



Pi-hole

CONTEXTE ● **Serveur PiHole**

SUJET ● **Mise en service**

Référence ● xxx - document d'exploitation.docx

Version ● 2

Statut ● Terminé

Créé le ● 06/06/2024 11:36:00

Par ● Julien BONNET

Mis à jour le ● 17/06/2024 21:58:00

Par ● Julien BONNET

Validé le ● 17/06/2024 21:58:00

Par ● Julien BONNET

Diffusé le ● 10/06/2024 17:00:00

À ● Julien LALLEMAND

**Péréemption, archivage
et restriction de
diffusion** ● Diffusion interne

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

Document d'exploitation (Nom Service concerné)	4
1. Supervision	4
1.1. Supervision système	4
1.2. Supervision applicative	4
2. Sauvegardes	4
2.1. Stratégie appliquée	4
2.2. Sauvegardes hebdomadaires	4
3. Restauration	5
3.1. Restauration du système	5
3.2. Restauration des applicatifs	5
3.3. Restauration des données	5
4. Procédure d'arrêt	5
4.1. Ordonnancement et séquençement	5
4.2. Arrêt global et validation	5
4.3. Arrêt spécifique d'une application ou d'un service spécifique	5
5. Procédure de démarrage	6
5.1. Ordonnancement et dépendance	6
5.2. Relance du serveur et des applications	6
6. Tests de bon fonctionnement	6
6.1. Contrôle quotidien des applications	6
6.2. Plan de reboot régulier des serveurs ou composants	6
7. Pilotage des environnements	6
7.1. Logs	6
7.2. Seuils et purges	6
7.3. Traitements et batchs	6
7.4. Gestion des droits applicatifs	6
8. Maintenance et support	7
8.1. Plage de maintenance	7
8.2. Mises à jour	7
9. Niveaux de support	7
9.1. Niveau 1 (standard)	7
9.2. Niveau 2 (critique)	7
9.3. Niveau 3 (très critique)	7
10. Niveaux de service	7
10.1. Niveau de service retenu	7
11. Sécurité	8
11.1. Conformité RGPD	8
11.2. Conformité NIS	8
11.3. Tests d'intrusion	8
11.4. Homologation ISO27001	8
12. Performances	8
12.1. Connexions concurrentes	8
12.2. Temps de réponse attendus	8
12.3. Test de charge	8
13. Support de formation	8

Document d'exploitation (Nom Service concerné)

1. Supervision

1.1. Supervision système

○ Surveillance des Ressources Computatoires:

- Gestion des ressources centrales, notamment la puissance de calcul (CPU) et la mémoire système (RAM).

○ Contrôle de l'Espace Disque:

- Examen périodique de la capacité disponible sur les disques d'ordinateur et l'analyse des taux d'occupation pour prévenir le risque de saturation.

○ Surveillance du Réseau :

- Évaluation constante des délais réseau, débits transferts et erreurs de communication.
- Vérification périodique de la fonctionnalité VPN:
 - a. Authentification et suivi des utilisateurs activant la connexion VPN pour assurer leur statut en ligne correct.

1.2. Supervision applicative

- État de la page d'accueil : vérifier l'accessibilité du WebUI de PiHole et sa réactivité

2. Sauvegardes

2.1. Stratégie appliquée

- Une Adoption d'une politique de sauvegarde complète effectuée quotidiennement pour assurer la conservation des données sans omission et maximiser la récupération après un incident.
- Création de sauvegardes différentielles en temps réel, enregistrant uniquement les changements apportés à chaque session pour maintenir une trace précise des données et faciliter la restauration rapide du système.
- Définition claire des étapes et horaires pour l'exécution des opérations de sauvegarde, avec une recommandation pour effectuer ces tâches dans la nuit pour réduire les interférences avec le fonctionnement quotidien du réseau.

2.2. Sauvegardes hebdomadaires

- Réaliser une sauvegarde totale chaque semaine
- Vérifier l'intégrité des sauvegardes hebdomadaires

3. Restauration

3.1. Restauration du système

- Utiliser l'outil de restauration des snapshots des serveurs via Hyper-V des VM Pfsence et Ubuntu(PiHole).

