# Syscheck version

**Dokumentation generated:** Sat Mar 28 22:35:24 CET 2009

## scripts-available

## sc_01_diskusage.sh

```
Script that checks for to much hard-disc usage, limit is: 95%)
0101/Diskusage ok (%s is %s percent used: Limit is %s percent)
0102/Diskusage exceeded (%s is %s percent used: Limit is %s percent)
to run with output directed to screen: add a '-s' or '--screen'
```

## sc_02_ejbca.sh

```
Script that connects to the ejbca health check servlet to check the status
of the ejbca application. The health check servlet checks JVM memory,
database connection and HSM connection.
0201/EJBCA : %s - No action is needed
0202/EJBCA : %s - Possible errors: \n"Error Virtual Memory is about to run
out, currently free memory : X" - you need to add more virtual memory to
application server/java process\n"Error Connecting to EJBCA Database" -
The internal check of database failed, try to connect to database directly
or restart database server\n"CA Token is disconnected" - activate token or
maybe a restart of pcscd can help
0203/EJBCA : Application Server is unavailable - The server is
non-responding, restart application-server(jboss) and/or check server log
to find the fault
to run with output directed to screen: add a '-s' or '--screen'
```

## sc_03_memory-usage.sh

```
Script that checks that there is enough free memory. The limit is
configured in the script, limit:  mem: 80% / swap 50 %
0301/Memory limit exceded (Memory is %s KB used: Limit is %s KB)
0302/Memory limit ok (Memory is %s KB used: Limit is %s KB)
0303/Swap limit exceded (Swap is %s KB used: Limit is %s KB)
0303/Swap limit ok (Swap is %s KB used: Limit is %s KB)
to run with output directed to screen: add a '-s' or '--screen'
```

## sc_04_pcsc_readers.sh

```
./sc_04_pcsc_readers.sh checks for the defined number of PCSC readers is
attached to the computer
0401/Right number of attatched pcsc-readers (%s) - No action is needed
0402/Wrong number of attached pcsc-readers (%s) - means that all reader is
NOT working correctly as defined by pcscd
0403/Perl module not installed(%s) - means that you've not installed the
```

module used by this script 'Chipcard::PCSC' To install perl-module: cpan
-i Chipcard::PCSC or get from http://search.cpan.org

# sc_05_pcscd.sh

./sc_05_pcscd.sh check that pcscd is running
0501/pcscd is running - pcscd needs to be restarted, if it dont start, run
it with: /path/to/pcscd --foreground --debug
0502/pcscd is NOT running -
0503/ -

# sc_06_raid_check.sh

./sc_06_raid_check.sh check the raid discs
0601/PhysicalDiscs is OK %s - No action is needed
0602/PhysicalDiscs is not OK %s - Change disc as soon as possible
0603/LogicalDiscs is OK %s - No action is needed
0604/LogicalDiscs is rebuilding %s - check back in a while to see this
error goes away, else you need to investigate
0605/LogicalDiscs has some other error %s - you need to investigate this
error ASAP
0606/HPTOOL not installed at: %s - the hptool is not installed, install
the tool to get working reports

# sc_07_syslog.sh

./sc_07_syslog.sh check to see that syslog is running and delivers
messages ok
0701/loggmessage did not come throu SYSLOG - syslog is running but the
messages dont comes throu to local file, restart and/or check config file
0702/no pid file found and syslog not found in ps-table - not even the
pid-file os syslog was found, try a restart
0703/syslog is not running - the process was not found amoung running
processes

# sc_08_crl_from_webserver.sh

./sc_08_crl_from_webserver.sh check the status of CRL, both that you can
get it and that its valid
0801/ CRL %s creation have failed - either the server is not up, it dont
produce CRL:s, it dont validate or the CRL is old
0802/ CRL %s is updated - No action is needed
0803/Unable to get CRL %s from webserver  - Check manually to get CRL from
webserver
0804/When getting CRL %s the size of file is 0 - Check discusage, try
manually to get CRL

# sc_09_firewall.sh

./sc_09_firewall.sh Check the firewall is configured and running
0901/ Firewall seems to be turned off. - check manually with iptables -L
-n (if you're running Linux), restart the firewall with /etc/init.d/
firewall start
0902/ Firewall doesn't seem to have the correct ruleset configured. -
Maybe something went wrong loading the firewall ruleset, because some very
basic rules are'nt present
0903/Firewall is up and configured properly - No action is needed

