Pulp - Issue #3347

Advise users to use `setsebool` to set pulp_manage_rsync

02/07/2018 06:59 PM - Ichimonji10

Status:	CLOSED - CURRENTRELEASE		
Priority:	Normal		
Assignee:	bizhang		
Category:			
Sprint/Milestone:			
Severity:	2. Medium	**Sprint Candidate:**	No
Version:		**Tags:**	Documentation, Pulp 2
Platform Release:	2.15.3	**QA Contact:**	
Blocks Release:		**Complexity:**	
OS:		**Smash Test:**	
Backwards Incompatible:	No	**Verified:**	No
Triaged:	Yes	**Verification Required:**	No
Groomed:	Yes	**Sprint:**	Sprint 32

Description

On Fedora 27, the semanage executable can be used to set the **default** state of a boolean, but not its **current** state. To wit:

```
# semanage boolean --list | head -n 1
SELinux boolean                State  Default Description
# semanage boolean --modify --off pulp_manage_rsync
# semanage boolean --list | grep pulp_manage_rsync
pulp_manage_rsync              (off  ,  off)  Allow pulp to manage rsync
# semanage boolean --modify --on pulp_manage_rsync
# semanage boolean --list | grep pulp_manage_rsync
pulp_manage_rsync              (off  ,   on)  Allow pulp to manage rsync
```

Notice how semanage sets a policy's "default" state, but not its current state? In prior versions of Fedora, both the "state" and "default" fields would be updated by this command. To set the current state of a boolean, the setsebool command now has to be used:

```
# semanage boolean --list | grep pulp_manage_rsync
pulp_manage_rsync              (off  ,  off)  Allow pulp to manage rsync
# setsebool pulp_manage_rsync on
# semanage boolean --list | grep pulp_manage_rsync
pulp_manage_rsync              (on   ,  off)  Allow pulp to manage rsync
```

Note that this behaviour applies to other policies on F27, too. Here's another arbitrary policy that I arbitrarily picked out:

```
# semanage boolean --modify --on zoneminder_run_sudo
# semanage boolean --list | grep zoneminder_run_sudo
zoneminder_run_sudo            (off  ,   on)  Allow zoneminder to run sudo
# semanage boolean --modify --off zoneminder_run_sudo
# semanage boolean --list | grep zoneminder_run_sudo
zoneminder_run_sudo            (off  ,  off)  Allow zoneminder to run sudo
```

The docs currently advise using semanage here. Let's tell readers about setsebool too.

