2.1.2 Linux Appendix

AS Security Standard
All units must comply with this Security standard

Scope

This Technical Specification provides the security settings and guidance to support the security requirements in ITCS 104 Chapter 1.

Chapter 1 also defines the systems/servers that must use this Technical Specification.

Version/Releases

Version - Release Levels	Last day of vendor support
RedHat Enterprise Linux Ver 3	31 October 2010
RedHat Application Server Ver 3	31 October 2010
RedHat Enterprise Linux Ver 4	29 February 2012
RedHat Application Server Ver 4	29 February 2012
RedHat Enterprise Linux Ver 5	31 March 2014
RedHat Enterprise Server Ver 5	31 March 2014
SuSE SLES 9	31 August 2011
SuSE SLED 10	31 July 2013
SuSE SLES 10	31 July 2013
SuSE SLES 11	31 July 2016
Debian 4	15 February 2010
Debian 5	not yet announced

Business Value

Safeguards IBM's image; security
Information technology security is a vital component of business success and it is especially important for IBM to demonstrate a leadership role in e-business security, including security for emerging on-demand IT services. Adherence to IBM Security standards and guidelines provides end-to-end security for applications and information across multiple hardware and software platforms and networks.

Compliance criteria

Compliance with the control requirements within the Detailed Description section of this document is mandatory and subject to Audit inspection.

- Deviations from the compliance criteria must be documented and approved in accordance with Corporate Instruction Finance 166.

All technical controls within this document are applicable to all Group 1 devices as defined in Chapter 1.

Encryption controls specified in Section 4.1 of this document are applicable to Group 3 and 4 devices as defined in Chapter 1.

Compliance Validation Approach

N/A

Detailed description

Version 8.2 – February 28, 2011

Document History

February 28, 2011

- Scope - Added SLES 11 and Debian 5 to the table
- 6.1 - Added content for rsyslog

1 Identification

1.1 Userids

System value/ parameter	Description	Required setting
UID	Applies to all uid's	Each uid must only be used once

2 Authentication

2.1 Reusable passwords

System value/ parameter	Description	Required setting
PASS_MAX_DAYS	Maximum password age	PASS_MAX_DAYS=90 in /etc/login.defs Field 5 of /etc/shadow must be "90" Note: This setting in /etc/shadow is not required on userids without a password, and on userids that meet the exceptions to password rules criteria below.
PASS_MIN_LEN	Minimum password length	One of these four options must be implemented: • PASS_MIN_LEN=8 in /etc/login.defs. • Parameters of "retry=3 minlen=8 dcredit=-1 ucredit=0 lcredit=-1 ocredit=0 type=" in /etc/pam.d/system-auth to the "password required pam_cracklib.so ..." stanza • parameters of "min=disabled,8,8,8,8 passphrase=0 random=0 enforce=everyone" in /etc/pam.d/system-auth to the "password required pam_passwdqc.so" stanza • Setting "minlen=8" in /etc/security/pam_pwcheck.conf (SuSE 9 and later only) Note: Debian and SuSE 10.x are permitted to use the "include" syntax in lieu of the use of pam_stack.so and the /etc/pam.d/system-auth file. Note: The "type=" parameter to pam_crackllib.so may be omitted if it causes problems. Note: Use of full path and/or $ISA to pam modules is optional.

