# Syscheck Installation and Upgrade

Henrik Andreasson

kinneh@users.sourceforge.net

http://sourceforge.net/apps/trac/syscheck/

2010-11-09

Version 1.0

## Table of Contents

# 1 New Installation

## 1.1 Get Syscheck

```
username@smartcard20-node1:/var/tmp/ wget http://sourceforge.net/projects/syscheck/files/syscheck-1.5.15/syscheck-1.5.15.zip/download
```

## 1.2 Unpack Syscheck

```
username@smartcard20-node1:/usr/local/# unzip  /var/tmp/syscheck-1.5.15.zip

[...]
```

## 1.3 Syscheck configuration

Configure the values in config/common.conf and the scripts you're using.

### 1.3.1 Activate selected syscheck scripts

```
username@smartcard20-node1:/usr/local/certificate-services/syscheck/scripts-enabled> sudo ln -s ../scripts-available/sc_02_ejbca.sh .

username@smartcard20-node1:/usr/local/certificate-services/syscheck/scripts-enabled> sudo ln -s ../scripts-available/sc_03_memory-usage.sh .

username@smartcard20-node1:/usr/local/certificate-services/syscheck/scripts-enabled> sudo ln -s ../scripts-available/sc_07_syslog.sh .
```

And so on for each syscheck-script you want active.

Verify there is soft links, no file copied into scritps-enabled!

```
username@smartcard20-node1:/usr/local/certificate-services/syscheck/scripts-enabled> ls -l

lrwxrwxrwx  1 root root   35 2010-06-04 14:25 sc_02_ejbca.sh -> ../scripts-available/sc_02_ejbca.sh

lrwxrwxrwx  1 root root   42 2010-06-04 14:25 sc_03_memory-usage.sh -> ../scripts-available/sc_03_memory-usage.sh

lrwxrwxrwx  1 root root   36 2010-06-04 14:25 sc_07_syslog.sh -> ../scripts-available/sc_07_syslog.sh

lrwxrwxrwx  1 root root   35 2010-06-04 14:25 sc_12_mysql.sh -> ../scripts-available/sc_12_mysql.sh

lrwxrwxrwx  1 root root   35 2010-06-04 14:25 sc_19_alive.sh -> ../scripts-available/sc_19_alive.sh
```

```
lrwxrwxrwx  1 root root   45 2010-06-04 14:25 sc_20_errors_ejbcalog.sh -> ../scripts-available/sc_20_errors_ejbcalog.sh
```

Also check the config for each script you activate, there may or may not be anything to config, but let's check.

```
username@smartcard20-node1:/usr/local/certificate-services/syscheck/> sudo vi config/02.conf

username@smartcard20-node1:/usr/local/certificate-services/syscheck/> sudo vi config/03.conf

username@smartcard20-node1:/usr/local/certificate-services/syscheck/> sudo vi config/07.conf

username@smartcard20-node1:/usr/local/certificate-services/syscheck/> sudo vi config/12.conf

username@smartcard20-node1:/usr/local/certificate-services/syscheck/> sudo vi config/19.conf

username@smartcard20-node1:/usr/local/certificate-services/syscheck/> sudo vi config/20.conf
```

### 1.3.2 Activate selected related scripts

Make the soft links in the related-enabled directory.

```
han@rp-ca-nod1:/usr/local/certificate-services/syscheck/related-enabled> ln -s ../related-available/904_make_mysql_db_backup.sh
.
```

Verify there is soft links and no copied files in enabled!

```
username@smartcard20-node1:/usr/local/certificate-services/syscheck/syscheck/related-enabled> ls -al

lrwxrwxrwx  1 root root   48 2010-06-04 14:25 904_make_mysql_db_backup.sh -> ../related-
available/904_make_mysql_db_backup.sh
```

