Managing SELinux in the Enterprise

Daniel J Walsh
Senior Principal Software Engineer
@rhatdan, danwalsh.livejournal.com,
dwalsh@redat.com
Jun 12 2013
How to manage SELinux in a large environment?

- Move blobs of data to remote machines.
- Execute commands on the remote machine.
- Centralize logging.

Any questions?
SELinux four things

1. Labeling
2. SELinux needs to know
   - booleans
   - semanage commands
3. Custom policy modules
4. You've been hacked!

http://danwalsh.livejournal.com/30837.html
SELinux is a Labeling System
SELinux is a Labeling System

Every process has a label
SELinux is a Labeling System

Every process has a label
Every file/directory/object has a label
SELinux is a Labeling System

Every process has a label

Every file/directory/object has a label

Policy rules define how process access objects via labels
SELinux is a Labeling System

Every process has a label
Every file/directory/object has a label
Policy rules define how process access objects via labels
The Kernel enforces the rules
If a file object is mislabeled you will get errors?
Someone put Skittles in the M&M dispenser!!!
Administrators can mess up labeling

- Creating files/directories can cause problems
  - `# mkdir /root/.ssh`
- Be careful with the `mv` command
  - `# mv ~/index.html /var/www/html/`

If you check the Ownership on a new file/directory?
Administrators can mess up labeling

- Creating files/directories can cause problems
  - `# mkdir /root/.ssh`
- Be careful with the `mv` command
  - `# mv ~/index.html /var/www/html/`

If you check the Ownership on a new file/directory?
Check the SELINUX LABEL, or just run restorecon
Administrators can mess up labeling

Creating files/directories can cause problems

- `# mkdir /root/.ssh`
- Be careful with the `mv` command
- `# mv ~/index.html /var/www/html/`

`restorecon -R -v /root/.ssh /var/www/html`

BIG improvements with label creation in RHEL7...

http://danwalsh.livejournal.com/46018.html
SELinux likes everything to be in the default location

If you change the location of content, FIX the labels.

If you put Apache content in /srv/myweb execute:

- `semanage fcontext -a -t httpd_sys_content_t '/src/myweb(/.*)?'`
SELinux likes everything to be in the default location

If you change the location of content, FIX the labels.

If you put Apache content in /srv/myweb execute:

- `semanage fcontext -a -t httpd_sys_content_t '/src/myweb(./.*)?'

If you put your homedirs in /myhome execute:

- `semanage fcontext -a -e /home /myhome`
SELinux likes everything to be in the default location

If you change the location of content, FIX the labels.

If you put Apache content in /srv/myweb execute

- semanage fcontext -a -t httpd_sys_content_t '/src/myweb(/.*)?'

If you put your homedirs in /myhome execute

- semanage fcontext -a -e /home /myhome

restorecon -R -v /myhome /src/myweb
SELinux needs to know?

SELinux Least Privilege
SELinux needs to know?

Reasonable

SELinux Least Privilege
SELinux needs to know?

Reasonable

SELinux Least Privilege

Standard configurations should work out of the box.
Alter Default Configuration?

If you

- Change Apache to send email
  - SELinux needs to know!!!
    - semanage boolean --on httpd_can_sendmail
Alter Default Configuration?

If you

• Change Apache to send email
  • SELinux needs to know!!!
    • semanage boolean --on httpd_can_sendmail

• Change sshd port to port 500?
  • SELinux needs to know!!!
    • semanage port -a -t sshd_port_t -p tcp 500
How do I know what types, booleans, port definitions are available?

> 700 man pages added to RHEL6

httpd_selinux(8) SELinux Policy httpd httpd_selinux(8)

NAME
httpd_selinux - Security Enhanced Linux Policy for the httpd processes

DESCRIPTION
Security-Enhanced Linux secures the httpd processes via flexible mandatory access control.

