
            └─795 /usr/sbin/apache2 -k start
              └─796 /usr/sbin/apache2 -k start
```

Nous pouvons constater que le service Apache2 est bien installé et actif, car le statut indique 'active'.

Une autre méthode pour vérifier que le service apache2 fonctionne consiste à ouvrir un navigateur web et à entrer l'adresse IP du serveur web. Si apache2 est fonctionnel, une page par défaut devrait apparaître, comme celle ci-dessous.



J'ai effectué ces actions sur les serveurs VM-SRV-WEB-01, VM-SRV-WEB-02. Après avoir installé le service apache2, j'ai importé la page web de Dualya sur les serveurs.

Importation de la page web de Dualya :

La page web a été conçue et développée sur l'ordinateur du service informatique. Il est donc nécessaire de la transférer vers le nouveau serveur web.

Pour importer la page web de Dualya, qui était sur l'ordinateur du SI, vers le serveur web, j'ai installé WinSCP sur l'ordinateur.

WinSCP est un outil permettant de copier des fichiers d'une machine vers une autre grâce au SSH.

Après avoir installé WinSCP, je l'ai lancé sur l'ordinateur.

Pour me connecter au serveur web, j'ai dû renseigner l'adresse IP de celui-ci ainsi que les informations de connexion (nom d'utilisateur et mot de passe).

Session

Protocole de fichier
SFTP

Nom d'hôte
10.85.220.193

Numéro de port
22

Nom d'utilisateur
tech

Mot de passe
●●●●●●●●

Sauver... Avancé...

Connexion Fermer Aide

Ensuite, j'ai déplacé le site web (index.html et style.css) dans le répertoire « /tmp/ » du serveur web, car je n'avais pas les droits pour les mettre dans « /var/www/html/ ».

C:\atuer\				/tmp/				
Nom	Taille	Type	Date de modification	Nom	Taille	Date de modification	Droits	Prop
+		Répertoire parent	18/04/2025 09:40:37	..		15/04/2025 10:48:18	rw-r--r--	root
index.html	2 KB	Microsoft Edge H...	15/04/2025 09:55:04	systemd-private-bda...		18/04/2025 09:16:40	rw-r--r--	root
style.css	2 KB	Document de feui...	15/04/2025 09:55:10	systemd-private-bda...		18/04/2025 09:17:02	rw-r--r--	root
				systemd-private-bda...		18/04/2025 09:16:32	rw-r--r--	root
				systemd-private-bda...		18/04/2025 09:16:38	rw-r--r--	root
				systemd-private-bda...		18/04/2025 09:16:32	rw-r--r--	root
				systemd-private-bda...		18/04/2025 09:16:32	rw-r--r--	root
				systemd-private-bda...		18/04/2025 09:16:32	rw-r--r--	root
				systemd-private-bda...		18/04/2025 09:16:32	rw-r--r--	root
				systemd-private-bda...		18/04/2025 09:16:25	rw-r--r--	root
				systemd-private-bda...		18/04/2025 09:17:00	rw-r--r--	root
				Temp-6f15ea8b-1111-...		18/04/2025 09:29:40	rw-r--r--	web
				tracker-extract-3-files...		18/04/2025 09:17:11	rw-r--r--	Debi
				tracker-extract-3-files...		18/04/2025 09:28:55	rw-r--r--	web
				VMwareDnD		18/04/2025 09:16:25	rw-rwxrwt	root
				vmware-root_422-591...		18/04/2025 09:16:35	rw-r--r--	root
				index.html	2 KB	15/04/2025 09:55:04	rw-r--r--	web
				style.css	2 KB	15/04/2025 09:55:10	rw-r--r--	web

Une fois les fichiers copiés dans /tmp/, j'ai utilisé la commande mv pour déplacer les fichiers de /tmp/ vers /var/www/html/.

