

Status of SELinux in Ubuntu

State of the Art

- Available in since Hardy
- Targeted/MCS style policy
- Jaunty/Karmic policy has many modules enabled
- Userspace looks solid
- Policy needs work

Why?

- I like Ubuntu 😊
- People asked for it
- Want more options for running SELinux
- Locking down servers
- Reaching more users
 - Ubuntu is still #1 on distrowatch afterall

Outline

- Installing SELinux on Ubuntu
- Initial policy load
- Updating policy
- Future work

Installing SELinux on Ubuntu

- Easy installation of SELinux
 - Turn it into a simple ‘apt-get install selinux’
- Handles
 - Updating of the initramfs
 - Installing the default system policy
 - Scheduling a system relabel
 - Switching ‘gracefully’ from Apparmor

Initial Policy Load

- Why not patch Upstart?
- Loading from the initramfs
 - load_policy
 - -i option for initial policy load
 - Moved to /sbin
 - initramfs scripts
 - /etc/initramfs-tools/scripts/init-bottom
 - Scripts for:
 - Loading the policy
 - Restoring chronically mislabeled files

initramfs scripts

- Scripts
 - `_load_policy`
 - `chroot`
 - `load_policy -i`
 - `mount selinuxfs`
 - `_restorecon`
 - `chroot`
 - `restorecon /dev`
- `update-initramfs`

update-selinux tools

- **update-selinux-config**
 - Installs a config if one doesn't already exist
 - Sets the selinux policy type
- **update-selinux-policy**
 - Build the policy
 - Uses the modules from `/etc/selinux.d`

/etc/selinux.d

- Mechanism for
 - Adding new policy
 - Replacing existing distro policy
- Policy updates don't override
- /etc/selinux.d/<store>/<module>.pp
- /usr/share/selinux/<store>/<module>.pp
- Matches Ubuntu standard config practices

Future Work

- More integration into the desktop
- Distro independent version of
 - system-config-selinux
 - setroubleshoot
- More modules enabled by default
- More documentation

Questions?