Rapport Final de la SAÉ 3.03

Pépinière Multi-Sites – Déploiement d’une infrastructure réseau multi-sites pour une entreprise en pleine expansion

| **Étudiants :**   * Leroy Rémi * Lernould Adam * Sailliot Valentin * Guyot Loïc | **Encadrants pédagogiques :**   * Sylvain Merchez * David Mercier * Alain Trouillez * Sohaib Lafifi |
| --- | --- |

## Dates du projet :

* Travail en autonomie : 06/01/2025
* Collaboration avec les RT1 : 13/01/2025
* Réalisation finale : 17/01/2025

sommaire

[**Dates du projet : 0**](#_5wx2ayx34538)

[**Résumé du Projet 2**](#_m7m35oimv7vd)

[**1. Introduction 3**](#_aj2raovp56qd)

[**2. Plan d’Adressage IP 5**](#_vxmje8hn34lb)

[Siège (172.31.X.X) 5](#_jzdn0fm5avq6)

[Succursale (172.32.X.X) 6](#_6pre7j2121dn)

[Ajout Spécifique : Routage et NAT 7](#_8alxtdwlz4ae)

[**3. Services Installés 8**](#_xf6d2molhj9w)

[3.1. Services Installés au Siège 8](#_uz3qqwqgq3vt)

[3.2. Services Installés à la Succursale 8](#_tupdv82ygx1m)

[**4. Détails de la Configuration Réseau des Équipements 9**](#_qw0in6oxw3nh)

[4.1. Configuration des Routeurs (R1 et R2) 9](#_z3ntx5trfkl3)

[a) Activation des Licences et des Fonctionnalités de Sécurité 9](#_rfcnrsoercnn)

[b) Routage Dynamique et OSPF 9](#_y3asxr7q0d9j)

[c) Interfaces LAN et WAN 9](#_j4yv97u2faqp)

[d) Tunnel GRE sur IPsec 9](#_cv53lnsid8az)

[e) Configuration NAT 10](#_rhpglmcq1vlp)

[4.2. Configuration des Commutateurs 10](#_14vpchjz5gq0)

[a) Commutateur de Niveau 2 (SW-L2 – Succursale) 10](#_lkxm0amqdpz6)

[b) Commutateurs de Niveau 3 (SW-L3-1 et SW-L3-2 – Site A) 10](#_1c3ioi779bi2)

[c) Sécurisation et Gestion des Accès 11](#_v7v9wz9izcy4)

[d) Qualité de Service (QoS) 11](#_skp9sy2sqoxf)

[4.3. Configuration du Serveur Windows (Services DHCP, DNS, Mail et Proxy) 11](#_sspn9qj7kw29)

[a) Configuration de l’Adresse IP 11](#_56zg0mcs8n0r)

[b) Installation et Configuration des Rôles 11](#_x6t0bla7fyr5)

[c) Vérifications et Tests 12](#_gd9jfdas68mo)

# 

# 

# 

# 

## Résumé du Projet

Ce projet consiste à concevoir, simuler, déployer et sécuriser une infrastructure réseau destinée à une entreprise en forte expansion disposant d’un site principal (Siège) et d’une succursale distante. Les principaux objectifs du projet étaient :

* **Installation et configuration de serveurs** : Mise en place des services essentiels tels que DNS, Active Directory, Proxy et Serveur Mail afin d’assurer la gestion et la sécurité des échanges.
* **Création de segments réseaux dédiés** : Définition de réseaux distincts pour différents usages (ADMIN, PRODUCTION, PERSONNEL, VIDÉO, etc.) avec des configurations de VLAN et d’adressage IP spécifiques.
* **Redondance et sécurisation** : Mise en place de solutions de redondance pour assurer la continuité de service ainsi que la sécurisation des connexions inter-sites.
* **Extension multi-sites** : Préparation d’une architecture ouverte à l’ajout futur de sites européens, en intégrant notamment le routage dynamique et le tunnel GRE pour assurer l’interconnexion sécurisée des sites.
* **Routage et NAT** : Configuration d’un routage OSPF inter-sites et l’implémentation d’un NAT sur les interfaces WAN pour permettre la connexion de la société à internet via des adresses IP publiquement routables.

