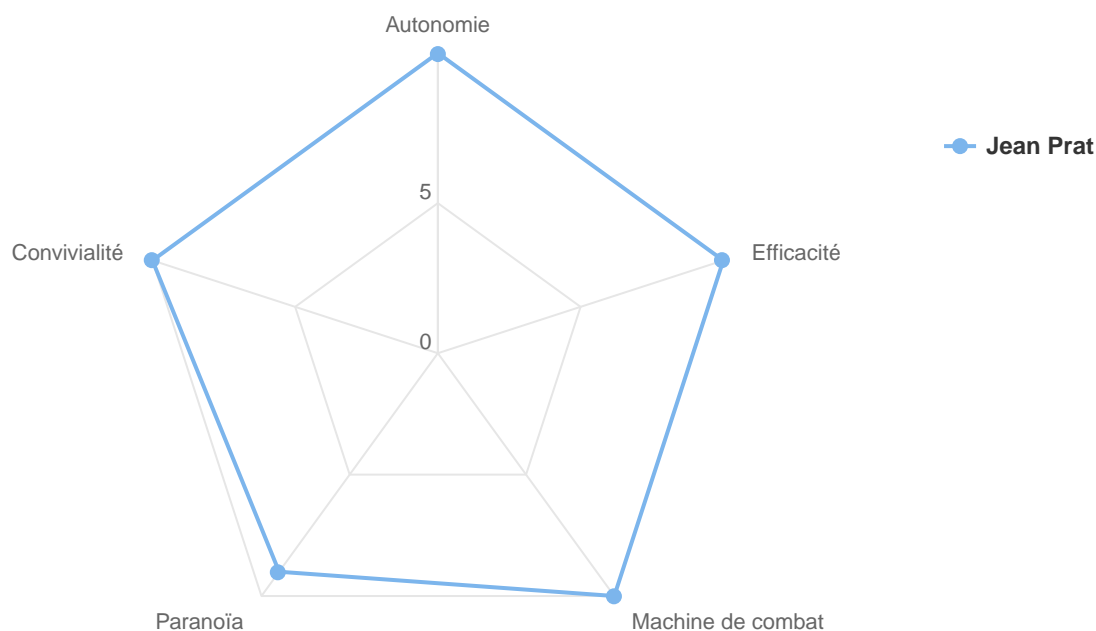


# Expert système et réseau

Jean Prat



## A Propos

Ayant beaucoup pratiqué l'autoformation durant mes 14 années d'expérience et l'écoute des personnes expérimentées autour de moi, autodidacte sur beaucoup de domaines, je me suis constitué une base de connaissance au fil des ans.

Ceci m'a permis de faire reconnaître mes compétences et de pouvoir mettre en avant mon expertise dans la gestion d'incidents et la vision technique.

J'ai commencé à travailler sur les environnements Unix en tant qu'administrateur SAP en 2004 pour devenir aujourd'hui administrateur système et réseaux avec un fort apport en matière de sécurité. Je travaille aujourd'hui essentiellement sur Linux, des logiciels Open Source ainsi que des équipements réseaux.

Autonome, je sais aller chercher l'information où elle est précise et faire preuve de réactivité afin de m'adapter aux situations complexes autant techniques qu'humaines.

J'ai réussi à m'insérer efficacement dans le cycle de développement, en combinant ceci à ma réactivité, j'ai pu ne jamais mettre en retard ou bloquer la livraison d'applications. Aujourd'hui je travaille en accord avec les développeurs et ceux ci me consultent sur les contraintes techniques.

J'ai pour projet de passer la certification OSCP.

## Experience

# **Depuis 2013 - Orange Applications for Business**

## **Responsable architecture système et réseau des plateformes de paiement, mise en sécurité et support Niveau 3**

Administrateur sur près de 200 machines et 70 équipements réseaux :

- En charge de la construction, sécurisation, administration et mise en conformité PCI-DSS. Participation aux audits, définition des plans de remédiation :
  - Réseau sur l'ensemble des plateformes OAB PCI-DSS (Service de carte bleue virtuelle, boutiques web, ...)
  - Système et réseau de la plateforme de paiement par CB de la boutique orange.fr et divers grands comptes.
- En charge de la sécurisation, le design et l'administration des plateformes de paiement :
  - saisie IBAN et leur tokenisation des boutiques sosh.fr et orange.fr.
  - Serveurs de paiement CB via code court sur le réseau mobile SS7 Orange France

Réalisations :