System value/ parameter	Description	Required setting
Minimum Password Age	The minimum number of days that must elapse between user-initiated password changes	PASS_MIN_DAYS=1 in /etc/login.defs Field 4 of /etc/shadow must be 1 for all userids with a password assigned.
remember parameter to the pam_unix.so module note: May require **touch /etc/security/opasswd** if this file does not already exist.	Prevent reuse of last eight passwords.	RedHat Enterprise Linux/RedHat Application Server (any version): **password $CONTROL pam_unix.so remember=7 use_authtok md5 shadow** • This statement must appear in /etc/pam.d/system-auth, if the file exists. • If /etc/pam.d/system-auth does NOT exist, this statement must appear in /etc/pam.d/login, /etc/pam.d/passwd, /etc/pam.d/sshd and /etc/pam.d/su. Note: $CONTROL in the following examples must be one of "required", or "sufficient". Note: Use of full path and/or $ISA to pam modules is optional. Note: It is acceptable to replace "md5" with "sha512" in the settings above.
		SuSE SLES/SLED 10 and SuSE SLES 9: Option 1 (include both): **password $CONTROL pam_unix2.so md5** **password $CONTROL pam_pwcheck.so remember=8** Option 2: **password $CONTROL pam_unix_passwd.so remember=7 use_authtok md5 shadow** • The statements from Option 1 or Option 2 must appear in /etc/pam.d/common-password, if the file exists. • If /etc/pam.d/common-password does NOT exist, the statements from Option 1 or Option 2 must appear in /etc/pam.d/login, /etc/pam.d/passwd, /etc/pam.d/sshd and /etc/pam.d/su. Additional requirements for SuSE SLES/SLED 10 and SuSE SLES 9: **md5 remember=8** must be in /etc/security/pam_pwcheck.conf **password: md5 shadow** must be in /etc/security/pam_unix2.conf Note: $CONTROL in the following examples must be one of "required", or "sufficient". Note: Use of full path and/or $ISA to pam modules is optional. Note: It is acceptable to replace "md5" with "sha512" in the settings above.

System value/ parameter	Description	Required setting
		Debian 4: **password $CONTROL pam_unix_passwd.so remember=7 use_authtok md5 shadow** • This statement must appear in /etc/pam.d/common-password, if the file exists. • If /etc/pam.d/common-password does NOT exist, this statement must appear in /etc/pam.d/login, /etc/pam.d/passwd, /etc/pam.d/sshd and /etc/pam.d/su. Note: $CONTROL in the following examples must be one of "required", or "sufficient". Note: Use of full path and/or $ISA to pam modules is optional. Note: It is acceptable to replace "md5" with "sha512" in the settings above.
Immediately expire new and manually reset passwords	Force users to change password immediately for a new or reset account unless change was performed by the user or an automated process.	chage -d 0 <userid> Note: This is a process directive and cannot be health checked.

Exemptions to password rules

Option A: User stanzas with the following attributes set are allowed to have non-expiring passwords:

File	Action	How implemented
/etc/passwd	direct or remote login	Value of login shell attribute in /etc/passwd must be /bin/false or /sbin/nologin
/etc/ftpusers or /etc/vsftpd.ftpusers Note: Filename is dependent on which ftp server is installed. Exception: On SuSE SLES 9, the vsftpd server uses /etc/ftpusers as its control file. Note: Only required if ftp is installed and enabled.	Restrict ftp access	Id must exist in file

Option B: Locked userids are allowed to have a non-expiring password:

/etc/shadow	Copy of passwd file containing the encrypted passwords	"!!" or "!" followed by an encrypted password string which indicates a locked account

Option C: Userids configured to have no password may be treated as if they have a non-expiring password:

/etc/shadow	Copy of passwd file containing the encrypted passwords	"x","!", "!!", or "*" specified in the password (2nd) field of the userid.

Option D: User stanzas with the following attributes set are allowed to have a non-expiring password:

/etc/pam.d/system-auth	Rules file used by PAM (Pluggable Authentication Modules) to control system authentication	**auth required /lib/security/$ISA/pam_listfile.so item=user sense=deny file=/etc/security/$FILENAMEonerr=succeed** Note: This entry must precede any entries of type **auth** whose control field is set to the value **sufficient**. Note: The actual filename may vary, but it must be placed in the /etc/security directory and have permissions set to 0640 or more restrictive. Note: Debian and SuSE 10.x are permitted to use the "include" syntax in lieu of the use of pam_stack.so and the /etc/pam.d/system-auth file.
/etc/security/$FILENAME	File containing a list of userids, one per line, that are not allowed to perform an interactive login to the system	Note: The actual filename may vary, but it must be placed in the /etc/security directory and be identical to the filename used in the preceding rule.
/etc/ftpusers or /etc/vsftpd.ftpusers Note: Filename is dependent on which ftp server is installed. Exception: On SuSE SLES 9, the vsftpd server uses /etc/ftpusers as its control file. Note: Only required if ftp is installed and enabled.	Restrict ftp access	Id must exist in file
/etc/ssh/sshd_config	Prevent ssh login from bypassing pam by setting "UsePAM yes" or enabling the AllowGroups directive and not listing any group of which the user is a member.	UsePAM yes Note: If your version of openssh-server does not support the UsePAM directive then you must use the AllowGroups directive and the userid must NOT be a member of any groups listed as parameters to this directive.

