

Formation Nginx : serveur web, proxy inverse, WAF

Durée :	3 jours
Public :	Administrateurs systèmes Linux
Pré-requis :	Administration système Linux
Objectifs :	Maîtriser nginx, du serveur web au WAF, en passant par le reverse proxy
Sanction :	Attestation de fin de stage mentionnant le résultat des acquis
Taux de retour à l'emploi:	Aucune donnée disponible
Référence:	LIN988-F
Note de satisfaction des participants:	4,89 / 5

Introduction

- Présentation de nginx
- Historique et versions
- Modèle économique, nginx plus
- Écosystème, modules et packages

Le protocole HTTP

- Rappel du fonctionnement du protocole
- Fonctionnement de TLS/HTTPS : problèmes de l'hébergement multiple
- Introduction à SPDY et HTTP/2
- Détail du protocole pour appréhender la configuration

Configuration de nginx en serveur Web

- Fichier de configuration global
- Directives et configuration du cœur
- Définition des racines
- Fonctionnement des hôtes virtuels (vhosts)
- Réécriture d'adresse
- Configuration des logs
- Mise en place de HTTPS, avec vhosts (SNI, wildcard, etc.)

Atelier pratique : installation et configuration de nginx, création de plusieurs vhosts

Nginx : serveur proxy inverse

- Présentation des modes de fonctionnement : HTTP FastCGI, uwsgi, SCGI, memcached
- Détail du du reverse proxy HTTP
- Détail du reverse proxy FastCGI

Détail de uwsgi

Utilisation spécifique en tant que serveur de cache

Atelier pratique : mise en place d'un reverse proxy pour un serveur Tomcat, utilisation de PHP-FPM pour exploiter FastCGI avec PHP, mise en place d'un cache transparent pour du contenu statique HTTP

Au delà du proxy : le répartiteur de charge

Load balancing simple : serveurs multiples

Surveillance des serveurs de backend, pondération

Terminaison SSL et décharge (offloading)

Reconfiguration à chaud, détection de modifications DNS

Atelier pratique : mise en place d'un loadbalancer avec nginx, avec détection active des pannes et pondération, mise en place d'un offloader SSL.

Nginx : utilisation comme Web Application Firewall

Introduction à la sécurité des applications web

Comparaison des différents types d'attaque

Limitation du périmètre d'attaque de l'applicatif par la configuration

Mise en place de Naxsi

Utilisation de nxcutil et génération des listes blanches

Présentation rapide et utilisation d'un profil Fail2Ban pour naxsi

Atelier pratique : Configuration de nginx pour protéger une application PHP, installation et configuration de naxsi, apprentissage de règle sur un CMS