This change appears to be intentional. The system journal shows no errors. Here's the output of journalctl --follow for the time period in which semanage boolean --modify --on is executed:

```
-- Logs begin at Wed 2018-02-07 11:10:04 EST. --
Feb 07 12:26:07 fedora-27-pulp-2-16-nightly kernel: SELinux:  policy capability open_perms=1
Feb 07 12:26:07 fedora-27-pulp-2-16-nightly kernel: SELinux:  policy capability extended_socket_cl
ass=0
Feb 07 12:26:07 fedora-27-pulp-2-16-nightly kernel: SELinux:  policy capability always_check_netwo
rk=0
Feb 07 12:26:07 fedora-27-pulp-2-16-nightly kernel: SELinux:  policy capability cgroup_seclabel=1
Feb 07 12:26:07 fedora-27-pulp-2-16-nightly kernel: SELinux:  policy capability nnp_nosuid_transit
ion=1
Feb 07 12:26:07 fedora-27-pulp-2-16-nightly audit[710]: USER_AVC pid=710 uid=81 auid=4294967295 se
s=4294967295 subj=system_u:system_r:system_dbusd_t:s0-s0:c0.c1023 msg='avc:  received policyload n
otice (seqno=21)
                                                                exe="/usr/bin/dbus-daemon" sauid=81 hostn
ame=? addr=? terminal=?'
Feb 07 12:26:07 fedora-27-pulp-2-16-nightly audit: MAC_POLICY_LOAD policy loaded auid=0 ses=11
Feb 07 12:26:07 fedora-27-pulp-2-16-nightly dbus-daemon[710]: [system] Reloaded configuration
Feb 07 12:26:08 fedora-27-pulp-2-16-nightly audit[3829]: USER_START pid=3829 uid=0 auid=0 ses=11 s
ubj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login id=0 exe="/usr/sbin/sshd" hostname=? add
r=192.168.101.1 terminal=/dev/pts/1 res=success'
Feb 07 12:26:08 fedora-27-pulp-2-16-nightly audit[3829]: CRYPTO_KEY_USER pid=3829 uid=0 auid=0 ses
=11 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=destroy kind=server fp=SHA256:0f:7f:33:2b
:ba:6c:3a:16:47:19:de:04:1f:f7:1e:e1:61:53:9c:34:cd:0b:ea:dd:80:8d:30:66:1c:e4:a1:e9 direction=? s
pid=8428 suid=0  exe="/usr/sbin/sshd" hostname=? addr=? terminal=? res=success'
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux: 32768 avtab hash slots, 108540 rules.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux: 32768 avtab hash slots, 108540 rules.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  8 users, 14 roles, 5094 types, 318 b
ools, 1 sens, 1024 cats
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  97 classes, 108540 rules
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Permission getrlimit in class proces
s not defined in policy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class sctp_socket not defined in pol
icy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class icmp_socket not defined in pol
icy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class ax25_socket not defined in pol
icy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class ipx_socket not defined in poli
cy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class netrom_socket not defined in p
olicy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class atmpvc_socket not defined in p
olicy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class x25_socket not defined in poli
cy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class rose_socket not defined in pol
icy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class decnet_socket not defined in p
olicy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class atmsvc_socket not defined in p
olicy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class rds_socket not defined in poli
cy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class irda_socket not defined in pol
icy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class pppox_socket not defined in po
licy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class llc_socket not defined in poli
cy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class can_socket not defined in poli
cy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class tipc_socket not defined in pol
icy.
```

```
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class bluetooth_socket not defined i
n policy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class iucv_socket not defined in pol
icy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class rxrpc_socket not defined in po
licy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class isdn_socket not defined in pol
icy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class phonet_socket not defined in p
olicy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class ieee802154_socket not defined
in policy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class caif_socket not defined in pol
icy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class alg_socket not defined in poli
cy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class nfc_socket not defined in poli
cy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class vsock_socket not defined in po
licy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class kcm_socket not defined in poli
cy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class qipcrtr_socket not defined in
policy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux:  Class smc_socket not defined in poli
cy.
Feb 07 12:26:18 fedora-27-pulp-2-16-nightly kernel: SELinux: the above unknown classes and permiss
ions will be allowed
Feb 07 12:26:20 fedora-27-pulp-2-16-nightly kernel: SELinux:  policy capability network_peer_contr
ols=1
Feb 07 12:26:20 fedora-27-pulp-2-16-nightly kernel: SELinux:  policy capability open_perms=1
Feb 07 12:26:20 fedora-27-pulp-2-16-nightly kernel: SELinux:  policy capability extended_socket_cl
ass=0
Feb 07 12:26:20 fedora-27-pulp-2-16-nightly kernel: SELinux:  policy capability always_check_netwo
rk=0
Feb 07 12:26:20 fedora-27-pulp-2-16-nightly kernel: SELinux:  policy capability cgroup_seclabel=1
Feb 07 12:26:20 fedora-27-pulp-2-16-nightly kernel: SELinux:  policy capability nnp_nosuid_transit
ion=1
Feb 07 12:26:20 fedora-27-pulp-2-16-nightly audit[710]: USER_AVC pid=710 uid=81 auid=4294967295 se
s=4294967295 subj=system_u:system_r:system_dbusd_t:s0-s0:c0.c1023 msg='avc:  received policyload n
otice (seqno=22)
                                                    exe="/usr/bin/dbus-daemon" sauid=81 hostn
ame=? addr=? terminal=?'
Feb 07 12:26:20 fedora-27-pulp-2-16-nightly audit: MAC_POLICY_LOAD policy loaded auid=0 ses=11
Feb 07 12:26:20 fedora-27-pulp-2-16-nightly dbus-daemon[710]: [system] Reloaded configuration
```

Associated revisions

Revision d337f46f - 02/19/2018 05:45 PM - werwty

Advise users on using setsebool to set pulp_manage_rsync selinux boolean

F27+ changed the behavior of semanage to set a selinux boolean by
default, but not change its current state.