Refer to section 5.2 for list of privileged users which can not have a non expiring password.

2.2 Authentication tickets/tokens

Not Applicable

2.3 Passphrases

Not Applicable. Note: cannot support requirement of "provided a minimum number of 5 words each with a minimum length of 4 characters are used." for a passphrase.

3 Authorization

3.1 Business use notice

Required	How implemented
Yes	/etc/motd or /etc/issue

3.2 User Resources

System value/ parameter	Description	Required setting
$HOME	General user's home directory	Default Permissions at time of creation: 700.
Default UMASK	User file creation default protection	umask x77 RedHat: Configured in /etc/bashrc SuSE: Configured in /etc/profile.local Other distributions listed in the Version/Releases table of this tech spec: not required at this time.

4 Information protection & confidentiality

System value/ parameter	Description	Required setting
/etc/passwd	Protection of password files: Contain userid, uid, gid, and other information	Must not contain passwords
/etc/shadow	Protection of password files: Contains userid, encrypted password and other information	File contains encrypted passwords
Anonymous FTP, Process for Receiving Files from Anonymous Users	Files that have been stored into a writeable directory must be examined (checked for IBM Confidential information, checked for inappropriate materials, etc) before being moved to a readable directory.	

4.1 Encryption

IBM's encryption requirements are defined in ITCS104 Chapter 1.2 Authentication, Chapter 1.4 Information Protection and Confidentiality, and Chapter 3 Application Security. This Technical Specification defines encryption facilities that support the basic requirements. If there are no encryption facilities specified, acceptable encryption algorhithms must be used. Other products can be used as long as they meet the Chapter 1.2, 1.4, and 3 requirements.

Encryption type	Encryption facility	Required setting
Native facilities		
Data Transmission	Multiple	All native encryption ciphers may be used, as long as they meet the minimum bit length value specified in ITCS104 Section 1.4.3.
File/Database storage	Multiple; gpg and openssl are two examples	All native encryption ciphers may be used, as long as they meet the minimum bit length value specified in ITCS104 Section 1.4.3.
Storage of passwords	Passwords must be protected with 128-bit encryption	Default setting with use of **md5 shadow** parameters to pam_unix.so in the password stanza as set in /etc/pam.d/passwd or /etc/pam.d/system-auth is sufficient. Note: Any file in /etc/pam.d containing "password required|sufficient (lib/security/$ISA)/pam_unix.so" must carry the md5 shadow options. Note: On SuSE 10 and later use pam_unix2.so or pam_unix_passwd.so Note: On SuSE SLES9/SLES10 the shadow parameter to pam_unix2 is no longer supported but is the default. Note: The **shadow** parameter is not supported on s390 SuSE SLES 9. Note: In SLES 9, **md5** can be globally set in /etc/security/pam_pwcheck.conf and /etc/security/pam_unix2.conf. Note: In SLES 10, **md5** can be globally set by specifying "CRYPT_FILES=md5" in /etc/default/passwd. Note: Debian and SuSE 10.x are permitted to use the "include" syntax in lieu of the use of pam_stack.so and the /etc/pam.d/system-auth file. Note: It is acceptable to replace "md5" with "sha512" in the settings above.
Protection of private keys	Minimum 1024-bit public key	Private key files must be readable and writeable only by the owner.
Add-on product options from IBM (not a comprehensive list or tested)		
File/Database Storage	None available	None available

5 Service integrity & availability

5.1 Operating system resources

Linux OSRs are defined as the following directories and all subdirectories (except as noted) and files that are listed below.

System value/ parameter	Required setting
~root/.rhosts	If the file exists: Read access only by root; write access only by root
~root/.netrc	If the file exists: Read access only by root; write access only by root
/	Settings for other on this directory must be r-x or more restrictive. Note: This particular requirement is not recursive. See entries below for subdirectories that do have recursive requirements for setting for other.