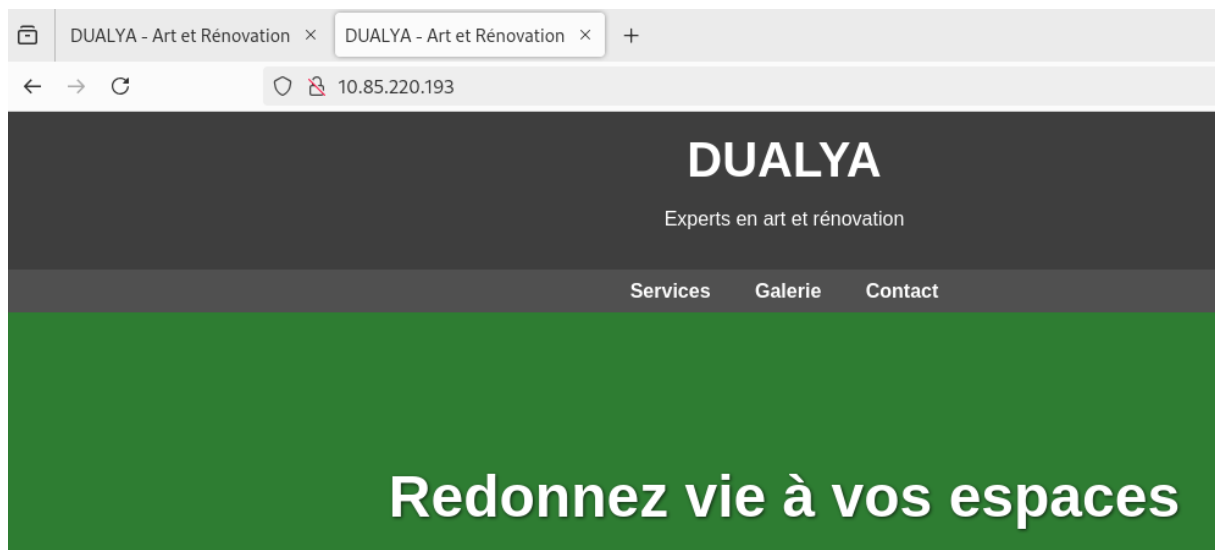
```
tech@VM-SRV-WEB-01:~$ sudo mv /tmp/index.html /var/www/html/
```

```
tech@VM-SRV-WEB-01:~$ sudo mv /tmp/style.css /var/www/html/
```

Pour finir, j'ai vérifié que le nouveau site web s'affichait bien à l'adresse IP du serveur.

Vérification du nouveau site web :

Pour tester si le nouveau site web s'affiche, je suis allé(e) sur un navigateur web et j'ai inséré l'adresse IP du serveur web.



Nous pouvons constater que cela fonctionne, car la page par défaut d'Apache2 a été remplacée par celle de Dualya.

Une modification a été apportée sur le site web de Dualya sur VM-SRV-WEB-02 afin de différencier la page web de VM-SRV-WEB-01 et de VM-SRV-WEB-02.

J'ai effectué ces actions sur les serveurs VM-SRV-WEB-01 et VM-SRV-WEB-02.

Mise en place de la redondance avec HAProxy :

Installation de HAProxy :

J'ai commencé par installer le service HAProxy.

```
tech@VM-DMZ-HAPROXY-01:~$ sudo apt install haproxy
```

Ensuite, j'ai vérifié la version de HAProxy.

```
tech@VM-DMZ-HAPROXY-01:~$ sudo haproxy -v
HAProxy version 2.6.12-1+deb12u1 2023/12/16 - https://haproxy.org/
Status: long-term supported branch - will stop receiving fixes around Q2 2027.
Known bugs: http://www.haproxy.org/bugs/bugs-2.6.12.html
Running on: Linux 6.1.0-33-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.133-1 (2025-04-10) x86_64
```

Après avoir installé et vérifié la version du service HAProxy, je l'ai configuré.

