去中心化puppet部署

huangmingyou@gmail.com

December 17, 2013

目录

前言

去中心化的puppet部署，舍弃puppetmaster，直接把puppet manifest 部署到puppet客户端进行执行。这样部署能带来两大好处，一是无穷的扩展性能，c/s方式部署的puppet,部署规模一大，puppetmaster性能会成为一个瓶颈。 二是增加安全性，c/s模式下的证书认证， 只能保证数据在传输过程中的安全性，但是一旦puppetmaster被黑，所有puppet agent也面临被黑的风险。

本手册的最新版本可以从:http://github.com/huangmingyou/puppet/pdf 获得。

第1章　部署

《草》

作者：白居易

離離原上草，一歲一枯榮。

野火燒不盡，春風吹又生。

遠芳侵古道，晴翠接荒城。

又送王孫去，萋萋滿別情。

1.1　整个系统的结构

核心思路，把puppet manifest 打包，通过gnupg 签名以后，通过任何手段传输到 puppet agent上执行。 这样带来的意义何在？

首先，不用puppet master来解释和分发代码，没有了单点负载压力，因为你可以通过ftp,rsync,https,等各种传输手段来分发puppet 的manifest到puppet agent。你甚至可以考虑用cdn来分发。当然，这样传输密码等关键信息是不行的，你完全可以设计另一条安全的路径来传输机密信息,比如scp。以我生产环境来说，我是用rsync来传输的，因为我的代码里面没有机密信息。也不怕公开。

其次，利用gpg对代码签名来保证puppet agent执行的代码是经过确认的安全代码，puppet agent上的gpg 公钥可以在安装系统的时候初始化安装。这样的安全性高于主流的c/s puppet部署方式。 c/s 部署的证书作用有两个，一是防止假的puppet agent 来puppet master 骗取puppet 配置。 二是作为https传输的证书。仅此而已！ 如果你的企业有上千台的机器部署了 c/s 模式的puppet. 那么所有的安全都系在puppet master的安全上了。一旦puppet master沦陷，所有机器沦陷。这都是因为puppet缺少一个puppet manifest代码的审核机制。只要puppet代码没有语法错误，puppet master就会解析执行并传送给puppet agent执行。总的说来，puppet还是缺少授权和对代码的认证。

利用gpg签名puppet manifest代码，安全性能提高不少，因为，只要保护好gpg私钥和密码，就能保证puppet agent执行的代码不是被篡改过的代码。 gpg

私钥可以通过保存到网络隔离的机器上来保证安全。并且做磁盘加密。能做到不错的安全程度,加密puppet manifest 代码的时候，利用u盘来拷贝。而puppet master很难做到网络隔离,网络都断了，还怎么和puppet agent通讯。

但是，没有绝对的安全！毕竟，太阳也有毁灭的一天。

1.2 部署实例

以我当前的生产环境的部署来作为例子，我利用一台最垃圾的pc作为私钥保存和签名的机器，并且网络隔离，做磁盘加密。利用rsync来分发代码。我们来看看这套系统怎样自己提着自己的鞋带把自己拉起来。

当运维上线一台新机器的时候，加入我们自己的私有软件仓库，然后用 apt-get 安装 xy-puppet-init包。这个包依赖puppet,会自动把puppet安装好。同时这个包会在/etc/cron.d/里面安装一个定时任务。这个定时任务会每隔一小时从rsync server去下载puppet manifest代码来执行。下面就是这个脚本的内容。

```
#!/bin/bash
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
[ -f /nopuppet ]&&exit 0
rsync -avz --delete --exclude='.svn' puppet@rsyncserver::puppet/ /opt/puppet/
[ -d /tmp/xy-puppet ]||mkdir /tmp/xy-puppet
rm /tmp/xy-puppet/* -rf
tar zxf /opt/puppet/puppet.tgz -C /tmp/xy-puppet
gpg --verify puppet.tgz.asc
[ $? -ne 0 ]&&exit 0
rsync -avz --delete /tmp/xy-puppet/puppet/ /etc/puppet/
puppet /etc/puppet/manifests/site.pp
/bin/run-parts /etc/puppet/file/shell/autorun/
```