System value/ parameter	Required setting
/usr	Settings for other on this directory must be r-x or more restrictive.
/etc	Settings for other on this directory must be r-x or more restrictive.
/etc/security/opasswd	The file must exist, and File permissions must be set: • rw- --- --- (or more restrictive)
/etc/shadow	File permissions must be set: • rw- --- --- (or more restrictive) Read access is allowed for group if either of the following conditions is satisfied: • The associated group is used only by set-GID operating system programs to avoid a need for root only access privileges. • The associated group has GID <= 99, per section 5.2.
/var	Settings for other on this directory must be r-x or more restrictive. Note: This particular requirement is not recursive. See entries below for subdirectories that do have recursive requirements for setting for other.
/var/log	Settings for other on this directory must be r-x or more restrictive. Note: subdirectories of /var/log may be world writable if and only if the permissions are 1777.
/var/log/faillog	File permissions must be set: • rw- --- --- (or more restrictive)
/var/log/messages	File permissions must be set: • rwx r-x r-x (or more restrictive)
/var/log/wtmp	File permissions must be set: • rwx r-x r-x (or more restrictive)
/var/log/secure or /var/log/auth.log	File permissions must be set: • rwx r-x --- (or more restrictive) Notes: • /var/log/secure is required on all Linux distributions except Debian • /var/log/auth.log is required on Debian Linux
/tmp	Settings for this directory must be rwxrwxrwt(1777). Note: This particular requirement is not recursive.

System value/ parameter	Required setting
snmpd.conf Note: possible locations are the /etc, /etc/snmp, or /etc/snmpd subdirectory	Permissions must be 0640 or more restrictive if the file exists

Exception to OSRs (exempt from OSR requirements)

Files of the following types may be world writeable:	• socket (s) • named pipe (p) • block special file (b) • character special file (c) • symbolic links (l)
For these files: • /var/log/faillog • /var/log/messages • /var/log/wtmp • /var/log/secure • /var/log/auth.log	Write access is allowed for group if either of the following conditions is satisfied: • The associated group is used only by set-GID operating system programs to avoid a need for root only update privileges. • The associated group has GID <= 99, per section 5.2.

5.2 Security & system administrative authority

Userids that are defined as having Security or System Administrative Authority.	• Users with access to the 'root' user account • Userids in groups with gid <= 99

System value/parameter	Description	Required setting
root	Super Userid	If a password is assigned, it must meet password expiration requirements.
		Login access to account must be restricted to the physical console, or to a method that provides accountability to an individual.
Identify and Authenticate Users		Sharing the root password (and accessing it via su) is not considered a technical control for maintaining accountability. Instead, sudo is required to be used as the technical control for accessing the root userid, and any other shared ID's. See the sudo technical specification for specific implementation and health checking requirements.
/etc/pam.d/other	Enforce a default no access policy	auth required pam_deny.so account required /lib/security/pam_deny.so Note: Use of full path and/or $ISA to pam modules is optional.

System value/parameter	Description	Required setting
/etc/ftpusers (or /etc/vsftpd.ftpusers for vsftpd) Exception: On SuSE SLES 9, the vsftpd server uses /etc/ftpusers as its control file.	Restrict ftp access	root Id must exist in file

5.3 Harmful code detection

Not Applicable

5.4 Systematic logon attacks

System value/ parameter	Description	Required setting
loginretries notes: Must precede any lines of same module-type with a control-flag of **sufficient** with the exception of pam_deny.so	Limit consecutive invalid login attempts to 5.	Settings to be used on RedHat AS/ES 5 (and other distributions not listed below): auth required pam_tally.so deny=5 account required pam_tally.so For SLES/SLED 9; RedHat AS/ES 3 & 4: auth required pam_tally.so no_magic_root account required pam_tally.so deny=5 reset no_magic_root For SLES/SLED 10: auth required pam_tally.so deny=5 onerr=fail per_user no_lock_time account required pam_tally.so Notes: • Debian and SuSE 10.x are permitted to use the "include" syntax in lieu of the use of pam_stack.so and the /etc/pam.d/system-auth file. • Note: If /etc/pam.d/system-auth exists, this is the control file. Otherwise, it must appear in all /etc/pam.d control files which require login authentication. • Note: Use of full path and/or $ISA to pam modules is optional.

