Gestion de configurations puppet - cfengine - ansible

Retour d'expérience Puppet au LIG (2013 -)

Retour d'expérience Puppet au LIG (2013 -)

Le Contexte

2013

Deux plateformes xen distinctes vieillissantes : passage vers une plateforme vmware mutualisé

- Départ non remplacé des deux personnes qui les maintenaient
- Moins de personnels => On a besoin d'une diminution du coût d'entrée pour des opérations simples (clonages, snapshots...)

Mise en place d'une infrastructure VMWare

- 2 hyperviseurs
- Une baie de disque 100 To

On table à terme sur une capacité de 250 machines virtuelles

Retour d'expérience Puppet au LIG (2013 -)

Choix préliminaires

Le piratage de l'un des site web (2013) va impacter une quarantaine d'autre sites sur le même serveur

- Chaque CMS = 1 VM et en cas de soucis on tire la prise
- Inventaires des OS serveurs :

  - Des serveur Windows

  - Des serveurs MacOS

  - Des serveurs Linux Redhat et Clone & Debian

- On ne supportera que ça dans notre périmètre.

On a besoin d'un gestionnaire de configurations (et vite !)

Retour d'expérience Puppet au LIG (2013 -)

Réflexion sur les gestionnaires de configurations

Présentation de chef au JRES 2013

- https://2013.jres.org/archives/166/paper166_article.pdf

Mais à l'époque seul Redhat et clones sont supportés.

Le seul qui à cette époque fonctionne avec tout notre périmètre : Puppet

donc Puppet

Retour d'expérience Puppet au LIG (2013 -)

Puppet et les ENC (External Node Classifier)

Puppet : architecture client serveur classique

De base, on définit comment et à quels serveurs s'appliquent les programmes Puppet (*Manifests*) dans le fichier *site.pp*

- Ce n'est pas du tout pratique, surtout quand le nombre de serveurs et de configurations augmentent

Puppet est justement fait pour en gérer beaucoup et on en a déjà beaucoup !

- On utilisera un ENC : Foreman https://www.theforeman.org

Retour d'expérience Puppet au LIG (2013 -)

Le couple Puppet Foreman

Un ENC, c'est une grosse base de données qui va gérer les serveurs et les configurations et va présenter tout ça avec une interface graphique simple

- On a choisi Foreman, projet libre et qui offrait pas mal de possibilités.

Bon choix in fine, le développement est toujours très actif, RedHat est derrière le projet et il répond parfaitement à nos besoins

(et même à ceux que l'on ignorait avoir)

Retour d'expérience Puppet au LIG (2013 -)

FOREMAN

Jean-Louis Mas

Surveiller | Conteneurs | Hôtes | Configurer | Infrastructure | Administrer

Vue globale

Filtre ... | Rechercher

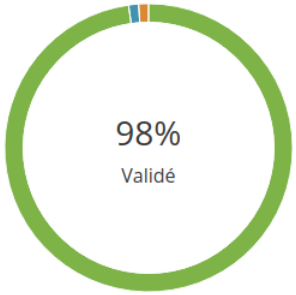
Généré le 01 Jul 20:41 | Gérer | Documentation

Statut de configuration des hôtes

Hôtes qui ont effectué des changements sans erreur	0
Hôtes en erreur	0
Bons rapports dans les derniers 35 minutes	88
Hôtes en attente de changements	0
Hôtes désynchronisés	1
Hôtes sans aucun rapport	1
Hôtes dont les alertes sont désactivées	0

Nombre d'Hôtes Total: 90

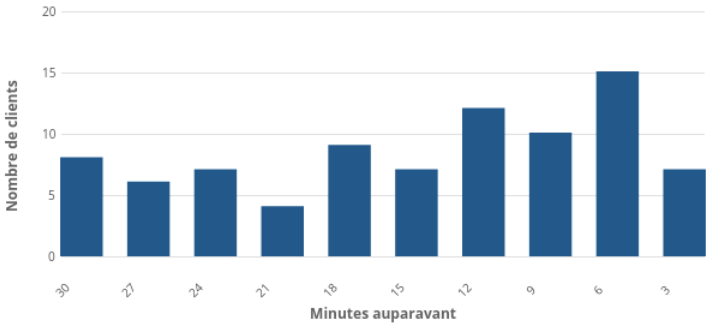
Diagramme de la configuration des hôtes



Dernier évènement

Hôte	A	R	F	FR	S	P
lig-info-sans-ordi.imag.fr	0	0	15	0	6	0
lig-sigma.imag.fr	1	1	0	0	0	0
lig-svl7.imag.fr	1	0	0	0	0	0
racer.imag.fr	1	0	0	0	0	0
lig-smb4-ad-rep.liglab.fr	0	0	2	0	0	0
lig-sigma.imag.fr	1	1	0	0	0	0
lig-sigma.imag.fr	1	1	0	0	0	0
zuul.imag.fr	0	0	1	0	0	0
lig-expire-web.imag.fr	1	0	0	0	0	0

Run Distribution (last 30 minutes)



Retour d'expérience Puppet au LIG (2013 -)

Notre infra 'Puppetisée' aujourd'hui (en fin de vie)

- Physique

  3 hyperviseurs 2x192 et 256 Go de RAM

  1 baie equallogic 100 To utiles

- Logiciel

  2 serveurs virtuels hébergeant Puppet & Foreman (à cause des soucis de montée de versions)

  Code des *manifests* Puppet sur git (Gitlab Gricad)

Sont gérés : 249 serveurs

137 Debian

112 Centos

Et finalement pas autre chose, cf le choix de départ qui, à la lumière de l'expérience aurait pu être remis en question.