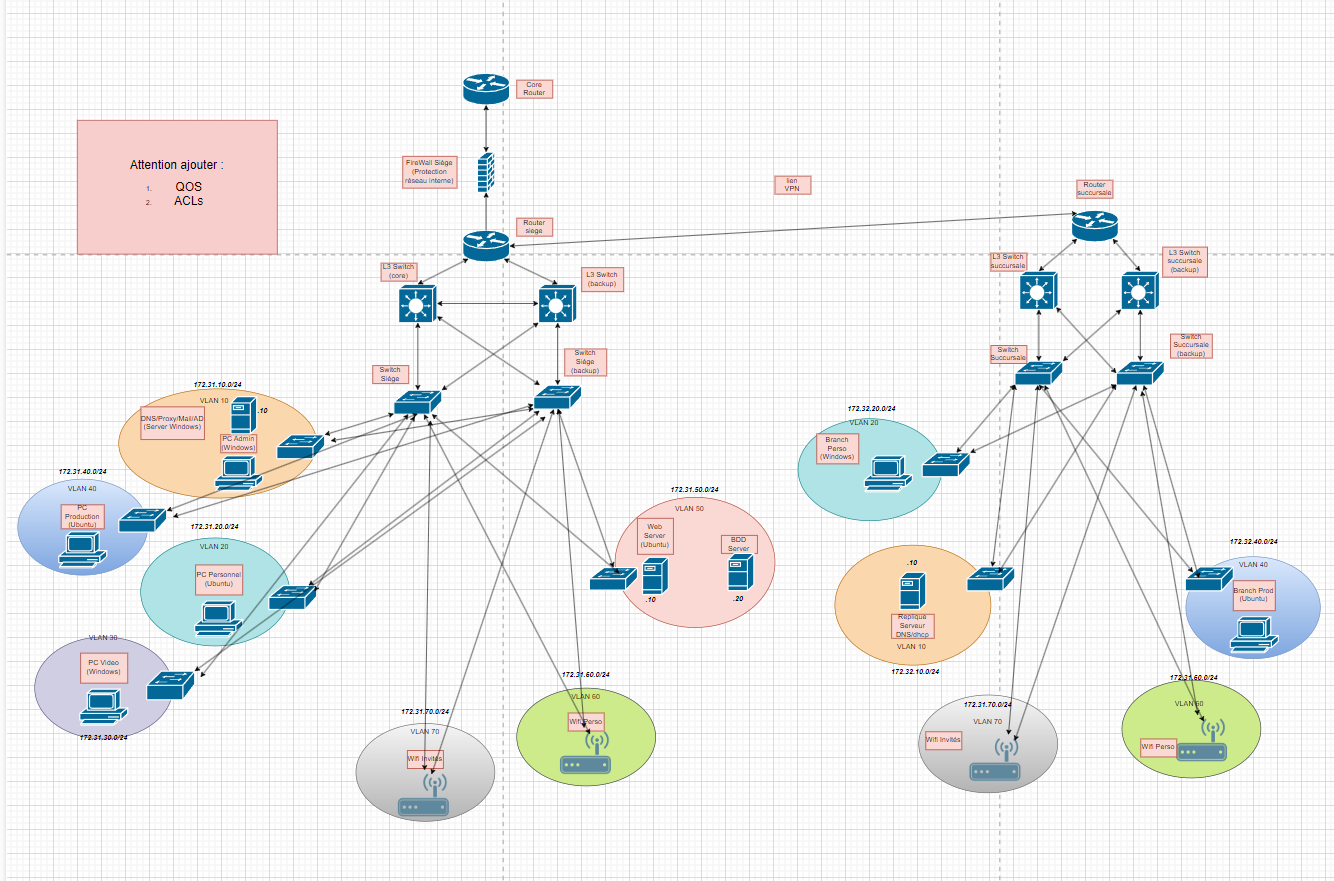
## 

## 1. Introduction

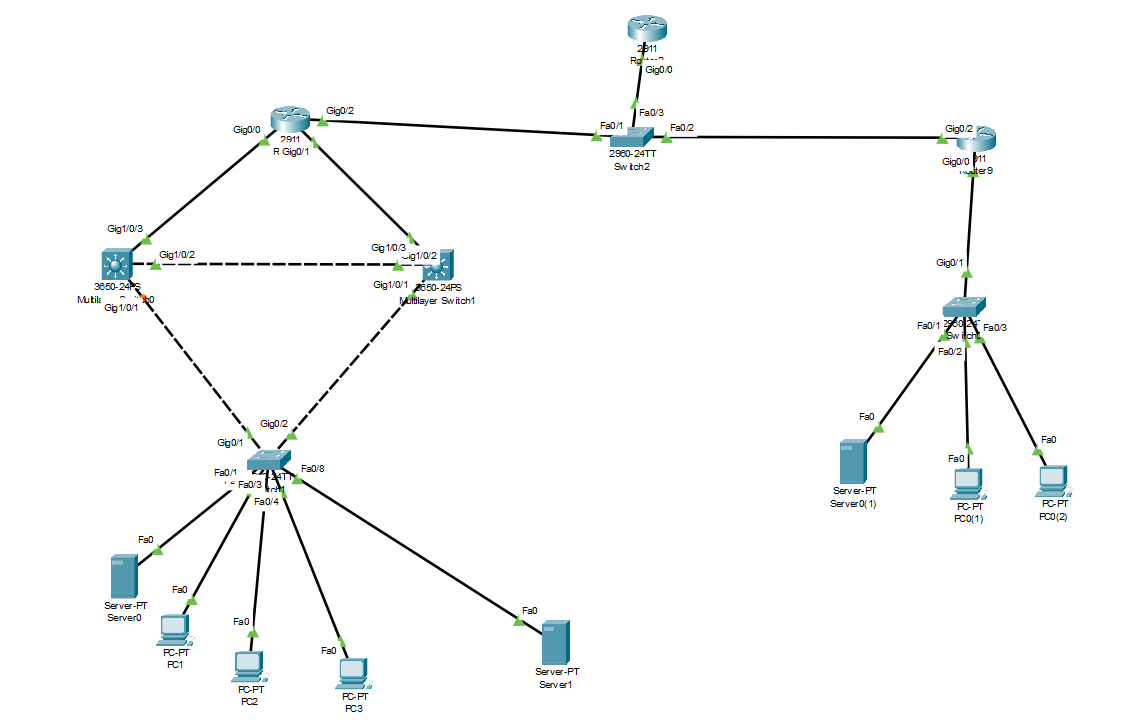
Ce document présente en détail la configuration mise en œuvre pour l’infrastructure réseau de l’entreprise, tant au niveau du Siège que de la Succursale. L’approche suivie comporte :

* Une description complète du plan d’adressage IP et des VLAN associés pour chaque site.
* La mise en place du routage inter-sites via OSPF et l’implémentation d’un tunnel GRE entre la succursale et le siège.
* L’installation des services essentiels (serveurs AD, DNS, Proxy, etc.) et leur répartition sur les différents VLAN.
* La sécurisation des accès via la configuration de politiques de routage et des adresses NAT adaptées aux interfaces WAN.

Un schéma détaillé de la topologie réseau (généré à l’aide de Cisco Packet Tracer) est joint en annexe afin d’illustrer l’architecture globale.



voir le schéma dans [Annexe (schéma](https://drive.google.com/open?id=16mMsj-vhsORfF-XjQ7jKQPj39lsA-EA8)) puis [TopologieV2.drawio](https://drive.google.com/open?id=1ZZ64BuctPytZWc07AQ_4dCIJegQk8xWw)



voir le schéma dans [Annexe (schéma)](https://drive.google.com/open?id=16mMsj-vhsORfF-XjQ7jKQPj39lsA-EA8) puis [Sim\_nat\_tunnel.pkt](https://drive.google.com/open?id=1RLa4DNLQziMk8Mbxk9lfGakeloSwi4D8)

### 

## 

## 2. Plan d’Adressage IP

### Siège (172.31.X.X)

La répartition des réseaux pour le Siège est organisée en fonction des VLAN dédiés à chaque usage.