re #3347
https://pulp.plan.io/issues/3347

Revision b6f3f042 - 02/19/2018 05:46 PM - werwty

Advise users on using setsebool to set pulp_manage_rsync selinux boolean

F27+ changed the behavior of semanage to set a selinux boolean by
default, but not change its current state.

re #3347
https://pulp.plan.io/issues/3347

Revision b6f3f042 - 02/19/2018 05:46 PM - werwty

Advise users on using setsebool to set pulp_manage_rsync selinux boolean

F27+ changed the behavior of semanage to set a selinux boolean by
default, but not change its current state.

re #3347
https://pulp.plan.io/issues/3347

Revision 93f876bb - 02/19/2018 05:47 PM - werwty

Advise users on using setsebool to set pulp_manage_rsync selinux boolean

F27+ changed the behavior of semanage to set a selinux boolean by
default, but not change its current state.

closes #3347
https://pulp.plan.io/issues/3347

Revision a5dbbf3f - 03/12/2018 06:05 PM - werwty

Advise users on using setsebool to set pulp_manage_rsync selinux boolean

F27+ changed the behavior of semanage to set a selinux boolean by
default, but not change its current state.

closes #3347
https://pulp.plan.io/issues/3347

(cherry picked from commit 93f876bb038ca7224fbdb0b2b522fb42cded5cbc)

Revision bc55e044 - 03/12/2018 06:06 PM - werwty

Advise users on using setsebool to set pulp_manage_rsync selinux boolean

F27+ changed the behavior of semanage to set a selinux boolean by
default, but not change its current state.

re #3347
https://pulp.plan.io/issues/3347

(cherry picked from commit d337f46fe34528f0a20796ccdba0d75ebbe213a3)

Revision 1842120e - 03/12/2018 07:07 PM - werwty

Advise users on using setsebool to set pulp_manage_rsync selinux boolean

F27+ changed the behavior of semanage to set a selinux boolean by
default, but not change its current state.

re #3347
https://pulp.plan.io/issues/3347

(cherry picked from commit b6f3f042d06077a844b35bfad8f1c752b4975d41)

Revision 1842120e - 03/12/2018 07:07 PM - werwty

Advise users on using setsebool to set pulp_manage_rsync selinux boolean

F27+ changed the behavior of semanage to set a selinux boolean by
default, but not change its current state.

re #3347
https://pulp.plan.io/issues/3347

(cherry picked from commit b6f3f042d06077a844b35bfad8f1c752b4975d41)

History

#1 - 02/07/2018 07:22 PM - lchimonji10

Also see: https://github.com/PulpQE/pulp-smash/pull/857

#2 - 02/07/2018 08:11 PM - dalley

- Sprint/Milestone set to 54

- Triaged changed from No to Yes

- Groomed changed from No to Yes

#3 - 02/19/2018 04:43 PM - bizhang

- Status changed from NEW to ASSIGNED

- Assignee set to bizhang

#4 - 02/19/2018 05:22 PM - bizhang

- Status changed from ASSIGNED to POST

PR: https://github.com/pulp/pulp_rpm/pull/1085
https://github.com/pulp/pulp_puppet/pull/270
https://github.com/pulp/pulp_docker/pull/224

#5 - 02/19/2018 07:20 PM - werwty

- Status changed from POST to MODIFIED

Applied in changeset pulp_rpm:93f876bb038ca7224fbdb0b2b522fb42cded5cbc.

#6 - 03/05/2018 05:27 PM - bmbouter

- Platform Release set to 2.15.3

#7 - 03/09/2018 12:32 AM - bmbouter

- Sprint set to Sprint 32

#8 - 03/09/2018 12:33 AM - bmbouter

- Sprint/Milestone deleted (54)

#9 - 03/12/2018 06:06 PM - werwty

Applied in changeset pulp_rpm:a5dbbf3fbee4f0d192fe799c3f05f448110774ae.

#10 - 03/16/2018 12:25 PM - bmbouter

- Status changed from MODIFIED to ON_QA

#11 - 03/20/2018 04:04 PM - bmbouter

- Status changed from ON_QA to CLOSED - CURRENTRELEASE

#12 - 04/15/2019 10:13 PM - bmbouter

- Tags Pulp 2 added