

Rapport final réseau d'entreprise

Rapport final réseau d'entreprise	1
Lien importants	1
Introduction	1
Cahier de charge	2
Environnement et méthodes de développement	12
Distribution des rôles	14
Rétrospections	14
Problèmes rencontrés et perte de temps	14
Fonctionnement général du groupe	14
Pistes d'améliorations	16
Conclusion	16
Bibliographie	16

Lien importants

Github : <https://github.com/melvinmajor/AuDD>

Trello : <https://trello.com/b/h982pQyl/r%C3%A9seau-dentreprise-audd>

Liste matériel :

https://docs.google.com/spreadsheets/d/1V622M3ScLUdscLeI2NHPm4h_KyVOoyUBM7P6woMcryY/edit?usp=sharing

Introduction

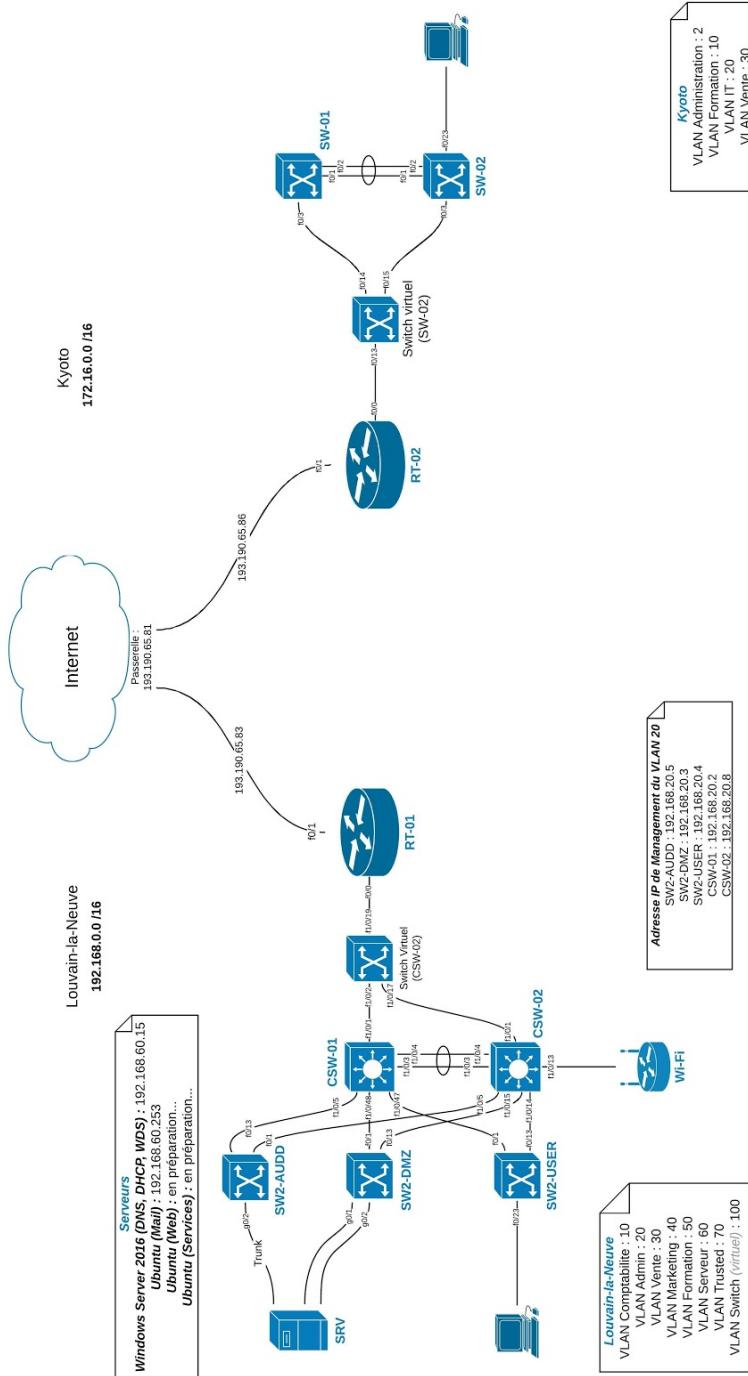
Dans le cadre du cours de réseau d'entreprise en 3TI, nous sommes amenés à réaliser un projet d'une semaine en groupe de 22 étudiants. Le groupe A a choisi comme nom de société: AuDD.

