BigFix® Security Configuration Management (SCM) AIX Parameters

BigFix, Inc.

Emeryville, CA

Last Modified: 9/18/2008

© 2008 BigFix, Inc. All rights reserved.

BigFix®, Fixlet® and "Fix it before it fails"® are registered trademarks of BigFix, Inc. iprevention, Powered by BigFix, Relevance Engine, and related BigFix logos are trademarks of BigFix, Inc. All other product names, trade names, trademarks, and logos used in this documentation are the property of their respective owners. BigFix's use of any other company's trademarks, trade names, product names and logos or images of the same does not necessarily constitute: (1) an endorsement by such company of BigFix and its products, and (2) an endorsement of the company or its products by BigFix.

Except as set forth in the last sentence of this paragraph: (1) no part of this documentation may be reproduced, transmitted, or otherwise distributed in any form or by any means (electronic or otherwise) without the prior written consent of BigFix, Inc., and (2) you may not use this documentation for any purpose except in connection with your properly licensed use or evaluation of BigFix software and any other use, including for reverse engineering such software or creating derivative works thereof, is prohibited. If the license to the software that this documentation accompanies is terminated, you must immediately return this documentation to BigFix, Inc. and destroy all copies you may have. You may treat only those portions of this documentation specifically designated in the "Acknowledgements and Notices" section below as notices applicable to third party software in accordance with the terms of such notices.

All inquiries regarding the foregoing should be addressed to:

BigFix, Inc.

1480 64th Street, Suite 200

Emeryville, CA 94608

Contents

© 2008 by BigFix, Inc.

© 2008 by BigFix, Inc.

Preface

Audience

This document describes the available parameters for the BigFix Security Configuration Management (SCM) on the supported AIX platforms. The supported platforms described in this document include:

- AIX 5.1
- AIX 5.2
- AIX 5.3

The BigFix AIX SCM site comes pre-packaged with configuration controls that provide assessment against the operating system for a given setting. Each of the controls includes a default value that you can customize to meet the specific policies or requirements of your organization. This is done by modifying the parameters passed to the control. This document describes the modifiable controls and the parameters you can pass to them. For more information on actual implementation of these parameters, see the UNIX section of the ***BigFix SCM Deployment Guide***.

The audience for this guide includes the administrators in IT operations responsible for managing and enforcing Federal and Industry Regulations on AIX systems. Security teams and IT managers in the enterprise can modify the security parameters and configurations to suit corporate policy.

Conventions Used in this Manual

This document makes use of the following conventions:

Bold Sans	Bold sans-serif font is used for headings.
Italics	Bold Italics are used for BigFix document titles.
`Mono-space`	Mono-space font is used for sample code and usage.

Product Requirements

To deploy and modify the parameters listed here, the BigFix deployment must be configured according to these minimum requirements:

- Console 7.0.9
- Web Reports 7.0.9
- Unix Client 7.0.2

© 2008 by BigFix, Inc.

Parameter Formats

The following sections provide the detail necessary for a user to properly configure the defined configuration settings. For each control, you will find the following information:

- **Control Names:** This provides the Source ID name (such as GEN000340), corresponding to standard DISA STIG definitions and the name of the control derived from the related Fixlet.
- **Control Description:** This provides a brief description of the control, condensed from the associated Fixlet.
- **Control Parameter Details:** This lists the parameter(s), along with the default setting(s).
- **Example Usage within Custom Parameter File:** This provides a working illustration of how the control parameter(s) might be implemented as described in the UNIX section of the ***BigFix SCM Deployment Guide***.

In many of these controls you will find parameters that modify file permissions. Before modifying these permissions, you should be familiar with the use of regular expressions. Failure to specify a correct value for PERMS_REGEX can cause false positives, false negatives or may prevent the control from functioning at all. For more information, consult the section **Using Regular Expressions to Specify File Permissions** at the end of this Guide.

© 2008 by BigFix, Inc.

AIX 5.1 Parameters

GEN000340: Reserved System Account UIDs

Control Description:

Ensures that uids 0 - 99 (0 - 499 for Linux) are reserved for system accounts.

Control Parameter Details:

Parameter 1: SYSTEM_ACCOUNTS - This Parameter is a space-separated list of user IDs to be considered system accounts. Accounts that are allowed to have UIDs < 100 should be specified in this parameter.

Default Setting: "root daemon bin sys adm uucp guest nobody lpd lp invscout snapp ipsec nuucp"

Example Usage Within Custom Parameter File:

```
GEN000340: SYSTEM_ACCOUNTS="root daemon bin sys adm uucp guest
nobody lpd lp invscout snapp ipsec nuucp"
```

GEN000360: Reserved System Account GIDs

Control Description:

Ensures that gids 0 - 99 (0 - 499 for Linux) are reserved for system accounts.

Control Parameter Details:

Parameter 1: SYSTEM_GROUPS - This parameter is a space-separated list of GIDs to be considered system groups. Accounts that are allowed to have GIDs < 100 should be specified in this parameter.

Default Setting: "system staff bin sys adm uucp mail security cron printq audit ecs perf shutdown lp invscout snapp ipsec"

Example Usage Within Custom Parameter File:

```
GEN000360:SYSTEM_GROUPS="system staff bin sys adm uucp mail
security cron printq audit ecs perf shutdown lp invscout snapp
ipsec"
```

© 2008 by BigFix, Inc.

GEN000480: Login Delay

Control Description:

Ensures that the logon delay between logon prompts after a failed logon is set to at least four seconds.

Control Parameter Details:

Parameter 1: VALUE - This parameter represents the number of seconds to delay after an unsuccessful login. This equates to the logindelay setting in /etc/security/login.cfg which, if present, sets the number of seconds to wait before the login failure message is printed to the screen.

Default Setting: 4

Example Usage Within Custom Parameter File:

```
GEN000480:SETTING=4
```

GEN000540: Minimum Password Age

Control Description:

Ensures that passwords are not changed more than once a day.

Control Parameter Details:

Parameter 1: VALUE - This parameter represents the minimum number of days before the password may be changed. This corresponds to the minage setting in /etc/security/user.

Default Setting: 1

Example Usage Within Custom Parameter File:

```
GEN000540:SETTING=1
```

© 2008 by BigFix, Inc.

GEN000580: Minimum Password Length

Control Description:

Ensures that all passwords contain a minimum of eight characters.

Control Parameter Details:

Parameter 1: VALUE - This parameter represents the minimum password length. This corresponds to the minlen setting in /etc/security/user.

Default Setting: 8

Example Usage Within Custom Parameter File:

```
GEN000580:SETTING=8
```

GEN000600a: Password Complexity - alphabetic characters

Control Description:

Ensures that passwords include at least two alphabetic characters, one of which must be capitalized.

Control Parameter Details:

Parameter 1: VALUE - This parameter represents the minimum number of alphabetical characters in passwords. This corresponds to the minalpha setting in /etc/security/user.

Default Setting: 2

Example Usage Within Custom Parameter File:

```
GEN000600a: SETTING=2
```

© 2008 by BigFix, Inc.

GEN000620: Password Complexity - numeric characters

Control Description:

Ensures that passwords include at least one numeric character.

Control Parameter Details:

Parameter 1: VALUE - This parameter represents the minimum number of numeric characters required in passwords. This corresponds to the minother setting in /etc/security/user.

Default Setting: 1

Example Usage Within Custom Parameter File:

```
GEN000620:SETTING=1
```

GEN000680: Password Complexity - no consecutive characters

Control Description:

Ensures that passwords contain no consecutive characters.

Control Parameter Details:

Parameter 1: VALUE - This parameter represents the maximum number of consecutive characters allowed in passwords. This corresponds to the maxrepeats setting in /etc/security/user.

Default Setting: 1

Example Usage Within Custom Parameter File:

```
GEN000680:SETTING=3
```

© 2008 by BigFix, Inc.

GEN000700: Maximum Password Age

Control Description:

Ensures that passwords are changed at least every 90 days.

Control Parameter Details:

Parameter 1: VALUE - This parameter represents the maximum number of weeks before a required password change. This corresponds to the maxage setting in /etc/security/user.

Default Setting: 12

Example Usage Within Custom Parameter File:

```
GEN000700:SETTING=12
```

GEN000800: Enforce Password History

Control Description:

Ensures that passwords will not be reused within the last ten changes.

Control Parameter Details:

Parameter 1: VALUE - This parameter represents the maximum number of prior passwords to keep, the maximum allowable value is 50. This corresponds to the histsize setting in /etc/security/user.

Default Setting: 10

Example Usage Within Custom Parameter File:

```
GEN000800:SETTING=10
```

© 2008 by BigFix, Inc.

GEN001180: Network Services Daemon Permissions

Control Description:

Ensures that all daemons have permissions of 755, or more restrictive. This control looks in /usr/bin and /usr/sbin (where system daemons are located) for files that have permissions less restrictive than 0755. Additional files may be specified and specific files may be excluded from this test.

Control Parameter Details:

Parameter 1: EXCLUDEFILES - This parameter may be used to exclude specific files from this test; it must be a space-separated list of the absolute paths of files to be excluded.

Default Setting: ""

Parameter 2: INCLUDEFILES - This parameter allows you to specify files outside of the /usr/bin and /usr/sbin directories to include in this test. It must be a space-separated list of the absolute path of the additional files you wish to include. This value may be null i.e. INCLUDEFILES="".

