Pulp - Issue #1764

SELinux denial on Celery attempting to read resolv.conf

03/09/2016 10:48 PM - rbarlow

Status:	CLOSED - CURRENTRELEASE	**Start date:**	
Priority:	High	**Due date:**	
Assignee:	rbarlow	**Estimated time:**	0:00 hour
Category:			
Sprint/Milestone:			
Severity:	3. High	**Groomed:**	No
Version:	Master	**Sprint Candidate:**	No
Platform Release:	2.8.3	**Tags:**	Pulp 2
OS:	Fedora Rawhide	**Sprint:**	
Triaged:	Yes	**Quarter:**	

Description

It seems that we are missing an SELinux permission and are being denied read access on the resolv.conf file:

```
type=AVC msg=audit(1457559807.664:2336): avc:  denied  { read } for  pid=4876 comm="celery" name="
resolv.conf" dev="dm-0" ino=261406 scontext=system_u:system_r:celery_t:s0 tcontext=system_u:object
_r:net_conf_t:s0 tclass=lnk_file permissive=0
```

audit2allow recommends this policy change:

```
$ sudo audit2allow -al

#============= celery_t ==============
allow celery_t net_conf_t:lnk_file read;
```

Associated revisions

Revision c1011cde - 03/16/2016 09:26 PM - Randy Barlow

Allow the Celery process to resolve domain names.

Fedora Rawhide restricts access to /etc/resolv.conf. This commit adds the sysnet_dns_name_resolve policy to the celery_t context which allows it to resolve hostnames.

https://pulp.plan.io/issues/1764

fixes #1764

Revision c1011cde - 03/16/2016 09:26 PM - Randy Barlow

Allow the Celery process to resolve domain names.

Fedora Rawhide restricts access to /etc/resolv.conf. This commit adds the sysnet_dns_name_resolve policy to the celery_t context which allows it to resolve hostnames.

https://pulp.plan.io/issues/1764

fixes #1764

Revision d2521fab - 03/30/2016 09:47 PM - Randy Barlow

Allow the Celery process to resolve domain names.

Fedora Rawhide restricts access to /etc/resolv.conf. This commit adds the auth_use_nss policy to the celery_t context which allows it to resolve hostnames.

https://pulp.plan.io/issues/1764

fixes #1764

Revision d2521fab - 03/30/2016 09:47 PM - Randy Barlow

Allow the Celery process to resolve domain names.

Fedora Rawhide restricts access to /etc/resolv.conf. This commit adds the auth_use_nss policy to the celery_t context which allows it to resolve hostnames.

https://pulp.plan.io/issues/1764

fixes #1764

History

#1 - 03/09/2016 11:14 PM - rbarlow

I believe that this is more than just an SELinux issue. It seems that the sender parameter we are receiving from Celery in our initialize_worker() function is not the hostname of the worker, as documented by us and by Celery. Instead, on Fedora Rawhide it is "resource_manager@/root". This is the reason we are receiving the "No such file or directory" error.

I've filed a Celery bug about the incorrect documentation, as well as the missing hostname.

I believe the missing hostname will not be a problem for us, as we do not recommend that our users share /var/cache/pulp across machines.

https://github.com/celery/celery/issues/3104

#2 - 03/10/2016 05:45 PM - rbarlow

- Subject changed from Pulp celery workers cannot start on Fedora Rawhide, and likely Fedora 24 to SELinux denial on Celery attempting to read resolv.conf

- Severity changed from 3. High to 2. Medium

This non-starting turned out to be a bug in systemd, and it looks like there was even an update to the systemd package overnight that fixed it on my dev box. Isn't it great when bugs get fixed without you even having to report them? The issue was that our unit files were using the %%h macro to substitute the hostname into Celery's --hostname argument. It turned out that systemd had been substituting "/root" instead of the hostname.

However, the SELinux denial remains so I am leaving this ticket open.

