

Rapport de projet

Sommaire :

Rapport de projet.....	1
1. Introduction.....	3
1.1 Objectifs du projet.....	3
1.2 Contexte.....	3
1.3 Structure du rapport.....	3
2. Contexte et enjeux du projet.....	3
2.1 Objectifs du projet.....	4
2.2 Implications de l'équipe.....	4
2.2.1 Mission.....	4
2.2.2 Responsabilités.....	4
2.3 Structuration du projet.....	4
3. Description des ressources utilisées.....	6
3.1 Environnement virtuel et réel.....	6
3.1.1 Machines virtuelles.....	6
3.1.2 Équipements réseau matériels.....	6
3.1.3 Pare-feu virtuels.....	6
3.2 Serveurs VMware ESXi et Proxmox VE.....	6
3.2.1 VMware ESXi.....	6
3.2.2 Proxmox VE.....	6
4. Configuration de base des appareils.....	6
4.1 Paramètres généraux.....	7
4.1.1 Nom d'hôte et domaine DNS.....	7
4.1.2 Résolution DNS.....	7
4.1.3 Politique de mot de passe.....	7
4.1.4 Authentification SSHv2.....	7
4.1.5 Temps d'inactivité et temps absolu de session SSH.....	7
5. Configuration de la commutation.....	7
5.1 Configuration des VLAN.....	7
5.1.1 VLAN présents.....	7
5.1.2 Distribution des VLAN via VTPv2.....	7
5.1.3 Configuration des interfaces.....	8
5.2 Protocoles.....	8
5.2.1 Configuration des Liaisons Interurbaines.....	8
5.3 Configuration du spanning tree protocol (STP).....	8
5.3.1 Utilisation de rapid-PVST.....	8

5.3.2 Configuration de la topologie STP.....	8
5.3.3 Désactivation du STP sur les ports hôtes.....	8
6. Configuration de l'adressage IP.....	8
6.1 Structure de l'adressage IP.....	9
6.1.1 Coeur de réseau (10.2.100.0/25).....	9
6.1.2 Connexion au site distant (10.116.2.0/30).....	9
6.1.3 Réseau du siège (10.2.10.0/26).....	9
6.1.4 Autres réseaux.....	9
6.2 Configuration des interfaces.....	10
6.2.1 Interfaces des switchs.....	10
6.2.2 Interfaces des routeurs.....	10
8. Configuration du routage.....	11
8.1 Configuration des paramètres TCP/IP.....	11
8.1.1 Core Switchs.....	11
8.1.2 Edge Routers.....	11
8.1.3 Configuration des interfaces WAN.....	11
8.1.4 Configuration du routage statique.....	12
9. Configuration des routeurs (Edge Routers).....	12
9.1 Redondance des passerelles.....	12
9.2 Configuration des interfaces WAN.....	12
9.3 Configuration du BGP (Border Gateway Protocol).....	13
9.4 Configuration du NAT/PAT.....	13
10. Configuration du routeur WANRTR.....	13
10.1 Utilisation de VRF pour la séparation du trafic.....	13
10.2 Configuration des interfaces WAN.....	13
10.3 Configuration du routage OSPF.....	14
10.4 Configuration de la redondance de la connexion MAN Privé.....	14
10.5 Routage des paquets.....	14
11. Tests et validation.....	14
11.1 Tests de l'infrastructure réseau.....	14
11.2 Tests des services informatiques.....	14
Conclusion.....	15
Annexe.....	16
1. Diagrammes de l'Infrastructure.....	16
2. Adressage IP.....	19
4. Configuration des périphériques réseau.....	20
4.1 ESXI.....	21
4.2 Configuration des routeurs/switchs.....	22
4.3 Configuration des serveurs :.....	28

1. Introduction

1.1 Objectifs du projet

L'objectif principal est de concevoir une infrastructure robuste et performante capable de répondre aux besoins complexes du sujet tout en garantissant la sécurité, la redondance et l'évolutivité du réseau.

L'objectif est non seulement de respecter les spécifications techniques fournies par l'architecte réseau, mais également de dépasser les attentes en intégrant des solutions optimisées et une approche axée sur la fonctionnalité.

1.2 Contexte

Nous sommes chargés de l'organisation globale, ce qui inclut la mise en place d'une infrastructure informatique performante capable de soutenir la coordination des équipes, l'échange de données , et de fournir des services réseau fiables pour l'ensemble des participants.

En conséquence, le projet inclut la configuration détaillée des équipements réseau, des switchs aux routeurs, en passant par les pare-feu virtuels, pour assurer une connectivité fluide et sécurisée.

1.3 Structure du rapport

Ce rapport détaillé est conçu pour documenter de manière exhaustive chaque aspect du projet. Chaque section sera dédiée à une phase spécifique du déploiement, couvrant les détails techniques, les configurations mises en œuvre, les considérations de sécurité, et les résultats des tests.

La section suivante fournira une vue d'ensemble des ressources utilisées, notamment les serveurs virtuels et les équipements matériels réels. Par la suite, chaque composant du réseau fera l'objet d'une configuration détaillée, conformément aux exigences spécifiées.

Le rapport sera agrémenté de captures d'écran, de diagrammes de topologie, et de scripts de configuration utilisés pour assurer une compréhension approfondie du processus de déploiement. Enfin, la section des tests détaillera la méthodologie utilisée, les résultats obtenus, et les actions correctives le cas échéant.

Ce projet représente une opportunité de démontrer l'expertise technique de l'équipe et de contribuer au succès d'un événement majeur. À travers ce rapport, nous visons à fournir une documentation complète et transparente pour permettre une évaluation approfondie du travail accompli.

2. Contexte et enjeux du projet

2.1 Objectifs du projet

- Coordonner les équipes de manière efficace.
- Assurer une connectivité fiable pour les participants.
- Mettre en œuvre des services réseau nécessaires.

2.2 Implications de l'équipe

2.2.1 Mission

La mission consiste à jouer un rôle clé dans la construction et le déploiement de l'infrastructure réseau. Cela inclut la configuration des switchs, des routeurs, et des pare-feu virtuels, ainsi que la gestion des aspects de sécurité, de connectivité et de performances.

2.2.2 Responsabilités

L'équipe, composée de sept membres, dont Léo Ecotiere, Lucas Deuscher, Adam Himmi, Ismael Boudebza, Hugo Loureiro, Simar Dogan, et Mateo Hirsh, sera responsable de la mise en œuvre des technologies réseau, de la configuration des paramètres requis, et de la réalisation des tests pour garantir le bon fonctionnement de l'ensemble.

2.3 Structuration du projet

Le projet se divise en plusieurs phases, allant de la configuration de base des appareils à la mise en place du routage et des tests. Chaque phase est conçue pour répondre aux exigences spécifiques du déploiement de l'infrastructure réseau, avec un accent particulier sur la fonctionnalité et la sécurité.

La section suivante détaillera les ressources utilisées dans le projet, notamment les serveurs virtuels et les équipements matériels, fournissant une base solide pour la construction de l'infrastructure.

Organisation et étapes de réalisation :

L'approche agile a été au cœur de notre organisation. Trello a été notre tableau de bord principal, offrant une vue claire de toutes les tâches à accomplir et de leur progression. Le diagramme de Gantt a, quant à lui, permis de visualiser l'échéancier du projet.

Les étapes de réalisation ont été définies conformément aux bonnes pratiques pour un projet d'infrastructure réseau. Nous avons débuté par la configuration du serveur DNS, élément central de notre architecture. Cependant, les jalons imposés ont parfois entravé notre progression, nous obligeant à des retours fréquents et parfois coûteux en termes de temps sur des configurations déjà effectuées.

Aspects Humains :

Le processus jalonné a suscité des frustrations au sein de l'équipe. L'imposition de jalons quotidiens a restreint notre liberté organisationnelle, générant parfois des allers-retours inutiles. Un équilibre entre structure et flexibilité aurait pu être plus bénéfique.

La taille de l'équipe a également présenté des défis. Si la collaboration à deux a été efficace sur des tâches complexes, elle a parfois entraîné des temps morts lorsque seul un utilisateur pouvait être actif sur une machine. Une évaluation continue de la taille de l'équipe aurait pu optimiser l'efficacité.

