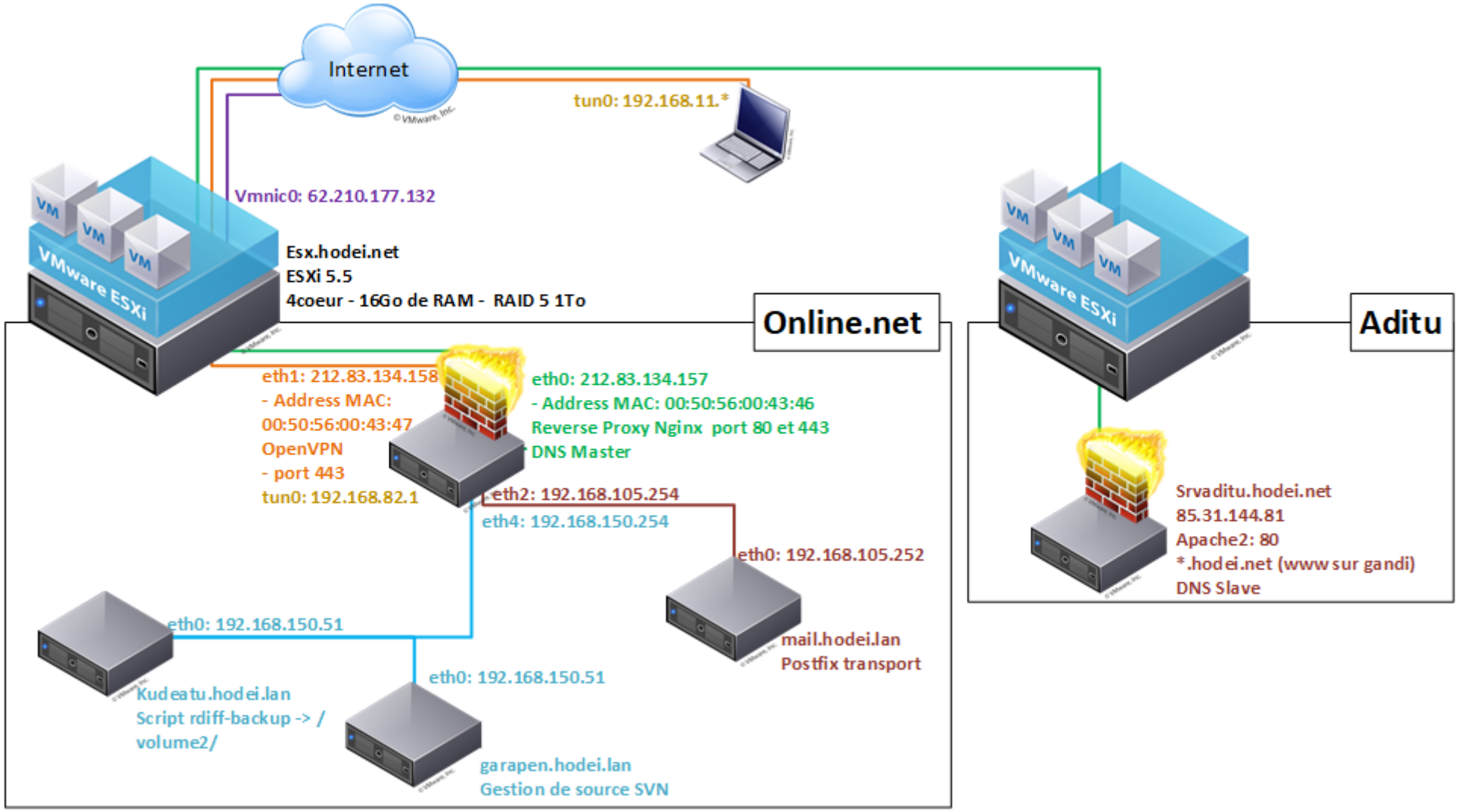
Hodei

Infrastructure Web Hodei

Septembre 2019

Schéma


Internet
tun0: 192.168.11.*
Vmnic0: 62.210.177.132
Esx.hodei.net
ESXi 5.5
4coeur - 16Go de RAM - RAID 5 1To
Online.net
Aditu
eth1: 212.83.134.158
- Address MAC:
00:50:56:00:43:47
OpenVPN
- port 443
tun0: 192.168.82.1
eth0: 212.83.134.157
- Address MAC: 00:50:56:00:43:46
Reverse Proxy Nginx port 80 et 443
DNS Master
eth2: 192.168.105.254
eth4: 192.168.150.254
eth0: 192.168.105.252
mail.hodei.lan
Postfix transport
Srvaditu.hodei.net
85.31.144.81
Apache2: 80
*.hodei.net (www sur gandi)
DNS Slave
eth0: 192.168.150.51
Kudeatu.hodei.lan
Script rdiff-backup -> /
volume2/
eth0: 192.168.150.51
garapen.hodei.lan
Gestion de source SVN

Présentation

L’architecture repose sur deux hébergeurs:

- Online.net: VM infrastructure hodei
- Aditu: Application Web dolibarr

Le serveur ESXi online.net héberge:

- Le reverse proxy des services dollibar
- La zone DNS hodei.net
- Les sauvegarde quotidienne dolibarr de production (Aditu)
- des serveurs LAMP personnel (Déménagement début octobre)
- Un relais mail pour les applications Web

Hodei

ADITU
plateforme de services numériques

Location d’une machine virtuelle pour l’hébergement des instances web Dolibarr

Serveur de production LAMP dolibarr

SRVADITU.HODEI.NET / 85.31.144.81

Matériel
- CPU : 1 coeur
- RAM : 3 Go
- HDD : 48 Go

Services
- DNS Secondaire
- HTTP
- Base de données MySQL
- SMTP Transport

Système
- Debian 6
- Iptables
- Bind 9
- Apache 2
- MySQL 5.1
- PHP 5.3

Configuration
- /root/iptables.sh
- /etc/bind9/
- /etc/apache2/site-enabled/
- /var/www/doliprod
- /var/mysql/my.cnf
- /var/lib/mysql/

Sauvegarde quotidienne de la VM par les services d' Aditu
Sauvegarde des sites (code / fichiers / bases de données) quotidienne depuis « kudeatu.hodei.lan »

