



TP :

Dylan CHAU
Lucas DUMONDIN
Rayane OUESLATI

1A-SISR

DOMOTech

Proof Of Concept

Date de création : 04/01/2023

Version : 7.0

Pour validation : DSI

A destination : DSI

Nombre de pages : 153

ESiEE[it]
L'école de l'expertise numérique

Table des matières

Table des matières	2
Métadonnées.....	3
Introduction.....	4
Planification.....	4
I. Le choix des systèmes d'exploitation.....	5
II. Documents utiles DOMOTech.....	6
1. Document d'architecture technique (DAT)	6
2. Configuration de la réplication AD, DNS, DHCP	6
3. Configuration du serveur de fichiers	6
4. Configuration de PFSense.....	6
5. Configuration de VEEAM	7
6. Configuration d'une solution de supervision	7
7. Configuration d'une solution NAS	7
III. Les axes d'amélioration de l'architecture	8
1. Réseaux :.....	8
2. Système :.....	8
IV. Contrôle et suivi.....	10
Cahier de tests	10
1. Infrastructure	10
2. Système.....	10
V. Glossaire	11
VI. Références.....	12
VII. Annexes.....	13

Métadonnées

Diffusion			
Périmètre de diffusion	Contrôlé	Interne	Libre

Historique des évolutions			
Auteur	Version	Objet de la version et liste des modifications	Date
Dylan CHAU	1.0	Initialisation du document	04/01
Dylan CHAU	7.0	Mise à jour	06/06

Validation			
Rédacteur		Valideur	
Nom	Date	Nom	Date
Dylan CHAU	04/01/2023	DSI	04/01/2023
Date d'application : 26/03/2023			

Introduction

La croissance de DOMOTech est telle, que nous devons aujourd'hui revoir entièrement l'infrastructure, afin de l'adapter aux besoins et futures évolutions qu'elle va rencontrer.

Pour cela, notre mission est de proposer et monter une infrastructure type que nous pourrons faire évoluer de façon simple en fonction de l'activité de notre startup, DOMOTech cherche avant tout à mettre une base solide, avant d'évoquer les aspects de scalabilité de l'infrastructure.

Planification

La planification prend tout d'abord en compte :

- Une première partie comprenant le choix des systèmes d'exploitation qui seront utilisés dans l'infrastructure.
- La seconde partie contient le document d'architecture technique avec les informations nécessaires à la compréhension de celle-ci. Le document contiendra une topologie du réseau, la liste des équipements et un plan d'adressage avec la nomenclature des assets. De plus, l'ensemble des documents nécessaires à la mise en place des différentes solutions de l'infrastructure seront présentés.
 - Réplication AD, DNS, DHCP
 - Serveur de fichiers
 - Routeur/firewall PFSense
 - Serveur de sauvegarde VEEAM Backup & Replication
- La troisième partie a pour objectif de préciser les futurs axes d'amélioration envisagés pour DOMOTech.

I. Le choix des systèmes d'exploitation

Windows 10 Enterprise :

Le système d'exploitation sera déployé sur les postes pour les raisons suivantes :

- Existence d'une version LTSC (Long Term Servicing Channel) et du service LTSB (Long Term Servicing Branch)
- La possibilité de rejoindre un nom de domaine
- La gestion de la stratégie de groupe
- Le chiffrement des disques durs avec BitLocker
- L'accès au bureau à distance
- L'accès au Windows Store pour entreprise
- Des facilités de déploiement
- Des outils de sécurité, comme la sécurité des données professionnelles
- La possibilité de centraliser les mises à jour du parc informatique
- Windows Defender ATP
- Microsoft Application Virtualization

Ces options ne sont pas disponibles, voir partiellement, sur les autres versions de Windows 10 (Famille, Education, S, Pro).