The httpd processes execute with the httpd_t SELinux type. You can check if you have these processes running by executing the ps command with the -Z qualifier.

http://danwalsh.livejournal.com/52156.html
Custom Policy Modules

Applications and SELinux policy can have bugs
Custom Policy Modules

Applications and SELinux policy can have bugs

- `grep httpd_t /var/log/audit/audit.log | audit2allow -M myhttpd`
- `semodule -i myhttpd.pp`
Custom Policy Modules

Applications and SELinux policy can have bugs

- `grep httpd_t /var/log/audit/audit.log | audit2allow -M myhttpd`
- `semodule -i myhttpd.pp`

You might want to ship your own policies for your own apps

- `sepolgen /usr/sbin/myapp`
- `semodule -i myapp.pp`
- RHEL7
  - `sepolicy generate ...`
Contribute back

- If you find bugs in applications or SELinux policy
  - Report them
- If you write policy,
  - Contribute it back to Red Hat/Upstream
You might be hacked

- SELinux is not a intrusion detection tool.
- setroubleshoot can do some detection, you should use it.
  - Confined apps attempting to turn off SELinux, PWND
  - Confined apps attempting to modify kernel, PWND
  - Confined apps attempting to clear log files, PWND
  - mmap_zero? Maybe unless it is whine. (Wine)
- You probably want remote logging setup for this
But how do you manage SELinux in the enterprise.

- How do you configure your remote machines?
- How do you manage your remote content.
But how do you manage SELinux in the enterprise.

- How do you configure your remote machines?
- How do you manage your remote content.
- SELinux customization is just configuration.
  - SELinux should be managed the same as other configuration.
Advanced semanage

Semanage is slooooonw

• Most semanage commands compile/load policy
Advanced semanage

Semanage is sloooooow

- Most semanage commands compile/load policy

Semanage Transactions

- Allows several semanage commands with one command.

```bash
semanage -S targeted -i - << _EOF
  boolean -m --on allow_polyinstantiation
  boolean -m --on xguest_connect_network
  boolean -m --on xguest_mount_media
  boolean -m --on xguest_use.bluetooth
_EOF
```

http://danwalsh.livejournal.com/41593.html
Setting up identical machines with SELinux

Modify one machine the way you like?
Now apply to five other identical machines.
Setting up identical machines with SELinux

Modify 1 machine the way you like?
Now apply to 5 other identical machines.

# semanage -o /tmp/selinux.mods
# scp /tmp/selinux.mods to remote machine

http://danwalsh.livejournal.com/41794.html
Setting up identical machines with SELinux

Modify 1 machine the way you like?
Now apply to 5 other identical machines.

# semanage -o /tmp/selinux.mods
# scp /tmp/selinux.mods to remote machine

On remote machine:

# semanage -i /tmp/selinux.mods

http://danwalsh.livejournal.com/41794.html
cat selinux.mods

boolean -D
boolean -1 allow_polyinstantiation
boolean -0 authlogin_nsswitch_use_ldap
user -D
fcontext -D
fcontext -a -f 'all files' -t httpd_sys_content_t '/myweb(/.*)'?
fcontext -a -f 'all files' -t public_content_t '/shared(/.*)'?
fcontext -a -f 'all files' -t samba_share_t '/shared/samba(/.*)'?
...

http://danwalsh.livejournal.com/41794.html
Red Hat Satellite

Shipping SELinux commands in RPM

- Run semanage commands in post install
- Packaging SELinux Policy modules within RPM
- In RHEL7
  - “sepolicy generate” will generate an example rpm spec file.
%define relabel_files() \restorecon -R /usr/sbin/rwhod; \

%define selinux_policyver 3.12.1-44

Name:   rwhod_selinux
Version:  1.0
Release:  1%{?dist}
Summary:  SELinux policy module for rwhod

Group:   System Environment/Base
...
Source0: rwhod.pp
Source1: rwhod.if
Source2:  rwhod_selinux.8
...
Requires: policycoreutils, libselinux-utils
Requires(post):  selinux-policy-base >= %{selinux_policyver}, policycoreutils
Requires(postun):  policycoreutils
BuildArch: noarch

%description
This package installs and sets up the SELinux policy security module for rwhod.

