Projet Administration Reseaux

Daouda David Coulibaly/IRIC1

January 5, 2024

Chapter 1

Introduction

L'administration réseau est une composante essentielle de toute infrastructure informatique. Ce rapport documente la configuration détaillée des services réseau sur un serveur Ubuntu, visant à fournir une infrastructure stable et sécurisée.

Chapter 2

Objectifs du Projet

Les objectifs de ce projet comprennent la mise en place et la configuration des protocoles DHCP, DNS, FTP, LDAP, Serveur Web, SSH, SMTP, et la mise en œuvre d'un pare-feu. De plus, nous implémenterons la supervision du réseau avec Nagios pour garantir la disponibilité des services.

Chapter 3

Configuration des Services

3.1 Configuration DHCP

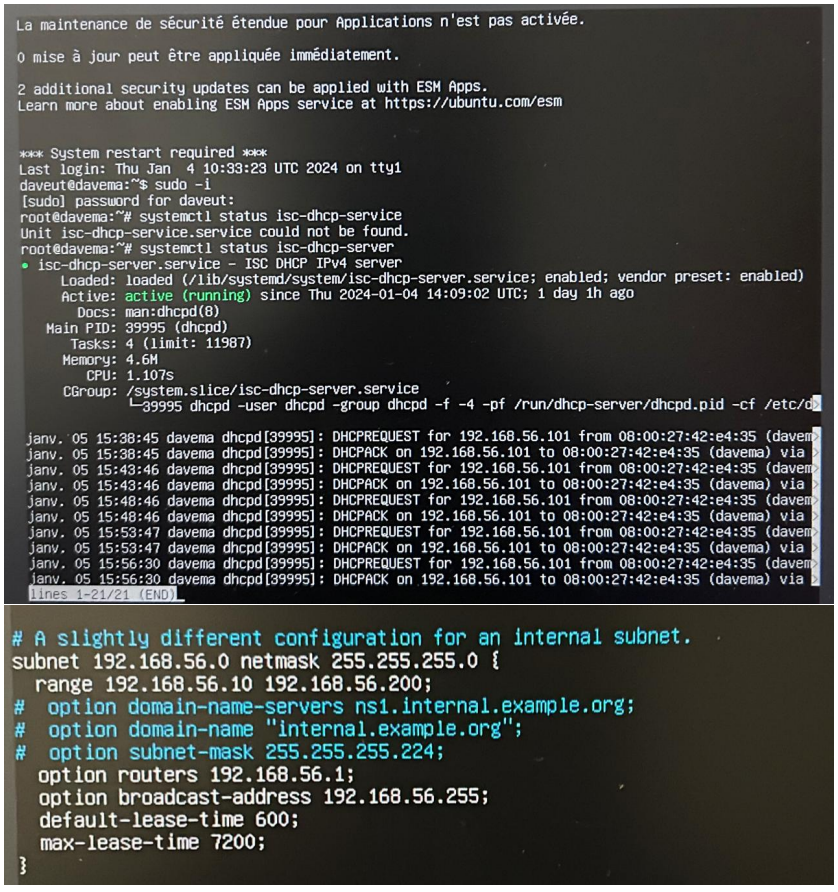

Figure 3.1: Image pour la configuration DHCP

Le protocole DHCP a été configuré pour attribuer dynamiquement des adresses IP aux clients du réseau. Nous avons défini une plage d'adresses et configuré les options spécifiques telles que le masque de sous-réseau et la passerelle par défaut.

