Protéger son serveur

Pratiques, astuces et outils

DEVCOMP

Speaker

- Marc Audefroy
- @MarcAudefroy
- Développeur passionné
- Padawan Agiliste
- Padawan Devops

DEVCAMP

Les points clés

- Super utilisateur
- Protéger l'accès
- Se prémunir des rootkits
- Antivirus
- Audit
- Monitoring
- Backup

DEVCAMP

Un grand pouvoir implique de grandes responsabilités

- Ne JAMAIS se connecter en root
- Utiliser sudo
- Deux méthodes
  - Élévation complète
  - Choix des commandes via sudoers

DEVCAMP

- https://wiki.debian.org/fr/sudo
- http://guide.andesi.org/html/ksudo.html
- http://homeserver-diy.net/wiki/index.php?title=Sudo,_premi%C3%A8re_approche_du_super_utilisateur
- http://blog.seboss666.info/2014/05/installer-et-utiliser-sudo-sur-debian

Vous ne passerez pas!

DEVCAMP

SSH

- apt-get install ssh
- Astuces :
  - Changer port 22
  - Restreindre les adresses IP/ utilisateurs
  - Authentification via clé publique/privée
  - Utiliser un agent ssh pour le passphrase

DEVCOMP

http://www.linux-france.org/prj/edu/archinet/systeme/ch13s03.html

Fail2Ban

- apt-get install fail2ban
- Analyse les logs et déclenche des actions
- Attaque brute-force SSH
- Attaque DDOS
- Scan des ports
- Notification par mail

DEVCAMP

http://blog.nicolargo.com/2012/02/proteger-son-serveur-en-utilisant-fail2ban.html
http://www.fail2ban.org/wiki/index.php/MANUAL_0_8

Firewall

- Configurer Netfilter
- Iptables
- Shorewall
- Nftables
- Bloquer tout par défault, autoriser le reste

DEVCAMP

iptable : http://doc.ubuntu-fr.org/iptables
shorewall : http://doc.ubuntu-fr.org/shorewall
Nftables :
http://linuxfr.org/news/nftables-successeur-diptables
https://home.regit.org/netfilter-en/nftables-quick-howto/

Rootkits

- Outils de dissimulation d'activité
- Anti-Rootkit : compare les hashs
- Rkhunter
- Chkrootkit
- Tips : Méfiez-vous des faux positifs

DEVCAMP

rkhunter : http://www.sublimigeek.fr/installer-paquet-rkhunter-debian
chkrootkit : http://doc.ubuntu-fr.org/rootkit

Antivirus

- Clamav
- Maldet

DEVCAMP

Audit

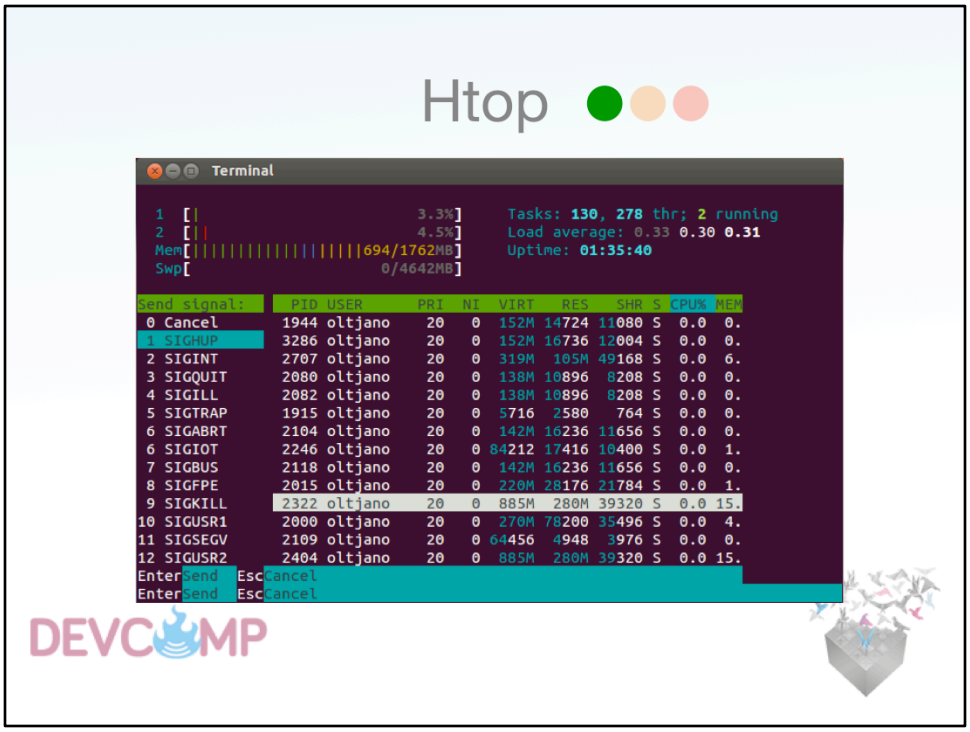
- Lynis
  - Outil d'audit de sécurité
- Debsums
  - Verifie les packets debian