%install
install -d %{buildroot}%{_datadir}/selinux/packages
install -m 644 %{SOURCE0} %{buildroot}%{_datadir}/selinux/packages
install -d %{buildroot}%{_datadir}/selinux/devel/include/contrib
install -m 644 %{SOURCE1} %{buildroot}%{_datadir}/selinux/devel/include/contrib/
%post
semodule -n -i %{_datadir}/selinux/packages/rwhod.pp
if /usr/sbin/selinuxenabled ; then
    /usr/sbin/load_policy
%relabel_files
fi;
exit 0

%postun
if [ $1 -eq 0 ]; then
    semodule -n -r rwhod
    if /usr/sbin/selinuxenabled ; then
        /usr/sbin/load_policy
        %relabel_files
    fi;
fi;
fi;
exit 0

%files
%attr(0600,root,root) %{_datadir}/selinux/packages/rwhod.pp
%{__datadir}/selinux/devel/include/contrib/rwhod.if
%{__mandir}/man8/rwhod_selinux.8.*
...

RPM specfile for SELinux
Can I ship the same policies in RHEL5 as RHEL6?
Can I ship the same policies in RHEL5 as RHEL6?

- No
- Newer Major Version include new access checks
  - open is checked in RHEL6 but not in RHEL5
Can I ship the same policies in RHEL5 as RHEL6?

- No
- Newer Major Version include new access checks
  - open is checked in RHEL6 but not in RHEL5.
- Policy should be stable for a major version
- Policy should be compiled and on the lowest minor version.
Puppet

- SELinux bindings
  - Built-in restorecon, selinux functions, semanage functions directly.
- Puppet recipes should include SELinux commands
- Shell out to semanage commands
  - A lot of Fedora Infrastructure built on top of Puppet
class proxy {
    include selinux-enforcing
    selboolean { [  
        "httpd_can_network_connect_db",  
        "httpd_can_network_relay",  
        "httpd_can_network_connect",  
        "allow_ypbind",  
    ]:  
        value => on,  
        persistent => true,  
    }
    semanage_port { "8081-8089":  
        type => "http_port_t",  
        proto => "tcp",  
    }
    semanage_port { "10001-10003":  
        type => "http_cache_port_t",  
        proto => "tcp",  
    }
    semanage_fcontext { "/srv/cache/mod_cache(/.*)?":  
        type => "httpd_cache_t",  
    }
}

Puppet Recipe
For SELinux
Ansible – http://www.ansible.cc

- Uses ssh protocol
  - advantage no destination daemon.
- Builtin selinux and seboolean functions.
- Ansible playbooks should include SELinux commands
- Execute semanage, same way administrator would.
  - Newer Fedora Infrastructure moving to Ansible
  - OpenShift infrastructure in Fedora setup using Ansible.
- name: set selinux bools appropriately
  action: seboolean state=true persistent=yes name=$item
  with_items:
  - httpd_unified
  - httpd_can_network_connect
  - httpd_can_network_relay
  - named_write_master_zones
  - allow_ypbind
- name: selinux module install - stickshift
  action: command semodule -i /usr/share/selinux/packages/rubygem-stickshift-common/stickshift.pp
- name: selinux module disable - passenger
  action: command semodule -d passenger
  ignore_errors: True
- name: selinux module install - other passenger
  action: command semodule -i /usr/share/selinux/packages/rubygem-passenger/rubygem-passenger.pp
- name: fix up files for selinux
  action: command $item
  with_items:
  - "fixfiles -R rubygem-passenger restore"
  - "fixfiles -R mod_passenger restore"
  - "restorecon -rv /var/run"
  - "restorecon -rv /usr/lib/ruby/gems/1.8/gems/passenger-*"
  - "restorecon -rv /usr/sbin/mcollectived /var/log/mcollective.log /run/mcollective.pid"
Other distributed tools for managing SELinux

