CEF: Cybersecurity Digital Service Infrastructure;

Core Service Platform – SMART 2015/1089

Version: 4.0.1

Date: 26/04/2019

Central Installation Manual

Contents

1 Introduction

This manual covers the installation of a central CSP system within an organization as well as the installation of the corresposding CSP modules that each Central CSP system should have installed.

Prerequisities

Before starting the procedure of installing and configuring a Central CSP system please make sure you have prepared the following:

- You have obtained **CSP Installation Manual** at its latest version, as it is referenced in this document.
- You have completed Preparatory steps, as described in chapter 1 of manual: **CSP Installation Manual**.
    - Regarding virtual hardware requirements of the VM (downloaded in OVA format) you may refer to chapter **8 (Annex A: Changing settings of the VM)** of manual: **CSP Installation Manual**. It is highly that you perform the steps mentioned there before proceeding to the installation of Central CSP.
    - Regarding software requirements of Central CSP, OS of Central CSP has to be Alpine 3.7 latest, which however is the OS version in the OVA you have received by email.
- You have prepared your network infrastructure, as described in chapter 2 of manual: **CSP Installation Manual**.
    - Additionally, you have to register a DNS entry for the Central CSP and its assigned IP, which is not listed in **CSP Installation Manual**. The DNS entry has to be formatted as: **central.<cspId>.[preprod.]melicertes.eu**, where <cspId> is your assigned CSP ID.
    - You have to ensure that Central CSP's port 22 (SSH) is accessible only by you (or your organization's administrator).
    - You have to ensure that Central CSP's port 5443 is accessible within your organization, as this is required for CSP installer's updates feature.
- You have downloaded the required certificates for the Central CSP, as is described in chapter 3 of manual: **CSP Installation Manual**
- You have received/downloaded a *.zip file named **central.zip**, which required software to setup the Central CSP instance. Please refer to chapter 6 (Annex A: Contents of central.zip for CSP version 4) of this manual.
- You have received/downloaded a *.zip file named **4.x.y-modules.zip**, which contains all modules of CSP version 4 that should be uploaded in Central CSP so as to be available in others CSP that refer to the Central CSP that is to be created. Please refer to chapter 7 (Annex B: Contents of zip file for CSP version 4 modules) of this manual.
- Optionally, you may have received updated version of the CSP Installer application that is also distributed to the CSP Nodes via Central CSP, i.e. a file named: conf-client-cspapp-4.0.6-SNAPSHOT.jar
- You can access the VM to be installed as Central CSP via SSH

2 Environment preparation

Following steps describe a set of shell commands that have to be executed in the order presented here in order to prepare the environment of the Central CSP installation.

Step 1

Login via SSH port 22 to the VM created for the Central CSP. Login credentials are: user: **`root`** and password: **`systempass`**.

You may use third party software (i.e. PuTTY, as described in section **4.2** of manual: **CSP Installation Manual**) or the command:

```
#   ssh root@{central hostname}
```

in a Linux terminal, where {central hostname} is the hostname or IP of the Central CSP machine.

Step 2

Execute the command to update the locale database of system packages:

```
#   apk update
```

Step 3

Execute the command to install docker:

```
#   apk add docker
```

Step 4

Execute the command to verify that the proper docker version is installed:

```
#   docker --version
```

The following should be displayed in your terminal:

```
#   Docker version 18.06.1-ce, build d72f525745
```

Step 5

Execute the command to verify docker is correctly installed:

```
#   docker run hello-world
```

The following should be displayed in your terminal:

```
#   Hello from Docker!
#   This message shows that your installation appears to be working correctly.
#
#   To generate this message, Docker took the following steps:
```

```
#    1. The Docker client contacted the Docker daemon.
#    2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
#       (amd64)
#    3. The Docker daemon created a new container from that image which runs the
#       executable that produces the output you are currently reading.
#    4. The Docker daemon streamed that output to the Docker client, which sent
   it
#       to your terminal.
#
#  To try something more ambitious, you can run an Ubuntu container with:
#    $ docker run -it ubuntu bash
#
#  Share images, automate workflows, and more with a free Docker ID:
#    https://hub.docker.com/
#
#  For more examples and ideas, visit:
#    https://docs.docker.com/get-started/
```