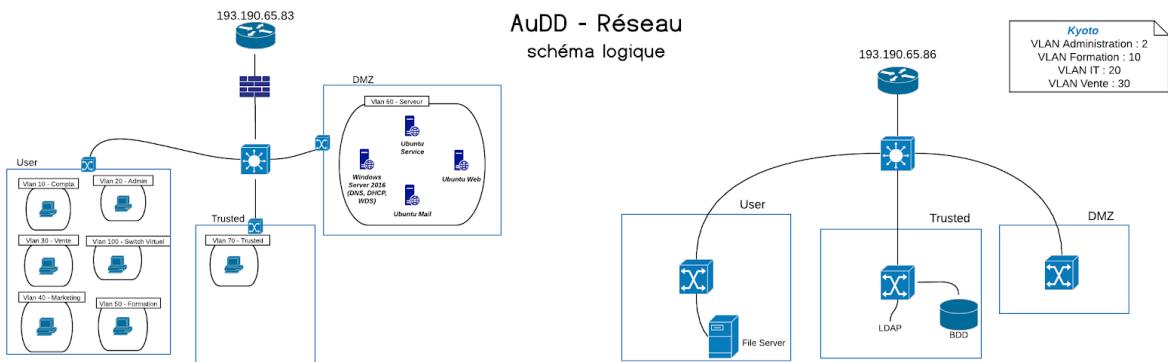
AuDD est une société qui offre des formations en ligne. Dans ce but, AuDD possède un site web. Le site principal se situe en Belgique.. Il nous a fallu penser et concevoir le réseau de notre entreprise, le configurer, le rendre accessible et le protéger. AuDD étant une société de formation en ligne, nous avons également mis en place un site web qui propose les solutions offertes par AuDD.

Aspects techniques

Infrastructure réseau

AuDD - Réseau schéma physique





Au niveau des choix techniques utilisés, nous avons décidé de déployer un réseau en maille (pour l'infrastructure de Louvain-la-Neuve), nous avons aussi implémenté des etherchannel pour la redondance des liens, mais également la création d'un switch L3 virtuel via HSRP. Tous ces choix nous permettent de limiter les "*Points of failure*" au routeur principale **RT-01**.

Afin de pallier au manque d'interface disponible sur les routeurs, nous avons dû créer des "switchs virtuels". Pour l'infrastructure de Louvain-la-Neuve nous avons implémenté VTP, ainsi qu'une connexion SSH pour l'accès aux différents devices, et nous avons utilisé OSPF pour le routage.

Administration réseau

Serveur

Les différents services sont hostes sur le serveur où est installé l'hyperviseur de type bare-metal de chez VMWare, Exsi 6.5. Chaque service tourne sur son propre OS, dans notre cas Ubuntu, pour améliorer la disponibilité des services proposés. Et finalement, pour améliorer la vitesse de déploiement, la modification ou suppression des services on utilise Docker.

DHCP

Configuration :

Scope :

- name : DHCP Compta
- description : DHCP pour le VLAN Comptabilité
- start IP address : 192.168.10.100

- end IP address : 192.168.10.240
- Subnet Mask : 255.255.255.0

- name : DHCP IT
- description : DHCP pour le VLAN IT
- start IP address : 192.168.20.100
- end IP address : 192.168.20.240
- Subnet Mask : 255.255.255.0

- name : DHCP Vente
- description : DHCP pour le VLAN Vente
- start IP address : 192.168.30.100
- end IP address : 192.168.30.240
- Subnet Mask : 255.255.255.0

- name : DHCP Market
- description : DHCP pour le VLAN Marketing
- start IP address : 192.168.40.100
- end IP address : 192.168.40.240
- Subnet Mask : 255.255.255.0

- name : DHCP Formation
- description : DHCP pour le VLAN Formation
- start IP address : 192.168.50.100
- end IP address : 192.168.50.240
- Subnet Mask : 255.255.255.0

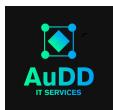
- name : VPN
- description : Pool pour le VPN
- start IP address : 192.168.60.100
- end IP address : 192.168.60.220
- Subnet Mask : 255.255.255.0

Lease Duration : 8 hours

Default gateways :

VLAN 10 : 192.168.10.10
VLAN 20 : 192.168.20.20
VLAN 30 : 192.168.30.30
VLAN 40 : 192.168.40.40
VLAN 50 : 192.168.50.50
VLAN 60 : 192.168.60.60

Paramètres DNS :



06-02-2020

- IP serveur DNS : 192.168.60.242
- nom de domaine DNS : audd.local

Options supplémentaires :

- NTP : serveur public
- PXE : configuration automatique

DNS interne

Configuration :

IP de serveur : 192.168.60.242

Masque de sous-réseau : 255.255.255.0

Passerelle par défaut : 192.168.60.60

DNS préféré : 8.8.8.8

DNS auxiliaire : 8.8.4.4

Zone principale ⇒ nom de domaine : audd.local

Fichier de zone : audd.local.dns

Zone de recherche inverse :

- Adresse IP du réseau : 192.168.0
- Fichier de zone : 0.168.192.in-addr.arpa.dns

DNS externe

Etant donnée que nous avons utilisé le même nom de domaine que nous avons acheté pour le cours de projet d'intégration chez OVH, nous avons modifié le fichier de zone de notre domaine.