Configuration du service HAProxy :

Pour configurer le service HAProxy, je suis allé(e) dans le fichier « haproxy.cfg ».

```
tech@VM-DMZ-HAPROXY-01:~$ sudo nano /etc/haproxy/haproxy.cfg
```

```

GNU nano 7.2                                tech@VM-DMZ-HAPROXY-01: ~
/etc/haproxy/haproxy.cfg
global
    log /dev/log      local0
    log /dev/log      local1 notice
    chroot /var/lib/haproxy
    stats socket /run/haproxy/admin.sock mode 660 level admin
    stats timeout 30s
    user haproxy
    group haproxy
    daemon

    # Default SSL material locations
    ca-base /etc/ssl/certs
    crt-base /etc/ssl/private

    # See: https://ssl-config.mozilla.org/#server=haproxy&server-version=2.0.3&config=intermediate
    ssl-default-bind-ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-R
    ssl-default-bind-ciphersuites TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256
    ssl-default-bind-options ssl-min-ver TLSv1.2 no-tls-tickets

```

Dans ce fichier, tout en bas, j'ai commencé par ajouter la configuration frontend.

```

frontend front_webserver
    bind *:80
    default_backend backend_webserver
    option forwardfor

```

Le frontend dans HAProxy est la partie qui reçoit les requêtes des clients. Dans cette configuration, il écoute sur le port 80, redirige les requêtes vers le backend backend_webserver, et utilise l'option forwardfor pour transmettre l'adresse IP du client aux serveurs backend.

Ensuite, j'ai ajouté la configuration backend.

```

backend backend_webserver
    balance roundrobin
    server VM-SRV-WEB-01 10.85.220.193:80 check
    server VM-SRV-WEB-02 10.85.220.194:80 check

```

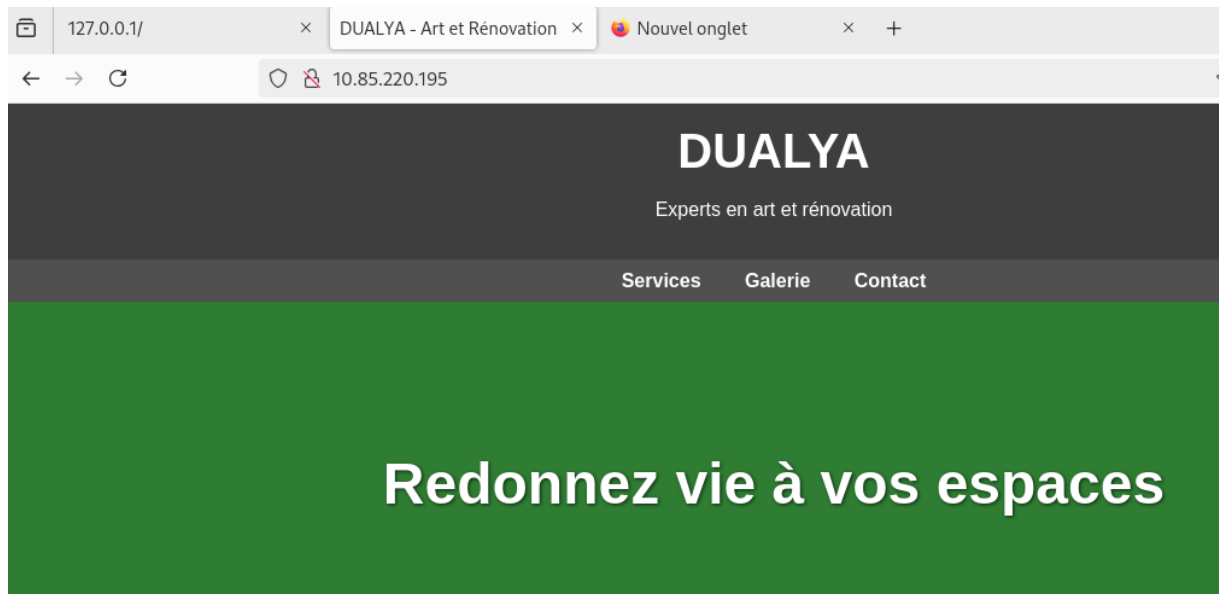
Le backend backend_webserver contient deux serveurs web. HAProxy distribue les requêtes entre eux en round-robin pour équilibrer la charge. Il effectue aussi des vérifications de santé (check) pour s'assurer que les serveurs sont disponibles.