Default Setting: "/usr/local/apache2/bin/httpd /usr/lib/ssh/sshd"

Parameter 3: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w][-x][-r]-[-x][-r]-[-x]"

Parameter 4: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0755"

Example Usage Within Custom Parameter File:

```
GEN001180:EXCLUDEFILES="";INCLUDEFILES="/usr/local/apache2/bin
/httpd /usr/lib/ssh/sshd";PERMS_REGEX="-[-r][-w][-x][-r]-[-
x][-r]-[-x]";PERMS_DESC="0755"
```

© 2008 by BigFix, Inc.

GEN001200: System Command Permissions

Control Description:

Ensures that all system commands have permissions of 755, or more restrictive. This test looks in INCLUDEDIRS for files that have permissions less restrictive than PERMS_REGEX. Additional directories may be specified and specific files may be excluded from this test.

Control Parameter Details:

Parameter 1: INCLUDEDIRS - This parameter allows you to specify which directories to apply this test to; it must be a space-separated list of directories to search and it must not be null.

Default Setting: "/etc /bin /usr/bin /sbin /usr/sbin /usr/ucb /usr/lbin"

Parameter 2: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0755"

Parameter 3: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w][-x][-r]-[-x][-r]-[-x]"

Parameter 4: EXCLUDEFILES - This parameter allows you to indicate specific files to exclude from this test, it must be an egrep regular expression specifying the absolute path of the files to exclude. It may be null i.e. EXCLUDEFILES="^$".

Default Setting: "^$"

Example Usage Within Custom Parameter File:

```
GEN001200:INCLUDEDIRS="/etc /bin /usr/bin /sbin /usr/sbin
/usr/ucb /usr/lbin";PERMS_DESC="0755";PERMS_REGEX="-[-r][-w][-
x][-r]-[-x][-r]-[-x]";EXCLUDEFILES="^$"
```

© 2008 by BigFix, Inc.

GEN001220: System Files - Programs and Directories Ownership

Control Description:

Ensures that the owner of all system files, programs, and directories is a system account.

Control Parameter Details:

Parameter 1: INCLUDEDIRS - This parameter is a space-separated list of directories in which to look for system files and programs.

Default Setting: "/etc /bin /usr/bin /sbin /usr/sbin /usr/ucb /usr/lbin"

Parameter 2: ALLOWED - This parameter is a pipe-separated list defining which usernames are considered system accounts.

Default Setting: "root|daemon|bin|sys|adm|uucp|lpd|lp|invscout|snapp|ipsec|imnadm"

Example Usage Within Custom Parameter File:

```
GEN001220:INCLUDEDIRS="/etc /bin /usr/bin /sbin /usr/sbin
/usr/ucb
/usr/lbin";ALLOWED="root|daemon|bin|sys|adm|uucp|lpd|lp|invsco
ut|snapp|ipsec|imnadm"
```

GEN001240: System Files - Programs - and Directories Group Ownership

Control Description:

Ensures that the group owner of all system files, programs and directories is a system group.

Control Parameter Details:

Parameter 1: INCLUDEDIRS - This parameter is a space-separated list of directories in which to look for system files and programs.

Default Setting: "/etc /bin /usr/bin /sbin /usr/sbin /usr/ucb"

© 2008 by BigFix, Inc.

Parameter 2: ALLOWED - This parameter is a pipe-separated list defining which group names are considered system groups.

Default Setting:
"system|bin|sys|adm|uucp|mail|security|cron|printq|audit|ecs|perf|shutdown|lp|invscout|snapp|ipsec|staff|imnadm"

Example Usage Within Custom Parameter File:

```
GEN001240:INCLUDEDIRS="/etc /bin /usr/bin /sbin /usr/sbin
/usr/ucb";ALLOWED="system|bin|sys|adm|uucp|mail|security|cron|
printq|audit|ecs|perf|shutdown|lp|invscout|snapp|ipsec|staff|i
mnadm"
```

GEN001260: System Log File Permissions

Control Description:

The SA will ensure all system log files have permissions of 644, or more restrictive. This control looks at the system log files returned by the output of the alog command and the system log files defined in /etc/syslog.conf.

Control Parameter Details:

Parameter 1: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-[-r]--[-r]--"

Parameter 2: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0644"

Example Usage Within Custom Parameter File:

```
GEN001260:PERMS_REGEX="-[-r][-w]-[-r]--[-r]--
";PERMS_DESC="0644"
```

© 2008 by BigFix, Inc.

GEN001280: Manual Page File Permissions

Control Description:

Ensures that all manual page files (i.e., files in the man and cat directories) have permissions of 644, or more restrictive. This control looks in the directory specified by the MANBASE parameter for files with permissions less restrictive than specified in the PERMS_REGEX parameter. It also provides an INCLUDEFILES parameter which allows users to specify additional single files which should be included in this test.

Control Parameter Details:

Parameter 1: MANBASE - This parameter must be a space-separated list of directories to check under, for example MANBASE="/usr/share/man /usr/local/man".

Default Setting: "/usr/share/man"

Parameter 2: INCLUDEFILES - This parameter must be a space-separated list of the absolute path of additional files to include in the test.

Default Setting: ""

Parameter 3: EXCLUDEFILES - This parameter must be space-separated list of the absolute path of files within MANBASE to exclude from this test.

Default Setting: ""

Parameter 4: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-[-r]--[-r]--"

Parameter 5: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0644"

Example Usage Within Custom Parameter File:

```
GEN001280:MANBASE="/usr/share/man";EXCLUDEFILES="";INCLUDEFILE
S="";PERMS_REGEX="-[-r][-w]-[-r]--[-r]--";PERMS_DESC="0644"
```

© 2008 by BigFix, Inc.

GEN001300: Library File Permissions

Control Description:

Ensures that all system library files have permissions of 755, or more restrictive. This control looks in the directories specified in the LIBBASE parameter for files with permissions less restrictive than specified in the PERMS_REGEX parameter. It also provides an INCLUDEFILES parameter which allows users to specify additional single files which should be included in this test.

Control Parameter Details:

Parameter 1: LIBBASE - This parameter must be a space-separated list of directories to check under.

Default Setting: "/lib /usr/lib"

Parameter 2: INCLUDEFILES - This parameter must be a space-separated list of the absolute path of additional files to include in the test.

Default Setting: ""

Parameter 3: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w][-x][-r]-[-x][-r]-[-x]"

Parameter 4: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0755"

Example Usage Within Custom Parameter File:

```
GEN001300:LIBBASE="/usr/lib";INCLUDEFILES="";PERMS_REGEX="-[-
r][-w][-x][-r]-[-x][-r]-[-x]";PERMS_DESC="0755"
```

© 2008 by BigFix, Inc.

GEN001360: NIS/NIS+/yp File Permissions

Control Description:

Ensures that all NIS/NIS+/yp files have permissions of 755, or more restrictive. This control checks the /usr/lib/netsvc/yp and /usr/lib/nis directories for files that have permissions less restrictive than specified by the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w][-x][-r]-[-x][-r]-[-x]"

Parameter 2: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0755"

Example Usage Within Custom Parameter File:

```
GEN001360:PERMS_REGEX="[-d][-r][-w][-x][-r]-[-x][-r]-[-
x]";PERMS_DESC="0755"
```

GEN001580: Run Control Scripts Permissions

Control Description:

Ensures that run control scripts have permissions of 755, or more restrictive. This control looks in /etc/rc* for files with permissions less restrictive than specified in the PERMS_DESC parameter. In addition it provides an INCLUDEFILES parameter that allows you to specify additional files that should be tested.

Control Parameter Details:

Parameter 1: INCLUDEFILES - This parameter allows you to specify additional files to include in this test.

Default Setting: ""

© 2008 by BigFix, Inc.

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w][-x][-r]-[-x][-r]-[-x]"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0755"

Example Usage Within Custom Parameter File:

```
GEN001580:INCLUDEFILES="";PERMS_REGEX="-[-r][-w][-x][-r]-[-
x][-r]-[-x]";PERMS_DESC="0755"
```

GEN001700: Run Control Scripts Execute Programs

Control Description:

Ensures that run control scripts only execute programs owned by a system account or an application default. This control looks in the directories specified by the RC_DIRS parameter and the files specified by the RC_FILES parameter for files that are not owned by either the accounts specified in the SYS_ACCOUNTS parameter or the APP_ACCOUNTS parameter.

Control Parameter Details:

Parameter 1: RC_DIRS - This parameter must be a space-separated list of directories to look in, in addition this list must be preceded and followed by a single character.

Default Setting: ""

Parameter 2: RC_FILES - This parameter must be a space-separated list of files to check. In addition it must be preceded and followed by a single character.

Default Setting: "/etc/rc*"

Parameter 3: SYS_ACCOUNTS - This parameter must be an egrep regular expression that will evaluate to the default system accounts.

Default Setting: ""^root$|^daemon$|^bin$|^sys$|^adm$|^lp$|^uucp$|^ipsec$"

© 2008 by BigFix, Inc.

Parameter 4: APP_ACCOUNTS - This parameter is appended to the SYS_ACCOUNTS parameter to construct an egrep regular expression of all the accounts that may be allowed to own run control scripts. Because the two regular expressions are combined the SYS_ACCOUNTS regular expression must start with a '|' (regular expression alternation) character.

