3.0 Configuration Guide

Introduction

This guide details the process for configuring the Direct Certificate Discovery Tool (DCDT, or the *Tool*).

Requirements

The following ports must be available for binding of services:

Ports	Service
25 (TCP)	Mail
53 (UDP and TCP)	DNS
10389, 11389, 12389 (TCP)	LDAP

Configure Tomcat

Stop the Tomcat 7 service by running:

```
sudo service tomcat7 stop
```

Append the following lines to the file /etc/default/tomcat7:

```
JAVA_HOME="/usr/lib/jvm/java-7-oracle"
JAVA_OPTS="-Djava.awt.headless=true -Xms384m -Xmx768m -XX:+UseConcMarkSweepGC"
ulimit -n 8192
```

> ⓘ The execution of the ulimit command above increases/sets the open files limit for the Tomcat 7 service process. The common default value on *nix systems is 1024, which is quite often insufficient.

If the file /usr/share/tomcat7/bin/setenv.sh does not exist, create it by running:

```
sudo touch /usr/share/tomcat7/bin/setenv.sh
```

Append the following lines to the file /usr/share/tomcat7/bin/setenv.sh:

```
CATALINA_OPTS="$CATALINA_OPTS -XX:PermSize=256m -XX:MaxPermSize=512m"
CATALINA_OPTS="$CATALINA_OPTS -Ddcdt.data.dir=<path to data directory> -Ddcdt.web.user.admin.secret=<admin
console admin user password>"
```

- *<path to data directory>*: path to a directory where you want data to be persisted.
- *<admin console admin user password>*: custom password (default="adminpass") to set for the admin console "admin" user.

Then, run the following command so that the Tomcat user will be able to create and write data in the specified directory:

```
sudo chown -R tomcat7:tomcat7 "$(dirname "<path to data directory>")"
```

Start the Tomcat 7 service by running:

```
sudo service tomcat7 start
```

Configure Authbind on Ubuntu

If you are installing DCDT on Ubuntu, authbind is required to allow the Tomcat user to run on privileged ports (port numbers 0-1023). For DCDT, the DNS service must bind to port 53 and the mail service must bind to port 25. Authbind may already be installed on your version of Ubuntu and can be found in /etc/authbind. If it is not already installed:

```
sudo apt-get install authbind
```

To enable authbind so that Tomcat can bind to privileged ports, change the default setting *AUTHBIND=no* to *AUTHBIND=yes* in /etc/default/tomcat7.

Since authbind requires the use of IPv4, add the following to /etc/sysctl.conf:

```
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
```

Reinitialize sysctl by running the following:

```
sudo sysctl -p
```

Restart the Tomcat service by running:

```
sudo service tomcat7 restart
```

Verify that Tomcat can access the privileged ports. The user ID of the Tomcat user can be viewed in /etc/passwd. A file with the name of the Tomcat user ID (e.g. 106) should exist in /etc/authbind/byuid/ and contain the following entry:

```
0.0.0.0/0:1,1023
```