THETA

The Higher Education Technology Agenda

SELinux administration through Puppet

Puppet is a popular Centralized Configuration Management tool.

SELinux is a Mandatory Access Control mechanism developed by the NSA and integrated into the Linux kernel.

While lots of organisations use Puppet, which requires at the least extensive experience in system administration to make the most of. In contrast, very few organizations use SELinux beyond turning it off. This is especially disappointing because SELinux:

1. Is non-disruptive in a properly set up Enterprise Linux environment;
2. Offers a ‘defense in depth’ mechanism that requires generally very few expertise (beyond the level of proficiency that Puppet already requires);
3. Becomes relatively intuitive once you get past the first few hurdles; and
4. Can be made to be very easy to maintain through Puppet.

The purpose of this talk is to:

- Quickly introduce some of the core concepts ofSELinux:
  - Where it fits into the defense in depth stack;
  - What the common pitfalls are;
  - What the core concepts that need to be understood are.
- Outline the means of implementing BASH commands in Puppet by way of example using SELinux commands; and
- Using node files to allow for the centralized management of SELinux settings.

The Puppet examples will outline methods of:

- Deploying custom types for files and ports using semanage;
- Setting sebooleans to enable pre-configured optional policies;
- Changing contexts on files directly;
- Deploying and managing SELinux custom policy modules; and

- Reusing this through the use of node files.

Using Puppet specific techniques such as:

- Defining re-usable types;
- Argument passing, including means of making arguments optional (by setting sensible defaults);
- Use of scope operators; and
- Type chaining.

SELinux concepts to be discussed will include:

- Using setroubleshootd and sealert;
- Contexts using semanage vs chcon; and
- The principles behind creating a custom policy.

The focus of this talk will be on CentOS 6, although if time permits may expand to include CentOS 7.

Christian Unger
Translational Research Institute