Security Hardening & Its Implications on System Upgrades

Revision History

Summary of Changes			
Date	**Description of Change**	**Rev#**	**Author**
Feb 2018	First edition for publication	1.0	SFT Members

Important Notes	
Date	
Mar 2018	Final version

Table of Contents

Contents

1. Introduction

This whitepaper was prepared for the use and benefit of Teradata customers. It was written by customers, for use by customers.

With the increased need for security to protect company data assets this Security Whitepaper was prepared to help provide a guide for the best practices for Security Hardening of Teradata systems. The paper will focus on the minimum required changes all admins should use when setting up their systems and also provide guidance on what to look for when upgrading a Teradata system.

Note to the reader. *This guide is provided as a courtesy of the Teradata Partners Service Focus Team (SFT). It comes as is; with no implied support. The procedures represent the combined learning of the customer members who contributed to it. The procedures are meant to be high level guides and do not represent step-by-step procedures. They are accurate to the best combined knowledge of the team, but should always be followed with caution and good judgment as they are not guaranteed to be free from flaws.*

2. What is security hardening and why is it important?

Security hardening is defined as the systematic process of identifying potential weaknesses in a system configuration and remediating or mitigating those weaknesses, thereby reducing the overall attack surface and improving the security posture of the system. It is the process of eliminating or reducing security risks to the extent possible without adversely affecting the overall intended functionality of the system, and it is an essential first step in better protecting systems from unauthorized use or unauthorized access to confidential data. Security hardening activities typically includes things such as:

- Securing user accounts (e.g. changing default passwords and disabling unnecessary user accounts)
- Disabling unnecessary services and protocols
- Controlling network access via firewalling
- Tightening up permissions and ownership of critical files and directories
- Logging and auditing of user access
- Configuring systems in accordance with corporate and regulatory security policies, standards and guidelines.

It is important to understand that there is no "one size fits all" approach to security. Teradata systems come pre-configured with sensible defaults designed to fit most customers basic needs, but default configurations tend to favor usability over security. Default configurations may be adequate for protecting non-confidential information, but threat actors stand a much better chance of gaining unauthorized access to a system with default configurations than a system that has been properly evaluated and architected to become more secure. The aim of security hardening is to make it much more difficult for these threat actors to be successful in their pursuits by employing a solid defensive posture. The intension is to thwart their attempts so much so that they go looking for weaker targets, or at least until their activities can be identified and stopped.

As an overarching principle, security hardening should be performed on all servers attached to the network, regardless of whether they store or process protected data. If a system cannot be hardened to a satisfactory minimum level of security then it should not be placed on the network. A threat actor can have many uses for a particularly vulnerable server that is not their direct target, including using it for persistent access back into the environment and as a staging ground for waging further attacks against their intended targets, among other things.

3. Security policies, standards and guidelines - How security hardening helps meet them

Security policies, standards and guidelines are the driving forces behind properly protecting data stored and processed by information technology systems according to its perceived value, and assist in achieving both corporate and regulatory compliance. These are defined as follows:

- **Security policy:** A high-level document that describes the specific requirements or rules that must be met by the organization to achieve corporate or regulatory compliance.
- **Security standard:** A collection of procedures designed to meet the requirements set forth by the security policy. Security standards are typically organized by platform, operating system or application, and include the commands that must be ran and the configurations that must be put in place to meet security policies. They can be thought of as the 'how' of security policies.
- **Security guideline:** Best practices or suggestions that are recommended to help increase the security of a system, but are not necessarily required to comply with security policies.

Security policies, standards and guidelines may be developed internally or taken from organizations such as the National Institute of Standards and Technology (NIST), the Center for Internet Security (CIS), and the International Organization for Standardization (ISO), just to name a few. Security hardening is in effect the application of security standards and guidelines to systems to meet or exceed the requirements defined by security policies. A system that has not been properly evaluated against security policies, standards and guidelines cannot be expected to meet them, and so stepping through the security hardening process is required to ensure systems are adequately protected.