Vu que l'adresse publique de notre routeur est 193.190.65.83, nous avons fait deux records A le référençant soient: funndeh.com

<input type="checkbox"/>	Domain	TTL	Type	Target	
<input type="checkbox"/>	funndeh.com.	0	NS	dns19.ovh.net.	
<input type="checkbox"/>	funndeh.com.	0	NS	ns19.ovh.net.	
<input type="checkbox"/>	funndeh.com.	0	MX	10 mail.funndeh.com.	
<input type="checkbox"/>	funndeh.com.	0	A	193.190.65.83	
<input type="checkbox"/>	mail.funndeh.com.	0	A	193.190.65.83	
<input type="checkbox"/>	funndeh.com.	0	TXT	"v=spf1 a mx ip4:193.190.65.83 include:_spf.google.com ~all"	
<input type="checkbox"/>	_dmarc.funndeh.com.	0	TXT	"v=DMARC1; p=none"	
<input type="checkbox"/>	www.funndeh.com.	0	CNAME	funndeh.com.	

Sécurité réseau

Proxy

Connexion ssh au Ubuntu Server : 192.168.60.250

- http_port option 3128 : listen to port 3128.
 - + transparent : prevent Squid from modifying our requests and responses.
- visible_hostname : AUDD.proxy
- acl blocked_websites dstdomain "/etc/squid/blocked.acl"
- http_access deny blocked_websites

Filtrage d'URL permettant de limiter l'accès à certaines catégories de sites :

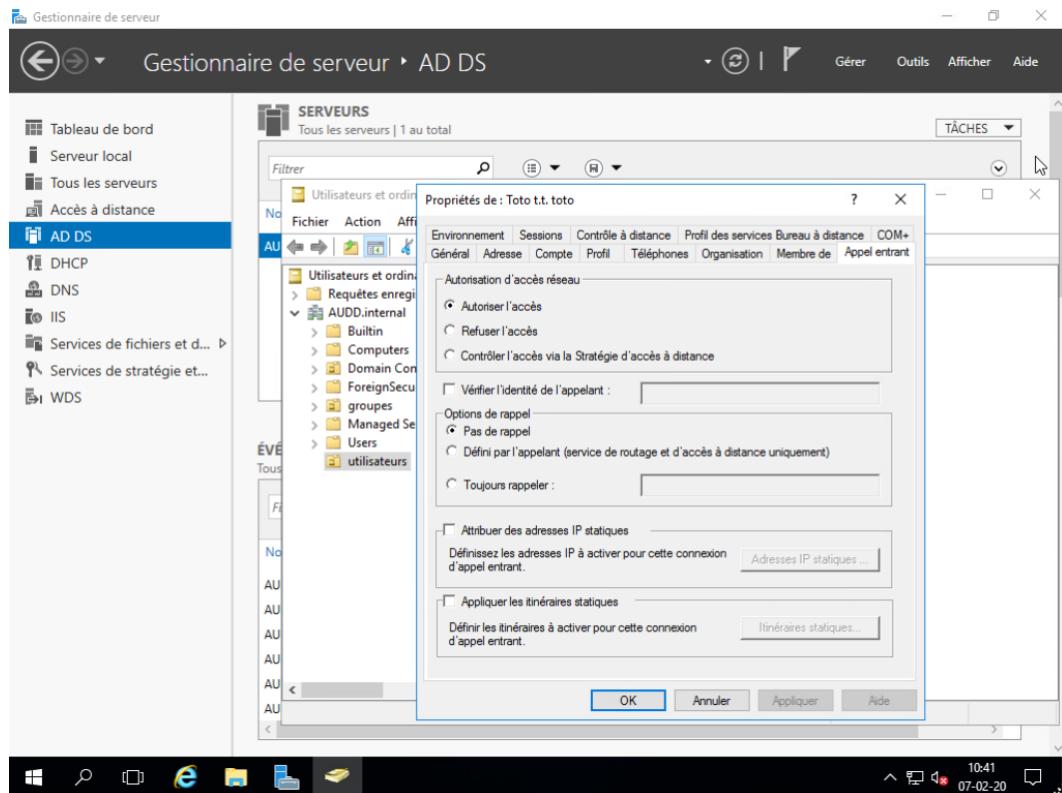
- .twitter.com
 - o Désactivé tout le temps
- .facebook.com
 - o Désactivé tout le temps
- .instagram.com
 - o Accessible du lundi au vendredi de 12h à 14h.

