Offres infogérance - Serveur web
Prérequis relatifs au Serveur

À la date du 14/03/2025

Dans un souci de standardisation de nos procédures et du suivi de vos serveurs, nous avons besoin de déployer des machines présentant 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 dans la deuxième partie le détail des éléments que nous installerons sur votre machine lors de sa configuration initiale, ainsi que les opérations effectuées chaque mois durant 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, fraîchement installé sous **Debian dans sa dernière version stable** (https://www.debian.org/releases/index.fr.html). Dans le cas où, pour certaines raisons, vous souhaiteriez un système d'exploitation différent, cela est éventuellement possible. Contactez-nous pour déterminer la faisabilité.

Si votre serveur est physique (Bare Metal), **il est impératif de mettre en place un système RAID**. Le type de RAID à utiliser dépendra des caractéristiques de votre 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. Ce partitionnement pourra, bien sûr, être simplifié sur les petits VPS avec peu d'espace disque.

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	Égal à la RAM

Une fois la machine en place selon ces recommandations, nous aurons besoin d'un accès SSH complet (root) afin de pouvoir effectuer la configuration initiale et lancer l'infogérance.

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

Lors de la réception de la machine, nous installons les éléments nécessaires à sa surveillance, sa sécurisation ainsi qu'à l'hébergement de vos sites web.

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

- Service NTP pour conserver le serveur à l'heure.
- Changement du mot de passe « root » par une suite aléatoire de 30 caractères.
- Mise en place d'un nouvel utilisateur de connexion SSH avec un mot de passe aléatoire de 30 caractères.
- Interdiction de l'utilisation du compte « root » pour les futures connexions SSH.
- Modification du port SSH afin d'éviter les attaques automatisées. Il est également possible, pour une sécurité renforcée, de filtrer l'accès SSH par IP si votre société est en mesure de fournir une adresse IP fixe ou si vous n'avez pas besoin d'accéder aux sites web par SFTP.
- Mise en place de courriels d'alerte nous prévenant instantanément de toute connexion root au serveur.
- Mise en place d'un pare-feu configuré de façon stricte. Celui-ci filtrera tout type de connexion par défaut en entrée. Seuls les ports strictement utiles à l'usage du serveur seront ouverts, un par un.
  En général, dans le cas d'un serveur web, les ports Ping, 80, 443 et SSH seront ouverts en entrée. Ce pare-feu sera automatiquement lancé au démarrage du serveur.
- Mise en place d'un système 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 de toute IP échouant après 6 tentatives d'authentification.
- 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 socket PHP-FPM et d'une base de données. Pour une sécurité maximale, chaque site web sera isolé grâce à ces éléments dédiés et à un chroot SFTP.
- Mise en place d'un certificat SSL pour chaque site web (Let's Encrypt ou fourni par vos soins, sauf dérogation mentionnée dans le devis).

Une fois l'installation terminée, nous vous enverrons tous les identifiants d'accès à votre serveur fraîchement configuré. Nous accordons une très grande importance à ce que nos clients soient maîtres de leurs données et de leur matériel : il est donc primordial à nos yeux que vous soyez en possession de tous ces accès.

Évidemment, en cas de souscription à un contrat de maintenance, nous vous demandons de ne pas modifier ces identifiants ou la configuration du serveur sans nous consulter, afin de ne pas entraver notre prestation.

Ces identifiants vous seront envoyés de manière sécurisée via un lien chiffré avec une durée de validité limitée. En cas de perte de ces identifiants, vous pouvez bien sûr nous demander à tout moment de vous les fournir de nouveau ; nous vous enverrons alors un nouveau lien chiffré.

Maintenance (lancée à la fin de configuration du serveur).

Une fois le serveur correctement configuré et sécurisé, nous mettons en place :

Un monitoring vérifiant la disponibilité de votre serveur chaque minute.
Notre système de monitoring nous prévient en cas d'échec à contacter votre serveur à cinq reprises.
En cas d'incident détecté, nous intervenons pour déterminer l'origine du problème. Si celui-ci est lié à la configuration de votre serveur, nous effectuons les correctifs nécessaires. Si l'incident est lié à l'hébergeur ou à une panne de votre machine, nous vérifions que l'hébergeur a bien détecté la panne et programmé sa résolution.
Si votre intervention est nécessaire ou si la panne engendre une forte indisponibilité, nous vous contactons pour que vous puissiez prendre les dispositions nécessaires.

Un script de sauvegarde automatique.
Celui-ci compresse les données importantes de votre serveur chaque nuit pour les envoyer sur un espace de

sauvegarde. Cet espace de sauvegarde est ensuite répliqué automatiquement dans 3 datacenters différents en France pour assurer un maximum de résiliance en cas d'incident. Nous conservons 7 sauvegardes quotidiennes et 6 archives mensuelles.

En plus de la surveillance et des sauvegardes, nous effectuons manuellement chaque mois des opérations de maintenance préventive afin de garantir le parfait fonctionnement de votre serveur.

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 (état SMART).
- Vérification de l'espace disponible sur les partitions.
- Vérification du bon fonctionnement de l'anti-brute-force (fail2ban).
- Vérification des services actifs sur la machine.
- Vérification du fonctionnement du pare-feu (scan complet des ports de votre serveur depuis une machine distante).
- Vérification des logs d'erreur.
- Vérification de la bonne exécution des sauvegardes et de l'espace disponible dans votre espace de sauvegarde.

Un rapport mensuel au format PDF vous sera remis chaque mois pour faire le bilan des éventuels incidents de monitoring et vous informer des opérations effectuées ainsi que des résultats de nos vérifications mensuelles.

Événements non prévus

En cas d'incident, nous interviendrons directement si vous disposez de temps d'intervention réservé.

N'hésitez pas à nous contacter par e-mail en cas de dysfonctionnement à l'adresse ci-dessous :

maintenance@conobium.com