# sc_10_cluster_master_db.sh

./sc_10_cluster_master_db.sh Cluster checks
1001/Primary Node is Master Database. - No action is needed
1002/Secondary Node is Master Database, schedule a resync! - A failover
has been preformed, mening secondary node is master and only DB. Make
seperate backups of both modes and make sure node1 is operational. Resync
DB and move back to node1. System downtime is needed/and required to
preforme the DB-resync.
1003/JBoss Database settings match between nodes, (as it should). - No
action is needed.

# sc_11_heartbeat.sh

./sc_11_heartbeat.sh Heartbeat checks
1101/heartbeat is running - No action is needed
1102/heartbeat is NOT running - heartbeat process needs to be (re)started,
try: /etc/init.d/heartbeat restart

# sc_12_mysql.sh

./sc_12_mysql.sh Mysql server checks
1201/mysql is running - No action is needed
1202/mysql is NOT running - mysql is not running, try /etc/init.d/mysql
stop, wait, /etc/init.d/mysql start

# sc_13_heartbeat-master.sh

./sc_13_heartbeat-master.sh Heartbeat for master node checks
1301/heartbeat is running on the master node. - No action is needed
1302/heartbeat is seem to have been failed over to slave. - heartbeat TODO

# sc_14_sw_raid.sh

./sc_14_sw_raid.sh: Linux software raid checks
1401 - means this script has not detected any errors
1402 - A disk has failed, you need to replace it
1403 - this script has found a not prediced error

# sc_15_apache.sh

./sc_15_apache.sh Check apache process is up and running
1501/Apache webserver is running - server is running and serving web pages
1502/Apache webserver is not running - check apache error.log, it is not
running

# sc_16_ldap.sh

./sc_16_ldap.sh Checks the ldap server to make sure it's running
1601/LDAP directory server is running - all ok
1602/LDAP directory server is not running - check you ldap server logs

# sc_17_ntp.sh

./sc_17_ntp.sh Check that ntp i running and is insync
1701/ntpd is up running - all ok
1702/ntpd is NOT running. - Start it with /etc/init.d/xntpd start
1703/ntpd can't synchronize a server - check the configuration or restart
ntpd
1704/ntpd can NOT synchronize to servers. - Check network connectivity and
configuration of ntp
1705/ntp.conf not found - Check your ntp installation

# sc_18_sqlselect.sh

./sc_18_sqlselect.sh Mysql select keepalive
1801/mysql is running and answering - No action is needed
1802/mysql is NOT answering to select statement check - mysql is not
running, try /etc/init.d/mysql stop, wait, /etc/init.d/mysql start

# sc_19_alive.sh

Sends alive messages to a central syscheck server run this script either
along with the rest of the syscheck scripts or in a crontab (then you can
run me more often...)
1901/Operating system just started - Message is sent when the server's
operating system is started
1902/Operating system is shutting down - Message is sent when the server's
operating system is shutdown
1903/I'm alive - Message is sent to make sure central server know's this
server is alive
to run with output directed to screen: add a '-s' or '--screen'

# sc_20_errors_ejbcalog.sh

./sc_20_errors_ejbcalog.sh checks fo new errors in the server log for ejbca
2001/No new errors in ejbca server log - No action is needed
2002/New error in log: %s - There was new ERRORS in the LOG file, please

attend to them
2003/Cant find the specified ejbca log %s - maybe you havn't configured
the script yet?

# sc_22_boks_replica.sh

./sc_22_boks_replica.sh BoKS Replica checks
2201/No action is needed - all boks processes are running
2202/This BoKS replikca processes IS NOT running %s - Not all boks
processes are running

# sc_23_rsa_axm.sh

./sc_23_rsa_axm.sh Checks the RSA Access Manager server to make sure it's
running
2301/RSA Access Manager is running - all ok
2302/At least one service is not running (%s)  - check the rsa access
manager server logs

# sc_24_weblogic.sh

./sc_24_weblogic.sh Checks the weblogic server to make sure it's running
2401/WebLogic server is running - all ok
2402/WebLogic server is not running (%s) - Start the WebLogic server