4. The security hardening process

The security hardening process can be broken down into the following four steps:

1. Performing a security assessment to determine what security hardening needs to be done to properly secure the environment in accordance with applicable security policies, standards and guidelines. It should include things such as reviewing vendor documentation for settings that can be used to increase system security and the system configurations themselves.
2. Designing and documenting procedures to implement any required configuration changes as part of security hardening.
3. Implementation of the security hardening procedures on applicable systems.
4. Periodic, documented validation of all security hardened settings, including the research and correction of any settings found not to be in compliance with requirements. These are changes that may have been made due to upgrades, user error and other causes.

It is important to note all too often security is treated like a "do it once and you are done" engagement, when in truth security is a process, not a product, that should never stop being refined. Proper management of risk through security hardening involves going back through these steps at regular intervals to account for both changes in the security policies, standards and guidelines governing what must be done to properly secure the environment as well as changes to the environment (e.g. OS and application upgrades) that may introduce new and potentially insecure or unwanted functionality into the environment.

5. What changes may impact security hardening on Teradata systems at the OS & related application levels?

Once a Teradata system has been hardened the settings should remain in-place indefinitely, but there are several activities where some or all hardened settings will be lost. The following types of upgrades will wipe out most or all security hardening performed at the OS level:

- SUSE Linux Enterprise Server (SLES) moves (e.g. going from SLES 10 to SLES 11) on bare metal servers. See knowledge article KAP19C6C6 via T@YS for the files kept during a SLES move operation.
- Xen virtual machine to kernel-based virtual machine (KVM) migrations on virtualized management servers (VMS). This includes service workstation (SWS) and Viewpoint virtual machines.
- Cabinet management interface controller (CMIC) and VMS upgrades. CMIC's and VMS's are not typically hardened however, as they are architected with mostly read-only file systems that prevent modification.

Service pack upgrades (e.g. going from SLES 11 SP1 to SLES 11 SP3) also have a tendency to wipe out some hardening settings, but not all. This list includes, but is not limited to, the following:

- Unrecognized pluggable authentication modules (PAM) from files within the /etc/pam.d/ directory. See knowledge article KCS005166 via T@YS for more information.
- Aging settings defined in the /etc/login.defs file.
- Default SLES users that have been removed as part of security hardening may be recreated.
- Some file and directory permissions and/or ownership.
- Some disabled services may be re-enabled. Examples include the 'at' daemon and Xwindows Display Manager (XDM).
- Files that are commonly deleted as part of hardening (e.g. the /etc/hosts.equiv file) may be recreated.

See Appendix A for a concise list of all Teradata Standard Hardening (TDSH) settings as applied by the Teradata Center for Enterprise Security team that are kept on SLES moves and wiped out on SLES service pack upgrades.

Typical OS and database patch upgrades generally do not affect security hardening settings, but this all depends on what has been done as part of security hardening in the first place as well as the packages being upgraded. This is especially true of OS level packages (SUSE developed or open source) that are not under Teradata engineering's direct control. Software developers may make any code changes they feel are necessary to support their software, and Teradata does not and could not vet each package individually to determine the changes they could make.
System administrators, database administrators, and support personnel that do not have a firm understanding of what has been done as part of security hardening, and the reasoning behind these changes, can also inadvertently or intentionally make changes detrimental to system security. This can include enabling previously disabled services, enabling new services, installing untested software, changing file and directory ownership and permissions, and modifying configuration files. Oftentimes these changes appear innocuous to the users making them, but sometimes they are intentionally made to make their work easier - all while knowing the possible security implications of such changes.

6. Pre/post-upgrade considerations

As discussed in the previous section, some types of system upgrades are generally known to revert or wipe out security hardening settings. Before performing system upgrades that are known to impact security hardening you should, at minimum:

- Backup all critical files and files that have been modified or created as part of security hardening (e.g. configuration files, certificate files and private keys, and Java keystores) that would take significant time and effort to reproduce. While they may not be directly transferable into the upgraded environment, they can at least be compared against to ensure all previously implemented security hardening gets re-implemented. This also lessens the time taken in re-hardening overall.
- Maintain a standard of all security hardening procedures implemented for use in re-hardening and validating the upgraded environment.