Test de HAProxy :

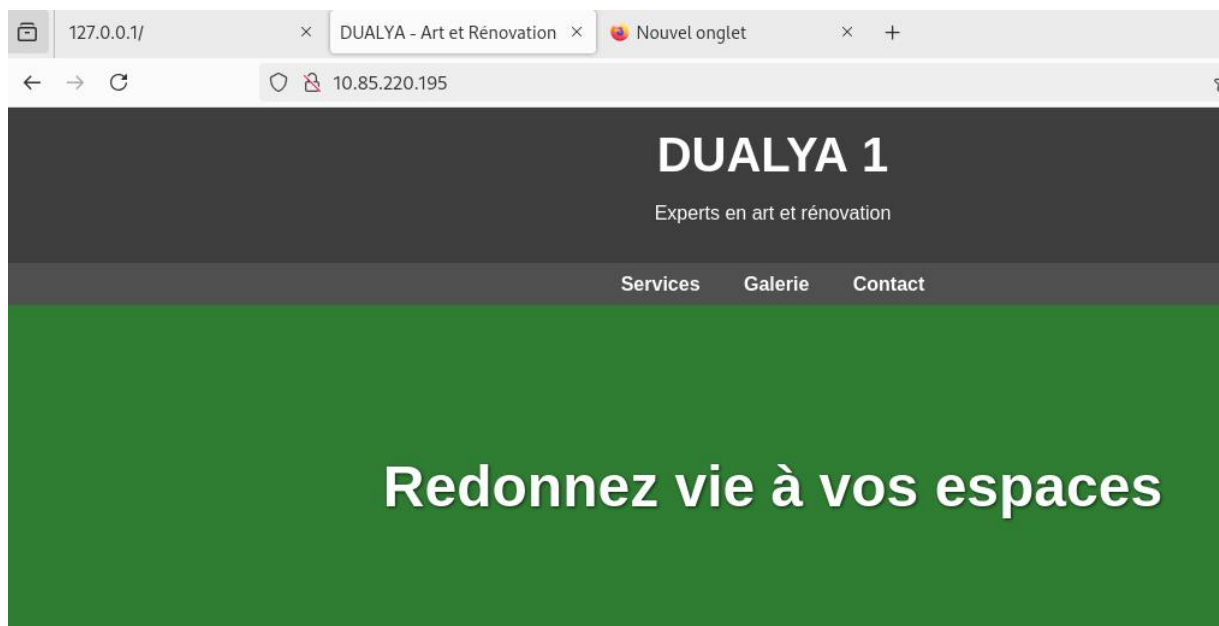
Pour le test, nous allons accéder à la page Web du serveur HAProxy à l'adresse « <http://10.85.220.195> » depuis un navigateur.

Nous devons rafraîchir plusieurs fois la page pour observer la répartition des requêtes et voir nos sites basculer de l'un vers l'autre.

VM-SRV-WEB-01 :



VM-SRV-WEB-02:



On voit que les requêtes sont équilibrées entre les deux serveurs web, car à chaque fois que l'on rafraîchit la page, l'autre serveur web apparaît.