- Interventions sur des portails à forte affluence, impliquant des opérations HNO, des études et solutions de diminution des arrêts de services.
- Mise à l'actualité de plateformes vieillissantes, implémentant une meilleure sécurité et une meilleure disponibilité.
- Que ce soit dans un projet de modernisation ou un départ à zéro, j'ai une autonomie complète.
- Développement par les tests de rôles Ansible et mise en oeuvre d'une intégration continue des rôles Ansible.
- Utilisation de lynis pour effectuer un scoring CIS.
- Mise en oeuvre d'un système de livraison continu compatible PCI-DSS via Gitlab-CI, Ansible et AWX.
- Mise en oeuvre d'un cloud privé à base de RHVM (KVM+QEMU sous libvirt) allant du choix du matériel réseau et serveurs à son installation, en passant par la sécurisation de l'infrastructure et l'automatisation du provisionning sous Ansible.
- Passage d'une architecture mono site à un multi site actif-actif pour le paiement CB orange.fr :  
les mises à jour des applications et systèmes se font maintenant en heure de bureau.
- Préparation des audits PCI-DSS et pentests.
- Réduction des temps de mise à jour des cluster de Pare feux et passage des upgrades sans interruption.
- Création d'indicateurs de bench, audit et optimisation des performance allant des aspects physiques des serveurs aux applicatifs tels que MySQL ou Apache.
- Mise à niveau à l'aide de puppet de l'infrastructure tri site hébergeant les services Orange utilisateurs finaux afin de mettre à jour l'ensemble des composants, améliorer la gestion du tri-site en refaisant la répartition des appels afin ne plus avoir de coupure de service.

- Refonte et automatisation de l'installation avec Ansible de l'infrastructure des Serveurs Vocaux pour passer sur VOIP, en bi site actif-actif, pour des services hébergeant des numéros tels que l'horloge parlante, Télérhôn ou bien des numéros surtaxés passant à la télévision.

Passage de 2 jours pour l'installation d'un serveur à 12 serveurs installés en 2 jours.

Systèmes : Linux

BDD : MySQL/MariaDB, Elasticsearch

HA : HA-Proxy, Keepalived, Corosync

Virtualisation : RHVM/Ovirt, libvirt, docker, vagrant

Automatisation/Intégration continue : Ansible, Puppet, Gitlab-CI, Ansible AWX

Réseau : Pare feux Cisco ASA, Juniper, Stormshield et Switchs Cisco, H3C et Procurve

Divers : Snort, Rsyslog, Logstash, Kibana, Grafana

## 2007-2013 - Cheops Technology France

## Responsable supervision

Responsable de la supervision de plus de 2000 équipements et support N3 :

- Support H24, administration, audit et optimisation par compétences :
  - Unix/Linux
  - Oracle
  - MySQL
  - SAP
  - Réseau
- Incident Manager de 2008 à 2010.

Réalisations :

- Nous avons monté un service infogérance partant de zéro pour des clients allant du géant de la cosmétique à des cliniques en passant par des sites de e-commerce à forte affluence.
- Certification Hebergeur de données de santé.
- Mise en place d'une plateforme redondante et multisite de supervision sous Nagios.
- Mise en oeuvre PRA/PCA multi site (Load balancing, geoDNS, boot on SAN, Réplication BDD)
- Administration Réseau en environnement cloud privé et mutualisé.
- Adaptation des outils à l'aide de PHP, MySQL et javascript, dont la création d'une interface de communication Nagios/GLPI.
- Développement des processus métiers et application de la méthodologie ITIL :
  - Mise en oeuvre d'une CMDB et d'un outil de gestion des SLA et incidents à base de GLPI et OCS inventory
  - Mise en oeuvre d'un outil de documentation sous mediawiki et conception des templates de pages.
  - Rédaction des procédures d'exploitation, d'incidents et des documents d'architecture.
  - Contrôle des liens entre les alarmes de supervision et procédures d'incidents.
- Construction d'un système de gestion des logs ELK intégrant plus de 2000 messages par secondes.

Systèmes : Linux, HP-UX

BDD : Oracle, MySQL, Elasticsearch

HA : Citrix Netscaler, Redhat cluster suite

ERP : SAP ECC6/ECC5/47/46/40B, SAP BW 7.0

Supervision : Nagios, Thruck, Cacti, PNP4Nagios, Icinga, Gearmand, SNMP

Virtualisation : VMware Vsphere, HyperV

Réseau : Pare feux Fortinet, NetAsq, Cisco PIX et Switchs H3C et Procurve. HP IMC

Sauvegarde : Dataprotector, Symantec Backup Exec, TINA.

## 2004 - 2007 - Arexia SAS

### Administrateur SAP

En charge de l'administration SAP, Oracle et Unix :

- Gestion des remontées de bug logiciel SAP.
- Mise en place et gestion des stratégies de sauvegarde.
- Gestion, intervention et résolution des incidents matériels et logiciels.
- Développement de programmes réduisant les temps des taches quotidiennes.

Systèmes : HP-UX, Linux, FreeBSD

BDD : Oracle, MySQL

ERP : SAP 47/46/40B, SAP BW 7.0

Sauvegarde : Dataprotector

## Sur mon temps personnel

La base de mes scripts ansible pour installer des serveurs sécurisés a été faite hors de mon temps de travail : [Github](#)

Cette publication est un partage de ce que je fais chez moi, bien sur, ce que j'utilise dans mon travail a été repensé pour un travail collaboratif.

Je maintiens des paquets archlinux soit sur [l'AUR](#) soit sur github : [Nominatif](#) ou [Anonyme](#)

J'ai testé des technologies comme l'OCR, la vision par ordinateur ou bien la reconnaissance vocale. Ces essais sont disponible sur mon [github](#).

## Formation

- 2016 - EC-Council Certified Ethical Hacker v8
- 2013 - MySQL Tuning
- 2004 - BTS Informatique de gestion, Pau (64)
- 2002 - Baccalauréat S, Lesparre (33)

## Langues

Anglais Technique