Step 6

Execute the command to install the curl tool:

```
#  apk add curl
```

Step 7

Execute the command to install docker-compose:

```
#  sudo                                curl                                -L
   "https://github.com/docker/compose/releases/download/1.22.0/docker-compose-
   $(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose
```

Step 8

Execute the command set proper permissions at the docker-compose:

```
#  sudo chmod +x /usr/local/bin/docker-compose
```

Step 9

Execute the command to verify you have installed the proper docker-compose version:

```
#  docker-compose --version
```

The following should be displayed in your terminal:

```
#  docker-compose version 1.22.0, build f46880f
```

3 Central CSP Installation – CSP Central role

At this stage all CSP modules should be uploaded and registered in Central CSP so as to be available in other CSPs for installation and/or updating their modules. To complete this phase the following steps have to be executed.

Step 1

Login via SSH port 22 to the VM created for the Central CSP. Login credentials are: user: **`root`** and password: **`systempass`** and also add a Port Forward rule for port 19090.

You may use third party software (i.e. PuTTY, as described in section **4.2** of manual: **CSP Installation Manual**) or the command:

```
#   ssh root@{central hostname} -L 19090:localhost:19090
```

in a Linux terminal, where {central machine hostname} is the hostname or IP of the Central CSP machine.

Step 2

Execute the command:

```
#   mkdir -p /home/central/
```

Step 3

Upload received file: **central.zip** to the directory: **/home/central**

You may use third party SFTP-related software (i.e. FileZilla) or SCP command:

```
#   scp {local path of central.zip} root@{central hostname}:/home/central/
```

in a Linux terminal, where:

- {local path of central.zip} is the local full path of the received file: central.zip
- {central hostname} is the hostname or IP of the Central CSP machine

Step 4

Execute the command to change directory:

```
#   cd /home/central/
```

Step 5

Execute the command to unzip the central.zip file:

```
#   unzip central.zip
```

The contents of file central.zip should be displayed in your terminal.

Step 6

Execute the command:

```
#   sh first-time.sh
```

Some informative messages should be displayed in your terminal. You have to wait for the command to finish.

Step 7

Execute the command:

```
#   docker-compose up -d
```

Step 8

At this step all CSP modules have to be registered via the configuration UI of Central CSP, which can be reached by opening a browser and navigating to URL: **http://localhost:19090**

For more information on registering a new module you may refer to manual: **CSP Central Configuration Manual** and specifically to section: **3.4 (Register a new Module)**.

Below is the complete list of the modules that have to be registered with all required information. Please be careful to the **Start Priority** field that should be entered as provided.

Table 1. Complete list of CSP Modules to be registered

#	Short Name	Start Priority	Default
1	base	0	No
2	postgres	100	No
3	redis	110	Yes
4	oam	200	No
5	cfg	301	No
6	ActiveMQ	400	No
7	anon	500	No
8	il	501	No
9	mocknode	502	No
10	es	800	No
11	kibana	801	No
12	logs	802	No
13	owncloud	820	No
14	trustcircles	900	No
15	misp	901	No
16	rt	902	Yes
17	intelmq	903	Yes
18	regrep	904	No
19	vcb	905	No

20	viper	906	No
21	apache crl	980	No
22	apache	990	No

Step 9

At this step the latest update/version of each CSP Module has to be uploaded and registered.

For more information on registering a new module you may refer to manual: **CSP Central Configuration Manual** and specifically to section: **4.4 (Register a new Module Version)**.

Below is the complete list of the module versions that have to be registered per module with all required information. Please notice that Description field is indicative.