6 Activity auditing

6.1 System access logging

System value/ parameter	Required setting
Login success or failure	**Requirements for systems that use syslog:** The following requirements cover RedHat, and SuSE. File:/etc/syslog.conf *.info;mail.none;authpriv.none;cron.none /var/log/messages authpriv.* /var/log/secure

System value/ parameter	Required setting
	The following requirements cover Debian Linux: auth,authpriv.* /var/log/auth.log *.*;auth,authpriv.none -/var/log/syslog *.=info;*.=notice;*.=warning; auth,authpriv.none; cron,daemon.none; mail,news.none -/var/log/messages Note: The use of the "-" in "-/var/log/...", which indicates that buffered writes are allowed, is optional in any Linux syslog configuration. Note: More extensive logging is permissible, e.g "cron.none" may be removed from the facility section of the control stanza for /var/log/messages.
	Requirements for systems that use syslog-ng: File:/etc/syslog-ng/syslog-ng.conf filter f_authpriv { facility(authpriv); }; destination authpriv { file("/var/log/secure"); }; source src { internal(); }; log { source(src); filter(f_authpriv); destination(authpriv); }; Note: More extensive logging beyond the minimums listed above is allowed.
	Requirements for systems that use rsyslog: (SuSE Sles 11, Debian 5.x) File:/etc/rsyslog.conf filter f_authpriv { facility(authpriv); }; destination authpriv { file("/var/log/secure;RSYSLOG_TraditionalFileFormat"); }; source src { internal(); }; log { source(src); filter(f_authpriv); destination(authpriv); };
/var/log/messages	Must exist
/var/log/wtmp	Must exist
/var/log/faillog	Must exist Notes: • Updated by pam_tally; see Section 5.4 • May require touch /var/log/faillog if this file does not already exist • If an account is locked when the deny count is reached, it may be reset by the root account with faillog -u <userid> -r
/var/log/secure or /var/log/auth.log	Must exist Notes: • /var/log/secure is required on all Linux distributions except Debian • /var/log/auth.log is required on Debian Linux

7 Assurance

7.1 Health checking

Requirement	Description

Confirm that mandatory access control system options are as specified	Validate:
	• Settings in sections 2.1 and 5.4
	• UMASK setting in section 3.2
	• These rows in section 5.2:
	  • root
	  • /etc/pam.d/other
	  • /etc/ftpusers

Verify that only approved users hold security administrative and system authority	Root and any userids that are members of groups which have gid's less than 99.
Check that all OSR access controls are set	Validate settings in section 5.1 Operating System Resources.
Ensure Harmful code detection programs are installed and operational	Does not apply to Linux at this time
Check that the required access and activity logs exist.	Verify the logs listed in section 6.1 exist.

8 Network settings

System settings	Required setting
Anonymous ftp system settings	
ftpd daemon options	If any directories will be made writable, the **-u 027** option must be used. Note: this is a wu-ftpd specific requirement
Configuration of the ftp account home directory	If it exists and anonymous ftp is enabled, it must be owned by root and grant write access only to the owner
Configuration of the bin subdirectory of the ftp account home directory	If it exists and anonymous ftp is enabled, it must be owned by root and grant write access only to the owner. Files contained in this directory must have a mode of 0111.
Configuration of the lib subdirectory of the ftp account home directory	If it exists and anonymous ftp is enabled, it must be owned by root and grant write access only to the owner. Files contained in this directory must have a mode of 0555.
Configuration of the etc subdirectory of the ftp account home directory	If it exists and anonymous ftp is enabled, it must be owned by root and grant write access only to the owner. If the directory contains a passwd file, the password fields (field 2) must be empty
Configuration of other files and subdirectories within the ftp account home directory	If it exists and anonymous ftp is enabled, it must not be owned by a general user account. If write access is granted to the group owner of the file or directory, membership in the group is a security administrative authority. Files and directories must allow only read/execute, write/execute, execute (directories only), or no access for other,
Directories enabled for Anonymous FTP access	If it exists and anonymous ftp is enabled, READ access via anonymous FTP must not be granted to directories containing classified data.
Access permissions for directories accessible via	If it exists and anonymous ftp is enabled, each directory may allow read access or write access to anonymous users, but not both.