Other questions to ask before performing system upgrades could include:

- What is being done that may adversely affect system security?
- What is the minimum access needed to perform the upgrades, and what else unrelated to the upgrades does it give the implementer access to? In some situations, it may be necessary to monitor the implementer to ensure they do not abuse the access they have been granted.
- If a new application is being installed, does it include default passwords that need to be changed or unnecessary, potentially insecure functionality that needs to be disabled? Application upgrades could also introduce unneeded new functionality into the environment.
- Is a reboot or application restart required? Application restarts typically do not adversely affect system security, but a server reboot stands more chance of doing so. For example, a

service that has been shut down, but not disabled (e.g. via chkconfig at the OS level), may once again be started on a reboot. As a best practice, all services critical to system security (e.g. anti-virus services, auditing and monitoring services, intrusion detection services, and firewall services) should also be checked following a server reboot to ensure they are functioning properly.

- For extremely secure environments, what is the risk of an attack against the system being successful during the time it may be most vulnerable, and what precautions should be taken to mitigate those risks (e.g. temporarily disconnecting servers being upgraded from the network and performing the upgrades on site)?

Post-upgrade, all previously implemented security hardening changes should be verified and re-implemented where necessary. This is typically accomplished through scripted processes or by manually verifying each security hardening change. However, the Teradata personnel performing an upgrade should never perform any security hardening validations following the upgrade. Teradata personnel that perform upgrades typically will not have a firm understanding of all the security hardening that has been done in the first place, but more to the point this would represent a conflict of interests. Customers or a trusted, disinterested 3rd party should always perform all security hardening validations.

7. Minimum security hardening steps all customers should implement

The following list represents the absolute minimum-security hardening steps that should be taken on all Teradata systems, in the order given:

- Configure default user aging settings in the /etc/login.defs file for newly created user accounts, in accordance with applicable security policies.
- Configure password length, complexity and history requirements in accordance with applicable security policies. This includes both at the OS level via PAM's in the files within the /etc/pam.d/ directory, and at the application and database levels, where possible.
- Create unprivileged user accounts that will be used by system administrators and Teradata support personnel. These user accounts should be given only those privileges necessary to perform their primary job functions.
- Change all default passwords. This includes:
    - OS user passwords, notably the root user. A list of all user accounts with passwords set can be obtained by running the command "`passwd -Sa | grep -E '(P|PS)'`" as the root user.
    - Application user passwords (e.g. the 'admin' user password on Viewpoint, and the 'root' or 'tdadmin' user password in the server management web client (SMweb))
    - Database passwords (e.g. dbc and systemfe)
- Lock out direct root logins over SSH (at least password based to prevent brute force login attempts), forcing users to authenticate using an unprivileged user account first.

8. Additional security best practices

Security hardening is just one part of a defense in-depth strategy to securing systems and data. Additional best practices include:

- Vulnerability scanning (both port and credentialed) using a widely available security vulnerability scanner is recommended to aid in identifying potential security vulnerabilities.
- Penetration testing, when performed by qualified analysts well versed in threat actor tools and methods, can also help determine previously unknown avenues of attack.
- Regularly scheduled patching, which is recommended to be performed quarterly at minimum, will remediate security vulnerabilities that cannot be corrected through configuration changes. In fact, patching systems on a regular basis is arguably the lowest cost and most effective method of preventing security breaches. Customers are highly encouraged to work with their support teams to develop effective patch management strategies to keep systems updated and as security vulnerability free as possible.

9. References and further reading

The following resources may also be helpful:

- SANS Institute information security policy templates, useful for getting started in creating security policies, standards and guidelines: https://www.sans.org/security-resources/policies
- NIST Risk Management Framework (RMF), used by many government organizations to assess risks, and select and implement security controls to reduce or avoid them: https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-(RMF)-Overview
- CIS benchmarks, which are hardening standards for a variety of popular applications and operating systems: https://www.cisecurity.org/cis-benchmarks/
- The Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG), a publicly accessible resource for hardening standards used to secure U.S. Department of Defense systems to a minimum level: https://iase.disa.mil/stigs/Pages/index.aspx
- Teradata knowledge article resources accessible via T@YS:
  - KAC142D7E, Monthly security vulnerability patch summaries. A monthly rollup of all the security patches released during the previous month.
  - KAP19C6C6, What system files are copied/preserved during a SLES9 to SLES10 or a SLES10 SP3 to SLES11 move operation?