Bilan Technique :

Les limitations matérielles ont constitué une entrave significative. Des espaces disques restreints ont eu un impact direct sur la performance des machines et serveurs, générant des temps de latence importants. Les interruptions soudaines, en particulier sur le serveur DNS, ont entraîné des pertes de données, soulignant la nécessité d'une infrastructure plus robuste.

Les problèmes techniques liés à l'ordre d'installation des services ont été un défi supplémentaire. Les erreurs rencontrées sur le serveur RDS, en particulier liées à l'interaction avec le serveur Web, ont créé des obstacles inattendus. Une meilleure planification aurait pu éviter ces complications.

Axes d'Amélioration :

1. **Flexibilité du Jalonnement** : Une révision du processus jalonné pour offrir plus de flexibilité aurait pu prévenir les allers-retours coûteux et stimuler la créativité de l'équipe.
2. **Optimisation de la taille de l'équipe** : Une évaluation continue de la taille de l'équipe aurait permis de maximiser l'efficacité opérationnelle, évitant les temps morts.
3. **Infrastructure matérielle** : Investir dans une infrastructure matérielle plus performante aurait pu atténuer les problèmes liés aux espaces disques restreints et aux arrêts soudains des serveurs.

En dépit des défis humains et techniques, notre équipe a démontré une bonne résilience. Les enseignements tirés de ce projet doivent orienter les futurs projets vers une amélioration continue. Une réflexion sur l'organisation et les ressources nécessaires à de tels projets est cruciale pour garantir le succès.

3. Description des ressources utilisées

3.1 Environnement virtuel et réel

3.1.1 Machines virtuelles

Le projet repose sur l'utilisation de machines virtuelles (VM) hébergées sur plusieurs serveurs VMware ESXi et Proxmox VE. Ces plateformes offrent la flexibilité nécessaire pour déployer et gérer les machines virtuelles de manière efficace. Chaque membre de l'équipe aura un accès dédié pour configurer et maintenir les VM en fonction des besoins spécifiques du projet.

3.1.2 Équipements réseau matériels

Outre les machines virtuelles, l'infrastructure comprend des équipements réseau matériels réels. Ces composants physiques, tels que switches et routeurs, joueront un rôle central dans la création d'un réseau fiable et performant. L'utilisation d'équipements matériels garantit une stabilité accrue et une gestion plus précise des flux de données.

3.1.3 Pare-feu virtuels

Deux pare-feu virtuels, REMFW (VM Cisco) et HQFWSRV (VM Linux), seront utilisés pour sécuriser les connexions et réguler le trafic réseau. Ces pare-feu joueront un rôle crucial dans la connectivité entre WorldSkills France (WSFR) et l'infrastructure de WSL2024, ainsi que dans la protection des services internes contre les menaces potentielles.

3.2 Serveurs VMware ESXi et Proxmox VE

3.2.1 VMware ESXi

VMware ESXi est une plateforme de virtualisation leader, offrant une gestion avancée des machines virtuelles. Les membres de l'équipe auront accès à ESXi pour configurer les groupes de ports nécessaires à la connectivité des machines virtuelles et des périphériques réseau.

3.2.2 Proxmox VE

Proxmox VE est une plateforme de virtualisation open source, offrant des fonctionnalités similaires à VMware ESXi. Les serveurs Proxmox VE seront utilisés pour héberger des machines virtuelles et assurer une flexibilité supplémentaire dans la gestion des ressources virtuelles.

4. Configuration de base des appareils

La configuration de base des appareils est essentielle pour établir un fondement solide avant d'implémenter des fonctionnalités plus avancées du réseau. Cette section détaillera chaque étape, depuis la configuration des paramètres généraux jusqu'à la mise en place de l'accès sécurisé via SSH.

4.1 Paramètres généraux

4.1.1 Nom d'hôte et domaine DNS

Chaque appareil du réseau doit être configuré avec un nom d'hôte conforme aux spécifications du diagramme. Le domaine DNS "wsl2024.org" sera utilisé pour garantir une résolution précise des noms.

4.1.2 Résolution DNS

La résolution DNS sera désactivée pour éviter des retards potentiels. Cette configuration garantit une gestion efficace des requêtes DNS locales.

4.1.3 Politique de mot de passe

Les mots de passe seront sécurisés et standardisés pour simplifier la gestion. Les détails d'authentification seront configurés avec un mot de passe commun "P@ssw0rd".

4.1.4 Authentification SSHv2

L'accès à distance sera configuré uniquement via SSHv2 avec une clé RSA de 2048 bits. Cela garantit une connexion sécurisée.

4.1.5 Temps d'inactivité et temps absolu de session SSH

Pour renforcer la sécurité, la session SSH sera automatiquement fermée après cinq minutes d'inactivité et vingt minutes au total.

5. Configuration de la commutation

La configuration des switchs est une étape essentielle pour établir des connexions réseau fluides et sécurisées. Cette section détaillera la configuration des VLAN, des protocoles de tronc, et du Spanning Tree Protocol (STP) sur l'infrastructure commutée (CORESWX et ACCSWX).

5.1 Configuration des VLAN

5.1.1 VLAN présents

Les switchs CORESWX et ACCSWX doivent être configurés pour prendre en charge plusieurs VLAN, chacun servant à une fonction spécifique. Les VLAN identifiés incluent les serveurs, les clients, la zone démilitarisée (DMZ), le réseau de gestion, et d'autres VLAN nécessaires à l'infrastructure.

5.1.2 Distribution des VLAN via VTPv2

La distribution des VLAN sera gérée par le protocole VTPv2. CORESW1 et CORESW2 seront configurés en tant que serveurs VTP, tandis qu'ACCSW1 et ACCSW2 seront configurés en tant que clients VTP.

5.1.3 Configuration des interfaces

Les interfaces des switchs nécessitent des configurations spécifiques pour faciliter la connectivité entre eux et avec les hôtes. Ces configurations incluent les paramètres nécessaires pour les différentes liaisons, les modes d'encapsulation, et la sélection des VLAN autorisés.

5.2 Protocoles

5.2.1 Configuration des Liaisons Interurbaines

Les liaisons interurbaines entre les switchs nécessitent des configurations spécifiques pour garantir une communication fluide. Seul le VLAN nécessaire à l'infrastructure doit être autorisé sur chaque liaison interurbaine, et la négociation automatique doit être désactivée.

5.3 Configuration du spanning tree protocol (STP)

5.3.1 Utilisation de rapid-PVST

Le Rapid Spanning Tree Protocol (RSTP) sera configuré pour assurer une convergence rapide en cas de changement de topologie, optimisant ainsi les performances du réseau.

5.3.2 Configuration de la topologie STP

La topologie STP sera configurée pour être basée en premier lieu sur CORESW1 et en second lieu sur CORESW2, garantissant une stabilité et une redondance efficaces.

5.3.3 Désactivation du STP sur les ports hôtes

Les ports hôtes ne nécessitant pas la participation au STP, ils seront configurés en mode PortFast pour éviter tout délai potentiel lors de la connexion d'hôtes.

La prochaine section abordera la configuration de l'adressage IP pour les différents réseaux, optimisant ainsi l'utilisation de l'espace d'adressage disponible.

6. Configuration de l'adressage IP

La configuration de l'adressage IP est une étape cruciale pour établir une communication efficace entre les différents composants du réseau. La mise en place de l'adressage IP suit un plan détaillé, prenant en compte les besoins spécifiques de chaque sous-réseau. Les adresses IP ont été attribuées aux différentes machines et interfaces conformément au schéma suivant.

