**GSA’s Server-based Certificate Validation Protocol (SCVP) test program (GSTP)**

Artifact Publication Guide

[This page intentionally left semi-blank]

Revision History

|  |  |
| --- | --- |
| Date | Notes |
| 2017-08-08 | First draft |
| 2017-08-16 | Update relative to delivered tools VM |
|  |  |
|  |  |

1 Overview 5

2 Quick Start 6

3 Generating and Publishing New Artifacts 7

3.1 PCP 7

3.2 Processing the Exported Artifacts 9

3.2.1 OCSP 9

3.2.2 Generating Apache Configurations 9

3.2.3 Deploying Apache Configurations 9

# Overview

This document provides guidance on republishing the artifacts used to support the GSA SCVP Test Program (GSTP). It is not anticipated that most users of the test program will find this to be necessary. Basic deployment steps using the existing VMs as well as direction for using an EC2-hosted instance is provided in the User Guide. The steps in this guide should only be necessary when artifacts are regenerated.

Two pre-configured Centos 7 Virtual Machines (VMs) are supplied with the test artifacts. The Tools VM contains PCP itself, the pcp databases used to generate artifacts, and assorted test and management utilities that facilitate publication of the artifacts. The Hosting VM is a minimal installation of Centos 7 with an apache httpd configured to host serve artifacts from host names that appear in Authority Information Access (AIA) and CRL Distribution Point (CRLDP) extensions in the generated certificates. It also contains OCSP responders that can answer requests for those certificates that have an OCSP AIA.

An EC2 instance named ficam-scvp-artifacts is also available. Its configuration is the same as the local hosting VM relative to artifact hosting.

# Quick Start

The most common need will be updating artifacts that have already been published. This is straightforward on a VM that is already configured to host an existing set. If no new hostnames have been added, all that’s necessary is placing a copy of the Hosts directory from the PCP export into /srv/sites on the VMs and ensuring that filesystem permissions are appropriate.

$ scp -r Hosts vmadmin@10.142.42.2:/tmp

$ ssh vmadmin@10.142.42.2

$ sudo -i

# cd /tmp

# systemctl stop httpd

# /bin/cp -rv Hosts/\* /srv/sites/

# find /srv/sites -type d -exec chmod 755 {} \;

# find /srv/sites -type f -exec chmod 644 {} \;

# chown -R vmadmin:apache /srv/sites/

# systemctl start httpd

Similarly, if OCSP responders were changed, simply copy the ocsp directory from the PCP export and stop/start all of the responders.

$ scp -r ocsp vmadmin@10.142.42.2:/tmp

$ ssh vmadmin@10.142.42.2

$ sudo -i

# cd /srv/ocsp

# bash stopall.sh

# /bin/cp -rv /tmp/ocsp/\* /srv/ocsp/

# bash startall.sh

The remainder of this document explains more advanced cases.

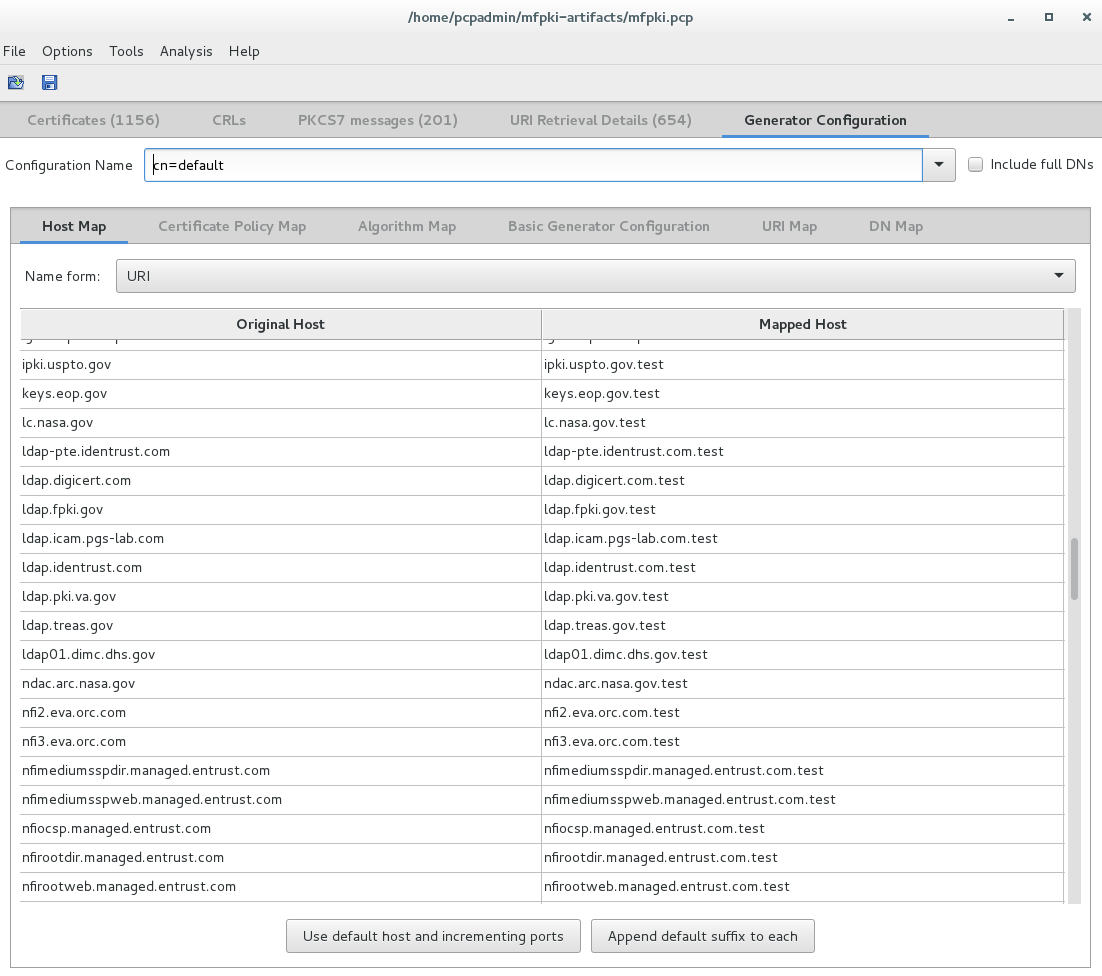
# Generating and Publishing New Artifacts