3.2 Configuration DNS

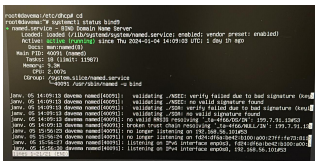

Figure 3.2:

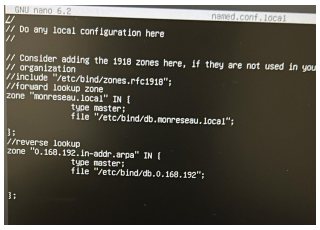

Figure 3.3:

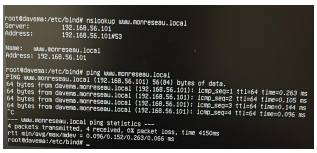

Figure 3.4:

Le serveur DNS a été configuré pour résoudre les noms de domaine dans notre infrastructure. Nous avons défini des zones de recherche directe et inverse, ainsi que les enregistrements A, CNAME et MX nécessaires pour le bon fonctionnement du réseau.

3.3 Configuration FTP

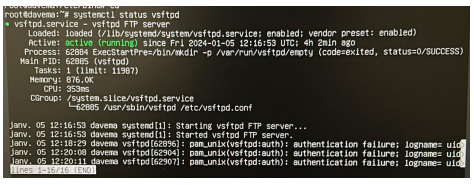

Figure 3.5:

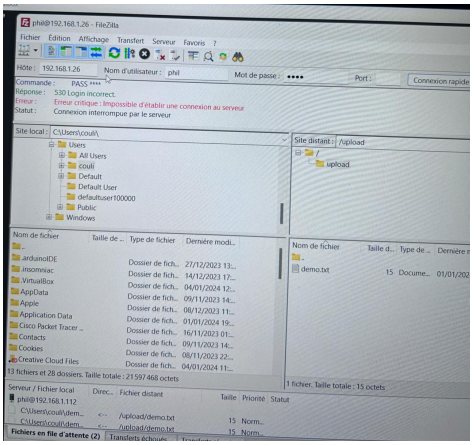

Figure 3.6:

Le serveur FTP a été mis en place pour permettre le transfert de fichiers entre les clients et le serveur. Nous avons configuré des comptes d'utilisateurs,

défini les autorisations d'accès aux répertoires et activé le chiffrement FTP pour renforcer la sécurité des transferts de fichiers.

3.4 Configuration LDAP

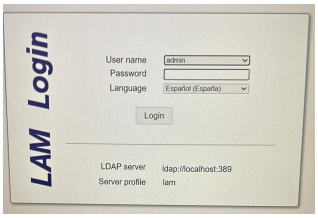

Figure 3.7:

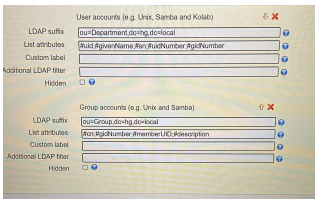

Figure 3.8:

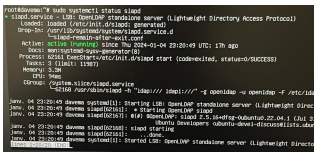

Figure 3.9:

Le serveur LDAP a été configuré pour gérer le répertoire d'annuaire. Nous avons défini les bases DN, configuré les schémas, créé des entrées d'utilisateurs et configuré l'accès sécurisé au serveur LDAP.

3.5 Configuration Serveur web

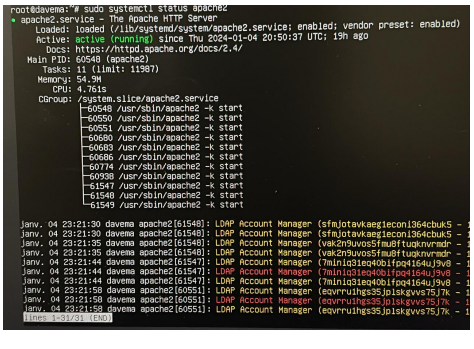

Figure 3.10:

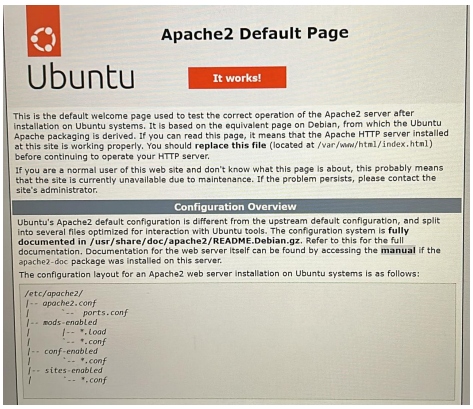

Figure 3.11:

Le serveur web a été configuré pour héberger des sites web. Nous avons défini des hôtes virtuels, configuré SSL/TLS pour le chiffrement, et paramétré les autorisations d'accès aux répertoires pour assurer la sécurité des données.