Windows Server 2019 Datacenter :

Les serveurs fonctionneront sur ce système d'exploitation. La version 2019 apporte de nombreuses fonctionnalités et a été choisie pour éviter les problèmes de compatibilité que la version 2022, récemment sortie, aurait posé. L'édition Datacenter permettra d'anticiper les besoins futurs de la startup notamment au niveau de la virtualisation.

II. Documents utiles DOMOTech

1. Document d'architecture technique (DAT)

Le DAT aide à comprendre l'infrastructure réseau de l'entreprise et la configuration matérielle. Il décrit en détail l'architecture du réseau, la configuration matérielle, la topologie, les politiques de sécurité et les instructions de configuration. Il est essentiel pour gérer et évoluer le réseau de manière éclairée. **(Annexe 1)**

2. Configuration de la réplication AD, DNS, DHCP

Une procédure détaillée pour mettre en place l'infrastructure, y compris les serveurs et les services associés tels que l'Active Directory (AD), le DNS et le DHCP, est disponible en annexe.

Cette procédure comprend la configuration initiale des serveurs, l'installation des rôles et des fonctionnalités nécessaires, la configuration des paramètres spécifiques. **(Annexe 2)**

3. Configuration du serveur de fichiers

Une procédure détaillée pour mettre en place le serveur de fichiers au sein de l'infrastructure est disponible en annexe. Le serveur de fichiers joue un rôle central dans le stockage et le partage des données au sein de l'entreprise. Sa configuration implique la mise en place des autorisations d'accès, la création de partages de fichiers. **(Annexe 3)**

4. Configuration de PFSense

PFSense est un pare-feu et routeur open-source basé sur FreeBSD, offrant des fonctionnalités avancées pour la gestion et la sécurisation des réseaux.

Nous avons décidé de mettre en place dans notre infrastructure une segmentation réseau via PFSense afin d'en tirer les nombreux avantages :

- Isolation logique : Séparation du trafic réseau et donc limitation de l'accès à certaines données/ressources.
- Gestion améliorée : Améliorer les performances réseaux et la gestion du trafic.
- Sécurité : Mise en place de politique de sécurité en fonction des VMNET.
- Scalabilité : Dans le cadre des futurs projets DOMOTech, la segmentation permettra de réorganiser l'infrastructure sans difficulté.

Vous trouverez une procédure PFSense détaillant sa configuration dans l'infrastructure de DOMOTech. **(Annexe 4)**.

Une matrice de flux de service est également présente et sert à la gestion et l'optimisation de l'infrastructure en fournissant une vue d'ensemble des flux de communication entre ses différents composants. **(Annexe 5)**

Une topologie de l'infrastructure est également fournie afin de faciliter la compréhension de la matrice. **(Annexe 6)**

5. Configuration de VEEAM

VEEAM Backup & Replication est une solution de sauvegarde et de réplication de données complète pour les environnements virtuels et physiques.

Ce document apporte des détails sur la mise en place de VEEAM Backup & Replication dans l'infrastructure DOMOTech. (**Annexe 7**)

Il existe d'autres solutions comme **Windows Backup, Commvault ou Altaro Backup**, cependant nous avons apporté plus de détails sur le choix de VEEAM Backup & Replication pour DOMOTech dans notre document.

6. Configuration d'une solution de supervision

La supervision informatique est aussi appelée monitoring du système informatique et vise à contrôler et à surveiller le système informatique de l'entreprise afin de s'assurer qu'il fonctionne bien. Il a été décidé de mettre en place une solution de supervision pour DOMOTech, vous retrouvez un dossier dans les annexes. (**Annexe 8**)

7. Configuration d'une solution NAS

La configuration d'une solution NAS, ou "Network Attached Storage", consiste à mettre en place un dispositif de stockage en réseau. Il a donc été décidé de mettre en place un NAS pour DOMOTech. Vous retrouverez le dossier dans les annexes. (**Annexe 9**)

III. Les axes d'amélioration de l'architecture

Une future maquette contenant l'ensemble des futures améliorations de DOMOTech a été réalisée. Elle est disponible dans les annexes. **(Annexe 10)**. Vous retrouverez le détail sur cette page.