Configuration de la page de statistique de HAProxy :

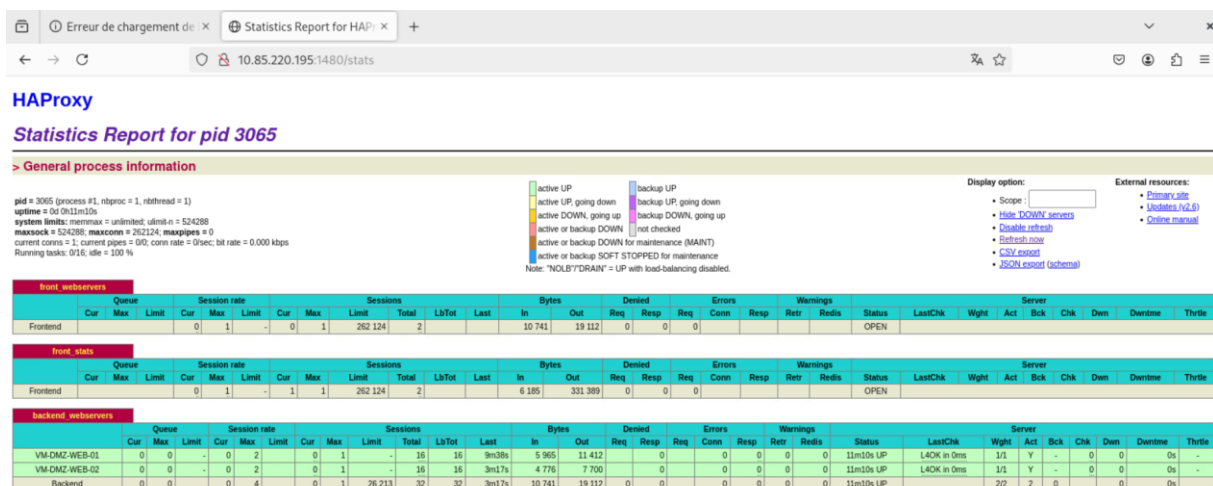
La page de statistiques HAProxy est un outil de monitoring web très pratique, accessible via un navigateur. Elle permet de voir en temps réel l'état d'une infrastructure de répartition de charge et d'agir rapidement en cas de souci, notamment pour basculer ou isoler un serveur.

Pour configurer la page de statistiques de HAProxy, nous sommes retournés dans le fichier « haproxy.cfg », puis nous avons ajouté la configuration de la page de statistiques.

```
frontend front_stats
    bind *:1480
    stats enable
    stats uri /stats
    stats hide-version
    stats refresh 10s
    stats realm Haproxy\ Statistics
    stats auth haproxy:p@ssword!
```

Cette configuration permet de mettre en place une page web sécurisée pour suivre en temps réel l'activité de HAProxy, accessible via « <http://IP:1480/stats> », avec une authentification et un rafraîchissement automatique.

Après avoir configuré la page de statistiques de HAProxy, je suis allé(e) sur un navigateur web puis j'ai inséré « <http://10.85.220.195:1480/stats> ».



Difficultés rencontrées :

Utilisation Linux :

Nous avons rencontré des difficultés lors de la mise en place des serveurs web et du serveur HAProxy, car nous ne connaissions pas l'environnement Linux.

La découverte de cet environnement nous a confrontés à des défis techniques liés à la maîtrise du terminal, à la configuration manuelle des services et à la gestion des droits, nécessitant un temps d'adaptation important.

Améliorations possibles :

Pour l'entreprise Dualya, compte tenu de sa taille et de sa croissance, le groupe HAssistance propose les améliorations suivantes :

Sécurisation :

La mise en place de la sécurité des serveurs web et du serveur HAProxy est indispensable. En effet, compte tenu de l'évolution de l'entreprise Dualya, il sera nécessaire de renforcer la protection des serveurs Linux, notamment en déployant Fail2ban afin de limiter le nombre de connexions SSH et web, ou encore en mettant en place le protocole HTTPS pour sécuriser les échanges.