- KAP314CCBE, Can I perform security hardening on a Teradata Hadoop Appliance Cluster?
- KAP1A58F6, What is Teradata's process for dealing with security vulnerabilities in the Linux environment?
- KCS005166, A SLES upgrade or SLES move causes user authentication (PAM) failures due to third-party PAM modules being removed.

10. Closing

The SFT is a committee of the PARTNERS User Group that works closely with Teradata on issues related to support services and other areas that fall beyond the scope of product enhancements. Members represent the concerns of Teradata customers by serving as catalysts for service improvements, providing ongoing feedback to Teradata and the PARTNERS Steering Committee.

The members of the SFT sincerely hope that you found this document useful. Please let us know of any comments or suggestions you may have. See you at Partners!

You can find our contact information and more about the SFT at our website:

http://www.teradata-partners.com/About/ServiceFocusTeam

11. Appendix A. Teradata Standard Hardening (TDSH) Settings Kept or Removed by Upgrades

The following lists represent the TDSH version 1.2.0 settings kept on SLES moves or removed/reverted by SLES service pack upgrades, organized by TDSH procedure number. These lists were verified using a SLES move from SLES 11 SP3 to SLES 12 SP2 on a generic node type, and a SLES service pack upgrade from SLES 11 SP1 to SLES 11 SP3 on a generic node type.

Note these lists are subject to change per SuSE and Teradata Engineering code changes, and TDSH procedural changes as developed by the Teradata Center for Enterprise Security team. Results may also be different depending on the node type (e.g. Teradata database node, Hadoop node, Aster node, Viewpoint, etc…) being upgraded. Customers are recommended to verify all security hardening settings following any upgrade operations as a best practice, not just the settings listed below.

a. SLES Moves - Settings Kept

- **1.1.50 Configure /etc/permissions.local:** /etc/permissions.local file copied without modification. Run 'chkstat --set /etc/permissions.local' as root to reapply permissions and ownership hardening settings as applicable. Reapplying the permissions will cover TDSH procedures 1.1.1 through 1.1.33, 1.1.38 and 1.1.39, except for removing /etc/at.deny and /etc/cron.deny as part of TDSH procedures 1.1.3 and 1.1.4.
- **2.3.2 Enable FIPS 180-4 Compliant Cryptographic Module for Password Hashes:** Local Linux user accounts from /etc/passwd and passwords from /etc/shadow are copied without modification. However, the hash algorithm used to encrypt Linux user passwords is set to the SLES default (blowfish for SLES 11, SHA-512 for SLES 12)
- **2.3.3 Set User Password Expiration Days, 2.3.4 Set Password Change Minimum Number of Days, and 2.3.5 Set Password Warning Number of Days:** Aging settings assigned to individual Linux user accounts will be retained, but the 'PASS_MAX_DAYS', 'PASS_MIN_DAYS' and 'PASS_WARN_DAYS' variables in the /etc/login.defs file will be set to default values of 99999 (never expire), 0, and 7, respectfully.
- **2.3.6 Lock Inactive User Accounts after XX Days:** Inactive days settings assigned to individual Linux user accounts will be retained, but the 'INACTIVE' variable in the /etc/default/useradd file will be set to the default value of -1 (never inactive).
- **2.3.13 Configure Network Time Protocol (NTP):** NTPD configuration file /etc/ntp.conf copied without modification.
- **2.3.15 Set Warning Banners for Standard Login Services:** Message of the day file /etc/motd copied without modification.
- **2.3.24 Verify Permissions & Validity on root user Home Directory:** The /root directory is recreated with root user and root group ownership, and 700 permissions by default.
- **2.3.26 Verify Permissions of User Home Directories and Initialization Files and 2.3.27 Verify Ownership of User Home Directories and Initialization Files:** Subdirectories of

/home are copied without modification, including file & directory permissions and ownership.