Les forces rebelles

On a une quinzaine de serveurs qui ne sont pas gérés par Puppet (Windows, MacOS et Linux)

- On a pas eu le temps de les intégrer (Windows ou MacOS, trop peu nombreux pour que le travail d'intégration soit rentable)
- Les utilisateurs refusent
- On ne sait rien de ces serveurs et on a pas d'accès dessus.

Retour d'expérience Puppet

Changements majeurs de versions sont pénibles (mais faisable)

- Puppet de la distribution

  Mauvaise idée : Les versions différentes ne sont pas compatibles entre elles; Ça marchotte et ce n'est pas stable

- On utilise les dépôts yum|apt.puppetlabs.com

  Bonne idée : Versions de Puppet identiques sur tous les serveurs.

Retour d'expérience Puppet au LIG (2013 -)

Retour d'expérience Puppet (suite)

Montée en versions de plus en plus fréquentes et souvent pénibles

- En prod on est passé de 2 => 3 => 4 => 5 (de manière transparente, enfin !)

Coté serveurs

- Changement de technologie => réinstallation complète du serveur (Foreman a aussi compliqué les choses)

Coté clients

- Syntaxes non compatibles entre les versions avec erreurs silencieuses

  => *puppet-lint*, *puppet parser validate* et lire les docs https://puppet.com/docs/puppet/5.5/deprecated_settings.html

- Changement de tous les chemins des répertoires Puppet

  => Installer et configurer Puppet avec Puppet

- Difficile de passer de serveurs en 3.7 vers le 4.8 sans tout détruire et tout réinstaller. Chemin des certificats des binaires totalement différents. Noms des paquets différents aussi.

Cotés modules LIG

- Revalidation régulière des modules

  => bouffe temps

Retour d'expérience Puppet (les bons cotés)

La puppet forge, base de modules installable et 'upgradable' en ligne de commande

- https://forge.puppet.com

Il y a beaucoup de choses, très facile de commencer son automatisation avec des modules pré-écrits

Et Puppet ça marche (vraiment) et ça tient ses promesses.

Retour d'expérience Puppet au LIG (2013 -)

Les modules au LIG

Écrit à la main, environ une quinzaine

On utilise trop peu la puppet forge

- Pas toujours très bon au début 2013, et la mauvaise habitude a été prise de ne pas suffisamment l'utiliser

  => Mais on y vient

Versionnés avec git + système de validation et tests automatique rudimentaire.

Gérés et déployés par foreman

Bonnes pratiques (demandée par des utilisateurs)

- Les fichiers modifiés par Puppet sont signalés dans l'entête de ceux-ci

Retour d'expérience Puppet au LIG (2013 -)

Qu'est ce que l'on déploie avec Puppet

Toutes les configurations de base communes ou presque à tous nos serveurs

- snmp, logs déportés, ntp, sauvegardes, firewall, authentification, mises à jour automatisées

Tout ce qui concerne les serveurs web (on en a beaucoup) de manière plus ou moins automatique

- apache, wordpress, drupal, fail2ban

Des choses spécifiques

- Les configurations des serveurs de calculs suivant les besoins des équipes, la possibilité d'envoyer des mails

Les correctifs des failles de sécurité

- Via un *manifest* sécurité vide que l'on ré-écrit en fonction des failles.

Retour d'expérience Puppet au LIG (2013 -)

Ce que l'on a appris sur Puppet et consorts

Les scripts c'est bien, mais ça trouve vite ses limites quand on doit gérer de l'hétérogénéité

- 4 versions de Debian et 2 de Centos en prod au LIG

Un gestionnaire de configuration, c'est indispensable dès que le parc grossit

- Il faut le mettre en place avant de se faire déborder de préférence (après c'est plus dur)

Un ENC c'est indispensable pour gérer de manière simple un gros parc de serveurs

- The foreman est un bon choix. Il est aussi compatible avec Chef, Salt et Ansible

Retour d'expérience Puppet au LIG (2013 -)

Le futur

Provisionnement automatique de serveurs 'from scratch'

- Ça fonctionne déjà, mais pas eu le temps de le valider pour la prod (Coucou Winter)

Progresser avec Puppet

- Échanger sur l'utilisation de puppet sur le campus, les échanges ont été trop rares

Faire faire encore plus de choses à puppet

- Ce n'est pas les idées qui manquent, mais le temps !

Retour d'expérience Puppet au LIG (2013 -)

Des questions ?