Conclusion :

Pour conclure, ce dossier nous a permis d'explorer les différentes étapes nécessaires à la mise en place de la redondance des serveurs web et de la répartition de charge grâce à HAProxy.

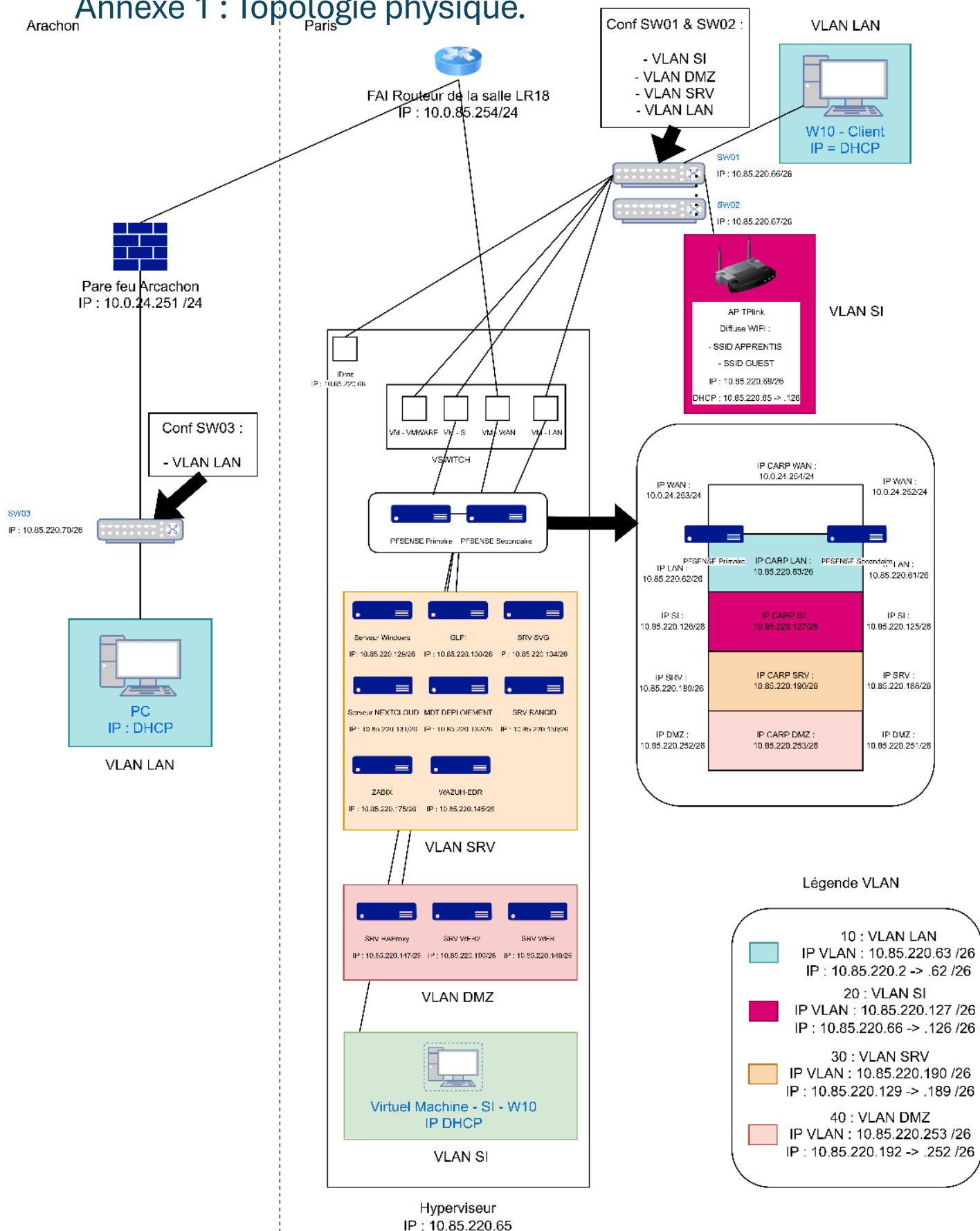
Bien que ponctuée de difficultés, cette démarche nous a permis de les surmonter avec succès tout en élargissant notre compréhension des infrastructures informatiques.