VPN

Nous avons configuré un serveur d'accès à distance sur le windows server 2016.

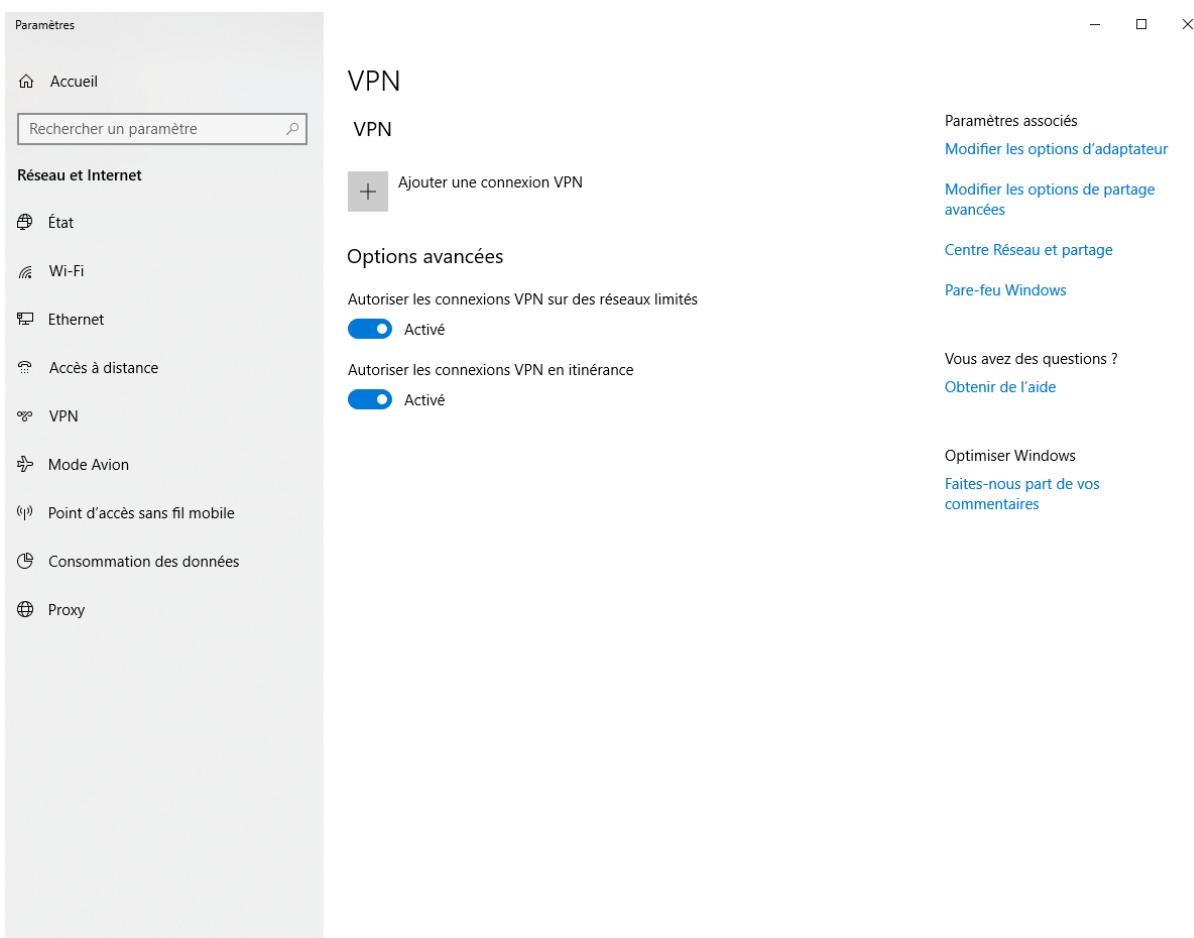
Nous avons attribué les adresses IP aux utilisateurs distants sur base de notre serveur DHCP.

Nous avons ensuite autorisé l'accès au serveur pour les utilisateurs en autorisant l'accès à distance dans l'Active Directory :



Il est dès lors possible d'accéder au réseau local depuis un réseau externe tel que EDUROAM.

Comment se connecter au VPN ?



