|  |  |  |
| --- | --- | --- |
| ***CONTEXTE*** | ⚫ | **DNS Controller** |
| ***SUJET*** | ⚫ | **Mise en service** |
|  |  |  |
| ***référence*** | ⚫ | *340 - dossier d'exploitation.docx* |
| ***version*** | ⚫ | 1.4 |
| ***statut*** | ⚫ |  |
|  |  |  |
| ***créé le*** | ⚫ | *06/06/2024 11:03:00* |
| ***par*** | ⚫ | Julien BONNET |
|  |  |  |
| ***mis à jour le*** | ⚫ | *16/06/2024 17:21:00* |
| ***par*** | ⚫ | Julien BONNET |
|  |  |  |
| ***validé le*** | ⚫ | *16/06/2024 17:21:00* |
| ***par*** | ⚫ |  |
|  |  |  |
| ***diffusé le*** | ⚫ |  |
| ***à*** | ⚫ |  |
|  |  |  |
| *Péremption, archivage et restriction de diffusion*  *Nature de la restriction : confidentiel, diffusion restreinte, diffusion interne, restriction annulée* | ⚫ |  |

|  |
| --- |
| **Table des mises à jour du document** |

|  |  |  |
| --- | --- | --- |
| **version** | **date** | **objet de la mise à jour** |
| 01 | 06/06/2024 | Version initiale |
| 02 | 10/06/2024 | Complétion du document |
| 03 | 16/06/2024 | Finalisation du document |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| **Table des matières** |

[1 Document d'architecture technique (Nom Service concerné) 3](#_Toc169432060)

[1.1 Fonctionnalité et domaine applicatif 3](#_Toc169432061)

[1.2 Architecture matérielle 3](#_Toc169432062)

[1.3 Architecture logicielle 4](#_Toc169432063)

[1.4 Architecture réseau et sécurité 4](#_Toc169432064)

[1.5 Organisation des données 5](#_Toc169432065)

[1.6 Installer Windows Server et activer Hyper-V. 5](#_Toc169432066)

[1.7 Créer les machines virtuelles pour pfSense et Ubuntu Server. 5](#_Toc169432067)

[1.8 Installer pfSense sur la VM dédiée. 5](#_Toc169432068)

[1.9 Installer Ubuntu Server sur la VM dédiée et installer Pi-hole. 5](#_Toc169432069)

[1.9.1 Installation de ubuntu 5](#_Toc169432070)

[1.9.2 Installation de Pihole 5](#_Toc169432071)

[1.10 Configuration 8](#_Toc169432072)

[1.10.1 Configuration de pfSense pour gérer le trafic WAN, LAN, et DMZ. 8](#_Toc169432073)

[1.10.2 Configuration de Pi-hole pour filtrer le DNS et bloquer les publicités. 8](#_Toc169432074)

[1.11 Sources d’informations 8](#_Toc169432075)

# Document d'architecture technique (Nom Service concerné)

## Fonctionnalité et domaine applicatif

|  |  |
| --- | --- |
| Domaine Data Management/aide à la décision |  |
| Domaine Investigation clinique |  |
| Domaine Informatique scientifique |  |
| Domaine Support aux départements |  |
| Domaine Outils collaboratifs et audiovisuels |  |
| Secteur Infrastructure logicielle | X |
| Secteur Infrastructure réseau | X |
| Secteur Ingénierie poste de travail |  |

## Architecture matérielle

Une image contenant texte, diagramme, capture d’écran, Plan

Description générée automatiquement

Figure 1 : schémas D’architecture réseaux

Hyper-V Host : Serveur physique avec Windows Server, Hyper-V activé.

- CPU : 8 Cores

- RAM : 32 GB

- Stockage : 500 GB SSD

* VM PFsense : VM PFsense : Pare-feu et routeur...
  + CPU : 2 Cores
  + RAM : 2 GB
  + Stockage : 20 GB
* VM Ubuntu Server : Serveur DNS avec Pi-hole.
  + CPU : 4 Cores
  + RAM : 4 GB
  + Stockage : 10 GB

## Architecture logicielle

Hyper-V Host : Windows Server avec Hyper-V activé.

VM PFsense : Système d\'exploitation pfSense pour les fonctionnalités de pare-feu et de routage.

VM Ubuntu Server : Ubuntu Server avec Pi-hole installé pour le filtrage DNS.