Hodei

Location d’un serveur pour l’infrastructure des services tiers, dns, sauvegarde, gestionnaire de sources, …

ESXi online.net

esx.online.net

Matériel
- CPU : 4 cœurs
- RAM : 16 Go
- HDD : 1 To
- RAID : 5 / 3 * 500Go
- vmnic0 : 62.210.77.34

Système
- ESX 5.5
- SSH

Configuration
- Datastore /vmfs/volume1/datastore1
- vSwitch0 / vmnic0:
  - PortGroup: VM Network
  - VmKernel: Management Network
- vSwitch1 / pas d'interface physique
  - Port Group: Production
- vSwitch3 / pas d'interface physique
  - Port Group: Production

Services
- Heberge les VMs de l'infrastructure hodei.net

Machine Virtuelle « gateway »:

passerelle de connexion à internet pour les VMs

- Reverse proxy
- Gestionnaire de zone DNS
- …

VM « gateway.online.net »

HODEI.NET

Matériel

- CPU : 1 coeur
- RAM : 3 Go
- HDD : 48 Go
- Network adapter 1 :
  - Port Group: VM Network
  - Adresse MAC: 00:50:56:00:43:46
- Network adapter 2 :
  - Port Group: VM Network
  - Adresse MAC: 00:50:56:00:43:47
- Network adapter 4 :
  - Port Group: LAN
- Network adapter 5 :
  - Port Group: Production

Système

- Debian 7
- Iptables
- Bind
- Nginx
- Postfix

Services

- DNS Primaires
- Reverse proxy Web
- Relais SMTP
- Passerelle LAN

Configuration

- /root/iptables.sh
- /etc/bind9/

VM « gateway.hodei.lan »

Passerelle réseau

HODEI.NET

Filtrage et Nat

2 IP Failover pour:

- Nginx https écoute sur 212.83.134.157:80/443
- openVPN écoute sur 212.83.134.158:443

Le filtrage s'effectue avec IPTABLES

- Nat vers internet sur l'interface eth0
- Fichier de configuration : /root/iptables.sh
- Exécution lors du chargement des interfaces: /etc/network/interfaces

OpenVPN

- Configuration : /etc/openvpn/server.conf
- Certificats et clés: /etc/openvpn/easy-rsa/keys/