6.1 Structure de l'adressage IP

6.1.1 Coeur de réseau (10.2.100.0/25)

- REMCLT DHCP
 - Adresse IP : DHCP (Dynamique)
- REMPROXSRV
 - Adresse IP : 10.2.100.1
- REMINFRASRV
 - Adresse IP : 10.2.100.2
- REMDCSRV
 - Adresse IP : 10.2.100.3
- REMFW
 - Adresse IP : 10.2.100.126

6.1.2 Connexion au site distant (10.116.2.0/30)

- REMFW
 - Adresse IP : 10.116.2.1
- WANRTR
 - Adresse IP : 10.116.2.2

6.1.3 Réseau du siège (10.2.10.0/26)

- HQDCSRV
 - Adresse IP : 10.2.10.1
- HQINFRASRV
 - Adresse IP : 10.2.10.2
- HQMAILSRV
 - Adresse IP : 10.2.10.3
- HQWEBSRV
 - Adresse IP : 10.2.10.4
- VIP CORESW
 - Adresse IP : 10.2.10.60
- HQFWSRV
 - Adresse IP : 10.2.10.59
- CORESW1
 - Adresse IP : 10.2.10.61
- CORESW2
 - Adresse IP : 10.2.10.62

6.1.4 Autres réseaux

- Réseau VLAN 100 (10.2.254.0/30)
 - CORESW1
 - Adresse IP : 10.2.254.9
 - EDGE1
 - Adresse IP : 10.2.254.10
- Réseau VLAN 200 (10.2.254.4/30)
 - CORESW2
 - Adresse IP : 10.2.254.21
 - EDGE2
 - Adresse IP : 10.2.254.22
- Réseau VLAN 30 (10.2.254.8/30)

- HQFWSRV
 - Adresse IP : 10.2.30.2
- HQWEBSRV
 - Adresse IP : 10.2.30.1
- client test
 - Adresse IP : 10.2.30.10
- Réseau DMZ (8.8.2.0/28)
 - INETSRV1
 - Adresse IP : 8.8.2.1
 - INETSRV2
 - Adresse IP : 8.8.2.2
 - DNSSRV
 - Adresse IP : 8.8.2.3
 - VPNCLT
 - Adresse IP : 8.8.2.4
 - INETCLT
 - Adresse IP : 8.8.2.5
 - WANRTR
 - Adresse IP : 8.8.2.6

6.2 Configuration des interfaces

6.2.1 Interfaces des switches

Les interfaces des switches seront configurées conformément à la structure d'adressage IP définie pour chaque VLAN. Les adresses IP seront attribuées aux interfaces SVI pour permettre la communication entre les VLAN.

6.2.2 Interfaces des routeurs

Les interfaces des routeurs seront configurées pour les différents réseaux, permettant ainsi le routage entre les sous-réseaux. Des routes statiques seront également configurées pour garantir une connectivité efficace.

La prochaine section abordera la configuration des paramètres TCP/IP sur tous les appareils du réseau.

8. Configuration du routage

La configuration du routage joue un rôle essentiel dans l'acheminement efficace du trafic entre les différents réseaux au sein de l'infrastructure. Cette section détaille les étapes spécifiques de configuration du routage, en tenant compte du plan d'adressage IP défini.

8.1 Configuration des paramètres TCP/IP

8.1.1 Core Switchs

Les switchs centraux (CORESW1 et CORESW2) assureront la redondance de la passerelle pour les réseaux 10.2.10.0, 10.2.20.0 et 10.2.99.0. La configuration VRRP sera adaptée au plan d'adressage IP suivant :

- VRRP (Virtual Router Redundancy Protocol) : Les adresses IP seront configurées conformément au plan d'adressage pour assurer la redondance des passerelles.
- Priorité : La priorité sera fixée à 110 pour CORESW1 et 100 pour CORESW2.
- Défaillance et Acheminement : En cas de défaillance de CORESW1, CORESW2 prendra en charge l'acheminement du trafic, basé sur la vérification de l'accessibilité IP de l'interface de liaison montante du routeur EDGE concerné.
- Reprise après Défaillance : Si CORESW1 revient en vie, il reprendra la gestion du trafic.

8.1.2 Edge Routers

Les routeurs (EDGE1 et EDGE2) assurent la redondance des passerelles pour le réseau 217.2.160.0. La configuration VRRP sera adaptée au plan d'adressage IP suivant :

- VRRP : Les adresses IP VIP seront configurées conformément au plan d'adressage pour garantir la redondance des passerelles.
- Priorité : EDGE1 aura une priorité de 110, tandis que EDGE2 aura une priorité de 100.
- Défaillance et acheminement : En cas de défaillance d'EDGE1, EDGE2 prendra en charge l'acheminement du trafic, basé sur la vérification de l'accessibilité IP de l'interface de liaison montante du routeur CORESW concerné.
- Reprise après Défaillance : Si EDGE1 revient en vie, il reprendra la gestion du trafic.

8.1.3 Configuration des interfaces WAN

Les interfaces WAN des routeurs EDGE seront configurées conformément au plan d'adressage IP suivant :

- Connexions WAN : Deux sous-interfaces logiques seront créées pour établir logiquement deux connexions WAN différentes (Internet et MAN privé) en utilisant une seule interface physique.
- Encapsulation : Le trafic sera encapsulé conformément au plan d'adressage spécifié pour chaque sous-interface logique.

8.1.4 Configuration du routage statique

Des routes statiques seront configurées sur les routeurs EDGE en tenant compte du plan d'adressage pour garantir une connectivité efficace avec les réseaux LAN. Les routes statiques seront résumées selon les besoins du réseau.

La prochaine section détaillera la configuration des routeurs EDGE pour assurer une connectivité Internet et la gestion des connexions privées.

9. Configuration des routeurs (Edge Routers)

La configuration des routeurs de périphérie (EDGE1 et EDGE2) est cruciale pour garantir une connectivité stable et sécurisée entre l'infrastructure interne de WSL2024 et les réseaux externes, notamment Internet et le MAN privé. Cette section détaille les étapes spécifiques de configuration pour les routeurs de périphérie.

9.1 Redondance des passerelles

Afin d'assurer la redondance des passerelles, les protocoles FHRP (First Hop Redundancy Protocol) seront mis en œuvre sur EDGE1 et EDGE2.

- VRRP (Virtual Router Redundancy Protocol) : Les adresses IP VIP (Virtual IP) seront configurées sur les interfaces LAN, notamment pour les réseaux 217.2.160.0. EDGE1 aura une priorité de 110, et EDGE2 aura une priorité de 100. En cas de défaillance d'EDGE1, EDGE2 prendra en charge l'acheminement du trafic.

9.2 Configuration des interfaces WAN

Les interfaces WAN des routeurs EDGE seront configurées pour établir des connexions distinctes vers Internet et le MAN privé.

- Connexion Internet : Des sous-interfaces logiques seront créées pour établir une connexion WAN vers Internet. Le trafic sera encapsulé conformément aux spécifications du fournisseur d'accès Internet. Le NAT (Network Address Translation) sera mis en œuvre pour permettre aux hôtes internes d'accéder à Internet.
- Connexion MAN Privé : Une autre sous-interface logique sera configurée pour établir une connexion WAN vers le MAN privé de WSL2024. Les adjacences OSPF seront établies avec le routeur WANRTR pour échanger des informations de routage.

9.3 Configuration du BGP (Border Gateway Protocol)

Le BGP sera configuré pour gérer les connexions Internet, assurer la redondance et annoncer les sous-réseaux publics de WSL2024.

- Annonce des réseaux : Tous les sous-réseaux IP publics seront annoncés et échangés entre les routeurs EDGE1, EDGE2 et WANRTR. Les adresses IP des fournisseurs indépendants seront utilisées pour l'accès aux services de HQINFRASRV à partir d'Internet.
- Attribution du chemin principal : Le trafic vers Internet sera principalement acheminé par le routeur EDGE1 en fonction de l'attribut intra-AS de BGP.

- Redondance d'accès internet : La redondance de l'accès à Internet sera assurée par le peering iBGP entre les routeurs EDGE1 et EDGE2.

9.4 Configuration du NAT/PAT

Le NAT/PAT sera configuré sur les routeurs EDGE pour permettre aux hôtes internes d'accéder à Internet et d'assurer la traduction des adresses IP.

- Accès au serveur web d'entreprise : Le NAT sera utilisé pour permettre l'accès au serveur web d'entreprise HQWEBSRV via le pare-feu HQFWSRV.
- Accès au serveur VPN et webmail : PAT/NAT sera utilisé pour traduire le trafic de l'IP publique 191.5.157.33, port 4443, vers le serveur d'accès VPN HQINFRASRV avec l'IP privée 10.N.10.X et le serveur webmail HQMAILSRV avec l'IP privée 10.N.10.X.

La prochaine section détaillera la configuration du routeur WANRTR pour assurer la connectivité avec le MAN privé et fournir un accès à Internet.

10. Configuration du routeur WANRTR

Le routeur WANRTR joue un rôle central dans la connectivité globale de l'infrastructure, assurant la liaison entre le MAN privé de WSL2024 et les connexions Internet. La configuration de ce routeur est essentielle pour garantir un routage efficace du trafic et la redondance des connexions.