Ajouter une connexion VPN

Ajouter une connexion VPN

Fournisseur VPN

Nom de la connexion

Nom ou adresse du serveur

Type de réseau privé virtuel

Type d'informations de connexion

Nom d'utilisateur (facultatif)

Mot de passe (facultatif)

Mémoriser mes informations de connexion

Complétez le nom de la connexion avec le nom que vous souhaitez et pour l'adresse du serveur, indiquez l'ip 193.190.65.83. Finalement, indiquez votre nom d'utilisateur et votre mot de passe. (Exemple : nom d'utilisateur : toto ; mot de passe : Ephec_audd)

Paramètres

Accueil

Rechercher un paramètre

Réseau et Internet

État

Wi-Fi

Ethernet

Accès à distance

VPN

Mode Avion

Point d'accès sans fil mobile

Consommation des données

Proxy

VPN

Ajouter une connexion VPN

AUDD

Se connecter Options avancées Supprimer

Options avancées

Autoriser les connexions VPN sur des réseaux limités
 Activé

Autoriser les connexions VPN en itinérance
 Activé

Paramètres associés

Modifier les options d'adaptateur

Modifier les options de partage avancées

Centre Réseau et partage

Pare-feu Windows

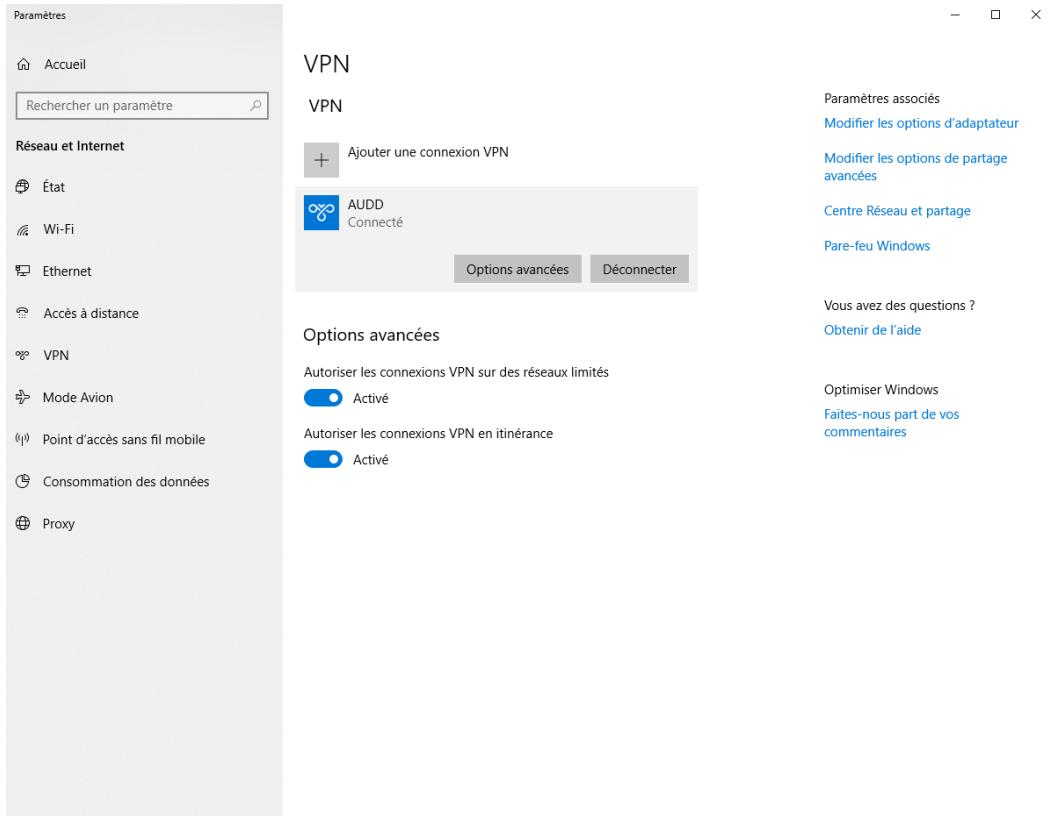
Vous avez des questions ?

Obtenir de l'aide

Optimiser Windows

Faites-nous part de vos commentaires

Ensuite, il suffit de "se connecter"



Pare-feu (FW)

L'objectif était de mettre en place un pare-feu via pfsense.
Il n'est pas finalisé.

Installation du WiFi

La mise en place du Wifi s'est faite via son interface de configuration, nous avons pu y accéder en nous connectant au wifi (par ethernet ou sans fil) et en entrant son adresse ip (par défaut 192.168.1.1) dans notre browser. Nous avons donc pu relier le routeur à notre infrastructure et lui attribuer son adresse ip, nom, et mot de passe. Au niveau, de la sécurité nous n'avions qu'un simple mot de passe c'est pourquoi nous avons décidé d'opter pour une meilleure sécurité en mettant en place une connexion par authentification (c'est à dire que chaque utilisateur dispose d'un identifiant et il se connecte au Wifi via celui-ci). Pour cela, il a fallu créer un serveur radius (disponible en bibliographie).

Service Mail

Notre service mail est constitué d'un serveur SMTP, IMAP ainsi que POP3. Vu que nous ne possédions pas une license Office 365 entreprise pour mettre en place un service mail à jour avec l'Active Directory, nous nous sommes contentés d'un système fonctionnant avec des outils tels que Postfix, Dovecot, Spamassassin, spf, Dmarc et Opendkim (*qui n'est pas totalement terminé*).