# sc_27_dss.sh

./sc_27_dss.sh
2701/Document SignServer is active - No action needed
2702/Document SignServer is running at ONLY ONE NODE - Check the failing
node asap
2703/Document SignServer is NOT active - resolve this issue asap
2704/Document SignServer is not installed at this host - maybe you've
configured wrong scripts or not yet installed signserver

# sc_28_check_vip.sh

./sc_28_check_vip.sh
2801/Node 1 has the VIP - No action needed
2802/Node 2 has the VIP - No action needed
2803/Both nodes has the VIP - Resolve this issue asap
2804/None of the nodes has the VIP - Resolve this issue asap

# related-available

# 900_export_cert.sh

```
Export certificate and archive them
9001/Export certificate run successfully -
9002/Export certificate failed (%s)  -
9003/Export certificate failed, script called without file -
to run with output directed to screen: add a '-s' or '--screen'
```

# 901_export_revocation.sh

```
9011/Export revocation run successfully -
9012/Export revocation failed (%s)  -
9013/Export revocation failed, script called without file -
to run with output directed to screen: add a '-s' or '--screen'
```

# 902_export_crl.sh

```
9021/Export CRL run successfully -
9022/Export CRL failed (%s)  -
9023/Export CRL failed, script called without file -
to run with output directed to screen: add a '-s' or '--screen'
```

# 903_make_hsm_backup.sh

```
/Backup of Nfast HSM run successfully
/Backup of Nfast HSM failed (%s)
to run with output directed to screen: add a '-s' or '--screen'
```

# 904_make_mysql_db_backup.sh

```
9041/Backed up db ok (file:%s) - no action needed
9042/Could not compress the backup (%s) - Check disk space and owner of
directory to write backup to
9043/Backup failed (%s) - Check username and password and access to
database
to run with output directed to screen: add a '-s' or '--screen'
```

# 905_publish_crl.sh

```
./905_publish_crl.sh <-s|--screen>
```

# 906_ssh-copy-to-remote-machine.sh

Script used to copy files to other hosts/directorys usage:
./906_ssh-copy-to-remote-machine.sh: file host    \n(if you dont specify
directory the file will end up in the user's homedirectory, \nif you dont
specify to-username the same user as the one executing this script will be
used, \nif from-ssh-key is not specified default key will be used)
9061/file transfered ok - ok
9062/specify a filename as first argument to this script - filename not
specified as argument
9063/specify a hostname as second argument to this script - Hostname not
specified as argument
9064/scp file transfer failed (%s) - check the error message and try to
fix it
to run with output directed to screen: add a '-s' or '--screen'

# 907_make_mysql_db_backup_and_transfer_to_rem

Script used to take backup of the sql database, compress and send to a
separate server.
/Backup and transfer was ok. - Ok
/Could not get the backup from MySQL (%s)  - Could not make a backup.
/Compression of the backup failed (%s)  - Could not compress the backup.
/Could not send the backup, maybe connection problem or problem logging in
(%s)  - Could not send the backup.
to run with output directed to screen: add a '-s' or '--screen'

# 908_clean_old_backups.sh

9081/Clean backupfiles run successfully - All is ok
9082/Clean backupfiles failed (%s)  - Unpredicted error while deleting
file %s
9083/Clean backupfile file did not exist (%s)  - Maybe the files has been
already removed or there was no files from start
to run with output directed to screen: add a '-s' or '--screen'

# 909_activate_CAs.sh

Activate the CA:s (automaticlly enter PIN codes)
9091/Activate CA:s run successfully - All is ok
9092/Activate CA failed (%s)  - Could be problems accessing the
application server, or token is not available  %s
9093/ -
to run with output directed to screen: add a '-s' or '--screen'

# 910_deactivate_CAs.sh

Deactivate the CA:s
9101/Deactivate CA:s run successfully - All is ok
9102/Deactivate CA failed (%s)  - Could be problems accessing the

application server, or token is not available  %s
9103/ -
to run with output directed to screen: add a '-s' or '--screen'

# 911_activate_VIP.sh

Activate the VIP
9111/Activate VIP run successfully - All is ok
9112/Activate VIP failed (%s)  - Could be problems accessing the
application server, or token is not available  %s
9113/Activate VIP failed since the VIP was already active - All is ok, if
the VIP was supposed to be on this host already
to run with output directed to screen: add a '-s' or '--screen'