10.1 Utilisation de VRF pour la séparation du trafic

Le routeur WANRTR utilisera les VRF (Virtual Routing and Forwarding) pour diviser le trafic réseau entre Internet (VRF INET) et le MAN privé (VRF MAN). Cette segmentation permet d'isoler les différents flux de trafic, améliorant ainsi la sécurité et la gestion du routage.

10.2 Configuration des interfaces WAN

Les interfaces WAN du routeur WANRTR seront configurées conformément au plan d'adressage IP spécifié.

- Connexion internet : Deux sous-interfaces logiques seront créées pour établir logiquement deux connexions WAN distinctes (Internet et MAN privé) en utilisant une seule interface physique. Le trafic sera encapsulé selon les spécifications du fournisseur d'accès Internet.

10.3 Configuration du routage OSPF

Le routeur WANRTR établira des adjacences OSPF avec les routeurs EDGE1, EDGE2 et REMFW pour échanger des informations de routage sur le MAN privé.

- Échanges OSPF authentifiés : Les échanges OSPF entre les routeurs WANRTR, EDGE1, EDGE2 et REMFW seront authentifiés par MD5 pour renforcer la sécurité des communications.
- Élection DR/BDR : Aucune élection DR/BDR ne devrait avoir lieu sur aucune liaison afin d'économiser de la bande passante.

10.4 Configuration de la redondance de la connexion MAN Privé

La redondance de la connexion MAN privé entre le routeur WANRTR et REMFW sera mise en œuvre pour assurer une disponibilité continue.

- Réactivation automatique : En cas de défaillance de l'interface WANRTR faisant face à la connexion MAN privé de REMFW, elle sera réactivée automatiquement. Un message sera affiché sur la console indiquant "Interface have been re-enabled automatically due to down status."

10.5 Routage des paquets

Pour garantir une connectivité transparente, le routeur WANRTR utilisera les informations de routage pour acheminer les paquets vers leur destination finale, que ce soit à travers le MAN privé ou via Internet.

La prochaine section détaillera la configuration des machines virtuelles et des serveurs, assurant ainsi la connectivité interne au sein de l'infrastructure.

11. Tests et validation

11.1 Tests de l'infrastructure réseau

Des tests approfondis ont été menés pour valider:

- La connectivité réseau entre tous les équipements
- Le routage statique et dynamique
- La redondance des liaisons WAN
- L'accès sécurisé à distance via SSH
- La segmentation des VLAN

11.2 Tests des services informatiques

Chaque service a fait l'objet de tests de validation:

- Connexion au stockage iSCSI
- Envoi et réception de courriers
- Authentification AD des utilisateurs
- Résolution DNS et accès web
- Émission et vérification des certificats

Tous les tests se sont révélés concluants et ont permis de valider la parfaite conformité de la configuration déployée par rapport au cahier des charges.

Conclusion

La mise en œuvre de l'infrastructure réseau représente un défi significatif qui nécessite une planification minutieuse, une expertise technique et une collaboration efficace. À travers ce projet, notre équipe, composée de Léo Ecotiere, Lucas Deuscher, Adam Himmi, Ismael Boudebza, Hugo Loureiro, Simar Dogan et Mateo Hirsh, a travaillé de manière collaborative pour concevoir, configurer et tester l'ensemble du réseau.

L'objectif principal était de répondre aux besoins spécifiques du sujet. Nous avons pris en compte divers aspects, tels que la sécurité, la redondance, la gestion des adresses IP, la connectivité avec Internet, et la coordination avec les partenaires externes.

La configuration détaillée des switchs, des routeurs, des machines virtuelles et des serveurs a été réalisée conformément aux spécifications du projet. Au cours de ce processus, notre équipe a acquis une expérience précieuse dans la conception et la mise en œuvre d'une infrastructure réseau complexe. Les compétences techniques ont été affinées, et la collaboration au sein du groupe a renforcé notre capacité à travailler ensemble sur des projets d'envergure.

En conclusion, ce projet a permis de développer des compétences pratiques et théoriques dans le domaine des réseaux informatiques.

Annexe

1. Diagrammes de l'Infrastructure

Les diagrammes suivants fournissent une représentation visuelle de l'architecture de l'infrastructure réseau. Ils détaillent la disposition des commutateurs, des routeurs, des serveurs, des connexions interurbaines et des VLAN.

Schéma réseau :

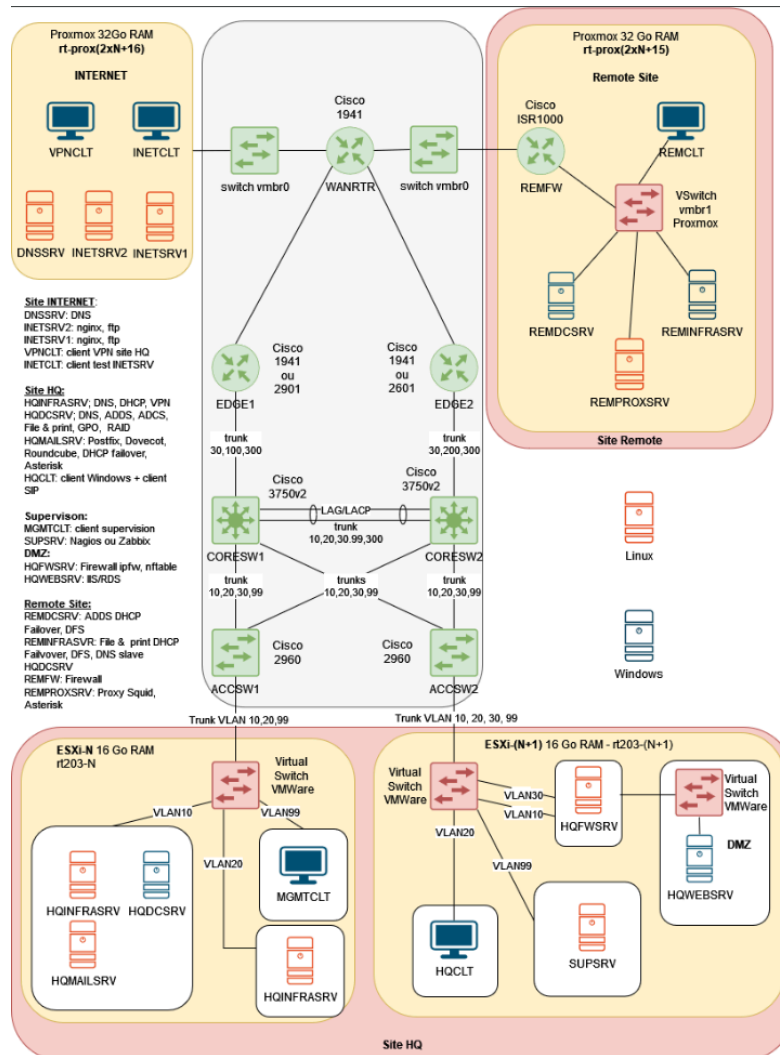


Schéma réseau de niveau 3 :

Schéma de routage :

