LOGO ENTREPRISE

Département du Système d'Information

CONTEXTE ● **Monitoring serveur web ubuntu**

SUJET ● **Mise en service**

référence	●	*xxx - dossier d'exploitation.docx*
version	●	1.1
statut	●	
créé le	●	*1/11/2020 11:03:00*
par	●	Edgar Cavaillez
mis à jour le	●	*17/06/2024 14:56:00*
par	●	Edgar Cavaillez
validé le	●	*17/06/2024 14:56:00*
par	●	En attente de confirmation
diffusé le	●	*16/06/2024*
à	●	18h30
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	16/06/2024	Version initiale

Table des matières

1 Document d'exploitation (Nom Service concerné)

1.1 Supervision

1.1.1 Supervision système

Utilisation de **Netdata** pour la surveillance en temps réel des ressources système (CPU, mémoire, réseau ect).

On a aussi une configuration des alertes pour les seuils critiques.

1.1.2 Supervision applicative

Mise en place de surveillance des services Nginx et SSH.

Utilisation de scripts personnalisés pour vérifier la disponibilité et les performances des services.

1.2 Sauvegardes

1.2.1 Stratégie appliquée

Sauvegardes quotidiennes du répertoire web et des configurations.

Utilisation de **rsync** pour synchroniser les fichiers vers un serveur de sauvegarde distant.

1.2.2 Sauvegardes journalières

Planification des sauvegardes avec **cron** pour une exécution automatique chaque nuit.

1.2.3 Sauvegardes hebdomadaires

Les sauvegardes complètes hebdomadaires sont stockées sur un serveur de sauvegarde distant pour garantir une rétention à long terme et une sécurité optimale

1.3 Restauration

1.3.1 Restauration du système

Procédures pour restaurer le serveur Ubuntu à partir d'une sauvegarde complète en cas de panne.

1.3.2 Restauration des applicatifs

Restauration des services Nginx et des configurations Netdata.

1.3.3 Restauration des données

Utilisation de **rsync** pour restaurer les fichiers web et les données de sauvegarde.

1.4 Procédure d’arrêt

1.4.1 Ordonnancement et séquencement

Arrêt des services non critiques en premier, suivi par les services critiques (Nginx, SSH).

1.4.2 Arrêt global et validation

Utilisation de scripts pour arrêter proprement tous les services et valider l'arrêt complet du système.

1.4.3 Arrêt spécifique d’une application ou d'un service spécifique

Commandes spécifiques pour arrêter Nginx et Netdata sans affecter les autres services.

1.5 Procédure de démarrage

1.5.1 Ordonnancement et dépendance

Démarrage des services critiques en premier (SSH), suivi par Nginx et Netdata.

1.5.2 Relance du serveur et des applications

Redémarrage du serveur.

Démarrage automatique des services via systemd.

Vérification des logs pour s'assurer que tous les services démarrent correctement.

1.5.3 Relance d’une application ou d'un service spécifique

Commandes spécifiques pour démarrer ou redémarrer Nginx et Netdata..

1.6 Tests de bon fonctionnement

1.6.1 Contrôle quotidien des applications

Vérification quotidienne de l'état des services et des ressources système via Netdata.

1.6.2 Plan de reboot régulier des serveurs ou composants

Reboot planifié des serveurs tous les mois pour maintenir la performance et appliquer les mises à jour critiques..

1.7 Pilotage des environnements

1.7.1 Logs

Collecte et analyse des logs de Nginx, SSH et Netdata pour détecter les anomalies.

1.7.2 Seuils et purges

Configuration des seuils d'alerte dans Netdata.

Scripts pour purger les logs anciens et libérer de l'espace disque.

1.7.3 Traitements et batchs

Utilisation de **cron** pour planifier les tâches de maintenance et les sauvegardes régulières.

1.7.4 Gestion des droits applicatifs

Permissions : Utilisation des commandes chmod et chown pour gérer les permissions des fichiers web et des configurations système.

1.8 Maintenance et support

1.8.1 Plage de maintenance

Création de fenêtres de maintenance régulières pour appliquer les mises à jour et effectuer des vérifications approfondies.

1.8.2 Mises à jour

Application régulière des mises à jour de sécurité pour Ubuntu, Nginx, et autres logiciels installés.

1.8.3 Contrats

Gestion des contrats de support pour le matériel et les logiciels utilisés.

1.8.4 Licences

Type de licences : Utilisation de logiciels open-source (Ubuntu, Nginx, Netdata, rsync) sous licence GPL, MIT ou similaire.

Emplacement : Les licences sont stockées dans les répertoires d'installation des logiciels.

Implémentation : Assurer la conformité en lisant et suivant les termes des licences lors de l'installation et de l'utilisation des logiciels.

1.9 Niveaux de support

1.9.1 Niveau 1

1.9.1.1 PLAGE HORAIRE

Support de niveau 1 disponible de 8h à 18h, du lundi au vendredi.

1.9.1.2 ACTEURS

Support qui assure la démarche et permet de nous diriger vers le niveau 2.

Contact : support@entreprise.com

1.9.1.3 ACTIONS REALISEES

Résolution des problèmes courants (accès, mots de passe).

Escalade des problèmes complexes vers le niveau 2..

1.9.2 Niveau 2

1.9.2.1 PLAGE HORAIRE

Support de niveau 2 disponible de 9h à 18h, du lundi au vendredi.

1.9.2.2 ACTEURS

Support assuré par des techniciens spécialisés.

Contact : tech@entreprise.com / Ext. 102.

1.9.2.3 ACTIONS REALISEES

Résolution des problèmes complexes (performances, configuration).

Escalade des problèmes critiques vers le niveau 3.

Retour vers le niveau 1 après résolution.

1.9.3 Niveau 3

1.9.3.1 PLAGE HORAIRE

Support de niveau 3 disponible 24/7.

1.9.3.2 ACTEURS

Support assuré par des experts système.

Contact : expert@entreprise.com

.

1.9.3.3 ACTIONS REALISEES

Gestion des incidents critiques et des défaillances système.

Résolution des problèmes nécessitant une expertise approfondie.

Retour vers les niveaux 1 et 2 après résolution.

1.10 Sécurité

1.10.1 Conformité RGPD

Mesures prises pour assurer la conformité avec le RGPD, y compris la gestion des données personnelles.

1.10.2 Conformité NIS

Conformité avec la directive NIS pour la sécurité des réseaux et des systèmes d'information..

1.10.3 Tests d'intrusion

Réalisation de tests d'intrusion réguliers pour identifier et corriger les vulnérabilités.

1.10.4 Homologation ISO27001

Certification ISO27001 pour garantir la sécurité des informations et des systèmes.

1.11 Performances

1.11.1 Connexions concurrentes

Le service doit supporter jusqu'à 500 connexions simultanées sans dégradation des performances.

1.11.2 Temps de réponse attendus

Temps de réponse moyen attendu pour le serveur web est de 200 ms.

Temps de réponse pour les applications critiques ne doit pas dépasser 500 ms.

1.11.3 Test de charge

Procédure : Réalisation de tests de charge avec des outils comme JMeter pour simuler jusqu'à 500 utilisateurs simultanés.

Résultats attendus : Maintien des temps de réponse sous les seuils définis et stabilité du système.

1.12 Support de formation

Matériel fourni : Manuels utilisateur, tutoriels vidéo, et ateliers pratiques adaptés aux différents niveaux de compétence des utilisateurs.

Accès : Disponibilité des supports de formation en ligne et lors de sessions de formation en personne.