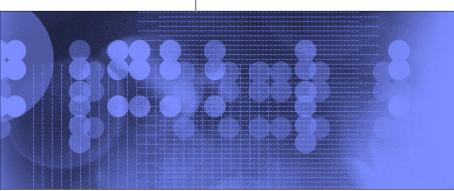# Making SELinux Easier to Use

Bryan Jacobson & Debora Velarde
Linux Plumbers Conference 2009

# Where are we coming from?

- A gradually increasing number of folks come to us with SELinux questions and issues.

- We believe SELinux would be more widely used if the docs:
  - Gave folks more help learning SELinux on their own.
  - Gave folks better help when solving problems.

- How can my IBM LTC Linux Security development team help?

# I've heard about Booleans, where can I find them?

**httpd_builtin_scripting (HTTPD Service)**
Allow HTTPD to support built-in scripting

`allow_httpd_sys_script_anon_write --> off`

To find the man page for this somehow you need to know
you should do: man httpd_selinux

# Example of documentation that one user was not able to understand.

httpd can be configured to turn off internal scripting (PHP). PHP and other loadable modules run under the same context as httpd. Therefore several policy rules allow httpd greater access to the system than is needed if you only use external cgi scripts.

```
setsebool -P httpd_builtin_scripting 0
```

"It doesn't do anything."

# Out of Date Documentation

- `httpd_selinux` man page list 19 booleans

- `getsebool -a | grep http` returns 23 httpd related booleans

- Short of reading the actual policy where can a user go to get information on the remaining httpd related booleans?

# Finding up to date SELinux documentation

- **There is a lot of great documentation available, the problem is finding current info for what you need**

- **Google search points to old information:**
  - "selinux documentation" - first hit is a year old
  - "selinux how to" - first five hits are from 2004 to 2007
  - "selinux howto" - first two hits from 2004
  - "selinux policy" - 1st hit from 2004, 2nd from 2006, 3rd bad link
  - "selinux user" - 1st hit RHEL 4 Manual from 2005

- *(Other Google searches did a better job finding recent docs.)*

- **Ideas:**
  - Write blog entries that point to good documentation
  - Other Ideas to increase page rank
  - Frequently mention: **http://selinuxproject.org/page/User_Resources**

# From the LinuxCon SELinux usability BoF

- It would help to have:
  - More Case Studies
  - More Use Cases (example: sandbox, safe browser)
  - More "How To" guides
  - Better (simpler) "getting started" SELinux documentation.

And: Lots is going on in the community to improve things.

We will post a BoF summary to the SELinux mailing list.

**Ideas / comments:**  bryan.jacobson@us.ibm.com

# setroubleshoot

- Very helpful the majority of the time

- Sometimes just tells user they need to create policy for something

- Messages can be very technical and scary to users

- IBM Brainstorming Ideas:
  - Re-write some of the messages with new users in mind
  - Learned this week: RedHat has been doing that

# James Carter's post on SELinux mailing list

- **"Problems related to using SELinux" thread posted on April 9, 2009**

- **Listed kinds of inadequate documentation:**
  - For the policy author
  - For the administrator
  - For the user
  - Low level mechanisms

# For the Policy Author

- Different policy tools are better suited for your environment (distro, version of distro, which policy you are using, GUI or command line)

- Idea: A matrix that pointed you to the recommended policy tools depending on:

  - Version of distro

  - Version of policy

  - GUI or command line

# For the Administrator

- **Context specific help**

  - `semanage login help`

- `adduser` **and** `useradd` **man pages could point to** `semanage`

- `selinux` **man page could point to** `semanage` **and** `seuser`

- `booleans` **man page could point to:** `ftpd_selinux, named_selinux, rsync_selinux, httpd_selinux, nfs_selinux, samba_selinux, kerberos_selinux, nis_selinux, ypbind_selinux`

# For the User

- **http://selinuxproject.org/page/User_Resources**
  - Points to lots of useful resources
  - What can we do to help new users find what they need more quickly?
  - Helpful to list dates so users can easily see which ones are older and perhaps outdated
  - Indicate if information at links are specific to a certain distro or type of policy
  - Some have a brief description of what the user will find at the link – this is very helpful
  - Could there be a community effort to improve some of these things?