Also check the config for each script you activate, there may or may not be anything to config, but let's check.

```
username@smartcard20-node1:/usr/local/certificate-services/syscheck/> sudo vi config/900.conf

username@smartcard20-node1:/usr/local/certificate-services/syscheck/> sudo vi config/904.conf

[...]
```

### 1.3.3 Mysql database configuration

Config database parameters, you can get the database-username/password information from ejbca it's in the file ejbca/conf/database.properties

```
less /usr/local/ejbca/conf/database.properties

database.url=jdbc:mysql://127.0.0.1:3306/ejbca

database.username=ejbca

database.password=sdfiuh3wrnj
```

Enter those parameters into the syscheck config/common.sh

```
DB_NAME=ejbca
```

DB_USER=**ejbca**

DB_PASSWORD="**sdfiuh3wrnj**"

If your installation has a weak(eg. foo123) mysql root password set a new with high security (eg. UiywfeW23)

# mysqladmin password  <new-pass> -u root --password=<old-password>

# mysqladmin password **UiywfeW23** -u root –password=**foo123**

**Alternativly use the mysql_secure_installation, this command removes test users and databases and sets a new mysql-root password**

**#** mysql_secure_installation

**Enter the new mysql root password  into syscheck/config/common.conf**

#Password for Mysql root

MYSQLROOT_PASSWORD="**UiywfeW23**"

### *1.4 Make the new version the default*

username@smartcard20-node1:/usr/local> **sudo rm syscheck**

username@smartcard20-node1:/usr/local> **sudo ln -s syscheck-1.5.11 syscheck**

# 2 Upgrade

### *2.1 Get Syscheck*

username@smartcard20-node1:/var/tmp/ wget http://sourceforge.net/projects/syscheck/files/syscheck-1.5.15/syscheck-1.5.15.zip/download

### *2.2 Unpack Syscheck*

username@smartcard20-node1:/usr/local/# unzip  /var/tmp/syscheck-1.5.15.zip

[...]

## 2.3 Migration of config from a previous version

If migrating a host to new hardware make a backup of syscheck to be transferred to the new hardware.

```
root@smartcard20-node1:/usr/local # zip -r9 /tmp/syscheck-backup-x.y.z.zip syscheck-x.y.z
```

Transfer the zip to the new host, then unpack the backup.

```
root@smartcard20-node1:/usr/local # unzip /tmp/syscheck-backup-x.y.z.zip
```

Copy enabled scripts

```
root@smartcard20-node1:/usr/local/syscheck # cp -a ../syscheck-<last-version>/related-enabled/* ./ related-enabled/

root@smartcard20-node1:/usr/local/syscheck # cp -a ../syscheck-<last-version>/scritps-enabled/* ./ scritps-enabled/
```

Run the copy config command to loop through the configs and check wheter you want to use ther old or the new config.
*Tip: Use the old if it's configured and only differs to the new config is the values you entered. Is there new options you need, use the new one and migrate the config manually*

```
root@smartcard20-node1:/usr/local/syscheck # ./lib/copy-config-from-old-version.sh /path/to/old/syscheck-<last-version>/config ./config/
```

Migrate old resouces.sh to the new common.conf

***Note: ONLY NEEDED IF UPGRADING FROM 1.4.0 or earlier***

```
root@smartcard20-node1:/usr/local/syscheck # diff -uw ../syscheck-<last-version>/resources.sh ./config/common.conf
```

Go though the differences and manually enter the changes you need to keep into the new common.conf

## 2.4 Make the new version the default

```
username@smartcard20-node1:/usr/local> sudo rm syscheck

username@smartcard20-node1:/usr/local> sudo ln -s syscheck-1.5.15 syscheck
```

# 3 References

## 3.1 Syscheck mysql database backup management

See the instruction for mysql database backup “syscheck-backup-management.pdf”

## 3.2 Using syscheck for database replication and failover

See the instruction in “database_replication_and_failover.pdf”

## 3.3 Using syscheck for certificate and revovation archival

See the instruction in “certificate_and_revovation_archival.pdf”