Pour la partie virtualisation, ce service est sur docker pour des questions de facilité de reconstitution en cas de défaillance informatique, utilise moins de ressources et permet de déployer rapidement ces applications.

Côté SMTP, nous avons un serveur tournant sur Postfix. En plus de permettre l'envoi des mails, il constitue également le service de relais SMTP.

Notre serveur IMAP (993) et POP3 (995) fonctionne sur Dovecot. La configuration autorise uniquement la réception des mails sur SSL.

Un système d'authentification a été mis en place pour récupérer les données existantes dans notre base de données. Lors de la création d'un nouvel utilisateur au sein de l'entreprise, l'administrateur système insère des données telles que nom d'utilisateur et mot de passe.

En ce qui concerne l'accessibilité du mail, nous arrivons à envoyer et recevoir les mails en interne. Par contre en externe, nous recevons bien les mails provenant de l'extérieur mais nous n'arrivons pas à les envoyer.

Installation de WDS et DFS

Concernant ces deux services propre à Windows Server, le premier est installé, configuré et prêt à l'emploi. Nous l'avons testé et il fonctionne comme attendu. Le second est installé et en cours de configuration, il sera prêt d'ici la présentation.

Windows Deployment Service (WDS) a été configuré comme détectable par n'importe quelle machine connectée sur le réseau mais une autorisation administrateur est nécessaire afin de réaliser l'installation de la machine.

Nous avons sélectionné 4 versions de Windows 10 pour les installations possibles, toutes dépendantes de la dernière version disponible à l'heure actuelle (1909) : Windows 10 Pro, Windows 10 Pro N, Windows 10 Pro for Workstations et Windows

10 Pro N for Workstations.

Nous avons choisi de ne pas proposer Windows 10 Home, Windows 10 Home N, Windows 10 Home Single Language, Windows 10 Education, Windows 10 Education N, Windows 10 Pro Education, Windows 10 Pro Education N étant donné qu'on ne juge pas d'intérêt particulier pour ces versions là dans le cadre de ce projet.

Afin d'accéder à l'installation via WDS, il suffit de démarrer l'ordinateur et d'accéder aux options de démarrage par le biais de la touche **F12** et de choisir ensuite NIC Onboard (si possible, via UEFI et non Legacy BIOS).

Concernant la partie Distributed File System (DFS), le service est installé et nous sommes en train de le configurer afin de proposer un environnement de partage de fichiers centralisé.

Site Web

Nous avons créer un site web qui en premier lieu permet à un utilisateur de se renseigner sur les différents services que propose AuDD qui sont des formations en lignes. Sur le site 3 types de formations sont disponible : Formations en langue, Formations en programmation et formations en réseau. 6 langues sont disponibles, 6 langages de programmation ainsi que 3 formations en réseau. L'utilisateur peut se créer un compte afin de s'inscrire à ces différentes formations. Nous n'avons malheureusement pas eu le temps ni la motivation de créer des formations car nous trouvions cela moins utiles comparé aux restes du projet.

Environnement et méthodes de développement

Pour assurer un bon fonctionnement au sein du groupe, nous avons mis en place différentes règles internes, acceptées et signées par les différentes personnes du groupe.

- Les horaires sont les suivants : de 8h30 à 17h30 avec une pause de midi entre 13h et 14h.
- Chaque rôle doit ranger le matériel lié à leur travail et le responsable de chacun des rôles se porte garant pour vérifier que tout soit correctement rangé.
- Également, chacun des responsables de rôle se voit attribuer l'écriture d'une courte description de l'état des activités du jour et doit le transmettre au responsable des rapports. Le responsable de rôle est défini en interne par chacun des rôles ayant plusieurs membres attribués.

- À partir de 17h15, une mise en commun des heures de travail est faite et dernière mise à jour sur les plateformes d'échanges mis en place.
- Les réunions au sein de l'équipe se réalisent chaque jour à 8h45.
- La réunion intergroupe se déroule tous les jours à 17h20 (sujet à modification).
- De plus, une courte réunion d'avancement et des problèmes à faire face est prévue après le temps de midi afin de rendre le travail en après-midi plus efficace.

