

id: security title: Puppet Security allowDiscussion: None subject: description: A description of the Puppet security model. contributors: creators: luke effectiveDate: 2005/08/29 20:47:27.123 GMT-5 expirationDate: None language: en rights: creation\_date: 2005/08/29 18:41:19.762 GMT-5 modification\_date: 2005/08/29 20:47:27.125 GMT-5 layout: document\_view Content-Type: text/x-rst

## Overview

Puppet relies on standards wherever possible. In the case of security, it uses standard SSL certificates for client and server verification. Because of the cost of buying signed certificates for every client and the complexity of managing your own certificate authority (CA), Puppet includes its own CA. This CA has been optimized for use with Puppet but could also be used to generate certificates for other purposes. The primary goal in certificate management within Puppet has been to keep it simple, and wherever possible to not make it even noticeable.

## Certificates

### Authentication

Certificates are the only method of authentication -- if a client's certificate can be verified using standard SSL verification mechanisms, then it is considered authenticated.

### Client Certificate Generation

The Puppet server, `puppetmasterd`, is normally also the CA. Clients who do not yet have signed certificates will automatically generate a key pair and a certificate request, and then will connect to the server and provide it with the certificate request. If the server has `autosign` turned on (which is not necessarily recommended), then the `autosign` configuration file (which defaults to `/etc/puppet/autosign.conf`) is checked for whether the client's name matches any contents. For instance, take the following configuration file:

```
hostname.domain.com
*.secure.domain.com
```

This configuration would `autosign` certificate requests for `hostname.domain.com` and any hosts coming from `*.secure.domain.com`.

This configuration file is read each time a signature is asked for, so changes to it can be short-lived and will be immediately noticed.

### Server-Side Certificate Management

In the normal case, certificate auto-signing will be disabled. In these cases, certificates will have to be signed using the `puppetca` utility. Prior to the 1.0 release it is expected that there will be email notification of certificate requests waiting to be signed, but for now either the logs must be watched or `puppetca --list` can be used list waiting requests.

Once a request arrives, `puppetca --sign <hostname>` can be used to sign the request. Adding the `--all` flag will sign all outstanding requests.

## Access and Authorization

Puppet currently has few network functions, so security has so far been treated by them individually. It is expected that there will be some system-wide security hooks prior to the 1.0 release, but the certificate authentication already provides significant security.

Recommendations on approaches are heartily recommended.