When new CAs (and especially new URLs) are added to the artifact collection, additional steps are necessary. This section is intended to highlight steps that are specifically relevant for publication. **Prior to executing these steps, follow the detailed procedures in the SCVP test program artifacts guide when regenerating any of the current datasets.**

## PCP

The steps in this section are **only** necessary for the MFPKI dataset; for all others, the artifacts produced by following the steps in the test program artifacts guide are consumed directly.

Within PCP, first ensure that all newly added hosts are mapped to .test. This is done on the “Host Map” tab within the Generator Configuration.



Also ensure that all single component DNs have “o=Mock” added to them, and that all Domain Component names get “dc=mock” also.

Save the database and exit PCP.

From a terminal within the pcp-scripts directory, first activate the python 2.7 virtual environment then run MapHttpsDps.py on the database to change any https references in that database to a high port plaintext http reference. Edit the vmconfig.ini file to reflect any restrictions that might be imposed within your environment, such as starting port numbers for HTTP and OCSP.

$ source ~/pcp/venv-pcp/bin/activate

$ python MapHttpsDps.py -d mfpki.pcp

Once that is complete, it’s necessary to map responder ports in a similar way. From a terminal in the same directory, first deactivate the 2.7 virtual environment and activate the 3.4 virtual environment, then run the MapResponders script.

(venv-pcp)[pcpadmin@pcp-host pcp-scripts]$ deactivate

[pcpadmin@pcp-host pcp-scripts]$ source ~/pcp/venv-py34-pcp/bin/activate

(venv-py34-pcp) [pcpadmin@pcp-host pcp-scripts]$ python MapResponders.py -d mfpki.pcp

Once this is complete, re-open the database in PCP, generate and export.

## Processing the Exported Artifacts

Once the artifacts have been generated and exported, a few additional steps are necessary prior to publication. After completing these steps, follow the Quick Start guide for publishing the artifacts.

### OCSP

For MFPKI, the OCSP responders must be generated next. Other datasets do not use OCSP AIAs.

To generate the responders, activate the python 3.4 virtual environment and execute the DumpResponders.py script:

$ source ~/pcp/venv-py34-pcp/bin/activate

$ python DumpResponders.py -d mfpki.pcp -o ocsp

### Generating Apache Configurations

For all datasets, apache configurations must be generated. This step only needs to be re-run when new AIA or CRLDP hosts are introduced to a dataset. In addition to generating apache configurations, this step generates a hosts file. Update the host VM’s IP address in vmconfig.ini to control the IP that lands in the hosts file.

$ source ~/pcp/venv-py34-pcp/bin/activate

$ python PrepareVHosts.py -d mfpki.pcp -o vhost-httpd-config

### Deploying Apache Configurations

When a virtual host is added or removed, it is necessary to copy all of the vhost\_\*.conf files generated above to /etc/httpd/conf.d on the target host VM.