- **2.3.34 Verify 'No Execute' (NX) Bit is Enabled:** The NX bit is enabled or disabled from within BIOS. A SLES move should not affect this setting.
- **3.1.16 Verify Network File System (NFS) Servers are Secure if Used:** NFS exports configuration file /etc/exports copied without modification.
- **4.1.12 Verify No IPv4 or IPv6 Tunnels Exist:** No IP tunnels will be created as part of a SLES move, nor will any pre-existing IP tunnels be recreated after the SLES move.

b. Service Pack Upgrades - Settings Removed/Reverted

- **1.1.3 Verify Permissions and User/Group Ownership on /etc/at.allow & Remove /etc/at.deny:** The /etc/at.deny file is recreated.
- **1.1.4 Verify Permissions and User/Group Ownership on /etc/cron.allow & Remove /etc/cron.deny:** The /etc/cron.deny file is recreated.
- **1.1.34 Verify Permissions and User/Group Ownership on /var/log/:** The /var/log directory is reverted from 750 permissions to 755 permissions. The /var/log/lastlog and /var/log/wtmp files are reverted from 640 to 644 and 664 permissions, respectfully.
- **1.1.37 Verify Permissions and User/Group Ownership on Skeleton Files in /etc/skel/:** All user environment initialization files (e.g. .bashrc, .profile, .vimrc, etc...) within the /etc/skel directory are reverted from 640 to 644 permissions. The /etc/skel/.xinitrc.template file is also reverted from 750 to 755 permissions.
- **1.1.40 Verify Permissions and User/Group Ownership on xinetd Files and Directories:** All Xinetd service configuration files within the /etc/xinetd.d directory are reverted from 640 to 644 permissions.
- **2.2.2 Configure User Account Locking for Failed Password Attempts:** The pam_tally2.so PAM, used to lock user accounts after a defined number of failed logins, is removed from the /etc/pam.d/common-auth-pc and /etc/pam.d/common-account-pc files.
- **2.2.3 Configure Password Complexity Requirements:** The 'use_authtok' option to the pam_pwhistory.so PAM is removed from the line in the /etc/pam.d/common-password-pc file.
- **2.2.5 Restrict Access to the 'su' Command:** The pam_wheel.so PAM that controls what users may su to the root account is removed from the /etc/pam.d/su and /etc/pam.d/su-l files.
- **2.3.1 Remove Unnecessary User Accounts:** The 'ftp', 'games' and 'news' Linux user accounts are recreated.
- **2.3.3 Set User Password Expiration Days, 2.3.4 Set Password Change Minimum Number of Days, and 2.3.5 Set Password Warning Number of Days:** The 'PASS_MAX_DAYS', 'PASS_MIN_DAYS' and 'PASS_WARN_DAYS' variables in the /etc/login.defs file will be reverted from customer defined values to default values of 99999 (never expire), 0, and 7, respectfully. User accounts that are recreated as noted in 2.3.1 above are created with -1 maximum (never expire), minimum (no minimum) and warning (never warn) days settings.
- **2.3.8 Set Default umask for Users:** The 'UMASK' variable in the /etc/login.defs file is reverted from a value of 027 or 077 to 022. The 'umask' variable settings in the /usr/lib64/sa/sa1 and /usr/lib64/sa/sa2 files are reverted from 0027 or 0077 to 0022.

- **2.3.11 Set Login Failure Delay:** The 'FAIL_DELAY' variable will be reverted from a value of 4 to 3.
- **2.3.25 Verify Users are Assigned Valid and Existent Home Directories:** The 'news' user account will be created, but the /etc/news home directory will not be created.
- **3.1.20 Verify Xwindows Only Enabled Where Necessary:** The X Display Manager (XDM) service will be enabled on servers where it was previously disabled. However, the service will not be started unless the server is started in runlevel 5 (multi-user mode with networking and graphical interface).

The following procedures must be implemented following a SLES 11 SP1 to SLES 11 SP3 upgrade. These procedures did not apply or applied differently in SLES 11 SP1:

- **2.1.6 Set FIPS 140-2 Compliant Cryptographic Modules & MACs:** The following MACs are now usable in the OpenSSH configuration file /etc/ssh/sshd_config in addition to hmac-sha1: hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512,hmac-sha2-256,hmac-sha1-etm@openssh.com
- **2.3.8 Set Default umask for Users:** A 'UMASK' variable can now be set in the /etc/default/useradd file.
- **3.1.19 Verify Unused Protocols are Disabled:** The RDS and TIPC kernel modules can be added to the /etc/modprobe.conf.local file to disable them. These kernel modules were previously either included in the kernel itself (thus, they could not be disabled via modprobe), or not included in the kernel itself and not included as loadable kernel modules.