# 912_deactivate_VIP.sh

Deactivate the VIP
9121/Deactivate VIP run successfully - All is ok
9122/Deactivate VIP failed (%s)  - Check manually with ifconfig -a and run
ifconfig  down
9123/While deactivating, the VIP was already NOT active on this host - If
the VIP was supposed to be at this host this event needs investigation
to run with output directed to screen: add a '-s' or '--screen'

# 913_copy_ejbca_conf.sh

9131/Copy run successfully - All is ok
9132/Copy failed (%s)  -
to run with output directed to screen: add a '-s' or '--screen'

# 914_compare_master_slave_db.sh

9141/Data read successfully - All is ok
9142/Could not get table data - Check connection, username and password
to run with output directed to screen: add a '-s' or '--screen'

# 915_remote_command_via_ssh.sh

Run command on another host with ssh ./915_remote_command_via_ssh.sh
[sshtouser] [sshfromkey]
9151/Command executed successfully (%s) - All is ok
9152/Host not found (%s) - You have to specify a hostname to connect to
9153/Command not found (%s) - Specify a command to run
9154/Command not executed (%s) - Check connection, username and password
to run with output directed to screen: add a '-s' or '--screen'

# 916_archive_access_manager_logs.sh

./916_archive_access_manager_logs.sh <-s|--screen>
Script used to move/archive Access Manager logfiles
9161/Files archived succefully (%s -> %s) - ok
9162/Failed to artchive files (%s -> %s) - test the underlying archive
script manually

# 917_archive_file.sh

Script used to copy files to other hosts/directorys usage:
./917_archive_file.sh: file host    \n(if you dont specify directory the
file will end up in the user's homedirectory, \nif you dont specify
to-username the same user as the one executing this script will be used,
\nif from-ssh-key is not specified default key will be used)
9171/File archived succefully Locally (%s -> %s) - ok
9172/Failed to move file to Local archive (%s -> %s) - Check write
premisions in archive dir
9173/Errornous input arguments - specify the right arguments (run
./917_archive_file.sh -h for help)
9174/Failed to get a filename from remote server - Check ssh connection
setup to remote server
9175/File Failed to be Archived on Remote Server (%s) - Check ssh
connection setup to remote server and write permissions in remote archive
dir
9176/File Archived successfully to Remote Server (%s) - ok
9177/File moved successfully to intransit folder (%s -> %s) - ok
9178/Failed to create file in the intransit folder (%s) - Check
permissions to write in the intransit folder
9179/Intransit dir not found - Create the dir with mkdir
to run with output directed to screen: add a '-s' or '--screen'

# 918_server_alive.sh

9181/machine(%s) has called in as it's supposed to (lastcall: %s). - no
action is needed
9182/machine(%s) has not called in within error limit (lastcall: %s) - two
missed log messages, this needs attention
9183/machine(%s) has not called in within warn limit (lastcall: %s) - one
missed log message, may be a glitch but should be checked
to run with output directed to screen: add a '-s' or '--screen'

# 919_certpublisher_remotecommand.sh

Takes a certificate and runs a configurable command at a remote host
./919_certpublisher_remotecommand.sh -c|--cert  [-s|--screen] [-h|--help]
9191/Remote command ran successfully (%s) -
9192/Remote command failed (%s) -
9193/File input error, failed (%s) -
to run with output directed to screen: add a '-s' or '--screen'

# 920_restore_mysql_db_from_backup.sh

```
Restore db, syntax: ./920_restore_mysql_db_from_backup.sh
9201/Failed to make backup of the pre-existing db prior to restore - run a
manual backup with /misc/src/syscheck/syscheck-1.5.0/related-available/
904_make_mysql_db_backup.sh -s to check if it works
9202/Restored the db from file (%s) - no action needed
9203/Failed to restore the db from the file (%s) consider to restore to
previously db (%s) -
to run with output directed to screen: add a '-s' or '--screen'
```

