Packaging - Issue #7189

SELinux policy doesn't using systemd's Type=notify

07/22/2020 04:00 PM - ekohl

Status:	NEW	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**Estimated time:**	0:00 hour
Category:			
Sprint/Milestone:			
Severity:	2. Medium	**Groomed:**	No
Version - Packaging:		**Sprint Candidate:**	No
Platform Release:		**Tags:**	SELinux
Target Release - Packaging:		**Sprint:**	
OS:		**Quarter:**	
Triaged:	No		

Description

gunicorn can use the systemd Type=notify (see https://docs.gunicorn.org/en/stable/deploy.html#systemd and https://www.freedesktop.org/software/systemd/man/systemd.service.html#Type=). However, the SELinux policy doesn't allow the creation of unix_dgram_socket.

This blocks the use of systemd socket activation which would be much more secure. Currently the process listens on 127.0.0.1:24817 which means anyone who can open a socket connection there can impersonate any admin user. That gives full API control to users who would normally be unauthenticated. By using systemd's socket activation, we can listen on /run/pulpcore-{api,content}.sock with apache as the owner and mode 0600. That means only Apache can access the socket.

There may be more permissions needed for this. I only tested with just using Type=notify, not with an actual socket.