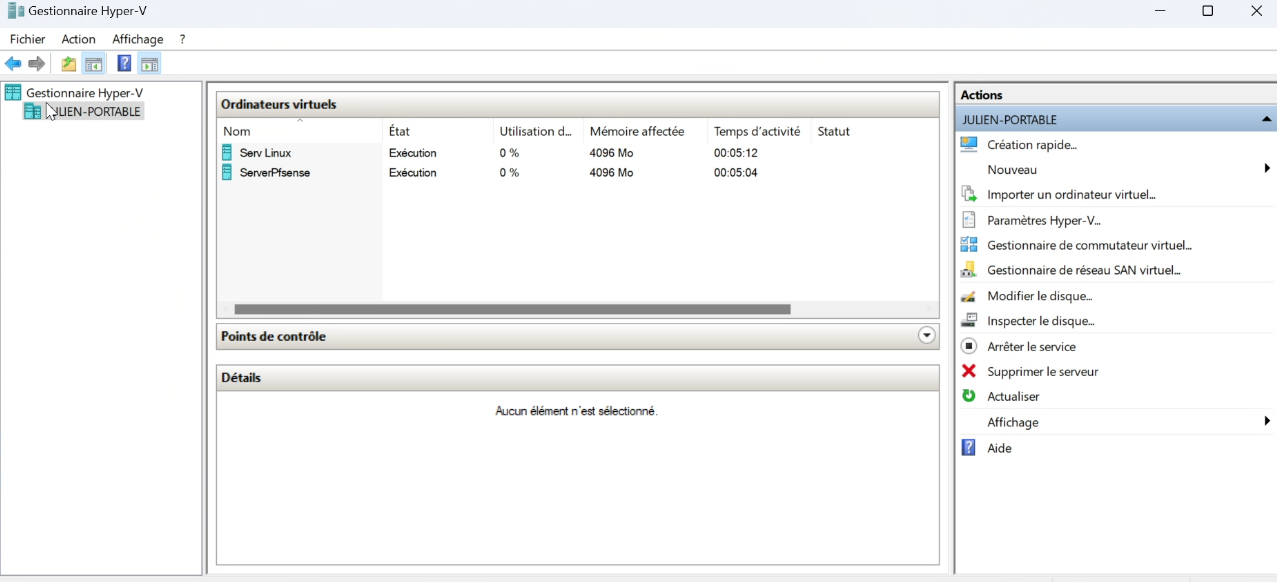


Figure 2 : Composition de l'hyperviseur

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Figure 3 : vue conf Pfsence

## Architecture réseau et sécurité

Réseaux virtuels configurés sur Hyper-V :

- ExternalSwitch : Connecté à l'interface WAN.

- InternalSwitch : Connecté à l'interface LAN.

- DMZSwitch : Utilisé pour la zone DMZ.

Règles de sécurité du pare-feu pfSense :

- Filtrage du trafic entrant et sortant basé sur les règles définies.

- Portail captif pour contrôler l'accès au réseau.

## Organisation des données

Schéma de données :

- pfSense : Configuration et logs stockés localement.

- Pi-hole : Base de données des requêtes DNS et listes de blocage.

## Installer Windows Server et activer Hyper-V.

## Créer les machines virtuelles pour pfSense et Ubuntu Server.

## Installer pfSense sur la VM dédiée.

## Installer Ubuntu Server sur la VM dédiée et installer Pi-hole.

### Installation de ubuntu

### Installation de Pihole

Une fois sur le terminale de la VM ubuntu tapez la commande suivante :



Figure 4 : commande d’installation de PiHole

Une image contenant texte, capture d’écran

Description générée automatiquementL’installation se lance :