Pour améliorer l'infrastructure sous ses différents aspects,

Les actions et solutions suivantes pourront être réalisées :

1. Réseaux :

- Mise en place de stack dans les locaux du bâtiment.
- Ajout de bornes Wifi.
- Configuration des différents VLAN pour les services, le serveur d'impression, téléphonie, administration et limiter les domaines de diffusion.
- Connexion des stacks au cœur du réseau par fibre.
- Ajout d'une fibre de backup.

2. Système :

- Configuration dans l'Active Directory des Group Policy Object, Politique de mot de passe.
 - Configuration des stratégies de groupe dans l'Active Directory pour définir des paramètres de sécurité et des restrictions sur les ordinateurs et utilisateurs du réseau.
 - Configuration de la politique de mot de passe pour définir les règles et les exigences de complexité des mots de passe utilisés par les utilisateurs.
- Configuration d'un chiffrement VPN pour accéder au réseau depuis l'extérieur de l'entreprise.
 - Mise en place d'un réseau privé virtuel (VPN) pour permettre aux employés d'accéder de manière sécurisée au réseau de l'entreprise depuis des emplacements externes.
 - Configuration du chiffrement pour protéger les données transitant entre les utilisateurs distants et le réseau interne.
- Un service de Cloud Computing (Azure, AWS)
 - Configuration d'un service de cloud computing pour permettre le stockage, l'accès et le partage de données à partir de ressources informatiques distantes.
 - Cela offre une flexibilité et une évolutivité accrues pour les applications et les services de l'entreprise.
- Un serveur de management
 - Mise en place d'un serveur dédié à la gestion des opérations informatiques et des ressources du réseau.
 - Ce serveur facilite la surveillance, la gestion des correctifs, la gestion des configurations et d'autres tâches de gestion du réseau.
- Un serveur GLPI
- Un serveur de déploiement
- Un serveur Broker
 - Mise en place d'un serveur Broker pour gérer et distribuer les connexions aux serveurs virtuels et aux services de l'entreprise.

- Ce serveur agit comme un intermédiaire entre les utilisateurs finaux et les ressources informatiques, garantissant une répartition équilibrée de la charge et une haute disponibilité.
- Un serveur RDS
 - Configuration d'un serveur RDS (Remote Desktop Services) pour permettre aux utilisateurs d'accéder à distance à des bureaux virtuels ou à des applications publiées.
 - Cela facilite la collaboration et l'accès aux applications depuis différents appareils et emplacements.
- Un serveur de virtualisation
 - Mise en place d'un serveur dédié à la virtualisation pour exécuter des machines virtuelles et consolider les ressources matérielles.
- Ajout d'un certificat SSL à l'Intranet
 - Installation et configuration d'un certificat SSL (Secure Sockets Layer) pour sécuriser les communications entre les clients et les serveurs.
 - Cela garantit que les données sont cryptées et protégées contre les interceptions et les manipulations non autorisées.
- Mise en place d'une DMZ
 - Création d'une zone démilitarisée (DMZ) qui agit comme une zone tampon entre le réseau interne et Internet.
 - Avec Cluster de Serveurs WEB contenant l'Intranet avec équilibreur de charge HAProxy et un serveur de messagerie pour gérer les demandes externes de manière sécurisée.

IV. Contrôle et suivi

Cahier de tests

1. Infrastructure

L'ensemble des tests pour la mise en place de nouvelles fonctionnalités et la migration du périmètre actuel seront réalisés sur Cisco Packet Tracer notamment pour la configuration des VLAN, la mise en place de nouveaux équipements sur l'architecture virtuelle pour les tests.

2. Système

Chaque procédure fournira un cahier de tests permettant de vérifier la nouvelle solution qu'elle permet d'instaurer.