Table 2. Complete list of updates/versions per CSP Module to be registered

#	Module	Version	File to be uploaded	Description
1	base	4.0.004	csp-basemodule-2018-09-03T1243-4.0.4.zip	Updated base modules for 4.0.4 (20180903 build)
2	postgres	2.0.000	csp-postgres-20180216.zip	pg 19/2
3	redis	3.6.001	csp-redis-20180529-3.6.001.zip	2018-05-29: added empty “external_host”
4	oam	3.6.005	csp-openam-20180605-3.6.005.zip	2018-06-05: fix for update-datastore line
5	cfg	3.6.006	csp-configuration-20180626-3.6.000.zip	Port fix
6	ActiveMQ	3.8.001	csp-activemq-20180719-3.8.0.zip	ActiveMQ Module
7	anon	4.0.001	csp-anonymization-20180831-4.0.001.zip	anonymization in arrays element fix
8	il	4.0.001	csp-integrationlayer-20180831-4.0.001.zip	vulnerability routing fixes
9	mocknode	2.0.001	csp-mocknode-20180220.zip	Migrating mockservices to node
10	es	4.0.002	csp-elasticsearch-20180903-4.0.002.zip	Elasticsearch with new misp-vulnerability support latest fix
11	kibana	2.0.000	csp-kibana-20180216.zip	kibana 19/2
12	logs	3.6.007	csp-logs-20180518-3.6.007.zip	3.6.007
13	owncloud	3.6.001	csp-owncloud-20180518-3.6.001.zip	Port moved to 6443 for public access
14	trustcircles	3.8.001	csp-trustcircles-20180801-3.8.001.zip	Fixed TeamContact sharing of field "description" Remove csp_id uniqueness requirement in TeamContacts
15	misp	4.0.002	csp-misp-20180831-4.0.002.zip	fix docker-compose
16	rt	3.6.003	csp-rt-20180620-3.6.003.zip	FIX the https://git-csp.athens.intrasoft-intl.private/csp/sxcsp/issues/4. There are NO log files from RT adapter under /opt/csp/logs added -

				/opt/csp/logs/:/opt/csplogs to dicker-compose volumes:
17	intelmq	4.0.005	csp-intelmq-20180919-4.0.5.zip	20180919 build
18	regrep	4.0.001	csp-regularreports-20180831-4.0.001.zip	Regular Reports with the latest fixes
19	vcb	3.8.002	csp-vcb-20180718-3.8.002.zip	vcb:3.8.002
20	viper	4.0.003	csp-viper-20180831-4.0.003.zip	image fix
21	apache crl	4.0.004	csp-apache-crl-20180917-4.0.4.zip	20180917 build
22	apache	4.0.006	csp-apache-20180920-4.0.6.zip	20180920 build

4 Central CSP Installation – CSP Node role

At this stage Central CSP has to be registered as a CSP instance. Also a set of CSP Modules have to be assigned and installed in the Central CSP.

Step 1

Login via SSH port 22 to the VM created for the Central CSP. Login credentials are: user: **`root`** and password: **`systempass`** and also add two (2) Port Forward rules for ports 18080 and 19090.

You may use third party software (i.e. PuTTY, as described in section **4.2** of manual: **CSP Installation Manual**) or the command:

```
# ssh root@{central hostname} -L 18080:localhost:18080 -L
19090:localhost:19090
```

in a Linux terminal, where {central machine hostname} is the hostname or IP of the Central CSP machine.

Step 2

At this step Central CSP is going to be registered as a CSP instance via the CSP Installer UI which can be reached by opening a browser and navigating to URL: **http://localhost:18080**

At this point you may refer to manual: **CSP Installation Manual** and specifically to sections: **5.1 (Installation of certificates)** and **5.2 (CSP Instance registration)**.

Notice:

*SMTP configuration details can be omitted since they are required for CSP modules **vcb** and **regrep**, which are not going to be installed in Central CSP.*

Step 3

At this step the CSP instance of Central CSP has to be assigned to receive updates. This can be done via the Configuration UI of Central CSP, which can be reached by opening a browser and navigating to URL: **http://localhost:19090**

At this point you may refer to manual: **CSP Central Configuration Manual** and specifically to section: **5.2 (Assignment of Module's Versions to organization's registered CSPs)** in order to assign CSP Modules to the newly registered CSP Instance of Central CSP.

Below is the complete list with the CSP Modules that have to be assigned to the Central CSP. Please note that ONLY the below listed CSP Modules are expected to be assigned to a Central CSP.

Table 3. List of CSP Modules to be assigned in Central CSP

#	Short Name	Version (or latest)
1	base	4.0.004
2	postgres	2.0.000
3	oam	3.6.005

4	ActiveMQ	2.8.001
5	cfg	3.6.006
6	anon	4.0.001
7	il	4.0.001
8	mocknode	2.0.001
9	es	4.0.002
10	kibana	2.0.000
11	logs	3.6.007
12	trustcircles	3.8.001
13	apache crl	4.0.004
14	apache	4.0.006

Step 4

At this step CSP Modules assigned to the Central CSP are going to be downloaded and installed via the CSP Installer UI which can be reached by opening a browser and navigating to URL: **http://localhost:18080**

At this point you may refer to manual: **CSP Installation Manual** and specifically to sections: **5.3 (Download of system updates)** and **5.4 (Modules installation)**.