Default Setting: "|^oracle$"

Example Usage Within Custom Parameter File:

```
GEN001700:RC_DIRS="";RC_FILES="/etc/rc*";CONTROL_FILES="/sbin/
rc.boot";SYS_ACCOUNTS="^root$|^daemon$|^bin$|^sys$|^adm$|^lp$|
^uucp$|^ipsec$";APP_ACCOUNTS="|^oracle$"
```

GEN001720: Global Initialization Files Permissions

Control Description:

Ensures that global initialization files have permissions of 644, or more restrictive. This control looks at /etc/.login /etc/profile /etc/bashrc /etc/environment /etc/security/environ and checks if their permissions are less restrictive than specified in the PERMS_REGEX parameter. In addition it provides an INCLUDEFILES parameter for specifying additional files to test, and an EXCLUDEFILES parameter for removing one or more of the default files from the test.

Control Parameter Details:

Parameter 1: EXCLUDEFILES - This parameter must be an egrep regular expression that will evaluate to the files to exclude from the test.

Default Setting: ""

Parameter 2: INCLUDEFILES - This parameter must be a space-separated list of the absolute path of additional files to include in the test.

Default Setting: ""

Parameter 3: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-[-r]--[-r]--"

© 2008 by BigFix, Inc.

Parameter 4: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0644"

Example Usage Within Custom Parameter File:

```
GEN001720:EXCLUDEFILES="";INCLUDEFILES="";PERMS_REGEX="-[-r][-
w]-[-r]--[-r]--";PERMS_DESC="0644"
```

GEN001800: Default/Skeleton Dot Files Permissions

Control Description:

Ensures that all default/skeleton dot files have permissions of 644, or more restrictive. This control checks that the permissions of all files specified by the SKEL_FILES parameter have permissions at least as restrictive as specified in the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: SKEL_FILES - This parameter must be a space-separated list of the absolute path of the skeleton directory.

Default Setting: "/usr/lib/security/mkuser.default /etc/security/.profile"

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-[-r]--[-r]--"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0644"

Example Usage Within Custom Parameter File:

```
GEN001800:SKEL_FILES="/usr/lib/security/mkuser.default
/etc/security/.profile";PERMS_DESC="0644";PERMS_REGEX="-[-r][-
w]-[-r]--[-r]--"
```

© 2008 by BigFix, Inc.

GEN001880: Local Initialization Files Permissions

Control Description:

Ensures that local initialization files have permissions of 740, or more restrictive. The following files/directories are to be excluded from GEN001880: .dt (a directory, this should have permissions of 755) and .dtprofile (which should also have permissions of 755). This control checks the local initialization files specified in the DOT_FILES parameter for permissions less restrictive than specified in the PERMS_REGEX parameter. It automatically excludes the ~/.dt directory from this test; in addition it provides the DTLOGIN parameter for specifying the location of the .dtprofile file.

Control Parameter Details:

Parameter 1: DOT_FILES - This parameter must be a space-separated list of the local initialization files to check.

Default Setting: ".login .cshrc .logout .profile .bash_profile .bashrc .bash_logout .env .dispatch .emacs .exrc"

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w][-x][-r]-----"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0740"

Parameter 4: DTLOGIN_FILE - This parameter must specify the basename (see man basename) of the .dtprofile file.

Default Setting: ".dtlogin"

Example Usage Within Custom Parameter File:

```
GEN001880:DOT_FILES=".login .cshrc .logout .profile
.bash_profile .bashrc .bash_logout .env .dispatch .emacs
.exrc";PERMS_REGEX="-[-r][-w][-x][-r]-----
";PERMS_DESC="0740";DTLOGIN_FILE=".dtlogin"
```

© 2008 by BigFix, Inc.

GEN002240: Device file locations

Control Description:

All device files will be located in the directory trees as installed and designated by the operating system and/or application vendor. This control checks that all device (block and character special) files are located in or under the directories specified by the DEVDIRS parameter. It also provides the EXCLUDEFILES and EXCLUDEDIRS parameters for specifying files and subdirectories of DEVDIRS that should be excluded from this test.

Control Parameter Details:

Parameter 1: DEVDIRS - This parameter must be a space-separated list of directories to test the files in.

Default Setting: "/dev"

Parameter 2: EXCLUDEFILES - This parameter must be an egrep regular expression of the absolute paths of files to exclude from this test.

Default Setting: ""

Parameter 3: EXCLUDEDIRS - This parameter must be an egrep regular expression of subdirectories of the directories specified in the DEVDIRS parameter to exclude from this test.

Default Setting: ""

Example Usage Within Custom Parameter File:

```
GEN002240:DEVDIRS="/dev";EXCLUDEFILES="";EXCLUDEDIRS=""
```

© 2008 by BigFix, Inc.

GEN002300a: Backup Files Ownership

Control Description:

Ensures that backup devices (e.g., tape and floppy disk device) and files will only be readable and writable by root. This control tests /dev/rmt* and /dev/fd* and ensures that they are owned by root. It also provides the EXTRAFILES parameter for specifying additional files.

Control Parameter Details:

Parameter 1: EXTRAFILES - This parameter must be a space-separated list of additional files to include in this test.

Default Setting: ""

Example Usage Within Custom Parameter File:

```
GEN002300a:EXTRAFILES=""
```

GEN002300b: Backup Files Ownership

Control Description:

Ensures that backup devices (e.g., tape and floppy disk device) and files will only be readable and writable by root. This control tests /dev/rmt* and /dev/fd* and ensures that they are group-owned by root. It also provides the EXTRAFILES parameter for specifying additional files.

Control Parameter Details:

Parameter 1: EXTRAFILES - This parameter must be a space-separated list of additional files to include in this test.

Default Setting: ""

Example Usage Within Custom Parameter File:

```
GEN002300b:EXTRAFILES=""
```

© 2008 by BigFix, Inc.

GEN002300c: Backup Files Ownership

Control Description:

Ensures that backup devices (e.g., tape and floppy disk device) and files will only be readable and writable by root. This control tests /dev/rmt* and /dev/fd* and ensures that the permissions only allow write access for the owner. It also provides the EXTRAFILES parameter for specifying additional files.

Control Parameter Details:

Parameter 1: EXTRAFILES - This parameter must be a space-separated list of additional files to include in this test.

Default Setting: ""

Example Usage Within Custom Parameter File:

```
GEN002300c:EXTRAFILES=""
```

GEN002320: Audio Device Permissions

Control Description:

Ensures that the audio devices have permissions of 644, or more restrictive. This control ensures that the audio device specified in the CONFIG_FILE parameter has permissions at least as restrictive as specified in the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must specify the absolute path of the audio device file; at this time only a single audio device file is supported.

Default Setting: /dev/paud0

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "[-c][-r][-w]-[-r]--[-r]--"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0644"

© 2008 by BigFix, Inc.

Example Usage Within Custom Parameter File:

```
GEN002320:CONFIG_FILE=/dev/paud0;PERMS_REGEX="[-c][-r][-w]-[-
r]--[-r]--";PERMS_DESC="0644"
```

GEN002340: Audio Device Ownership

Control Description:

Ensures that the owner of audio devices is root. This control checks that the file specified in the CONFIG_FILE parameter is owned by the user specified in the VALUE parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must be the absolute path of the audio device file. At this time only a single file is supported.

Default Setting: /dev/paud0

Parameter 2: VALUE - This parameter must be the user account that should own the file specified in the CONFIG_FILE parameter.

Default Setting: "root"

Example Usage Within Custom Parameter File:

```
GEN002340:CONFIG_FILE=/dev/paud0;VALUE="root"
```

GEN002360: Audio Device Group Ownership

Control Description:

Ensures that the group owner of audio devices is root, sys, or bin. This control checks that the owner of the file specified in the CONFIG_FILE parameter is group owned by one of the accounts specified in the VALUE parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must be the absolute path of the audio device file. At this time only a single file is supported.

Default Setting: /dev/paud0

© 2008 by BigFix, Inc.

Parameter 2: VALUE - This parameter must be a space-separated list of the group account names that may group-own the file specified in the CONFIG_FILE parameter.

Default Setting: "system sys bin audio"

Example Usage Within Custom Parameter File:

```
GEN002360:CONFIG_FILE=/dev/paud0;VALUE="system sys bin audio"
```

GEN002520: Public Directories Ownership

Control Description:

Ensures that the owner of public directories is root or the application user. This control checks that all world-writable directories with the sticky bit set are owned by a user specified in the VALUE parameter. In addition it provides an EXCLUDEDIRS parameter for excluding specific directories from this test.

Control Parameter Details:

Parameter 1: EXCLUDEDIRS - This parameter must be a space-separated list of directories to exclude from this test.

Default Setting: "/var/spool/samba"

Parameter 2: VALUE - This parameter must be a space-separated list of usernames that may own world-writable directories.

Default Setting: "root bin mail uucp"

Example Usage Within Custom Parameter File:

```
GEN002520:EXCLUDEDIRS="/var/spool/samba"VALUE="root bin mail
uucp"
```

© 2008 by BigFix, Inc.

GEN002540: Public Directories Group Ownership

Control Description:

Ensures that the group owner of public directories is root, sys, bin, or the application group. This control checks that all world-writable directories with the sticky bit set are group-owned by one of the accounts specified in the VALUE parameter. In addition it provides an EXCLUDEDIRS parameter for specifying directories that should be excluded from this test.

Control Parameter Details:

Parameter 1: EXCLUDEDIRS - This parameter must be a space-separated list of directories to exclude from this test.

Default Setting: "/var/spool/samba"

Parameter 2: VALUE - This parameter must be a space-separated list of group account names that should group-own the directories specified above.