# 921_copy_htmf_conf.sh

```
9211/ -
9212/ -
to run with output directed to screen: add a '-s' or '--screen'
```

# 922-simple-database-replication-check.sh

```
Simple replication test
9221/Value replicated ok - ok, no action needed
9222/Value differs - databse not replicating (%s != %s), manually check
the database with check master and check slave script
9223/No value from node2 (%s) - check connection manually, ping, telnet,
mysql -h node2 -u dbadmin -p ...
9224/No value from node1 (%s) - check connection manually, ping, telnet,
mysql -h node1 -u dbadmin -p ...
to run with output directed to screen: add a '-s' or '--screen'
```

# database-replication

# 800-create-mysql-ejbca-db.sh

```
Creates an empty ejbca db
8001/Created the db ok - no action is needed
8002/the db was already created  - if you really want to create a new db
the run: 801-drop-existing-and-create-empty-ejbca-db.sh
8003/The db couldn't be created (%s) - Run the script with sh -x
./800-create-mysql-ejbca-db.sh -s to get max verbose output
to run with output directed to screen: add a '-s' or '--screen'
```

# 801-drop-existing-ejbca-db.sh

```
Drop old and creates an empty ejbca db
8011/Dropped the db ok - no action is needed
8012/Dropped the db failed - run the script with sh -x
./801-drop-existing-ejbca-db.sh -s to find out more info
8013/Failed to backup the database before drop - Enable
904_make_mysql_db_backup.sh in related-enabled
```

8014/ -
to run with output directed to screen: add a '-s' or '--screen'

# 802-create-mysql-ejbca-user-db-user.sh

grants access to the ejbca user
8021/access rules inserted into mysql db ok - no action is needed
8022/failed to insert access rules into mysql db - run the script with sh
-x ./802-create-mysql-ejbca-user-db-user.sh -s to find out more info
to run with output directed to screen: add a '-s' or '--screen'

# 803-create-mysql-replication-user.sh

grants access to the ejbca user
8031/Replication access rules inserted into mysql db ok - no action is
needed
8032/failed to insert replication access rules into mysql db - run the
script with sh -x ./803-create-mysql-replication-user.sh -s to find out
more info
to run with output directed to screen: add a '-s' or '--screen'

# 804-make-mysql-server-act-as-master.sh

grants access to the ejbca user
8041/Mysql server made to act as a master - no action is needed
8042/Failed to make mysql server act as a master - check that /etc/my.cnf
has log-bin=mysql-bin and a unique server-id
to run with output directed to screen: add a '-s' or '--screen'

# 805-make-mysql-server-act-as-slave.sh

Makes this mysql server acts as a slave
8051/Mysql server made to act as a slave - no action is needed
8052/Failed to make mysql server act as a slave - check that /etc/my.cnf
has log-bin=mysql-bin and a unique server-id
to run with output directed to screen: add a '-s' or '--screen'

# 806-change-active-mysql-server-in-jboss-datasource.sh

arg1 must be the node to enter in the ds conf (node1 or node2)

# 807-test-table-create-table.sh

/ -
/ -
/ -

/ -

# 808-test-table-update-and-check-master-and-slave.sh

/ -
/ -
/ -
/ -

# 809-show-mysql-slave-status.sh

```
Show the mysql server slave status
8091/Slave status shown - no action is needed
8092/Failed to make mysql server show slave status - check that /etc/
my.cnf has log-bin=mysql-bin and a unique server-id
to run with output directed to screen: add a '-s' or '--screen'
```

# 810-show-mysql-master-status.sh

```
Show the mysql server master status
8101/Master status shown - no action is needed
8102/Failed to make mysql server show master status - check that /etc/
my.cnf has log-bin=mysql-bin and a unique server-id
to run with output directed to screen: add a '-s' or '--screen'
```

# 811-master-node-flush-tables-with-read-lock.sh

```
Set mysql server FLUSH TABLES WITH READ LOCK;
8111/Set mysql FLUSH TABLES WITH READ LOCK ok - no action is needed
8112/Failed to set mysql server FLUSH TABLES WITH READ LOCK; - try
manually with mysql mysql -u root -p then > FLUSH TABLES WITH READ LOCK;
to run with output directed to screen: add a '-s' or '--screen'
```

# 812-master-node-unlock-tables.sh

```
cant open configfile (/misc/src/syscheck/syscheck-1.5.0/config/812.conf)
```

# 813-mysql-console-as-root.sh

/ -
/ -

/ –
/ –

# 814-mysql-console-as-db-user.sh

/ –
/ –
/ –
/ –