Distribution des rôles

Chef de projet (+ photos) : Melvin
Assistant chef de projet : Clément
TimeSheet : Clément, Ludo
Sécurité physique : Ibrahima
Infrastructure réseau : Nicolas, Filipp, Adrien, Manuelle
Administration réseau : Mathias, Brieuc, Nicky
Sécurité réseau : David, Quentin
Mail : Manuelle, Nicolas, Ibrahima
Service déploiement : Hymed, Nathan
Ressources informatique : Nathan, Manuelle
Site web : Alexandre, Timothy, Clément, Melvin
WiFi (+ aide site web) : Thibaut, Tristan, Ludo, Brian, Melvin
Responsable rangement : Hymed, Jean, Quentin
Rapports : Jean

Rétrospections

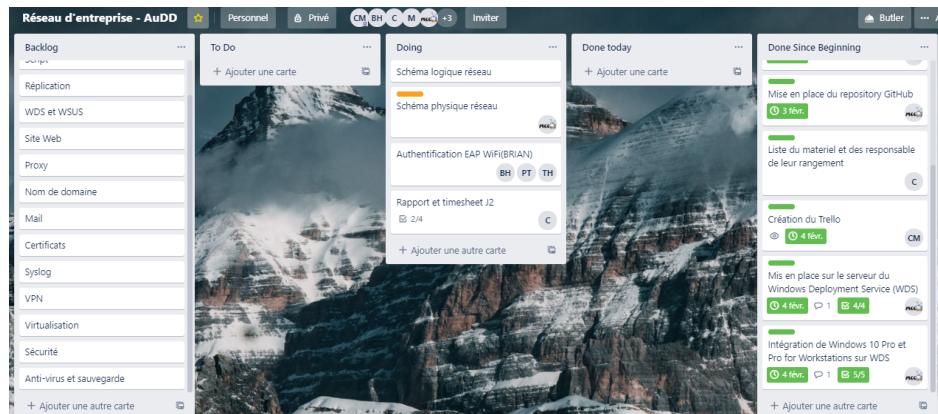
Problèmes rencontrés et perte de temps

- Problème wifi: les pings fonctionnent mais ne se connectent pas au réseau
- Soucis de communication au départ du projet pour les parties virtualisation et déploiement.
- Problème de mémoire vive sur le serveur.
- OS sur le serveur qu'il a fallu écraser.
- Vétusté du serveur ne permettant pas le déploiement de la dernière version d'ESXi proposé sur la plateforme VMware (dernière version 6.7U3, version déployée 6.5).

Fonctionnement général du groupe

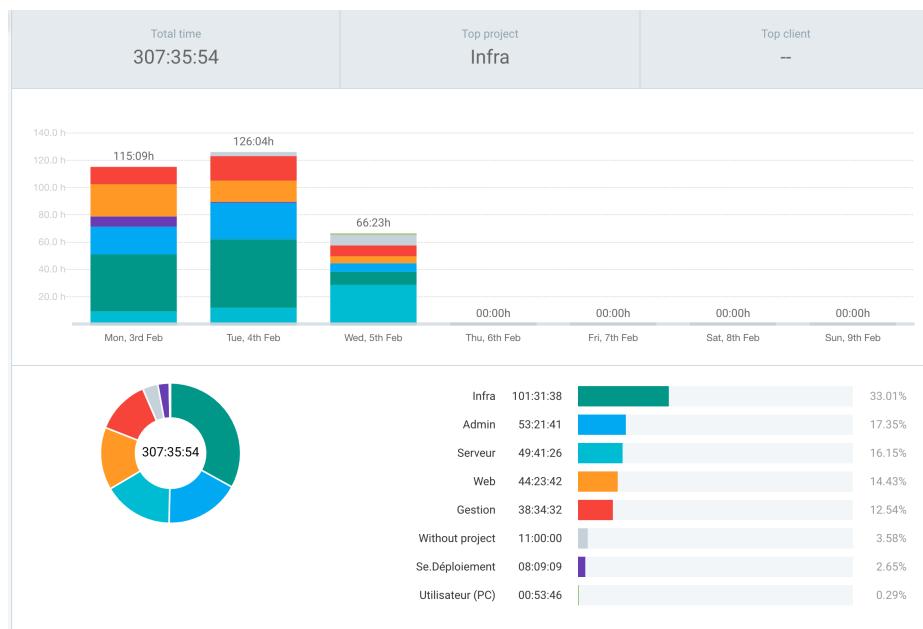
- Outils collaboratifs :