| **Réseau** | **VLAN** | **Adresse Réseau** | **Plage IP Utilisable** | **Passerelle** |
| --- | --- | --- | --- | --- |
| **ADMIN** | 10 | 172.31.10.0/24 | 172.31.10.20 – 172.31.10.200 | 172.31.10.254 |
| **PERSONNEL** | 20 | 172.31.20.0/24 | 172.31.20.20 – 172.31.20.200 | 172.31.20.254 |
| **VIDEO** | 30 | 172.31.30.0/24 | 172.31.30.20 – 172.31.30.200 | 172.31.30.254 |
|  |  |  |  |  |
| **PRODUCTION** | 40 | 172.31.40.0/24 | 172.31.40.20 – 172.31.40.200 | 172.31.40.254 |
| **DMZ** | 50 | 172.31.50.0/24 | 172.31.50.20 – 172.31.50.200 | 172.31.50.254 |
| **WIFI-PERSO** | 60 | 172.31.60.0/24 | 172.31.60.20 – 172.31.60.200 | 172.31.60.254 |
| **WIFI-GUEST** | 70 | 172.31.70.0/24 | 172.31.70.20 – 172.31.70.200 | 172.31.70.254 |
| **LAN-CORE-1** | 80 | 172.31.80.0/24 | 172.31.80.1 – 172.31.80.254 | 172.31.80.1 |
| **LAN-CORE-2** | 90 | 172.31.90.0/24 | 172.31.90.1 – 172.31.90.254 | 172.31.90.1 |

### Succursale (172.32.X.X)

Pour la succursale, la logique de segmentation est similaire au siège, avec une adaptation de l’adressage.

#### 

| **Réseau** | **VLAN** | **Adresse Réseau** | **Plage IP Utilisable** | **Passerelle** |
| --- | --- | --- | --- | --- |
| **ADMIN** | 10 | 172.32.10.0/24 | 172.32.10.20 – 172.32.10.200 | 172.32.10.254 |
| **PERSONNEL** | 20 | 172.32.20.0/24 | 172.32.20.20 – 172.32.20.200 | 172.32.20.254 |
| **VIDEO** | 30 | 172.32.30.0/24 | 172.32.30.20 – 172.32.30.200 | 172.32.30.254 |
| **PRODUCTION** | 40 | 172.32.40.0/24 | 172.32.40.20 – 172.32.40.200 | 172.32.40.254 |
| **DMZ** | 50 | 172.32.50.0/24 | 172.32.50.20 – 172.32.50.200 | 172.32.50.254 |
| **WIFI-PERSO** | 60 | 172.32.60.0/24 | 172.32.60.20 – 172.32.60.200 | 172.32.60.254 |
| **WIFI-GUEST** | 70 | 172.32.70.0/24 | 172.32.70.20 – 172.32.70.200 | 172.32.70.254 |
| **LAN-GRE** | 80 | 192.168.1.0/30 | 192.168.1.1 – 192.168.1.2 | 192.168.1.1 |

### Ajout Spécifique : Routage et NAT

Afin d’assurer la connectivité entre le Siège et la Succursale et permettre l’accès à Internet, les éléments suivants ont été configurés :

* **Interface WAN (Siège) :**
  + Plage IP : 10.7.1.0/8
  + IP Passerelle : 10.0.0.1
* **Interface WAN (Succursale) :**
  + Plage IP : 10.7.2.0/8
  + IP Passerelle : 10.0.0.1
* **Tunnel GRE :**
  + Sous-réseau : 192.168.1.0/30
  + Siège : 192.168.1.1
  + Succursale : 192.168.1.2

Le routage dynamique (via OSPF) est mis en place pour l’échange de routes entre les différents réseaux des deux sites, assurant ainsi une connectivité fluide et résiliente. Par ailleurs, le NAT sur les interfaces WAN permet de traduire les adresses IP privées en adresses routables sur Internet, renforçant la sécurité de la structure tout en facilitant les échanges externes.

## 

## 3. Services Installés

### 3.1. Services Installés au Siège

Les services déployés sur le site principal sont organisés en fonction des VLAN dédiés, permettant de garantir des niveaux de sécurité et de performance adaptés à chaque fonction :

| **Réseau** | **VLAN** | **Adresse IP** | **Service** |
| --- | --- | --- | --- |
| **ADMIN** | 10 | 172.31.10.10 | Serveur Windows (AD, DNS principal, Proxy) |
| **ADMIN** | 10 | 172.31.10.11 | Serveur Mail (Exchange ou équivalent) |
| **ADMIN** | 10 | 172.31.10.12 | Serveur de fichiers (espaces utilisateurs) |
| **DMZ** | 50 | 172.31.50.10 | Serveur Web public (Apache/Nginx) |
| **DMZ** | 50 | 172.31.50.11 | Réplicat BDD Production |
| **PROD** | 40 | 172.31.40.10 | Serveur principal BDD « production » |
| **WIFI-PERSO** | 60 | 172.31.60.x DHCP | Appareils WiFi personnels sécurisés |
| **WIFI-GUEST** | 70 | 172.31.70.x DHCP | Appareils WiFi invités (accès Internet restreint) |