Default Setting: "system sys bin mail uucp"

Example Usage Within Custom Parameter File:

```
GEN002540:EXCLUDEDIRS="/var/spool/samba";VALUE="system sys bin
mail uucp"
```

GEN002980: /etc/cron.allow Permissions

Control Description:

Ensures that the cron.allow file has permissions of 600, or more restrictive. This control checks that the file specified by the CONFIG_FILE parameter has permissions at least as restrictive as specified in the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must be the absolute path of the file to check.

Default Setting: /var/adm/cron/cron.allow

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-------"

© 2008 by BigFix, Inc.

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0600"

Example Usage Within Custom Parameter File:

```
GEN002980:CONFIG_FILE=/var/adm/cron/cron.allow;PERMS_REGEX="-
[-r][-w]-------";PERMS_DESC="0600"
```

GEN003060: Default System Accounts and Cron

Control Description:

Ensures that default system accounts (with the possible exception of root) will not be listed in the cron.allow file. If there is only a cron.deny file, the default accounts (with the possible exception of root) will be listed there. This control checks that the system accounts specified by the CRON_SYS_ACCT_USERS parameter are not present in the file specified by the CRON_ALLOW_FILE parameter. If the file specified by the CRON_ALLOW_FILE parameter does not exist, it checks that the accounts are present in the file specified by the CRON_DENY_FILE parameter.

Control Parameter Details:

Parameter 1: CRON_SYS_ACCT_USERS - This parameter must contain a space-separated list of usernames that should not be allowed to use the cron utility.

Default Setting: "daemon bin sys adm uucp guest nobody lpd lp invscout snapp ipsec nuucp"

Parameter 2: CRON_ALLOW_FILE - This parameter must specify the absolute path of the cron.allow file.

Default Setting: /var/adm/cron/cron.allow

Parameter 3: CRON_DENY_FILE - This parameter must specify the absolute path of the cron.deny file.

Default Setting: /var/adm/cron/cron.deny

Example Usage Within Custom Parameter File:

```
GEN003060:CRON_SYS_ACCT_USERS="daemon bin sys adm uucp guest
nobody lpd lp invscout snapp ipsec
nuucp";CRON_ALLOW_FILE=/var/adm/cron/cron.allow;CRON_DENY_FILE
=/var/adm/cron/cron.deny
```

© 2008 by BigFix, Inc.

GEN003080: Crontab files Permissions

Control Description:

Ensures that crontabs have permissions of 600, or more restrictive. This control checks that all files in the directory specified by the CRONTAB_DIR parameter have permissions at least as restrictive as specified in the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CRONTAB_DIR - This parameter must be the directory that the crontab files reside in.

Default Setting: /var/spool/cron/crontabs

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-------"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0600"

Example Usage Within Custom Parameter File:

```
GEN003080:CRONTAB_DIR=/var/spool/cron/crontabs;PERMS_REGEX="-
[-r][-w]-------";PERMS_DESC="0600"
```

© 2008 by BigFix, Inc.

GEN003100a: Cron directory permissions

Control Description:

Ensures that cron and crontab directories have permissions of 755, or more restrictive. This control checks that the permissions of the directory specified in the CONFIG_FILE parameter are at least as restrictive as specified in the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must be the absolute path of the cron directory.

Default Setting: /var/spool/cron

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "d[-r][-w][-x][-r]-[-x][-r]-[-x]"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0755"

Example Usage Within Custom Parameter File:

```
GEN003100a:CONFIG_FILE=/var/spool/cron;PERMS_REGEX="d[-r][-
w][-x][-r]-[-x][-r]-[-x]";PERMS_DESC="0755"
```

GEN003100b: Crontab Directory permissions

Control Description:

Ensures that cron and crontab directories have permissions of 755, or more restrictive. This control checks that the permissions of the directories specified in the CRON_DIRS parameter have permissions at least as restrictive as specified in the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CRON_DIRS - This parameter must be a space-separated list of the absolute paths of the cron and crontab directories.

Default Setting: /var/spool/cron/crontabs

© 2008 by BigFix, Inc.

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "d[-r][-w][-x][-r]-[-x][-r]-[-x]"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0755"

Example Usage Within Custom Parameter File:

```
GEN003100b:CRON_DIRS=/var/spool/cron/crontabs;PERMS_REGEX="d[-
r][-w][-x][-r]-[-x][-r]-[-x]";PERMS_DESC="0755"
```

GEN003180: Cronlog Permissions

Control Description:

Ensures that cron logs have permissions of 600, or more restrictive. This control checks that the file specified in the CONFIG_FILE parameter has permissions at least as restrictive as specified in the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must specify the absolute path of the cron logfile.

Default Setting: /var/adm/cron/log

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-------"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0600"

Example Usage Within Custom Parameter File:

```
GEN003180:CONFIG_FILE=/var/adm/cron/log;PERMS_REGEX="-[-r][-
w]-------";PERMS_DESC="0600"
```

© 2008 by BigFix, Inc.

GEN003200: cron.deny Permissions

Control Description:

Ensures that the cron.deny file has permissions of 600, or more restrictive. This control checks that the file specified by the CONFIG_FILE parameter has permissions at least as restrictive as specified by the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must specify the absolute path of the cron.deny file

Default Setting: /etc/cron.d/cron.deny

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-------"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0600"

Example Usage Within Custom Parameter File:

```
GEN003200:CONFIG_FILE=/var/adm/cron/cron.deny;PERMS_REGEX="-[-
r][-w]-------";PERMS_DESC="0600"
```

© 2008 by BigFix, Inc.

GEN003320: Default System Accounts and At

Control Description:

Ensures that default system accounts (with the possible exception of root) are not listed in the at.allow file. If there is only an at.deny file, the default accounts (with the possible exception of root) will be listed there. This control checks that the usernames specified in the ACCOUNTS parameter are not in the file specified by the AT_ALLOW parameter. If the file specified by the ALLOW parameter does not exist, it checks that the usernames are listed in the file specified by the DENY parameter.

Control Parameter Details:

Parameter 1: ACCOUNTS - This parameter must be a space-separated list of usernames that are not allowed to use the at utility.

Default Setting: "daemon bin sys adm uucp guest nobody lpd lp invscout snapp ipsec nuucp"

Parameter 2: DENY - This parameter must specify the absolute path of the at.deny file.

Default Setting: /var/adm/cron/at.deny

Parameter 3: ALLOW - This parameter must specify the absolute path of the at.allow file.

Default Setting: /var/adm/cron/at.allow

Example Usage Within Custom Parameter File:

```
GEN003320:ACCOUNTS="daemon bin sys adm uucp guest nobody lpd
lp invscout snapp ipsec
nuucp";DENY=/var/adm/cron/at.deny;ALLOW=/var/adm/cron/at.allow
```

© 2008 by BigFix, Inc.

GEN003340a: at.allow Permissions

Control Description:

Ensures that the at.allow and at.deny files have permissions of 600, or more restrictive. This control checks that the file specified by the CONFIG_FILE parameter has permissions at least as restrictive as specified by the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must be the absolute path of the at.allow file

Default Setting: /var/adm/cron/at.allow

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-------"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0600"

Example Usage Within Custom Parameter File:

```
GEN003340a:CONFIG_FILE=/var/adm/cron/at.allow;PERMS_REGEX="-[-
r][-w]-------";PERMS_DESC="0600"
```

GEN003340b: at.deny Permissions

Control Description:

Ensures that the at.allow and at.deny files have permissions of 600, or more restrictive. This control checks that the file specified by the CONFIG_FILE parameter has permissions at least as restrictive as specified by the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must be the absolute path of the at.deny file.

Default Setting: /var/adm/cron/at.deny

© 2008 by BigFix, Inc.

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-------"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0600"

Example Usage Within Custom Parameter File:

```
GEN003340b:CONFIG_FILE=/var/adm/cron/at.deny;PERMS_REGEX="-[-
r][-w]-------";PERMS_DESC="0600"
```

GEN003780: Services file Permissions

Control Description:

Ensures that the services file has permissions of 644, or more restrictive. This control checks that the permissions of the file specified by the CONFIG_FILE parameter has permissions at least as restrictive as specified by the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must specify the absolute path of the services file.

Default Setting: /etc/services

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-[-r]--[-r]--"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0644"

Example Usage Within Custom Parameter File:

```
GEN003780:CONFIG_FILE=/etc/services;PERMS_REGEX="-[-r][-w]-[-
r]--[-r]--";PERMS_DESC="0644"
```

© 2008 by BigFix, Inc.

GEN004000: traceroute command permissions

Control Description:

Ensures that the traceroute command has permissions of 700, or more restrictive. This control checks that the file specified by the CONFIG_FILE parameter has permissions at least as restrictive as specified by the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must specify the absolute path of the traceroute command.

Default Setting: /usr/bin/traceroute

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w][-x]------"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0700"

Example Usage Within Custom Parameter File:

```
GEN004000:CONFIG_FILE=/usr/bin/traceroute;PERMS_REGEX="-[-r][-
w][-x]------";PERMS_DESC="0700"
```

GEN004380: aliases file permissions

Control Description:

Ensures that the aliases file has permissions of 644, or more restrictive. This control checks that the file specified by the CONFIG_FILE parameter has permissions at least as restrictive as specified by the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must specify the absolute path of the sendmail aliases file.

Default Setting: /etc/mail/aliases

© 2008 by BigFix, Inc.

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-[-r]--[-r]--"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0644"

Example Usage Within Custom Parameter File:

```
GEN004380:CONFIG_FILE=/etc/mail/aliases;PERMS_REGEX="-[-r][-
w]-[-r]--[-r]--";PERMS_DESC="0644"
```

GEN004900: ftpusers file does not contain root

Control Description:

Ensures that the ftpusers file contains the usernames of users not allowed to use FTP, and contains, at a minimum, the system pseudouser's username and root. This control checks that the file specified by the FTPUSERS_FILE parameter contains all the usernames specified in the FTP_USERS parameter.