System settings	Required setting
Anonymous FTP	See Section 4 - Information Protection & Confidentiality for additional requirements for anonymous write enabled directories,
Trivial file transfer protocol (tftp) system settings	
tftp access control	The permitted directory must be specified with the -s parameter to server_args.
Directories enabled for TFTP access	Access via TFTP may be granted only to directories containing unclassified data, where the storage of IBM Confidential data is prohibited. This restriction also applies to any subdirectories of the directory.
Network file system (nfs) system settings	
/etc/exports	The file must exist, if NFS server is installed and running, and must be owned by root and have 0644 permissions.
/etc/exports	Directories that are permitted to contain IBM Confidential data may not be exported unless the requirements specified in the next row are met.
Network File System (NFS), Process for Exporting IBM Confidential Data Without Strong Authentication	Access to data classified IBM Confidential may be granted though NFS on an exception basis under the following conditions: • The /etc/exports file must contain a list of hosts and their mount permissions for all directories that may contain IBM Confidential files • A process is established to validate all hosts specified in /etc/exports, at the health checking interval, for all directories that may contain IBM Confidential files. If access to directories that may contain IBM Confidential files is provided to netgroups, the host in the netgroups must be validated at the health checking interval defined for the server. • A process is established to ensure that all hosts specified in /etc/exports, for all directories that may contain IBM Confidential files, share common userids and uid numbers and group and gid number mapping.
Berkeley remote access commands system settings	
/etc/hosts.equiv	Must not be used as an access control mechanism.
/etc/pam.d/rlogin /etc/pam.d/rsh	If the file exists and there is a /lib/security/pam_rhosts_auth.so stanza present, the **no_hosts_equiv** parameter must be present.
Remote execution daemon (rexd) system settings	
rexd daemon	Must be disabled
Net news transfer protocol (nntp) system settings	
NNTP authentication and identification	Must be configured to require authentication and identification of all users if any of the newsgroups on the server are classified IBM Confidential
TCP/IP denial of service prevention	
Must be disabled on all internet servers	CHARGEN, DAYTIME, DISCARD, ECHO, FINGER, SYSTAT, WHO, NETSTAT
Must be disabled if not required to support an application	BOOTPS, CHARGEN, DAYTIME, DISCARD, ECHO, FINGER, NETSTAT, PCNFSD, RSTATD, RUSERD, RWALLD, SPRAYD, TFTP, WHO, CMSD, DTSPCD, TTDBSERVER
SNMP Service	Community name of 'public' and 'private' are not permitted if the SNMP service is active
/etc/sysctl.conf	net.ipv4.tcp_syncookies =1 note: Enable tcp syncookies to prevent syn flooding note: directly supported on Debian. Users of other distributions should add the

System settings	Required setting
	following, as a single line, to a boot startup script: **echo 1 >/proc/sys/net/ipv4/tcp_syncookies**
/etc/sysctl.conf	net.ipv4.icmp_echo_ignore_broadcasts = 1 note: Turn off ICMP broadcasts note: directly supported on Debian. Users of other distributions should add the following, as a single line, to a boot startup script: **echo 1 >/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts**
/etc/sysctl.conf	net.ipv4.conf.all.accept_redirects = 0 note: Disable ICMP Redirect Acceptance note: directly supported on Debian. Users of other distributions should add the following, as a single line, to a boot startup script: **echo 0 >/proc/sys/net/ipv4/conf/all/accept_redirects**
Network information services (nis) settings, including nis+ in nis compatibility mode	
yppasswd daemon	Must be disabled.
NIS maps	Must not be used to store IBM Confidential data, including user passwords or other authentication credentials, in any form. If the NIS passwd maps are used, all encrypted passwords must be removed from the source file before the maps are generated.
Network information services plus (nis+) settings	
NIS+ maps	If IBM Confidential data, including user passwords or other authentication credentials in any form, access may not be granted to the other or unauthenticated permissions class.

Implementation & migration

Migration path
Actions required to achieve compliance with the modifications applied within the version 8.2 publication of this document must be completed by May 31, 2011.

Key dates -
All existing projects/applications must comply by: 05/31/2011
All projects implemented after this date must comply: 05/31/2011
Any project which has not exited the Plan phase by this date must comply: 05/31/2011

Geographic considerations
N/A

Contact: Todd D. (Doug) Inman
Author: Todd D. (Doug) Inman
Content coordinator: Kathleen L. (Kitty) Garcia
Business owner: Linda Betz
Executive owner: Linda Betz
This document was published on 02/28/2011 and is scheduled for review on 08/28/2011