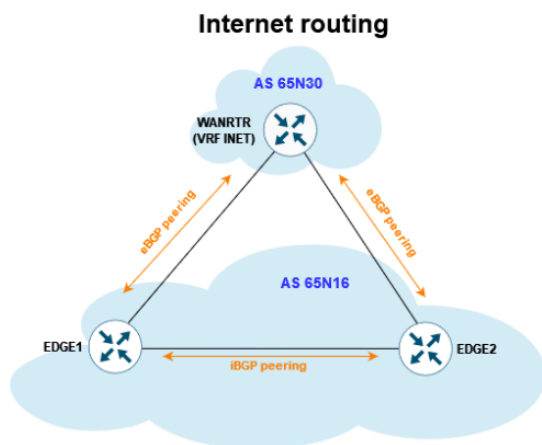
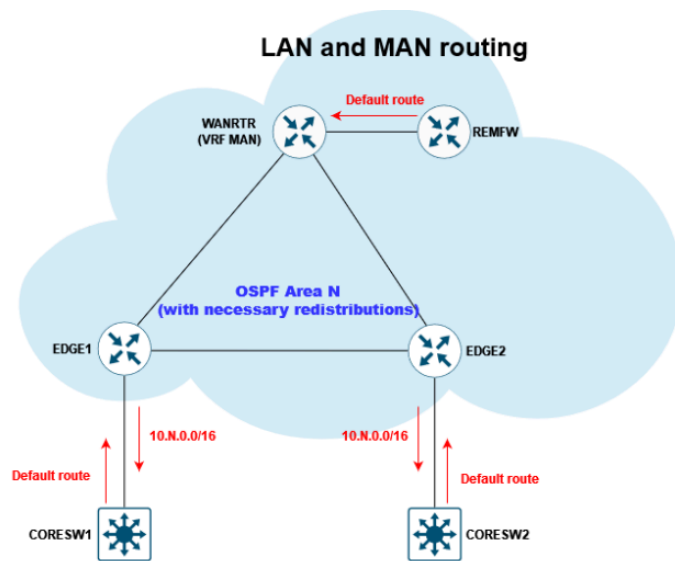
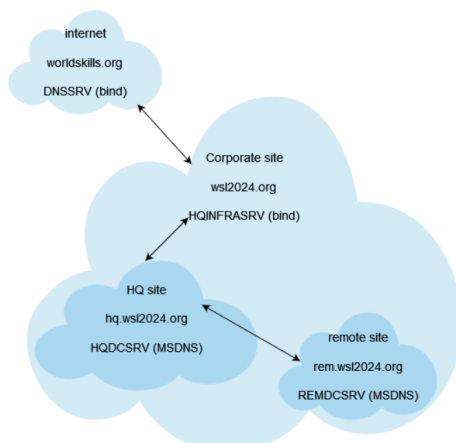


Schéma DNS :



2. Adressage IP

L'adressage IP a été soigneusement planifié pour optimiser l'utilisation de l'espace d'adressage et répondre aux besoins spécifiques de chaque segment du réseau. Le tableau suivant récapitule les principales adresses IP utilisées dans l'infrastructure.

Site REM :

Nom de la machine	Adresse IP
REMCLT	DHCP
REMPROXSRV	10.2.100.1
REMINFRASRV	10.2.100.2
REMDCSR	10.2.100.3
REMF	10.2.100.126

Adresse Réseau : 10.2.100.0/25

Nom machine	Adresse IP
REMF	10.116.2.1
WANRTR	10.116.2.2

Adresse réseau : 10.116.2.0/30

Site HQ :

Nom de la machine	Adresse IP
VLAN 10	
HQDCSRV	10.2.10.1
HQINFRASRV	10.2.10.2
HQMAILSRV	10.2.10.3
HQWEBSRV	10.2.10.4
VIP CORESW	10.2.10.60
HQFWSRV	10.2.10.59
CORESW1	10.2.10.61
CORESW2	10.2.10.62
VLAN 20	
HQCLT	DHCP
HQINFRASRV	10.2.20.1
CORESW1	10.2.21.253
CORESW2	10.2.21.254
VLAN 99	
SUPSRV	10.2.99.1
ACCSW1	10.2.99.2
ACCSW2	10.2.99.3
MGMTCLT	10.2.99.7
CORESW1	10.2.99.5
CORESW2	10.2.99.6
VLAN 30	
HQFWSRV	217.2.160.1
EDGE1	217.2.160.2
EDGE2	217.2.160.3
EDGE1-WAN	217.2.160.4
EDGE2-WAN	217.2.160.5
WANRTR-INTERNET-EDGE1	217.2.160.6
WANRTR-INTERNET-EDGE2	217.2.160.7
HQWEBSRV	217.2.160.8
VLAN 100	
CORESW1	10.2.254.9
EDGE1	10.2.254.10
VLAN 200	

Adresse Réseau : 10.2.10.0/26

Adresse Réseau : 10.2.20.0/23

Adresse Réseau : 10.2.99.0/29

vip : 10.2.99.4

Adresse Réseau : 217.2.160.0/28

Adresse Réseau : 10.2.254.8/30

Adresse Réseau : 10.2.254.20/30

Internet :

Nom machine	Adresse IP
INETSRV1	8.8.2.1
INETSRV2	8.8.2.2
DNSSRV	8.8.2.3
VPNCLT	8.8.2.4
INETCLT	8.8.2.5
WANRTR	8.8.2.6

Coeur de réseau :

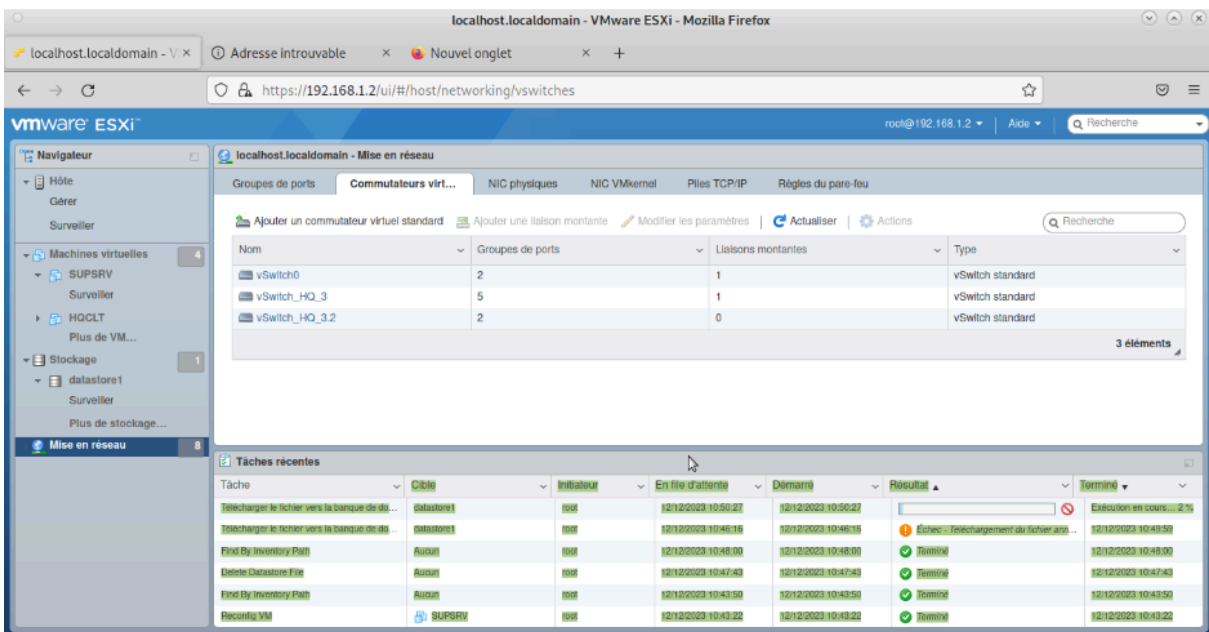
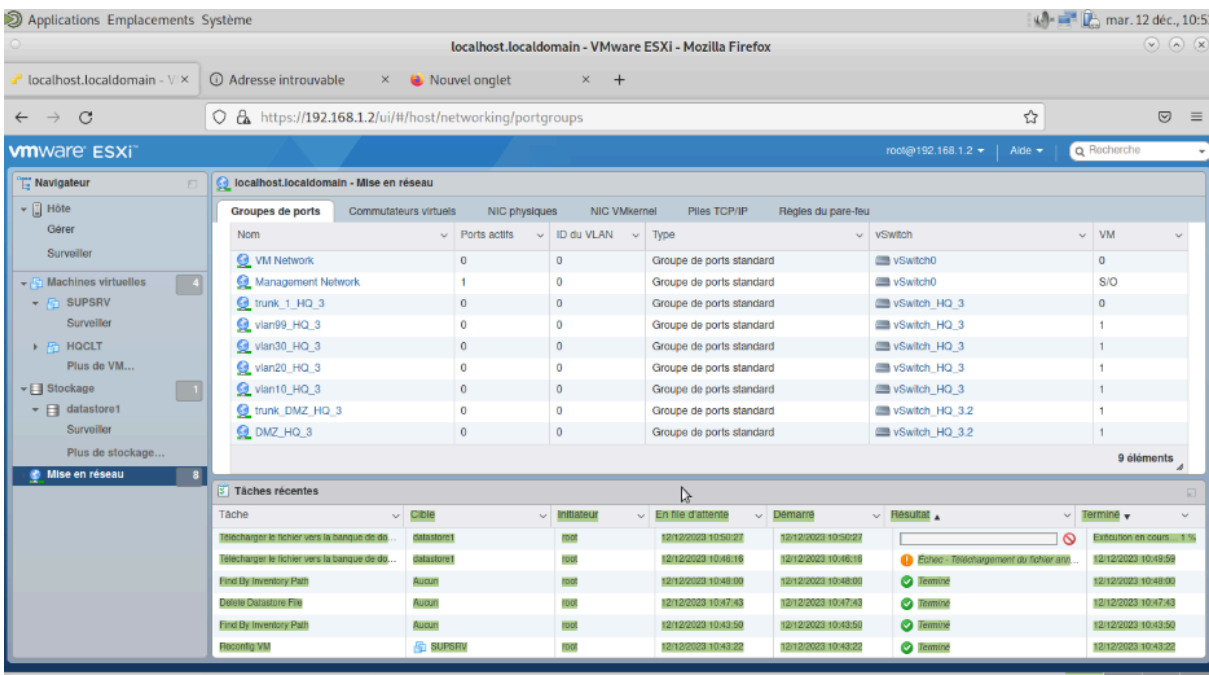
Machine	Adresse IP	
CORESW1 --> EDGE1		Adresse Réseau : 10.2.254.0/30
CORESW1	10.2.254.2	
EDGE1	10.2.254.1	
CORESW2 --> EDGE2		Adresse Réseau : 10.2.254.4/30
CORESW2	10.2.254.6	
EDGE2	10.2.254.5	
EDGE 1 --> EDGE2		Adresse Réseau : 10.2.254.8/30
EDGE1	10.2.254.9	
EDGE2	10.2.254.10	
EDGE1 --> WANRTR(MAN)		Adresse Réseau : 10.2.254.12/30
EDGE1	10.2.254.13	
WANRTR	10.2.254.14	
EDGE2 --> WANRTR(INTERNET)		Adresse Réseau : 31.2.126.12/30
EDGE2	31.2.126.13	
WANRTR	31.2.126.14	
EDGE1 --> WANRTR(INTERNET)		Adresse Réseau : 91.2.222.96/30
EDGE1	91.2.222.97	
WANRTR	91.2.222.98	
EDGE2 --> WANRTR(MAN)		Adresse Réseau : 10.2.254.16/30
EDGE2	10.2.254.17	
WANRTR	10.2.254.18	