Control Parameter Details:

Parameter 1: FTP_USERS - This parameter must contain a space-separated list of the usernames that should not be allowed to use the ftp service.

Default Setting: "root daemon bin sys adm uucp guest nobody lpd lp invscout snapp ipsec nuucp"

Parameter 2: FTPUSERS_FILE - This parameter must be the absolute path of the ftpusers file.

Default Setting: /etc/ftpusers

Example Usage Within Custom Parameter File:

```
GEN004900:FTP_USERS="root daemon bin sys adm uucp guest nobody
lpd lp invscout snapp ipsec nuucp";FTPUSERS_FILE=/etc/ftpusers
```

© 2008 by BigFix, Inc.

© 2008 by BigFix, Inc.

AIX 5.2 and AIX 5.3 Parameters

GEN000340: Reserved System Account UIDs

Control Description:

Ensures that uids 0 - 99 (0 - 499 for Linux) are reserved for system accounts.

Control Parameter Details:

Parameter 1: SYSTEM_ACCOUNTS - This Parameter is a space-separated list of user IDs to be considered system accounts. Accounts that are allowed to have UIDs < 100 should be specified in this parameter.

Default Setting: "root daemon bin sys adm uucp guest nobody lpd lp invscout snapp ipsec nuucp"

Example Usage Within Custom Parameter File:

```
GEN000340: SYSTEM_ACCOUNTS="root daemon bin sys adm uucp guest
nobody lpd lp invscout snapp ipsec nuucp"
```

GEN000360: Reserved System Account GIDs

Control Description:

Ensures that gids 0 - 99 (0 - 499 for Linux) are reserved for system accounts.

Control Parameter Details:

Parameter 1: SYSTEM_GROUPS - This parameter is a space-separated list of GIDs to be considered system groups. Accounts that are allowed to have GIDs < 100 should be specified in this parameter.

Default Setting: "system staff bin sys adm uucp mail security cron printq audit ecs perf shutdown lp invscout snapp"

Example Usage Within Custom Parameter File:

```
GEN000360:SYSTEM_GROUPS="system staff bin sys adm uucp mail
security cron printq audit ecs perf shutdown lp invscout
snapp"
```

© 2008 by BigFix, Inc.

GEN000480: Login Delay

Control Description:

Ensures that the logon delay between logon prompts after a failed logon is set to at least four seconds.

Control Parameter Details:

Parameter 1: VALUE - This parameter represents the number of seconds to delay after an unsuccessful login. This equates to the logindelay setting in /etc/security/login.cfg which, if present, sets the number of seconds to wait before the login failure message is printed to the screen.

Default Setting: 4

Example Usage Within Custom Parameter File:

```
GEN000480:SETTING=4
```

GEN000540: Minimum Password Age

Control Description:

Ensures that passwords are not changed more than once a day.

Control Parameter Details:

Parameter 1: VALUE - This parameter represents the minimum number of days before the password may be changed. This corresponds to the minage setting in /etc/security/user.

Default Setting: 1

Example Usage Within Custom Parameter File:

```
GEN000540:SETTING=1
```

© 2008 by BigFix, Inc.

GEN000580: Minimum Password Length

Control Description:

Ensures that all passwords contain a minimum of eight characters.

Control Parameter Details:

Parameter 1: VALUE - This parameter represents the minimum password length. This corresponds to the minlen setting in /etc/security/user.

Default Setting: 8

Example Usage Within Custom Parameter File:

```
GEN000580:SETTING=8
```

GEN000600a: Password Complexity - alphabetic characters

Control Description:

Ensures that passwords include at least two alphabetic characters, one of which must be capitalized.

Control Parameter Details:

Parameter 1: VALUE - This parameter represents the minimum number of alphabetical characters in passwords. This corresponds to the minalpha setting in /etc/security/user.

Default Setting: 2

Example Usage Within Custom Parameter File:

```
GEN000600a: SETTING=2
```

© 2008 by BigFix, Inc.

GEN000620: Password Complexity - numeric characters

Control Description:

Ensures that passwords include at least one numeric character.

Control Parameter Details:

Parameter 1: VALUE - This parameter represents the minimum number of numeric characters required in passwords. This corresponds to the minother setting in /etc/security/user.

Default Setting: 1

Example Usage Within Custom Parameter File:

```
GEN000620:SETTING=1
```

GEN000680: Password Complexity - no consecutive characters

Control Description:

Ensures that passwords contain no consecutive characters.

Control Parameter Details:

Parameter 1: VALUE - This parameter represents the maximum number of consecutive characters allowed in passwords. This corresponds to the maxrepeats setting in /etc/security/user.

Default Setting: 1

Example Usage Within Custom Parameter File:

```
GEN000680:SETTING=3
```

© 2008 by BigFix, Inc.

GEN000700: Maximum Password Age

Control Description:

Ensures that passwords are changed at least every 90 days.

Control Parameter Details:

Parameter 1: VALUE - This parameter represents the maximum number of weeks before a required password change. This corresponds to the maxage setting in /etc/security/user.

Default Setting: 12

Example Usage Within Custom Parameter File:

```
GEN000700:SETTING=12
```

GEN000800: Enforce Password History

Control Description:

Ensures that passwords will not be reused within the last ten changes.

Control Parameter Details:

Parameter 1: VALUE - This parameter represents the maximum number of prior passwords to keep; the maximum allowable value is 50. This corresponds to the histsize setting in /etc/security/user.

Default Setting: 10

Example Usage Within Custom Parameter File:

```
GEN000800:SETTING=10
```

© 2008 by BigFix, Inc.

GEN001180: Network Services Daemon Permissions

Control Description:

Ensures that all daemons have permissions of 755, or more restrictive. This control looks in /usr/bin and /usr/sbin (where system daemons are located) for files that have permissions less restrictive than 0755. Additional files may be specified and specific files may be excluded from this test.

Control Parameter Details:

Parameter 1: EXCLUDEFILES - This parameter may be used to exclude specific files from this test; it must be an space- separated list of the absolute paths of files to be excluded.

Default Setting: ""

Parameter 2: INCLUDEFILES - This parameter allows you to specify files outside of the /usr/bin and /usr/sbin directories to include in this test. It must be a space-separated list of the absolute path of the additional files you wish to include. This value may be null i.e. INCLUDEFILES="".

Default Setting: "/usr/local/apache2/bin/httpd /usr/lib/ssh/sshd"

Parameter 3: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w][-x][-r]-[-x][-r]-[-x]"

Parameter 4: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0755"

Example Usage Within Custom Parameter File:

```
GEN001180:EXCLUDEFILES="";INCLUDEFILES="/usr/local/apache2/bin
/httpd /usr/lib/ssh/sshd";PERMS_REGEX="-[-r][-w][-x][-r]-[-
x][-r]-[-x]";PERMS_DESC="0755"
```

© 2008 by BigFix, Inc.

GEN001200: System Command Permissions

Control Description:

Ensures that all system commands have permissions of 755, or more restrictive. This test looks in INCLUDEDIRS for files that have permissions less restrictive than PERMS_REGEX. Additional directories may be specified and specific files may be excluded from this test.

Control Parameter Details:

Parameter 1: INCLUDEDIRS - This parameter allows you to specify which directories to apply this test to; it must be a space-separated list of directories to search and it must not be null.

Default Setting: "/etc /bin /usr/bin /sbin /usr/sbin /usr/ucb /usr/lbin"

Parameter 2: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0755"

Parameter 3: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w][-x][-r]-[-x][-r]-[-x]"

Parameter 4: EXCLUDEFILES - This parameter allows you to specify specific files to exclude from this test; it must be an egrep regular expression specifying the absolute path of the files to exclude. It may be null i.e. EXCLUDEFILES="^$".

Default Setting: "^$"

Example Usage Within Custom Parameter File:

```
GEN001200:INCLUDEDIRS="/etc /bin /usr/bin /sbin /usr/sbin
/usr/ucb /usr/lbin";PERMS_DESC="0755";PERMS_REGEX="-[-r][-w][-
x][-r]-[-x][-r]-[-x]";EXCLUDEFILES="^$"
```

© 2008 by BigFix, Inc.

GEN001220: System Files - Programs and Directories Ownership

Control Description:

Ensures that the owner of all system files, programs, and directories is a system account.

Control Parameter Details:

Parameter 1: INCLUDEDIRS - This parameter is a space separated list of directories in which to look for system files and programs.

Default Setting: "/etc /bin /usr/bin /sbin /usr/sbin /usr/ucb /usr/lbin"

Parameter 2: ALLOWED - This parameter is a pipe-separated list defining which usernames are considered system accounts.

Default Setting: "root|daemon|bin|sys|adm|uucp|lpd|lp|invscout|snapp|ipsec"

Example Usage Within Custom Parameter File:

```
GEN001220:INCLUDEDIRS="/etc /bin /usr/bin /sbin /usr/sbin
/usr/ucb
/usr/lbin";ALLOWED="root|daemon|bin|sys|adm|uucp|lpd|lp|invsco
ut|snapp|ipsec"
```

GEN001240: System Files - Programs - and Directories Group Ownership

Control Description:

Ensures that the group owner of all system files, programs and directories is a system group.

Control Parameter Details:

Parameter 1: INCLUDEDIRS - This parameter is a space-separated list of directories in which to look for system files and programs.

