一.Puppet的工作流程

1）客户端puppetd调用facter，facter探测出主机的一些变量，例如主机名，内存大 小，ip地址等。pupppetd 把这些信息通过ssl连接发送到服务器端；

2）服务器端的puppetmaster 检测客户端的主机名，然后找到manifest里面对应的node配置， 并对该部分内容进行解析，facter送过来的信息可以作为变量处理，node牵涉到的代码才解析，其他没牵涉的代码不解析。解析分为几个阶段，语法检查，如果语法错误就报错。如果语法没错，就继续解析，解析的结果生成一个中间的“伪代码”，然后把伪代码发给客户端；

3）客户端接收到“伪代码”，并且 执行，客户端把执行结果发送给服务器；

4）服务器端把客户端的执行结果写入日志。

工作流程的安全性：

1） 为了保证安全，client和master之间是基于ssl和证书的，只有经maste证书认证的 client可以与master通信；

2）puppet会让系统保持在你所期望的某种状态并一直维持下去，如检测某个文件并保证其一直存在，保证ssh 服务始终开启，如果文件被删除了或者ssh服务被关闭了，puppet下次执行时（默认30分钟），会重新创建该文件或者启动ssh服务。

3)puppet 的agent在请求与master连接时，需要与master签署证书，证书的算法可指定（取决于openssl版本），默认为MD5算法

Puppet的安全性：

Puppet的连接是采用ssl隧道通信的，在master和agent连接前，agent需要向master申请注册证书，只有master签发证书后才能建立起连接。Master可以对证书进行管理，但进行证书过期或者删除操作以后必须重启puppetmaster服务。