Offres infogérance - Serveur web
Prérequis relatifs au Serveur

Version du 03/12/2022

Dans un souci de standardisation de nos procédures et du suivi de vos serveurs, nous avons besoin de déployer des machines avec certaines caractéristiques communes.

Nous pourrons prendre en charge votre serveur dans le cadre de l'offre d'infogérance **uniquement s'il répond aux caractéristiques ci-dessous et qu'il est configuré par nos soins**.

De plus, vous trouverez en deuxième partie le détail des éléments que nous mettrons en place sur votre machine lors de sa configuration initiale, ainsi que les opérations effectuées chaque mois lors de la phase de maintenance.

Prérequis (à fournir par vos soins)

Pour que nous puissions mettre en place l'infogérance, nous avons besoin d'un **serveur nu fraichement installé sous Debian** dans sa dernière version stable (https://www.debian.org/releases/index.fr.html).

Si votre serveur est physique, **nous vous conseillons fortement de mettre en place un RAID**. Le type de RAID sera à déterminer selon les caractéristiques de la machine, n'hésitez pas à en discuter avec nous avant toute installation.

Si possible, vous trouverez ci-dessous le partitionnement que nous préconisons pour un serveur d'hébergement web.

Partition	Type	Système de fichiers	Taille en Mo
/	Primaire	ext4	Tout le reste
/var/log	Logique	ext4	10000
/tmp	Logique	ext4	10000
SWAP	Logique	Swap	2048

Une fois la machine en place suivant ces recommandations, nous avons besoin d'un accès SSH complet pour que nous puissions effectuer la configuration initiale et lancer l'infogérance.

Configuration initiale (effectué par nos équipes à réception du serveur)

Lors de la réception de la machine, nous installons les éléments nécessaires à sa surveillance, sa sécurisation et à l'hébergement de votre site web.

Voici la liste de ces éléments pour notre configuration standard de serveur web, celle-ci pourra être adaptée selon vos besoins spécifiques.

- Changement du mot de passe « root » par une suite aléatoire de 30 caractères
- Mise en place d'un nouvel utilisateur de connexion SSH avec mot de passe aléatoire de 30 caractères
- Interdiction du compte « root » pour les futures connexions SSH

- Modification du port SSH pour éviter les attaques automatisées (peu dangereuses, mais alourdissant inutilement les logs)
- Mise en place de mails d'alerte nous prévenant instantanément de toute connexion root au serveur
- Mise en place d'un pare-feu configuré de façon strict. Celui-ci filtrera tout type de connexion par défaut en entrée et en sortie. Seuls les ports strictement utiles à l'usage du serveur seront ouverts en exclusion un en un.
  En général, dans le cas d'un serveur web Ping, 80, 443 et SSH en entrée – 22, 53, 123, 80, 443, 67, 68, 25, 587 en sortie.
  Ce pare-feu sera automatiquement lancé au démarrage du serveur via un script systemd.
- Mise en place d'un anti force brute (fail2ban) sur les services avec authentification ouverts en entrée.
  Dans le cas d'un serveur web, surveillance de SSH et HTTP. Configuration stricte avec bannissement définitif de toute IP échouant 6 tentatives d'authentification.
- Service NTP pour conserver le serveur à l'heure
- Installation et configuration de NGINX (serveur HTTP) associé à PHP-FPM pour gérer l'exécution du site web
- Installation et configuration de MariaDB pour gérer la base de données du site web
- Mise en place pour chaque site web d'un utilisateur dédié (Debian et MariaDB), d'un vhost, d'un pool PHP-FPM et d'une base de données
- Mise en place d'un certificat SSL pour chaque site web (**à fournir par vos soins**, sauf dérogation lors du devis)

Maintenance mensuelle (effectuée par nos équipes une fois par mois)

Une fois le serveur correctement configuré et sécurisé, nous effectuons chaque mois des opérations de maintenance préventive pour assurer son bon fonctionnement.

Voici la liste des opérations effectuées chaque mois :

- Mise à jour de tous les paquets Debian
- Nettoyage des paquets inutilisés et de leurs fichiers de configuration
- Vérification de l'état du RAID (si présent sur votre machine)
- Vérification des disques sur les serveurs physiques (espace disponible et état SMART)
- Vérification des services systemd
- Vérification du bon fonctionnement de l'anti brute (fail2ban)
- Vérification des services actifs sur la machine
- Scan complet des ports (1 à 3000) de la machine depuis un serveur externe pour vérifier le bon fonctionnement du pare-feu

Un rapport mensuel au format PDF vous sera remis chaque mois pour vous signaler tout problème qui serait repéré lors de ces opérations de maintenance.

Événements non prévus

En dehors de ces opérations préventives, nous effectuons une surveillance continue de votre serveur chaque jour.

Celui-ci sera pingé par nos serveurs chaque minute pour vérifier sa disponibilité. Nous recevrons de plus les mails de monitoring du serveur directement sur une boite mail dédiée (connexion root, bannissement fail2ban).

En cas d'incident détecté, nous interviendrons directement si vous disposez d'heures d'interventions réservées. Dans le cas contraire, nous vous avertirons pour que vous puissiez prendre les mesures appropriées.