Default Setting: "/etc /bin /usr/bin /sbin /usr/sbin /usr/ucb"

© 2008 by BigFix, Inc.

Parameter 2: ALLOWED - This parameter is a pipe-separated list defining which group names are considered system groups.

Default Setting:
"system|bin|sys|adm|uucp|mail|security|cron|printq|audit|ecs|perf|shutdown|lp|invscout|snapp|ipsec"

Example Usage Within Custom Parameter File:

```
GEN001240:INCLUDEDIRS="/etc /bin /usr/bin /sbin /usr/sbin
/usr/ucb";ALLOWED="system|bin|sys|adm|uucp|mail|security|cron|
printq|audit|ecs|perf|shutdown|lp|invscout|snapp|ipsec"
```

GEN001260: System Log File Permissions

Control Description:

The SA will ensure all system log files have permissions of 644, or more restrictive. This control looks in the system log files returned by the output of the alog command and the system log files defined in /etc/syslog.conf.

Control Parameter Details:

Parameter 1: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-[-r]--[-r]--"

Parameter 2: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0644"

Example Usage Within Custom Parameter File:

```
GEN001260:PERMS_REGEX="-[-r][-w]-[-r]--[-r]--
";PERMS_DESC="0644"
```

© 2008 by BigFix, Inc.

GEN001280: Manual Page File Permissions

Control Description:

Ensures that all manual page files (i.e., files in the man and cat directories) have permissions of 644, or more restrictive. This control looks in the directory specified by the MANBASE parameter for files with permissions less restrictive than specified in the PERMS_REGEX parameter. It also provides an INCLUDEFILES parameter which allows users to specify additional single files which should be included in this test.

Control Parameter Details:

Parameter 1: MANBASE - This parameter must be a space-separated list of directories to check under, for example MANBASE="/usr/share/man /usr/local/man".

Default Setting: "/usr/share/man"

Parameter 2: INCLUDEFILES - This parameter must be a space-separated list of the absolute path of additional files to include in the test.

Default Setting: ""

Parameter 3: EXCLUDEFILES - This parameter must be space-separated list of the absolute path of files within MANBASE to exclude from this test.

Default Setting: ""

Parameter 4: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-[-r]--[-r]--"

Parameter 5: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0644"

Example Usage Within Custom Parameter File:

```
GEN001280:MANBASE="/usr/share/man";EXCLUDEFILES="";INCLUDEFILE
S="";PERMS_REGEX="-[-r][-w]-[-r]--[-r]--";PERMS_DESC="0644"
```

© 2008 by BigFix, Inc.

GEN001300: Library File Permissions

Control Description:

Ensures that all system library files have permissions of 755, or more restrictive. This control looks in the directories specified in the LIBBASE parameter for files with permissions less restrictive than specified in the PERMS_REGEX parameter. It also provides an INCLUDEFILES parameter which allows users to specify additional single files which should be included in this test.

Control Parameter Details:

Parameter 1: LIBBASE - This parameter must be a space-separated list of directories to check under.

Default Setting: "/lib /usr/lib"

Parameter 2: INCLUDEFILES - This parameter must be a space-separated list of the absolute path of additional files to include in the test.

Default Setting: ""

Parameter 3: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w][-x][-r]-[-x][-r]-[-x]"

Parameter 4: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0755"

Example Usage Within Custom Parameter File:

```
GEN001300:LIBBASE="/usr/lib";INCLUDEFILES="";PERMS_REGEX="-[-
r][-w][-x][-r]-[-x][-r]-[-x]";PERMS_DESC="0755"
```

© 2008 by BigFix, Inc.

GEN001360: NIS/NIS+/yp File Permissions

Control Description:

Ensures that all NIS/NIS+/yp files have permissions of 755, or more restrictive. This control checks the /usr/lib/netsvc/yp and /usr/lib/nis directories for files that have permissions less restrictive than specified by the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w][-x][-r]-[-x][-r]-[-x]"

Parameter 2: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0755"

Example Usage Within Custom Parameter File:

```
GEN001360:PERMS_REGEX="[-d][-r][-w][-x][-r]-[-x][-r]-[-
x]";PERMS_DESC="0755"
```

GEN001580: Run Control Scripts Permissions

Control Description:

Ensures that run control scripts have permissions of 755, or more restrictive. This control looks in /etc/rc* for files with permissions less restrictive than specified in the PERMS_DESC parameter. In addition it provides an INCLUDEFILES parameter that allows you to specify additional files that should be tested.

Control Parameter Details:

Parameter 1: INCLUDEFILES - This parameter allows you to specify additional files to include in this test.

Default Setting: ""

© 2008 by BigFix, Inc.

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w][-x][-r]-[-x][-r]-[-x]"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0755"

Example Usage Within Custom Parameter File:

```
GEN001580:INCLUDEFILES="";PERMS_REGEX="-[-r][-w][-x][-r]-[-
x][-r]-[-x]";PERMS_DESC="0755"
```

GEN001700: Run Control Scripts Execute Programs

Control Description:

Ensures that run control scripts only execute programs owned by a system account or an application default. This control looks in the directories specified by the RC_DIRS parameter and the files specified by the RC_FILES parameter for files that are not owned by either the accounts specified in the SYS_ACCOUNTS parameter or the APP_ACCOUNTS parameter.

Control Parameter Details:

Parameter 1: RC_DIRS - This parameter must be a space-separated list of directories to look in; in addition this list must be preceded and followed by a single character.

Default Setting: ""

Parameter 2: RC_FILES - This parameter must be a space-separated list of files to check. In addition it must be preceded and followed by a single character.

Default Setting: "/etc/rc*"

Parameter 3: SYS_ACCOUNTS - This parameter must be an egrep regular expression that will evaluate to the default system accounts.

Default Setting: ""^root$|^daemon$|^bin$|^sys$|^adm$|^lp$|^uucp$|^ipsec$"

© 2008 by BigFix, Inc.

Parameter 4: APP_ACCOUNTS - This parameter is appended to the SYS_ACCOUNTS parameter to construct an egrep regular expression of all the accounts that may be allowed to own run control scripts. Because the two regular expressions are combined the SYS_ACCOUNTS regular expression must start with a '|' (regular expression alternation) character.

Default Setting: "|^oracle$"

Example Usage Within Custom Parameter File:

```
GEN001700:RC_DIRS="";RC_FILES="/etc/rc*";CONTROL_FILES="/sbin/
rc.boot";SYS_ACCOUNTS="^root$|^daemon$|^bin$|^sys$|^adm$|^lp$|
^uucp$|^ipsec$";APP_ACCOUNTS="|^oracle$"
```

GEN001720: Global Initialization Files Permissions

Control Description:

Ensures that global initialization files have permissions of 644, or more restrictive. This control looks at /etc/.login /etc/profile /etc/bashrc /etc/environment /etc/security/environ and checks if their permissions are less restrictive than specified in the PERMS_REGEX parameter. In addition it provides an INCLUDEFILES parameter for specifying additional files to test, and an EXCLUDEFILES parameter for removing one or more of the default files from the test.

Control Parameter Details:

Parameter 1: EXCLUDEFILES - This parameter must be an egrep regular expression that will evaluate to the files to exclude from the test.

Default Setting: ""

Parameter 2: INCLUDEFILES - This parameter must be a space-separated list of the absolute path of additional files to include in the test.

Default Setting: ""

Parameter 3: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-[-r]--[-r]--"

© 2008 by BigFix, Inc.

Parameter 4: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0644"

Example Usage Within Custom Parameter File:

```
GEN001720:EXCLUDEFILES="";INCLUDEFILES="";PERMS_REGEX="-[-r][-
w]-[-r]--[-r]--";PERMS_DESC="0644"
```

GEN001800: Default/Skeleton Dot Files Permissions

Control Description:

Ensures that all default/skeleton dot files have permissions of 644, or more restrictive. This control checks that the permissions of all files specified by the SKEL_FILES parameter have permissions at least as restrictive as specified in the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: SKEL_FILES - This parameter must be a space-separated list of the absolute paths of the skeleton directory.

Default Setting: "/usr/lib/security/mkuser.default /etc/security/.profile"

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-[-r]--[-r]--"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0644"

Example Usage Within Custom Parameter File:

```
GEN001800:SKEL_FILES="/usr/lib/security/mkuser.default
/etc/security/.profile";PERMS_DESC="0644";PERMS_REGEX="-[-r][-
w]-[-r]--[-r]--"
```

© 2008 by BigFix, Inc.

GEN001880: Local Initialization Files Permissions

Control Description:

Ensures that local initialization files have permissions of 740, or more restrictive. The following files/directories are to be excluded from GEN001880: .dt (a directory, this should have permissions of 755) and .dtprofile (which should also have permissions of 755). This control checks the local initialization files specified in the DOT_FILES parameter for permissions less restrictive than specified in the PERMS_REGEX parameter. It automatically excludes the ~/.dt directory from this test.

Control Parameter Details:

Parameter 1: DOT_FILES - This parameter must be a space-separated list of the local initialization files to check.

Default Setting: ".login .cshrc .logout .profile .bash_profile .bashrc .bash_logout .env .dispatch .emacs .exrc"

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w][-x][-r]-----"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0740"

Example Usage Within Custom Parameter File:

```
GEN001880:DOT_FILES=".login .cshrc .logout .profile
.bash_profile .bashrc .bash_logout .env .dispatch .emacs
.exrc";PERMS_REGEX="-[-r][-w][-x][-r]-----";PERMS_DESC="0740"
```

GEN002240: Device file locations

Control Description:

All device files will be located in the directory trees as installed and designated by the operating system and/or application vendor. This control checks that all device (block and character special) files are located in or under the directories specified by the DEVDIRS parameter. It also provides the EXCLUDEFILES and EXCLUDEDIRS parameters for specifying files and subdirectories of DEVDIRS that should be excluded from this test.