### 3.2. Services Installés à la Succursale

La succursale intègre des services adaptés à la continuité de l’activité et à la gestion locale du réseau :

| **Réseau** | **VLAN** | **Adresse IP** | **Service** |
| --- | --- | --- | --- |
| **ADMIN** | 10 | 172.32.10.10 | Réplicat DNS (du siège) / DHCP |
| **PROD** | 40 | 172.32.40.10 | Appareils connectés au hall de production |
| **WIFI-PERSO** | 60 | 172.32.60.x DHCP | WiFi personnel sécurisé |
| **WIFI-GUEST** | 70 | 172.32.70.x DHCP | WiFi invité (accès Internet restreint) |

## 

## 4. Détails de la Configuration Réseau des Équipements

Dans cette section, nous décrivons les principaux éléments et choix de configuration appliqués aux routeurs et commutateurs, en expliquant le rôle et les objectifs de chaque bloc de configuration.  
**(Pour des raisons de concision, les configurations détaillées sont consultables en annexe.)**

### 4.1. Configuration des Routeurs (R1 et R2)

#### **a) Activation des Licences et des Fonctionnalités de Sécurité**

**Licence de sécurité** :  
Pour garantir l’utilisation des fonctionnalités avancées (notamment les options liées à la sécurité et au chiffrement), la licence de sécurité est activée sur les équipements via la commande :  
  
license boot module c2900 technology-package securityk9

* Cette étape préliminaire assure que le routeur puisse utiliser les protocoles IPSec et autres fonctionnalités de sécurisation du trafic.

#### **b) Routage Dynamique et OSPF**

* **Mise en place d’OSPF** :  
  Les routeurs (R1 au Siège et R2 à la Succursale) sont configurés pour échanger leurs routes via le protocole OSPF.
  + Les réseaux internes (adressages 172.x.x.x, 10.x.x.x et le sous-réseau GRE 192.168.1.0/30) sont annoncés en OSPF afin de garantir une mise à jour dynamique des routes entre les deux sites.
  + **Log des changements d’adjacence** est activé pour faciliter le suivi et le dépannage.

#### **c) Interfaces LAN et WAN**

* **Interfaces internes (LAN)** :  
  Sur le routeur du siège (R1), deux interfaces LAN (GigabitEthernet0/0 et 0/1) sont configurées avec les adresses IP respectives pour les réseaux « LAN-CORE-1 » et « LAN-CORE-2 ».  
  Ces interfaces incluent la désignation "ip nat inside" pour indiquer que ce trafic sera sujet au NAT.
* **Interface WAN** :  
  L’interface connectée à Internet (GigabitEthernet0/2) reçoit une adresse IP publique (ou semi-publique dans notre simulation) et est marquée comme "ip nat outside".  
  Cette interface est également associée à une carte crypto pour protéger les tunnels GRE par IPSec.

#### **d) Tunnel GRE sur IPsec**

* **Tunnel GRE** :  
  Un tunnel GRE (interface Tunnel0) est mis en place entre R1 et R2 pour assurer une connectivité sécurisée entre les deux sites.
  + L’interface Tunnel0 est configurée avec une adresse IP dans le sous-réseau 192.168.1.0/30.
  + La source et la destination du tunnel sont spécifiées pour pointer respectivement sur les interfaces WAN des deux routeurs.
* **Sécurisation du Tunnel avec IPSec** :
  + Un profil IPSec est défini (via des politiques ISAKMP et des transform-sets) afin de chiffrer le trafic GRE.
  + Une ACL identifie le trafic GRE à protéger, et une crypto-map est appliquée sur l’interface WAN pour assurer que le tunnel bénéficie du chiffrement.

#### **e) Configuration NAT**

* **NAT Overload (PAT)** :  
  L’adresse de sortie du trafic Internet est traduite grâce au NAT Overload.
  + Une ACL (liste 101) est utilisée pour exclure le trafic échangé entre les sites privés, garantissant ainsi que seul le trafic Internet (et non le trafic inter-sites) soit traduit.
  + Le NAT est appliqué sur l’interface WAN pour permettre l’accès à Internet tout en préservant l’adressage interne.