Figure 5 : Installation de PIHole

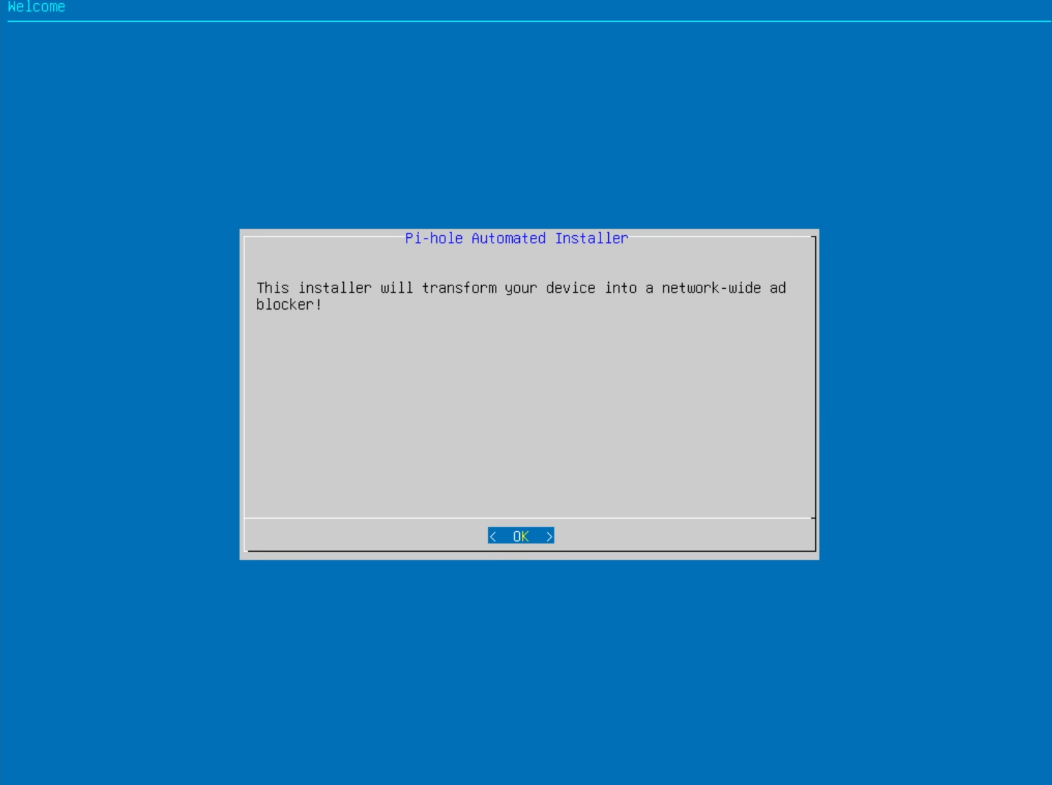
Suivre le SetupWizard de PiHole :

Figure 6 : PiHole Setup Wizzard

Paramétrage de L’ip de la VM ubuntu en mode Static :

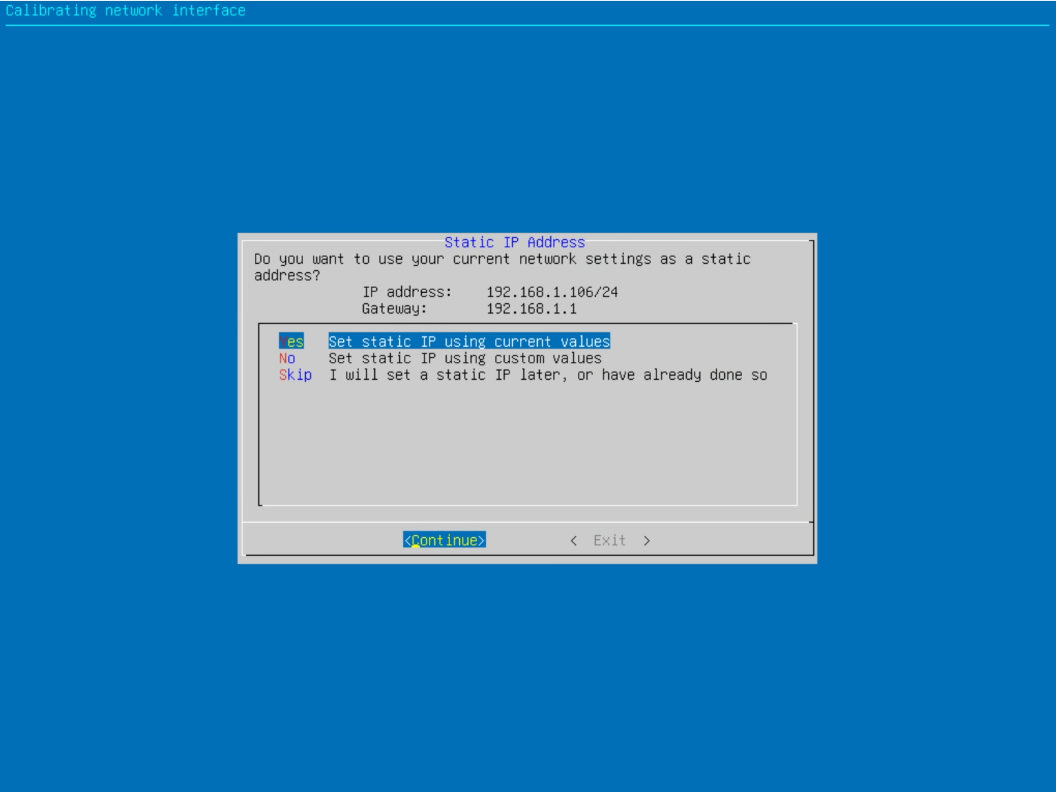


Figure 7 : Configuration IP Statique Server DNS

Acceptez l’installation du WebUI pour configuration du Server DNS :