© 2008 by BigFix, Inc.

Control Parameter Details:

Parameter 1: DEVDIRS - This parameter must be a space-separated list of directories to test the files in.

Default Setting: "/dev"

Parameter 2: EXCLUDEFILES - This parameter must be an egrep regular expression of the absolute paths of files to exclude from this test.

Default Setting: ""

Parameter 3: EXCLUDEDIRS - This parameter must be an egrep regular expression of subdirectories of the directories specified in the DEVDIRS parameter to exclude from this test.

Default Setting: ""

Example Usage Within Custom Parameter File:

```
GEN002240:DEVDIRS="/dev";EXCLUDEFILES="";EXCLUDEDIRS=""
```

© 2008 by BigFix, Inc.

GEN002300a: Backup Files Ownership

Control Description:

Ensures that backup devices (e.g., tape and floppy disk device) and files will only be readable and writable by root. This control tests /dev/rmt* and /dev/fd* and ensures that they are owned by root. In addition it provides the EXTRAFILES parameter for specifying additional files.

Control Parameter Details:

Parameter 1: EXTRAFILES - This parameter must be a space-separated list of additional files to include in this test.

Default Setting: ""

Example Usage Within Custom Parameter File:

```
GEN002300a:EXTRAFILES=""
```

GEN002300b: Backup Files Ownership

Control Description:

Ensures that backup devices (e.g., tape and floppy disk device) and files will only be readable and writable by root. This control tests /dev/rmt* and /dev/fd* and ensures that they are group-owned by root. It also provides the EXTRAFILES parameter for specifying additional files.

Control Parameter Details:

Parameter 1: EXTRAFILES - This parameter must be a space-separated list of additional files to include in this test.

Default Setting: ""

Example Usage Within Custom Parameter File:

```
GEN002300b:EXTRAFILES=""
```

© 2008 by BigFix, Inc.

GEN002300c: Backup Files Ownership

Control Description:

Ensures that backup devices (e.g., tape and floppy disk device) and files will only be readable and writable by root. This control tests /dev/rmt* and /dev/fd* and ensures that the permissions only allow write access for the owner. In addition it provides the EXTRAFILES parameter for specifying additional files.

Control Parameter Details:

Parameter 1: EXTRAFILES - This parameter must be a space-separated list of additional files to include in this test.

Default Setting: ""

Example Usage Within Custom Parameter File:

```
GEN002300c:EXTRAFILES=""
```

GEN002320: Audio Device Permissions

Control Description:

Ensures that the audio devices have permissions of 644, or more restrictive. This control ensures that the audio device specified in the CONFIG_FILE parameter has permissions at least as restrictive as specified in the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must specify the absolute path of the audio device file; at this time only a single audio device file is supported.

Default Setting: /dev/paud0

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "[-c][-r][-w]-[-r]--[-r]--"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0644"

© 2008 by BigFix, Inc.

Example Usage Within Custom Parameter File:

```
GEN002320:CONFIG_FILE=/dev/paud0;PERMS_REGEX="[-c][-r][-w]-[-
r]--[-r]--";PERMS_DESC="0644"
```

GEN002340: Audio Device Ownership

Control Description:

Ensures that the owner of audio devices is root. This control checks that the file specified in the CONFIG_FILE parameter is owned by the user specified in the VALUE parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must be the absolute path of the audio device file. At this time only a single file is supported.

Default Setting: /dev/paud0

Parameter 2: VALUE - This parameter must be the user account that should own the file specified in the CONFIG_FILE parameter.

Default Setting: "root"

Example Usage Within Custom Parameter File:

```
GEN002340:CONFIG_FILE=/dev/paud0;VALUE="root"
```

GEN002360: Audio Device Group Ownership

Control Description:

Ensures that the group owner of audio devices is root, sys, or bin. This control checks that the owner of the file specified in the CONFIG_FILE parameter is group-owned by one of the accounts specified in the VALUE parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must be the absolute path of the audio device file. At this time only a single file is supported.

Default Setting: /dev/paud0

© 2008 by BigFix, Inc.

Parameter 2: VALUE - This parameter must be a space-separated list of the group account names that may group-own the file specified in the CONFIG_FILE parameter.

Default Setting: "system sys bin audio"

Example Usage Within Custom Parameter File:

```
GEN002360:CONFIG_FILE=/dev/paud0;VALUE="system sys bin audio"
```

GEN002520: Public Directories Ownership

Control Description:

Ensures that the owner of public directories is root or the application user. This control checks that all world-writable directories with the sticky bit set are owned by a user specified in the VALUE parameter. In addition it provides an EXCLUDEDIRS parameter for excluding specific directories from this test.

Control Parameter Details:

Parameter 1: EXCLUDEDIRS - This parameter must be a space-separated list of directories to exclude from this test.

Default Setting: "/var/spool/samba"

Parameter 2: VALUE - This parameter must be a space-separated list of usernames that may own world-writable directories.

Default Setting: "root bin mail uucp"

Example Usage Within Custom Parameter File:

```
GEN002520:EXCLUDEDIRS="/var/spool/samba"VALUE="root bin mail
uucp"
```

© 2008 by BigFix, Inc.

GEN002540: Public Directories Group Ownership

Control Description:

Ensures that the group owner of public directories is root, sys, bin, or the application group. This control checks that all world-writable directories with the sticky bit set are group-owned by one of the accounts specified in the VALUE parameter. In addition it provides an EXCLUDEDIRS parameter for specifying directories that should be excluded from this test.

Control Parameter Details:

Parameter 1: EXCLUDEDIRS - This parameter must be a space-separated list of directories to exclude from this test.

Default Setting: "/var/spool/samba"

Parameter 2: VALUE - This parameter must be a space-separated list of group account names that should group-own the directories specified above.

Default Setting: "system sys bin mail uucp"

Example Usage Within Custom Parameter File:

```
GEN002540:EXCLUDEDIRS="/var/spool/samba";VALUE="system sys bin
mail uucp"
```

GEN002980: /etc/cron.allow Permissions

Control Description:

Ensures that the cron.allow file has permissions of 600, or more restrictive. This control checks that the file specified by the CONFIG_FILE parameter has permissions at least as restrictive as specified in the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must be the absolute path of the file to check.

Default Setting: /var/adm/cron/cron.allow

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-------"

© 2008 by BigFix, Inc.

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0600"

Example Usage Within Custom Parameter File:

```
GEN002980:CONFIG_FILE=/var/adm/cron/cron.allow;PERMS_REGEX="-
[-r][-w]-------";PERMS_DESC="0600"
```

GEN003060: Default System Accounts and Cron

Control Description:

Ensures that default system accounts (with the possible exception of root) will not be listed in the cron.allow file. If there is only a cron.deny file, the default accounts (with the possible exception of root) will be listed there. This control checks that the system accounts specified by the CRON_SYS_ACCT_USERS parameter are not present in the file specified by the CRON_ALLOW_FILE parameter. If the file specified by the CRON_ALLOW_FILE parameter does not exist, it checks that the accounts are present in the file specified by the CRON_DENY_FILE parameter.

Control Parameter Details:

Parameter 1: CRON_SYS_ACCT_USERS - This parameter must contain a space-separated list of usernames that should not be allowed to use the cron utility.

Default Setting: "daemon bin sys adm uucp guest nobody lpd lp invscout snapp ipsec nuucp"

Parameter 2: CRON_ALLOW_FILE - This parameter must specify the absolute path of the cron.allow file.

Default Setting: /var/adm/cron/cron.allow

Parameter 3: CRON_DENY_FILE - This parameter must specify the absolute path of the cron.deny file.

Default Setting: /var/adm/cron/cron.deny

Example Usage Within Custom Parameter File:

```
GEN003060:CRON_SYS_ACCT_USERS="daemon bin sys adm uucp guest
nobody lpd lp invscout snapp ipsec
nuucp";CRON_ALLOW_FILE=/var/adm/cron/cron.allow;CRON_DENY_FILE
=/var/adm/cron/cron.deny
```

© 2008 by BigFix, Inc.

GEN003080: Crontab files Permissions

Control Description:

Ensures that crontabs have permissions of 600, or more restrictive. This control checks that all files in the directory specified by the CRONTAB_DIR parameter have permissions at least as restrictive as specified in the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CRONTAB_DIR - This parameter must be the directory that the crontab files reside in.

Default Setting: /var/spool/cron/crontabs

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-------"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0600"

Example Usage Within Custom Parameter File:

```
GEN003080:CRONTAB_DIR=/var/spool/cron/crontabs;PERMS_REGEX="-
[-r][-w]-------";PERMS_DESC="0600"
```

© 2008 by BigFix, Inc.

GEN003100a: Cron directory permissions

Control Description:

Ensures that cron and crontab directories have permissions of 755, or more restrictive. This control checks that the permissions of the directory specified in the CONFIG_FILE parameter are at least as restrictive as specified in the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must be the absolute path of the cron directory.