3.6 Configuration SSH

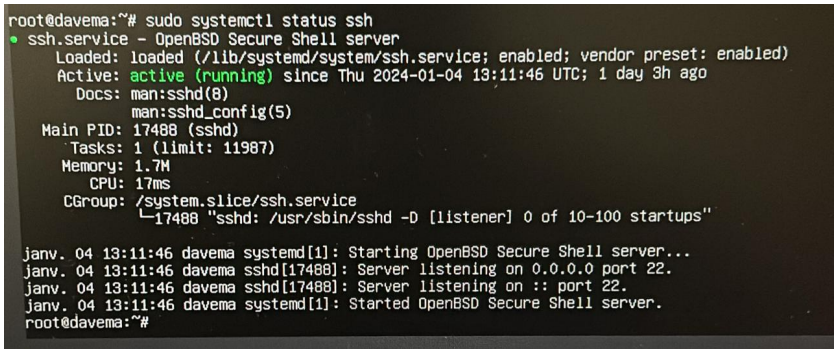

Figure 3.12: Image pour la configuration SSH

Le service SSH a été configuré pour permettre un accès sécurisé au serveur en utilisant des clés publiques/privées. Nous avons désactivé l'authentification par mot de passe, configuré des restrictions d'accès basées sur les adresses IP, et activé le journal d'audit pour surveiller les connexions.

3.7 Configuration SMTP

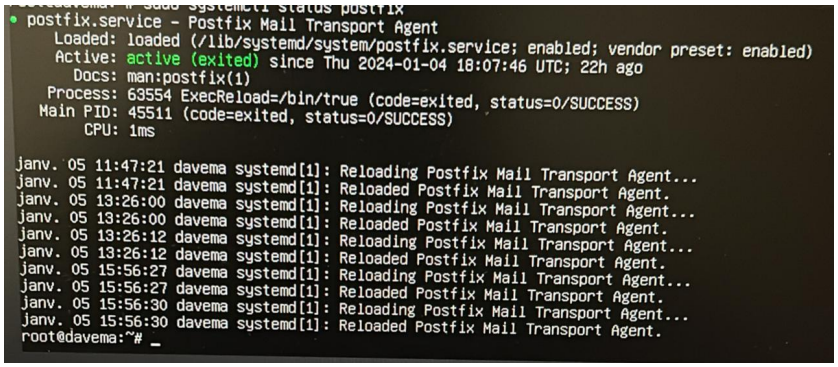

Figure 3.13: Image pour la configuration SMTP

Le serveur SMTP a été configuré pour la gestion des e-mails. Nous avons défini les domaines autorisés à envoyer des e-mails, configuré les enregistrements MX, et activé les fonctionnalités de filtrage pour lutter contre le spam.

