Département du Système d'Information

CONTEXTE	●	**Serveur Wazu**
SUJET	●	**Mise en service**
Référence	●	*xxx - document d'exploitation.docx*
Version	●	2
Statut	●	En cour de rédaction
Créé le	●	*06/06/2024 11:36:00*
Par	●	*ISMAILI Yanisse*
Mis à jour le	●	*17/06/2024 21:40:00*
Par	●	*ISMAILI Yanisse*
Validé le	●	*En cour*
Par	●	Julien LALLEMAND
Diffusé le	●	*17/06/2024*
À	●	Julien LALLEMAND
Péremption, 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	16/06/2024	Version final
03	17/06/2024	Version corrigée

Table des matières

Document d'exploitation

1. Supervision

1.1. Supervision système

- Processus : surveiller l'utilisation des ressources (CPU, RAM)
- Espace disque : vérifier régulièrement l'espace disponible et les taux d'occupation
- Réseau : surveiller la latence, les débits et les erreurs réseau

1.2. Supervision applicative

Accessibilité des services : Vérifier l'accessibilité et la réactivité des services applicatifs.

2. Sauvegardes

2.1. Stratégie appliquée

- Une sauvegarde totale : une fois par semaine
- Une sauvegarde différentielle : une fois par jour
- Heure des sauvegardes : Programmée à 02:00 AM.

2.2. Sauvegardes journalières

- Automatisation : Utiliser un script automatisé pour réaliser les sauvegardes différentielles.
- Stockage : Stocker les sauvegardes sur un serveur dédié avec redondance

2.3. Sauvegardes hebdomadaires

- Intégrité des sauvegardes : Vérifier l'intégrité des sauvegardes hebdomadaires

3. Restauration

3.1. Restauration du système

Outil de restauration : Utiliser l' outil de restauration de l'image du serveur pour remettre en état le système.

3.2. Restauration des applicatifs

Réinstallation : Réinstaller les applications et restaurer les configurations à partir des fichiers de sauvegarde

3.3. Restauration des données

Données utilisateurs : Restaurer les données des utilisateurs à partir des sauvegardes hebdomadaires et journalières

4. Procédure d'arrêt

4.1. Ordonnancement et séquencement

- Informer les utilisateurs de l'arrêt prévu
- Arrêter les services de manière ordonnée pour éviter toute perte de données

4.2. Arrêt global et validation

- Validation : Confirmer que tous les services ont été arrêtés correctement
- Arrêt du serveur : Arrêter le serveur après validation

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

Arrêter ciblé : Arrêter uniquement les services impactés et laisser les autres services opérationnels

5. Procédure de démarrage

5.1. Ordonnancement et dépendance

- Démarrage du serveur : Démarrer le serveur
- Relance des serveur :Relancer les services réseau, puis les services applicatifs.

5.2. Relance du serveur et des applications

Vérification : Vérifier l'intégrité des services après redémarrage

5.3. Relance d’une application ou d'un service spécifique

Démarrage ciblé : Démarrer uniquement les services nécessaires

6. Tests de bon fonctionnement

6.1. Contrôle quotidien des applications

Accessibilité : Vérifier l'accessibilité des applications et des services

6.2. Plan de reboot régulier des serveurs ou composants

Planification : Planifier un redémarrage mensuel pour maintenance

7. Pilotage des environnements

7.1. Logs

Agrégation et analyse : Utiliser un outil comme Grafana pour l'agrégation et l'analyse des logs.

7.2. Seuils et purges

Seuils d’alerte : Définir les seuils d'alerte pour l'espace disque et l'utilisation CPU

7.3. Traitements et batchs

Tâches automatisées : Planifier des tâches de maintenance automatisées

7.4. Gestion des droits applicatifs

Profils d'utilisateurs : Définir des profils d’utilisateurs et administrateurs avec droits spécifiques

8. Maintenance et support

8.1. Plage de maintenance

Heures de maintenance : Maintenance planifiée chaque dimanche de 01 :00 AM à 03:00 AM

8.2. Mises à jour

Vérification et application : Vérifier les mises à jour sur le site officiel de wazuh et appliquer mensuellement

8.3. Contrats

Contrat de support : Contrat de support avec le fournisseur et le mainteneur du serveur physique

8.4. Licences

Conformité des Licence de wazuh : wazuh et un logiciel open source

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 wazuh
- Actions : Résolution des problèmes critiques

10. Niveaux de service

10.1. Niveau de service retenu

Cocher la case correspondante

Standard	
Critique	X
Très critique	

11. Sécurité

11.1. Conformité RGPD

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

11.2. Conformité NIS

Sécurisation des réseaux : Sécurisation des réseaux et des systèmes d'information critiques

11.3. Tests d'intrusion

Tests réguliers : Réalisation de tests réguliers pour identifier et corriger les vulnérabilités

11.4. Homologation ISO27001

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

12. Performances

12.1. Connexions concurrentes

Support : Supporter jusqu'à 40 connexions concurrentes

12.2. Temps de réponse attendus

Réponse : Temps de réponse maximal : 2 secondes

12.3. Test de charge

Tests de performance : Réalisation de tests pour vérifier les performances sous charge

13. Support de formation

Guide d'utilisation : https://documentation.wazuh.com/current/index.html

https://learn.microsoft.com/fr-fr/windows-server/

Ce document doit fournir une base solide pour déployer et gérer une infrastructure de supervision avec Wazuh et Windows Server, ainsi que pour la formation et le support des utilisateurs. N'hésitez pas à ajouter des détails spécifiques à votre environnement ou des captures d'écran pour plus de clarté. Si vous avez besoin de sections supplémentaires ou de précisions, faites-le moi savoir !