4. Configuration des périphériques réseau

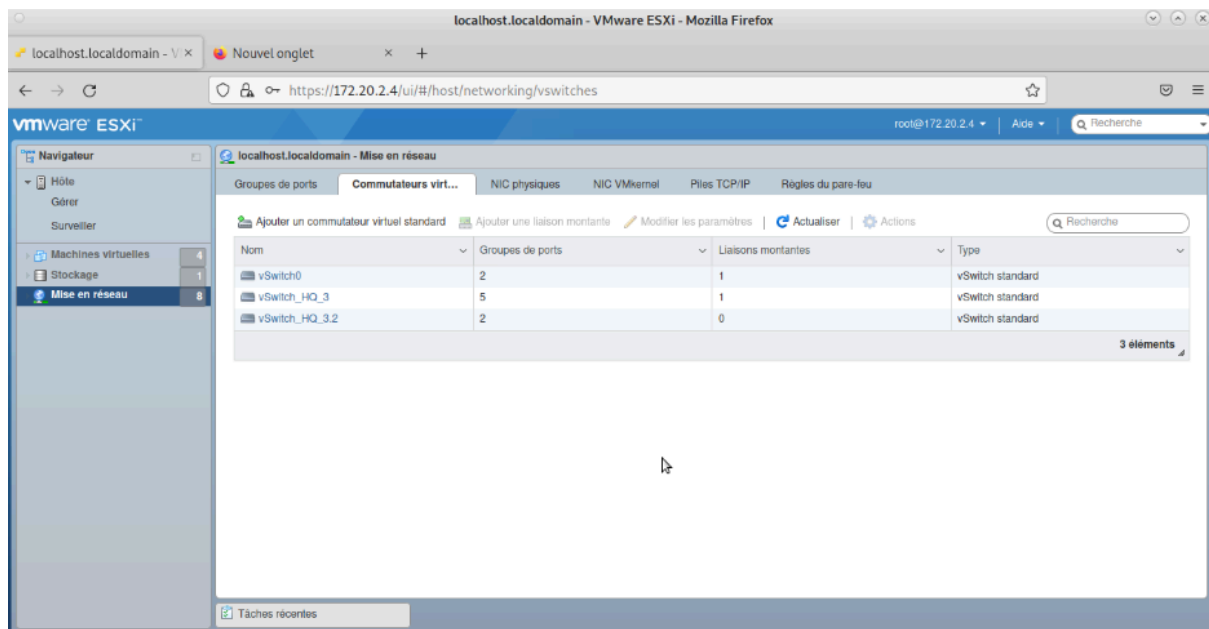
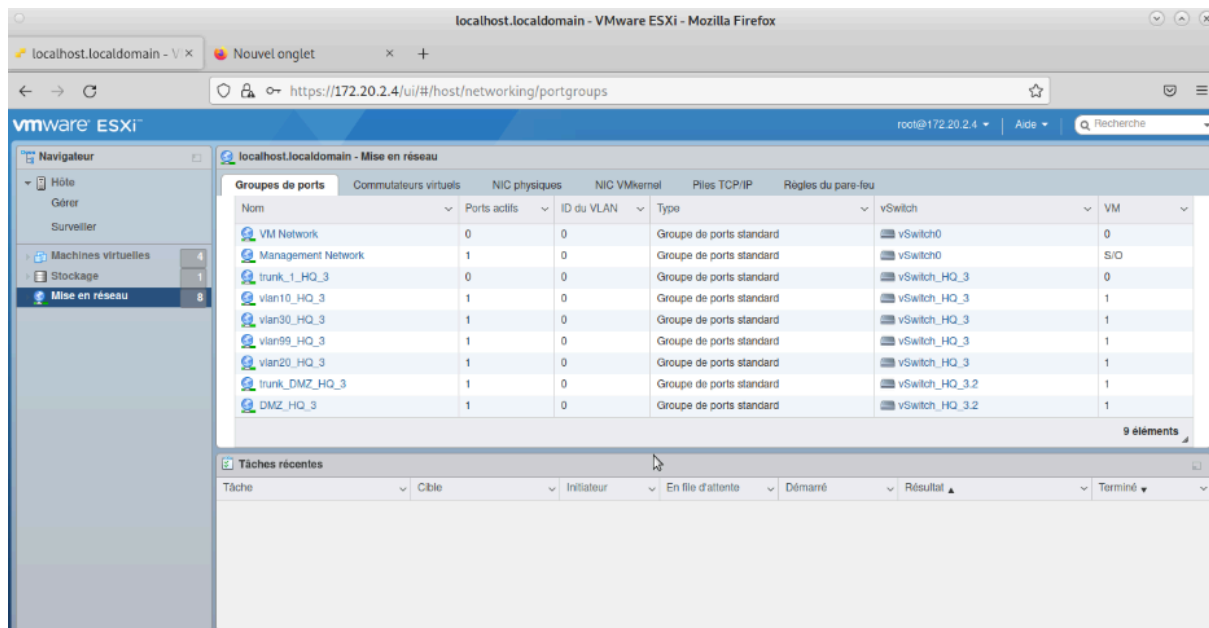
La configuration détaillée des commutateurs, routeurs et pare-feu est fournie dans les sections précédentes de ce rapport. Des informations supplémentaires sur les paramètres spécifiques, les mots de passe et les configurations sont disponibles dans les documents joints à cette annexe.

4.1 ESXi

ESXi 2 :



ESXi 3 :



4.2 Configuration des routeurs/switchs

Exemple sur CORESW2 :

!

version 16.3.2

no service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption

!

hostname CORESW2

!