V. Glossaire

- AD DS : Active directory, constituent les fonctions essentielles d'Active Directory pour gérer les utilisateurs et les ordinateurs et pour permettre aux administrateurs système d'organiser les données en hiérarchies logiques.
- Backup : Un serveur de sauvegarde (ou de backup en anglais) est un serveur informatique qui est utilisé pour stocker des copies de données importantes et critiques, en vue de leur récupération en cas de perte, de corruption ou de défaillance du système d'origine.
- DHCP : Dynamic host configuration protocol, est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau.
- DNS : Domaine Name System, est un service informatique distribué qui associe les noms de domaine Internet avec leurs adresses IP
- Firewall : dispositif de sécurité informatique qui est utilisé pour contrôler le trafic réseau entrant et sortant d'un système informatique ou d'un réseau. Le pare-feu sert à bloquer les connexions non autorisées ou les attaques malveillantes provenant d'internet ou d'autres réseaux, en filtrant les paquets de données selon des règles préétablies.
- Job : Tâche de sauvegarde ou de réplication qui spécifie les paramètres de protection de données pour les workloads que vous souhaitez protéger.
- NAS : NAS signifie "Network Attached Storage" en anglais, ce qui se traduit par "stockage en réseau". Il s'agit d'un dispositif de stockage connecté au réseau qui permet le partage de fichiers entre plusieurs utilisateurs et appareils.
- Routeur : dispositif de réseau informatique qui permet de connecter plusieurs réseaux ensemble et de diriger le trafic entre eux.
- Serveur de fichiers : Un serveur de fichiers est un système informatique qui est spécifiquement conçu pour stocker, gérer et partager des fichiers avec d'autres utilisateurs ou clients sur un réseau.
- Supervision informatique : La supervision informatique désigne l'ensemble des ressources déployés pour veiller au bon fonctionnement du système d'information.
- OS : ensemble de programmes qui dirige l'utilisation des ressources d'un ordinateur par des logiciels applicatifs

VI. Références

- OpenClassrooms: <https://openclassrooms.com>
- ESIEE-IT : Cours de système et réseaux
- RDR-IT : <https://rdr-it.com>
- Neptunet : <https://neptunet.fr/>
- Backup :
 - o Documentation VEEAM : <https://www.veeam.com/>
 - o Ports et protocoles VEEAM : <https://helpcenter.veeam.com/docs/backup/vsphere/overview.html>
- Supervision :
 - o www.axido.fr
 - o www.appitel.fr
 - o openclassrooms.com
 - o rdr-it.com/centreon
 - o fr.wikipedia.org
 - o docs.centreon.com
 - o amorri.fr/installation-et-configuration-de-nagios/
 - o www.nagios.com
 - o www.zabbix.com
 - o www.it-connect.fr/configurer-snm-p-sous-windows-server-2012-r2/
- NAS :
 - o www.tech2tech.fr
 - o www.truenas.com/docs/
- SSL :
 - o <https://www.remipoignon.fr/>
 - o <https://www.adminmalin.fr/creer-certificat-auto-signe-openssl/>
 - o <https://www.sslmarket.fr/ssl/help-installation-de-certificat-ssl-sur-le-serveur-apache/>
 - o <https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/reseau/certificat/certificatca>

