Rapport d’intervention suite à incident

Service concerné : service informatique

Début incident : 05/11/2021

Clôture de l’incident :05/112021

Résumé du traitement de l’incident :

À la suite de la perte du disque dur, on a eu une alerte que notre site web n’est plus opérationnel, donc on a restauré le dernier backup dans une nouvelle machine virtuelle qui nous a permis de rendre le service fonctionnel.

Table des matières

I - Détection de l’incident :

L’équipe de monitoring ont configuré des systèmes pour surveiller, détecter, hiérarchiser et analyser proactivement les incidents prioritaires, dans le but de reconnaître toute menace ou activité anormale et suspecte dans l’environnement réseau, susceptible de perturber le flux de travail.

Une alerte mail reçu informant que le site web ne réponds plus ainsi qu’une alerte informant que le serveur web ne réponds plus non plus au ping

II - Détail du déroulé des opérations :

Les opérations se sont déroulées dans l’ordre suivant :

1. Test de connexion manuelle sur le site par le lien : le site ne répond pas
2. Essai de se connecter sur le serveur en ssh le serveur ne réponds plus
3. Mettre des downtime dans Nagios pour les services monitoré pour acquitter l’alerte
4. Connection direct sur le serveur aucun disque n’est détecté
5. Après identification du problème du disque, Réinstallation d’une machine virtuelle avec le même nom et @IP
6. Exécution du script de restauration qui inclut l’installation des services WordPress et Mysql, création et sécurisation de la base de données mysql et finalement restauration du site et de la base à partir de la sauvegarde de la veille.
7. Vérification de la bonne exécution du site
8. Réactiver le monitoring

III - Impact sur le(s) service(s) :

La panne a rendu le service complètement indisponible puisque le serveur repose sur la disponibilité du seul disque dur existant

IV - Préconisations d'améliorations :

IV.1 - Amélioration de la détection d'incident :

L'équipe de monitoring doit travailler davantage sur la gestion des problèmes.

Changer les indicateurs des sondes pour ne pas tomber dans la catastrophe

Ajouter une sonde qui vérifie l'état de santé du disque dur (taux d'erreur en lecture, taux d'erreur d'accès aux têtes, température, nombre de secteurs réallouées, secteurs défectueux, etc) permettant d'anticiper la dégradation totale de disque

IV.2 - Réduction du risque :

Mise en place d'un raid de disque pour tolérer au moins la perte d'un disque sans arrêt du service et permettre le changement du disque corrompu.

IV.3 - Amélioration de la résolution d'incident :

Création d'un script qui permet de :

- Recréer une machine virtuelle (en configurant le volume, la ram, le nombre de core désiré...)
- Faire au script de restauration.