**Etude des Besoins – Load Balancer**

1. **Identification des Parties Prenantes**

* Responsables des processus Métier : Administrateur Système et Réseau– KONTE Amara
* Responsables Informatique : Directeur Cybersécurité – GOMIS Kwency
* Utilisateur : Equipe Informatique.

1. **Collecte des Exigences**

***Disponibilité - Le système d'information doit être disponible 99,9% du temps***

*Quels sont les services, systèmes ou données critiques pour l’organisation ?*

* *Serveur : odyshap01p ; odyshap02p*
* *Réseaux : 001-int-prd-odys*
* *Données : Configuration des Serveurs.*

*Quels sont les conséquences d’une perte de disponibilité ?*

*Assurer que le serveur de load-balancing est toujours disponible pour répartir la charge entre les serveurs backend*

***Intégrité - Assurer l'intégrité des données sensibles***

*Quels sont les processus et les données qui doivent être protégés contre toute altération non autorisée ?*

*Les données de configuration doivent être protégées.*

*Comment garantir l'intégrité des données pendant leur stockage, leur transmission et leur traitement ?*

*Mises à jour régulières et surveillance continue des performances pour détecter tout comportement anormal.*

***Confidentialité - Garantir la confidentialité des informations clients***

*Quelles informations sont considérées comme sensibles ou confidentielles ?*

*Adresses IP des serveurs backend, Protocoles de communication (HTTP, HTTPS, TCP, UDP, etc.), Port d'écoute du load balancer, Algorithmes d'équilibrage de charge utilisés.*

*Comment assurer la confidentialité des données contre l'accès non autorisé ?*

*Le chiffrement des communications avec le serveur de load balancing et la gestion sécurisée des informations d'authentification et des clés privées utilisées pour les connexions sécurisées.*

***Preuve - Mettre en place des mécanismes de preuve pour les transactions critiques***

*Quelles sont les exigences en matière de préservation des preuves numériques ?*

*Avoir l’historiques des opérations effectuées par le serveur. (Ex : Trafic entrant et sortant)*

*Comment garantir l'intégrité et l'authenticité des preuves numériques en cas d’incident ?*

*Grâce à l’historique protégé et conservé pendant 5 ans.*

*Choix de notre DICP et Criticité au vu de notre besoin :*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Disponibilité** | **Intégrité** | **Confidentialité** | **Preuve** | **Criticité** |
| 03 - Fort | 02 - Significatif | 02 - Significatif | 02 - Significatif | 01 - Non critique |

1. **Évaluation des Ressources**

Voici les ressources disponibles :

* *Equipe Informatique*
* Serveurs : odyshap01p ; odyshap02p
* Réseaux : 001-int-prd-odys
* *Financières :* **Installation initiale d'un Load Balancer :**
  + Pour un load balancer matériel dédié : Entre 5 000 et 20 000 euros.
  + Pour un load balancer logiciel : Entre 2 000 et 10 000 euros.
* **Coûts annuels de maintenance et de support :**
  + Entre 10% et 20% du coût initial d'achat.

1. **Conformité Réglementaire**
2. *Minimisation des données : Assurez-vous que le load balancer ne collecte et ne traite que les données strictement nécessaires à sa fonction principale. Évitez la collecte ou le traitement de données personnelles inutiles.*
3. *Finalité du traitement : La collecte et le traitement des données par le load balancer doivent être alignés avec une finalité légitime et spécifique. En général, le load balancer ne devrait pas traiter de données personnelles, mais plutôt s'occuper de la gestion du trafic réseau.*
4. *Sécurité : Mettez en place des mesures de sécurité adéquates pour protéger le load balancer contre tout accès non autorisé ou toute utilisation abusive. Cela peut inclure des mécanismes de chiffrement, des restrictions d'accès, etc.*
5. *Durée de conservation : Minimisez la durée de conservation des données sur le load balancer. Les données temporaires nécessaires au fonctionnement du load balancer doivent être effacées dès qu'elles ne sont plus nécessaires.*
6. *Traçabilité : Assurez-vous que les activités du load balancer sont tracées de manière appropriée, mais évitez autant que possible la collecte de données de journalisation qui pourraient contenir des informations personnelles identifiables.*
7. *Analyse d'impact sur la protection des données (AIPD) : Si le load balancer est impliqué dans le traitement de données personnelles à grande échelle ou est susceptible de présenter un risque élevé pour les droits et libertés des personnes, une Analyse d'impact sur la protection des données peut être nécessaire.*
8. *Contrats avec les sous-traitants : Si le load balancer est fourni par un tiers (sous-traitant), assurez-vous que des contrats appropriés sont en place pour garantir la conformité au RGPD et définir les responsabilités de chaque partie.*
9. *Notification des violations de données : Si le load balancer est compromis et qu'une violation de données survient, vous pourriez être tenu de notifier cette violation aux autorités de contrôle et, dans certains cas, aux personnes concernées.*
10. **Elaboration d’un Cahier des Charges**

**NGINX Plus :**

1. Préparation de la machine virtuelle :

- Créez une machine virtuelle avec les spécifications nécessaires (RAM, CPU, espace disque) et le système d'exploitation compatible avec NGINX Plus.

2. Téléchargement de NGINX Plus :

- Obtenez la version de NGINX Plus auprès de la source officielle (via le site NGINX ou leur fournisseur) et téléchargez le package.

3. Installation :

- Suivez les instructions spécifiques au système d'exploitation pour installer NGINX Plus.

- Configurez les paramètres de base comme les ports, les certificats SSL si nécessaire.

4. Configuration du Load Balancing :

- Utilisez la documentation de NGINX Plus pour configurer le load balancing en définissant les serveurs backend, les règles de répartition de charge, etc.

5. Test et Validation :

- Vérifiez la configuration en testant le load balancing avec des requêtes HTTP ou des simulations de trafic.

- Assurez-vous que le load balancing fonctionne comme prévu.

**HAProxy :**

1. Préparation de la machine virtuelle :

- Créez une machine virtuelle avec les spécifications requises et un système d'exploitation compatible avec HAProxy.

2. Installation de HAProxy :

- Installez HAProxy sur la machine virtuelle en suivant les instructions spécifiques à votre système d'exploitation.

3. Configuration du Load Balancing :

- Éditez le fichier de configuration de HAProxy pour définir les serveurs backend, les algorithmes de répartition de charge, les règles de routage, etc.

4. Vérification et Redémarrage :

- Vérifiez la syntaxe de la configuration HAProxy pour éviter les erreurs.

- Redémarrez HAProxy pour appliquer les nouvelles configurations.

5. Surveillance et Maintenance :

- Configurez des outils de surveillance pour suivre les performances du load balancer et effectuer des ajustements si nécessaire.