Grâce à cette expérience, nous sommes désormais en mesure de proposer des améliorations pertinentes et adaptées aux besoins de l'entreprise Dualya.

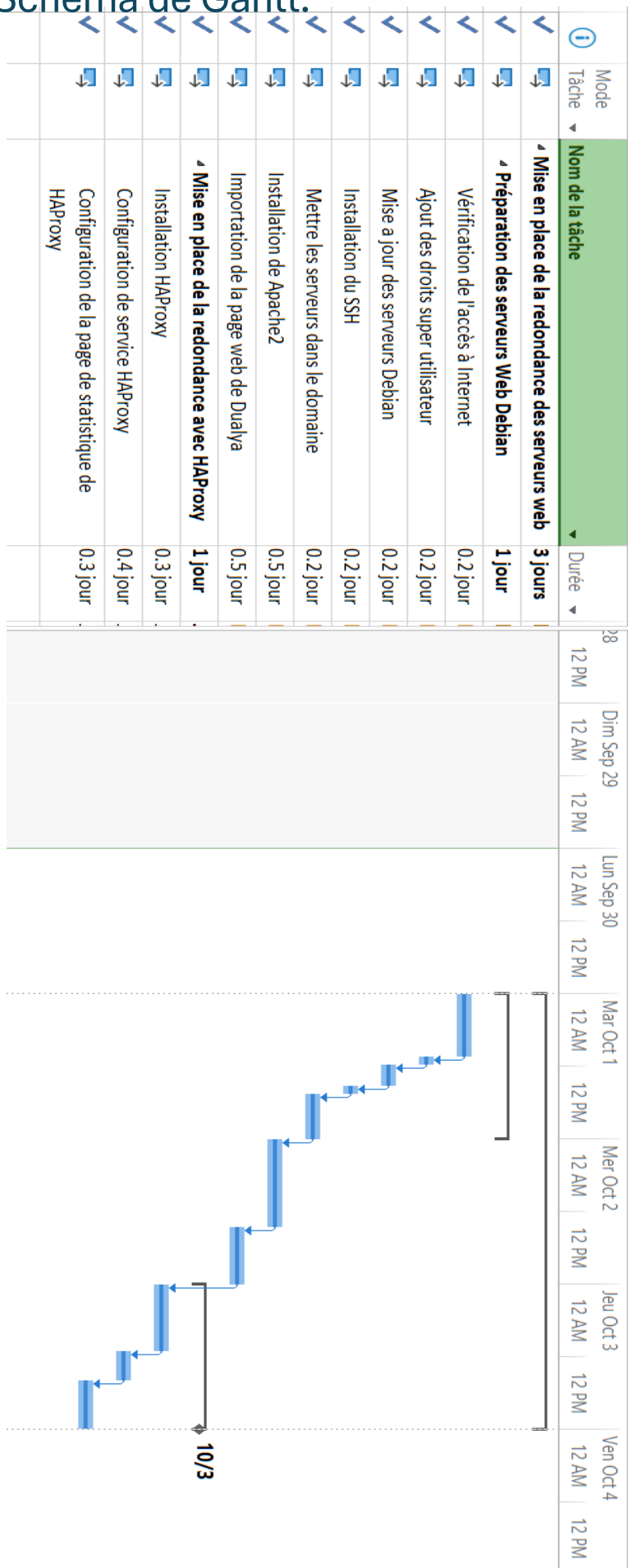
Vous pouvez retrouver ce dossier dans mon portefeuille via l'adresse suivante :

<https://nicolas.hachet.formaton-esiac.fr>

Annexe 1 : Topologie physique.