3.2. Restauration des applicatifs

- Réinstaller PiHole à partir de son WebUI restaurer les configurations à partir des fichiers de sauvegarde

3.3. Restauration des données

- Restaurer les données des utilisateurs à partir des sauvegardes hebdomadaires et journalières

4. Procédure d'arrêt

4.1. Ordonnancement et séquençement

- Informer les utilisateurs de l'arrêt prévu
- Arrêter les services PiHole via le WebUI pour procéder à l'arrêt du serveur puis les services L'arrêté la VM Pfsence via Hyper-V

4.2. Arrêt global et validation

- Confirmer que toutes les VMs ont bien été arrêtés correctement
- Arrêter le l'hyperviseur après validation

4.3. Arrêt spécifique d'une application ou d'un service spécifique

- Arrêter uniquement les services impactés et laisser les autres services opérationnels

5. Procédure de démarrage

5.1. Ordonnancement et dépendance

- Démarrer le serveur
- Relancer l'hyperviseur Hyper-V
- Relancer La VM Ubuntu(PiHole)
- Relanc

5.2. Relance du serveur et des applications

- Vérifier l'accessibilité des Portails Pfsence et PiHole .
- Vérifié le fonctionnement du blocage des pubs

6. Tests de bon fonctionnement

6.1. Contrôle quotidien des applications

- Vérifier l'accessibilité au WebUI Pfsence et PiHole.

6.2. Plan de reboot régulier des serveurs ou composants

- Planifier un redémarrage mensuel pour maintenance

7. Pilotage des environnements

7.1. Logs

- VM d'agrégation et d'analyse des logs (PiHole)

7.2. Seuils et purges

- Définir les seuils d'alerte pour l'espace disque et l'utilisation CPU

7.3. Traitements et batchs

- Planifier des tâches de maintenance automatisées

7.4. Gestion des droits applicatifs

- Profils d'utilisateurs et administrateurs avec droits spécifiques

8. Maintenance et support

8.1. Plage de maintenance

- Maintenance planifiée : chaque dimanche de 02 :00 AM à 04:00 AM

8.2. Mises à jour

- Vérifier les mises à jour sur le site officiel de PiHole et appliquer mensuellement
- Vérifier les mises à jour sur le site officiel de gravité de PiHole et appliquer mensuellement
- Vérifier les mises à jour sur le site officiel de Pfsense et appliquer mensuellement

9. Niveaux de support

9.1. Niveau 1 (standard)

- Plage horaire : 9h00 - 18h00 ; 7j7
- Acteurs : Équipe IT interne
- Actions : Résolution des problèmes basiques et escalade si nécessaire

9.2. Niveau 2 (critique)

- Plage horaire : 9h00 - 18h00 ; 7j7
- Acteurs : Administrateurs systèmes
- Actions : Gestion des incidents majeurs

9.3. Niveau 3 (très critique)

- Plage horaire : 9h00 - 18h00 ; 7j7
- Acteurs : Fournisseur et experts PiHole
- Actions : Résolution des problèmes critiques

10. Niveaux de service

10.1. Niveau de service retenu

Cocher la case correspondante

Standard	
Critique	
Très critique	

11.Sécurité

11.1. Conformité RGPD

Mise en place de politiques de protection des données personnelles et formation des utilisateurs

11.2. Conformité NIS

Sécurisation des réseaux et des systèmes d'information critiques

11.3. Tests d'intrusion

Réalisation de tests réguliers pour identifier et corriger les vulnérabilités

11.4. Homologation ISO27001

Mise en œuvre des meilleures pratiques de sécurité de l'information

12.Performances

12.1. Connexions concurrentes

Supporter jusqu'à 10000 connexions concurrentes

12.2. Temps de réponse attendus

Temps de réponse maximal : 1 secondes

12.3. Test de charge

Réalisation de tests pour vérifier les performances sous charge

13.Support de formation

Liens d'information :

- Documentation officielle pfSense : <https://docs.netgate.com/pfsense/en/latest/>
- Documentation officielle PiHole : <https://docs.pi-hole.net/>