- cfengine
- pulp
- func
- tivoli?
- openview?
- OpenLMI
  - Were working on it
Modifying SELinux in kickstart

Example: Configure MLS/LSPP system in RHEL6

```
sed -i 's/SELINUXTYPE=targeted/SELINUX=mls/g' /etc/selinux/config
setenforce 0
load_policy 2>&1 | grep -v no.longer.in.policy
echo "Fixing file labels..."
# FIXME: fixfiles ignores allegedly R/O filesystems due to bad /etc/mtab ?
cat /proc/mounts > /etc/mtab
fixfiles -Ff restore
restorecon -Fr /root /home
```
What about You've been hacked?
Audit subsystem remote logging

On the clients

- `/etc/audisp/plugins.d/au-remote.conf`
  - `active = yes`
- `/etc/audisp/audisp-remote.conf`
  - `remote_server=remote-audit.redhat.com`

On the server

- `/etc/audit/auditsd.conf`
  - `tcp_listen_port = 60`
Setroubleshoot Remote Logging

/etc/setroubleshoot/setroubleshoot.conf

- [email]
- smtp_host = smtp.foobar.redhat.com
- # from_address: The From: email header
- from_address = SELinux_Troubleshoot.HOSTNAME

/var/lib/setroubleshoot/email_alert_recipients

- dwalsh@redhat.com
[SELinux AVC Alert] SELinux is preventing /usr/sbin/httpd from read access on the file /var/www/html/index.html.

To Walsh, Daniel

SELinux is preventing /usr/sbin/httpd from read access on the file /var/www/html/index.html.

***** Plugin restorecon (92.2 confidence) suggests ***********************

If you want to fix the label, /var/www/html/index.html default label should be httpd_sys_content_t.
Then you can run restorecon.
Do

```
# /sbin/restorecon -v /var/www/html/index.html
```

***** Plugin catchall_boolean (7.83 confidence) suggests ***********************

If you want to allow httpd to read user content
Then you must tell SELinux about this by enabling the 'httpd_read_user_content' boolean.
What about RBAC?

How I confined my wife with SELinux?
Confined Users

- **Terminal user/ssh - guest_t**
  - No Network, No setuid, no exec in homedir
- **Browser user/kiosk - xguest_t**
  - Web access ports only. No setuid, no exec in homedir
- **Full Desktop user - User_t**
  - Full Network, No SETUID
- **Confined Admin/Desktop User - Staff_t**
  - Full Network, sudo to admin only, no root password.
  - Usually a confined admin
- **Unconfined user - unconfined_t (Default)**
  - SELinux does not block access
IDM/FreeIPA supports SELinux Confined Users

- At login sssd contacts FreeIPA for user@machine
- Downloads /etc/selinux/targeted/logins

```
cat dwalsh
sshd:staff_u:s0-s0:c0.c1023
*:guest_u:s0-s0:c0.c1023
```

- Sudo be configured by IPA with SELinux Config
  - dwalsh ALL=(ALL) TYPE=webadm_t ROLE=webadm_r ALL
Confined users using LDAP

- LDAP does not have User-Machine Mapping
- LDAP could be setup for global mapping
- /etc/selinux/targeted/seusers

```
  system_u:system_u:s0-s0:c0.c1023
  root:unconfined_u:s0-s0:c0.c1023
  __default__:unconfined_u:s0-s0:c0.c1023
  xguest:xguest_u:s0
  dwalsh:staff_u:s0-s0:c0.c1023
```
Confined Users Active Directory

• Being worked on
Questions?
Improving SELinux Usability

- SELinux UXD usability tests in the GSS booth.
- Added > 700 Man pages for each confined domain
- Adding GUI to be application focused
  - How does SELinux confine domain X?
    - What booleans? What Types? What Network Ports?
    - How can I modify them?