DEVCAMP

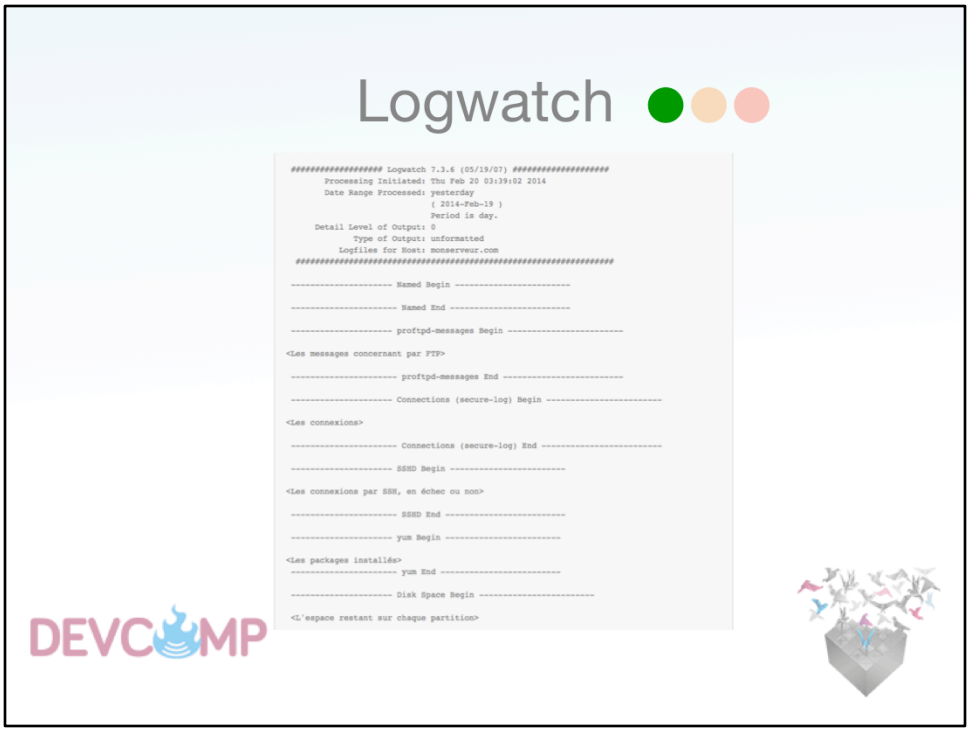
Lynis:
http://www.it-connect.fr/scan-de-votre-systeme-unix-avec-lynis/
http://la-vache-libre.org/lynis-un-soft-sympa-pour-auditer-son-systeme-ou-son-serveur-gnulinux-ubuntu-debian/