Step 5

At this step Central CSP is going to be started as a CSP instance via the CSP Installer UI which can be reached by opening a browser and navigating to URL: **http://localhost:18080**

At this point you may refer to manual: **CSP Installation Manual** and specifically to sections: **6.1 (Starting)** and **6.2 (Stopping)**.

Assuming you have started Central CSP and all installed modules (except base and cfg) of Table 3 are reporting Running state, you may perform Smoke tests of the Central CSP installation, as described in chapter **7 (Smoke-testing the Installation)** of manual: **CSP Installation Manual**.

Important notice #1:

After executing the command:

```
#   docker stats --all --format "table {{.Name}}\t{{.CPUPerc}}\t{{.MemUsage}}" --no-stream | sort
```

as it is described in chapter **7 (Smoke-testing the Installation)** of manual: **CSP Installation Manual** the output should include the following CSP-related lines:

```
#   csp-anon
#   csp-apache
```

```
#   csp-apache-crl
#   csp-es
#   csp-filebeat
#   csp-il
#   csp-kibana
#   csp-kibana_logs
#   csp-logstash
#   csp-misp-filebeat
#   csp-misp-logstash
#   csp-mock
#   csp-oam
#   csp-oam-filebeat
#   csp-oam-logstash
#   csp-postgres
#   csp-sa_cfg
#   csp-sa_cfg_client
#   csp-tc
#   csp-tc-dsl
```

Important notice #2:

Individual services that have to be smoke-tested, as it is described in section **7.2 (Connecting to individual services)** of manual: **CSP Installation Manual** are:

Table 4. Individual CSP-services that need to be smoke-tested

#	Module	URL
1	oam	https://auth.{central CSP DNS}/openam
2	anon	https://anon-ui.{central CSP DNS}
3	il	https://integration-ui.{central CSP DNS}
4	kibana	https://search.{central CSP DNS}
5	logs	https://logs.{central CSP DNS}
6	trustcircles	https://tc.{central CSP DNS}

where: {central CSP DNS} is the actual DNS of Central CSP, i.e. central.preprod.melicertes.eu.

5 Central CSP Installation – CSP Installer updates

Apart from managing and delivering modules to registered nodes, the Central CSP instance is also responsible for delivering updates to CSP Installer application, which is configured to be automatically self-updated.

This role can be accomplished by the following set of steps.

Step 1

Prepare Apache to serve updates, by executing the following:

```
#  cd /opt/csp/apache2/csp-sites
#  touch central.ssl.conf
#  vi central.ssl.conf
```

Paste the following snippet in the file opened for editing, and replace `<DOMAIN>` with the proper domain of the CSP environment, i.e. preprod.melicertes.eu

```
Listen 80
<VirtualHost *:80>
    DocumentRoot "/etc/apache2/csp-sites/www/repo/html"

    ServerName central.<DOMAIN>

    <Directory /etc/apache2/csp-sites/www/repo/html>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>

    CustomLog /var/log/apache2/central-access.log combined
    ErrorLog /var/log/apache2/central-error.log
</VirtualHost>
```

Save and exit.

Step 2

Create required directories and prepare contents with the following commands.

```
#  mkdir -p /opt/csp/apache2/csp-sites/www/repo/html/repo-load/vm
```

The following file structure has to be created:

```
/opt/csp/apache2/csp-sites/www/repo/html/
      +-----repo-load
            +-----vm
            |      latest
            |      conf-client-cspapp-X.Y.Z-SNAPSHOT.jar
            |      conf-client-cspapp-A.B.C-SNAPSHOT.jar
      |      favicon.ico
      |      index.html
      |      robots.txt
```

The contents/role of each file is as follows:

index.html

```
<html>
    <head>
        <title>Invalid request</title>
    </head>
    <body>
        <h1>This is a protected resource and access is monitored.</h1>
    </body>
</html>
```

robots.txt

```
User-agent: *
Disallow: /
```

favicon.ico

An *.ico file of your choice. File is optional.

conf-client-cspapp-X.Y.Z-SNAPSHOT.jar

Various CSP Installer applications to be distributed.

latest

A simple text file containg the name of the latest file to be distributed. An example is provided below:

```
conf-client-cspapp-4.0.6-SNAPSHOT.jar
```

assuming that 4.0.6 is the latest version.