Annexe 2 : Schéma de Gantt.



Annexe 3 : Gestionnaire de mot de passe.

Vous retrouverez ci-dessous le tableau de tous les mots de passe disponible sur l'infrastructure :

Ordinateurs :

Nom de l'appareil	Nom d'utilisateur	Mot de passe
VM-W10-01 (virtuelle)	admin	Du@ly@85-HA-W10
PC1 (PC portable)	admin	Du@ly@85-HA-PC1
PC2 (PC portable)	admin	Du@ly@85-HA-PC2

Serveurs :

Nom de l'appareil	Nom d'utilisateur	Mot de passe
HYPERVERSEUR	root	Du@ly@85-HA-ESXI
IDRAC	root	Du@ly@85-HA-IDRAC
VM-SRV-WINDOWS-SERVER-01	administrateur	Du@ly@85-HA-WS
VM-SRV-GLPI-01	tech	Du@ly@85-HA-GLPI
VM-SRV-DEP-01	administrateur	Du@ly@85-HA-DEP
VM-SRV-SVG-01	administrateur	Du@ly@85-HA-SVG
VM-SRV-RANCID-01	administrateur	Du@ly@85-HA-RANCID
VM-DMZ-WEB-01	tech	Du@ly@85-HA-WEB1
VM-DMZ-WEB-02	tech	Du@ly@85-HA-WEB2
VM-SRV-HAPROXY-01	tech	Du@ly@85-HA-HAPROXY
VM-SRV-ZABBIX-01	tech	Du@ly@85-HA-ZABBIX
VM-SRV-NEXTCLOUD-01	tech	Du@ly@85-HA-NEXTCLOUD
VM-SRV-EDR-01	tech	Du@ly@85-HA-EDR

Toutes les machines virtuelles linux disponible dans la liste ci-dessus dispose un utilisateur root pour faire toutes les manipulations administrateur.

Nom d'utilisateur	Mot de passe
root	Du@ly@85-HA-R00T

Réseaux :

Nom de l'appareil	Nom d'utilisateur	Mot de passe
SWITCH 1	admin	Du@ly@85-HA-SW1
SWITCH 2	admin	Du@ly@85-HA-SW2
SWITCH 3	admin	Du@ly@85-HA-SW3
VM-FW-01 (PFSENSE PRINCIPAL)	admin	Du@ly@85-HA-FW01
VM-FW-02 (PFSENSE SECONDAIRE)	admin	Du@ly@85-HA-FW02
FORTINET (Site ARCACHON)	admin	Du@ly@85-HA-FORTINET
BORNE WIFI TP-LINK		Du@ly@85-HA-TPLINK
Partage de fichier (SMB)	hassistance	P@ssw0rd

Utilisateurs du domaine AD :

Nom d'utilisateur	Mot de passe
philippe.pastel	Du@1y@85-pp!
pierre.parry	Du@1y@85-pp
ulyse.alain	Du@1y@85-ua!
baptiste.ludwig	Du@1y@85-bl!
jade.caillaux	Du@1y@85-jc!
sophie.ratier	Du@1y@85-sr!
remy.loiseau	Du@1y@85-rl!
pierre.sabord	Du@1y@85-ps!
sacha.lens	Du@1y@85-sl!
jeanne.reil	Du@1y@85-jr
serge.lay	Du@1y@85-sl!
sybille.gautier	Du@1y@85-sg!
helene.varon	Du@1y@85-hv!
pauline.provost	Du@1y@85-pp!
cecilia.claire	Du@1y@85-cc!
yann.bertrand	Du@1y@85-yb!

Interface des sites web :

Nom du service	Nom d'utilisateur	Mot de passe
GLPI	glpi	Du@ly@85-HA-GLPI
NEXTCLOUD	administrateur	Du@ly@85-SUIVANTNUAGE
WAZUH	admin	Du@ly@85-HA-WAZUH