Default Setting: /var/spool/cron

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "d[-r][-w][-x][-r]-[-x][-r]-[-x]"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0755"

Example Usage Within Custom Parameter File:

```
GEN003100a:CONFIG_FILE=/var/spool/cron;PERMS_REGEX="d[-r][-
w][-x][-r]-[-x][-r]-[-x]";PERMS_DESC="0755"
```

GEN003100b: Crontab Directory permissions

Control Description:

Ensures that cron and crontab directories have permissions of 755, or more restrictive. This control checks that the permissions of the directories specified in the CRON_DIRS parameter have permissions at least as restrictive as specified in the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CRON_DIRS - This parameter must be a space-separated list of the absolute paths of the cron and crontab directories.

Default Setting: /var/spool/cron/crontabs

© 2008 by BigFix, Inc.

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "d[-r][-w][-x][-r]-[-x][-r]-[-x]"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0755"

Example Usage Within Custom Parameter File:

```
GEN003100b:CRON_DIRS=/var/spool/cron/crontabs;PERMS_REGEX="d[-
r][-w][-x][-r]-[-x][-r]-[-x]";PERMS_DESC="0755"
```

GEN003180: Cronlog Permissions

Control Description:

Ensures that cron logs have permissions of 600, or more restrictive. This control checks that the file specified in the CONFIG_FILE parameter has permissions at least as restrictive as specified in the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must specify the absolute path of the cron logfile.

Default Setting: /var/adm/cron/log

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-------"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0600"

Example Usage Within Custom Parameter File:

```
GEN003180:CONFIG_FILE=/var/adm/cron/log;PERMS_REGEX="-[-r][-
w]-------";PERMS_DESC="0600"
```

© 2008 by BigFix, Inc.

GEN003200: cron.deny Permissions

Control Description:

Ensures that the cron.deny file has permissions of 600, or more restrictive. This control checks that the file specified by the CONFIG_FILE parameter has permissions at least as restrictive as specified by the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must specify the absolute path of the cron.deny file

Default Setting: /etc/cron.d/cron.deny

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-------"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0600"

Example Usage Within Custom Parameter File:

```
GEN003200:CONFIG_FILE=/var/adm/cron/cron.deny;PERMS_REGEX="-[-
r][-w]-------";PERMS_DESC="0600"
```

© 2008 by BigFix, Inc.

GEN003320: Default System Accounts and At

Control Description:

Ensures that default system accounts (with the possible exception of root) are not listed in the at.allow file. If there is only an at.deny file, the default accounts (with the possible exception of root) will be listed there. This control checks that the usernames specified in the ACCOUNTS parameter are not in the file specified by the AT_ALLOW parameter. If the file specified by the ALLOW parameter does not exist it checks that the usernames are listed in the file specified by the DENY parameter.

Control Parameter Details:

Parameter 1: ACCOUNTS - This parameter must be a space-separated list of usernames that are not allowed to use the at utility.

Default Setting: "daemon bin sys adm uucp guest nobody lpd lp invscout snapp ipsec nuucp"

Parameter 2: DENY - This parameter must specify the absolute path of the at.deny file.

Default Setting: /var/adm/cron/at.deny

Parameter 3: ALLOW - This parameter must specify the absolute path of the at.allow file.

Default Setting: /var/adm/cron/at.allow

Example Usage Within Custom Parameter File:

```
GEN003320:ACCOUNTS="daemon bin sys adm uucp guest nobody lpd
lp invscout snapp ipsec
nuucp";DENY=/var/adm/cron/at.deny;ALLOW=/var/adm/cron/at.allow
```

© 2008 by BigFix, Inc.

GEN003340a: at.allow Permissions

Control Description:

Ensures that the at.allow and at.deny files have permissions of 600, or more restrictive. This control checks that the file specified by the CONFIG_FILE parameter has permissions at least as restrictive as specified by the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must be the absolute path of the at.allow file.

Default Setting: /var/adm/cron/at.allow

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-------"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0600"

Example Usage Within Custom Parameter File:

```
GEN003340a:CONFIG_FILE=/var/adm/cron/at.allow;PERMS_REGEX="-[-
r][-w]-------";PERMS_DESC="0600"
```

GEN003340b: at.deny Permissions

Control Description:

Ensures that the at.allow and at.deny files have permissions of 600, or more restrictive. This control checks that the file specified by the CONFIG_FILE parameter has permissions at least as restrictive as specified by the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must be the absolute path of the at.deny file.

Default Setting: /var/adm/cron/at.deny

© 2008 by BigFix, Inc.

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-------"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0600"

Example Usage Within Custom Parameter File:

```
GEN003340b:CONFIG_FILE=/var/adm/cron/at.deny;PERMS_REGEX="-[-
r][-w]-------";PERMS_DESC="0600"
```

© 2008 by BigFix, Inc.

GEN003780: Services file Permissions

Control Description:

Ensures that the services file has permissions of 644, or more restrictive. This control checks that the permissions of the file specified by the CONFIG_FILE parameter has permissions at least as restrictive as that specified by the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must specify the absolute path of the services file.

Default Setting: /etc/services

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-[-r]--[-r]--"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0644"

Example Usage Within Custom Parameter File:

```
GEN003780:CONFIG_FILE=/etc/services;PERMS_REGEX="-[-r][-w]-[-
r]--[-r]--";PERMS_DESC="0644"
```

GEN004000: traceroute command permissions

Control Description:

Ensures that the traceroute command has permissions of 700, or more restrictive. This control checks that the file specified by the CONFIG_FILE parameter has permissions at least as restrictive as specified by the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must specify the absolute path of the traceroute command.

© 2008 by BigFix, Inc.

Default Setting: /usr/bin/traceroute

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w][-x]------"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0700"

Example Usage Within Custom Parameter File:

```
GEN004000:CONFIG_FILE=/usr/bin/traceroute;PERMS_REGEX="-[-r][-
w][-x]------";PERMS_DESC="0700"
```

GEN004380: aliases file permissions

Control Description:

Ensures that the aliases file has permissions of 644, or more restrictive. This control checks that the file specified by the CONFIG_FILE parameter has permissions at least as restrictive as specified by the PERMS_REGEX parameter.

Control Parameter Details:

Parameter 1: CONFIG_FILE - This parameter must specify the absolute path of the sendmail aliases file.

Default Setting: /etc/mail/aliases

Parameter 2: PERMS_REGEX - This parameter must be an egrep regular expression that matches the canonical file permissions of the maximum allowable file permissions.

Default Setting: "-[-r][-w]-[-r]--[-r]--"

Parameter 3: PERMS_DESC - This parameter must be the octal representation of the maximum allowable file permissions.

Default Setting: "0644"

© 2008 by BigFix, Inc.

Example Usage Within Custom Parameter File:

```
GEN004380:CONFIG_FILE=/etc/mail/aliases;PERMS_REGEX="-[-r][-
w]-[-r]--[-r]--";PERMS_DESC="0644"
```

GEN004900: ftpusers file does not contain root

Control Description:

Ensures that the ftpusers file contains the usernames of users not allowed to use FTP, and contains, at a minimum, the system pseudouser's usernames and root. This control checks that the file specified by the FTPUSERS_FILE parameter contains all the usersnames specified in the FTP_USERS parameter.

Control Parameter Details:

Parameter 1: FTP_USERS - This parameter must contain a space-separated list of the usernames that should not be allowed to use the ftp service.

Default Setting: "root daemon bin sys adm uucp guest nobody lpd lp invscout snapp ipsec nuucp"

Parameter 2: FTPUSERS_FILE - This parameter must be the absolute path of the ftpusers file.

Default Setting: /etc/ftpusers

Example Usage Within Custom Parameter File:

```
GEN004900:FTP_USERS="root daemon bin sys adm uucp guest nobody
lpd lp invscout snapp ipsec nuucp";FTPUSERS_FILE=/etc/ftpusers
```

© 2008 by BigFix, Inc.

Using Regular Expressions to Specify File Permissions

Many of the file permission DISA STIG regulations recommend file permissions of 0755 or more restrictive. SCM for AIX uses **egrep regular expressions** to detect compliance with permission requirements.

You must thoroughly understand egrep regular expressions (especially character classes) before you attempt to customize these controls. Failure to specify a correct value may cause a large number of false positives, false negatives or may prevent the control from functioning at all.

For file permissions, there are three user classes: owner, group and other. For each class, three bits are used to grant permission to read, write or execute a given file. For example, a file permission of 0775 equates to:

- Owner: read, write, execute (111 binary = 7 octal)
- Group: read, execute (101 binary = 5 octal)
- Other: read, execute (101 binary = 5 octal)

This can be represented by nine regular expression character classes, one for each bit in the overall file permission. Regular expressions represent character options in square brackets, so [-r] can stand for either a dash (for zero, or no permission) or an ‘r’ (for read permission). Therefore, the expression below indicates octal 7 (read, write, execute) *or more restrictive:*

```
[-r][-w][-x]
```

While the following expression indicates octal 5 (read, execute) *or more restrictive:*

```
[-r]-[-x]
```

Therefore a file with permissions of 0755 or more restrictive would be expressed as:

```
-[-r][-w][-x][-r]-[-x][-r]-[-x]
```

If you wish to ensure that the file is a **character special file** with permissions of 0755 or more restrictive, the regular expression would be:

```
c[-r][-w][-x][-r]-[-x][-r]-[-x]
```

In addition **absolute** file permissions may also be specified. In this case, a regular file with 0555 (no writing) permissions would be expressed as:

```
-r-xr-xr-x
```

Detection of SUID and SGID files as well as “sticky bit” directories use other methods and are beyond the scope of this document.

NOTE: Setting a custom parameter does not update the Fixlet name or its description.

© 2008 by BigFix, Inc.