VII. Annexes

Annexe 1 : Document d'architecture
technique DOMOTech

Nombre de page : 6

Annexe 2 : Configuration Réplication AD DNS DHCP

Nombre de page : 25

Annexe 3 : Configuration Serveur de fichiers

Nombre de page : 20

Annexe 4 : Configuration PFSense DOMOTech

Nombre de page : 15

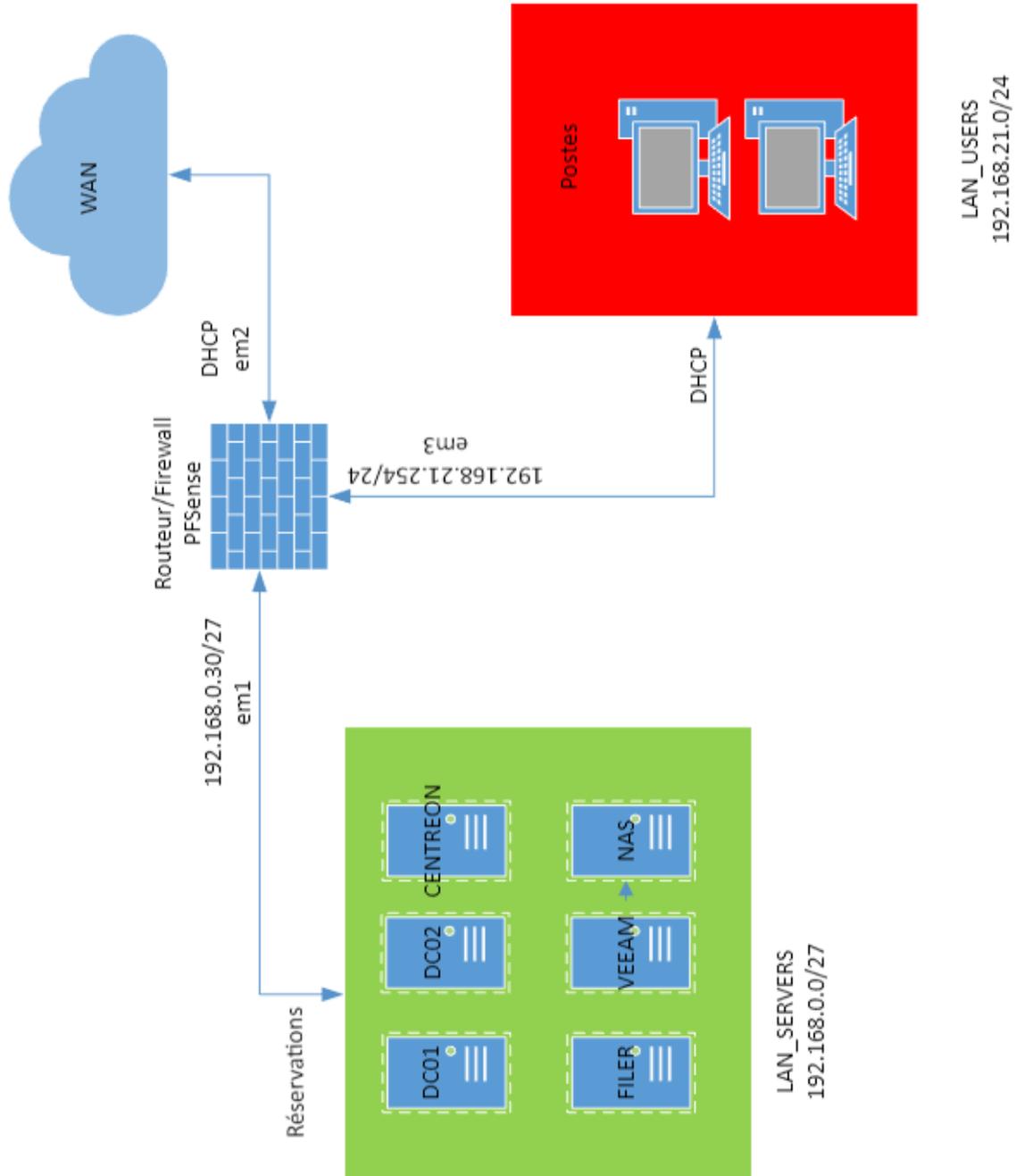
Annexe 5 : Matrice de flux des services

DOMOTech

Nombre de page : 3

Annexe 6 : Topologie de l'infrastructure

Nombre de page : 1



Annexe 7 : Configuration VEEAM DOMOTech

Nombre de page : 15

Annexe 8 : Configuration Centreon SNMP DOMOTech

Nombre de page : 19

Annexe 9 : Configuration NAS DOMOTech

Nombre de page : 23

**Annexe 10 : Topologie de
l'infrastructure avec futurs axes
d'amélioration**

Nombre de page : 1