### 4.2. Configuration des Commutateurs

#### **a) Commutateur de Niveau 2 (SW-L2 – Succursale)**

* **Gestion des VLANs et Ports d’Accès** :
  + Les VLANs correspondant aux différents segments (ADMIN, PERSONNEL, VIDÉO, PRODUCTION, DMZ, WIFI\_PERSONNEL et WIFI\_INVITE) sont créés et nommés.
  + Les ports physiques sont configurés en mode accès et assignés aux VLANs respectifs, assurant ainsi la segmentation au niveau L2.
* **Configuration de Trunks** :
  + Deux ports en mode trunk permettent de relier le commutateur SW-L2 aux commutateurs de niveau 3 (SW-L3) pour le transport de l’ensemble des VLANs, garantissant ainsi la continuité du trafic entre les différents segments du réseau.

#### **b) Commutateurs de Niveau 3 (SW-L3-1 et SW-L3-2 – Site A)**

* **Routage Inter-VLAN** :
  + La fonction « ip routing » est activée sur chaque commutateur L3 afin de permettre l’intercommunication entre les VLANs configurés localement.
  + Pour chaque VLAN, une interface de routage (SVI) est créée. Chaque SVI obtient une adresse IP dans son sous-réseau ainsi qu’une adresse de passerelle virtuelle via HSRP pour assurer la redondance.
* **HSRP (Hot Standby Routing Protocol)** :
  + Les interfaces VLAN sont configurées avec des adresses de secours et des priorités différentes entre SW-L3-1 et SW-L3-2, pour garantir la continuité du service en cas de défaillance d’un équipement.
* **Trunks et Interfaces vers le Routeur** :
  + Des interfaces trunk relient les commutateurs entre eux et avec le routeur R1.
  + Des interfaces en mode routé permettent de connecter les commutateurs au routeur, facilitant ainsi l’acheminement du trafic sortant vers le WAN.

#### **c) Sécurisation et Gestion des Accès**

* **Accès SSH et Gestion à Distance** :
  + Chaque équipement dispose d’une configuration pour l’authentification locale (création d’un utilisateur administrateur et génération de clés RSA) qui permet l’accès sécurisé via SSH.
  + Les consoles VTY sont configurées pour n’accepter que le trafic SSH, avec une durée d’inactivité limitée pour renforcer la sécurité.

#### **d) Qualité de Service (QoS)**

* **Application de QoS sur le trafic vidéo** :
  + Une ACL identifiant le trafic vidéo (notamment le flux UDP sur le port 5004) permet de mettre en place une class-map.
  + La policy-map associée, appliquée sur l’interface de sortie vers le WAN, assure une priorité accrue pour le trafic vidéo, garantissant ainsi des performances optimales pour les applications sensibles à la latence.

### 4.3. Configuration du Serveur Windows (Services DHCP, DNS, Mail et Proxy)

#### **a) Configuration de l’Adresse IP**

* Le serveur Windows possède une adresse IP statique (172.31.10.10) avec des IP secondaires (172.31.10.11 pour le service Mail et 172.31.10.12 pour le service Proxy).
* La configuration se fait manuellement via les paramètres réseau du serveur.

#### **b) Installation et Configuration des Rôles**

* **DHCP et DNS** :
  + Les rôles DHCP et DNS sont installés via le Gestionnaire de serveur.
  + Pour chaque VLAN, des étendues spécifiques sont créées afin de gérer l’attribution automatique des adresses IP aux clients.
* **ARR et Proxy** :
  + Le rôle ARR (Application Request Routing) est installé et configuré pour servir de proxy, permettant ainsi la répartition du trafic web et offrant une couche supplémentaire de sécurité et de contrôle.
* **Mail (MailEnable)** :
  + Le service MailEnable est installé pour fournir une messagerie d’entreprise complète.
  + La configuration inclut la création de Post Offices, de boîtes aux lettres et l’intégration avec IIS pour offrir un accès Webmail sécurisé aux utilisateurs.

#### **c) Vérifications et Tests**

* Des tests de connectivité et des vérifications des logs sont réalisés à l’issue de chaque configuration.
* Les outils en ligne de commande (comme *ping*, *ipconfig* et *nslookup*) permettent de valider le bon fonctionnement de chaque service avant la mise en production.