Configuration réseaux:

eth0: Port Group « VM Network »

- Adresse MAC: 00:50:56:00:43:46
- Adresse IP: 212.83.134.157

eth1: Port Group « VM Network »

- Adresse MAC: 00:50:56:00:43:47
- Adresse IP: 212.83.134.158

eth2: Port Group « LAN »

- Adresse IP: 192.168.105.254

eth4: Port Group « Production »

- Adresse IP: 192.168.150.254

Passerelle par défaut:

- Adresse IP: 62.210.177.1
- Interface: eth0

VM « gateway.hodei.lan »

Service DNS

HODEI.NET / 212.83.134.157 & 212.83.134.158 / TCP:53 & UDP:53

Serveur BIND 9
Serveur Primaire installé sur «gateway.hodei.lan»
Serveur Esclave installé sur «srvaditu.hodei.net»
Transfert des requêtes autorisés pour les réseaux 192.168.150.0/24 & 192.168.105.0/24

Zone:

- hodei.net
- hodei.lan

Configuration:

- /etc/bind/named.conf
- /etc/bind/db.hodei.net
- /etc/bind/db.hodei.lan

Mettre à jour le champs serial dans un fichier de zone lorsque le fichier est modifié pour déclencher la synchronisation vers l'esclave.

Pas de modification du fichier de zone « hodei.net » sur le serveur « srvaditu.hodei.net »

VM « gateway.hodei.lan »

Service Reverse Proxy

HODEI.NET / 212.83.134.157 / TCP : 80 & 443

Serveur Nginx 1.2.1
*.hodei.net : transfert des requêtes vers le serveur « srvaditu.hodei.net »
www.hodei.net : transfert des requêtes vers le service « http://gpaas6.dc0.gandi.net »
analytics.hodei.net : transfert des requêtes vers le service « http://192.168.150.51:80/piwik/ »

Configuration
- /etc/nginx/server.conf/
- /etc/nginx/sites-enabled/

Certificat SSL
- /etc/ssl/

Log:
/var/log/nginx/

VM « gateway.hodei.lan »

Service Relais Mail

HODEI.NET / 212.83.134.157 / TCP:25

Serveur Postfix

Règle de transport: /etc/postfix/mysql-transport_maps.cf

Hodei

Machine Virtuelle « kudeatu »:

- Sauvegarde et restauration des instances Dolibarr
- Administration des bases de données

VM « kudeatu.hodei.lan »

KUDEATU.HODEI.LAN | 192.168.150.51

Matériel
- CPU : 1 cœur
- RAM : 1 Go
- HDD 1 : 25 Go /
- HDD 3: 100 Go /volume2
- Network adapter 1 :
  - Port Group: Production

Système
- Debian 7
- Apache 2
- MariaDB 5.5
- PHP 5.4
- Rdiff-backup 1.2.8
- Phpmyadmin

Configuration
- eth0 : 192.168.150.51
- Passerelle: 192.168.100.254 eth0
- dns: hodei.lan 192.168.100.254

Services

Sauvegarde des serveurs « online.net » et « Aditu »

Accès PHPmyadmin en local ou VPN: http://kudeatu.hodei.lan

- Base de données accessible:
  - srvaditu.hodei.net
  - garapen.hodei.lan
  - localhost

VM « kudeatu.hodei.lan »

Service de sauvegarde

KUDEATU.HODEI.LAN | 192.168.150.51 | TCP 22

Outil rdiff-backup (rsync + versionning)

Fonctionnement

- Cron root : 0 1 * * * /root/script/backup_hodei.sh (tous les jours à 1h)
- Stockage des sauvegardes: /volume2/hodei/[host]/
- Rétention de 30 jours
- Traitement SSH (clé public de « kudeatu » déployé sur les serveurs)

Utilisation

Déclaration d'un serveur

- Création d'un fichier « .conf » nommé avec le fqdn du serveur à sauvegarder
- Exemple: monserveur.mondomaine.com

Options disponible:

- Dump des bases de données (option: mysql:*[host]|[user]|[mdp]|[bdd]/ 'all'*
- Compression des dossiers (option: conf: */chemin1/ /chemin2/)*
- Copie des fichiers (option: file: */chemin1/ /chemin2/*)

Restauration