After all files are in place the following command has to be executed:

```
#  docker restart csp-apache
```

6 Annex A: Contents of central.zip for CSP version 4

For installation of Cemtral CSP you should have received an email with a link to download the **central.zip** file. The file has to be verified by its checksum as follows:

```
#   md5sum central.zip
#   6bc054403663ec3928855f83cf607f44  central.zip
```

Table below lists the contents of central.zip together with their checksums.

Table 5. Contents of central.zip file

#	File	Checksum (md5sum)
1	central-images.tar.bz2	4cae758d60c576cbfef0302427761e3c
2	conf-client-cspapp-4.0.0-SNAPSHOT.jar	e56ef22b4f9d5c6052798ad47c8722f3
3	conf-server-3.6.0-SNAPSHOT-exec.jar	55f5fcadae3ca7cf04af8241f9106da9
4	docker-compose.yml	5af6130bafbb7841c3d6d9f5dbe4a9d4
5	first-time.sh	bbca8c9e22a03c24ca60886481a9a90d

7 Annex B: Contents of zip file for CSP version 4 modules

For installation of Cemtral CSP you should have received an email with a link to download a zip file containing all required modules for version 4. The file has to be verified by its checksum as follows:

```
#   md5sum 4.0.0-modules.zip
#   271b901eaedee4535926a854e7a69cc3  4.0.0-modules.zip
```

Table below lists the contents of central.zip together with their checksums.

Table 6. Contents of 4.0.0-modules.zip file

#	File	Checksum (md5sum)
1	csp-activemq-20180719-3.8.0.zip	4b3816dd28e28219611abf9c93faa409
2	csp-anonymization-20180831-4.0.001.zip	fbc4d050f1f28deb581fadaaeae57ed8
3	csp-apache-20180920-4.0.6.zip	792f4bc9de88a6146c9db31935340c2a
4	csp-apache-crl-20180917-4.0.4.zip	c5e946e57b4442edeb11d0510ebca012
5	csp-basemodule-2018-09-03T1243-4.0.4.zip	5bfa9a00218e9e3e12329fff5d0dbdf4
6	csp-configuration-20180626-3.6.000.zip	d9d1f6a6c0bb406ab47680f13bdd0051
7	csp-elasticsearch-20180903-4.0.002.zip	2c43eb4567681d1c62ce24cb6e6748d0
8	csp-integrationlayer-20180831-4.0.001.zip	6659a8d57b4a4c0b6f95826a4a8d7b89
9	csp-intelmq-20180919-4.0.5.zip	0781d08065d2cdaf37ee838157333b16
10	csp-kibana-20180216.zip	aaf17d6e01aed415a51dae1581858bdb
11	csp-logs-20180518-3.6.007.zip	4cde3dfe5e9b070a60057451128f2329
12	csp-misp-20180831-4.0.002.zip	cd7c858e8973cf40ceb7f079717f6510
13	csp-mocknode-20180220.zip	0f88b57050ab6f14f615954a757e0b78
14	csp-openam-20180605-3.6.005.zip	b3ff4208a198ea1b06417bf7eb6c11c0
15	csp-owncloud-20180518-3.6.001.zip	4ddf82e930434faa2b9af4337308d5db
16	csp-postgres-20180216.zip	f7b6d69330659ef2896f1c4d48283a27
17	csp-redis-20180529-3.6.001.zip	255ca88e69bbb2cb4860579a3456f705
18	csp-regularreports-20180831-4.0.001.zip	f168d7a0bb3474a648efeece4e0c93c8
19	csp-rt-20180620-3.6.003.zip	995ce6678cadcc9d2ad33f2e896108f6
20	csp-trustcircles-20180801-3.8.001.zip	7a83d3f19cb857d33d9214e9a6e1f52c
21	csp-vcb-20180718-3.8.002.zip	1d4bf92f5a4f38e83351704e2b0101ce

22	csp-viper-20180831-4.0.003.zip	35c563161ce07ebfd0b83e252d44b93a

- End of document-