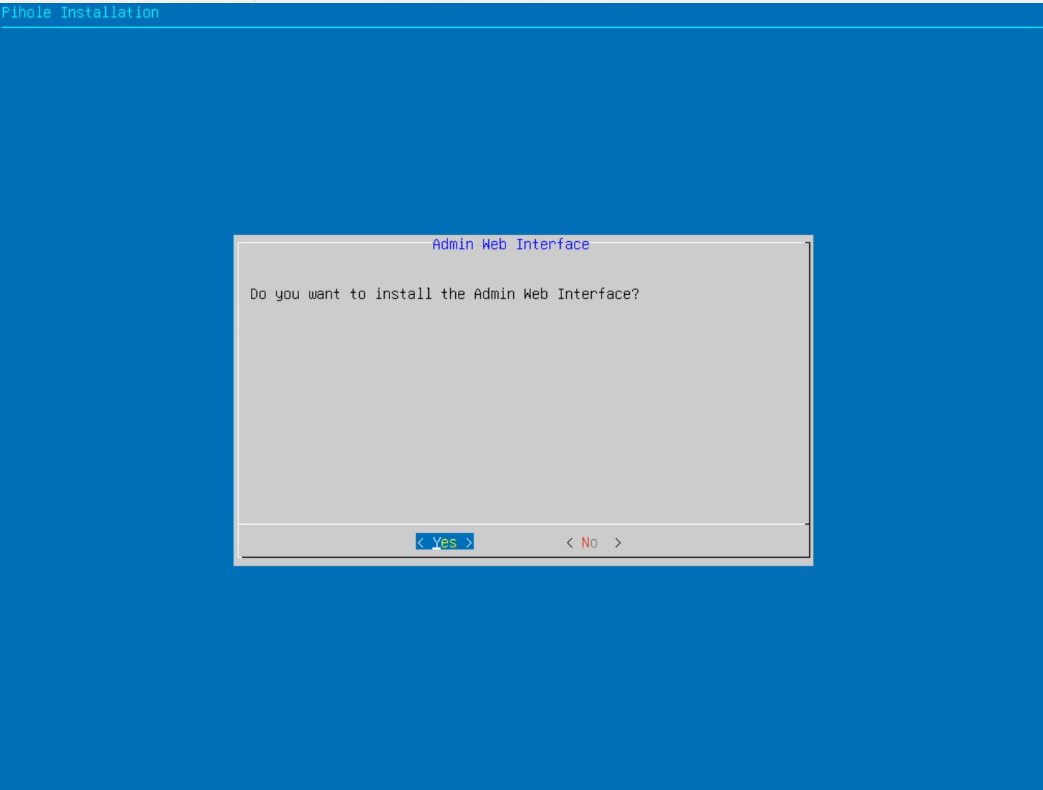


Figure 8 : Installation du WebUI

Étape importante choisir selon la politique de l’entreprise le mode de surveillance des requestes DNS :

Une image contenant texte, capture d’écran, affichage, logiciel

Description générée automatiquement

Figure 9 : Mise à Jour de La Politique de Confidentialité

Enfin resumé de l’installation :



Figure 10 : Résumer de l’installation

Une fois PIhole installer se connecter a l’aide d’un navigateur de la machine physique sur le lien : <http://192.168.0.106/admin/login.php>

Une image contenant capture d’écran, texte, Logiciel multimédia, logiciel

Description générée automatiquement

Figure 11 : Page d’accueil PiHole

## Configuration

### Configuration de pfSense pour gérer le trafic WAN, LAN, et DMZ.

### Configuration de Pi-hole pour filtrer le DNS et bloquer les publicités.

A ce moment le Pihole est accessible sur le réseau LAN de HyperViseur, pour faire sa configuration :

- Par une autre VM quelque soit L’os (os avec navigateur internet ) connecter au réseaux LAN.

- Par la Machine physique car celle-ci garde un accès sur ce réseau privé LAN,

- Par le VPN ; pour ce mode de configuration, il faut avoir déployer un server VPN sur PFsence)

## Sources d’informations

Liens d’information :

- Documentation officielle pfSense : https://docs.netgate.com/pfsense/en/latest/

- Documentation officielle Pi-hole : https://docs.pi-hole.net/