3.8 Configuration du Pare-feu

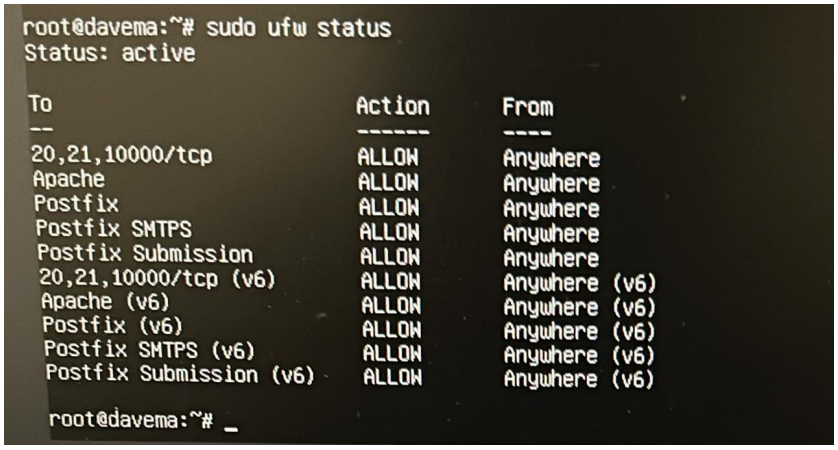

Figure 3.14: Image pour la configuration du Pare-feu

Un pare-feu a été mis en place pour contrôler le trafic réseau. Nous avons configuré des règles pour autoriser ou refuser le trafic en fonction des protocoles, des ports et des adresses IP. Cela renforce la sécurité du serveur en limitant l'accès non autorisé.

3.9 Supervision avec Nagios

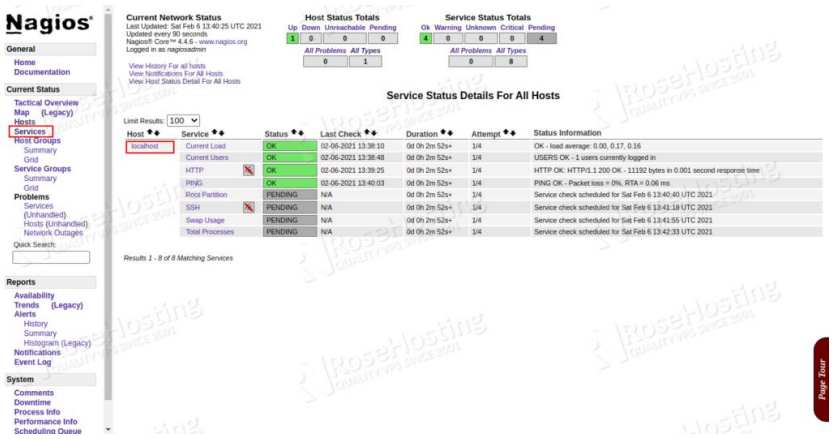

Figure 3.15: Image pour la supervision avec Nagios

Nagios a été déployé pour superviser l'état du réseau. Nous avons configuré des vérifications périodiques des services tels que le serveur web, le serveur

FTP, le serveur LDAP, etc. Les alertes sont générées en cas de défaillance, assurant une réponse rapide aux problèmes potentiels.

Conclusion

Le projet d'administration réseau sur un serveur Ubuntu a abouti à la configuration réussie d'une infrastructure complète, répondant aux besoins variés d'une organisation moderne. Chaque service, du protocole DHCP au serveur LDAP, a été déployé avec une attention minutieuse aux détails, garantissant une gestion robuste et sécurisée du réseau.

La connexion réussie de trois machines clientes a démontré la fonctionnalité opérationnelle de l'infrastructure. Les utilisateurs ont pu bénéficier d'une attribution dynamique d'adresses IP, de la résolution efficace des noms de domaine, du transfert sécurisé de fichiers, de l'accès à un annuaire LDAP, et de la mise en œuvre réussie des protocoles SSH, SMTP, et d'autres services cruciaux.

La surveillance continue avec Nagios a permis de détecter rapidement toute anomalie potentielle, assurant une réactivité optimale face à d'éventuels problèmes de services. Les mécanismes de sécurité, tels que le pare-feu configuré pour contrôler le trafic réseau, ont renforcé la robustesse globale du réseau, minimisant les risques liés à d'éventuelles menaces.

En résumé, ce projet a non seulement atteint ses objectifs en matière de configuration de services réseau, mais il a également établi une fondation solide pour une gestion future. Les connaissances acquises tout au long de ce processus permettront de maintenir et d'évoluer efficacement cette infrastructure réseau, assurant ainsi la continuité des opérations et la sécurité des communications au sein de l'organisation.