Monitoring

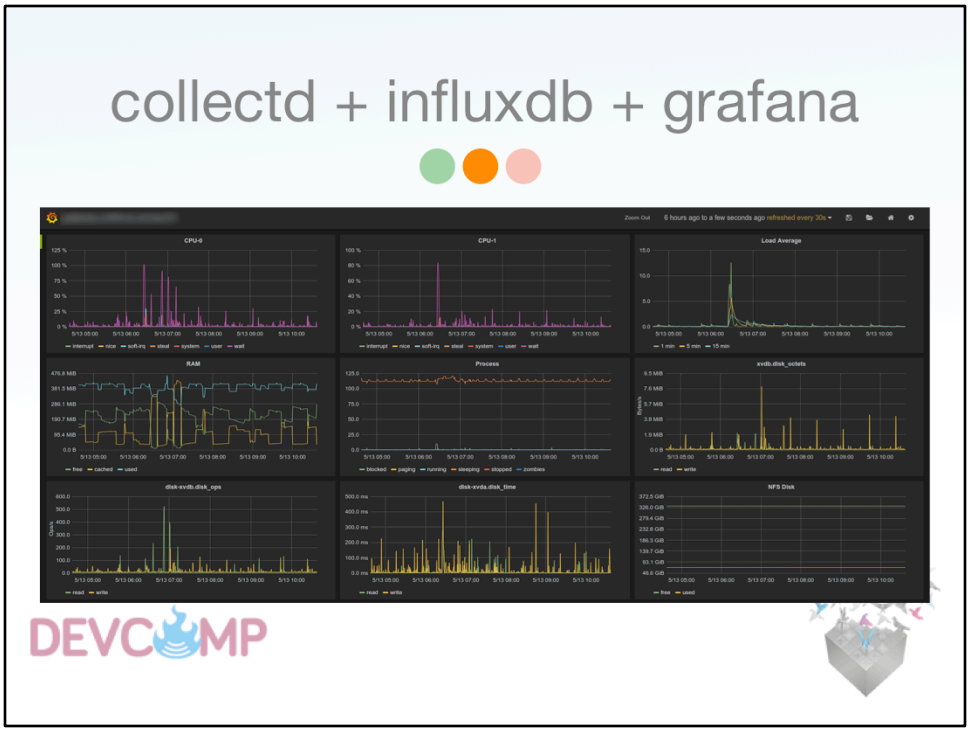
DEVCAMP



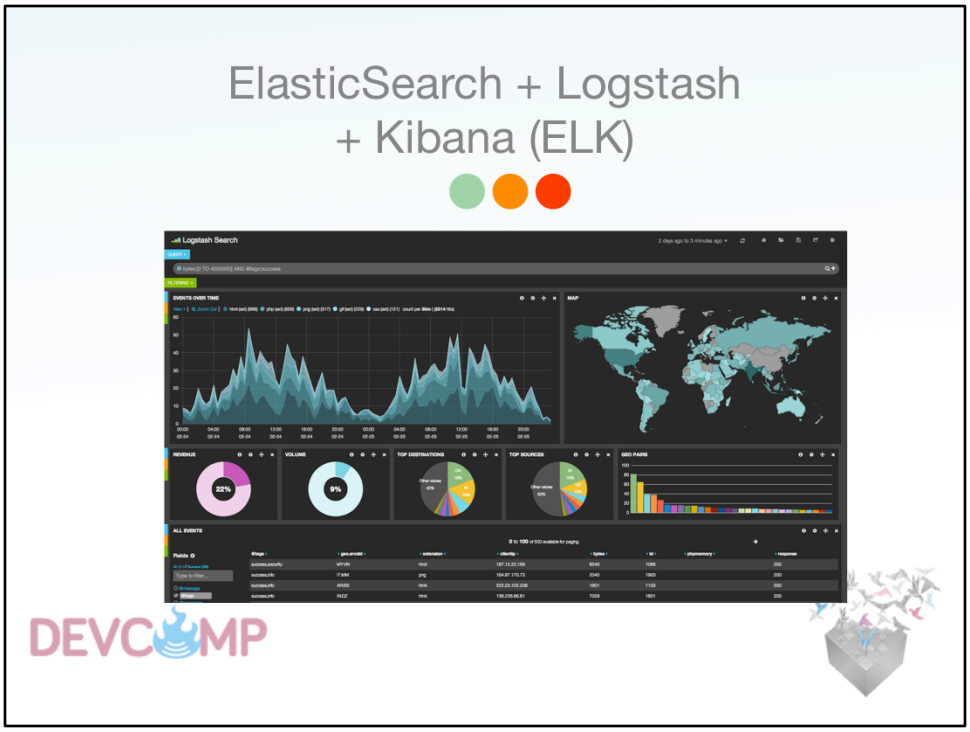
http://www.unixmen.com/monitor-system-processes-on-linux-with-htop/



https://www.digitalocean.com/community/tutorials/how-to-install-and-use-logwatch-log-analyzer-and-reporter-on-a-vps
http://www.partage-it.com/surveillez-les-logs-de-votre-serveur-avec-logwatch/



http://vincent.composieux.fr/article/grafana-monitorez-des-metriques-via-influxdb-inserees-depuis-collectd
https://www.shellandco.net/monitor-and-graph-your-linux-bind-servers-with-grafana/



Logstash, ElasticSearch & Kibana:
http://linuxfr.org/news/gestion-des-logs-avec-logstash-elasticsearch-kibana
https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-4-on-centos-7
http://thepracticalsysadmin.com/introduction-to-logstashelasticsearchkibana/

Kibana :
http://www.elastic.co/guide/en/kibana/current/index.html

Mise à jour et Backup

- Cron-apt
- Backup-manager
- Duplicity

DEVCAMP

http://blog.pastoutafait.fr/billets/Mise-%C3%A0-jour-automatique-avec-Cron-APT

Backup-manager :

http://doc.ubuntu-fr.org/backup-manager

http://howto.biapy.com/fr/debian-gnu-linux/systeme/logiciels/installer-et-configurer-backup-manager-sur-debian

https://github.com/devcamp

http://www.meetup.com/fr/DevCamp/

@MarcAudefroy
@LaCNR
@devcampRennes

Merci!

DEVCAMP