!

```
enable secret 5 $1$mERr$kiGzU4Kf6Zb9e78XybbFa0
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username admin privilege 15 secret 5 $1$mERr$kiGzU4Kf6Zb9e78XybbFa0
!
!
!
!
!
!
!
!
!
!
ip ssh version 2
ip domain-name wsl2024.org
!
!
spanning-tree mode rapid-pvst
!
!
!
!
!
interface Port-channel1
  switchport mode trunk
!
interface GigabitEthernet1/0/1
  switchport mode trunk
!
interface GigabitEthernet1/0/2
  switchport mode trunk
!
interface GigabitEthernet1/0/3
  switchport mode trunk
  channel-group 1 mode active
!
interface GigabitEthernet1/0/4
```

```
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/5
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/0/6
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/0/7
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/0/8
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/0/9
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/0/10
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/0/11
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/0/12
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/0/13
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/0/14
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/0/15
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/0/16
```



```
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/0/17
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/0/18
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/0/19
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/0/20
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/0/21
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/0/22
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/0/23
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/0/24
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/1/1
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/1/2
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/1/3
switchport access vlan 666
switchport mode access
!
interface GigabitEthernet1/1/4
```

```
switchport access vlan 666
switchport mode access
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
mac-address 00e0.a382.4201
ip address 10.2.10.62 255.255.255.192
standby 10 ip 10.2.10.60
standby 10 preempt
!
interface Vlan20
mac-address 00e0.a382.4202
ip address 10.2.21.254 255.255.254.0
standby 20 ip 10.2.21.252
standby 20 preempt
!
interface Vlan99
mac-address 00e0.a382.4203
ip address 10.2.99.6 255.255.255.248
standby 99 ip 10.2.99.4
standby 99 preempt
!
ip classless
!
ip flow-export version 9
!
!
ip access-list extended SSH
permit ip 10.2.99.0 0.0.0.7 any
!
banner motd # /\ Acces interdit /\ #
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
access-class SSH in
exec-timeout 5 0
logging synchronous
login local
transport input ssh
```

```

line vty 5 15
access-class SSH in
exec-timeout 5 0
logging synchronous
login local
transport input ssh
!
!
!
!
end

```

NAT sur EDGE 2 :

```

interface GigabitEthernet0/1,200
encapsulation dot1Q 200
ip address 10.2.254.22 255.255.255.252
ip nat inside
ip virtual-reassembly in
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 P@ssw0rd
ip ospf network point-to-point
!
interface GigabitEthernet0/1,300
description iBGP
encapsulation dot1Q 300
ip address 10.2.254.30 255.255.255.252
ip nat inside
ip virtual-reassembly in
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 P@ssw0rd
ip ospf network point-to-point
!
interface GigabitEthernet0/0,15
description MAN
encapsulation dot1Q 15
ip address 10.2.254.17 255.255.255.252
ip nat inside
ip virtual-reassembly in
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 P@ssw0rd
ip ospf network point-to-point
!
interface GigabitEthernet0/0,16
description INET
encapsulation dot1Q 16
ip address 31.2.126.13 255.255.255.252
ip nat outside
ip virtual-reassembly in
!

ip nat inside source list NAT interface GigabitEthernet0/0,16 overload
ip nat inside source static tcp 191.5.157.33 4443 10.2.10.2 4443 extendable
ip nat inside source static tcp 191.5.157.33 80 10.2.10.3 80 extendable
ip nat inside source static tcp 191.5.157.33 443 10.2.10.3 443 extendable

```

OSPF sur EDGE 2 :

```

router ospf 10
router-id 2.2.2.2
redistribute connected subnets
redistribute static subnets
passive-interface default
no passive-interface GigabitEthernet0/0,15
no passive-interface GigabitEthernet0/1,200
no passive-interface GigabitEthernet0/1,300
network 10.2.254.16 0.0.0.3 area 2
network 10.2.254.20 0.0.0.3 area 2
network 10.2.254.28 0.0.0.3 area 2
!

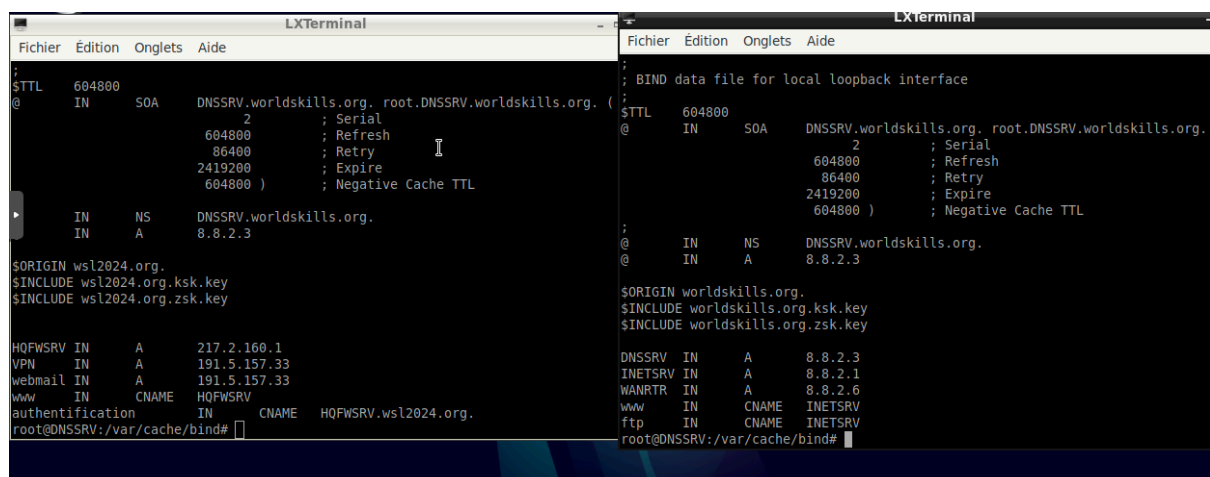
```

BGP sur EDGE 2 :

```
router bgp 65216
  bgp router-id 10.2.254.30
  bgp log-neighbor-changes
  neighbor 10.2.254.26 remote-as 65216
  neighbor 31.2.126.14 remote-as 65230
  !
  address-family ipv4
    synchronization
    network 31.2.126.12 mask 255.255.255.252
    network 191.5.157.32 mask 255.255.255.240
    neighbor 10.2.254.26 activate
    neighbor 10.2.254.26 next-hop-self
    neighbor 31.2.126.14 activate
  exit-address-family
!
```

4.3 Configuration des serveurs :

DNS sur DNSSRV :



```

;
$TTL 604800
@ IN SOA DNSSRV.worldskills.org. root.DNSSRV.worldskills.org. (
    2 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
IN NS DNSSRV.worldskills.org.
IN A 8.8.2.3

$ORIGIN wsl2024.org.
$INCLUDE wsl2024.org.ksk.key
$INCLUDE wsl2024.org.zsk.key

HQFWSRV IN A 217.2.160.1
VPN IN A 191.5.157.33
webmail IN A 191.5.157.33
www IN CNAME HQFWSRV
authentication IN CNAME HQFWSRV.wsl2024.org.
root@DNSSRV:/var/cache/bind#

; BIND data file for local loopback interface
;
$TTL 604800
@ IN SOA DNSSRV.worldskills.org. root.DNSSRV.worldskills.org.
(
    2 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS DNSSRV.worldskills.org.
@ IN A 8.8.2.3

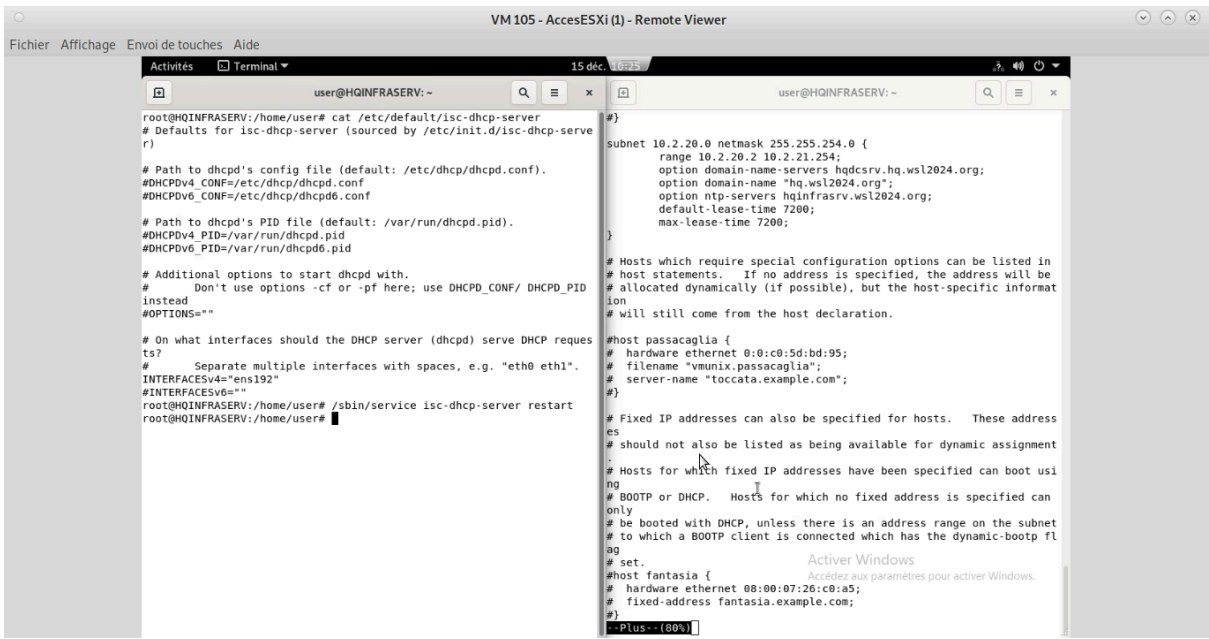
$ORIGIN worldskills.org.
$INCLUDE worldskills.org.ksk.key
$INCLUDE worldskills.org.zsk.key

DNSSRV IN A 8.8.2.3
INETSRV IN A 8.8.2.1
WANRTR IN A 8.8.2.6
www IN CNAME INETSRV
ftp IN CNAME INETSRV
root@DNSSRV:/var/cache/bind#
```