#3 - 03/10/2016 06:20 PM - rbarlow

- Severity changed from 2. Medium to 3. High

This SELinux denial is causing Celery to be unable to resolve hostnames. During a docker sync, I see this error:

```
Mar 10 12:18:56 boole.usersys.redhat.com pulp[1601]: nectar.downloaders.threaded:WARNING: Skipping requests to
 registry-1.docker.io due to repeated connection failures: HTTPSConnectionPool(host='registry-1.docker.io', po
rt=443): Max retr
ies exceeded with url: /v2/ (Caused by NewConnectionError('<requests.packages.urllib3.connection.VerifiedHTTPS
Connection object at 0x7fa5a8872510>: Failed to establish a new connection: [Errno -2] Name or service not kno
wn',))
```

#4 - 03/10/2016 06:20 PM - rbarlow

- Description updated

#5 - 03/11/2016 05:11 PM - mhrivnak

- Status changed from NEW to ASSIGNED

- Assignee set to rbarlow

- Platform Release set to 2.8.1

- Triaged changed from No to Yes

#6 - 03/11/2016 09:34 PM - rbarlow

- Status changed from ASSIGNED to POST

I am still testing this change, but here is a pull request with a fix that does work on Rawhide:

https://github.com/pulp/pulp/pull/2477

#7 - 03/11/2016 11:50 PM - rbarlow

After running pulp-smash, I see one more recommendation from audit2allow:

```
#============= celery_t ==============
allow celery_t self:process setrlimit;
```

#8 - 03/16/2016 09:31 PM - Anonymous

- Status changed from POST to MODIFIED

- % Done changed from 0 to 100

Applied in changeset pulp|c1011cde0b26a48ac75af8fd7b31755c468f6095.

#9 - 03/23/2016 07:56 PM - semyers

- Status changed from MODIFIED to 5

#10 - 03/30/2016 09:47 PM - Anonymous

- Status changed from 5 to MODIFIED

Applied in changeset pulp|d2521fabb524ec0faafa77eeb0432145bca3e70d.

#11 - 04/05/2016 10:39 PM - semyers

- Platform Release changed from 2.8.1 to 2.8.2

#12 - 04/06/2016 10:24 PM - semyers

- Platform Release changed from 2.8.2 to 2.8.3

#13 - 04/27/2016 12:38 AM - semyers

- Status changed from MODIFIED to 5

#14 - 05/10/2016 03:01 PM - pthomas@redhat.com

- Status changed from 5 to 6

verified

```
[root@ibm-x3550m3-09 ~]# sudo audit2allow -al

[root@ibm-x3550m3-09 ~]# rpm -qa |grep pulp
python-pulp-common-2.8.3-0.2.beta.el7.noarch
python-kombu-3.0.33-5.pulp.el7.noarch
python-pulp-rpm-common-2.8.3-0.2.beta.el7.noarch
pulp-server-2.8.3-0.2.beta.el7.noarch
pulp-docker-plugins-2.0.1-0.2.beta.el7.noarch
pulp-admin-client-2.8.3-0.2.beta.el7.noarch
python-isodate-0.5.0-4.pulp.el7.noarch
python-pulp-puppet-common-2.8.3-0.2.beta.el7.noarch
python-pulp-docker-common-2.0.1-0.2.beta.el7.noarch
python-pulp-oid_validation-2.8.3-0.2.beta.el7.noarch
pulp-rpm-plugins-2.8.3-0.2.beta.el7.noarch
pulp-puppet-plugins-2.8.3-0.2.beta.el7.noarch
python-pulp-bindings-2.8.3-0.2.beta.el7.noarch
pulp-puppet-admin-extensions-2.8.3-0.2.beta.el7.noarch
pulp-docker-admin-extensions-2.0.1-0.2.beta.el7.noarch
python-pulp-streamer-2.8.3-0.2.beta.el7.noarch
python-pulp-repoauth-2.8.3-0.2.beta.el7.noarch
pulp-selinux-2.8.3-0.2.beta.el7.noarch
python-pulp-client-lib-2.8.3-0.2.beta.el7.noarch
pulp-rpm-admin-extensions-2.8.3-0.2.beta.el7.noarch
[root@ibm-x3550m3-09 ~]#
```

#15 - 05/17/2016 09:31 PM - semyers

- Status changed from 6 to CLOSED - CURRENTRELEASE

#17 - 04/15/2019 10:33 PM - bmbouter

- Tags Pulp 2 added