- Création d'un Trello de groupe



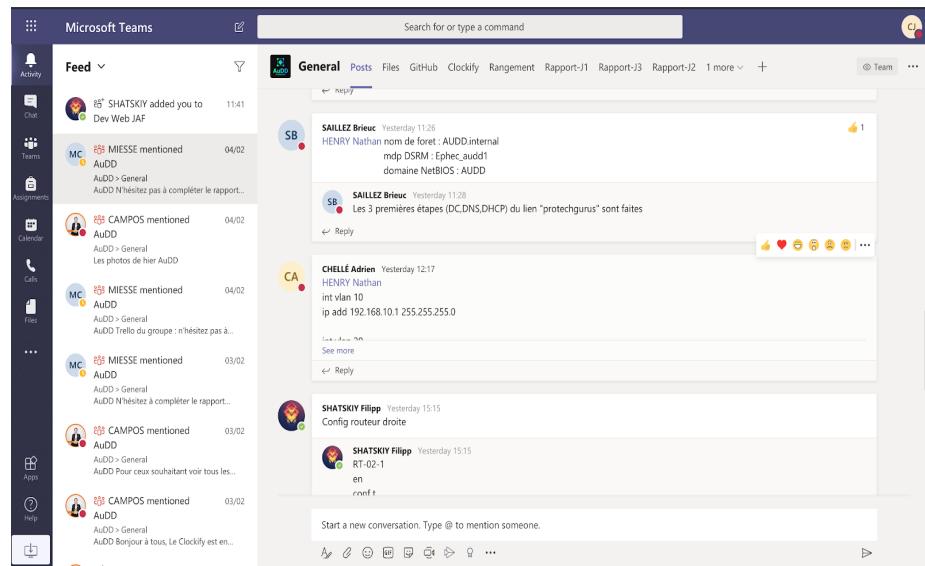
- Clockify :

<https://clockify.me/bookmarks/5e3d33e59fdab913d810eaff>



- Github: <https://github.com/melvinmajor/AuDD>

- Microsoft Teams



Bibliographie

- **WDS :**

 - <https://protechgurus.com/install-configure-wds-windows-server-2016/>
 - <https://www.microsoft.com/en-us/software-download/windows10ISO>
 - <https://www.wintips.org/how-to-extract-install-esd-to-install-wim-windows-10-8/>

- **DFS :**

 - <https://www.it-connect.fr/cest-quoi-le-dfs-windows-server/>
 - <https://www.it-connect.fr/windows-server-2012-r2-installation-du-role-dfs/>
 - <https://www.it-connect.fr/windows-server-2012-r2-configuration-dun-serveur-dfs/>

- **DHCP :**

Windows server 2016 :

- <https://networkcorp.fr/configuration-serveur-dhcp-windows-serveur-2016/>

Comparison between dhcp on server or router :

- https://www.reddit.com/r/sysadmin/comments/1t3on8/dhcp_on_the_router_or_on_a_server_your_opinion/

- **DNS interne :**

Windows server 2016 :

- <https://no-impact.eu/do-it-yourself-post-6-Configuration-DNS-sur-Windows-Server-2016>

Host un site web sur windows server (DNS étape 7)

- <https://www.faqforge.com/windows-server-2012-r2/host-web-site-internet-information-server-manager-windows-server-2012-r2/>

- **DNS externe :**

- **Proxy :**

- <https://www.supinfo.com/articles/single/812-configurer-serveur-proxy-squid>
- <https://phoenixnap.com/kb/setup-install-squid-proxy-server-ubuntu>
- <https://www.gfi.com/support/products/how-to-force-proxy-settings-via-group-policy>
- <https://www.youtube.com/watch?v=EJyB-Hh9DYU>
- <https://openclassrooms.com/fr/courses/1733551-gerez-votre-serveur-linux-et-ses-services/5236086-configurez-un-proxy-cache-avec-squid>

- **VPN :**

Ubuntu server :

- <https://doc.ubuntu-fr.org/openvpn>
- <https://guide.ubuntu-fr.org/server/openvpn.html>

pfsense :

- <https://www.ceos3c.com/pfsense/configure-openvpn-for-pfsense-2-3-step-by-step/>
- <https://www.ceos3c.com/pfsense/pfsense-openvpn-linux-client/>
- <https://openclassrooms.com/fr/courses/1946106-securisez-votre-reseau-grace-aux-vpn-et-firewall/5241681-securisez-votre-infrastructure-grace-a-pfsense>
- <https://www.supinfo.com/articles/single/1165-creation-vpn-windows-server-2012-r2>
- https://www.youtube.com/watch?v=m_wwqspLJSM

- *Serveur Radius :*
- <https://all-it-network.com/radius/?fbclid=IwAR112mF9v88fvsOZ75gGxmANyZGTkrX2r67zFd3Ue46u0hCoZhSy6siYQo>
- *Serveur Mail :*
- <https://github.com/Manste/Projet-Admin>
- <https://hub.docker.com/r/tvial/docker-mailserver/>
- <https://www.digitalocean.com/community/tutorials/how-to-configure-a-mail-server-using-postfix-dovecot-mysql-and-spamassassin>
- <https://www.binarytides.com/linux-mail-with-smtp/>
- https://michaelwiki.geekgalaxy.com/index.php/Check_IMAP_and_POP_with_OpenSSL