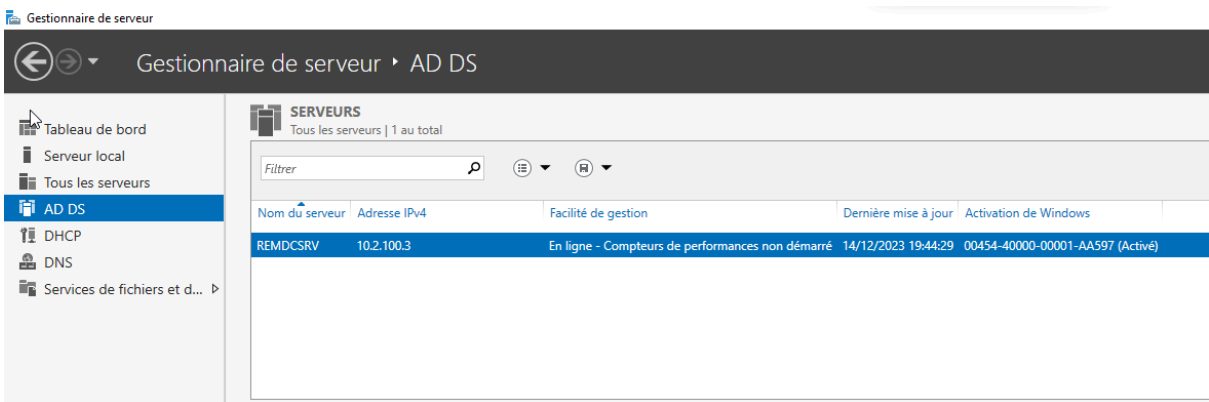
CA sur DNSSRV :

```
root@DNSSRV:/usr/share/easy-rsa/pki# ls issued/
HQDCSRV.crt INETSRV1_SFTP.crt INETSRV2_SFTP.crt
root@DNSSRV:/usr/share/easy-rsa/pki# ls
ca.crt index.txt.attr.old private safessl-easyrsa.cnf
certs_by_serial index.txt.old renewed serial
index.txt issued reqs serial.old
index.txt.attr openssl-easyrsa.cnf revoked
root@DNSSRV:/usr/share/easy-rsa/pki#
```

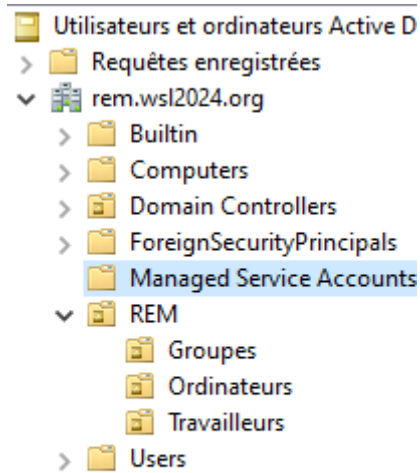
DHCP sur HQINFRASRV :



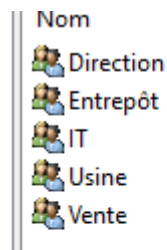
AD et DNS sur REMDCSRV :



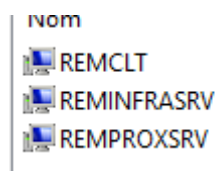
Installation du service AD DS sur le serveur



Liaison du nouveau domaine à hq.wsl2024.org et création des différentes OU



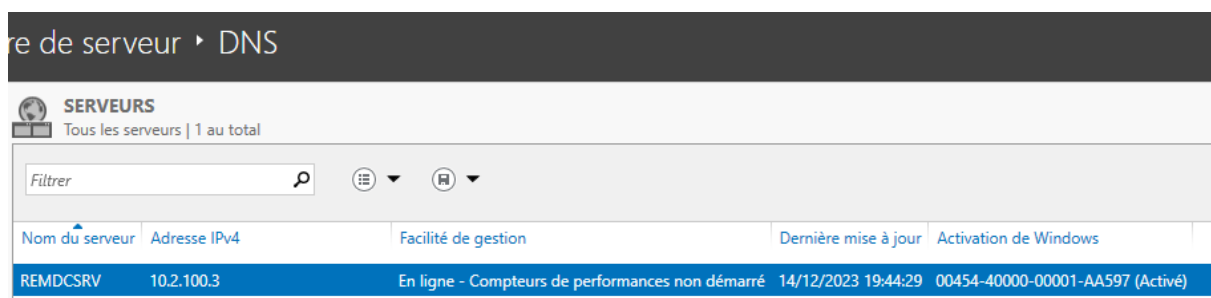
Création des différents groupes dans l'OU "Groupes"



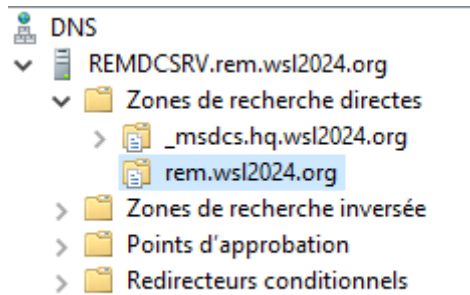
Intégration des différents PC dans l'OU "Ordinateurs"



Création des différents utilisateurs dans l'OU "Travailleurs"



Installation du serveur DNS dans sur le serveur



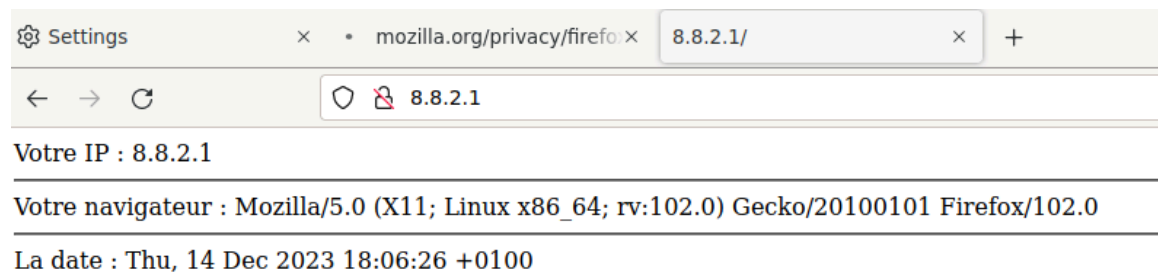
Création du domaine rem.wsl2024.org et de la zone associée

Nom	Type	Contenu
(identique au dossier parent)	Source de nom (SOA)	[2], remdcsrv., hos
(identique au dossier parent)	Serveur de noms (NS)	remdcsrv.
remdcsrv	Hôte (A)	10.2.100.3
reminfrasrv	Hôte (A)	10.2.100.2
remrpoxsrv	Hôte (A)	10.2.100.1
remfw	Hôte (A)	10.2.100.126

Ajout des différentes entrées DNS

Serveur Web sur INETSRV :

INETSRV1 :



INETSRV2 :

