CIS Docker 1.11 Benchmark – Discussion of Items Not Scored/Tested

1.3 Harden the container host – Cannot be tested, should be taken as a direction to the user

1.4 Remove all non-essential services from the host – Could potentially become a scored test in one of two ways: 1) if we have a list of all required services on host, can test to ensure no other services, or 2) can test to ensure that certain services at least are not on the host

1.5 Keep Docker up to date – Currently modified to ensure version is at least 1.10.3, could be modified again to ensure an exact version

2.7 Set default ulimit as appropriate – Currently scored to test nproc=1024:2048 and noline=100:200

4.2 Use trusted base images for containers – Cannot be tested, should be taken as a direction to the user

4.3 Do not install unnecessary packages in the container – Could potentially become a scored test in one of two ways: 1) if we have a list of all required packages for the container, can test to ensure no other packages, or 2) can test to ensure certain packages at least not in container

4.4 Rebuild the images to include security patches – Cannot be tested, should be taken as a direction to the user

5.8 Open only needed ports on container – Not currently implemented as test, but could be once it is known what ports are needed for the container

5.17 Do not directly expose host devices to containers – Currently implemented as a test to ensure that no host devices can be accessed from the container, can be modified if it is determined that a container must access a host device

5.18 Override default ulimit at runtime only if needed – Currently implemented as a test to ensure that no container can override the default ulimit settings, can be modified if it is determined that a container needs to override the ulimit settings

6.1 Perform regular security audits of your host system and containers – Cannot be tested, should be taken as a direction to the user

6.2 Monitor Docker containers usage, performance and metering – Cannot be tested, should be taken as a direction to the user

6.3 Backup container data – Cannot be tested, should be taken as a direction to the user

6.4 Avoid image sprawl – Currently implemented as a test that determines the difference between the instantiated images and the images present on the system (assumes no need to keep old and unused images on system)

6.5 Avoid container sprawl – Currently implemented as a test that determines whether the number of containers is less than or equal to the user-defined manageable number of contaienrs