Installing Trust Agent as non-root user

# Overview

Installing and running trust agent as a non-root user enhances security by mitigating a successful attack on the trust agent itself so the attacker does not automatically gain access to the entire system.

Starting with version 2.0.6, the trust agent runs as the non-root user “tagent”. There are two approaches to installing the trust agent: running the installer as “root” or running it as “tagent”. Either way the trust agent will run as “tagent” after installation. The difference is primarily the amount of automation that can be accomplished by the installer.

The installer, when running as root, can automatically create the “tagent” user and necessary directories, use the package manager to install pre-requisites, and register the “tagent” start-up script. When running as non-root, the installer cannot do these things and the root user must perform certain steps before and after installation.

Upgrading to version 2.0.6 from a previously installed version can be accomplished seamlessly by running the installer as root. Running the installer as non-root for an upgrade is also possible but requires the root user to prepare the environment first.

The rest of this document describes the steps that must be taken by the root user before and after installing trust agent as a non-root user.

# Configuration

A new installation requires 4 configuration settings related to the Mt Wilson server, shown here with example values:

MTWILSON\_API\_URL=https://192.168.1.100:8443/mtwilson/v2

MTWILSON\_API\_USERNAME=admin

MTWILSON\_API\_PASSWORD=password

MTWILSON\_TLS\_CERT\_SHA1=06d8cf367822b3ccf05c6311784ea8c126eb9b63

There is an optional configuration setting to control whether the TPM password should be registered with Mt Wilson. The default is not to register, so you only need to set this variable if you want the password to be registered:

REGISTER\_TPM\_PASSWORD=yes

There is also an optional configuration setting for the TPM password. A new install can specify what the TPM password should be, or leave it undefined to automatically generate a new random TPM password. An upgrade or re-installation can provide the current TPM password using this setting in order to avoid having to clear and reactivate the TPM.

TPM\_OWNER\_SECRET=eaf68097599b5cbf66eac75e933ca7d738f2683d

The following variables must be defined in order to either install tagent as root and later run it as non-root

export TRUSTAGENT\_HOME=/opt/trustagent

export TRUSTAGENT\_USERNAME=tagent

# Actions to take as root before installation

## Install required packages

### SUSE

Use either zypper or yast:

zypper install openssl libopenssl-devel libopenssl1\_0\_0 openssl-certs trousers-devel

yast -i openssl libopenssl-devel trousers trousers-devel tpm-tools make gcc unzip

### RedHat and Fedora

Use yum:

yum -y install openssl trousers trousers-devel tpm-tools make gcc unzip

Now check for missing libcrypto link, add if necessary:

has\_libcrypto=`find / -name libcrypto.so.1.0.0 | head -1`

libdir=`dirname $has\_libcrypto`

has\_libdir\_symlink=`find $libdir -name libcrypto.so`

has\_usrbin\_symlink=`find /usr/bin -name libcrypto.so`

if [ -n "$has\_libcrypto" ]; then

if [ -z "$has\_libdir\_symlink" ]; then

echo "Creating missing symlink for $has\_libcrypto"

ln -s $libdir/libcrypto.so.1.0.0 $libdir/libcrypto.so

fi

if [ -z "$has\_usrbin\_symlink" ]; then

echo "Creating missing symlink for $has\_libcrypto"

ln -s $libdir/libcrypto.so.1.0.0 /usr/lib/libcrypto.so

fi

ldconfig

fi

### Ubuntu

Use apt-get:

apt-get -y install openssl libssl-dev libtspi-dev libtspi1 trousers make gcc unzip

## Disable monit temporarily

This step is only necessary if Monit is already installed and monitoring Trust Agent

Remove existing Monit configuration for Trust Agent:

rm -f /etc/monit/conf.d/ta.monit

Restart Monit to apply changes:

service monit restart

## Create Trust Agent User

The following commands create a home directory and user for the Trust Agent. The shell is set to BASH so you can login as this user and perform the installation. However, it is recommended to lock the account after installation, and this is described in the section “Actions to take as root after installation”

mkdir -p $TRUSTAGENT\_HOME

useradd --comment "Mt Wilson Trust Agent" --home $TRUSTAGENT\_HOME --system --shell /bin/bash $TRUSTAGENT\_USERNAME

chown -R $TRUSTAGENT\_USERNAME:$TRUSTAGENT\_USERNAME $TRUSTAGENT\_HOME

## Configure firewall

Ensure the system firewall has port 1443 open for trust agent

## Configure authbind

This step is only necessary if Trust Agent will be configured to use privileged ports such as 80 and 443; the default port 1443 is non-privileged and does not require use of authbind.

The following commands allow trust agent to listen on port 443:

mkdir -p /etc/authbind/byport

touch /etc/authbind/byport/443

chown $TRUSTAGENT\_USERNAME /etc/authbind/byport/443

chmod 500 /etc/authbind/byport/443

## Update system information

Trust agent has a command for this (“tagent update-system-info”) which can be run as root, but this information is also needed during setup, so currently you must run the following commands as root before the first non-root install.

TRUSTAGENT\_VAR=$TRUSTAGENT\_HOME/var

mkdir -p $TRUSTAGENT\_VAR/system-info

dmidecode -s bios-vendor > $TRUSTAGENT\_VAR/system-info/dmidecode.bios-vendor

dmidecode -s bios-version > $TRUSTAGENT\_VAR/system-info/dmidecode.bios-version

dmidecode -s system-uuid > $TRUSTAGENT\_VAR/system-info/dmidecode.system-uuid

dmidecode --type processor > $TRUSTAGENT\_VAR/system-info/dmidecode.processor

lsb\_release -a > $TRUSTAGENT\_VAR/system-info/lsb\_release

virsh version > $TRUSTAGENT\_VAR/system-info/virsh.version

chown -R $TRUSTAGENT\_USERNAME:$TRUSTAGENT\_USERNAME $TRUSTAGENT\_HOME

## Upgrade considerations

To upgrade from a previous version of trust agent that was installed as root, you may run into permission errors. Ensure files are owned by “tagent” to resolve most issues.

The init script link must be replaced:

rm -f /etc/init.d/tagent

ln -s /opt/trustagent/bin/tagent /etc/init.d/tagent

# Run Trust Agent Installer as non-root

First copy the trustagent.env file into /opt/trustagent (created earlier):

cp trustagent.env $TRUSTAGENT\_HOME

Next switch to the trustagent user and run the installer.

su - $TRUSTAGENT\_USER

./mtwilson-trustagent-installer-2.0.6.bin

# Running Trust Agent as non-root

export PATH=$TRUSTAGENT\_HOME/bin:$PATH

tagent start

# Actions to take as root after installation

## Locking Trust Agent account

If you set up the trustagent to launch automatically as non-root on every reboot, or have a watchdog/supervisor process for ensuring that it’s running, so that you don’t need to login to the trustagent user account itself, then you should lock that account:

usermod --lock $TRUSTAGENT\_USERNAME -s /bin/false

## Register trust agent startup script (as root)

ln -s /opt/trustagent/bin/tagent /etc/init.d/tagent

### RedHat, Fedora, and SUSE

chkconfig --add tagent

### Ubuntu

update-rc.d tagent defaults

## Update system info automatically on every boot

Type the following line to edit the crontab:

crontab -e

Add the following line to the crontab, then save & exit:

@reboot /opt/trustagent/bin/tagent update-system-info

## Install and configure monit (as root)

TBD