How to Update sysck.cfg in the TCB Database

Special Notices

Information in this document is correct to the best of our knowledge at the time of this writing. Please send feedback by fax to "AIXServ Information" at (512) 823-4009.

Please use this information with care. IBM will not be responsible for damages of any kind resulting from its use. The use of this information is the sole responsibility of the customer and depends on the customer's ability to evaluate and integrate this information into the customer's operational environment.

Note: The information in this document has **not** been verified for AIX 4.1.

About This Document

This document describes how to update the /etc/security/sysck.cfg TCB database to match what is currently installed on your system.

The Trusted Computing Base is responsible for enforcing the information security policies of the system. All of the computer's hardware is included in the TCB.

Warning Do not run tcbck -y ALL unless you are sure the files on the system match the contents of the sysck.cfg database. This command will disable the ACL's of any files that do not match.

Please read about the the tcbck command in InfoExplorer and become familiar with its options and functions.

Procedure

The following shows some examples for the use of the tcbck command. Please refer to the man page for the tcbck command for a full description of function, flags and attributes.

1. Log in as root.
2. Execute the following script.

   Note: This will overwrite /etc/security/sysck.cfg. Save a copy of this file before starting this script.

```
#!/bin/ksh
for x in $( grep : /etc/security/sysck.cfg | sed 's/://g' | tail +2 )
  do
        echo "working on" $x
        if [ -d "$x" -o  -c "$x" -o -b "$x" ]
        then
#   if directory or special file - size and checksum do not apply

                tcbck -a $x owner group type mode
        else
                tcbck -a $x owner group type mode size checksum
        fi
    done
```

3. If you want to add a new file to the TCB Database - execute

   ```
   tcbck -a /path_name/new_file  owner group type mode size checksum
   ```

   This will create a new stanza in /etc/security/sysck.cfg with the attributes; owner, group, type, mode, size and checksum.

4. To remove an attribute like a symbolic link execute

   ```
   tcbck -a tcb_file_name symlinks=
   ```

5. Periodically you can execute " tcbck -n ALL " to check the integrity of your system

6. The command

   ```
   tcbck -n tree
   ```

   checks all files in the filesystem to ensure that all relevant files are defined in the sysck database. Files defined in the database are checked against their definitions. Files not in the database, that have the following attributes will be reported:

   - have the trusted computing base attribute set.
   - be setuid or setgid to an administrative ID.
   - be linked to a file in the tcbck database.
   - be a device special file.

7. If the TCB attribute is defined in the sysck.cfg database for a specific file but is not set on the file on your system you will receive the following error:

   ```
   3001-027 The file /usr/bin/acledit has the wrong TCB attribute value.
   ```

   This message is not referring to the rwx attributes of the module. Rather it is referring to the Trusted Computing Base attribute. In /etc/security/sysck.cfg, the stanza for a module will have line mode = TCB,555. This means the permissions are r-xr-xr-x and the TCB flag is set.

   The following command can be used to modify and query the TCB attribute of the file.

```
chtcb query /usr/bin/acledit    -- will display the attribute
chtcb on    /usr/bin/acledit    -- will set the attribute
chtcb off   /usr/bin/acledit    -- will reset the attribute
```

8. After applying PTF's (fixes) to your system "tcbck -n ALL" may report errors for the newly installed files such as, the size, and checksum. To correct the size and checksum in the database to match your system execute:

   ```
   tcbck -a /path_name/changed_file size checksum
   ```

   This command will re-calculate the size and checksum of the changed file and update the sysck database.

Reader's Comments

Please fax this form to (512) 823-4009, attention "AIXServ Information". You may also e-mail comments to: elizabet@austin.ibm.com. These comments should include the same customer information requested below.

Use this form to tell us what you think about this document. If you have found errors in it, or if you want to express your opinion about it (such as organization, subject matter, appearance) or make suggestions for improvement, this is the form to use.

If you need technical assistance, contact your local branch office, point of sale, or 1-800-CALL-AIX (for information about support offerings). These services may be billable. Faxes on a variety of subjects may be ordered free of charge from 1-800-IBM-4FAX. Outside the U.S. call 415-855-4329 using a fax machine phone.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Note: If you have a problem report or item number, supplying that number may help us determine why a procedure did or did not work in your specific situation.

Problem Report or Item #: Branch Office or Customer #:

Be sure to print your name and fax number below if you would like a reply:

Name: Fax Number:

END OF DOCUMENT (about.tcbck.32.cmd, 4FAX# 1074)